2018년 한국정보보호학회 하계학술대회

CISC-S'18

Conference on Information Security and Cryptography 2018 Summer

2018. 6. 21일(목) ~ 6. 22일(금)

동신대학교 중앙도서관 1층 동강홀(전남 나주시)



> 주 최 : 한국정보보호학회

> 주 관 : 동신대학교

> 후 원 : 국가정보원, 네이버, 교육부, 한국연구재단, 한국전력공사, 전력거래소, 한국인터넷진흥원, 국가보안기술연구소, 한전KPS(주), 한전KDN(주), 한국방송통신전파진흥원

한국정보보호학회

Korea Institute of Information Security & Cryptology

초대의 글

신록의 계절 6월을 맞이하여 회원님들의 건승과 학술적인 발전을 기원 드립니다. 이번 학술대회는 회원님들의 참여와 관심으로 많은 논문이 모집되었습니다. 이에 감사드리며, 회원님들의 학술적 가치와 노고가 결실을 맺는 자리가 한국정보보호학회 하계학술대회 (CISC-S'18) 임을 새삼 깨닫게 되어 기쁘게 생각합니다. 이번 하계학술대회는 접수된 논문 중 100편의 논문 채택되어 23개의 구두발표 세션으로 나뉘어 발표될 예정입니다.

정보통신 기술과 인공지능의 융합으로 정보통신분야에도 많은 변화를 가져왔고, 인터넷 은행 허가와 암호화폐 활성화로 인한 금융보안이 요구되는 한 해입니다. 금융보안에서는 암호화폐 환경에서 발생하는 보안 위협에 대한 분석 및 블록체인 기술을 이용한 인증 방안에 대한 논의가 활성화되고 있고 이를 반영하듯 이번 학술대회에서는 암호화폐 및 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 동신대학교 당국과 재정적으로 후원해 주신 회원사와 후원 및 협찬 기관들에게 심심한 감사를 드립니다. 또한 이번 하계학술대회 준비를 위해서 수고해 주신 동신대 이동휘 운영위원장님과 고려대 김승주 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.

2018. 6. 21

한국정보보호학회 회장 **홍 만 표**

조직도

학술대회장

한국정보보호학회 학회장 홍만표

운영위원회

운영위원장	이동휘	동신대학교		
운영위원	강승호	동신대학교	박원형	극동대학교
	강지원	세종대학교	서정택	순천향대학교
	김민수	목포대학교	오진수	전력거래소
	김점구	남서울대학교	유승재	중부대학교
	김종선	한국전력공사	이영숙	호원대학교
	김태희	동신대학교	이형효	원광대학교
	김홍기	동신대학교	장항배	중앙대학교
	박남제	제주대학교	홍득조	전북대학교

프로그램위원회

프로그램위원장	김승주	고려대학교		
프로그램위원	곽 진	아주대학교	이경현	부경대학교
	김광조	카이스트	이동훈	서고려대학교
	김윤정	서울여자대학교	이만희	한남대학교
	김인석	고려대학교	이옥연	국민대학교
	김형식	성균관대학교	이임영	순천향대학교
	류재철	충남대학교	임율규	한양대학교
	박창섭	단국대학교	장항배	중앙대학교
	서승현	한양대학교	조은선	충남대학교
	서정택	순천향대학교	최대선	공주대학교
	신상욱	부경대학교	최형기	성균관대학교
	영흥열	순천향대학교	하재철	호서대학교
	오희국	한양대학교	한동국	국민대학교
	유일선	순천향대학교	허준범	고려대학교
	윤지원	고려대학교		

프로그램 일정표

날짜	시간	행사내용								비 고
6월 21일 (목)	11:30 ~ 13:00	등록 및 리셉션 (중앙도서관 1층)								
	13:00 ~ 14:20	세션 A – 정보전산센터								
		암호화폐/ 블록체인1 좌장:허준범 (고려대학교)	네트워크1 좌장:최대선 (공주대학교)	암호이론1 좌장:한동국 (국민대학교)	IoT보안1 좌장:강승호 (동신대학교)	관리정책 교육1 좌장:김태희 (동신대학교)	컴퓨터보안1 좌장:이만희 (한남대학교)	개인정보보호 좌장:신상욱 (부경대학교)	CPS보안 좌장:서정택 (순천향대학교)	
	14:20 ~ 14:30	Break Time								
	14:30 ~ 16:10	세션 B – 정보전산센터								
		암호화폐/ 블록체인2 좌장:임을규 (한양대학교)	네트워크2 좌장:김광조 (카이스트)	암호이론2 좌장:이동훈 (고려대학교)	IoT보안2 좌장:이임영 (순천향대학교)	관리정책 교육2 좌장:이경현 (부경대학교)	취약점분석 좌장:박창섭 (단국대학교)	산업보안 좌장:오희국 (한양대학교)	악성코드 좌장:하재철 (호서대학교)	
	16:10 ~ 16:20	Break Time								
	16:20 ~ 16:50	중앙도서관 1층 동강홀	초청강연 : Post Quantum Crypto 표준화 추진 현황 및 KISA의 역할(한국인터넷진흥원)							
	16:50 ~ 17:00		특별강연 : 연구 윤리 및 출판							
	17:00 ~ 17:30		**개회식 /** 사회 : 운영위원장 **이동휘** 교수							
			개회사 동신대학교 **김필식** 총장 환영사 한국정보보호학회 **홍만표** 학회장 축 사 한국인터넷진흥원 **김석환** 원장 국가보안기술연구소 **조현숙** 소장 한국전력공사 **김종갑** 사장				우수논문 시상식 **행안부 장관상, 한국인터넷진흥원장상, 한국전력공사사장상, 한국전자통신연구원장상, 국가구보안연구소장상, 학회장상(암호분야 특별상), 학회장상, 여성과학자상**			
			경품추천							
	17:30 ~ 18:00	이동								
	18:00 ~ 20:00	만찬 : 빛가람 호텔 만찬홀 (구:M-STAY Hotel) : 사회 서정택 교수								
6월 22일 (금)	10:00 ~ 10:30	등록 (정보전산센터 1층)								
	10:30 ~ 11:50	세션 C – 정보전산센터								
		암호화폐/ 블록체인3 좌장:유일선 (순천향대학교)	암호화폐/ 블록체인4 좌장:현상원 (조선대학교)	관리정책 교육3 좌장:김인석 (고려대학교)	관리정책 교육4 좌장:장항배 (중앙대학교)	컴퓨터보안2 좌장:서승현 (한양대학교)	여성과학자 + invited talk 좌장:심미나 (성결대학교)	기 타 좌장:이옥연 (국민대학교)		26개 논문 한국전력 공사 견학
	12:00 ~ 13:00	중식(교직원식당)								중식 (한전구내식당)
	13:00 ~ 14:30									한국전력거래소 견학
	14:30 ~ 16:00									한국인터넷 진흥원 견학
	16:00 ~ 16:30	KTX, SRT 나주역 이동 후 종료								

우수논문상

시상내역	논문 저자	논문 제목
장 관 상	홍기섭	S7CommPlus 제어 프로토콜 통신 보안 위협을 통한 기계학습 기반 이상징후 탐지 방안 연구
KISA 원장상	오윤석, 김애영, 서승현	탈취대응을 위한 상황인지 기반 드론 제어 메커니즘 설계
한국전력공사사장상	지우중, 김형식	무인 복합 출력기 솔루션의 취약성 분석(Security Vulnerability Analysis for Printer Kiosks)
ETRI 원장상	류권상, 옥도민, 최대선	스마트 시계 활용 무자각 지속 인증 강화 연구
정보보호학회장상 (암호분야 특별상)	안형철, 김광조	블록체인 기반 분산형 키 관리 시스템의 설계
정보보호학회장상	오진혁, 한주홍, 양광열, 이옥연	스마트 가로등 환경에서의 보안 설계 및 실험
NSR 소장상	이수연, 정형근, 조은선	스마트 계약 언어에서 함수 호출의 안전성 향상을 위한 코드 재작성 기법
여성과학자상	이선우, 이동훈	ECG를 이용한 인증 시스템에 대한 원격 공격 가능성 분석
여성과학자상	김미연, 염흥열	블록체인 기반 개인정보 처리 추적 관리 시스템 모델 제안
여성과학자상	장혜린, 박문찬, 진홍주, 이동훈	C++의 동적 디스패치에 적용된 제어 흐름 무결성 검증기법 분석



구두 발표 세션 A

6월 21일(목) 13:00-14:20 **정보전산센터**

208호	발표 논문
암호화폐/ 블록체인 1	블록체인 기반 분산형 키 관리 시스템의 설계 안형철, 김광조
	분기로 발생된 미확인 트랜잭션의 우선적인 처리기법 박승윤, 오희국
	블록체인 기반 디지털증거 해시 관리 시스템 구현 정재완
	암호화폐 키 관리에 의한 보안 사고 및 대응방안 연구 김근영, 박준후, 오원찬, 류재철
좌장: **허준범** 교수 (고려대학교)	

303호	발표 논문
네트워크 1	스마트 계약 언어에서 함수 호출의 안전성 향상을 위한 코드 재작성 기법 이수연, 정형근, 조은선
	6LoWPAN Neighbor Discovery 주소 등록 분석 및 취약점 평가 한상우, 박창섭
	웹 크롤링을 이용한 교통정보 수집 기법 박세진, 윤지원
	ZigBee 프로토콜에서의 향상된 인증 방안에 관한 연구 조정석, 곽진
좌장: **최대선** 교수 (공주대학교)	

304호	발표 논문
암호이론 1	진난수생성기에 대한 부채널 공격 및 난수성 분석 사례 조사 최낙준, 이지은, 김광조
	중첩된 무한 해시체인을 이용한 Lamport OTP 확장 신동진, 박창섭
	Linux OS 상에서의 커널 및 응용 LEA 암호모듈 구현 및 호출 분석 송행권
	Survey of Functional Encryption and its Functionality 윤현도, 권현수, 허준범
좌장: **한동국** 교수 (국민대학교)	

305호	발표 논문
IoT보안 1	스마트 시계 활용 무자각 지속 인증 강화 연구 류권상, 옥도민, 최대선
	라즈베리 파이를 이용한 휴대용 영상감시시스템 개발 최경호, 김현진, 현부영, 김종민, 이동휘
	LR Guard : ARM TrustZone을 활용한 제어 흐름 보호 기법 설계 진홍주, 장혜린, 이동
	IoT 기반의 스마트 홈 보안 동향 박정인, 이가연, 윤현경, 염흥열
좌장: **강승호** 교수 (동신대학교)	

306호	발표 논문
관리정책 교육 1	악성코드 감염 예방을 위한 보안정책 수립사례 분석 이준희
	4차 산업혁명 환경에서 Trust Service 제공을 위한 사회과학적 정보보호 기반조성 연구 박상호, 나원철, 장항배
	VR과 IoT를 활용한 전공탐색 기반의 대학 홍보전략 최경호, 김병석, 전영재, 진용기, 이동휘
좌장: **김태희** 교수 (동신대학교)	

307호	발표 논문
컴퓨터보안 1	안드로이드 클립보드를 활용한 악의적 e-mail 탐지 기술 이효진, 장수인
	기호실행을 이용한 바이너리 난독화 해제 기술 연구 주하종, 김민재, 염흥열
	Shannon 엔트로피 값 분석을 통한 파일 암호화 판별에 관한 연구 고주성, 곽진
	모바일에서의 애플리케이션 접근 제어 메커니즘 분석 김이진, 최형기
좌장: **이만희** 교수 (한남대학교)	

B01-B호	발표 논문
개인정보보호	모바일 앱 개인정보 유출과 최신 TLS 적용 필요성 연구 김성진, 허준범
	양자 컴퓨팅 환경에 안전한 생체 인증 우주, 이동
	개인정보의 비식별 처리 시 발생가능한 문제점 분석 및 대응방안 제시 한경수, 류지민, 서정택
	Mixnet 적용을 통한 자율주행차 운영환경 프라이버시 보호방안 연구 강기완, 서정택
좌장: **신상욱** 교수 (부경대학교)	

B06-B호	발표 논문
CPS보안	스마트 가로등 환경에서의 보안 설계 및 실험 오진혁, 한주홍, 양광열, 이옥연
	스마트시티 서비스에 대한 사이버공격 피해사례 및 파급효과 분석 김호, 박영 , 백인홍, 신바야르, 서정택
	안전한 스마트공장 연계를 위한 크로스 도메인 보안 방법 김기현, 박혜용, 안혜선, 김일용, 하재철
	국내 스마트시티 인프라 사이버보안 취약점 분석 및 대응방안 제시 이성원, 송진우, 서정택
좌장: **서정택** 교수 (순천향대학교)	

구두 발표 세션 B

6월 21일(목) 14:30-16:10 **정보전산센터**

208호	발표 논문
암호화폐/블록체인 2	블록체인 기반의 차량 평판 시스템 안전성에 관한 연구 이경모, 이경현
	블록체인 모델에 대한 고찰 김혜빈, 박지선, 김종규, 신상욱
	P2P 스토리지를 이용한 블록체인 기반의 EHR 관리 시스템 김현우, 이경현
	블록체인을 기반의 안전한 전자투표 시스템에 관한 연구 노창현, 이임영
	A Blockchain Based On Data Provenance in Healthcare Domain Kweka Bruno Joachim, 이경현
좌장: **임을규** 교수 (한양대학교)	

303호	발표 논문
네트워크 2	5G HetNet 환경을 지원하기 위한 MIH(Media Independent Handover) 기반의 고속의 안전한 핸드오버 인증기법 연구 김지윤, 권순현, 유일선
	OAuth 2.0 인증 프로토콜의 취약점에 대한 대응방안 제시 서동화, 윤가헌, 오장욱, 서정택
	1Kbps 미만 무선 통신 센서 네트워크에서의 개체 인증 및 키 관리 김현기, 이옥연
	CAN 내부 취약점에 대한 분석 및 신규 대응방안 연구 김장 , 한경수, 최홍석, 서정택
	데이터 플레인 가속화 기술을 안전하게 적용하기 위한 상용 IPsec 분석 최준태, 류승호, 박승윤, 사미 울라, 오희국
좌장: **김광조** 교수 (카이스트)	

304호	발표 논문
암호이론 2	격자 암호를 위한 HNF (Hermite Normal Form) 구현 방안 분석 윤혜민, 임성희, 김윤정
	경량 블록 암호 SPECK에 대한 데이터 마스킹 기법 설계 및 구현 권홍필, 하재철
	양자 알고리즘 연구 동향 김 기, 이동
	부채널 분석 공격에 대응하는 SIMON 암호 구현을 위한 마스킹 기법 제안 권홍필, 하재철
	부채널 분석에 안전한 스칼라 곱셈 알고리즘에 대한 단일 파형 비밀 키 비트 종속 공격 심보연, 강준기, 한동국
좌장: **이동훈** 교수 (고려대학교)	

305호	발표 논문
IoT보안 2	탈취대응을 위한 상황인지 기반 드론 제어 메커니즘 설계 오윤석, 김애영, 서승현
	CCTV 환경에서의 속성기반 프록시 재암호화를 사용한 영상데이터 접근제어 기술 연구 황용운, 이임영
	스마트 축사 모니터링 시스템 박환, 박용석, 김진보, 김미선, 서재현
	자율주행 자동차 센서 신뢰도 향상 및 공격 탐지 알고리즘 분석 선현진, 이동
	소프트웨어 난독화 기법 평가 기술 연구 동향 백은수, 석재혁, 이재윤, 이동
좌장: **이임영** 교수 (순천향대학교)	

306호	발표 논문
관리정책 교육 2	ICT 기반 보안 개념과 영역에 관한 조사 연구 전민서, 나원철, 장항배
	보안성숙도 모델을 활용한 정보보호 관리수준 점검방안에 관한 연구 이상규, 김인석
	가상화폐 거래소의 보안성 확보를 위한 정보통신망 이용촉진 및 정보보호 등에 관한 법률 개정(안) 제시 전형율, 오장욱, 서정택
	데이터베이스 삭제 방법과 관련 법률의 지시사항 격차 확인을 통한 개선방향 제시 임창완, 조성영
	딥 러닝을 활용한 CVSS 점수 예측에 관한 연구 김현우, 송기범, 류승진, 윤한준, 이만희
좌장: **이경현** 교수 (부경대학교)	

307호	발표 논문
취약점분석	무인 복합 출력기 솔루션의 취약성 분석 지우중, 김형식
	Most Significant Bit가 Most Significant Power이다 – Case Studey : Chip Whisperer 이지우, 김주환, 이종혁, 한동국
	평창 올림픽 악성코드 분석을 통한 향후 공격 예측 김찬진, 탁현주, 김민서, 임수민, 염홍열
	안드로이드 모바일 게임 어플리케이션 보호 솔루션에 대한 분석 및 공격 기법 연구 조동민, 최형기
	임베디드 디바이스의 펌웨어 리버스 엔지니어링 방법 연구 박재현, 김승주
좌장: **박창섭** 교수 (단국대학교)	

B01-B	발표 논문
산업보안	S7CommPlus 제어 프로토콜 통신 보안 위협을 통한 기계학습 기반의 이상징후 탐지 방안 연구 홍기섭, 김효빈, 서정택
	풍력발전 제어시스템의 사이버 보안위협 분석을 통한 공격 가능시나리오 도출 및 대응방안 제시 송진우, 윤건, 전형율 ,서정택
	산업제어시스템 보호를 위한 ICS DPI Firwall 개발 노권수, 한상헌, 박혜용, 김기현
	SCADA 프로토콜 보안위협 및 보안요구사항 분석 위한샘, 이옥연
	쇼단을 이용한 제어시스템 공격 사례분석 및 대응방안 박현진, 박재용, 김인수, 서정택
좌장: **오희국** 교수 (한양대학교)	

B06-B	발표 논문
악성코드	금융권 보안 사고 악성코드 간 유사도 분석 김예준, 이재경, 류기백, 이유정, 염흥열
	난독화된 자바 악성코드에 대한 탐지 프로세스 제안 김광 , 염흥열
	해양 산업에서 사이버 해적의 위협 분석 조용현, 강준모, 차영균
	매그니튜드 익스플로잇 킷을 통해 유포되는 마이랜섬의 변화 동향 분석 김동현, 임명은, 양준호, 염흥열
	랜섬웨어 Native API 정보 분석을 통한 탐지 방법 연구 장준영, 김우재, 옥정윤, 임을규
좌장: **하재철** 교수 (호서대학교)	



구두 발표 세션 C

6월 22일(금) 10:30-11:50 **정보전산센터**

208호	발표 논문
암호화폐/블록체인 3	스마트 컨트랙트의 취약점과 취약점 분석 도구에 대한 연구 민정기, 김승주
	비트코인 거래 생성 시간 필드를 추가한, 이기적 채굴 대응방안 개선 이지혜, 김윤정
	국외 블록체인 기반 전력 시스템 보안 연구 동향 및 국내 블록체인 기반 전력시스템 적용 방안 김효빈, 홍기섭, 서정택
	블록체인 확장성 문제에 대한 분석과 고찰 노시완, 이경현
좌장: **유일선** 교수 (순천향대학교)	

303호	발표 논문
암호화폐/블록체인 4	블록체인을 활용한 공동인증서비스 기술 분석 이연수, 이가영, 이혜지, 염홍열
	(D)PoS 기반 블록체인의 거래 및 합의 방식 분석 한성호, 홍동연, 최낙준, 이나비, 김광조
	IoT 환경의 확장성을 위한 블록체인을 이용한 키 교환 프로토콜 이정호, 최형기
	비트코인 탈익명화 사례 분석 홍지형, 김윤정
좌장: **현상원** 교수 (조선대학교)	

304호	발표 논문
관리정책 교육 3	정보통신망 이용촉진 및 정보보호 등에 관한 법률 제49조 "비밀"의 분류 및 정의 윤우석, 박재용, 서정택
	내부 정보 유출 경로별 통합 시나리오 점검 방법 연구 권현우, 이익준, 염홍열
	블록체인 기술 적용과 개인정보 삭제 및 제3자 제공의 법적 문제에 관한 연구 (A Study on Legal Issues between the Application of Blockchain Technology and Deletion and the Third Party Supply of Personal Information) 최용혁
	공공의 이익을 위한 의료 빅데이터의 활용관련 법률 분석 및 의료법 개정(안)제시 한종찬, 박지환, 서정택
좌장: **김인석** 교수 (고려대학교)	

305호	발표 논문
관리정책 교육 4	국내외 정보보호제품 도입정책 동향 분석 및 수준 비교 연구 손효현, 김광준, 오형근, 이만희
	UAV 편대를 위한 그룹 리더 기반의 효율적인 보안 그룹 관리 기법 김승민, 최문원, 이우엽, 계동욱, 조인휘
	FAIR에 기반한 기업 정보유출사고시 발생하는 법적배상비용의 통계적 검정을 통한 산출 최상원, 유영인, 이경호
좌장: **장항배** 교수 (중앙대학교)	

306호	발표 논문
컴퓨터보안 2	Towards the Advance Persistent Threat' Detection Events Sami Ullah, 오희국
	윈도우 감사 로그를 활용한 침해사고 모니터링 방안 연구 윤인재
	조건문을 통한 점프테이블 크기 유추에 따른 인다이렉트 점프 주소 계산 방법 김문회, 하동수, 오희국
	전자파 오류 주입을 통한 인증 우회 공격 – Case Study : 지문 인식 시스템 이종혁, 조영진, 한동국
좌장: **서승현** 교수 (한양대학교)	

307호	발표 논문
여성 과학자	블록체인 기반 개인정보 처리 추적 관리 시스템 모델 제안 김미연, 염흥열
	ECG를 이용한 인증 시스템에 대한 원격 공격 가능성 분석 이선우, 이동
	C++의 동적 디스패치에 적용된 제어 흐름 무결성 검증기법 분석 장혜린, 박문찬, 진홍주, 이동
	Invited talk : 지금 시대가 필요로 하는 정보보호 인재상 윤혜정 실장(인터파크)
좌장: **심미나** 교수 (성결대학교)	

B01-B	발표 논문
기 타	열차 무인운전시스템 랜섬웨어 공격 파급효과 분석 및 대응방안 제시 이영비, 이동주, 윤우석, 서정택
	사이버 위협 시나리오 분석 및 예측의 자동화 방법 조성영, 정현숙, 신영섭, 이동재, 임창완, 오행록
	이동 경로 정보를 활용한 주소 인증 박호성, 남승수, 최대선
	부인방지 기능을 제공하는 이동형 전기자동차 충전기용 보안 에이전트 설계 장찬국, 이재 , 이옥연
좌장: **이옥연** 교수 (국민대학교)	



2018 한국정보보호학회 하계학술대회

A1 암호화폐/블록체인 1

허 준 범 (고려대학교)

- **블록체인 기반 분산형 키 관리시스템의 설계**
  안형철, 김광조
- **분기로 발생된 미확인 트랜잭션의 우선적인 처리기법**
  박승윤, 오희국
- **블록체인 기반 디지털증거 해시 관리 시스템 구현**
  정재완
- **암호화폐 키 관리에 의한 보안사고 및 대응방안 연구**
  김근영, 박준후, 오원찬, 류재철

블록체인 기반 분산형 키 관리 시스템의 설계[1)]

안형철* 김광조*
*카이스트 정보보호대학원

Design of Blockchain-based Decentralized Key Management System

Hyeongcheol An* Kwangjo Kim*
*Graduate School of Information Security, KAIST.

요 약

블록체인은 2008년 Bitcoin에서 처음으로 제안되었으며, 분산형 데이터베이스 기술이다. 현재 키 관리 시스템 중 하나인 공개키 기반 구조(Public Key Infrastructure, PKI) 기술은 중앙집중형 시스템으로 단일 장애 지점(single point failure)의 가능성이 존재한다. 또한 대표적인 암호화폐인 비트코인과 이더리움에서 사용되는 전자서명 알고리즘인 ECDSA는 Shor 알고리즘에 따라 양자 컴퓨터 공격에 취약하다는 문제점이 존재한다. 이에, 본 논문에서는 양자 내성 암호 기술을 적용한 블록체인 기반 키 관리 시스템에 대하여 제안한다. 분산형 구조인 블록체인을 기반으로 설계하여 single point failure에 안전하다. 또한, 대표적인 양자 내성 암호(Quantum-resistant Cryptography)인 래티스(lattice)기반 전자서명인 GLP 전자서명을 사용하기 때문에 양자컴퓨터의 공격에도 안전하며, 장기간 안전성을 보장한다.

I. 서론

최근 분산형 데이터베이스 시스템인 블록체인이 큰 각광을 받고 있다. 블록체인은 2008년 Nakamoto의 비트코인(Bitcoin)[1]에서 처음으로 제안되었다. 비트코인을 포함한 암호화폐는 기존의 중앙집중형 서버-클라이언트 방식이 아닌 P2P(peer to peer) 방식으로 통신을 하기 때문에 분산형 데이터베이스로 활용할 수 있다. 암호학적 관점에서 비트코인은 전자서명 방식으로 타원곡선(ECDSA)를 사용하고 해시함수로 SHA-256을 사용하고 있다. 또한 이더리움(Ethereum)[2]과 같은 2세대 블록체인에서도 ECDSA를 적용하여 전자서명을 한다.

한편, 비트코인에서 사용하는 전자서명 암호 기술 중 하나인 ECDSA는 이산 대수 문제의 어려움에 기반하기 때문에 Shor 알고리즘[3]에 따라 양자 컴퓨터 공격에 깨지게 된다. 따라서 양자컴퓨터 공격에도 안전한 전자서명이 필요하다. 양자 내성 암호(Quantum-resistant Cryptography)의 필요성이 제기되고 있으며, 그 중 하나로 래티스(lattice)기반 전자서명 알고리즘이 알려져 있다.

본 논문에서는 양자 내성 기술을 적용한 블록체인 기반 키 관리 시스템을 제안한다. 기존의 암호화폐의 블록체인에서 사용하는 전자서명 알고리즘인 ECDSA를 대체하여 GLP[4] 전자서명 알고리즘을 사용하여 양자컴퓨터의 공격에 안전하게 설계한다. 또한 기존의 공개키 기반 구조(Public Key Infrastructure, PKI)의 문제점인 single point failure를 분산형 구조인 블록체인을 기반으로 설계하였기 때문에 안전하다.

1) 본 연구는 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행되었습니다. (No.2017-0-00555, 양자 컴퓨터 환경에서 래티스 문제를 이용한 다자간 인증키교환 프로토콜 연구)

1.1 논문의 구성

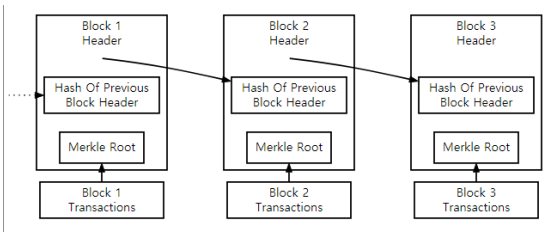
본 논문의 구성으로 Ⅱ장에서는 블록체인과 PKI 시스템에 대하여 간략히 설명하고, Ⅲ장은 블록체인 기반 키 관리 시스템과 프로토콜에 대하여 제안한다. Ⅳ장에서는 기존에 사용하고 있는 PKI 시스템과의 비교에 대하여 논한다. 마지막으로 Ⅴ장에서는 결론과 본 논문 성과를 이용한 추후 연구에 대한 가능성을 제시한다.

II. 배경지식

2.1 블록체인

비트코인은 최초의 분산 암호 및 가상화폐이며 2008 년 Nakamoto에 의해 P2P 네트워크 기반으로 설계되었다. 중앙집중형 방식인 서버-클라이언트 방식을 사용하지 않기 때문에 합의 프로토콜(consensus protocol)이 필요하며, 비트코인에서는 작업증명(Proof-of-Work, PoW) 방식을 사용한다. 블록체인 네트워크의 모든 사용자는 공개키 암호화를 사용하여 트랜잭션을 생성하고 전파할 수 있다. [그림 1]은 비트코인 블록체인의 단순화한 구조이다. 모든 블록의 헤더에는 이전 블록 헤더의 해시 값이 존재한다. 또한 각 블록의 트랜잭션을 사용하여 머클 해시 트리(Merkle hash tree)를 만들 수 있다. 이전 블록의 해시값을 새로운 블록에 추가하는 방법으로 이전 블록의 변조에 대한 안전성을 확보할 수 있다.

비트코인이 제안 된 이후, 2014년 이더리움 등 많은 암호화폐가 제안되었다. 따라서 블록체인은 TTP(Trusted Third Party)가 없어도 무결성을 지원하는 데이터베이스를 만들 수 있다.



[그림 1] 블록체인의 구조

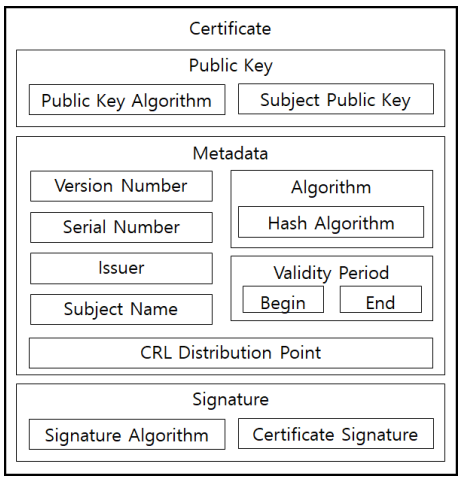
2.2 공개키 기반 구조

PKI 시스템의 인증서는 공개키 및 메타데이터(metadata)가 포함된 디지털 문서이다. 합법적인 CA(Certificated Authority)만이 유효한 인증서를 발급할 수 있다. 현재 PKI 시스템은 X.509[5] 표준으로 정의되어 있다. [그림 2]는 X.509 v3 인증서의 구조에 대하여 설명한다.

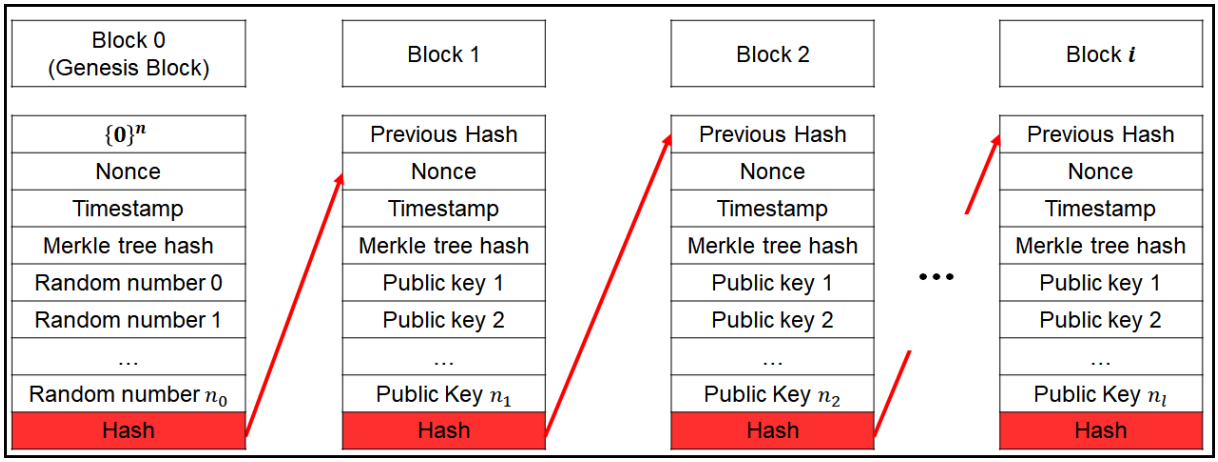
현재 PKI 시스템은 중앙 집중식 데이터베이스를 기반이 특징이다. 그러나 이로 인하여 단일 장애 지점(single point failure)의 취약점이 있다. 블록체인은 분산된 네트워크에서 변경되지 않는 원장을 제공하는 것을 목표로 하기 때문에 공개키의 저장 및 관리에 적합하다. 블록체인 기반 키 관리 시스템에 대한 최근 연구결과는 다음과 같다.

Emercoin (EMC)[6]은 블록체인 기반 PKI 시스템에 사용되는 암호화폐로, OpenSSH와 EMC 블록체인을 통합하여 분산 PKI를 구성한다. 합의 프로토콜로 PoW 및 PoS(Proof-of-Stake)를 사용한다. 또한 SHA-256을 해시 함수로 사용한다. 암호학적 특징 때문에 EMC는 양자 컴퓨팅 공격으로부터 안전하지 않다는 단점이 있다.

Matsumoto 등은 2016년에 IKP[7]라는 이더리움 기반 PKI 시스템을 제안하였다. 그러나 IKP는 이더리움 플랫폼에 기반하여 설계하였기 때문에 장기간 안전성을 보장하지 못한다.
이더리움은 ECDSA 서명 알고리즘을 사용하기 때문에 양자컴퓨터의 공격에 취약하다는 단점이 존재한다.



[그림 2] X.509 v3 인증서의 구조



[그림 3] 양자 내성 블록체인 키 관리 시스템의 구조

III. 블록체인 기반 키 관리 시스템

3.1 블록체인 기반 키 관리 시스템의 설계

- **Setup**(1^λ): 파라미터 λ를 선택하고 $n, q, \sigma = \sqrt{16/2} \approx 2.828$을 출력한다.

- **KeyGen**(n, q): 다항식 곱셈과 덧셈에서 NTT (Number Theoretic Transformation) 연산을 사용하여 가우시안 분포로부터 샘플링 된 다항식 r_1, r_2를 출력한다. 각각의 사용자 i에 대한 공개키는 $(\hat{a_i}, \hat{p_i}, \hat{t_i}) \in pk_i$이고, 비밀키는 $(\widehat{r_{1,i}}, \widehat{r_{2,i}}, \widehat{y_{1,i}}, \widehat{y_{2,i}}) \in sk_i$이다.

- **GenesisBlock**(): [그림 3]과 같이 Setup, Merkle, Final로 구성되어 있으며, 초기에 첫 번째 블록을 생성한다. 해시값은 다음과 같이 계산한다.

$$H_{Block0} = H((\{0\})^n || nonce || timestamp || H_{root})$$

- **User.Setup**(pk_i, H_{root}): 사용자의 공개키를 추가하기 위하여 setup을 한다.

- **User.Add**(ID_i, $Username$, sk_i, pk_i): 사용자의 공개키 추가는 다음과 같이 계산한다.

$$H(ID_i), \quad ID_i \leftarrow \text{User ID};$$

$$H(Username_i), \quad Username_i \leftarrow \text{Username};$$

$$(\hat{r}_{1,i}, \hat{r}_{2,i}, \hat{y}_{1,i}, \hat{y}_{2,i}) \leftarrow sk_i;$$

$$y_{1,i} \leftarrow \text{NTT}^{-1}(\hat{y}_{1,i}); \quad y_{2,i} \leftarrow \text{NTT}^{-1}(\hat{y}_{2,i});$$

$$(\hat{a}_i, \hat{p}_i) \leftarrow pk_i; \quad a_i \leftarrow \text{NTT}^{-1}(\hat{a}_i);$$

$$c_i \leftarrow H(a_i y_{1,i} + y_{2,i}, ID_i); \quad \hat{c}_i \leftarrow \text{NTT}(c)$$

$$r_{1,i} \leftarrow \text{NTT}^{-1}(\hat{r}_{1,i}); \quad r_{2,i} \leftarrow \text{NTT}^{-1}(\hat{r}_{2_i});$$

$$Sign(ID_i, a_i, r_{1,i}, r_{2,i});$$

- **User.Verify**(ID_i, pk_i, **Sign**(ID_i)): 사용자의 공개키 및 서명을 검증하기 위하여 다음과 같이 계산한다.

$$\hat{a_i}, \hat{t_i} \leftarrow pk_i;$$

$$a_i \leftarrow \text{NTT}^{-1}(\hat{a}_i); \quad t_i \leftarrow \text{NTT}^{-1}(\hat{t}_i);$$

$$z_{1,i}, z_{2,i}, \hat{c}_i \leftarrow Sign(ID_i);$$

$$c_i \leftarrow \text{NTT}^{-1}(\hat{c}_i);$$

$$Verify(ID_i, z_{1,i}, z_{2,i}, c_i, a_i, t_i);$$

- **User.Enc**(pk_i, m): 메시지 m을 암호화하기 위하여 다음과 같이 계산한다.

$$(\hat{a}_i, \hat{p}_i, \hat{t}_i) \leftarrow pk_i;$$

$$(a_i, p_i, t_i) \leftarrow (\text{NTT}^{-1}(\hat{a}_i), \text{NTT}^{-1}(\hat{p}_i), \text{NTT}^{-1}(\hat{t}_i));$$

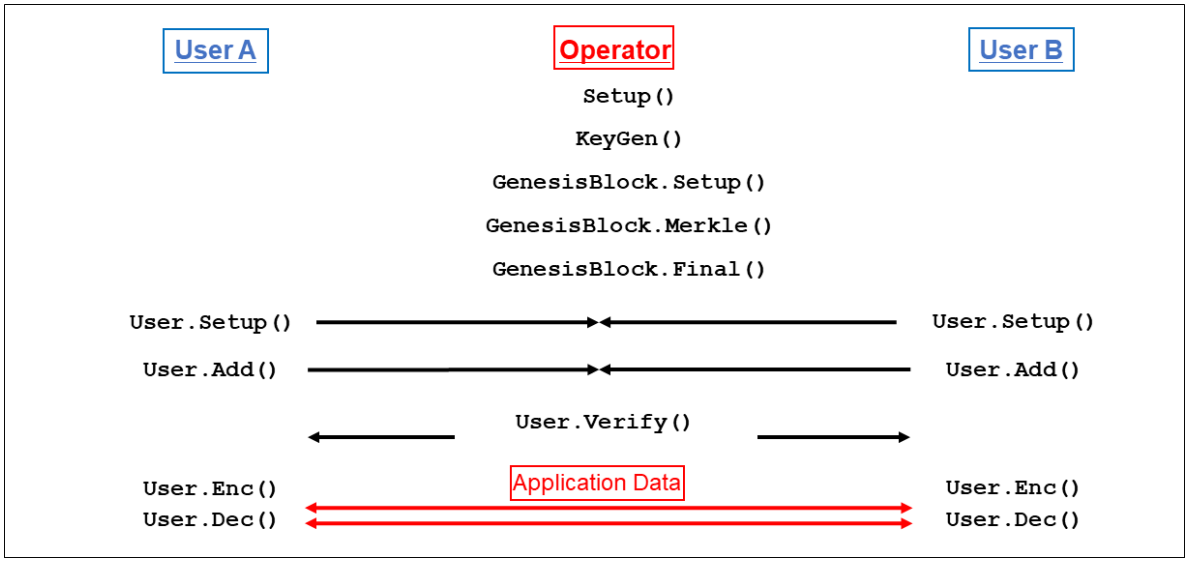
$$e_1, e_2, e_3 \leftarrow \chi_\sigma;$$

$$\hat{e}_1 \leftarrow \text{NTT}(e_1); \quad \hat{e}_2 \leftarrow \text{NTT}(e_2);$$

$$\hat{m} \leftarrow m \cdot \left\lfloor \frac{q}{2} \right\rfloor;$$

$$(\hat{c}_1, \hat{c}_2) \leftarrow (\hat{a}_i * \hat{e}_1 + \hat{e}_2, \quad \hat{p}_i * \hat{e}_1 + \text{NTT}(e_3 + \hat{m}));$$

암호문 $c = (\widehat{c_1}, \widehat{c_2})$를 출력한다.



[그림 4] 양자 내성 블록체인 기반 키 관리 프로토콜

- User.Dec(sk_i, c): 암호화된 메시지 $c=(\hat{c_1},\hat{c_2})$를 복호화 하기 위하여, 비밀키 sk_i를 사용하여 다음과 같이 계산한다.

$$\hat{r}_{2,i} \leftarrow sk_i;$$

$$(\hat{c}_1, \hat{c}_2) \leftarrow c;$$

$$m' \leftarrow \mathsf{NTT}^{-1}(\hat{c}_1 * \hat{r}_2 + \hat{c}_2);$$

$$m \leftarrow \mathsf{Decode}(m');$$

Decode()함수는 다음과 같이 정의한다.

$$\mathsf{Decode}(m) := \left\lfloor \frac{2}{q} \cdot m \cdot \lfloor q/2 \rfloor \right\rceil \cdot \left\lfloor \frac{q}{2} \right\rfloor$$

[그림 4]는 본 논문에서 제안한 양자 내성 기반 키 관리 프로토콜에 대한 그림이다.

3.2 GLP 서명 알고리즘

래티스 기반 전자서명 알고리즘인 GLP[8]는 Ring-LWE에 기반하여 양자컴퓨터 공격에 안전하다. 본 논문에서 사용하는 수정 GLP 전자서명은 다항식 덧셈과 곱셈에서 NTT 연산을 추가하여 연산의 효율성을 증가하였다.

· 해시함수: $H: \{0,1\}^* \rightarrow D_{32}^n$

· 서명키: $r_1, r_2 \xleftarrow{\$} \chi_\sigma$

· 검증키: $a \xleftarrow{\$} R_q,\ \hat{a} \leftarrow NTT(a),\ \hat{r_1} \leftarrow NTT(r_1),$

$\hat{r_2} \leftarrow NTT(r_2),\ \hat{t} \leftarrow \hat{a} \bullet \hat{r_1} + \hat{r_2}$

Sign(μ, a, r_1, r_2)

```
2  begin
3    y1, y2 ←$ R_q^k;
4    c ← H(a·y1 + y2, μ);
5    ĉ = NTT(c);
6    ẑ1 ← r̂1 * ĉ + ŷ1;
7    ẑ2 ← r̂2 * ĉ + ŷ2;
8    z1 ← NTT^-1(ẑ1);
9    z2 ← NTT^-1(ẑ2);
10   if z1 ∉ R_q^(k-32) or z2 ∉ R_q^(k-32) then
11     go to line 3;
12   else
13     return (z1, z2, c);
14   end
15 end
```

Verify(μ, z_1, z_2, c, a, t)

```
17 begin
18   if z1, z2 ∈ R_q^(k-32) then
19     c ≠ H(a·z1 + z2 − t·c, μ);
20     return reject;
21   else
22     return success;
23   end
24 end
```

[표 1] 양자 내성 블록체인 기반 키 관리 시스템과 X.509 v3와의 비교

키 관리 시스템	양자 내성 블록체인 기반 키 관리 시스템	X.509 v3
Connection	Off-line	On-line
Non-repudiation	O	O
Revocation	O	O
Scalability	$O(n)$	$O(n)$
Trust Model	분산형	중앙집중형

IV. 블록체인 기반 키 관리 시스템의 안전성 분석

4.1 안전성 및 공격 복잡도 분석

Grover 알고리즘[9]은 양자컴퓨터를 이용한 효율적인 데이터베이스 검색 알고리즘이다. 본 논문에서 설계한 블록체인 기반 키 관리 시스템에서 n_1비트의 해시함수의 경우, 전수조사(brute-force) 공격의 복잡도는 $O(2^{n_1/2})$이다. 또한, n_2비트의 비밀키를 가지는 Ring-LWE 기반 전자서명인 GLP에서 SVP(Shortest Vector Problem)을 찾는 경우 $2^{1.799n_2+O(n_2)}$이다[10]. 따라서 양자컴퓨터를 이용한 공격의 경우 전체 공격복잡도는 $\min(O(2^{n_1/2}), 2^{1.779n_2, O(n_2)})$인 것을 알 수 있다.

한편 현재 사용하는 슈퍼컴퓨터를 활용한 공격에서는 Grover 알고리즘은 적용되지 않는다. 따라서 해시함수의 공격 복잡도는 $O(2^{n_1})$이다. 또한 GLP 전자서명에서 사용하는 Ring-LWE의 SVP를 찾는 경우 효율적인 다항식 시간 내에 풀 수 있는 효율적인 알고리즘은 존재하지 않는다. 현재까지 알려진 가장 효율적인 BKZ-2.0[11]을 사용할 경우 공격복잡도는 $2^{2.465n_2+O(n_2)}$이다. 따라서 슈퍼컴퓨터를 사용한 공격자를 가정할 경우 전체 공격복잡도는 $\min(O(n_1), 2^{2.465n_2+O(n_2)})$이다.

결론적으로 양자컴퓨터를 포함한 모든 공격자에 대하여 안전하므로 본 논문에서 제시한 블록체인 기반 키 관리 시스템은 장기간 안전성을 달성할 수 있다.

4.2 기존 키 관리 시스템과의 비교

[표 1]에서는 양자 내성 블록체인 기반 키 관리 시스템과 X.509 v3과의 비교를 보여준다.

- Connection: 시작 블록을 제외한 오프라인 상태를 유지할 수 있다. 반면에 X.509는 TTP가 항상 온라인 상태를 유지해야 한다. TTP가 오프라인인 경우 사용자는 공개키가 인증되었는지 확인할 수 없다.

- Non-repudiation: 서명이 있는 사용자의 공개키로 구성된 블록을 가지고 있다. 사용자는 공개키 및 사용자 ID와 같은 공개 정보를 거부 할 수 없다. X.509는 공개키, 사용자 이름 및 서명으로 구성된 인증서를 가지고 있다. 따라서 사용자는 자신의 유효한 인증서를 거부 할 수 없다.

- Revocation: 각 블록 및 사용자 정보에 타임스탬프를 사용한다. 초기에 각 블록에 타임스탬프를 사용하여 만료 시간을 설정할 수 있다. 또한 revocation에 대한 복잡도는 $O(\log_2 n)$이다. X.509는 사용자 인증서에 해지 기록을 저장한다. 그리고 CRL에 대한 블록체인을 만들어 해지 목록을 관리 할 수 있다.

-Scalability: 본 설계의 확장성에 대한 복잡도는 $O(n)$이다. 그러나 사용자 및 공개 정보 수가 증가하더라도 TTP 서버 수를 늘릴 필요가 없다는 점이 장점이다. 그러나 X.509는 사용자의 공개 정보를 추가하기 위해 서버 확장에 대한 문제가 존재한다.

-Trust model: 본 설계의 핵심은 PKI 시스템에 대한 분산 서비스이며, TTP가 필요하지 않다. X.509는 TTP가 필수적이므로 단일 장애 지점(single point failure)의 문제가 존재한다.

V. 결론

본 논문에서는 양자 내성 기술을 적용한 블록체인 기반 키 관리 시스템에 대하여 제안하였다. 기존의 블록체인 기반 키 관리 시스템은 양자컴퓨터의 공격에 해독이 가능하다는 단점이 존재한다. 그러나 본 논문의 설계에서는 양자 내성 전자서명을 적용하여 양자컴퓨터의 공격에도 안전하다. 또한 양자 및 고전 공격자에 대한 공격복잡도를 제시하여 안전한 것을 검증하였다. 한편 기존의 X.509기반 PKI 시스템과 대비하여 분산형 구조로 설계한 것을 확인할 수 있었으며, 키 관리 시스템에서의 요구조건을 만족하는 것을 알 수 있었다.

향후 연구 과제로는 합의 프로토콜에 대한 고려가 필요하다. 키 관리 시스템의 경우 private, consortium, public 블록체인에 모두 활용될 수 있다. 따라서 public 블록체인의 PoW 또는 PoS, private과 consortium 블록체인에서는 BFT계열의 합의 프로토콜을 적용할 것 이다.실제 구현하여 본 연구 성과의 성능을 검증할 것이다. 또한 블록체인 기술은 키 관리 시스템 뿐만 아니라 접근통제(access control), 인증과 같은 부분에 사용될 수 있기 때문에 연구를 확장할 예정이다.

[참고문헌]

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[2] G. Wood, “Ethereum: A secure decentralized generalized transaction ledger,” Ethereum Project, Yellow Paper, vol. 151, 2014.

[3] 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.

[4] T. Güneysu, V. Lyubashevsky, and T. Pöppelmann, "Practical lattice-based cryptography: A signature scheme for embedded systems," in Conference on Cryptographic Hardware and Embedded Systems, CHES'12, pp. 530-547, Springer, 2012.

[5] P. Yee, “Updates to the internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile," 2013.

[6] “Emercoin", https://emercoin.com

[7] S. Matsumoto and R. M. Reischuk, “IKP: Turning a PKI around with blockchains.," IACR Cryptology ePrint Archive, 2016/1018, 2016.

[8] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D. Stehle, “Classical hardness of learning with errors," in Proceedings of the forty-fth annual ACM symposium on Theory of computing, STOC'13, pp. 575-584, ACM, 2013.

[9] T. Güneysu, V. Lyubashevsky, and T. Pöppelmann, ”Practical lattice-based cryptography: A signature scheme for embedded systems.," in Conference on Cryptographic Hardware and Embedded Systems, CHES'12, pp. 530-547, Springer, 2012.

[10] L. K. Grover, ”A fast quantum mechanical algorithm for database search," in Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing, STOC'96, pp. 212-219, ACM, 1996.

[11] Y. Chen and P. Q. Nguyen, “BKZ 2.0: Better lattice security estimates," in International Conference on the Theory and Application of Cryptology and Information Security Asiacrypt'11, pp. 1-20, Springer, 2011.

분기로 발생된 미확인 트랜잭션의 우선적인 처리기법*

박승윤† , 오희국‡

한양대학교 컴퓨터공학과

The Prioritizing Method of Mining a Unconfirmed Transaction Generated by Forking

Seungyun Park and Heekuck Oh

Department of Computer Science and Engineering, Hanyang University.

요 약

비트코인의 블록체인은 일시적인 분기가 발생했을 때에 작업증명의 총량을 계산하여 주 체인을 결정함으로서 네트워크를 유지해 나아간다. 분기가 해결되는 과정에서 버려지는 블록에 있는 트랜잭션들은 다시 메모리 풀로 돌아가며 마이닝 노드에 의해 채굴되기를 기다린다. 또한, 버려지는 블록에 의해 생성되는 오르판 블록은 메모리 풀로 돌아간 트랜잭션이 다시 채굴되어 체인에 연결될 때까지 기다려야만 한다. 이러한 네트워크의 비효율성을 해결하기 위하여 메모리 풀로 되돌아온 트랜잭션에 Priority를 부여하여 마이닝 노드의 예비 블록에 수집될 확률을 높여 트랜잭션 딜레이를 해결하고 네트워크의 효율성을 높이는 트랜잭션 처리기법을 제안하였다.

I. 서론

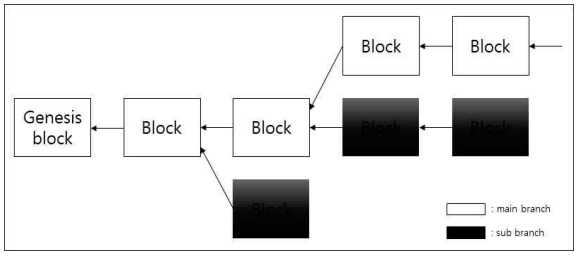
비트코인 블록체인은 일시적인 분기가 발생했을 때에 작업증명의 총량을 계산하여 주 체인을 결정함으로서 네트워크를 유지해 나아간다. 분기가 해결되는 과정에서 버려지는 블록에 있는 트랜잭션은 낭비되며 메모리 풀로 돌아가 다시 채굴되기를 기다린다. 즉, 미확인 상태로 돌아온다. 버려지는 블록을 채굴한 마이닝 노드는 사용한 컴퓨팅 파워를 낭비하게 된다. 이로 인해 발생되는 고아 블록(Orphan block)과 트랜잭션 딜레이는 네트워크의 비효율성을 야기하는 문제를 가지고 있다. 현재 비트코인 네트워크는 높은 수수료를 가진 트랜잭션을 우선적으로 채굴하는 룰을 가지고 유지되고 있다. 그렇기 때문에 일시적 분기에 의한 버려지는 블록의 트랜잭션들은 한번 채굴이 되었음에도 불구하고 또 한번 높은 수수료를 가진 트랜잭션들과의 수수료 경쟁을 하는 비효율적인 문제점을 가지고 있다. 본 논문에서는 블록을 블록체인 네트워크에 전파하는 과정에서 생기는 일시적인 분기에 대한 기존의 비효율적인 처리방법보다 보다 효율적인 처리방법을 제안하여 네트워크의 효율성을 유지하는 방법을 서술한다.

본 논문의 구성은 다음과 같다. 본 논문의 2장에서는 트랜잭션 처리기법의 문제점에 대해 서술한다. 3장에서는 **Priority**를 부여함으로서 트랜잭션을 효율적으로 처리하는 기법에 대해 서술한다. 4장에서는 제안하는 처리기법에 의해 기대되는 효과에 대해 서술한다. 5장에서는 앞으로 해결해야하는 과제에 대해서 서술한다. 6

* 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ITCT연구센터육성지원사업의 연구결과로 수행되었음(IITP-2018-2014-1-00636)
이 논문은 2015년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2015R1D1A1A09058200)

† 주저자 : superkidd@hanyang.ac.kr

‡ 교신저자 : hkoh@hanyang.ac.kr



[그림-1] 분기가 발생한 블록체인의 일부분

장에서는 논문의 결론을 맺는다.

II.기존 트랜잭션 처리기법의 문제점

2.1 일시적인 분기

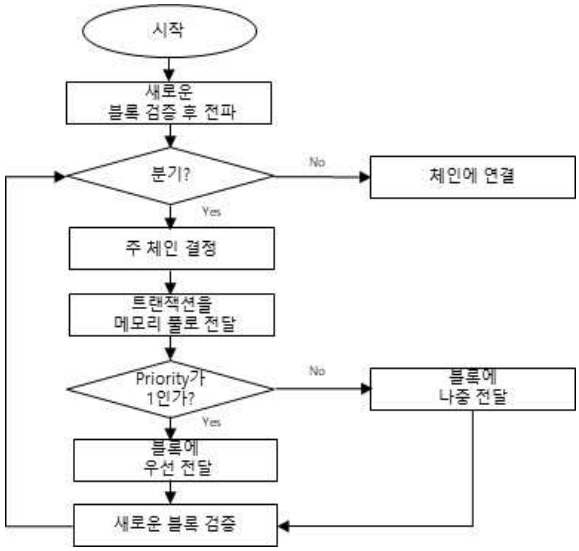
각각의 마이닝 노드는 비트코인 네트워크를 통해 인근의 노드에게 자신의 블록을 전파하여 체인에 유효한 블록을 추가할 수 있다. **[그림-1]**과 같이 만약 다수의 마이닝 노드가 이전 블록(부모 블록)이 같은 블록을 동시에 만들면 체인은 분기를 형성한다. 다른 마이닝 노드들은 이후에 분기들 중 하나에 새로운 유효 블록을 추가할 수 있다.

체인에 분기가 발생하면 이러한 분기를 해결하기 위하여 비트코인 네트워크는 마이닝 노드가 채굴해야하는 하나의 체인 즉, 메인 체인을 결정해야한다. 그 기준은 가장 무거운 체인을 선택하는 것이고 각 분기의 작업증명의 총량을 측정해서 더 큰 작업증명량을 가진 체인을 알 수 있다. 선택받지 못한 즉, 서브 브랜치에 있는 블록은 버려지고 블록의 트랜잭션들은 메모리 풀로 돌아온다. 즉, 다시 미확인 상태가 되어 돌아온다. 버려지는 브랜치에 있는 블록들을 채굴한 노드들은 보상을 받지 못하며 컴퓨팅파워를 낭비하게 된다.

분기가 해결되면 마이닝 노드들은 메인 체인에서 마이닝을 다시 시작한다. 결과적으로, 되돌아온 트랜잭션은 또 한번 마이닝 풀에서 기존의 트랜잭션들과 같은 룰 아래에서 수집되길 기다리며 메모리 풀로 되돌아온 트랜잭션이 수집되지 않는다면 본 논문에서 언급하는 비효율성을 야기한다.

2.2 고아 블록(Orphan block)

체인 내에서 상위 블록이 없는 블록을 고아 블록이라고 한다. 고아 블록은 고아 블록 풀에



[그림-2] 우선권을 부여하는 트랜잭션 처리방법

저장되어 상위 블록이 수신될 때까지 유지된다. 상위 블록이 수신되어 체인에 연결되면 고아 블록이 고아 블록 풀에서 빠져나가 상위 블록에 연결되어 체인의 일부가 된다. 비트코인 네트워크에서 일시적으로 분기가 발생하면 고아 블록이 발생하며 분기를 해결하면 고아 블록 역시 해결된다. 일단 고아 블록이 생성되면 트랜잭션의 딜레이가 일어나며 일시적으로 비트코인 네트워크의 비효율성을 초래한다.

III. 트랜잭션의 효율적 처리방법

비트코인의 경우, 채굴과정에서 일시적인 분기가 일어나면 버려지는 블록들의 트랜잭션들은 채굴이 될 때까지 다시 기다려야 하는 비효율적 문제가 생긴다. 그러므로 메모리 풀로 돌아온 트랜잭션에 대해 **Priority**를 부여한다.

Priority는 예비 블록에 트랜잭션을 수집하는 기준에 우선권을 주는 것을 의미한다. **Priority**는 메모리 풀로 되돌아온 트랜잭션인지에 대한 검증여부를 판단해야 하며 이러한 트랜잭션을 예비 블록에 우선적으로 수집하여 블록을 채굴한 노드에게 추가 보상을 주는 것을 의미한다. **[표-2]**에서 보는 바와 같이 **Priority**는 트랜잭션 내부 코드에 작성을 하며 분기가 일어난 후에 버려지는 블록의 트랜잭션들이 메모리 풀로 돌아올 때에 동적으로 트랜잭션 내부구조에 그 여부를 할당함으로서 근거를 남긴다.

```
Algorithm.1: Give a Priority
On mining algorithm

    if  block include Priority Tx then
        A <- Priority block's incentive

    else
        B <- origin block's incentive

    if   A < B     then
        A <- Priority block's incentive +
             extra incentive

    else if A = B  then
        mining Priority block or not

    else
        mining Priority block
```

표-1 priority를 부여하는 pseudo code

마이닝 노드들은 기존 마이닝 법칙에 의해서 예비 블록에 각 노드들의 메모리 풀에 있는 트랜잭션들을 높은 수수료를 가진 순서에 따라 수집하지만 본 논문에서 제시하는 마이닝 알고리즘에서는 추가적으로 주어지는 보상 즉, extra incentive에 대해서도 고려한다.

Priority가 없는 트랜잭션을 채굴할 것인지 **Priority**가 있는 트랜잭션을 채굴할 것인지의 판단 여부는 채굴함으로서 얻는 총 보상이다. **[표-1]**에서 보는 바와 같이, A와 B를 각각 **Priority** 트랜잭션을 포함한 블록의 인센티브 그리고 일반적인 블록의 인센티브라고 하자. 만약에 A가 B보다 크거나 같다면 추가적인 보상을 부여하지 않아도 **Priority** 트랜잭션을 포함한 블록은 채굴되어서 체인에 연결 될 확률이 매우 높다. 하지만 A가 B보다 작다면 **Priority** 트랜잭션은 채굴되지 않을 가능성이 매우 높다. 채굴이 되지 않으면 **Priority** 트랜잭션은 계속해서 메모리 풀에서 채굴될 때까지 기다린다. 때문에 **Priority** 트랜잭션을 포함한 블록에 추가적인 보상을 부여함으로서 블록이 채굴될 확률을 높인다. 추가적인 보상 부여 정도는 적어도 A와 B가 같아질 만큼의 양을 부여해야 채굴 확률을 높일 수 있으며 높은 수수료를 가지는 트랜잭션을 우선적으로 수집하는 기존의 마이닝 룰에 의해 그 이하의 추가적인 보상은 의미가 없다.

요약하면, 기존의 마이닝 룰에 의하면 **Priority** 트랜잭션의 채굴이 지연될 수 있는 가능성이 있지만 제안하는 마이닝 알고리즘에 의하면 추가적인 보상을 부여함으로서 전체적으로 **Priority** 트랜잭션의 채굴 확률을 높일 수 있다.

The real code of transaction

```
On mining {
  "hash":"5a42590fbe……50990b8b6b",
  "ver":1,
  "vin_sz":2,
  "vout_sz":1,
  "lock_time":0,
  "size":404,
  "count": 0 or 1
  "in":[
    {
      "prev_out": {
        "hash":"3be4ac……7d7928",
        "n":0
      },
      "scriptSig":30440……3f3a4ce81"
    }
  ],
  "out":[
    {
      "value":10.12287.."+"extra incentive",
      "scriptPubKey":OP_DUP
        OP_HASH160 . OP_EQUALVERIFY
        OP_CHECKSIG"
    }
  ]
}
```

표-2 트랜잭션 실제 내부코드

IV. 기대되는 효과

본 논문에서 제시하는 기법을 마이닝 알고리즘에 반영하기 위해서는 예비 블록에 트랜잭션을 수집할 때에 높은 트랜잭션 수수료에 따르는 기존의 마이닝 룰을 거스르지 않는다는 전제가 있어야 한다. 각 노드들은 채굴함으로서 얻는 총 보상의 양을 최대화 시키려 하기 때문에 높은 수수료를 가지는 트랜잭션을 우선순위로 수집하려고 한다. 추가적인 보상만을 우선적으로 고려하여 네트워크의 효율성을 바라는 것은 경제학적인 관점에 바르지 않고 네트워크적으로도 기존의 룰을 사용할 때보다 적은 보상을 얻을 수 있으며 기존의 룰보다 더 큰 비효율성을 야기할 수 있다. 제안하는 기법을 도입함으로서 일반적인 블록의 인센티브와 **Priority** 트랜잭션을 포함한 인센티브를 비교해서 **Priority** 트랜잭션의 채굴확률을 높일 뿐이다.

이런 조건 안에서 트랜잭션 딜레이에 대한 문제 해결에 기여할 수 있다. 이론적으로 비트

코인은 30만 건의 트랜잭션을 처리하고 이 양은 초당 3~4건에 이른다. 많은 양을 처리하지만 실제로 하루 평균 4000건의 트랜잭션이 처리되지 않는다. 이 중에서 실제 분기에 의해서 버려진 블록의 트랜잭션의 양은 적지만 이로 인한 고아 블록은 꾸준히 발생한다. 제안하는 기법을 이용하여 고아 블록의 이전 블록이 되는 트랜잭션들의 채굴확률을 높여 트랜잭션 처리가 기존의 룰보다 효율적으로 가능하게끔 된다면 고아 블록의 체인 연결은 기존의 룰을 사용했을 때보다 상대적으로 빨라질 수 있다. 제안하는 트랜잭션 처리기법을 사용하면 트랜잭션 딜레이에 대한 문제 해결에도 기여할 수 있다.

앞으로 비트코인이 화폐의 가치를 인정받고 실질 화폐를 대체하는 시장의 안정화가 이루어진다면 발생되는 트랜잭션 수는 기하급수적으로 늘어날 것이다. 이에 따라서 네트워크에 참여하는 노드가 증가하고 분기가 발생할 확률이 높아질 것이다. 수반되는 네트워크의 비효율적 트랜잭션 처리에 대해서 본 논문에서 제안하는 트랜잭션 처리기법을 이용하여 효율적인 트랜잭션 처리를 기대한다.

V. 해결해야 할 과제

제안하는 기법을 비트코인 네트워크에 직접 사용하기 위해서 3가지 과제를 해결해야 한다.

첫째로, 트랜잭션 내부구조에 **Priority**를 입력하고 **Priority**에 의한 블록의 추가적인 보상을 부여하기 위한 실질적인 알고리즘이 필요하다. 실제 **[표-2]**에서 보인 트랜잭션 내부 코드는 기존의 트랜잭션 코드에 표시되는 **Priority**와 추가적인 보상에 대한 코드를 제시한 것이며 실질적으로 마이닝 알고리즘에 **Priority**와 추가적인 보상을 부여하기 위한 구체적인 설계와 구현이 필요하다.

둘째로, 알고리즘 안에 들어갈 추가적인 보상의 정확한 비율이 증명되어야 한다. 추가적인 보상의 값이 아무런 기준 없이 부여되면 마이닝 노드는 값이 크면 기존의 rule을 무시하고 변형된 트랜잭션만을 채굴할 것이며 값이 마이닝 노드의 수집에 영향을 주지 못 할 정도로 작다면 추가적인 보상의 의미가 퇴색된다.

셋째로, 새로운 마이닝 룰을 비트코인 네트워크에 반영하기 위한 네트워크의 분산 합의가 필요하다. 블록체인 자체는 분산적 합의를 통해 네트워크를 유지하기 때문에 본 논문에서 제안한 아이디어를 네트워크 내의 단일노드만 적용하는 것은 의미가 없을뿐더러 트랜잭션 수수료에 **Priority**를 두는 기존의 룰과는 달리 마이닝 알고리즘 안에서 트랜잭션에 **Priority**를 부여하는 새로운 룰은 기본적으로 비트코인의 포킹을 전제로 한다. 즉, 추가적인 보상을 부여하는 것은 네트워크의 전체적 합의가 필요하기 때문에 그 방법을 모색해야 한다.

VI. 결론

앞의 장들에서 서술한 네트워크의 비효율성을 해결하기 위하여 메모리 풀로 되돌아온 트랜잭션에 대해서 **Priority**를 부여하였고 마이닝 노드의 예비 블록에 수집될 확률을 높여 트랜잭션 딜레이를 해결하고 네트워크의 효율성을 높이는 방법을 제안하였다. 제안한 기법을 비트코인 네트워크에 반영하기 위해서는 **Priority**와 추가적인 보상을 부여하기 위한 실질적 알고리즘을 구현해야하고 추가적인 보상의 정확한 비율을 계산하여 증명해야만 한다. 또한, 네트워크의 노드들의 합의가 진행되어야 하며 그에 따른 포킹이 이루어져야 한다.

앞으로 발전할 코인시장이 더욱 커진다면 발생하는 트랜잭션의 수는 많이 늘어날 것이며 트랜잭션을 효과적으로 처리해야 하는 방법에 대해서 더욱 연구해야 할 것이다.

[참고문헌]

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

[2] Antonopoulos, Andreas M. Mastering Bitcoin: unlocking digital cryptocurrencies. " O'Reilly Media, Inc.", 2014.

[3] Kroll, Joshua A., Ian C. Davey, and Edward W. Felten. "The economics of Bitcoin mining, or Bitcoin in the presence of adversaries." Proceedings of WEIS. Vol. 2013. 2013.

[4] Eyal, Ittay, et al. "Bitcoin-NG: A Scalable Blockchain Protocol." NSDI. 2016.

블록체인 기반 디지털증거 해시 관리 시스템 구현

정재완*

*방어진고등학교

Implementation of digital evidence hash management system based on blockchain

Jaewan Jeong*

*Bangeojin High School

요 약

디지털증거에 대한 무결성을 증명하는 과정에서 수학적으로 증명된 해시를 이용한다. 따라서 해시의 무결성에 대한 관리가 필요해진 상황이다. 이에 본 논문에서는 해시 관리에 있어서 더욱 안전하고, 무결성을 제공할 수 있는 블록체인의 기술을 이용하여 디지털증거 해시 관리 시스템을 구현하며 이를 제안한다.

I. 서론

1.1 디지털증거 해시 관리에 대한 필요성

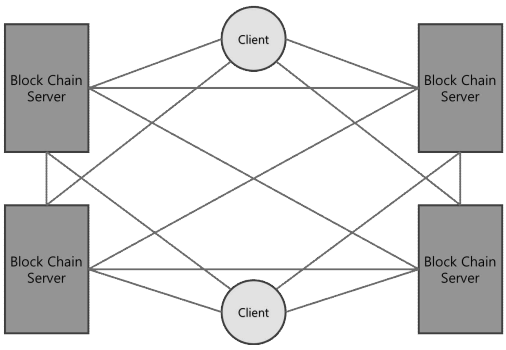
해시는 디지털포렌식에 있어 중요한 역할을 한다. 디지털포렌식 실무에서는 흔히 MD5 해시 방법을 사용하고 있으며, 최근 여러판례 역시 MD5 해시를 이용하여 무결성이 입증된 디지털 증거들을 인정하고 있다. 따라서 파일 해시에 대한 위/변조 가능성을 대비하여 증거물 당사자의 확인 서명을 받는 등의 여러 노력이 있으나, 기술적으로 디지털화하여 저장 및 보존해야 할 필요성은 존재한다.

따라서 본 논문에서는 조금 더 안정적이고 신뢰할 수 있는 관리를 위해 블록체인을 기반으로 디지털증거의 정보나 해시를 관리하는 시스템을 구현하고자 제안한다.

II. 구현 배경

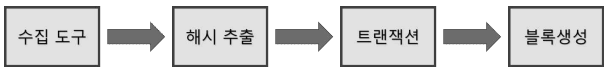
2.1 디지털증거 해시의 탈중앙화 관리 개념

최근 4차 산업 혁명과 관련하여 많은 이슈로 떠오른 기술 중 블록체인은 전 세계적으로 많은 관심을 보인다. 흔히 코인과 같은 암호화폐 시장에서 기반기술로 사용하고 있으며 블록체인의 탈중앙화라는 특성은 보안에서도 긍정적 효과를 보인다.

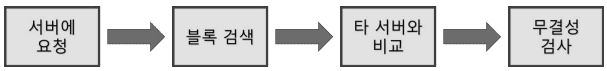


▲[그림 1] 탈중앙화 에 대한 모식도

이는 정보에 대한 신뢰성을 보장하고 있으며, 모두가 함께 보증하는 이러한 시스템에서 디지털증거의 해시와 같이 보존과 인증이 필요한 정보를 저장할 경우 효과적으로 관리를 할 수 있을 것으로 예측한다.



▲[그림 2] 탈중앙화 시스템에서 데이터 등록순서.



▲[그림 3] 탈중앙화 시스템에서 해시비교 순서.

본 논문에서 구현될 탈중앙화 시스템은 컨소시엄 블록체인(Consortium Blockchain)의 성격을 가진다. 허가된 기관에 블록체인 노드들이 위치하고, 허가된 클라이언트만이 트랜잭션을 발생시킬 수 있다. 또한 이를 확인하는 작업 또한 허가된 사람 또는 기관이 할 수 있으나, 분산되어 있다.

기본적인 과정에서는 수집 도구에서 해시를 추출한 뒤 곧바로 트랜잭션을 발생시켜 블록체인 서버에 도달하게 되는데, 블록체인 서버에서는 해당 트랜잭션을 저장하거나 블록을 생성한다. 그 뒤 다른 블록체인서버에 해당 트랜잭션과 생성된 블록을 전달하게 된다.

이러한 과정으로 모든 블록체인 서버들이 동일한 데이터를 나눠가지게 되며, 여러 블록의 연결상태를 가지고 있어 데이터의 변조 가능성이 적다.

III.구현

3.1 구현 환경

본 논문에서 구현 및 실험 환경은 다음과 같다.

프로그래밍 언어 : Java

시스템 : Windows 10

네트워크 : 내부 망 (192.168.0.0 / 24)

사용포트 : 3343(트랜잭션), 3344(검색)

3.2 트랜잭션 생성

수집된 증거물에 대하여 해시를 계산한 뒤, 해당 데이터와 함께 블록체인 서버에 곧바로 트랜잭션을 발생시킨다. 트랜잭션에 포함되는 데이터들은 다음 [그림 4]와 같다.

Transaction	
Transaction Hash	SHA256(Data + Time)
Data Hash	SHA256(Data)
Data	Data
	Case Number
	Identifier
	Sign
	File Name
	File Path
	File Size
	MD5
	SHA1
	SHA256

▲[그림 4] 트랜잭션 포함되는 데이터들

그러나 이 트랜잭션은 단순히 이 구조로 전송되는 것이 아니라 특수한 구조를 갖고 네트워크에 전송되도록 구현하였는데. 이때 전송되는 특수한 구조를 Transmit Transaction이라고 명명한다.

Transmit Transaction
Sender IP
RTTL
Transaction

▲[그림 5] Transmit Transaction 구조

Transmit Transaction에는 보내는 측의 IP가 포함된다. 이 부분의 내용은 추후 3.3 트랜잭션의 기록에서 상세하게 다루도록 한다. 또한 해당하는 트랜잭션이 몇 번을 거쳐 왔는지 확인하기 위해 RTTL이라고 하는 상수를 저장할 구조를 만들었다. TTL은 노드를 지날 때마다 숫자가 하나씩 줄어들지만 Transmit Transaction의 경우 숫자가 반대로 증가하기에 RTTL(Reverse TTL) 이라고 이름 붙였다.

3.3 트랜잭션의 기록

본 논문에서는 같은 시간에 하나의 클라이언트만 트랜잭션을 발생시킴을 기본 원칙으로 하며, 같은 시간대에 두 개 이상의 클라이언트가 트랜잭션을 발생시키지 아니함을 원칙으로 한다.

클라이언트(수집 도구)에서 발생한 트랜잭션이 처음의 서버에 도달하였을 때 RTTL 은 0을 나타내게 된다. 이때 첫 번째 서버에서는 해당하는 트랜잭션을 곧바로 저장한다. 만약 블록이 없는 경우, 새로 블록을 생성한다. 블록 생성에 대한 내용은 3.4 블록 생성 부분에서 상세하게 다루도록 한다. 트랜잭션이 기록되면 곧바로 블록체인 서버에 등록되어있는 다른 서버의 IP로 해당하는 트랜잭션을 발생시키게 되는데, 이때 RTTL 은 기존 숫자에서 1 증가한다. 또한 Sender IP 영역도 자신의 IP로 변경한 뒤 트랜잭션을 발생시킨다.

만약 두 번째 혹은 그 이상의 순서에 도달하여 RTTL 이 1 이상일 경우 Pending 영역에 트랜잭션을 보관한다. 그리고 트랜잭션을 등록하기에 앞서, Transmit Transaction 영역에 존재하는 Sender IP 영역에 명시된 서버로 검색을 요청한다. 검색결과 해당 트랜잭션이 존재할 경우 해당 트랜잭션을 등록한다. 그러나 현재 존재하는 블록의 기록 가능한 공간이 부족하거나 존재하지 않을 경우 자신에게 보낸 이전 서버에서 받은 블록을 추가하고 그 뒤로 트랜잭션을 기록한다.

그리고 트랜잭션을 발생시킬 때 Database에 로그를 저장하고, 이미 발생한 트랜잭션을 다른 서버로 중복하여 발생시키는 것을 방지하기 위해 수시로 로그에서 검색절차를 거친다.

이로써 모든 서버가 동기화된 트랜잭션을 가질 수 있게 된다.

3.4 블록의 생성

위 3.3 트랜잭션의 기록에서 설명하였듯, 트랜잭션이 들어왔으나 블록이 없는 경우 블록이 생성되는데, 단 해당하는 트랜잭션은 무조건 RTTL이 0인 상태에서만 블록을 생성할 수 있게 된다. 다른 블록체인들과는 달리 본 논문에서 구현된 블록 생성의 주체는 트랜잭션을 먼저 받은 상태에서 전체 블록체인에서 해당 트랜잭션이 기록될 공간이 존재하지 않을 때 해당 트랜잭션을 받은 서버로 정한다. 해당 서버는 블록을 생성하여 다른 서버로 전송함을 원칙으로 한다. 이때 생성되는 블록의 구조는 [그림 6]과 같다.

Block	
Block Code	1 ~ n
Header HASH	SHA256(Header)
Header	Header
Transaction[10]	Version
Extra Data	Transaction Count
	Previous block Hash
	T Root
	Created Time

▲[그림 6] 블록의 구조

블록코드는 초기 블록에 경우 1로 가지며 새로 생성될 때마다 값이 1씩 증가한다. 그리고 Header의 해시를 포함하며, Header와 Transaction 10개의 배열을 가진다. Extra Data의 경우 서버마다 자율적으로 설정할 수 있다. 이는 추후 3.5 블록 및 트랜잭션 관리에서 상세히 설명한다.

블록 Header의 경우 현재 블록의 버전과 현재 블록에 저장된 트랜잭션의 개수, 이전의 블록 Header의 해시가 있으며 트랜잭션 10개를 각각 해시 계산한 뒤 나열하여 한 번 더 SHA256 해시를 계산한 T root 가 있고, 블록이 생성된 시간 정보를 담고 있다.

블록이 생성된 직후, 다른 블록체인 서버들에 블록을 전송하게 된다. 이 때 트랜잭션과 마찬가지로 특수한 구조를 갖고 전송이 되는데 그 구조를 Transmit Block이라 명명한다.

Transmit Block
Sender IP
RTTL
Block

▲[그림 7] Transmit Block 구조

Transmit Block에서도 마찬가지로, Sender IP와 RTTL을 가진다. 다른 서버로부터 받은 트랜잭션이 존재하나 블록이 없을 때 새로 블록을 생성하지 않고 다른 서버에서 받은 블록을 등록하는 방식인데, 이때 역시 Sender IP를 참조하여 해당 블록을 보낸 서버에 질의하여 존재 여부를 확인한 뒤 본인 서버에 추가한다.

이로써 블록과 트랜잭션이 동일하게 저장되게 할 수 있으며, 더욱 용이한 기록과 관리를 할 수 있다.

3.5 블록과 트랜잭션 관리

본 논문에서 구현된 시스템에서는 한번 저장된 블록은 지우거나 변조할 수 없다. 또한 데이터들은 데이터베이스에 보관되며, 해당 블록이나 트랜잭션의 열람 또는 검색의 경우 웹사이트나 특수한 프로그램을 이용하여야만 한다.

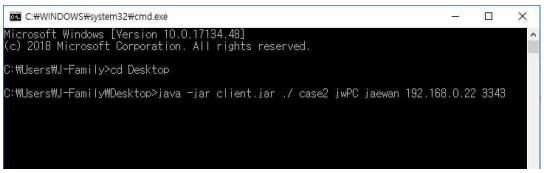
데이터베이스에 블록을 저장할 때 블록의 기본 정보와 Header만 저장하고 트랜잭션은 따로 분리된 테이블에 저장한다. 또한 소프트웨어적으로 트랜잭션과 블록을 다시 데이터베이스에서 검색해 불러와 유효성 검사를 꼭 해야 한다.

3.6 블록 검증

만약 N 번의 블록을 검증하고 싶을 경우 먼저 자신이 가지고 있는 N 번의 블록을 불러와 내부 트랜잭션들의 해시를 이용하여 T-Root와 비교하여 저장된 데이터에 문제가 있는지 확인한다. 그리고 난 뒤 Header의 해시를 계산, 현재 블록에 저장된 본인의 해시 정보를 비교한다. 만약 N + 1 번의 블록이 존재한다면 N + 1 번의 블록 Header에 저장된 이전 블록의 해시와 비교하여 N 번의 블록을 검증한다. 또한 Search를 이용하여 타 서버에 존재하는 N 블록과 Header 해시를 질의하여 결론을 도출해 낼 수도 있다.

IV.구현 결과

4.1 클라이언트 프로그램



▲[그림 8] Client 프로그램 실행 화면.

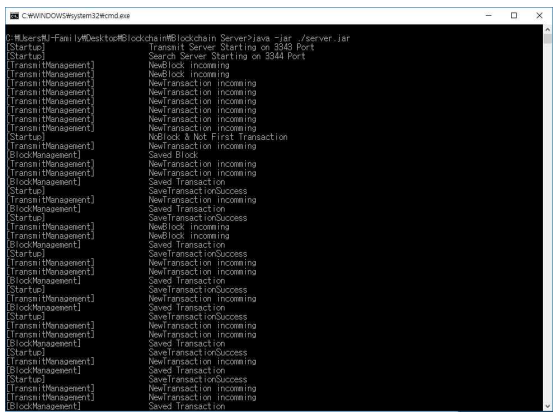
클라이언트 프로그램에서는 파일 혹은 디렉터리를 선택하면 해당하는 파일의 해시를 계산하고 부가 정보를 삽입한 뒤 트랜잭션을 생성한다.

만약 단일 파일 하나를 선택한 경우 하나의 트랜잭션이 생성되며, 디렉터리를 선택한 경우 해당하는 디렉터리 내의 모든 파일을 계산하여 각각의 트랜잭션을 발생시킨다.

하나의 파일이 하나의 트랜잭션을 이루게 되며, 해시가 같은 파일이 여러 개 존재할지라도 각각 새로운 트랜잭션이 생성되게 된다.

클라이언트 프로그램은 TUI 기반이므로 실행 시 각종 정보를 함께 추가하여 실행해야 하는데, 순서는 <파일/디렉터리> <Case Number> <Identifier> <Sign> <IP> <Port> 순이다.

4.2 서버 프로그램

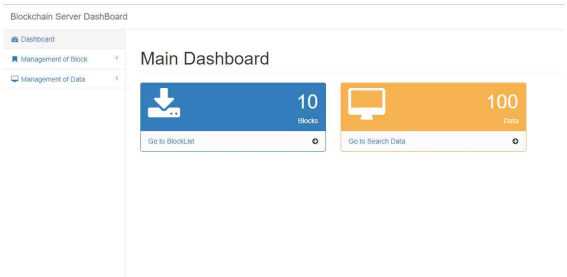


▲[그림 9] Server 프로그램 실행 및 트랜잭션 처리화면.

서버 프로그램의 경우 데이터를 수신받아 저장하고 다른 서버로 트랜잭션을 발생시켜 데이터를 분산 저장하도록 한다. 트랜잭션을 받으면 일시적으로 저장하였다가 순차적으로 처리하며,

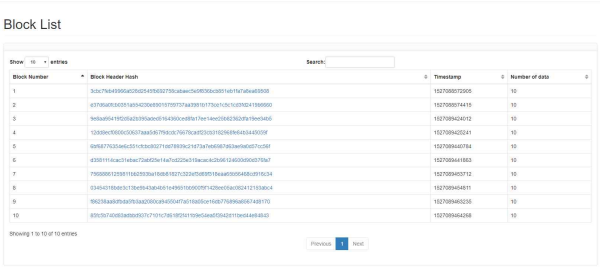
트랜잭션이 블록에 기록되기 전 받은 트랜잭션에 대해 보낸 쪽에 저장이 되어 있는지 수시로 질의하며 기록하는 데 있어서 오류를 줄인다.

4.3 조회 웹사이트



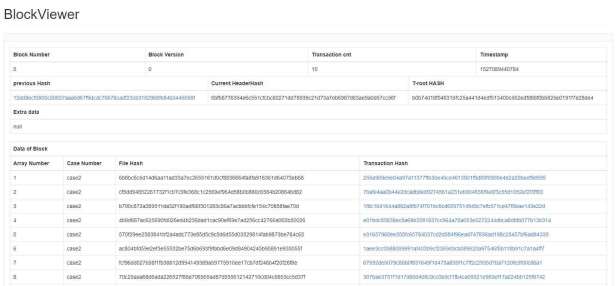
▲[그림 10] 메인 대시보드.

메인 대시보드에서는 전체 블록의 개수와 기록된 전체 트랜잭션의 수를 확인 할 수 있다.



▲[그림 11] 블록 리스트.

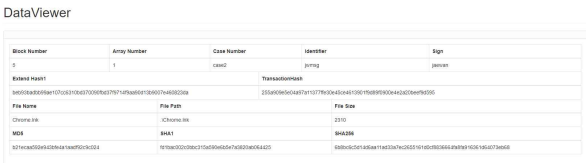
블록 리스트에서는 존재하는 모든 블록의 목록을 확인 할 수 있으며 해당하는 블록 Header의 해시를 클릭하면 블록의 상세정보를 열람할 수 있다.



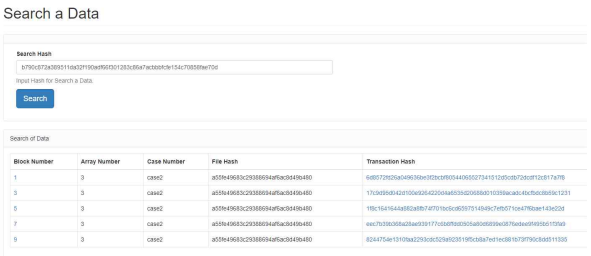
▲[그림 12] 블록 뷰어.

블록 뷰어에서는 블록에 존재하는 모든 트랜잭션의 목록과 더불어 이전 블록의 해시 등 블록에 포함된 모든 정보를 열람할 수 있다.

트랜잭션 목록에서 트랜잭션 해시를 클릭하면 해당 트랜잭션의 더욱 자세한 정보를 확인할 수 있는데, 트랜잭션에 포함된 파일의 해시와 데이터들을 볼 수 있다.



▲[그림 13] 데이터 뷰어.



▲[그림 14] 서치.

웹에서는 파일의 해시를 이용하여 발생한 트랜잭션을 검색할 수 있다. 위에서 언급하였듯 파일의 데이터가 같아 디지털증거의 해시가 일치하더라도 각자 다른 트랜잭션을 생성하여 저장하기에 여러 항목을 확인할 수 있다.

검색 시 MD5, SHA1, SHA256, 외에도 Transaction 해시까지 이용해 검색할 수 있다. 무결성을 확인하는 작업에서 해당하는 파일의 해시만 알고 있다면 저장된 데이터에서 검색하여 비교를 손쉽게 할 수 있게 된 셈이다.

Search에서도 마찬가지로 Transaction 해시 영역을 클릭하면 각자의 Transaction 정보를 열람할 수 있는 데이터 뷰어로 이동한다

.

V.결론

5.1 요약 및 기대사항

본 논문에서는 블록체인의 기술 부분을 이용하여 디지털포렌식에서 무결성을 검증하기 위한 해시와 파일의 이름과 같은 데이터들을 여러 서버에 분산 저장하면서 관리하는 시스템을 구현 및 제안했다. 본 논문에서 집중적으로 다루고자 한 부분은 증거의 해시를 보관하고 관리하는 데 있어서 안전성을 높이고 무결성을 유지하는 데 목적을 두었다. 따라서 수사관이나 수사기관에서 데이터를 관리하면서 증거로서의 무결성을 지킬 수 있다.

따라서 이번 구현 및 실험의 결과로 데이터가 안정적으로 여러 서버에 저장이 되고, 검색과 관리가 쉽게 이뤄지게 되어 추후 증거의 정보나 해시에 대한 관리가 편리해 지기를 기대한다.

[참고문헌]

[1] Satoshi Nakamoto, 『Bitcoin: A Peer-to-Peer Electronic Cash System』 pg.3

[2] National Institute of Standards and Technology [NIST](2018), 『Draft NISTIR 8202 - Blockchain Technology Overview 』 pg.15 ~ pg.19

[3] 2017 IEEE 6th International Congress on Big Data (2017), 『An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends』 pg. 559 ~ pg. 561

[4] 오세용(2017), 『블록체인을 활용한 전자거래에서 데이터 사전 유효성 검증 및 플랫폼 구현에 관한 연구』 pg.37 ~ pg. 38

암호화폐 키 관리에 의한 보안 사고 및 대응방안 연구

김근영*, 박준후*, 오원찬*, 류재철*

*충남대학교

A Study on Security Accidents and Countermeasures by Cryptocurrency Key Management

Geunyoung Kim*, Junhoo Park*, Wonchan Oh*, Jaecheol Ryou*

* Chungnam National University

요 약

본 논문에서는 암호 화폐의 키 관리로 인해 발생한 보안 사고 및 대응 방안에 대해서 연구하였다. 암호 화폐는 블록체인을 기반으로 공개키 구조를 가지며, 거래에 서명을 함으로써 화폐가 이전되기 때문에 개인키 관리가 보안에 있어서 매우 중요하다. 개인키는 하드웨어 및 소프트웨어, 웹을 이용하여 사용자가 직접 관리하거나, 거래소에서 관리가 되기 때문에 마운트곡스, 마이이더월렛, 유빗 해킹사건과 같이 개인키를 보관하는 주체에 대한 악의적인 공격이 증가하고 있다. 뿐만 아니라 Dapp과 같이 스마트 컨트랙트를 기반으로 하는 지갑이 암호 화폐를 보관하기 때문에 공격 대상이 될 수 있다. 이에 대한 대응으로 안전한 하드웨어 지갑 사용, 거래소 지갑의 보안, 스마트 컨트랙트의 안전성 검증과 같은 연구가 진행되어 왔다.

ABSTRACT

In this paper, we have studied security incidents and countermeasures caused by key management of cryptocurrency. Cryptocurrency has a public key structure based on a blockchain, and private key management is very important for security because money is transferred by signing a transaction. Private keys are managed directly by users using hardware, software, and the Web, or are managed by exchanges, resulting in an increase in malicious attacks on entities that keep private keys, such as the Mt.GOX, Myetherwallet and Yubit incident. In addition, smart contract-based wallets, such as Dapp, can be targeted because they store cryptocurrencies. In response, research has been conducted on the use of secure hardware wallets, the security of exchange wallets, and the verification of the safety of smart contracts.

I. 서론

블록체인 기술을 기반으로 하는 최초의 암호화폐인 비트코인을 시작으로 2018년 1월 기준 1500 종류 이상의 암호 화폐가 출시되었다[1]. 2세대 블록체인의 시초라고 할 수 있는 이더리움이 스마트 컨트랙트를 이용 가능한 플랫폼을 구축함으로써 최근에는 새로이 발행하는 암호 화폐의 자금은 확보하기 위한 ICO 또한 활발히 진행되고 있다. 특히 국내에서는 2018년 1월 국내 암호 화폐 거래 참여자는 300만명이상, 암호 화폐 거래를 중개하는 거래소는 18개로 국내의 암호 화폐 이용자가 활발하게 증가함을 알 수 있다[2].

암호 화폐에 사용되는 블록체인은 화폐 소유권의

이전을 나타내는 트랜잭션 내용에 전자서명을 하여 일정 시간마다 합의를 거쳐 블록 단위로 기록해 나가는 기술이다. 트랜잭션마다 표기되는 전자서명은 공개키 기반으로 구성되며, 개인키를 가진 사용자가 서명을 함으로써 트랜잭션은 완성된다. 따라서, 암호 화폐의 소유권을 증명하고 거래를 성사시키기 위해서는 개인키의 안전한 보관과 활용이 필수적으로 수반되어야 한다.

개인키를 편리하고 안전하게 관리하기 위하여 개발된 다양한 소프트웨어 및 하드웨어 지갑이 존재하고, 나아가 사용자의 계정만 있으면 별도의 소프트웨어 설치 없이 거래를 할 수 있도록 지원하는 웹 지갑, 실제 블록체인에 저장되지는 않지만 사용자에게 즉각적인 응답을 통해 거래 속도를 향상시킨 거래소 등 다양한 방식의 키 관리 방법이 제시되고 있다.

하지만, 암호 화폐에 대한 가치가 상승함에 따라 2014년 2월 마운트곡스 해킹사건[3]을 시작으로, 마이이더월렛 해킹사건[4], 유빗 해킹사건[5] 등과 같이 개인키를 획득하기 위한 악의적인 공격이 계속해서 발생되어 왔다. 이에, 블록체인 거래 환경에 대해 정확히 이해하고 개인키 관리와 지갑 해킹 사례에 따라 안전한 키 관리를 통한 신뢰할 수 있는 거래 인프라가 조성되어야 할 필요가 있다.

본 논문에서는 각종 개인키와 지갑에 의한 해킹 사고에 대해 분석하고 이에 대한 대응방안을 소개한다. 본 논문의 구성은 다음과 같다. 2장에서는 블록체인 거래 환경에 대해 설명하고 3장에서는 각종 지갑의 동작 방식과 종류, 보안 사고를 분석하였다. 4장에서는 지갑 보안에 대한 대응 방안을 제시하고 5장에서 결론을 내린다.

II. 블록체인 거래 환경

2.1 트랜잭션

암호화폐 거래를 하기 위한 지갑주소와 개인키 생성 방법은 Fig 1과 같다. 먼저 난수 생성기를 통해 256비트의 엔트로피(무작위성)를 만들어 개인키로 사용한다. 생성된 개인키에 타원곡선 곱셈 함수(ECC)를 이용하여 공개키를 생성한다. 비트코인 주소는 공개키를 이용하여 SHA256 해시를 산출한 후 그 결과값에 다시 RIPEMD160 해시를 산출한 뒤 Base58Check 인코딩을 통해 지갑 주소를 생성한다[6].



Fig 1. Wallet address generation

생성된 개인키를 이용한 서명을 통해 트랜잭션을 생성할 수 있다. 트랜잭션 모델에 따라 서명 구조가 달라진다.

비트코인 트랜잭션은 Input과 Ouput이 구분되는 UTXO(Unspent Transaction Output) 구조를 지닌다. Fig 2와 같이 UTXO구조의 트랜잭션은 송신자가 가진 트랜잭션의 UTXO로부터 새로 작성하는 트랜잭션의 Input 값과 연결된다. 이 때, UTXO는 트랜잭션의 수신자, 즉 소유주의 공개키 주소에 대응되는 개인키로 해제할 수 있는 스크립트가 존재한다. 트랜잭션 작성 시 개인키를 이용하여 스크립트를 실행하여 서명을 Input에 포함하고, Output에는 수신자의 주소를 이용하여 스크립트를 생성한다. 비트코인의 경우 특정 주소의 UTXO를 모두 더한 값이 해당 주소의 잔액이 된다.

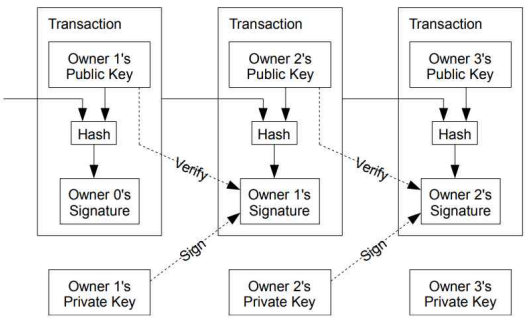


Fig 2. UTXO-based transactions[7]

이더리움은 UTXO 구조가 아닌 Account를 사용하는데, 블록이 생성될 때마다 Fig 3과 같이 Account의 상태가 변하는 상태 변환 구조를 가진다. 이더리움은 스크립트 방식의 서명 구조가 아닌 트랜잭션에 서명 값을 추가하는 방식으로 동작하며, 개인 키 사용에 대한 중복성을 방지하기 위하여 트랜잭션에 해당 계정으로부터 발생한 트랜잭션 수를 카운트하는 nonce 필드가 포함되어 있다.

또한, 이더리움의 스마트 컨트랙트도 Account를 가지는데 개인키를 가지지 않는 스마트 컨트랙트는 서명이 없는 메시지를 출력한다.

비트코인과 이더리움과 같이 개인키는 금액 소유의 증명과 동시에 거래를 위해 필요한 서명을 하는데 사용된다. 따라서 개인키를 가지고 있는 개인의 저장소와 트랜잭션을 작성하는 소프트웨어인 지갑은 해킹의 대상이 된다.

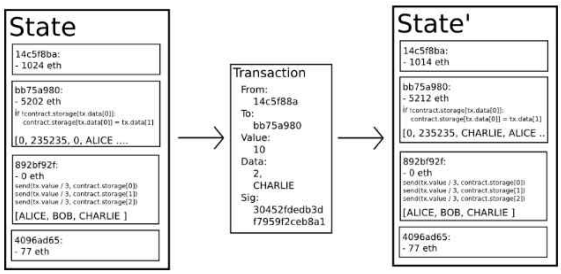


Fig 3. Account-based transactions[8]

2.2 스마트 컨트랙트

스마트 컨트랙트란 프로그래밍 가능한 계약을 의미하며, 이더리움에서 최초로 구현되었다. 이더리움의 스마트 컨트랙트는 블록을 만드는 채굴자들이 가진 가상 환경인 EVM(Ethereum Virtual Machnie)에서 실행된다. 스마트 컨트랙트를 실행하기 위한 트랜잭션을 발생시키기 위하여 수신자 주소를 스마트 컨트랙트로 하고, 호출하고자 하는 컨트랙트 내의 함수명을 트랜잭션에 작성하면 합의 시에 채굴자에 의해 스마트 컨트랙트가 실행된다.

이더리움 등의 암호 화폐에서 사용되는 스마트 컨트랙트는 개인키가 존재하지 않는다. 하지만, 스마트 컨트랙트도 주소를 가진 Account로 존재하기 때문에 화폐를 보관하는 주체가 될 수 있다. 특히, 스마트 컨트랙트를 이용한 지갑의 경우 코드에 변수 값으로 owner를 지정하여 소유주의 주소 값을 저장해두고, 추 후 소유주가 발생시킨 트랜잭션에 의해서만 출금이 가능하도록 프로그래밍 가능하다. 대표적인 암호 화폐 지갑인 Parity 사의 컨트랙트 지갑은 Fig 4와 같이 작동한다[9].



Fig 4. create parity wallet

스마트 컨트랙트가 계약 과정에서 암호 화폐를 보관하기 때문에 해커의 공격 대상이 될 수 있다. The DAO 해킹 사건[10]과 같이 DAO 컨트랙트에 보관 중인 암호 화폐를 해커의 주소로 이체하게는 등 컨트랙트 내의 취약점을 이용하여 화폐를 이전시킬 수 있기 때문이다.

III. 지갑 해킹에 의한 보안 사고

지갑은 여러 가지 형태로 존재하게 되는데 보관 주체가 개인키를 안전하게 관리하지 못할 경우 해킹 사고가 발생할 수 있다. 본 장에서는 개인키의 보관 장소에 따라 사용자 지갑, 거래소 지갑, 컨트랙트 지갑으로 분류하여 작동 방법과 보안 사고에 대해서 분석한다.

3.1 사용자 지갑

사용자 지갑은 암호 화폐 사용자가 직접 개인키를 관리할 수 있는 지갑으로 하드웨어 지갑과 웹 지갑, 데스크탑 지갑으로 나눌 수 있다.

하드웨어 지갑의 경우 USB와 같이 사용자의 개인키 접근하기 위해서는 하드웨어를 통해야 하기 때문에 온라인을 통한 해킹으로부터 안전하다. 웹 지갑은 사용자가 선택한 비밀번호로 개인키를 암호화하여 온라인으로 저장하게 된다. 암호화된 개인키가 온라인 서버에 저장되어 있으므로 인터넷에 연결된 모든 장치에서 간편하게 접근할 수 있다는 이점이 존재하지만, 비밀번호가 노출되거나 웹사이트가 다운되면 코인에 대한 접근이 불가능하다는 단점이 존재한다. 데스크탑 지갑의 경우 개인키를 사용자의 하드디스크에 저장한다. 사용자의 성향에 따라 비밀번호로 암호화 하여 개인키를 저장 할 수 있다. PC자체가 해커에게 장악되었을 경우 개인키가 해킹 당할 위험이 존재한다.

개인키를 직접적으로 관리해야 하는 사용자 지갑의 경우 PC를 장악하거나, 웹에서 유포되는 악성코드로 인해 피해를 입을 수 있다. 2017년 12월 발견된 악성코드는[12] '강남스타일'이라는 단어를 이용하여 웹을 통해 유포되었다. 해당 악성코드에 감염되면 사용자 PC에 있는 암호화폐 지갑 주소와 패스워드를 수집해 해커의 명령제어 서버로 전송한다. 또한 서버로부터 해커의 지갑 주소를 수신해 사용자가 지갑 주소를 복사하는 시점에 '클립보드'에 저장된 주소를 해커의 지갑 주소로 바꿔치기한다. 이로 인해 1억원 정도의 비트코인이 탈취된 사건이 발생하기도 하였다.

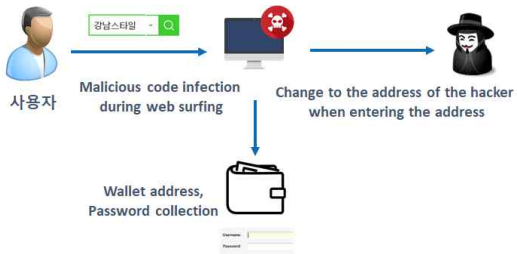


Fig 5. User wallet hacking scenario

뿐만 아니라 인기 암호화폐 지갑 서비스인 '마이이더월렛'의 경우, 인터넷 근간을 이루는 라우팅프로토콜(BGP) 및 도메인네임시스템(DNS)의 취약점을 파고들어 이용자들의 이더리움 15만 달러가 도난되기도 하였다. 해커는 BGP 하이재킹을 통해 위조된 라우팅 정보를 분산 시킴으로써 myetherwallet.com에 대한 DNS 요청을 가로 채어 러시아 서버를 주소의 정당한 소유자처럼 보이게 한 것이다.

2.2.2 거래소 지갑

거래소 지갑은 사용자가 직접 지갑을 관리하는 사용자 지갑과는 달리 개인키를 직접적으로 관리하는것이 어렵기 때문에 거래소 내부의 데이터베이스를 이용하여 암호화폐 거래에 최적화된 지갑이다.

거래소에서는 미리 많은 지갑을 생성하고, 다수의 코인을 인터넷에 연결되지 않은 콜드 월렛에 보유한다. 사용자는 거래소에 현물화폐를 이용하여 거래소 내부에서 거래되는 암호화폐를 구매하고 거래소에서는 내부 데이터베이스에 사용자의 암호화폐 정보를 저장한다[13].

대량의 암호화폐를 보관하고 있는 거래소는 해커들의 주요 타겟이 된다. 거래소 서버를 해킹한다면 많은 사용자의 개인정보뿐만 아니라 거래소가 보유한 인터넷에 연결된 핫월렛의 인키도 탈취할수 있기 때문이다. 거래소 또한 서버를 장악하기 위한 악성코드를 주로 사용한다. 최근 북한의 소행으로 보이는 공격은 Fig 6와 같다[14].

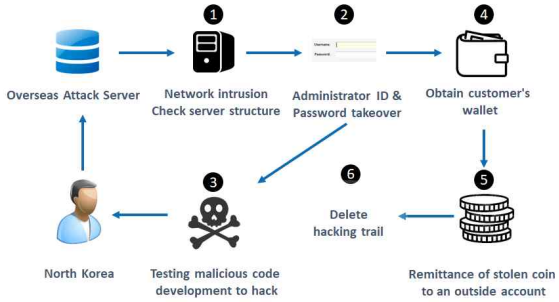


Fig 6. Cryptocurrency exchange hacking scenario

거래소를 공격하기 위한 악성코드는 '이력서' 등 관리자가 호기심을 가질 만한 제목을 사용하여 e-mail등을 통하여 유포한다. 이러한 악성코드는 기존 백신으로 탐지되지 않는 해커가 새롭게 만들어 유포하는 악성코드로, APT(Advance Persistent Threat: 지능형 지속 공격)라고 한다. 악성코드가 심어지면 패턴을 체크하고, 감시가 느슨한 시간을 골라 공격하게 된다. 2018년 2월까지의 암호화폐 거래소 피해 상황은 Table 1과 같다[15].

Domestic exchange		Contents of hacking
Youbit	Cryptocurrency stolen	· $ 5 million of bitcoin · 17% of Exchange assets
Coinis	Cryptocurrency stolen	· $ 2 million of bitcoin
Bithumb	Member information stolen	· 36,000 member's info
Overseas exchange		**Contents of hacking**
Mt. Gox	Cryptocurrency stolen	· $ 4900 million of bitcoin
Bitstamp	Cryptocurrency stolen	· $ 5 million of bitcoin
Bitfinex	Cryptocurrency stolen	· $ 63 million of bitcoin
Bitgrail	Cryptocurrency stolen	· $ 1713 million of Nano
Coincheck	Cryptocurrency stolen	· $ 5280 million of Nem

Table 1. Exchange's cryptocurrency hacking case

3.3 컨트랙트 지갑

컨트랙트 지갑은 스마트 컨트랙트 코드를 사용하는 지갑이다. 또한 스마트 컨트랙트를 사용하는 형태의 어플리케이션을 Dapp(Distributed APPlication)이라 한다. Dapp은 컨트랙트 코드를 기반으로 동작하기 때문에 컨트랙트 코드 상의 취약점으로 해킹을 당할 수 있다. 2017년 7월에 발생한 Parity wallet 해킹 사건에 대한 내용은 다음과 같다[16].

Parity wallet을 생성하면 지갑에 대응되는 스마트 컨트랙트를 생성한다. 생성된 컨트랙트는 초기설정 코드로 소유자를 지정한다. 초기 설정 코드가 스마트 컨트랙트 코드 상의 결함으로 누구나 실행하여 소유자를 변경할 수 있었다(delegate call). 이 결함에 의해 해커에게 153,037 ETH를 도난당하는 사건이 발생했다. Fig 7은 취약한 코드(맨 윗줄)와 수정된 코드(두번째 줄)를 보여준다.

```
- function initWallet(address[] _owners, uint _required, uint _daylimit) {
+ function initWallet(address[] _owners, uint _required, uint _daylimit) only_uninitialized {
    initDaylimit(_daylimit);
    initMultiowned(_owners, _required);
  }
```

Fig 7. Vulnerability of parity wallet

Ⅳ. 대응방안

4.1 사용자 지갑 보안

사용자 지갑은 대부분 핫월렛을 사용하기 때문에 인터넷이 연결되어 있는 온라인 상태에서는 수많은 위험에 노출되어 있다. 그렇기 때문에 보다 안전한 방법은 Table 2와 같이 하드웨어 지갑을 사용하는 것이 바람직하다[17]. 하드웨어 지갑을 분실하더라도 최초 설정시 알려주는 24개의 영어 단어를 통해 언제든지 복구 가능하다.

Type	Trezor	Ledger Nano S	KeepKey
Shape			
Crypto currency	14 support	27 support	10 support
LCD	O	O	O
FIDO	O	O	X
PIN	O	O	O
Restore	O	O	O
Price	$99	$99	$129

Table 2. Comparison of hardware wallet

하드웨어 지갑을 사용할 수 없을 때에는 개인키를 암호화 한 파일에 보관을 하는 방법과 개인키를 종이에 적어놓고 안전하게 보관하는 종이 지갑(Paper Wallet)등을 이용하여 최대한 안전한 곳에서 관리해야 한다.

4.2 거래소 지갑 보안

상대적으로 많은 거래가 일어나는 거래소 지갑에서는 온라인에 가장 많이 노출될 수 밖에 없다. 그렇기 때문에 최소한의 거래금액만을 핫월렛에 보관하는 것이 좋다. 2017년 9월, 과학기술정보통신부에서는 가상통화 예치금의 70% 이상을 콜드월렛에 유지하도록 권고안을 내리기도 하였다[18].

또한 핫월렛 지갑의 보안을 강화하기 위해서 멀티시그 지갑을 사용한다. 주요 국내 거래소(코인원,코빗)에서 제공하는 멀티시그 지갑의 경우 비밀키 3개를 제공하여 위험을 분산하고, 거래소가 해킹 당해도 사용자의 암호화폐를 안전하게 보호 할 수 있는 심층 보안 시스템이다. 암호화키를 분배 할때에는 시크릿 쉐어링(Secret Sharing) 방법을 사용하여 암호화키를 안전하게 공유한다[19].

4.3 컨트랙트 지갑 보안

Dapp 지갑의 경우 스마트 컨트랙트로 동작한다. 스마트 컨트랙트 또한 프로그래밍 언어의 일종이라 볼 수 있기 때문에 구현 과정에서 코드상의 결함이 있을 수 있다. 따라서 스마트 컨트랙트를 안전하게 사용하기 위해서는 코드 감사가 필요하다. 이에 대한 도구로는 Symbolic Execution을 이용하여 바이트 코드레벨에서 취약점을 찾아내는 도구인 OYENTE[20], 스마트 컨트랙트를 바이트코드에서 Solidity로 변환해주는 디컴파일러인 Porosity[21], 바이트 코드를 LLVM 비트 코드로 변환하여 요약 실행을 통해 취약점을 찾아내는 ZEUS[22] 등이 있다.

뿐만 아니라 이러한 취약점 탐지 기술을 이용하여 스마트 컨트랙트 안정성 검증 서비스인 fujitsu[23](Fig 8)를 활용하여서 개발 시에 스마트 컨트랙트에 대한 보안을 강화할 필요가 있다.

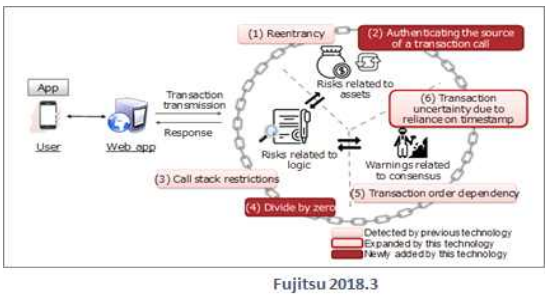


Fig 8. Contract stability verification service

Ⅴ. 결론

본 논문에서는 암호화폐 지갑의 작동원리와 종류, 그리고 실제 보안 사고를 통해 발생할 수 개인키 탈취 사례에 대한 분석과 그에 대한 대응방안을 연구하였다. 개인키의 안전한 보관을 위해 사용자의 각별한 주의가 요구되며, 콜드월렛인 하드웨어 지갑 등을 이용하는 것 뿐만 아니라 거래소 및 지갑을 제공해주는 공급자는 사용자의 개인키 보관을 위해 더욱 더 안전한 보안 대책을 강구하여야 한다.

Acknowledgement

이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (2018-0-00251, 스마트 컨트랙트 프라이버시 보호 및 취약점 분석 기술개발)

References

[1] Cryptocurrency market, https://coinmarketcap.com/

[2] Korea's exchange, https://namu.wiki/w/암호화폐 거래소

[3] Mt. Gox hacked, https://www.wired.com/2014/03/bitcoin-exchange/

[4] Myetherwallet hacked, https://twitter.com/myetherwallet/status/988830652526092288

[5] Youbit hacked, http://www.hankookilbo.com/v/846d71ef368a483db1c9e6173f28338e

[6] Andreas M. Antonopoulos, Mastering Bitcoin: Programming the Open Blockchain 2nd Edition. 2014

[7] NAKAMOTO, Satoshi. Bitcoin: A peer-to-peer electronic cash system. 2008.

[8] BUTERIN, Vitalik, et al. A next- generation smart contract and decentralized application platform. white paper, 2014.

[9] Parity wallet soruce code, https://github.com/paritytech/parity/releases

[10] The DAO attacked, http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/

[11] Crypto currency wallet, https://www.buybitcoinworldwide.com/wallets/

[12] Malicious codes stealing virtual money wallets, https://www.hauri.co.kr/security/notice_view.html?intSeq=461&page=1

[13] Exchange's wallet http://www.sporbiz.co.kr/news/ articleView.html?idxno=176043

[14] North Korea's cryptocurrency hacking , http://news.joins.com/article/22348215

[15] Exchange attacked, http://it.chosun.com/news/article.html?no=2845905&sec_no=1

[16] Parity wallet hacked, http://www.boannews.com/media/view.asp?idx=55898

[17] Hardware wallet, https://www. buybitcoinworldwide.com/trezor-keepkey-ledger/

[18] The voluntary regulation of the exchange, http://www.sporbiz.co.kr/news/articleView.html?idxno=176043

[19] secret sharing, https://en.wikipedia.org/wiki/Secret_sharing

[20] OYENTE, https://github.com/ethereum/oyente

[21] Porosity, Safety inspection tool https://github.com/comaeio/porosity

[22] ZEUS, http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2018/02/ndss2018_09-1_Kalra_paper.pdf

[23] Fujitsu, Smart contract safety validation Service, http://www.fujitsu.com/global/about/resources/news/press-releases/2018/0307-01.html

2018 한국정보보호학회 하계학술대회

A2 네트워크 1

최 대 선 (공주대학교)

- **스마트 계약 언어에서 함수 호출의 안전성 향상을 위한 코드 재작성 기법**
  이수연, 정형근, 조은선
- **6LoWPAN Neighbor Discovery 주소 등록 분석 및 취약점 평가**
  한상우, 박창섭
- **웹 크롤링을 이용한 교통정보 수집 기법**
  박세진, 윤지원
- **ZigBee 프로토콜에서의 향상된 인증 방안에 관한 연구**
  조정석, 곽 진

스마트 계약 언어에서 함수 호출의 안전성 향상을 위한 코드 재작성 기법*)

이수연* 정형근** 조은선***

*충남대학교 컴퓨터공학과

Code rewriting techniques for improving the safety of function calls in smart contract languages

Sooyeon Lee*, Hyungkun Jung**, Eun-Sun Cho***

*Department of Computer Science and Engineering, Chungnam National University.

요 약

Solidity에서 다른 계약의 함수를 호출할 때 특정 문제로 인해 호출할 수 없으면 fallback함수가 실행된다. 이 fallback함수는 임의로 작성될 수 있는 함수로 어떤 동작을 하는지 정해지지 않았기 때문에 함수의 동작을 알 수 없어 공격에 이용되기 쉽다. 그래서 본 연구에서는 개발자의 부담 없이 이러한 위험성을 줄이기 위해 전처리기를 이용한 해결방법을 제안한다.

I. 서론

Solidity[1]란 암호 화폐 중 하나인 이더리움(Ethereum)의 스마트 계약(smart contract)을 만들기 위한 high-level 언어 중 가장 널리 사용되는 것이다. 이더리움 사용자는 Solidity를 이용해서 계약을 작성해 거래에 이용할 수 있다.

하지만 Solidity는 여러 가지 취약점을 가지고 있다고 알려져 있다. 대표적인 취약점은 계약이 다른 계약의 함수를 호출하는 코드를 포함하고 있는 상태에서, 계약이 실행될 때 해당 함수가 제대로 실행되지 않는 것이다. 이 경우 실행 중 예외가 발생한 상황이므로 계약의 fallback 함수가 호출된다. 이 때 다른 계약의 함수를 호출한 계약(Caller)은 fallback함수가 호출되었는지 여부를 알 수 없고, 어떠한 동작을 하는지도 알 수 없어 공격에 사용될 수 있으므로 대표적인 취약점으로 분류되고 있다.[2]

Solidity의 이러한 위험성을 줄이는 방법들로 프로그램을 미리 분석[3][4]하거나 타입을 지원하는 새로운 언어를 제시하는 방법 등이 있었고[5] 암호적인 기법을 써서 개인정보보호를 향상시키는 방법[6] 등이 있었다. 그러나 이러한 방법들은 분산 수행되는 스마트 계약의 속성을 충분히 반영하기 어렵거나, 새로운 언어를 도입해야하는 등의 부담이 있다. 본 논문에서는 기존의 Solidity 언어 개발자들이 새로운 언어나 분석도구를 배우지 않아도 간단히 안전성을 높일 수 있는 방안을 전처리기를 통해 제공하는 방법을 소개한다.

*) 이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (2018-0-00251, 스마트 컨트랙트 프라이버시 보호 및 취약점 분석 기술개발)

II. 본문

2.1 연구 배경

2.1.1 다른 계약의 함수 호출 시 call방식

Solidity에서는 적절한 조건 아래서 다른 계약의 함수를 호출할 수 있도록 해준다. 이 때 컴파일러는 해당 함수의 시그니처 등을 가지고 처리하는 코드로 바꾼다. Solidity의 low-level 함수 호출을 살펴보면 call, call-code, delegate-call등이 있고 delegate-call방식은 call 방식처럼 다른 계약의 코드를 실행할 때 쓰이는데, 다만 계약이 실행될 때 계약을 실행시킨 계약의 context를 사용한다.

그림 1은 위에 언급한 방법 중 call함수를 이용해 다른 contract의 함수를 호출하고 있다.

```
contract B {
    address contract_A=0xcf804947e5c324c61c4f91c53fa8f14a20447aeb;
    A _a =  A(contract_A);
    function Dangerous_call(uint256 _value)  {
        contract_A.call(bytes4(sha3("f1(uint256)")),_value);
    }
}
```

그림 1 다른 계약의 함수를 호출하는 함수

call을 이용하면 계약이 다른 계약의 저장소 또는 변수에 접근하여 값을 조작할 수 있다. 이는 Java의 reflection의 메소드 invoke와 유사한 방식으로써, 주어진 주소 값을 통해서 호출하게 된다. 하지만 이러한 방식으로 계약에 대한 기능을 호출하면 계약에 대한 보안 위험성을 수반한다. 따라서 call, delegatecall, callcode등의 호출방식은 Solidity가 의도한 것과 달리 타입 안전성(type-safety)를 위배할 수 있기 때문에 세심한 주의가 요구된다.

2.1.2 Fallback 함수와 취약점

Fallback함수란 Solidity의 계약 내에 이름과 인자 없이 임의로 작성될 수 있는 함수이다. 계약 실행 중에 예외 상황이 발생하여 계약을 더 이상 실행할 수 없을 경우 실행되는 함수이다. 예외 상황이란, 계약 실행 중 특정 함수를 호출했을 때 해당함수와 일치하는 시그니처가 없거나 계약 실행 중 gas가 부족해 실행이 불가능할 때, 함수 호출 시 타입 또는 인자가 맞지 않는 상황 등을 말한다..

그림 2에서는 call함수를 이용하지 않고 직접 다른 계약을 주소를 이용해 객체로 선언하여

```
contract Alice { function ping(uint) returns (uint) }
contract Bob   { function pong(Alice c){ c.ping(42); } }
```

그림 2 계약 예시[1]

다른 계약의 함수를 호출하는 예를 보여준다. 여기서 c는 Alice의 주소를 의미한다. 하지만 'c.ping(42);' 는 잘못된 참조일 가능성이 있다. 왜냐하면 실제로 컴파일러는 ping 이라는 함수의 인터페이스가 정의되어있는지만 확인한다. 즉, c가 실제로 contract Alice의 주소인지와 Bob에 정의된 인터페이스가 실제로 Alice의 인터페이스와 일치하지 않는다. 그 때문에 Alice의 ping함수를 사용할 수 없게 되고, 'c.ping(42);' 가 실행될 때 이 함수와 시그니처가 일치하는 함수가 없는 상태가 되어 예외상황이 발생한다. 그러면 fallback함수가 자동 실행되는데, 이때 Bob은 앞서 언급한 대로 fallback함수가 호출되었는지 여부와 fallback함수의 동작을 알 수 없어 위험하다. 또한, 만약 악의적인 목적을 가진 사용자가 위와 같은 계약을 작성하고 fallback함수 내에 악성코드를 넣어둔 후에 계약이 실행된다면 본래의 fallback함수의 기능 대신 악성코드가 실행될 가능성이 있다.

2.1.3 기존 연구

기존에 존재하는 스마트 컨트랙트의 보안에 대한 연구는 Oyente[3]와 DappGuard[4]가 있다. 이 두 가지 연구는 스마트 컨트랙트의 코드의 보안을 점검해주는 도구이다. Oyente는 Mishandled exception, Transaction-ordering dependence, Timestamp dependence, Reentrancy Handling의 4가지 취약점들을 정해두고 symbolic execution을 이용해 해당 취약점들이 있는지 분석하는 도구이다. DappGuard 또한 스마트 컨트랙트 코드를 점검하는데 점검할 때 Oyente를 이용한 정적분석을 한다. 다만 Oyete보다 점검하는 취약점의 종류가 많다. 위에 언급한 두 가지 도구는 스마트 컨트랙트에 대해 취약점이 있는지 분석을 해서 사용자에게 결과를 보여주지만 보다 적극적으로 코드를 안전하게 바꿔주거나 바꿔야하는 가이드라인을 알려주지는 않

는다.

2.2 제안하는 전처리 기법

이러한 문제에 대한 해결방법으로 본 논문에서는 call방식을 이용해 다른 계약에 접근하는 코드의 존재여부를 확인하는 방법을 제안한다. 이것은 안전한 코드로 수정하는 것과 fallback 함수의 호출 여부를 개발자에게 알려 수정을 권고하는 것이다.

```
grammar Solidity;

@header{
        package kr.ac.cnu.plas;
}

sourceUnit
  : (pragmaDirective | importDirective | contractDefinition)* EOF ;

pragmaDirective
  : 'pragma' pragmaName pragmaValue ';' ;

pragmaName
  : identifier ;

pragmaValue
  : version | expression ;

version
  : versionConstraint versionConstraint? ;

versionOperator
  : '^' | '>=' | '>' | '<' | '<=' ;

versionConstraint
  : versionOperator? VersionLiteral ;

importDeclaration
  : identifier ('as' identifier)? ;
```

그림 3 Solidity 문법의 일부

그림 3은 Solidity 문법의 일부이다.

ANTLR[7]를 이용해 solidity.g4파일을 기반으로 계약을 재작성하는 전처리기를 제공하는 방법으로 문제를 해결한다. 전처리기는 그림 1에서와 같은 함수 호출 코드를 ANTLR파서로 식별한 후 개발자에게 알리는 코드를 삽입하는 형태로 재작성 한다. 그로 인해 개발자가 코드가 올바르게 사용되었는지 확인할 수 있도록 유도한다. 바이트코드를 변경하여 적용할 수도 있으나 여기서는 더 경량의 솔루션인 전처리기를 활용한다.

```
contract Alice { function ping(uint) returns (uint) }

contract Bob {function pong(Alice c) {
            c.ping(42, NONFALLBACK);
        }
        function () payable{
          .....
        }
}
```

그림 4 전처리기 실행 전 코드 예시

```
contract Bob {function pong(Alice c) {
                c.ping(42, NONFALLBACK);
                if( getfb == FALLBACK ) {
                   error
                }
        }
        function () payable{
           getfb == FALLBACK
           ......
        }
}
```

그림 5 전처리기를 실행한 후 바뀐 코드 예시

개발자가 그림 4화 같이 c.ping(42, NONFALLBACK); 이라고 fallback함수가 불리지 않기를 원하는 의사 표시를 하면, 그림 5에서 나타난 바와 같이 fallback함수가 불릴 경우 오류로 나타내주는 코드를 삽입한다. 즉, (ⅰ) c.ping함수의 주소를 계산하고, (ⅱ) (ⅰ)에서 계산된 c.ping함수가 fallback함수안지 확인하여 (ⅲ)(ⅱ)의 결과에 따라 예외처리를 해준다.

이를 위해 함수를 호출하는 코드에 위에 예시로 든 것처럼 c.ping(42, NONFALLBACK); 으로 NONFALLBACK이라는 키워드가 포함되어있다면 'if(c.getfb) == FALLBACK then error' 와 같은 조건문을 추가하여 fallback함수가 호출되었는지 확인하게 된다. 조건문을 활용하기 위해 Solidity 코드에 전처리기를 이용해서 fallback함수의 구현에 특정 상태변수 fb를 set하는 코드를 추가해야한다.

이러한 방식으로 코드를 재작성하고 나면, 실행 시 fallback함수가 실행될 경우 상태변수 fb가 설정되고, if 조건문에서 fb가 설정된 것을 확인한 후 개발자에게 알려주게 된다. 따라서 개발자는 자신이 코드 수정이 없이 전처리기를 사용함으로써 보다 안전한 코드를 작성할 수 있게 된다.

III.결론

Solidity에서 다른 계약의 함수를 호출할 때 특정 문제로 인해 호출할 수 없으면 fallback함수가 실행된다. 이 fallback함수는 임의로 작성될 수 있는 함수로 어떤 동작을 하는지 알 수 없어 공격에 이용되기 쉽다. 그래서 전처리기를 이용해 fallback함수의 body 시작에 특정 상태변수를 set하는 코드를 추가하고, 함수를 호출할 때 조건문을 이용해 함수를 호출한 계약에게 알리는 방법을 제안하였다. 이전에는 fallback 함수의 호출 여부를 개발자가 알기 어려웠지만 이 방법을 이용하면 호출 여부를 알 수 있어 코드 수정을 유도하는 장점이 있다. 현재는 별도의 전처리기를 제작하고 있다. 그러나 이 방법은 fallback함수가 실행된 후에 결과를 알 수 있다는 단점이 있다. 향후에는 해당 문제점을 보완하는 다른 방법을 고안해볼 예정이다. 또한 작성중인 전처리기는 Solidity개발환경과 별도로 수행될 것이지만 이후에는 Solidity개발환경과 통합하여 지원할 계획이다.

[참고문헌]

[1] Solidity URL : https://solidity.readthedocs.io/en/ develop/

[2] Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli, A survey of attacks on Ethereum smart contracts, Proceedings of the 6th International Conference on Principles of Security and Trust, Page164-186, April 22-29, 2017

[3] Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena and Aquinas Hobor, Making Smart Contracts Smarter, Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Pages 254-269, October 24 - 28, 2016

[4] Thomas Cook ,Alex Latham and Jae Hyung Lee, DappGuard : Active Monitoring and Defense for Solidity Smart Contracts, mit, 2017

[5] Jack Pettersson and Robert Edström, Safer smart contracts through type-driven development Using dependent and polymorphic types for safer development of smart contracts Master's thesis in Computer Science Department of Computer Science and Engineering Computing Science Division Chalmers University of Technology and University of Gothenburg Gothenburg, Sweden 2016

[6] Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In Proceedings of the 2016 IEEE Symposium on Security and Privacy, SP '16. IEEE Computer Society, 2016

[7] ANTLR URL : http://www.antlr.org/

6LoWPAN Neighbor Discovery 주소 등록 분석 및 취약점 평가*

한상우, 박창섭

단국대학교

6LoWPAN Neighbor Discovery Address Registration Analysis and Vulnerability Assessment

Sang-Woo Han, Chang-Seop Park

Dankook University

요 약

IEEE 802.15.4 기반의 6LoWPAN은 다양한 IoT (Internet of Things) 응용 프로그램을 위한 사실상의 표준 플랫폼이다. 저 전력 무선 개인 영역 네트워크 (LoWPAN, Low-power Wireless Personal Area Network)를 부트스트랩 하려면 각 장치가 고유 한 IPv6 주소를 각 장치에 할당 할 수 있도록 6LoWPAN-ND (6LoWPAN Neighbor Discovery) 주소 등록을 수행해야한다. 적절한 보안 메커니즘이 없다면, 6LoWPAN-ND는 손상된 노드 공격을 포함한 다양한 보안 공격에 취약하다. 몇 가지 보안 메커니즘이 제안되었지만 IEEE 802.15.4 홉 바이 홉 보안에 의존하기 때문에 만족스럽지 않다. 본 논문에서는 6LoWPAN-ND 주소 등록을 분석하고 이전 연구에서의 보안 취약점을 논의한다.

I. 서론

IETF (Internet Engineering Task Force) 는 무선 센서 네트워크를 저전력 무선 개인 영역 네트워크 (LoWPAN, Low-power Wireless Personal Area Network) 로 규정하였고, IEEE 802.15.4 [1] 는 LoWPAN의 MAC / PHY 계층을 위한 사실상의 표준이다. 6LoWPAN [2, 3]은 IEEE 802.15.4와 같은 저 전력의 손실이 많은 링크를 통해 IPv6 패킷을 전송할 수 있게 하는 IoT 네트워크 프로토콜이다. LoWPAN 내의 자원이 제약적인 디바이스는 6LoWPAN Border Router (6LBR)를 통해 IPv6 인터넷 호스트에 연결될 수 있다. LoWPAN과 상호 운용되는 IoT 네트워크 아키텍처의 보안 문제는 데이터 영역과 제어 영역의 두 영역에서 발생한다. 데이터 영역에서 Clinet - Server 모델에서의 CoAP(Constrained Application Protocol) [4] 또는 Subscriber-Publisher 모델의 MQTT (Message Queuing Telemetry Transport)[5]를 통해 교환되는 애플리케이션 데이터는 종단 간 보안을 보장하기 위해 보호되어야한다. 제어 영역에서는 다양한 보안 위협으로부터 IoT 네트워크 인프라를 보호하기 위해 신호 메시지를 보호해야 한다. 본 논문에서는 IEEE 802.15.4 기반의 6LoWPAN의 제어 평면과 관련된 보안 문제를 조사하고 이전에 제안된 연구들에 대한 보안 분석을 제시한다. 2장에서는 IEEE 802.15.4 와 6LoWPAN-ND에 대한 배경 지식을 설명하고, 3장에서는 6LoWPAN-ND 주소 등록과 관련된 보안 문제를 조사한다. 4장에서는 이전 연구들에 대한 보안 분석을 수행한다. 마지막으로 5장에서 결론을 맺는다.

* 본 연구는 과학기술정보통신부 및 한국인터넷진흥원의 "고용 계약형 정보보호 석사과정 지원사업"의 연구결과로 수행되었음. (과제번호 H2101-18-1001)

* 본 논문은 2018년도 정부(교육부)의 제원으로 한국 연구재단의 지원을 받아 수행된 기본 연구지원사업 성과임. (NRF-2017R1D1A1B03027862)

II. IEEE 802.15.4 와 6LoWPAN-ND 배경 지식

본 장에서는 IEEE 802.15.4 기반의 LoWPAN 환경에 대한 분석을 수행하고, 6LoWPAN Neighbor Discovery 주소 등록 프로토콜을 설명한다.

2.1. IEEE 802.15.4 기반 LoWPAN

IEEE 802.15.4 기반 LoWPAN은 FFD (Full Functional Device) 또는 RFD (Reduced Functional Device)와 같은 디바이스로 구성되며 64bit의 Long MAC Address로 식별된다. FFD는 활성화 된 후에

자체적인 LoWPAN 설정을 통하여 LoWPAN을 관리하는 PC (PAN Coordinator)의 역할을 수행할 수 있다. 설정이 완료되면 각 디바이스들은 FFD를 통해서만 LoWPAN에 가입할 수 있게 된다. Fig.1.과 같이 새로운 디바이스 I_C가 I_A, I_B 및 PC로 구성된 LoWPAN에 가입하려면 I_A로 부터 *Beacon* 메시지를 수신 한 후 가입 프로토콜이 시작된다. 새로운 디바이스 I_C는 *Association Request* 메시지를 I_A 디바이스에 전송한다. 새로운 디바이스가 LoWPAN에 참여하도록 허용되면 I_A는 16비트의 Short MAC Address가 포함 된 *Association Response* 메시지로 응답한다. 따라서 LoWPAN의 각 디바이스에는 Short MAC Address(*MAC16*)와 long MAC Address(*MAC64*)의

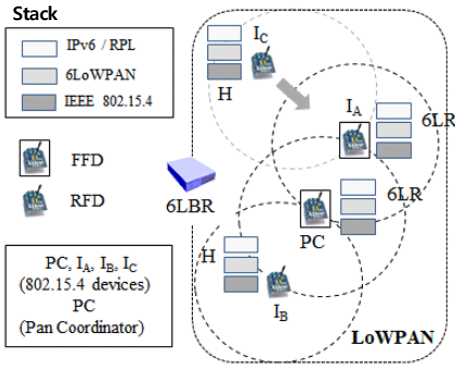


Fig. 1 . IEEE 802.15.4 based LoWPAN

두 가지 유형의 MAC 주소를 가지게 된다. 모든 디바이스는 서로의 범위 내에 있는 다른 디바이스와 통신 할 수 있다. 그러나 새로운 디바이스 IC는 IEEE 802.15.4가 다중 홉 통신을 지원하지 않기 때문에 2 홉 거리에 있는 PC로 데이터 프레임을 보낼 수 없다.

IEEE 802.15.4 기반 LoWPAN의 멀티 홉 통신은 Layer 2 Forwarding ("Mesh-Under" Routing)과 Layer 3 Forwarding ("Route-Over" Routing)의 두 가지 방식으로 지원 될 수 있다. IPv6 헤더 압축 및 단편화 외에도, 6LoWPAN은 Layer 2 Forwarding을 지원 한다 [2, 3]. 6LoWPAN 스택이 각 디바이스의 IEEE 802.15.4 스택 위에 추가되면 디바이스는 데이터 프레임을 여러 홉 거리에 있는 다른 디바이스로 보낼 수 있다. 또한 각 디바이스는 6LBR (6LoWPAN Border Router)를 사용하여 인터넷 상의 모든 호스트와 IPv6 패킷을 교환 할 수 있다. 이 경우, 각 디바이스는 6LoWPAN 호스트 (H)가 된다. 반면 Layer 3 Forwarding은 RPL 스택이 6LoWPAN의 상단에 추가 될 때 가능하다. IEEE 802.15.4 기반 LoWPAN이 Layer 3 Forwarding을 지원하면, 각 디바이스는 6LoWPAN 노드 (6LN)가 된다. 6LN은 6LoWPAN 호스트 (H)와 6LoWPAN 라우터 (6LR)의 두 가지 유형으로 나뉜다. 6LR은 IPv6 패킷을 LoWPAN 내부로 라우팅 할 수 있는 FFD가 역할을 수행할 수 있다. LoWPAN 외부의 인터넷 호스트와 통신하기 위해 각 6LN은 6LoWPAN Neighbor Discovery (6LoWPAN-ND)을 수행하여 IPv6 접두어 및 인터페이스 식별자 (*IID*) [6]로 구성된 자체 IPv6 주소를 구성할 수 있다.

2.2. 6LoWPAN Neighbor Discovery

6LoWPAN 및 RPL 프로토콜을 지원하는 IEEE 802.15.4 디바이스 (6LN)가 LoWPAN에 처음 배포되면 LoWPAN에 가입하기 위한 프로토콜과 IPv6 주소 구성을 위한 프로토콜의 두 가지 부트스트랩 프로토콜을 수행해야 한다. 그 결과, 각 6LN은 LoWPAN 내에서 사용될 주소인 Link Local Address와 전역적으로 사용될 주소인 Global Unicast Address의 두 가지 유형의 IPv6 주소를 구성한다.

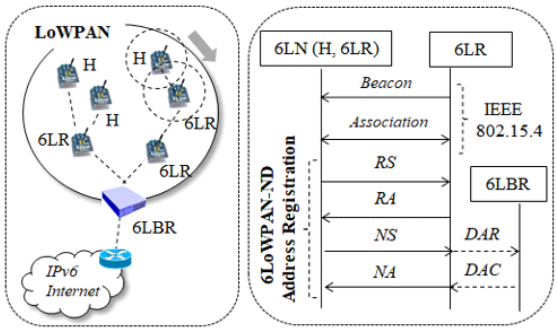


Fig. 2. 6LoWPAN neighbor discovery for address registration

Fig. 2.에 보이는 바와 같이, *RS* (Router Solicitation) 및 *RA* (Router Advertisement) 메시지는 6LN 과 6LR 사이에서 교환되며, 여기서 *RA* 메시지는 6LBR 정보(*Prefix*..)를 포함한다. *RA* 메시지를 수신 할 때, 6LN은 자신의 Long MAC Address (*MAC64*) 또는 Short MAC Address (*MAC16*)에서 파생 된 6LN의 인터페이스 식별자 인 *IID*와 *Prefix*를 사용하여 고유한 Global Unicast Address 인 *GP* = *Prefix* :: *IID*를 구성 할 수 있다. 생성 된 *GP*의 고유성을 보장하고 6LBR에 등록하기 위해 6LoWPAN-ND 주소 등록 프로토콜 [Protocol 1] [6]을 수행해야 한다.

[Protocol 1] *Address Registration*

6LN → 6LR : *RS*
6LN ← 6LR : *RA {6LBR_Info}*
6LN → 6LR : *NS {Addr}*
6LR → 6LBR: *DAR {Addr}*
6LR ← 6LBR: *DAC {Status}*
6LN ← 6LR : *NA {Status}*

6LN이 *Addr* = *(MAC64, GP16, LT)*를 갖는 Neighbor Solicitation (*NS*) 메시지를 전송할 때, *MAC64*는 LoWPAN 내에서 6LN의 유일한 식별 값이 된다. *NS*를 수신한 6LR은 중복 주소 확인을 위한 Duplicate Address Request (*DAR*) 메시지를 통해 6LBR에게 *Addr*를 전달한다. 6LBR은 LoWPAN에 등록 된 모든 6LN의 *(MAC64, GP16, LT)* 항목을 유지하는 Duplicate Address Detection (*DAD*) 테이블을 사용하여 *GP16*이 중복 주소인지 여부를 확인할 수 있다. *LT*는 (MAC64, GP16)의 등록 수명을 나타내며,

그 동안 *DAD* 테이블에 항목이 유지된다. 6LBR은 중복 검사 결과(*Status*)를 *DAC* 메시지를 통해 6LR로 전송하고, 6LR은 *NA* 메시지를 통해 6LN에게 결과를 전달한다.

III. 6LoWPAN 주소등록 및 보안

주소 등록 프로토콜 [Protocol 1] 은 IEEE 802.15.4 hop-by-hop 보안이 6LoWPAN-ND 메시지 (*RS / RA / NS / NA / DAR / DAC*)의 무결성을 위해 시행된다고 가정한다. 이 가정은 접근 제어 문제를 해결하기 위해 만들어졌으며, 즉 사전 공유 키를 가진 6LN만이 LoWPAN에 액세스 할 수 있다는 것을 나타낸다. 그러나, 일반적으로 6LN은 개방 환경에 배치되기 때문에 권한이 부여 된 6LN에 동일한 키가 배포된 경우 손상된 노드 문제로 인해 키가 유출 될 수 있다 [7]. IEEE 802.15.4 홉 바이 홉 보안의 일환으로 대칭키 설정 프로토콜에 대한 많은 연구가 이뤄졌지만 아직 많은 문제가 남아있다. 4장에서 이전 연구가 IEEE 802.15.4 홉 바이 홉 보안에 적합하지 않는 이유에 대해 논의 한다.

손상된 노드 공격이 가능하다고 가정하면 6LoWPAN-ND 주소 등록에 대한 두 가지 유형의 공격이 가능하다. 하나는 합법적 인 6LN 또는 6LR을 위장하여 공격하는 방법과 다른 하나는 6LoWPAN-ND 메시지에 대해 변조 공격을 수행하는 방법이다. 두 가지 공격 모두 정상적인 주소 등록을 방해하는 리디렉션 및 스푸핑 공격을 유도할 수 있다. *RS* 메시지를 제외하고 다른 다섯 개의 6LoWPAN-ND 메시지는 메시지의 악의적 인 변조로부터 보호되어야 한다. *RA* 메시지가 보호되지 않으면 메시지를 통해 전달된 *prefix* 정보를 수정하여 6LN에 구성된 *GP16*이 유효하지 않게 할 수 있다. 6LBR의 *DAD* 테이블에 $(MAC64_3, GP16_3, LT_3)$의 항목이 있다고 가정한다면, 공격자는 $(MAC64_3, GP16_3, 0)$을 포함하는 *NS* 메시지를 6LBR에게 전송하고 해당 메시지가 처리 된다면 기존 항목의 등록이 취소되고 $GP16_3$ 이 다른 6LN에 할당 될 수 있게 된다. TABLE 1은 본 논문에서 사용 된 표기법을 보여준다.

TABLE 1 NOTATIONS

Notation	Description
$6LN_j$	6LoWPAN nodes, j = 1, 2, 3, …
$MAC16_j$	short (16-bit) MAC address of $6LN_j$
$MAC64_j$	long (64-bit) MAC address of $6LN_j$
$GP16_j$	global unicast address of $6LN_j$ derived from $MAC16_j$
LT_j	(registration) lifetime of $6LN_j$
$Addr_j$	$(MAC64_j, GP16_j, LT_j)$
Ctr_j	counter value maintained by $6LN_j$ and 6LBR
K_G	global key shared among all the 6LNs
K_j	device key pre-shared between $6LN_j$ and 6LBR
K_{ji}	link key shared between $6LN_j$and$6LN_i$
$h(.)$	cryptographic hash function
$Auth_N(K_j)$	Authenticator generated by $6LN_j$
$Auth_B(K_{ji})$	Authenticator generated by 6LBR
$E_K(m)$	encryption of $m$withsymmetrickey$K$
$MIC(K)$	message-integrity code computed with a key K covering all preceding messag e fields

IV. 관련 연구 분석 및 취약점 평가

본 장에서는 3장에서의 취약점을 해결하기 위해 제안된 관련 연구에 대한 분석을 수행한다. 분석은 취약점 해결 여부에 초점을 두고 진행하며, 새로운 문제 발생 여부를 조사한다.

4.1. Lightweight SEND for 6LoWPAN-ND 분석

경량 SEND (L-SEND) [10]는 LoWPAN 내부의 주소 도난 및 위장 공격으로 부터 IPv6 주소의 소유자를 보호하기 위해 제안되었다. $6LN_3$은 *6LBR_Info*로부터 구성된 $Addr_3 = (MAC64_3, GP16_3, LT_3)$을 안전하게 등록하기 위해 EC 공개 키 PK_3와 개인 키 PR_3를 생성해야 한다. 그 후, 생성된 PK_3을 사용하여 암호화 식별자 $CID_3 = h(PK_3, param)$를 계산한다. *param*은 부가적인 공개 파라미터이고, CID_3는 $MAC64_3$과 함께 $6LN_3$을 식별하기 위해 사용된다. Fig. 3.에 보이는 바와 같이, $6LN_3$은 6LR을 통해 6LBR에 ① $NS\{Addr_3, CID_3\}$ 메시지를 전송할 때 *Nonce*를 전송 받는다. 그 후, $\{Addr_3, Nonce, PK_3\}$ 를 PR_3를 사용하여 *Sig* 값을 생성하고 *NS* 메시지에 포함하여 6LBR로 전송한다. *Sig*가 유효하고 $GP16_3$이 아직 할당되지 않은 경우 주소 등록은 성공적으로 이루어진다. Fig. 3.과 같이, 기존의 6LoWPAN-ND 어드레스 등록 프로토콜 [프로토콜 1]에서 보안을 보장하기 위해 ① 및 ②가 추가되었다.

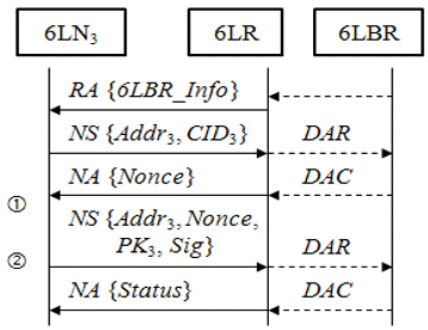


Fig. 3. Lightweight SEND

L-SEND의 주요 목적은 주소가 6LBR에 등록 된 뒤, $GP16_3$이 *DAD* 테이블에서 악의적으로 등록 취소되지 않도록 보호하는 것이다. L-SEND는 IEEE 802.15.4 홉 - 바이 - 홉 (hop-by-hop) 보안을 사용하여 보안이 유지된다고 가정하였지만, 손상된 노드 공격 하에서 L-SEND의 몇 가지 보안 약점이 관찰되었다. 첫 째, L-SEND는 6LN이 LoWPAN에 가입한 뒤 IPv6 주소를 등록 할 수 있다는 점에서 접근

제어 문제를 해결하지 못한다. 이로 인해 공격자는 *DAD* 테이블을 과부하 시키기 위해 6LBR에 많은 IPv6 주소를 등록하는 공격을 수행할 수 있다. 둘째, *RA* 메시지의 무결성이 보장되지 않기 때문에 위조된 *6LBR_Info*를 사용하여 6LN의 주소구성을 방해할 수 있다. 셋 째, *SIG*를 계산하기 위한 ECDSA 알고리즘은 많은 계산 부담을 야기하므로, 공격자는 임의로 생성한 *SIG*가 포함된 *NS* 메시지를 6LBR에게 다량 전송하여 계산 량 부하를 야기 시킬 수 있다. 넷 째, L-SEND는 *NS* / *NA* 메시지의 추가적인 교환이 필요하다.

4.2. Network Admission Control Protocol 분석

Network Admission Control (NAC) 프로토콜 [8]은 IEEE 802.15.4 hop-by-hop 보안을 가정하지 않고 기존 6LoWPAN-ND 주소 등록 프로토콜 [Protocol 1]에 보안을 직접 내장하였다. 이는 대칭 키 메커니즘을 사용하여 6LoWPAN-ND 메시지를 보호하는데 기반을 둔다. NAC 프로토콜은 다음과 같은 사전 조건 수행 및 필요를 가정한다. 첫 째, 인증 된 각 6LN은 6LBR과 고유 한 대칭 키 *Kn* 을 미리 공유하고, 전역 키 K_G는 6LBR을 포함하여 모든 인증 된 6LN 간에 공유된다고 가정한다. 둘 째, 6LBR은 승인 된 6LN 목록을 관리한다. 셋 째, 6LN이 LoWPAN에 참여할 권한이 있는지 확인하기 위한 두 개의 메시지 (*Challenge* 및 *Response* 메시지)가 새로 정의된다.

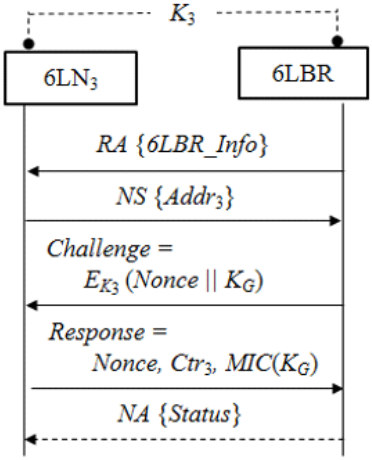


Fig. 4. Network Admission Control Protocol

Fig. 4.에 보이는 바와 같이, 6LBR이 $6LN_3$의 *NS* 메시지를 수신하면 *Nonce*를 생성하여 *Challenge* = E_{k_3} *(Nonce* || K_G*)*를 계산하여 전송한다. *Challenge*를 수신한 $6LN_3$은 응답 메시지인 *Response = Nonce, Ctr*$_3$*, MIC(*K_G*)*를 계산하여 응답한다. 여기서 *Ctr*$_3$은 응답 메시지의 신선도에 대한 카운터 값이고 *MIC(*K_G*)*는 무결성 검증에 사용된다. 6LoWPAN-ND 주소 등록이 성공적으로 완료 되면 6LBR은 각 6LN에 인증 된 6LN 목록을 배포한다. 따라서 NAC 프로토콜은 안전한 6LoWPAN-ND 주소 등록 프로토콜이며 이전의 주소 등록이 만료되기 전, 즉 *LT* 값을 높이기 위한 주소 재등록에도 사용될 수 있다.

그러나 우리는 NAC 프로토콜의 몇 가지 약점을 발견했다. 첫 째, NAC 프로토콜은 6LN 과 6LBR 간 단일 홉 거리의 LoWPAN환경에만 적용될 수 있다는 점에서 제한적이다. 둘 째, *RA*와 *NS* 메시지가 보호되지 않기 때문에, $6LN_3$은 위조 된 *prefix* 정보를 기반으로 IPv6 주소를 구성하고 위조된 6LBR과 연결될 수 있다. 셋 째, 6LBR에 대한 인증이 수행되지 않기 때문에 상호 인증이 지원되지 않는다. 넷 째, 전역키가 사용됨에 따라 하나의 6LN이 손상되면 전체 LoWPAN이 손상 될 수 있다. 이러한 약점은 NAC에 대해 다음과 같은 보안 공격을 초래할 수 있다.

[Protocol 2] ***Rogue 6LBR Attack***

$6LN_3$ ← Adv: *RA {6LBR_Info*$_{Adv}$*}*
$6LN_3$ → Adv: *NS {Addr*$_3$*}*
$6LN_3$ ← Adv: *Challenge**
$6LN_3$ → Adv: *Nonce*, Ctr*$_3$*, MAC(*K_G*)*

첫 째, 공격자 Adv는 위조된 6LBR 공격을 통하여 정상적인 노드의 연결을 방해하고 위조된 6LBR로의 연결을 야기할 수 있다. $6LN_3$이 6LBR에 대한 초기 주소 등록을 이미 완료했다고 가정한다. 공격자 Adv은 위조된 *prefix* 정보인 *Prefix*$_{Adv}$를 토대로 생성한 *6LBR_Info*$_{Adv}$를 *RS*메시지를 통하여 브로드캐스트로 전송한다. 메시지를 수신한 $6LN_3$은 *Addr3 = (MAC64*$_3$*, GP16*$_3$*, LT*$_3$*)*을 재구성하여 *NS* 메시지로 응답한다. *Challenge* =* E_{K3} *(Nonce * || KG)*가 초기 주소 등록 중에 6LBR에 의해 사용되고 Adv에 의해 관찰되었다고 가정하면, 그것은 $6LN_3$에 재생되어 사용될 수 있다. 해당 응답 메시지가 생성 되더라도 더 이상 처리될 필요가 없기 때문에, 결과적으로 정상 6LBR과의 연결이 종료되고 불량 6LBR과의 새로운 연결이 시작된다.

[Protocol 3] ***Man-In-The-Middle Attack***

$6LN_3$ → Adv : *NS {Addr*$_3$*}*
Adv → 6LBR : *NS {Addr*$_{Adv}$*}*
$6LN_3$ ← Adv ← 6LBR*: Challenge*
$6LN_3$ → Adv → 6LBR*: Response*

둘 째, NAC 프로토콜은 *MITM Attack*이 발생할 수 있다. $6LN_3$과 6LBR 사이의 공격자 Adv는 $6LN_3$ 이 전송하는 *NS* 메시지를 가로 채고 자신의 *Addr*$_{Adv}$로 수정 한다. *Addr*$_3$ *= (MAC64*$_3$*, GP16*$_3$*, LT*$_3$*)*은 *Addr*$_{Adv}$ *= (MAC64*$_3$*, GP16*$_3$*, 0)*로 수정되어 6LBR에게 전송된다. 그 후, Adv는 *Challenge* 및 *Response* 메시지를 중계한다. 그러나, Adv의 *LT*$_3$ *= 0*의 변조 공격으로 인하여 6LBR의 *DAD* 테이블에 있는 $6LN_3$ 항목은 영구적으로 제거되고 *GP16*$_3$은 다른 6LN에 할당 될 수 있게 된다.

4.3. 관련 연구 및 취약점 분석

위의 분석들로 안전한 주소 등록을 위해서는 6LoWPAN-ND 메시지의 보호가 필요하다는 점이 확인되었다. 본 절에서는, 6LoWPAN-ND 메시지의 보호를 위해 제안된 보안 기법에 대해서 설명하고 그에 따른 취약점 분석을 수행한다.

훼손된 노드 공격이 가능하다면, IPv6 주소가 네트워크 내에서 고유 한 경우 모든 디바이스가 네트워크에 참여할 수 있기 때문에 SEND [9]와 L-SEND [10] 프로토콜은 허가받지 않은 디바이스가 기존 네트워크에 참여하는 것을 보호할 수 없다. 위의 문제에 대한 연구의 일환으로, 안전한 6LoWPAN-ND를 위한 몇 가지 연구가 제안되었는데, 대부분은 6LN과 6LR 간의 키 인증 및 설정에 중점을 두었다. [11, 12]에서, 6LBR 또는 키 서버는 6LN의 공개키를 분배하기 위한 키 분배 서버의 역할을 하며, 공개키 연산은 6LowPAN-ND 메시지를 보호하기 위해 사용된다. [13]에서, Authentication Server (AS) 는 인증된 6LN만이 LoWPAN에 가입하도록 허용 할 수 있다. 하지만, 디바이스 ID에 대한 기밀성은 제공하지만 6LoWPAN-ND 메시지의 기밀성은 제공하지 않는다.

IEEE 802.15.4는 LoWPAN에서 hop-by-hop 보안을 위한 몇 가지 보안 기능을 제공한다. 그러나 IEEE 802.15.4 표준에서는 키 관리 문제가 해결되지 않았았다. 그렇기 때문에, 현재 IEEE 802.15.4 기반 LoWPAN의 두 디바이스 간에 키를 설정하는 방법은 사전 키 분배, 키 분배 센터 (KDC)의 사용 및 인증서 접근 방법을 권고하고 있다. 첫 째, 사전 키 분배 [14, 15]는 하나 이상의 대칭 키 또는 키 재료를 각 디바이스에 미리 로드하여 각 디바이스 쌍 간에 대칭 키를 공유 할 수 있도록 한다. 그러나 많은 디바이스가 다중 홉 LoWPAN에 배포되어야 하므로, 이 방법은 각 디바이스에서 상당한 메모리 공간을 사용하게 한다. 둘 째, KDC 기반 접근법에서 [16, 17], Pan Coordinator (PC)는 키 분배 센터의 역할을 수행한다. 디바이스 I_A가 다른 디바이스 I_B와 대칭 키를 설정하기 위해, I_A는 PC의 대칭 키를 요청한다. PC는 키를 생성하여 I_A와 I_B 두 디바이스에 전송한다. 셋 째, 인증서 기반 접근법은 인증서를 소유 한 두 디바이스가 Authenticated Key Establishment (AKE)를 수행 할 수 있다는 점에서 확장 가능하다. 그러나 수백 바이트 크기의 X.509 인증서를 사용하면 LoWPAN에 적합하지 않으므로 6LBR에서 단편화 및 재조립으로 인해 성능이 저하된다. IEEE 802.15.4 프레임 크기가 127 바이트로 제한된다는 점을 감안할 때, 수십 바이트 크기 인 ECQV 인증서 [18, 19]의 사용은 두 디바이스 간에 경량 AKE를 위해 제안되었다. PC는 6LoWPAN에 가입하는 디바이스에 ECQV 인증서를 발급하는 인증기관 (CA) 역할을 수행한다. 인증서 기반 접근 방식은 확장 가능하지만 ECDH (Elliptic-Curve Diffie-Hellman) 키 교환으로 인해 디바이스에 상당한 연산량 부하를 유발할 수 있다.

V. 결론

본 논문에서는 6LoWPAN-ND 주소 등록과 관련된 보안 문제를 조사했다. 또한 기존의 6LoWPAN-ND의 취약점을 보안하기 위해 제안된 연구들을 분석한 결과, 자원 제약적인 환경인 LoWPAN 환경에 적합하지 않음을 발견하였다. 향후, 이전의 취약점들을 분석하여 안전한 6LoWPAN-ND 보안 메커니즘을 구상하고 기존의 연구와 비교 분석을 수행하고자 한다.

[참고문헌]

[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] J. Hui and P. Thubert, “Compression Format for IPv6 Datagrams over IEEE 802.15.4-based Networks,” IETF RFC 6282, Sep. 2011.

[4] Z. Shelby, K. Hartke, and C. Bormann, “The constrained application protocol (CoAP),” IETF RFC 7252, Jun. 2014.

[5] ISO/IEC 20922:2016: Information technology - Message Queuing Telemetry Transport (MQTT) v3.1.1, International Organization for Standardization, Jun. 2016.

[6] Z. Shelby, S. Chakrabarti, E. Nordmark, and C. Bormann, “Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs),” IETF RFC 6775, Nov. 2012.

[7] K. F. Krentz, H. Raflee, and C. Meinel, “6LoWPAN Security: Adding Compromise Resilience to the 802.15.4 Security Sublayer,” in Proc. of Int’l Workshop on Adaptive Security, article no. 1, Zurich, Switzerland, Sep. 8-12, 2013.

[8] L. Oliveira, J. Rodrigues, A. Sousa, and V. Denisov, “Network Admission Control Solution for 6LoWPAN Networks Based on Symmetric Key Mechanisms,” IEEE Trans. on Industrial Informatics, vol. 12, no. 6, pp. 2186-2195, Dec. 2016.

[9] J. Arkko, J. Kempf, B. Zill, and P. Nikander, “Secure Neighbor Discovery,” IETF RFC 3971, Mar. 2005.

[10] P. Thubert, B. Sarikaya, and M. Sethi, “Address Protected Neighbor Discovery for Low-power and Lossy Networks,” IETF 6lo

WG Internet-Draft, draft-ietf-6lo-ap-nd-06, Feb. 2018.
[11] S. Misra, S. Goswam, C. Taneja, A. Mukerjee, and M. Obaidat, “A PKI Adapted Model for Secure Information Dissemination in Industrial Control and Automation 6LoWPANs,” IEEE Access, vol. 3, pp. 875-889, 2015
[12] Y. Qiu and M. Ma, “A Mutual Authentication and Key Establishment Scheme for M2M Communication in 6LoWPAN Networks,” IEEE Trans. on Industrial Informatics, vol. 12, no. 6, pp. 2074-2085, Dec. 2016.
[13] A. Esfahani, G. Mantas, R. Matischek, F. B. Saghezchi, J. Rodriguez, A. Bicaku, S. Maksuti, M. Tauber, C. Schmittner, and J. Bastos, “A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment,” IEEE Internet of Things Journal, 2017.
[14] L. Eschenauer and V. Gligor, “A Key Management Scheme for Distributed Sensor Networks,” in Proc. of 9th ACM conference on Computer and Communications Security (ACM-CCS), pp. 41-47, Washington D.C., U.S.A., Nov. 18-22, 2002.
[15] H. Chan, A. Perrig, and D. Song, “Random Key Pre-distribution Schemes for Sensor Networks”, in Proc. of the IEEE Symposium on Security and Privacy, 2003, pp. 197-213, Washington D.C., U.S.A., May 11-14, 2003.
[16] ZigBee-2007, ZigBee-2007 Specification, ZigBee Alliance, USA, 2008.
[17] B. W. Kim and C. S. Park, “Secure and Energy-Efficient Join-Leave Operations in ZigBee Network,” KSII Trans. on Internet and Information Systems, vol. 7, no. 11, pp. 2874-2892, Nov. 2013.
[18] 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.
[19] C. S. Park, “A Secure and Efficient ECQV Implicit Certificate Issuance Protocol for the Internet of Things Applications,” IEEE Sensors Journal, vol. 17, no. 7, pp. 2215-2223, Apr. 2017

웹 크롤링을 이용한 교통정보 수집 기법1)

박세진*, 윤지원**
고려대학교 정보보호대학원 정보보호학과

Traffic Information Collection Method Using Web Crawling

Sejin Park*, Jiwon Yoon**
Graduate School of Information Security, Korea University.

요 약

현존하는 다양한 기법의 교통정보 수집 기법들은 설치 및 운영비, 인건비 등을 포함한 인적·물적 자원이 요구된다. 또한 설치 구간에 따른 공간적 범위의 제한, 유효표본수에 따른 한계, 시간 또는 날씨 환경에 따른 오류발생 등 다양한 한계점이 존재하고 있다. 이에 대한 대안으로 본 논문에서는 웹 크롤링(web crawling)을 이용한 교통정보 수집을 제안한다. 이는 적은 자원으로 많은 양의 정보를 얻을 수 있으며, 다양한 웹 문서로부터 다양한 종류의 데이터들을 얻을 수 있다는 장점이 있다. 본 연구의 목적은 웹 문서 기반의 데이터 수집을 통해 이를 정형화하고, 추후에는 이를 활용하여 어떤 방식으로 실시간 교통정보 예측 알고리즘을 설계할 것인지에 대해 설명한다.

I. 서론

디지털 지도는 차선정보, 가드레인, 도로 곡률 및 경사, 신호등 위치, 교통 표식 등 시스템에 필요한 3차원 도로 환경정보를 수십 센티미터 수준의 정확도로 제공한다. 이는 단순 내비게이션보다 더 자세한 정보를 담고 있다는 의미에서 정밀지도(High Definition, HD 혹은 Highly Automated Driving, HAD)라고 부른다. 정밀지도를 구축하려면 고가 장비를 갖춘 측량 차량 여러 대가 도로 곳곳을 하나하나 탐색하는 작업을 거친 후 특수 소프트웨어나 수작업 등의 후처리 공정을 통해 정보를 추출해야 하는데, 이러한 방법은 많은 인적·물적 자원이 요구된다.

이러한 모든 정보는 주행 판단 및 제어에 영향을 미치므로 상당히 중요한 요소라 볼 수 있다. 차량에 탑재된 다양한 장치가 높은 수준의 정확도를 제공하도록 하는데, 대표적 장치들로는 고정밀 GPS, 관성항법장치(INS), 360도 카메라, 3차원 레이저 스캐너 등이 있다.[1]

이러한 방법 외에도 GPS 구간 검지 방식 기반의 교통정보 수집[2], 하이패스 단말기를 이용한 교통정보 수집[3], V2V기반 교통정보수집체계[4][5]와 관련된 연구들도 진행되고 있다.

본 연구는 웹으로부터 많은 양의 데이터를 수집하고 이를 가공하여 유의미한 정보만을 추출하는 웹 크롤링 기법을 이용해 뉴스, 블로그, SNS, 관공소 홈페이지 등으로부터 수집된 다양한 유형의 웹 문서로부터 신뢰도 높은 데이터를 활용하여 정형화된 데이터 형식으로 가공하는 기법을 통해 빠르고 적은 비용으로도 가능한 교통정보 수집에 대해 제안하고자 한다.

1) 이 논문은 2018년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(R7117-18-0161, 자율주행 스마트자동차용 이상징후 탐지핵심기술개발)

II. 관련 기법

교통정보를 수집하기 위한 기법으로 지점 검지 기술과 구간 검지 기술로 구분할 수 있다.

2.1 지점 검지 기술[2]

2.1.1 차량 검지 시스템(Vehicle Detection System, VDS)

차량 검지 시스템은 도로 본선에 매설하여 교통정보를 수집하는 매설형 검지가와 도로 본선이 아닌 도로변에 설치하여 수집하는 비매설형 검지기로 구분할 수 있다. 매설형 검지기로는 루프, 자기 등이 있으며 대부분 루프가 많이 사용되고, 비매설형 검지기로는 영상, 초단파, 적외선, 초음파 등이 있으며 현재 영상이 가장 많이 사용된다. 차량 검지 시스템은 해당 도로 지점에서 차로 별로 통과하는 개별 차량의 속도, 차량 길이, 점유율, 통과시간 등의 정보를 수집하여 일정 주기(예로 1분, 5분)로 교통정보를 센터에 제공하게 된다.

유지관리 용이성은 비매설형이 매설형에 비해 좋지만 운용비용은 매설형이 저렴하고, 설치 및 운용비용은 수명주기에 따라 다음 식과 같이 계산한다. (n: 운영년수, i: 이자율)

수명주기비용 = [(장비단가*수량)+설치비용]*

$$[\frac{i(1+i)^n}{(1+i)^n-1}]$$+연간유지보수비용

2.1.2 폐쇠회로 텔레비전(Closed-Circuit Television, CCTV)

폐쇠회로 텔레비전은 비디오카메라를 이용하여 특정 장소의 상황에 대해 동영상 정보를 수집하는 기술로 도로변에 설치되어 직접 육안으로 교통상황을 관찰할 수 있다. 이를 이용해 실시간으로 모니터링이 가능하며 수집된 정보를 바탕으로 돌발 상황 검지가 가능하다.

시스템은 그림1과 같이 현장 시스템과 센터 시스템으로 구성되며, 현장에서 교통정보 비디오를 수집하여 센터로 전송하면 센터 내에서 상황판으로 전송하여 표출한다.

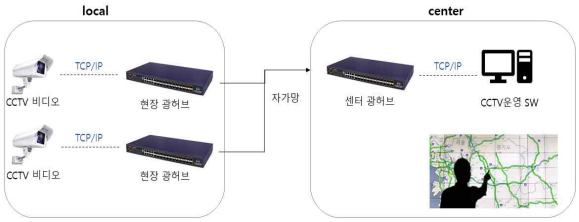


그림 1 폐쇄회로 텔레비전의 시스템 구성

정보 이용자에게 직접적인 영상 제공이 가능하므로 현장의 실시간 교통상황을 효율적으로 제공할 수 있으며 검지영역의 변경 및 설정이 센터 내에서 가능하다는 장점이 있지만, 영상수집 영역의 잘못된 선정으로 정보수집의 오류가 발생할 수 있으며 검지영역의 공간적 범위가 제한적이라는 한계가 있다.

2.2 구간 검지 기술[6]

2.2.1 차량 자동 인식 장치(Automatic Vehicle Identification, AVI)

도로 특정 구간의 상·하단 지점을 통과하는 차량을 대상으로 그림 2와 같이 차량의 두 지점의 검지시간 차이와 검지기 간 거리 차를 이용하여 구간속도, 통행시간 등의 정보를 생성하는 기술이다. 이는 설치 지점의 모든 차량을 대상으로 차량 번호판 정보를 판독하여 정보를 수집하는데, 이러한 번호판 판독기술은 일부 주차장에서 입차 또는 출차 하는 차량의 번호판을 판독하기 위한 시스템에도 이용된다.

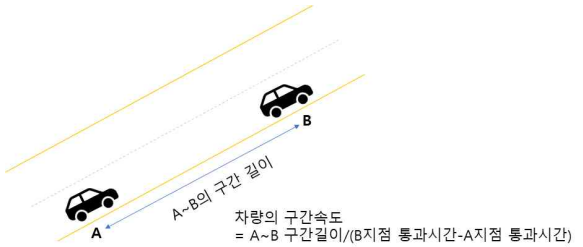


그림 2 차량 자동 인식 장치 기법

수집된 정보의 높은 신뢰성은 유효 표본수가 확보될 때 가능하며, 유효표본수를 많이 확보하기 위해서는 도로가 교차하는 지점과 같이 회전 교통량이 적은 곳에 설치를 해야 한다. 대부분의 고속도로와 수도권 북부 일반국도의 경우

는 5km간격으로 설치한다.

이 기술은 무선통신기술이 아닌 검지기 중 유일하게 가장 정확한 구간 정보를 생성할 수 있다는 장점이 있으며 유효표본수만 충분히 획득할 수 있다면 신뢰도가 높은 정보를 얻을 수 있다. 그러나 안개 낀 날씨나 어두운 시간대처럼 차량 번호판 인식이 어려운 조건에서는 판독 오류의 가능성이 높다.

2.2.2 비콘

무선 노변 센서와 소형 기지국이라는 전용 통신망을 통해 실시간 차량의 주행정보를 수집하는 구간 검지 교통정보 수집 서비스를 의미한다. 이는 프로브 차량의 단말기로부터 수집되는 정보를 가공하여 제공하는 방식이며, 정보수집을 위해 RF비콘 방식과 DGPS방식을 혼합하여 차량 주행정보를 실시간으로 수집하는 구간 검지 교통정보 시스템이다. 비콘 시스템은 프로브 차량, 비콘, 기지국, 교통정보센터 등으로 구성되어 있으며, RF 모듈이 장착된 프로브 차량이 도로를 주행할 때 교차로에 설치되어있는 비콘이 신호를 교통정보센터로 송신하고 수집된 교통정보는 기지국을 통해 실시간으로 교통정보센터로 전송한다.

상대적으로 설치 및 운영비가 저렴하고 시스템이 간단하고 용이하며 구간속도의 정확도가 상대적으로 우수하다는 장점이 있지만, 통신 속도가 상대적으로 느리며 한 주기(1.7초)에 3대 차량의 데이터만 받을 수 있다는 한계가 있다.

III. 제안 기술

이 절에서는 웹 크롤링 기법을 이용하여 교통정보를 수집하고 이를 정형화된 형식으로 저장하는 기법에 대해 설명하고 있으며, 이를 활용하여 추후에는 실시간 교통 예측 시스템을 설계하고 이를 기존 내비게이션과 비교하여 정확도를 측정하고 검증할 예정이다. 정형화된 상태로 공개되어 있는 정형화 교통정보와 비정형화되어 있는 상태로 가공이 필요한 비정형화 교통정보로 구분지어 웹으로부터 데이터를 크롤링하며, 이때 데이터 구조는 다음과 같이 정의한다.

road	TEXT	`road` TEXT
direction	TEXT	`direction` TEXT
msg	TEXT	`msg` TEXT
date	DATETIME	`date` DATETIME
time	DATETIME	`time` DATETIME
weekday	TEXT	`weekday` TEXT
weight	TEXT	`weight` TEXT

그림 3 데이터 구조

3.1 정형화 교통정보 수집 기법

정형화 교통정보는 웹 사이트(한국도로공사, 국가 교통정보센터, 민원 24, 기상청 등)에서 제공하는 데이터로 정형화되어 있는 상태이므로 쉽게 정보 수집이 가능하다. 이를 이용해 실시간 교통량, 집회 및 시위, 스포츠 경기 일정, 각종 행사 일정에 대한 정보를 수집한다.

3.2 비정형화 교통정보 수집 기법

비정형화 교통정보는 갑작스러운 폭발 및 화재 사건이 발생하거나 불법 집회, 지역 내 행사 등 사전에 조사되지 않는 정보들에 해당한다. 특히 교통흐름과는 무관하게 보이는 대형 유통업체의 개점일, 마트 휴무일 등은 주변 교통 혼잡도에 큰 영향을 주기 때문에 뉴스, SNS 등을 이용하여 정보를 수집할 필요가 있다. 또한 기상청의 예측과 다른 갑작스러운 기상변화 지진, 우박 등도 교통 흐름과 관련도가 높으므로 관련 키워드(예로 지진, 우박, 교통사고 등)를 포함하는 데이터를 크롤링하여 정보를 수집할 수 있다.

	road	direction	msg	date	time	weekday	weight
	필터	필터	필터	필터	필터	필터	필터
1	경부고속도로	서울방향	옥산부근(312…	2018-05-04	03:54	FRI	NULL
2	경부선	서울방향	기흥(388K)(2…	2018-05-03	22:34	THU	NULL
3	경인고속도로	인천방향	부평(14K)(1…	2018-05-03	22:29	THU	NULL
4	상주영천고속…	상주방향	동군위부근(5…	2018-05-03	22:18	THU	NULL
5	중앙고속도로	춘천방향	남산터널부근…	2018-05-03	22:11	THU	NULL
6	중앙고속도로	춘천방향	다부터널(125…	2018-05-03	22:08	THU	NULL
7	서해안고속도로	서울방향	당진(265K)-…	2018-05-03	14:05	THU	NULL
8	평택제천선	서평택방향	송탄(21.2K)(…	2018-05-02	22:04	WED	NULL
9	경부고속도로	부산방향	옥천(260K)(2…	2018-05-02	22:02	WED	NULL
10	서해안고속도로	목포방향	서평택분기점…	2018-05-02	21:00	WED	NULL
11	서울외곽선	구리방향	장수(90K)-장…	2018-05-02	20:58	WED	NULL
12	올림픽대로	김포방향	(한남대교→…	2018-05-02	20:54	WED	NULL
13	중부내륙고속…	양평방향	충주분기점부…	2018-05-02	18:52	WED	NULL
14	제2중부고속…	하남방향	하번천부근(3…	2018-05-07	22:02	MON	NULL
15	경부고속도로	부산방향	달래내(410K)…	2018-05-07	14:56	MON	NULL
16	중부내륙고속…	양평방향	남성주(73K)(…	2018-05-07	14:38	MON	NULL
17	익산장수고속…	익산방향	익산분기점부…	2018-05-07	09:05	MON	NULL

그림 4 교통정보 데이터

그림 4와같이 모든 데이터의 형식을 도로명, 방향, 메시지, 날짜, 시간, 요일, 가중치로 하였

다. 사용자가 목적지를 입력하면 이를 도로와 방향(혹은 구간)에 대한 정보로 세분화하고, 그 항목에 따른 수집된 정보를 바탕으로 그 구간에 해당하는 메시지를 읽어올 수 있다.

3.3 교통정보 예측 알고리즘

현재 교통정보센터에서 제공하는 도로별 소통상태 기준 속도는 다음과 같다.

	원활	서행	정체
고속도로	80km/h	~	40km/h
도시고속도로	50km/h	~	30km/h
국도	40km/h	~	20km/h
시내부	30km/h	~	15km/h

표 1 도로별 소통상태 기준 속도

위에서 수집한 웹 크롤링을 통한 데이터에서 msg에 해당하는 칼럼에는 해당 도로의 현재 속력에 대한 정보와 사고 및 사건에 대한 정보가 포함되어 있다. 속력에 관한 정보로 표1의 기준에 따른 도로교통 현황에 대한 알고리즘을 구현하고, 사건 및 사고에 대한 정보는 알림 메시지를 이용해 우회하도록 권고하도록 하는 알고리즘을 구현할 것이다.

또한 기상청 웹 사이트로부터 크롤링한 데이터로부터 눈이나 비에 대한 정보를 파악하여 시야확보나 노면상태로 인한 운행속도 감속(20~50%)를 고려하여 도로별 소통 상태를 제공하고, 급격한 핸들조작이나 급제동을 삼가고 전조등을 켤 것을 권고하는 알림 메시지도 함께 제공할 예정이다.

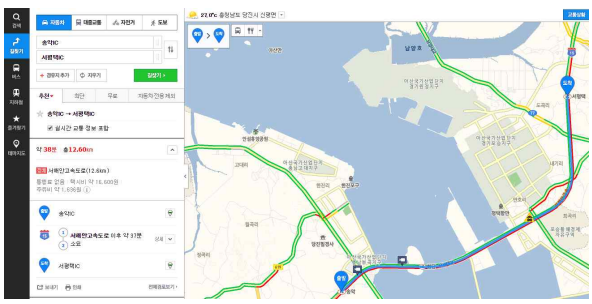


그림 5 실시간 교통정보 검색 결과

서해안고속도로	서울방향	서해대교부근(28.1K)(3차로)화물차단독사고처리중==>송악IC~서평택IC,10km정체
서울외곽선	구리방향	송내(88.2K)(3,4차로)승용차관련사고처리중==>1km정체
경부고속도로	서울방향	수원부근(390K)(4,5차로)화물차관련사고처리중==>동탄JC~수원신갈IC,6km정체
중앙고속도로	춘천방향	삼마치터널부근(348K)(2차로)화물차화재사고처리중
상주영천고속…	영천방향	영천영업소부근(89.2K)(2,3길)1톤화물차화재사고처리중
대구부산고속…	양방향	대동JCT(10.5K)(1차로)VMS설치작업중참고하시어감속안전운행하시기바랍니다.
광주원주고속…	경기광주방향	신평JC부근(54K)(1차로)승용차단독사고처리중주의운전바랍니다.
경부고속도로	부산방향	안성분기점(365K)(5차로)1톤화물차단독사고처리중주의운전바랍니다.

그림 6 크롤링을 이용한 교통정보 수집 결과

그림 5는 네이버 지도에서 송악IC로부터 서평택 IC까지의 실시간 교통정보를 검색한 결과이다. 이를 보면 거리는 총 12.60km이며 약 38분이 소요되므로 도로의 소통상태가 정체 구간이라 판단된 것을 볼 수 있다. 그러나 정체의 원인이 안개인지 사고인지 또 다른 원인이 있는지 불분명하다. 하지만 본 연구에서 제안한 크롤링 기법을 이용하여 정보 수집을 한 결과에 따르면 그림 6과 같이 정체 구간이라는 정보와 함께 화물차 사고로 인한 정체라는 것까지도 확인할 수 있도록 구현할 예정이다.

IV. 앞으로의 연구

본 연구에서는 수많은 양의 웹 문서로부터 유의미한 데이터를 추출하기 위해 키워드를 포함한 데이터를 크롤링하고 이를 정형화된 형식으로 맞추었다. 이를 통하여 추후에는 빅데이터를 활용한 실시간 교통 흐름 예측 알고리즘을 구현할 예정이며, 다른 내비게이션과 비교 및 분석을 통한 알고리즘의 정확도를 계산할 예정이다.

이 알고리즘을 통해 기존의 수집 기법을 통한 데이터 이외에도 다른 데이터를 통해 정밀한 교통 흐름을 예측할 수 있다. 특히 교통정보 기능에서 우박이나 폭우 등의 기상 상태나 교통 흐름에 영향을 미칠 수 있는 큰 행사 일정에 대한 정보를 포함함으로써 원활, 서행, 정체 등 실시간 교통상황을 편리하게 알아보고 교통 혼잡 구간을 회피할 수 있는 알고리즘을 구현함으로써 차별화된 연구 및 개발을 진행할 예정이다.

웹 문서로부터 크롤링된 데이터는 데이터의 신뢰도에 대한 한계가 존재하지만, 수많은 데이터에 대한 교차 검증 등을 통해 이를 보완한다면 적은 비용으로 정확도 높은 데이터들을 수

집할 수 있을 것으로 기대할 수 있다.

[참고문헌]

[1] https://news.samsung.com/kr/?p=364603

(출처: 삼성전자 뉴스룸)

[2] 김재민. (2004). GPS 구간 검지 방식 기반의 Network 설계를 통한 교통정보 수집 및 제공. 한국통신학회지 (정보와통신), 21(5), 70-79.

[3] 이승우, 신승중, & 유희경. (2008). 하이패스 단말기를 이용한 교통정보수집 시스템에 관한 연구. 한국인터넷방송통신학회 논문지, 8(6), 165-172.

[4] 홍승표, 오철, 김원규, 김현미, & 김태형. (2008). V2V 기반 교통정보수집체계 설계 및 요구사항분석. 대한교통학회지, 26, 251-264.

[5] Biswas, S., Tatchikou, R., & Dion, F. (2006). Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety. IEEE communications magazine, 44(1), 74-82.

[6] 도시부 간선도로 교통정보의 수집 및 제공 체계 분석(출처: 온-나라 정책연구)

ZigBee 프로토콜에서의 향상된 인증 방안에 관한 연구

조정석*, 곽 진**

*아주대학교 컴퓨터공학과 정보보호응용및보증연구실,

**아주대학교 사이버보안학과

Improved Authentication Method in ZigBee Protocol

Jeong-Seok Jo*, Jin Kwak**

*ISAA Lab., Department of Computer Engineering, Ajou University

**Department of Cyber Security, Ajou University

요 약

다양한 IoT 통신 프로토콜들 중 ZigBee 프로토콜은 제한적인 IoT 환경에 맞추어 보안 서비스를 제공하고 있다. 하지만 최근 ZigBee 프로토콜의 취약점을 분석하고 제1)시하는 연구가 다수 진행되고 있다. 본 논문에서는 ZigBee 프로토콜의 인증 과정에서의 취약점을 분석하고 개선사항을 제시함으로써 ZigBee 프로토콜의 인증 방식을 향상시키고자 한다.

I. 서론

최근 무선 네트워크 기반 IoT 기기들의 취약점에 대한 연구가 활발히 진행되고 있다. IoT 기기들이 무선 통신을 위해 사용하는 기술에는 Z-wave, ZigBee, KNX-RF, Bluetooth 등이 있으며, 이러한 기술들의 효과적인 활용을 위해 IEEE 802.15.4 표준이 제정되었다[1].

ZigBee는 IEEE 802.15.4 의 물리(PHY), 매체 접근 제어(MAC) 계층의 기능을 기반으로 동작하며, ZigBee 표준에서 정의된 NWK(네트워크) 계층과 APL(애플리케이션) 계층을 더한 형태로 구성된다[2].

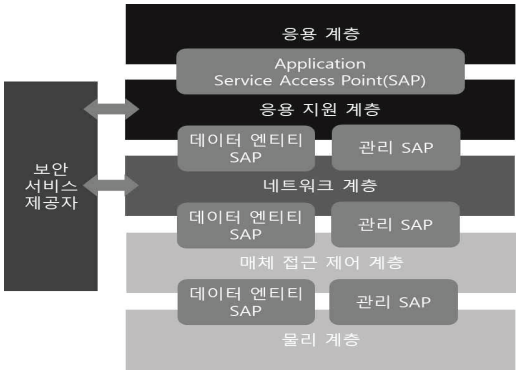
이러한 ZigBee 스택구조를 바탕으로 ZigBee 프로토콜의 인증 과정에서 Address Spoofing 취약점이 존재한다. 또한 ZigBee 프로토콜에서의 재인증을 위한 시도-응답 과정에서의 재전송 취약점 또한 존재한다.

본 논문에서는 Address Spoofing의 피해를 줄이고, 인증의 효율성을 높일 수 있는 방법을 제시하고 기기 재인증 과정에서의 시도-응답 재전송공격 방지를 위한 시도-응답 과정을 제시하고자 한다.

본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음(IITP-2018-2015-0-00403)

II. 관련 연구

2.1 ZigBee 프로토콜 스택 구조



(그림 1) ZIgBee 프로토콜 스택 구조

ZigBee 스택 구조는 (그림 1)과 같다. 해당 구조에서 ZigBee 프로토콜은 응용 계층, 네트워크 계층 그리고 보안 서비스 제공자가 함께 보안 서비스를 제공한다. 특히 해당 계층들에서 보안에 필요한 키들(마스터 키, 링크 키, 네트워크 키)에 관한 정보들이 저장되어 있다[2].

ZigBee 프로토콜은 ZigBee Coordinator(ZC), ZigBee Router(ZR), ZigBee End Device(ZED)로 구성된다. ZC는 ZigBee 네트워크에서 하나만 존재하고 네트워크제어의 기능을 수행한다. ZR은 ZED의 데이터를 수집 및 전송하는 기능을 수행한다. ZED는 데이터를 전송하는 역할을 수행하고, ZC 또는 ZR과 통신한다[3].

2.2 ZigBee 프로토콜 키 생성 및 인증 과정

ZigBee 프로토콜 키 생성 및 인증 과정은 (그림 2)와 같다. 해당 방식은 ZED가 미리 마스터 키를 가지고 있다고 가정한다. ZigBee에서는 SKKE(Symmetric-Key Key-Establishment) 프로토콜을 기반으로 키를 생성한다. 앞서 언급한 마스터 키와 랜덤하게 생성한 QEU, QEV 값들을 이용하여 링크 키를 생성한다. 생성한 링크 키를 이용해 인증을 수행한다. 인증 과정은 아래와 같다[4].

Step 1. Association Request(ZED→ZR)

ZED가 ZR에게 연결을 요청한다.

Step 2. Association Response(ZR→ZED)

ZR이 ZED의 연결 요청에 대한 응답을 전송한다.

Step 3. Update-Device(ZR→ZC)

기기 목록 갱신을 위해 ZC에게 Update-device 전송한다.

Step 4. SKKE-1(ZC→ZED)

생성한 임의의 값 QEU를 ZED에게 전송한다.

Step 5. SKKE-2(ZED→ZC)

SKKE-1를 수신한 뒤, 생성한 임의의 값 QEV를 ZC에게 전송한다.

Step 6. SKKE-3(ZC→ZED)

ZC는 확보한 QEV의 값으로 $MacTag_2$를 생성하여 전송한다.

$$MacData_2 = 03_{16} \| V \| U \| QEU \| QEV$$

$$MacTag_2 = MAC_{MasterKey}(MacData_2)$$

Step 7. SKKE-4(ZED→ZC)

ZED는 $MacTag_1$을 구성하여 전송한다.

$$MacData_1 = 02_{16} \| V \| U \| QEU \| QEV$$

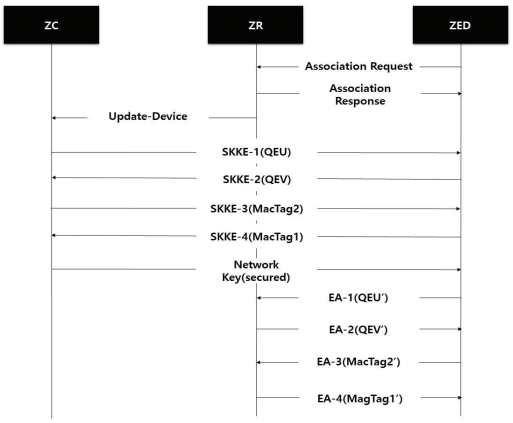
$$MacTag_1 = MAC_{MasterKey}(MacData_1)$$

Step 8. Network Key(secured)

$MacTag_1$, $MacTag_2$를 이용해 생성한 링크 키를 이용해 네트워크 키를 전송한다.

Step 9. EA-1 ~ EA-4

SKKE와의 동일한 원리로 ZR과 ZED의 인증을 수행한다.



(그림 2) ZigBee 프로토콜 인증 과정

2.3 시도-응답 인증 방식

시도-응답을 통한 인증 방식은 (그림 3)과 같다. 해당 방식은 난수와 대칭키를 이용하여 상호 인증을 수행하는 방식이다. 수행 과정은 아래와 같다[5].

Step 1. Challenge(ZC→ZED)

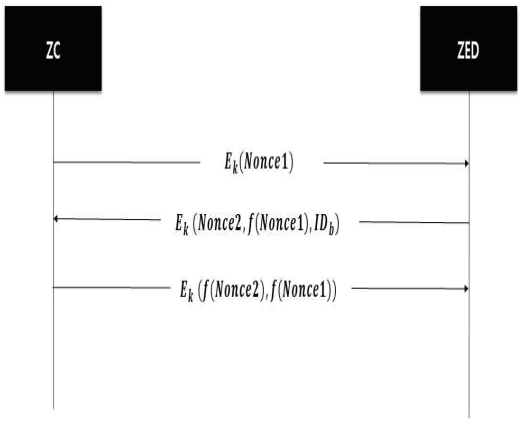
ZC가 ZED에게 생성한 난수를 암호화($E_k(Nonce1)$)하여 전송한다.

Step 2. Response(ZED→ZC)

ZED가 생성한 난수, 수신한 난수의 비트 연산 결과 값 그리고 ID를 ZC에게 암호화하여 전송한다.($E_k(Nonce2, f(Nonce1), ID_B)$)

Step 3. 비트 연산 수행(ZC→ZED)

비트 연산 결과 값들을 암호화하여 전송한다.($E_k(f(Nonce2), f(Nonce1))$)



(그림 3) 시도-응답 과정

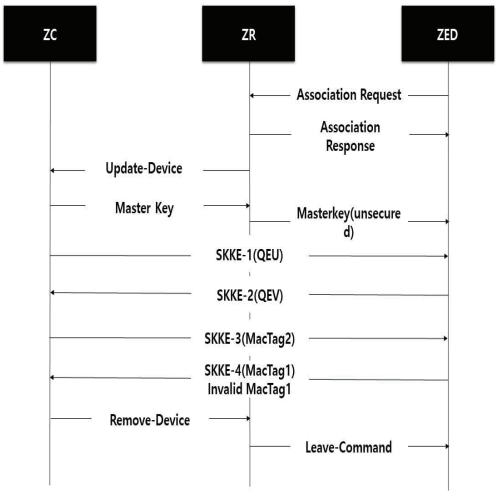
2.4 ZigBee 프로토콜 취약점

❒ ZigBee 인증 과정 자원 고갈 취약점

우선 ZigBee의 인증 과정에서 ZC는 ZED가 마스터키 소유 여부를 알 수 없으므로 공격자가 Address Spoofing 공격을 이용해 자원 고갈이 발생할 수 있다. 공격 방식은 (그림 4)와 같다.

기존의 인증 방식으로 진행할 경우 SKKE-4의 프레임에서 ZED는 마스터 키를 모르기 때문에 정상적인 MacTag1를 구성할 수 없기 때문에 ZC는 SKKE-4 값에 대한 검증이 불가능하므로 Remove-Device 과정을 수행한다.

하지만 이러한 과정 또한 ZR-ZC의 자원 낭비를 초래한다. 그 결과, 자원 고갈 공격이 성립하게 된다.



(그림 4) ZigBee 자원 고갈 공격

❒ 시도-응답 재전송 공격

ZigBee 프로토콜 기기 간 재인증 과정에서 시도-응답을 수행할 때 기존의 사용된 값들을 재전송하여 재인증을 수행할 수 있다.

III. 제안사항

3.1 ZigBee 프로토콜 인증 개선 방안

기존의 ZC, ZR, ZED의 인증 방식을 개선한 인증 방식은 (그림 5)와 같다. 해당 방식은 ZED가 미리 마스터 키를 가지고 있다고 가정한다.

Step 1. ~ ***Step 3.*** 의 과정은 기존의 인증 과정과 동일하다.

Step 4. SKKE-1(ZC→ZED)

기존의 방식과 달리 생성한 QEU를 마스터 키로 암호화($E_{MK}(QEU)$)하여 ZED에게 전송한다.

Step 5. SKKE-2(ZED→ZC)

생성한 QEV와 SKKE-1에서 복호화하여 얻은 QEU 그리고 (QEU, QEV)를 이용하여 생성한 MacTag1을 전송한다.

Step 6. SKKE-3(ZC→ZED)

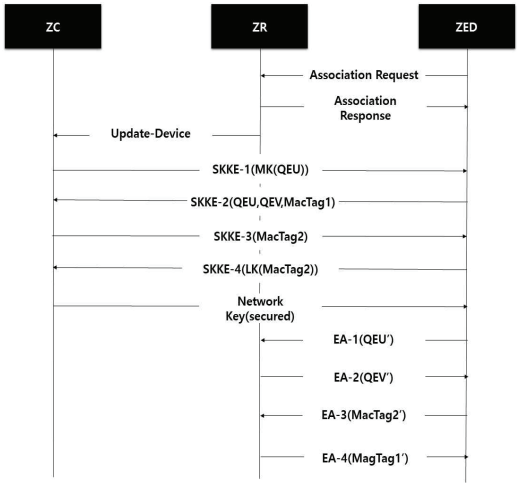
ZC는 확보한 QEV의 값으로 MacTag2를 생성하여 전송한다.

Step 7. SKKE-4(ZED→ZC)

ZED는 생성한 링크 키를 이용해 MacTag2를 암호화($E_{LK}(MacTag2)$)하여 전송한다.

Step 8. 의 과정은 기존의 인증 과정 ***Step 9.*** 과 동일하다.

위에 제시한 방안을 통해 앞서 제시한 취약점에 대한 대응이 가능하다. 우선, 지속적인 인증 시도를 통한 에너지 고갈 취약점에 대응하여 ZC, ZR의 에너지 효율을 증가시킬 수 있다. SKKE-2 과정에서 MacTag1 값과 QEU 값에 대한 검증을 통해 ZED에 대한 우선적인 검증이 가능하다. 또한 SKKE-4 과정을 통해 생성된 링크 키에 대한 검증이 가능하다.



(그림 5) ZigBee 인증 개선 방안

3.2 시도-응답 개선 방안

IoT 환경에서 인증을 위해 주로 수행하는 방법은 시도-응답이다. 하지만 기존의 시도-응답의 과정에서 공격자가 ZED로 위장했을 경우, 그에 대한 재인증을 위해 시도-응답을 수행할 경우 이전에 사용된 난수를 재전송하여 인증을 수행하는 공격이 수행 가능하다. 이에 대해본 절에서는 IoT 기기의 캐시를 이용하여 기존의 시도-응답 방안의 재전송 공격 방지를 위한 개선 방안을 제시한다. 시도-응답 개선방안은 (그림 6)과 같다.

개선된 시도-응답 수행 과정은 아래와 같다.

Step 1. Challenge(ZC→ZED)

ZC가 ZED에게 생성한 난수를 암호화($E_k(Nonce1)$)하여 전송한다.

Step 2. Response(ZED→ZC)

ZED가 생성한 난수, 수신한 난수의 비트 연산 결과 값 그리고 ID, TimeStamp값을 ZC에게 암호화하여 전송한다.

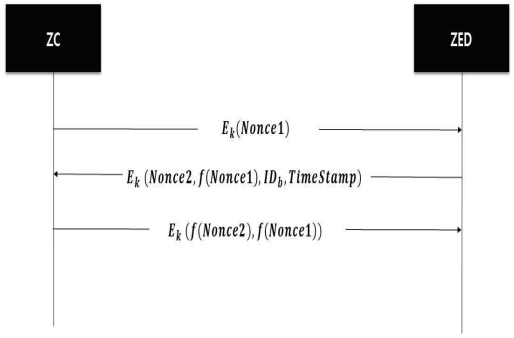
$(E_k(Nonce2, f(Nonce1), ID_B, TimeStamp))$

Step 3. 비트 연산 수행(ZC→ZED)

ZC는 수신한 값들을 점검하여 비트 연산 결과 값들을 암호화하여 전송한다.

$E_k(f(Nonce2), f(Nonce1))$

해당 개선 사항을 통해 기가 간 재인증 취약점을 개선할 수 있다.



(그림 6) 시도-응답 개선 방안

3.3 개선 방안

제시한 개선 방안을 정리한 표는 [표 1]과 같다.

[표 1] 개선 사항

	기존 방식	개선 방안
ZigBee 자원 고갈 취약점	- SKKE-4에서의 마스터 키 검증을 통한 자원 효율 감소 - 링크 키 검증 수행하지 않음	- SKKE-1에서의 마스터 키 검증을 통한 자원 효율 향상 - SKKE-4를 통한 링크 키 검증 수행
시도-응답 재전송 공격	- 재전송 공격의 취약점 존재	- 타임스탬프를 활용한 재전송 공격 방지

IV.결론

본 논문을 통해 ZigBee 프로토콜의 인증 과정과 시도-응답 과정을 분석하고 각각의 취약점을 제시하여 프로토콜 개선의 필요성을 강조하였다.

ZigBee 프로토콜 인증 과정의 자원 고갈 취약점 개선을 위한 인증 과정을 제안하였다. 해당 개선 사항은 ZC는 ZED의 마스터 키와 링크 키 검증을 통해 ZED에 대한 인증이 가능하도록 제안하였다.

또한 시도-응답 개선 사항을 통해 시도-응답에 사용되는 값들의 재전송 여부 탐지를 위한 개선사항을 제안하였다.

향후 ZigBee 프로토콜에서의 인증 방식의 전반적인 개선방안을 연구할 예정이다.

[참고문헌]

[1] Stefan Marksteiner, “An Overview of Wireless IoT Protocol Security in the Smart Home Domain”, 2017

[2] ZigBee Alliance, ZigBee Specification: ZigBee Document 053474r20, September, 2012.

[3] 김봉환, 임정미, 박창섭, “ZigBee 보안 메커니즘 분석”, 보안공학연구논문지, 제 9권 제 5호, 2012

[4] Moazzam Khan, “The Cost of Security: Performance of ZigBee Key Exchange Mechanism in an 802.15.4 Beacon Enabled Cluster”, 2007

[5] Mohammad A. Alia, “Cryptography Based Authentication Methods”, 2014

2018 한국정보보호학회 하계학술대회

A3 암호이론 1

▌한 동 국 (국민대학교)▐

- **진난수생성기에 대한 부채널 공격 및 난수성 분석 사례 조사**
  최낙준, 이지은, 김광조
- **중첩된 무한 해시체인을 이용한 Lamport OTP 확장**
  신동진, 박창섭
- **Linux OS 상에서의 커널 및 응용 LEA 암호모듈 구현 및 호출 분석**
  송행권
- **Survey of Functional Encryption and its Functionality**
  윤현도, 권현수, 허준범

진난수생성기에 대한 부채널 공격 및 난수성 분석 사례 조사1)

최낙준* 이지은** 김광조*,**

KAIST *정보보호대학원 **전산학부

Side-Channel Attack and Randomness Analysis of True Random Number Generators

Nakjun Choi* Jeeun Lee** Kwangjo Kim*,**

*Graduate School of Information Security, **School of Computing, KAIST

요 약

암호기술을 적용하는 보안 산업에서 필수적으로 사용되는 난수생성기의 결함은 보안에 직접적인 영향을 미칠 수 있으므로, 안전성을 갖춘 고성능 난수생성기를 개발하는 것이 매우 중요하다. 대부분의 진난수생성기는 물리적인 칩 형태로 존재하기 때문에 타이밍 공격 또는 오류 주입 공격 등과 같은 부채널 공격의 위험에 항상 노출될 수밖에 없으며, 실제로 난수생성기를 대상으로 유효한 부채널 공격을 성공시킨 연구들이 꾸준히 발표되고 있다. 본 논문에서는 난수생성기와 하드웨어 기반 부채널 공격들에 대해 간략히 설명하고 실제 난수생성기를 대상으로 한 부채널 공격 사례들을 소개하며, 이를 토대로 난수생성기의 부채널 공격 대응 연구의 중요성에 대해 논한다.

I. 서론

현대 사회에서 난수생성기(Random Number Generator, RNG)는 IoT, 인공지능, 데이터베이스, 정보보호 등 여러 분야에 걸쳐 매우 광범위하게 사용되고 있다. 특히 암호기술을 적용하는 보안 산업에서 필수적으로 사용되는 난수생성기의 결함은 보안에 직접적인 영향을 미칠 수 있으므로, 안전성을 갖춘 고성능 난수생성기를 개발하는 것이 매우 중요하다.

이에 따라, 물리적인 현상을 이용하여 완전한 난수를 생성하는 진난수생성기(True Random Number Generator, TRNG)의 개발이 활발하게 이루어지고 있다. 최근에는 반투명 거울을 통해 이동하는 광자, 핵붕괴 방사선원, 전자 회로의 양자 기계적 잡음 등과 같이 예측할 수 없는 양자역학적 현상을 이용하여 양자난수생성기(Quantum Random Number Generator, QRNG)의 개발이 이루어지고 있다.

하지만 대부분의 난수생성기들은 물리적인 칩 형태로 존재하기 때문에 타이밍 공격(timing attack) 또는 오류 주입 공격(fault injection attack) 등 부채널 공격의 위험에 항상 노출될 수밖에 없으며, 실제로 난수생성기를 대상으로 유효한 부채널 공격을 성공시킨 연구들이 꾸준히 발표되고 있다 [1-4]. 따라서 난수생성기의 보안성이 인정받기 위해서는 해당 난수생성기가 부채널 공격에도 안전함을 보이는 것이 매우 중요하다.

본 논문에서는 난수생성기와 하드웨어 기반 부채널 공격들에 대해 설명하고 실제 난수생성기를 대상으로 한 부채널 공격 사례들을 소개한다. 또한 이러한 공격으로 인해 난수생성기의 난수성에 어떤 변화가 있는지 비교분석하고, 이를 토대로 난수생성기의 부채널 공격 대응 연구의 중요성에 대해 논한다.

1) 이 논문은 SK Telecom Network R&D Center의 지원을 받아 수행된 연구임.

본 논문의 구성으로 Ⅱ장에서는 난수생성기와 부채널 공격에 속하는 전력 분석 공격(power analysis attack), 글리치 공격(glitch attack), 오류 주입 공격에 대해 간단하게 설명하고, Ⅲ장에서는 실제로 난수생성기를 대상으로 수행된 글리치 공격, 주파수 주입 공격(frequency injection attack), 전자기 공격(electromagnetic attack)과 같은 부채널 공격 사례들을 소개하고 그 결과를 보여준다. 마지막으로 Ⅳ장에서는 결론 및 이를 토대로 한 향후 연구 계획에 대해 논한다.

II. 배경지식

2.1 난수생성기

난수는 정의된 범위 내에서 무작위로 선정된 수를 말한다. 난수생성기를 통해 만들어진 난수는 (1) 다음으로 어떤 난수가 생성될지 예측이 불가능해야하며(unpredictable), (2) 이전에 생성된 난수와 이후에 생성된 난수간의 상관관계가 없어야하며(uncorrelated), (3) 생성된 난수가 어느 한 쪽으로 편향되지 않아야 한다(unbiased). 하지만 실제 컴퓨터 환경에서는 난수를 결정론적인 방법으로 생성하기 때문에 완벽하게 무작위인 난수를 얻기는 어렵다. 이렇게 얻어진 난수는 진정한 의미의 난수가 아니기 때문에 의사난수(Pseudo-Random Number)라 부르며 소프트웨어에서 난수를 생성하는 코드를 의사난수생성기(Psudeo-Random Number Generator, PRNG)라 한다.

난수를 생성하기 위해 사용하는 난수생성기 중 진난수생성기는 컴퓨터 프로그램이 아닌 물리적인 현상을 이용하여, 예측할 수 없는 무작위 현상을 샘플링 함으로써 난수를 생성한다. 최근에는 양자역학적 현상의 예측할 수 없는 특성을 이용한 양자난수생성기가 개발되었고 스위스 ID Quantique사의 Quantis RNG [6], SK Telecom사의 QRNG Chip [7,8]이 대표적이다.

난수생성기를 통해 만들어진 난수는 NIST STS [12], dieharder [13]와 같은 난수성 테스트 또는 비트스트림으로 표현한 결과를 분석하여 난수성을 검증한다.

2.2 전력 분석 공격

[9]에서 처음 소개 된 전력 분석 공격은 공격 대상에 직접적인 손상 또는 변형을 가하지 않기 때문에 수동(passive) 공격 및 비침입 공격으로 분류된다. 전력 분석 공격은 크게 단순 전력 분석(Simple Power Analysis, SPA)과 차분 전력 분석(Differential Power Analysis, DPA)으로 나뉜다.

단순 전력 분석은 암호 장치의 연산 과정에서 소비되는 전력 변화를 측정 후 분석하여 비밀키 등의 유용한 정보를 얻어내는 공격 방법이고, 차분 전력 분석은 측정된 전력 소모량의 통계적 특성을 비교하여 비밀키를 추정해내는 방법이다. 전력 분석 공격을 막기 위해서는 연산에 소모되는 소비전력에 무작위성을 부여하거나 중간 값을 감추는 마스킹 기법 등이 사용되어야 한다.

2.3 글리치 공격

글리치 공격은 암호처리 프로세서가 들어있는 하드웨어 장치에 가해지는 공격이며 스마트카드가 주요 공격 대상이다 [5]. 하드웨어 장치의 회로를 분석하여 외부에서 오는 전원 또는 클록 신호에 글리치 신호를 추가하는 방법을 통해 장치에 예측할 수 없는 동작이 발생하도록 한다. 스마트카드의 경우 내부 클록이 증가하여 인증 과정이 우회되는 결과를 낳기도 한다. 글리치 공격을 막기 위해서는 하드웨어 장치가 쉽게 분석되지 않도록 회로를 불규칙하게 구성해야 한다.

2.4 오류 주입 공격

오류 주입 공격은 공격 대상에게 직접 접근하여 장치의 비정상적인 동작을 끌어내기 때문에 능동(active) 공격으로 분류된다. 주로 암호 연산 과정에서 발생하는 계산상의 오류를 이용하여 유효한 결과를 얻어내는데, 이를 위해 의도적으로 전력을 낮추거나 올리고 장치의 온도를 조절하는 cold boot 공격 [10] 등의 행위를 한다.

오류 주입 공격은 공격자가 수행할 수 있는 의도적인 행위의 선택폭이 넓고 대부분의 암호 장치에 쉽게 적용할 수 있기 때문에 널리 사용되는 부채널 공격 중 하나이다.

III. 부채널 공격 사례

3.1 글리치 공격

스펜인의 Honorio 연구팀은 self-timed ring 기반 진난수생성기에 전력 글리치 공격, 클록 글리치 공격을 수행하였으며 이로 인해 편향된 난수들을 발생 시킬 수 있음을 증명하였다 [1].

원활한 전력 글리치 공격을 위해 진난수생성기의 기본 전력을 1.2V에서 0.7V로 하향한 뒤 전력 글리치를 주입하는 시간을 늘려가며 실험을 진행하였다. [그림 1]의 (a)는 기존 진난수생성기의 난수 출력을 비트스트림으로 표현한 결과이고 (b)와 (c)는 각각 62.5μs, 187.5μs 동안 전력 글리치 신호를 주입한 결과이다 [1]. 주입 시간이 길어질수록 난수성이 감소하는 모습을 통해 공격의 유효성을 확인 할 수 있다.

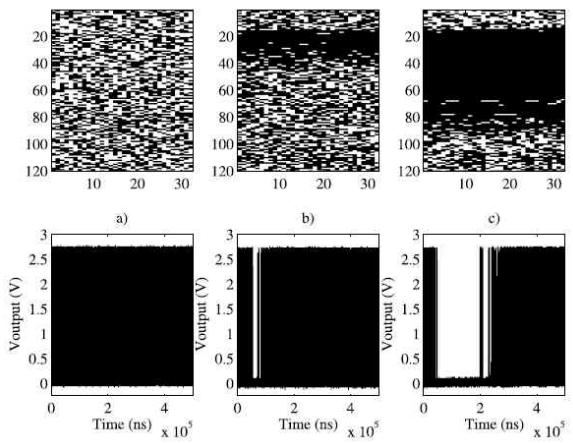
또한 클록 글리치 공격을 위해 기존 20MHz의 클록 신호 대신 40MHz의 클록 신호를 주입하였고 이를 통해 진난수생성기의 출력 난수를 완전히 통제 가능하다는 것을 실제로 증명하였다.

3.2 주파수 주입 공격

2009년 Markettos 링 발진기(ring oscillator) 기반의 진난수생성기의 주파수 주입 공격 방법을 발표 하였다 [2]. 스마트카드 또는 보안 마이크로 컨트롤러의 전원 공급 장치에 사인파 신호를 주입하여 의도적으로 링 발진기의 동작 조건을 수정하고 편향된 출력 신호를 얻어내는 결과를 보여주었다. 난수성의 감소를 비교 및 분석하기 위하여, 사인파 신호 주입 이후 시행된 난수성 검증 결과를 [표 1]에 정리하였다 [2]. NIST STS 통과율은 약 15%, dieharder 테스트는 약 32% 수준으로 하락하는 결과를 통해 주파수 주입 공격의 유효성을 확인하였다.

[표 1] 난수성 검증 결과

NIST	Pass			Fail
No injection	187			1
Injection	28			160
Dieharder	**Pass**	**Poor**	**Weak**	**Fail**
No injection	86	6	6	9
Injection	28	16	5	58



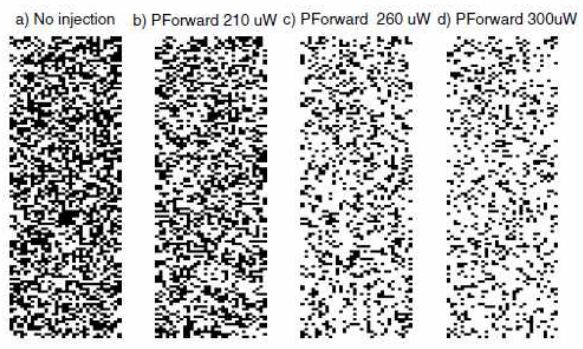
[그림 1] 전력 글리치 공격의 결과

3.3 전자기 공격

2012년 [2]에서 수행된 주파수 주입 공격을 개선한 전자기 공격이 발표되었다 [11]. 일반적으로 전자기 공격은 암호화 장치에서 방출되는 전자기의 특성을 분석하는 비침입 공격이다. 하지만 [2]에서는 프로브를 이용하여 전자기를 직접 암호화 장치에 주입하는 능동 공격의 형태를 보여준다. [2]와 마찬가지로 링 발진기 기반의 진난수생성기에 공격을 수행하였으며, 전원 패드에 직접 신호를 주입할 필요가 없는 향상된 공격 방법이다.

[그림 2]는 진난수생성기의 출력 난수를 비트스트림으로 표현한 결과이다 [11]. 강한 전자기가 주입될수록 난수성이 감소하는 모습을 관측할 수 있고 이를 통해 공격의 유효성을 확인할 수 있다.

또한 비트스트림을 조작하여 특정한 문장이 나타나도록 하는 등 추가적인 실험을 통해 진난수생성기의 난수를 완전히 통제할 수 있음을



[그림 2] 전자기 공격의 결과

성공적으로 증명하였다. 공격자는 이러한 공격들을 통하여 난수의 정확한 값을 취하고 암호화 알고리즘 구현의 비밀 키 정보를 손쉽게 추출할 수 있기 때문에 진난수생성기의 부채널 공격 안전성을 높이기 위한 연구가 활발히 이루어져야 한다.

IV. 결론 및 향후 연구

본 논문에서는 현대 사회에서 필수로 사용되고 있는 난수생성기에 대해 간략히 설명하고 하드웨어 기반 부채널 공격의 종류 및 적용 가능성에 대해 언급하였다. 또한 난수생성기를 대상으로 한 부채널 공격의 실제 공격 사례들을 소개함으로써 난수생성기의 부채널 공격 대응 연구의 중요성을 강조하였다.

2002년, 스위스 ID Quantique사에서 세계최초로 양자난수생성기를 출시한 이후 진정한 무작위성을 가진 난수를 생성하기 위한 연구가 계속되어 왔다. 최근에는 대한민국의 EYL사가 방사성동위원소 반감기를 이용한 초소형 양자난수생성기 칩을 개발하고 [14], SK Telecom사가 세계최소형 양자난수생성기 칩을 개발하는 등 현재까지도 양자역학적 특성을 이용한 난수생성기의 연구가 활발히 이루어지고 있다. 이에 따라 향후 연구로는 현재 상용 또는 개발 중인 양자 난수생성기에 널리 알려진 전력분석 공격, 글리치 공격, 오류 주입 공격 등의 부채널 공격을 수행한 후 각 장치들의 안전성을 비교 및 분석 하고자 한다.

[참고문헌]

[1] H. Martin, T. Korak, M.E. San, M. Hutter, Fault attacks on STRNGs: Impact of glitches, temperature, and underpowering on randomness, *IEEE transactions on information forensics and security*, 10(2), 266-277. 2015.

[2] A.T. Markettos, S.W. Moore, The frequency injection attack on ring-oscillator-based true random number generators, Springer, Cryptographic *Hardware and Embedded Systems-CHES 2009*, 317-331. 2009.

[3] P. Bayon, L. Bossuet, A. Aubert, V. Fischer, Electromagnetic analysis on ring oscillator-based true random number generators, *Circuits and Systems (ISCAS), 2013 IEEE International Symposium on,* 1954-1957. 2013.

[4] https://hal-ujm.archives-ouvertes.fr/file/index/docid/833822/filename/2013_APEMC_Bayon.pdf

[5] Glitch attack, https://www.pcmag.com/encyclopedia/term/43805/glitch-attack

[6] Quantis RNG, https://www.idquantique.com/random-number-generation/products/quantis-random-number-generator

[7] SK Telecom QRNG Chip, https://www.globalskt.com/home/info/2108

[8] Quantis QRNG Chip, https://www.idquantique.com/random-number-generation/products/quantis-qrng-chip

[9] Power analysis attack, http://softknow.com/up2/file/20130930/20130930141438_0781.pdf

[10] J.A. Halderman, S.D. Schoen, N. Heninger, W. Clarkson, W. Paul, J.A. Calandrino, A.J. Feldman, J. Appelbaum, E.W. Felten, Lest we remember: cold-boot attacks on encryption keys, *Communications of the ACM*, 52(5), 91-98. 2009.

[11] P. Bayon, L. Bossuet, A. Aubert, V. Fischer, F. Poucheret, B. Robisson, P. Maurine, Contactless electromagnetic active attack on ring oscillator based true random number generator, Springer, *International Workshop on Constructive Side-Channel Analysis and Secure Design*, 151-166. 2012.

[12] NIST STS, https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final

[13] dieharder, https://webhome.phy.duke.edu/~rgb/General/dieharder.php

[14] EYL QRNG, http://www.eylpartners.com/index.php/quantum-random-number-generator

중첩된 무한 해시체인을 이용한 *Lamport* OTP 확장*

신동진, 박창섭
단국 대학교

Lamport OTP Extension using Overlapped Infinite Hash Chains

Dong-Jin Shin, Chang-Seop Park
Dankook University

요 약

Lamport 일회용 패스워드(OTP)는 고정된 패스워드 그리고 패스워드의 사전공유라는 단순 패스워드가 지니는 문제점을 해결하기 위해 해시체인에 기반을 두고 있다. 하지만 *Lamport* 방식은 길이가 유한한 해시체인의 해시값을 OTP로 사용하기 때문에 해시체인을 구성하는 해시값들을 모두 소진한 이후에는 새로운 해시체인의 루트 해시값을 재 등록해야 한다는 단점을 가지고 있다. 본 논문에서 제안하는 해시체인 기반 OTP는 *Lamport* 방식의 OTP의 핵심인 하나의 긴 해시체인 대신에 여러 개의 짧은 해시체인을 중첩 구성하여 *Lamport* 방식의 장점을 유지하면서 동시에 단점을 해결한다.

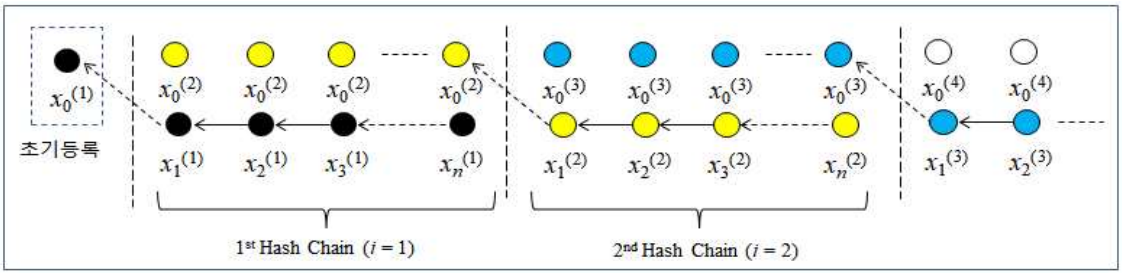
I. 서론

해시체인 기반의 *Lamport* 일회용 패스워드(OTP) [1]는 단순 패스워드의 세 가지 보안 취약점인 고정된 패스워드의 사용, 패스워드의 낮은 안전성 및 증명자와 검증자간 패스워드 사전공유를 근본적으로 해결하기 위해 제안되었다. 특히 암호해시함수를 활용한 해시체인의 개념은 키 관리 및 인증 메커니즘을 설계하는 데에도 널리 활용되고 있다. 세 가지 표준 OTP 시스템이 존재하는데, 해시체인 기반 OTP (HOTP) [2], 카운터 기반 OTP (COTP) [3] 및 시간 기반 OTP (TOTP) [4]가 있다. HOTP는 *Lamport*의 OTP를 사용자 수준에서 사용하기 위해 채택 된 표준으로써 암호해시함수로부터의 결과 값이 소수의 문자들로 구성된 워드로 변환된다는 특징을 가지고 있다. 따라서 HOTP는 클라이언트의 사용상 편의를 위해 확장한 방식이므로 *Lamport* 방식과 동일하다고 볼 수 있다.

* 본 연구는 과학기술정보통신부 및 한국인터넷진흥원의 “고용 계약형 정보보호 석사과정 지원사업”의 연구결과로 수행되었음. (과제번호 H2101-18-1001)
* 본 논문은 2017년도 정부(교육부)의 재원으로 한국 연구재단의 지원을 받아 수행된 기본 연구지원사업 성과임. (NRF-2017R1D1A1B03027862)

해시체인 기반의 *Lamport* OTP는 난수에 암호해시함수를 연속적으로 적용하여 생성한 해시체인의 해시값을 역순으로 사용한다. 검증자는 증명자로부터 전송된 마지막 해시값을 유지하고 있기 때문에, 증명자가 전송하는 OTP인 이전 해시값을 검증 할 수 있다. *Lamport* OTP는 보안 및 효율성 측면에서 두드러진 특징을 가지고 있지만 자체 취약점이 존재한다. 첫째, 해시체인을 구성하는 모든 해시값을 소모하게 되면, 증명자는 새로운 해시체인을 생성하고 검증자에게 루트 해시값을 재 등록해야한다. 둘째, 증명자측이 성능이 제한된 디바이스일 경우, 해시체인의 길이가 길어질수록 OTP를 계산 또는 저장하는 부담이 발생된다.

본 논문에서는 OTP 생성 및 검증을 위한 새로운 해시체인을 설계하고 구성한다. *Lamport* OTP에서의 하나의 긴 역방향 해시체인과는 다르게, 제안하는 새로운 해시체인은 여러 개의 짧은 역방향 해시체인으로 구성되며 각 해시체인은 순차적으로 상호 연결된다. *Lamport* OTP의 장점을 유지하는 동시에 위에서 서술한 *Lamport* 방식의 단점을 해결한다. 해시체인의 루트 해시값을 사전에 최초 등록 이후부터는 추가 재 등록 없이 무제한의 OTP를 생성하고 검증 할 수 있다. 본 논문의 구성은 다음과 같다. 2장에서는 추가적인 재 등록이 필요하지 않은 중첩된 무한 해시체인 기반 OTP를 제안하고. 3장에서는 이를 비교분석하며 4장에서는 결론을 맺는다.



(그림 1) 중첩 무한 해시체인 기반의 OTP

II. 중첩 무한 해시체인 기반의 OTP 제안

2.1 설계 원리

*Lamport*가 제안하는 방식은 증명자 측에서 OTP로 사용하는 해시체인{$x_j = h(x_{j+1})$, $j \in [0,n-1]$ and $x_n = seed$}을 모두 소진하게 되면 초기화 및 등록과정이 반복되는 단점이 존재한다. 본 연구에서 제안하는 방식은 (그림 1)에서와 같이 증명자 측에서 해시체인{$x_j^{(i)} = h(x_{j+1}^{(i)})$, where $j \in [0,n-1]$, $i \in [1,\infty]$, and $x_n^{(i)} = seed^{(i)}$}의 해시값을 OTP로 사용하여 인증 하는 과정 속에 추가적으로 다음 해시체인의 루트 해시값 $x_0^{(i+1)}$을 검증자 측에 전송함으로써 재 등록 과정을 거치지 않고 검증자가 다음 해시체인의 루트 해시값을 보관할 수 있게 하는 기법이다.

[초기화 및 등록단계]

① $seed^{(1)}$, $seed^{(2)} \in_R \{0,1\}^m$
② $x_{n+1}^{(1)} \leftarrow seed^{(1)}$, $x_{n+1}^{(2)} \leftarrow seed^{(2)}$
③ *generate* $x_j^{(1)} = h(x_{j+1}^{(1)})$ for $j \in [0,n]$
④ *generate* $x_j^{(2)} = h(x_{j+1}^{(2)})$ for $j \in [0,n]$
⑤ $root^{(1)} \leftarrow x_0^{(1)}$, $root^{(2)} \leftarrow x_0^{(2)}$
⑥ *register* (ID_p,$root^{(1)}$) to *Verifier*

본 연구에서 제안하는 OTP는 *Lamport*가 제안하는 방식과 동일하게 초기화 및 1회성 등록단계가 선행되어야 한다. 먼저, 증명자는 OTP로 사용할 해시체인을 계산하기 위한 m비트 길이의 $seed^{(1)}$, $seed^{(2)}$를 생성하고 보관한다(①, ②). 그 후에 반복적으로 해시체인의 길이 n만큼 암호해시함수 $h(.)$를 연속적용하여 루트 해시값 $x_0^{(1)}$, $x_0^{(2)}$를 계산하고(③, ④) 자신의 식별자인 ID_p와 함께 $root^{(1)}$를 검증자측에 등록한다(⑤, ⑥).

2.2 OTP 생성 및 검증

증명자가 검증자에게 자신의 ID인 ID_p를 전송하면 검증자는 현재 세션에 사용될 OTP의 인덱스 (i, j)을 증명자에게 보낸다. 이때, i는 현재 해시체인 인덱스 그리고 j는 해당 해시체인내의 해시값 인덱스를 지칭한다. 즉, 검증자는 증명자가 이전 세션에서 제시한 $x_{j-1}^{(i)}$을 보관하고 있는 상태이다. 증명자는 검증자가 전달한 인덱스 j에 따라 $x_j^{(i)}$를 생성하여 OTP로 사용한다. (그림 1)를 기준으로 예를 들면 (i = 1, j = 2)일 경우에 검증자가 보관하고 있는 이전 OTP 값은 ($x_1^{(1)}$, $x_0^{(2)}$)이고 증명자가 제시해야 하는 OTP는 ($x_2^{(1)}$, $x_0^{(2)}$)가 된다. 이때, 다음 해시체인의 루트 해시값 $root^{(i+1)}$ (위의 예를 기준으로 할 경우 $root^{(i+1)} = x_0^{(2)}$)을 OTP와 함께 전달하기 때문에 두 가지 경우 (j = 1인 경우와 그렇지 않을 경우)가 존재한다.

[OTP 생성 및 인증단계]

If $j = 1$
① $seed^{(i+1)} \in_R \{0,1\}^m$
② $x_{n+1}^{(i+1)} \leftarrow seed^{(i+1)}$
③ *generate* $x_j^{(i+1)} = h(x_{j+1}^{(i+1)})$ for $j \in [0,n]$
④ $root^{(i+1)} \leftarrow x_0^{(i+1)}$
⑤ *return* $\{x_j^{(i)}, root^{(i+1)}\}$
else
⑥ *return* $\{x_j^{(i)}, root^{(i+1)}\}$

첫째, 검증자가 증명자에게 전달하는 인덱스 j가 1인 경우 즉, 첫 번째 OTP $x_1^{(i)}$인 경우에는 다음 해시체인을 위한 새로운 $seed^{(i+1)}$을 생성하고(①) 암호해시함수를 반복적으로 해시체인 길이만큼 적용하여 $root^{(i+1)}$을 계산(③)하여 보관하고 이를 전달한다(⑤). 둘째, 인덱스 j가 1이 아닌 경우에는 새롭게 루트 해시값 $root^{(i+1)}$을 계산 할 필요가 없으므로 인증에 필요한 OTP $x_j^{(i)}$ 만 계산하여 이전에 계산한 $root^{(i+1)}$과 같이 전달한다(⑥).

[OTP 검증단계]

If $x_{j-1}^{(i)} = h(x_j^{(i)})$

① *if* $j = n$, *store*(ID_p, $i+1$, 1, *root*$^{(i+1)}$,_)
② *else store*(ID_p, i, $j+1$, $x_j^{(i)}$, *root*$^{(i+1)}$)
③ *return "success"*
else
④ *return "fail"*

인증과정에서 *Lamport* 방식의 경우에는 전달받은 OTP x_j에 암호해시함수 $h(.)$를 적용하여 자신이 보관하고 있던 해시값 x_{j-1}과 비교한다. 제안하는 방식도 전달받은 OTP $x_j^{(i)}$에 암호해시함수 $h(.)$를 적용하여 증명자를 검증한다. 이에 추가적으로 *Lamport* 방식의 단점을 해소하기 위해 증명자 측에서 전달한 다음 해시체인의 루트 해시값을 검증에 성공한 경우엔 보관해야 하기 때문에, 이에 대한 처리가 요구된다. 검증자에게 전달하는 OTP $x_j^{(i)}$가 해시체인의 마지막 해시값일 때, 즉 $j=n$일 때는 다음 인증 시도 시 전달되는 새로운 해시체인 해시값을 검증할 수 있게끔 root$^{(i+1)}$값을 다음 인증 시도 시에 비교할 해시값 $x_0^{(i+1)}$으로 보관한다. 그리고 해시체인의 인덱스 i는 값을 증가시키고, OTP 인덱스 j는 1로 초기화된다(①). 결과적으로 증명자가 다음 해시체인의 해시값을 이용할 경우, 검증자는 정상적으로 검증할 수 있고(③), 인증 성공 시 증명자가 새롭게 생성한 $seed^{(i+1)}$ 값으로 계산하여 전달하는 root$^{(i+1)}$을 보관한다. 이 경우를 제외하면, *Lamport* 방식과 동일하게 증명자가 전달하는 OTP $x_j^{(i)}$에 암호해시함수를 적용하여 보관하고 있던 해시값 $x_{j-1}^{(i)}$과 비교하여 검증하고, 검증이 성공적으로 이루어지면 OTP와 같이 전달받은 다음 해시체인의 루트 해시값을 보관하고(②) OTP 인덱스 j값을 증가시킨다(③).

III. 안전성 및 효율성 분석

3.1 해시체인 기반의 OTP 안전성

본 논문에서 제안하는 해시체인 기반 OTP방식은 *Lamport* 방식과 같이 암호해시함수 $h(.)$의 안전성, 즉 역상 저항성(pre-image resistance)에 기반을 두고 있다. 증명자가 일회용 패스워드 $x_j^{(i)}$ ($i\in[1,\infty]$, $j\in[0,n]$)를 노출한 이후에 악의적인 공격자가 $x_{j+1}^{(i)}$를 도출해 내기 위해서는 해당 암호해시함수의 역상저항성을 깬다는 것을 의미하는데, 사실상 불가능하다. 일회용 패스워드와 같이 전송되는 다음 해시체인의 루트 해시값 $x_0^{(i+1)}$의 경우도 공격자가 후속 $x_j^{(i+1)}$ (j = 1, 2, ..., n)을 도출해 내야하기에 이 역시 불가능하게 된다. 특히, *Lamport* 방식과 마찬가지로 제안방식은 증명자와 검증자간에는 무결성이 보장되는 채널이 요구되며 또한 검증자에 대한 인증이 선행되어야 하기에 전송되는 OTP 값의 변조는 불가능하게 된다.

3.2 기존 OTP와의 비교분석

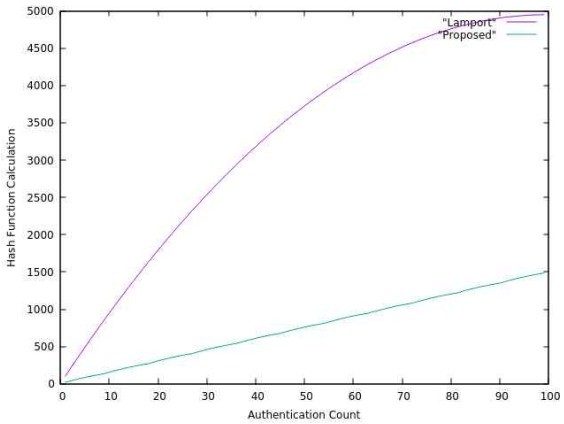
해시체인 기반의 *Lamport* 방식과 TOTP, COTP와 본 논문에서 제안하는 방식을 비교한다. 첫째, TOTP와 COTP의 경우 증명자와 검증자간 사전 비밀 정보를 공유해야 인증 프로세스를 수행할 수 있는 반면, 해시체인 기반의 *Lamport* 방식과 제안하는 방식은 사전에 비밀정보를 공유하지 않아도 인증 프로세스를 수행할 수 있다. 둘째, *Lamport* 방식은 해시체인의 해시값을 모두 소모한 경우 새로운 해시체인을 생성하여 다음 루트해시값을 등록해야 하지만 TOTP, COTP, 그리고 제안방식은 인증 프로세스를 계속 수행 할 수 있다. 추가적으로 <표 1> 언급된 방식들은 OTP 생성을 위한 인덱스를 추가적인 프로세스 없이 동기화 할 수 있다.

<표 1> *Lamport,* TOTP, COTP, Proposed 비교

	Lamport	TOTP	COTP	Proposed
사전 공유키 불필요	O	X	X	O
재 등록 불필요	X	O	O	O
동기화 지원	O	O	O	O

3.3 Lamport 방식과 제안방식 비교

Lamport 방식의 OTP는 재 등록 문제를 피하기 위해 해시체인 길이를 증가시킬수록 증명자가 인증을 위해 암호해시함수를 반복적으로 사용하여 생성하는 OTP의 계산량 부담이 증가한다. 본 연구에서 제안하는 해시체인 기반 OTP는 하나의 긴 해시체인을 사용하는 *Lamport* 방식과는 다르게 짧은 해시체인을 사용하여 재 등록문제를 해결하고 증명자의 계산 부담을 줄이는 결과를 보여준다.



(그림 3) 암호해시함수 $h(.)$ 사용횟수 비교

(그림 3)은 *Lamport* 방식과 본 논문에서 제안하는 방식의 인증횟수가 증가함에 따라 증명자측에서 부담하는 암호해시함수 $h(.)$ 계산량을 보여준다. 먼저 하나의 긴 해시체인을 사용하는 *Lamport* 방식은 해시체인 길이를 100으로 설정하고 상대적으로 짧은 해시체인을 사용하는 본 논문에서 제안하는 방식은 길이를 10으로 하여 비교 분석 하였다. x축은 누적 인증횟수를 나타내고, y축은 암호해시함수

누적 계산량을 나타낸다. 인증횟수가 증가함에 따라 *Lamport* 방식은 상대적으로 긴 하나의 해시체인을 이용해 인증이 이루어지기 때문에 본 논문에서 제안하는 방식과 비교 했을 때 상대적으로 누적 계산량이 많은 것을 알 수 있다.

IV. 결론

본 논문에서는 해시체인 기반의 OTP 시스템이 논의되었다. 기존 *Lamport* OTP는 2가지 실용적인 측면의 문제점을 지니고 있다는 사실에 기인하여, 중첩된 무한 해시체인 기반의 OTP를 제안하였다. 새로이 제안된 OTP는 기존 *Lamport* OTP의 장점을 그대로 유지하면서 기존 문제점을 해결할 수 있음을 보였다. 해시체인 기반의 OTP는 사용자 인증 분야뿐만 아니라 키관리 및 사물인터넷의 기기인증 등에도 활용이 가능하기에 본 연구에서 제시한 OTP 기법의 활용성은 매우 높을 것으로 기대된다.

[참고문헌]

[1] Leslie Lamport, “Password Authentica tion wit h Insecure Communication”, Communications of the ACM, Vol. 24, pp. 770-772, Nov. 1981.

[2] N. Haller, C. Metz, P Nesser, and M Straw, “One-Time Password System”, RFC 2289, Fe b. 1999.

[3] D.M. Raihi, M. Bellare, F. Hoornaert, D. Nacc ache, and O. ranen, “HOTP: An HMAC-Base d One-Time Password Algorithm”, RFC 4226, Dec. 2005.

[4] D.M. Raihi, S. Machani, M. Pei, and J. Rydell, “TOTP: Time-Based One-Time Password Al gorithm”, RFC 6238, May. 2011.

[5] D. Coppersmith, “Almost optimal hash sequenc e taversal”, Proceedings of the 4th Conference on Financial Cryptography, pp. 102-119, Feb. 2002

[6] M. Jakobsson, “Fractal hash sequence represen tation and traversal”, Proceedings of the 2002 IEEE Symposium on Information Theory, Jul. 2002.

[7] M. Fischlin, “Fast verification of hash chains”, Proceedings of the RSA Security Cryptograph er's Track, pp. 339-352, Feb. 2004.

[8] M.H. Elderfrawy, M.K. Khan, and K. alghathb ar, “Broadcast Authentication for Wireless Se nsor Networks Using Nested Hashing and the Chinese Remainder Theorem”, Sensors, vol. 1 0, no. 9, pp. 8683-8695, Sep. 2010.

[9] M.H. Elderfrawy, M.K. Khan, and K. alghathb ar, “One-time password authentication with in finite nested hash chains”, U.S. Patent Applic ation Publication US20130191899 a1, 2013.

[10] S. Bittl, “Efficient construction of infinite len gth hash chains with perfect forward secrecy using two independent hash functions”, Procee dings of the 11th International Conference on Security and Cryptography, Aug. 2014.

[11] K. Bicakci, N. Baykal, “Infinite length hash c hains and their applications”, Proccedings of t he 11th IEEE International Workshops on Ena bling Technologies: Infrastructure for Collabor ative Enterprises, pp 57-61, Jun. 2002.

Linux OS 상에서의 커널 및 응용 LEA암호모듈 구현 및 호출 분석

송행권*, 이옥연*

*국민대학교 금융정보보안학과

Implementation and Call analysis of kernel Application LEA Cryptographic Module on Linux OS

Haeng-Gwon Song*, Ok-Yeon Yi*

*Cryptography & Information Security Institute, Kookmin University

요 약

오늘날의 사회는 정보통신의 기술의 발달로 인하여 모든 사물이 인터넷과 연결되는 디지털 메시 사회가 되고 있다. 과거 간단한 기능을 제공하던 소형 경량기기들이 인터넷과 연결되면서 본래의 기능 뿐 아니라 제어, 관리, 보안 통신 등 다양한 기능이 요구되고 있다. 소형 기기들이 고유의 기능 만을 수행할 때에는 하드웨어, 펌웨어 형태로 제작 되었으나 최근 소형 기기에서도 다양한 기능들을 탑재하기 위하여 운영체제를 탑재한 소형기기들이 출시되고 있다.

운영체제가 탑재된 소형기기가 네트워크와 연결되면서 개인의 프라이버시를 침해 할 수 있는 데이터들의 보호를 위하여 보안 기능은 필수적으로 요구된다. 본 논문에서는 소형 기기들에 많이 탑재되는 Linux OS상에서 데이터 기밀성을 제공하기 위하여 사용되는 경량 암호 알고리즘 LEA암호모듈을 구현하고 또한 운영체제 상에서 효율적인 암호화를 위한여 커널 및 응용 환경에서 호출 방법에 대한 분석을 수행하였다.

I. 서론

미국 시장조사기관 가트너(Gartner)에서 매년 발표하는 10대 전략기술을 살펴보면 사물인터넷(IoT, Internet of Things)은 2012년부터 매년 선정되어 왔으며, 2016년에는 디지털메시(Digital Mesh)[1]라는 개념을 정의하면서 IoT 환경을 넘어서 우리가 사용하고 있는 모든 디바이스들이 그물 구조로 촘촘하게 연결되어 정보를 교환할 것이라고 전망하고 있다.

과거 사물들은 사용자가 요청하는 정보나 서비스를 빠르게 제공하는 것이 중요하였지만 현재 사물들에 요구되는 기능은 제어, 관리, 통신, 보안 등의 기능이 요구되고 있다. 다양한 기능을 소형 기기에서 수행하기 위해서는 운영체제를 탑재하여 관리하는 것은 필수적으로 요구된다. 하지만 소형기기들은 데스크탑 환경과 달리 프로세스, 메모리 등 한정된 자원을 사용하여 기능들을 제공해야 한다. 따라서 소형기기에 탑재되는 OS는 크기가 매우 작아야 하며 제공하는 기능들의 구현 및 호출이 최대한 효율적인 방법으로 수행되어야 한다.

본 논문에서는 소형기기에 탑재되는 Embedded Linux를 타겟으로 하여 Linux 환경에서 커널 모듈을 구현하는 방법을 연구하였다. 또한 기밀성을 제공하는 LEA(Lightweight Encryption Algorithm)[2]를 커널 및 응용 암호모듈로 구현함으로써 소형 기기에서 효율적인 암호모듈 구현 및 호출 방법에 대한 연구를 수행하였다.

본 논문의 구성은 2장에서 기밀성을 제공할 수 있는 대칭키 암호 알고리즘인 LEA에 대해 소개하고, 3장에서는 Linux 상에서 커널 모듈을 구현 할 수 있는 적재가능한 동적 암호모듈에 대하여 소개한다. 4장에서는 효율적인 암호모듈의 구현 및 호출의 관계를 증명하기 위한 실험 방법 및 결과에 대해 제시하며 이를 바탕으로 5장에서는 결론을 맺는다.

II. LEA(Lightweight Encryption Algorithm)

블록암호 LEA 알고리즘은 2012년 국가보안기술연구소에서 개발한 높은 안전성과 우수한 효율성을 제공하는 128비트 블록암호 알고리즘이다. LEA알고리즘은 다양한 SW환경에서, 국제 표준암호인 AES(Advanced Encryption Algorithm)대비 1.5배~2배 성능을 제공하며, 스마트폰 등 모바일 기기에서의 저 전력 데이터 암호화, 대용량 데이터 서버에서의 고속 데이터 암호화 등에 적합한 알고리즘이다.

LEA알고리즘은 128비트 데이터 블록을 암호화 하는 알고리즘으로 128, 192, 256비트 비밀키를 사용할 수 있으며 요구되는 안전성 기준에 따라서 구분하여 사용 할 수 있다. LEA의 라운드 함수는 32비트 단위의 ARX(Addtion, Rotation, XOR)연산만으로 구성되어 있으며, 이들 연산을 지원하는 범용 32비트 소프트웨어 플랫폼에서 고속으로 동작한다. 기존 블록암호 알고리즘과 다른 점은 S-Box 사용을 배제하여 메모리의 효율성을 갖는 경량 구현이 가능하도록 하였다.

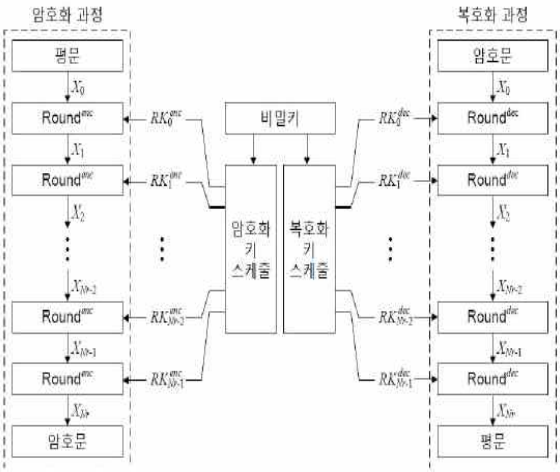


그림 1 LEA알고리즘 암·복호화 과정

LEA 알고리즘은 키 길이에 따라 128, 192, 256으로 구분되며, 블록 암호 LEA의 규격은 표 1과 같이 정리 할 수 있다. (Nb : 블록 바이트, Nk : 비밀키 길이, Nr : 라운드 수)

구분	Nb	Nk	Nr
LEA-128	16	16	24
LEA-192	16	24	28
LEA-256	16	32	32

표 1 LEA 규격

III. 동적 커널 모듈(Dynamically Loadable Kernel Module)

동적 커널 모듈(DLKM, Dynamically Loadable Kernel Module)은 모듈을 동적으로 커널 속으로 로드 또는 언로드 할 수 있는 목적 파일을 의미한다. 적재 가능 커널 모듈을 사용함으로써 얻을 수 있는 장점은 시스템을 재부팅하지 않고 필요 기능을 제공하는 커널을 추가 할 수 있다.

커널 모듈의 경우 응용프로그램에서 사용하는 메모리와 다른 별도의 커널 메모리를 가지고 있다. 응용프로그램의 경우 가상의 메모리와 연결되어 프로그램을 동작시키지만 커널에서 동작하는 프로그램은 물리적인 메모리와 직접 연결되는 커널 메모리를 사용한다. 물리적 메모리의 속도는 가상 메모리의 속도보다 빠르기 때문에 커널에서 동작하는 모듈은 사용자 영역에서 실행되는 프로그램보다 빠르게 실행된다.

또한 적재된 커널 모듈은 커널 레벨의 모듈에 의해 호출 되거나 ioctl(Input Output ConTrol)에 의하여 사용자 프로그램에서 호출되어 사용 할 수 있다. 커널 모듈에서 동작하는 프로그램은 프로세스의 우선권을 가지고 있기 때문에 사용자 프로그램보다 빠르게 실행 될 수 있으며 ioctl 함수의 경우도 프로세스 Lock을 통해 해당 프로세스를 점유하여 사용 할 수 있다.

IV. 실험 방법 및 결과

본 논문에서는 커널 영역과 응용프로그램 영역에서 암호모듈을 구현하였다. 구현된 암호모듈은 각각의 영역에서 다시 호출 되어 총 3

가지의 방법으로 호출 관계를 정의 하였다. 또한 LEA알고리즘의 효율적인 호출 방법을 실험하기 위하여 키 생성과 암·복호화를 함께 수행하는 on the fly 방법과, 키 생성과 암·복호화를 분리해서 처리하는 기법인 Key-unrolling 기법을 적용하여 실험을 수행하였다.

운영체제	Ubuntu 14.04
프로세서	Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz
메모리	2039784 KB
컴파일러	gcc 4.8.4

표 2 실험 환경 명세

암호모듈을 호출하는 방법은 총 3가지로 정의하였다. 커널프로그램에서 커널 모듈을 호출하는 방법(KO-KO), 응용프로그램에서 커널모듈을 호출하는 방법(APP-KO), 응용프로그램에서 응용모듈을 호출 하는 방법(APP-APP)으로 나뉜다.

각 호출 관계마다 on the fly기법과 key unrolling 기법을 적용하여 실험을 수행 하였다. 암호화 데이터는 16바이트의 값을 전송하여 암호화를 수행하였으며 1,000,000번 반복 암·복호화를 수행하여 실행되는 속도를 측정하였다.

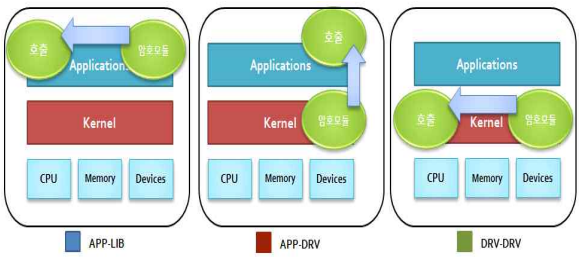


그림 2 암호모듈 호출 관계

응용 프로그램 영역의 암호모듈은 SO파일 형태로 제공되며 커널 영역의 암호모듈의 경우 KO파일 형태로 제공된다. 응용 프로그램에서의 응용암호모듈 호출은 동적라이브러리 참조의 형태로 호출 되었다. 응용프로그램에서 커널 암호모듈을 호출 할 경우 에는 IOCTL 함수를 이용하여 암호모듈을 호출 한다. 리눅스 2.6.39버전 이전에는 IOCTL 함수를 호출 하였을 경우 BKL(Big Kernel Lock)을 사용하여 CPU 전체 lock을 수행한 후 커널 모듈을 호출 하였다. 하지만 리눅스 커널 2.6.39 버전 이후부터는 BKL의 단점을 보안하기 위하여 사용하고 있는 CPU의 프로세스의 LOCK을 수행하여 IOCTL 함수를 지원한다. 프로세스 LOCK을 통하여 커널 모듈을 빠르게 수행 할 수 있지만 응용영역에서 커널 영역으로 메모리 복사 등의 추가적인 작업이 필요하다. 커널 프로그램에서 KO파일 형태의 암호모듈을 호출하기 위하여서는 심볼 테이블 참조를 통하여 사용하는 커널 모듈을 호출 할 수 있다.

	key_unrolling	on the fly
app-app	0.291521	0.527119
app-ko	0.124202	0.162519
ko-ko	0.110933	0.126938

표 3 실험결과(실험단위 : 초)

APP-APP호출 관계를 기준으로 하였을 경우 APP-KO호출은 Key unrolling 기법은 2.34배 빠르게 수행되며 on the fly 기법은 3.24배 빠르게 동작하는 것은 확인 할 수 있다. KO-KO호출의 경우에는 Key unrolling 기법은 2.63배 빠르게 수행되며 on the fly 기법의 경우 4.15배 빠른 것을 확인 할 수 있다. APP-KO호출과 KO-KO호출을 비교 하였을 경우 Key unrolling 기법은 1.12배 빠르게 수행되며 on the fly 기법은 1.28배 빠르게 동작하는 것을 확인 할 수 있다.

V. 결론

IoT 서비스가 활성화되면서 경량 기기에 대한 다양한 기능적 요구가 증가함에 따라서 OS의 선택은 불가피한 상황이 되었다. 본 논문에서는 소형 기기에서 보안 모듈을 구현 할 수 있는 두 가지 방법을 제시 하였으며 실험을 통하여 각각의 효율적인 암호모듈의 호출 관계를 증명하였다.

소형 장비에서 암호모듈을 사용하기 위해서

는 응용프로그램 영역에서 암호모듈을 구현하는 것이 아니라 커널 영역에서 필요한 암호모듈을 구현하여 커널 영역에서 보안을 제공하는 것이 가장 효율적인 방법임을 증명하였다. 또한 대칭키 암호 알고리즘의 효율적인 운영을 위하여 키 확장과 암·복호화를 나누어 사용하는 Key unrolling 기법을 사용하여 적용할 경우 최소 1.1배에서 2배까지의 효율을 확인 할 수 있다.

향후 커널 모듈의 쓰래드 선점, 스케줄링, 불필요한 메모리 카피나 커널영역과 사용자 영역 스위칭 등에 대한 연구를 통하여 더 효율적인 암호화 방법을 제시하며 거기에 따른 정량적 분석을 통한 증명이 필요하다.

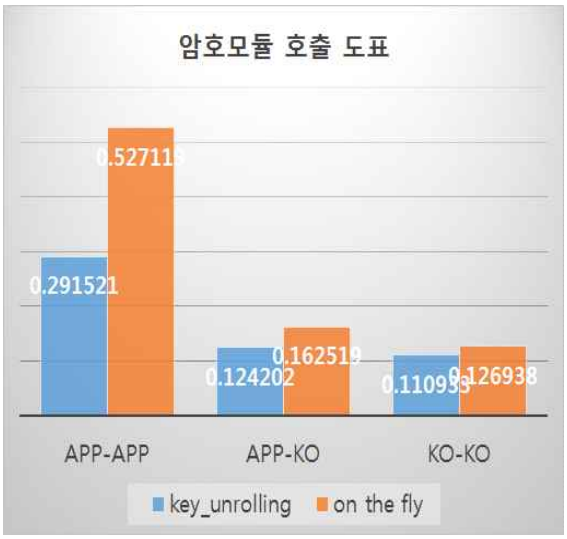


그림 3 실험결과 도표

[참고문헌]

[1] Viveca Woods, http://www.gartner.com/newsroom/id/3143521, October, 6, 2015

[2] KISA, https://seed.kisa.or.kr/iwt/ko/sup/EgovLeaInfo.do, 2013

[3] 송행권, “ARM8기반의 암호모듈 구현과 효율적인 모듈 호출”, 한국정보처리학회 2013년 제 40회 추계학술발표대회, VOL20, No 02, PP 0790 ~0792, 11, 2013

[4] 남의석, “Development of a Linux Kernel-Thread Secure Socket Layer (SSL) WEB Accelerator” VOL 10-C NO. 06 PP. 0657 ~ 0664 (2003. 10)

Survey of Functional Encryption and its Functionality

Hyundo Yoon, Hyunsoo Kwon, Junbeom Hur

Department of Computer Science and Engineering, Korea University.

Abstract

The public-key encryption has been used ubiquitously in many areas for security issues. As new computer services, such as “cloud” system, emerge and needs for selective security increase, the original public-key encryption needed to be ameliorated and changed in their encryption scheme. Functional Encryption has broadened the vision of the public-key encryption. It also allowed the key holder to learn only the function of encrypted data, but nothing more about the data. In Functional Encryption, many encryption schemes have been proposed that are proven adequately secure. In this paper, each encryption schemes will be shown and analyzed.

I. Introduction

Public-key encryption is an invaluable tool and it is used ubiquitously in many areas. Few years ago, “functional encryption” (FE) has emerged as a new paradigm for public-key encryption which has supplemented some limits of the public-key encryption. For instance, “cloud” services needed new broad vision of encryption, or security, which showed the insufficiency of original public-key encryption. Based on its secret key and a given cipher text, a receiver can learn the functions of the underlying message. In functional encryption, there are two types of Predicate Encryption

- Predicate Encryption with public index
  - Identity-Based Encryption
  - Attribute-Based Encryption
- Predicate Encryption
  - Hidden Vector Encryption
  - Inner Product Predicate

Identity-Based Encryption and Attribute-Based Encryption are below Predicate Encryption scheme with public index. There is another class for Predicate Encryption that consists of Hidden Vector Encryption and Inner Product Predicate.

Sahai, Waters, and Boneh have set the formal definition and challenges for the Functional Encryption in 2011. In this paper, the schemes of each functional encryptions and the differences between the schemes will be compared and explained.

II. Syntax and Security Notion

As mentioned above, there are three types of functional encryption algorithm. Those three algorithms, in details, have differences in a way they encrypt data, but their basic encryption scheme is similar.

2.1 Functional Encryption (General)

The functionality F, which is the syntactic definition of functional encryption (FE), describes the functions of a plaintext that can be obtained from the ciphertext.

$FE=(Setup,\ KDer,\ Enc,\ Eval)$

- Setup: input 1^k outputs a *master public key* and *master secret key* sk.
- KDer: input sk and a function $f \in F$ outputs an evaluation token sk_f for f.
- Enc: input a pk and a message $m \in \sum$ outputs a ciphertext c.
- Eval: input an evaluation token sk_f and a ciphertext c outputs a string y or $\perp$.

The *functionality F is defined over* (K,X), where $F: K \times X \rightarrow \{0,1\}^*$. The general functional encryption scheme follows the standard public-key encryption.

2.2 Predicate Encryption

The Predicate Encryption scheme is defined in terms of a polynomial time.

$$P: K \times X \rightarrow \{0,1\}$$
$$F(k \in K, (\in d, m) \in X) := \begin{cases} m \text{ if } P(k, \in d) = 1 \\ \perp \text{ if } P(k, \in d) = 0 \end{cases}$$

When decrypting, the payload of the ciphertext is revealed only with the condition of . However, it reveals nothing new about the with other cases or conditions. Even though, in the and is known, the payload in cannot be known unless the condition is satisfied.

2.3 Identity-Based Encryption (IBE)

In Identity-Based Encryption(IBE), the ciphertexts and private keys are generally associated with in the form of string that are considered as "identities and a key can decrypt when the two strings, or identities, are equal. The scheme of the IBE is described similarly with the Predicate Encryption scheme.

- The key space $K := \{0,1\}^* \cup \{\epsilon\}$.
- The plaintext = $(ind,\ m)$, where the index space $I := \{0,1\}^*$.
- $P(k \in K \backslash \in d \in I) := \begin{cases} 1 \text{ if } k = \in d \\ 0 \ otherwise \end{cases}$

The plaintext is a pair of (index) and payload message . For instance, for email, the index may be the sender and the payload message may be the content of the email.

2.4 Attribute-Based Encryption(ABE)

Attribute-Based Encryption(ABE), introduced by Sahai and Waters, is encryption scheme that one could express complex access policies. Attribute-Based Encryption has two different of formulations: Key Policy ABE and Ciphertext-Policy ABE.

The Key-Policy ABE with n variables is described as a predicate encryption scheme, $P_n: K \times I \rightarrow \{0,1\}$ and with the Boolean formulas.

- The key Space K : the set of all poly-sized Boolean formulas ϕ in n variables $\vec{z} = (z_1, \ldots\ldots, z_n) \in \{0,1\}^n$. $\phi(\vec{z})$: the value of the formula ϕ at $\vec{z}$.
- Plaintext: a pair $(ind = \vec{z}, m)$

  Index space: $I := \{0,1\}^*$

  $\vec{z}$: bit vector representing the boolean values $(z_1, \ldots\ldots, z_n)$.
- $P_n(\phi \in K \backslash \{\epsilon\}, ind = \vec{z} \in I) := \begin{cases} 1 \text{ if } \phi(\vec{z}) = 1 \\ 0 \ otherwise \end{cases}$

In Key-Policy ABE, the access formula is provided by the key. Furthermore, a set of attributes in the access formula should be evaluated true to decrypt the message m.

The Ciphertext-Policy ABE (CP-ABE) has reversed role for ciphertext and key. Like the Key-Policy ABE, the CP-ABE with variables can be described as predicate encryption scheme for the predicate $P_n: K \times I \rightarrow \{0,1\}$.

- The key space $K := \{0,1\}^n$: the set of all n bit strings representing n boolean variables $\vec{z} = (z_1, \ldots\ldots, z_n) \in \{0,1\}^n$.
- Plaintext: a pair $(ind = \phi, m)$
  the index space I : the set of all poly-sized boolean formulas ϕ over n variables
- $P_m(\vec{z} \in K \backslash \{\epsilon\}, ind = \phi \in I) := \begin{cases} 1 \text{ if } \phi(\vec{z}) = 1 \\ 0 \ otherwise \end{cases}$

2.5 Hidden Vector Encryption(HVE)

In HVE, both a ciphertext and a private key contains a vector of elements. For a ciphertext, it contains elements in $\{0,1\}^*$. For a private key, it contains elements in $\{*\} \cup \{0,1\}^*$.

- The key space K : all $(v_1, \ldots\ldots, v_n)$ where each $v_i \in \{*\} \cup \{0,1\}^*$.
- Plaintext: a pair $(ind = (w_1, \ldots\ldots, w_n), m)$ where each $w_i \in \{0,1\}^*$.
- Index Space I : $(\{0,1\}^*)^n$.

- $P_n((v_1,\ldots\ldots,v_n)\in K\{\epsilon\}, \text{ind}=(w_1,\ldots\ldots,w_n))$
  $:=\begin{cases}1 \text{ if } v_i = u_i \text{whenever } v_i \neq * \\ 0 \text{ otherwise}\end{cases}$

2.6 Inner Product Predicate

The Inner Product Predicate allowed a scheme to evaluate more complex disjunction, polynomials, and CNF/DNF formulae. This scheme, which is constructed over the field F_p, also described with the predicate for vectors of length n.

- The setup algorithm: a randomly chosen prime p of length κ(security parameter) is defined.
- The Key Space K: all $\boldsymbol{v}=(v_1,\ldots\ldots,v_n)$ where each $v_i \in F_p$.
- Plaintext: a pair $(ind=(u_1,\ldots\ldots,u_n), m)$ where each $u_i \in F_p$.
- Index Space $I := (F_p)^n$.
- $P_{n,p}((v_1,\ldots,v_n)\in K\setminus\{\epsilon\}, ind=(u_1,\ldots,u_n))$
  $:=\begin{cases}1 \text{ if } \sum_{i=1,\ldots n} v_i \cdot u_i = 0 \\ 0 \text{ otherwise}\end{cases}$

III. Analysis & Challenges

In Predicate Encryption, scheme with public index consists of Identity-Based Encryption and Attribute-Based Encryption. When predicate encryption is applied to software or systems, depending on the structure of the system, or purpose of the security, Identity-Based Encryption or Attribute-Based Encryption is chosen.

3.1 IBE's Open Problem

Key Escrow Problem. The Private Key Generator(PKG) makes the private key for the user using its master secret key. Thus, the PKG can decrypt or sign any messages. The key escrow property may be useful in some situation, but, because of the essential requirement of digital signature, it is generally not desirable.

Revocation Problem. In email system, where the IBE is used widely, the revocation problem is not fully solved. When the owner of the email wants third person to used his or her email address to encrypt the messages. The problem occurs as his or her email address has been compromised, thus cannot use the email address as a public key no longer.

3.2 IBE vs. ABE

Unlike Attribute-Based Encryption(ABE), Identity-Based Encryption(IBE) has limitation in access control. Since identity in IBE is view as a single attribute, IBE cannot deal with multiple attributes. For instance, in email system, for ABE, email as a whole can be considered as a attribute. However, in IBE, an ID is considered an identity and content is payload message.

When dealing with the collusion problem, IBE with the multiple hierarchical identities has inefficiently high cost compared to ABE. In addition, the access control of IBE is inefficient and cannot be solved. ABE, in contrast, has sufficient access control for colluding users with lower costs.

3.3 ABE vs. KP-ABE vs. CP-ABE

[Table 1] Comparison of each ABE schemes

Crietria	ABE	KP-ABE	CP-ABE
Fine-grained access control	No	Yes	Yes
Data scalability	No	No	No
Data Confidentiality	Yes	Yes	Yes
User accountability	No	No	Yes
User revocation	No	Yes	Yes
Collusion resistant	Yes	Yes	Yes

According to the Table 1, all three types of Attribute-Based Encryption schemes do not satisfy the data scalability and used accountability criteria. However, criteria of collusion resistant and data confidentiality are satisfied. Since the ABE uses a private key to match the attributes, it only guarantees the minimum-security requirements.

Common problem for the schemes is illegal key sharing between users. The tracing of users' sharing the key is difficult. This problem has caused the ABE schemes cannot achieve certain criteria above.

3.4 Challenges for Hidden Vector Encryption

There are some problems for HVE to be solved. Since HVE should support the wild-card in tokens for randomness, it is hard for the scheme to have constant size of ciphertext. The delegation property, which was achieved in hierarchical IBE, is a problem for HVE. Even though a HVE scheme for delegation property was proposed, the cost for the decryption was proportional to the number of attributes.

IV. Conclusion

The various algorithms of functional encryption have brought a new paradigm in public- key encryption. The functionality of the schemes can be modified according to the needs of the security. This means that the functional encryption can be applicable to various fields with good efficiency. However, it is clear that there are still some problems and challenges for those encryption schemes that need to be solved. In this paper,

Acknowledgement

This work was supported as part of Military Crypto Research Center(UD170109ED) funded by Defense Acquisition Program Administration(DAPA) and Agency for Defense Development(ADD).

[Reference]

[1] Boneh, D., Sahai, A., Waters, B.: Functional encryption: Definitions and challenges. Cryptology ePrint Archive, Report 2010/543 (2010), http://eprint.iacr.org/2010/543

[2] O'Neill, A.: Definitional issues in functional encryption. Cryptology ePrint Archive, Report 2010/556 (2010), http://eprint.iacr.org/2010/556

[3] Lee, Cheng-Chi, et al. "A Survey on Attribute-Based Encryption Schemes of Access Control in Cloud Environments." *International Journal of Network Security*, vol. 15, no. 4, July 2013, pp. 231-240.

[4] Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: ACM CCCS (2006)

[5] J. Baek, R. Safavi-Naini, J. Hindmarsh, and W. Susilo. A Survey of Identity-Based Cryptography. In Identification and Authentication Issues in Computing, Proceedings of 10th Australian Unix User Group (AUUG) Conference, pages 95-102, 2004.

2018 한국정보보호학회 하계학술대회

A4 IoT보안 1

강 승 호 (동신대학교)

- **스마트 시계 활용 무자각 지속 인증 강화 연구**
  류권상, 옥도민, 최대선
- **라즈베리 파이를 이용한 휴대용 영상감시시스템 개발**
  최경호, 김현진, 현부영, 김종민, 이동휘
- **LR Guard : ARM TrustZone을 활용한 제어 흐름 보호 기법 설계**
  진홍주, 장혜린, 이동훈
- **IoT 기반의 스마트 홈 보안 동향**
  박정인, 이가연, 윤현경, 염흥열

스마트 시계 활용 무자각 지속 인증 강화 연구[1)]

류권상*, 옥도민**, 최대선**†

*공주대학교 융합과학과 대학원, **공주대학교 의료정보학과

A Study on Active Authentication Reinforcement Using Smart Watch

Gwonsang Ryu*, Tomin Ok**, Daeseon Choi**

*Convergence Science Graduate School, Kongju National University,
**Dept. of Medical Information, Kongju National University

요 약

본 논문에서는 무자각 지속 인증을 강화하기 위해 스마트 시계를 추가로 활용하여 COI(Context of Interst)의 유사도 점수 측정방법을 제안한다. 스마트폰에서 사용자 COI 주변 무선 AP 정보와 스마트 시계의 블루투스 정보를 수집하고 스마트 시계에서 스마트폰의 블루투스 정보를 수집하였으며, Autoencoder를 이용하여 사용자 COI 모델을 생성하고 COI 유사도 점수를 측정하였다. 사용자의 COI 유사도 점수 측정실험 결과, 주변 AP 정보만을 이용한 것보다 블루투스 정보를 같이 활용했을 때 COI 유사도 점수가 0.9 이상 나온 비율이 30% 더 높게 측정되었다.

I. 서론

스마트 기기의 급격한 발전과 동시에 보급률이 급증하면서 금융 및 건강과 같은 사용자의 민감한 정보를 다루는 애플리케이션이 증가하였다. 따라서 사용자의 민감한 정보를 보호하기 위해 스마트 기기의 보안에 대한 중요성 또한 상당히 증가하였다. 하지만 [1]에 따르면 불편하다는 이유로 스마트폰 사용자 34%는 4자리 PIN(Personal Identification Number) 조차 사용하지 않는다고 보고되었다. 따라서 사용자에게 편리성을 제공함과 동시에 안전한 무자각 지속 인증기술이 활발히 연구되고 있다.

Riva et al.[2]은 애플리케이션이 가지고 있는 사용자의 민감한 정보에 따라 애플리케이션의 인증 레벨을 public, private, 그리고 confidential로 분류하였으며 사용자의 인증 레벨을 결정하기 위해 얼굴, 목소리 등을 사용하였다. Crawford et al.[3]은 현재 스마트 기기를 가지고 있는 사람이 주인인지 확인하기 위해 Keystroke dynamic과 목소리를 사용하였다. Ryu et al.[4]은 사용자들이 사용한 애플리케이션에서 실제로 사용하고 있는 인증기술에 따라 인증레벨을 1~4단계로 분류하였으며 얼굴 인증을 통한 Grade-Up과 주변 무선 AP(Access Point) 정보 또는 블루투스 정보를 통해 사용자가 지정한 COI(Context of Interest)의 유사도 점수를 측정하여 Grade-Extend를 제공하여 명백한 인증을 하지 않고 애플리케이션을 사용할

1) 이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원(No.2016-0-00173, 핀테크 서비스 금융사기 방지를 위한 비대면 본인확인) 및 한국연구재단의 지원(No.2016R1A4A1011761, 핀테크 서비스를 위한 금융 보안 핵실 기술 개발)을 받아 수행된 연구임

* 주저자, gsryu1026@smail.kongju.ac.kr

† 교신저자, sunchoi@kongju.ac.kr

수 있는 무자각 지속 인증기술을 제안하였다.

본 논문에서는 Ryu et el.이 사용자 주변 무선 AP 정보와 블루투스 정보 중 하나만 사용한 것보다 COI 유사도 점수를 더욱 정확한 측정을 위해 사용자 주변 무선 AP 정보와 스마트 시계를 통해 수집된 블루투스 정보를 이용하며 Autoencoder를 통해 사용자의 COI를 모델링하여 유사도 점수를 측정하는 방법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 사용한 데이터와 특징 추출 방법을 설명하고, 3장에서는 COI 유사도 점수 측정 방법을 설명한다. 4장에서는 제안 방법을 이용한 COI 유사도 점수 측정 실험을 설명한다. 마지막으로 5장에서 결론을 맺는다.

II. 데이터 및 특징 추출

이번 장에서는 수집한 데이터와 특징 추출 방법에 대해서 다룬다. 사용자가 지정한 COI의 유사도 점수 측정을 하기 위해 실험 참가자 22명에게 데이터 수집 애플리케이션을 제공하여 20일 동안 3회씩 COI의 무선 AP 정보와 스마트 시계의 블루투스 정보를 수집하였다.

2.1 수집 데이터

무선 AP 정보는 무선 AP의 MAC 주소(Media Access Control address)를 의미하는 BSSID(Basic Service Set Identifier)와 스마트폰에서 수신한 무선 AP의 신호 세기인 RSSI(Received Signal Strength)를 수집하였다. 블루투스 정보는 스마트 시계에서 스마트폰의 블루투스 MAC 주소와 RSSI를 수집하였으며 스마트폰에서는 스마트 시계의 블루투스 MAC 주소와 RSSI를 수집하였다. 스마트폰과 스마트 시계에서 수집한 환경정보는 Table 1.에서 보여준다.

Table 1. 스마트 기기에서 수집한 환경정보

기기	수집 정보	세부 정보
스마트폰	무선 AP	BSSID
		RSSI
	블루투스	MAC address
		RSSI
스마트 시계	블루투스	MAC address
		RSSI

2.2 특징 추출

Autoencoder를 이용하여 사용자의 COI 모델을 만들기 위해 수집한 무선 AP 정보와 블루투스 정보를 특징 추출하였다.

무선 AP 정보는 학습 데이터에 대해서 RSSI가 강한 3개의 BSSID를 저장한 후 등록된 BSSID가 있으면 해당 BSSID의 RSSI 값을 사용하였으며, 등록된 BSSID가 없으면 무의미한 값을 사용하였다. RSSI가 강한 무선 AP 3개만 사용한 이유는 RSSI가 약한 무선 AP는 사용자의 COI와 거리가 멀어 구분력이 떨어지기 때문이다[5]. 블루투스 정보도 학습 데이터에 대해서 스마트폰과 스마트 시계의 블루투스 MAC 주소와 저장한 후 등록된 스마트폰과 스마트 시계의 블루투스 MAC 주소가 있으면 해당 MAC 주소의 RSSI 값을 사용하였으며, 등록된 MAC 주소가 없으면 무의미한 값을 넣어 사용하였다.

III. Autoencoder를 활용한 COI 유사도 점수 측정방법

이번 장에서는 Autoencoder를 활용하여 사용자의 COI 유사도 측정방법에 대해서 다룬다.

3.1 Autoencoder

Autoencoder를 활용하여 사용자의 COI 모델을 만든다. Autoencoder는 비지도 학습법을 사용하는 인공신경망으로 다음과 같은 구조를 가진다.

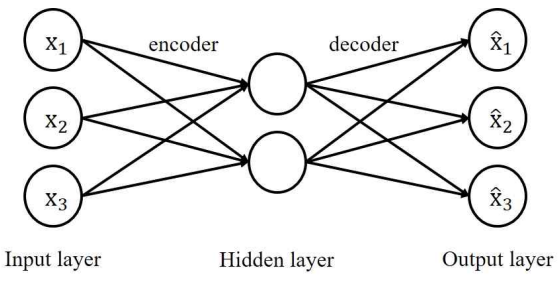


Fig 1. Autoencoder의 기본 구조

Autoencoder는 Fig 1.에서 보이는 것처럼 encoder와 decoder로 구성된다. encoder는 다음과 같이 정의된다.

$$z = \sigma_1(Wx + b) \quad (1)$$

위 식에서 σ_1은 활성화 함수(Activation function), W는 가중 행렬(Weight matrix), x는 입력 벡터, 그리고 b는 편향 벡터(Bias vector)를 의미한다. decoder는 z를 입력값 x와 동일한 모양인 x′을 생성하며 다음과 같이 정의된다.

$$x' = \sigma_2(W'z + b') \quad (2)$$

Autoencoder는 다음과 같이 x와 x′의 차이를 의미하는 손실계수(Cost)가 최소화되도록 학습시킨다.

$$\text{cost} = \frac{\sqrt{(x - x')^2}}{n} \quad (3)$$

위 식에서 n은 입력 벡터의 총 개수를 의미한다. Autoencoder는 입력값과 출력값이 최대한 같아지도록 학습하는 알고리즘이기 때문에 주로 특징 추출, 이상 탐지 및 사용자 인증에 사용된다.

3.2 COI 유사도 점수 측정방법

Autoencoder로 사용자의 COI 모델을 만든 후 COI 유사도 점수는 다음과 같이 측정될 수 있다.

$$score = 1 - \frac{\text{cost}_i}{\max(\text{cost})} \quad (4)$$

위 식에서 cost_i는 i번째 입력 벡터에 대한 cost를 의미하며, max(cost)는 사용자 COI 모델에서 나올 수 있는 cost의 최대값을 의미한다. 따라서 COI 유사도 점수는 0~1 사이의 값을 가지며 1에 가까울수록 사용자가 지정한 COI에 있을 확률을 나타낸다.

IV. COI 유사도 점수 측정 및 고찰

이번 장에서는 제안한 방법을 이용하여 COI 유사도 점수 측정실험에 대해서 다룬다. 사용한 22명의 실험 참가자들이 20일 동안 하루에 3회씩 COI 주변 환경정보이다. 전체 사용자에 대한 환경정보는 총 1320개가 있으며, 한 사용자에 대한 환경정보는 60개가 있다. 사용자의 환경정보 60개 중 21개를 학습 데이터로 사용하였으며, 나머지 39개를 COI 유사도 점수 측정을 위해 사용하였다. 실험은 스마트폰에서 수집한 주변 무선 AP 정보만을 이용하여 COI 유사도 점수 측정실험과 스마트폰에서 수집한 주변 무선 AP 정보 및 스마트 시계의 블루투스 정보와 스마트 시계에서 수집한 스마트폰의 블루투스 정보 모두 사용하여 COI 유사도 점수 측정실험을 수행하였다.

4.1 스마트폰에서 수집한 주변 무선 AP 정보만 사용한 COI 유사도 측정실험

실험 참가자들이 스마트폰에서 수집한 COI 주변 무선 AP 정보만을 사용하여 Autoencoder로 사용자 COI 모델을 만든 후 COI 유사도 측정실험을 수행하였다.

Table 2. 무선 AP 정보만 이용하여 측정한 COI 유사도 점수 비율

유사도 점수 범위	비율
0.5 미만	0.12
0.5 이상 0.6미만	0.01
0.6 이상 0.7미만	0.02
0.7 이상 0.8미만	0.05
0.8 이상 0.9미만	0.11
0.9 이상	0.69

실험결과 유사도 점수가 0.5 미만으로 측정된 비율이 12%로 측정되었으며, 0.9 미만으로 측정된 유사도 점수는 31%로 상당히 높았다. Table 2.는 전체 사용자의 테스트 데이터 세트에서 COI 유사도 점수가 나온 비율을 보여준다.

4.2 스마트폰과 스마트 시계에서 수집한 환경정보 모두 사용한 COI 유사도 측정실험

실험 참가자들이 스마트폰과 스마트 시계에서 수집한 모든 환경정보를 이용하여 Autoencoder로 사용자 COI 모델을 만든 후 COI 유사도 측정실험을 수행하였다.

실험결과 유사도 점수가 0.8 미만으로 측정된 비율이 0%로 측정되었으며, 0.9 이상으로 측정된 비율은 99%로 무선 AP 정보만 이용하여 측정한 것보다 30% 더 높게 측정되었다. Table 3.은 전체 사용자의 테스트 데이터 세트에서 COI 유사도 점수가 나온 비율을 보여준다.

Table 3. 스마트폰과 스마트 시계에서 수집한 모든 환경정보를 이용하여 측정한 COI 유사도 점수 비율

유사도 점수 범위	비율
0.5 미만	0.00
0.5 이상 0.6미만	0.00
0.6 이상 0.7미만	0.00
0.7 이상 0.8미만	0.00
0.8 이상 0.9미만	0.01
0.9 이상	0.99

4.3 고찰

무선 AP 정보만 이용하여 사용자 COI 모델 생성 후 COI 유사도 점수 측정했을 때 실험 참가자들이 자신의 COI에서만 주변 무선 AP 정보를 수집했음에도 불구하고 COI 유사도 점수의 31%는 0.9를 넘지 못했다. 그 이유는 참가자 COI 주변 무선 AP들이 항상 작동하고 있는 것이 아니기 때문이다. 따라서 무선 AP 정보만을 이용하여 COI 유사도 점수를 측정하는 것은 적절하지 못하다.

스마트폰과 스마트 시계에서 수집한 COI의 모든 환경정보를 이용하여 사용자 COI 모델 생성 후 COI 유사도 점수를 측정했을 때 0.9 이상인 COI 유사도 점수의 비율이 99%로 측정되었다. 그 이유는 무선 AP 정보와는 달리 스마트 시계는 사용자 주변에 있기 때문이다. 하지만 스마트폰과 스마트 시계에서 수집한 서로의 블루투스 정보만을 이용하여 사용자 COI 모델을 만들어 COI 유사도 점수를 측정하는 것은 적절하지 못하다. 그 이유는 사용자가 COI에 머무르지 않을 때의 COI 유사도 점수는 항상 좋게 측정될 것이기 때문이다. 따라서 COI의 주변 무선 AP 정보와 블루투스 정보 모두 사용하는 것이 더 정확한 COI 유사도 점수를 측정할 수 있다.

V. 결론

본 논문에서는 무자각 인증 강화를 위해 스마트 시계를 추가로 활용하여 더 정확한 COI 유사도 점수 측정방법을 제안하였다. 스마트폰과 스마트 시계에서 수집한 COI 환경정보를 특징 추출하여 Autoencoder를 통해 사용자 COI 모델을 만들어 COI 유사도 점수를 측정하였다. 실험결과 COI 주변 무선 AP 정보만 이용했을 때보다 주변 무선 AP 정보와 블루투스 정보를 함께 이용했을 때 COI 유사도 점수가 0.9 이상 나오는 비율이 30% 더 높게 측정되었다.

[참고문헌]

[1] Consumer reports. https://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm.

[2] O. Riva, C. Qin, K. Strauss, and D. Lymberopoulos, Progressive Authentication: Deciding When to Authenticate on Mobile Phones, USENIX Security Symposium, 301-316, 2012.

[3] H. Crawford, K. Renaud, and T. Storer. A framework for continuous, transparent mobile device authentication. Computers & Security 39, 127-136, 2013.

[4] G. Ryu, S. Park, D, Choi, Y. Kim, S. Kim, S. Kim, D. Kim, and D. Kwon, Active Authentication Experiments Using Actual Application Usage Log, In RESEC'18: The 1st Radical and Experiential Security Workshop, June, 2018.

[5] G. Ryu, C. Seo, and D. Choi, Location Authentication based on Wireless Access Point Information to Prevent Wormhole Attack in Samsung Pay, Advances in Electrical and Computer Engineering, 17(3), 71-76, 2017.

라즈베리 파이를 이용한 휴대용 영상감시시스템 개발

최경호*, 김현진**, 현부영**, 김종민***, 이동휘****

* 사이버보안평가기술원 기업부설연구소 연구소장

** 동신대학교 에너지융합대학 정보보안전공

*** 경기대학교 융합보안학과 초빙교수

**** 동신대학교 에너지융합대학 정보보안전공 교수(Corresponding Author)

A Development of Portable Video Monitoring System using Raspberry Pi

Kyong-ho Choi*, Hyun-Jin Kim**, Bu-Young Hyun**,

Jong-Min Kim***, DongHwi Lee****,

* Head of Research Center, Institute of Cyber Security Technology

** Information Security, Dongshin University

*** Convergence Security, Kyonggi University

**** Information Security, Dongshin University (Corresponding Author)

요 약

발전하는 정보통신기술들은 우리의 삶에 유용하게 이용되고 있다. 그중에서도 원거리, 폐쇄된 공간 등 관리 담당자의 인지능력이 닿지 않는 곳을 모니터링하는 기술들의 발전은 우리가 알지 못하는 곳에서, 알지 못하는 때에 발생하는 사건 및 사고들에 대해 적시적인 조치를 할 수 있는 기회를 가져다주고 있다. 그러나, 특정 장소를 24시간 내내 촬영하여 범죄 예방 및 사건 추적 등으로 활용하고 있는 CCTV 장치는 영상 데이터의 저장 및 보관도 필요하기 때문에 내부 네트워크 또는 와이파이 환경에서 고정형으로 이용하는 경우가 대다수이기에, 일시적인, 임시적 공간에서의 영상감시로 활용하기는 어려운 상황이다. 그러므로 본 논문에서는 이동성과 일시적 수요에 능동적인 대응이 가능한 휴대용 영상감시장치를 개발하는 것을 주 목적으로 하여, 손쉽게 가지고 다닐 수 있는 편리성을 확보하기 위해 저비용, 저전력 및 소형화한 제품을 구현하는 것을 보이기로 한다.

I. 서론

발전하는 정보통신기술들은 우리의 삶에 유용하게 이용되고 있다. 그중에서도 원거리, 폐쇄된 공간 등 관리 담당자의 인지능력이 닿지 않는 곳을 모니터링하는 기술들의 발전은 우리가 알지 못하는 곳에서, 알지 못하는 때에 발생하는 사건 및 사고들에 대해 적시적인 조치를 할 수 있는 기회를 가져다주고 있다. 그러므로 이를 적절히 잘 활용한다면 의도치 않은 일들로 인해 발생 가능한 손실들을 줄일 수 있고, 예상 가능한 위협들을 제거할 수 있는 능동적인 활동이 가능할 것이다.

사용자가 모니터링을 필요로 하는 지역을 효과적으로 관리하기 위한 수단은 여러 가지가 있지만, 그중에서도 영상, 음성 및 행위 인식 등을 통합적으로 분석 가능한 지능형 영상보안

시스템은 그 유용성으로 인해 다양하게 활용되고 있다. 기존 단순 영상촬영 및 관리자의 점검으로 진행되던 영상보안은 지능형 영상감시, 생체인식, CCTV/DVR (Digital Video Recorder) 영상보안 기술 등 각기 다른 배경과 응용기술로 발전되어 왔으며, 공항, 군사, 항만, 도로, 교량 등 주요 국가시설, 지하철, 버스, 빌딩, 경기장, 주차장, 카지노, 응급상황 감시 및 자동차/모바일기기에 이르기까지 그 응용분야도 확대되고 있다[1, 2].

그러나, 특정 장소를 24시간 내내 촬영하여 범죄 예방 및 사건 추적 등으로 활용하고 있는 CCTV 장치는 영상 데이터의 저장 및 보관도 필요하기 때문에 내부 네트워크 또는 와이파이 환경에서 고정형으로 이용하는 경우가 대다수이기에, 일시적인, 임시적 공간에서의 영상감시로 활용하기는 어려운 상황이다. 공공기관에서의 광범위한 영상감시/관제[3], 공유모델[4]과 개인들의 가정과 사업장 보호를 위한 사설 감시체제들은 모두 특정된 영역을 위한 것들이며, 단기적으로 또는 이동 중인 상황에서의 영상감시는 기 설치된 외부조직의 것들에 의존할 수 밖에 없다. 즉, 범죄 발생 이후 유관 조직의 협조를 얻어 관련된 영상들을 얻어야 하는 절차로 넘어가야 한다는 것이다. 이동성만 본다면 차량용 블랙박스가 일견 이를 해결하는 것처럼 보이지만, 일시적인 수요에 대한 처리가 어렵다는 점은 동일한 문제로 드러난다. 차량용 블랙박스 역시 차량 내부에 고정되어 있다는 것을 유념해야 한다.

그러므로 본 논문에서는 이동성과 일시적 수요에 능동적인 대응이 가능한 휴대용 영상감시 장치를 개발하는 것을 주 목적으로 하여, 손쉽게 가지고 다닐 수 있는 편리성을 확보하기 위해 저비용, 저전력 및 소형화한 제품을 구현하는 것을 보이기로 한다.

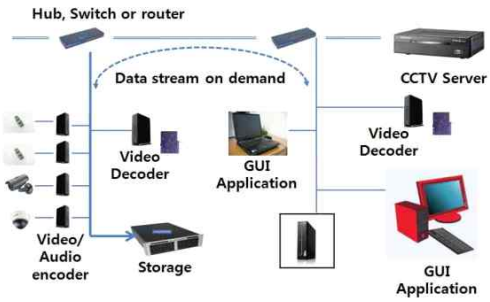
이를 위해 이어지는 2장에서는 지능형 영상감시시스템과 저렴하게 이용 가능한 오픈 소스 기반의 싱글보드에 대해 알아보고, 3장에서 휴대용 영상감시 장치를 설계한다. 이후 4장에서 구현된 내용을 살펴보고, 마지막으로 결론을 맺기로 한다.

II. 관련 연구

2.1 지능형 영상감시시스템

영상감시시스템은 국내 보안시장에서 잇따르는 여러 가지 보안 사고에 따른 보안 감시시스템의 강화, 경찰서/교통 관련 공공기관 등의 보안장비의 업그레이드 등으로 수요가 증가하는 추세이며, 향후 수요처는 원격감시 기능이 일반 가정으로까지 확대되는 추세로 연결될 것으로 전망되고 있고[5], 이러한 전망은 댁내 또는 어린이집 등의 보육환경 모니터링, 개별 사업장 안전관리 등의 목적으로 CCTV가 이용되면서 현실화되고 있다.

영상감시시스템은 CCTV를 기반으로 특정 지역을 24시간 실시간 감시하며, 이를 유/무선 네트워크를 통해 저장하고, 관제센터에 데이터를 전송하여 분석 및 대응할 수 있게 해주는 구조로 구성된다. 그래서 범죄 예방에 관심 있는 정부 부처, 공공기관을 중심으로한 수요가 높으며, 고도화된 기술의 부가가치 또한 높다.



[그림 1] 지능형 영상감시시스템의 구성도[6]

최근의 영상감시시스템은 지능형 영상감시시스템이라 불리우며, 움직임 검출(change detection), 영역 검출(region detection), 물체 추적(object tracking), 객체 분류(objects classification), 객체 인식 및 추적(objects identification and tracking) 등의 모듈이 추가되며 발전하고 있고, 그 응용 영역 또한 넓고 깊어지고 있다[5].

2.2 라즈베리 파이

라즈베리 파이(Raspberry Pi)는 2012년 2월에 출시된 소형 교육용 컴퓨터 보드로 PC에서 사용되는 다양한 주변장치들을 직접 연결해서 적은 비용으로 리눅스 기반의 컴퓨터를 구성할 수 있다[7]. 그리고 필요로하는 기능들이 모듈화되어 있어 목적에 따라 센서 또는 쉴드를 구매, 장착하여 확장시킬 수 있기 때문에 적은 비용으로 최적화된 컴퓨팅 능력을 제공할 수 있어 목적에 따른 특화된 장치를 개발하기에 유용하다. 특히, 교육용으로 개발된 덕분에 인터넷에서 프로그래밍과 응용에 관한 자료를 손쉽게 구할 수 있어 일반인들의 접근성이 뛰어나다는 강점을 가지고 있다.



[그림 2] 라즈베리 파이용 각종 센서 및 장치들[8]

이러한 라즈베리 파이는 IoT 기반 홈 보안 시스템[9], 불꽃 감지를 이용한 스마트 경보[10], 소리를 인식하는 보안카메라[11] 및 얼굴검출 시스템[12] 등으로 응용되며, 지능형 영상감시시스템 분야 적용 시의 유용성을 이미 입증한 바 있다.

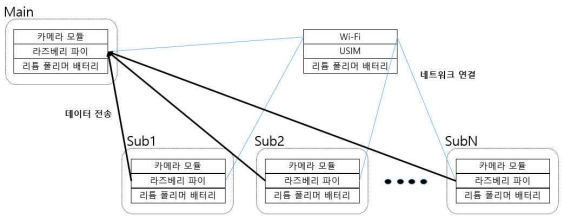
III. 시스템 설계 및 구현

3.1 시스템 설계

본 연구에서 제안하는 휴대가 용이한 영상감시시스템은 필요한 장소에서 필요한 경우에 즉시적으로 설치 및 활용하고, 사용 목적 달성 후에는 바로 철거가 가능하며, 또 다른 곳에서의 재사용을 가능하게 할 수 있도록 하려 한다. 따라서, 다음과 같은 요구사항들이 제기된다.

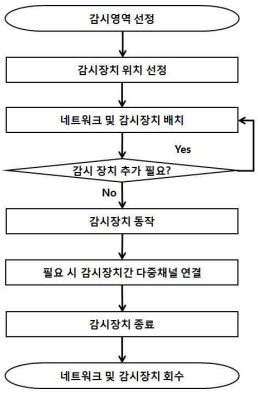
- 전기 사용이 불가한 곳에서의 사용이 가능하도록
- Wi-Fi(wireless fidelity: 무선 데이터 전송 시스템)가 없는 상황에서의 정보 송수신
- 일시적이긴 하나 다양한 각도의 감시를 위한 영역 확장
- 용이한 휴대를 위한 경량화, 소형화

상기 요구사항들을 해결하기 위해서는 배터리와 USIM(Universal subscriber identity module) 기반의 직접 데이터 전송 네트워크를 이용할 수 있으며, 라즈베리 파이 카메라를 병렬 연결하여 다중 감시체제를 확립할 수 있다. 이러한 제안 시스템의 구성도는 다음 그림 3과 같다.



[그림 3] 제안시스템 구성도

그리고 제안된 시스템은 중요 또는 민감한 물체나 장소에서 일정 기간 동안 영상감시를 해야 할 필요성이 제기될 때 사용할 수 있으며, 이의 활용 절차는 다음 그림 4와 같다. 휴대가 용이한 감시장치는 USIM을 이용하는 Wi-Fi 장치와 함께 사용되어 네트워크를 구성하며, 특정 영역을 감시해야 하는 영상감시시스템이 사각지역을 없게 하기 위해 다중 채널 또는 360도 회전 등을 이용하는 것처럼 본 연구에서 제안된 시스템은 다중 채널 연결을 활용하여 사각지대를 제거할 수 있다.



[그림 4] 제안시스템 활용절차

3.2 시스템 구현

제안된 시스템을 물리적으로 구현하는 방법은 라즈베리파이 3(Raspberry Pi3) 보드에 영상감시를 위해 필요한 카메라 모듈(V2 8Megapixel)과 라즈베리파이의 동작과 감시영상 저장을 위한 저장장치(Sandisk SDXC Ultra MicroSD 16GB 메모리카드)를 추가하는 것이다. 이때, 보드와 카메라 모듈은 버전에 따라 호환성이 다를 수 있으므로, 필요 성능 또는 물리적으로 갖출 수 있는 조건 등에 따라 변화될 수 있다. 제안된 시스템의 물리적 구현 내용은 다음 그림 5와 같이 볼 수 있으며, 여기서 라즈베리파이 기반 영상감시장치의 물리적인 특징인 소형, 경량 그리고 가장 큰 특징인 싱글보드에 필요 모듈만 추가하면 되는 간편, 비용최소화 등의 장점을 볼 수 있다.



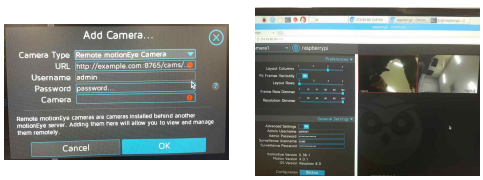
[그림 5] 라즈베리파이 보드와 카메라모듈 결합

이후 준비된 하드웨어 구성에 맞추어 라즈베리파이 SD 카드에 운영체제(Raspbian 4.9)를 설치한다. 이후 카메라 모듈을 CCTV로 활용하기 위해 Motion 4.0-1과 MotionEye 4.1을 설치하여 소프트웨어적인 구성을 한다. 이때 프로그램 활용을 위한 ffmpeg, v4l-utils, libmariadb client18, libpq5 등의 라이브러리도 함께 설치되어야 한다.

IV. 구현 시스템 평가

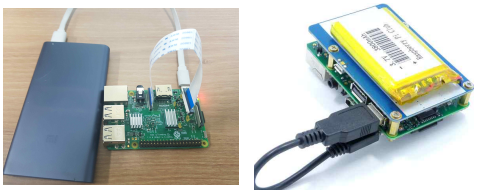
제안된 시스템은 기본적으로 사용자에게 영상감시시스템에 대해 저비용으로 높은 접근성을 제공한다. CCTV와 여기서 발생하는 영상데이터 저장을 위한 NVR (Network Video Recorder) 설치 및 네트워크 구성 시보다 약 1/4 정도의 저렴한 비용으로 영상감시시스템의 직접 설치 및 운영을 가능하게 한다. 이러한 강점은 현재의 영상감시시스템을 대체하는 면에서 볼 때 보다 큰 파급효과를 가질 수 있을 것으로 기대된다. 고정형으로 설치되는 CCTV 카메라들을 대체하면 소형화된 장치를 사용하면서도 무선 네트워크를 채용할 수 있어, 선로 공사 등의 소요가 줄어 설치, 운영 및 관리 상의 비용효과성과 편의성이 높고, 이러한 효과는 관리 대상 CCTV 카메라 수량 증가와 감시영역의 증대에 있어 보다 더 파급력을 가지게 될 것이다.

그리고 제안된 시스템은 소프트웨어적인 병렬 연결을 통해 다중 채널 감시로 확장 가능하여, 저비용으로 감시 영역의 확대와 사각지대 해소라는 장점을 극대화시킬 수 있다. 2개의 감시장치 연결 시 다음 그림 6과 같이 하나의 화면에서 함께 볼 수 있으며, 이는 중심이 되는 라즈베리파이 보드로 다른 라즈베리파이 카메라들이 데이터를 전송하여 영상감시 데이터를 한 곳으로 모아 살펴보는 효과를 얻을 수 있게 해주기 때문이다.



[그림 6] 라즈베리파이 기반 감시장치 다중채널 연결

본 연구에서 제안한 시스템을 통해 얻고자 했던 가장 큰 장점인 휴대성과 이동성도 충분히 안정적으로 확보되었다. 라즈베리파이 보드, 리튬 폴리머 배터리 및 카메라 모듈 부착 시에도 그 크기와 무게는 일반적인 CCTV 카메라보다 절반 정도의 수준이며, 자체 충전된 전력과 이동통신망을 이용한 데이터 통신을 활용하기에 야외나 격오지 등 전기 및 유/무선 네트워크 사용이 어려운 곳에서의 사용도 용이하다. 또한 구성되는 감시장치 및 네트워크 연결이 무선으로 이루어져 있는 점과 감시장치, 네트워크 장치들이 소형화된 단일 품목이라는 점에서 배치, 철거 및 이동이 간편한 점도 특징적으로 나타난다.



[그림 7] 싱글보드에 적용 가능한 배터리 예시[13]

단, 라즈베리파이를 어떤 목적으로 이용하느냐에 따라 전력 사용량은 달라질 수 있으며, 본 연구에서는 구현 및 실험을 위해 필요한 운영체제와 MotionEye 외에는 보드에 그 어떤 소프트웨어도 설치하지 않았다. 이는 라즈베리파이와 이에 연결된 모듈들이 필요로 하는 전력, 라즈베리파이 모델별 기본적으로 소요되는 전력 그리고 구성된 라즈베리파이 기반 시스템 운영 시 소모되는 전력 등을 모두 고려해서 배터리 용량과 충전 방식을 고려해야 하기 때문이다. 즉, 예상되는 소요 전력량은 구현하는 시스템을 휴대용으로 이용했을 때의 가능한 한계 시간을 알 수 있게 해주기 때문에, 목적에 맞는 최소한의 운영은 일시적 영상감시 필요에 따른 실행 가능 최대 시간을 확보해 줄 수 있다. 이에 반해, 배터리 용량을 늘리는 방법이 손쉬운 대안으로 생각될 수 있으나, 배터리 크기가 커질수록 장치의 크기와 무게는 더욱 더 커지기 때문에, 휴대성과 이동성은 하락한다고 볼 수 있다.

V. 결론

본 연구에서는 라즈베리파이 기반의 휴대용 영상감시시스템을 개발하는 것을 주된 목적으로 하였다. 라즈베리파이는 오픈소스로 누구나 손쉽게 활용 가능하며, 소프트웨어적인 업그레이드로 다채널 감시, 객체 추적 등 지능형 영상감시시스템으로 발전시킬 수 있어, 영상감시 분야에서 비용효과적인 선택이 될 수 있는 장치이다. 비록 본 연구에서는 소형, 경량을 특징으로 하는 휴대성과 이동성에 초점을 맞추어 개발을 진행하였으나, 소리 탐지나 선택 영역 감시 등의 기술을 추가하는 등의 추가 개발 노력을 통한다면, 현재의 영상감시시스템을 효과적으로 대체하고, 보다 더 지능적인 영상감시시스템을 개발하기 위한 기반을 마련할 수 있을 것으로 기대된다.

그러나 본 연구에서 제안한 시스템은 이러한 장점들 외에 한계점도 분명히 존재한다. 먼저 USIM 기반 무선공유기의 저전력화 달성이 필요하다. 네트워크 이동성을 고려할 때, 상용화된 USIM을 이용한 무선공유기의 활용은 적절한 것으로 생각되나, 보다 더 소형화하고 경량화하면서도 전력 소모를 낮출 수 있는 대체품이 존재하거나, 개발할 수 있을 것으로 생각된다.

그리고 휴대성과 이동성에 초점을 맞춘 라즈베리파이 기반 영상감시장치는 소형 CCTV 카메라가 도난, 분실 및 멸실 등에 취약한 것과 같이 동일한 문제점에 직면해 있다. 악의적 사용자가 라즈베리파이 기반 영상감시장치를 물리적으로 절취한다면, 감시영역에 공백이 생기는 것 뿐만 아니라, 감시 내용이 저장된 영상데이터의 유출 문제도 함께 발생하는 것이다. 이에 대한 대응으로는 SD카드에 영상 저장 시 암호화하는 방안이 좋을 것으로 생각되며, 전력 소모량와 실시간 운용 능력을 저하시키지 않는 범위 내에서 추진되어야 할 것이다.

이외에도 개인프라이버시 보호 문제 등 여러 한계점들이 더 나타날 수 있겠지만, 보다 더 중요한 것은 그 한계들을 극복하고, 문제점들을

개선하며, 보다 혁신적인 기술들을 제공하려는 노력들을 경주하는 것이다. 이를 통해 더 많은 사람들이 자신만의 영상감시 환경을 구성하고, 더욱 더 발전된 기술들을 적용할 수 있어 안전한 사회와 가정환경을 만들어 가는데 일조할 수 있을 것이다.

[참고문헌]

[1] 유장희, 문기영, 조현숙, 지능형 영상보안 기술현황 및 동향, 전자통신동향분석, 23권, 4호, pp. 80-88, 한국전자통신연구원, 2008.

[2] 강희조, 사회안전을 위한 지능형 영상감시분석시스템, 디지털콘텐츠학회지, 17권, 4호, pp. 273-278, 한국디지털콘텐츠학회, 2016.

[3] 권창환, 서창갑, 부산광역시 CCTV통합관제센터구축 사례연구, 디지털융복합연구, 9권, 3호, pp. 191-202, 한국디지털정책학회, 2011.

[4] 강푸름, 김귀남, CCTV 영상자료 통합포털 구축 모델에 관한 연구, 정보·보안논문지, 12권, 2호, pp. 43-51, 한국융합보안학회, 2012.

[5] 송재민, 김동진, 정용배, 박영석, 김태효, 임베디드 시스템 기반 지능형 영상 감시 시스템 구현, 신호처리·시스템학회 논문지, 13권, 2호, pp. 83-90, 한국신호처리·시스템 학회, 2012.

[6] 강희조, 스마트 재난관리 영상감시시스템과 적용, 한국항행학회논문지, 15권, 6호, pp. 1234-1240, 한국항행학회, 2011.

[7] 김동경, 우종호, 라즈베리 파이를 이용한 무선 자동차번호판 영역 추출 모듈 개발, 한국멀티미디어학회논문지, 18권, 10호, pp. 1172-1179, 한국멀티미디어학회, 2015.

[8] 인터넷 쇼핑몰에서의 상품 예시,

https://www.coupang.com/vp/products/30307844?itemId=115425154&vendorItemId=3231121141&q=%EB%9D%BC%EC%A6%88%EB%B2%A0%EB%A6%AC%ED%8C%8C%EC%9D%B4&itemsCount=36&searchId=3fc53615767647b6a75f4a07f5ec2162&rank=8

[9] 김강철, 한석붕, IoT 기반 홈 보안 시스템, 한국전자통신학회 논문지, 12권, 1호, pp. 147-154, 한국전자통신학회, 2017.

[10] 이영민, 손경락, 라즈베리파이 기반 미소불꽃 감지를 이용한 스마트 경보 서비스 시스템 구현, 한국마린엔지니어링학회지, 39권, 9호, pp. 953-958, 한국마린엔지니어링학회, 2015.

[11] 박대복, 김선혁, 김주영, 노영주, 라즈베리파이 기반 소리인식 보안카메라 개발, 한국정보처리학회 2015년도 추계학술발표대회 논문집, 제22권, 제2호, pp. 1563-1566, 한국정보처리학회, 2015. 10.

[12] 김강철, 라즈베리파이를 이용한 얼굴검출 및 인식 시스템 개발, 한국전자통신학회 논문지, 12권, 5호, pp. 859-864, 한국전자통신학회, 2017.

[13] 라즈베리파이용 배터리팩 사용 예시는 인터넷 쇼핑몰 참조

http://item.gmarket.co.kr/

Item?goodscode=847686273

LR Guard : ARM TrustZone을 활용한 제어 흐름 보호 기법 설계*

진홍주*, 장혜린*, 이동훈*
*고려대학교 정보보호학과

LR Guard: Control flow protection scheme design using ARM TrustZone*

Hongjoo Jin*, Hyerean Jang*, Dong Hoon Lee*
*Graduate School of Information Security, Korea University.

요 약

다양한 분야에서 활용되는 임베디드 시스템은 일상생활의 여러 측면에 침투하였고, 임베디드 디바이스에 각종 센서와 통신기능이 내장된 사물 인터넷 시장 규모가 크게 증가하였다. 하지만 네트워크 연결을 고려하지 않은 임베디드 시스템은 보안에 취약하다. 메모리 공간을 보호하기 위한 다양한 기법들이 제안되었고, 원칙적으로 간접 점프의 대상을 임의로 수정하는 것을 방지하는 제어 흐름 무결성 기법이 제안되었다.

본 논문에서는 코드 재사용 공격을 사용하는 강력한 공격자 모델에 대한 프로그램 보호를 위해 ARM TrustZone을 활용한 LR Guard를 제안한다. 제안하는 제어 흐름 보호 기법을 설명하고 성능 오버헤드를 발생시키는 두 요소를 확인한다.

I. 서론

최근 임베디드 시스템 시장은 급격하게 성장하고 있고, 산업, 의료 등 다양한 분야에서 활용되는 임베디드 시스템은 일상생활의 여러 측면에 침투하였다[1]. 정보통신기술의 발달로 임베디드 디바이스에 각종 센서와 통신기능이 내장되었다. 이에 따라 사물 인터넷(Internet of Things) 시장 규모도 크게 증가하였다. 하지만 임베디드 디바이스는 네트워크 연결을 고려하지 않은 리눅스 시스템으로 구성되고, 리소스가 제한적이기 때문에 보안에 취약하다[2].

임베디드 리눅스는 C/C++ 언어로 작성되어 프로그래머에게 효율적인 메모리 접근을 제공한다. 하지만 이는 메모리 관련 버그를 유발하기 때문에 공격자가 프로그램의 동작을 변경하거나 시스템을 완전히 제어할 수 있다[3]. 메모리 관련 버그 중 가장 빈번하게 활용되는 버그는 버퍼 오버플로 보안 약점이다. 공격자들은 버퍼 오버플로를 이용해 스택(Stack) 메모리 공간에 공격자가 원하는 코드를 주입시키는 코드 인젝션(Code Injection) 공격을 수행한다. 코드 인젝션 공격에 대한 대응으로 스택 메모리 공간을 보호하기 위한 기법인 StackGuard[4] 기법과 DEP(Data Execution Prevention)[5] 기법 등의 다양한 방어 기법이 제안되었다. 하지만 공격자는 기존 코드를 이용하는 새로운 공격 기법을 통해 제안된 방어 기법을 우회하였다. 이처럼 소프트웨어의 취약점에 대한 정교한 공격은 배포된 보호 매커니즘을 우회해 왔다. 이는 기존의 StackGuard, DEP 등의 방어 기법이 근본적인 문제를 해결하기보다는 특정 공격 기술에 초점을 맞추었기 때문이다.

이처럼 소프트웨어의 취약점에 대한 방어기법은 새로운 공격 기법에 의해 우회되었다. 따

* 이 성과는 2018년도 과학기술정보통신부의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2017R1A2B3009643).

라서 기존 방어 기법의 한계를 넘어선 제어 흐름 무결성(Control Flow Integrity)[6] 기법이 제안되었다. 제어 흐름 무결성 기법은 공격자가 간접 점프(Indirect Jump)의 대상을 임의로 수정하는 것을 방지하는 원칙적인 기법이다. 또한 제어 흐름의 무결성을 보장하여 프로그램의 실제 실행이 항상 올바르게 정의된 경로(Path)로 진행하게 하여 공격자가 의도한 실행을 허용하지 않는다. 하지만 제어 흐름 무결성 기법의 시행은 큰 성능 오버헤드가 발생하기 때문에 리소스가 제한적인 임베디드 환경에서 적용하기 어렵다.

임베디드 시스템에서 주로 사용되는 ARM 아키텍처는 리소스의 한계로 일반적으로 사용되는 보안 매커니즘을 적용하기 어렵다. ARM 프로세서에서 낮은 비용으로 제어 흐름의 무결성을 보장할 수 있으면 임베디드 시스템의 보안성 향상에 크게 기여할 수 있다. 본 논문에서는 임베디드 시스템에서 주로 사용되는 ARM 아키텍처에서 제어 흐름을 보호하기 위한 기법을 설계한다. 가장 보편적으로 사용되는 코드 재사용(Code Reuse) 공격을 원천적으로 막기 위한 기법을 제안하고, 기법에 대한 설계(Design)를 제시한다.

II. 배경지식

2.1 리턴 지향 프로그래밍

리턴 지향 프로그래밍(Return-Oriented Programming, ROP)[7] 기법은 빈번하게 사용되는 코드 재사용 공격 기법중 하나이다. ROP 공격은 ret 명령어(Instruction)로 끝나는 짧은 코드 조각인 가젯(Gadget)을 사용하여 새로운 실행 흐름을 구성하여 공격을 형성하거나, 공격자가 원하는 코드 실행을 위한 부분 경로를 생성한다. 공격자는 알려진 라이브러리 코드 등에서 신중하게 선택한 가젯들을 연결해 공격자가 원하는 코드(ex. 쉘 코드)를 실행하기 위한 가젯체인을 만든다. 이를 통해 공격자는 프로그램 실행에 대한 제어권을 탈취하여 시스템을 제어할 수 있다. 공격자는 ROP 공격을 위해 주로 함수의 에필로그(Epilogue)를 사용한다. 그 이유

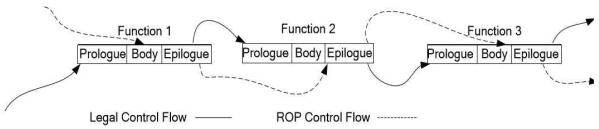


Fig. 1. ROP 공격을 위한 가젯의 제어 흐름 예시.

는 함수 프롤로그(Prologue)의 경우 매개 변수(Parameter) 초기화, 스택 프레임 할당 등 스택 구조를 변경하는 작업으로 인해 공격자가 예상치 못한 제어 흐름이 발생할 수 있기 때문이다. Fig. 1.에서 ROP 공격을 위해 사용하는 가젯 체인의 제어 흐름 이동을 확인할 수 있다.

2.2 제어 흐름 무결성 기법

제어 흐름 무결성 기법은 정적 분석으로 간접 점프가 도달할 수 있는 위치를 결정하여 제어 흐름의 무결성을 보장한다. 대상 프로그램에 대한 정적 분석을 통해 제어 흐름 그래프(Control Flow Graph)를 얻고, 실제 프로그램의 제어 흐름이 제어 흐름 그래프에 맞게 진행되는지 실행 시간에 검사한다[6]. 기존에 제시되었던 제어 흐름 무결성 기법은 실행 시간 검사에 따른 성능 오버헤드가 크다. 따라서 성능 오버헤드를 줄이기 위해 하드웨어 자원을 활용한 기법들이 제안되었다[8][9]. 이 기법들은 인텔 아키텍처에서 지원하는 경량 암호화 지원인 AES-NI[10]을 사용하거나 하드웨어 레벨에서 어셈블리 명령어에 대한 제어 흐름 보호 기법을 적용하였다.

본 논문에서는 임베디드 기기에서 많이 사용되는 프로세서인 ARM 아키텍처에서 제어 흐름을 보호하기 위한 기법을 제안한다.

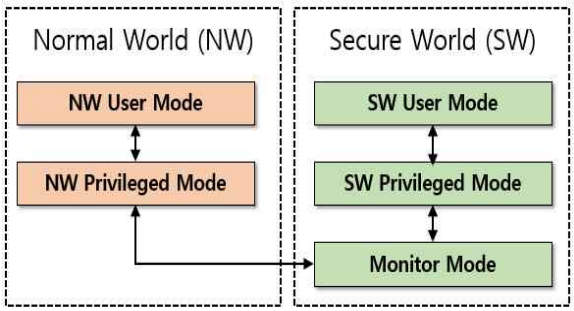


Fig. 2. ARM TrustZone 하드웨어 아키텍처 구성.

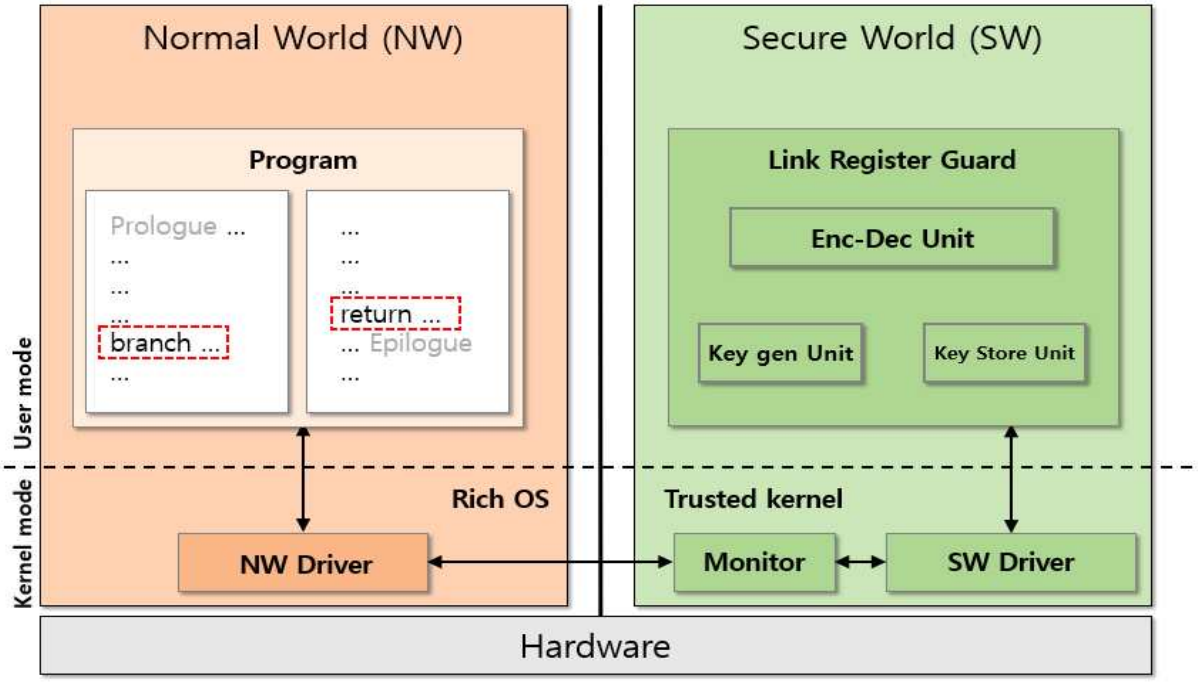


Fig. 3. ARM TrustZone을 활용해 제어 흐름 보호를 위한 LR Guard 설계.

2.3 ARM TrustZone

ARM 아키텍처는 낮은 전력을 사용하도록 설계하여 임베디드 시스템에 주로 사용되는 RISC(Reduced Instruction Set Computer) 프로세서이다. 사물 인터넷의 등장과 각종 보안 위협의 증가에 대응해 ARMv6 프로세서부터 보안을 위한 TrustZone[11]이 추가되었다. TrustZone은 신뢰성과 무결성이 보장되어야 하는 특수 작업에 대하여 안전하고 개별적인 환경을 제공하기 위한 솔루션이다.

TrustZone은 Normal World와 Secure World라 불리는 두 개의 분리된 환경으로 구성된다. 두 환경을 이용하여 일반적인 작업은 Normal World에서 수행하고, 신뢰성과 무결성의 보장이 필요한 애플리케이션의 실행이나 작업은 Secure World에서 수행할 수 있다. 기본적으로 Normal World에서 Secure World의 자원에 직접 접근하지 못하며, Normal World의 특권 모드(Privileged Mode)에서 SMC(secure monitor call) 명령어 호출을 통해서만 Secure World로 진입할 수 있다. Fig. 2.는 ARM TrustZone 하드웨어 아키텍처 구성을 간략하게 보여준다.

III. LR Guard

3.1 공격자 모델

LR Guard는 프로그램 내부의 버퍼 오버플로 취약점을 이용하며, 함수의 에필로그 가젯을 연결해 ROP 공격을 수행하는 공격자 모델을 가정한다. 공격자가 의도한 가젯은 프로그램과 라이브러리 어디에서든 구할 수 있으며, 이를 연결하여 공격자가 원하는 코드를 실행하는 가젯 체인을 구성할 수 있다. 가젯 체인을 이용하여 시스템 제어 혹은 권한 변경을 통한 접근 제어 해제 등을 수행한다.

3.2 LR Guard

ARMv8 아키텍처의 TrustZone을 활용하여 제어 흐름 보호를 적용하는 Link Register Guard를 설계하였다. ROP 공격을 수행하는 공격자에 대한 보호를 위해 프로그램의 프롤로그와 에필로그 시 암호화 및 복호화 작업을 수행한다.

LR Guard는 Secure World 에서 제어 흐름 보호 기능을 수행한다. 안전하게 분리된 영역에서 AES(Advanced Encryption Standard) 암호 프리미티브를 사용하기 위한 대칭키를 생성하

여 안전하게 보관한다. Fig. 3.의 Key gen Unit에서 대칭키를 생성하며, Key Store Unit에서 대칭키를 관리한다. Enc-Dec Unit은 반환 주소에 대한 암호화, 복호화를 담당한다.

프로그램의 프롤로그 이후 서브루틴으로의 분기(Branch)가 발생할 때, Link Register(lr)에 반환 주소가 저장되고, 스택 메모리 공간에 반환 주소를 저장한다. lr 레지스터에 저장된 반환 주소를 스택 메모리 공간에 푸시(Push)할 때 LR Guard의 Enc-Dec Unit으로 반환 주소에 암호화를 적용한다. 또한 서브루틴에서 에필로그가 수행되어 반환할 때 스택 메모리 공간에 저장한 반환 주소를 lr 레지스터로 팝(Pop)하여 기존 영역으로 복귀한다. 이때 LR Guard의 Enc-Dec Unit으로 반환 주소에 복호화를 적용하여 정상적인 반환 주소로 복구한다. 이 과정에서 ROP 공격을 수행하는 공격자가 정당한 복호화가 적용되지 않은 에필로그를 이용하려 할 때, 공격자가 이용하기 위해 덮어 쓴 반환 주소에 복호화가 적용되기 때문에 원하는 제어 흐름으로 이동할 수 없다.

3.3 성능 분석

임베디드 시스템에 구현하는 보안 기능에서 성능 오버헤드는 치명적으로 작용한다. 본 논문에서 제안한 기법은 Normal World과 Secure World 사이의 World 전환 오버헤드와 AES 암호화 및 복호화에 따른 성능 오버헤드를 가진다. LR Guard의 제어 흐름 보호를 위해서 모든 함수의 프롤로그와 에필로그에서 SMC 명령어를 통한 World 전환이 발생한다. World 전환에 따른 오버헤드는 최신 ARM 아키텍처에서 많이 개선되고 있다. Zhichao Hua 등[12]의 연구에서 ARMv7과 ARMv8의 World 전환 수행 시간은 ARMv8이 약 10배 정도 빠른 것을 확인할 수 있었다. 또한, 고성능 AES 암호화 및 복호화를 지원하기 위해 ARMv8 프로세서에 암호 확장(Cryptography Extension)[13]이 추가되었다. AES 암호화 과정의 라운드 연산, 믹스 칼럼(Mix Column) 연산 등을 명령어로 구현하여 빠른 암호화 및 복호화 성능을 제공한다.

IV. 결론

본 논문에서는 ROP 공격을 수행하는 공격자 모델에 대한 제어 흐름 보호 기법을 제안하였다. LR Guard는 ARMv8 아키텍처의 TrustZone을 사용하도록 설계하였다. ARMv8 아키텍처의 고성능 AES 암호화 및 복호화를 이용하여 함수의 간접 분기와 반환에 사용되는 반환 주소를 보호한다. SMC 명령어를 통한 World 전환 오버헤드는 최신 ARM 아키텍처를 사용하더라도 성능에 큰 영향을 끼치는 한계가 있다. 구현 과정에서 성능 오버헤드를 줄이는 방법을 찾아 개선해야 할 것이다.

[참고문헌]

[1] Hexa Research, http://www.abnewswire.com/pressreleases/embedded-system-market-to-witness-a-cagr-of-63-by-2020-hexa-research_124346.html.

[2] P. Kocher, R. Lee, G. McGraw, and A. Raghunathan. “Security as a new dimension in embedded system design,” In ACM/IEEE Design Automation Conference, pp. 753-760, Jun. 2004.

[3] L. Szekeres, M. Payer, T. Weiz, and D. Song. “Sok: Eternal war in memory,” In IEEE Symposium on Security and Privacy, May. 2013.

[4] C. Cowan, C. Pu, D. Maier, H. Hinton, P. Bakke, S. Beattie, A. Grier, P. Wagle, and Q. Zhang, “StackGuard: Automatic Adaptive Detection and Prevention of Buffer-Overflow Attacks,” Proc. 7th USENIX Security Conf., vol. 81, pp. 346-355, Jan. 1998.

[5] S. Andersen and V. Abella, “Data Execution Prevention: Changes to Functionality in Microsoft Windows XP Service Pack 2, Part 3: Memory Protection Technologies,” http://technet.microsoft.com/en-us/library/b

b457155.aspx, 2004.

[6] M. Abadi, M. Budiu, and U.E.J. Ligatti, “Control-Flow Integrity,” In Proceedings o f the ACM Conference on Computer and Communications Security, pp. 340-353, Nov. 2005.

[7] S. Checkoway, L. Davi, A. Dmitrienko, A. R. Sadeghi, H. Shacham, and M. Winand y, “Return-oriented programming without returns,” In 17th ACM CCS, pp. 559-572, Oct. 2010.

[8] A. J. Mashtizadeh, A. Bittau, D. Boneh, a nd D. Mazieres, “CCFI: Cryptographically Enforced Control Flow Integrity,” in Proce edings of the 22nd ACM SIGSAC Confere nce on Computer and Communications Se curity, 2015.

[9] P. Qiu, Y. Lyu, J. Zhang, D. Wang, and G. Qu, “Control Flow Integritybased on Li ghtweight Encryption Architecture,” IEEE Trans. Comput. Des. Integr. Circuits Sys t., pp. 1-1, Aug. 2017.

[10] R. Manley, D. Gregg, “A program genera tor for intel AES-NI instructions,“ in Pro gress in Cryptology - INDOCRYPT 201 0, Vol. 6498 of Lecture Notes in Compute r Science, Springer, pp. 311-327, Dec. 2010.

[11] ARM Inc., “ARM Security Technology B uilding a Secure System using TrustZone Technology,” http://infocenter.arm.com/hel p/index.jsp?topic=/com.arm.doc.prd29genc-0 09492c/index.html, 2009.

[12] Z. Hua, J. Gu, Y. Xia, H. Chen, B. Zang, and H. Guan, “vTZ: Virtualizing ARM tru stzone,” in In Proc. of the 26th USENIX Security Symposium, pp. 541-556 Aug. 2017.

[13] ARMv8 Cryptography Extension, “ARM® Cortex®-A57 MPCore Processor Cryptogr aphy Extension,” 2013.

IoT 기반의 스마트 홈 보안 동향

박정인, 이가연, 윤현경, 염흥열
순천향대학교 정보보호학과

Smart Home For IoT-based Security Trends

Jeong-In Park, Ga-Yeon Lee, Hyeon-Gyeong Yun, Heung-Youl Yum
Department of information security, Suncheonhyang University.

요 약

4차 산업혁명에 접어들면서 스마트 홈은 실생활과 밀접한 가정, 보안기기, 소비장치 등 여러 분야를 통신망으로 연결해 모니터링하고 통제하며 보편적으로 사용되어가고 있다. 지난 5년간 스마트 홈에 이용되는 IoT의 이용자 통계는 147만에 이른다.[1] IoT 사용자가 급증하는 와중에 IoT 취약점 신고 현황은 총 701건에 다다른다.[1] 이처럼 IoT 이용, 선호도는 높아져 가지만 쏟아지는 보안 위협에 대한 대응 방안은 미미한 수준으로 제시되고 있다. 따라서 본 논문은 사생활과 밀접한 연관이 있어 강력한 보안이 필요한 이 시점에 현재까지 발생한 보안 위협 사례를 알아보고 그에 대한 대응 방안을 설명한다.

I. 서론

4차 산업이 산업혁명에 들어서면서 사물에 인터넷을 접목한 사물인터넷(IoT) 디바이스들이 등장하고 있다. 사람들은 스마트 폰에 대한 편리함을 넘어서 집에서도 편의성을 원해 생긴 시스템이 스마트 홈이다. 스마트 홈이란 가정에 필요한 용품들을 IoT 디바이스들로 꾸린 것으로 자동화 시스템, 원격 제어 시스템 등을 제공하는 주거 공간이다.



그림 1. 스마트 홈

출처: 최형욱(커넥팅랩), "미래의 스마트홈, 1인가구에서 꽃 피우다", 2018.02.26.

스마트 홈 환경에서의 대표적인 사물인터넷으로는 IP카메라(가정용 CCTV), 스마트 전구, 스마트 보일러 등이 있다. 1인 가구가 증가하면서 가정에 혼자 있는 반려견을 확인한다거나, 집에 들어가기 전에 보일러를 켜두는 등 네트워크로 연결되어 있어 에너지를 절약하고 삶의 질을 향상시킨다.

이처럼 우리 실생활에 가까운 위치에 있는 스마트 홈은 보안이 뚫렸을 때 가장 위험하기 때문에 스마트 홈의 장점에 대해 마냥 기뻐할 수 없다. 스마트 홈에서 수집되는 데이터는 개인 정보와 사생활에 대한 정보를 포함하고 있어[2] 유출 시 금전적, 물리적, 정신적인 피해가 발생할 수 있다. 또한 [3]에 따르면 스마트 홈은 내부적으로 지능을 갖춰 프로그래밍이 된 알고리즘에 따라 의사결정을 할 수 있고, 홈 게이트웨이나 클라우드 서버 통신을 위해 데이터 기능을 포함할 수 있어 이들 디바이스들이 스스로 알아서 동작하기 때문에 보안 침해가 발생해도 최종 사용자가 이를 파악하고 교정할 방법이 매우 적다고 설명하였다.

스마트 홈 보안 위협 사례로는 국내 IP카메라 1천여 대를 해킹한 사람들이 적발된 사건, 해커들이 중국 업체의 카메라 취약점을 SNS에 공유한 사건 등 해킹으로 인해 많은 사람들의 사생활 침해 사건들이 발생하고 있다. 또한,

2017년 9월 자신의 스마트 홈 도어락 해킹을 통해 무단 침입이 가능할 정도로 심각한 취약점이 발견된 사건이 있다.

이처럼 스마트 홈 환경에서의 다양한 IoT 디바이스들이 다양한 보안 위협에 처해있어 IoT 디바이스 해킹 이슈가 끊이지 않고 발생한다. 본 논문에서는 어떤 위협들이 존재하고 어떻게 대응해야 할 지에 대해 서술하여 사람들에게 위험성을 인식시킨다.

II. 본론

본 논문에서는 스마트홈을 구성하는 IoT 디바이스들의 보안 위협 및 대응 방안을 살펴볼 것이다.

2.1 스마트 홈에서의 IoT

현재 출시 되어있는 스마트홈 IoT 디바이스들의 종류로는 스마트 트래커, 스마트 플러그, 공기 모니터 등 일상에 필요한 기기들이 다양하게 존재한다. 이러한 기기들의 발전은 미래에 기상 시나 출근 후에도 인공지능 음성인식 디바이스로 가전제품들을 관리 할 수 있게 할 것이다. 가정 내에 있는 카메라로 자녀의 안전 유무를 확인하고 귀가 전 보일러를 미리 켜두며, 불 켜고 잠자리에 들었을 때 사용자의 숨소리를 IoT가 인지하여 스스로 불을 끈다. 이처럼 미래에는 IoT가 우리 생활에 없어서는 안 될 부분이 될 것이다.

2.2 취약한 인증시스템 위협 및 대응 방안

도어락, 스마트 전등, 스마트 TV 등의 IoT 디바이스들을 통해 인증된 사용자가 아닌 제3자가 인증된 사용자처럼 제어 권한을 가질 경우 우리의 평범한 일상들이 위협받을 수 있다. 먼저 도어락 및 스마트 전등 제어에 대한 공격 시나리오는 다음과 같다.

첫 번째, 제3자가 인증 시스템이 취약한 네트워크에 접속한다. 두 번째, 해당 네트워크에 연결된 IoT 디바이스들의 제어 권한을 가져온다. 세 번째, 도어락 잠금 해제, 차량 개폐기 열기 등이 가능하다.



그림 2. 취약한 인증시스템 공격 시나리오

아이콘 출처: Freepik, https://www.flaticon.com

이에 대한 최근 사례로 2017년 12월 한 공대생이 자신의 스마트 홈 치명적인 보안 취약점을 찾아냈다. 공대생은 자신의 스마트 홈 보안성에 의구심이 들어 동료 4명과 함께 ('Emohtrams'팀) 점검을 했다. 그 결과 스마트 홈 보안 취약점을 악용하면 공격자가 차를 타고 차량 개폐기를 통과해 주차장 로비 도어, 현관도어락까지 열고 집 안에도 자유자재로 출입할 수 있었다. 그리고 조명조종 기능, 난방조종, 방문자 기록 확인 등 스마트 홈에서 제공하는 모든 서비스들을 제어할 수 있었다.[4]

대응방안으로 인증된 사용자만이 이용 및 제어하기 위해 인증된 사용자인지 확인하고 ID, 비밀번호, IP주소 등 다양한 인증 방법들을 사용한다.[2] 또한 변조할 수 없는 지문이나 홍채 등을 사용하는 인증 방법이 있다.

다음은 [10]을 참고해 초기 설정값이 존재하고 사용자에 의해 설정이 바뀌는 경우에 대한 대응방안이 있다. 먼저 기존 설정이 있는 상태에서 사용자가 스마트 폰으로 기업 서버에게 설정값, 사용자 스마트폰 정보와 랜덤값(이때, 기업에서 제공하는 otp값)을 보낸다. 서버에서 인증된 사용자 정보와 자신이 제공한 랜덤값으로 해시함수 통해 해시값을 만든다. 또한 사용자가 보낸 정보와 랜덤값으로 해시값을 만든다. 두 개의 해시값이 같을 경우 무결성이 인증되어 IoT설정을 사용자가 보낸 설정값으로 바꾼다. 다를 경우 기업에 알리거나 차단하는 등 적절한 대응이 필요하다.

또 다른 대응방안으로는 [7]에서 IP Camera

에 담기는 개인정보를 보호하기 위한 '마스킹 기법' 이라는 대응 방안이 제시된 바 있다. 이는 IP Camera에서 촬영되는 영상이 암호화 되지 않고 영상 그대로 기기에 전달되는 위험성을 보완해 제시된 기법이다. IP Camera에서 개인정보는 Camera에서 촬영되는 개인의 얼굴인데, 이를 보호하기 위해 탐지->추출->마스킹 처리->저장의 단계를 거쳐야 한다고 설명한다. 또한 IP Camera가 촬영한 정보를 실시간으로 보내면 시스템에서 권한이 없는 사용자는 데이터 제어가 불가능하도록 설계해야한다고 설명했다.

2.3 패스워드 위협 및 대응 방안

스마트 홈 기기 중 대표적으로 쓰이고 우리의 실생활과 가장 가까운 IP Camera는 보안 침해가 발생했을 때 큰 피해를 줄 수 있다. 쉽게 피해를 보는 여러 사례들 중 하나는 보안성이 높지 않은 아이디와 비밀번호가 원인인 경우가 많다.

이에 대한 사례로 최근 중국에서 한국 IP Camera를 해킹하는 자동화 도구가 대량 유포되었는데, 사용자가 비밀번호를 설정하지 않거나 알기 쉬운 비밀번호를 사용해 보안에 더더욱 취약했다. 또한, 이와 비슷한 사례로 [5]에서 전 세계 약 73000대의 IP Camera가 해킹당해 '인세캠(Insecam)'이라는 사이트를 통해 생중계된 사건이 있다.

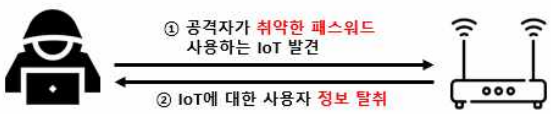


그림 3. 취약한 패스워드 공격 시나리오

아이콘 출처: Freepik, https://www.flaticon.com

공격자는 초기 비밀번호를 바꾸지 않고 사용하는 IP Camera들을 노려 공격했고, 사이트에 공개된 장소들은 지극히 사적인 가정집, 공연장, 사무실 등이었다. 이들 대부분의 아이디는 admin, 비밀번호는 12345 또는 admin이었다. '인세캠(Insecam)' 운영자는 보안 설정의 중요성을 환기시키기 위해 사이트를 제작했다고 설명했다.

이와 같은 보안 침해 사례들의 대응 방안으로 KISA[2]에서는 보안성 높은 비밀번호 사용하고, ID와 비밀번호 주기적 변경 및 소프트웨어를 최신 버전으로 업데이트할 것을 권고한다.

2.4 외산 IP Camera 보안 위협 및 대응방안

NSHC Red Alert, KAIST 시스템 보안 연구실은 [6]에서 저렴한 가격에 유통되고 있는 외산 IP camera와 CCTV에 대한 보안 위협과 문제점을 설명하였다. 최근 급격하게 확산되고 있는 일부 제품군에서 Hidden Backdoor를 확인했으며, 중국 제조사의 클라우드 서버에서만 접근할 수 있다고 설명한다. [6]에서는 백도어(Backdoor)를 통해 기기가 촬영 중인 영상을 원격으로 보고 제어할 수 있으며, 내부망 접근을 통해 내부망 시스템을 대상으로 2차 공격까지 가능하다고 설명한다. 이에 NSHC Red Alert, KAIST 시스템 보안 연구실은 [6]에서 대응 지원 전담 부서 투입, 클라우드 서비스 IP 접근 차단 및 통제, 검증되지 않은 장비 회수 및 사용 금지, 사내에 보안이 검증된 사용기기 외에 설치 불가 등의 대응 방안을 제시했다.

2.5 Malware 공격 및 대응방안

IoT 보안의 문제점은 공격에 활용된 IoT 디바이스 자체에는 아무런 이상이 발견되지 않고, 사용자들이 불편을 느끼지 못하기 때문에 자신의 IoT가 악성코드에 감염이 되었는지 인식하지 못하는 점이다. 이러한 현상을 유발하는 Mirai malware 공격이 있다.

Mirai malware는 네트워크에서 취약한 IoT 디바이스를 찾아 그에 대한 정보를 C&C로 보낸다. 정보를 통해 IoT 디바이스를 감염시켜 자신의 숙주로 만들고, 목표 대상물을 공격하면서 주변에 감염되지 않은 다른 IoT 디바이스들을 감염시킨다. 이처럼 빠르게 감염을 확산시키면서도 여러 곳에서 공격을 하는 Mirai malware를 방어하기가 쉽지 않다. 이러한 Mirai 봇넷을 통해 피해를 본 사례로 2016년 10월, 주요 도메인 네임 시스템(DNS) 제공업체인 DYN을 대상

으로 한 DDoS 사건이 있다. DNS는 브라우저가 요청한 콘텐츠를 전달할 수 있도록 올바른 서버를 찾아 연결에 필요한 IP주소로 변환시키는 서비스이다. 이 서비스를 제공해주는 DYN은 서버에 DDoS 공격을 받아, 사용자들이 이용하는 데 불편함을 겪었다. 또한, DNS 서버를 통해 라우팅 되어 있는 모든 사용자의 전체 네트워크망이 공격받았다. 공격자는 많은 IoT 디바이스들의 알려진 취약점과 출고 당시 기본 패스워드를 사용한 점을 이용해 악성코드를 감염시켜 공격에 이용했다. [7]

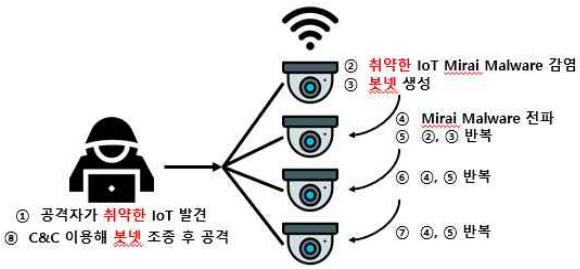


그림 4. Mirai Malware 공격 시나리오

아이콘 출처: Freepik and Pixel perfect, https://www.flaticon.com

제조사들이 기본적인 보안 장치들만 설치해 준다면 malware의 공격을 막는 것이 가능하다. 디폴트 비밀번호를 어렵게 설정해놓거나, 사용자가 설정하도록 만들어야 한다. 또한 업데이트가 용이하게 되도록 설계해 나중에 문제가 발생했을 때 조치를 취할 수 있도록 해야 한다.[8]

III. 결론

현재까지도 스마트 홈은 우리 실생활에 편리함을 제공하고 있고, 여러 가지 디자인으로 거부감 없이 스며들고 있다. 하지만 이러한 스마트 홈은 보안 위협을 당했을 때 가장 큰 피해를 입히고 금전적, 물리적, 정신적인 피해가 발생할 수 있다. 스마트 홈은 여러 가지 기기가 존재하는 만큼 다양한 방법으로 침투될 수 있다. 이에 본 논문에서는 스마트 홈 다양한 공격 사례들 중 제어기기와 IP Camera의 공격 사례 및 대응 방안을 설명하며 보안에 대한 인식을 향상시킨다.

향후 가정에서나 공공기관에서 사용이 보편화 될 스마트 홈은 네트워크 침투, DDoS공격 등 수많은 보안 위협을 겪고 있다. 이러한 보안 위협들에 대응할 수 있는 방안을 찾고 연구해야 하는 것이 앞으로의 과제로 남아있다.

[참고문헌]

[1] 김태진, “IoT 보안 비상...3년간 신고 700여 건”, ZDNet Korea, 2017.09.22.

[2] 한국인터넷진흥원(KISA), 사물인터넷 소형 스마트 홈·가전 보안 가이드[이용자용], 2016.12.

[3] Tang Yiming, Eric Seow, Sarah Woo, 인피니언 테크놀로지스, “스마트 홈 환경에서 매우 중요한 보안 문제 ”, 전자과학 , 2017.12.06.

[4] 길민권, “[긴급] 아파트 스마트홈에 심각한 취약점 발견...수십만 입주민 위험에 노출”, 데일리시큐, 2017.12.13.

[5] 유재연, “전세계 CCTV 7만3000개 뚫렸다” , 중앙일보 , 2014.11.08.

[6] NSHC Red Alert, KAIST 시스템 보안 연구실, 외산 CCTV 및 IP-Camera의 긴급 보안 위협 보고서, 2015

[7] 유성경, “미라이 봇넷, IoT의 DDoS 공격”, GRAYWNEWS, 2017.02.01.

[8] 문가용, “IP 카메라의 위기 : 네 가지 멀웨어가 경쟁한다”, 보안뉴스, 2017.06.09.

[9] 황기진, 박재표, 양승민, 지능형 IP 카메라를 이용한 CCTV 시스템에서의 실시간 개인 영상정보 보호, 2016

[10] IoT보안얼라이언스, 홈·가전 IoT 보안가이드 p106-p109, 2017.07.

A5 관리정책교육 1

김 태 희 (동신대학교)

- **악성코드 감염 예방을 위한 보안정책 수립사례 분석**
  이준희
- **4차 산업혁명 환경에서 Trust Service 제공을 위한 사회과학적 정보보호 기반조성 연구**
  박상호, 나원철, 장항배
- **VR과 IoT를 활용한 전공탐색 기반의 대학 홍보전략**
  최경호, 김병석, 전영재, 진용기, 이동휘

악성코드 감염예방을 위한 보안정책 수립사례 분석

이준희*

*고려대학교 정보보호학과

Jun-Hee Lee*

*Division of information security, Korea University.

요 약

오늘날 전 세계적으로 급증하는 악성코드 공격으로 인해 많은 기업의 정보자산 피해가 지속적으로 증가하고 있다. 하지만 사용자 PC의 악성코드 감염은 다양한 경로로 발생하기 때문에 보안부서의 기술적 대책과 통제만으로는 완벽하게 감염을 예방할 수 없다. 따라서, 기업은 관리적인 측면에서 직원 개인별 보안인식에 대한 접근이 필요하다. 이에 따라 본 연구에서는 다양한 정보보호 정책준수에 관한 이론 중 억제이론에 바탕을 두고, 기업의 적절한 보안정책 수립사례 분석을 통해 악성코드 감염예방의 실효성을 분석한다.

I. 서론

1.1 연구배경 및 필요성

오늘날 IT기술은 비약적 발전을 통해 많은 기업들에게 생산성 향상과 혁신적인 비즈니스 변화를 가져왔으나 그와 더불어 DDoS 공격, APT 공격, 웹 취약점 공격 등 다양한 해킹기법이 끊임없이 진화를 거듭하며 보안환경을 위협하고 있다. 이러한 변화는 단지 개인과 기업에 한정될 뿐만 아니라 국가 간 분쟁까지 영향을 미칠 수 있는 공격으로 확장되고 있다[1].

이에 따라 각 기업은 악성코드 감염을 통한 정보유출, 사이버 침해 등을 방지하기 위하여 다양한 정보보호시스템을 도입하고 운영하며 대응하고 있으나, 사용자 PC의 악성코드 감염은 전자메일, 외부저장매체, P2P, S/W 취약점 공격, APT 등 다양한 경로로 이뤄지기 때문에 기술적 대책만으로는 악성코드 감염을 완전히 예방할 수 없는 것이 현실이다. 따라서 기업의 보안 업무 담당자는 정보보안 교육, 적절한 보안정책 수립 등 관리적 방안을 통해 임직원의 보안에 대한 관심과 인식을 높여 개개인이 악성코드 감염에 대한 주의를 기울이게 함으로써 기술적 대책의 부족한 점을 상호 보완할 필요가 있다. 이때 보안부서에서는 악성코드 감염 예방을 위한 보안정책을 수립 시, 어떻게 정책을 수립하고 집행해야 직원들의 보안으로 인한 스트레스를 줄이면서 어느 정도의 강제성을 부과해야 실효성이 있을지 고민하게 된다.

따라서 이번 연구에서는 정책수립 시 참고할 만한 선행연구를 소개하고 실제 사례 분석을 통해 악성코드 예방과 관련된 적절한 보안정책 수립방안 가설을 검증함으로써, 향후 많은 기업의 악성코드 감염 예방을 위한 관리적 보안정책 수립에 도움이 되고자 한다.

1.2 연구목적 및 방법

본 연구의 세부목적을 순서대로 나열하면 가장 먼저 (1) '기업의 악성코드 감염 예방'을 들 수 있다. 이어서 예방을 위한 관리적 대책으로 범위를 좁혀 (2) '적절한 보안정책 수립'이 필요하며, 수립된 정책을 직원들이 준수할 수 있도록 (3) '효과적인 정책 준수방안'을 연구함으로써, 최종적으로 (4) '악성코드 감염예방을 통한 기업의 보안 수준 향상'을 그 목적으로 한다.

그동안 관리적 대책분야에서 보안정책 준수의도 및 동기유발 요인에 대한 연구는 오래전부터 국내외에서 꾸준히 진행되어 왔으나, 대부분의 연구들은 신뢰성이 있는 타당한 가설을 수립하고 검증하는 단계까지의 이론적 한계를 나타냈다. 따라서 본 연구는 기존 연구와는 다르게 한 단계 더 나아가, 실제 보안정책을 적용한 기업의 데이터를 수집하여 현상을 기반으로, 기존에 연구되었던 가설을 검증하고 학문적 이론을 어떻게 적용할 수 있을지 확인한다는 점에서 차이가 있다.

II. 이론적 배경

2.1 악성코드 공격 동향

악성코드란 컴퓨터나 시스템에 심어져 기계를 장악하여 공격자가 원하는 행동을 수행하는 유해 프로그램을 뜻한다[2]. 초창기 악성코드는 대부분 단순 바이러스를 의미했으며, 주로 불법적인 소프트웨어를 통해 확산이 이루어졌기에 피해범위나 확산성이 높지 않았다. 하지만 인터넷이 발전하고 대중화 되면서 공격과 피해범위가 다양해지고 대응하기 어려워졌으며 확산성이 높아지게 되었다. 이에 따라 백신, 침입탐지 시스템 등 여러 정보보호시스템이 개발되었으나 창과 방패처럼 악성코드 역시 기술적 발전을 거듭하면서 진화해 왔다.

2017년의 국내 사이버 공격 동향을 살펴보면 국가 간 정치적 갈등 상황이 심화되며 디도스 공격, APT 공격 등으로 사이버 위협이 고조된 한해였다. 또한 전 세계적으로 금전적 이득을 노린 사이버 범죄가 증가하였으며, 랜섬웨어라는 신종 악성코드가 기승을 부린 한해라고 할 수 있다. 랜섬웨어는 몸값(Ransom)과 소프트웨어(Software)의 합성어로, 이용자의 시스템을 잠그거나 데이터를 암호화해 사용할 수 없도록 하고 이를 인질삼아 금전을 요구하는 악성 프로그램을 말하는데, 가상화폐의 등장과 맞물려 폭발적인 증가를 하여 일반인, 공공기관 할 것 없이 피해를 입혔다. 실제로 특정 국가에서는 조직적인 해커들을 구성해 랜섬웨어 공격을 통해 국가 자금 마련을 하는 사례도 있었다[3,4].

2017년 국내 악성코드 유포지 탐지현황은 다음과 같다. 악성코드 유포지는 전년 동기 대비 460건에서 763건으로 66%나 증가하였으며, 악성코드의 유형별 비율은 랜섬웨어가 28.3%의 비율로 가장 높았으며, 그 이외에도 금융정보 유출, 다운로더, 드롭퍼, 비트코인, 백도어 순으로 악성코드 유형이 다양하게 나타났다[5].

한국인터넷진흥원의 '2017년 4분기 사이버 위협 동향 보고서'를 살펴보면 아래와 같이, 지속적으로 악성코드의 종류가 다양해지고, 탐지 건수가 증가하고 있음을 알 수 있다.

[표 1] 2017년 국내 악성코드 유형통계

	악성코드 종류	1분기	2분기	3분기	4분기
1	랜섬웨어	275	255	347	463
2	정보탈취	80	130	44	82
3	원격제어	224	38	8	25
4	애드웨어	2	13	0	0
5	파밍	38	0	31	21
6	DDoS	8	0	0	0
7	다운로더	0	0	14	2
8	인젝터	0	0	8	4
9	기타	0	0	0	46
	합계	627	436	452	643

2.2 억제이론(Deterrence Theory)

이 파트에서는 사용자의 보안정책 준수를 위한 다양한 정보보호정책 준수에 관한 이론 중 억제이론에 대해서 소개한다.

억제이론 또는 합리적 선택이론의 핵심은 범죄를 행한 결과로서 따르는 처벌의 위협이 사람들로 하여금 범죄를 짓지 않게 하는 효과를 지니게 되는 것이며, 범죄에 대한 확실하고(certain) 엄격한(severe) 처벌은 개인에게 범죄를 저지르지 않도록 하는 억제효과가 있다는 이론으로, 이를 적용하여 적절한 제재가 직원들로 하여금 기업의 보안정책을 준수하는데 긍정적 영향을 미칠 수 있다는 기반 이론이다[6].

지금까지 일반 억제이론을 IT사례에 적용한 연구는 국내·외로 다양하게 진행되어 왔다. Straub(1990)는 처벌과 개인의 보안정책 미수행에 대한 연관성 연구를 수행하였으며, Siponen & Vance(2010)의 억제이론을 기반으로 사용자 중화기술이론과 제제의 효과 연구, Bulgurcu et al.(2010)의 합리적 선택이론에 근거한 비용과 보상 연구 등 지속적으로 연구되어왔으나[7,8,9], 그동안의 조직 행동모델 연구 결과가 항상 일관성 있지는 않았다는 한계점이 있다[10].

2.3 선행연구 및 가설수립

위의 억제이론을 바탕으로 정책의 강제성과 준수효과에 대한 가설수립을 위해, 선행연구 중 연관성 있는 결과를 몇 가지 살펴보기로 한다.

첫째로 Xue et al.(2011)는 조직이 처벌 정책을 효과적으로 만들고 싶다면 정책이 분배적이고 절차적이고 정보적 정의를 상징해야 한다고 말했다. 또한 조직에서 조직원이 준수 행동 미수행에 대한 처벌을 실제로 공정하게 수행할 경우, 공정한 처벌에 대한 신뢰감이 생기고, 처벌 정의에 대한 인식으로 인해 조직원들의 IT 정책 준수의도를 지속적으로 유지시킬 수 있다고 주장 하였다[11,12].

마찬가지로, Hwang & Lee(2016)는 보안 정책 실행 방법인 제재가 개인의 효능감에 긍정적인 영향을 미친다는 사실과, 엄격하고 공정한 조직의 보안에 대한 제재는 조직원이 조직의 보안정책 준수를 위한 효능감을 높일 수 있음을 증명하였다[12].

다음으로, Kim & Song(2011)은 내부조직원의 관점에서 외·내부적 동기요인이 조직원의 준수행동에 영향을 미치며, 그중 외적 동기요인(강압적 요인)인 패널티 강도, 보안위반 적발도, 규범적 신념 역시 정보보안 정책 준수의도에 긍정적 영향을 줄 수 있음을 검증하였다[13].

마지막으로 Park et al.(2017)은 억제지향성과 정보보안 준수혜택과의 관계 분석을 통해, 억제지향성 인지가 높을수록 정보보안 준수 혜택이 증가함을 나타냈으며, 억제지향적 정보보호 정책수단에 대한 사용자 인지가 높으면 준수로 인한 긍정적 신념이 강화되고 결국 준수의도의 제고로 이어짐을 검증했다[14].

위의 공통된 결과들을 종합해보면, '보안정책의 공정한 제재는 개인의 인지에 영향을 미쳐 결국 조직원의 보안준수 의도를 높일 수 있다'라고 축약할 수 있다. 이는 다시 말하면, 기업에서 직원들의 보안정책 준수를 위해서 보안정책을 수립한 뒤, 공정한 처벌 등 외적 제재를 가하면 직원들이 정책을 더 잘 따를 것 이라고 기대해 볼 수 있다는 것이다.

이번 연구의 실제 사례에서는 수립한 보안정책의 제재수단으로 인사 징계가 아닌 직원들로 하여금 처벌 관련 정보를 정확하게 제공받고 지속적인 모니터링을 할 수 있도록 '부서평가'라는 간접제재 방안을 채택하였으며, 이런 정책을 통해 기업의 악성코드 감염률이 감소할 것이라고 기대하였다.

이를 위한 본 연구의 가설은 다음과 같다.

○ 가설 : 부서별로 직원들의 악성코드 감염 건수를 부서평가에 반영할 경우, 기업 내 전체 악성코드 감염률은 감소할 것이다.

III. 결과분석

3.1 수집대상 및 특성

분석을 위한 자료는 공공기관 A사의 3년간의 업무망(망 분리 기관) 내 악성코드 감염건수 일체를 수집하였다. A사는 악성코드 감염률을 줄이기 위한 노력으로 2016년부터 각 부서원의 업무망 악성코드 감염실적을 부서 평가에 반영하였고, 매 분기마다 전사 악성코드 감염현황 공지를 통해 직원들에게 주의 및 개선을 독려하였다. 상세 평가지표는 아래와 같다.

○ 평가방안 : 부서 내 조직원의 악성코드 감염건수가 이전 분기대비 감소 시, 공로를 인정하여 횟수별 평가점수를 부서평가에 반영

[표 2] 내부평가 반영방법 (예)

이전 분기 대비 악성코드 감소 회수	평가 점수
4 회	100 점
3 회	75 점
2 회	50 점
1 회	25 점
0 회	0 점

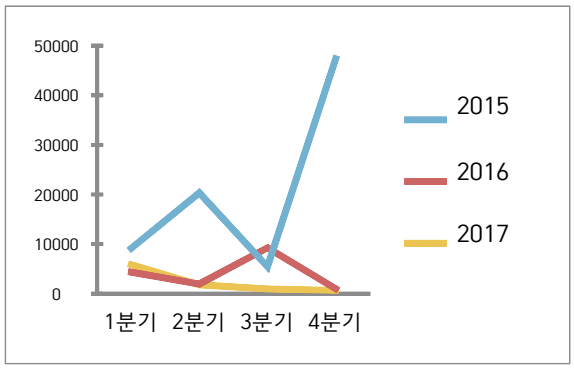
3.2 분석결과

정확한 비교분석을 위해 정책을 반영하기 1년 전의 데이터부터, 평가를 적용한 이후의 2년간 총 악성코드 감염 건수를 수집하였다.

[표 3] 악성코드 감염 결과 (단위 : 건)

구분	2015년	2016년	2017년
1분기	9,152	4,352	5,894
2분기	20,330	1,971	1,786
3분기	5,472	9,254	953
4분기	47,343	1,006	692
합계	**82,297**	**16,583**	**9,325**
비고	평가 미반영	평가 반영	

시각적 비교를 쉽게하기 위해 그래프로 나타낼 경우 아래의 그림과 같다.



[그림 1] 연도별 악성코드 감염 그래프

악성코드 감염률 감소효과를 측정하기 위해 월평균 악성코드 감소율을 계산해보면 아래의 표와 같다.

[표 4] 연도별 감소율 (단위 : 건)

구분	총 합계	월 평균	전년대비 감소율
2015년	82,297	6,858	-
2016년	16,583	1,381	**약 80% 감소**
2017년	9,325	777	**약 40% 감소**

위의 결과를 살펴보면 이 연구에서 다루지 못한 악성코드 감염과 관련된 수많은 변수들이 있음에도 불구하고, 단순히 수집된 데이터의 감염건수 숫자 비교만으로도 악성코드 감염률이 눈에 띄게 감소한 것을 알 수 있다.

특히, 처음 평가를 반영한 해에는 월평균 악성코드 감염률이 정책이 적용되기 전과 대비하여 80%나 대폭 감소했음을 알 수 있다. 이는 악성코드 감염방지를 위한 정보보호시스템 등 기술적 환경이라는 변수는 고정되어 있었음에도 적절한 통제를 통한 개개인들의 노력과 관심, 즉 관리적 방안으로 악성코드 감염 예방에 어느 정도 효과를 나타낼 수 있음을 나타낸다.

따라서 올바른 보안정책을 수립하고 적절한 제재를 통해 강제성을 갖춘다면, 기업의 악성코드 감염예방과 정보보호 수준 향상에 도움이 될 수 있음을 확인하였다.

IV. 결론

본 연구는 기업의 악성코드 감염 예방을 위해 어떻게 보안정책을 수립해야 하는가에 대한 질문에서 시작하였다. 먼저 보안정책에 대해 조직원의 준수의도를 높이기 위한 선행이론을 살펴보았고, 그 중 억제이론을 바탕으로 수립한 가설과 실제 데이터와의 비교를 통해 신뢰성을 검증하였다.

물론 이 연구에서 미처 다루지 못했던 수많은 이론과 변수들이 있으며 한계는 존재한다. 특히 '16년도 3분기 데이터를 보면 알 수 있듯이 악성코드 탐지건수라는 것은 사용자의 노력이나 의지와는 무관하게 탐지패턴 업데이트로 인해 비정상적으로 오탐이 늘어나는 사례도 발생하며, 또한 단순히 감염건수가 줄었다고 보안수준이 향상했다고 단언 할 수는 결코 없다. 하지만 이번 연구는 정책을 통한 기업의 악성코드 감염예방 이라는 초기 목적에서는 의미 있는 데이터 분석이라고 할 수 있다.

본 연구가 제시하는 결과는 기업의 보안 인력에 이론적, 실무적 시사점을 가진다. 아무리 많은 비용을 투자하고, 전문 인력을 확보하고, 최신의 정보보호시스템을 도입하여 운영한다 하더라도, 기업 내 직원들이 다 함께 노력하지 않으면 기업의 말단 시스템인 사용자 PC의 악성코드 감염조차 해결하기 어렵다는 점이다.

향후 효과적인 정보보호 정책을 수립하기 위해 많은 보안업무 담당자들이 고민하고 지금처럼 지속적으로 많은 연구들이 이뤄진다면, 악성코드 감염예방 뿐만 아니라 기업의 전체 정보보호 수준을 높일 수 있는 정책수립에 커다란 도움이 될 것이라 기대한다.

[참고문헌]

[1] 1Q Cyber Threat Trend Report, KISA, April, 2018.

[2] E Skoudis, L Zeltser, Malware: Fighting malicious code, Prentice Hall, p.2, 2003.

[3] 2018 national information security report, NIS & government, 2018.

[4] http://www.etnews.com/20180205000384

[5] malicious code hiding site detection trend report, Ministry of Science and ICT & KISA, 2017.

[6] S.J. Yeon, "the deterrent effect of punishment on Crime", Korea Criminal Policy Institute, 11-155, 2003.

[7] D.W. Straub, Effective IS Security : An Empirical Study, Information Systems Research, 255-276, September, 1990.

[8] M. Siponen, and A. Vance, Neutralization: New insight into the problem of employee information systems security policy violation. MIS Quarterly, 34, 487 - 502, September, 2010.

[9] B. Bulgurcu, H. Cavusoglu, I. Benbasat, Information security policy compliance: An empirical study on rationality-based beliefs and information security awareness. MIS Quarterly, 34, 523 - 548, September, 2010.

[10] K.H. Guo, Y. Yuan, N.P. Archer, and C. E.Connelly, Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model, Journal of Management Information Systems, Vol. 28, No. 2, 203-236, December, 2014.

[11] Y. Xue, H. Liang, and L. Wu, Punishment, Justice, and Compliance in Mandatory IT Settings, Information Systems Research, Vol. 22, No. 2, 400-414, February, 2011.

[12] I.H. Hwang, H.Y.g Lee, The Employee's Information Security Policy Compliance Intention : Theory of Planned Behavior, Goal Setting Theory, and Deterrence Theory Applied, Journal of Digital Convergence, 14(7), 155-166, 2016.

[13] S.H. Kim, Y.M. Song, An Empirical Study on Motivational Factors Influencing Information Security Policy Compliance and Security Behavior of End-Users (Employees) in Organizations, The e-Business Studies 12(3), 327-349, September, 2011.

[14] Jong Won Park, Hyun Jong Woo, Hyun Gyu Kim "Relationship between Information Security Policy Orientation and Information Security Compliance Intention : within Classified Information Management Context", Korean Review of Corporation Management 8(1), 285-315, February, 2017.

4차 산업혁명 환경에서 Trust Service 제공을 위한 사회과학적 정보보호 기반조성 연구

박상호*, 나원철**, 장항배***

*,**중앙대학교 일반대학원 융합보안학과

***중앙대학교 경영경제대학 산업보안학과

A Study on the Foundational Composition of Social Science Information Security for Providing Trust Service in the 4th Industrial Revolution Environment

Sangho Park*, Onechul Na**, Hangbae Chang***

*,**Department of Security Convergence, Chung-Ang University.

***Department of Industrial Security, Chung-Ang University

요 약

4차 산업혁명 출현에 따른 보호대상 다양화로 대규모 보안사고 발생이 증가하고 있다. 최근 발생하는 보안사고는 사회공학 기법의 외부 사이버 공격과 내부 구성원(전·현직 직원)에 의한 정보유출이 주를 이루고 있다. 특히 4차 산업혁명 시대는 모든 사물에 정보처리 및 통신기능이 부여되어 초연결성 및 초지능화의 특성을 통해 산업 전반의 패러다임을 급변시키고 보안위험 또한 변화될 것으로 예상된다. 따라서 본 연구는 선제적으로 대응해야 할 새로운 위험요소의 파악과 이를 최소화하는 다차원적 정보보호 산업 대응전략에 대해 연구하고자 한다. 세부적으로 먼저 4차 산업혁명 시대의 새로운 기술적·사회적 변화요소 특성을 예측함으로써, 이를 토대로 예상 가능한 자율적 서비스 시나리오를 설계하고자 한다. 다음으로 설계된 시나리오 전개에 따른 다차원적 보안 위협 및 취약점 등을 분석하고 이에 대한 사회과학적 측면 대응방안(경영관리, 범죄심리, 경제성)을 수립하고자 한다.

I. 연구배경 및 필요성

4차 산업혁명 출현에 따른 보호대상 다양화로 인하여 대규모 보안사고(외부 사이버 공격, 내부 정보유출 등) 발생이 증가하고 있다. 국내 랜섬웨어 감염 피해 수는 2016년 15만 건으로, 2015년 5만3천 건 대비 9만7천 건(35.3%)이 증가하였으며, 2016년 랜섬웨어 피해 추정금액은 약 3,000억 원으로 조사되었다[1]. 아울러 디지털화된 중요정보(기술문서, 공학 설계도면, 개인정보 등)가 유출된 사고건수도 2013년 49건에서 2014년 63건으로 증가하였으며, 2014년 기술유출 피해업체의 예상 피해액은 50조 원에 이른다[2].

본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2018-2014-1-00636)

특히 2017년 5월 12일, '워너크라이 랜섬웨어' 대규모 공격으로 전 세계 20만대 이상의 컴퓨터가 감염되었으며, 이 랜섬웨어의 가장 큰 특징은 웜 바이러스와 유사하게 네트워크를 통해 감염되기 때문에 인터넷에 연결되어 있기만 해도 감염될 가능성이 있다는 점이다[1].

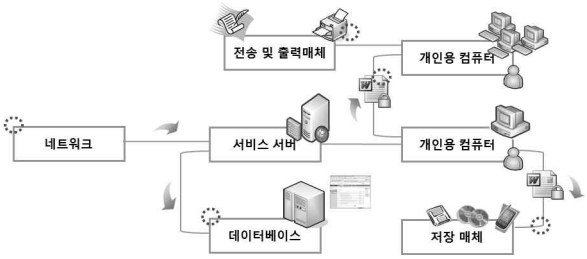
최근에 발생하고 있는 사이버 보안사고(외부 사이버 공격)의 특징은 보안사고 발생경로가 다양해지고 이에 따른 전파속도도 빠르게 증가하며, 최근 이슈 및 사용자들 사이에 신뢰관계 등을 악용하는 사회공학(Social Engineering) 기법이 증가하고 있는 추세이다. 또한 짧은 시간에 대량의 시스템 감염을 위하여 다양한 경로가 악성코드 유포에 활용되고 있으며, 전 세계가 네트워크로 연결되고 통신 속도가 급격히 증가하면서 악성코드는 물리적 매체를 통해 실시간

으로 전파되고 있다. 나아가 각종 사회적 이슈(일본 후쿠시마 원전사고, 스티브 잡스, 김정일 사망 등)와 관련된 제목과 내용으로 악성코드를 첨부하여 전자메일을 발송하거나, Social Network Service(Facebook, Twitter 등), 검색엔진 최적화 등을 통해 악성코드를 유포하는 사회공학적인 전파가 진행되고 있다[3].

<표 2> 보안사고 발생에 따른 피해 확산속도

악성코드 발생년도	악성코드 전파시간
1986년, Brain 바이러스(컴퓨터 시동 섹터를 감염)	3년 (미국→한국)
1998년, 'CIH' 바이러스(컴퓨터 시동섹터 감염)	1개월 (대만→한국)
2003년, 'Slammer' 웜 (특정 시스템을 악의적으로 공격)	수십 분 (전 세계 인터넷 망 마비)
2011년, 'Distributed' 서비스 거부공격 (여러 대의 공격자가 특정 시스템을 악의적으로 공격)	수 분 (국내 정부, 공공기관 마비)
2017년, 'WannaCrypt' 랜섬웨어(윈도우 시스템 감염시킨 후 비트코인 요구)	찰나의 순간(인터넷 접속하는 순간 감염, 전세계 기준 사상 최대 피해)

아울러 사이버 보안사고와 함께 내부 정보유출 사고도 심각한 사회적 문제가 되고 있는데, 이는 주로 첨단기술을 대상으로 내부 구성원(전·현직 직원)에 의해 계획적으로 시도되고 있으며, 과거 단순 생계형 정보유출 사건에서 보다 더 대형화, 조직화된 형태로 변모하고 있다[4]. 내부 정보유출 사고는 해당기술을 잘 알고 있는 첨단기술 개발참여자가 별다른 죄의식(개발된 기술에 대한 개인적 소유의식) 없이 전자메일이나 이동 저장장치 등을 활용하여, 무단 보관, 내부공모, 매수, 공동연구, 위장 합작 등의 방법으로 발생하고 있다. 또한 국가와 기업 경쟁력 강화를 위하여 상대적 우위에 있는 첨단기술을 확보하기 위해, 유출대상이 '시설, 장비, 제품 등에 대한 정보'에서 '산업기술 인력과 기술자체를 확보를 위한 정보'의 수집으로 이동하고 있으며, 유출방식은 문서 등과 같은 단편적 수단에서 대용량 소형 이동식 기기 등을 통한 최첨단 기법으로 전환되고 있다[4]. 따라서 내부 정보유출 사고의 경우 증거확보와 추적이 곤란하고, 피해사실을 인지하기 어려운 경우가 많다.



<그림 1> 정보흐름 관점 정보유출 경로분석

II. 4차 산업혁명 환경 보안문제

최근 사회는 모든 사물에 정보처리 및 통신 기능을 부여함으로써, 사람의 개입 없이 자율적 서비스가 제공되어 자동화와 연결성이 극대화되는 제 4차 산업혁명 시대에 진입하고 있다. 제 4차 산업혁명은 '초연결성(Hyper-Connected)', '초지능화(Hyper-Intelligent)의 특성을 가지고 있고, 이를 통해 모든 것이 상호 연결되고 보다 지능화된 사회로 변화하여 향후 10년간 산업 전반의 패러다임을 급변시킬 것으로 예상된다. 제 4차 산업혁명 기반의 사물인터넷(IoT), 클라우드 등 정보통신기술(ICT)의 급진적 발전과 확산은 인간과 인간, 인간과 사물, 사물과 사물 간의 연결성을 기하급수적으로 확대시키고 있고, 이를 통해 '초연결성'이 강화되고 있다. 2020년까지 인터넷 플랫폼 가입자가 30억 명에 이를 것이고 500억 개의 스마트 디바이스로 인해 상호간 네트워킹이 강화될 것이라는 전망은 초연결 사회로의 진입을 암시하고 있다. 또한 4차 산업혁명은 인공지능(AI)과 빅데이터의 연계 및 융합으로 인해 기술 및 산업구조가 '초지능화' 될 수 있음을 보여준다. 2016년 3월 인간 '이세돌'과 인공지능 컴퓨터 '알파고(Alphago)'와의 바둑 대결은 '초지능화' 사회의 시작을 알리는 단초가 되었고, 많은 사람들이 인공지능과 미래사회 변화에 대해 관심을 갖기 시작했다[5].

이에 따라 보안위험에도 변화가 생기기 시작하였다. 4차 산업혁명 시대의 핵심기반기술인 사물인터넷(IoT) 기술을 바탕으로 똑똑한 사물들 사이의 동조화(conformity) 상호작용을 통하여 현실세계(Physical World)과 가상세계(Electronic World)에 존재하는 다양한 정보들이 시·공간적인 제한 없이 수집되고 침해될 수 있다. 이는 드러난 컴퓨팅에 의해 한정된 공간에서 일정한 명령행위에 의한 개인 행적을 어느 정도 분산·디지털화 하는 현재의 컴퓨팅 환경과는 달리, 숨겨진 컴퓨팅에 의해 일정한 명령행위 없이 언제 어디서나 개인의 행적을 집약적·전자적 기록으로 남기는 컴퓨팅 환경으로 변화를 의미한다[6]. 4차 산업혁명 환경으로 진화하는 선행적 환경 의미의 “Cloud Service” 환경 및 “Big Data” 환경에서도 새로운 보안 취약점들이 발생하고 있다. 의료, 항공, 섬유, 건설 등의 기존의 산업들은 ICT 융합을 통해 지능성·내재성·연결성 등을 갖게 됨에 따라 새로운 형태의 제품과 서비스가 창출되었지만, 그에 따른 새로운 융합보안 위험이 나타났다. 또한 4차 산업혁명의 등장으로 인한 융합보안 사고 사례가 증가하고 있으며, 다차원적인 공격 시나리오들(관리적인 취약점을 틈탄 물리적·기술적인 정보유출 행위)이 발견되고 있다[7].

하지만 이러한 위험에 선제적으로 대응하기 위한 국내 보안 산업 시장규모는 2016년 기준 약 75억 달러로 전 세계 시장 3.9% 수준의 미약한 상태이다. 대규모 보안사고가 잇따르면서 국내 보안 산업은 연평균 7.9% 성장률을 기록하며 2015년 8조 2100억 원에서 2016년 8조 9500억 원의 시장규모를 형성하고 있으나, 보안 산업에 진출한 국내 기업들 대부분은 자본금 10억 미만의 중소기업(62.5%)인 것으로 조사되었다. 아울러 종업원 수 100인 미만의 중소기업은 76.5%(20인 미만 중소기업 36.1%)로 조사됨으로써 보안관련 기업들 대부분은 규모가 작은 것으로 조사되었다. 2016년 기준으로 보안 산업에 종사하는 인력 수는 39,928명으로 타 산업(전자 187,006명, 기계 145,847명, 자동차 115,621명, 반도체 90,492명)에 비하여 고용창출 기여도가 상대적으로 낮은 상태이다[8].

따라서 제 4차 산업혁명 시대에 지속가능한 사회를 보장하고 안정적인 사회를 구축하기 위해서는 새로운 신 성장 동력사업으로 정보보호 산업을 튼튼하게 육성할 필요가 있으며, 조직대상의 정보보호 제품 및 서비스 활용촉진을 통한 새로운 일자리 창출목적의 기반조성 연구가 선행되어야 한다. 정보보호 산업은 매년 고성장을 보이고 있으나, 저수익·저임금·장시간 노동이라는 열악한 산업 환경을 개선해야 한다는 과제를 안고 있으며, 정보보호시장 성장을 든든하게 뒷받침해야 하는 중견기업이 충분하지 않고, 소규모 기업과 대기업으로 양분되어 있어 시장이 건강하게 성장하지 못하고 기형적인 모습을 보이고 있다. 균형감 있는 건강한 정보보호 기반환경을 조성하기 위해서는 생물적 요소인 정보보호 기술·제품·서비스 등에 대한 고도화와 함께 비 생물적 요소(주위환경)인 정보보호 경영관리, 보안사고 범죄·심리학 정보보호 경제성 등에 대한 기반조성 구축이 함께 진행되어야 한다.

III. 결론

향후 연구 목표 달성을 위해 크게 2단계를 거쳐 연구를 진행하고자 한다. 먼저 향후 컴퓨팅 환경변화가 가져올 수 있는 기술적 요소와 사회적 변화요소(특성)를 예측함으로써, 예상 가능한 자율적인 서비스 시나리오 설계와 함께 요구되는 건강한 정보보호 기반환경 조성 주제들을 가시화하고자 한다. 세부적으로 현재(또는 미래) 서비스 사용자(조직)들의 행위(업무절차)를 시간적 흐름에 따라 조사한 후, 이를 해결하기 위한 서비스 시나리오를 새로운 환경 변화에 맞춘 기술적·사회적 특성 관점에서 설계하고자 한다.

다음으로 4차 산업혁명 시대의 환경전환을 위한 사회과학 정보보호 기초연구를 진행하고자 한다. 정보보호 경영관리 영역에서는 개인적 수준의 보안인식(인성) 수준을 측정할 수 있는 변수를 설계·검증하고, 이와 연관된 보안구성요소 분석을 실증적으로 진행할 예정이다. 보안사고 범죄·심리 영역에서는 조직관점의 보안사

고 최소화를 위한 정보보호 기반조성을 위해 범죄·심리 상황적 관점에서 보안사고 특성을 해석·분류하고자 한다. 정보보호 경제성 영역에서는 기 발생된 조직관점의 보안 사고를 대상으로 객관적 피해규모 산정모형을 설계하고 이에 대한 실증연구를 진행하고자 한다.

마지막으로 4차 산업혁명 시대의 안착을 위한 사회과학 정보보호 개선연구를 진행하고, 정보보호 기술과 사회과학적 연구의 안정적 통합을 이루고자 한다.

본 연구는 그동안 학문적 영역의 한계성으로 인하여 분리되어 왔던 정보보호 관련 법·제도, 경영학, 범죄학, 심리학, 경제학 등을 새로운 환경변화(제 4차 산업혁명)에 부합되도록 학문간 융합을 통해 집단지성 플랫폼 연구를 수행함으로써 건강한 정보보호 기반환경 조성에 새로운 합의점을 도출할 수 있을 것으로 예상된다.

[참고문헌]

[1] 한국인터넷진흥원, "'16년 랜섬웨어 동향 및 '17년 전망", 2017.

[2] 과학기술정책연구원, "미래사회 변화에 따른 산업기술보호 전략", 2016

[3] 김종현, 임선희, 김익균, 조현숙, 노병규, "빅데이터를 활용한 사이버 보안 기술 동향", 한국전자통신연구원, 전자통신동향분석 제28권, 제3호, 2013

[4] 한국인터넷진흥원, "2015년 국가정보보호백서", 2015.

[5] 한국과학기술기획평가원, "제4차 산업혁명 시대, 미래사회 변화에 대한 전략적 대응 방안 모색", 2016.

[6] 한국인터넷진흥원, "사물인터넷 보안 위협 동향", 2014

[7] 과학기술정보통신부, "K-ICT 융합보안 발전 전략", 2016

[8] 한국인터넷진흥원, "2017 글로벌 정보보호 산업시장 동향 조사", 2017

[9] 김용훈, "유비쿼터스 컴퓨팅환경의 정보보안 인력공급시스템 연구", 경영컨설팅연구, 제11권, 제3호, 2011, pp. 95-115

[10] 김정덕, "국가 정보보안 이슈 및 정책방안에 관한 연구", 디지털정책연구, 제10권 제1호, 2012, pp. 105-111.

[11] 이창무, "정보화 사회에서의 사이버 범죄", 과학사상, 제49호, 2004, pp. 36-52.

[12] 이창무, "프로파일링 기법을 통한 산업기밀 유출방지의 필요성", 산업보안연구논총, 제6호, 2010, pp. 115-172.

[13] 이창무 외, "10년 후 세상: 개인의 삶과 사회를 바꿀 33가지 미래상", 서울: 청림, 2012.

[14] 장상수, 신승호, 노봉남, "정보보호 안전진단 성과관리 측정 모델 및 성과분석", 정보보호학회논문지, 제20권, 제6호, 2010, pp.127-146

[15] 한국인터넷진흥원, 2013년 국내 지식 정보보안 산업 실태조사, 2013

[16] Baggett WO. "Creating a culture of security," The Internal Auditor, Vol. 3 No. 60, 2003, pp. 37-41.

[17] Cardinali, R. "Reinforcing our moral vision: Examining the relationship between unethical behaviour and computer crime," Work Study, Vol. 44, No. 8, 1995, pp. 11-18.

[18] CISCO, "The Internet of Things: How the Next Evolution of Internet Is Changing Everything, 2011

[19] CNN, "Hacking Anything Connected to the Internet", 2013

VR과 IoT를 활용한 전공탐색 기반의 대학 홍보전략

최경호*, 김병석**, 전영재**, 진용기**, 이동휘***

* 사이버보안평가기술원 기업부설연구소 연구소장

** 동신대학교 에너지융합대학 정보보안전공

*** 동신대학교 에너지융합대학 정보보안전공 교수(Corresponding Author)

Promotion Strategy of University based on Major Exploring Program using VR and IoT

Kyong-ho Choi*, Byeong-seok Kim**, Young-Jae Jeon**,

Yong-Ki Jin**, DongHwi Lee***,

* Head of Research Center, Institute of Cyber Security Technology

** Information Security, Dongshin University

*** Information Security, Dongshin University (Corresponding Author)

요 약

계속되는 인구 감소와 해외 유명 대학의 국내 진입 등과 같은 새로운 경쟁체제는 국내 대학들을 고등 교육의 공급자 입장에서 신입생 유치에 전력을 다해야 하는 학생 수요자로 전락시키는 극명한 입장 전환을 만들며, 이들에게 생존을 위한 자구책 마련 노력을 더욱 촉구하고 있다. 따라서 본 연구에서는 기존 대학 홍보 전략을 분석하고, 이를 기반으로 대학 입시생들의 참여도와 이해도를 높일 수 있도록 체험형 홍보 전략을 수립하여 대학의 인지도 및 선호도를 높일 수 있는 방안을 강구하려 한다. 이를 위해 전공탐색 및 진로체험 행사에 체험형 IT (Information Technology)기술인 VR(Virtual Reality)과 IoT(Internet of Things)를 응용시켜 적용하였다. 이의 결과는 행동하는 과정이 앎을 습득시켜 주기에 보다 더 많은 학생들이 이해하고 관심을 가질 수 있는 기회가 된다는 것을 보여주었다. 그래서 본 연구에서는 입학 예정생들에게 VR과 IoT 기술을 적용한 전공탐색 기반의 대학 홍보콘텐츠를 개발하고 이에 대한 체험자들의 반응을 평가하여, 체험형 홍보의 효과가 기존 집체 교육보다 더 나은 것임을 확인하였다.

I. 서론

교육 통계가 보여주는 인구 감소로 인한 대학 입시생 감소, 입시생들의 수도권 대학 선호, 고교 졸업 후 진학보다는 취업을 택하는 학생들이 증가하고 있는 경제/사회적 환경, 지방 대학들의 정원 초과 현상은 대학이 직면한 어려움들을 여실히 보여주고 있다. 이러한 문제는 2000년대 초반부터 지방전문대학을 중심으로 현실화되었으며, 많은 지방전문대학들은 직접 학생을 유치하기 위해 고등학교를 찾아다니며 대학홍보를 하고 있고, 잠재적 입학 예정생들과 대학진학상담교사를 대학에 초청하여 캠퍼스 투어를 실시하는 등 다양한 홍보활동을 수행하고 있다[1].

그리고 오늘날, 수도권에 소재한 대학들 및 국립대학의 경우에는 여전히 지원자가 정원을 넘어 지속적으로 우수한 학생들을 유치하고 있으나, 지방에 소재한 대학들의 경우 많은 대학들이 정원을 채우지 못하고 있으며 정원을 채운다고 하더라도 정원을 경우 충족시키는 대학이 여전히 많은 상황이다[2]. 특히, 꾸준한 대학

홍보 노력에도 불구하고 점점 입학생들이 감소하고 있는 현실은 지방대학의 위기를 더욱 심화시키고 있어, 대학 입시생들의 선호를 획득하기 위한 혁신적인 노력을 요구하고 있다. 이같은 현실은 점점 확대되어 국내 모든 대학들이 당면하는 문제가 될 것이고, 해외 유명 대학의 국내 진입 등과 같은 새로운 경쟁체제는 국내 대학들의 자구책 마련을 더욱 촉구할 것이다.

따라서 본 연구에서는 기존 대학 홍보 전략을 분석하고, 이를 기반으로 대학 입시생들의 참여도와 이해도를 높일 수 있는 체험형 홍보 전략을 수립하여 대학의 인지도 및 선호도를 높일 수 있는 방안을 강구하려 한다. 이를 위해 이어지는 2장에서는 대학 홍보와 여기에 응용 가능한 체험형 IT (Information Technology)기술인 VR(Virtual Reality)과 IoT(Internet of Things)를 살펴본다. 이를 토대로 3장에서는 대학 홍보에 활용 가능한 VR과 IoT 기반의 콘텐츠들을 설계하고, 4장에서는 이들의 효과성을 분석한다. 마지막으로는 연구 결과의 검토 및 향후 발전 방향을 모색해보도록 한다.

II. 관련 연구

2.1 대학 홍보 전략

과거 대학 홍보는 신문, 라디오와 같은 제한된 매체를 통해 단순한 공고 형식의 정보를 제공해 왔으나 IT사업의 발전으로 인터넷(Internet)을 이용한 매체의 기능적 폭을 수용할 수 있게 되면서 인터넷 홍보가 가능하게 되었다[3]. 뿐만 아니라 영상 콘텐츠[4], 유명 인사의 학생 또는 교수 영입[5] 등 대학의 인지도를 높일 수 있는 다양한 방법들을 시도하고 있다.

이러한 노력들은 인구 감소로 인한 대학 입학생 수 감소가 지속적인 현상으로 방향성을 가지게 되면서 대학들이 수요자 입장으로 전환되며, 학생들을 모집해야 하는 상황에 놓이며 가속화되고 있다. 이제는 대학 입시생들에게 먼저 다가갈 수 있는 친숙한 도구들을 모색하여 이를 이용한 홍보 전략을 수립해야만 호응을 얻을 수 있는 시대가 된 것이다. 그러므로 본 연구에서는 최근 체감형 엔터테인먼트, 교육용 기기로 각광 받고 있는 VR과 프로그래밍 교육을 주도 하고 있는 IoT 기술을 기반으로한 대학 홍보 콘텐츠를 개발하여 이의 효과성을 분석해보려한다.

2.2 VR

VR은 사용자가 가상세계에 몰입하여 가상의 콘텐츠와의 실시간 상호작용을 통해 실감 체험을 제공하는 기술이다[6]. VR기술을 이용한 체험형 교육콘텐츠는 체험한다는 것을 통해서 관련된 행위를 하며 알게 되고, 이 행동하는 과정 속에서 앎을 습득하게 되는 장점을 가져다준다[7]. 이러한 맥락에서 교육 효과 극대화를 위해 VR 기반 교육콘텐츠 개발이 이루어지고 있다[8, 9]. 그러므로 VR 기술을 통해 입학 예정생들에게 대학 홍보콘텐츠를 시연하는 것이 타당한 것으로 보여진다. 이는 VR이 대학이 추구하는 바와 입학 예정들에게 대학을 선택할 수 있는 유인에 대해 효과적으로 전달할 수 있는 매개체로써의 역할을 충분히 해낼 수 있을 것으로 기대되는 것에 따른다.

2.3 IoT

IoT는 인간과 사물, 서비스 세 가지 분산된 환경 요소에 대해 인간의 명시적 개입 없이 상호 협력적으로 센싱, 네트워킹, 정보 처리 등 지능적 관계를 형성하는 사물 공간 연결망으로 볼 수 있다[10]. 이 IoT 기술이 발전하며 정보화시대에서 모든 사물은 서로 연결되어 상호작용하게 되었고, 이로 인해 프로그래밍의 중요성이 부각되어, 교육적인 측면에서의 선호도 높아지게 되었다. 프로그래밍 교육을 통하면 학생들이 스스로 일상 생활에 적용할 수 있는 IoT 시스템을 고안할 수 있게 해줄 수 있기 때문에[11], 편의성과 부가가치를 높일 수 있는 자동화 기술 개발 능력을 갖추기 위해 국내외를 막론하고 어렸을 때부터의 프로그래밍 교육을 통한 응용력 향상이 중요하게 여겨지고 있다. 그러므로 본 연구에서는 대학 내 전공에서 배울 수 있는 기술들과 향후 취업전망 등을 담을 수 있는 IoT 콘텐츠를 기반으로 입학 예정생들의 체

험과 전공탐색 및 대학홍보 효과를 극대화시킬 수 있는 방안을 강구하려 한다.

III. 홍보콘텐츠 설계 및 구현

3.1 홍보콘텐츠 설계

본 연구에서 제안하는 홍보콘텐츠는 크게 VR 기반 대학 홍보콘텐츠와 IoT 기반 전공탐색콘텐츠로 구성된다. 이는 VR 콘텐츠 제작과 체험형 장비 자체가 고가이기 때문에 전공 단위에서의 사용보다는 학교 단위의 사용이 바람직하다고 보여지기 때문이며, 전체적인 비전과 정책을 보여주기에 적합하다고 생각되기 때문이다. 그리고 IoT 기술들은 새롭고 또 관심 있는 것들을 직접 만들어 낼 수 있기 때문에 전공 학습을 통해 이룰 수 있는 것들과 향후 예상되는 진로들을 보여주기에 적당하다 사료된다.

그러므로 VR 콘텐츠는 대학이 직면한 대내외 환경, 강점 및 능력 위주의 입학 예정생들이 관심을 가질 만한 이슈들을 담아내고, 이후 기 구축된 산학협력 기반과 주변의 공공기관 인사들의 증언형 영상을 담아 신뢰도를 확보하고자 하였다. 이는 영상콘텐츠 자체가 인터넷 상에서 쉽게 이용될 수 있음에 따라, 범용적인 사용자들의 접근이 가능해져 입학 예정생들의 주변에 긍정적인 영향을 미칠 수 있기 때문이다. 이미 부모, 교사 등을 대상으로한 대학 이미지를 높이는 것이 가장 효과적인 대학입시 전략[12]라는 것이 널리 알려진 현실에서 영상콘텐츠 활용 효과의 극대화를 추진하기 위해서는 보편적인 내용을 보여주는 것이 가장 좋을 것이다.

그리고 IoT 기반 전공탐색콘텐츠는 입학 예정생들이 직접 체험한 후, 시중에서 쉽게 구할 수 있는 기기들로 인터넷 학습을 통해 스스로 구현 가능하면서도 전공탐색이 가능한 것들로 구성하고자 하였으며, 여러 IoT 제품군 중 LED Box, 스마트팜, 스마트하우스 그리고 스마트 RC카를 선정하였다.

이는 라즈베리파이 또는 아두이노 등 코딩 학습이 가능한 싱글보드에 LED 전구를 동작시키고, 이후 습도 센서를 부착하여 토양에 수분을 공급하고, 다음 단계로 댁내 사물을 동작시킬 수 있는 등 단계적이고도 심화적인 학습이 가능하도록 구성하려는 노력의 결과이며, 대학 1학년생들이 평균적으로 1-2일 이내에 제작 가능한 제품군을 선택한 것이다.

이와 같이 구성한 홍보콘텐츠의 활용 예시는 다음 표 1과 같다.

<표 1> 홍보콘텐츠별 주요 내용

구분	콘텐츠명	대학 관련	전공 관련
VR	홍보영상	비전, 강점	지원체계
IoT	LED Box	산학협력 기반	IoT 기술
	스마트팜		IoT 기술 신재생에너지
	스마트하우스		IoT기술, 융합정보보안
	스마트 RC카		신소재, 전기차제어

3.2 홍보콘텐츠 구현

본 연구에서 제안한 VR 기반 대학 홍보콘텐츠는 최근 D대학이 이룩한 성과부터 품고 있는 비전, 그리고 산학연 협력체계 소속 주요 인사들이 바라본 대학과 그 소속 전공들의 전망에 대한 의견을 피력하는 것을 중심으로 스토리보드를 작성 및 영상을 촬영하여 제작되었고, 이를 VR 콘텐츠 전용 글래스를 이용하여 입학 예정생들이 직접 체험할 수 있는 환경에서 홍보물로 제공하였다.

그리고 IoT 기반 전공탐색콘텐츠도 IoT, 신재생에너지, 융합정보보안, 신소재, 전기차제어 전공 등의 교육과정과 진로에 대한 설명을 포함하여, 기반 기술 설명을 1:1로 직접 들으며 체험이 가능하도록 제품과 체험공간이 함께 제공되었다.









[그림 1] VR 기반의 대학 홍보콘텐츠와 체험 현장


<LED Box>


<스마트팜>



<스마트 하우스 내외부>


<스마트 RC카>




[그림 2] IoT 기반의 전공탐색콘텐츠와 체험 현장

여기서 LED Box는 싱글 보드에 LED 램프를 부착하여, 스위치 On/Off로 단순히 등을 켜고 끌 수 있는 간단한 장치이며, 이를 이용해 유리 액정에 그림을 그려 그림자 놀이를 할 수 있도록 하였다.

그리고 스마트팜은 습도 센서를 이용해 화분 토양의 습도를 실시간으로 체크하며, 일정 시간 간격에 일정 시간 동안 자동으로 수분을 공급할 수 있도록 자동화하였고, LED 램프를 이용해 식물 생장 환경에 적합한 빛을 지속적으로 공급하게 하였다.

스마트하우스는 태양광을 에너지원으로 하여 동작하게한 라즈베리파이를 기반으로 제작되었으며, 스마트폰을 이용하여 실내외등과 선풍기의 On/ Off 및 커튼을 내리고 올릴 수 있게 하였다. 그리고 이러한 기능을 한 명의 체험자가 동작시고 있을 때, 또 다른 체험자는 실내에 설치된 CCTV에 스마트폰으로 접속하여 카메라를 동작시켜 내부를 모니터링할 수 있도록 구성하였다.

마지막으로 스마트 RC카는 리튬 폴리머 배터리를 에너지원으로 하여 동작하는 아두이노 보드 기반으로 제작되었으며, 스마트폰을 이용하여 체험자가 직접 조종할 수 있다. 그리고 LED 투광기로 가상의 태양광을 발생시켜 전력을 생산하는 태양광 발전기도 제작하여, 체험자가 직접 계속적으로 충전되고 있는 배터리팩을 RC카의 배터리와 교체 또는 RC카의 직접적인 전기 충전을 진행하게 함으로써 전기 자동차의 활용법을 경험할 수 있게 하였다.

IV. 구현 콘텐츠 평가

본 연구에서 진행한 VR과 IoT 기술을 활용한 전공탐색 기반의 대학 홍보콘텐츠는 D대학 내 체육관을 이용한 대외행사에서 직접 시연하며 체험자들의 반응을 인터뷰하여 평가하였으며, 이 데이터는 기존 입학 예정생들의 교내 방문 시 진행하던 집체 교육 방식의 홍보 성과와 대조되었다. 여기서 집체 교육은 본 연구에서 제안한 홍보콘텐츠와 동일한 내용으로 진행하였기는 하나, VR은 고화질 영상으로, IoT는 관련 기술을 소개하는 것과 유튜브에 있는 관련 영상을 이용해 간접적이지만 육안으로 확인시켜주는 강의식으로 진행되었다. 이 역시 강의

종료 후 수강생들의 반응을 인터뷰하여 평가하였으며, 대조에 활용한 두 그룹의 인터뷰 대상은 각각 20명씩으로 이루어졌다. 각 그룹에서 콘텐츠 항목별 의견을 제시한 내용들의 평균값들은 다음에 이어지는 표들에 나타나있다.

표 2. VR와 IoT 기술 기반 콘텐츠의 만족도

만족도		매우 만족	만족	보통	불만	매우 불만
VR		■				
IoT	LED Box			■		
	스마트팜		■			
	스마트 하우스	■				
	스마트 RC카	■				
합계		■				

표 3. VR와 IoT 기술 기반 콘텐츠의 이해도

이해도		매우 높음	높음	보통	낮음	매우 낮음
VR		■				
IoT	LED Box	■				
	스마트팜		■			
	스마트 하우스		■			
	스마트 RC카		■			
합계			■			

상기 결과를 분석해보면, VR과 IoT 기술을 이용한 콘텐츠의 만족도와 이해도가 집체 교육 기반 콘텐츠보다 높은 것을 볼 수 있다. 이는 체험자가 새로운 것들을 직접 경험함으로써 신기함에서 오는 높은 만족도와 즐거움을 얻을 수 있는 것에서 비롯된 것으로 보인다. 그러나 LED Box의 만족도에서 볼 수 있는 것처럼, 단순한 기능으로 손쉬운 이해가 가능한 것은 체험자의 호기심을 자극하기 어려워, 기술에 대한 이해도는 높일 수 있으나, 체험 만족도는 높일 수 없음을 알 수 있었다.

그리고 집체 교육 시의 콘텐츠 만족도와 이해도는 중간 이상의 값을 가지는 '만족'과 '높음'의 응답이 많았는데, 이는 집체 교육의 특성 상 단체로 보게 된 것들에 대해 보편적이고 일반화된 답변을 한 것으로 보인다. 다시 말하면, 대학별 비슷한 유형을 보이는 홍보영상물에 대해 좋은 평가를 내려주고, 직접 경험하지 않았어도 영상물을 통해 알게 된 기술 내용들을 적당히 습득한 정보로 인식하여 알게되었다라고 답변을 한 것으로 생각된다. 이러한 판단은 스마트팜의 예를 들어 두 그룹의 답변을 되짚어 보면, IoT 기술을 체험한 그룹은 수분 공급 시 습도 센서의 수치가 변화한다는 것을 기억하는데 반해, 집체 교육을 한 그룹은 습도를 모니터링하여 수분을 공급한다라고 일반화된 답변을 한다는 것이다.

표 4. 집체 교육 기반 콘텐츠의 만족도

만족도		매우 만족	만족	보통	불만	매우 불만
홍보영상			■			
IoT	LED Box			■		
	스마트팜		■			
	스마트 하우스		■			
	스마트 RC카		■			
합계			■			

표 5. 집체 교육 기반 콘텐츠의 이해도

이해도		매우 높음	높음	보통	낮음	매우 낮음
홍보영상			■			
IoT	LED Box		■			
	스마트팜		■			
	스마트 하우스		■			
	스마트 RC카		■			
합계			■			

이러한 결과는 행동하는 과정이 앎을 습득시켜 준다는 기존 연구[7]의 주장을 더욱 강화시켜 주고 있으며, 대학 홍보 자체가 더욱 더 입학 예정생들과의 상호 작용을 통한 방법들을 사용하여야 더욱 효과가 있을 것이라는 것을 알게 해준다.

V. 결론

본 연구에서는 입학 예정생들에게 VR과 IoT 기술을 적용한 전공탐색 기반의 대학 홍보

콘텐츠를 개발하고 이에 대한 체험자들의 반응을 평가하여, 체험형 홍보의 효과가 기존 집체 교육보다 더 나은 것임을 확인하였다. 특히, VR을 활용한 것은 체험자로 하여금 짧은 시간 내에 직접 많은 경험을 하게할 수 있어 강력하고 중요한 정보를 전달하기에 적절했던 것으로 생각된다. 그러나, VR도 체험자가 관심을 가지고 정보를 받아들일 때 효과가 있다는 것을 주지하여야 하며, VR 자체는 홍보를 위한 매개체가 되어야 하지 주가 되어서는 안된다는 것을 알아야 한다. 그러므로 단순한 흥미 유발, 신기효과 유발에 그치지 않고 체험자의 적극적인 참여와 탐구력을 이끌어 낼 수 있는 스토리보드 작성과 내용 구성이 필요하다.

그리고 IoT 기술 관련 체험은 개인보유기기를 활용(Bring Your Own Device: BYOD)하였는데, 이것 역시 체험자들에게 직접 시행할 수 있는 기회를 준 형태가 되어 긍정적인 요소로 작용하였다. 체험자들이 개인의 스마트폰 등을 이용한 체험은 자신이 직접 움직인다는 점이 있어 참여도를 높일 수 있는 유인이 되었다. 그리고 이러한 점은 정보화시대에서 태어나 자라고 있는 현재의 학생들에게는 당연한 추세로 보이며, 이 갖추어진 기본 인프라를 잘 활용하면 더 많은 체험형 홍보콘텐츠를 구상하고 제작할 수 있는 기반이 될 것으로 보인다.

[참고문헌]

[1] 고동원, 지방전문대학홍보에서 인터넷 매체의 효율적 활용, 한국콘텐츠학회논문지, 10권, 9호, pp. 478-486, 한국콘텐츠학회, 2010.

[2] 하강진, 문재영, 대학 홍보요인의 인식경로가 대학의 지원과 선택에 미치는 영향에 관한 연구, 한국품질경영학회보, 41권, 1호, pp. 69-77, 한국품질경영학회, 2013.

[3] 장승영, 스마트시대의 대학 홍보를 위한 CIM 인터페이스 기법 : 스마트 웹 중심, 한국전자통신학회 논문지, 7권, 3호, pp. 597-606, 한국전자통신학회, 2012.

[4] 백재훈, 대학 홍보에 있어 영상콘텐츠의 활용현황 연구 : 부산지역 종합대학을 중심으로, 조형미디어학, 15권, 4호, pp. 71-78, 한국일러스아트학회, 2012.

[5] 유재웅, 유명 인사(Celebrity)의 대학홍보활동이 개인브랜드에 미치는 역전이 효과, 브랜드디자인학연구, 10권, 3호, pp. 197-208, 한국브랜드디자인학회, 2012.

[6] 박종일, 서병국, 최지윤, 박정식, 실재감과 상호작용의 영상 기술 : 3D/UHD, VR, 그리고 AR, 정보과학회지, 28권, 8호, pp. 26-37, 한국정보과학회, 2010.

[7] 정유경, UX 디자인 방법론을 적용한 VR 소방체험 교육콘텐츠 개발, 한국콘텐츠학회논문지, 17권, 3호, pp. 222-230, 한국콘텐츠학회, 2017.

[8] 김진곤, VR기술기반 융합교육을 위한 교과목 개발 사례연구, 커뮤니케이션 디자인학연구, 47권, pp. 31-44, 한국커뮤니케이션디자인협회 커뮤니케이션디자인학회, 2014.

[9] 배성실, 이정민, 안정수, 3D VR 기반의 교육 콘텐 개발 시스템 구현, 디지털산업정보학회지, 12권, 1호, pp. 97-106, 디지털산업정보학회, 2016.

[10] 김호원, 김동규, IoT 기술과 보안, 정보보호학회논문지, 22권, 1호, pp. 7-13, 한국정보보호학회, 2012.

[11] 최숙영, 김세민, 앱 인벤터와 아두이노를 이용한 피지컬 컴퓨팅 교육이 공업계 고등학생의 창의·융합적 사고에 미치는 영향, 컴퓨터교육학회논문지, pp. 45-54, 한국컴퓨터교육학회, 2016.

[12] 오대영, 정보원과 신뢰도가 학생의 대학이미지와 대학결정에 미치는 영향 차이 : 대인커뮤니케이션, 미디어, 대학을 중심으로, 언론과학연구, 15권, 3호, pp. 181-220, 한국지역언론학회, 2015.

2018 한국정보보호학회 하계학술대회

A6 컴퓨터보안 1

이 만 희 (한남대학교)

- **안드로이드 클립보드를 활용한 악의적 e-mail 탐지 기술**
  이효진, 장수인
- **기호실행을 이용한 바이너리 난독화 해제 기술 연구**
  주하종, 김민재, 염흥열
- **Shannon 엔트로피 값 분석을 통한 파일 암호화 판별에 관한 연구**
  고주성, 곽 진
- **모바일에서의 애플리케이션 접근 제어 메커니즘 분석**
  김이진, 최형기

안드로이드 클립보드를 활용한 악의적 e-mail 탐지 기술

이효진, 장수인, 김형종
서울여자대학교 정보보호학과

Detection of malicious E-mail using clipboard of Android

Hyo-jin Lee, Su-in Jang, Hyung-Jong Kim
Division of information security, Seoul Women's University.

요 약

Phishing E-mail 및 스미싱 등 악의적 목적으로 전송된 메시지로 인해 지속적으로 피해 사례가 발생하고 있다. 본 연구의 목적은 사용자들이 좀 더 쉽게 메시지 내의 악의적 의도를 알게 하는 데에 있다. 본 연구에서 개발된 도구에서는 의심 단어, 링크, 첨부파일의 유무로 위험 요소가 포함되어 있다는 것을 사용자에게 알려주고 이것의 차단 여부를 사용자에게 선택하도록 한다. 본 연구에서 선택한 클립보드를 기반으로한 악성 메시지 탐지 기술은 안드로이드 환경의 E-mail뿐만 아니라 문자, Social Network Service 타임라인, 채팅 Application 등에도 활용할 수 있다. 본 연구의 기여점은 클립보드를 기반으로한 악성 메시지의 탐지 기술의 설계 및 구현에 있다.

I. 개요 및 연구의 필요성

한국인터넷진흥원(KISA)이 발표한 '국내 스피어 피싱 유형 분석'에 따르면 기업과 기관을 노리는 표적 공격의 91%가 Spear Phishing E-mail에서 시작되고 공격 대상의 76%가 기업이나 정부 기관인 것으로 나타났다[1]. 기업을 대상으로 솔루션을 제공하거나 스팸 메일을 탐지하는 프로그램은 비교적 많이 있지만, 개인이 손쉽게 클립보드를 이용해서 Phishing을 탐지하는 프로그램이 필요하다고 판단되어 본 연구를 시작했다.

이 프로그램은 사용자가 E-mail을 읽어야 검사할 수 있다. 그러나 E-mail을 열어보는 것만으로는 아무 일도 일어나지 않고 E-mail에 포함된 첨부파일이나 링크에 속아 정보가 유출된다고 생각하기 때문에 큰 문제가 아니라고 생각하고, 의심단어, 첨부파일, 링크를 주요 판단 근거로 삼는다.

이와 관련하여 통상적으로 효과적인 정보보호를 위해서는 적절한 교육이 필수적이다.[2]. 사용자들이 스스로 판단하고 생각에 도움이 될 수 있도록 처음 실행 화면에 지침서를 넣었다.

현재 메일 보안 솔루션으로 언급할 만한 것은 다음과 같다. PC 버전으로는 '지란지교시큐리티'의 'SPAM SNIPER', '다우기술'의 '테라스메일' 그리고 'Symantec', 'Trend Micro', 'ForcePoint', 'FireEye' 등의 솔루션이 있는데 이는 모두 기업 업무환경에 적용되는 솔루션이다. 모바일 버전으로는 다양한 애플리케이션이 존재하지만, 스팸 메일에는 효과적인 반면에 Phishing 메일 혹은 메시지는 차단하지 못한다.

이처럼 기존의 솔루션 대부분이 일반 사용자가 대상이 아닌 기업이 대상인 것이 많고 Phishing 메일 필터링에는 효과적이지 못하다고 판단했다. 본 연구는 일반 사용자도 악성 메일을 쉽게 검사할 수 있도록 구성된 안드로이드 애플리케이션이다.

사용자가 PC보단 스마트폰을 통해 메일을 더

자주 열람한다고 생각해, 프로그램을 스마트폰용 애플리케이션으로 제작했다. 프로그램 이름은 Phishing E-mail을 차단한다는 의미에서 Phishing E-mail과 Killer를 합성한 'Philler'라고 정했다.

메일 사용자들은 메일 서비스 업체들이 정상 메일과 악성 메일을 완벽히 구분했다고 신뢰하기에 자신들이 받은 메일들을 의심 없이 열람한다. 하지만 이 차단 기능에는 악성 메일이 아닌데 악성 메일로 판정하는 False Positive와 악성 메일임에도 불구하고 정상메일로 판정하는 False Negative 판단 오류가 존재한다[3]. 이 두 가지 판단 오류 중 False Negative 발생이 더 치명적인데[4], 메일 사용자는 악성 메일의 발신자, 메일 내용 그리고 첨부파일을 신뢰하면서 큰 피해를 본다. 해당 애플리케이션은 악성 메일 여부를 판단한 후, 차단하지 않고 사용자에게 위험도를 알린다. 이는 모든 차단 프로그램이 False Positive의 가능성을 갖고 있으므로 최종 판단은 사용자에게 맡기는 방식을 택했다.

이 애플리케이션은 서버가 차단하지 못한 피싱 메일 및 스미싱 들을 추가적으로 탐지하는 기술로 활용이 가능하다.

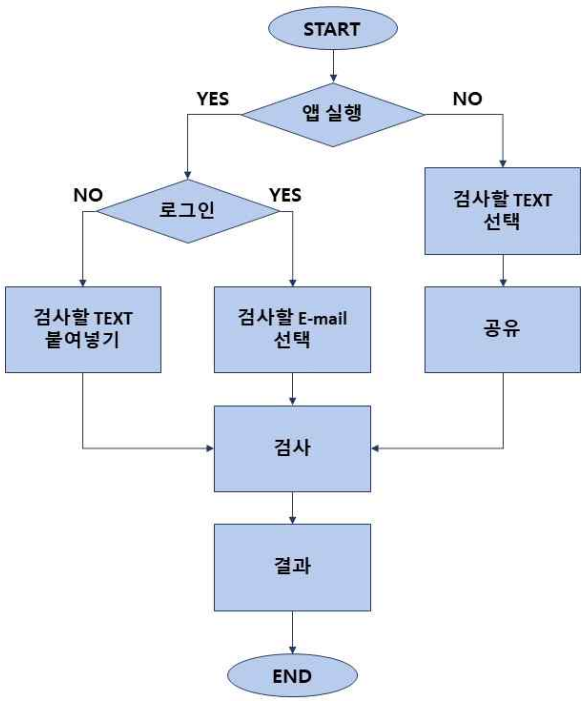
II. 전체 구성

2.1 Philler App의 개발 및 기능

본 연구에서 제시하고 있는 메시지에 대한 악성 여부 검사 방법은 다음 두 가지가 있다.

(Philler App을 통한 검사) 사용자가 Philler 애플리케이션을 실행해 검사하고자 하는 메일이 있는 메일 서비스 업체(ex. naver, daum 등)에 로그인한다. 그리고 Phishing 메일로 의심되는 메일을 열람해 그 내용을 클립보드에 복사하고 애플리케이션 하단에 있는 텍스트 창에 앞서 복사한 E-mail 내용을 붙여 넣는다. 검사 버튼을 누르면 해당 메일의 위험도의 정도가 오른쪽 아래에 팝업 창으로 나온다. 이 방법은 사용자에게 판단 결과를 팝업창 형식으로 알려, 사용자가 더욱 빠르게 업무 수행할 수 있도록 돕는다. 그러므로 검사 결과를 다른 창으로 이동해서 보여주지 않고 즉시 확인할 수 있도록 팝업창 기능을 사용했으며, 사용자가 검사 버튼을 누르는 과정에서 팝업창이 뜨는 과정까지가 빨리 이루어진다.

(메일 혹은 메신저 App의 공유기능 활용) 사용자가 검사하고자 하는 SMS나 Social Network Service, 메신저의 글을 클릭해 Philler 애플리케이션으로 공유한다. 사용자의 스마트폰 화면은 자동으로 Philler 애플리케이션으로 전환되면서 공유한 내용의 위험도 정도가 화면에 나타난다. 이 방법은 SNS와 SMS 그리고 메신저 적용에 효과적인 방법으로, 메일 또한 적용할 수 있다. 스미싱에 활용될 수 있는 SMS와 카카오톡 메신저에서 편리하게 활용할 수 있는 방법으로, 받은 메시지를 2초 이상 터치하고 있을 때 팝업되는 메시지 옵션의 공유 기능을 활용한다.



[그림 1] 플로우 차트

Philler App은 Android Studio를 활용하여 개발 하여 안드로이드 환경에서 구동되는 소프트웨어 이다. 기존의 악성 메일들을 수집해 메일별로 토큰 구분된 단어의 발생 값을 기록하여 이를 Bayes 확률공식에 적용해 학습 데이터를 얻어낸 후, 새로 들어온 메일에 대해 악성 메일 여부를 판단하는 기술인 Bayesian Filter 기술[5]이 가지고 있는 기능 중 기존 악성 메일들을 수집해 학습한다는 개념을 적용했다. 검사는 단어, 첨부파일, 첨부된 링크를 통해 진행한다.

스팸메일과 Phishing E-mail이 가진 특징을 학습 및 분석하기 위해서 메일 사용자들에게 실제로 피해를 준 메일들을 수집하여 공통으로 가진 단어들을 DB에 적용했다. 위험도 결과를 나타내는 심볼 이미지 파일을 만들어 사용자 인터페이스로 활용하였다.

2.2 Philler App 기능별 세부 설명

2.2.1 검사 알고리즘

메일 또는 텍스트에 있는 단어, 첨부파일, 첨부된 링크를 통해 악성 메일 또는 SMiShing 메시지 여부를 판단한다.

(단어 분리) 검사할 메일 또는 텍스트를 직접 정한 기준을 통해 단어별로 분리한다. 예를 들어 검사할 내용이 '서울 여자 대학교'라면, ' '를 기준으로 '서울', '여자', '대학교'와 같이 세 단어로 분리한다. 이 분리 기준은 조사, 띄어쓰기, 줄 바꿈 그리고 스팸메일에 자주 사용되는 기호로 현재 21개가 동시 적용되고 있다.

(count에 저장) DB에 스팸메일 또는 Phishing E-mail에 자주 사용되는 단어들이 저장되어 있는데, 이를 알고리즘에 갖고 온다. 이 단어들과 "분리된 단어"들을 일일이 비교한 후, 일치할 경우 count 값을 증가시킨다.

(count_ex에 저장) 미리 정해놓은 첨부파일의 확장자와 '분리된 단어'들과 비교한 후, 일치할 경우 수를 센다. 이 확장자는 실제 피해자들이 받은 첨부파일들의 것으로 설정했다.

(count_domain에 저장) DB에 첨부된 링크를 화이트리스트 방식으로 분석하는 데 필요한 도메인들이 저장되어있는데, 이를 알고리즘에 갖고 온 후 분리된 단어들과 비교한 후, 일치할 경우 수를 센다.

(판단) count, count_ex, count_domain 값을 보고 결과를 판단한다.

2.2.2 화이트 리스트

첨부된 링크를 분석하기 위해 화이트리스트 기술(White List)을 적용한다. 이는 악성 링크를 DB로 만드는 블랙리스트의 반대되는 개념으로, 안전하다고 알려진 링크로 화이트리스트를 만들어 이에 적용되는 링크는 언제나 수용하는 방식이다[6].

해당 애플리케이션에 적용된 화이트리스트에는 국내 인터넷 사용자가 가장 많이 방문하는 상위 50개의 사이트가 저장되어있다. 리스트는 다음과 같다.

사이트 주소	사이트 주소
www.naver.com	www.google.co.kr
www.youtube.com	www.daum.net
www.google.com	www.facebook.com
www.news.naver.com	www.tistory.com
www.dcinside.com	www.donga.com
www.ppomppu.co.kr	www.twitter.com
www.client.net	www.inven.co.kr
www.instagram.com	www.namu.wiki
www.etorrent.co.kr	www.todayhumor.co.kr
www.shopping.naver.com	www.nate.com
www.ilbe.com	www.11st.co.kr
www.gmarket.co.kr	www.blog.me
www.hitomi.la	www.tumblr.com
www.msn.com	www.torrentkim3.net
www.wikipedia.org	www.auction.co.kr
www.danawa.com	www.zipbogo.net
www.ddanzi.com	www.interpark.com
www.tosarang2.net	www.map.naver.com
www.movie.naver.com	www.cafe24.com
www.kakao.com	www.chosun.com
www.slrclub.com	www.afreecatv.com
www.coupang.com	www.nexon.com
www.amazon.com	www.finance.naver.com
www.news.nate.com	www.linktender.net
www.github.com	www.bobaedream.co.kr

[표 1] 국내 상위 50개의 방문 사이트

첨부된 링크가 화이트리스트에 없는 링크라면 '위험한 링크가 포함되어 있습니다.'라는 문구가 적힌 결과 창을 띄운다.

그런데 이 방법에는 첨부된 링크가 실제 위험한 링크가 아님에도 불구하고 화이트리스트에 존재하지 않기에 위험링크로 분류될 수 있는 허점이 존재한다. 이렇듯 화이트리스트 이외의 모든 링크가 위험한 것이 아니라, 더욱 높은 위험 확률을 갖고 있기에 주의가 필요하다는 것을 사용자에게 알린다.

2.3 주의사항 고지 기능

애플리케이션 메뉴 내에 있는 '주의사항' 버튼을 누르면 악성 메일 예방수칙을 확인할 수 있도록 했다. 내용은 다음과 같다.

- 발신인인 불분명한 메일은 확인하지 않는다.
- 메일에 포함된 첨부 파일은 백신 프로그램으로 검사를 한 후 열람하도록 한다.
- 백신 프로그램을 설치하여 최신 엔진을 유지하고 실시간 감시 기능을 사용한다.
- 메일 본문에 포함된 링크는 가급적 접속을 하지 않도록 한다.
- 메일 내용 중 링크를 걸어두고 일반 사이트로 접속한 것처럼 비슷하게 꾸며 사용자의 정보를 입력하게 만들어서 그 정보를 가로챈다.
- 금융결제원 홈페이지(www.kftc.or.kr) 및 인터넷지로 홈페이지(www.giro.or.kr)에서는 어떠한 경우에도 전화 또는 인터넷상으로 금융정보를 요구하지 않는다.

Ⅲ. 개발 결과

본 장에서는 개발 결과를 개발 화면을 통해 설명한다.

3.1 애플리케이션을 통한 점검

[그림 2]의 각 과정을 설명하면 다음과 같다.

(가) 애플리케이션을 실행한 후 검사하고자 하는 메일이 있는 메일 서비스 업체에 로그인한다.

(나) 검사하고자 하는 메일을 복사한다.

(다) 하단에 있는 텍스트 창에 붙여넣고 검사 버튼을 누른다.

(라) 오른쪽 아래에 팝업창으로 나온 결과를 확인한다.

3.2 '공유'기능을 통한 점검

[그림 3]의 각 과정을 설명하면 다음과 같다.

(마) 검사하고자 하는 글을 선택한다.

(바) Philler 애플리케이션으로 공유한다.

(사) 공유한 내용이 애플리케이션에 나타난 것을 확인한 후 검사 버튼을 누른다.

(아) 위험도를 확인한다.



[그림 2] 애플리케이션을 통해 실행하는 과정



(마) (바) (사) (아)

[그림 3] 공유 기능으로 실행하는 과정

IV. 결과 및 향후방향

이 애플리케이션은 악성 메일, 특히 Phishing E-mail에 효과적인 애플리케이션이다. 메일 서버 내에 있는 필터링 기능은 주로 스팸메일 차단에 효과적이긴 하지만, Phishing E-mail 차단에는 여전히 취약하다. 메일 서버 내 차단 기능을 1차 필터링, Philler 애플리케이션을 2차 필터링 그리고 사용자가 해당 애플리케이션의 판단 결과 창을 통해 메일을 신뢰할지 아닐지에 대한 최종 결정을 한다. 이는 False Negative와 False Positive의 문제점을 보완하도록 노력한 부분이다.

메일 뿐만 아니라 모든 텍스트를 갖고 검사할 수 있는 장점이 있고 가벼운 구동과 쉬운 이용방법으로 사용자 누구에게나 편리하게 다가갈 수 있다.

향후 더 많은 악성 메일을 수집해 그에 대한 특징을 분석하고 DB 목록을 보완하고, 국내 사이트 외에도 안전한 국외 사이트 또한 DB 목록에 추가할 계획이다. 이를 위해 안전한 링크 여부 분석을 위해 필요한 분야를 학습하고 연구를 해야 한다.

현재 메일 내용 분리 기준이 한국어를 초점으로 되어있는데, 영어도 추가하고, 직접 클립보드에 복사해서 붙여넣는 방식이 아닌, 좀 더 간편한 방법을 찾아보고 연구할 계획이다.

[참고문헌]

[1]한국인터넷진흥원, 국내 스피어피싱 유형 분석, https://www.krcert.or.kr/filedownload.do?attach_file_seq=826&attach_file_id=EpF505.pdf

[2]손유승 외, 「스피어 피싱 대응을 위한 관리적 보안대책에 의한 접근」, 한국정보통신학회, 2013

[3]남명국 외, 「사용자 패턴 기반의 부정오류(FN) 수준 평가를 활용한 스팸메일 분류」, 한국정보과학회, 2008

[4]Thomas Calabrese, 『Information Security Intelligence: Cryptographic Priciples and Applications』, Thomson Learning, 2004, p.354

[5]김두환 외, 「송・수신 이메일의 학습을 통해 긍정 오류를 줄이는 개선된 베이지안 필터링 기법」, 한국정보보호학회, 2008

[6]한국정보통신기술협회, http://www.tta.or.kr

기호실행을 이용한 바이너리 난독화 해제 기술 연구

주하종*김민재*염흥열**

순천향대학교 정보보호학과

Binary Deobfuscation using Symbolic Execution

Ha-Jong Joo*, Min-Jae Kim*, Heung-Youl Youm**

*Department of Information Security Engineering, SoonChunHyang University.

요 약

바이너리 난독화는 컴파일된 프로그램의 코드를 복잡하게 만들어 역공학을 방해하는 기술로, 소프트웨어 보안을 위해 사용하기도 하며, 악성코드에서 분석을 방해하기 위해 사용하기도 한다. 그 중에서도 코드 가상화 기법으로 난독화된 프로그램은 원본 기계어 코드를 가상 기계의 명령어로 변환하여 역공학을 방해하는 기술로, 기계어 자체를 해석할 수 없기 때문에 일반적인 바이너리 난독화 기법보다 분석이 어렵다. 본 논문에서는 기호 실행을 이용해 가상화된 코드의 핵심 동작을 추출하고, 이를 원본 기계어 코드로 재구성 하는 도구를 구현함으로써 가상화 난독화 기법이 적용된 프로그램을 효율적으로 분석할 수 있도록 한다. 또한 본 도구에 어떠한 한계점이 있는지 알아보고, 향후 연구 방향에 대해 살펴본다.

I. 서론

현대사회에서 소프트웨어는 IoT와 같은 간단하지만 실생활에 밀접한 프로그램부터 빅데이터를 처리하는 대형 서버 프로그램에 이르기까지 광범위하게 사용되고 있다. 이렇게 소프트웨어가 보편적으로 사용됨에 따라서 소프트웨어 보안의 중요성 또한 증가하고 있으며, 역공학(Reverse-Engineering)에 의해 소프트웨어가 분석될 경우 분석 정보를 악용할 수 있기 때문에 역공학을 방해하기 위해 “Bogus Control Flow”, “Control Flow Flattening”, “Instruction Substitution” 등 다양한 방식의 바이너리 난독화 기법이 연구되고 있다[1],[11].

이러한 바이너리 난독화 기법은 악성코드에도 빈번하게 적용되고 있는데, 악성 행위 분석을 어렵게 하기 위한 난독화 기법이 갈수록 고도화 되고 있으며, 최근에는 코드 가상화를 이용한 난독화(Virtualization-Obfuscation) 기법까지 빈번하게 적용되고 있다[1],[10].

코드 가상화를 이용한 난독화 기법은 원본 기계어 코드를 가상 기계의 명령어로 변환하여 역공학을 방해하는 기술이다. 코드 가상화를 이용해 난독화된 코드는 기존의 디스어셈블러(Disassembler)로 전혀 해석되지 않기 때문에 단순히 실행흐름을 복잡하게 만드는 기존의 난독화 기법들에 비해 훨씬 더 분석하기 어렵다. 이렇게 가상화된 코드를 분석하기 위해서는 가상 코드를 해석하고 실행시키는 가상 기계를 먼저 분석하는 것이 일반적이다. 그러나 이러한 분석 방식은 분석에 소요되는 시간이 매우 길어질 뿐만 아니라, 난독화가 완전히 해제된 바이너리를 확보하지 못하므로 난독화된 코드의 분석 결과를 저장하거나 공유하는 것이 매우 까다롭다[10].

이와 같이 가상화 난독화된 코드의 수동 분석이 매우 어려움에 따라 가상화된 코드를 자동으로 분석하는 연구가 다수 진행되었다[2][9][10]. 본 논문에서는 그 중 기호 실행

(Symbolic Execution)을 이용해 가상화된 코드의 핵심 동작을 추출하는 방식[9]을 사용하여 가상화 난독화된 코드로부터 원본 기계어 코드를 추출하고, 난독화가 해제된 바이너리를 자동으로 생성하는 도구를 제작하였다.

또한 기존의 방식[9]에서는 난독화가 해제된 실행 가능한 바이너리를 생성하기 위해서 가상화된 함수 이외의 모든 코드를 분석하고 이를 소스코드로 직접 복원해야 한다는 한계점이 있었다. 본 논문에서는 원본 바이너리의 파일 헤더를 조작해 새로운 섹션에 원본 코드를 삽입하고 코드 후킹을 통해 난독화가 해제된 함수가 호출되도록 수정함으로써 별도의 분석 없이도 바이너리를 생성할 수 있도록 하였다.

II. 기호 실행을 통한 분석

2.1 기호 실행

기호실행이란 소프트웨어 실행 시 특정 메모리를 실제 값(Concrete Value)이 아닌 기호로 두고 실행하는 바이너리 동적 분석 기법이다. 기호로 지정된 메모리에 어떠한 연산이 이루어질 경우, 해당 메모리 값은 특정 값이 아닌 연산식(Symbolic Expression)으로 구성된다.[9] 이렇게 생성되는 연산식을 분석하면 해당 메모리에 어떠한 연산이 이루어졌는지 파악할 수 있으며, 해당 메모리 값이 특정 분기문에 영향을 끼칠 경우 그 분기 조건을 파악할 수 있다. 이러한 기호실행 기법은 바이너리 자동 분석, 취약점 자동 탐지 등 다양한 연구에 활용되고 있다[2].

2.2 기호 실행을 이용한 핵심 코드 추출

가상화된 코드는 실제 기계의 명령어를 가상 기계의 명령어로 재구성한 코드로, 디스어셈블러나 일반 프로세서가 해석할 수 없으며, 별도로 탑재된 가상 기계에서 해석하고 실행시킨다. 이렇게 가상화된 코드는 겉보기에는 완전히 달라 보이지만 실제로는 결국 동일한 동작을 한다. 예를 들어, xor 명령어를 가상화한 경우, 가상화된 코드는 해석할 수 없지만, 해당 코드를 해석하고 실행시키는 핸들러(Handler) 내에서는 최종적으로 특정 메모리에 대해 원래의 기계어 코드 xor 명령어를 실행시킨다. 이러한 점에 착안하여 연산 대상이 되는 메모리를 기호로 두고 기호 실행을 수행한다면, 가상화된 코드를 거친 후, 해당 메모리에는 실제로 이루어진 연산 집합이 Symbolic Expression 형태로 생성된다[2],[10].

III. LLVM-IR을 이용한 코드 복원

3.1 LLVM Compiler Infrastructure

LLVM은 재사용성을 강조하는 모듈식 컴파일러 기반 구조이다. LLVM은 컴파일 과정에서 LLVM IR(Intermediate Representation) 이라는 중간 언어를 사용하며, LLVM IR에 대해 난독화와 최적화를 수행한다[4],[7].

3.2 LLVM-IR을 이용한 재컴파일

Jonathan Salwan 등의 논문[9]에서는 기호실행을 통해 수집된 Symbolic Expression을 LLVM-IR로 변환하여 최적화 옵션과 함께 컴파일 하는 방법을 제시하였다. 이를 통해 가상화된 코드로부터 추출한 핵심 연산을 실행 가능한 기계어 코드로 변환할 수 있다.

3.3 코드 삽입 및 후킹을 이용한 실행파일 재구성

Jonathan Salwan 등의 논문[9]에서는 가상화 되지 않는 코드는 직접 분석하고 이를 소스코드로 복원하였다. 이러한 방식은 실용적인 단계에서 매우 비효율적이다. 본 논문에서는 가상화 난독화가 해제된 코드를 원본 실행파일에 삽입하고, 해당 함수 호출 부를 후킹하는 방식으로 별도의 분석 없이 난독화 해제된 프로그램을 생성하도록 하였다.

IV. 난독화 해제 도구 구현 결과

4.1 가상화 난독화가 적용된 프로그램

본 논문에서는 [표 2]와 같이 사용자로부터 입력받은 값에 대해 xor 연산을 수행하는 프로

그램을 대상으로 실험을 진행하였다. xor 연산을 수행하는 func 함수는 가상화 되어있다.

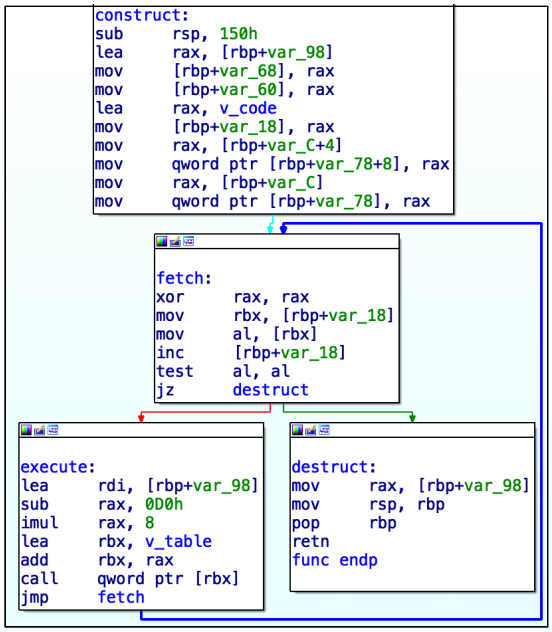
```
#include<stdio.h>
int func(int x, int y)
{
    return x ^ y;
}
int main(int argc, char *argv[])
{
    int x, y;
    printf("x: ");
    scanf("%d", &x);
    printf("y: ");
    scanf("%d", &y);
    printf("result: %d\n", func(x, y));
    return0;
}
```

[표 2] 실험 대상 프로그램의 원본 소스코드

가상화된 func 함수 코드는 [그림 1]과 같으며, 이렇게 가상화된 코드는 [그림 2]와 같이 구현된 가상 기계를 통해 해석되고 실행된다.

```
.data:0000000000604130 v_code          db 0D0h
.data:0000000000604131                 db 0D5h
.data:0000000000604132                 db 0BBh
.data:0000000000604133                 db    6
.data:0000000000604134                 db  12h
.data:0000000000604135                 db 0DAh
.data:0000000000604136                 db  0Bh
.data:0000000000604137                 db 0ECh
.data:0000000000604138                 db  12h
.data:0000000000604139                 db 0D4h
.data:000000000060413A                 db 0AFh
.data:000000000060413B                 db    5
.data:000000000060413C                 db  12h
.data:000000000060413D                 db 0D5h
```

[그림 1] 가상화된 코드



[그림 2] 가상 CPU

4.2 가상화 난독화 해제

main 함수에서 func 함수를 호출하는 루틴을 보면 2개의 인자를 전달한다는 것을 알 수 있다. 본 실험에서는 Triton[6] 도구를 이용해 인자로 전달하는 두 변수를 기호로 설정하고 기호 실행을 수행하였다. 기호 실행 결과 생성된 연산식의 일부는 [그림 3]과 같다.

```
ref_20699 = (ref_20697 ^ ref_20693) # XOR operation
ref_18705 = ref_18578 # MOV operation
ref_18578 = sx(0x20, (ref_12876 & 0xFFFFFFFF)) # MOVSXD operation
ref_18707 = (ref_18705 & 0xFFFFFFFF) # MOV operation
ref_276 = ((ref_270 >> 24) & 0xFF) # Byte reference - MOV operation
ref_277 = ((ref_270 >> 16) & 0xFF) # Byte reference - MOV operation
ref_278 = ((ref_270 >> 8) & 0xFF) # Byte reference - MOV operation
ref_279 = (ref_270 & 0xFF) # Byte reference - MOV operation
```

[그림 3] 기호실행을 이용해 추출한 동작 일부

이렇게 생성한 Symbolic Expression을 Triron을 이용해 LLVM-IR로 변환한 결과의 일부는 [표 3]과 같다[7],[9].

```
%".137" = xor i64 %".72", %".136"
%".138" = trunc i64 %".137" to i32
%".139" = zext i32 %".138" to i64
%".140" = trunc i64 %".139" to i32
%".141" = trunc i32 %".140" to i8
```

[표 3] 추출한 동작을 LLVM-IR로 변환한 결과 일부

이렇게 추출한 LLVM-IR을 최적화 옵션과 함께 컴파일한 결과 [그림 4]와 같이 가상화 난독화가 해제된 기계어 코드를 획득할 수 있었다.

```
        deobfuscated    proc near
31 F7                   xor     edi, esi
48 89 F8                mov     rax, rdi
C3                      retn
        deobfuscated    endp
```

[그림 4] 가상화 난독화가 해제된 기계어 코드

마지막으로 난독화가 해제된 실행 파일을 생성하기 위해 원본 실행파일의 헤더 정보를 조작하여 섹션을 추가하고, [그림 5]와 같이 해당 섹션에 난독화가 해제된 기계어 코드를 삽입하였다.

```
; Segment type: Pure code
; Segment permissions: Read/Write/Execut
_deobfuscated   segment byte public 'COD
                assume cs:_deobfuscated
                ;org 40420Ch
                assume es:nothing, ss:no

; ================ S U B R O U T I N E ==


sub_40420C      proc near
                xor     edi, esi
                mov     rax, rdi
                retn
sub_40420C      endp

_deobfuscated   ends
```

[그림 5] 가상화 난독화가 해제된 코드를 원본 실행파일에 삽입한 결과

이후 [그림 6]과 같이 가상화 난독화된 함수를 호출하는 코드를 난독화 해제된 함수를 호출하도록 변조하였다.

```
mov     edi, [rbp+var_8]
mov     esi, [rbp+var_C]
mov     [rbp+var_1C], eax
call    sub_40420C
mov     rdi, offset aResultD ; "result: %d\n"
mov     esi, eax
mov     al, 0
call    _printf
```

[그림 6] 난독화가 해제된 함수를 호출하는 코드

V. 결론

본 논문에서는 가상화 난독화된 코드가 연산을 수행하는 메모리를 기호로 설정해 기호 실행을 수행한 후, 수집된 연산식을 LLVM-IR로 변환하여 최적화 옵션과 함께 컴파일 하는 방식의 분석 방식[9]을 소개하였고, 가상화가 해제된 실행파일을 얻기 위해 원본 실행파일에 섹션을 추가하여 가상화 난독화가 해제된 기계어 코드를 삽입한 뒤, 코드를 후킹하여 가상화 난독화가 해제된 함수를 호출하는 방식을 제안하였다. 또한 이러한 방식을 이용해 자동으로 가상화 난독화가 해제된 실행 파일을 생성하는 프로그램을 구현하고, 본 프로그램을 통해 실제로 가상화 난독화가 해제된 결과를 확인하였다.

하지만 본 논문에서 소개한 가상화 난독화 해제 방식은 기호로 설정된 메모리에 대한 연산만을 추출하기 때문에 특정 메모리에 대한 동작만을 복원할 수 있다는 한계점을 지니고 있다.

향후 이러한 한계점을 개선하기 위한 연구가 진행되면 가상화 난독화된 코드를 더욱 정확하게 분석할 수 있게 되어 가상화 난독화가 적용된 악성코드에 더욱 효과적으로 대응할 수 있을 것이라 기대된다.

[참고문헌]

[1] 최석우, “난독화 바이너리 분석 방안”, 정보과학회지, 제 36권, 제3호, 26p-31p, 3, 2018

[2]James C. King, "Symbolic execution and program testing", Communications of the ACM, ACM New York, NY, USA, 385p-394p, 1976

[3] Igor V. Popov, Saumya K. Debray, Gregory R. Andrews, “Binary Obfuscation Using Signals”, 16th USENIX Security Symposium, Tucson, AZ 85721, USA, 275p-290p 2007

[4] The LLVM Complier Infrastructure, “LLVM”, https://llvm.org

[5] Wikipedia, “Satisfiability modulo theories”, https://en.wikipedia.org

[6] Triton - A DBA Framework, “Triton”, https://triton.quarkslab.com

[7] C. Lattner and V. Adve, “LLVM: A compilation framework for lifelong program analysis & transformation.” in the international symposium on Code generation and optimization(CGO), IEEE Computer Society Washington, DC, USA, 75p 2004.

[8] Kevin Lawton, “Running multiple operating systems concurrently on an IA32 PC using virtualization techniques”, 1999.

[9] Jonathan Salwan, Sébastien Bardin and Marie-Laure Potet, “Désobfuscation binaire : Reconstruction de fonctions virtualisées”, SSTIC 2017

[10] 홍대영, 고원석, 임성수, “보안과 신뢰성있는 컴퓨팅을 위한 가상화 기술, 정보과학회지, 26, 10, 50p-57p, 10, 2008

[11] Pascal Junod, Julien Rinaldini, Johan Wehrli and Julie Michielin, “Obfuscator-LLVM – Software Protection for the Masses“, IEEE/ACM 1st International Workshop on Software Protection, 5, 2015

Shannon 엔트로피 값 분석을 통한 파일 암호화 판별에 관한 연구

고주성*, 곽진**

*아주대학교 컴퓨터공학과 정보보호응용및보증연구실

**아주대학교 사이버보안학과

Determining File Encryption Status through Shannon Entropy Criteria Analysis

Ju-Seong Ko*, Jin Kwak**

*ISAA Lab., Department of Computer Engineering, Ajou University.

**Department of Cyber Security, Ajou University.

요 약

최근 안드로이드 환경에서 랜섬웨어로 인한 피해를 방지하기 위해 악의적인 앱의 암호화 동작을 실시간으로 탐지할 수 있는 방안에 대한 연구가 진행되고 있다. 암호화 동작을 실시간으로 탐지하기 위한 방안 중 하나는 파일의 암호화 여부를 실시간 모니터링하는 것으로 암호화 여부 판단을 위해 shannon 엔트로피 값을 이용할 수 있다. 하지만 shannon 엔트로피를 이용한 기존 연구에서는 엔트로피 값의 기준을 명확히 하지 않아 실제 환경에서 적용은 어려운 실정이다. 따라서 본 논문에서는 다양한 파일 종류 별 shannon 엔트로피 값 기준을 제시하여 파일 암호화 여부 판별의 정확성을 높이고자 한다.

I. 서론

사용자의 중요 데이터를 암호화한 후 이를 이용해 이득을 취하는 랜섬웨어는 2015년 4월 광범위하게 유포되기 시작하였고, 전 세계적으로 많은 피해를 발생시켰다[1]. 한국인터넷진흥원은 2017년 분기별 악성코드들 중 랜섬웨어가 모든 분기에서 가장 높은 발생 수를 기록했다고 분석하였으며, 해당 수치에는 안드로이드 기기를 대상으로 한 공격도 포함되었다[2].

랜섬웨어에 감염되어 데이터가 암호화된 경우 이를 복구하기 어렵기 때문에 사전에 예방할 수 있는 방안이 필요하다. 이를 위해 안드로이드 환경에서 랜섬웨어 앱을 실시간 탐지해낼 수 있는 방안에 대한 연구가 활발히 진행 중이다[1].

Jing Chen 등의 연구[3]에서는 특정 앱이 기기 내의 데이터를 암호화할 때 사용자가 암호화 행동을 인지하고 있는지, 그리고 암호화로 인해 발생하는 결과를 파악하고 있는지의 여부로 랜섬웨어 앱과 정상 암호화 기능 앱을 구분하고 있다.

해당 논문에서 제시한 과정 중 첫 단계에서는 보호되어야 할 파일들을 모니터링 대상으로 정의하고, 파일의 엔트로피 값을 측정하여 해당 파일이 암호화되었는지의 여부를 판단한다[4]. 하지만 안드로이드 기기 내에 보호되어야 할 파일의 종류는 다양하기 때문에 암호화 여부의 기준이 될 엔트로피 값을 파일의 종류에 따라 다르게 설정해야 할 필요가 있다.

본 논문의 2장에서는 랜섬웨어 앱 실시간 탐지 방안, 랜섬웨어와 관련된 정보, 그리고 엔트로피 값 측정을 위한 관련 연구를 다룬다. 3장에서는 측정을 위해 구현한 시스템에 대해 설명하며, 4장에서는 측정 결과 분석을 통해 파일 종류별 기준 값을 제시한다. 마지막으로 5장에서는 향후 연구에 대해 언급하며 결론을 맺는다.

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2017R1E1A1A01075110).

II. 관련 연구

2.1 랜섬웨어 앱 실시간 탐지 방안

Jing Chen 등의 연구[3]에서는 정상 암호화 기능 앱과 랜섬웨어 앱을 구분하기 위해 현재 수행 중인 암호화 과정을 사용자가 인지하고 있는지 판단한다. 이 판단을 위해 3단계의 분석 과정을 거치는데, 3단계의 내용은 [표 1]과 같다.

[표 1] 랜섬웨어 앱 실시간 탐지 방안 단계

단계	분석 내용
1	모니터링 대상 데이터의 암호화 여부
2	사용자의 암호화 기능 인지 여부
3	사용자와 암호화 앱의 상호작용 여부

단계 1에서는 모니터링 중인 데이터가 암호화된 파일인지를 판단한다. 이를 위해 shannon 엔트로피를 이용하는데, 데이터의 엔트로피 값이 높아질 경우 암호화된 것으로 판단하고 다음 단계를 시작하게 된다[3].

2.2 shannon 엔트로피

shannon 엔트로피는 데이터 파일 내 값들의 분포를 이용해 암호화 여부를 판단한다. 암호문 내의 값들은 평문에 비해 균등한 분포를 가진다는 점을 이용해 특정 파일이 암호화되었는지 판단한다. 이는 암호화 과정에서 발생하는 혼돈 효과를 이용한 것이다. 엔트로피 값 e는 다음과 같이 계산할 수 있다[4].

$$e = \sum_{i=0}^{255} P_{B_i} \log_2 \frac{1}{P_{B_i}}, \quad P_{B_i} = \frac{F_i}{total bytes}$$

(F_i는 파일 내 값 i의 개수, total bytes는 파일의 크기)

파일 내의 값 분포가 0x00부터 0xFF까지 모두 균등한 경우, e는 최대값인 8이 된다.

2.3 랜섬웨어에서 사용되는 암호 알고리즘

2017년 1월, 기존 윈도우용 킬디스크 악성코드의 변종인 리눅스용 킬디스크가 발견되었다. 파일 암호화 방식은 윈도우에서 AES와 RSA를 이용했던 점과 달리 리눅스에서는 Triple-DES 방식을 이용하였다[5].

2017년 5월, 전 세계에서 워너크립터 랜섬웨어의 감염 사례가 보고되었다. 랜덤으로 생성한 AES 키를 이용해 AES_128 CBC 방식으로 데이터를 암호화한 후 RSA 공개키로 AES 키를 암호화하는 방식을 이용하였다[6]. AES_128 CBC 방식은 인코더 랜섬웨어에서도 사용되었다[5].

2017년 5월, 재프 랜섬웨어가 네커스 봇넷을 이용한 스팸 메일을 통해 국내에 급속도로 유포되고 있는 정황이 포착되었다. API를 이용해 랜덤한 키를 생성하였고, AES_256 CBC 방식으로 암호화하였다.

[표 2]는 주요 랜섬웨어 별로 사용한 암호 알고리즘을 정리한 것이다.

[표 2] 주요 랜섬웨어 별 암호 알고리즘

No	랜섬웨어 명	암호 알고리즘
1	킬디스크	Triple-DES CBC
2	워너크립터, 인코더	AES_128 CBC
3	재프	AES_256 CBC

2.4 랜섬웨어의 주요 타겟 파일

SOMANSA는 랜섬웨어가 문서 파일과 DB 파일이 존재하는 폴더를 암호화 대상으로 삼고 있으며, 시스템 폴더와 결제 유도에 사용되는 Tor 폴더들은 제외 대상으로 포함되었다고 분석하였다[8]. 또한 Nolen Scaife 등의 연구[4]에서는 랜섬웨어 앱들이 pdf, docx, pptx 등 문서 파일에 가장 많은 접근을 수행했다는 결과를 도출하였다.

2.5 CrypTool

CrypTool은 다양한 암호 알고리즘들을 직접 시연해볼 수 있는 오픈소스 프로젝트로 다양한 해시함수, 키 교환 프로토콜, 그리고 블록 및 공개키 암호 등 400개 이상의 알고리즘을 지원하고 있다. 알고리즘의 입력과 출력으로 문자열, 바이트 값, 파일 등 형태의 제한 없이 이용할 수 있다[9].

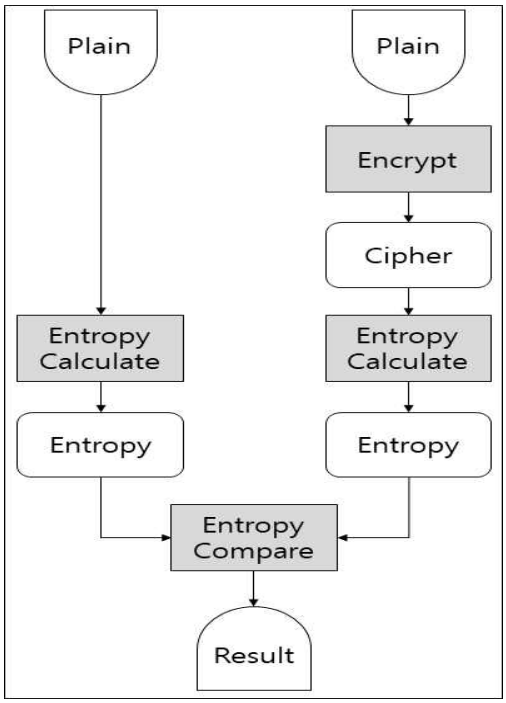
III. 측정 방안 및 구현

3.1 엔트로피 값 종류 별 기준의 필요성

Jing Chen 등의 연구[3] 중 단계 1에서는 모니터링 중인 데이터의 shannon 엔트로피 값이 높을 경우 암호화된 파일로 간주하였다. 하지만 엔트로피 값이 높다는 기준이 명확하지 않아 이에 대한 기준 설정이 필요하다. 또한 Nolen Scaife 등의 연구[4]에서는 파일들의 특성이 다르기 때문에, 파일 종류 별로 shannon 엔트로피 값을 형성하는 범위가 다르다는 것을 언급하였다.

따라서 파일 종류 별 암호화 전·후의 엔트로피 값 비교를 통해 암호화 여부를 판단할 수 있는 파일 종류 별 기준을 제시해야 한다.

3.2 측정 방안



(그림 1) 엔트로피 값 비교과정

랜섬웨어 앱이 많이 접근하는 문서 파일들을 대상으로 암호화 전·후의 엔트로피 값 비교를 수행한다. (그림 1)은 평문과 암호문의 엔트로피 값 비교를 위한 순서도를 나타낸 것이다. Encrypt와 Entropy Calculate에 관한 내용은 각각 3.3, 3.4절에서 구체적으로 다룬다.

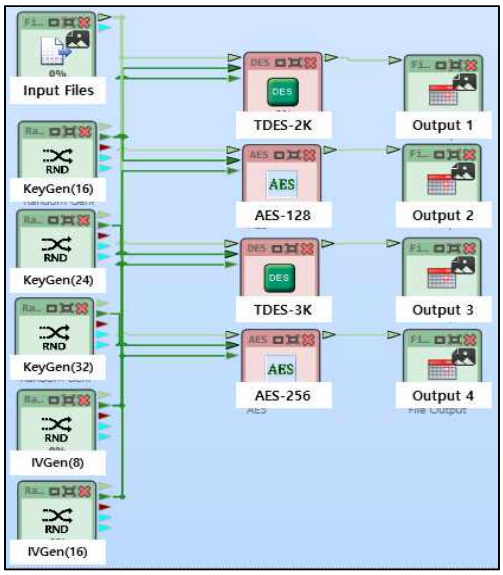
분석 대상 파일 종류는 pdf, pptx, docx, xlsx 총 4가지이며, 각 종류 별로 50개의 평문 데이터를 수집하였다. 비교에 이용할 암호 알고리즘은 랜섬웨어에서 주로 이용되었던 알고리즘들인 TDES-2K(Triple DES 2key), TDES-3K(Triple DES 3key), AES_128, AES_256 총 4가지로 수행하며 모두 CBC 모드를 이용한다.

[표 3]은 분석에 이용될 문서 파일, 암호 알고리즘 종류를 정리한 것이다.

[표 3] 분석 대상 파일 및 암호 알고리즘

항목	분석 대상
문서 파일	pdf, pptx, docx, xlsx
암호 알고리즘	TDES-2K, TDES-3K, AES-128, AES-256

3.3 암호화 수행



(그림 2) CrypTool을 이용한 암호화 구현

(그림 2)는 (그림 1)의 Encrypt 단계를 구체화한 것이다. CrypTool 2.1(stable)을 이용하였으며, 파일 종류 별 구분을 위해 (그림 2)와 같은 워크스페이스를 4개 만들었으며, 각 워크스페이스는 Input Files와 Output 외에 모두 동일한 조건을 가진다.

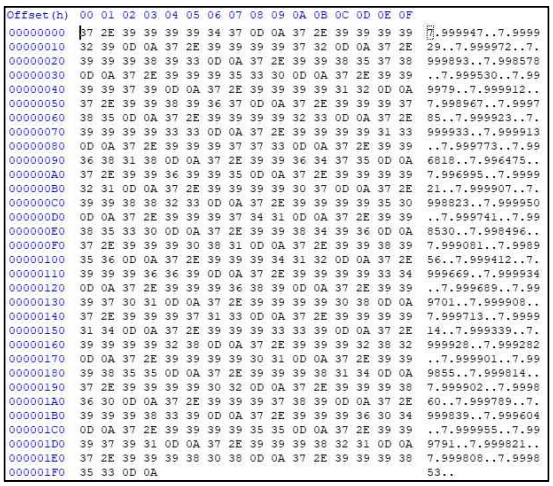
각 워크스페이스는 암호 알고리즘으로 TDES-2K, TDES-3K, AES-128, AES-256을 포함하고 있다. 암호 알고리즘의 입력으로는 Input Files, KeyGen(N), IVGen(N)을 가지는데

Input Files는 각 종류 별 50개의 파일, KeyGen(N)은 N-byte 크기의 키 생성, IVGen(N)은 N-byte 크기의 Initial Vector 생성을 의미한다. 암호 알고리즘의 출력으로는 Output이 있는데, 이는 각 대응되는 암호 알고리즘의 수행 결과인 암호문이다. [표 4]는 각 워크스페이스에 포함된 항목에 대한 설명을 정리한 것이다.

[표 4] 구현 항목 설명

구현 항목	수행 내용
Input Files	특정 종류에 속하는 파일 50개
Output N	대응되는 알고리즘의 암호문
KeyGen(N)	N-byte 크기의 키 생성
IVGen(N)	N-byte 크기의 IV 생성

3.4 엔트로피 계산 및 비교



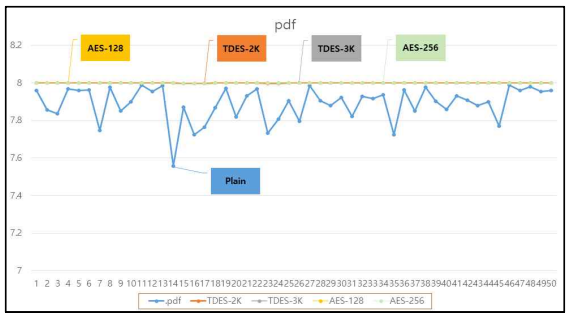
(그림 3) 엔트로피 계산 결과

(그림 3)은 (그림 1)의 Entropy Calculate를 수행한 예이다. Entropy Calculate는 2.2절의 수식을 구현함으로써 구체화할 수 있다. 각 파일 종류 별로 (그림 2)의 Input Files, Output 1-4에 해당하는 파일에 엔트로피 계산을 수행하기 때문에 총 5개의 엔트로피 값 결과 파일이 나오게 되며, 각 결과 파일에는 50개의 엔트로피 값이 포함된다.

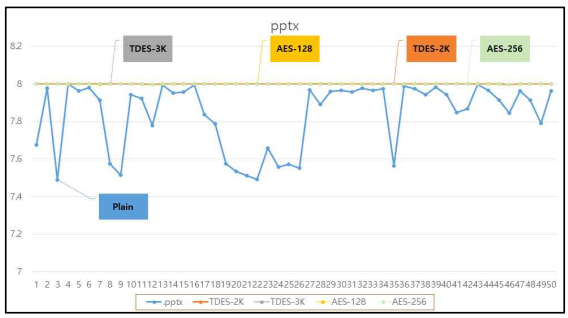
엔트로피 값 비교는 각 파일 종류 별로 평문 엔트로피 값과 4개의 암호문 엔트로피 값을 비교하여 수행한다.

IV. 수행 결과 및 기준 제시

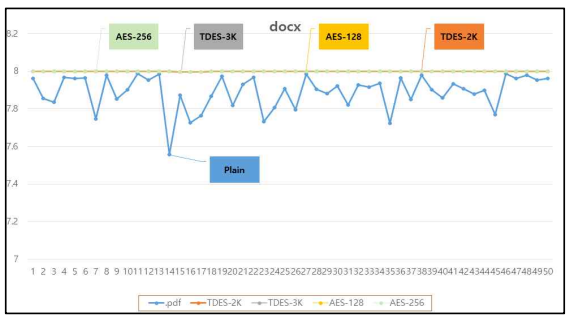
4.1 수행 결과 및 분석



(그림 4) pdf 대상 수행 결과



(그림 5) pptx 대상 수행 결과



(그림 6) docx 대상 수행 결과



(그림 7) xlsx 대상 수행 결과

(그림 4)-(그림 7)은 각각 pdf, pptx, docx, xlsx에 대한 엔트로피 값 비교 결과를 그래프로 나타낸 것으로 x축은 파일 번호, y축은 엔트로피 값이다. 위 결과를 분석한 정보는 다음 두 가지이다.

① 평문 - 평문 간 엔트로피 값 비교

4가지 수행 결과 모두 개별 파일에 따라 상이한 엔트로피 값을 가지지만, pdf와 pptx 파일은 대체적으로 높은 엔트로피 값을 가지는 것을 알 수 있다. 따라서 각 파일 종류 별로 개별적인 엔트로피 값 기준을 제시해야 한다.

② 평문 - 암호문 간 엔트로피 값 비교

4가지의 암호 알고리즘에서 모든 암호문의 엔트로피 값이 8에 근접하였음을 알 수 있다.

[표 5]는 파일 종류 별 엔트로피 최소/최대값을 정리한 것이다.

[표 5] 파일 종류 별 엔트로피 최소/최대값

분석 대상		최소값	최대값
pdf	Plain	7.557820	7.988754
	TDES-2K	7.995848	7.999979
	TDES-3K	7.996367	7.999981
	AES-128	7.996475	7.999979
	AES-256	7.996759	7.999977
pptx	Plain	7.489538	7.993521
	TDES-2K	7.997166	7.999985
	TDES-3K	7.996879	7.999985
	AES-128	7.997184	7.999984
	AES-256	7.997032	7.999985
docx	Plain	7.133540	7.911868
	TDES-2K	7.927723	7.999979
	TDES-3K	7.922660	7.999978
	AES-128	7.923519	7.999979
	AES-256	7.926397	7.999979
xlsx	Plain	7.038296	7.968575
	TDES-2K	7.983629	7.999924
	TDES-3K	7.981825	7.999927
	AES-128	7.981290	7.999928
	AES-256	7.982834	7.999934

4.2 엔트로피 값 기준 제시

실제 환경에서 암호화된 파일에 대해 어떤 암호 알고리즘으로 암호화되었는지는 알 수 없다. 따라서 평문 엔트로피의 최대값과 전체 암호문 엔트로피의 최소값을 비교하여 엔트로피 값 기준을 제시한다. [표 6]은 파일 별로 평문 엔트로피의 최대값, 암호문 엔트로피의 최소값을 비교하여 기준 값을 제시한 것이다.

[표 6] 엔트로피 값 비교 및 기준 제시

종류	평문 최대	암호문 최소	기준
pdf	7.988754	7.995848	7.99
pptx	7.993521	7.996879	7.996
docx	7.911868	7.922660	7.92
xlsx	7.968575	7.981290	7.98

위 기준을 적용한 예로, 한 pdf 파일의 엔트로피 값이 기준 값인 7.99보다 큰 경우에는 해당 파일이 암호화된 것으로 간주한다.

V. 결론

본 논문에서는 랜섬웨어 앱 실시간 탐지 방안에서 파일의 암호화 여부를 파악하기 위한 암호화 전·후의 shannon 엔트로피 값을 분석하였다. 파일 종류 별로 형성하고 있는 엔트로피 값이 다르기 때문에 종류 별로 기준이 주어져야 함을 확인하였고, 그에 따라 종류 별 기준을 제시하였다.

하지만 종류 별 수집 데이터 수는 50개씩으로 기준에 대한 정확성이 미흡할 수 있다. 또한 특정 파일들의 경우 암호화되지 않았음에도 기준 엔트로피보다 높은 엔트로피 값을 가질 수 있다.

따라서 향후 연구에서는 많은 수의 데이터 집합을 가지고, 특정 조건의 파일에 대해서도 적용할 수 있는 더 정확한 기준을 마련하고, 이를 랜섬웨어 앱 실시간 탐지에 적용할 수 있도록 해야 한다.

[참고문헌]

[1] 한국인터넷진흥원, "'16년 랜섬웨어 동향 및 '17년 전망", 2017.01.

[2] 한국인터넷진흥원, "2017년 4분기 사이버 위협 동향 보고서", 2018.01.

[3] Jing Chen, Chiheng Wang, Ziming Zhao, Kai Chen, Ruiying Du, Gail-Joon Ahn, "Uncovering the Face of Android Ransomware: Characterization and Real-Time Detection", IEEE Transaction on Information

Forensics and Security, Vol.13 No.5, 2017.12.

[4] Nolen Scaife, Henry Carter, Patrick Traynor, Kevin R.B. Butler, “CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data”, 2016 IEEE 36th International Conference on Distributed Computing Systems, 2016.06.

[5] 안랩 시큐리티대응센터(ASEC) 분석팀, “‘리눅스 랜섬웨어’ 본격화되나”, AhnLab 보안 이슈 게시판 “http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=26564”, 2017.07.

[6] 안랩 시큐리티대응센터(ASEC) 분석팀, “워너크립터 랜섬웨어 분석 보고서”, Analysis Report, 2017.05.

[7] 안랩 시큐리티대응센터(ASEC) 분석팀, “[VOL.87] 2017년 2분기 주요 보안 이슈”, ASEC 리포트, 2017.07.

[8] SOMANSA, “MALWARE ANALYSIS REPORT No.7 Cerber 랜섬웨어 분석보고서(Rig EK)”, 악성코드 리포트, 2016.12.

[9] https://www.cryptool.org/de/cryptool2

모바일에서의 애플리케이션 접근 제어 메커니즘 분석

김이진, 최형기*
성균관대학교

Analysis of Access Control Mechanism for Mobile Application

Ejin Kim, Hyoung-Kee Choi
Sungkyunkwan University

요 약

iOS 샌드박스란 iOS의 보안 메커니즘 중 하나로, 샌드박스에 대한 정책이 정의된 iOS 샌드박스 프로파일에 따라 애플리케이션의 동작을 제한한다. 본 연구에서는 샌드박스 프로파일을 분석하여 각 애플리케이션에 어떤 정책이 적용 되는가를 파악하고자 한다. 샌드박스 프로파일은 바이너리 형태로 변환되어 저장되며, iOS 버전에 따라 바이너리 샌드박스 프로파일의 구조가 달라진다. 버전에 따른 바이너리 샌드박스 프로파일에 대한 분석을 수행하여 추후 샌드박스의 안전성을 파악하는 연구에 활용하고자 한다.

I. 서론

iOS 샌드박스는 Apple 사에서 iOS의 보안을 위해 사용하는 메커니즘 중 하나로, iOS 샌드박스 프로파일에 명시된 정책에 따라 앱에 대한 접근 제어를 수행한다. 샌드박스와 샌드박스 프로파일을 분석하여 샌드박스를 우회하는 방안을 모색할 수 있으며, 샌드박스의 정책을 사전에 파악하여 점검함으로써 iOS의 보안을 향상시키기 위한 연구 또한 가능하다. 그러나 샌드박스 내부 구조 및 동작 방식에 대한 공식적인 문서가 존재하지 않아 샌드박스에 대한 이해와 지식이 부족하다. 바이너리 형식의 iOS 샌드박스 프로파일은 사람이 이해하기 쉬운 SBPL(Sandbox Profile Language) 형식으로 작성되어 내부적으로 처리가 용이한 바이너리 형식으로 컴파일 후, 파일 시스템 또는 커널에 저장된다. 그러나 바이너리 형식의 프로파일의 구조에 대해서도 공개된 자료가 거의 없어 iOS 관련 연구를 진행하는 데 많은 어려움이 존재한다.

본 연구에서는 iOS 8 이상 버전의 샌드박스 프로파일을 연구 대상으로 바이너리 형태의 샌드박스 프로파일의 구조 분석을 진행하였다. iOS 샌드박스 프로파일을 연구하기 위하여 개발된 샌드박스 프로파일 해석 도구인 Stefan Esser의 도구[1],[2]와 이를 발전시켜 개발된 SandBlaster[3],[4]를 통해 연구를 진행하였다.

* 교신저자(Corresponding author)

II. 배경 지식

1.1 iOS 샌드박스의 안전성

iOS 샌드박스는 Apple 사에서 iOS 앱에 대해 적용하는 보안 메커니즘 중 하나로, 앱이 사전에 정의된 정책 내에서만 동작하도록 제한하는 기술이다. iOS의 모든 앱은 샌드박스 내에 자신에게 허용된 사용자 데이터와 시스템

자원에만 접근이 가능하다. 특정 앱에 대한 공격이 성공하여도 자신에게 허용되지 않은 다른 앱의 사용자 데이터나 시스템 자원에는 접근이 허용되지 않는다. iOS 샌드박스를 사용할 경우, 특정 앱에 대한 공격이 성공해도 공격의 영향이 다른 앱에 전파되지 않아 공격에 대한 피해 범위를 공격당한 앱으로 축소시킬 수 있다는 장점을 가진다.

앱에 적용하고자 하는 샌드박스에 대한 정책이 정의되어 있는 파일을 샌드박스 프로파일(profile)이라고 한다. Apple 사에서 기본적으로 제공하는 대부분의 시스템 앱은 자신의 샌드박스 프로파일을 가지며, 각자의 프로파일에 정의된 정책 내에서 동작한다. 일부 시스템 앱과 모든 써드파티(third-party) 앱에는 디폴트(default) 샌드박스 프로파일인 컨테이너(container) 프로파일이 적용된다.

iOS 샌드박스는 iOS 앱에 대한 보안성을 크게 향상시키고 있으나, Apple 사에서 제공하는 샌드박스의 동작 방식이나 샌드박스 프로파일의 구조 등 샌드박스 내부에 대한 공식적인 자료는 미비한 상태이다. 따라서, Apple 사에서 샌드박스를 통해 앱에 어떤 정책을 적용하고 있는지를 파악할 필요가 있다. 샌드박스 프로파일에 샌드박스를 우회할 수 있는 결함이 존재하는지를 점검하여 추후에 발생할 수 있는 공격의 위협으로부터 iOS를 보다 안전하게 보고해야 한다. 특히, 써드파티 앱에 적용되는 컨테이너 프로파일의 안전성에 대한 검증은 필수적이다.

1.2 iOS 샌드박스 프로파일

샌드박스 프로파일은 SBPL(SandBox Profile Language) 형식으로 작성되는데, SBPL 형식은 사람이 쉽게 읽고 이해할 수 있는 구조로 이루어진다. SBPL 형식의 샌드박스 프로파일은 앱에 적용하고자 하는 정책을 표현하기 위해, 크게 operation, filter, decision 3가지 요소를 사용한다.

Operation은 프로세스에서 호출되는 시스템 콜(system call) 등에 대한 추상화된 동작으로, 파일을 읽어 들이는 file-read, 디렉터리 구조를

```
1 sandbox_profile
2     -> operation, decision
3             -> filter
4             -> filter
5             ...
6     -> operation, decision
7             -> filter
8             -> filter
9             ...
10
```

그림 1. iOS 샌드박스 프로파일 구조

파악할 수 있는 mach-lookup 등이 있다. operation은 조건문인 filter를 만족하는지에 따라 수행될 것인가에 대한 허용 여부가 결정되는데, 이러한 허용 여부를 나타낸 것이 decision이다. 앱이 수행하려는 동작이 filter를 만족하여 operation이 수행되는 것을 허용하고자 할 경우, decision은 허용 상태(allow)로 설정한다. 반대로, 앱이 수행하려는 동작이 filter를 만족하여 operation이 수행되는 것을 허용하지 않고자 할 경우, decision은 거부 상태(deny)로 설정한다.

Operation, decision, filter는 그림 1과 같이 구성된다. 하나의 앱은 제한하고 싶은 동작을 표현한 operation에 filter를 적용한다. 하나의 앱에는 여러 개의 operation에 대한 정책이 정의될 수 있다. 또한, 하나의 operation에 대해 다수의 filter가 적용될 수 있다.

iOS 샌드박스 프로파일은 사람이 쉽게 읽고 이해할 수 있는 SBPL 형식으로 작성되지만, 내부적으로 빠르게 처리하기 위하여 iOS 커널 내부에는 바이너리 형식으로 컴파일되어 저장된다. 그러나 바이너리 형태의 샌드박스 프로파일은 사람이 이해하기 어려운 형식으로 구성되어 분석하는 데 어려움이 존재한다. 샌드박스 프로파일을 분석하기 위해서는 바이너리 형식의 샌드박스 프로파일을 사람이 읽을 수 있는 형식으로 변환하는 디컴파일 과정이 필요하다.

1.3 관련 연구

추출된 바이너리 형태의 프로파일에 대한 디컴파일 도구를 개발하는 연구가 진행되고 있다. 2011년부터 시작된 연구를 기반으로 하여 이전 연구의 한계를 보완하는 방향으로 연구가

진행되고 있다. iOS 샌드박스 프로파일의 분석 도구로는 최초로 개발된 XNUSandbox를 시작으로, 2014년 공개된 Stefan Esser의 샌드박스 프로파일 분석 도구 및 2016년에 발표된 SandBlaster가 존재한다.

XNUSandbox[5],[6]는 2011년 최초로 iOS 샌드박스의 내부 구조를 파악하여 개발된 iOS 샌드박스 프로파일 분석 도구이다. iOS 4 버전 이후 펌웨어에 대하여 샌드박스 프로파일을 추출하여 사람이 이해하기 쉬운 형식으로의 변환을 제공한다. 그러나 iOS 샌드박스 프로파일을 디컴파일한 결과 정보가 SBPL 형식이 아닌 내부 데이터 구조로 표현된다는 한계를 지닌다. 또한, Apple 사가 iOS 7 이후부터 샌드박스 프로파일의 바이너리 형식을 변경함에 따라 최신 iOS 버전에서는 호환이 되지 않는다.

Stefan Esser가 개발한 샌드박스 프로파일 분석 도구[1],[2]는 XNUSandbox의 발전된 형태로, iOS 7 이후 버전에서 등장하는 새로운 바이너리 형태의 샌드박스 프로파일에 대한 디컴파일이 가능하다. 또한, 샌드박스 프로파일을 SBPL 형식에서 바이너리 형식으로 컴파일하는 기능을 제공한다. 그러나 추출한 바이너리 형식의 샌드박스 프로파일을 디컴파일한 결과는 SBPL 형식이 아닌 중간 언어(intermediate language)로 표현된다.

SandBlaster[3],[4]는 바이너리 형식의 iOS 샌드박스 프로파일을 사람이 이해할 수 있는 SBPL 형식으로 디컴파일하는 도구이다. iOS 7 이후 버전에 대해 iOS 샌드박스 프로파일 데이터를 추출하고, 추출한 프로파일을 SBPL 형태로 변환한다. SBPL 형태로의 변환을 통해 샌드박스의 보안에 대한 분석이 가능하다. 또한, 기존의 연구에서 지원하지 못했던 구 버전의 iOS와 최신 버전의 iOS에 대한 디컴파일을 수행한다.

III. iOS 샌드박스 프로파일 구조

바이너리 형식의 iOS 샌드박스 프로파일은 iOS 버전에 따라 다른 구조를 가진다. iOS 8 버전에서는 각 샌드박스 프로파일이 분리되어 저장되지만, iOS 9 이상 버전에서는 여러 샌드박스 프로파일이 하나의 구조로 번들(bundle)되어 저장된다.

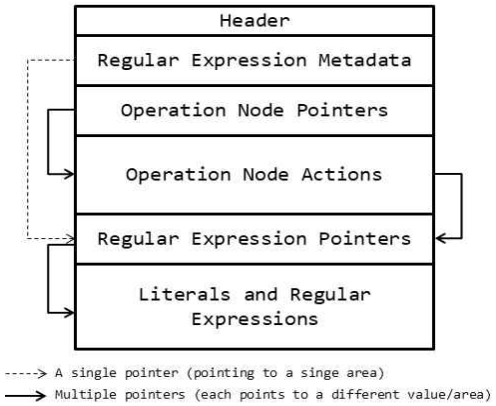


그림 2. iOS 8.0의 바이너리 샌드박스 프로파일

iOS 8 버전에 대한 샌드박스 프로파일은 iOS 8.0 버전을 기준으로, iOS 9 버전에 대한 샌드박스 프로파일 분석은 iOS 9.3.3 버전을 기준으로, iOS 10 이상 버전의 샌드박스 프로파일은 iOS 10.2 및 iOS 11.1 버전을 기준으로 분석을 진행하였다.

3.1 iOS 8 버전의 샌드박스 프로파일

iOS 8 버전의 샌드박스 프로파일은 그림 2와 같이 6개의 섹션으로 나누어진다.

헤더(header) 섹션에는 해당 바이너리 샌드박스 프로파일이 프로파일마다 분리된 형태인지, 모든 샌드박스 프로파일이 결합된 형태인지를 나타내는 플래그가 담겨 있다. 샌드박스 프로파일이 분리된 형태일 경우 플래그는 0x0000의 값을 가지며, 모든 샌드박스 프로파일이 결합된 형태일 경우 0x8000의 값을 가진다. iOS 8 버전의 경우, 모든 샌드박스 프로파일이 분리된 형태를 가지므로 헤더 섹션은 0x0000의 값을 가진다. iOS 8.0 버전을 기준으로 총 95개의 분리 형식 샌드박스 프로파일이 존재한다.

헤더 섹션 다음에 위치한 정규 표현식 메타데이터(Regular Expression Metadata) 섹션은 정규 표현식이 목록화되어 있는 테이블에 대한 오프셋이 담겨있다. 이 포인터는 정규 표현식 포인터(Regular Expression

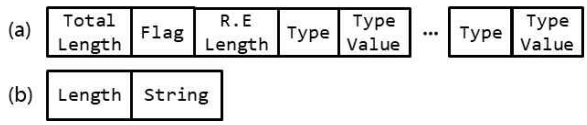


그림 3. 문자열 및 정규 표현식 섹션의 구조 (a) 정규 표현식이 저장되는 구조; (b) 문자열이 저장되는 구조.

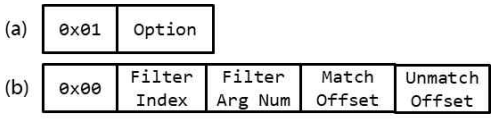


그림 4. Operation 노드의 구조 (a)터미널 노드; (b) 넌-터미널 노드.

Pointers) 섹션을 가리킨다. 또한, 정규 표현식 테이블의 크기가 명시되어 있는데, 이는 정규 표현식의 개수를 의미한다. 정규 표현식 메타데이터 섹션이 가리키는 정규 표현식 포인터 섹션에는 실제 정규 표현식에 대한 오프셋이 담겨 있다. 이는 정규 표현식 메타데이터 섹션에 명시된 테이블 크기인 정규 표현식의 개수만큼 존재한다.

실제 정규 표현식이 어떠한 형태로 저장되어 있는지는 문자열 및 정규 표현식 섹션에서 확인할 수 있다. 문자열 및 정규 표현식 (Literals and regular expressions) 섹션에는 다른 섹션에서 참조하여 사용하는 정규 표현식과 문자열이 존재한다.

먼저, 정규 표현식은 문자열이 가지는 패턴이나 규칙 등의 조건을 표현하기 위해 사용한다. 예를 들어, 특정 위치에서 숫자가 들어가야 하는 패턴을 정규식을 통해 나타낼 수 있다. 정규식은 그림 3의 (a)와 같은 구조로 문자열 및 정규 표현식 섹션에 저장된다. 정규 표현식은 바이너리 시리얼라이제이션(binary serialization)된 형식으로 저장된다. iOS 내부에서 정규 표현식을 사용할 때 처리를 위해 파싱을 수행해야 하는데, 이것을 사람이 사용하는 정규 표현식의 형태 그대로 저장해 놓으면 사용할 때마다 파싱을 해주어야 한다. 따라서 미리 처리하기 용이한 형태로 파싱하여 저장하는 것이다. 즉, 사람이 읽을 수 있는 형태의 정규 표현식을 iOS 내부에서 빠르게 처리할 수 있도록 타입(type)과 타입 값(type value) 형식으로 인코딩하여, 타입 뒤에 저장되어 있는 타입 값을 어떻게 처리할지 결정한다.

문자열은 변경 없이 그대로 사용하는 값이기 때문에 별도의 파싱 과정이 필요하지 않아, 저장 시에도 문자열을 그대로 저장하여 사용한다. 문자열은 그림 3의 (b)와 같은 구조로 문자열 및 정규 표현식 섹션에 저장된다.

Operation 노드 포인터 섹션은 각 operation 노드에 대한 오프셋을 담고 있는 포인터이다. Operation 노드는 각 operation에 적용할 filter와 decision을 나타낸다. operation 노드는 두 종류로 나누어진다. 첫 번째는 operation에 대한 decision을 나타내는 노드인 터미널 노드(terminal node)이다. 터미널 노드의 구조는 그림 4의 (a)와 같다. 터미널 노드를 나타내는 플래그는 0x01이며, 터미널 노드는 해당 operation을 허용할지 거부할지에 대해 decision 옵션(decision option)에 따라 결정된다. decision 옵션의 마지막 비트가 0이면 해당 operation에 대한 허용을 나타내며, 마지막 비트가 1이면 해당 operation에 대한 거부를 나타낸다. 두 번째는 operation에 적용할 filter를 나타내는 넌-터미널 노드(non-terminal node)이다. 넌-터미널 노드의 구조는 그림 4의 (b)와 같다. 넌-터미널 노드의 플래그는 0x00이다. 플래그 다음으로 filter 타입(filter type)과 filter 인자(filter argument)가 저장된다. 저장된 filter 타입에 따라 어떤 filter를 적용할 것인지가 결정되며, filter 인자에 따라 filter의 상세 규칙이 결정된다.

Operation 노드 섹션은 다수의 operation 노드로 구성되어 있다. filter를 만족하는지 여부에 따라 operation 노드로 이동할지가 결정되는데, 만족할 경우 일치 노드 오프셋(match node offset), 아닐 경우 불일치 노드 오프셋(unmatch node offset)에 따라 이동한다. 한 operation은 여러 operation 노드를 지날 수 있는데, 이는 한 operation에 여러 filter가 적용됨을 의미한다. 최종적으로 터미널 노드에

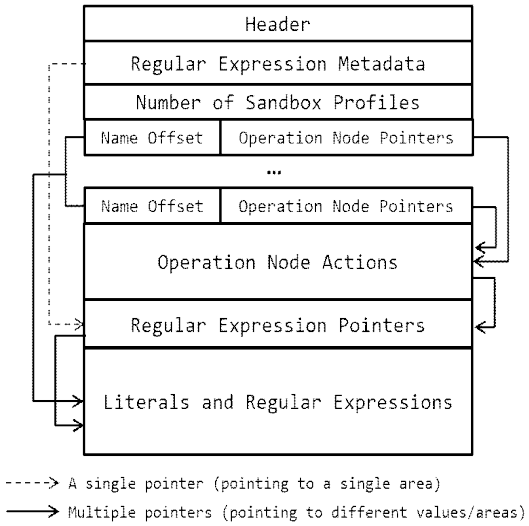


그림 5. iOS 9의 결합 형식 바이너리 프로파일

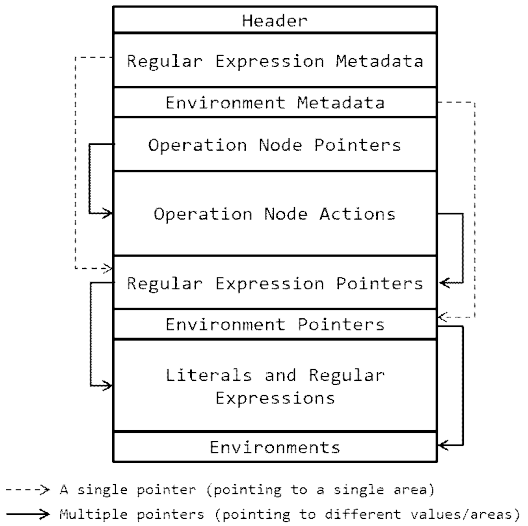


그림 6. iOS 10 이상의 분리 형식 바이너리 프로파일

도달하면 지금까지의 조건에 따라 해당 operation을 허용할지 거부할지가 결정된다.

3.2 iOS 9 버전의 샌드박스 프로파일

iOS 9 버전의 샌드박스 프로파일은 분리 형식의 바이너리 프로파일과 결합 형식의 바이너리 프로파일이 존재한다. 분리 형식의 바이너리 프로파일은 iOS 8 버전과 같은 형태를 가지며, 결합 형식의 바이너리 프로파일은 그림 5와 같이 나타낼 수 있다.

분리 형식의 바이너리 프로파일의 개수는 한 개로, 플랫폼에 대한 샌드박스 프로파일로 정의된다. 결합 형식의 바이너리 프로파일은 iOS 9.3.3 버전을 기준으로 총 121개의 프로파일이 하나의 프로파일로 존재한다.

헤더 섹션, 정규 표현식 메타데이터 섹션, 정규 표현식 포인터 섹션, 문자열 및 정규 표현식 섹션은 iOS 8 버전의 샌드박스 프로파일과 동일한 구조를 가진다. iOS 8 버전에서 분리 형식으로 존재하던 샌드박스 프로파일을 결합 형식으로 하나의 구조로 구성하기 위하여 operation 노드 포인터 섹션을 각 샌드박스 프로파일에 따라 프로파일 이름 섹션으로 분리한다.

3.3 iOS 10 이상 버전의 샌드박스 프로파일

iOS 10 이상 버전의 샌드박스 프로파일은

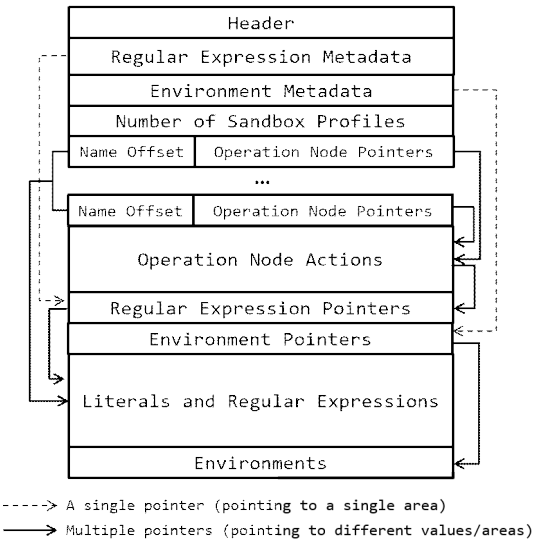


그림 7. iOS 10 이상의 결합 형식 바이너리 프로파일

그림 6, 7과 같이 나타낼 수 있다. iOS 10 버전에 새롭게 추가된 환경변수(environment) 관련 섹션인 환경변수 메타데이터(Environment Metadata) 섹션, 환경변수 포인터(Environment Pointers) 섹션, 환경변수(Environments) 섹션 이외에는 iOS 9 버전과 동일한 구조를 가진다.

환경변수란 ${HOME}과 같이 디렉터리의 경로를 저장하는 변수이다. 환경변수는 filter 매개변수로 참조되는 문자열에서 사용되는데, 별도의 처리 없이 문자열 그대로 저장하던 iOS 9 버전과 달리 환경변수 테이블을 구성하여 테이블을 참조하는 형태로 사용된다. 문자열에 반복되는 환경변수가 중복으로 저장되는 것을

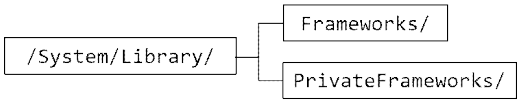


그림 8. 트리 형태로 저장되는 문자열

차단하여 저장 용량을 축소시킬 수 있다.

환경변수는 정규 표현식과 비슷한 형태로 관리된다. 환경변수 메타데이터 섹션에는 환경변수의 테이블 위치와 환경변수의 개수가 담겨있다. 환경변수 테이블은 환경변수 포인터 섹션에 위치하는데, 이 섹션에서는 실제 환경변수의 위치를 테이블 형태로 저장하여 가리킨다. 이 테이블은 환경 변수 메타데이터 섹션에 담겨있는 환경변수의 개수만큼의 환경변수를 담고 있다. 실제 환경변수는 환경변수 섹션에 존재한다. 환경변수는 문자열에서 환경변수 테이블의 인덱스를 통해 호출하는 형태로 사용된다. iOS 10 버전에는 ${HOME}, ${FRONT_USER_HOME}라는 총 2개의 환경변수가 존재한다.

정규 표현식은 이전 버전과 같은 형태이나, 문자열의 저장 방식은 크게 변경되었다. 중복되는 문자열에 대해 트리 구조의 형태로 저장하는 방식을 사용한다. 한 operation에 여러 문자열 filter가 적용될 때, 반복적으로 사용되는 문자열을 줄이기 위하여 중복되는 문자열을 트리 형태로 시리얼라이제이션하여 저장한다. 트리 구조 형태의 문자열 저장 방식은 그림 8과 같이 추상화하여 나타낼 수 있다. literal filter에서 /System/Library/ 구문이 반복될 경우, 반복되는 구문은 한번만 저장하고 다음 레벨에 Framework/와 PrivateFramework/를 배치하여 저장 용량을 최소화한다.

IV. 결론

본 논문에서는 iOS의 강력한 보안 메커니즘 중 하나인 샌드박스의 보안성을 점검하기 위한 사전 연구로써 샌드박스 프로파일의 구조를 분석하는 연구를 진행하였다. iOS 샌드박스 프로파일은 버전에 따라 다른 구조를 가지며, 데이터를 효율적으로 저장하는 방식으로 점차 발전하고 있음을 파악할 수 있다.

ACKNOWLEDGMENT

이 논문은 2016년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No.2016R1D1A1B03936211).

[참고문헌]

[1] Stefan Esser, "iOS 8: Containers, Sandboxes and Entitlements", Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016.

[2] sandbox_toolkit [Online]. Available: https://github.com/sektioneins/sandbox_toolkit, Accessed on: May 2018.

[3] Ravan Deaconescu and, *et al.*, "SandBlaster: Reversing the Apple Sandbox", Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016.

[4] SandBlaster:Reversing the Apple Sandbox [Online]. Available: https://github.com/malus-security/sandblaster, Accessed on: May 2018.

[5] The Apple Sandbox [Online]. Available: https://media.blackhat.com/bh-dc-11/Blazakis/BlackHat_DC_2011_Blazakis_Apple%20Sandbox-Slides.pdf, Accessed on: May 2018.

[6] XNU Sandbox [Online]. Available: https://github.com/dionthegod/XNUSandbox, Accessed on: May 2018.

[7] Luke Deshotels and et al., "SandScout: Automatic Detection of Flaws in iOS Sandbox Profiles", ACM SIGSAC Conference on Computer and Communications Security (ACM CCS), 2016.

2018 한국정보보호학회 하계학술대회

A7 개인정보보호

신 상 욱 (중부대학교)

- **모바일 앱 개인정보 유출과 최신 TLS 적용 필요성 연구**
  김성진, 허준범
- **양자 컴퓨팅 환경에 안전한 생체 인증**
  우 주, 이동훈
- **개인정보의 비식별 처리 시 발생가능한 문제점 분석 및 대응방안 제시**
  한경수, 류지민, 서정택
- **Mixnet 적용을 통한 자율주행차 운영환경 프라이버시 보호방안 연구**
  강기완, 서정택

모바일 앱 개인정보 유출과 최신 TLS 적용 필요성 연구

김성진* 허준범**

*고려대학교 컴퓨터정보통신대학원 **컴퓨터학과

Mobile App Personal Information Leak Research on the Necessity of Applying the latest TLS

Sung-Jin Kim* Junbeom Hur**

*Graduate school of Computer and Information Technology,

**Department of Computer Science and Engineering

Korea University

요 약

최근 스마트폰 사용률이 데스크톱PC와 노트북 등 사용률보다 훨씬 높게 나타나며, 일상생활을 편리하게 해주는 모바일 어플리케이션(이하 앱)의 사용이 계속해서 증가되는 실정이다. 하지만, 휴대성과 편리성을 제공해주는 모바일 앱의 사용으로 인한 개인정보 데이터 유출이 심각한 상황이다. 본 논문은 500만명(국민 10%) 이상 이용하고 있는 멤버쉽(포인트)앱의 개인정보 유출 패킷 데이터를 분석하고, 모바일 앱에 최신 TLS(Transport Layer Security) 암호화 프로토콜의 적용 필요성을 제안한다.

I. 서론

지난 구글 발표에 의하면 한국인 스마트폰 사용률은 91%로 데스크톱 PC와 노트북 등 컴퓨터 사용률 73%보다 훨씬 높은 것으로 나타났다. 대한민국 스마트폰 사용자 평균 53개의 앱을 단말기에 설치하였고, 이 수치는 아시아·태평양 국가 중 앱 설치 갯수가 가장 많았다[1]. 하지만, 모바일 앱의 다양성·휴대성·편리성을 제공해주었으나, 개인정보 데이터 유출이라는 심각한 보안 취약성을 가지고 있다. 이에 본 논문에서는 국내 500만명(국민 10%) 이상 사용하는 멤버쉽·포인트 모바일 앱의 개인정보 유출 데이터 패킷을 분석하고, 앱 사용만으로 제3자가 데이터를 스니핑(Sniffing) 할 수 있다는 것을 증명해보고자 한다. 앱 분석을 통한 개인정보 데이터 유출의 심각성을 살펴보면서, 최신TLS(Transport Layer Security) 암호화 프로토콜 적용의 중요성과 필요성에 대해 제안한다.

II. SSL/TLS

SSL/TLS는 웹사이트와 모바일 어플리케이션(이하 앱)에서 가장 널리 사용되고 있는 보안 서비스로 미국 Netscape사가 웹 브라우저와 웹 서버 간의 암호화된 정보 송수신을 위해 개발한 프로토콜을 말한다. 서버와 클라이언트의 진위여부를 조사하여 사이버 공간에서의 정보전달을 안전하게 만드는 역할을 하는 통신규약이며, HTTP뿐만 아니라 파일 전송 규약(FTP) 등 다른 TCP/IP 계층의 모바일 앱에도 적용이 가능하다는 장점을 지니고 있다. 하지만 낮은 버전에서는 수많은 취약점이 발견되었으므로 최신버전을 사용해야 한다[2][3]. TLS(Transport Layer Security)는 인터넷 표준으로서 상업적 프로토콜인 안전한 소켓 계층인 SSL(Secure Sockets Layer)에서 버전이 올라가며 진화되었다. 현재 최신 버전은 1.2로 RFC 5246에 정의되고 있으며[4], 차기버전 TLS 1.3은 최종 비준 마무리 단계에 있다.

III. 모바일 앱 분석

3.1 모바일 앱 선정

2017년에 만들어진 500만개의 스마트폰 앱 중에서 개인정보를 필요로 하는 멤버쉽·포인트앱을 선정하였다. 국내 500만명(국민 10%) 이상이 사용하는 앱 중에서도 가장 대중적으로 많이 사용하고 있는 H앱을 분석해보았다. H앱은 스마트폰을 소지하면 휴대성과 편리성 외 각종 할인혜택과 제휴 프렌차이즈 매장의 포인트를 적립하여 일정부분 쌓이면 언제 어디서나 사용할 수 있는 방식으로 많은 국민들이 애용하고 있다.

3.2 분석방법

노트북의 무선랜카드를 이용하여 무선AP(WIFI) 생성해주고, 스마트폰은 WIFI를 이용하여 모바일 앱을 사용하는 동안 노트북(제3자)에서 패킷을 캡쳐하여 분석하였다.

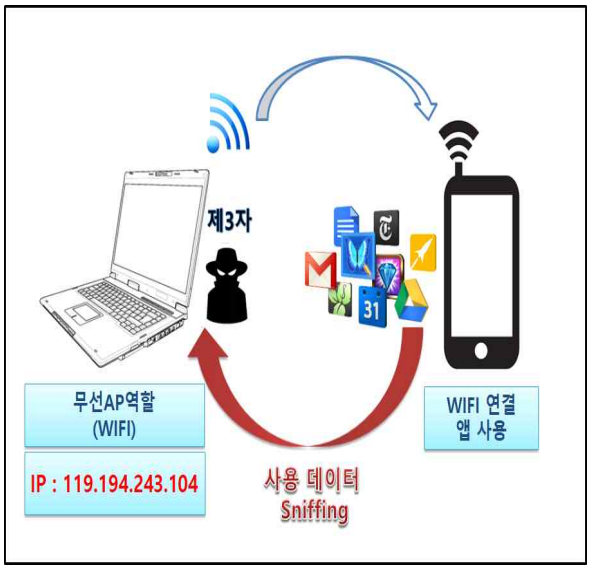


그림 1. 네트워크 구성환경
Fig. 1 Network configuration environment

① H앱 모바일 IP확인

대표적으로 사용하는 멤버쉽·포인트앱 중에서 H앱을 선택하고, 스마트폰 앱 사용시 메타 데이터를 저장하여 패킷 캡쳐 및 분석할 수 있는 툴을 활용하였다. 해당 앱의 아이피(IP :13.125.100.40)와 날짜, 패킷 데이터들이 캡쳐 되는 것을 확인 할 수 있다.

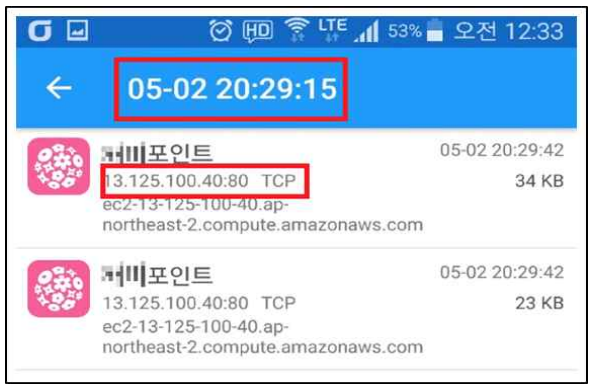


그림 2. H앱 IP확인
Fig. 2 H application IP verification

② 노트북에서 H앱 패킷확인

그림 3을 보게 되면, 무선 AP역할을 해주는 노트북(IP :119.194.243.104)에서 H앱(IP :13.125.100.40)의 패킷이 계속해서 캡쳐 되는 것을 볼 수 있다.

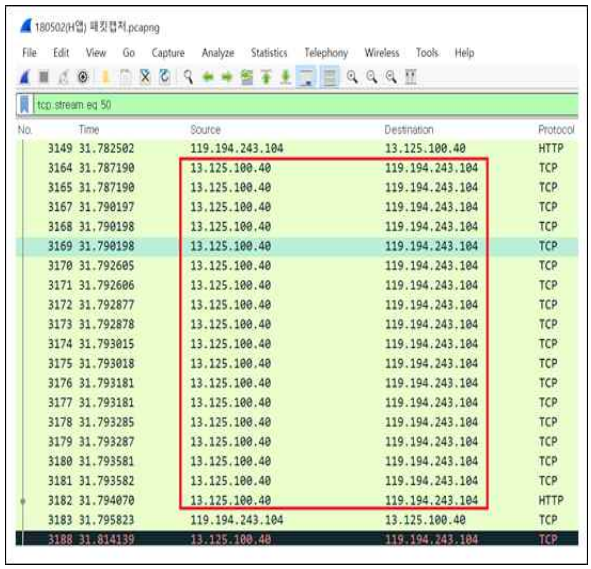


그림 3. H앱 패킷캡처
Fig. 3 H application paket capture

② H앱 개인정보 패킷 분석

그림 4의 첫 번째 H앱의 패킷을 확인해보면, 모바일에서 캡쳐 되었던 패킷과 같은 날짜를 확인할 수 있고, 어플리케이션의 이름 그리고 사용자의 안드로이드 OS버전과 단말기 기종이 유출되는 것을 볼 수 있다. 앱을 사용하는 사용자의 단말기 정보와 안드로이드 OS버전이 유출되는 것은 매월 버전마다 버그리포트가 실시간으로 올라오는 시점에서 상당한 취약성을 보인다[5].

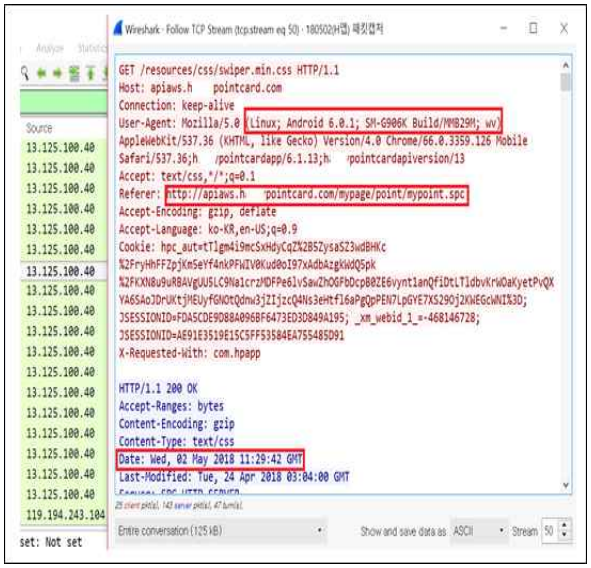


그림 4. H앱 패킷 TCP Stream(1)
Fig. 4 H application packet TCP Stream(1)

그림 5의 H앱의 두 번째 패킷을 살펴보면, 사용자의 정보 및 이력들을 살펴 볼 수 있다. ❶사용자 아이디 ❷사용자의 포인트 카드번호 ❸포인트 카드 사용 장소 ❹사용날짜 등을 알 수 있다.

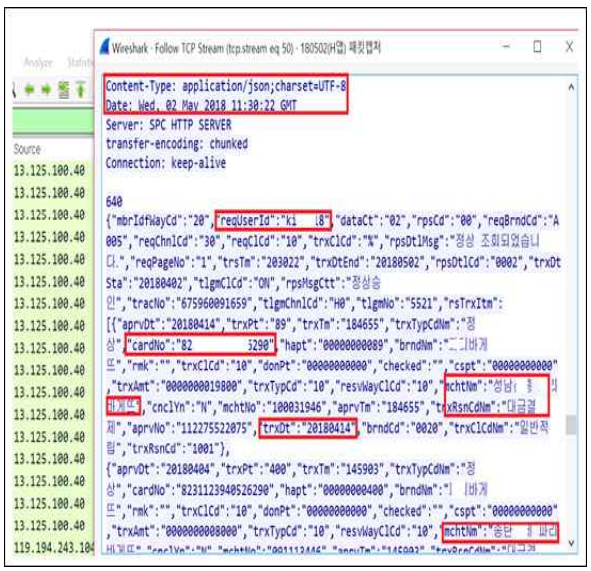


그림 5. H앱 패킷 TCP Stream(2)
Fig. 5 H application packet TCP Stream(2)

그림 6의 세 번째 H앱의 패킷을 확인해보면, 사용자의 개인정보 데이터가 모두 유출되는 것을 확인 할 수 있다. ❶생년월일 ❷사용자의 포인트 카드 번호 ❸사용자 아이디 ❹잔여 포인트 내역 ❺사용자 이름 ❻이메일주소 ❼휴대전화번호 ❽사용자 나이 등을 알 수 있다.

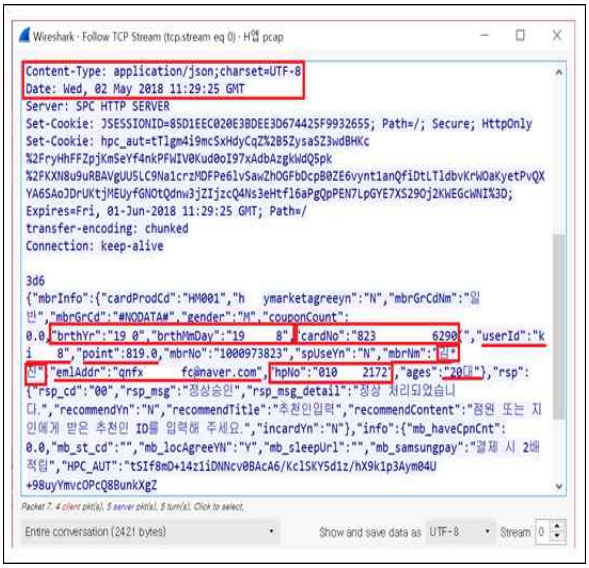


그림 6. H앱 패킷 TCP Stream(3)
Fig. 6 H application packet TCP Stream(3)

H앱과 더불어 국민들이 많이 사용하고 있는 C앱을 동일하게 패킷을 분석하여 표 1과 같이 비교해보면, C앱을 사용하는 사용자의 많은 개인정보 데이터가 유출 되는 것을 확인 할 수 있다.

앱 종류 / 유출목록	H앱	C앱
앱 이용자수	500만명이상	500만명이상
단말기 정보 (OS버전)	O	O
멤버십·포인트 카드번호	O	O
사용 장소내역	O	X
이름	△(부분유출)	O
성별	O	O
생년월일	O	△(부분유출)
전화번호	O	O
사용자 아이디	O	O
이메일 주소	O	O
잔여 포인트 내역	O	O

표1. H앱과 C앱 개인정보 유출비교
Table. 1 Compare H and C application privacy Leak

IV. 문제점 및 해결방안

4.1 개인정보 유출로 인한 문제점

표1과 같이 앱 사용만으로 개인정보가 유출 된다면 여러 가지로 큰 문제가 될 수 있다.

첫째, 유출된 전화번호, 생년월일, 카드번호 만으로도 현금처럼 사용하는 포인트를 제 3자가 사용할 수 있다는 점에서 금전적 손실이 발생할 수 있다.

둘째, 단말기정보(OS버전), 전화번호, 이메일주소 등 유출된 정보를 이용해 악성코드를 심은 문자와 이메일을 통해 스마트폰을 해킹할 수 있다는 점이다.

셋째, H앱 같은 경우 앱 사용할 때마다 사용자의 방문지점 및 매장명이 유출되고, 사용일시와 과거이력들이 유출되어 사생활 침해에 큰 문제로 작용 할 것으로 보인다.

4.2 해결방안

첫째, 스마트폰 사용자는 단말기의 최신 안드로이드 OS버전 업데이트가 필요하다. 낮은 안드로이드 버전의 사용자는 악성코드 감염 및 해킹에 취약하기 때문에 보안패치가 포함되는 안드로이드 OS 버전 업데이트는 필수적이다.

둘째, 스마트폰 사용시 공공장소 무료와이파이 사용에는 각별한 주의가 필요하며, 제공자가 불분명한 무선 공유기는 사용을 금지해야한다. 앞서 모바일 앱 분석에서 살펴보았듯이 공유기는 전파를 전송매체로 사용하기 때문에 패킷이 다른 통신기기에도 수신 될 수 있다. 해킹 당한 공유기를 이용할 경우 단말기의 사용자 데이터가 제3자에게 노출 될 수밖에 없다[6].

셋째, 앞서 소개했던 최신 TLS(Transport Layer Security) 암호화 프로토콜 적용이 필요하다. 패킷을 분석했던 H앱 같은 경우도 TLS가 적용은 되었지만, 암호화가 부분적으로 적용되어 많은 개인정보 데이터가 유출되었다. 개인정보를 활용하는 앱을 개발한다면, 최신 TLS 암호화 프로토콜 버전 적용과 그 안에서 활용되는 키 교환방식, 블록 암호화 방식, 블록 암호 운용방식, 메시지 인증 등을 엄격히 적용하여[7] 개인정보 데이터를 암호화함으로 앱 사용으로 인한 개인정보 유출 막아야 할 것이다.

V. 결론

본 논문에서는 국내 많은 사용자를 보유한 멤버쉽·포인트앱의 유출되는 개인정보 데이터 패킷을 분석하였다. 앱 사용만으로 제 3자에게 수많은 개인정보가 유출되는 것을 증명함으로써 최신버전 TLS 암호화 프로토콜의 적용 필요성과 중요성이 확인되었다.

향후 연구에서는 다양한 모바일 앱을 카테고리별로 분류하고 유출되는 개인정보 데이터 패킷을 분석함으로써 대한민국 국민의 개인정보와 사생활 보호를 위한 구체적인 모바일 앱 암호화 정책을 연구해보고자 한다.

[참고문헌]

[1] Mobile Apps in APAC: 2016 Report - Think with Google APAC, November, 2016

[2] MEYER, C., AND SCHWENK, J. SoK: Lessons Learned From SSL/TLS Attacks. In Proceedings of the 14th International Workshop on Information Security Applications (Berlin, Heidelberg, Aug. 2013), WISA 2013, Springer-Verlag.

[3] MONTHLY SOFTWARE ORIENTED SOCIETY 09, pp. 34-43, September, 2016

[4] RFC 5246, The Transport Layer Security(TLS) Protocol Version 1.2, Retrieved 16, Feb. 2015, http://tools.ietf.org/html/rfc5246

[5] Android Secrurity Bullentins - Android Open Source Project, 2018, https://source.android.com/security/bulletin

[6] Reddy, S. Vinjosh, et al. "Wireless hacking-a WiFi hack by cracking WEP," 2010 2nd International Conference on, vol. 1, pp. 189-193, 2010.

[7] K. Bhargavan, C. Fournet, M. Kohlweiss, A. Pironti, P.-Y. Strub, and S. Zanella-Beguelin, "Proving the TLS handshake secure (as it is)," in CRYPTO, 2014

양자 컴퓨팅 환경에 안전한 생체 인증 연구 동향*

우 주[1†] , 이동훈[1‡]

[1]고려대학교 정보보호대학원

A Research on Post-quantum Biometric Authentication

Joo Woo[1†] , Dong Hoon Lee[1‡]

[1]Graduate School of Information Security, Korea University

요 약

사용자 인증 수단으로 생체 정보의 이용이 늘고 있으며 생체 정보 기반 인증은 사용자가 어떠한 정보도 소유하거나 기억할 필요가 없으므로 매우 편리하다. 그러나 기존의 패스워드 기반 인증과 다르게 생체 정보는 추출할 때마다 측정 값이 달라지므로 인증 수행 시 허용 범위 내의 오차를 처리할 수 있어야하고 생체 정보가 고유성과 불변성을 갖기 때문에 한 번 노출되면 영구적으로 사용할 수 없게 되어 안전성을 위해 생체 정보의 개인 프라이버시 보호가 필수적이다. 또한 양자 컴퓨팅 환경에서 이산대수 문제와 인수 분해 문제가 풀리게 되면서 레티스와 코드 기반 등 다른 문제에 기반하는 많은 암호 시스템이 연구되고 있는데 생체 인증 또한 양자 알고리즘에 안전하게 설계되고 있는 추세이다. 본 논문에서는 양자 컴퓨팅 환경에 안전한 생체 정보 기반 인증 프로토콜들을 비교 분석하며 향후 연구 방향을 제시한다.

I. 서론

생체 인증(Biometric Authentication)은 사용자의 신원 확인을 위해 지문, 홍채, 얼굴, 음성 등 개인의 고유한 생체 정보를 이용하여 본인을 인증하는 차세대 개체 인증 방식 기술이다. IT 기술의 지속적인 발전과 보편화로 지문 인식과 안면 인식을 통한 휴대기기의 잠금 해제, 은행 업무를 비롯한 다양한 접근 제어 시스템의 보안 분야에서 생체 인증이 많이 활용되고 있다.

기존의 패스워드 기반 인증, OTP(one-time password) 기반 인증의 경우 아이디에 대한 패스워드를 사용자가 직접 기억하고 있거나 OTP 기기를 소유하고 있어야 하는 반면에, 생체 정보 기반 인증 방법은 사용자가 기억하거나 소유해야 하는 별도의 장치 없이 지문과 홍채 등 자신의 생체 정보를 이용하여 인증을 수행한다. 또한 기존의 인증 방법들에 비해 타인의 도용이나 복제가 어렵고 본인 상관성이 높으며, 사용이 편리하다는 장점을 가진다. 최근 대부분의 은행들은 좀 더 편하고 안전한 금융을 위해 생체 인증 기술을 모바일 뱅킹과 스마트 키오스크 등에 적용하고 있다.

그러나 패스워드와 다르게 생체 정보는 동일한 사용자에 대해서도 측정할 때마다 측정 값에 오차가 발생한다. 따라서 미리 설정된 오차 범위 내에 속하는 생체 데이터 값들은 같은 사용자로부터 측정된 생체 정보로 인식하는 인증 수행 방식이 필요하다.

또한 생체 정보의 고유성과 불변성으로 사용자 임의로 생체 데이터를 변경할 수 없으며, 한 번 노출되면 영구적으로 사용이 불가능하게 된다. 따라서 생체 정보의 안전성을 위해 개인 프라이버시 보호가 필수적이다. 이를 위해 다양한 암호학적

* 본 연구는 고려대 암호기술 특화연구센터(UD170109ED)를 통한 방위사업청과 국방과학연구소의 연구비 지원으로 수행되었습니다.

† 주저자, woojoo0121@korea.ac.kr

‡ 교신저자, donghlee@korea.ac.kr

도구로 생체 정보를 보호하여 인증을 수행한다.

기존의 많은 프리미티브들은 이산대수 문제와 인수분해 문제에 기반하여 설계되었는데 1994년 Shor가 제안한 양자알고리즘에 의해 두 문제가 다항 시간 이내에 풀리게 되면서 기존의 암호시스템은 양자 컴퓨팅 환경에서는 더이상 안전하지 않게 되었다. 이에 따라 암호화 기법, 서명, 키 교환 등 양자 알고리즘에 대한 저항성을 갖는 다양한 암호 시스템 연구가 최근 활발히 진행되고 있다. 양자 알고리즘에 안전한 생체 인증 기법 또한 설계되고 있는데 본 논문에서 살펴볼 생체 인증 프로토콜들은 양자 알고리즘에 안전하다고 알려져 있는 코드 기반 문제와 레티스 기반 문제에 기반하여 설계되었다.[2][3][4]

먼저, 코드 기반 문제는 정보 이론적 안전성(Information-theoretic security)을 갖는데 이는 이산 대수 문제나 인수 분해 문제같이 계산이 어려운 난제에 기반하여 설계된 것이 아니기 때문에 양자 컴퓨팅은 물론, 컴퓨팅 파워가 무한한 공격자에게도 저항성이 있고 안전성이 대칭키 암호시스템과 같이 입력 값의 엔트로피에 의존한다.[5]

LWE(Learning with Errors) 문제는 레티스 기반 문제로서 특정 파라미터 조건 하에 양자 알고리즘에 안전한 레티스 문제인 GapSVP, SIVP 문제로 환원된다는 것이 증명되었다.[6][7]

본 논문에서는 생체 정보에 대한 프라이버시 보호가 가능하고 본래의 인증 목적을 이룰 수 있으면서도 양자 컴퓨팅에 안전한 다양한 생체 인증 기법들을 소개하고 비교 분석한다.

II. 배경지식

본 장에서는 생체 인증 프로토콜과 보안 스케치(Secure Sketch)와 랜덤 추출기(Randomness Extractor)[2], 퍼지 추출기(Fuzzy Extractor)[2], 동형 암호(Homomorphic Encryption)[3]에 대해 정의한다.

2.1 생체 인증 프로토콜

생체 인증 프로토콜은 다음과 같은 알고리즘으로 구성된다.

- $enrollment$: 사용자가 생체 데이터 w를 이용하여 추출된 값을 서버에 저장한다.
- $authentication$: 사용자는 생체 데이터를 다시 측정하고 그 때 측정된 w'를 이용하여 추출된 값을 서버에 전송한다. 서버는 추출된 값과 서버에 저장된 값을 연산하여 w와 w'이 허용된 오차 범위 내에 있는지를 비교하여 인증을 완료한다.

2.2 보안 스케치와 랜덤 추출기[2]

보안 스케치를 구성하는 2개의 알고리즘과 랜덤 추출기의 알고리즘은 다음과 같다.

- $sketch(w) \rightarrow s$: 생체 데이터 w 를 입력받고 헬퍼 데이터(helper data) s를 출력한다. (이 때, s 값은 서버에 저장되는 공개된 값이기 때문에 s를 통해 w에 대한 정보가 노출되어서는 안된다. 이는 생체 정보의 프라이버시 보호에 필수적인 요소이다.)
- $recovery(w', s) \rightarrow w$: 다시 측정된 생체 데이터 w'와 저장된 s를 입력받아 w를 출력한다. 단, w'과 w의 오차가 초기에 설정된 오차 범위 내에 있을 때에만 $(1-\delta)$의 확률로 복구된다.
- $extract(w, x) \rightarrow r$: 생체 데이터 w와 랜덤 시드 x를 입력받아 추출 값 r을 출력한다.

2.3 퍼지 추출기[2]

퍼지 추출기는 아래의 2개 알고리즘으로 구성된다.

- $generate(w) \rightarrow r, p$: 생체 데이터 w 를 입력받고 추출 값 r과 헬퍼 데이터 p를 출력한다. (이 때, p 값은 서버에 저장되는 공개된 값이기 때문에 p를 통해 r에 대한 정보가 노출되어서는 안된다.)
- $reproduce(w', p) \rightarrow r$: 다시 측정된 생체 데이터 w'와 저장된 p를 입력받아 r를 출력한다. 단, w'과 w의 오차가 초기에 설정된 오차 범위 내에 있을 때에만 $(1-\delta)$의 확률로 복구된다.

2.4 동형 암호[3]

동형 암호는 아래의 4개 알고리즘으로 구성된다.

- $\mathrm{Setup}(\lambda) \rightarrow pk, sk$: 보안 상수 λ를 입력 받고 비밀키 sk와 공개키 pk를 출력한다.
- $\mathrm{HEnc}(pk, x) \rightarrow \overline{x}$: 공개키 pk와 메시지 x를 입력받아 암호문 $\overline{x}$를 출력한다.

- HDec$(sk,\overline{x})\rightarrow x$: 비밀키 sk와 암호문 $\overline{x}$를 입력받아 메시지 x을 출력한다.
- Evaluate$(pk,\overline{x}_1,...,\overline{x}_n,f)\rightarrow\overline{x}_f$: 공개키 pk와 주어진 여러 개의 암호문 $\overline{x}_1,...,\overline{x}_n$을 입력받아 연산 함수 f를 통해 새로운 암호문 $\overline{x}_f$를 출력한다.

III. 생체 인증 프로토콜

본 장에서는 보안 스케치와 랜덤 추출기로 만들어지는 퍼지 추출기[2], 계산 안전성을 갖는 퍼지 추출기(Computational Fuzzy Extractor)[4], 그리고 동형 암호[3]를 이용한 3가지 생체 인증 프로토콜에 대해 소개한다.

3.1 보안 스케치와 랜덤 추출기 기반

보안 스케치와 랜덤 추출기를 이용한 퍼지 추출기 기반 생체 인증의 등록 및 인증과정은 다음과 같은 알고리즘으로 구성된다.

3.1.1 등록 단계

- $sketch$: 생체 데이터 w를 입력받아 헬퍼 데이터 s를 출력한다.
- $enrollment$: w 값과 랜덤 추출기를 이용하여 추출 값 r을 서버에 등록한다.

3.1.2 인증 단계

- $recover$: 다시 측정된 생체 데이터 w'와 헬퍼 데이터 s을 입력받고 w와 w' 사이의 오차가 미리 설정된 t 이하라면 w 값을 출력한다.
- $authentication$: $recovery$ 과정을 통하여 재생성된 w 값과 랜덤 추출기를 이용하여 r 값을 추출하고, 서버에 저장되어 있던 r 값과 비교하여 두 값이 같으면 인증이 통과된다.

3.2 계산 안전성을 갖는 퍼지 추출기 기반

계산 안전성을 갖는 퍼지 추출기를 이용한 생체 인증의 등록 및 인증 과정은 다음과 같다.

3.2.1 등록 단계

- $generate$: 생체 데이터 w를 입력받아 비트열 r을 추출하여 서버에 저장하고 헬퍼 데이터 p를 출력한다.

3.2.2 인증 단계

- $reproduce$: 다시 측정된 생체 데이터 w'와 저장되어 있던 헬퍼 데이터 p를 입력받고 w와 w' 사이의 오차가 t 이하라면 r 값을 추출되고, 서버는 이 추출된 값과 서버에 저장되어 있던 r 값과 비교함으로써 두 값이 같으면 인증을 통과시킨다.

3.3 동형 암호 기반

동형 암호를 이용한 생체 인증의 등록과 인증 과정은 다음과 같은 알고리즘으로 구성된다.

3.3.1 등록 단계

- $enrollment$: 생체 데이터 w와 동형 암호의 암호화 알고리즘을 이용하여 HEnc$(pk,w)=\overline{w}$ 값을 서버에 등록한다. 암호화된 데이터는 원래의 생체 정보를 노출하지 않으며, sk가 제공되지 않는 한 정보 노출이 되지 않음이 보장된다.

3.3.2 인증 단계

- $evaluate$: 사용자가 인증을 위하여 다시 측정한 생체 데이터 w'를 동형 암호의 암호화 알고리즘을 이용하여 생성한 HEnc$(pk,w')=\overline{w'}$ 값을 서버에 보내면 서버는 동형 암호의 연산 알고리즘을 이용하여 HD$(\overline{w},\overline{w'})$ 값을 구한다. (단, $\overline{w}=(\overline{w}_0,...,\overline{w}_{n-1})$, $\overline{w'}=(\overline{w'}_0,...,\overline{w'}_{n-1})$ 일 때, HD$(\overline{w},\overline{w'})=\sum_{i=0}^{n-1}(\overline{w}_i-\overline{w}_i')^2$ 이다. 이는 두 데이터의 Hamming distance 값과 같다.)
- $match$: 동형 암호의 복호화 알고리즘을 이용하여 HDec(HD$(\overline{w},\overline{w'})$)=HD$(w,w')$ 값을 구한다. HD(w,w') 값이 기존에 설정된 허용 오차 범위 내에 속하면 사용자는 인증을 통과하게 된다.

IV. 생체 인증 프로토콜 비교분석

본 장에서는 보안스케치를 이용한 퍼지 추출기, 계산 안전성을 갖는 퍼지 추출기와 동형 암호를 이용한 3가지 생체 인증 프로토콜들을 비교분석 한다.

3.1 기법의 정보 이론적 안전성을 갖는 퍼지 추출기를 이용한 생체 인증의 $authentication$ 과정

에서 서버에 저장되어 비교 값으로 사용되는 r 값의 엔트로피는 생체 데이터의 엔트로피를 넘지 못한다는 한계가 있다. 또한 헬퍼 데이터 s가 w' 값으로부터 w 값을 복구해내는데 충분한 정보를 갖고 있어야 하기 때문에 이로 인해 w 값의 엔트로피의 손실이 발생하는 문제점이 발생한다.[4]

3.2 기법의 계산적 퍼지 추출기는 헬퍼 데이터 p 값과 측정된 생체 데이터 w' 값을 이용하여 초기에 저장된 생체 데이터 w 값을 복구시키는 게 아닌, r 값을 바로 추출하기 때문에 헬퍼 데이터로 인한 엔트로피 손실을 최소화하였으나 여전히 추출 값의 엔트로피가 w의 엔트로피에 의존한다는 한계가 있다.[4]

3.3 기법인 동형 암호를 이용한 생체인증의 $authentication$ 과정에서 서버에 저장되는 추출 값은 동형 암호의 비밀 키를 이용해서 생체 데이터를 직접 암호화한 값이므로 안전성이 생체 데이터의 엔트로피와 독립적이지만 생체 인증을 위해 동형 암호의 비밀 키를 사용자가 보관해야 하는 점은 생체 인증의 편리함을 저해시키는 요소가 된다. 이를 해결하기 위해 비밀키를 보관하는 인증 서버 기관을 따로 만드는 시스템 모델도 제안되었으나 안전성에 대한 추가적인 가정이 필요하다는 문제점이 발생한다.[8]

V. 결론

본 논문에서는 양자 컴퓨팅 환경에서 안전한 생체 인증 프로토콜에 대해 살펴보았다. 추가적인 키 관리나 저장이 필요없는 계산적 안전성을 갖는 퍼지 추출기는 사용자 측면에서 편리하지만 저장되는 추출 값의 길이가 생체 데이터의 엔트로피에 의존한다는 문제점이 있다. 또한 동형 암호를 이용한 생체 인증은 생체 데이터의 엔트로피와 독립적인 추출 값을 사용하지만 별도의 키 관리가 필요하다. 따라서 양자 컴퓨팅 환경에 안전하고 사용자 측면에서 별도의 키 관리가 없으며 생체 데이터의 엔트로피와 독립적인 추출 값으로 인증 수행이 가능한 기법에 대한 연구는 흥미로운 연구 주제가 될 것이다.

[참고문헌]

[1] P. Shor, “Algorithms for Quantum Computation: Discrete Logarithms and Factoring,” Foundations of Computer Science, 1994

[2] Y. Dodis, L. Reyzin, A. Smith, “Fuzzy Extractor : How to Generate Strong Keys from Biometrics and Other Noisy Data,” In Eurocrypt, pp.523-540, 2004.

[3] J.H. Cheon, H. Chung, M. Kim, K. Lee, “Ghostshell: Secure Biometric Authentication using Integrity-based Homomorphic Evaluations,” https://eprint.iacr.org/2016/484.pdf, 2016.

[4] B. Fuller, X. Meng, L. Reyzin, “Computational Fuzzy Extractors,” In Asiacrypt, pp.174-193, 2013.

[5] CE. Shannon, “Communication Theory of Secrecy Systems,” Bell Labs Technical Journal, pp.656-715, 1949.

[6] O. Regev, “On Lattices, Learning with Errors, Random linear codes, and Cryptography,” In Symposium on Theory of Computing, pp. 84-93, 2005.

[7] C. Peikert, “Public-key Cryptosystems from the Worst-case Shortest Vector Problem: Extended Abstract,” In Proceedings of the 41st Annual ACM Symposium on Theory of Computing, pp.333-342, 2009.

[8] M. Yasuda, T. Shimoyama, J. Kogure, K. Yokoyama, T. Koshiba, “Packed Homomorphic Encryption based on Ideal Lattices and its Application to Biometrics,” In Security Engineering and Intelligence Inf, pp.55-74, 2013.

개인정보의 비식별 처리 시 발생가능한 문제점 분석 및 대응방안 제시

한경수, 류지민, 서정택

순천향대학교 정보보호학과

Analyzing the problems that may occur in the process of non-identification of personal information and suggesting countermeasures

Gyeong Soo Han, Ji Min Ryu, Jung Taek Seo

Department of Information Security Engineering, Soonchunhyang University.

요 약

4차산업이 성장하면서 빅데이터의 중요성이 높아지고 있다. 그러나 우리나라는 빅데이터의 사용률이 OECD 국가 중 최하위권에 속해있다. 이를 해결하기 위해 정부에서 발표한 빅데이터 비식별 조치 가이드라인에 따라 빅데이터의 활성화와 개인정보보호를 함께 증진시키려 했다. 그러나 비식별 조치된 정보의 재식별 가능성, 분야별 특성을 고려하지 않은 일관된 기준으로 인해 개인정보보호 활용과 보호의 문제점이 발생하였다. 이로 인해 4차산업의 성장이 늦어지고 있다. 이를 개선하기위해 본 논문에서는 해외의 비식별 처리 정보의 효율적 사용과 안전성, 그 차이점을 비교, 분석하여 개인정보의 비식별 처리 시 명확한 정의 및 범위와 분야별 개별적인 기준을 정하는 대응방안을 서술하고 이에 따른 기대효과를 서술한다.

I. 서론

4차 산업혁명이 도래 하면서 빅데이터의 중요성이 대두되고 있다. 빅 데이터는 개인의 데이터에서 가치를 뽑아내어 수집, 분석, 활용하는 기술을 말한다. 현재 매일 데이터가 쏟아져 나오면서 우리의 생활과 산업 전반에 걸쳐 빅데이터의 중요성도 점차 커지고 있다. 기업에서의 소비자 마케팅, 생산성 향상 등에 빅데이터가 적극 활용되면서 관련 시장도 급성장하는 추세다. 하지만 정작 4차 산업혁명의 핵심 기술인 클라우드, 빅데이터 사용률은 경제협력개발기구(OECD) 회원국 중 우리나라의 사용률은 최하위권의 사용률을 보이고 있다. 이는 즉 4차 산업혁명에서의 성장의 도태됨을 나타낼 것이다.

빅데이터 사용률 향상과 개인정보보호를 개선하기 위해서 2016년 6월 행정자치부 등 정부부처들은 빅데이터 산업 활성화를 위하여 개인정보 관련 빅데이터 개인정보보호 가이드라인[1]을 공표하였다. 정부가 공표한 가이드라인 '제2조 4항에서 "비식별화"란 데이터 값 삭제, 가명처리, 총계처리, 범주화, 데이터 마스킹 등을 통해 개인정보의 일부 또는 전부를 삭제하거나 대체함으로써 다른 정보와 쉽게 결합하여도 특정 개인을 식별할 수 없도록 하는 조치를 말한다'. 라고 명시하였다. 비식별 처리를 통해 빅데이터 활성화 와 개인정보보보호를 동시에 증진 시키는 효과를 기대하였으나 개인정보 범위의 모호성과 비식별 처리의 대한 안정성을 충분히 검토하지 않았다는 의견이 계속하여 나오고 있는 상황이다.

정부의 가이드라인에서 공표한 비식별 처리의 문제점은 비식별 처리한 정보는 동의 없이 제3자에게 제공, 이용이 가능하다. 라고 명시하여 비식별 처리정보를 개인정보로 보지 않고 있으나 가명처리, 총계처리 정보를 다른 정보

와 교차 했을 시 개인의 식별이 가능하다는 연구 결과가 나왔다[2]. 이는 즉 개인정보보호 법 제2조 개인정보란 살아있는 개인에 대한 정보로서 성명, 주민번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로 개인을 알아볼 수 없더라도 다른 정보와 쉽게결합하여 알아볼 수 있는 정보)의 위반 됨을 말한다. 이에 따라 개인정보의 비식별 처리 정보의 새로운 정의, 범위를 제시함과 이를 위반 시 명확한 법적 처벌, 산업 군 특성 개별법을 고려한 빅데이터의 활용성과 안전성을 동시에 증진 시킬 수 있는 새로운 대안을 제시한다.

본 논문 Ⅱ부터 비식별 현재의 처리정의와 문제에 관해 서술하고 이에 따른 대안을 본 논문 Ⅲ부터해외 법 사례와 비교 분석하여 본 논문 Ⅳ에서 대안을 제시한다.

II. 국내 비식별 처리 정의 및 문제점

현재 우리나라의 빅데이터 활용에 대해서 비식별 조치를 한 후 수집, 이용이 가능함을 원칙으로 하고 있지만 비식별 처리 기준의 문제점이 있어 Ⅱ장에서는 비식별처리의 정의와 우리나라의 비식별처리의 문제점 측면에서 살펴본다.

2.1 국내 비식별 처리 정의

비식별 조치된 정보는 개인정보의 무분별 적 수집을 막고 산업 전반에 합법적인 빅데이터 데이터의 수집, 이용을 위해 개인을 식별 할 수 없는 정보이다.

위의 상술한 것과 같이 정부에서 공표한 “개인정보 가이드라인”의 비식별 처리 절차는 4가지 단계로 볼 수 있다. 먼저 1단계 사전검토 단계에서 처리하는 정보가 개인정보에 해당하여 개인을 식별 할 수 있는지 검토 후 개인의 식별이 가능하면 2단계 비식별 조치를 취해야한다. 비식별 조치 단계에서는 개인의 성명, 주소, 전화번호, 고유식별정보 등 개인에 관련해 고유하게 보유된 값, 또는 이름의 식별자정보, 신체, 가족관계, 경력, 사회활동 등 개인과 관련되어 다른 정보와 결합 시 개인을 식별 할 수 있는 속성자 정보에 관해서는 비식별 조치를 취해야 한다. 비식별 조치 기법은 표<1>과 같은 기법을 사용한다[1].

표<1> 비식별 조치 사용기법 예

처리기법	예
가명처리 (Pseudonymization)	-홍길동,26세, 서울, 한국대 재학 ⇨ 임꺽정, 20대,서울, 우리대 재학
총계처리 (Aggregation)	-홍길동:180cm,임꺽정:170cm,장보고:160cm, 김수로:150cm ⇨총합:660cm 평균키:165cm
데이터 삭제 (Data Reduction)	주민등록번호:931234-1234123 ⇨90년대 생, 남자
데이터범주화 (Data Suppression)	홍길동,26세, 홍씨, 20~30대
데이터마스킹 (Data Masking)	-홍길동,26세, 서울, 한국대 재학 ⇨홍xx,26세, 서울, xx 재학

위의 표<1>의 기술들을 단독 또는 복합적으로 사용하여 정보를 비식별 조치를 취했다면 3단계인 적정성평가 단계를 외부 평가단을 통해 비식별 조치의 적정성, 안전성을 평가한다. 이를 통해 다른 정보와의 결합으로 개인의 식별 가능성을 사전 방지를 한다.

마지막 4단계 사후관리 단계에서는 비식별 정보의 안전한 활용과 오남용 방지를 위한 조치사항을 이행한다. 그에 필요한 관리적, 기술적 조치는 표<2>와 같다.

표<2> 비식별 처리정보에 대한 관리적, 기술적 보호 조치

구분	비식별 정보 보호조치
관리적 보호조치	1.비식별 정보파일 관리담당자 지정 2.비식별 정보파일 대장관리 3.원본정보 관리부서와 비식별 정보 관리 부서 간 비식별 정보 공유 금지 4.이용목적 달성 시 지체 없이 파기 5.비식별 정보파일 유출 시 대응계획 수립
기술적 보호조치	6.비식별 정보 파일에 대한 접근권한 관리 및 접근통제 7.비식별 정보 보관시스템에 대한 접속 기록 관리 8.악성 코드 방지등을 위한 보안프로그램 설치, 운영

2.2 우리나라의 비식별처리의 문제점

비식별 조치로 제안되는 K-익명화는 다양한 데이터 유형에 적용하기 어려우며, 산업 군 별로 데이터의 특성이나 형태에 따른 다양한 요구를 만족하기 어렵다. 따라서 기업의 적용 사례가 줄어들고 있다. 또한 비식별 처리된 정보를 다른 정보와 교차해서 분석 시 개인을 재식별 할 수 있다는 결과가 발표 되었으며 이는 즉 개인을 알아 볼 수 없게 하는 현재의 비식별 조치 문제점이라 할 수 있다[2].

가이드라인 제6조(새로운 정보의 생성) 1항 정보통신서비스 제공자는 비식별 조치하여 수집한 공개된 정보 및 이용내역정보를 정보 처리 시스템을 통해 조합·분석하여 새로운 정보를 생성할 수 있다. 다만, '새롭게 생성된 정보에 개인정보가 포함되어 있을 경우, 즉시 파기하거나 비식별 조치를 취하여야 한다'. 에서 생성된 정보의 개인정보가 포함되어 있을 경우라 명시함은 현재 비식별 처리 정보가 재식별 가능 하며 안전성을 보장 하지 못한다는 것을 나타내는 것이며 가이드라인 제2조 4항의 비식별의 정의와 모순이 되는 부분이다. 또한 크게 목적이 다르지 않은 개인정보의 사용 목적도 번번이 개인의 동의를 구해야하는 어려움이 있다.

현행법에는 비식별 처리에 대한 법이 제정되어 있지 않고 가이드라인만 있는 상황이다. 이 경우에는 가이드라인에 강제성이 없기 때문에 기업에서는 빅데이터 활용과 개인정보보호에 대한 고민을 할 수 밖에 없다.

표<3> 우리나라 비식별 처리의 문제점

1.비식별 처리의 애매한 정의 2.산업 군 특성을 고려하지 않은 일관된 기준 3.비슷한 목적의 개인정보의 사용에도 상시 동의를 구해야하는 번거로움

Ⅲ. 해외 비식별 처리 기준 및 사용현황

3.1 EU 비식별 처리 사례

EU는 1995년 만들어진 EU Directive(95/46/EC) 지침이 있다. 비록 Directive의 형식이기는 하지만, 개인정보보호 관련한 EU 차원 최초의 입법이라는 점에서는 그 의미가 크다. 주요 내용으로 1.목적, 개념정의, 적용범위, 2.개인정보 처리 일반 원칙, 3정보주체의 권리, 4.개인정보처리자 등의 통지의무, 5.실효성 확보와 권리 구제, 6.개인정보의제3국 이전, 7.행동강령, 8.감독기관 등에 대해 규정하고 있다. 그러나 EU 내에서 Directive는 전체적인 통일성이 일치 하지 않을 수 있다[4].그래서 EU는 보다 통일된 개인정보보호 법체계를 구현하기 위하여 2016년 4월27일 GDPR(General Data Protection Regulation)을 채택하였다.

GDPR 전문 제 26조에서 정보주체를 알아볼 수 없도록 익명처리 된 정보에 지침에 따른 개인정보보호원칙이 적용되지 않는다고 규정하고 있다. 다만 GDPR은 개인정보의 목적 외 처리를 광범위 하게 허용하여 정보 활용 측면을 강조하고 있다. 또한 Directive에서는 역사적 통계적, 과학적 연구 목적의 경우만 목적 외 추가적 처리를 규정하고 있는 것과 달리 GDPR 제6조

제4항은 정보 주체의 동의를 받는 경우, 제23조 제1항에 명시된 목적을 보호하기 위하거나 EU 또는 회원국 법류에 근거한 경우, 개인정보가 최초 수집될 때 동의 받은 목적과 다른 목적이 최초 수집 목적과 같은 경우 목적 외 활용을 허용한다. 라고 명시되어있다[4][5.]

3.2 일본의 비식별 처리 사례

우리나라의 공공데이터 개방으로부터 시작된 빅데이터 관련 정책은 일본의 사례와 매우 유사하다. 그러나 우리나라 개인정보보호법과 달리 일본의 개인정보보호법은 민간 분야만을 규율하고 있고, 공공 분야에 대하여는 '행정기관이 보유하는 개인정보보호법', '독립행정법인 등이 보유하는 개인정보보호법'이 규율하고 있다.

일본은 "개인정보 이용 및 활용에 관한 제도개정 대강"에서는 개인정보에 있어 옵트아웃(Opt-out) 방식 도입, 개인정보의 익명성 저감조치와 민감정보의 취급개선 개인정보보호의 사각지대 해소 개인의 권리와 이익침해의 사전방지를 목적으로 한다.

일본의 2014년 대강에서는 "익명가공 정보" 즉 개인을 특정할 수 있는 정보를 가공에 의해 익명화 한 후의 정보는 본인의 동의 없이도 데이터를 제공, 이용이 가능하다[6].라고 명확히 명시 하여 개인정보의 정의와 사용범위를 설명해 주고 있다.

3.3 미국의 비식별 처리 사례

미국 보건복지부는 HIPAA 프라이버시 규칙(HealthI nsurance Portability and Accountability Act Privacy Rule)에 따른"의료정보 비식별 방법에 대한 가이드"를 제시 하였다.(2012.11.26) HIPAA프라이버시 규칙이 있다.

□ 개인을 식별하지 않는 개인정보와 개인을 식별할 수 있게 한다는 합리적 근거가 없는 건강 정보가 아니다.

이는 비식별된 의료개인정보의 제한이 없는 이용을 허용하는 것이다[7].

미국 FTC(Federal Trade Commission)은 개인정보 공개 시 지켜야 할 개인정보 비식별 조치내용을 담은 보고서를 발표했으며, 내용은다음과 같다.

□ 소비자, 컴퓨터 또는 다른 장치와 결합될 수 있는 개인정보는 반드시 비식별 되어야한다.

□ 공개된 정보에 대해서는 재식별화를 시도하지 않아야 한다.

□ (타 기업 등에 비식별 데이터 제공시)데이터를 재식별하지 않도록 계약 상 명문화하도록 한다.[8]

미국 NIST(National Institute of Standards and Technology)에서는 수집된 개인정보의 익명화와 재식별화 방지 가이드 보고서를 발표했다.

□ 비식별이란 수집된 개인정보의 식별성을 제거하거나 데이터 셋과 정보주체의 연관성을 제거하는 과정을 말한다.

□ 연구 목적으로 의료 정보를 공개 시 이름 , 주민등록번호, 연락처, 상세 주소와 같은 특정 개인을 식별할 수 있는 요소를 제거하는 것으로 가명처리, 총계처리, 데이터 값 삭제, 범주화 ,데이터 마스킹 등의 방법이 있다.

□ 비식별은 빅데이터의 활용 증가와 정부의 정보개방 정책에 따라 등장해 최근 주목받고 있는 개념으로, 연구 등의 목적으로 공개된 비식별 된 개인정보가 SNS나 다른 연구기관 등에 의해 공개된 개인정보와 결합돼 특정인이 다시 재식별화 되지 않도록 목적이 있다.

□ 재식별화는 비식별된 개인정보가 인터 또는 공공기관의 정보 개방을 통해 공개된 정보 또는 데이터 비교, 연계, 결합 등을 통해 특정 개인이 다시 식별되는 과정을 의미한다.[8].

이처럼 미국은 분야별로 맞춤형 개별 가이드라인을 발표함으로서 보다 쉬운 환경을 만들었다.

표<4> 해외사례와 우리나라의 비식별 처리비교

	법률	비식별처리원칙
EU	EU GDPR (유럽연합일반 데이터보호규정)	익명처리 된 정보에는 지침에 따른 개인정보보호 원칙
일본	민간분야 공공분야 개별법	민간분야 공공분야 맞춤형 원칙
미국	분야별 맞춤형 개별법	분야별 맞춤형 원칙
한국	개인정보 비식별 조치 가이드 라인	1.사전검토 2.비식별조치 3.적정성 평가 4.사후 관리

IV. 비식별 처리 가이드라인 개선(안)제시

4.1 비식별 처리 정보에 대한 개인정보 정의 및 범위 명확화

정부에서 공표한 “개인정보비식별처리가이드라인“에 따르면 비식별 처리 된 정보는 개인정보가 아니라 보고 있다. 그러나 다른 비식별 정보와 교차 시 개인을 식별할 수 있음으로 개인정보라 취급하여야한다. 그러므로 빅데이터 안에서의 개인정보보호 개선 방안은 다음과 같다.

1. 개인정보 범위에 관한 구체적 명시(재식별 가능성 등을 고려한 처리범위)와 이를 위반 시 엄격한 법적 제재
2. 일본 대강의 '개인정보보호 법률'과 같은 비식별화, 익명화 정보를 특별한 규정으로 입법

이를 통해 기업의 개인정보 수집, 이용 방법에 대한 합법적 테두리 안에서의 적당, 적합하게 개인정보를 사용하면 빅데이터 활성화를 증진시킬 수 있을 것으로 기대가 된다.

4.2 분야별 맞춤형 개별법

비식별 처리에 개선 방안으로 산업별 맞춤형 개별법을 제안한다. 이에 대한 사례로 미국의 법을 예로 들 수 있다. 미국은 의료(HIPAA프라이버시규칙), 개인(FTC,NIST “개인정보익명화와 재식별 방지 가이드”)등 비식별 조치된 정보의 활용을 보장하기위해 단일화 된 일반법이 아닌 각 분야별 특성을 고려한 맞춤형 개별법을 통해 보다 나은 빅데이터 환경을 만들었다. 우리나라도 단일화 된 일반법 보다는 미국의 법과 유사한 분야별 맞춤형 개별법을 제정하여 보다 나은 빅데이터 이용 환경을 만드는 것이 분야별 특성마다 적용하기 유용할 것이다.

4.3 서비스 추가, 파생 등의 정보에 관한 상시 동의 개선

빅데이터 분석기술의 활성화을 위해 지금 우리나라의 개인정보보호법은 일본, 미국, EU의 법에 비교 하면 활용성 면에서는 큰 걸림돌이 되고 있다. 우선 정보를 분석해 새로운 데이터를 생산해 내는 빅데이터에서 기존 수집, 이용의 동의를 받은 데이터가 그 목적 내에서만 사용되기는 현실적으로 제한적, 비효율적이라 할 수 있다[9]. 이를 개선하기위해 EU GDPR의 '개인정보가 최초 수집될 때 동의 받은 목적과 다른 목적이 최초 수집 목적과 같은 경우 목적 외 활용을 허용한다.' 와 같이 기존 정보주체가 수집, 이용에 동의했던 서비스가 새롭게 파생된 서비스와 크게 다르지 않고 유사한 목적인 경우에는 정보주체 개개인에게 번번이 동의를 받지 않고 서비스 제공자가 수집, 이용 할 수 있게 하여 빅데이터의 활용성을 높일 수 있게 한다.

4.4 기대효과

비식별 처리 정보에 대한 정확한 명시를 통해 기업이 비식별 정보 이용 시 명확한 법률에 따라 정보의 이용이 가능해 혼란이 적어지고 분야별 맞춤 개별법에 따라 분야별 특성을 고려해 조금 더 효율성 있는 환경을 조성, 목적이 크게 다르지 않은 정보에 대해 번번이 동의를 구해야 하는 어려움을 제거하여 빅데이터 활성화와 4차 산업 증진에 도움이 될 것이라 예상한다.

V. 결론

본 논문에서는 4차 산업이 성장하면서 빅데이터의 중요성이 높아짐에 따라 정보수집에 용이한 개인정보 비식별 처리에 대한 문제에 대해 연구하였다. 또 해외 법 사례를 통하여 우리나라와 해외의 비식별 처리에 대한 우리나라와의 차이점에 대해 분석하였다. 이에 우리나라는 빅데이터의 사용률이 현저히 떨어짐에 따라 비식별 처리에 대한 가이드라인의 개선안을 제시한다. 향후 본 논문에서 제시하는 대응방안이 적용이 된다면, 우리나라의 빅데이터 사용률이 증가하고, 기업들의 4차산업의 발전을 증진시키는 환경을 조성하여서 합법적이고 효율적인 개인정보 사용과 개인정보 보호 강화에 더욱 이바지 할 것으로 기대된다.

[참고문헌]

[1] 국무조정실 행정자치부 방송통신위원회 금융위원회 미래장조과학부 보건복지부 “개인정보 비식별 조치 가이드라인”

[2] 미디어 오늘,“개인정보 비식별화하면 괜찮다? 교차하면다나온다”

http://www.mediatoday.co.kr/?mod=news&act=articleView&idxno=130802

[3] 보안뉴스,“개인정보비식별조치,세계각국은 어떻게하고있나요”

http://www.boannews.com/media/view.asp?idx=57111&page=3&kind=2

[4] 이은우“1-2강-GDPR 핵심 개념과원칙”

[5] 한국법제연구원 윤석진 “빅데이터 법제에 관한 비교법적 연구”

[6] 한국인터넷진흥원 수탁기관:한국정보보호학회,“신규 ICT 환경의 해외 개인정보 활용 사례 및 법제동향 분석연구”

[7] 한국인터넷진흥원,“NIST, 개인정보 비식별화 가이드라인 공개”

[8] 법제처,한국법제연구원 빅데이터 관련 개인정보 보호법제 개선방안 연구

[9]이상직 변호사 “제4차 산업혁명과 개인정보보호 문제”

Mixnet 적용을 통한 자율주행차 운영환경 프라이버시 보호방안 연구

강기완, 서정택

순천향대학교 정보보호학과

Research on the privacy protection of the self-driving vehicle operating environment using mixnet

Ki Wan Kang, Jung Taek Seo

Department of Information Security Engineering, Soonchunhyang University.

요 약

최근 세계적으로 자율주행차와 관련하여 많은 기술들이 발표되고 있다. 하지만 기술적인 부분은 점점 구체화 되고, 발전하고 있는 반면에 보안위협에 대한 대응책은 아직 완벽하지 못하다. 관련하여 자율주행차 운영환경에 대한 보안은 정책적인 부분은 많이 구체화되고 있으나, 보안 기술 측면은 아직 많이 부족한 실정이다. 특히, 자율주행차의 효율적인 운영을 위해서는 목적지 정보, 위치 정보, 주행거리 등 프라이버시와 관련된 데이터들을 수집한다. 해당 데이터의 노출 시 차량 도난, 인명피해 등 사용자에게 직접적인 피해가 발생 가능하다. 본 논문에서는 Mixnet 기술의 적용을 통한 자율주행차 운영 환경의 데이터 송신자와 데이터의 연결성을 제거함으로써 프라이버시를 보호하는 방안을 제시한다.

I. 서론

최근 자동차에 ICT(Information & Communication Technology) 기술이 결합된 자율주행차가 등장하면서 최근 자동차 시장 환경이 크게 변화됐다. 특히 자율주행차 시장은 기존의 자동차 제조사와 ICT 기술기업이 서로 협력관계를 맺고 시장구도를 형성하며 빠르게 성장할 것으로 예상된다[1].

자동차, 교통 환경이 점차 자율주행, 지능형 교통시스템으로 발전하면서, 자동차는 점점 많은 기능들을 담으며 복잡화, 지능화 되어가고 있다. 특히 시간이 지날수록 도로/교통 인프라와 자동차 간의 연결성이 증가함에 따라 공격자의 공격범위 또한 같이 증가하고 있다. 대표적으로 2014년에 지프 체로키를 해킹 후 원격 조정하여 시속 100km로 주행 중인 지프 체로키 차량을 급정거시키고, 핸들을 임의로 조작하여 차량을 배수로로 곤두박질시키기도 하였다. 위와 같이 시스템에 악의적으로 접근하여 자동차에 대해 물리적인 피해를 입히는 것 외에도 추후 자율주행환경에서 오고가는 데이터에 대해 탈취하고 분석하여 2차적으로 도난, 인명피해 등을 입힐 수 있다[2].

자율주행차는 주행 중 자신의 위치정보, 목적지 정보, 주행거리 등 다양한 정보들을 주변의 자율주행차나 인프라에 전송한다. 자율주행차는 데이터들을 판단하여 어느 구간에 대해 교통부하가 걸려있는지, 상황에 따라 운전자를 안전하고 빠르게 데려다 줄 수 있는 경로를 판단한다.

본 논문에서는 해당 데이터들을 안전하게 보호하기 위해 Mixnet의 핵심인 익명 통신로를 활용한다. Mixnet을 적용해 데이터 송신자와 데이터의 연결성을 제거하여 위치정보, 목적지 정보 등 프라이버시와 관련된 데이터를 보호하는 기술에 대해 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 자

율주행차 개념에 대해 분석하고, 3장에서는 자율주행차 통신 보안 표준에 대해 분석한다. 4장에서는 자율주행차 운영환경에서 발생 가능한 취약점에 대해 분석하고, 5장에서는 4장에서 다룬 보안 취약점을 대응할 수 있는 기술에 대해 제안한다. 마지막으로 6장에서 결론을 맺는다.

II. 자율주행차 개념

국내 「자동차관리법」 제2조 제1의 3호에서는 자율주행차를 '운전자 또는 승객의 조작 없이 자동차 스스로 운행이 가능한 자동차'로 정의가 되어있다.

현재 대부분 국가에서는 자율주행차의 개념을 사람의 개입 없이 완벽하게 스스로 주행할 수 있는 자동차를 자율주행차로 정의하고 있다.

자율주행차의 주행 과정은 사람과 동일하게 "인지-판단-제어" 3단계 과정을 거쳐 주행을 한다.

[표 1] 자율주행차 작동 과정

단계	설명
인지	차량에 장착된 센서와 외부와의 통신을 통해 주변 상황에 대한 정보를 수집하고 인지
판단	인지된 정보를 해석하여 주행상황을 판단하고, 사람을 대신해 조향 및 속도조절을 하여 스스로 경로를 따라 운행
제어	제어시스템을 통해 결정된 판단을 실제 주행에 반영하기 위해 운전 시스템을 제어

자율주행차는 5개의 주요요소와 4개의 핵심기술로 구성되어 있다. 주요 요소는 크게 환경인식 센서, 위치인식 및 맵핑, 판단, 제어, HCI(Human Computer Interaction)으로 구성되어 있다. 핵심기술은 ADAS(Advanced Driver Assistance System), V2X(Vehicle to Everything), 정밀지도, HMI(Human Machine Interface)로 구성되어 있다[3].

다음 표는 자율주행차의 주요 요소에 대한 설명이다.

[표 2] 자율주행차 주요 요소

주요기술	설명
환경인식 센서	· 레이더 카메라 등의 센서 · 정적장애물(전봇대 등), 동적 장애물(보행자 등), 도로 표식(차선 등), 신호 등을 인식
위치인식 및 맵핑	· GPS/INS/Encoder, 기타 맵핑을 위한 센서 사용 · 자동차의 절대/상대적 위치 추정
판단	· 목적지 이동, 장애물 회피 경로 계획 · 주행 상황별(차선유지/변경, 추월 등) 행동을 스스로 판단
제어	· 운전자가 지정한 경로대로 주행하기 위해 조향, 속도변경, 기어 등 액츄에이터 제어
HCI	· HVI를 통해 운전자에게 경고/정보 제공 운전자의 명령 입력 · V2X 통신을 통해 인프라 및 주변 차량과 주행정보 교환

*HVI(Human Vehicle Interface)

다음 표는 자율주행차의 핵심기술에 대한 설명이다.

[표 3] 자율주행차 핵심기술

주요기술	설명
ADAS	교통사고를 미연에 방지하기 위한 능동 안전시스템
V2X	통신을 통해 다른 차량의 진행방향, 전방의 교통현황 등 정보 제공
정밀지도	정적인 정보 및 동적인 정보 등 도로의 상세한 정보를 제공
HMI	사람-컴퓨터간 소통을 위한 아날로그-디지털 전환 인터페이스

III. 자율주행차 통신 보안 표준

본 장에서는 현재 자율주행차 운영환경에서의 통신 보안 표준인 IEEE 1609.2와 SCMS(Security Credential Management System)에 대해 다룬다.

3.1 IEEE 1609.2 표준

IEEE 1609.2 표준은 차량 간 및 차량-기지국간에 교환되는 메시지에 대한 암호화나 무결성 지원 기능 등을 제공하고 있다. 해당 표준에서는 전자서명과 암호화 기술을 활용, 인정서를 기반으로 안전한 통신을 구현한다. 메시지 무결성 지원을 위한 서명 기능은 비대칭키 기반의 ECC(Elliptic Curve Cryptography) 알고리즘을 이용하며, 암호화 기능은 대칭키 기반의 AES- CCM(Advanced Encryption Standard - Counter with CBC-MAC) 암호화 알고리즘을 이용한다[4].

3.2 SCMS

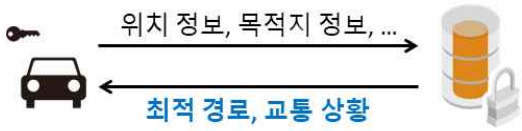
SCMS는 V2V(Vehicle to Vehicle) 및 V2I(Vehicle to Infra) 통신을 위한 POC 메시지 보안 솔루션이다. 이는 암호화 및 인증서를 활용하여 신뢰할 수 있는 통신을 구성한다. 프라이버시 데이터를 유지하며, 오작동 장치를 식별하고 제거하여 메시지의 내용을 보호하는 역할을 한다[5].

IV. 자율주행차 운영환경 보안 취약점

지금까지 제어과정에서의 공격을 통해 차량을 악의적으로 제어하는 사례가 대부분이었다. 본 장에서는 제어 과정이 아닌 인지와 판단과정에서 발생 가능한 보안 취약점에 대해 다룬다.

4.1 MITM(Man in the middle attack)

자율주행차는 데이터 센터에 자신의 위치 정보, 목적지 정보 등을 전송하여 주변의 교통상황 및 최적의 경로를 제공받게 된다. 정상적인 통신 과정이라면 다음 그림과 같이 제공받은 데이터를 바탕으로 자율주행차가 최적의 경로를 판단하여 목적지까지 주행하는 것이다.



[그림 1] 정상적인 데이터 송수신 과정

위와 다르게 악의적인 공격자가 개입하여 데이터에 대한 무결성을 침해할 경우 올바른 판단을 하지 못해 목적지까지 최적의 거리가 아닌 비정상적인 길로 주행하게 된다.



[그림 2] 비정상적인 데이터 송수신 과정

4.2 프라이버시 침해

자율주행 환경에서 오고가는 데이터에는 앞에서 다룬 위치 정보, 목적지 정보, 주행거리, 자율주행차의 정보 등 민감한 정보들이 담겨져 있다. 자율주행차 운영환경 중 발생하는 데이터를 분석함으로써 사용자가 하루에 집을 비우는 빈도, 자주 가는 장소 등 자신의 생활에 대해 노출하게 된다. 해당 정보들을 악용해 사용자에게 직접적인 피해를 입힐 수 있다.



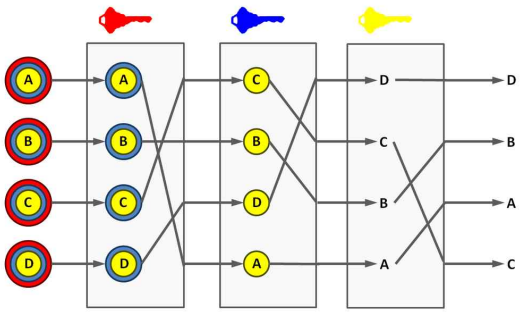
[그림 3] 프라이버시 침해 과정

V. Mixnet 적용을 통한 자율주행차 운영환경 프라이버시 보호

본 장에서는 기존의 인증서를 활용한 방법이 아닌 Mixnet이라는 기술을 활용하여 자율주행차 운영환경에서 발생 가능한 프라이버시 침해에 대한 대응책을 제안하였다.

5.1 Mixnet 개념

여러 발신자로부터 메시지를 가져와서 임의의 순서로 다음 대상으로 다시 보내는 믹스라는 프록시 서버 체인을 사용하여 추적하기 어려운 통신을 만드는 라우팅 프로토콜이다. 다수의 프록시 서버를 사이에 두고, 각각의 노드가 암호화된 메시지를 주고받는 과정을 여러번 수행한다. 또한 각 Mix 내부의 순서를 짐작하기 어렵기 때문에 중간에 도청을 당하더라도 공격자는 데이터 송신자와 데이터 간의 연결 관계를 추측하기 어렵다[6].



[그림 4] Mixnet 과정

위 그림은 간단한 Mixnet 구성도이다. 메시지는 일련의 공개키로 암호화되고 각 믹스 노드는 자체적인 비공개키를 사용하여 암호화 계층을 제거합니다. 각 노드는 메시지 순서를 섞어 결과를 다음 노드로 전송합니다.

5.2 Mixnet을 적용한 자율주행차 운영환경

앞에서 다룬 Mixnet 개념과 자율주행차를 접목시켜 자율주행차가 각각의 노드가 되어 각 자율주행차량의 공개키로 암호화한다. 그 후 Mix 서버가 암호문을 복호하고 결과의 순서를 랜덤하게 배열하여 프라이버시 데이터를 보호할 수 있다.

현재 믿을 수 있는 제 3자가 있다는 가정아래 인증서 기반 익명성 통신을 제공하지만, 본 논문에서 제안하는 기술은 제 3자가 존재하지 않아도 익명성을 가질 수 있다는 점이 가장 큰 특징이다.

Mixnet을 적용한 자율주행 운영환경에서의 데이터 전송 단계는 다음과 같다.

*가정: 3번의 믹스를 거침

Step 1. 랜덤으로 주변 차량 3대(A, B, C)의 공개키 수집

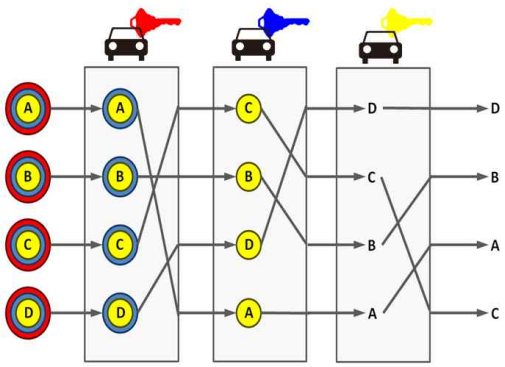
Step 2. 보내고자 하는 데이터를 수집한 공개키로 암호화

Step 3. 첫 번째 믹스를 거치면 A의 개인키를 통해 데이터 복호화 진행

Step 4. Step 3과 동일하게 진행

Step 5. 복호화가 완료되면 데이터만 존재

본 논문에서 제안하는 Mixnet 기술은 모든 믹스가 침해되지 않는 이상 안전하게 데이터를 보호 가능하다.



[그림 5] 자율주행차와 Mixnet 접목

5.3 Mixnet 적용을 통한 기대효과

Mixnet 적용을 통해 3장에서 도출한 자율주행차 운영환경에서 발생 가능 보안 취약점에 대해 보호가 가능하다. 데이터 송신자와 데이터 사이의 연결 관계를 없애 중간자 공격이 통하지 않게 하며 대응관계를 알 수 없어 해당 데이터가 누구의 데이터인지 알 수 없다. 따라서 데이터에 대한 정보를 획득하여도 데이터를 악용하여 2차적인 피해를 입힐 수 없다.

VI. 결론 및 향후 연구방향

현재 자율주행차 운영환경에서는 SCMS 규격을 기반하여 인증서를 통한 익명성 보호를 추구하고 있다. 믿을 수 있는 제3자가 필요한 현재의 익명성 보호는 우리가 현재 사용하고 있는 공인인증서와 같이 불안한 점은 계속 존재할 것으로 예측된다. 본 논문에서 다룬 Mixnet 기반 통신은 믿을 수 있는 제3자가 존재하지 않아도 자율주행차 운영환경에서 발생하는 프라이버시 데이터를 보호가능하다. 데이터 송신자와 데이터 간의 연결성이 없을 뿐만 아니라 자율주행차가 각각의 노드가 되어 데이터를 랜덤으로 배열함으로써 익명성을 보장하고, 중간에 도청을 당한다 하더라도 사용자와 사용자 메시지 간의 연결성이 존재하지 않아 역추적이 불가능하다.

향후 연구로는 본 논문에서 제안한 결과를 바탕으로 현재 SCMS에서 제안하는 기술과 Mixnet을 적용한 기술을 비교하는 연구가 필요하며, 실제 자율주행차 운영환경에 적용 가능한 프로토콜을 개발하고 검증하는 연구가 필요하다.

본 연구는 2018년도 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 과제입니다. (No. 20162220200010)

[참고문헌]

[1] 이현숙, 자율주행자동차 기술개발의 특징 및 정책동향, 융합연구정책센터, 2017.10.

[2] 권혁찬 외 5명, 자율주행 자동차 보안기술 동향, ETRI, 2018.02.

[3] 자율주행 자동차 기술동향, 한국전자통신연구원, 2013

[4] IEEE 1609.2-2013: IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Security Services for Applications and Management Messages, April, 2013.

[5] Security Credential Management System Proof - of - Concept Implementation EE Requirements and Specifications Supporting SCMS Software Release 1.2.2, Made Available to the United States Department of Transportation National Highway Traffic Safety Administration (NHTSA), November, 2016.

[6] Wikipedia, Mix network, May, 2018.

2018 한국정보보호학회 하계학술대회

A8 CPS보안

서 정 택 (순천향대학교)

- **스마트 가로등 환경에서의 보안 설계 및 실험**
  오진혁, 한주홍, 양광열, 이옥연
- **스마트시티 서비스에 대한 사이버공격 피해사례 및 파급효과 분석**
  김 호, 박영훈, 백인홍, 신바야르, 서정택
- **안전한 스마트공장 연계를 위한 크로스 도메인 보안 방법**
  김기현, 박혜용, 안혜선, 김일용, 하재철
- **국내 스마트시티 인프라 사이버보안 취약점 분석 및 대응방안 제시**
  이성원, 송진우, 서정택

스마트 가로등 환경에서의 보안 설계 및 실험

오진혁, 한주홍, 양광열, 이옥연
국민대학교 정보보안암호수학과

An Experiment in smart streetlight environment applied security

Jin Hyeok Oh, Ju Hong Han, Kwang Yeol Yang, Okyeon YI
Dept. of Information Security Cryptography Mathematics
Kookmin University

요 약

가로등은 밤길에 보행자와 차량 운전자의 어두운 길목을 밝혀주는 필수 시설이다. 최근 국내에 주변 밝기나 사물의 움직임을 감지해 자동 또는 원격으로 조도 및 동작이 제어되는 스마트 가로등이 빠른 속도로 설치되고 있다. 실제로 부산광역시에 SK telecom, 과학기술정보통신부가 주관하여 LoRa를 활용한 스마트 가로등 구축사업이 진행되고 있다. 스마트 가로등 환경에서는 센서 데이터들이 무선 통신인 LoRa, LTE로 데이터 송·수신이 되고 있으며 이에 따른 데이터 노출 및 위·변조, 중간자 공격, 재전송 공격, 내부망 접근과 같은 수많은 보안 위협이 존재한다. 본 논문에서는 LoRa를 활용하여 스마트 가로등 환경을 구축하고, 위와 같은 위협에 대해 보호할 수 있는 End-to-End 보안과 SSL VPN 기술을 스마트 가로등 환경에 적용하고자 한다.

I. 서론

생활편의시설인 가로등은 밤길에 보행자와 차량 운전자의 어두운 길목을 밝혀주는 필수 시설이다. 이러한 가로등 시설에 최근에 IoT를 접목한 스마트 가로등이 국내에 도입되고 있다. 스마트 가로등은 주변 밝기나 사물의 움직임을 감지해 자동 또는 원격으로 조도 및 동작이 제어되는 시스템으로 밝기 조절 뿐 아니라 CCTV와 음향 감지 시스템을 활용해 주변 정보를 통신 및 관제 시스템을 통해 불필요한 전력 사용을 줄이고 범죄예방까지 하는 다양한 기술이 접목된 4차 산업혁명 시대에 IoT 기술이다. 실제로 과학기술정보통신부, SK telecom이 주관하여 LoRa를 활용한 스마트 가로등을 부산광역시에 8만7천여 개를 도입하는 지능형 전력망 구축사업을 추진하고 있다[1]. 하지만 이러한 스마트 가로등에서는 유·무선 통신환경에서의 데이터 노출 및 위·변조, 통신 기기들에 대한 인증에 대한 문제가 존재하고 있다.

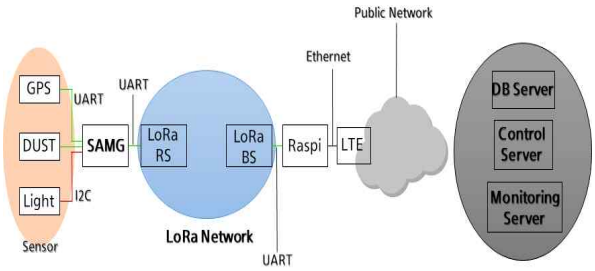
본 논문에서는 IoT 통신중 하나인 LoRa (Long Range) 통신을 활용하여 스마트 가로등 네트워크 환경을 구축하고, Cortex M4 기반의 MCU에 국내 암호알고리즘인 LEA를 활용한 데이터 암·복호화와 SSL VPN을 적용하여 센서 데이터를 관제서버로 전송하는 서비스를 구성하였다. 위와 같이 스마트 가로등 통신 환경을 구축한 이유와 보안 기술 적용에 대한 기대효과 및 MCU에서 암호를 탑재 했을 때의 성능에 대해 서술하고자 한다.

II. 본론

본 장에서는 LoRa를 이용하여 스마트 가로등 네트워크를 구성하고 스마트 가로등 네트워크에 있는 보안위협을 제시한다[2]. 그리고 그에

따른 보안 솔루션을 제안한다.

2.1. LoRa를 활용한 스마트 가로등 네트워크 구성



[그림 1] 스마트 가로등 네트워크 예상 구성도

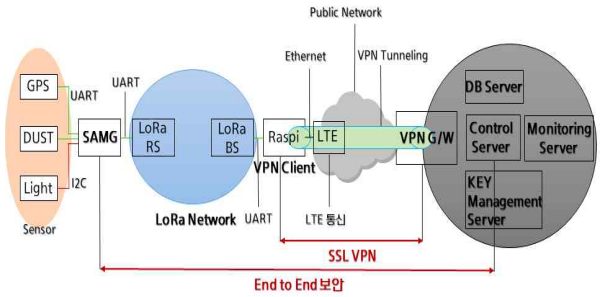
IoT 환경은 목적에 따라 데이터 전송 빈도수와 크기가 다르다. 따라서 그에 맞는 적절한 통신 방법을 선택해야 한다. 스마트 가로등 환경에서는 주변 센서 데이터를 수집해 20~80 바이트 내외인 소량의 데이터를 전송하며, 한번 설치 시 3~10년까지의 사용을 목표로 한다. 또한, 유선통신의 경우 통신설비 설치비용 및 유지보수 비용이 무선통신에 비해 크다. 이러한 소량의 데이터를 전송할 때에는, LPWA (Low-Power Wide-Area) 기술을 사용할 수 있다. LPWA는 저전력, 낮은 구축비용, 넓은 커버리지 등과 같은 특성을 가지고 있으므로 스마트 가로등 환경에서 사용될 수 있다. LPWA 기술에는 대표적으로 LoRa, NB-IoT 등이 있는데 NB-IoT의 경우에는 이동통신사 망을 사용하여 비용이 발생하여 NB-IoT 보다는 정부로부터 별도의 사용 허가 없이 사용 가능한 ISM band(Industrial Scientific Medical band)를 사용하는 LoRa를 선택하였다[3][4]. 실제 스마트 가로등에서 수집한 데이터를 LoRa망을 활용해 데이터를 중앙 관제서버까지 전송해야 하는데 LoRa RS(Radio Station)들로부터 데이터를 전송받는 LoRa BS(Base Station) 에서는 IP를 사용할 수 없기 때문에 LoRa망만 가지고서는 중앙 관제 서버까지 데이터 전송이 불가능하다. 따라서 Gateway 역할을 하는 Raspberry Pi 3를 두고 LTE 모뎀의 DHCP (Dynamic Host Configuration Protocol)기능을 통해서 기기에 IP를 할당 해 서버와 통신을 수행할 수 있게 하였고, Raspberry Pi 3와 LoRa BS는 UART를 사용해 통신하도록 구성하였다.

2.2. 보안 위협

보안이 적용되지 않은 스마트 가로등 환경에서는 센서 데이터가 암호화 되지 않고 무결성 검증을 하지 않은 채 무선 통신인 LoRa, LTE로 송·수신되기 때문에 데이터 유출 및 데이터 위·변조의 위협이 있다. 또한 데이터-출처인증, 사용자 인증을 하지 않으므로 중간자 공격, 재전송 공격도 가능하다. 그리고 스마트 가로등 환경에 필요한 기기들은 각각 서로 다른 회사 제품이기 때문에 기기들에 백도어가 설치되어 있을 가능성도 없지 않아 있다.

따라서 본 논문에서는 End-to-End 보안, SSL VPN기술을 적용을 하여 위와 같은 공격들에 대처할 수 있는 방법을 제시하고자 한다.

2.3. 보안 적용



[그림 2] 보안이 적용된 스마트 가로등 네트워크 구성도

본 절에서는 실험에 사용한 SSL VPN을 사용할 때의 요구사항을 설명하고 End-to-End 보안, SSL VPN이 제공하는 보안적 기능 및 기대효과에 대해 설명한다.

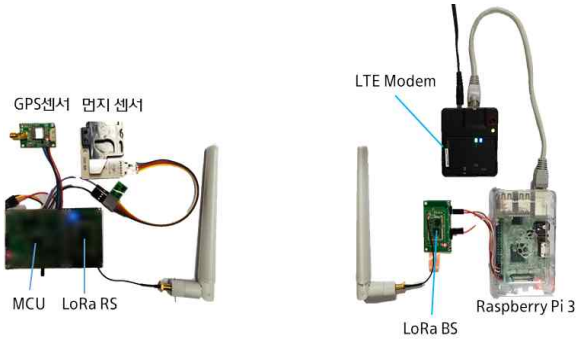
위 [그림 2]를 보면 MCU와 중앙제어서버 구간에서 End-to-End 보안을 적용하였다. MCU는 센서 데이터를 수집하여 국내 암호알고리즘인 LEA-128-CTR 알고리즘을 사용하여 데이터를 암호화하여 기밀성을 제공하고, SHA-256 알고리즘을 사용하여 무결성을 검증함으로써

데이터 노출 및 위·변조에 대한 위협으로부터 데이터를 보호할 수 있다. 그리고 통신 기기들에 백도어가 설치되어 있더라도 데이터가 암호화 되어있기 때문에 데이터가 노출되더라도 공격자는 의미 없는 데이터들을 보게 되어 백도어의 위협으로부터 데이터를 보호할 수 있다.

Raspberry Pi 3와 중앙 관제서버 구간에는 LTE용 라우터 SSL VPN 기술을 활용하여 보안을 적용하였다[5]. 위 실험에서 사용한 LTE용 라우터 SSL VPN 터널에서는 검증필암호모듈의 검증 대상 알고리즘인 LEA를 사용하여 기밀성을 제공하여 데이터 노출에 대한 위협을 보호할 수 있다. 검증필암호모듈의 검증 대상 알고리즘을 사용한 이유는 전자정부법 56조와 동법 시행령 69조에 따라 국가·공공기관에서는 국가정보원장이 검증한 검증필암호모듈 탑재가 필수이기 때문이다[6]. 그리고 LTE용 라우터 SSL VPN 터널에서 SHA-256를 사용하여 데이터 무결성을 검증함으로써 데이터 위·변조에 대한 위협을 보호할 수 있다. 또한 ECDSA p-256 기반 인증서를 사용하여 상호 인증 기능도 제공함으로써 인증되지 않은 기기나 공격자의 내부망 접근, 중간자 공격, 재전송 공격과 같은 보안 위협으로부터 데이터를 보호할 수 있다. 또한 LTE 라우터용 SSL VPN 터널 형성에 사용되는 TLS는 v1.2를 지원하여 안전한 프로토콜을 구성할 수 있다[7][8]. 따라서 검증필암호모듈이 탑재된 LTE 라우터용 SSL VPN을 사용함으로써 기밀성, 무결성, 인증을 제공하여 스마트 가로등 환경에서 발생할 수 있는 보안 위협에 대해 보호할 수 있다.

2.4. 실험 환경

본 논문에서 진행한 실험은 아래 [그림 3]과 같다.



[그림 3] 실험환경 구성

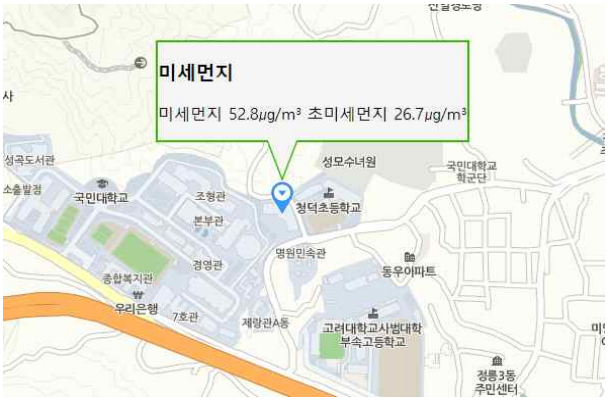
LTE 통신 및 LTE 라우터용 SSL VPN을 지원하기 위해서는 우선 IP 통신이 가능해야 하고, S/W 기반 암호모듈 동작을 위해서 OS가 탑재된 기기가 필요하다. 동시에 LoRa BS가 UART 통신을 지원하기 때문에 UART 통신이 지원 가능한 기기가 필요하다. 위의 조건을 만족시키는 기기들 중 우리는 Raspberry Pi 3을 실험에 사용하였는데, Raspberry Pi 3은 Ethernet 모뎀과 UART 모뎀을 탑재하였고 OS는 기본 리눅스를 제공하기 때문에 위와 같은 동작 환경을 제공할 수 있었다[10].

센서는 GPS센서, 먼지센서로 구성하였으며 MCU가 센서 데이터를 수집하여 LEA-128-CTR을 사용하여 암호화를 한다. 그리고 UART, LoRa 통신을 통해 Raspberry Pi 3까지 데이터 송신이 된다. Raspberry Pi 3에는 본 랩에서 보유한 검증필암호모듈 KMULiB v2.0을 탑재한 LTE 라우터용 SSL VPN 클라이언트를 적용하고 BS로부터 수신한 암호화된 데이터를 LTE 통신을 통해 중앙 관제서버까지 전송한다. 이때, LTE 라우터용 SSL VPN에서 LEA-128-CTR을 사용하여 데이터를 암호화하여 기밀성을 제공하고, SHA-256을 사용하여 무결성 검증을 하였다. 그리고 LTE 라우터용 SSL VPN에서 ECDSA p-256 기반 인증서를 사용하여 상호 인증을 제공하였다.

중앙 관제서버는 Ubuntu 16.04버전의 서버를 사용하였고 KMULiB v2.0를 탑재한 SSL VPN 게이트웨이를 구성하였다.

2.5. 실험 결과

아래 [그림 4]은 중앙제어서버에서 센서 데이터를 수집하여 네이버 지도 API를 사용해 센서 데이터 값을 나타낸 결과이다.



[그림 4] 복호화를 실행한 서버 결과

2.5.1 암호 탑재 성능 분석

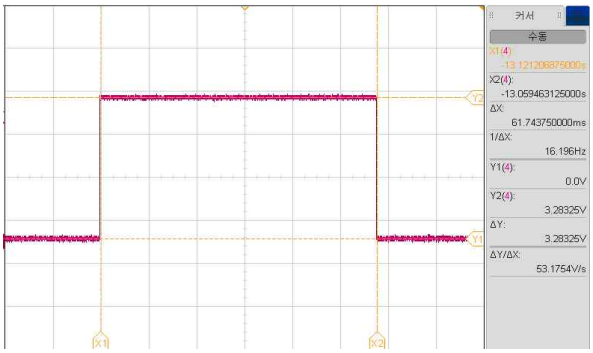
암호화 처리 속도는 내부 MCU의 알고리즘 속도, 암호 키 및 암호 처리를 위한 핵심 구성 요소뿐만 아니라 CRC(Cyclic Redundancy Checking)를 포함한 데이터 입출력 속도에 따라 달라진다. 또한, 각각의 처리속도는 MCU, 컴파일러, 운영 환경에서 각각 다른 측정치를 보인다[9]. 따라서 아래 [그림 7], [그림 8]과 같이 오실로스코프를 사용하여 암호화 처리 속도를 측정하였으며 실험을 위해 [그림 5]의 동작환경 에서 [그림 6]와 같이 컴파일 된 실행코드를 적용했다.

Categories	Target
CPU	Cortex-M4 120MHZ 32-bit
Memory	SRAM 160 KB 이상 Flash 256 KB 이상
IDE	Atmel Studio 7.0, ARM/GCC 6.3.1 (Advanced Software Framework 4)

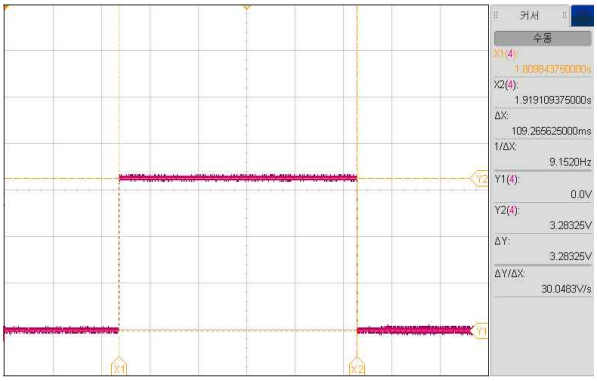
[그림 5] 동작환경 정보

Categories	MCU
Optimization	-O0
Binary Code	11 KB
LEA-128-CTR	4 KB

[그림 6] 컴파일환경 정보



[그림 7] 암호화 되지 않은 데이터 전송 시간



[그림 8] 암호화 100회 시행 후 데이터 전송 시간

[그림 7]의 Δx값 61.743750000ms는 50바이트의 암호화 하지 않은 데이터를 전송하는데 걸린 시간이다. [그림 8]의 Δx값 109.265625000ms는 50바이트 데이터를 LEA-1 28-CTR을 적용한 암호화 100회 시행 후 전송하는데 걸린 시간이다.

즉, 50바이트 데이터에 LEA-128-CTR을 이용한 암호화 1회 수행 시에는 약 0.475ms만큼의 시간이 필요했다. 50바이트의 암호화 하지 않은 데이터를 전송하는데 걸린 시간인 61.743750000ms에서 암호화 1회 수행 시 걸린 시간 0.475ms라는 시간은 데이터 전송에 있어 대략 0.77% 라는 아주 작은 성능저하가 발생하므로 통신과정에 암호 알고리즘을 충분히 적용할만하다.

III. 결론

현재 국내에 스마트 가로등의 도입이 빠르게 진행되고 있다. 스마트 가로등에 보안이 적용되

지 않았을 시 영상 데이터 유출로 인해 사생활 침해와 같은 수많은 보안 위협 사례가 생겨날 수 있으므로 보안 적용이 시급한 상황이다. 이에 본 논문에서는 생겨날 수 있는 보안 위협들로부터 기기 성능에 영향을 크게 주지 않고 데이터를 보호할 수 있는 보안 기술을 제시하였다.

향후 스마트 가로등 환경에서 LoRa 망에서의 안전한 보안 프로토콜 설계, 키 관리 등 추가적인 보안기술에 관한 연구가 필요하다.

[참고문헌]

[1] 글로벌 스마트시티 스마트 가로등, http://k-smartcity.kr/service/service04.php

[2] 한주홍, 오진혁, 이재훈, 이옥연, “LoRa를 활용한 IoT 환경에서의 보안 설계 및 실험”, 2018 한국통신학회 동계학술대회, 2018. 01

[3] 전자통신동향분석, https://ettrends.etri.re.kr/ettrends/158/0905002120/0905002120.html

[4] About LoRa Alliance, https://www.lora-alliance.org/

[5] 장찬국, 이재훈, 이옥연, “공공 무선망의 보안을 위한 SSL VPN 적용 방안에 관한 연구”, 2018 한국통신학회 동계학술대회, 2018. 01

[6] KS X ISO/IEC 19790, 24759 Korea Cryptographic Module Validation Program

[7] NIST Special Publication 800-113, Guide to SSL VPNS

[8] NIST SP 800-52, Guidelines for the Selection and Use of Transport Layes Security (TLS), at http://csrc.nistgov/publications/nistpubs/

[9] 안현정, 윤승환, 이옥연, “Performance Evaluation of Firmware Cryptographic Modules on Various MCU Environments”, IEEE, 2016.04

[10] Raspberry Pi Learning Resources, https://www.raspberrypi.org/

스마트시티 서비스에 대한 사이버공격 피해사례 및 파급효과 분석

김호, 박영훈, 백인홍, 신바야르, 서정택

순천향대학교 정보보호학과

Analysis of Cyber Attack Damage and Its Effect on Smart City Service

Ho Kim, Young-hoon Park, In-hong Baek, Shinebayar, Jung-Taek Seo

Department of Information Security Engineering, Soonchunhyang University

요 약

최근 제4차 산업혁명의 시대가 도래하면서 첨단 정보통신기술과 기존의 산업이 융합되어 새로운 산업이 형성되고 있다. 스마트시티는 제 4차 산업혁명에 의한 도시발전 형태로 모든 사물이 네트워크로 연결되어 서비스를 제공하는 도시이다. 사물 네트워크를 구성하기 위해 다양한 무선 네트워크 기술이 적용되고 있지만, 다양한 취약점 분석을 통한 보안위협이 존재하며 무선 네트워크를 공격했을 때 파급효과는 치명적인 피해가 예상이 된다. 이에 따라 본 논문은 최근 설계되는 스마트시티의 네트워크를 목표로 한 공격시나리오에 대한 파급효과와 대응방안을 제시한다.

Keyword : IoT, SmartCity, ZigBee, Bluetooth, Wireless-network, Cyber-Attack

I. 서론

최근 대통령직속 4차 산업혁명위원회가 발족되어 부산의 에코델타시티, 세종시의 5-1 생활구역, 올 하반기에는 추가적으로 스마트시티 조성에 박차를 가하기 위하여 추가적인 계획을 갖고 있다. 스마트시티란, 정보통신기술을 기반으로 도시와 사람이 하나의 신경망처럼 구성되어 사람에게 편의를 서비스하는 것과 동시에 도시에서 소모되는 자원들의 효율적인 관리를 실현시키는 도시를 말한다. 예를 들어 교통량의 관리, 효율적인 에너지 관리를 통한 운영비절감, 사용자 친화적인 환경 제공 등을 볼 수 있다[1]. 스마트시티를 구성하기위해서는 표 1의 기술들이 사용된다. 스마트시티에 적용가능한 통신기술을 지원하기 위해서 5G, 와이파이 등의 무선통신기술이 주목받고 있으며, 이와 함께 실내 메쉬 네트워크 인프라를 구축하는 저전력 통신프로토콜로 ZigBee(지그비)와 Bluetooth(블루투스) 등의 기술들이 제시되고 있다[2]. 저전력 통신프로토콜은 통신 인프라의 구축이 어려운 장소에 설치되어, 패킷 암호화, 통신 주파수 호핑 등의 보안기능을 제공하며 장기간동안 네트워크를 유지할 수 있다. 하지만 저전력 장치의 한계로 한정된 환경에서 연산되는 보안기능은 쉽게 공격이 가능하며 통신 프로토콜 상의 보안취약점도 발견되고 있다. 본 논문은 스마트시티에 사용된 무선 통신 네트워크가 가질 수 있는 취약점을 정리하고, 공격자가 네트워크를 공격 시도했을 때의 파급효과와 이에 따른 대응방안을 제시한다.

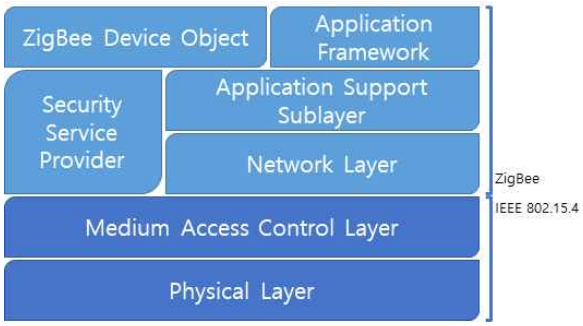
센서	각종 수단을 통해 주위의 데이터를 정확히 수집
통신	유/무선 통신을 통해 디바이스간의 데이터를 교환
분석	수집된 데이터를 분석하여 필요에 따른 서비스를 제공

표 1. 스마트시티 구성 기술

II. 무선 통신 취약점

저전력 프로토콜 단체에서는 개발자를 위해 프로토콜 구조를 공개하고 개발킷을 배포하고 있다. 많은 개발자들이 이 개발킷을 이용하여 제품을 제작하거나 보다 나은 프로토콜을 위해 분석하고 있다. 이미 전부터 주목받아온 Bluetooth(블루투스)는 지금까지도 많은 취약점이 발견되어 패치 하였으며 개선된 프로토콜 구조와 하드웨어 기술을 통해 Bluetooth 5.0까지 공개 되었다. ZigBee(지그비)의 경우 블루투스보다 느린 전송속도를 지원하지만, 가격이 매우 저렴하고, 구조가 간단하며 배터리 수명이 타 무선 통신기술들보다 길어 근거리 단순통신 무선 네트워크 구성에 적합한 기술로 기대받고 있다. 프로토콜 패킷레이어에서 자체적으로 보안기능을 지원하지만 저전력 프로토콜의 한계로 높은 수준의 보안기능을 지원하지 못한다. 본 장에서는 블루투스와 ZigBee에서 발견된 취약점을 분석하고 공격방법을 설명한다[3][4].

2.1 ZigBee(지그비)의 취약점



[그림 1]. ZigBee 스택구조

지그비는 IEEE 802.15.4 프로토콜을 기반으로 [그림 1]의 스택구조로 구성되어 있다[4]. ZigBee의 보안은 SSP(Security Service Provider)에서 기본 보안모드와 높은수준의 보안모드를 지원한다. 암호화 키는 표 2의 MK, LK, NK의 3종류로 128비트 대칭키 블록암호화와 인증기능을 사용하며 Open Trust Model을 사용해 장치 스스로의 신뢰성만을 보장하고 다른 장치가 암호화과정을 알 수 없게한다. 신규 ZigBee장치가 네트워크에 가입할 때, NK 또는 MK를 전송하여 네트워크 키를 분배하는데 이 키를 안전하지 않은 채널을 사용하여 교환하기 때문에 키가 노출되는 문제가 있다. 또한 이때 추가되는 노드에 대한 인증이 이루어지지 않고 네트워크 통신 패킷에서 고유 식별자가 노출되는 취약점을 가지고 있다. 위 취약점에 따라 ZigBee에 새로운 노드가 추가될 때 해당 통신을 수집하여 MK, LK를 획득 하거나, 정상적인 노드를 위장하여 네트워크에 연결할 수 있으며, 네트워크에 라우팅되는 패킷을 수집하면 네트워크 구성 형태와 요소를 알 수 있다[5].

키	역할
Master Key (MK)	LK를 생성하기 위해 장치간 공유되는 키
Link Key (LK)	장치간의 메시지를 암호화
Network Key (NK)	네트워크 내 모든 장치가 공유 NWK Layer의 보안을 담당

표 2. ZigBee의 암호화키 종류

2.2 Bluetooth(블루투스)의 취약점

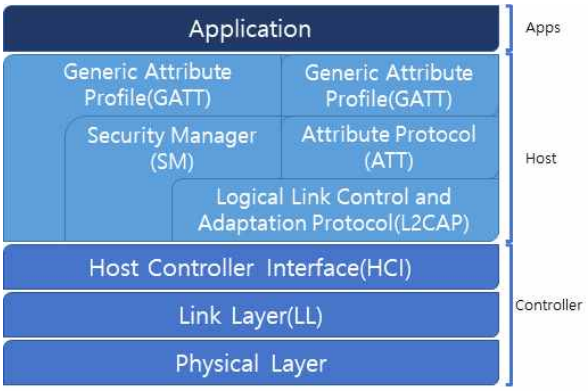


그림 2. Bluetooth 스택구조

블루투스는 무선 개인 통신망 표준 위원회의 태스크 그룹 1(IEEE 802.15.1)에서 다뤄지는 무선통신 기술로 현재는 Bluetooth SIG(Bluetooth Special Interest Group)의 단체로 구성되어 연구, 개발이 이뤄지고 있다. 블루투스의 스택은 그림 2의 Controller, Host, Apps로 구성된다[6]. 블루투스의 보안기능은 Host의 Security

키	역할
Temporary Key (TK)	STK를 생성하기 위해 사용되는 임시키
Short Term Key (STK)	연결의 암호화를 위해 사용하는 임시키
Long Term Key (LTK)	재연결 시 암호화에 사용하는 키

표 3. Bluetooth의 암호화키 종류

Manager에서 지원하여 블루투스 장치간의 페어링 무결성, 암호화와 인증을 관리한다. 블루투스 네트워크 장치는 Master와 Slave로 이루어져 있어 페어링 시 표 3에서 정리된 128bit의 키를 교환해 Slave가 Master에 등록되는 형태로 네트워크에 연결된다. 블루투스는 페어링을 통해 교환한 키를 기반으로 일정 주파수 대역을 계속 바꿔가면서 통신을 하는데 이를 호핑이라고 한다. 이 기능으로 블루투스는 타 무선 통신기술보다 주파수 간섭과 재밍공격에 강하다. 이 때문에 타 무선 통신기술보다 통신패킷 수집이 어렵지만 패킷 수집 디바이스로 쉽게 수집이 가능하다. 블루투스 장치는 실행 중 주기적으로 연결가능한 장치를 스캔하기 때문에 네트워크 작동 중 모든 장치가 노출될 수 있다. 장치가 특정되면 해당 장치에서 송신되는 패킷을 수집할 수 있고, 프토토콜 취약점을 이용한 암호화키 및 데이터를 획득하여 장치에 대한 접근권한을 얻을 수 있다. 또한 단순히 노출된 장치에 대한 지속적인 접속요청으로 블루투스 장치의 수명을 줄이는 공격을 할 수 있다[7][8].

III. 스마트시티 서비스 네트워크 구조

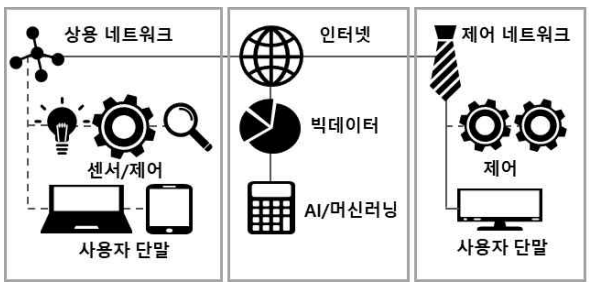


그림 3. 스마트시티 서비스 네트워크 구조

스마트시티의 전체적인 네트워크는 그림 3과 같이 데이터를 수집하는 센서와 센서의 데이터를 모으는 마스터 장치, 수집된 데이터를 저장하고 처리하는 서버, 수집된 정보를 사용자에게 제공하는 UI(User Interface)장치들로 구성되어 있다. 서버와 원격에 위치한 마스터 장치는 유선통신으로 연결되며 무선통신으로 대체할 경우 두 장치에는 충분한 하드웨어 기술이 적용되어 높은 수준의 보안을 지원하는 네트워크를 구성할 수 있다. 서비스 지역에서는 마스터 장치를 게이트웨이 역할로 하는 무선 메쉬(Mesh) 네트워크를 구성한다. 메쉬 네드워크의 모든 장치들은 스스로 라우터의 역할을 하여 다른 장치를 네트워크에 연결한다[9]. 네트워크에서 한정된 전력으로 운용되는 센서는 장기간 운용을 목적으로 설계된 ZigBee, Bluetooth 등의 저전력 통신 프로토콜을 사용하여 낮은 보안수준에 의한 많은 취약점과 공격위협을 가지고 있다. 본 장에서는 센서의 무선 네트워크가 연결된 스마트시티 서비스의 구조를 상용 네트워크와 제어 네트워크로 나누어 분석한다.

3.1 상용 네트워크 서비스

상용 네트워크는 인터넷에 연결되어 주로 홈 네트워크와 빌딩 관리 네스워크를 말한다. 상용 네트워크는 사용자의 편의를 제공하거나 효율적인 에너지 관리를 통한 관리비의 절감을 목적으로 한다. 사용자의 요구에 맞는 서비스 제공을 위해 상용 네트워크의 통신 데이터는 사용자의 개인정보가 많이 포함되어 있다. 통신 프로토콜이 설치된 단말들이 메쉬 네트워크를 형성하고 데이터를 수집하고 수집한 정보를 인터넷을 이용한 서비스를 제공한다[10].

① 홈 네트워크 서비스

스마트시티의 홈 네트워크에서 사용자에게 서비스하는 장치들은 대부분 중앙 제어시스템에 연결되거나 개인 비서 AI 장치에 연결되어 서비스를 제공한다. 사용자는 인터넷과 연결된 제어시스템에 연결하여 원격에서 홈 네트워크를 제어할 수 있다[11]. 실내 일조량을 수집하여 실내 전등 밝기를 조절할 수 있고, 사용자의 귀가시간에 맞추어 미리 불을 켜 둘 수 있다. 전력이나 가스의 사용을 제어하여 사용자가 자택에 있을 때 사용자의 위치와 이동 경로를 확인하여 서비스를 제공한다. 또한 개인정보를 입력하여 사용자의 취향에 맞는 서비스를 제공하여 최적의 생활환경을 조성한다.

3.2 제어 네트워크 서비스

제어 네트워크는 특정 대상에대한 데이터를 수집하고 사용자가 원하는 작업을 수행하는 서비스를 제공한다. 홈 네트워크보다 넓은 범위의 네트워크 망을 구성하여 데이터를 수집하여 필

요한 정보를 도출한다. 생산에 관련된 제어 시스템에서는 대상으로한 장비가 수행할 작업을 명령하고 장비의 이상 유무 등을 보고받는다. 제어 네트워크에서 전달되는 데이터는 환경 정보의 전달이기에 단순 유출시에는 큰 문제를 야기하진 않지만 데이터가 전송중에 변조되거나 네트워크의 문제로 수신을 하지 못했을 때 큰 문제가 발생할 수 있다.

① 스마트 가로등

스마트 가로등과 메쉬 네트워크에서 전송이 될 정보로는 가로등에 설치된 각기 다른 센서들이 모은 정보로써 일조량을 체크하여 가로등의 밝기 조절, 가로등 CCTV를 통한 방범, 교통사고, 단속 등 스마트시티에 대한 모니터링이 가능해지고, 사용자들의 위치정보를 이용한 안심귀가 서비스, 날씨 정보 등 스마트 도시 서비스를 하기 위한 데이터들이 실시간으로 전송이 이루어져야한다. 이러한 데이터들은 서버에 저장이 되어 안전하게 관리가 되어야 한다.[12]

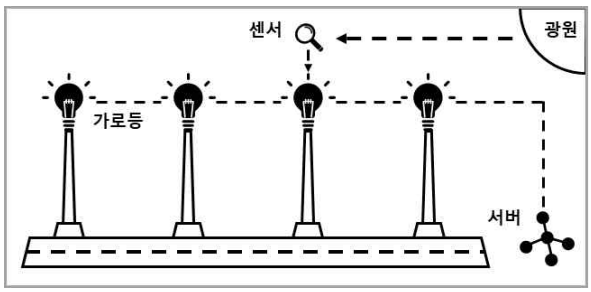


그림 4. 스마트시티 가로등 네트워크

② 스마트 교통

무인 전철과 버스처럼 대중교통수단의 진화가 눈에 띄게 달라질 것이다. 목적지를 설정할 경우 센서들이 사용자의 위치를 파악하여 가장 빠르고 안전한 경로를 찾아 해당하는 대중교통 및 네비게이션의 역할을 해주게 될 것이다. 현재는 도로상의 센서들과 카메라들을 통해 얻어지는 제한된 데이터를 의존하지만 스마트 시티에서는 모든 도로상의 사용자들의 위치정보를 이용할 수 있기 때문에 잠재적인 사고위험이 줄어들고 더욱 빠르게 이동을 할 수가 있다.[13]

IV. 스마트시티 서비스 공격 시나리오

본 장에서는 스마트시티의 서비스 네트워크가 3장의 그림 3의 구성으로 이루어졌다고 가정하고 메쉬 네트워크를 구성하는 통신 프로토콜의 취약점을 통한 공격시나리오를 제안한다.

공격 유형	공격 방법
데이터 위변조	패킷 재전송
	장치 탈취-데이터 변조
데이터 유출	암호키 획득
네트워크 공격	DDoS
	재밍

표 4. 무선 네트워크 공격 방법

스마트시티의 서비스를 제공하는 장치들에서 통신되는 데이터는 일반 통신망에서 교환되는 데이터에 비교해서 굉장히 작은 크기를 가지고 있어서 단일의 데이터 유출은 큰 피해를 야기하기 힘들다. 하지만 통신의 재전송 공격이나 네트워크 암호키를 획득하게 되면 메쉬 네트워크 전체의 데이터 수집을 통한 공격이 가능하다. 본 논문의 시나리오는 무선 네트워크 장치에 접근하고 해당 장치에대한 공격을 실행함으로 전체 네트워크를 공격하는 시나리오이다.

① 서비스 장치 접근

무선 네트워크 장치에 접근하여 통신 패킷을 수집한다. 수집한 패킷을 재전송하여 네트워크에 혼란을 줄 수 있다.

통신패킷을 분석하거나 네트워크 가입 취약점을 이용해 네트워크의 암호키를 획득한다. 이 암호키를 기반으로 네트워크의 데이터를 수집하고 변조된 데이터를 전송 할 수 있다.

장치에대한 네트워크 가입 요청을 계속 실행하여 장치의 수명을 단축시킨다.

② 마스터 장치를 통한 인터넷 접근

메쉬 네트워크를 구성하는 장치의 암호키를 획득하면 마스터 장치에 대한 접근권한을 취득할 수 있다. 이를 통하여 마스터 장치를 공격하여 데이터를 유출하거나, 외부 DB에서 처리되는 데이터에 혼란을 야기할 수 있다.

이와 같은 시나리오에서 메쉬 네트워크의 공격은 주로 네트워크 암호키 획득을 통해 이루어진다. 장치에 악성코드를 감염시켜 주기적인

시스템		에너지 관제 시스템		출입통제 시스템		생활밀착형 시스템
시스템 개요		구성 환경에서 사용되는 전력, 가스 등의 에너지를 관리하는 시스템		센서, 카메라 등의 장치를 통해 대상을 확인하고 감시하는 시스템		사용자의 개인정보를 토대로 서비스를 제공하는 시스템
구성 네트워크		전력 관리 네트워크	가스 관리 네트워크	CCTV / IP카메라	도어락	개인비서 AI
공격유형	데이터 위변조	전력의 공급/차단을 임의로 변경 에너지 효율감소	가스의 공급/차단을 임의로 변경 가스 안전 위협	장치의 정상적인 인식 불가	정상적인 인가확인 불가	사용자가 원하는 서비스의 정상적인 제공 불가
	데이터 유출	전력 사용 장치를 확인하여 사용자의 사생활 노출	가스 사용량을 확인하여 사용자의 사생활 노출	카메라 정보를 통한 개인의 사생활 노출	인가 정보 노출에 의한 접근권한 탈취	사용자 개인정보 노출
	네트워크 차단/지연	사용자가 요구하는 전력 관리 불가	사용자가 요구하는 가스 안전 위협	감시기능 마비	개폐장치 마비	서비스 제공 불가
시스템		스마트 그리드		교통 제어 시스템		공장 제어 시스템
시스템 개요		전력의 효율적인 생산과 소비를 실현하기 위한 전력 감시 시스템		도로(철도) 위에서의 안전하고 원활한 교통의 흐름을 제어하는 시스템		공장 생산과정을 감시·제어하기 위한 시스템
구성 네트워크		스마트 미터 네트워크	배전 네트워크	자가용 네트워크	무인 대중교통 네트워크	기계 제어 시스템
공격유형	데이터 위변조	전력 소비량 변조 전력 필요량 조작 과금 내역 조작	전력의 과부하 유발	신호등 조작 교통 흐름을 임의적으로 방해	무임승차 교통사고 유발	목적과 다른 기계 제어
	데이터 유출	전력 사용량을 확인하여 사용자의 사생활 노출	지역별 전력 사용량 유출	시스템 내의 이용자 정보 노출	시스템 내의 이용자 정보 노출	명령 탈취에 의한 제품 정보 유출
	네트워크 차단/지연	전력 생산 차질	정상적인 배전 불가	교통 혼잡 사고 유발	무인 대중교통의 오작동	기계 작동 오류 발생

표 5. 서비스 네트워크에서 공격유형에 따른 피해[11][14][15][16]

데이터 유출을 야기하거나 많은 장치를 이용한 DDoS(Distributed Denial of Service attack)공격에 이용할 수 있다. 또한 제어 명령을 수정하여 장치를 파괴하거나 부수적인 피해를 입힐 수 있다.

V. 스마트시티 서비스 공격 파급효과

스마트시티의 서비스 네트워크를 공격했을 때 상용네트워크와 제어 네트워크에 각기 다른 피해가 기대된다. 상용 네트워크에 대한 공격 시 네트워크에서 가장 큰 예상 피해는 개인정보 유출과 사생활 침해를 볼 수 있다. 반면 제어 네트워크에 대한 공격은 시스템 파괴를 야기할 수 있는 피해가 예상된다.

① 상용 네트워크 공격 파급효과

상용 네트워크에서 개인 비서 AI장치를 중심으로 구성된 가정 네트워크가 공격당했을 때, 단순 정보의 유출을 통하여 생활정보가 노출될 수 있다. 보다 고급 정보가 전달되는 IP 카메라 등의 동영상 정보가 유출되면 높은 수준의 사생활 침해가 일어난다. 가정 네트워크가 완벽히 장악되었을 때 공격자가 사용자의 생활을 정확하게 파악하고 출입통제 시스템을 공격하여 사용자의 집으로 침입이 가능하다.

② 제어 네트워크 공격 파급효과

스마트 그리드의 스마트 미터에 대한 공격 실행 시 다수의 스마트 미터를 장악하여 전력 소비량을 실제와 다르게 보이도록 변조한다. 이를 통하여 전력의 공급이 실제 소비량과 다르게 공급되어 정전 또는 에너지 낭비를 야기한다.

댐, 계곡 등의 수위 측정 장치를 해킹할 시 댐의 실제 저수량을 다르게 해 댐의 정상적인 저수능력을 방해한다. 해당 장치를 통해 댐의 방류 시스템에 접근하여 방류량을 조절해 홍수

를 야기하거나, 댐의 붕괴를 유발 할 수 있다.

공장제어 시스템의 장치를 공격했을 시 장치들에 내려진 명령들을 탈취하여 제품 정보를 획득 할 수 있고, 설계된 제품과 다른 작업을 하도록 하여 금전적 피해를 입힐 수 있다.

VI.네트워크 공격 대응방안

본 장에서는 4장에서 나온 공격시나리오를 토대로 대응방안을 제시한다.

장치	개발단계에서 시큐어코딩
	저전력 암호화 알고리즘 보안장비 설치
	취약점 진단을 통한 보안패치 실시
	무선 네트워크 장치에 물리적인 접근제어
네트워크	탈취된 네트워크 초기화·대체를 위한 별도의 네트워크 구성
	대규모 메쉬 네트워크의 구성 중 타 장치의 보안성 지원을 위한 보안장비 설치
	장치 등록 시 해당 장치를 인증 할 수 있는 시스템 구비

표 6. 네트워크 공격 대응방안

VII. 결론

최근 스마트시티에서 일정한 구역 전체를 네트워크를 통해 제어 및 관리가 이루어지도록 설계되고 있다. 이 구역에서 수집되는 정보는 사용자들의 다양한 정보가 담겨있으며 이를 수집하는 장치 또한 타 장치와 연계하여 다양한 서비스를 제공한다. 따라서 이 네트워크에 대한 공격이 이루어 질 경우 파급력이 매우 클 수 있다. 스마트시티의 정상적인 서비스 제공을 위해 네트워크 취약점을 분석하고 제시한 네트워크 공격 시나리오에 대한 파급효과와 대응방안을 제시하였다. 상용 네트워크에서는 사용자의 개인정보의 유출이 가장 큰 피해로 예상되며, 제어 네트워크는 데이터 변조에 의한 금전적 피해발생, 장치의 명령 변조를 통한 기계 오작동에 따른 사고 및 경제적 손실이 예상된다. 따라서 네트워크 공격을 막기 위해 장치, 네트워크 측면의 대응방안을 제시했다. 스마트시티의 발전하면서 더 많은 장치가 네트워크에 연결됨에 따라 커지는 피해를 최소화하기 위해 다방면의 스마트시티 네트워크 공격 시나리오를 작성하고 이에 대한 대응방안에 대한 연구가 필요하다.

"본 연구는 2018년도 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 과제입니다. (No. 20162220200010)"

[참고문헌]

[1] [스마트 홈&시티]미래 도시 문제의 해결책, 스마트 시티! 2018.05.14 삼성증권 블로그 Samsung Pop Brief https://blog.naver.com/samsung_fn/221273448967
[2] DSE 2018, 스마트 시티의 미래를 전망하다. 2018.04.26. Naver-포스트 삼성SDS https://m.post.naver.com/viewer/postView.nhn?volumeNo=15321129&memberNo=36733075&vType=VERTICAL
[3] ZigBee Alliance. http://www.zigbee.org
[4] Bluetooth SIG. https://www.bluetooth.com
[5] Shahin Farahani, ZigBee Wireless Networks And Transceivers, ELSEVIER
[6] 김봉환, 임정미, 박창섭, ZigBee 보안 메커니즘 분석, 보안공학연구논문지, 2012. 10.
[7] Bluetooth Network Encapsulation Protocol (BNEP) Specification, Bluetooth SIG
[8] 권기원, 조성현, Bluetooth Low Energy 보안 취약점에 관한 연구, 한양대학교, 2016.
[9] 이효석, 최형기, 복잡한 통신 프로토콜의 문제점: Bluetooth 인증 프로토콜, 한국통신학회, 2017
[10] 전성환, 무선 메쉬 네트워크의 기술 동향 및 활용 방안, 중앙대학교 대학원, 2008. 06.
[11] LIU, Dan, The Implementation of Smart Home System Based on 3G and ZigBee in Wireless Network System, 전남대학교 대학원, 2012. 08.
[12] 스마트도시에서 스마트 도시재생으로의 접근 가능성, 2017.01.04. 想像의 숲
[13] 2030 스마트 시티의 미래모습 - 스마트 교통, 2016.11.24. 想像의 숲
[14] 김민수, 스마트팩토리 적용이 가능한 IoT 연계형 현장스마트운영자 중심의 제어모듈 설계 및 구현에 관한 연구, 2017. 08.
[15] 최준호, ZigBee를 이용한 스마트 빌딩 활용방안에 관한 연구, 한세대학교 대학원, 2011. 02.
[16] 조광제, 스마트 그리드에서 수요반응을 적용하기 위한 IoT기반의 SEP2.0-6LoWPAN 무선통신 구현, 한양대학교 대학원, 2017. 02.

안전한 스마트공장 연계를 위한 크로스 도메인 보안 방법†

김기현*, 박혜용*, 안혜선*, 김일용*, 하재철**††
*㈜앤앤에스피, **호서대학교

Cross Domain Security Method to Connect Secure Smart Factory

Ki-Hyun Kim*, Hye Yong Park*, Hye Seon An*, Il-Yong Kim*, Jae-Cheol Ha**
*NNSP Co., Ltd., **Hoseo University

요 약

세계적으로 스마트공장은 제조업 경쟁력 강화를 위해 국가 차원의 전략으로 부상하고 있지만 스마트공장에 대한 보안대책은 미흡한 실정이다. 본 논문에서는 생산 공장과 본사를 연계하기 위한 경계보안 모델로 방화벽, 망연계 시스템, 데이터 다이오드의 구성과 보안취약점을 분석하고 스마트공장 환경에서 가장 효율적인 망연계 방법으로 듀얼 다이오드를 이용한 망연계 방법을 제안한다. 본 제안은 공장과 본사 간 상호 자료전달이 가능하며 화이트리스트 기반으로 기업정보 유출을 방지하고 공장정보 위·변조를 차단하며 한쪽 회선이 끊어진 데이터 다이오드 기술을 적용함으로써 본사 또는 외부망에서 현장 공장으로의 해킹을 원천적으로 차단한다.

I. 서론

세계적으로 스마트공장은 제조업 경쟁력 강화를 위한 국가 차원의 전략으로 부상하고 있으나 보안대책은 미흡한 실정이다.

스마트공장은 생산 현장의 설비제어 자동화와 공장 통합운영에서 시작하여 본사의 MES, ERP, PLM 등과 연계되어 공장과 본사 간 상호 자료전달이 이루어지므로 본사 시스템이 해킹될 경우 생산 현장인 공장까지 영향을 미칠 수 있다.

한국인터넷진흥원의 “스마트공장 중요정보 유출방지 가이드”[1]에서는 스마트공장의 기업정보 유출에 중점을 두고 있다. 대부분 보안대책은 IT 보안대책과 유사하며 산업제어시스템 네트워크 구성도에는 공장과 본사 간 상호 자료 교환이 필요한 스마트공장 환경임에도 불구하고 제어시스템 영역을 폐쇄망으로 구성하고 단방향 전송장비로 외부망과 연결하는 구성을 제시하고 있다.

스마트공장추진단과 고려대학교의 “스마트공장을 위한 최소 정보보안가이드라인”[2] 역시 IT 보안대책과 유사하며 내부망으로 침입을 차단하기 위해 방화벽 운영을 권고하고 있다.

이와 별도로 국내 망분리 정책에서는 분리된 망간 자료전송을 위해 망연계 시스템을 사용한다.

국제적으로 산업제어시스템에 대한 보안은 NIST SP800-82[3], ANSI/ISA99[4], ISA/IEC 62443[5] 등에서 찾아볼 수 있으며 경계 보안 모델로 대부분 방화벽을 기반으로 하고 있다.

본 논문에서는 생산 공장과 본사를 연계하기 위한 방법으로 방화벽, 망연계 시스템, 데이터 다이오드(단방향 전송장비)의 구성과 보안취약점을 분석하고 스마트공장 환경에서 가장 효율적인 망연계 방법을 제안한다.

† 본 논문은 중소벤처기업부의 재원으로 지원을 받아 수행된 “안전한 스마트팩토리 연계를 위한 산업용 통합보안장치 개발” 사업의 연구결과입니다.
†† 교신저자 : jcha@hoseo.edu

II. 제조 제어망과 업무망 간 연계 보안 방법 고찰

본 논문에서는 스마트공장 환경에서 공장 제어망과 본사 업무망 간 연계를 위해 경계 보안 모델로 사용되는 방화벽(Firewall), 망연계 솔루션, 데이터 다이오드(Data Diode)를 기반으로 제어망과 업무망 연계 방법으로 4가지 구성 방식을 정의한다.

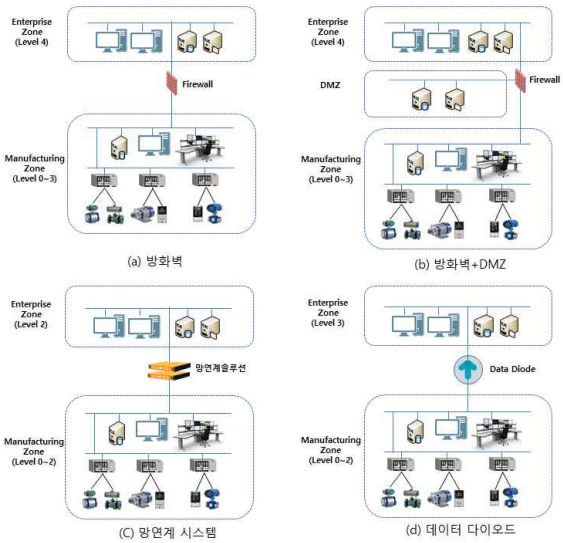
첫 번째 연계 방식은 NIST SP800-82 “Guide to Industrial Control Systems(ICS) Security”[3]에서 제시하고 있는 5가지 방화벽 구성 방식 중 듀얼 홈 컴퓨터(Dual-Homed Computer) 구성, 단일 방화벽 구성, 라우터+방화벽 구성 등 3가지 방식을 방화벽 구성으로 정의한다. 방화벽 구성은 ANSI/ ISA99[4], ISA/IEC 62443[5] 등에서 제어시스템 영역 간 트래픽 통제를 위해 적용 사례를 보여주고 있다.

두 번째 연계 방식은 NIST SP800-8에서 나머지 2가지 방화벽 구성 방식으로 단일 방화벽을 이용한 DMZ 구성과 이중 방화벽을 위한 DMZ 구성을 방화벽+DMZ 구성으로 정의한다. 방화벽과 DMZ의 구성은 미국 ICS-CERT의 ICS 심층방호 전략(Defense-in-Depth Strategies)[5]에서 권고 보안 네트워크 아키텍처로 ISA/IEC 62443 권고 모델을 기반으로 DMZ를 사용한다.

국내에서 망분리 정책[9]에서 업무망과 인터넷 연결망을 분리한 후 망간 자료교환을 위해 사용되는 망간자료전송장비인 망연계 솔루션이 가장 폭넓게 적용되고 있으므로 이를 다섯 번째 연계 방식으로 정의한다. 망연계 솔루션은 “국가용 정보보호제품 보안요구사항”[10]에 서로 다른 영역 간 사용자 PC 자료 및 서버 스트림을 보안정책에 따라 안전하게 전송해주는 시스템으로 정의되어 있으며 보안영역인 업무망과 비-보안영역인 인터넷 연결망 간 자료교환을 위해 사용된다.

이외 다른 ICS 경계 보안 방법으로 미국 ICS-CERT의 ICS 심층방호전략(Defense-in- Depth Strategies)[5]에서는 방화벽(Firewall)과 더불어 경계 보안 솔루션으로 데이터 다이오드(Data Diode)를 정의하고 있어 세 번째 연계 방식으로 데이터 다이오드 구성을 정의한다.

데이터 다이오드는 국내 주요정보통신기반시설 보호를 위해 권고[6]하고 있으며 제어시스템 보안 가이드라인[7]에 정의되어 있다. 국내의 경우 산업제어시스템 보안요구사항[8]에서 Level 0에서 Level 2를 제어망으로 정의하고 업무망을 Level 3로 정의하고 있으며 제어망에서 업무망으로 데이터를 단방향으로만 전송하고 업무망에서 제어망으로는 물리적으로 단선되어 데이터를 전달하지 못함으로 스마트공장에 적용하기에는 제한적이다.

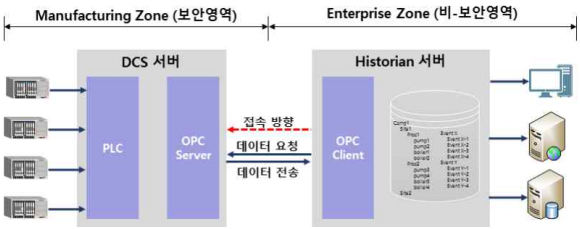


(그림 1) 제어망과 업무망 연계 방법

III. 제어망과 업무망 연계 방법에 대한 취약점 분석

산업제어시스템에서 현장장치로부터 데이터를 수집하고 DCS(Distributed Control System)에서 중앙제어센터(Central Control Center)의 히스토리언(Histrorian)으로 데이터를 전송하거나 스마트공장의 MES(Manufacturing Execution System)이나 ERP(Enterprise Resource Planning)으로 데이터 전송하기 위해 가장 많이 사용되는 프로토콜이 OPC(Ole for Process Control)이며 Industrial 4.0 생산의 구현에서는 센서로부터 ERP 레벨에 이르기까지 일관성을 유지하기 위해 국제표준으로 OPC UA(Unified Architecture)가 정의되어 있다.

Classic OPC(DA, HDA, A&E)와 OPC UA 모두 서버-클라이언트 구조로 제어망 DCS에 OPC 서버를 두고 업무망 히스토리언에서 OPC 클라이언트로 데이터를 수집하는 구조로 되어 있다.

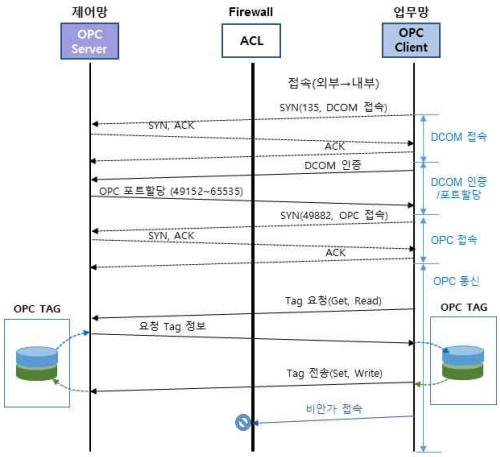


(그림 2) 산업제어시스템 OPC 연결 구조

본 장에서는 상기 산업제어시스템 OPC 연결 구성과 같이 비-보안영역인 업무망에서 보안영역인 제조 제어망으로 접속하는 환경에서 2장의 제조 제어망과 업무망 간 연계를 위해 사용될 수 보안 게이트웨이 적용에 대한 프로토콜 관점에서의 보안취약점을 분석한다.

3.1 방화벽 구성 보안취약점 분석

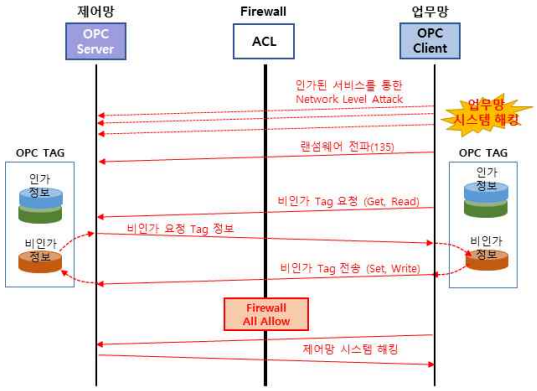
제어망과 업무망을 방화벽으로 직접 연결하는 경우 업무망 시스템에서 제어망 시스템으로 직접 접속이 이루어지며 방화벽은 업무망에서 제어망으로의 인가된 접속만 허용하고 비인가된 접속은 차단한다.



(그림 3) 방화벽 구성 정상동작

그러나 비-보안영역인 업무망에서 보안영역인 제어망으로의 접속을 허용하므로 다양한 공격이 가능해진다.

비-보안영역의 업무망 시스템이 해킹될 경우 인가된 서비스를 이용한 다양한 네트워크 공격이 제어망 시스템에 전달되며 OPC와 같이 DCOM을 사용하는 프로토콜은 135번 포트를 통하여 랜섬웨어 전파 등이 가능하다.



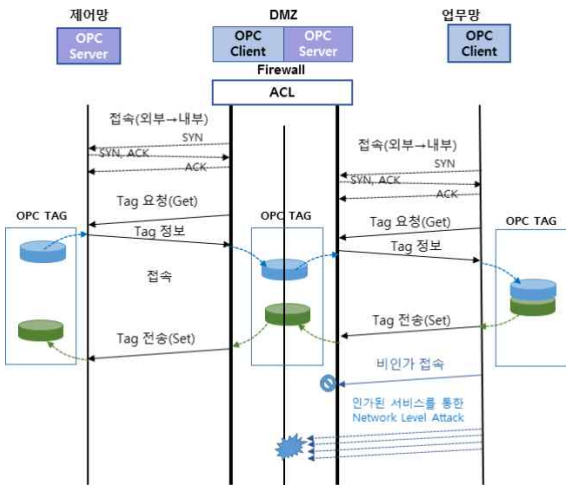
(그림 4) 방화벽 구성 보안취약점

또한 업무망의 OPC 클라이언트에서 비인가 Tag 정보를 요청할 경우 제어망의 OPC 서버로부터 Tag 정보를 받을 수 있으며 반대로 OPC 서버에 비인가 Tag 정보를 쓸 수도 있다.

방화벽 정책이 모두 허용하는 정책일 경우 업무망 시스템에서 제어망 시스템으로 해킹이 가능하여 방화벽 정책 관리에 주의해야 한다.

3.2 방화벽+DMZ 구성 보안취약점 분석

제어망과 업무망 사이에 방화벽을 이용한 DMZ를 구성하는 경우 제어망 시스템과 업무망 시스템 간 직접 접속은 이루어지지 않으며 제어망 시스템에서 DMZ 시스템으로 Tag 정보를 갖다 놓으면 업무망 시스템에서 DMZ 시스템로 접근하여 Tag 정보를 가져간다.

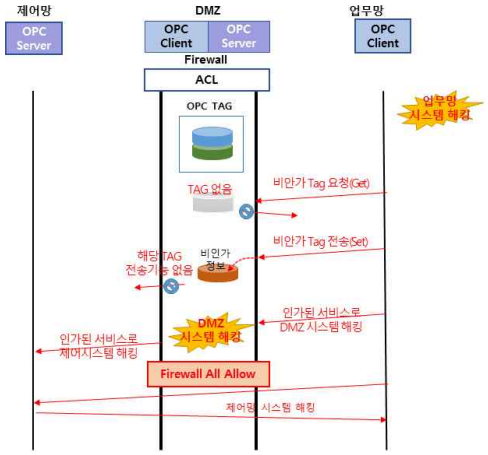


(그림 5) 방화벽+DMZ 구성 정상동작

이 경우 방화벽은 DMZ 영역으로 접근하는 제어망 시스템과 업무망 시스템을 통제하며 인가된 접속만 허용하고 비인가된 접속은 차단한다.

또한 DMZ 영역에 중계 서버를 둠으로써 업무망의 네트워크 레벨 공격이 DMZ 영역에는 영향을 미칠 수 있으나 제어망으로 전파되지 않는다.

비-보안영역의 업무망 시스템이 해킹되어 비인가 Tag를 요청할 경우 DMZ 중계 서버에 해당 Tag 정보가 없어 전달되지 않으며 비인가 Tag 정보를 쓸 경우 DMZ 중계 서버에서 전달기능이 없어 제어망이 안전하게 유지될 수 있다.



(그림 6) 방화벽+DMZ 구성 보안취약점

제어망 시스템을 해킹하기 위해서는 DMZ 중계서버를 해킹한 후 DMZ 중계 서버에서 제어망 시스템을 해킹해야 한다.

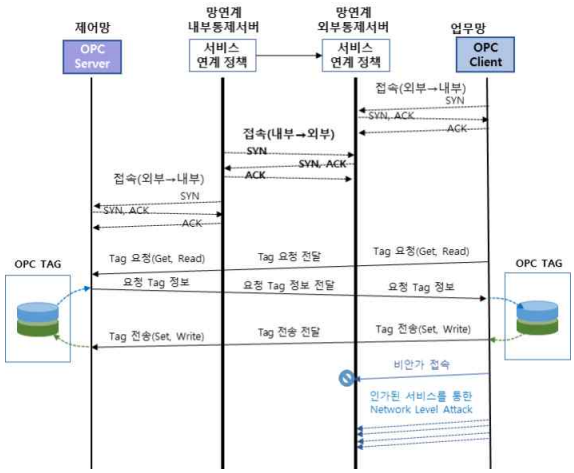
방화벽 정책이 모두 허용하는 정책일 경우 업무망 시스템에서 제어망 시스템으로 해킹이 가능하여 방화벽 정책 관리에 주의해야 한다.

3.3 망연계시스템 구성 보안취약점 분석

망연계 시스템은 인터넷망과 업무망을 분리한 경우 사용되는 망간자료전송제품으로 사용자 PC 간 자료교환을 위한 자료전송제품과 서버 간 서비스 전송을 위한 스트림연계제품으로 구분된다.

망간자료전송제품은 통신 요청은 보안영역 전송통제서버에서 비-보안영역 전송통제서버로만 이루어지도록 하고 있으며 그 외 통신 요청은 불허하여 안전한 것을 알려져 있다.

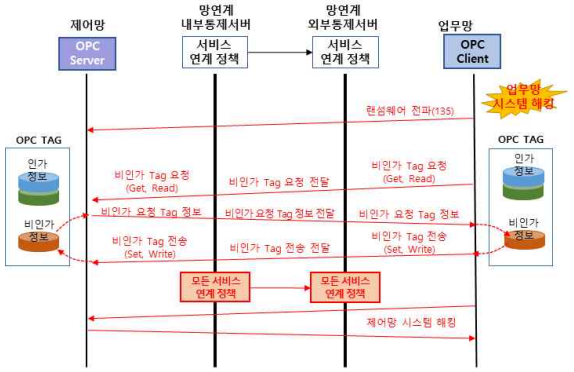
업무망 시스템에서 망연계 외부통제서버로 접속을 요청하면 망연계 내부통세서버에서 망연계 외부통제서버로 접속이 발생하고 다시 망연계 내부통제서버에서 제어망 시스템으로 접속이 발생하여 안전하게 보인다.



(그림 7) 망연계 솔루션 구성 정상동작

그러나 4개의 시스템 간 서로 다른 네트워크 레벨의 통신 세션이 발생하지만 접속이 이루어지면 업무망 시스템의 명령어가 제어망 시스템으로 명령어를 보내면 망연계 외부통제서버에서 받아 망연계 내부통제서버로 전달되고 망연계 내부통제서버에서 제어망 시스템으로 명령어를 전달하므로 업무망 시스템에서 제어망 시스템 간 응용 세션이 연결되는 현상이 발생한다.

즉, 망연계 솔루션을 이용한 스트림 연계 방식은 업무망 시스템에서 제어망 시스템으로 직접 접속하는 결과를 제공한다.



(그림 8) 망연계 솔루션 구성 보안취약점

망연계 솔루션을 이용한 연결은 DMZ 영역을 두는 것과 마찬가지로 업무망의 네트워크 레벨 공격이 망연계 외부통제서버에 영향을 미칠 수

있으나 제어망으로 전파되지 않는다.

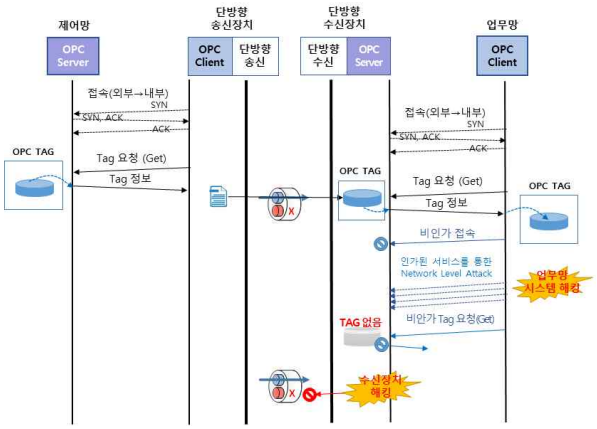
그러나 업무망 시스템에서 제어망 시스템으로 응용 세션이 직접 연결되므로 방화벽을 이용한 직접 연결과 같은 취약성이 발생한다.

3.4 데이터 다이오드로 구성 보안취약점 분석

데이터 다이오드는 물리적 단방향 전송장비로 단방향 송신장치에서 제어망 시스템으로 접속하여 Tag 정보를 수집하고 단방향 송신장치에서 단방향 수신장치로 데이터를 단방향으로 전송하며 업무망 시스템에서 Tag 정보 요청이 있으며 해당 Tag 정보를 제공한다.

데이터 다이오드는 방화벽이나 망연계 솔루션과 마찬가지로 ACL 기능을 가지고 있으므로 업무망에서으 비인가 접속에 대한 차단 기능을 제공하며 DMZ 영역을 두는 것과 마찬가지로 업무망의 네트워크 레벨 공격이 단방향 수신장치에 영향을 미칠 수 있으나 제어망으로 전파되지 않는다.

업무망 시스템이 해킹되어 비인가 Tag를 요청하더라도 단방향 수신장치 전달된 해당 Tag 정보가 없으므로 전달되지 않으며 단방향 수신장치가 해킹되더라도 제어망으로의 회선이 물리적으로 끊어져 있어 해킹이 불가능하다.



(그림 9) 데이터 다이오드 구성 정상동작

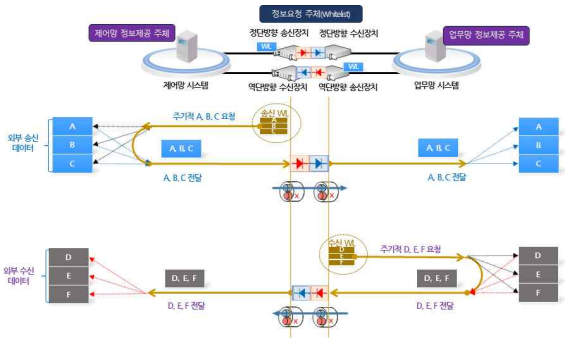
IV. 안전한 스마트공장 연계를 위한 크로스 도메인 보안 방안

스마트공장에서 현장 공장의 운영정보를 본사 MES, ERP 등에 적용하고 다시 현장 공장으로 정보를 제공하기 위해서는 두 네트워크 도메인 간 양방향 데이터 교환이 필요하다.

본 장에서는 제어망과 업무망을 연결하는 4가지 방식 중 가장 안전한 방식인 데이터 다이오드를 이용하여 상호 데이터 교환이 가능한 듀얼 다이오드 방식을 제안한다.

4.1 스마트공장 크로스 도메인 보안을 위한 듀얼 다이오드 설계

스마트공장의 현장 공장과 본사 간 크로스 도메인 보안을 위한 듀얼 다이오드는 아래 그림과 같이 제어망에서 업무망으로의 정단방향 송신장치와 정단방향 수신장치를 구성하고 별도의 동일 시스템으로 역단방향 송신장치와 역단방향 수신장치로 구성한다.



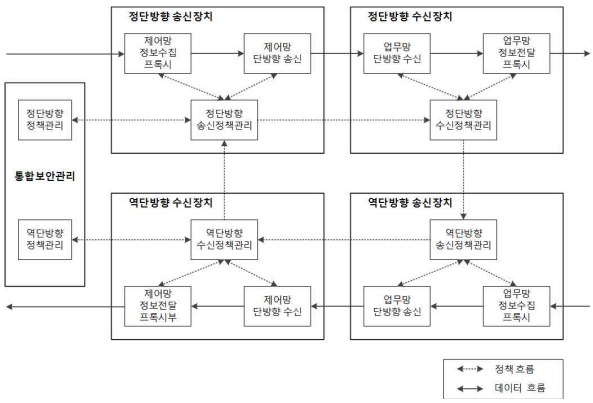
(그림 10) 듀얼 다이오드 개념 모델

정보를 제공하는 제어망 시스템과 업무망 시스템은 서버로 구성하고 단방향 송신장치와 단방향 수신장치는 클라이언트로 구성한다.

정보요청 주체는 단방향 송신장치로 망간 인가된 제공 정보로 구성된 화이트리스트(Whitelist)에 기반하여 정보를 요청한다.

인가된 화이트리스트에 기반하여 정보를 요청하고 제공하므로 현장 공장의 비인가 정보의 외부 유출이나 본사 업무망 시스템 해킹으로 인한 현장 공장의 정보 위변조를 방지한다. 또한 물리적 정단방향 시스템과 물리적 역단방향 시스템을 분리 운영함으로써 외부망 시스템이 해킹되더라도 물리적 회선이 끊어져 있어 현장 공장으로의 해킹을 원천적으로 차단한다.

스마트공장의 현장 공장과 본사 간 크로스 도메인 보안을 위한 듀얼 다이오드 구성도는 다음과 같다.



(그림 11) 듀얼 다이오드 시스템 구성도

듀얼 다이오드 시스템에서 단방향 데이터 플로우는 정단방향 데이터 플로우와 역단방향 데이터 플로우로 구분된다.

정단방향 데이터 플로우는 정단방향 송신장치의 제어망 정보수집 프록시에서 제어망 시스템에 접속하여 화이트리스트 기반으로 정보를 수집하여 제어망 단방향 송신모듈로 전달하고 업무망으로 데이터를 단방향으로 전송한다. 업무망 단방향 수신모듈에서 단방향 데이터를 수신하면 업무망 정보전달 프록시로 전달하고 업무망 정보전달 프록시는 업무망 시스템으로 접속하여 데이터를 전달한다.

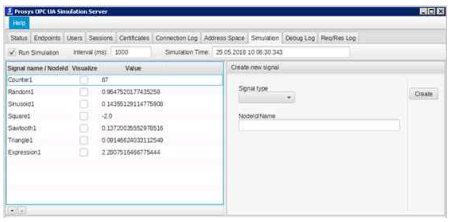
역단방향 데이터 플로우는 역단방향 송신장치의 업무망 정보수집 프록시에서 업무망 시스템에 접속하여 화이트리스트 기반으로 정보를 수집하여 업무망 단방향 송신모듈로 전달하고 제어망으로 데이터를 단방향으로 전송한다. 제어망 단방향 수신모듈에서 단방향 데이터를 수신하면 제어망 정보전달 프록시로 전달하고 제어망 정보전달 프록시는 제어망 시스템으로 접속하여 데이터를 전달한다.

듀얼 다이오드 시스템에서 정책은 단방향 데이터 플로우와 별도로 정책 플로우를 구성한다. 듀얼 다이오드 관리시스템은 보안영역인 제어망에 두며 정단방향 정책관리와 역단방향 정책관리를 통합하여 구성한다.

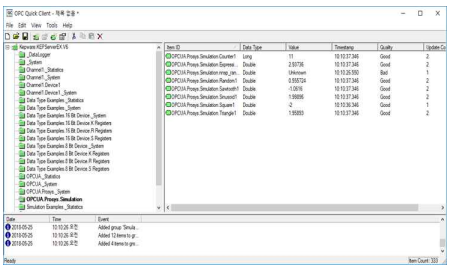
듀얼 다이오드 시스템의 정책 플로우는 물리적 단방향 특성을 고려하여 정단방향 송신장치→정단방향 수신장치→역단방향 송신장치→역단방향 수신장치→정단방향 송신장치로의 루프를 구성하며 단방향 데이터 전송 채널과 분리하여 관리 채널을 구성한다.

4.2 스마트공장 크로스 도메인 보안을 위한 듀얼 다이오드 구현

듀얼 다이오드 시스템은 스마트공장 환경을 고려하여 Classic OPC와 OPC UA로 서버와 프록시를 구성하였다.

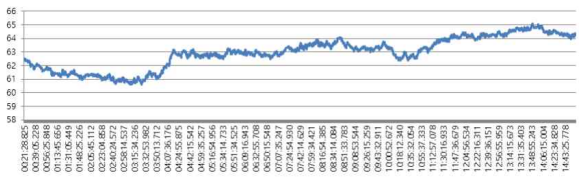


(그림 12) OPC UA 서버 구성

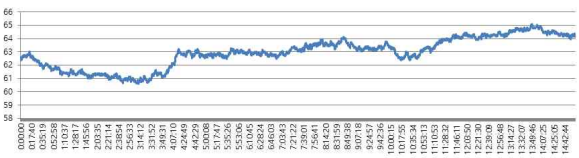


(그림 13) OPC UA 클라이드 구성

제어망 시스템에서 듀얼 다이오드 정단방향 시스템을 통하여 업무망 시스템으로 정보가 전달되거나 업무망 시스템에서 듀얼 다이오드 역단방향 시스템을 통해 제어망으로 정보가 전달되었을 경우, 제어망 시스템의 OPC Tag 정보와 업무망 시스템의 OPC Tag 정보가 동일하게 유지됨을 확인할 수 있다.



(그림 14) 제어망 OPC Tag 트랜드



(그림 15) 업무망 OPC Tag 트랜드

듀얼 다이오드 관리시스템은 정단방향 송신장치와 수신장치 정책, 역단방향 송신장치와 수신장치 정책책을 통합관리하며 다음과 같다.



(그림 16) 정단방향 송신장치 정책



(그림 17) 역단방향 송신장치 정책

4.3 크로스 도메인 보안 방법 비교·고찰

본 논문에서 제안한 듀얼 다이오드 방식은 기존 다이오드 방식을 이용하여 상호 데이터 교환을 위해 제안한 방식으로 2장과 3장에서 분석한 모두 서로 다른 도메인 간 상호 데이터 교환방식인 방화벽 직접 연결 방식, 방화벽과 DMZ를 이용한 연결 방식, 망연계 시스템을 이용한 연결 방식과 비교하면 다음과 같다.

[표 1] 크로스 도메인 보안 방법 비교

구분	본 제안	방화벽	방화벽 DMZ	망연계
두 도메인간 자룍교환	가능	가능	가능	가능
비인가 서비스 접속	차단	차단	차단	차단
인가서비스 네트워크공격	차단	허용	차단	차단
OPC 포트 랜섬웨어공격	차단	허용	DMZ해킹시 가능	허용
비인가 Tag Read	차단	허용	차단	허용
비인가 Tag Write	차단	허용	차단	허용
ACL 정책이 모두 허용	제어망 접근차단	제어망 접근가능	제어망 접근가능	제어망 접근가능
업무망해킹 제어망공격	차단	허용	차단	허용

일반적으로 방화벽보다 망연계 시스템이 안전하다고 생각하며 상기 결과에서도 인가된 서비스를 통한 네트워크 공격이 보안영역으로 전달되지 않아 방화벽보다는 보안성이 높다.

그러나 방화벽을 이용하여 DMZ를 구성할 경우 망연계 솔루션을 사용하는 것보다 보안성이 높음을 알 수 있다.

논 논문에서 제안한 듀얼 다이오드 방식은 한쪽 회선이 끊어져 있고 화이트리스트 기반으로만 동작하므로 가장 안전한 방식임을 확인할 수 있다.

V. 결론

본 논문에서는 스마트공장 환경에서 분리된 네트워크 영역 간 자료전달을 위해 경계 보안모델로 방화벽 구성, 방화벽과 DMZ 구성, 망연계 시스템 구성, 데이터 다이오드 구성에 대해 살펴보고 취약성을 분석하였다.

경계 보안모델의 보안성은 방화벽 < 망연계 시스템 < 방화벽+DMZ < 데이터 다이오드 순으로 분석되었으나 데이터 다이오드의 단방향 특성으로 인하여 공장과 본사 간 상호 자료전달이 어려운 문제점이 있다.

본 논문에서는 공장 제어망과 본사 업무망을 안전하게 연계하기 위해 데이터 다이오드를 정단방향과 역단방향으로 사용하는 듀얼 다이오드를 이용한 망연계 방법을 제안하였다.

듀얼 다이오드를 이용한 망연계 방법은 공장과 본사 간 상호 자료전달이 가능하며 화이트리스트 기반으로 기업정보유출을 방지하고 공장 정보 위변조를 차단하며 한쪽 회선이 끊어진 물리적 단방향 기술을 적용함으로써 현장 공장으로의 해킹을 원천적으로 차단함으로써 방화벽이나 망연계 시스템보다 보안성이 뛰어나다.

본 연구에서는 스마트공장에 대한 안전한 망연계 방안을 제시하고 있으며 향후 스마트시티 등 4차 산업혁명 다양한 분야로 확장할 예정이다.

[참고문헌]

[1] 한국인터넷진흥원, 스마트공장 중요정보 유출방지 가이드, 2017. 03.

[2] 스마트공장추진단, 고려대학교, 스마트공장을 위한 최소 정보보안 가이드라인, 2016. 09.

[3] NIST SP 800-82, Guide to Industrial Control System Security, May. 2015.

[4] ISA-95.00.01-CDV3, Enterprise-Control System Interation, Part 1: Models and Terminology, 2008.

[5] IEC TS 62443-1-1:2009, Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models, Jul. 2009.

[6] ICS-CERT, Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, 2016. 09.

[7] 국가보안기술연구소, 산업제어시스템 보안요구사항, 2017. 11.

[8] IT보안인증사무국, 국가용 정보보호제품 보안요구사항, 2014.

[9] 행정안전부, 한국정보화진흥원, 국가기관 망분리 구축가이드, 2008.

[10] ISA-62443-1-1, Security for Industrial Automation and Control System, Mar. 2017.

[11] 망연계 솔루션, Hanssak Co. Ltd., http://www.hanssak.co.kr

[12] 망연계 솔루션, SQLsoft Co. Ltd., http://www.sqisoft.com

[13] 망연계 솔루션, Hunesion Co. Lted., http://www.hunesion.com/

[14] 데이터 다이오드, NNSP Co. Ltd., http://nnsp.co.kr

[15] 데이터 다이오드 Waterfall Security Solutions Ltd., https://waterfall-security.com/

[16] 데이터 다이오드 Owl Cyber Defence Solution, https://www.owlcyberdefense.com/

국내 스마트시티 인프라 사이버보안 취약점 분석 및 대응방안 제시

이성원, 송진우, 서정택

순천향대학교 정보보호학과

Analyzing cyber security vulnerability of domestic smart city infrastructure and proposing measures

Seong Won Lee, Jin Woo Song, Jung Teak Seo

Department of information security Engineering, Soonchunhyang University.

요 약

최근 스마트시티를 위한 기술 개발과 인프라 구축이 활발하게 추진되고 있으며, 새롭게 구축되는 국내 스마트시티들에 대하여 많은 논의가 진행되고 있다. 정부와 민간단체는 더 나은 스마트시티 구축을 위해 간담회개최 등을 통하여 발전 방법을 모색하고 있다. 그러나 스마트시티의 특성상 다수의 사이버 보안 취약점이 존재하고 해당 취약점을 통해 스마트시티 인프라가 붕괴될 경우 시민들의 안전과 재산에 위협이 발생가능하다. 따라서 본 논문에서는 국내에서 구축되었거나, 구축 진행 중인 인천과 부산의 스마트시티를 대상으로 해당 스마트시티 인프라 구축에 참여하는 민간업체의 각 업체별 적용예정기술을 분류하고 이를 통한 해당 스마트시티 인프라 사이버보안 취약점을 분석한다. 또한 분석한 취약점을 바탕으로 공격가능시나리오를 도출하고 스마트시티에 적용 가능한 대응방안에 대해 제시한다.

I. 서론

국내에서는 급격한 도시화로 인한 환경적인 문제들이 발생하면서 ICT 기술을 접목한 스마트시티 구축이 활발하게 추진되고 있다. 국외의 스마트시티 선진국인 미국의 경우, 콜롬버스에 서비스공모, 챌린지 운영을 통해 기업 및 시민 참여를 도모하는 스마트시티를 구축하였고, 스페인의 경우 리빙랩, 테스트베드를 구축을 통해 산탄데르에 실증단지를 구축하였다. 세계 각각 정부에서는 스마트시티 구축을 위하여 각 도시들이 가지고 있는 잠재력으로 알맞은 콘텐츠를 도입함으로써 시장 경쟁력을 키우고 시민의 편의성을 보전하기 위한 투자를 진행 중이다. 국내에서도 마찬가지로 서울을 비롯한 대구, 대전, 세종, 부산 등 여러 광역시에서 스마트시티 실증단지 구축이 추진되고 있다[1].

기존에 U-City에서 스마트시티로 탈바꿈한 인천 스마트시티가 운영되고 있다. 현재진행형인 도시는 부산 에코델타시티와 세종 스마트시티 등이 있다. 해당 스마트시티는 '민간이 주도하는 서비스' 라는 스마트시티의 모토를 가지고 편리한 삶을 위한 도시구축을 진행 중이다.

스마트시티를 구성하는 인프라는 네트워크로 연결되어 있으며 각종 센서들은 광범위에 산재되어 있다. 따라서 관리에 취약하고 해킹에 노출될 위험이 높으며, 다수의 사이버 보안 취약점이 존재한다. 해당 취약점을 통해 스마트시티의 인프라가 붕괴될 경우, 인명 피해 및 재산 피해가 발생가능하다.

이에 본 논문에서는 안전한 스마트시티 인프라 구축을 위하여 해당 스마트시티 사업에 참여하는 민간업체의 각 업체별 적용기술을 분류하고 스마트시티 인프라의 사이버보안 취약점을 분석한다. 또한 분석한 사이버보안 취약점을 바탕으로 사이버 공격가능시나리오를 제시하고 그에 따른 대응방안을 제시하고자 한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서 국내 스마트시티 인프라 구축현황 분석을 위해 유비

쿼터스 도시 건설사업(이하 U-City)에서 스마트시티로 탈바꿈한 인천의 스마트시티와 2018년 스마트시티 시범도시로 선정된 부산의 에코델타시티에 대해 분석한다. Ⅲ장에서는 스마트시티 인프라의 사이버보안 취약점과 보안위협에 대해 분석한다. Ⅳ장에서는 분석한 취약점을 바탕으로 스마트시티들의 공격가능시나리오를 도출하고, Ⅴ장에서는 Ⅲ장과 Ⅳ장에 따른 대응방안에 대해 제시한다. 마지막으로 Ⅵ장에서는 결론 및 향후 연구 방향에 대해 서술한다.

II. 국내 스마트시티 인프라 구축현황

1.1 인천 스마트시티

U-City에서 진행되었던 유비쿼터스 컴퓨팅 기술, 정보통신 기술을 기반으로 도시 전반의 영역에서 자연 인터페이스를 매개로 목적에 맞는 서비스를 이용할 수 있는 환경을 구현하였다. 홈페이지를 두고 지역별 지도로 구별하여 환경적 변수들, 미세먼지, 날씨 정보, 도로 구간 정보, 지하철 정보, CCTV나 무선통신 수단인 WiFi의 상태 등을 실시간으로 확인 가능하게 하여 통합 서버와 연계를 통해 시민들에게 편의를 제공하고 있다. 다음 [그림 1]과 같이 교통, 방범, 시설관리, 방재, 환경, 도시민 정보제공을과 민간 서비스를 통해 민간인 참여를 이끌고 있다[2][3].



[그림 1] 인천 smart city 구성 출처 : 인천스마트시티

1.2 부산 에코델타시티

스마트시티 선도국으로 비상하기 위한 추진 전략에서, 도시 성장 단계별 접근, 맞춤형 기술, 주체별 역할로 밀도 높은 연구와 시민참여를 통해 국가 시범도시 신규 조성을 위해 단계별로 진행 중이다. 1단계, 에코델타시티를 비롯한 세종 5-1 생활권을 국가 시범도시로 선정하고, 2단계에서 지자체나 민간 등의 의견을 통합하여 시범도시에 적용시킬 수 있도록 정부와 민간기업이 협력하여 관련 정책을 추진 중에 있다.

18년 4월 5일, 국토교통부에서 민간기업을 초청하여 '스마트시티 시범도시 민간기업·시민 주도 조성'을 주제로 간담회를 개최했다. 국민이 참여할 수 있는 정책을 제안함으로써 기존의 U-City 사업에서 더 나은 국가 시범도시의 구축을 추진하였다. 국토교통부는 향후 설계를 완료하기 위해 민간기업과 협업하여 민관협의체 구성, 네이밍 대국민 공모, 시행계획 수립과 같은 계획을 수립하였다[4][5]. 해당 간담회에 참여한 민간기업과 해당 기업의 보유기술 및 장비는 다음[표1]과 같다.

[표 1] 에코델타시티 간담회에 참여한 민간업계와 기술

민간기업	보유 기술 및 장비
현대자동차	자율주행
KT	통신 및 네트워크
포스코건설	스마트홈
롯데정보통신	플랫폼
한화 큐셀	태양광
이큐브랩	쓰레기처리
더웨이브톡	수질관리
PNU드론	드론
프리폼연구소	3D 프린터
컴퍼니비	엑셀러레이터

III. 국내 스마트시티 인프라 취약점

본 장에서는 민간기업 간담회에 참여했던 민간기업의 스마트시티 인프라 구축에 적용된, 혹은 적용예정인 기술 및 장비의 취약점을 분석하고, 스마트시티 인프라의 사이버보안취약점에 대해 분석한다.

3.1 현대자동차 자율주행 시스템 취약점

현대자동차에 적용된 텔레매틱스 구조의 경우, 보안 메커니즘이 존재하지 않는 CAN 네트워크를 사용하고 외부와 연결가능한 블루투스, WiFi와 같이 이동통신 모듈을 지니고 있다. 해당 통신모듈을 활용하여 무선 업데이트 기술 OTA 서비스에 접근 후 악성코드를 삽입하여 차량을 제어할 수 있는 권한을 탈취할 수 있다[6].

3.2 WiFi 통신 취약점

WiFi의 보안 프로토콜인 WPA2는 WPA보다 견고한 암호화 프로토콜이다. WPA2에 안드로이드 사용자들에게 해당되는 취약점이 존재한다. KRACK이라고 하는 재설치 공격은 사용자가 이미 사용 중인 키를 다시 설치하도록 유도하여 암호화 핸드 셰이크를 조작할 수 있다. 해당 취약점은 2017년 10월 패치되었으나 아직 업데이트를 진행하지 않은 공공 WiFi망에서 위협이 될 수 있다[7][8].

3.3 스마트시티 인프라 사이버보안 취약점

스마트시티의 구조를 크게 두 가지로 분류하여 취약점을 분석을 진행하였다. 하나는 스마트시티를 부분적으로 관찰하고 건물이나 교통 및 기상의 상태 정보를 얻어오는 IoT 기기 센서이고, 다른 하나는 도시 내의 등록된 사용자의 개인정보, 센서를 통해 얻은 데이터를 저장하고 전송하는 시티 네트워크이다.

그 중 스마트시티 구축 사업에서 가장 시장 규모가 크고 많은 투자가 필요한 영역은 IoT분야이다. IoT 기반의 기기들은 외부로부터 다양한 형태의 제로데이, 취약점 공격이 발생할 수 있고, 이는 개인 정보 탈취를 통한 프라이버시 침해와 스마트시티 내의 경제적, 사회적 문제 등이 발생가능하다. 스마트시티 인프라 사이버보안 취약점은 다음[표2]와 같다.

[표 2] 스마트시티 인프라 사이버보안 취약점

범위	취약점
시 티 네트워크	WPA2의 취약점을 이용한 핸드 셰이크 조작 공격
	인가되지 않은 WiFi망 액세스
	불충분한 ID, 인증 정보 및 접근 권한 관리
	서비스 거부 공격
	무선 업데이트 기술 OTA 서비스를 이용한 악성 펌웨어 업로드 공격
	공유 메모리와 리소스에 대한 접근 권한 부여 문제
IoT 센서	물리적 보안 취약점
	레거시 시스템 및 이기종간 연결을 통한 오류 발생
	외부 사용자 접근 용이 취약점
	인증 메커니즘 부재
	추가된 센서 암호 미변경
	전송데이터 보호 부재

IV. 대상 모델 공격 가능 시나리오

본 장에서는 최근 발표된 2018년 코드게이트의 스마트홈 해킹 시나리오와 스마트시티 공격 가능시나리오에 대해서 분석한 내용을 기술한다.

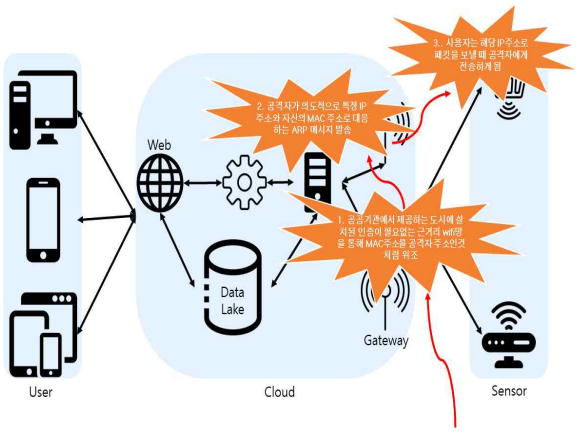
2018년 4월, Emohtrams Team은 'smart home hacking in Real World' 라는 주제로 스마트홈의 인프라와 관련된 모의해킹을 진행했다. 이들의 경우 상호 연결된 모바일 앱과 가정용 월 패드를 이용하여 CCTV 포트 스캐닝을 통해 정보를 수집하였다. 스트리밍 데이터를 수신하여 영상 데이터를 복원하거나 획득한 펌웨어로 root shell을 획득하여 스마트홈 내 기기를 조작하여

집 안까지 침입이 가능하였다[9].

4.1 스마트시티 ARP 스푸핑 공격가능시나리오

ARP(Address Resolution Protocol) 스푸핑은 주소 결정 프로토콜을 이용한 중간자 공격으로 공격자가 자신이 게이트웨이라고 속여 사용자의 데이터를 훔치는 공격을 의미한다.

아래[그림 2]는 ARP 스푸핑을 통한 스마트시티 내 공공 WiFi망에 대한 공격가능시나리오를 나타낸다.



[그림 2] ARP스푸핑을 통한 공공 WiFi망 공격가능시나리오

Step1. 인가되지 않은 공격자가 스마트시티 내에 사용자들이 사용하는 WiFi 무선 공유기를 이용하여 기기의 사용자 목적지 주소를 자신의 IP로 변경한다.

Step2. 이후에, 공격자가 의도적으로 특정 IP 주소와 자신의 MAC 주소로 대응하는 ARP 메시지를 발송한다.

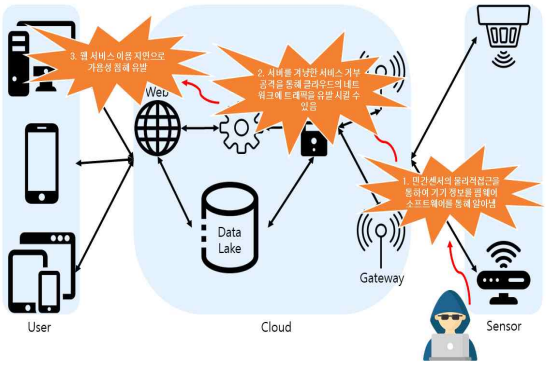
Step3. 사용자는 해당 IP주소로 패킷을 보낼 때 공격자에게 전송한다.

ARP스푸핑을 통한 공공 WiFi망 공격가능시나리오의 결과로, 공격자는 사용자가 보내는 패킷을 모두 볼 수 있으며, 해당 패킷분석을 통하여 악의적인 위·변조 패킷전송이 가능하다.

4.2 스마트시티 분산서비스거부 공격가능시나리오

분산 서비스 거부 공격(Distributed DoS)은 여러 대의 공격자를 분산적으로 배치하여 동시에 서비스 거부 공격을 하는 방법이다. 공격자가 IoT 기기에 물리적으로 접근하여 오픈 포트를 이용한 펌웨어 습득을 통해, 리버싱 분석으로 악의적으로 펌웨어 변조가 가능하다.

아래[그림 3]은 스마트시티 내 웹서비스에 대한 분산 서비스 거부 공격을 이용한 공격가능시나리오를 나타낸다.



[그림 3] 분산 서비스 거부 공격을 이용한 웹 서비스 지연 공격가능시나리오

Step1. 공격자는 웹 사이트 지도 정보로 쉽게 찾을 수 있는 센서를 통해 센서의 오픈 포트 취약점이나 펌웨어 취약점, 인터넷의 열려있는 텔넷 포트를 이용하여, IoT기기를 컨트롤러로 사용한다.

Step2. 권한을 탈취한 센서가 일정량 이상 수집되면, 웹 사이트로 과도한 트래픽을 전송하여 서비스 거부 공격을 유발한다.

Step3. 웹 서비스 이용 지연으로 가용성 장애를 유발시킨다.

분산 서비스 거부 공격을 통한 스마트시티 내 웹서비스 공격가능시나리오의 결과로, 공격자는 과도한 트래픽전송을 통하여 서비스 거부를 일으킬 수 있다.

V. 대응방안

각 Ⅲ장과 Ⅳ장에서 분석한 취약점을 바탕으로 본 장에서는 스마트시티 인프라 사이버보안취

약점에 대한 대응방안을 제시하였다.

5.1 시티 네트워크 취약점 대응방안

- 서비스 이용과 IoT 기기를 위한 별도 네트워크를 사용하여 모니터링을 통해 트래픽 과부하와 기업의 핵심 네트워크 접속을 사전에 차단
- WiFi망의 안전을 위해서 웹 서버에서 스마트시티의 거주자, 혹은 입주자에게 각각의 고유 ID를 부여하여 외부 사용자에 대한 불법 네트워크 접근을 차단하고 안전하게 사용자의 계정을 보호

5.2 IoT 취약점 대응방안

- 펌웨어 변조와 유포를 방지하기 위하여 TPM(Trusted Platform Module)을 이용한 펌웨어 업데이트와 서버 내에서 SSH(secure shell)를 통한 무결성 검사로 지속적인 펌웨어 무결성 체크 실시
- 이 기종 네트워크간의 상호 연결을 통한 전송데이터를 보호하기 위해 IoT 보안 게이트웨이 적용 및 개발

VI. 결론 및 향후 연구방향

본 논문에서 국내 스마트시티의 인프라에 대해 분석하고 참여하는 민간업계의 기술에 대해서 분류하였다. 에코델타시티와 같은 스마트시티에 적용될 기술에서 문제가 있음을 확인하였고 그 밖에 시티 네트워크와 IoT 센서들의 취약점을 나열하였다. 또한 스마트시티 내에서 ARP스푸핑 공격과 분산 서비스 거부 공격이 위협이 될 수 있어 보안 망분리, 펌웨어 업데이트, 보안 게이트웨이 개발과 같은 대응방안을 제시하였다. 그러나 아직 밝혀지지 않은 민간기업의 기기들의 분석을 통해 민간기업의 IoT 디바이스가 스마트시티에 적합한지 판단하고, 서비스 이용과 IoT 기기를 위한 별도 네트워크 망을 구축하여 인프라 보안을 지속적으로 유지하기 위한 기술 및 적용에 대한 향후연구가 필요하다.

[참고문헌]

[1] 송진우 외 3명, “스마트시티 인프라 구축현황 분석 및 사이버보안 고려사항 연구”, 순천향대학교, 2018

[2] http://www.ismartcity.co.kr/06/ucity6_1.php, 인천스마트시티, 2017

[3] 신우재 외 3명, “U-City의 국제 경쟁력 구축을 위한 Smart City와의 차이점 비교 분석 연구”, 성균관대학교, 2015

[4] 박푸르뫼, “국내 스마트시티 추진동향 및 시사점”, 정보통신 산업진흥원, 2017

[5] 김현미, “스마트시티 시범도시 민간기업·시민 주도 조성” , 동정자료, 2018

[6] 김태형, “텔레매틱스의 보안 취약점 및 대응방안 연구” , 경북대학교, 2017

[7] 김선애, “와이파이 프로토콜 취약점” http://www.datanet.co.kr/news/articleView.html?idxno=115785, 2017

[8] Mathy Vanhoef, https://www.krackattacks.com, IMEC-DISTRINET, 2017

[9] 조성준, 박상현, “Smart Home Hacking in Real World”, Team Emohtrams, 2018

2018 한국정보보호학회 하계학술대회

B1 암호화폐/블록체인 2

임 을 규 (한양대학교)

- **블록체인 기반의 차량 평판 시스템 안전성에 관한 연구**
  이경모, 이경현
- **블록체인 모델에 대한 고찰**
  김혜빈, 박지선, 김종규, 신상욱
- **P2P 스토리지를 이용한 블록체인 기반의 EHR 관리 시스템**
  김현우, 이경현
- **블록체인을 기반의 안전한 전자투표 시스템에 관한 연구**
  노창현, 이임영
- **A Blockchain Based On Data Provenance in Healthcare Domain**
  Kweka Bruno Joachim, 이경현

CH1.
JUISDICTION



I 최소한의 접촉 (Minimum Contact)

◎ **미국 수정헌법 제14조 적법절차(Due Process)**

1) 최소한의 관련성 (Sufficient Minimum Contact)
2) 공정경쟁과 실질적 정의 (Fair play and Substantial justice)

◎ **최소한의 접촉(Minimum Contact)** - ★★★ *기출 (2007 1학기 기말고사)*

1) 의도적으로 이익을 추구 (Purposefully Availment)
2) 피고의 행위(Activity)로부터 직접 소송 제기
3) 재판관할권 소송이 제기 가능성 예상 (Reasonably Foreseeable)

1 "International Shoe Co. v. Washington" (1945) - ★★★★

(개요) 원고인 International Shoe는 미주리 주에 본점을 두고 있는 신발회사로 워싱턴 주에 사무실, 창고 등을 소유하지 않고, 워싱턴 주에 근무하는 직원을 통해 신발을 주문받는 형태로 사업을 수행하였다. 이에 대해 워싱턴 주는 원고에게 실업 보험세를 과세하였고, 원고는 워싱턴 주에는 사무실, 창고 등의 '물리적인 존재(physical presence)'가 없으므로 영업활동을 한 적이 없다고 주장하며 재판관할권 무효 소송을 제기하였다.

(결과) 법원은 공정 경쟁과 실질적 정의(fair play and substantial justice)의 관념에 비추어 볼 때, 원고는 법정지가 위치한 워싱턴 주에서 이익을 추구하였기 때문에 최소한의 관련성(minimum contact)이 인정되므로 워싱턴 주가 재판을 관할할 수 있다고 판결하였다.

(의의) 비거주자에 대한 대인 재판관할권이 성립되기 위해서는 '물리적 존재(physical presence)'가 있어야 한다는 "Pennoyer v. Neff" 사건의 판결을 깨고, 최소한의 접촉(minimum contact)을 최초로 인정한 획기적인 판결(landmark decision)이다.

2 "Burger King Corp. v. Rudzewicz" (1985) - ★★★

(개요) 시카고에 거주하는 Rudzewicz는 플로리다에 본사를 두고 있는 Burger King과 프랜차이즈 계약을 체결하고 시카고에서 장사를 하였으나, 해당 계약이 해지된 후에도 Burger King 상표를 계속해서 사용하였다. 이에 대해 원고인 Burger King이 상표권 침해(Trademarks Infringement)로 소송을 제기하였고, 피고인 Rudzewicz는 Burger King 상표는 시카고에서 사용하였기 때문에 사업을 하였기 때문에 Burger King은 재판관할권이 없다고 주장한 사건이다.

(결과) 피고인 Rudzewicz는 플로리다에 대리점 등의 '물리적 존재(physical presence)'는 없지만, 계약해지 후에도 Burger King의 상표를 사용함으로써 1)의도적(purposefully)으로 이익을 추구했고, 2)계약체결이 원고의 법정지에서 이루어져 원고의 법정지에서 2)재판관할권 문제가 제기될 것을 예상할 수 있었기 때문에 최소 관련성(minimum contact)이 인정되므로 Burger King에게 재판관할권이 있다고 판결하였다.

3 “CompuServe v. Patterson"

(개요) 텍사스 주에 거주하는 Patterson은 오하이오 주의 ISP 사업자인 CompuServe와 S/W 프로그램 공급계약을 체결한 후, 원고인 CompuServe에게 공급하는 S/W와 비슷한 프로그램을 개발하여 피고의 웹사이트를 통해 판매하였다. 이에 원고인 CompuServe가 이를 문제 삼아 Patterson을 고소한 사건이다.

(결과) 제1심에서는 텍사스에 거주하는 Patterson이 승소하였으나, 원고가 항소한 결과 Patterson은 CompuServe를 이용하여 1)이익을 추구할 목적(purposefully)으로 상품을 팔았고, 2)원고와 피고간 상호간에 맺은 계약이 존재하고, 이에 따라 3)재판관할권 문제가 제기될 것을 예상할 수 있었기 때문에 최소 관련성(minimum contact)이 인정되므로 CompuServe에게 재판관할권이 있다고 판결하였다.

4 “Verizon Online Service v. Ralsky" (2002) - ★★★★★

(개요) 미시간 주에 거주하는 Ralsky는 버지니아 주의 통신회사인 Verizon Online Service(이하 Verizon사)의 네트워크를 이용하여 대용량의 상업적 스팸메일(commercial spam-mail) 지속적으로 발송하였다. Verizon사는 자사의 통신망을 이용한 스팸메일전송 금지정책을 사용자가 알 수 있도록 웹사이트에 고시하고 있었기 때문에 Ralsky에게 스팸메일 발송을 자제해 줄 것을 요청하였으나, Ralsky는 언론의 자유를 근거로 스팸메일을 지속적으로 발송하였다. 이에 Verizon사는 Ralsky가 보낸 수십만 건의 스팸메일이 자사의 컴퓨터시스템의 수용용량의 상당부분을 차지하여 내재적인 재산상의 손실이 발생했다고 주장하며 Ralsky를 고소한 사건이다.

(결과) 피고인 Ralsky가 보낸 스팸메일에는 상품이나 서비스에 대한 광고가 상당부분 게재되어 있었기 때문에 이러한 행위는 1)의도적(purposefully)으로 이익을 목적했으며, 2)Verizon사가 이용약관(Terms of Use)에 스팸메일을 금지하고 있었고, 이로 인해 3)재판관할권 문제가 제기될 것을 예상할 수 있었기 때문에 최소 관련성(minimum contact)이 인정되므로 Verizon사에게 재판관할권이 있다고 판결하였다.

5 "Volkswagan Corp v. Wooden" (2002) - ★★

(개요) Wooden이 뉴욕에서 Volkswagan Audi 차량을 구입한 후, 직접 운전하여 텍사스로 돌아오던 중 오클라호마 근처에서 Audi 차량이 폭발하는 교통사고를 당하자, 차가 폭발한 것은 차량 설계 오류로 'PL법(Product Liability, 제조물책임법) 위반'이라고 주장하며 텍사스 주에 위치한 Volkswagan사를 상대로 소송을 제기하였고, 아울러 오클라호마에서 사고가 발생하였으므로 오클라호마 법원에서 재판을 받겠다고 주장한 사건이다.

(결과) 법원은 피고인 Volkswagan사가 오클라호마 주에 지사도 없기 때문에 차량 폭발사고는 예측할 수 없었던 우발적인 사고이므로 최소한의 관련성(mininum contact)을 충족하지 못하므로 원고의 주장은 '합리적이고 공정한(reasonable and fair) 원칙'에 어긋난다고 판단하여 Volkswagan이 승소한 사건이다.

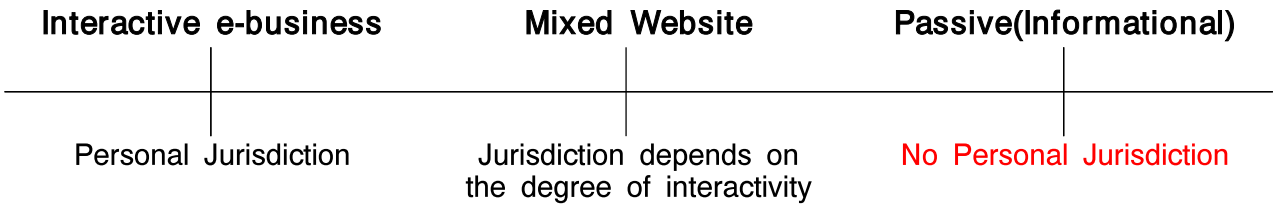
(의의) 이미국 수정헌법 제14조의 적법절차(due process)에 따라 '최소한의 관련성(minimum contact)'을 인정받기 위해서는 "피고의 행위에 의해 피고가 그 주의 법원에 제소당할 것을 합리적으로 예측할 수 있어야 한다"고 판결함으로써 대인 관할권을 확대 해석하는 경향을 제한한 사례로 중요한 의미를 가진다.

Ⅱ 온라인 환경에서의 재판관할권 (Jurisdiction In Online)

온라인(on-line) 환경에서는 웹사이트를 통해 e-business를 수행하게 되는데, 이런 경우에 웹사이트를 Passive Web Sites와 Interactive Web Sites로 구분할 수 있으며 다음과 같은 특성이 있다.

Passive Web Sites	Interactive Web Sites
· 단지 정보만 제공 · 비즈니스용이 아님(이익을 추구하지 않음) · 일반적으로 다른 지역의 대인관할권 (personal jurisdiction)이 적용되지 않음	· 구매결정 등에 대한 정보를 제공 · 비즈니스용(이익을 추구) · 타 지역의 대인관할권(personal jurisdiction)이 적용될 가능성이 존재

Sliding-Scale Analysis of Personal Jurisdiction



6 "Digital Equipment Corp. v. AltaVista Tech." - ★★★

(개요) AltaVista는 Digital에게 Trademark를 양도하면서 앞으로는 회사명과 URL에만 제한하여 사용하기로 계약하였음에도 불구하고 Web Site를 Digital의 AltaVista Web Site와 비슷하게 하는 등 영업에 이용한 사건으로 계약에 의해 준거법을 정하고 있으며, AltaVista **Web Site를 Active하게 운영**한 사실이 인정되어 Digital의 재판관할에 따를 것을 인정한 사례

7 "Zippo Manufacturing Company v. Zippo Dot Com. Inc." (1997) - ★★

(개요) 원고인 Zippo Manufacturing Co.는 펜실베니아 주에서 유명한 Zippo 라이터를 생산하는 회사이고, 피고인 Zippo.Com은 캘리포니아 주에서 [zippo.com], [zippo.net], [zipponews.com] 이라는 도메인명을 사용하여 인터넷 뉴스를 제공하였다. 이에 원고는 피고가 해당 도메인명을 사용함으로써 원고의 Zippo 상표권을 침해(infringement)하였다며 소송을 제기하였다.

(결과) 법원은 피고(zippo.com)가 원고의 법정지인 펜실베니아 주에서 약 3,000명의 웹사이트 회원들과 계약을 체결한 점을 근거로 능동적 웹사이트(Interactive e-business website)로 판단하여 원고에게 재판관할권이 있다고 판결했다.

즉, 피고는 펜실베니아 주의 접촉은 우연성에 의한 것이라고 주장하지만, 계약체결이 거주자의 신청서를 받고 비밀번호를 부여하는 방식으로 반복적이고 지속적으로 이루어졌기 때문에 우연이라고 보기 어렵다고 판단하였다.

8 "Bensusan Restaurant Corp. v. King" (1996) - ★

(개요) 원고인 Bensusan Restaurant Corp.는 뉴욕에서 유명한 Jazz club인 'Blue Notes'를 상표 등록하였으나, 미주리 주에 거주하는 King이 원고의 상호명과 동일한 'Blue Notes' 웹사이트를 만들어 운영하였다. 이에 원고는 피고인 King의 웹사이트가 상표권 침해(trademark infrigement)라고 주장하며 소송을 제기한 사건이다.

(판결결과) 법원은 피고인 King이 운영한 'Blue Notes'는 단순한 광고와 정보만 전달하는 수동적인 웹사이트(Passive website)이고, 서비스 대상을 미주리 주의 주민으로 제한하고 있으므로 뉴욕에서 재판관할권을 행사할 수 없다고 판단했다.

즉, King의 웹사이트는 단순정보 전달을 위한 수동적인 웹사이트이므로 이를 통해 뉴욕 주에서 상품을 선전, 판매 등의 행위를 할 의도가 없었기 때문에 뉴욕 주에 영향을 끼칠 수 있다는 단순한 예견사항으로 대인관할권을 행사하기에는 적절하지 못하다고 판단하였다.

Ⅲ 효과이론 (Effect Doctrine)

최소한의 관련성(minimum contact)이 없어도 실질적인 영향(substantial effect)을 미쳤을 경우에는 판결에 영향을 미칠 수 있다는 이론이다. 따라서 서로 다른 위치에서 재판관할권을 요구할 경우에 최소한의 관련성(minimum contact)을 판단하여 결정하되 사항에 따라서 효과이론(effect doctrine)을 적용할 수 있다.

9 "Calder v. Jones" (1984) - ★★★★

(개요) 플로리다에서 연애잡지 기자인 Calder는 캘리포니아에서 살고 있는 여배우 Jones에 대해 악의적인 기사를 연애잡지(National Enquirer)에 게재하였다. 이에 여배우 Jones은 잡지사와 취재기자, 편집인을 상대로 캘리포니아 법원에 명예훼손 소송을 제기하였고, 피고인 Calder는 해당 잡지는 대부분 플로리다 주에서 판매되고 있으므로 캘리포니아 주와는 '충분한 최소한의 관련성(sufficient minimum contact)'이 없기 때문에 플로리다에서 재판을 해야 한다고 주장하였다.

(결과) 법원은 '최소한의 관련성(minimum contact)'은 없으나, 원고인 Jones은 유명한 여배우로 캘리포니아 사람들에게 관심 대상이라는 점과 원고에게 심리적 고통과 직업적 명예를 훼손하여 추후 악영향을 끼칠 수 있으므로 '효과이론(effect theory)'을 적용하여 재판관할권이 원고의 법정지인 캘리포니아에 있다고 판결하였다.

(의의) 최소한의 관련성(minimum contact)으로 설명되지 않는 사건을 '효과이론(effect theory)'을 적용하여 판결한 최초의 사례로서 의미를 가진다.

10 "Pavlovich v. DVD Copy Control Assn." (2002) - ★★★★★

1심에서 DMCA에 의해 불법 인정, 그러나 2심에서 번복(재판관할 행사 불가)

(개요) 인디애나 주에 거주하는 Pavlovich는 DVD 판독코드를 자신의 웹사이트에 게시하였다. 이에 대해 캘리포니아 주의 영화사업자들은 해당 DVD 판독코드로 인해 영화 및 컴퓨터 산업에 심각한 피해를 입었다고 주장하며 영화산업이 가장 집중된 캘리포니아 법원에 소송을 제기하였다. 이 사건의 경우 아래와 같이 2가지 관점에서 접근할 수 있다.

1) 재판관할권 관점

DVD 판독코드가 실질적으로 캘리포니아 주의 영화산업 전반에 악영향을 미쳤으므로 효과이론(effect theory)에 근거하여 Pavlovich의 행위는 불법 행위로서 간주된다.

2) DMCA(Digital Millenium Copyright Act) 관점

사전에 예고되고 학구적인 목적을 제외한 모든 Decoding를 금지하는 DMCA 법상으로는 Pavlovich의 행위는 불법행위로 간주된다.

(결과) 1심에서는 1)번, 2)번 모두 받아들여 캘리포니아에 재판관할권이 있다고 판결하였으나, 2심에서는 Pavlovich가 위법사실을 충분히 알고 있었던 부분은 인정되나, Pavlovich의 행위가 상업적 목적이 없어 심각한 수준이 아닌 점과 영화산업에 미친 실질적인 효과가 크지 않은 점을 고려할 때, 법정지 이외의 지역인 캘리포니아에서 재판을 받는 것은 적법절차(due process)에 어긋나므로 California에서 jurisdiction을 행사할 수 없고, Pavlovich의 고향인 Texas나 해당 Hacking Code를 Site에 올렸을 때 살았던 Indiana에서 jurisdiction을 행사할 수 있다고 판결함

IV 부종계약 (Adhesion Contract)

계약은 항상 "합리적이고 공정하게(reasonable and fair)" 이루어져야 하며, 상호간에 "자율적으로 협상(freely negotiated)" 되어야 한다는 의미로 그렇지 못한 경우에는 소비자 보호(comsumer protection) 관점에서 다루어져야 한다.

즉, 계약은 소비자의 자유의지(free will)에 의해 선택(choice)될 수 있어야 한다.

11 "Am. Online, Inc. v. Superior Court (Mendoza)" (2001) - ★★★

(개요) 캘리포니아에 거주하고 있는 Mendoza는 버지니아에 본사가 있는 온라인 사업자인 AOL에 인터넷서비스 해지를 요청하였으나, AOL은 그의 신용카드에서 서비스 사용료를 지속적으로 인출하였다. 이에 Mendoza는 비슷한 상황을 겪은 다른 이용자들과 함께 징벌적인 손해배상(compenstatory and punitive damage)을 요구하는 집단소송(class action)을 제기하였다.

이 때 AOL은 인터넷서비스 이용과 관련한 어떤 분쟁에 대해서도 버지니아 주가 재판관할권을 갖는다는 조항을 이용약관(terms of service)에 명시하고 있었다.

(결과) 계약이 효력을 가지려면, 계약(contract)은 계약 당사자가 내용을 충분히 이해한 상태에서 자유의지(free will)에 따라 공정하고 합리적(fair and reasonable)으로 이루어져야 하는데, AOL은 회원 가입시 이용약관(TOS)에 대한 동의를 일방적으로 요구하였기 때문에 이 약관이 이용자의 자유의지에 따라 공정하고 합리적으로 이루어졌다고 볼 수 없기 때문에 재판관할권이 캘리포니아주에 있다고 판결하였다.

(의의) 이 사건은 인터넷 사이트상의 이용약관이 과연 계약으로서 효력이 있는가에 대한 판례로 이용자의 자유의지(free will)가 충분히 반영되었는지 여부가 판단의 중요한 잣대라는 사실을 알려주는 사례이다.

12 "Jacobson v. Mailboxes, Etc. USA., Inc." (1955)

(개요) 재판관할권이 일방적이고 교섭없이(non-negotiated) 불공정하고 불합리(unfair and unreasonable)하게 체결된 부종계약(adhesion contract)이라는 문제이고, 불공정하고 불합리(unfair and unreasonable)하게 체결되었다면 강제력이 있어 이 계약을 적용하여야 한다.

13 "The Bremen v. Zapata OffShore Co." (1972)

(개요) 계약이 상호 "freely negotiated" 되어야 한다는 판결사례

V 국제 재판관할권 (International Jurisdiction)

초기 미국법원은 외국에서 이루어진 행위에 대하여 미국법원이 그 관할권을 행사하는 역외적용(extra-territorial application)에 대해 부정적인 입장이었으나, 1945년 Aloca사건에서 '효과이론(effect doctrine)'을 취함으로써 역외적용을 인정하였다. 이로 인해 국제사회에서 여론이 악화되자 이익형량이론(interest balancing theory)으로 소극적인 태도를 보이다가 1993년 Hartford 사건을 통해 다시 '효과이론(effect doctrine)'을 받아들여 적극적인 입장으로 선회하였다.

결과적으로 미국은 국가를 우선시하는 나라로 비록 다른 국가에서 일어난 행위라도 자국에 '실질적인 영향(substantial effect)'를 준다면 처벌하겠다는 것

- ○ **Territoriality principle** : 다른 나라와 배타적으로 물리적인 영토로 자국에만 적용
- ○ **Nationality principle** : 영토와 상관없이 자국의 국민에게 적용
- ○ **Effect principle** : 국가에 손해를 끼치는 각종 행위를 범죄로 취급함으로써 자신의 국익을 보호하는 방식(예; 2002.9월 중국 국민에게 구글 접속 차단)

14 "Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme" (2001) - ★★★★★

(개요) 프랑스는 나찌(Nazi) 관련 이야기, 기념품 판매 등은 법으로 금지하고 있는데, 캘리포니아에 위치한 Yahoo. Inc는 Yahoo.com의 Yahoo.프랑스 Auction 사이트에서 나찌(Nazi) 관련 기념품을 판매하고 있었다. 이것을 확인한 프랑스에 거주하는 Marc Knobel이 Yahoo의 Auction 사이트는 누구나 쉽게 접근·구매할 수 있으므로 프랑스 법을 위반한 것이라고 주장하며 LLCRA의 대표자로서 Yahoo!를 프랑스 법원에 고소하였다.

이에 프랑스 법원은 Yahoo. Inc.에게 Yahoo.프랑스 및 Yahoo.com 사이트에서 나찌(Nazi) 관련 자료를 모두 삭제할 것을 명령하였다. 이에 대해 Yahoo. Inc.는 Yahoo.프랑스 사이트에서는 해당 자료를 필터링 후 삭제하였지만, Yahoo.com 사이트에 대해서는 "프랑스 법원의 판결은 미국 법원에서 효력이 없다"고 주장하며 미국법원에 소송을 제기하였다.

(결과) 캘리포니아 법원은 프랑스 법원의 판결이 적절하다 할지라도 미국 법원의 관점에서 볼 때, 미국 헌법상의 권리를 박탈하고 미국 등 다른 지역에는 영향을 끼치지 않으므로 인정할 수 없다는 이유로 캘리포니아의 재판관할권을 인정하였다.

(의의) 이 판례로 인해 국제적으로 다른 나라의 법률과 습관을 존중하는 국제의례(the comity of nations)가 자리 잡게 된 계기가 되었다.

15 "United States v. Thomas" (1996) - ★★★★★

(개요) 캘리포니아 주에 거주하던 Thomas 부부가 집에서 AACBBS(Amateur Action Computer Bulletin Board System)으로 Porno Download Service를 운영하던 중 테네시 주의 한 주민이 U.S. Postal Inspector인 David Dirmeyer에게 이 사실에 대해 불평을 제기하였다. 테네시 주에서는 Thomas가 제공하던 Porno는 불법이었으므로 원고는 Thomas를 기소하였다.

Thomas는 (테네시에서는 음란일지 몰라도 캘리포니아에서는 단순 포르노로 취급하기 때문에) 서버가 캘리포니아에 있기 때문에 자신들의 Porno가 테네시 주 밖에서는 합법적이고, 아울러 테네시 주에서 확인된 porno가 자신들이 전송한 것이 아니라 테네시 주의 사용자가 다운로드 한 것이므로 테네시 주가 재판관할권을 행사할 수 없다고 주장하였다.

(결과) 법원은 피고가 제공한 포르노 서비스가 테네시 주에 미친 효과(effect)가 크고, 상업적으로 사용하였기 때문에 테네시 주에서 재판관할권을 행사 할 수 있다고 판결하였다.

(의의) 이 판결 이전에는 다른 주민에 대해 재판관할권을 행사한 경우가 거의 없었다는 점에서 이번 판례는 큰 의미를 갖는다.

16 "Lorraine v. Markel American Ins. Co." (2007) - 참고

(개요) Lorraine이 소유한 요트가 벼락으로 인해 손상됨. 이 요트는 Online으로 Markel에 보험이 가입되어 있었음. 이에 Lorraine이 Markel에 피해 금액을 청구, 보상을 받아 수리를 함. 며칠 뒤 요트에 손상된 부분을 추가로 발견, 이를 또 청구하자 Markel이 이를 일부 거부함. 이에 Lorraine이 계약의 불이행(Breach of Contract)으로 고소한 Case.
피고 측에서는 이메일 등의 전자문서는 그 효력을 발휘할 수 없다고 주장

Lorraine과 Markel간의 Contract가 Electronic 상에서 E-mail을 통해 이루어 졌으므로 중간에 negotiation 과정에 사용된 E-mail에 대해 어디까지 증거로 인정을 할 수 있는가가 쟁점이 됨. 원고가 주장한 전자문서들은 그 효력을 발휘할 수 없다. 그 문서들이 효력을 발휘하기 위해서는 원고가 그 문서들에 대한 무결성을 증명해 내야 한다고 판결

e디스커버리 규제 시대에서 e허용성(E-Admissibility) 규제 시대로의 변화를 알리는 중요한 판례로 기업들의 e디스커버리 대응전략에 변화가 필요함을 시사한다. 폴 그림 판사는 101페이지에 달하는 판결문을 통해 이메일을 포함한 웹사이트 게시글, 디지털 사진 등 다양한 유형의 전자정보들이 법적 증거로 허용될(admissible)수 있는 조건들을 조목조목 상세히 적고 있다. 이 판결문은 전자정보들이 일정한 조건을 갖추지 않으면 증거에서 배제될 수 있으며, 전자정보가 위·변조되지 않았다는 원본성(Authenticity)등을 당사자가 직접 증명함으로써 법적 증거로서 인정받을 것을 요구하고 있다.

17 "Columbia v. Bunnell" (2007) - 참고

(개요) Bunnell은 미국회사이지만 서버를 EU(네덜란드 암스테르담)에 두고 사업을 영위하고 있는 상황에서 Columbia가 소송을 제기 미국은 재판관할을 인정하고, 저작권 훼손관련 건수를 파악하기 위하야 데이터의 제출을 요청하였으나 이에 응하지 않자 서버 압수수색을 하게 되는 등 결과적으로 한 건당 3만 달러의 손해배상을 할 것을 판시 한편 EU에서는 미국 법원에 고객의 정보를 제출하는 것은 고객의 Privacy를 침해하게 되는 것으로 위법이므로 1억1,000만 달러의 손해배상을 선고하여 Bunnell 회사는 결국 파산하게 되는 사건 이는 미국과 네덜란드 양쪽에서 재판관할을 행사한 사건임

18

(개요) 변호사는 Neff에게 받아야 할 돈이 있었다. 당시 Neff는 Oregon주에 거주하지 않았지만 땅을 소유하고 있었으므로 변호사는 Oregon 주법원에 소송을 걸었다. 그래서 변호사는 일정 기간 동안 공지를 게재하고, Oregon 법원이 Neff의 땅을 매매하여 Pennoyer가 그 땅을 사게 되었다. 시간이 흐른 뒤 Neff는 "Notice를 받지 못했다"며 땅을 찾으려고 연방법원에 무효신청을 했다. Pennoyer는 합법적으로 돈을 내고 산거라고 자신의 소유를 주장했고, Neff는 Origon주는 자신에 대한 사법권이 없고, 소송공지는 적법하지 않았다며 자신의 소유를 주장했다.

(결과) "물리적 존재(Physical Presence)"가 없으므로 무효라고 판결하였다.
: 물리적인 존재가 없는 가운데 Jurisdiction을 행사 할 수 없다.
Unreasonable burden : 예전에는 다른 주에 있는 사람을 불러오는 행위
Unfair >> Due Process

(의의) 비거주자 피고인(Nonresident Defendant)에 대한 Jurisdiction은 해당 State 내에 Physical Presence가 있는 경우에만 가능하고 이에 대한 Notification이 있어야 함을 판시한 사례.

VI 기출문제

2007년 1학기 기말고사(사이버법률)

◎ 온라인 환경에서의 Personal Jurisdiction에 관한 문제이다. 대법원은 사건의 사실 관계가 General Jurisdiction이나 Specific Jurisdiction을 만족한다면 Due Process 여하에 따라 사건의 재판관할권을 판단한다. General Jurisdiction은 'The out of state defendant had a substantial, continuous, and systematic presence in the foreign state'를 의미한다. **Specific Jurisdiction의 Minimum contacts 3가지를 기술하라.**

=> minimum contact(의도적이익추구, 피고의행위로소제기, 관할예상)

◎ Verizon Online Service Inc. v. Ralsky(2002)는 Burger King v. Rudzewicz(1985)을 적용한 판례이다. 이를 감안하여 분석하라.

=> minimum contact(의도적이익추구, 피고의행위로소제기, 관할예상)

◎ Nonresident E-Business의 Personal Jurisdiction에서 Sliding-Scale Analysis가 의미하는 바가 무엇인지 간단히 설명하고, **Jacobson v. Mailboxes, Etc. USA Inc.(1995)** 사건의 판결과 판결의 근거를 간단히 설명하라.

=> interactive Web, mixed Web, passive(information) Web, 위 소송은 온라인상의 forum selction clause를 협의없이 일방적으로 동의하여 공정하지 않고 합리적이지 못한 계약에 의하기에 재판관할권을 판단하는 것은 옳지 못하다고 판시(adhesion contact)

2005년 2학기 종합시험

◎ 파블로비치 사건

2006년 1학기 종합시험

◎ 리니지의 개인명의 도용 사건에 대한 jurisdiction 관점에서 논하시오.

2007년 1학기 중간고사 (정보법학)

◎ Pavlovich v. The Superior Court of Santa Clara County and DVD Copy Control Assn. Inc. 사건을 Jurisdiction 관점에서 논하라.

=> 파블로비치의 행위가 영화산업에 미치는 Effect를 가지고 판단, 산업에 미치는 영향이 적다고 판단하여 파블로비치의 관할 법정지에서 재판을 수행하도록 함

◎ Verizon Online Services, Inc. v. Ralsky(2002)는 Burger King v. Rudzewicz(1985)을 적용한 판례이다. 이를 감안하여 분석하라.

=> Minimum contact(의도적이익추구, 피고의행위로소제기, 관할예상)

CH2.
COPYRIGHT



Ⅰ 저작권 보호대상 판단기준(Criteria for Copyright Protection)

1 **Originality** (독창성) : 유사하지 않은 독자적 표현

2 **Creativity** (창조성) : 직접 제작한 고유의 창조물이어야 함

3 **Fixed form** : 저작권 보호대상이 고정적 형태이어야 함

Ⅱ 저작권 침해(Copyright Infringement) - ★★★ 기출 (2007 1학기 기말고사)

1 직접침해(Direct Infringement)

- 저작권자 허가 없이 저작권 존속기간 중에 사용하거나 만드는 행위

2 기여침해(Contributory Infringement)

- 1) 저작권이 침해되는 것을 알았거나 알수 있음에도 불구하고, 2) 침해행위를 유발하거나 그 침해행위에 상당부분 기여한 경우 그 침해행위에 대한 간접책임을 지는 것

3 대위침해(Vicarious Infringement)

- 회사가 1)침해행위를 감독할 능력과 권리(right and ability of control)를 가지고 있고, 제3자의 침해행위로 인해 회사가 2)직접적인 금융이익을 받게 되는 경우

Ⅲ 저작권 보유자가 가지고 있는 권리 (Exclusive statutory Rights) - ★기출 (2005-1)

1 저작물에 대한 재생산권 (to reproduce the copyrighted work)

☞ MAI System v. Peak Computer

2 저작물의 판매, 대여, 배포권리 (to sell, rent, or distribute copyright work)

☞ Playboy v. Frena

3 원 저작물의 파생저작물(소설, 영화 등)에 대한 권리

☞ Lewis Galoob Toys, Inc. v. Nintendo, Inc

4 대중 또는 공공에게 저작물의 공연 또는 전시할 권리

☞ Columbia Picture v. Aveco, Inc

IV 저작권 소유자 독점 권리의 한계(Limit on copyright owner's right)

1 Fair Use Doctrin - ★★★★★ 기출 (2005 1학기 중간고사)

저작권 침해에 대한 폭넓은 인정은 연구 활동 등에 냉각효과를 가져올 수 있으므로 저작권자의 불필요한 권리를 제한하는 법률(다음중 2개 이상을 만족하면 Fair Use 인정)

① 저작물의 사용목적과 성격 (purpose and character of the use) ☞ Marcus v. Rowley
② 저작물의 성격 (nature of the copyrighted work) : 뉴스의 가치가 있거나 이벤트 정보
③ 인용된 저작물의 양과 실재성 (Amount and substantiality) ☞ Harper v. Napster
④ **저작물의 사용이 시장에 미치는 영향** (Effect upon work's value) ★

2 First Sale Doctrin - ★★★★★

정당하게 구매한 물품에 대해서는 중고판매도 인정, 하지만 컴퓨터 프로그램과 같은 디지털매체나 자료는 사용에 대한 라이센스(License)만 부여한 것이므로 저작권 소유자의 허락을 받지 않는다면 저작권 위반임 ☞ (ProCD, Inc. v. Zeidenberg)

3 Public Domain

정부 간행물이나 저작권을 포기한 저작물 또는 저작권 보호기간이 만료된 저작물로 저작권 침해가 성립하지 않음

4 Copyright of common(CC)

무료로 사용하되 저작권을 인정하면 안됨 (ex : LINUX)

V 저작권 침해에 대해 원고가 취할 수 있는 행동 (Remedies for copyright infringement of Plaintiff)

1 **Monetary damages** : 패해 금액과 피고의 수익 등에 대한 금전적 보상

2 **Statutory damages** : 건당으로 피해금액 보상, 악의적인 경우 징벌적 처벌 대상

3 **Attorney's fees** : 변호사 비용 보상 가능

4 PI(Preliminary Injunction) or TRO (Temporary Restraining Orders) :
가처분 및 영업정지처분 등

Ⅵ 디지털저작권 보호법(DMCA, Digital Millennium Copyright Act)

□ **입법 취지** : 미국은 Information Highway라는 국가정보망 구축을 위해 교환되는 정보에 대한 지적재산권 보호를 위해 동 법을 제정 - ★★★★★

□ **주요 내용** : 저작권으로 보호되는 ① 'Digital Lock' 저작물의 보호조치 또는 기술적인 조치를 우회하여 무력화 시키는 어떠한 행위도 금지하며, ② 정보의 이용 및 제공시 저작권자에게는 저작권 침해사실에 대한 통지의무를 부여하고 ③ ISP에게는 가능한 범위내에서 저작권 침해 방지활동을 한다면 해당 손해배상을 면책해 준다는 것이 핵심 내용

☞ Private Interest를 위한 Digital Lock Infringement (Reverse Engineering)나 Trafficking Circumvention Tool의 경우에는 면책되지 아니함(저작권 침해에 해당)

☞ Digital Lock이란, 저작권 보호를 위한 암호화, 접근통제, Scramble 등의 방안임

☞ 개인 취향을 위한 Reverse Engineering 등의 경우에도 저작권 침해에 해당

Ⅶ Safe Harbor for OSP under DMCA

□ **개념 : 2차적 책임의 면제(Exemption from secondary liability),** 즉 인터넷, 온라인서비스제공자(OSP)가 암호화, 접근통제(Access control) 등 합리적 조치(Reasonable measure)로 컨텐츠(Contents)를 보호하고, 회원들에게 적절한 공지(Proper notification)를 취한 경우에는 면책한다.

□ **기타** : 온라인서비스제공자(OSP)를 Publisher로 보는 경우 통제력(Control power)이 있으므로 책임(Liability)이 있을 수 있으나, 배포자(Distributor)인 경우 냉각효과(Chilling Effect)를 고려하여 면책한다.

다만, 아동 포르노(child porno), 마약(drug) 등 사회적으로 실질적인 효과(Substantial effect)가 있는 경우에는 면책에서 제외한다.

Ⅷ 기 타

□ 악의적인 경우 처벌 기준

· [Bad] Knowingly
· [Worse] willfully (=intentionally + voluntarily) 고의적/자발적
· [Worst] with malice 악의적 = 명예훼손이 성립하기 위해서는 malice가 있어야 함
· 단순실수(mistake)의 경우에도 의료사고, 환경문제, 저작권 등 파장이 클 경우 엄격한 책임(strict liability)을 물을 수 있음

□ Linking to a Web Site

사전 동의 없이 웹 사이트에 링크한 경우는 배포권에 관한 침해이므로 주의해야 한다.

□ Lock-In Effect

제품을 바꾸는데 Switching cost가 클 경우 소비자는 그 제품이 어느 정도 획기적이지 않다면 잘 옮기거나 바꾸려고 하지 않는다. 이 때문에 인터페이스 공유가 이루어지지 않는다면 해당 상품의 독점효과가 나타날 수 있다.

□ 저작권 보호연장법(CTEA, Sonny Bono Copyright Term Extension Act of 1998)

· Duration of copyright - Eldred v. Ashcraft (소급위법, retro-active)
· 보호기간을 20년씩 증가 (78년 이전 : 47년 - 67년, 78년 이후 : 50년 - 70년)
· 월트디즈니사의 강력한 로비에 의하여 등장한 법이라고 하여, 미국 내에서 입법화될 때부터 국민들로부터 강한 비난을 받고 '미키마우스법'이라는 조롱을 받기도 했던 법

□ No Electronic Theft Act (NET)

· 저작권 침해와 관련하여 위법의도와 경제적 이득에 관계없이 피해액이 $2500 이상이면 형사 사범(Criminal)으로 처벌 가능함

□ 통신품위법(CDA, Communications Decency Act)

· Good Samaritan Provision
· 온라인서비스제공자(OSP)가 합리적 수단(Reasonable measure)을 통해 중재(Internal control) 한 것이 인정되는 경우 면책 가능함

IX 사례 분석 (CASE STUDY)

1 "Playboy Enter. Inc. v. Frena" (1993) - ★★★

(개요) 피고인 Frena는 Playboy가 저작권을 가진 170여개의 이미지를 제공하는 게시판 시스템(BBS)을 운영하고 있었다. 이에 대해 Playboy는 '저작권 및 상표권 침해(Copyright& Trademark Infringement)' 등의 이유로 Frena를 고소하였다.

(결과) Frena는 '공정사용(Fair Use)'을 주장하였으나, 법원은 피고가 운영한 게시판 시스템이 1)상업적인 목적(Commercial purpose)을 가지며, 2)Entertainment의 Nature를 갖는 Work의 Important Part이고, 3) Playboy의 사업이익에 영향을 주기 때문에 'Fair Use'를 기각하였다.

또한 피고는 Playboy의 저작권 중 '배포권(Right of Distribution)과 공연·전시권(Right to Perform and Display Publicly)'을 침해(Infringement)하였다고 판결하였다.

(의의) 이 사건은 게시판 서비스(BBS)에 대해 직접침해(direct infrigement)를 최초로 인정한 사례로 게시판 운영자는 게시판에 대한 철저한 모니터링 의무가 있음을 알리는 계기가 되었다. 즉, 게시판 운영자는 저작권이 있는 문서 등을 저작권 소유자의 허락 없이 게시하거나 고객들로부터 다운로드 받게 하면 저작권법에 위반될 수 있다는 것이다.

2 "Viacom v. google" (2007) - 참고

(개요) Viacom은 MTV, Paramount의 지주회사로 U-Tube에 저작권 침해(Copyright infringement) 관련 동영상이 게시되자, 해당 저작물 게시자는 개인으로 배상할 능력이 없으므로 Google에게 2차적인 책임이 있다며 소송을 제기하였다.

(결과) 이 사건의 경우 Google이 문제의 동영상 게시를 방조했는지와 저작권 침해 규모가 어느 정도 인지를 파악하는 것이 중요한데, 이를 위해서는 해당 동영상을 업로드 및 다운로드한 개인정보를 알아야 하나, NGO가 프라이버시 침해로 반대하여 결과적으로 재판부는 Google에게 책임을 묻지 않았다.

(의의) 이는 저작권(copyright)과 프라이버시(privacy)간의 상호 대립적인 관계를 알 수 있으며, 이 점에 대하여 사회적 합의를 이끌어내는 것이 중요한 당면 과제임을 인지시키는 사례이다.

3 "Rural Telephone Services Inc. v. Feist Publications, Inc" (1991) - ★★

(개요) Rural사는 캔자스주 북서부 지역의 전화사업자로서 고객을 위해 알파벳 순서에 따라 인명편과 상호편으로 구성된 전화번호부를 발간하였다. 피고인 Feist는 출판업자로서 위 지역을 포함한 광역 전화번호부를 출판하고자 원고에게 해당 전화번호부의 이용 허락을 요청했으나 원고가 이를 거부하자, 피고인 Feist는 원고의 전화번호부의 일부를 임의로 복제하여 CD형태의 디지털 전화번호부(Digital phone-book)를 만들어 판매하였다.

이에 대해 원고는 저작권 침해 소송을 제기하였으나 피고는 복제사실은 인정했지만 전화번호부는 그 성격상 지속적으로 갱신되므로 독창성(Originality)이 없으므로 원고의 전화번호부는 저작권이 없다고 주장하였다.

(결과) 법원은 알파벳 순으로 단순 배열한 전화번호부는 독창성(Originality)이 없기 때문에 저작권 보호대상으로 판단하기 어렵다는 이유로 저작권이 없다는 Feist의 주장을 인정하였다.

(의의) 저작권 보호는 1)독창성(Originality), 2)창조성(Creativity), 3)고정된 형태(Fixed form) 요건을 갖출 때 비로소 인정될 수 있다는 획기적인 판결(landmark decision) 사례이다.

4 "CCC Information Services v. McAllen Hunter Market Reports" (1994) - ★★

(개요) 중고차 회사인 CCC Information Service는 "Red Book"이라는 중고차 소개 책자를 발간하였고, 피고인 McAllen사는 이를 CD로 만들어서 배포하였다. 이에 원고는 저작권침해로 소송을 제기하였다.

(결과) "Red Book"은 < Rural Telephone Service v. Feist Publication > 판례와 달리 단순한 정리 수준이 아니라 중고차의 특성, 평가 등 소비자가 원하는 것을 찾기 쉽도록 아이디어를 갖고 책을 구성했기 때문에 독창성(Originality)이 인정되므로 저작권침해로 볼 수 있다고 판결하였다.

(의의) 저작권은 1)독창성(Originality), 2)창조성(Creativity), 3)고정된 형태(Fixed form) 요건을 갖출 때 보호될 수 있음을 알 수 있다.

5 "*MAI Sytems Corp. v. Peak Computer, Inc.*" (1993) - ★★★★★

(개요) 컴퓨터 수리 전문회사인 Peak사는 MAI사의 컴퓨터 진단 S/W 프로그램을 구입하여 고객의 컴퓨터를 수리하는데 사용하였다. 이에 원고인 MAI사는 피고가 해당 S/W 프로그램을 사내용으로만 사용하는 것을 전제로 라이센스(License) 계약을 체결하였으므로 일반 고객의 컴퓨터 수리용으로 사용한 것은 해당 S/W를 설치, 진단 후 즉시 삭제하였다 할지라도 저작권 침해라며 소송을 제기하였다.

(결과) 법원은 해당 S/W 프로그램이 RAM에 복사되는 것은 충분히 영속성이 있고, 고정된 형태(fixed form)라고 볼 수 있으므로 저작권 침해라고 볼 수 있으며, 피고는 해당 S/W를 사내용 이외의 목적으로 사용하기 위해 저작권 소유자인 원고와 상업적인 계약(Commercial contract)을 체결하지 않았기 때문에 해당 프로그램을 회사 외에서 사용한 것은 불법이라고 판결하였다.

(의의) 이 판례 이전에는 RAM에 일시적으로 저장되는 정보에 대하여 저작권침해를 인정하지 않은 판례(Apple Computer v. Formula International)를 S/W 프로그램에 대한 사용허가 없이 다운로드 혹은 설치하는 것이 '재생산권(Reproduction right)'를 침해함으로서 저작권을 침해할 수 있음을 경고하는 판례이다.

6 "Universal City Studio v. Sony Corp. US" (1984) - ★★★★★

(개요) Universal사는 Sony사가 제조한 VCR이 자사가 제작한 TV프로그램을 녹화하는데 사용되고 있어 기여적인(contributory) 저작권 침해가 있다는 내용으로 소송을 제기하였다.

(결과) VCR를 이용한 영상 녹화는 다음과 같은 이유로 공정이용(Fair Use)에 해당한다고 판결하였다.

1) **(사용목적 및 성격)** 부재 중 프로그램을 녹화하여 이것을 나중에 사적인 공간에서 시청하는 것은 비상업적인 이용이라고 판단

2) **(저작물의 성격)** 공정이용은 주로 보도, 비평, 교육물에 해당되지만 오락물에 대해서도 저작물이 새롭거나 전환적인 이용에 기여한다면 공정이용이라고 판단한다. 따라서 VCR에 녹화한 후 다른 시간대에 본다는 점과 공중파 서비스는 원래 무료이기 때문에 문제되지 않음

3) **(저작물의 양과 실제성)** VCR로 전체를 녹화하기 때문에 공정이용을 적용받기 힘들지만 의미 있는 시청을 위해서는 전체의 녹화가 불가피하다고 판단

4) **(시장에 미치는 영향)** 녹화로 인해 전체 시청자수가 증가하여 잠재적 시장가치 이익을 침해하지 않는다고 판단

(의의) 새로 도입된 기술과 영상산업의 저작권 보호에 대한 마찰을 보여주는 대표적인 판례로 저작권자의 경제적 이윤 감소 우려 때문에 신기술의 합법적 사용이 제한될 수 없음을 보여주는 판례

☞ 사회 전체적으로 판결의 효과, 영향에 대하여 심층적으로 고려하여 판결하는 것이 중요함

7 "A&M Records, Inc. v. Napster, Inc." (2001) - ★★★★

(개요) Napster는 웹사이트에서 불법 복제된 MP3 음악파일을 공유할 수 있는 교환시스템을 운영하고 있었다. 일반 온라인 서비스 제공자와는 달리 Napster 서버에는 저작물이 복제, 전송, 저장되는 행위가 일어나지 않고 다만, 해당 복제 파일의 목록과 이용자의 하드디스크 정보만 저장하고 있었다. 이에 대해 A&M(음반제작자 및 저작권자)은 Napster가 저작권을 침해했다며 소송을 제기하였고, 피고인 Napster는 "Fair Use"와 디지털저작권보호법(DMCA) 상의 512(a) "SafeHabor" 조항에 의거 직접, 간접 책임이 면책된다고 주장하였다.

(결과) **<Universal v. Sony>** 사례와는 달리 Napster의 파일 교환시스템은 대부분 저작권 침해 용도로 사용되었으므로 1)기여침해(contributory infringement)가 인정되고, 이런 행위에 대해 조치할 능력(ability of measure)이 있었기 때문에 2)대위침해(vicarious infringement)도 적용된다. 또한, MP3 파일이 Napster 서버에서 직접 제공되지 않기 때문에 Napster는 '온라인 서비스 제공자(Online Service Provider : OSP)'가 아니므로 3)DMCA의 "Safe Harbor" 조항도 인정되지 않는다고 판결하였다.

(의의) 이 사건의 경우 저작권 침해 여부를 판단할 때, 통제능력(Control Power)의 존재여부와 실제 사용 용도가 중요한 판단 기준이 된다. 즉 사용자의 편의를 위한다는 명목만으로는 모든 것이 면죄되지 않는다.

8 "Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd." (2005) - ★★★★

(개요) Grokster가 P2P S/W를 무료로 배포하자, MGM이 2차적 저작권 침해로 고소하였다. 이에 대해 Grokster는 단순히 S/W만 제공했을 뿐, 이에 대한 통제능력(Control Power)이 없으며, 경제적 이익을 얻은 사실도 없기 때문에 원고의 저작권 침해 주장은 성립되지 않는다고 주장하였다.

(결과) Grokster가 P2P S/W 배포행위가 저작권 침해에 사용된다는 것을 대체로 인지하고 있었지만, Grokster가 주장하는 바와같이 이에 대한 실질적인 통제력(Control Power)이 없어 기여침해(Contributory Infringement)를 적용할 수 없고, 직접적인 경제적 이익을 취한 것도 아니므로 대위침해(Vicarious Infringement)도 적용할 수 없으므로 Grokster 승소를 판결했다.

(의의) 이 사건의 경우 저작권 침해 여부를 판단할 때, 통제능력(Control Power)의 존재여부가 중요한 판단 기준이 된다.

☞ 강의내용과 다르므로 추가확인 필요

9 "Harper & Row Publishers, Inc. v. Nation Enterprise" (1985) - ★★★★

(개요) H&R 출판사는 독점 계약한 포드 대통령 자서전의 출간을 앞두고 Nation Enterprise 잡지사가 자서전 내용 중 가장 하이라이트 부분인 "닉슨 대통령을 사면한 부분"을 원본 그대로 복사하여 기고하였다. 이에 대해 H&R사는 Nation Enterprise를 저작권 침해로 기소하였다.

(결과) Nation Enterprise사가 양은 적지만 자서전의 하이라이트에 해당하는 핵심부분을 인용하였기 때문에 저작권을 침해하였고, 특히 잠재적 시장가치에 심각한 타격을 입힘에 따라 공정이용(Fair Use)으로 볼 수 없으므로 Nation Enterprise가 저작권을 침해하였다고 판결하였다.

(의의) 이는 저작물의 비영리적, 교육적 이용이 공정이용으로 추정된다는 주장에 대해 법원이 거부한 사례이며, 공정 이용의 판단 기준을 제시하는 판결문으로 의의를 갖는 판례이다. 공정이용(Fair use)은 어디까지나 저작물의 시장성을 손상시키지 않는 범위에서 적용되어야 한다.

10 "American Geophysical Union v. Texaco Inc." (1994) - ★★

(개요) AGU에서 발간하는 잡지를 Texaco가 1부씩 구독하여 Texaco내 도서관에 비치하였는데, 이 잡지가 유용하기 때문에 Texaco 직원들이 이 잡지를 복사해서 사용하였다. 이에 대해 AGU는 Texaco를 저작권 침해(Copyright Infringement)로 고소하였고, 이에 Texaco는 해당 잡지를 사내 도서관에 비치한 후 연구목적으로 사용하였기 때문에 '공정이용(Fair Use)'이라고 주장했다.

(결과) Texaco의 경우 구매능력이 충분히 있음에도 불구하고 복사를 이용하여 직원들에게 제공함으로써 잡지 판매량, 즉 시장에 영향을 미쳤다고 볼 수 있다. 또한 Texaco에서 연구 목적으로 사용했다고 하나 Texaco가 교육기관도 아닐뿐더러 이는 잠재적으로 Texaco의 상업적 이익을 위한 것이므로 순수 연구목적이라 보기 어려우므로 '공정이용'을 적용할 수 없다고 판결했다.

(의의) 공정이용(Fair use)의 1) 사용목적 및 성격, 2) 저작물의 성격, 3) 사용된 양과 실제성 등 3개의 조건을 모두 만족시킨다 하더라도 4)피고의 행동이 원고의 시장에 영향을 끼친 경우에는 "공정이용(fair use)"이 아니라고 판단할 수도 있다.

11 "Sega Enterprise Ltd v. Maphia" (1994) - ★★★

(개요) Maphia는 OSP(Online Service Provider)이고, MAPHIA Chad Sherman이라는 사람이 운영하는 게시판 시스템이다. Sega는 Video Game의 비등록 해적판 12편이 MAPHIA 게시판을 통해 배포되고 있음을 알고 Sherman를 저작권, 상표권 위반 등을 이유로 기소하였다.

(결과) Sherman은 Fair Use를 주장했지만 법원에서는 **<MAI Systems Corp. v. Peak Computer, Inc.>** 사건을 근거로 "MAPHIA" 게시판을 통해 복사가 이루어졌으므로 저작권 침해를 고려해야 한다고 판결했다.

Sega 게임은 1)상용 S/W이고(사용의 목적), 단순한 정보물이 아니라 2)창작품이며(당해 저작물의 성질), 3)게임을 통째로 복사하여 내려 받고(저작물의 양), 그 결과 경제적인 손실을 준다고 판단하였다. 게시판의 성격상 업로드와 다운로드가 자유롭다는 측면에서 운영자가 이를 게시하였다는 증거가 약하므로 직접책임(direct infringement)은 없지만, 게시판 운영자는 사용자들을 관리하고 저작권을 보호해야 할 책임이 있음에도 소홀히 한 부분이 있으므로 기여책임(contributory infringement)을 인정하였다.

(의의) 이 사건은 기여책임이 최초로 인정된 사례이다. 만일 게시판 운영자가 자료를 게시하고 일정한 수익을 받았다면 기여책임이 아닌 대위책임(vicarious infringement) 위반이 된다.

12 "Religious Technology Center v. Netcom On-Line Communication Services, Inc" - ★★★

(개요) 원고 RTC는 신흥종교인 Scientology의 창립자인 L. Ron Hubbard의 writing에 대해 copyright를 가지고 있었고, 피고 Ehrlich는 Scientology의 전직 목사(former minister)로써 Scientology를 비판할 목적으로 Klemesrud의 유료 BBS(Internet 직접 연결 X)에 Hubbard의 writing의 일부를 게재하였고, 이를 Netcom(ISP)을 이용하여 Usenet의 Newsgroup에 게재함. 이에 대해 RTC가 Ehrlich에게 posting의 중단을 요청했고, 이 요청이 받아지지 않자 Klemesrud와 Netcom에게 삭제 요청을 하였으나 Klemesrud와 Netcom이 owner of copyright를 요구하자 이를 거부하고 고소한 사례임.

RTC는 Netcom이 copyright infringement의 source는 아니지만, Direct & Secondary Infringement라고 주장. 이에 대해 Netcom은 "Fair Use"를 주장함

(결과) 법원은 **<MAI Systems Corp. v. Peak Computer, Inc.>**를 근거로 Ehrlich가 writing을 Newsgroup에 올리는 행위는 Copyright Infringement라고 인정하고, Ehrlich는 Direct Infringement가 적용된다고 판결하였음.

원고 RTC는 **< Playboy Enterprises, Inc. v. Frena >**에서 Frena의 BBS가 Copyright의 Right of Distribution과 Right to Perform and Display Publicly를 침해한 것으로 판결한 것을 근거로 Netcom의 Direct Infringement를 주장했으나, 이 Case에서 Court는 Copying 자체에 관한 것이므로 이를 기각.

또한 **< Sega Enterprises Ltd. v. MAPHIA >**에서 BBS의 User에게는 Direct Infringement를 적용할 수 있으나 전자적인 게시판을 운영한 것으로는 Direct Infringement를 적용할 수 없다고 판결한 것을 근거로 Netcom에게 Direct Infringement를 적용할 수 없다고 판결하였음

Netcom은 Infringement를 통보받고도 아무런 조치를 취하지 않았지만, 이를 사전에 막을 수 있는 조치수단(Measure)도 없을 뿐만 아니라 Ehrlich의 posting의 copyright infringement 여부를 확인할 수 없었기 때문에 (RTC가 reasonable measure를 취하지 않음) Contributory Infringement도 적용할 수 없다고 판결하였음

또한 Netcom이 이로 인해 얻는 direct financial benefit이 없으므로 Vicarious Infringement도 적용 할 수 없다고 판결하였음, 결과적으로 Netcom이 승소한 사건임

(의의) Contributory Infringement가 적용되지 않은 Case로 정보 흐름의 중간자 역할을 하는 ISP에게 direct infringement liability를 묻는 것은 적절하지 않으며 또한 직접적인 financial benefit이 없다면 vicarious infringement 역시 인정되기 힘들다고 판결한 사례임.

12 "Eldred v. Ashcroft(법무장관) (2003)" - ★★★★

(개요) 저작권의 보호기간을 사후 50년으로 규정했는데, 이를 사후 70년으로 20년간 연장시킨 일로 CTEA(저작권 보호기간 연장법)이 위헌인지 여부를 판단하기 위한 재판이다. CTEA에 대해서 반대하는 사람들이 법무장관 Ashcroft에 대해 소송을 제기하였다. Eldred는 온라인상으로 저작권이 만료된 문학 작품을 공개하는 프로젝트를 진행하고 있었는데 저작권 기간이 연장되면서 기존에 공개하였던 것까지 모두 공개하지 못 할 상황에 처하자 수정헌법 1조의 표현의 자유에 대한 기본 취지에 어긋나 모든 사람이 공용 자료를 이용하지 못하게 한다고 주장하면서 CTEA 파기를 신청한 사건이다.

(결과) 특허 등의 지적재산권의 기간이 연장되는 것은 당연한 것으로 지나친 것이 아니라고 판결.

(의의) 이 사건으로 인해 저작권 보호기간을 70년으로 연장한 CTEA의 위헌판정 논란에서 벗어날 수 있었다.

13 "Lotus v. Borland (1990)" - ★★★★ *Lock-in Effect에 대한 인터페이스 공유는 저작권침해 불인정*

(개요) Lotus는 회계분석 프로그램 회사이다. 이 당시 Lotus사가 개발한 Lotus 1-2-3 라는 프로그램은 편리함으로 인해 많은 사용자들에게 인기 있는 제품이었다. 하지만 Borland에서 87년 새로운 회계프로그램(Quattro Pro)을 만들었고, 큰 인기를 끌게 되었다. 그런데, Borland에서 제공하는 회계프로그램은 Lotus사의 회계분석 프로그램과 동일한 인터페이스를 사용하였다. 이에 Lotus사는 Borland사의 인터페이스는 자신의 인터페이스에 대한 2차적 저작물이라며 지적재산권 침해 소송을 제기한 사건이다.

(결과) Borland사가 만든 회계 프로그램은 Lotus사의 인터페이스를 그대로 착안했지만 이는 소비자가 기존의 인터페이스에 대해 **Lock-In*** 되어 있기 때문에 교체비용(switching cost)을 줄여 궁극적으로 소비자에게 도움을 주기 위한 행위이므로 "공정사용(Fair use)"라고 판결하였다.

* 제품을 바꾸는데 Switching cost가 클 경우 소비자는 그 제품이 어느 정도 획기적이지 않다면 잘 옮기거나 바꾸려고 하지 않는다. 이 때문에 인터페이스 공유가 이루어지지 않는다면 해당 상품에 대한 독점이 발생하여 시장의 진입장벽이 높아질 수 있다.

(의의) Software에 적용되는 Copyright의 범위를 확인한 사례로 저작권은 인정되지만 인터페이스에 대해서는 공유하는 것이 국제적인 판결의 유형이라고 한다. 소비자를 위한 부분에 대해서는 지적재산권의 공유를 강조하고 있다.

14 "Lewis Galoob Toys v. Nintendo, Inc. (1992)" - ★★★★

(개요) 피고인 Lewis가 원고인 닌텐도사의 비디오 게임기인 "Cartridge"의 콘솔박스를 Reverse Engineering 하여 작동원리를 알아낸 후 "Game Genie"라는 S/W를 만들어 판매하였다. 이에 닌텐도사는 저작권 침해로 소송을 제기하였다.

(결과) 법원은 **<Lotus v. Borland>** 사건을 근거로 Lewis가 만든 "Game Genie"는 닌텐도사의 비디오 게임기의 인터페이스를 이용하여 성능을 향상시킨 것으로 소비자들에게 이익이 되므로 저작권의 근본적인 목적에 위배되지 않는다고 판결하였다. 참고로 이 당시에는 '디지털저작권 보호법(DMCA)'이 만들어지지 않았다.

15 "Columbia Pictures, Ind. v. Aveco, Inc. (1986)" - ★★★

(개요) 피고인 Aveco는 비디오 테이프를 대여한 후 비디오 관람실에서 일반 대중에게 관람하게 함으로써 대중 공연(public performances)을 부적절하게 허가하였다.

(결과) 법원은 비디오 테이프를 대중에게 상영하기 위해서는 저작권자의 허락이 필요하다고 판결.

16 "Marcus v. Rowley" - ★

(개요) 피고인 Rowley은 24페이지 책자를 발간하면서, 원고인 Marcus가 작성한 케익 제조관련 요리책의 35페이지 중에서 11페이지를 해당 책자에 포함하여 출간하였고, 이 책자는 학원 수강생들에게 교육적 목적으로 배포되었다. 이에 Marcus는 Rowley를 상대로 저작권 침해 소송을 제기함

(결과) 법원은 해당 책자가 배포된 곳이 학원이므로 단순 교육적 목적을 넘어 상업적 목적으로 사용되었고, 복제한 양이 너무 많으므로 저작권 침해가 인정된다고 판결하였다.

17 "Steele v. Bulova Watch Co. (1952)" - ★

(개요) 피고인 Steele은 미국 시민권자로 멕시코에 시계 조립공장을 설립하고, 미국에서 부품을 조달후 멕시코 공장에서 조립하여 "Bulova" 상표를 붙여 미국에서 판매하였다. 이에 대해 원고인 Bulova사가 Steele를 상대로 저작권 침해 소송을 제기한 사건이다.

(결과) 법원은 Steele이 가짜 "Bulova" 시계를 멕시코에서 제작하였으므로 저작권 침해가 멕시코에서 발생하였으나, 해당 시계를 미국에서 판매하였고 원고인 Bulova Wathch Co.의 평판에 부정적인 영향을 주었으므로 미국의 저작권법을 적용하여 저작권을 침해하였다고 판결하였다.

18 "ProCD, Inc. v. Zeidenberg" - ★★★★★ *[기출]*

(개요) Zeidenberg가 ProCD의 'SelectPhone™'이란 전화번호와 검색 SW가 담긴 CD를 구매, 이를 이용 자신의 웹사이트에서 유료로 CD의 정보를 판매하였다. 이에 대해 ProCD가 Zeidenberg를 고소한 사건이다.

ProCD의 SelectPhone™의 Term of Use에는 사용자가 사적 이용에 한하여 copy를 허용하고, 양도나 대여, 네트워크에서의 동시사용은 허용하지 않는 내용이 있었고, 이는 manual에 있는 것만이 아니라 SW 실행시 마다 표시되도록 되어 있었음

Zeidenberg는 1) 돈을 주고 산 것이니 사용 권한은 나에게 있고, 2) CD의 포장에 조그맣게 붙어 있는 Notice(Shrink Wrap license)는 잘 보이지도 않기 때문에 계약이 성립되지 않는다고 주장

(결과) 법원은 Zeidenberg가 SW를 사용한 것은 Term of Use에 대한 Agreement로 볼 수 있다고 판결하여 ProCD 승소하였음

(의의) Shrink Wrap License의 Enforceability를 인정한 사례임

19 "NTP, Inc. v. Research In Motion, Ltd." - ★

(개요) NTP는 Patent Licensing Company(=Patent Troll)이고, RIM은 Wireless Device Company이며, NTP가 RIM의 'Black Berry'의 기술 일부에 대하여 Patent Infringement로 고소, PI와 TRO를 요청한 사건이다.

(결과) Distinct Court에서는 RIM을 Willful Infringement(고의적 침해)로 판정, RIM에게 Permanent Injunction과 Fine을 판결함. 이에 RIM이 항소하였으나 Federal Court에서 Distinct Court의 판결에 대해 Infringement는 인정하나 Permanent Injunction(영구적 금지명령)은 취소, 일부 파기 일부인용을 내리고 다시 Distinct Court로 환송을 명함. 이에 다시 RIM이 Supreme Court에 상고하였으나 신청이 인정되지 않았음

2006년 NTP와 RIM이 Full & Financial Settlement로 RIM이 NTP에게 합의금으로 6억$이상을 주고 종결됨

(의의) 특허에 대해 잘 확인하고 영업을 해야 한다는 점을 확인시켜 준 판례로 PI(Preliminary Injunction, 금지명령)와 TRO(Temporary Restraining Orders, 가처분)가 지속되면 Damage가 크기 때문에 Settlement로 가는 경우가 대부분임.

20 "Qualcomm. v. Broadcom" - ★

(개요) Qualcomm의 Chip에 사용된 Energy Saving 기술에 대해 Broadcom이 Patent Infringement로 고소, PI와 TRO를 요청한 사건이다.

21 "Cubby v. Compuserver" - ★★★★

(개요) Cubby에 대한 악성루머가 CompuServe의 게시판에 올라온 것에 대해 Cubby가 OSP인 CompuServe를 Defamation에 대한 Secondary Liability(2차적 책임)로 고소한 Case.

(결과) Court에서는 CompuServe는 단순 Distributor로 Bookstore-Owner와 같이 Service를 제공할 뿐, 그 내용에 있어서는 Control Power가 없으므로 Defamation을 적용할 수 없다고 판결. CompuServe 승소.

(의의) 시대적 상황, 기술으로 보았을 때 reasonable measure가 소극적으로 해석되었음.

[기출문제1] 기여침해와 대위침해의 차이에 대해 기술하시오? - ★★★★★

기출문제

X 기출문제

2005년 2학기 종합시험

◎ Universal studio v. Sony 판결과 현 소리바다 대법원 판결은 상반되고 있다. 자신의 견해를 기술하시오.

=> Universal은 자체제작한 프로그램을 Sony의 VCR로 녹화하는 것을 문제삼아 Sony에게 기여적인 저작권 침해를 했다고 소송을 제기하였으나 Fair Use로 판시한 사례

2006년 1학기 종합시험

◎ 저작권 침해에 대한 사례를 쓰시오.

2007년 1학기 중간고사 (정보법학)

◎ Copyright Owner의 독점적 권리와 관련 판례이다. 하나를 선택하여 분석하라.

(1) To reproduce the copyrighted work : **MAI System Corp. v. Peak Computer Inc.**
(2) To sell, rent, lease or otherwise distributes copies of the copyright work to the public - **Playboy Enter. Inc. v. Frena**

◎ WCDMA 3G 시대를 맞이하여 유무선의 Infra 제약이 사라지고 있다. 모바일 UCC가 더욱 활성화 될 것이며, 지적재산권 보호 측면에서 저작권 소유자, 3G 서비스 제공자, 정부의 입장은 서로 상충되는 면이 크다. 이에 대해 논하라.

2007년 1학기 기말고사

◎ 저작권 침해의 책임은 3가지 이론으로 설명된다. 다음을 설명하라

(1) Direct Infringement
(2) Contributory Infringement
(3) Vicarious Infringement

◎ Copyright owner의 독점적 권리와 관련 판례이다. 다음을 분석하라

To Sell, rent, lease or otherwise distributes copies of the copyright work to the public - **Playboy Enter. Inc. v. Frena**

CH3.
TRADEMARKS



Ⅰ 상표권(Trademark)의 정의

상표나 서비스가 다른 것과 식별되는 특별한 이름이나 단어, 심볼 등으로 USPTO(U.S. Patents and Trademark Office)에 등록한 것을 말한다.

상표권은 1)상표에 대한 재산권을 보호하고, 2)유사상표의 사용으로 소비자의 혼란을 막아 소비자를 보호하며, 3)유명하게 된 것(reputation)에 무임승차(free-riding)하는 것을 막아 불공정경쟁을 방지하는데 목적이 있음

Ex) 대표적인 사건 coke v. Koke (1920)

회사는 상표권을 연구개발(R&D)하고 광고(AD)하는 등 투자를 하였으니 상표권을 재산으로 인정하는 것은 당연한 것이다.

Ⅱ 상표권 구분(Trademark Distinguish)

1 **Genertic mark** : 일반적인 표시 ⇒ 이건 보호대상이 아니다.
ex) 일반명사인 '애플'은 등록 불가

2 **Descriptive mark** : 처음부터 특별(inherently distinctive)했고, 시장에서 2차적 의미(secondary meaning)를 부여됐음을 증명하지 못하면 보호받지 못함

ex) 컴퓨터 업체인 '애플'은 처음부터 독창적이었기에 상표권 등록 가능
ex) inherently distinctive : 마이클조던은 단지 이름에 불과
secondary meaning : 마이클조던은 농구선수라는 새롭게 의미가 부여됨

⇒ 따라서 2차적 의미(secondary meaning)를 갖기 전에는 보호대상이 아님

3 **Suggestive mark** : 상품이나 서비스의 품질을 제시
ex) '애플'은 사과 먹는 것처럼 쉽다는 의미를 제시하는 '애플로고'를 등록 가능

4 **Arbitrary mark** : 일반적인 의미와 전혀 관계없는 임의적인 표시
ex) 컴퓨터와 사과는 처음부터 관련이 없었기에 '애플'이란 상표는 등록 가능

5 **Fanciful mark** : 제품과 처음부터 관련성이 없는 표시
ex) 컴퓨터와 관련성이 있는 상표권 '애플'과 '매킨토시'는 별 관련성이 없으므로 모두 등록 가능

Ⅲ Service Mark & Trade Dress

☐ **Service Mark** : 회사의 서비스를 표시하고 차별화하기 위해서는 해당 상표를 USPTO에 등록하여야만 법적 보호를 받음. 즉, 서비스 상표(service mark)도 본질적으로 식별(inherently distinctive)되고, 2차적 의미(secondary meaning)를 가질 때 보호대상이 된다.

☐ **Trade dress** : trade mark가 확장된 개념으로 특정 브랜드의 인테리어와 같이 제품이 연상되는 색상의 디자인이나 모양새를 말하며, 이것도 2차적 의미(secondary meaning)를 가질 때 보호받을 수 있다.

ex) 파스꾸지(pasccuzi), 맥도널드(Macdonald), 스타벅스(Starbox)의 인테리어 등

Ⅳ 상표권 유효기간(Trademark Duration)

상표권은 최초 등록 후 5년, 5년차에 갱신하며 10년 단위로 계속해서 연장가능, 5년차에 갱신하지 않으면 6년차 말에 자동적으로 취소

* NSI : Network Solutions, Inc(1992-1997)
ICANN : Internet Corporation for Assigned Names and Numbers(1998-) : 도메인 등록처

Ⅴ 상표권 침해(Trademark Infringement)

혼동 가능성이 있는 상표권(likelihood of confusion)을 사용하는 경우 상표권 침해가 발생하며, 상표권의 침해와 관련하여 혼동 여부를 점검하기 위한 기준으로 다음의 Lapp Factors 10가지가 있음

[Lapp 10 Factors : 5~7번이 중요] - ★★★★★

1) **S**trength of the mark : generic mark은 보호하지 않는다.
2) **K**ind of mark : descriptive mark는 덜 보호한다.

3) **Similarity** of the goods : 상품에 관계가 있어야 한다.

4) **Channel** of trade : cyber space에서의 concurrent market은 혼동 가능성의 증거일 수 있다.

5) **Consumer Sophistication** : 인터넷 소비자는 오프라인 유저보다 sophisticated 하므로 경쟁자를 구분할 수 있어야 한다.

6) **Wrongful Intent** : 혼동을 입증할 필요는 없으나 만약 나쁜 의도가 있다면 혼동의 강한 증거가 된다.

7) **Actual Confusion** : resonable prudent consumer가 혼동할 만한가?

8) **Zone** of natural Expansion : 원고는 피고가 시장을 확장했다는 증거를 제공해야 한다.

9) **Length of Time** the defendant used the mark : 혼동 없이 사용한 기간이 길면 길수록 원고의 주장은 약해질 수 있다.

10) **Same sales Efforts** : 같은 사업에 들인 노력의 크기도 혼동의 증거가 된다.

VI 상표권 희석화(Trademark Dilution)

원고의 입증책임	피고의 방어
상표권 소유 그 상표는 famous and distinctive 피고의 사용으로 dilution되었음을 입증	등록 상표의 소유권 상품을 홍보하고 타 제품과 구별할 수 있도록 하는 공정하게 사용(fair use) 비영업적 사용(noncommercial use) 단순 소식(news)을 전하는 정도임을 주장

* **famous trademarks** : trademarks dilution을 입증하기 위해서는 우선 상표권이 유명해야 함

[상표권이 Famous한지 결정하는 8가지 가이드라인]

1) inherrent and acquired distinctiveness 정도
2) 상표의 사용 기간과 범위
3) 상표에 대한 광고, 홍보의 기간 및 범위
4) 상표가 사용된 영업지역에 대한 지리적인 범위
5) 상표가 사용된 제품이나 서비스의 거래 채널
6) 거래에 있어 상표에 대한 인식의 정도
7) 제3자에 의해 동일하거나 유사한 상표가 사용되는 특성 및 정도
8) 상표가 등록되었는지 여부

Ⅶ 기타

○ Dilution by Tarnishment

- 건전하지 않은, 평판이 좋지 않은, 조잡한 제품에 사용하여 상표권을 훼손

○ Dilution by Blurring

- 비슷하지 않은 다른 제품 등에 사용하여 상표권 훼손
  (ex : 금융회사인 피델리티<Fidelity>의 이름을 딴 온라인 의류 쇼핑몰)

○ ACPA(Anticybersquatting Consumer Protection Act)

- 도메인 등록에 관한 사항으로 처음에는 먼저 등록한 자가 서비스를 점유(First Come First Serve)한다는 개념이었으나, 이에 대한 문제점이 제기되어 이를 방지하기 위한 법 (☞ Julia Roberts v. Russell Boyd)

○ Internet Technology and Trademark Infrigement

- 상표권 침해와 관련된 온라인 관련 기술이 deeplinking, metatags, framing 3가지이며, 이들은 보이지 않는 상표권 침해로 연결될 수 있음

  1) deeplinking : Hyperlinking 개념으로 HTML에 URL을 삽입
  2) metatags : HTML에 보이지 않는 embeded code
  3) framing : 웹사이트에서 다른 웹사이트의 내용이 보이도록 하는 웹 기술

○ Paris Convention

- 국가의 산업 재산권을 보호하기 위해 구성된 국가간의 협의체(Union)

○ Madrid Protocol

- 여러 나라에 상표권 등록을 쉽게 하기 위한 프로토콜 (WIPO에 출원하면 각 국에 동시 출원), 한국은 2003년에 가입

IX 사례 분석 (CASE STUDY)

1 "Wal-Mart Store v. Samare Brother" - (Trade Dress)

(개요) Samare은 아이들 옷을 만들어 판매하는 회사인데, Wall-Mart가 이들 옷의 디자인을 기초하여 아이들 옷을 만들어 팔자 Samare가 상표권 침해소송을 제기함

(결과) 법원은 Samare에서 만든 옷의 디자인이나 컬러는 inherently distinctive하지 못하다고 하여 상표권 침해를 인정하지 않았음

2 "Two pesos v. Taco Cabana, Inc. (1992)" - (Trade Dress)

(개요) Two pesos는 텍사스에 있는 인테리어가 특이해서 유명한 레스토랑이었는데 사업을 휴스톤까지 확장하다 보니 휴스톤에 있는 Taco cabana와 인테리어가 비슷한 것을 알고, trade dress로 해석해 달라고 소송을 제기한 사건임

(결과) 법원은 Two Peso의 디자인이 처음부터 특별(Inherently distinctive) 하였고, 2차적 의미(Secondary meaning)를 가진다고 판시한 사례 (Two pesos가 승소)

3 "Checkpoint Systems v. Check Point Software Tech." - (Trademark Infringement)

(개요) Checkpoint Systems은 도난방지 등을 위한 보안장비회사이고, Check Point Software는 이스라엘의 '방화벽' 관련회사인데, Checkpoint Systems이 <checkpoint.com> 도메인을 신청하려 하니 Check Point Software가 이미 등록해 놓은 상태로 도메인 등록위반이라며 소송을 제기

(결과) 이는 위의 **Lapp Factor에 의해 판시한 사건**으로 1) 각 회사의 제품은 경쟁관계에 있지 아니하고, 2) 이미 Check Point Software가 도메인을 등록하고 자기 회사 제품에 3년 이상 사용해다는 점, 3) 각 회사 제품은 고가이고 제품 구입시 전문가가 참여함에 따라 서로 혼동의 가능성이 낮다는 점, 4) 각 회사 제품을 같은 채널에 광고한 사례가 없다는 점, 5) 고객층도 분명히 구분된다는 점 등을 감안하여 원고가 도메인을 돌려받지 못한 사례임

참고로 각 회사의 제품이 융합(converging)된다는 것은 서로 경쟁관계에 있다는 것을 나타내므로 향후 혼동의 여부를 판단할 때 융합에 대한 부분을 고려해야 할 것임

4 "A.B.C. Carpet Co. v. Naeini" - (Trademark Infringement)

(개요) A.B.C. Carpet은 "ABC" 또는 ABC Carpet" 표기를 사용하는 카펫 회사였으며, Naeini는 American Basic cleaning Carpet and Home Restoration이란 회사를 운영하면서 카펫 청소 사업을 해왔고 1998년에 <ABCcarpetandhome.net> 도메인을 등록하였음

(결과) 원고는 피고가 ACPA(Anticybersquatting Consumer Protection Act)를 위반하여 bad faith 목적으로 도메인을 등록했다고 주장하고, 광고비로 매출의 상당부분을 지출했음에도 불구하고 상표가 famous하지 않다는 이유로 원고 주장을 기각한 사례 (상표권 침해에 대한 혼동 여부를 점검하기 위한 기준인 Lapp Factor도 검토함)

5 "Toy 'R' US v. Akkaoui" - (Dilution by tanishment)

원고는 장난감 체인인 Toy "R" Us를 운영하던 중 피고가 성인용품을 팔기 위해 웹사이트 <AdultRUs.com>를 사용하는 것을 알고, 상표권 훼손(Trademark Dilution)으로 인한 가처분 신청을 요청하여 재판부에서 인정된 사례

6 "Toy 'R' US v. Richard Feinburg" - (Dilution by tanishment)

원고는 장난감 체인인 Toy "R" Us를 운영하던 중 피고가 총기류를 팔기위해 웹사이트 <gunsareus.com>를 사용하는 것을 알고 상표권 훼손(Trademark Dilution)으로 인한 가처분 신청을 요청하여 재판부에서 인정된 사례

7 "Harbor. Inc. v. The Internet Entertainment Group" - (Dilution by tanishment)

원고의 유명한 가족 보드게임인 Candyland를 피고가 성인 포르노 웹사이트 도메인으로 사용하여 상표권이 훼손되었다고 주장하였으며 재판부는 원고의 주장을 받아들여 가처분신청(PI)을 인정한 사례

8 "Julia Roberts v. Russell Boyd" - (ACPA, Dillusion by Blurring)

(개요) 줄리아 로버츠는 유명한 영화배우이고 Russell이 <JuliaRoberts.com> 도메인을 소유하고 있고, 다른 여자의 사진으로 웹사이트를 꾸며 놓아서 해당 도메인을 돌려달라고 한 사건임.

(결과) 이는 1) identity or Confusing Similarity, 2) Rights or Legitimate Interest, 3) Bad Faith 관점에서 논의되었는데, 1) "Julia Roberts"라는 Trademark에 <JuliaRoberts.com>라는 도메인은 identical하므로 혼란을 초래할 수 있고, 2) Russell은 그 도메인을 가질 수 있는 권한이나 이익도 없을 뿐만아니라 3) 다른 여러 도메인을 갖고 있는 것으로 보아 선의로 볼 수 없어 Julia Roberts에게 양도하라고 조정한 사례임 (Julia Roberts 승소)

9 "E & J Gallo Winery v. Spider Webs" - (ACPA Problem)

(개요) 원고는 유명한 와인회사로 글로벌 브랜드인 "Ernest & Julio Gallo"라는 상표권을 등록해 놓았으며, 피고인 Spider Webs 회사는 도메인 개발 전문 회사로 여러 가지 도메인을 보유하고 있었는데 그 중 <ernestandjuliogallo.com>이라는 것도 보유

(결과) 재판부는 피고가 도메인 이름을 파는 상업적인 목적으로 도메인을 가지고 있는 것으로 볼 수 있고, 그 도메인을 실제적으로 Active하게 사용하였던 것은 아닌 것으로 보아 피고는 bad faith factor를 가지고 있어 원고의 주장을 인정한 사례

10 "Brookfield Communications, Inc. v. West Coast Entertainmnet Corporation"

(개요) 원고인 BrookField는 연예정보 제공회사로 “Movie Buff"라는 상표를 사용하고 있었으나, 비디오 대여 체인 사업자인 피고가 ”Movie Buff" 상표를 자사의 웹사이트 도메인명과 Metatag로 사용하였다. 이에 원고가 이런 행위는 상표권 침해 및 불공정행위에 해당된다며 소송을 제기

(결과) 법원은 원고가 “Moviebuff" 상표의 선 사용자이므로 피고가 해당 상표를 사용하는 것은 소비자에게 혼동을 줄 수 있고, 이를 Metatag로 등록하는 것도 Lanham Act 하에서 소송의 대상이 된다고 판결하였음

11 "Playboy Enterprise Inc. v. Welles" - Internet Technology (Metatag problem)

(개요) Playboy사의 유명한 Playmate로 일했던 피고인 Wells는 자신의 홈페이지에 Metatag를 이용하여 "playboy"와 “playmate"라는 상표를 게시하여 사용하자 Playboy사가 소송을 제기

(결과) 법원은 피고가 Playboy에서 모델로 일하면서 playmate인 적도 있었기에 피고를 bad faith로 볼 수 없으며, 원고는 그 상표를 피고가 사용하지 못한다는 계약도 제시하지 못하였고, Metatag에서도 사용한 두 상표이외에 원고가 가지고 있는 다른 상표는 사용하지 않았기에 원고의 주장을 받아들이지 않은 사례

12 - 기출문제 ★★★★★

(개요)

CH4.
PATENTS



Ⅰ Business Method Patent - ★★★ 기출 (2007 1학기 기말고사, BM특허 ?)

비즈니스 방법이 컴퓨터 기술과 결합한 것으로 비즈니스에서 행해지는 다양한 영업방식이나 사업 아이디어를 특허로 보호하는 것 (즉, 컴퓨터, 네트워크 등 통신기술과 사업 아이디어가 결합된 영업방법의 발명을 뜻함)

◈ USPTO : United States Patents and Trademark Office, 미국특허청
☞ 특허와 상표권을 관할하는 미국 연방정부 기관

◈ CAFC : 특허전문고등법원

※ 특허관련 판결은 1심은 대법원에서 하고, 2심은 CAFC에서 판결하는 구조임

Ⅱ BM Patent의 조건 - ★★★ 기출 (2007 1학기 기말고사, BM특허에 대해 설명하라 ?)

발명이나 발견(invention or discovery)을 했을 경우, 다음 조건을 만족해야만 특허(patent)로 인정받는다.

1) Novel : 발명이나 발견은 이전에 되지 않았던 것 (☞ 새로운 것, ★ New)
2) Useful : 쓸모가 있어야 함 (☞ ★ practical result가 있어야 함, 예: 하버드 마우스)
3) Non-obvious : 일반적인 기술로 충분히 생각할 수 있는 것이 아니어야 함 (☞ 누가 봐도 뻔한 것은 안된다는 의미, ★ inventive step 필요)

이와 같이 특허(patent)로 보장받기 위해서는 ① **Full Disclosure** (improve, drive 촉진 목적)해야 하며, ② **Operate**(≠invalid)를 만족(알고리즘 만으로는 안되고 실제 구현해야 함)해야 하며, ③ Natural(수학적 알고리즘 등)이 아닌 **Man-made** 한 것이어야 한다.

※ 마음속으로 생각한 절차나 아이디어(purely mental processes or abstract ideas), 자연현상(naturally occurring phenomena), 자연과학 법칙(scientific laws) 등은 특허가 안 됨 (참고로 80년대 들어서는 수학적 알고리즘도 특허로 인정 -> 예: RSA)

Ⅲ 기 타

□ 출원우선주의 (First to File a Patent)

- 미국은 처음에는 발명우선주의(First to Invent), 유럽이나 아시아 등에서는 대부분 출원우선주의(First to File a Patent)를 채택하고 있어, 미국도 2006년부터 출원우선주의로 변경하였다.

□ Doctrin of Equivalent - ★★★★★

- 비슷한 특허가 있는 경우 특허를 또 발행해서는 안 된다.
  ☞ Winas v. Denmead (1854)
  ☞ Fesco Corp v. Shoketsu Kinzoku Kogyo Kabushiki Co (2002)

□ Burden of Proof

- 특허권이 있는 경우 이에 대한 무효나 양도권 소송시 원고는 clear and convincing evidence를 제시해야 함

□ Prosecution History of 'Estoppel (금발언, 말을 바꾸는 것을 금지함)'

- 특허권을 신청한 사람은 최대한 Coverage를 크게 가져가려 하므로 심사관과 Coverage를 줄여가는 과정

□ PCT (Patent Cooperation Treaty)

- 국가에서 특허를 출원하면 WIPO(World Intellectual Property Organization)에 가입되어 있을 경우, 다른 나라보다 1년간 우선권을 가진다. 하지만, 각 나라마다 모두 출원하기 어려우므로 PCT(Patent Cooperation Treaty)를 통해 여러 나라에 국제특허를 출원하는 효과를 얻을 수 있다.

□ Shop Right

- 회사에서 발명한 특허에 대한 사용권은 회사가 가질 수 있다는 것

IV 사례 분석 (CASE STUDY)

1 "State Street Bank & Trust Co. v. Signature Financial Group, Inc. (1998)" - ★★

(개요) 피고인 SFG가 파생상품인 Mutual Fund를 빠르고 정확하게 평가하는 S/W를 개발하여 판매하였다. 이에 원고인 SSB가 피고의 S/W는 단순히 수학적 공식을 코딩한 것이며, 수학공식은 특허 대상이 될 수 없다며 특허 무효(Patent Invalidity) 소송을 제기함. 이에 대해 CAFC에서 원고의 주장을 받아들여 피고의 특허 무효를 결정하자, SFG가 대법원에 상고한 사건임

(결과) 대법원은 피고의 상고를 받아들여 과거와는 달리 현재는 e-Business가 발달하여 수학적 알고리즘(Mathematical Algorithm)이 S/W와 결합되어 1)새롭고(Novel), 2)유용하고(Useful), 3)창의적(Non-obvious) 이라면 특허로 인정된다고 판결함

(의의) 수학적 알고리즘(Mathematical Algorithm)은 특허 대상이 될 수 없으나, 구현된 Algorithm의 결과가 useful(유용하고), concrete(구체적), tangible(유형의 자산) 할 경우에는 특허가 될 수 있다고 판시함으로서 특허의 범위가 확산되는 계기가 된 사례임(예:RSA 알고리즘)

3 "Diamond v. Diehr (1981)" - ★★★

(개요) 고무파동으로 인해 합성고무의 수요가 급증하자, Diehr가 기존의 합성고무 제작방법에 비해 효율성이 높은 S/W를 이용한 자동제어식 합성고무 제작방법을 개발하여 특허를 신청함. 이에 USPTO는 해당 S/W에 적용된 제작공정은 일반적인 기술이며, Computer Program을 이용한 방식은 특허 대상이 될 수 없다고 결정함. 이에 Diehr는 CCPA에 항소한 사건임

(결과) CCPA에서는 특허 출원에 Computer가 포함되어 있는 이유로 특허 대상이 아니라고 할 수 없으며, 해당 S/W를 이용해 매우 유용한 결과(Useful Result)를 가져왔으므로 특허로 인정한다고 판결하였으며, 연방법원(Federal Court)에서도 이를 지지함.

(의의) Computer와 관련된 발명에 대해 특허를 인정한 최초의 판례이며, 이로 인해 특허의 범위가 S/W 분야까지 확대되는 계기가 되었다. 즉, "law of nature, natural phenomena, and abstract ideas"는 특허가 될 수 없다고 하면서 Application이 Useful result를 가져올 때는 특허 대상이 될 수도 있다고 판시 (경제에 미치는 영향을 충분히 고려한 판례)

5 "Marketel International Inc. v. Priceline.com (2001)"

(개요) Priceline이 역경매와 관련한 특허를 출원하자 Marketel이 원래 자기의 것(prior art)라고 특허권 양도소송을 제기함

(결과) 특허는 특허권을 가진 자에게 우선권이 있으므로 Marketel이 분명하게 증거를 제시하지

못하면 인정되지 아니하며, 특허가 되기 위해서는 아이디어 차원이 아닌 S/W를 구현해서 작동할 수 있어야 한다고 하며 Priceline이 S/W를 통해 역경매 방식을 구현하였으므로 특허권을 인정

(의의) 특허권자에게 우선권을 줘 특허권 논란이 생기는 경우, 특허권자가 아닌 자에게 입증책임을 부여하여 'Clear and Convincing evidence'를 제시하도록 한 사례임

6 "Amazon.com v. Barnesandnoble.com (2001)"

(개요) 아마존은 'One-Click Ordering System'이라고 하는 온라인상의 구매방법의 특허를 보유하고 있었으며, BaN도 'Express Lane'이라는 Trademark를 가지고 있었고 이를 광고하고 있었음. 그런데 BaN이 온라인으로 사업을 확장하면서 아마존은 자기가 가지고 있는 특허를 침해했다고 소송을 제기하였으며, BaN은 특허는 1) Novel, 2) Useful, 3) Non-obvious 3가지 요건을 만족할 때, 특허로 인정될 수 있으나, 아마존의 'One-click Ordering System'은 e-Business 시대를 예측하는 과거의 책에서 주문과 관련하여 이미 소개된 아이디어로 1) Novel 항목을 만족하지 못하므로 특허무효(Patent Invalidity)를 주장하였음

(결과) 법원은 Amazon이 BaN에게 가처분금지(Preliminary Injunction)를 할 정도로 필요한 입증자료를 제시하지 못했기 때문에 특허권 침해가 아니라고 판결하였음

(의의) Patent Invalidity에 관하여 논란이 된 사건임

CH5.
Trade Secret



Ⅰ Trade Secret (영업비밀)

영업비밀(Trade Secret, Undisclosed information)이란, 일반적으로 개인 또는 기업이 영업활동을 함에 있어서 경쟁상의 우위를 확보하기 위하여 많은 비용과 인력 및 시간을 투입하여 개발·축적한 비밀정보로서 기술상 정보뿐만 아니라 경영상의 정보도 포함하는 것.

copyright, patent, trademark등은 그 내용을 공개함으로써 지켜주지만 trade secret의 경우에는 공개하지 않음에도 그 존재를 인정받는 부분이다. 법적으로 이 부분에 대해 인정을 받기 위해서는 ★★정책적, 기술적으로 결과적, 합리적인 조치를 하였을 때만 보호★★받을 수 있다. 때문에 보호받기 힘든 면이 있다.

Ⅱ Trade Secret Law (부정경쟁방지 및 영업비밀보호에 관한법률)

1) 영업 비밀의 정의

영업비밀이라 함은 공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서 상당한 노력에 의하여 비밀로 유지된 생산방법·판매방법 기타 영업활동에 유용한 기술상 또는 경영상의 정보를 말한다.

2) 영업 비밀의 요건

① 공연히 알려져 있지 않은 business 관련 정보
② 그 비밀은 생산, 판매, 영업활동에 유용한 기술 및 경영상의 정보
③ 비밀 보유자가 당해 정보의 가치를 유지하기 위한 합리적 노력을 하고 있을 것

Ⅲ EEA(Economic Espionage Act, 산업스파이 방지법) - ★★★★

정보를 훔쳐간 관계자가 국가와 관계되었다고 인정될 때에는 산업스파이로 간주하고 EEA에 의거 불법취득에 대해 가중처벌이 된다. 우리나라의 「첨단산업기술보호법」과 유사한 성격의 제도 (예: 보잉사 기술자인 중국계 미국인 징역 15년형)

Ⅲ Business Practice & Trade Secret

1) 대상 : 폭넓게 적용됨

2) **영업비밀 관리 : Resonable Measure를 취해야 하며, Continuous Effort를 해야 함**

3) 직원의 의무 : 비밀보호 등 신뢰의 의무(fiduciary duty)

4) **Trade Secret Agreements - ★★★★★**

- Non Disclosure Agreements (회사의 동의 없이 임의로 공개하지 않겠음)
- Non Competition Agreements (경쟁업체에 일정기간 취업하지 않겠음)
  ☞ 직업선택의 자유와 충돌될 수 있으므로 균형을 유지할 필요
- Non Solicitation Agreements (경쟁업체의 꼬임에 유인되지 않겠음)
  ☞ 회사를 옮길 때 머리에 기술을 넣어 가는 것도 영업비밀 유출에 해당됨

5) 물리적, 네트워크 보안 관리
  ☞ 핵심인원에 대한 모니터링 등을 할 수 있을 것으로 직원의 프라이버시(privacy) 문제와 충돌될 수 있어 정책적인 관점에서 관리 필요

6) **영업비밀 관련 소송에서의 쟁점**

- Misappropriation (횡령)
  ☞ 부정한 방법으로 영업비밀을 취득하는 것은 합법적이지 못함
  ex) 도둑, 강도, 스파이, 계약 불이행 등
- Breach of Contract (계약위반)
  ☞ 대부분 직원의 employment agreements에 해당
- Inevitable Disclosure (피할수 없는 공개, 예: PepsiCo. Inc. v. Redmond)
  ☞ 대부분 영업 비밀을 다루던 직원의 이직 등으로 이뤄짐

Ⅳ 기 타

□ 분쟁 당사자가 되었을 경우 방어할 수 있는 방법 (역공학)

1) 역공학(Reverse Engineering)

- 부정한 방법으로 영업 비밀을 취득했다고 하면 당사자는 역공학을 통해 취득했다고 할 수 있음. DMCA법에 의하면 미리 소유자의 허가를 받아야 하나 영업비밀의 경우에는 그렇지 아니함

2) 독자개발(Independet Derivation)

- 같은 영업비밀의 경우 각자 개발될 수 있는 성격이 있음. 그러나 이는 기술수준 등을 조사해 보면 다 알 수 있음

IV 사례 분석 (CASE STUDY)

1 "두산중공업 v. STX"

(개요) 두산중공업의 담수관련 기술인 영업비밀을 직원이 STX에 스카웃 되어 이직하면서 관련 기슬을 가져감. 최근 이 소송에서 이직한 부사장은 유죄판결, 징역형을 선고 받음

2 "엔씨소프트의 리니지"

(개요) 엔씨소프트의 리니지 게임개발자들이 단체로 게임 소소를 들고 퇴사하여 게임과 관련되는 다른 회사를 차림. 물론 엔씨소프트는 employmemnt Agreements로 관련 조치를 취하였음. 최근 판결결과 관련자 11명 전원 유죄, 20억의 배상판결

3 "삼성중공업의 드릴선(drillship) 건조에 대한 영업비밀"

(개요) 해당 기술을 유출하려고 하는 기술자가 최근에 잡힘. 만약 이러한 기술이 유출될 경우 피해가 막대하고, 중국 등 다른 나라로 유출될 경우 국가적 손실을 매우 클 것임

4 "PepsiCo. Inc. v. Redmond"

(개요) 펩시에서 제조기술을 담당했던 직원이 케토레이를 만드는 경쟁사로 이직을 하려 하자 이직을 못하도록 소송을 제기하여 승소한 사건

☞ 1) 개인 입장에서 직업선택의 자유도 헌법상의 권리이고, 2) 기업입장에서 재산권도 헌법상의 권리이므로 두가지 측면이 충돌하는 사례임

5 "DVD Copy Control Association v. Bunner"

(개요) Association는 CSS라고 불리우는 DVD의 라이센싱을 관리하는 협회인데 Bunner가 그 CSS의 암호화 시스템을 DeCSS(복호화)하여 이를 인터넷에 게시하여 삭제요청을 한 사건임.

Association는 CSS를 영업비밀로 보호되어야 한다고 하고, Bunner는 표현의 자유를 들어 문제없다고 주장

이 소송에서 보듯 영업비밀과 관련하여 사전적으로 제한(Prior Restraint)하는 것은 어려우나 최근 판결은 회사의 영업비밀을 존중하여 회사편이 이기는 사례가 증가하는 추세임

CH7.
Online Contract



Ⅰ Online Contract

◈ 과거에는 온라인과 오프라인 계약이 명백한 차이가 존재했으나 현재는 없음

◈ 온라인 계약도 **법적 강제성**이 있고 계약 불이행시 손해배상과 집행 가능

◈ 미성년자, 만취 등으로 제정신이 아닌 경우, 장기매매, 마약거래 등의 Agreement들은 Contract로 미 인정

◈ 단, 유언장의 경우 법적인 강제성이 없는 경우도 있음

Ⅱ Requirement of Contract - ★★★★★

1) **Mutual Assent (상호동의)** : 상호간에 알고 동의를 해야 함 (★ Informed Consent ★)

- 홈쇼핑의 금액이 잘못기재되 소비자가 구매한 것은 offer가 아님

2) **Consideration** : 계약을 행할 의지가 있음을 알게 하고자 상호 교환할 가치가 있는 것

- 증인, 계약서, 선불금 등이 없으면 계약이 성립되지 않음

3) **Capacity** : 계약을 할 수 있는 법적인 능력을 갖는 사람들 사이에서 이뤄져야 함

- 미성년자, 중독자, 금치산자 등과의 계약은 무효

4) **Legality** : 불법행위와 관련된 계약은 무효 (도박, 마약거래, 협박, 가격담합 등)

- 가격을 담합해 소비자가 불리한 상황에서 계약이 체결되는 불법적인 상황

5) **Form** : 여러 가지 형태일 수 있으나, 어떤 경우 일정한 형태를 갖추고 있어야 함

- 유언장, 부동산 관련 거래, 1년 이내에 완수할 수 없는 계약, 보증서는 계약, 500$ 이상의 상품거래(서비스는 1,000$)일 경우 반드시 Written Form을 가져야 함

Ⅲ 기 타

□ Sherman Act

- '불법한 제한 및 독점으로부터 거래를 보호하기 위한 법률'의 통칭이다. 8조로 된 간단한 내용의 규정이지만 미국에서의 Anti-Trust Act의 중요한 법원이며, 그 후에 제정된 클레이턴법이나 연방거래위원회법과 함께 각국의 독점금지 규제의 모델이 되었음

□ Doctrin of promissory estoppel (금반언의 법칙)

- 말 or 약속을 뒤집는 것을 금하는 법칙
- 둘 사이에 Consideration이 오가지 않았더라도 reasonable한 이유로 둘 사이의 약속을 믿고 계약을 이행하던 중 상대방이 계약을 파기하려 해서 약속을 신뢰한 자가 피해를 얻는 것이 reasonable하게 되는 경우 금반언의 법칙에 따라 동 약속을 이행해야 함

□ 구두증거 배제의 법칙 (The Parol Evidence Rule)

- Final written contract가 있는 경우 계약서 작성 전이나 작성 중 구두로 계약한 내용은 계약서에 명시되어 있지 않으면 효력이 없음

- 단, 계약서 작성 후 term의 의미를 바꾸지 않는 수준에서 내용에 대해 설명하는 정도로의 수정은 가능

□ Unconscionable Contract

- 소비자가 이해할 수 없는 계약은 무효 (불가피한 선택 앞에서의 계약)
- AOL v. Mendoza 사건

□ Dell's Warranty

- 보장 제외사항 등 중요사항에 대해서 '대문자'로 강조하여 표시
- Unconscionable Contract를 피하기 위한 수단

□ 전자서명 (Electronic Signature)

- 전자로 되어 있는 문서에 법적 효력을 인정해 주는 것
- 특별한 경우를 제외하고는 계약시 동등하게 쓰일 수 있다는 점이 장점
  (예: 생체인식, 디지털 서명 등)
- 예를 들어, 지문을 전자서명으로 쓴다고 하면 지문 자체가 해킹될 수 있으므로 은행들은 자신이 해킹 당한게 아니고 고객이 해킹 당했다는 것을 증명해야함 (이를 위해 보안에 더욱 힘을 쓰게 됨)

□ Software Licensing

- Click-Wrap : 웹에서 '동의버튼'을 Click하는 행위로 계약내용에 동의한다는 것
- Shrink-Wrap : 포장제품을 Open하는 순간 명시된 계약내용에 동의한다는 것
- Browse-Wrap

⇒ 위의 같은 방식은 물리적 동의에 해당되므로 유효한 계약이 된다.

□ Cyber Insurance

- 보험증서(Policy), 보험금(Premium), 생명보험증권(Life Policy)

IV 사례 분석 (CASE STUDY)

1 "Lorraine v. Markel American Ins. Co. (2007)" - ★★★★★

(개요) Lorraine이 소유한 요트가 벼락으로 인해 손상됨. 이 요트는 Online으로 Markel에 보험이 가입되어 있었음. 이에 Lorraine이 Markel에 피해 금액을 청구, 보상을 받아 수리를 함. 며칠 뒤 요트에 손상된 부분을 추가로 발견, 이를 또 청구하자 Markel이 이를 일부 거부함. 이에 Lorraine이 계약의 불이행(Breach of Contract)으로 고소하였고, 피고 측에서는 이메일 등의 전자문서는 그 효력을 발휘할 수 없다고 주장

(결과) 법원은 원고가 주장한 전자문서들은 그 효력을 발휘할 수 없으며, 그 문서들이 효력을 발휘하기 위해서는 원고가 그 문서들에 대한 무결성을 입증해야 한다고 판결함

(의의) 계약법상의 판례를 e-Commerce에 적용시키는 기준이 된 판례이며, 이전에는 계약당사자가 Offline에서 직접만나서 계약서를 작성했지만, 현재는 IT기술의 발달로 인해 e-Contract 환경으로 변화하고 있으므로 기업은 이러한 변화에 대응하기 위해서는 리스크관리 차원에서 접근하는 것이 매우 중요하다는 것을 상기시켜 준다.

참고로, Paul Grimm 판사는 101페이지에 달하는 판결문을 통해 e-mail를 포함한 웹사이트 게시글, 디지털 사진 등 다양한 유형의 전자정보들이 법적 증거로 허용될(Admissible)수 있는 조건들을 조목조목 상세히 적고 있다. 이 판결문은 전자정보들이 일정한 조건을 갖추지 않으면 증거에서 배제될 수 있으며, 전자정보가 위·변조되지 않았다는 원본성(Authenticity)등을 당사자가 직접 증명함으로써 법적 증거로서 인정받을 것을 요구하고 있다.

3 "ProCD, Inc. v. Zeidenberg" - ★★★★★ [기출]

(개요) Zeidenberg가 ProCD의 'SelectPhone™'이란 전화번호와 검색 SW가 담긴 CD를 구매, 이를 이용 자신의 웹사이트에서 유료로 CD의 정보를 판매하였다. 이에 대해 ProCD가 Zeidenberg를 고소한 사건이다.

ProCD의 SelectPhone™의 Term of Use에는 사용자가 사적 이용에 한하여 copy를 허용하고, 양도나 대여, 네트워크에서의 동시사용은 허용하지 않는 내용이 있었고, 이는 manual에 있는 것만이 아니라 S/W 실행시 마다 표시되도록 되어 있었음

Zeidenberg는 1) 돈을 주고 산 것이니 사용 권한은 나에게 있고, 2) CD의 포장에 조그맣게 붙어 있는 Notice(Shrink Wrap license)는 잘 보이지도 않기 때문에 계약이 성립되지 않는다고 주장

(결과) 법원은 Zeidenberg가 S/W를 사용한 것은 Term of Use에 대한 Agreement로 볼 수 있다고

판결하여 ProCD 승소하였음

(의의) 이 판결에 의해 Shrink-Wrap(봉투를 뜯는 것으로 계약이 성립)이 유효한 계약으로 인정됨

CH7.
Privacy



Ⅰ Privacy의 개념

◈ Privacy는 사생활에 대해 간섭받지 않을 권리를 뜻함 (오늘날 보호가 절실한 권리)

☞ The right "to be let alone (1890)" : 다른 사람에 침해받지 않고 홀로 있을 권리

◈ Privacy 개념은 오래전부터 있었지만 정보화사회인 현대에는 개인정보에 대한 통제권(Self-control on personal information)이라는 보다 적극적 개념으로 변모

◈ 이는 Privacy를 침해받지 않을 자유권적 성격 뿐만 아니라 기록된 개인정보가 부당함을 사전에 막기 위해 자신이 정보를 확인하고 정정할 수 있는 청구권적 성격도 갖게 된다는 의미

◈ 이러한 경향은 커뮤니케이션 기술의 발달로 의사소통이 일방향에서 쌍방향으로 바뀐데 기인함

Ⅱ Personal Data의 개념

◈ 개인을 identify 할 수 있는 특정 정보나 물건을 지칭
(다른 어떤 것 보다 우선순위)

◈ 개인정보는 회사의 중요한 자산이므로 사용자의 요구가 있더라도 개인정보를 쉽게 삭제하지 않음

Ⅲ 미국 수정헌법에 나타난 Privacy Right

1) **제9조** : 어떤 권리가 헌법조항에 열거되지 않더라도 거부되거나 무시되어서는 안됨
(Privacy가 헌법에서 보장한 기본 권리임을 명시)

2) **제4조** : 영장에 의하지 아니하고는 압수수색을 할 수 없음

3) **제5조** : 형사사건의 경우 누구든지 자기에게 불리한 증언이나 자백을 강요당하지 아니함

※ 이러한 법들이 초기에는 초상권에 직간접적으로 연관이 있었으나 이후 Privacy 관련 판례가 증가하면서 1974년 Privacy법이 제정되었음

IV Reasonable Expectation of Privacy - ★★★ 기출 (2007 1학기 기말고사)

◈ 미국의 Privacy 보호범위는 기본적으로 "프라이버시에 대한 합리적인 기대"에 의해 설정 (즉, Privacy의 보호범위는 자신이 Privacy를 유지하려는 노력의 합리적인 결과물로 정해짐)

◈ Reasonable Expectation of Privacy의 두가지 개념

1) A person exhibit an actual expectation of privacy
(자신이 프라이버시 보호를 위해 합당한 조치를 취하였는가?)

2) Society recognizes the expectation as reasonable
(사회가 그러한 개개인의 기대를 합당하다고 받아들일 수 있는지?)

◈ 예를 들어, 자신의 목욕탕 창문을 크게 만들어 놓고 다른 사람이 이를 보지 않기를 기대하는 것은 Privacy보호에 대한 합리적 기대가 아니며, 불투명한 작은 창문을 만들어 두었는데, 다른 사람이 고성능 카메라를 사용하여 나체 사진을 찍은 것은 Privacy침해에 해당됨

V Privacy Intrusion에 대한 증명

◈ 적어도 2가지는 성립해야 하고, 3가지 만족해야 성공할 수 있음

① privacy가 침해됐을 때 고의적이여야 한다. (by intend, knowingly)
② privacy가 Expected하고 있는 상황이여야 하고
③ 침해정도가 실질적이고 피해정도가 어느정도인가 파악하는 것도 필요
(우리나라의 대부분은 정신적 피해정도만 언급하는 경향이 있음)

VI SB 1386 (캘리포니아 데이터베이스 보안위반법)

◈ 캘리포니아에서 활동하는 모든 기업은 데이터 침해를 공지해야만 함 (데이터 침해나 정보유출을 고객에게 알림)

◈ 백업데이터에 저장된 고객정보에 문제가 생겨도 법원이 정한데로 공개해야 함

◈ 개인정보를 수집하여 사용하는 경우 합법적 기대에 따른 합리적 조치를 취해야 함

◈ 법안이 Dynamic 하므로(개인정보 보관 DB에 접근이 내부에서 많음) 보안 수준에 대한 적절한 Balance를 통해 SB 1386을 적용

VII Federal Privacy Laws *(Figure 9.1)*

PPA (Privacy Protection Act) (p.268) - ★★★★★

Attoney-Client Privilege, Doctor-Patent Privilege 라는 게 있다. 고객이 변호사나, 의사에게 진솔한 얘기를 해야 하는데 의사나 변호사가 이러한 얘기를 공개하면 윤리 위반이다. 환자도 전염병 등을 얘기해야 하는데, 이러한 것이 공개되면 당연히 얘기안 할 것이고 사회적으로도 손해가 된다.

이러한 것을 막기 위해 수사관이 의사나 변호사 PC를 압수수색할 때 영장에 있는 것만 확보하도록 위원회를 거쳐 영장을 발부하게 하는 법이 만들어졌다. (즉 감청 영장이 대법원장 허락이 있어야 하는 것처럼)

1972년에 캘리포니아 쪽에서 월남전 반대 데모가 많이 일어났는데, 경찰이 스탠포드 대학에서 데모하는 주동자들을 멀리서 사진 찍고 사후에 체크하였으나, 한번은 사진을 못 찍어 경찰이 이 당시 사진을 찍던 스탠포드 대학 학보사를 압수수색하면 사진을 확보할 수 있다고 생각했다. 이 당시 판사가 보수파였는지 경찰에게 압수수색 영장을 발부해주었고 사진을 확보한 경찰은 이를 가지고 기소하였는데 사회적인 문제가 커졌다.

1979년에 National Security v. Freedom of Speech expression의 대결에서

National Security가 우세하여 스탠포드 학보사가 대법원에서 패소하였다. 이 당시 First Amendment 에 의해 판결을 내렸지만 언론사를 압수수색할 때 감청 영장과 같은 걸해야 하게끔 의회가 법을 고치면 법원은 따르겠다고 판결하여 언론사를 보호하기 위한 PPA가 만들어진 계기가 되었다.

이와 같이 이 법은 매우 중요하나, 우리나라에는 아직 제정되지 않았다.

CFAA(The Computer Fraud and Abuse Act, 1986) - p.271

우리나라 정보통신망법의 모태가 되는 법으로 컴퓨터에 권한이 없는 자가 망에 붙어 정보를 빼가거나 장애를 일으켰을 때, 미수행위라도 처벌할 수 있는 법이다.

1986년 컴퓨터라는 용어만 존재할 때 생긴 법인데 지금은 스마트폰 등 다양한 매체가 있음에도 불구하고 법 이름이 바꾸지 않는 것은 “Computer" 라는 이름의 정의를 계속해서 유연하게 변경하기 때문이다. 우리나라도 현재 법명이 나중에 어떻게 쓰일지 모르므로 유연하게 대처할 수 있어야 한다.

GLBA (Gramm-Leach-Bliley Act) - p.272 (시사하는 바가 큰 법이다)

금감원이 생기기전 은행, 증권, 보험감독원이 별도로 있었는데, 자통법에 의해 금융지주가 생겨나면서 은행, 증권, 보험영역이 형식적으로 분리되었지 실질적으로 통합하게 되어 고객정보가 합쳐짐에 따라 생기는 문제점을 미국에서는 GLBA라는 법을 만들어 해결하였다. 즉 금융회사는 고객정보를 지키기 위해 다음과 같은 Measure를 취하라는 것이다.

Reasonable(합리적), Proactive(능동적), Preemptive(선제적)

우리나라 감독규정에는 키보드 해킹, 방화벽 등을 명시하고 있는데 이러한 것들만 하면 되는가?

신기술을 가장 먼저 사용하는 곳이 범죄 집단이다. 따라서 이러한 것을 막기 위해 회사가 선제적으로 대응해야 한다는 것이다.

HIPAA (Health Insurance Portability and Accountability Act) - p.274

1996년 클린턴 정부시절 만들었고 2003년에 시행되었다.
우리나라도 점점 고령화 사회로 접어들어 향후 집에 있는 노인들을 대상으로 원격진료를 개발했지만 의료법이 개정되어야 한다. 원격진료는 불법의료행위로 진료해도 의료수가에 반영되지 않으므로 자선행위 외에는 행하지 않고 있다. 원격진료 후 의료사고가 나면 누가 책임질 것인가?

의사들은 개인병원 차리고 의료사고 터지면 한방에 날라 간다.
향후에 국가적으로 초고속망이 깔리면 원격진료가 활성화 될 수밖에 없다. 우리나라는 의료법이 애매모호한 부분이 많다. 따라서 보험에서 Cover해야 한다.
미국은 애매모호한 것을 없애 사보험으로 처리한다. Covered Entity(보험회사, 앰블런스회사..)가 많다.

10년전 교수가 안식년? 으로 1년 뉴욕에 머물렀다. 보험 1년짜리 가입했는데 부인이 1년이 지나서 2주일 더 묶는 기간 LA에 가자고하여 LA에서 슬롯머신 도중 빈혈인지 음식을 잘 못 먹었는지 쓰러졌다. 앰블런스 부르고 병원에 입원했고 2일후 퇴원했다. 나중에 한국에 와서 진료비가 처음 800$ 나왔는데 알고보니 앨블런스 비용 이었다. 이후 진료의사비 1천불, 병실사용료 등등해서 4천불이 나왔다.

이러한 Covered Entity가 많은데 이러한 회사들끼리 진료행위를 공유할 수 밖에 없다. 하지만 의료정보는 Sensitive information 이다. 예전 영화 필라델피아에서 톰 행크스가 변호사였는데 AIDS병이 알려져 로펌에서 해고 되었고 차별금지법으로 로펌 상대로 소송을 하였다.

일본에서는 개인정보보호법이 엄격해서 교회, 동창회 회원 명부도 일일이 동의를 받아야 한다. 이로 인해 각종 명부들이 사라졌고 조직이 활성화되지 못했다. 일본이 2004년에 법이 만들어졌는데, 이 후 경기침체가 계속되는 것도 이러한 여파가 있지 않나 싶다.

HIPAA는 병원과 보험회사가 가지고 있는 개인 의료정보에 대해 이러한 정보들을 넘겨줄 수 있으나 이에 대한 동의를 어떻게 받아야 되는지를 정의하고 있다.

Ⅷ 기 타

□ Zone of Privacy

- 국가가 사회적 질서유지나 가치관 보호를 위해 일부영역은 관습하여야 하나 국가가 관습하지 못하는 영역이 있다는 것

□ Information Privacy

- Self-Control Power on Personal Data
- 개인정보에 대한 '자기결정권'으로 판단. 즉 개인의 정보를 개인이 알고 동의하는 등의 결정과정을 거쳐야 한다는 것

☞ 동의 철회시는 개인의 모든 정보를 즉시 폐기하여야 함

○ PET (Privacy Enforcing Technology)

익명화 기술, 암호화 기술로 personal data 보호 향상기술로 발전하는 추세

○ 직장 내에서의 Privacy

- 개인 정보유출이 privacy 차원을 넘어서 2차적, 3차적 피해를 유발
- privacy를 주장하려면
  ① privacy를 expected하고 있어야 하고
  ② reasonable해야 한다.

○ Cyber promotion : spamer

- 불법적인게 아니면 표현의 자유에 의한 상업적 speech이기 때문에 일정한 제한은 있지만 보호대상으로 볼 수 있고 거부 의사를 나타낼 경우 받지 않을 수 있다.
- spam의 경우 full protection은 안되고 제한적인 보호만 가능

○ 인터넷 사업자의 고객 개인정보 수집

- 이용약관에 대한 notice가 있고 고객의 동의가 있어야 하고, 이는 반드시 지켜져야 함
- 고객은 내 정보가 제대로 보관되고 있는지 접근할 수 있는 권리가 있는 것지 회원탈퇴시 본인 정보 삭제는 실제 이루어지지 않고 있음 (피해가 크므로 동의를 철회할 수 있는 부분 필요)

○ privacy는 단순히 기술적인 것만으로는 해결이 불가능

- 기술적인 조치 + 법적인/정책적인 조치 + 시장적조치가 함께 되어져야 함

(시장석 조치 : 벌금을 엄청 때리고, 피해비를 왕창 물리고)

IX 사례 분석 (CASE STUDY)

1 "Olmstead v. United States (1928)"

(개요) 밀주업자인 Olmstead가 금주법을 위반한다는 정보를 입수한 FBI가 증거부족으로 영장 발부가 안되자, 사실을 확인, 검거하기 위해 Olmstead의 전화내용을 Tapping을 통해 녹음한 후 현장을 덮쳤으나 실패하자, 녹음내용을 증거로 Olmstead를 기소하였음, 이에 Olmstead는 <Wedcs v. U.S (1910)> 사건의 '위법수집증거배제의 원칙'을 근거로 적법절차를 거치지 않은 증거는 사용될 수 없다며 Privacy 침해를 주장함

(결과) 법원은 당시에는 유선 감청을 Physical Intrusion으로 보지 않고, 청각을 사용하여 대화 내용을 청취한 것은 압수가 아니므로 영장이 없어도 법적 행동이 가능하다고 판결 (Olmstead 폐소)

(당시 : 1928년 에는 도청이 privacy 침해로 인정받지 못하던 시기)

2 "Katz v. United States (1967)" - ★★★★★

(개요) 경마장에서 일하는 Katz가 경마장 말의 컨디션 등 도박과 관련된 정보를 공중전화를 통해 외부에 알렸고, 이 사실을 알게된 FBI가 증거 수집을 위해 공중전화 외부에 도청장치를 설치하여 Katz가 부스 문을 닫고 얘기한 내용을 녹음하고 이를 근거로 Katz를 기소함.

이에 Katz는 전화도청은 영장없는 압수수색과 마찬가지라며 Privacy가 침해되었다고 주장하였고, FBI는 전화도청을 전화부스 밖에서 했으므로 Physical Intrusion이 아니라고 주장함

(결과) 법원은 Katz가 공중전화박스 문을 닫고 있었으므로 이는 Privacy 보호를 기대하는 행위로 도청은 Privacy 침해에 해당한다고 판결함. 또한 미국 수정헌법 4조 "영장에 의하지 않고서는 압수수색을 당할 수 없다."에 의거 영장 없이 도청한 증거는 위법수집증거배제원칙에 의거하여 법적 효력을 가지지 않는다고 판결함

(의의) 유선 감청을 Physical intrusion으로 볼 수 없다는 <Olmstead v. United States (1928)> 사건을 뒤집은 판례이고, 최초로 도청이 Privacy 침해로 인정된 사례임. 이후 **'도청방지법 (Wiretap Act, 1968)'**이 제정되었다.

3 "Griswold v. Connecticut (1965)"

(개요) Connecticut 주에는 의사가 일반인들에게 피임정보를 제공하는 것은 불법이었는데, Connecticut 주의 의사인 Griswold가 기혼 부부들에게 피임방법을 설명하여 주법 위반으로 벌금형을 받게 됨. 이에 Griswold는 이 법에 대해 위헌소송을 제기하였으나 주법원에서 패소하자 연방대법원에 제소한 사건임

(결과) 연방대법원에서는 'Zone of Privacy'에 의거 피임이나 낙태는 개인의 사적 영역으로 이를 국가가 간섭하는 것은 과도하며, 따라서 해당 법규가 적법절차(Due process)에 근거한 Privacy를 침해하였으므로 위헌이라고 판결함

4 "Roe v. United States"

(개요) 미국에서 낙태(Abortion)가 불법으로 지정되어 있으므로 다른 국가에서 낙태한 것에 대해 위반이라고 한 것에 대해 위헌 소송을 제기한 사건

(결과) 판단기준 : 6개월 이상이면 사람으로 보고 낙태를 금지하고, 3개월 까지는 의사의 견해를 적용하여 낙태 가능토록 판결

5 "In v. Vinhee"

(개요) 아맥스카드가 Vinhee에게 대금을 청구하자, Vinhee는 자신은 아맥스카드를 사용한 적이 없고 타인이 자신의 아맥스카드를 조작하여 사용한 것이라고 주장

(결과) 법원은 금융기관은 고객정보 보호를 위해 능동적이고, 합리적이고, 선제적인 조치를 취할 의무가 있으나, 아맥스카드의 CSO는 보안전문가도 아니기 때문에 전문성이 없으므로 적극적인 보안조치를 취했다고 볼 수 없으므로 아맥스카드에 책임이 있다고 판결함 (아맥스 패소)

6 "Doe v. United States (1988)"

(개요) Doe가 조세피난처(스위스, 카브리해)에 Paper Company를 통해 조세피난을 했는데, 검찰이 압수수색을 통해 금고를 찾아낸 후, 수사관이 Doe에게 비밀번호를 물어서 금고 속의 탈세 장부를 가져가서 Doe를 기소함. 이에 Doe는 수사관이 금고의 비밀번호를 강요했다면 소송 제기

(결과) 법원은 수사관이 Doe의 머리 속에 있는 금고번호를 강요했기 때문에 "Fruits of the poison(과실에 대한 독소조항)"에 해당된다고 판결함. Doe 승소.

(의의) 이 사건으로 인해 비밀번호를 요구할 수 없는 계기가 됨

8 "Kyllo v. United States (2001)" - 1990년대 사건으로 2001년에 대법원 최종 판결

(개요) Kyllo가 2층 골방에서 할로겐 램프를 잔뜩 키고 대마초를 피웠다. 이러한 사실이 경찰에 제보로 접수되었는데 신빙성은 있으나, 영장이 없어 집안을 압수수색할 수 없게 되자, 경찰은 열 추적기를 이용하여 스캔 후 영상을 찍고 이를 근거로 영장을 발부 받아 Kyllo 집을 수색하여 증거를 찾아내서 Kyllo를 마약 위반법으로 기소함.

이에 대해 변호인단은 애당초 영장발부가 열을 스캔한 사진인데, Kyllo는 이러한 열 추적기가 있는지 알 수 없었으며, Privacy를 침해하는 신기술이 등장하면 개인이 보호할 수 없으므로 국가가 보호를 강화해주어야 한다고 하였다. 따라서 이러한 Privacy를 침해하는 최신 도구의 사용은 불법이라고 주장하여 이를 법원에서 받아들였다. (Kyllo 승)

8 - 2 "Kyllo v. United States (2001)" - 족보

(개요) Kyllo가 2층 골방에서 할로겐 램프를 잔뜩 키고 대마초를 피웠다. 이러한 사실이 경찰에 제보로 접수되었는데 신빙성은 있으나, 영장이 없어 집안을 압수수색할 수 없게 되자, 경찰은 열 추적기를 이용하여 스캔 후 영상을 찍고 이를 근거로 영장을 발부 받아 Kyllo 집을 수색하여 증거를 찾아내서 Kyllo를 마약 위반법으로 기소함. 이에 Kyllo가 수정헌법 4조에 의거 영장 없는 수색이므로 위법수집증거배제원칙에 위배된다며 소송 제기

(결과) 법원에서는 Kyllo가 방출되는 고강도 전등의 열을 숨기려고 한 적이 없어 Subjective Expectation of Privacy가 없었고, 열 영상 자체가 단순히 열의 유무만 보여줄 뿐 다른 정보가 없으므로 Reasonable Expectation of Privacy가 성립하지 않는다고 판결함

(의의) 신기술을 이용한 수색의 Privacy 침해 문제는 신중하게 다루어야 한다는 것을 의미 즉, 새로운 기술에 대해 사람들이 인지하고 있는 경우 Reasonable Expectation이 있으므로 Privacy 침해가 될 수도 있지만, 그렇지 않은 경우 Privacy 침해가 될 수 없다는 것

9 "Scarfo v. United States (1999)" - 1심판결, 뉴저지주

(개요) FBI가 불법사채, 고리대금업자인 Scarfo에 대해 영장을 발부받아 사무실을 수색하던 중 PC에서 의심되는 파일을 찾았으나 '암호화'가 되어있어 증거를 수집하는데 실패하자, 2번째 영장을 발부 받아 Scarfo의 PC에 KLS(Key Logger System)라는 키보드 해킹 툴을 몰래 설치 후, 일정 시간의 Key-logging 내용을 FBI 서버로 전송 받아 분석하여 해당 파일의 암호를 알아내고 3번째 영장을 발부 받아 해당 파일에서 증거를 찾아내서 Scarfo를 기소함. 이에 Scarfo는 불법 감청을 주장하고, 증거 중지 소송제기

(결과) 법원은 KLS를 사용하는 것은 암호파일 뿐만이 아닌 모든 Data를 기록하는 것으로 세부적인 영장이 필요하나, 두 번째 영장에서 KLS 사용이 명시되었으므로 정당한 수색임이 인정되고, 또한, FBI는 원고가 1968년에 제정된 '도청방지법(Wiretap Act)'에 의거해서 주장하는 불법감청 문제를 방지하기 위해 KLS 프로그램이 실시간 통신에 필요한 통신포트가 닫혀 있는 경우에만 작동되도록 조치하였기 때문에 불법감청을 주장하는 Scarfo의 주장을 기각하였음.

하지만, 키보드해킹이 생소하던 시설이라 FBI의 키보드 해킹 툴 사용이 일반인들에게 사회적 파장을 일으켰고, FBI도 Scarfo에게 유죄를 인정하면 집행유예로 풀려나게끔 해준다고 설득하여 합의로 결론내림.

10 Dennis M. O'connor, et al. v. Magno J. Ortega

① 주립병원 의사인 오르테가가 병원에서 physician 교육을 받던 중 컴퓨터 구매와 관련된 부정과 병원내 여직원에 대한 성희롱 등 관리적 문제로 병원내에서 의심을 받음
② 이에 병원장인 오코너는 오르테가에게 휴가를 주고 오르테가의 책상 등을 뒤져 증거를 획득한 후 고소하였고 오르테가는 privacy 침해를 주장
③ 법원에서는 workplace내에서 고용자가 expectation of privacy가 있더라도 관리나 control을 위해 모든 것이 reasonable한 상황이면 privacy 침해로 볼 수 없다고 판시
(이런 수사가 privacy와 균형을 이루기 위해서는 사내 policy가 필요)

블록체인 모델에 대한 고찰

김혜빈*, 박지선*, 김종규*, 신상욱**

*부경대학교 정보보호학협동과정

**부경대학교 IT융합응용공학과

A Study on Blockchain Model

Hye-Bin Kim*, Ji-Sun Park*, Jong-Kyu Kim*, Sang-Uk Shin**

*Interdisciplinary Program of Information Security, Graduate School, Pukyong National University

**Dept. of IT Convergence and Application Eng., Pukyong National University

요 약

블록체인 기술은 비트코인 프로토콜의 등장과 함께 지금까지 여러 분야에 적용되어 왔다. 하지만 기존의 공개 블록체인의 형태로는 기술의 적용에 한계가 있었고 이는 허가받은 노드만이 네트워크에 참여할 수 있는 사설 블록체인의 등장으로 이어졌다. 본 논문에서는 블록체인 네트워크 접근 및 트랜잭션 읽기 권한 여부, 그리고 트랜잭션 및 합의 과정 참여 권한 유무에 따라 크게 4가지 유형의 블록체인으로 분류하고 특성 및 적용 분야를 분석한다.

I. 서론

블록체인(Blockchain)은 2008년 비트코인(Bitcoin)과 함께 처음 등장한 이후로 이더리움(Ethereum)과 같은 여러 암호화폐의 근간으로 적용되어 왔다. 블록체인 그 자체는 탈 중앙화 분산 데이터베이스이기 때문에, 암호화폐 뿐만 아니라 여러 분야에도 적용될 수 있다[1]. 하지만 분야마다 다른 특징이 있고 블록체인 기술은 그에 맞는 변화가 필요하였다. 기존의 블록체인은 네트워크 내의 모든 노드가 트랜잭션 읽기, 쓰기 과정을 할 수 있다. 이는 비트코인과 이더리움에 적용된 블록체인 방식이다. 하지만 위에 서술한 여러 분야, 예를 들어 기업과 같은 조직에서 민감한 데이터 관리를 위해 블록체인을 도입하는 경우에는 모든 노드들에게 읽기 권한을 부여하는 것은 적합하지 않을 수 있다. 이러한 필요성을 통해 네트워크 내에 신원이 알려져 있고, 따로 선정된 노드들만이 참여할 수 있는 블록체인이 등장하게 되었다. 이를 사설 블록체인(Private Blockchain)이라고 한다. 본 논문에서는 블록체인 네트워크 접근 및 트랜잭션 읽기 권한 여부, 그리고 트랜잭션 및 합의 과정 참여 권한 유무에 따라 크게 4가지 유형의 블록체인으로 분류하고 특성 및 적용 분야를 분석한다.

II. 관련 연구

2.1 블록체인

블록체인은 관리 대상이 되는 트랜잭션 정보를 기록한 분산 장부 데이터베이스이다. 네트워크에 참여하는 각 노드들은 각각 자신의 장부를 가지고 있고, 이 장부의 내용은 합의 알고리즘에 의해 동일하게 유지된다[2]. 블록에 포함시킬 트랜잭션을 생성한 노드는 P2P네트워크에 전달하고, 채굴 노드가 그것들을 모아 블록을

생성한다. 생성된 블록을 시간에 흐름에 따라 사슬(Chain)구조로 연결한 것이 블록체인이다. 각 블록에는 생성 당시의 타임 스탬프(Time Stamp)값과 이전블록의 해시 값이 포함 되어 있다. 따라서 한 블록의 내용이 변경되면 다른 연결된 블록이 잇따라 변경되는 구조이고, 분산 장부의 특성상 모든 노드가 변경의 결과를 열람할 수 있기 때문에 블록을 임의로 변경하거나 누락할 수 없다[3]. 그런 이유로 상대적으로 높은 안전성과 트랜잭션이 모두에게 투명하게 공개되는 장점이 있다.

2.2. 합의 알고리즘

합의 알고리즘(Consensus Algorithm) 은 블록체인의 핵심적인 부분이다. 앞 문단에서 서술했듯이 기본적으로 신뢰관계를 모르는 노드들이 네트워크를 구성하기 때문에, 블록체인에서는 합의 알고리즘을 이용하여, 네트워크에 참여하는 노드들의 신뢰도를 증명하고, 그들끼리 블록에 대한 합의를 시행함으로써 하나의 결과를 도출하며, 기존의 분산 데이터베이스 시스템이 갖고 있던 여러 문제를 해결한다. 비트코인 프로토콜에서 사용된 합의 알고리즘은 작업증명(PoW, Proof-of-Work)으로, 노드들의 컴퓨팅 파워를 이용하여 합의를 도출하는 방식이다[4]. 이 외에도 노드들의 지분을 이용한 지분증명(PoS, Proof-of-Stake)등이 있다. 블록체인에 종류에 따라 적용되는 합의 알고리즘의 방식에서 양상의 차이를 보인다.

III. 공개 블록체인과 사설 블록체인

3.1 기존 공개 블록체인의 한계

기본적으로 블록체인이 여러 장점들을 가지고 있다는 것을 살펴보았지만, 블록체인의 기술적 제약사항에 따라서 단점도 존재하며, 응용분야에 있어서 크게 두 가지 갈등상황에 직면하게 되었다[5].

3.1.1 투명성의 보장 vs 프라이버시 보호

기존 공개 블록체인에서는 네트워크에 참여하는 모든 노드들이 트랜잭션들을 검증하는 방식으로 이중 지불(Double-spending) 문제를 해결한다. 트랜잭션의 내용이 모든 노드에게 투명하게 공개된다는 장점이 있는 반면에, 프라이버시 보호가 되지 않는다는 단점이 있다.

3.1.2 높은 보안성 vs 속도

또한 공개 블록체인은 블록 데이터를 위·변조가 되지 않기 위해 모든 노드들로 하여금 작업증명을 이용하여 nonce값을 찾는 것과 같은 계산 퍼즐을 풀 것을 요구한다. 이는 트랜잭션 데이터를 보호할 수 있지만, 모두가 참여하는 만큼 시간이 많이 걸림에 따라 체인에 블록이 포함되는 속도가 느리다는 단점이 존재한다. 두 가지 관점에 따라 블록체인이 무허가형(Permissionless)과 허가형(permissioned)으로 분류된다.

3.2 사설 블록체인

기존의 투명성의 장점보다는 프라이버시를 보호하기 위한 목적으로 사설 블록체인이 등장하게 되었다. 여기엔 신원이 검증된 노드들만이 참여할 수 있다. 따라서 외부의 해커나 악의적인 노드의 참여는 제한이 된다. 또한, 트랜잭션 내용이 무분별하게 공개되지 않는 점에서 프라이버시 보호가 된다고 볼 수 있다. 그리고 기존의 공개 블록체인이 P2P 네트워크가 특징이었던 점과는 달리 중앙 관리자(Central Autority)를 두어 네트워크의 규칙이나, 트랜잭션의 내용을 수정하거나 잘못된 트랜잭션을 승인하게 된 경우에 개입하여 문제를 해결할 수 있다. 또한, 악의적인 노드들이나 트랜잭션을 추적할 수 있다는 것도 장점이다.

이는 기존의 공개 블록체인이 비트코인이나 이더리움과 같은 암호 화폐에만 적용된 것과는 달리 블록체인의 본질적인 기능인 분산 기록 저장소의 역할을 하거나[6], 트랜잭션 내역이 투명하게 공개되어선 안 되는 금융권이나 의료계에서 사용 될 수 있다.

IV. 블록체인 모델 분류 및 분석

블록체인 네트워크에 대한 접근과 트랜잭션 데이터를 읽을 수 있는 권한여부에 따라 공개

와 사설 유형으로 분류하고, 트랜잭션 데이터를 생성하고, 분산 합의 과정에 참여할 수 있는 지에 따라 무허가형과 허가형 유형으로 분류한다. 권한에 따라 [표 1]과 같이 크게 4가지 종류의 블록체인으로 분류할 수 있다[5].

		네트워크 접근, 트랜잭션 읽기 권한	
		Public	Private
트랜잭션 생성 권한	Permission-less	공개 · 무허가형 블록체인	사설 · 무허가형 블록체인
	Permissioned	공개 · 허가형 블록체인	사설 · 허가형 블록체인

[표 1] 권한에 따른 블록체인 분류

4.1 공개, 무허가형 블록체인

네트워크에 참여하는 모든 노드는 트랜잭션 데이터를 읽고 쓰는 것이 가능하고 그것들을 모아 채굴을 하여 블록을 생성할 수도 있다. 누구나 자신의 의지대로 참여하거나 떠날 수 있고, 대형 네트워크를 유지할 수 있는 것이 장점이다.

해당 블록체인은 신뢰관계가 입증되지 않은 노드들로 이루어져 있기 때문에 최대한 많은 노드가 참여를 해야 안정된 분산 네트워크를 유지할 수 있다. 이렇게 다수의 노드의 참여를 유도하기 위해 블록 채굴에 성공한 노드에게는 내부화폐(Token)로 인센티브(Incentive)를 지급한다. 이 인센티브는 노드들에게 네트워크에 정직하게 참여할 동기 부여 함으로써 전체 시스템을 유지할 수 있다. 따라서 공개 ·무허가형 블록체인 모델을 토큰 기반 마이닝 (Token based with mining) 모델이라고도 볼 수 있다[6]. 이 점을 잘 보여주는 사례가 비트코인이다. 작업증명을 이용하여 nonce값을 제일 먼저 계산한 노드가 블록을 생성하고, 이 블록은 다른 노드들에게 전파(Broadcast)된다. 전달 받은 노드들은 트랜잭션의 유효성을 검사한 다음, 블록이 옳다고 판단되면 채택한다. 채택된 블록을 채굴한 노드는 수수료(Fee)와 보상(Reward)을 비트코인으로 받게 된다. 또 다른 예로는 이더리움, 합의 알고리즘으로는 작업증명과 지분증명이 있다.

4.2 공개 · 허가형 블록체인

어떤 노드라도 네트워크에 참여할 수 있고, 트랜잭션 데이터를 읽을 수 있으나, 데이터를 생성하고 그것들을 모아 채굴하여 블록에 포함시키는 행위는 선정된 노드들만이 할 수 있다. 접근과 읽기는 모든 노드가 가능하지만 쓰기와 합의 과정에는 선정된 노드들만이 참여하기 때문에 공개 · 무허가형 보다는 속도가 빠르다.

이 모델은 4.1절에서 서술한 모델과 같이 내부화폐를 사용하기 때문에, 토큰 기반이라고 할 수 있으나, 선정된 노드들만 합의과정에 참여하기 때문에, 이 과정에서 다수의 노드를 인센티브를 부여하는 방법으로 끌어들일 필요가 없다. 따라서 본 모델은 토큰 기반이긴 하지만 인센티브가 다량의 채굴을 유도하기 위한 것은 아니라는 점에서 마이닝 없는 토큰 기반 모델(Token based Without mining)이라고 할 수 있다[6]. 선정된 대표적인 합의 알고리즘으로 텐더민트(Tendermint)가 있고, 적용된 사례로는 Cosmos가 있다. 텐더민트는 지분증명에서 파생된, 위임형 지분증명(DPoS, Delegated Proof-of-Stake)과 PBFT(Practical Byzantine Fault Tolerance)가 결합된 합의 프로토콜이다[6]. 지분을 기반으로 투표하여 최소 100명에서 최대 300명의 검증자(Validator)만이 합의 과정에 참여한다. 내부 화폐로는 아톰(atom)이라는 지분 토큰이 사용된다[7]. 검증자가 아닌 노드들은 아톰 토큰을 검증자에게 위임하고, 이를 이용해 검증자들은 블록에 대한 투표를 한다[8]. 검증자의 2/3이 동의를 하면, 다음 단계로 진행이 되는데, 이 때 검증자가 이중 투표를 하지 못하게 투표를 한번하면 지분에 대한 lock을 걸어 Nothing-at-stake문제를 해결한다. 그 외에 악의적인 행위가 발각되면, 검증자는 투표권과 위임된 지분 토큰을 잃게 된다.

4.3 사설・무허가형 블록체인

신원이 검증되고 네트워크 내에 알려진 노드들만이 네트워크 접근과 트랜잭션 읽기가 가능하지만, 트랜잭션 데이터를 생성하고 블록에 포함시키는 것에 있어서는 누구나 참여 가능하다. 해당 블록체인 형태는 아직까지는 범주로만 존재한다.

4.4 사설・허가형 블록체인

신뢰할 수 있는 소수의 노드에게만 네트워크의 접근 권한, 트랜잭션 데이터 읽기 권한, 그리고 트랜잭션 생성과 그에 따른 분산 합의 과정에 참여할 수 있는 권한을 부여한다. 분산된 데이터베이스 그 자체를 목표로 하며 주로 금융권에서 사용하는 블록체인에 적용이 된다. 참여하는 노드가 제한 되어있기 때문에 개인 정보의 보호가 이루어지고, 노드들의 권한이 다양한 것이 특징이며, 선정된 노드들만 합의 과정에 참여하기 때문에 속도가 다른 모델들에 비해 빠르다. 네 가지 모델들 중 가장 제약사항이 많다.

네트워크 참여 노드가 중앙 관리자에 의해 제한되는 멤버쉽(Membership)형태의 블록체인이므로, 기존의 퍼블릭 블록체인에서 노드의 많은 참여를 유도하기 위해 사용하였던 내부화폐와 채굴에 성공하면 지급하던 인센티브가 필요하지 않게 되었다. 그래서 해당 블록체인을 토큰이 없는(Token-less) 블록체인 모델 이라고도 볼 수 있다[6]. 예로는 Hyperledger와 R3 Corda, 합의 알고리즘으로 PBFT등이 있다.

하이퍼레저 프로젝트(Hyperledger Project)는 리눅스 재단이 개발한 산업간의 블록체인 기술 발전을 위해 조직된 오픈소스 협업이다. 그 중 패브릭(Fabric)은 금융권 뿐만 아니라, 멤버십이 따로 필요한 비즈니스 관련 분야의 블록체인 어플리케이션이나 솔루션 개발을 위한 블록체인 프레임워크이다[9]. COP라 불리는 권한 관리 모듈을 통하여 참여 노드들의 권한을 관리하고, 내부화폐가 필요하지 않으며, 트랜잭션은 그에 해당하는 암호화 키를 가진 관련 노드만 확인할 수 있다. 합의알고리즘으로는 PBFT가 사용되고, 거래를 관리하는 비즈니스 규칙은 Go언어로 작성된 체인코드(Chaincode)라는 스마트 계약(Smart Contract)을 통해 자동화된다[10].

V. 결론

본 논문에서는 지금까지 접근, 트랜잭션 읽기 권한에 따라 공개 또는 사설 블록체인으로, 트랜잭션 생성과 합의 도출 과정 참여권한에 따라서 허가형, 무허가형으로 구분한 후 이를 종합하여 블록체인을 크게 4가지 유형으로 분류하였다. 언급되었던 분야들 말고도 블록체인은 물류・유통, 교통 상황, 의료 데이터 관리와 같은 분야에서도 적용될 수 있다.

1) 물류・유통

물류・유통 단계에는 여러 집단이 관여를 하고 그만큼 처리 절차도 복잡하다. 이를 공개 블록체인 모델을 이용하게 되면 소비자들에게 투명하게 유통과정이 공개 될 뿐만 아니라. 위・변조의 위험도 적기 때문에 중간 과정에 문제가 생길 시 책임 소재를 명확히 할 수 있다.

2) 의료 데이터 관리

의료 정보는 환자의 보호받아야 할 개인 정보이기 때문에 블록체인 모델을 이용한다면, 접근과 합의 과정 모두 의료 종사자이거나 관련 노드만이 참여할 수 있게끔 해야 한다. 의료 데이터를 블록체인에 등록하면 이전 데이터들을 바탕으로 환자의 정확한 상태를 진단할 수 있고 환자가 병원을 옮길 시에 데이터를 새로 수집할 필요가 없다.

본 연구는 향후 기술이 적용될 여러 분야에 부합하는 블록체인 모델을 선정하는데 있어서 기초가 될 것이다.

Acknowledgement

본 연구는 한국전자통신연구원 연구운영비지원 사업의 일환으로 수행되었음. [18ZH1200, 데이터 안심사회를 위한 트러스트 데이터 커넥톰 핵심 원천 기술 개발]

[참고문헌]

[1] Buterin, Vitalik. "Ethereum white paper." GitHub repository , 2013.

[2] 임종철, 유현경, 곽지영, 김선미, “블록체인과 합의 알고리즘.”, 전자통신동향분석, Vol. 33, No.1, pp. 45-56, 2018.

[3] Dominique Guegan, “Public blockchain versus Private blockchain”, 2017. URL https://halshs.archives-ouvertes.fr/halshs-01524440

[4] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

[5] 다니엘 드레셔. 『블록체인 무엇인가?』.이병욱(역). 이지스퍼블리싱, 2018.

[6] David LEE Kuo Chuen, Robert H. Deng. “Blockchain - From Public to Private”, *Handbook of Blockchain Digital Finance and inclusion* , pp. 145-177, 2017.

[7] Kwon Jae. “Cosmos: A Network of Distributed Ledgers.”, URL https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md, 2016.

[8] Kwon, Jae. Tendermint: Consensus without mining. 2014. URL https://tendermint.com/static/docs/tendermint. pdf.

[9] IBM Blockchain Platform Starter Plan. 2018 .URL https://www.ibm.com/developerworks/cloud/library/cl-ibm-blockchain-101-quick-start-guide-for-developers-bluemix-trs/index.html

[10] Androulaki, Elli, et al. "Hyperledger fabric: a distributed operating system for permissioned blockchains." Proceedings of the Thirteenth EuroSys Conference. ACM, 2018.

P2P 스토리지를 이용한 블록체인 기반의 EHR 관리 시스템

김현우*, 이경현**
*부경대학교 정보보호학협동과정
**부경대학교 IT융합응용공학과

EHR Management System Based on Blockchain Using P2P Storage

Hyunwoo 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

현대인들의 건강관리에 대한 관심과 수요의 증대로 인해 헬스케어 산업에서 효율적인 전자의무기록의 관리하는 것이 대두되고 있다. P2P 스토리지 이용한 블록체인 기반의 EHR 관리시스템을 제안하며, 블록체인을 통해 개인 의료기관 중심에서 발생한 환자의 전자의무기록(EHR)의 파편화를 해결하고 환자중심의 데이터 관리를 가능하게 한다. 또한 P2P 스토리지를 사용시 저장 공간 제공 노드의 참여를 유도하기 인센티브 시스템을 적용하였고 인센티브를 줄 시 기존의 지불방법을 개선하여 지불시 여러 개의 트랜잭션을 생성하는 방법과 다르게 하나의 트랜잭션으로 인센티브를 지급하는 다중 지불 스마트 컨트렉트을 통해 트랜잭션 전송에 발생하는 수수료의 효율성을 증대시켰다. 환자와 P2P노드는 상호간평판을 평가하는 평판관리 스마트 컨트렉트를 통해 측정된 평판이 낮은 개체는 블록체인 네트워크에서 자동적으로 퇴출되는 구조를 통해 정상적인 행위로 참여함을 유도할 수 있다.

I. 서론

블록체인 기술의 발전과 더불어 이를 활용한 다양한 응용서비스가 연구되고 있다. 대표적인 예로는 헬스케어 분야에서 블록체인을 적용하여 환자의 전자의무기록 (EHR, Electronic Health Record) 데이터를 공유하는 의료정보시스템이다.

기존의 의료정보시스템에서 EHR은 환자를 진료한 개별 의료기관 중심으로 관리 되고 있어 개별 의료기관 중심의 의료정보시스템은 환자 EHR 데이터의 파편화를 초래하여 데이터의 활용을 저해하는 요인으로, 이전 의료기관에서 진료 받은 EHR 데이터를 다른 의료기관이 열람하기 힘들어 병원 간 상호운용성을 저해하며 이로 인해 이중검사 등의 추가적인 비용을 발생할 수 있다. 병원 간 상호운용성에 대한 요구는 의료제공자를 비롯하여 의료관련 산업계, 환자들에 의해 끊임없이 제기되었고 블록체인의 등장이 이를 개선시킬 수단으로 많은 연구자들에 의해 연구되어지고 있다[2], [3], [4].

블록체인을 활용한 EHR 공유 시스템을 구축 할 시 EHR 데이터는 환자의 민감한 개인정보이기 때문에 블록체인에 직접 저장하는 On-Chain방식이 아닌 블록체인 외부에 저장하는 Off-Chain방식으로 저장된다[1]. Medrec의 경우 EHR 데이터는 개별 의료기관의 로컬 데

이터베이스에 저장되고 블록체인에 이에 대한 요청값(Query value)이 저장된다[2]. 그러나 이러한 방식은 개별 의료기관마다 환자의 EHR데이터를 나눠 저장함으로 데이터의 파편화를 초래하며 데이터베이스의 관리자의 조작과 실수에 의한 데이터 유실 등에서 자유롭지 않다. 이러한 문제점을 보완하기 위해 EHR 데이터를 클라우드 스토리지에 저장하는 방법이 제안되었다[3]. 그러나 IBM이 2014년 발표한 "IBM Health and Social Programs Summit"에 의하면 인간이 평생 만들어내는 데이터의 크기는 의료데이터가 0.4TB, 유전체 데이터가 6TB, 그 외 스마트폰이나 웨어러블 디바이스에 발생한 데이터는 1100TB이다. 100GB의 데이터를 저장할 경우 매달 발생하는 요금은 클라우드에 저장할 경우 Dropbox기준 $8.25인 반면 P2P기반의 스토리지를 사용할 경우 $2.96으로 비용을 대폭 절감 할 수 있다[6]. MediBloc[5]의 경우 P2P 스토리지를 사용할 계획을 밝혔지만 자체 플랫폼 내에서

본 논문에서는 블록체인을 통해 의료기관간의 상호운용성을 향상시키고 블록체인에 저장할 수 없는 민감 데이터인 EHR 데이터를 P2P 스토리지에 저장함으로써 로컬 데이터베이스와 클라우드 스토리지 및 P2P 스토리지에 저장할 때 발생하는 여러 문제점을 해결하고자 하며 스마트 컨트랙트를 통하여 P2P 노드들에게 인센티브를 지급하며 인센티브를 지급하지 않을 경우 환자의 평판을 관리하는 스마트 컨트랙트를 통하여 사용자가 저장 공간을 제공하는 P2P 노드에 비용을 정당하게 지불하지 않으면 그들에 의해 평판이 낮아져 사용자는 시스템에서 퇴출 된다.

논문의 구성은 2장에서는 P2P 스토리지를 이용한 블록체인 기반의 EHR 관리시스템 아키텍처와 시스템을 제안하고 3장에서는 보안요구사항을 분석하며 4장에서는 결론을 맺는다.

II. 시스템 모델

2.1 개체 역할

제안하는 EHR 공유 시스템의 참여 개체는 아래와 같다.

- 환자 (Patient) : 환자는 본인의 EHR 데이터를 P2P 노드에게 저장하고 필요시 의료서비스 제공자인 의사에게 EHR 데이터를 공유하여 본인의 진료내역을 볼 수 있게 한다. 환자는 공개키, 개인키 쌍 pk_p, sk_p을 가지고 있다.
- 의료 서비스 제공자 (Medical Service Provider, MSN) : 환자에게 의료 서비스를 제공하며, EHR을 생성하여 환자에게 전송하며 필요에 따라 환자에게 EHR 데이터를 요청할 수 있다. MSN는 공개키, 개인키 쌍 pk_M, sk_M을 가지고 있다.
- 블록체인 네트워크 : 공개형 블록체인으로 이더리움 환경과 동일하게 동작한다.
- 저장 공간제공 노드 (Space Node, SN) : P2P 스토리지를 제공하는 노드로써 환자의 편의성과 EHR의 안전한 보관을 위해 모든 SN는 공개키, 개인키 쌍 pk_{SN}, sk_{SN}을 가지고 있다.

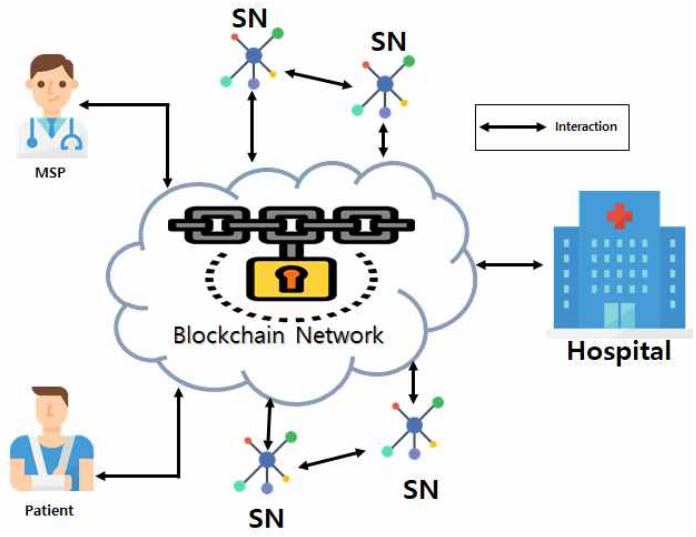


그림 1 시스템 모델

2.2 EHR 저장 및 채굴 과정

환자가 EHR 데이터를 SN에게 저장하는 과정은 아래와 같다.

1. MSN는 환자에게 의료서비스를 제공하고 이를 EHR형태로 생성하여 $DATA_1$을 암호화하여 환자에게 전송한다.

$$DATA_1 = Enc_{pk_p}(EHR)$$

2. 환자는 MSN에게 받은 $DATA_1$를 복호화한다. $Dec_{sk_p}(EHR)$
3. 환자는 복호화한 $DATA_1$을 그림 2와 같이 n개의 데이터로 shard하고 랜덤한 값으로부터 n개 만큼의 Lamport OTP를 생성하여 한 EHR 데이터당 하나의 값을 사용해 shard한 값을 암호화하며 SN의 공개키(pk_{sp})로 암호화하여 $msg_1,\cdots,msg_n$을 전송한다. $msg_n = H(pk_p), shard_n$
4. 환자는 트랜잭션(tx)를 생성하여 블록체인 네트워크에 전파한다.

$tx = locations\ of\ SP, , Lists\ of\ hash\ of\ shards, Sig(sk_p), Hash\ of\ EHR$

5. 각 SN는 본인 스토리지 내에 환자의 공개키의 해시값 $H(pk_p)$을 구하여 각각의 환자의 $shard$된 모든 데이터를 저장한다.
6. SN노드들은 이더리움의 PoW와 동일한 과정을 거쳐 트랜잭션을 새로운 블록으로 블록체인에 추가한다.

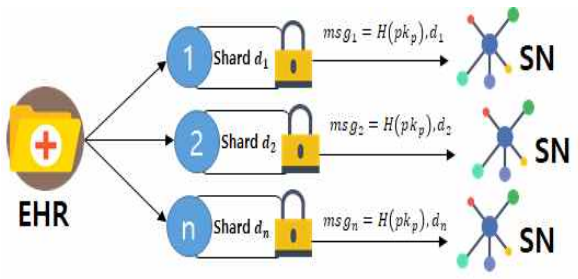


그림 2 n개의 데이터로 shard후 n개의 P2P 노드의 스토리지에 저장 프로세스

2.3 EHR 공유과정

진료받은 EHR 데이터를 다른병원의 MSN에게 제공해야할 경우 shard된 환자의 EHR 데이터를 MSN에게 제공하는 과정은 아래와 같다.

1. 환자는 EHR 데이터를 MSN에게 공유하기 위해 공유해야할 EHR데이터의 해시값을 블록체인에 검색하여 저장된 SN의 위치를 파악하여 해당 SN에게 요청 메시지 req_msg를 전송한다.

$$req_msg = H(pk_p)$$

2. SN는 req_msg의 $H(pk_p)$ 통해 환자를 식별하여 해당 환자의 EHR shard값을 응답 메시지 rep_msg를 통해 환자에게 전송한다.

$$rep_msg = Enc_{pk_p}(shard_n)$$

2.4 인센티브 구조

P2P 스토리지에서는 Peer가 항상 온라인 상태임을 보장하지 못하여 인센티브 지급을 통해 온라인 상태임을 유도한다. 스마트 컨트랙트를 통해 토큰을 지불수단으로 하여 인센티브를 SN에게 지불하게 된다. 이때, 스마트 컨트렉트의 하나의 트랜잭션에서 여러 유저에게 토큰을 다중 지불하는 트랜잭션을 통해 [5]의 접근방법에서 하나의 트랜잭션으로 하나의 SN에게 지불되던 비효율적인 방법을 개선한다. 알고리즘은 다음과 같다.

Algorithm 1 Multiple Payments for incentive

```
function multiplepaytoken(address[] addresses, uint256 _value) onlyowner {
  for (uint i = 0; i < addresses.length; i++)
{        balances[owner] -= _value;
         balances[addresses[i]] += _value;
         Transfer(owner, addresses[i], _value;
}
}
```

2.5 개체 간 평판관리

환자는 SN에게 shard값을 받고 인센티브로 토큰을 주지 않을 환자의 평판을 내리며 SN는 낮은 대역폭을 제공하거나 변조된 shard값을 제공하거나 shard값을 제공하지 않았을 경우 환자는 SN의 평판을 내려 블록체인에 저장되어 낮은 평판값을 가진 개체는 다른 개체가 스마트 컨트렉트를 맺지 않을 것이므로 자동적으로 퇴출 될 수 있다.

III. 보안 요구사항

2장의 모델은 다음과 같은 최소한의 보안요구사항을 만족하여 환자의 EHR데이터의 프라이버시를 보장할 수 있다.

1. Shard한 데이터의 위조 탐지 : SN가 저장

하고 있는 shard값이 위조 되지 않았다는 것을 보장하기 위해서는 블록체인에 저장된 shard의 해시값을 비교하여 같은 해시결과가 나오는지 여부를 비교하여 shard값의 무결성을 보장받을 수 있다.

2. 허가받지 않은 유저의 Shard 값 복호화 하는 행위 방지 : 환자외의 허가받지 않은 유저는 암호화에 사용된 OTP 값을 알 수 없기 때문에 각각의 shard값들을 모아도 복호화 할 수 없다.

3. 악의적인 개체 패널티 : 환자가 SN에게 정상적인 인센티브를 보상하지 않거나 SN가 환자에게 정상적인 서비스를 제공하지 않을 경우 상호 평판 값을 평가하여 낮은 평판 값을 가진 개체는 자동적으로 블록체인 네트워크에서 퇴출되어진다.

IV. 결론

본 논문에서는 P2P 스토리지 이용한 블록체인 기반의 EHR 관리시스템을 제안하였다.

P2P 스토리지에서 노드들이 항상 온라인 상태임을 보장하지 못한다는 문제점이 있어 인센티브 시스템을 사용하지만 기존[4],[6]의 경우와 같이 환자가 정당한 인센티브를 SN에게 지불하지 않는 경우가 존재한다. 이러한 문제점을 보완하기 위해 스마트 컨트랙트를 통해 계약기간 내에 정상적인 서비스를 제공하지 않을 경우의 환자와 SN 개체 간 평판관리 시스템을 통하여 악의적인 행동을 한 개체는 낮은 평판 값을 가져 블록체인 네트워크에서 퇴출되어 어떠한 서비스를 제공하거나 제공받지 못하는 구조를 통해 기존 모델의 보다 SN의 참여 동기를 향상시켰으며 또한 토큰을 활용하여 하나의 트랜잭션으로 여러 P2P 노드들에게 인센티브를 지불하여 트랜잭션 수수료를 감소시켰다.

Acknowledgments

이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2017-0-00156, 블록체인의 정보보호 프레임워크 및 평가 방법 개발)

[참고문헌]

[1] R.J Krawiec., et al., "Blockchain: Opportunities for health care." Proc. NIST Workshop Blockchain Healthcare. 2016.

[2] A. Azaria, et al., “Medrec: Using Blockchain for medical data access and permission management,” Open and Big Data(OBD), International Conference on, IEEE, 2016.

[3] C. ESNosito, et al., “Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?,” IEEE Cloud Computing 5.1, pp. 31-37, 2018.

[4] S. Wilkinson, et al.,. “Metadisk a blockchain-based decentralized file sotrage application,“ Technical Report. 2014.

[5] MediBloc Team, MEDIBLOC WHITEPAPER, v.1.0, Oct, 2017.

[6] S. Wilkinson, “Storj: A Peer-to Peer Cloud Storage Network,”, 2014.

[7] W.S. Ng, et al., "PeerDB: A P2P-based system for distributed data sharing." Data Engineering, 2003. Proceedings. 19th International Conference on. IEEE, 2003.

블록체인을 기반의 안전한 전자투표 시스템에 관한 연구+

노창현, 이임영

순천향대학교 컴퓨터학과

A Study on Secure Electronic Voting System Based on Block Chain

Chang-Hyun Roh, Im-Yeong Lee

Dept of Computer Science and Engineering, Soonchunhyang University

요 약

전자투표(e-Voting)는 선거의 과정들을 모두 전자적으로 변환하여 선거 관리자와 투표자들이 편리하게 온·오프라인으로 선거를 진행하는 시스템이다. 전자투표에는 다양한 암호 알고리즘을 이용하여 안전성을 확보하고, 다양한 보안 요구사항을 보장하여야 한다. 기존의 시스템에서는 암호 알고리즘을 사용하여 보안 요구사항들을 보장하였지만 신뢰를 얻지 못해 널리 사용되지 않고 있다. 이러한 문제를 해결하기 위해 분산원장 기술 중의 하나인 블록체인을 전자투표 시스템에 적용하는 연구들이 계속되고 있다. 블록체인이란 P2P(Peer to Peer) 네트워크에서 모든 노드들이 같은 데이터를 가지는 공공 거래 장부라고 이야기하며, 블록체인에 참여한 모든 노드는 각각의 거래 장부를 비교하여 데이터를 조작할 수 없도록 하고, 새로운 데이터를 추가할 경우 합의 알고리즘을 이용하여 데이터의 위·변조를 막을 수 있는 기술로 주목받고 있다.

본 논문에서는 데이터의 위·변조를 막고 투표자들의 신뢰와 공격자가 데이터를 위·변조 할 수 없는 안전한 전자투표 시스템을 제안한다.

I. 서론

현대 사회에서 정보통신기술이 발달함에 따라 정치의 부분에서도 많은 변화를 거듭하고 있으며, 그 중 민주주의의 개념에서 가장 중요하게 생각 되고 있는 투표도 마찬가지이다. 인간들은 투표를 통하여 투표자 본인의 의사를 표현하는데 사용하고 있고, 이는 작은 모임에서부터 크게는 국가의 대표를 선출하는 대통령선거까지 우리가 생활하는 대부분에 걸쳐 여러 분야에 사용되고 있다. 이러한 투표를 전자적으로 구성하는 것이 전자투표다. 전자투표는 투표를 진행함에 있어 전자적 수단으로 투표행위를 하는 것을 정의할 수 있으며 많은 나라에서 발생하는 저조한 투표율의 향상을 도모하기 위한 대안으로 제시되고 있다. 현재 사용되고 있는 투표 방식은 투표자가 지정된 투표소에서 투표용지에 직접 도장으로 기표하여 진행하는 방식이다. 하지만, 이러한 방식은 투표자에 수를 미리 파악하여 투표용지를 인쇄해야하며, 투표를 진행하기 위한 투표 공간을 확보해야 한다. 또한, 선거를 관리하기 위한 인력들까지 확보해야 한다는 선거 관리상의 문제가 있다. 투표자는 정해진 투표소에서 투표를 위해 시간을 할애하여야 하고, 투표자의 실수로 인한 무효표가 발생할 수 있어 투표자의 의도를 재대로 반영하지 못하는 경우도 발생할 수 있다. 이러한 기존의 투표과정의 문제점들을 해결하기 위해 전자투표 시스템이 연구되고 있다. 전자투표 시스템은 비밀성, 완전성 등의 다양한 요구사항이 보

+ 이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2017-0-00156, 블록체인의 정보보호 프레임워크 및 평가 방법 개발)

장되어야 하며, 이러한 요구사항을 만족하기 위해 많은 연구들이 진행되고 있다. 과거에는 암호학적 기법만을 적용한 전자투표 시스템에 많은 관심을 가졌지만, 최근에는 블록체인을 적용한 전자투표 시스템을 많이 연구하고 있다.

블록체인은 최근 미래를 바꿀 혁신적인 기술로 주목받고 있다. 거래가 발생하는 모든 산업에서 효율성과 경제성을 위한 도입이 전 세계적으로 확산되고 있다. 블록체인이란 분산된 데이터베이스 기술로 말할 수 있으며, 블록체인에 참여한 모든 노드에 데이터를 분산하고 기록하여 보관하는 과정을 가지며, 이런 데이터를 모든 노드가 동기화하여 관리하기 때문에 데이터의 위·변조가 어려워 무결성과 신뢰성을 보장할 수 있는 기술이다[1].

본 논문에서는 블록체인 플랫폼과 암호학적 알고리즘을 이용하여 안전하고 추적 불가능성을 보장하는 전자투표 시스템을 제안한다. 투표 준비 단계에서는 후보자 선정 후 투표를 위한 투표키 쌍을 생성하고 투표의 정책과 투표자들을 설정한다. 그리고 투표자들의 지갑 주소로 토큰을 보내어 투표 준비를 완료한다. 투표 단계에서는 투표자들의 지갑에서 자신이 원하는 후보자를 선택하여 그 데이터를 투표를 위한 공개키로 암호화하고 투표 서버로 토큰을 전송하고, 마지막으로 개표 단계에서는 생성된 블록에서 암호화된 후보자 정보를 복호화하여 계산하고 공표한다.

II. 관련연구

2.1 전자투표

전자투표는 투표의 과정들을 전자적 수단으로 구성하여 투표와 개표가 전자적으로 가능한 기술을 말한다. 전자투표는 투표관리의 생산성 증대와 투표율을 향상시킬 수 있으며, 국내의 부재자 투표문제 해결과 같은 문제들을 해결할 수 있다[2]. 전자투표의 특징으로는 정당하게 이루어진 모든 유효투표를 정확하게 집계하여야 하며, 부정 투표를 차단하여야 하며, 투표권을 가진 사람만이 오직 한 표만을 참여할 수 있도록 해야 한다.

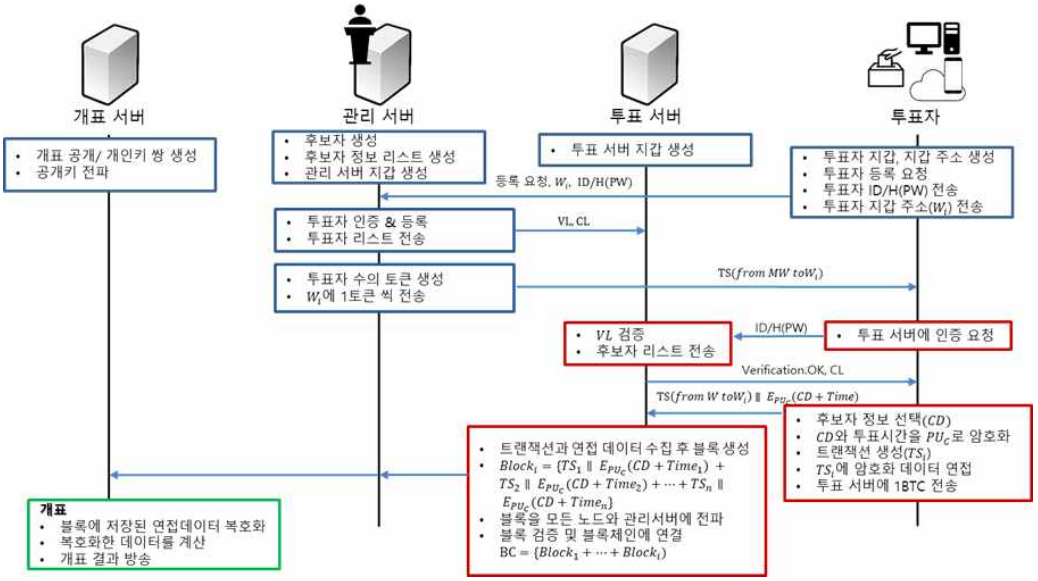
2.1.1 전자투표의 요구사항

전자투표에는 전자투표의 특징을 보장하기 위해 다음과 같은 보안 요구사항을 충족하여야 한다[3].

- 완전성(Completeness) : 모든 정당한 투표는 정확하게 투표 결과에 집계되어야 함
- 건전성(Soundness) : 부정 투표자에 의해 투표가 방해되지 않아야 하며, 투표 결과에 부정 투표가 집계되지 않아야 함
- 비밀성(Privacy) : 모든 투표는 비밀이 보장되어야 하며, 투표자의 투표 내용을 알 수 없어야 함
- 재사용 불가능성(Unreusability) : 투표자는 두 번 이상의 투표를 진행할 수 없음
- 적임성(Eligibility) : 투표는 정당한 투표권자만이 투표를 진행해야 함
- 공정성(Fairness) : 어떠한 일이 있더라도 투표에는 영향이 끼치는 일이 없어야 함
- 검증성(Verifiability) : 투표 결과를 조작할 수 없도록 투표자의 투표내용이 투표결과에 반영되었는지를 검증할 수 있어야 함

2.1.2 전자투표의 문제점

전자투표는 투표 관리자와 투표자 모두에게 많은 편리성과 비용을 절감할 수 있는 효과를 제공하지만, 실제로 전자투표 시스템을 적용한 나라는 많지 않다. 그 이유로는 1) 신원확인 절차를 거쳐 투표자를 등록해야 하며, 2) 투표를 진행함에 있어서 보안의 문제가 있으며, 3) 투표 결과에 대한 검증을 보장하는 신뢰성에 대한 문제가 있다. 이러한 문제를 해결하기 위해 많은 연구들이 진행되었으며, 안전성 기반 기술들을 사용하여 전자투표 시스템을 구현하려 했다. 또한, 최근에는 블록체인을 적용하여 투표 데이터에 대한 무결성을 제공하고, 누구나 투표 결과를 검증할 수 있어 신뢰성을 제공하는 블록체인 기술을 적용하는 연구가 계속되고 있다.



(그림 1) 제안방식의 전체 시나리오

<표 1> 블록체인의 종류별 특징 및 사례

구분	개념 및 특징	사례
Public	블록체인을 최초로 사용한 플랫폼 누구나 접속 가능 거래 속도가 느림	Bitcoin Ethereum DASS
Private	개인형 블록체인 하나의 노드가 블록체인을 관리 선정된 노드만이 접속할 수 있음	Nasdaq 등
Consortium	반 중앙형 블록체인 선정된 노드만이 접속할 수 있음 확장성과 거래 속도가 장점	R3 CEV, HSBC 등

2.2 블록체인

블록체인은 분산 원장 기술 중의 하나로써 블록체인에 참여하는 모든 노드가 같은 데이터를 가지기 때문에 데이터에 대한 무결성을 보장하고 데이터를 쉽게 위·변조하기 어렵다는 장점을 가진다[4]. 블록체인은 Public, Private, Consortium의 환경으로 나뉘며 자세한 내용은 <표 1>과 같다.

Public 블록체인은 주로 암호화폐의 기능을 하는 플랫폼에서 많이 사용하고 있으며, Private 블록체인은 분산 원장 기술을 중점적으로 활용하는 플랫폼인 Linux 재단의 Hyper Ledger에서 주로 사용하고 있다. Consortium 블록체인은 노드를 하나의 기관이나 회사로 구성하여 공동으로 블록체인을 운영하며 R3 CEV나 HSBC 등이 많이 사용하고 있다. 블록체인은 계속해서 다양한 분야와 환경에 적용하기 위한 연구들이 계속해서 진행되고 있으며, 전자투표에 관한 연구들도 계속해서 증가하고 있다.

III. 제안방식

본 장에서는 토큰을 이용한 블록체인을 전자투표에 적용한 시스템을 제안한다. 구성 요소로는 관리 서버, 투표 서버, 투표자, 개표 서버로 구성되며, 전체 시나리오는 선거 등록단계, 투표단계, 개표단계로 구성된다(그림 1).

3.1 선거 등록단계

선거 등록단계에서는 먼저 개표 서버의 공개·개인키 쌍을 생성하고 공개키를 전파한다. 투표 서버는 투표 서버의 지갑을 생성한다. 관리 서버에서 투표를 설정한다. 관리서버는 후보자들을 생성하고, 후보자 정보 리스트를 생성한다. 그 후 관리 서버의 지갑을 생성한다. 그 후, 투

표자는 투표자의 지갑을 생성하고, 관리 서버에 투표자 등록 요청 메시지와 ID, 해시화한 PW를 전송한다. 관리 서버에서는 투표자를 인증하고 등록하며, 투표자 리스트가 완성되면 투표 서버로 전송한다. 다시 관리 서버는 투표자 수만큼 토큰을 생성하고 투표자들의 지갑 주소로 1 토큰씩 전송한다.

3.2 투표단계

투표 단계에서는 미리 등록한 투표자만이 투표를 진행할 수 있도록 하였고, 투표 서버와 투표자 간의 통신을 통해 투표를 진행한다. 투표자는 정해진 시간에 투표 서버에 인증 요청을 보낸다. 인증 요청을 받은 투표 서버에서는 투표자가 보낸 정보 값으로 검증을 진행하고 후보자 리스트를 준비 한다. 그 후, 인증 완료 메시지와 후보자 리스트를 전송하여 투표자에게 보여주고, 투표자는 후보자를 선택하여 후보자 정보를 생성한다. 후보자 정보는 투표 시간과 함께 개표 서버의 공개키로 암호화하고, 토큰을 보내는 트랜잭션과 연접하여 투표 서버로 전송한다. 투표 서버에서는 전송받은 트랜잭션과 연접 데이터들을 수집하여 블록을 생성하며, 생성한 블록은 모든 투표 서버에게 전파하여 검증을 진행하고, 모든 블록체인에 연결되게 된다. 블록체인에 연결되게 되면, 투표단계는 종료된다.

3.3 개표단계

개표단계는 개표 서버에서 진행한다. 개표 서버는 투표가 종료되었을 때에 투표 서버에 블록을 요청한다. 투표 서버는 요청에 따라 블록 전체를 개표 서버에 전송하게 되고, 개표 서버는 블록에 저장된 암호화된 연접 데이터를 복호화하여 개표를 진행한다. 그 후 개표의 내용을 공표함으로써 개표가 종료된다.

IV. 보안요구사항분석

- 완전성(Completeness) : 블록체인에 저장된 투표는 모두 결과에 집계됨
- 건전성(Soundness) : 1 Token 으로 진행되는 투표 방식이라 부정 투표가 불가능함
- 비밀성(Privacy) : 투표된 후보자의 정보를 암호화하여 진행하기에 보장 됨
- 재사용 불가능성(Unreusability) : 1 Token 으로 진행되는 투표 방식이라 재사용 할 수 없음
- 적임성(Eligibility) : 인증과 토큰을 통한 정당한 투표권자 인식 가능
- 공정성(Fairness) : 블록체인으로 투표 데이터를 저장하여 단일지점 공격방식을 차단함
- 검증성(Verifiability) : 누구든지 블록체인의 데이터를 이용하여 검증 가능함

V. 결론

본 논문에서는 토큰을 이용하는 블록체인 플랫폼에 전자투표를 적용하는 방법을 제안하였다. 전자투표의 요구사항에 따라 보안 요구사항을 만족하면서 기존의 투표 시스템에서의 중앙화된 시스템을 탈피하였다. 향후 구체화된 블록체인 플랫폼에 적용하여 실제 구현을 진행함으로써 실생활에 확장될 수 있는 연구가 필요할 것으로 생각된다.

[참고문헌]

[1] 이루다, “블록체인을 활용한 전자투표 시스템 구축”, 상명대학교 대학원, 2017

[2] 정진우, “전자투표의 효과와 문제점에 관한 탐색적 연구”, 서울대학교 행정대학원, 2003

[3] 허원근, 김희선, 김광조 “전자선거 프로토콜의 요구사항 연구”, 정보보호학회지, 2000.

[4] S. Nakamoto. “Bitcoin : A Peer-to-peer Electronic Cash System” bitcoin.org, 2009.Electronic Cash System” bitcoin.org, 2009.

A Blockchain Based On Data Provenance in Healthcare Domain

Kweka Bruno Joachim*, Kyung-Hyune Rhee**

*Interdisciplinary Program of Information Security, Graduate School,
Pukyong National University.

**Department of IT Convergence and Application Engineering
Pukyong National University

Abstract

For clarity of any sort of errors occurred in the data, how data is being transformed from one point of the system to another, it required to maintain a sort of data provenance which map the data origin from where it comes from, who participate and what they performed. In case of healthcare system whereby heterogeneous of systems are involving in processing the data can be tricky and complex hence lead to faults in reading diagnosis, fraud of results and hardship to tracking patient's treatment history that can lead to poor decision making in the process. Therefore, to overcome the above challenges we propose the model of data provenance that utilize blockchain and we introduced the blockchain for enhancement of data provenance operation. Such as any file access or operation user performed will be captured and send to the blockchain and becomes unaltered and creates the tamper of proof timestamps that help in conducting a validation in case of any fraud or misdiagnoses. The reason of using blockchain in this model it works on decentralized environment no third party is involved.

I. INTRODUCTION

Many fields that use computerized system, Data is very important however due to the massive existence of the complex structure of the system that interlinked together makes difficult to have a confidence in the quality and timeliness of the data that a user is working with. For instance in healthcare applications data can be distributed among diversified and self-reliant information systems. Different hospitals, departments within and other practitioners they formed a complex information system that resulted into chaos of making a decision as well tracing the document's validity. Numerous of incidence had occurred because of not carefully observed the data origin, who is the owner and what modifications undergo in the data. For example during experimental trials unethical doctors may tempt to falsify the diagnosis [1]. With this kind of mistakes sometimes hinders patient treatment because of patient's history and other details had been tampered and there is no way out to solve and make a decision.

To avoid such kinds of data fraud in the environment that a data can be manipulated, the data provenance has to be introduced and maintained. Data provenance is the process of trailing and recording the origin of data and

its movement across different systems [2]. Maintaining the data provenance will help to answer doubtful documents and fastening the decision making toward a certain issue. Therefore, integrating this method into healthcare unit it helps users to trace and inform how particular results was reached. Such system that maintain this data provenance helps to examine distributed healthcare service's performance and audit given procedure whether it follow the correct procedures without a problem.

The main challenges of any information system that wants to adopt data provenance model are collection, changeless storage of provenance data, verifiability and guarantee of the privacy[3]. Above are the most challenges that needs to be tackled and be able to have a pure provenance data. Some researchers had suggested the methods of integrating provenance awareness system into the healthcare unit [4]. However most of the infrastructure are in centralized governance still makes easy to tamper with the data due to the preserve of authority that governing the system from top to bottom and existence of centralized database that attract attackers to conduct malicious activities. Hence, makes easy to demeanor any data modifications and accelerating other fraud.

In this paper we present the model of data provenance based on blockchain technology which emphasis on data immutability, guarantee tamper of proof and works on decentralize nature with no third part authority control the whole system as well as with its usage of cryptographic mechanism (hash function) for preserving the privacy.

II. BACKGROUND AND RELATED WORK

This section we describe some of related work in data provenance and also provide Blockchain background

2.1 Data Provenance

The state of art so called data provenance it plays huge role in various fields concerning with knowing the data origin. For instance, in cloud computing area where heterogeneous of information are shared among other systems. There are numerous of research had been done in utilizing data provenance in a diverse sector [5]. However, the new technology Blockchain offer different strategy on handling data provenance as many of proposed system work are in centralized which can be easy to be manipulated while in blockchain does not allow. Apart from that in this paper we propose use of blockchain in data provenance for the healthcare because it is impossible to change documents once it is submitted (tamper of proof evidence) since its database shared among peer any changes will be detected and it is difficult to forge. Hence, creation of logs or reports will be easy and with integrity as well as conducting auditing. This proposed work motivated by the existing proposal using blockchain in data provenance [6,7].

2.2 Blockchain

Currently the blockchain is the one of the hot issue attracted by many researchers and other stakeholder for instance in government, finance, and healthcare sector. With its unique features that enable to function in any environment seems to be untrusted. Also, to perform an attack in blockchain environment require to control a huge computational power that will control the majority of nodes who are honest which in practical is impossible. Furthermore, the blockchain it is supervised and maintained by the miners who are involving in validation of transactions and

creation of blocks. They receive incentive by solving the cryptography puzzle. And identification of users depends on public and private address. Therefore, the credentials in blockchain is tough compare to traditional one (username & password).

Until now there are a lot of big platforms such as Ethereum, Hyperledger offer their services using blockchain. And many decentralized applications are being developing. Several decentralized application offer number of service from enterprises level and it depends on organizational needs. For example Storj[8] use blockchain to provide a service of storage. Tierion [9] use blockchain to records any data or business flow of transaction in the blockchain and it offers variety of API to the clients and have many advantages toward capturing business processes.

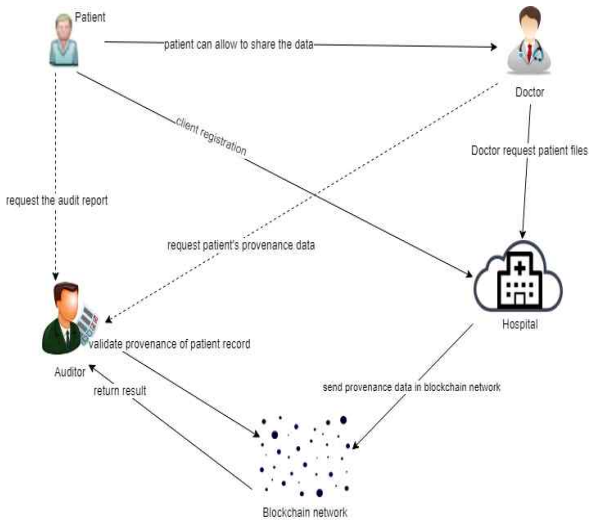


Figure 1. System overview

III. SYSTEM ARCHITECTURE

The proposed architecture is based on blockchain with capability to audit data operations in hospital and the blockchain network used is the private network not a public therefore only allowed participants will be able to see all transactions. The proposed system achieves the following objectives. **Immutability of data**: when the client sends a data, the provenance system will capture the intended information and sends to the blockchain network where it will broadcast to all peers. A nature of blockchain is all participants who have been allowed they will see the data. The proposed system creates the timestamped log for all users operations that they perform in the data without involving the third party in case of tamper of evidence will be easy to detect. **Privacy Preservation** User ID is hashed to guarantee the privacy. When the broadcast of the data provenance records onto the blockchain network neither any nodes will learn the user identity nor auditor will not be able to identify the record owner.

The proposed architecture (Fig 1) works in this manner, first the patient has to be registered in the hospital cloud storage. The doctors will request the patient's files concerning diagnosis reports or any patient information. For the doctor to access the patient files he needs to obtain a permission from data owner(patient). Therefore, keys exchange must take place to allow data sharing between participants. An auditor main task is to confirm the transactions and give back the feedback requested by the participants. For instance, if doctor wants to get more details about diagnosis of a patient, he will request an auditor to give the patient data provenance record. Patient case can also do the same. blockchain network the provenance records are captured and send them into the blokchain. Per block multiple of data operations can be stored. The most important record is file access operation such as create, deletion, share, change and apart from that we capture username and filename, location, type of file. Blockchain we do not store the file since it is expensive to store the files in the

blockchain.

For auditor to get the results he will use blockchain receipt (transaction id) as an identifier used to locate the anchored data in the blockchain. In case of any tamper of evidence the auditor can confirm by using the blockchain receipt. And any data stored in the blockchain it becomes immutable.

The below table represent the structure of data provenance. Provenance records may include other fields but not limited to the mentioned below.

ID	Timestamp	Userid	Details operation				Block-hash	Validate
002	25-10-2000	YYY	Filename	Description	Location	Action	n-bits	True
003	27-10-2000	zzz	B	Blood test	Busan	create	n-bits	True
004	29-10-2000	ggg	C	Patient check	Ulsan	share	n-bits	True

Table1: structure of data provenance

3.1 Data validation

The records that are published in the blockchain, the auditor can confirm those records by using blockchain receipt using Tierion API. Because the blockchain receipt have the detailed information of the transaction and Merkle proof for validation of the transaction.

IV. SUMMARY

We summarize the proposed model as follows:

•For any file operating and any access to the data, we captured them and send to the blockchain. By doing so, we create an unchangeable record with secured and permanent as well as tamperproof ime stamp. Any modification, blockchain will detect it by validating the transaction receipt.

•The privacy and security is achieved by hashing the user id.

•By integrating the blockchain in this modal, it creates the trustfulness environment by neglecting the third party. Furthermore, to attack blockchain network is very difficult and expensive compare to centralized system which are vulnerable to several attacks such as DDos attack.

V. CONCLUSION

In this work we explored data provenance with the primary focus on the health care domain. Which we developed the model of data provenance based on blockchain for auditing, generate reports and as well as guarantee the privacy to all actors(patients) in the model. We also see how blockchain integration can enhance data integrity in and provide the trustiness environment because of its immutability nature can create the tamper of proof logs.

Acknowledgment

This research was supported by the MSIT(Ministry of Science, ICT),Korea, under the ITRC(Information Technology Research Center) support program (IITP-2018-2015-0-00403)supervised by the IITP(Institute for Information &communications Technology Promotion)

References

[1] George, S. L., &Buyse, M. (2015). Data fraud in clinical trials. Clinical investigation, 5(2), 161.

[2]Ram, S., &Liu, J. (2006, November). Understanding the semantics of data provenance to support active conceptual modeling. In International Workshop on Active Conceptual Modeling of Learning (pp. 17-29). Springer, Berlin, Heidelberg.

[3]Asghar, M. R., Ion, M., Russello, G., &Crispo, B. (2012). Securing data provenance in the cloud. In Open problems in network security (pp. 145-160). Springer, Berlin, Heidelberg.

[4]Kifor, T., Varga, L. Z., Vazquez-Salceda, J., Alvarez, S., Willmott, S., Miles, S., & Moreau, L. (2006). Provenance in agent-mediated healthcare systems. IEEE Intelligent Systems, 21(6), 38-46.

[5]Álvarez, S., Vázquez-Salceda, J., Kifor, T., Varga, L. Z., & Willmott, S. (2006, May). Applying provenance in distributed organ transplant management. In International Provenance and Annotation Workshop (pp. 28-36). Springer, Berlin, Heidelberg.

[6]Peterson, K., Deeduvanu, R., Kanjamala, P., & Boles, K. (2016). A blockchain-based approach to health information exchange networks. In Proc. NIST Workshop Blockchain Healthcare (Vol. 1, pp. 1-10).

[7]Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data. In Proceedings of IEEE Open & Big Data Conference (Vol. 13, p. 13).

[8] Visit https://storj.io/

[9] isit https://tierion.com

2018 한국정보보호학회 하계학술대회

B2 네트워크 2

김 광 조 (카이스트)

- **5G HetNet 환경을 지원하기 위한 MIH(Media Independent Handover) 기반의 고속의 안전한 핸드오버 인증기법 연구**
  김지윤, 권순현, 유일선
- **OAuth 2.0 인증 프로토콜의 취약점에 대한 대응방안 제시**
  서동화, 윤가헌, 오장욱, 서정택
- **1Kbps 미만 무선 통신 센서 네트워크에서의 개체 인증 및 키 관리**
  김현기, 이옥연
- **CAN 내부 취약점에 대한 분석 및 신규 대응방안 연구**
  김장훈, 한경수, 최홍석, 서정택
- **데이터 플레인 가속화 기술을 안전하게 적용하기 위한 상용 IPsec 분석**
  최준태, 류승호, 박승윤, 사미 울라, 오희국

5G HetNet 환경을 지원하기 위한 MIH(Media Independent Handover) 기반의 고속의 안전한 핸드오버 인증기법 연구

김지윤, 권순현, 유일선*

*순천향대학교 정보보호학과

Study on Fast and Secure Handover Authentication Scheme based on MIH(Media Independent Handover) for 5G HetNet Environment

Jiyoon Kim, Soonhyun Kwon, Ilsun You*

*Department of Information Security Engineering, Soonchunhyang University.

요 약

오늘날 이종의 유/무선 액세스 네트워크 환경에서 안정적인 네트워크 제공을 위하여 MIH가 개발되었다. 이는 이종간 핸드오버를 지원하며 IEEE 802.21a-2012™ 문서를 통해 보안과 사전 인증 서비스를 제공한다. MIH는 그 특성 상 다양한 이종의 액세스 네트워크에서 잦은 핸드오버가 일어나는 5G HetNet 구조에 적합하며, 본 논문에서는 5G HetNet 환경을 지원하기 위한 MIH 기반의 고속의 안전한 핸드오버 인증기법에 대하여 연구하였다.

I. 서론

오늘날 정보통신 기술의 발달을 통해 사용자들은 다양한 기기를 통해 인터넷에 접속하여 수많은 정보를 제공받을 수 있다. 또한, 인터넷 액세스 패러다임이 변화하면서, WiMAX[1], Wi-Fi[2], 3GPP UMTS/LTE/LTE-A[3-5]와 같은 다양한 유/무선 액세스 네트워크 환경들이 개발되었다. 이에 따라, 이종의 유/무선 액세스 네트워크 환경에서 안정적인 네트워크를 제공하기 위해 IEEE[6]는 IEEE 802.21 문서를 통해 특정 액세스 네트워크에 의존하지 않는 효율적인 이동성 관리와 핸드오버를 지원하는 MIH(Media Independent Handover)의 표준을 제공하였다[7-9].

본 논문은 다음과 같이 구성된다. 2장에서는 MIH(Media Independent Handover)에 대하여 분석하고, 3장에서는 MIH의 보안에 대한 문서인 IEEE 802.21a-2012에 대하여 분석한다. 마지막으로 4장에서 결론을 맺는다.

II. MIH(Media Independent Handover)

2.1 MIH 개요

MIH(Media Independent Handover)는 IEEE 802.21 문서를 통해 제안된 네트워크 환경에 독립적인 핸드오버 기술로서 이종의 액세스 네트워크를 동시에 활용하는 환경에 적합하다.

MIH는 링크계층과 네트워크 계층 사이에 존재하며, MIH에서 사용되는 엔터티로는 스마트폰과 같은 이동노드(MN: Mobile Node), 이동성 관리 프로토콜인 MIH 사용자(MIH User), 그리고 네트워크(Ethernet, WLAN, 3GPP 등)로 구성된다.

IEEE 802.21 표준에서는 MIHF(Media Independent Handover Function)가 제공하는 서비스를 3가지로 분류하여 정의하였다.

- 이벤트 서비스 : 하위 계층(매체 접근 제어 계층, 물리 계층)의 핸드오버, 연결 설정 및 해제와 같은 상태 변화, 링크 파라미터 변경 등과

같은 정보를 제공함.

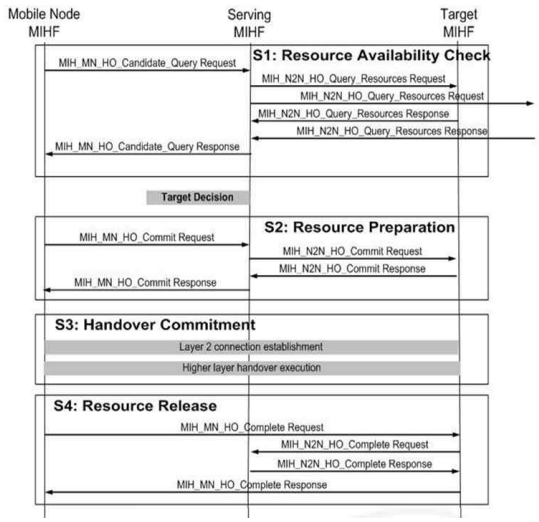
- 커맨드 서비스 : 상위 계층부터 하위 계층까지의 명령을 제공하며, 링크 상태를 변경하거나 다중 모드 단말을 조정함.

- 정보 서비스 : MIHF 사용자들에게 네트워크와 관련된 정보를 제공하고, 네트워크를 발견하고 선택할 때에 필수적인 요소임.

MIH 프로토콜에서 MIH PoS(Point of Service)는 무선랜의 AP(Access Point) 또는 WiMAX의 BS(Base Station)과 같은 2계층의 연결접속장치인 PoA(Point of Attachment)에 위치하거나 3계층의 네트워크 접속 장치인 IP 라우터나 별도의 원격 네트워크 서버에 위치한다.

MIH PoS가 PoA에 위치할 경우, 이동노드와 MIH PoS간의 통신은 2계층 프레임을 통해 이루어지며, 이외에는 통상 3계층 이상의 IP 상위계층 프로토콜을 활용함.

MIH 핸드오버는 [그림 1]과 같으며 크게 4단계로 나눌 수 있다.



[그림 1] MIH 핸드오버 절차

2.2 IEEE 802.21a-2012™

2.1의 IEEE 802.21의 MIH는 이종의 액세스 네트워크 환경에서 이동노드의 핸드오버를 지원하기 위한 기법이며 보안에 대하여 고려하지 않았다. 이를 보완하기 위해 IEEE에서는 IEEE 802.21a-2012 문서를 제안하였다.

IEEE 802.21a-2012 문서에서는 MIH 서비스를 보호하기 위해 제안되었으며 MIH 서비스 보안과 사전인증을 포함한다.

2.3 MIH 서비스 보안

MIH 서비스를 보호하기 위해서는 필수적으로 이동노드와 접속 네트워크의 PoS 사이에 상호 인증 및 키 교환이 제공되어야 한다. IEEE 802.21a-2012는 TLS(Transport Layer Security)[10], EAP(Extensible Authentication Protocol)[11], 그리고 ERP(EAP Re-authentication Protocol)[12] 기반의 솔루션을 소개하였다.

- TLS 기반의 솔루션(UDP의 경우 DTLS를 적용할 수 있음)은 이동노드가 공개키 방식의 암호화를 지원할 수 있고, 인증서를 갖고 있다면 TLS의 상호인증 옵션을 통해 인증과 키 교환을 제공할 수 있음.

- EAP 기반의 솔루션은 이동노드가 AAA(Authentication Authorization Accounting) 도메인에 소속되어 자신의 AAA 홈 서버를 통해 인증이 가능할 때, EAP 기반의 적합한 인증 프로토콜을 수행할 수 있음.

- ERP 기반의 솔루션은 EAP 기반의 솔루션에서와 같이 AAA 인증서버와 인증을 하여 비밀키를 공유하고 있는 상황일 경우, 이동노드는 EAP의 최적화 버전인 ERP를 실행할 수 있음.

2.4 MIH 사전인증

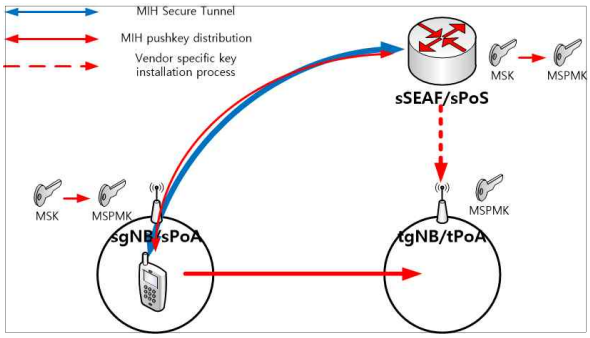
사전인증(Proactive authentication)이란 이동노드의 핸드오버가 발생하기 전에 인증을 수행하여 핸드오버 지연을 최소화하는 기법이며, IEEE 802.21a-2012에서는 인증 지연 시간을 최적화하기 위해 UMAP(Unbundled Media Access Proactive Authentication)와 BMAA(Bundled Media Access Proactive Authentication)의 2가지 기법을 제안하였다. MIH의 사전인증 기법에 대한 설명은 [표 1]과 같다.

인증기법		설명
UMAP		이동노드와 sPoS 간의 비밀키가 없을 경우(Unbundled)를 지원하는 옵션으로 핸드오버 이전에 이동노드는 sPoS와 sPoA의 도움으로 목적 PoA와 사전인증을 수행하여 이동노드와 목적 PoA는 MSK를 공유함.
BMAA	Push Key Distribution	이동노드는 핸드오버 이전에 sPoS에게 목적 PoA로 새로운 MSPMK(Media Specific Pairwise Master Key)를 전송하도록 유도함. sPoS는 목적 PoA에게 MSPMK를 전송하고 결과를 이동노드에게 통보함.
	Reactive Pull Key Distribution	핸드오버 이전에 이동노드와 sPoS가 새로운 MSPMK를 생성하고, 핸드오버 후에 이동노드와 목적 PoA의 인증을 위해 sPoS가 이동노드의 홈 AAA 인증서버 역할을 수행함.
	Optimized Proactive Pull Key Distribution	핸드오버 이전에 이동노드와 목적 PoA가 sPoS와의 보안 채널을 통해 사전인증을 진행함. sPoS는 AAA 인증서버로 간주하며, sPoS와 이동노드는 사전에 MSPMK를 기반으로 상호인증을 수행함.

[표 1] MIH 사전인증 기법

III. 5G HetNet 환경에 적합한 MIH 프로토콜 연구

5G 환경에서는 이종의 액세스 네트워크 상에서 잦은 핸드오버가 일어날 것이다. 따라서 2장의 MIH의 사전인증 기법을 활용하면 이종의 네트워크에서의 잦은 핸드오버에 대한 오버헤드를 경감할 수 있을 것으로 예상된다. [표 1]의 Push Key Distribution 기법을 적용한 5G HetNet 핸드오버 시나리오는 [그림 2]와 같다.



[그림 2] Push Key Distribution 기법을 적용한 5G HetNet 핸드오버 시나리오

(1) 핸드오버 이전, 이동노드는 MSK에서 MSPMK를 생성하고, sSEAF에게 MSK에서 파생한 MSPMK를 tgNB에게 전송하도록 요청함.

(2) sSEAF는 sgNB와 동일한 방식의 키 파생 방법을 활용하여 MSPMK를 생성하고 이를 tgNB에게 전송함.

(3) tgNB는 sSEAF가 전송한 MSPMK를 저장함.

(4) sSEAF는 tgNB가 MSPMK를 저장하는 것을 확인하고 해당 결과를 이동노드에게 통보함.

MIH는 [그림 2]와 같은 사전인증 기법을 통해 키를 분배하고, 이동노드가 tgNB로 이동하면 EAP나 ERP 등의 기법을 활용하여 인증을 진행한다. 잦은 핸드오버가 발생하는 5G HetNet 환경에서는 인증지연 시간에 민감하며, 이를 경감할 필요성이 있다. 각 사전인증 기법의 인증지연 시간을 [표 2]에서 비교하였다.

	인증지연 시간
EAP 기반의 솔루션	T_{MIH_Auth} + T_{MIH_Push} + T_{EAP}
ERP 기반의 솔루션	T_{MIH_Auth} + T_{MIH_Push} + T_{ERP}

T_{MIH_Auth} : MIH 인증시간
T_{MIH_Push} : MIH Key Push 시간
T_{EAP} : EAP 인증시간
T_{ERP} : ERP 인증시간
일반적인 상황에서 $T_{EAP} > T_{ERP}$ 가 충족됨.

[표 2] 인증지연 시간 비교

[표 2]에 따르면 Push Key Distribution 기법 이후 EAP와 ERP를 활용하였을 때, 일반적으로 ERP가 EAP에 비하여 인증지연 시간이 짧기

때문에, ERP 기반의 솔루션이 EAP 기반의 솔루션에 비하여 상대적으로 인증지연 시간이 짧음을 알 수 있다.

IV. 결론

본 논문에서는 5G HetNet 환경을 지원하기 위한 MIH 기반의 고속의 안전한 핸드오버 인증기법에 관하여 분석하였다. MIH는 이종의 액세스 네트워크 상에서 상호 간의 핸드오버를 지원하기 위하여 개발되었으며, 사전인증 기법을 통하여 핸드오버 오버헤드를 경감시켰다. 이러한 MIH는 이종의 액세스 네트워크에서 잦은 핸드오버가 일어나는 5G HetNet 구조에 적합하며 3장에서 이를 적용하였다. 본 논문의 연구는 앞으로 복잡한 5G 네트워크 상에서 신속한 핸드오버가 요구되는 상황에서 활용될 수 있을 것으로 기대된다.

Acknowledgement

이 논문은 2017년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. 2016R1D1A1B03935619).

[참고문헌]

[1] C. Eklund, R.B. Marks, K.L. Stanwood and S. Wang, "IEEE Standard 802.16: A Technical Overview of the WirelessMAN™ Air Interface for Broadband Wireless Access," IEEE Communication Magazines, pp.98-107, June, 2002.

[2] IEEE 802.11™ Wireless Local Area Networks, "http://www.ieee802.org/11/" [Online; accessed on May 7, 2018]

[3] A. Samukic, "UMTS universal mobile telecommunications system: development of standards for the third generation," IEEE Transactions on Vehicular Technology, Vol. 47, No. 4, pp.1099-1104, Nov. 1998.

[4] 3GPP LTE, "http://www.3gpp.org/technologies/keywords-acronyms/98-lte" [Online; accessed on May 7, 2018]

[5] 3GPP LTE-A, "http://www.3gpp.org/technologies/keywords-acronyms/97-lte-advanced", [Online; accessed on May 7, 2018]

[6] IEEE, "https://www.ieee.org/" [Online; accessed on May 7, 2018]

[7] "IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services, IEEE 802.21-2008", a contribution to IEEE 802.21 WG,January 2009.

[8] "802.21a-2012 - IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services - Amendment for Security Extensions to Media Independent Handover Services and Protocol," May 2012.

[9] R. Marin-Lopez et al., "A new Standard for securing media independent handover: IEEE 802.21A," IEEE Wireless Communications, Vol. 20, no. 6, pp. 82-90, December 2013.

[10] D. Simon, B. Aboba, and R. Hurst, "The EAP-TLS Authentication Protocol," IETF RFC 5216, March 2008.

[11] J. Arkko, H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)," IETF RFC 4187, January 2006.

[12] V. Narayanan and L. Dondeti, "EAP Extensions for EAP Re-authentication Protocol (ERP)," IETF RFC 5296, August 2008

OAuth 2.0 인증 프로토콜의 취약점에 대한 대응방안 제시

서동화, 윤가헌, 오장욱, 서정택

순천향대학교 정보보호학과

A Provide Countermeasures against Vulnerabilities of OAuth 2.0 Authentication Protocol

Dong Hwa Seo, Ga Heon Yoon, Jang Wook Oh, Jung Taek Seo

Department of Information Security Engineering, Soonchunhyang University

요 약

최근 많은 사용자들의 SNS 사용 증가로 많은 웹 서비스에서 SSO(Single Sign On)의 일종인 OAuth 2.0을 인증방식으로 사용하고 있다. 그러나 페이스북 해킹 사례와 해외 Cloudflare 정보 노출사고 등 OAuth 2.0을 사용함으로 나타나는 다양한 취약점으로 인해 OAuth 2.0 인증방식을 사용하는 많은 사이트들이 해킹에 노출되고 있다. 본 논문에서는 OAuth 2.0의 인증 프로토콜의 취약점에 대한 기존의 대응방안에 대한 설명과 새로운 대응방안을 제안하고자 한다.

I. 서론

최근 통합로그인(SSO)의 일종인 OAuth 2.0의 간편한 인증을 사용하는 사이트들이 증가함에 따라 해킹위험도 잇따라 증가하고 있다. 최근 국내에서 페이스북 계정을 해킹하여 사용자 정보를 탈취하여 다른 사람을 사칭해 돈을 요구한 사례가 있었으며, 해외에서는 Cloudflare가 사용자 인증을 위한 암호 및 쿠키 인증토큰 정보를 노출하였으며, OAuth 2.0을 사용하는 많은 사이트에서 그에 따른 취약점이 들어나고 있다.[1][2]

앞서 언급한 사례처럼 앞으로 OAuth 2.0은 더욱 많이 사용될 것이고, 취약점을 보완하지 않으면 많은 사용자들의 개인정보가 위험함에 따라, 본 논문에서는 나타날 수 있는 취약점을 분석하고 이에 따른 대응방안을 제시한다.

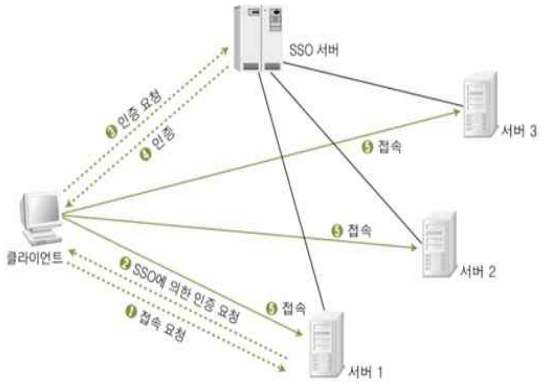
본 논문의 구성은 다음과 같다. Ⅱ장에서 SSO의 정의와 OAuth 2.0 인증 프로토콜의 대한 분석 및 발생할 수 있는 취약점에 대해 분석을 진행한다. Ⅲ장에서는 OAuth 2.0의 취약점에 대한 기존의 대응방안에 대한 설명과 새로운 대응방안을 제시하고, 기존의 대응방안과의 차이점을 비교, 분석한다. 마지막으로 Ⅳ장에서는 향후 연구 방향을 제시하면서 결론을 맺도록 한다.

II. OAuth 2.0 인증 프로토콜

2.1 통합로그인 SSO(Single Sign On)

OAuth 2.0을 설명하기에 앞서 근원이 되는 통합로그인을 먼저 살펴 볼 필요가 있다. 통합로그인은 Single Sign On의 약자로 한번의 로그인을 통해 다른 시스템 서버에 접속할 수 있는 권한을 갖는 시스템이다.

[그림 1]을 보게 되면 클라이언트는 서버1에 접속요청을 하게 되고 서버1은 SSO 서버의 인증을 요구하게 된다. 클라이언트는 SSO 서버에 인증요청을 해서 인증을 하게 되고 서버1뿐만 아니라 서버2, 서버3까지도 접근을 할 수 있게 된다.



[그림 1] 통합 로그인(SSO) 인증과정 도식화

2.2 OAuth 2.0 인증 프로토콜

OAuth는 Open Authorization의 약자로 웹, 모바일, 어플리케이션에서 권한 인증을 수행할 수 있는 단순하고 표준 방법인 Open 프로토콜이다. 인증 프로토콜 설명에 앞서 용어를 [표 1]로 정리했다.[3]

[표 1] OAuth 2.0 인증 프로토콜 용어

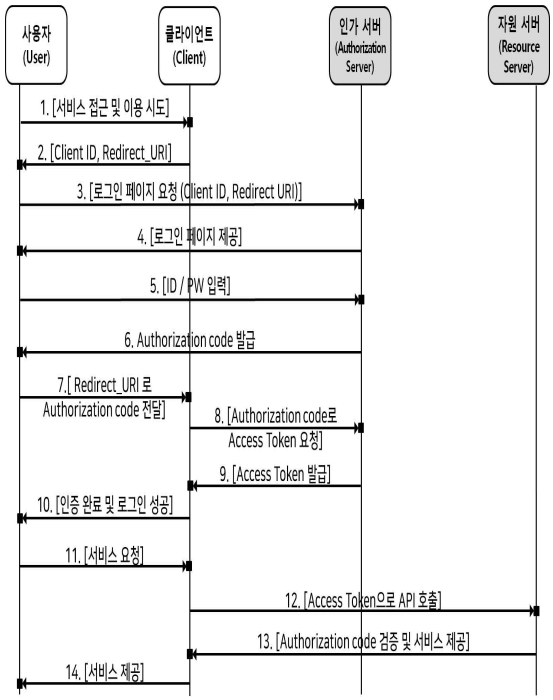
자원서버 (Resource Server)	보호된 정보를 제공하는 서버
자원 소유자 (Resource Owner)	자원 서버에 계정을 가지고 있는 사용자
클라이언트 (Client)	자원 소유자를 대신해 자원 서버의 서비스를 사용하는 자
인가서버 (Authorization Server)	클라이언트가 자원 서버의 서비스를 사용 할 때 사용하는 접근 토큰을 발행하는 서버



[그림 2] OAuth 2.0의 인증 과정[4]

[그림 2]와 같이 인증 과정은 다음과 같다. 사용자는 인증을 위해 인가서버에 요청을 하면 인가서버는 정당한 사용자이면 Authorization code를 발급한다. Authorization code으로 Access Token을 발급하여 사용자는 서비스 서버에 접근을 할 수 있다.

[그림 2]에서는 간단한 인증과정을 도식화 했다면, [그림 3]은 OAuth 2.0의 인증 프로토콜을 도식화 한 것이다. 다음의 순서에 따라 인증이 진행 된다.



[그림 3] OAuth 2.0의 인증 프로토콜 [4]

사용자가 클라이언트에게 서비스 접근 및 로그인 요청을 한다.

1. 사용자의 요청에 의해, Client ID와 Redirect_URI을 사용자에게 보내준다.

2. 사용자는 인가서버에게 Client ID와 Redirect_URI로 로그인 페이지를 요청을 한다.

3. 인가 서버는 사용자에게 로그인 페이지를 제공해준다.

4. 사용자는 로그인 페이지에 ID, PW를 입력한다.

5. 인가 서버에서 입력된 ID, PW를 확인하여 정당한 사용자이면 Authorization code를 사용자에게 보내준다.

6. 사용자는 인가 서버에게 받은 Authorization code와 Redirect_URI를 클라이언트로 전달한다.

7. 클라이언트에서는 인가 서버에게 Authorization code로 Access Token을 요청한다.

8. 인가 서버는 Authorization code을 이용해 Access Token을 만들어 클라이언트에게 전달한다.

9. 클라이언트는 사용자에게 Access Token을 전달하여 인증 완료 및 로그인 성공을 확인한다.

10. 사용자는 클라이언트에게 자원 서버의 서비스를 요청한다.

11. 클라이언트는 자원 서버에게 Access Token으로 자원 서버의 API을 호출 한다.

12. 자원 서버는 클라이언트에게 받은 Access Token으로 Authorization code을 검증을 하고 정당한 Authorization code이면 자원 서버는 클라이언트가 요청한 서비스를 제공한다.

13. 클라이언트는 사용자가 요청한 서비스를 제공한다.

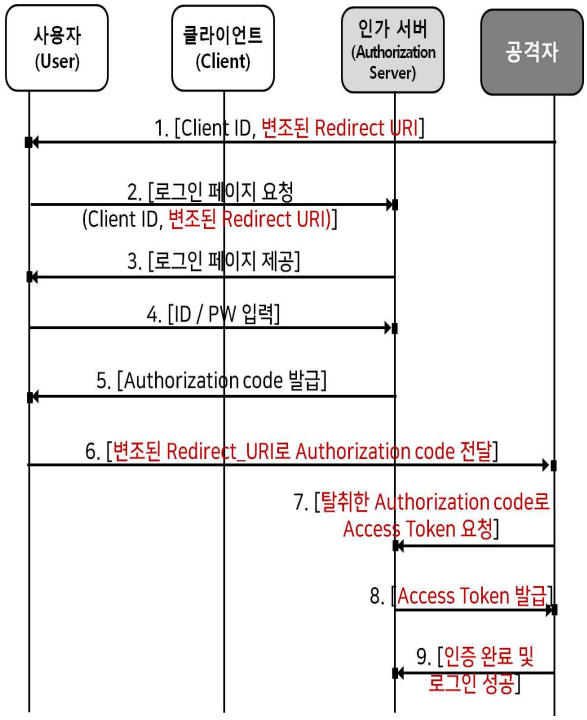
앞서 프로토콜에서는 인증코드와 Redirect_URI을 통해 사용자와 클라이언트간의 인증을 인증서버와 자원서버를 통해 인증토큰이 제공 되고 그것을 통해 인증 하는 것을 볼 수 있다.

하지만 이에 따른 보안위협이 있다. 다음 장에서는 OAuth 2.0 인증 프로토콜의 대표적인 보안위협과 이에 따른 기존의 대응방안, 그리고 새롭게 제안하는 대응방안을 제시한다.

2.3 OAuth 2.0 인증 프로토콜의 보안 위협

[표 3] OAuth 2.0의 보안위협 [4]

분류	보안위협
권한코드 유출	권한코드 도청 및 유출 Covert Redirect와 CSRF 공격을 통해 권한 코드 획득 공격
서비스 거부(DoS)	반복된 권한요청을 통하거나 악의적으로 생성된 권한코드를 통해 권한서버의 서비스 거부 공격
불법권한 획득	권한 코드 추측, 클릭재킹을 통한 권한획득 공격
신분/세션 도용	자원 소유자 신분도용 이용자 세션 도용



[그림 4] Covert Redirect 취약점 [4]

[표 3]과 같이 OAuth 2.0에는 여러 보안위협이 있다. OAuth 2.0의 대표적인 보안 위협으로는 Covert Redirect이다. [그림 4]는 Covert Redirect 취약점에 대한 설명이다. 위 보안위협은 클라이언트가 인가서버에 권한을 요청 할 때, Redirect_URI에 인자 값을 보내게 되는데 이것을 중간에 가로채서 사용자의 서버로 Redirect_URI을 변조하여 권한 코드 및 접근 토큰 등을 탈취 하는 공격이다. 그 밖에도 서비스 거부 공격(Denial of Service attack)을 통해 권한서버를 마비시키는 공격과 클릭재킹(Click Jacking)을 통해 웹페이지를 변조해서 공격자가 원하는 페이지로 이동하게 하는 공격, 사용자의 신분도용과 이용자 세션을 도용하는 공격들이 존재한다. [5]

III. OAuth 2.0 인증 프로토콜의 취약점에 대한 대응방안 제시

3.1 OAuth 2.0의 기존 대응방안

[표 4] OAuth 2.0의 보안위협에 대한 대응방안 [4]

분류	대응방안
권한코드 유출	SSL/TLS 기반의 HTTP를 통해서 클라이언트와 서버 간 통신구간 보호 권한 코드의 유효기간의 짧게 설정 SQL 인젝션에 대한 대응 Redirect_URI을 비교해서 검증
서비스 거부(DoS)	이용자별 발급 가능한 접근 토큰 개수 제한 비정상 권한 코드를 일정 횟수 이상 서버에 전송하는 경우 차단
불법권한 획득	권한 코드에 메시지 서명적용 인증 및 권한 부여 웹페이지에서 iFrame을 비활성화 하도록 옵션 추가
신분/세션 도용	CAPTCHA사용 본인인증 E-Mail을 통한 인증

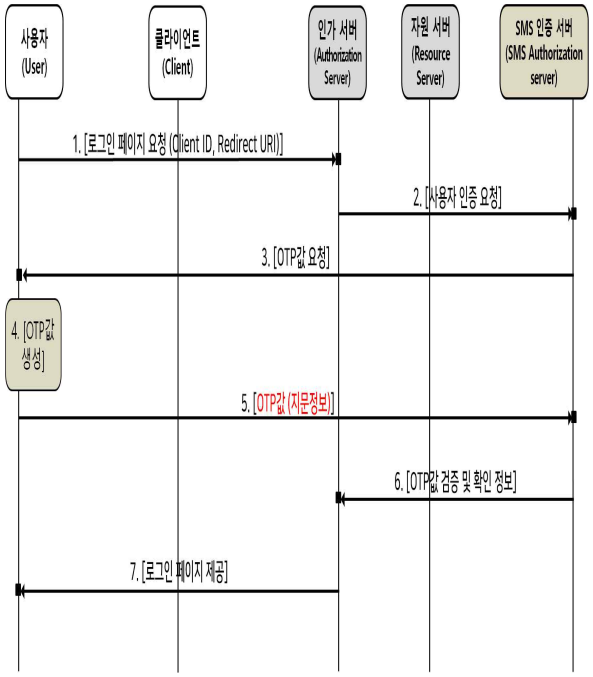
[표 4]와 같이 기존의 대응방안에는 SSL/TLS를 통해 클라이언트와 권한 서버간의 통신구간을 암호화해 Redirect_URI을 보호하는 방법, 권한 코드의 유효기간을 짧게 설정 하여 일정시간이 지나면 재 인증을 요구하는 방법, 최초 등록된 Redirect_URI과 전달된 Redirect_URI을 비교 하여, 클라이언트의 IP주소, 기타 시스템 정보를 비교하는 검증하는 방법 등이 있다.

서비스거부(DoS)공격의 경우 과도하게 권한 요청을 하지 못하게 접근 가능한 토큰의 개수를 제한하고 비정상 권한코드를 일정 횟수 이상만큼 서버에 전송하는 경우 서버에서 차단하여 막을 수 있다.

불법권한 획득에는 중간에서 가로채도 알 수 있게 메시지 서명을 적용하고 권한코드에 1회성의 임의 값을 추가하는 방법, 인증 및 권한 부여 웹페이지는 iFrame을 비활성화 하도록 서버 옵션 추가 등이 있다.

또한, 신분이나 세션을 도용을 방지 하는 대응방안으로는 변형된 이미지를 사용해 사용자가 실제 사람인지 확인 하는 방법인 CAPTCHA인증 방법, E-Mail을 통해 본인인증을 하는 도용을 막을 수 있는 방법 등이 있다.

3.2 신규 OAuth 2.0 인증 프로토콜 제시



[그림 5] SMS를 통한 사용자 인증 방법 제안

[표 5] SMS를 통한 사용자 인증 방법

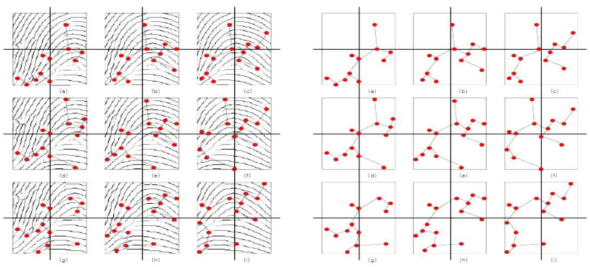
순서	인증 방법
1	사용자는 인가서버에게 Client ID와 Redirect_URI로 로그인 페이지를 요청을 한다.
2	로그인 페이지 요청을 받은 인가서버는 SMS 인증 서버에 사용자 인증을 요청한다.
3	SMS 인증 서버는 사용자에게 OTP값을 요청한다.
4	사용자는 SMS 인증 서버에 미리 등록한 지문정보를 통해 OTP값을 생성한다.
5	사용자는 생성된 OTP값을 입력해 SMS 인증 서버로 보낸다.
6	SMS 인증 서버는 OTP값을 검증하여, 정당한 사용자임을 확인하고 확인한 정보를 인가서버로 보낸다.
7	인가서버는 사용자에게 로그인 페이지를 제공해준다.

[그림 5]와 [표 5]는 신규 제안하는 OAuth 2.0의 프로토콜이다. 본 프로토콜은 [그림 3]의 OAuth 2.0의 기본 프로토콜 인증 과정에서 3번 과정 이후에 제안하는 프로토콜을 이용해 모바일

SMS 인증 서버를 사용한 추가 인증을 요구하는 방법이다.

본 논문에서는 기존의 대응방안과는 다르게 사용자의 SMS를 통해 변조된 Redirect URI에 입력하는 로그인 값을 아이디와 패스워드를 통해 정당한 사용자를 인증하지 않고 OTP를 이용해 사용자를 인증을 하는 방법을 제안한다.

인증 방법은 다음과 같다. 사용자는 가입할 때 0~9까지 특정한 번호4개를 선택한다. 이때의 번호는 자릿수가 된다. 스마트 폰을 통해 지문인식을 사용하는데 지문인식을 할 때 항상 같은 곳으로 인식하는 것이 아니라 [그림 6]처럼 모바일 기기를 통해 매번 위치를 바꾸어 인식하게 되어서 그에 따른 특정한 좌표 값도 다르게 나오고 그것을 랜덤 값으로 만들어 지문의 특정한 좌표 값으로 랜덤한 번호 10개를 만든다. 이것을 SMS서버에 미리 저장하게 되고, 인증시, 사용자는 SMS를 통해 랜덤한 번호 10개를 받으면 가입할 때 선택한 4개의 번호순서로 OTP값을 입력한다.



[그림 6] 지문의 위치에 의한 특징 점 변화 [6]

위에서 언급한 제안방식을 사용하게 되면, 공격자가 변조된 Redirect URI를 통해 사용자의 로그인 값을 가로챘더라도 OTP방식으로 인증하기 때문에 유출이 되면 사용자의 정한 번호 자릿수를 모르기 때문에 공격자는 Access Token을 얻을 수 없다. 그리고 변조된 Redirect URI로 공격자가 인증을 요청하면 사용자의 SMS 알림으로 확인이 가능하다.

SMS으로 확인이 가능하기 때문에 사용자도 인증을 인지할 수 있게 됨으로써 자신이 공격당하고 있고 나의정보로 인증 되고 있다는 사실을 알 수 있게 된다. 또한 아이디와 비밀번호를 입력하지 않기 때문에 개인정보 유출에도 안전하다.

3.3 제안된 OAuth 2.0 인증방식과 기존 방식 비교

현재 사용되고 있는 E-Mail을 통해 인증하는 방법은 같은 하드웨어를 사용하여 인증하는 방법이라는 점 때문에 하드웨어가 공격받을 경우, 피싱 공격 및 파밍 공격으로 인한 탈취 가능성이 존재한다.

본 논문에서 제안하는 SMS를 통한 사용자 인증 방식은 두 하드웨어를 통한 인증방식으로 피싱 공격 및 파밍 공격에 대응가능 하다.

또한, 사용자 지문의 특징 점을 이용하여 OTP를 생성하여 인증하는 방식으로 Covert Redirect 취약점을 막을 수 있고, 사용자는 개인정보 유출을 막을 수 있다.

IV. 결론 및 향후 연구방향

최근 SNS 이용자의 증가에 따라 많은 웹 서비스들은 OAuth 2.0 프로토콜을 사용해 사용자 로그인을 지원하고 있다. OAuth 2.0 프로토콜은 사용자들의 편의성을 위해 제안된 프로토콜이지만, 편의성을 얻는 대신 보안 위협이 존재하며, 보안 위협의 내용은 2.3에서 설명하였다.

본 논문에서 제안하는 SMS를 통한 사용자 인증 방식은 하나의 하드웨어 장치가 아닌 다른 하드웨어 장치(모바일 기기)를 추가하여 인증을 하는 방법으로, 3.3에서 설명한 것과 같이 E-Mail을 통한 사용자 인증 방식과는 달리, 피싱 공격 및 파밍 공격으로부터 안전하다.

또한, 사용자의 지문 특징 점을 이용한 OTP 생성 인증 방식을 사용함으로서, OAuth 2.0의 취약점인 Covert Redirect 취약점을 막을 수 있다는 장점을 가진다.

이에 대한 기대효과로는 OAuth 2.0 통합 인증 서비스를 지원하는 온라인 쇼핑몰이나 전자상거래, 공공기관에서의 안전한 사용자 인증과 보안성이 높고 신뢰성이 있는 서비스 제공을 기대할 수 있다.

본 논문에서 제안한 OAuth 2.0 인증 프로토콜은 Redirect_URI에 대한 취약점을 보완한 것이다. 그러나 인증서버에 대한 보안도 중요하며 그에 따른 취약점은 서비스거부(DoS)공격 및 불법권한 획득 공격이 가능하기 때문에 향후 이에 따른 연구가 지속적으로 이루어져야 보다 안전한 OAuth 2.0 인증 프로토콜을 구현할 수 있다.

본 연구는 2018년도 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 과제입니다. (No.2162220200010)

[참 고 문 헌]

[1] 조선비즈(2014), “페북 메신저 해킹은 ‘통합 로그인’ 보안 취약 때문”

http://biz.chosun.com/site/data/html_dir/2014/05/25/2014052502275.html

[2] ars TECHNICA, ‘Serious Cloudflare bug exposed a potpourri of secret customer data’

https://arstechnica.com/information-technology/2017/02/serious-cloudflare-bug-exposed-a-potpourri-of-secret-customer-data/

[3] 티스토리, ‘Oauth의 짧은 설명’

http://bsnippet.tistory.com/18

[4] TOAST, ‘OAuth 2.0 대표 취약점과 보안 고려 사항 알아보기’

http://meetup.toast.com/posts/105

[5] 금융보안원, “OAuth 2.0 개요 및 보안 고려사항”

[6] 차병래, 고일석, ‘An OTP(One Time Password) Generation Method Using the Features of Fingerprint’, 2015

[7] 채철주, 최광남, 최기석, 예용희, 신용주, ‘OAuth 2.0 프로토콜에서 E-mail을 이용한 사용자 권한 인증’, 2015

1Kbps 미만 무선 통신 센서 네트워크에서의 개체 인증 및 키 관리

김현기*, 이옥연*

*국민대학교 금융정보보안학과

Entity Authentication and Key management in a wireless sensor network under 1 Kbps communication capability

Hyun-Ki Kim*, Ok-Yeon Yi*

*Division of Financial information security, Kookmin University.

요 약

각종 사물과 센서에 통신 기능을 내장해 상호간 인터넷으로 정보를 주고받는 장비들이 늘어나고 있다. 소물 인터넷은 사물 인터넷을 소형화하여 센싱 능력과 저성능의 통신능력만을 가지는 센서로 볼 수 있다. 저성능의 센서는 고품질의 통신을 사용하기에 어려움이 있으며, 고 성능의 무선통신 기기에서 사용하는 무선 보안을 적용할 수 없다. 따라서 본 논문은 속도 1Kbps 미만의 통신을 사용하며 제한된 성능을 가지는 센서 네트워크에서 적용할 수 있는 개체 인증 및 키 관리를 제안한다.

I. 서론

모바일 장비나, IoT(Internet of Things)들이 보급되면서 센서 네트워크 기반 인프라 시스템이 상당부분 다가와 있다. 지상에서는 센서 네트워크에 적합한 다양한 RF(Radio Frequency) 신호를 사용할 수 있어 센서 노드 간 비교적 장거리 통신이 가능하다.

IoT 중에서도 작은 센서와 통신 모듈로 소량에 데이터를 주고받는 IoST(Internet of Small Things)가 주목 받고 있다. IoST는 기기를 저전력, 저성능이면서 비교적 저렴하게 생산할 수 있는 소형 센서로 볼 수 있다.

하지만 모든 통신 노드가 보안 위협에 노출될 수 있듯이 이러한 IoST도 예외는 아니다. 기능이 상당부분 제한된 IoST 및 센서는 고성능 기기에서 적용 가능한 보안 방식을 동일하게 적용할 수 없기 때문에 오히려 고성능 기기에 비해 훨씬 취약하다.

따라서 본 논문은 통신 속도 및 성능이 낮은 IoST, 센서 등이 이루는 무선 센서 네트워크 환경에서 네트워크를 이루는 노드 간 안전한 채널(Secure channel)을 형성하기 위한 키 관리 방식을 제안하며, 해당 제안 기법이 제공하는 보안을 분석한다.

II. 관련 연구

2.1 RF기반 지상 센서 네트워크

지상에서의 센서 네트워크는 RF신호를 사용하여 네트워크를 구성한다. 센서 네트워크에서 사용가능한 RF 신호의 종류로는 LTE(Long Term Evolution), LTE-M(LTE for M2M), LoRa(Long Lange), NB-IoT(Narrow Band-IoT), ZigBee, Bluetooth 등이 있다. 하지만 센서 네트워크에는 다양한 제약사항이 있기 때문에 빠르고 품질이 보장되는 통신을 적용하기에는 어려움이 따른다.

주파수의 면허/비면허 대역사용 유무가 주된 제약사항 중 한 가지이다. LTE와 NB-IoT 통신은 면허대역의 주파수와 통신사의 인프라를 사용하기 때문에, 통신 범위가 넓고 속도, 신뢰성 면에서 품질이 좋지만 통신비가 부과된다는 단점이 있다. 일반적으로 센서 네트워크는 다량의 센서가 통신하기 때문에 요금이 부과되는 통신은 적합하지 않다. 이에 반해LoRa, ZigBee, Wi-Fi 등 ISM 대역(Industrial Scientific Medical band)의 비면허 대역 통신은 무료로 사용가능하지만 면허대역 통신보다 상대적으로 통신 속도가 느리며 품질이 낮다.

센서는 중거리에 산개/배치되며 각 노드와 장기간 간헐적으로 통신한다. 즉 센서 네트워크를 효율적으로 구성하기 위해서는 노드 간 거리 이상의 통신 범위 및 데이터 전송량, 통신 전력 소모가 적은 것을 택해야 한다. 따라서 센서 네트워크는 일반적으로 비면허 대역 중 해당 인프라에 적합한 통신을 선택하여 사용한다. 대표적으로 LoRa와 ZigBee는 모두 통신 전력 소모가 적으며, LoRa는 약 2 ~ 14Km, ZigBee는 약 10 ~ 100m까지 통신이 가능하여[1] 센서 네트워크에서 사용한다. 하지만 이러한 조건을 만족하는 통신이라도, LoRa의 경우 Bit-rate가 거리에 따라 약 250bps ~ 5.5kbps이며 벽 투과가 어려운 주파수대역을 사용하는 등 제약조건이 있다. 현재 LoRa로 지상에서 한번 통신할 때 전송할 수 있는 payload의 길이는 평균 60-Byte로서 센서 네트워크를 구성하기에 제한적이다.

2.2 음파기반 수중 센서 네트워크

바다는 지구 표면의 약 70%를 차지하므로 물속에서도 센서 네트워크를 이룬다면 지상보다 더 다양한 정보를 수집할 수 있을 것이라 기대할 수 있다. 수중에서는 RF신호로 통신하는 것은 비효율적이기 때문에 RF 신호보다 효율적 통신이 가능한 음파를 주로 사용하며[2], 세계적으로 9개국 60여개에 달하는 기관이 수중음파통신을 개발하고 있다.[3]

하지만 음파의 통신속도는 $1.5\,km/s$로, RF 기반 통신에 비해 매우 느리고 사용할 수 있는 주파수 대역이 10 ~ 50kHz로 RF의 대역인 300 MHz ~ 30 GHz 보다 상당히 좁아서 한 번에 전송할 수 있는 데이터양이 매우 적다. 또한 Bit-rate는 100bps ~ 1kbps로 전송률이 낮으며 해저의 지형적인 특성과 해류 등에 의해 음파의 다중간섭과, 송수신 데이터의 손실이 자주 발생한다.

현재 음파로 수중에서 한 번에 전송할 수 있는 payload의 길이는 평균 30-Byte로서 센서 네트워크를 구성하기에 제한적이다.

2.3 센서 네트워크의 인프라 구조

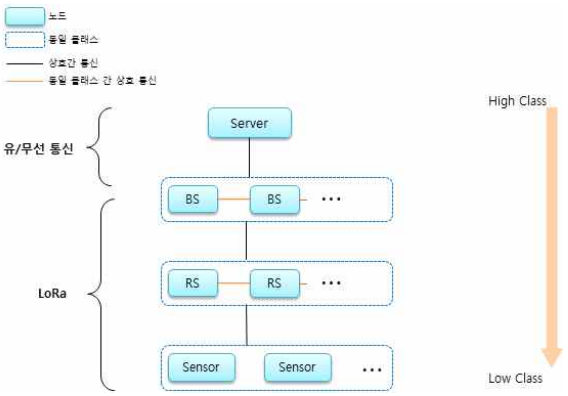


그림. 1. 센서 네트워크 인프라 구조도

그림. 1은 센서 네트워크의 인프라를 개체별 능력 정도에 따라 클래스로 구분하여 나타낸 것이다.

센서 네트워크에서 Server부터 BS(Base Station)까지는 하위 노드들 보다 상대적으로 개체 수가 적으며 고성능의 기기로 이루어져있기 때문에 성능이 좋은 유/무선 통신을 적용할 수 있다. BS의 하위 노드인 RS(Relay Station)와 Sensor는 개체 수가 많고, 생산비용이 낮아야하기 때문에 상위 노드보다 저성능이며 Bit Rate가 낮거나 느린 통신을 사용한다.

RF기반과 음파 기반 센서 네트워크는 위의 인프라 모델에 따라 클래스로 구분할 수 있으며 각 개체는 위에서 아래로 내려갈수록 다음과 같은 특징을 가진다.

- 연산/통신 능력 저하
- 메모리 크기 감소
- 개체의 수 증가
- 생산 원가 낮아짐
- 개체의 크기 감소
- 배터리 교체 어려움 증가

각 클래스별 제약사항 및 특징 때문에 각 노드들은 이를 고려하여 보안을 적용해야 한다. 따라서 본 논문에서는 네트워크의 계층 구도를 통해 상대적 상위/하위 클래스 노드를 구분하고, 그 클래스 별 개체 인증 및 키 분배, 키 갱신/파기를 진행한다.

〔표 1〕 1Kbps 미만 무선 통신을 사용하는 센서 네트워크

구분	음파 기반	RF 기반 (ex. LoRa)
사용 주파수 대역	10 ~ 50 KHz	920MHz
Bit Rate	100bps ~ 1Kbps	250bps ~ 5.5Kbps
한 번에 전송 가능한 페이로드 길이	30-Byte	60-Byte

III. 클래스별 개체 인증 및 키 분배

3.1 적용 범위

제안하는 '개체 인증 및 키 분배' 방식을 적용할 범위는 센서 네트워크에서 노드의 통신 및 연산, 메모리 등의 성능이 상대적으로 낮고, 통신 속도가 1Kbps 미만인 구간으로 제한한다.

음파 기반 수중 센서 네트워크와 1kbps 미만 통신을 사용하는 센서 네트워크에서 Base Station 및 Relay Station, Sensor사이로 제한한다.

3.2 가정 사항

- 노드 Identifier와 키 간 매핑

키와 해당 키를 사용하는 노드의 식별자는 매핑되어 있어, ID 정보를 통해 키를 검색할 수 있다.

- 난수 생성

센서 네트워크 내 저성능의 노드는 암호학적으로 안전한 8 byte 난수를 생성할 수 있다.

- 현장에 배치된 노드

제안하는 방식을 적용하는 센서 네트워크의 구조는 그림 1과 같이 노드 간 클래스가 존재한다. 각 네트워크에서는 고성능의 상위노드(BS)가 저성능의 하위노드(RS, Sensor)보다 현장에 먼저 배치되어 작동한다.

- 제안 방식에서 사용되는 기호

〔표 2〕 제안기법에서 사용되는 변수 목록

기호	설명	크기
K_i	키 설립 전 공유하고 있던 키	16-byte
K_{AB}	키 설립으로 노드 A와 B가 공유한 새로운 키	16-byte
ID_i	노드 i 의 식별자 정보	8-byte
N_i	노드 i 가 생성한 nonce 값	8-byte
$iMAC$	노드 i가 생성한 인증 값	8-byte 16-byte
RES	인증 절차 중 Challenge에 대한 응답 값	8-byte
$XRES$	***RES*** 검증에 사용되는 비교 값	8-byte

3.3 키 분배 (Key Distribution)

- 키 사전 분배 (Key Pre-distribution)

센서 네트워크 인프라의 관리자는 전체 키 공간 K에서 키풀 L을 추출한다. 각 노드는 m 개의 키로 이루어진 부분 키 집합을 L에서 추출하여 오프라인으로 분배받는다.

부분 키 집합을 분배받은 임의의 두 노드는 공유 키를 x개 $(0 \le x \le i, 1 \le i \le m)$가질 수 있다. 두 노드 간 공유 키 개수가 0개이면 두 노드는 인증이 불가능하다.

- 동일 클래스 간 인증 및 키 공유

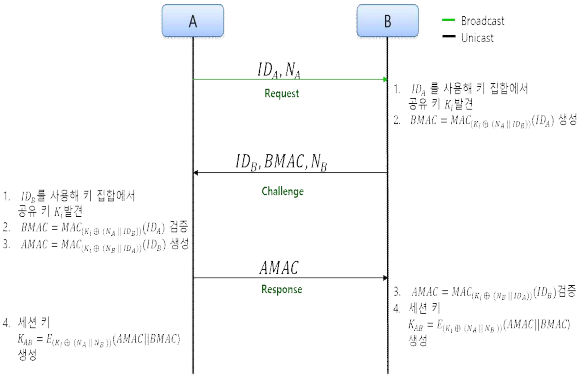


그림. 2. 동일 클래스 간 개체 인증 및 키 공유

동일 클래스 간 통신은 BS와 BS, RS와 RS, 등 자신과 동등한 개체와의 통신을 뜻한다.

통신을 진행하기 전에 안전한 세션(secure session)을 설립하기 위해 통신할 두 노드는 인증 및 키 교환을 진행한다.

- 다른 클래스 간 인증 및 키 공유

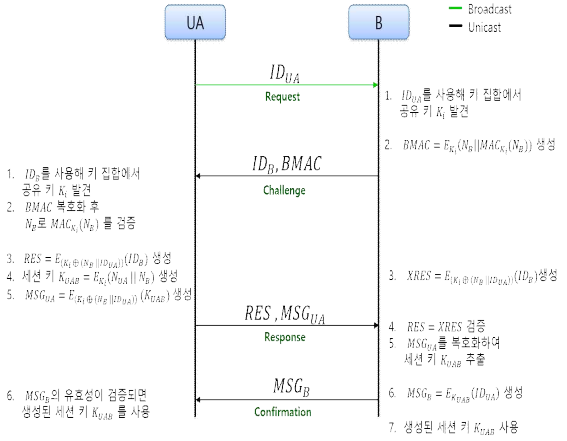


그림. 3. 다른 클래스 간 개체 인증 및 키 공유

다른 클래스 간 통신은 BS부터 하위 클래스인 RS 및 Seneor 노드 간 통신을 뜻한다. 가정에서와 같이 상위 노드는 하위 노드보다 현장에 먼저 배치되어 있어, 주기적으로 브로드 캐스팅하여 주변 새로운 노드를 찾는다. 다음 절차의 진행의 우선순위는 상위 노드가 가지고 있어서 항상 먼저 시작하며, 다음 절차에서 상위 노드를 UA(Upper A)로, 하위 클래스를 B로 표현한다.

3.4 노드의 키 파기(Key Revocation)

센서 네트워크 특성상 배치된 노드들은 개체 수가 많고, 배터리 교체에 어려움이 있다. 때문에 배터리 수명이 다한 노드는 회수하지 않고, 버려진다. 이 때, 물리적으로 버려진 노드를 통해 센서 네트워크 내 다른 노드와의 통신에서 사용가능한 키를 추출해낼 수 있으므로, 해당 노드는 주변 노드와 공유하고 있던 키(K_i)를 삭제한다.

수명을 다한 노드는 자신과 세션키(K_{AB} 혹은 K_{UAB})를 공유한 각 노드에게 안전한 세션 내에서 ID 정보를 전송한다. 수신 노드는 수신한 ID에 매핑되어 있는 키들(오프라인으로 분배받은 키)을 삭제한다.

수명을 다한 노드는 소유하고 있던 모든 키(오프라인으로 분배받은 키, 세션키)를 제로화하며, 센서 네트워크에서 탈퇴한다.

3.5. 노드의 키 갱신(Re-Keying)

노드 간 사용하는 키의 생명주기(Life Cycle)가 만료되었지만 통신할 능력이 남아있다면 키를 갱신해서 통신을 유지할 수 있다. 키 파기 방식과 비슷하지만 모든 키를 파기하지 않고 생명주기가 만료된 키만 파기한다. 안전한 세션이 사라진 두 노드는 새롭게 키 분배 방식 중 인증 및 키 공유 절차를 진행한다.

IV. 제안 기법 분석

4.1. 키 분배 상식에 따른 확률

p-th 노드와 q-th 노드가 가진 m개의 키 중 공유키가 i개일 확률은 수식(1)과 같다.

$$p(i) = \frac{\binom{L}{i}\binom{L-i}{2(m-i)}\binom{2(m-i)}{m-i}}{\binom{L}{m}^2} \qquad (1)$$

L개의 키 풀에서 m개의 키를 각각 두 번 추출한다고 할 때, L개의 키풀에서 공유할 i개의 키를 비복원 추출한 다음, $L-i$ 개 중에서 서로 다른 $2(m-i)$개를 추출하고 그 서로 다른 $2(m-i)$ 개를 반으로 나눈 값이 된다.

임의의 두 노드가 공유한 키의 수가 $i=1$이면 $p(i)$가 낮아지므로 '개체 인증 및 키 공유' 절차를 수행할 두 노드 간의 인증 실패 가능성이 높아진다. 반면 공유키의 수i가 과도하게 많으면 $p(i)$는 높아지지만 공격자에게 노드를 물리적으로 탈취당하거나, 노드가 잠식당했을 경우 공유키의 많은 부분이 노출된다. 따라서 노드가 탈취 등의 물리적인 공격을 당했을 때 노출되는 정보를 줄이면서, $p(i)$를 높일 수 있는 전체 키풀의 크기L과 부분키 집합의 크기m, 공유키의 개수i를 선택해야한다.

그림4는 센서 네트워크에서 노드 간 공유할 키의 개수가 $i=4$일 때 부분키 집합의 크기변화에 따른 확률이다. 전체 키풀의 크기L과 두 노드 간의 공유키 개수i를 고정한 상태에서 노드가 가져야 할 부분키 집합의 크기m의 값을 변화시킬 때의 확률을 보인다.



그림.4. 4개의 키 공유 시 부분키 집합 크기 변화에 따른 확률

따라서 현장의 네트워크 규모와 배치할 노드의 수 등에 따라 전체 키풀의 크기L과 각 노드 간 공유할 키의 수i를 정하고, 해당 조건에서 $p(i)$가 가장 높아지도록 부분키 집합의 크기 m을 선택해야한다.

4.2 안전성 분석

- 데이터 위변조 공격

각 노드의 개체 인증 절차가 없다면 공격자가 네트워크에 쉽게 참여할 수 있어 도청으로 수집한 패킷이나, 데이터 위변조가 가능하다. 따라서 노드가 네트워크에 참여하기 위해선 개체 인증을 수행해야만 하며, 메시지 인증 코드를 전송함으로서 데이터 위변조 공격을 방지가능하다.

인증 절차에서 각 노드는 상대의 ID만을 보고 상대와 세션키 공유가 가능한지 여부를 확인하며 매핑되는 노드의 ID가 자신의 부분 키 집합에 없다면 불필요한 연산을 수행하지 않는다.

- 라우팅 공격 및 재전송 공격

공격자는 노드의 ID값을 가장하거나 여러 개의 식별자, 가짜 라우팅 정보로 악의적인 노드를 네트워크에 잠입 시키는 등의 공격 기법이 가능하다. 이러한 라우팅 공격은 동일 클래스 및 다른 클래스 간 진행하는 상호 인증절차를 통해 방지할 수 있다. 또한 공격자가 과거에 프로토콜 상에서 유출된 토큰이나 식별자, 데이터의 무결성을 제공하는 값 등을 저장해두었다가, 이후에 유효한 같은 값을 재전송하여 인증과정을 통과하는 등의 재전송 공격도 가능하다. 이는 인증 과정에서 각 노드가 매번 값을 다르게 생성하는 Nonce로 막을 수 있다.

- 키 관리 관점 분석

동일 클래스 간 인증과 다른 클래스 간 인증 과정에서 노드 간 Challenge/Response 방식으로 개체 인증을 진행할 때와 세션 키를 생성하여 안전한 세션을 맺을 때 모두 프로토콜 첫 단계에서 발견한 두 노드의 공유키를 사용한다. 하지만 암호 설계원칙에 따라 한 개의 키를 여러 목적으로 사용하는 것은 바람직하지 않기 때문에[5], 첫 단계에서 발견한 공유키를 그대로 사용하지 않는다. 인증과 키 공유 각 단계에서 생성된 Nonce와 ID 값을 키와 XOR 함으로서 키의 용도를 분리해서 사용한다.

또한 세션키 생성 과정에서 메모리 사용량을 줄이며 보유하고 있는 알고리즘을 활용할 수 있도록 세션키 생성 시 키유도함수 대신 암호화 함수로 대신한다. 인증 및 키 공유를 통해 생성된 세션키 K_{AB} 혹은 K_{UAB}의 안전성은 각 과정에서 사용한 사전 공유키 K_i에 의존한다.

V. 결론

본 논문은 RF/음파 기반 센서 네트워크를 구성하는 인프라 및 노드의 성능, 저품질 통신 환경 등을 고려하여 통신 속도가 1Kbps 미만인 제한된 노드에 적합한 인증 및 키 관리를 제안한다. 이는 센서 네트워크를 능력에 따라 계층적으로 구분하여 특정 개체에서만 적용할 수 있는 방식이 아니라 연산능력, 통신능력, 저장공간 등이 제한적인 구조에서 부분적으로 키 설립을 제공할 수 있다.

향후에는 센서 네트워크에서 새롭게 추가된 노드에 대한 확장성을 제공하는 방법과 키를 추출하는 공간인 키 풀의 크기에 대한 효율성/

안전성에 대한 trade-off를 분석해야할 것이다.

[국문 사사]

“이 논문은 2018년 해양수산부 재원으로 한국해양과학기술진흥원의 지원을 받아 수행된 연구임(수중 광역 이동통신 시스템 개발)”

[참고문헌]

[1] LoRa, https://www.lora-alliance.org/

[2] “수중음파통신 네트워크 시스템 개요 및 요구사항”, TTAK.KO-06.0352, 2013년 12월 18일

[3] 임형곤, “수중무선통신 시스템 개발사업 개요”, 한국해양연구원

[4] Hyunki Kim, Jaehoon Lee, Okyeon Yi,: “Key managements of Underwater Acoustic Communication Environments”, World Conference on Information Security Application, Agust, 2017

[5] Alfred j. Menezes, Paul C. Van Oorschot, Scoot A. Vanstone, a Handbook of Applied Cryptography(1996, pp. 582)

[6] Sunghyuck Hong, “Research on Wireless Sensor Networks Security Attack and Countermeasures: Survey”, 2014

[7] Laurent Eschenauer, “A Key-Management Scheme for Distributed Sensor Networks”, November, 2002

CAN 내부 취약점에 대한 분석 및 신규 대응방안 연구

김장훈, 한경수, 최홍석, 서정택

순천향대학교 정보보호학과

Analysis of CAN internal vulnerabilities and new countermeasures

Jang Hoon Kim, Gyeong Soo Han, Hong Seok Choi, Jung Taek Seo

Department of Information Security Engineering, Soonchunhyang University.

요 약

CAN(Controller Area Network)은 1986년 Bosch에 의해 개발된 Non-Host bus방식의 시리얼 통신 프로토콜로서 국제표준화기구에 의해 ISO11898 표준으로 규정되었다. 차량 내 센서를 제어하는 모듈인 ECU(Electronic Control Unit)는 CAN을 통해 차량의 주요동작을 제어한다. 하지만 자체보안메커니즘이 적용되지 않은 CAN은 임의의 조작에 대한 내부 취약점이 존재한다. 공격자는 OBD포트, OTA 등의 접근방법을 악용하여 CAN에 접속할 수 있다. 이를 통해 ECU간의 통신 메시지를 조작하고 CAN의 주요 기능을 제어할 수 있다. 따라서 본 논문에서는 공격자의 악의적인 메시지 조작을 막기 위한 방법으로 메시지에 MDC(Modification Detection Code)를 적용하여 무결성을 검증하는 방법을 제안한다.

I. 서론

CAN은 1986년 Bosch에 의해 개발된 Non-Host bus방식의 시리얼 통신 프로토콜로서 국제표준화기구에 의해 ISO1898표준으로 규정되었다.[1][10]

CAN은 다수의 ECU 모듈로 구성되어있으며 이를 통해 차량의 동작을 제어한다. 하지만 CAN 자체에 인증 및 엑세스 제어 등의 보안 메커니즘이 존재하지 않아 메시지의 조작여부를 파악하기 어렵다는 취약점을 가지고 있으며 이를 통해 공격자가 OBD포트 및 OTA의 동작방식을 악용하여 CAN 내부에 대한 접근 및 제어를 할 수 있게 된다.

이에 대한 해결방안으로 본 논문에서는 공격자가 CAN의 내부에 침입한 상황에서 메시지를 조작하는 것을 MDC를 이용하여 검증하기 위한 방법을 제시한다.

MDC를 이용하여 메시지의 무결성을 검증한다. 조작여부를 판별 하고 부적절한 동작실행을 방지한다.

[표 1]은 본 논문에서 사용하는 용어의 대한 정의를 정리하였다.

[표 1] 주요 용어 정의

용어	정의
CAN (Controller Area Network)	자동차 내에서 호스트 컴퓨터 없이 ECU 장치들의 통신을 위해 설계된 표준 통신 규격
ECU (Electronic Control Unit)	자동차 내부의 개별적인 전자제어장치
OBD (On-Board Diagnostics)	자동차의 전기/전자적인 작동 상태를 확인하고 제어하기 위한 규격
OTA (Over The Air)	무선 Wi-Fi나 LTE 등을 이용하여 펌웨어/소프트웨어를 업데이트하는 방식

본 논문의 Ⅱ장에서는 CAN의 정의와 동작 및 구성에 대해 설명하였고 Ⅲ장에서는 CAN의 보안 취약점에 대해 분석하였으며 Ⅳ장에서는

MDC를 이용한 신규 대응방안을 제시하였다. Ⅴ장에서는 본 논문의 결론과 향후 연구방향을 제시하고 논문을 마친다.

II. CAN(Controller Area Network)

2.1 CAN의 정의

CAN은 1986년 Bosch에 의해 개발 되었으며 ISO표준규격(ISO 11898, 1993)화 된 프로토콜이다.

CAN은 ECU간 높은 데이터 전송률과 안전성을 제공한다. 거리에 따라 최고 1Mbps의 전송률을 보이며 충돌한 메시지의 자동 재전송과 CRC(Cycle Redundancy Check)를 제공한다. 또한 오류 검출과 같은 안정성을 제공 하는 분산제어 네트워크이다[1][3][4].

2.2 CAN의 동작 및 구성

CAN은 최대 1Mbps의 다양한 전송속도를 제공하며, 토폴로지로는 버스형(bus Structure)과 스타형(star Structure)을 지원한다. 링형의 토폴로지는 한 부분의 고장이 전체 시스템에 영향을 주어 신뢰성이 떨어진다. 반면 버스형과 스타형은 한 부분의 고장이 발생하더라도 시스템 일부의 사용이 가능하기 때문에 고장의 파급효과를 최소로 줄일 수 있다.[6]

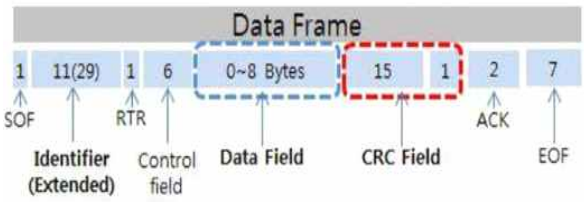
CAN은 데이터 전송을 위해 각각의 ECU노드에 대한 ID 값을 부여한다. CAN Controller는 ECU노드에서 발생하는 메시지를 ID 값을 이용한 브로드캐스팅 방식으로 전달한다. 만약 메시지 전송 오류가 발생한다면 유니캐스트 방식으로 재전송을 바로 요청한다.

ECU노드에서 발생하는 메시지의 구조는 Date 프레임, Remote 프레임 Error 프레임, Overload 프레임으로 구성된다. [표 2]는 ECU 노드에서 발생하는 메시지 구조의 각 프레임에 대한 기능을 간단히 설명 하였다[1][6].

[표 2] 메시지의 각 프레임에 대한 설명

형태	기능
Data Frame	데이터 전송
Remote Frame	데이터 프레임의 전송 요구
Error Frame	지역적으로 감지도니 에러의 전역적인 신호
Overload Frame	Data Frame/Remote Frame들의 앞뒤에서 메시지 간의 전송 간격 조절

실질적으로 ECU간의 통신은 [그림 1]과 같은 Data 프레임을 통해 이뤄진다. Data 필드에 0~8byte의 메시지를 담고 있으며 Identifier 필드의 값을 통해 수신 노드에서 수신 여부를 결정 하며 CRC 필드를 통해 오류 여부를 판별한다. 이 외 SOF(Start-of-Frame)필드와 RTR필드, Control 필드, ACK 필드, EOF 필드가 있다[1][3].



[그림 1] CAN의 Data Frame 구조

III. CAN의 보안 취약점

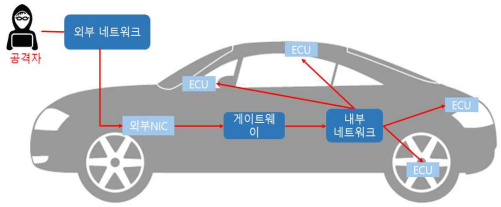
외부에서 CAN에 접근하는 방법과 이에 대한 보안 취약점은 [표 3]과 같다.

[표 3] CAN 보안 취약점

접근 방법	보안 취약점
인터넷 연결장치	인터넷 연결에 대한 CAN의 보안 메커니즘이 존재하지 않음.
OBD 포트	접속기기에 대한 인증과정 부재
OTA	소프트웨어/펌웨어 업데이트 과정에서 악성코드 주입

인터넷 연결장치를 통한 접근 방법은 CAN 내

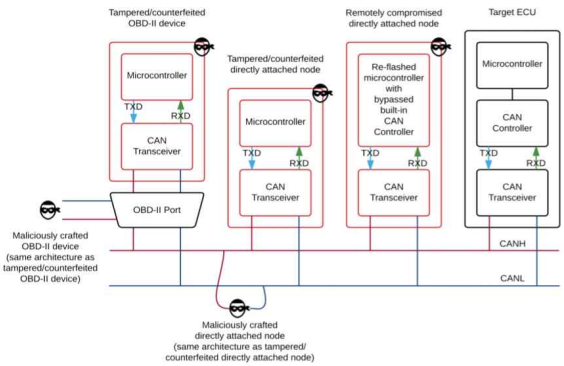
부의 보안 메커니즘의 부재로 해커가 인터넷 연결 장치를 통해 CAN에 접근하여 CAN 내부에서 발생하는 메시지에 대한 제어를 할 수 있게 되는 취약점이다.



[그림 2] 외부인터넷을 통한 공격 시나리오

해커는 차량 내 NIC와 접속을 하는 외부 네트워크를 해킹하여 CAN에 접속한다. 이후 해커는 보안 매커니즘이 없는 CAN 내부의 ECU를 조작하게 된다. 2014년 NSA해커 찰리밀러와 보안 전문회사 연구원인 크리스 발라섹은 피아트크라이슬러 그룹의 자동차인 지프체로키를 대상으로 이 취약점을 적용하였다. 이 실험에서 해커는 무선인터넷으로 연결된 환경에 접속하여 차량과 멀리 떨어진 장소에서 차량의 중요 기능을 조작했다.[7]

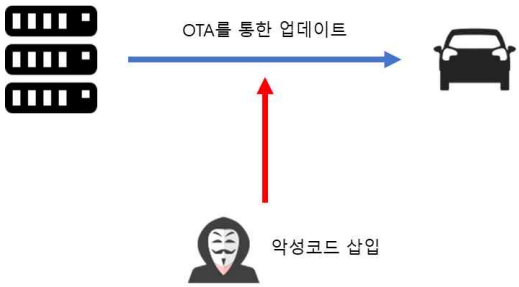
OBD 포트는 차량을 진단하기 위한 OBD장치나 승인된 스마트폰 또는 외부장치를 연결하기 위한 포트이다.



[그림 3] OBD포트를 통한 공격 시나리오

해커가 OBD포트에 접속하게 되면 OBD컨트롤노드를 제어할 수 있게 된다. 이를 통해 해커는 정상적인 메시지로 위장한 악의적인 공격을 할 수 있게 된다. 2017년 아르고스 사이버 시큐리티는 이 취약점을 통해 OBD포트에 연결된 장치를 해킹하여 차량의 중요 기능을 조작했다.[8]

OTA(Over The Air)는 차량 내부의 펌웨어나 소프트웨어를 업데이트하기 위한 방법 중 하나로 물리적인 장치를 연결하지 않고 Wi-Fi나 LTE 등의 무선으로 업데이트 하는 기술을 말한다.



[그림 4] OTA 취약점을 통한 공격 시나리오

해커는 OTA를 통한 소프트웨어/펌웨어 업데이트 과정에서 악성코드를 삽입하여 CAN에 접근한다.

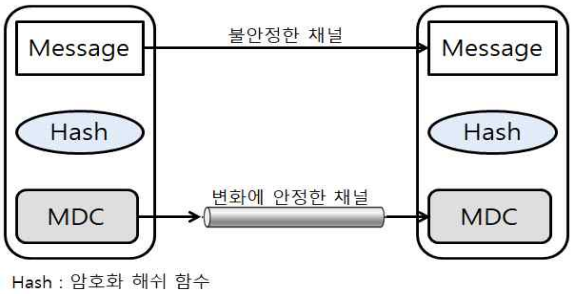
위와 같이 CAN의 다양한 보안위협이 있다. CAN의 대표적인 보안 문제는 인증 또는 접근 제어 같은 보안메커니즘이 없다는 것이다. 따라서 본 논문에서는 반복적인 오류 메시지 전송으로 인해 일어나는 공격에 대한 대응방안으로 MDC를 이용한 CAN Data Frame 무결성 검증 방법을 제안한다.

IV. MDC를 이용한 신규 대응방안 제시

4.1 MDC(Modification Detection Code)

MDC는 메시지의 무결성 즉, 메시지가 변하지 않았다는 것을 보장하는 메시지 인증 코드이다.

위의 그림은 MDC의 작동방식이다. 송신자는

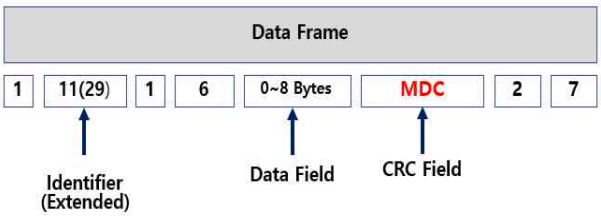


[그림 5] MDC의 작동방식

수신자에게 메시지와 메시지의 다이제스트를 수신자에게 송신 하게 된다. 수신자는 송신자로부터 받은 메시지를 해시함수를 통해 다이제스트 값을 구하여 송신자로부터 받은 메시지의 다이제스트와 비교한다. 서로의 다이제스트 값을 비교하여 값이 같을 경우 Access, 다를 경우 Inject 한다. [9]

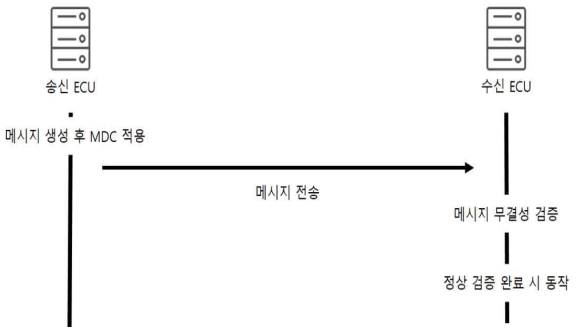
4.2 MDC를 적용한 신규 대응방안

앞서 설명한 접근방법과 취약점에 의해 공격자가 CAN의 내부에 접속하게 되면 CAN 내부의 메시지를 중간에 가로채어 조작할 수 있게 된다. 따라서 본 논문에서 제안하는 신규 대응방안은 [그림 1]에서 제시한 기존 Data Frame의 CRC필드에 MDC 기능을 추가하여 메시지 무결성 검증을 위해 사용한다.



[그림 6] MDC를 적용한 CAN Data Frame

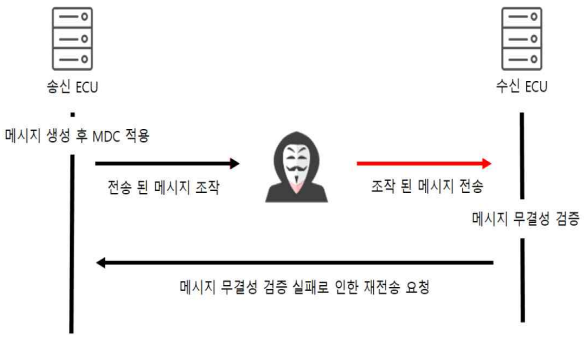
[그림 6]에서와 같이 CAN Data Frame의 CRC필드 값을 CAN Data Frame 무결성 검증을 위한 공간으로 사용한다. 기존 ECU 간의 통신 방식에는 차이가 없으나 CRC필드 값에 메시지에 대한 MDC값을 추가함으로서 서로 통신하는 메시지의 무결성을 검증 할 수 있다.



[그림 7] 정상적인 메시지의 대한 검증과정

정상적인 메시지의 대한 검증과정

① 송신ECU에서 수신ECU로 보낼 메시지를 생성 후 MDC를 적용하여 전송한다.
② 수신ECU는 받은 메시지에 대한 무결성을 검증한다.
③ 메시지의 무결성 검증이 정상적으로 완료되면 메시지에 대한 동작을 수행한다.



[그림 8] 조작된 메시지의 대한 검증 과정

조작된 메시지의 대한 검증 과정

① 송신ECU에서 수신ECU로 보낼 메시지를 생성 후 MDC를 적용 및 전송한다.
② 공격자는 중간에서 전송되는 메시지를 조작하여 수신ECU에게 조작된 메시지를 전송한다.
③ 수신ECU는 받은 메시지의 대한 무결성을 검증한다.
④ 조작된 메시지의 무결성 검증 실패로 송신ECU에게 메시지의 재전송을 요청

V. 결론 및 향후 연구방향

본 논문에서는 공격자가 CAN 내부에 침입하여 발생시키는 가짜 메시지 공격에 대한 대응

방안을 MDC를 이용하여 제안하였다. 이를 통해 공격자는 중간에 메시지를 가로채어 조작하더라도 기능과 권한에 대한 접근을 할 수 없게 된다. 하지만 공격자가 메시지를 송신하거나 수신하는 정상적인 노드를 해킹하여 메시지를 발생시킨다면 이 메시지는 정상 메시지로 인식되기 때문에 무결성 검증으로 해결할 수 없다. 따라서 향후 정상적인 메시지를 가장한 공격에 대한 연구를 할 계획이다.

본 연구는 2018년도 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 과제입니다. (No. 20162220200010)

[참고문헌]

[1] Controller Area Network (CAN) Overview - NATIONAL INSRUMENTS

http://www.ni.com/white-paper/2732/en/

[2]CAN 프로토콜 성능 해석에 관한 연구 - 홍승호, 김욱현 [1998]漢陽大學校 工學技術硏究所

[3] CAN통신의 이해 - 페스카로(FESCARO)

http://www.fescaro.com/2016/10/can-%ED%86%B5%EC%8B%A0%EC%9D%98-%EC%9D%B4%ED%95%B4/

[4] CAN (Controller Area Network) 통신 소개 및 동작 방법 - 슈어 소프트테크

https://m.blog.naver.com/suresofttech/220793847337

[5] CAN 버스 접근제한을 통한 스마트카 보안 강화 연구- 廉 升 龍(崇實大學校 情報科學大學院[2016]

[6] CAN(Controller Area Network) 분석

https://blog.naver.com/PostView.nhn?blogId=ahtz&logNo=20099345780&proxyReferer=http%3A%2F%2Fwww.google.com%2Furl%3Fsa%3Dt%26rct%3Dj%26q%3D%26esrc%3Ds%26source%3Dweb%26cd%3D5%26ved%3D0ahUKEwid_Zz88p7bAhVELpQKHfTPCoQQFgg9MAQ%26url%3Dhttp%253A%252F%252Fm.blog.naver.com%252Fahtz%252F20099345780%26usg%3DAOvVaw1RDazjo7D73XrMQXEyXQEi

[7] 보안뉴스 "자동차 해킹 늘어난다 싶더니 결국 대규모 리콜 "

http://www.boannews.com/media/view.asp?idx=47167

[8] 오토헤럴드 "해킹에 뚫린 보쉬 OBD-II동글 ,긴급 패치 배포"

http://www.autoherald.co.kr/news/articleView.html?idxno=21966

[9] MY LINE OF SIGHT, 정보보안기사 정리 2-해시함수,MDC,MAC(메세지 인증 코드)

http://vnfmsehdy.blogspot.kr/2016/06/2-mdc-mac.html

[10] INTERNATIONAL STANDARD,

ISO 11898-1 [First edition 2003]

데이터 플레인 가속화 기술을 안전하게 적용하기 위한 상용 IPsec 분석*

최준태† , 류승호, 박승윤, 사미 울라, 오희국‡

한양대학교 컴퓨터공학과

*Analyzing IPsec for Secure Application of Data Plane Acceleration Technology**

Joontae Choi† , Seungho Ryu, Seungyoon Park,
Ullah Sami, and Heekuck Oh‡

Department of Computer Science and Engineering, Hanyang University.

요 약

최근 정보 통신기술의 발전으로 인해 데이터 플레인 기술과 같은 고속화 패킷 처리 기술이 등장하였지만 충분한 안전성을 확보하지 못하고 있다. 그러므로 안전한 고속화 패킷처리를 위해 고속화 패킷처리 기술에 기존에 사용되고 있는 보안 프로토콜을 접목할 종합적인 분석이 필요하며, 연동 모델이 필요하다. 따라서 본 논문에서는 데이터 플레인 가속화 기술 중 대표적인 Intel의 DPDK와 상용 IPsec 프로그램을 분석하고 분석을 바탕으로 연동 모델을 제시한다. 제안하는 모델을 통해 IPsec과 IKE를 가속화 할 수 있을 것이며, 안전에 취약한 고속화 네트워크 패킷처리를 IPsec의 암호화와 인증 절차를 통해 더욱 안전하게 데이터를 전송할 수 있다.

I. 서론

네트워크 장비의 인터페이스 속도는 10Gbps를 넘어서 40Gbps까지 증가하였지만, 커널의 네트워크 패킷 처리 속도의 한계 때문에 그만큼 속도를 내지 못한다는 문제가 있었다. 이 문제를 해결하기 위해 데이터 플레인 가속화 기술이 등장하였지만, 기존 보안 프로토콜의 적용은 아직 해결하지 못하였다.

대표적으로 Intel DPDK의 경우 공식 홈페이지[1]에도 'DPDK is not a networking stack and does not provide functions such as Layer-3 forwarding, IPsec, firewalling, etc. '라고 명시되어있으며, IPsec 기능, 방화벽 기능을 전혀 제공하지 않는 것을 확인할 수 있다. 그러므로 빠르고 안전한 데이터 통신을 위해 보안을 고려한 데이터 플레인 가속화 기술의 연구가 필요하다.

본 논문에서는 안전한 고속 패킷 처리를 위해 위해 네트워크 패킷의 암호화 전송을 하는 IPsec 프로토콜에 대해서 논의할 것이다. 이후 데이터 플레인 가속화 기술과 IPsec과의 연동을 위한 분석에 대하여 서술하고, 분석을 바탕으로 상용 기술과 소프트웨어의 연동 모델 및 상용 기술과 리눅스 커널 IPsec 스택과의 연동 모델을 제안한다.

본 논문의 구성은 다음과 같다. 본 논문의 2장에서는 현재의 데이터 플레이 가속화 기술의 문제를 서술한다. 3장에서는 상용 IPsec 프로그램의 문제에 관해 설명한다. 4장에서는 상용 기

* 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ITCT연구센터육성지원사업의 연구결과로 수행되었음(IITP-2018-2014-1-00636)
이 논문은 2015년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2015R1D1A1A09058200)

† 주저자 : joontaechoi@hanyang.ac.kr
‡ 교신저자 : hkoh@hanyang.ac.kr

분류	저하의 원인
프로세서 및 스케쥴 관리	인터럽트 처리에서의 비효율적인 CPU 접근 과정을 통한 CPU 캐시율 저하
	인터럽트 처리를 위한 인터럽트 서비스 루틴 및 컨텍스트 스위칭
메모리 관리	커널 네트워크 스택처리의 공유 자원에서 사용하는 비효율적인 메모리 잠금 과정
	커널내부의 처리를 위한 중복적인 메모리 복사
	사용자 영역에서의 중복적인 버퍼 관리

[표 1] 커널 패키처리 과정의 저하 원인

술 및 소프트웨어 대해 분석을 하며 분석을 토대로 5장에서 데이터 플레인 가속화 기술의 안전한 통신을 위한 기법을 소개한다. 마지막으로 6장에서 논문의 결론을 맺는다.

II. 데이터 플레인 가속화 기술의 문제

네트워크 장비의 인터페이스 처리속도는 10Gbps, 40Gbps 등 크게 증가하였다. 하지만 시스템의 패킷 처리 성능은 [표 1]과 같은 이유로 네트워크 장비의 인터페이스 속도를 따라가지 못 한다. 이를 극복하기 위해서 새로운 기술들이 제안되었으며, 데이터 플레인 가속화 기술(Data Plane Acceleration, DPA)이라고 한다.

현재 OpenOnLoad, Netmap, PF_RING, DPDK, ODP(Open Data Plane)와 같은 다양한 데이터 플레인 가속화 기술들이 등장하였지만, 현재는 가장 기본적인 보안 문제도 다루지 않고 있다. [표 2]는 현존하는 데이터 플레인 기술들이 제공하는 보안 기술들을 정리하였으며, 안전성의 고려는 부족한 것을 나타낸다. 그러므로 빠르고 안전한 네트워크 통신 환경을 위하여 데이터 플레인 가속화 기술에 보안 기술을 접목할 필요가 있다.

III. 상용 IPsec 프로그램의 문제

현재 IPsec을 제공하는 소프트웨어는 많이 존재한다. 대표적으로, strongSwan, Openswan, libreswan, FreeS/WAN, SoftEhter VPN 등이 있다. 하지만 이 프로그램들의 경우 IKE를 수행하기 위해 네트워크 통신을 커널의 소켓 API를 사용하여 이루어진다. 그러므로 2장에서 기술한 커널 내부의 네트워크 지연이 발생할 수밖에 없으며, 10Gbps 이상의 속도를 낼 수 없는 문제가 존재한다.

기술	보안 기술 제공 여부	
	IPsec	방화벽
OpenOnLoad	×	×
Netmap	×	×
PF_RING	×	△
DPDK	×	×
ODP	△	○

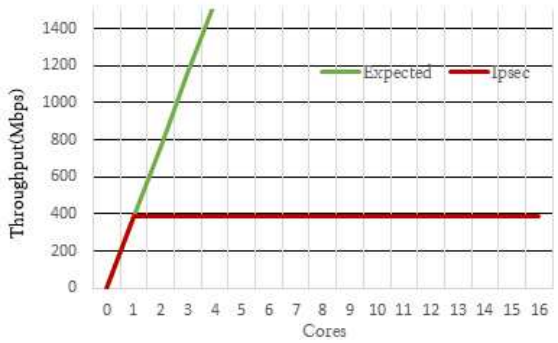
[표 2] 각 데이터 플레인 보안 기술 제공 여부

이와 더불어 재사용 공격(Replay Attack)을 방지하기 위한 패킷의 일련번호(Sequence Number) 및 패킷 검증 과정이 포함된 IPsec의 특성상 멀티 코어로 동작하지 못하는 문제가 존재한다. [그림 1]은 'secunet'에서 실험한 결과로 코어가 증가함에 따라 처리량은 선형적으로 증가하길 바라지만, 기존 IPsec 소프트웨어 및 IKE 소프트웨어의 설계상 코어의 수가 증가하여도 코어 1개의 처리량밖에 나타나지 못함을 보여준다[3].

그러므로 상용 IPsec 프로그램에서도 데이터 처리량 증가를 위한 데이터 플레인 가속화 기술의 접목이 필요하며, 멀티 코어 환경에서 그에 걸맞게 처리량이 최대한 선형적으로 증가시킬 수 있는 가속화 기법이 필요하다.

IV. 상용 기술 및 소프트웨어 분석

다양한 가속화 기술과 다양한 IPsec 소프트웨어가 존재하므로, 서로 다른 기술과 소프트웨어를 접목하게 된다면 무수히 많은 방법이 존재할 수 있다. 하지만 본 논문에서는 여러 가짓수



[그림 1] 멀티코어 환경에서의 IPsec 처리량 실험[3]

를 제외하며 개발자 및 사용자에게 가장 친숙한 각각 하나의 기술과 소프트웨어를 선정하여 분석한 내용을 바탕으로 IPsec 처리 모델링을 제시한다.

이에 따라 데이터 플레인 가속화 기술은 Intel에서 개발한 오픈 소스 DPA 기술인 DPDK 선택하였으며, IPsec/VPN 소프트웨어는 리눅스에서 가장 많이 사용하는 strongSwan을 선택하였다. 이번 절에서는 제시하는 기법의 이해를 도울 만한 각 기술 및 소프트웨어의 간략한 소개를 한다.

4.1. Intel DPDK

DPDK는 Data Plane Development Kit의 약자로 Intel 아키텍처 기반 고성능 패킷 처리 최적화를 위한 시스템 소프트웨어이다.

DPDK의 가장 큰 특징은 기존 리눅스 기반의 패킷 처리 과정과는 다르게 애플리케이션이 사용자 영역의 DPDK API와 EAL(Environment Abstraction Layer)를 통해서 통신한다는 점이다. 즉, DPDK는 커널을 통과하지 않고 직접 네트워크 인터페이스 카드에 접근할 수 있는 통로를 제공한다는 것이다. 또한, DPDK의 모든 구현은 사용자 영역에서 구현되었으며, 폴 모드 방식으로 동작, 링 라이브러리 구현, Lockless 방식의 구현 등 기존의 커널 내부의 패킷 처리 성능 저하 문제를 해결하였다.

DPDK는 멀티 코어 환경을 지원하며, 제공되는 멀티 코어 환경은 다음과 같다. 프로그램을 가장 먼저 수행하는 코어가 마스터 코어가 된다. 그 후 프로그램 시작 과정에서 인자로 받은 코어의 개수에 따라서 논리적인 슬레이브 코어를 생성하고 처리할 일을 할당하여 병렬적으로 처리할 수 있다.

4.2. strongSwan

strongSwan[2]은 리눅스 환경에서 가장 대중적으로 사용하는 IPsec/VPN 소프트웨어이다. 또한, 가장 완벽한 IPsec의 구현이다. 인증 메커니즘과 스마트카드에서의 개인키 및 인증서의 선택적 보안 저장 기능을 제공하며, IPsec 패킷 처리 및 암호화는 커널의 IPsec 스택을 사용하고, 주로 키 교환 업무(IKE)를 담당한다.

strongSwan의 동작 과정은 다음과 같다. strongSwan은 starter부터 시작되며 charon이라는 데몬을 실행시킨다. charon은 시작과정에서 필요한 플러그인들을 로드하며, 큐에 처리해야 할 작업을 삽입한다. 그 후 동작 과정에서 큐에 있는 작업을 꺼내 실행하는 구조로 되어 있다. 로드하는 플러그인들 중에 커널과 통신하는 플러그인, 키 교환하는 플러그인, 암복호화 처리하는 플러그인 등 다양한 플러그인이 존재한다.

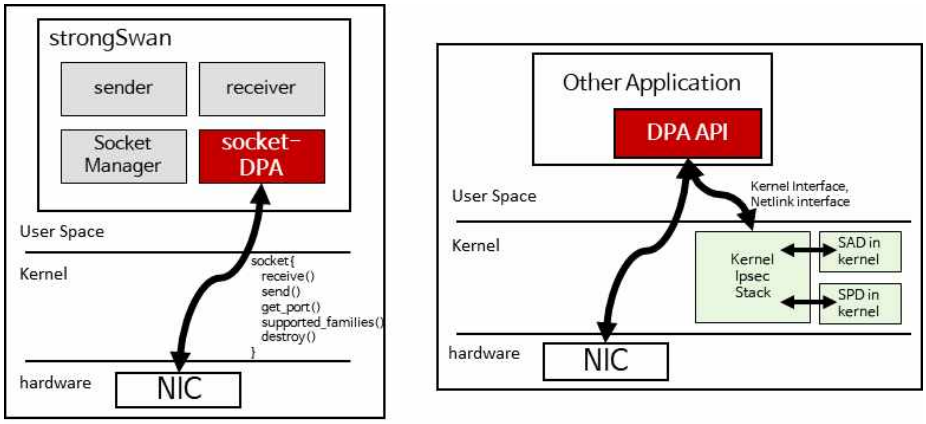
여기서 중요한 플러그인은 'socket-default' 플러그인이다. strongSwan도 네트워크 통신을 위해서 리눅스 커널의 socket API을 통해서 통신하는데 커널의 socket을 구현한 부분이 'socket-default' 플러그인이기 때문이다.

V. 데이터 플레인 가속화 기술의 안전한 통신을 위해 제안하는 기법

이번 장에서는 안전하고 보다 빠른 네트워크 패킷 처리를 위해 제안하는 기법에 관해서 설명하도록 한다.

5.1. IKE의 가속화

IKE의 가속화를 위해 DPA 기술과 상용 IPsec 프로그램인 strongSwan과의 연동 구조를 제시한다. 제시하는 기법은 비교적 간단하다. 기존의 strongSwan은 4장에서 설명한 것과 같이 socket을 사용해 네트워크와 통신을 하며 이 socket은 socket manager에 의해 관리된다. 그러므로 적



[그림 2] 제시하는 가속화 IPsec을 위한 모델

용할 DPA 기술이 socket manager에 의해 관리될 수 있도록 수정하면 된다. 이렇게 해서 설계된 모델은 [그림 2]의 왼쪽 모습과 같다.

5.2. IPsec 패킷 처리의 가속화

IPsec 패킷은 일반적으로 커널의 IPsec 스택에서 이루어진다. 리눅스 커널의 IPsec 스택은 키 교환이 이루어진 후 교환된 정보를 저장한 SAD (Security Association Database)와 SPD (Security Policy Database)의 정보를 바탕으로 IPsec 패킷 처리가 이루어진다. 리눅스 커널에서 IPsec 스택은 XFRM, NETKEY(PF_KEY) 등 다양한 종류가 있으며 커널의 모듈 형태로 구성되어 있다. 그러므로 DPA 기술을 사용하는 사용자 영역의 다른 애플리케이션은 커널 영역의 SAD와 SPD를 사용하기 위해 제공하는 인터페이스를 사용하여 연동하여야 IPsec 패킷을 처리할 수 있다. 이 내용을 바탕으로 설계한 모델은 [그림2] 의 오른쪽 모습과 같다.

VI. 결론 및 향후 연구계획

본 논문에서는 데이터 플레인 가속화 기술과 상용 IPsec을 결합하여 빠르고 안전한 데이터 통신을 위해 대표적인 기술과 소프트웨어를 분석하였다. 또한, 분석한 결과를 바탕으로 현재 데이터 플레인 가속화 기술을 실제 IPsec에 적용하였을 시 소프트웨어의 구조 변화와 동작 과정을 어떻게 다룰 것인가에 대하여 논하였다.

앞으로의 연구 계획은 상용 IPsec 프로토콜에 데이터 플레인 가속화 기술을 적용하기 위한 실제 시뮬레이션 환경을 구축할 것이며, 더욱 빠른 가속화를 위하여 IPsec 패킷을 병렬적으로 처리할 모델을 설계할 것이다. 또한, 새롭게 설계한 모델에서 발생할 수 있는 문제점이나 보안 이슈 등을 연구하고 발전시켜나갈 예정이다.

[참고문헌]

[1] https://dpdk.org/

[2] https://www.strongswan.org/

[3] Steffen Klassert, 'Parallelizing IPsec: switching SMP to 'On' is not even half the way,' secunet Security Networks AG, June 2010.

[4] Loh, Pan-Loong, Alwyn Remedios, Bob Pabla, Walter Gilmore, Wajdi Feghali, Robert Ottavi, and Bradley Burres. "IPSec acceleration using multiple micro engines." U.S. Patent Application 10/742,512, filed June 23, 2005.

[5] Cheng, Dong-Nian, Yu-Xiang Hu, and Cai-Xia Liu. "Parallel algorithm core: A novel IPSec algorithm engine for both exploiting parallelism and improving scalability." Journal of Computer Science and Technology 23, no. 5 (2008): 792-805.

2018 한국정보보호학회 하계학술대회

B3 암호이론 2

이 동 훈 (고려대학교)

- **격자 암호를 위한 HNF (Hermite Normal Form) 구현 방안 분석**
  윤혜민, 임성희, 김윤정
- **경량 블록 암호 SPECK에 대한 데이터 마스킹 기법 설계 및 구현**
  권홍필, 하재철
- **양자 알고리즘 연구 동향**
  김훈기, 이동훈
- **부채널 분석 공격에 대응하는 SIMON 암호 구현을 위한 마스킹 기법 제안**
  권홍필, 하재철
- **부채널 분석에 안전한 스칼라 곱셈 알고리즘에 대한 단일 파형 비밀 키 비트 종속 공격**
  심보연, 강준기, 한동국

격자 암호를 위한 HNF (Hermite Normal Form) 구현 방안 분석*

윤혜민 임성희 김윤정

서울여자대학교 정보보호학과

HNF (Hermite Normal Form) Implementation Strategy Analysis for Lattice Cryptography

Hyemin Yun Sunghee Lim Yoonjeong Kim

Dept. of Information Security, Seoul Women's University.

요 약

격자 기반 암호는 포스트-양자 암호의 강력한 후보자로 평가되고 있다. 정수 행렬의 Hermite Normal Form 은 격자 기반 암호의 공개키 크기를 줄이거나 격자의 고유 기저를 제공하는데 사용할 수 있다. 본 논문에서는 Hermite Normal Form을 계산하는 Tourloupis 알고리즘 2가지를 C언어로 구현한 경험을 소개한다.

Ⅰ. 서론

1.1 격자암호

양자컴퓨터의 구현 현실성이 커지면서 양자컴퓨터 도래 이후의 환경에서 안전하게 사용되는 암호에 대한 요구가 커지고 있다. 양자컴퓨팅 환경에서도 상대적으로 안전하다고 평가되는 격자 암호의 중요성이 더 커지고 있다. 격자 기반 암호 시스템은 EIGamal, RSA, ECC 등의 대수 로그 기반 시스템보다 빠르다고 평가되고 있다.

Goldreich, Goldwasser, Halevi는 공개키 암호화와 디지털 서명을 할 수 있는 트랩도어 기능인 GGH를 제안했다. 특히 GGH는 트랩 도어 기능을 구성하는 근본적인 문제로 CVP (Closest Vector Problem)을 사용했다. 이 기능은 암호화, 복호화, 디지털 서명 및 검증을 위한 시간이 모든 보안 매개 변수에서 2차적이라는 점에서 RSA, EIGamal 암호화 시스템보다 효율적이나 공개키 크기는 두 시스템보다 비효율적이다 [1].

* 본 연구는 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원(No. NRF-2016R1A2B4011984)과 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2018-2014-1-00636)

1999년에 Nguyen은 GGH에 대한 결함을 발견했다. 암호문이 정보를 누출하는 것과 암호문을 해독하는 문제로, 이를 일반적인 문제보다 더 쉽게 해결할 수 있는 가장 가까운 벡터 문제 SVP (Special Closest Vector Problem)로 줄일 수 있음을 보였다. 이 결함들로 인해 GGH를 사용하려면 보안을 위해 격자가 500보다 큰 차원으로 정의 되어야 했고, 변경한 후에도 보안성을 충족시키지 못하였다고 발표했다 [2].

1.2. AD 암호 시스템

AD 암호알고리즘은 SVP 기반으로, 키 크기와 효율성 면에서 취약하지만 Ajtai에 의해 안전성이 보통의 경우와 최악인 경우로 나뉘어 증명이 되었다. 또한, 암호화 과정이 비트단위로 이루어져 메시지 확장이 좋고, 암호문 크기는 평문 크기의 최소 100배 이상이다.

1.3. GGH 공개키 암호시스템

GGH의 공개키 시스템은 공개키 암호 기반이기 때문에 비밀키와 공개키의 쌍이 필요하다. 이 때 비밀키는 좋은 기저 (good basis)이고 공개키는 나쁜 기저 (bad basis)이다. 그림 1에서 왼쪽은 좋은

기저의 예로 2개의 벡터가 거의 직교하는 상태 이고 오른쪽은 나쁜 기저의 예로 2개의 벡터가 거의 수평인 상태이다.

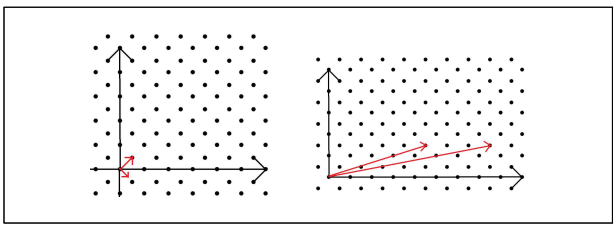


그림 1. GGH의 좋은 기저, 나쁜 기저 예

GGH는 3단계로 구성되어 있다. 설치 단계에서는 격자 L의 좋은 기저 G, 나쁜 기저 B를 계산하여 두 격자가 동일한 격자 L을 갖도록 한다. 이 때, B를 공개 기저 키, G를 개인 기저 키로 설정한다. 서명 단계에서는 G를 사용하여 벡터에 가장 가까운 벡터의 효율적인 근사치를 계산한다. 이 때 초기 벡터는 메시지이고 근사치는 서명이다. 검증 단계에서는 근사치가 격자에 걸쳐져 있는지를 B를 이용하여 확인한다.

이 시스템의 보안은 3가지로 고려해야 한다. G에서 B를 계산하는 것은 쉬우나 B에서 G를 계산하는 것은 어려워야 하고, CVP의 근사치를 G로 계산하기는 쉬우나 B로 계산하기로는 어려워야 한다. 또한 B가 존재할 때 격자에 G가 포함되어 있는지 쉽게 확인할 수 있어야 한다.

GGH 공개키 시스템에서 암호화 및 복호화 과정은 다음과 같다. 여기서, 영희가 송신자이고, 철수가 수신자이다. 먼저 영희는 키 생성 단계에서 비밀키 V={$v_1 \sim v_m$}, 정수 행렬 U, 공개키 W={$w_1 \sim w_m$}를 만든다. 이 때 $W = UV^{-1}$ 이다.

암호화 단계에서 철수는 평문 벡터 m={$x_1 \sim x_n$}과 임의 벡터 r을 이용하여 암호문 e를 만든다. 여기서, e는 $e = W \bullet m + r = w_1x_1 + \ldots + w_nx_n + r$이다.

$$m = \lfloor W^{-1} \bullet e \rceil \quad (1)$$

$$m' = U \lfloor eV^{-1} \rceil = m + U \lfloor rV^{-1} \rceil \quad (2)$$

위에서 $W = UV^{-1}$ 이므로 $W^{-1} = U^{-1}V$ 이다. 이를 이용해 식 (1) 을 계산하면 식 (2) 가 나오게 된다. 또한, V는 반드시 좋은 기저여야만 복호화가 가능하기 때문에 V는 trapdoor function이다.

1.4. Hermite Normal Form과 GGH 개선 암호 시스템

Hermite Normal Form은 보안을 손상시키지 않으면서 키 길이와 계산 시간 측면에서 격자 기반 암호 시스템의 효율성을 향상시킨다. 또한 디지털 서명 시스템에서 사용되는 경우 개인키를 복구하기 어렵고, 다이제스트를 검증하는 것도 어렵다. 2001년 Micciancio는 GGH의 속도와 보안에 대해 몇 가지 주요 개선 사항을 제안했고 특히 공개키 크기가 330KB 이하인 격자 기반 트랩 도어 기능을 구축하는 방법을 보여주었다. 그는 Hermite Normal Form 행렬을 사용해 행렬을 만들었는데, 이 행렬은 정수에 대해 감소된 단계와 유사한 상삼각 행렬이다. Hermite Normal Form은 i,j가 정수일 때, H = ($h_{i,j}$)로 표현되고, 이를 만족시키기 위해서는 3가지의 조건을 만족해야 한다. 여기서, H는 상삼각행렬을 가정한다.

1. i>j 일 때 $h_{i,j} = 0$ 이다.
2. 모든 i에 대해 $h_{i,i} > 0$ 이다.
3. i < j일 때 $0 \le h_{i,j} < h_{i,i}$ 이다.

또한 모든 정수 행렬 A와 단일 행렬 U가 있을 때 $H = A \bullet U$ 로 표시할 수 있다. HNF 행렬 H는 GGH 공개키 시스템과 유사한 디지털 서명 체계에 대한 공개키를 형성한다.

Micciancio는 GGH 공개키 시스템의 속도와 보안을 개선하기 위해 public key 크기가 330 KB 이하인 Lattice 기반 트랩도어 기능을 구축하였고 이 때 Hermite Normal Form을 사용하였다. 비밀키 R은 Lattice L(R)에서 CVP를 해결하고 메시지를 해독하게 하는 좋은 기저이다. 이 때 R에 대한 정보를 최소로 제공하기 위해 Lattice L에 대한 다른 기저인 공개키가 필요하다. 복잡한 랜덤 변환을 R에 적용하여 공개키 B를 계산하는 대신에, GGH 개선 시스템에서는 공개키 B를 R의 HNF 즉, B=HNF(R)로 설정한다. 즉 L이 B의 Lattice 도 되는 것이다. HNF(R)은 L(R)에만 의존하기 때문에 개인키 R에 대한 정보는 제공하지 않는다 [3].

Ⅱ. HNF 알고리즘 [4]

본 장에서는 Hermite Normal Form을 계산하는

Tourloupis 알고리즘 두 가지를 소개한다.

2.1. Tourloupis 알고리즘 1

정수 계수 ($a_{i,j}$)로 구성된 mxn행렬 A를 이용해 다음과 같은 알고리즘을 통해 HNF H를 구한다. 여기서 $h_{i,j}$는 H의 계수이다.

입력 : 정수 계수 ($a_{i,j}$)로 구성된 $n \times m$ 행렬 A

출력 : A의 HNF H

```
k ← 1;
for j ← 1 to n do
  // Choose Pivot
  i0←{i ∈ [k,n] : a_{i,j} = min{|a_{i,j}|: i ∈ [k,n]}};
  if i0 > k then
[1]   Exchange row A_K with row A_{i_o};
    if a_{k,j} < 0 then
      A_k ← -A_k;
    end if
  end if
  // Reduce Rows
  b ← a_{k,j};
  for i ← (k + 1) to n do
    q ← ⌊ a_{i,j}/b ⌉ ;
[2]   A_i ← A_i - q x A_k;
  end for
 k←k + 1;
end for

// Final Reductions
k ← 1;
for j ← 1 to n do
 if a_{k,j} < 0 then
    A_k ← -A_k;
 end if
 b ← a_{k,j};
 if b = 0 then
   continue;
 else
   for i ← 1 to (k - 1) do
     q ← ⌊ a_{i,j}/b ⌉ ;
   A_i ← A_i - q x A_k;
   end for
  end if
 k ← k + 1;
end for

for i ← 1 to n do
[3]  H_i ← A_i;
end for
```

Tourloupis 알고리즘 1의 진행을 예를 통해 설명하겠다. 아래와 같은 행렬 A가 있다고 가정하고 모든 행렬들의 값을 $a_{i,j}$라고 표현하자. 즉, 왼쪽 제 일 위의 값인 3은 $a_{1,1}$이라 하자.

$$A=\begin{pmatrix}3&3&1&4\\2&1&-4&-1\\1&0&19&16\\0&0&2&3\end{pmatrix}$$

[1] 첫 번째 열을 보면 $a_{1,1}$, $a_{2,1}$, $a_{3,1}$이 각 3, 2, 1이다. 즉 $a_{1,1}$이 $a_{3,1}$보다 작으므로 1행과 3행을 바꾼다.

$$A=\begin{pmatrix}1&0&19&16\\2&1&-4&-1\\3&3&1&4\\0&0&2&3\end{pmatrix}$$

[2] 첫 번째 열의 $a_{2,1}$, $a_{3,1}$값을 모두 0으로 만들고자 한다. 먼저 A 2행 - (A 1행*2) 을 계산해서 $a_{2,1}$을 0으로 만들고, A 3행 - (A 1행*3)을 계산하여 $a_{3,1}$을 0으로 만든다.

$$A=\begin{pmatrix}1&0&19&16\\0&1&-42&-33\\0&3&-56&-44\\0&0&2&3\end{pmatrix}$$

[2] 세 번째 열의 $a_{3,2}$ 값도 0으로 만들어야 하므로 (A 2행*3) - A 3행 을 계산한다.

$$A=\begin{pmatrix}1&0&19&16\\0&1&-42&-33\\0&0&70&55\\0&0&2&3\end{pmatrix}$$

[2] 네 번째 열의 $a_{4,3}$ 값도 0이어야 하므로 (A 4행 *35) - A 3행을 계산한다.

$$A=\begin{pmatrix}1&0&19&16\\0&1&-42&-33\\0&0&70&55\\0&0&0&50\end{pmatrix}$$

[3] 즉, A의 Hermite Normal Form H는 다음과 같다.

$$H=\begin{pmatrix}1&0&19&16\\0&1&-42&-33\\0&0&70&55\\0&0&0&50\end{pmatrix}$$

2.2. Tourloupis 알고리즘 2

마찬가지로 정수 계수 ($a_{i,j}$)로 구성된 mxn행렬 A를 이용해 다음과 같은 알고리즘을 통해 HNF H를 구한다. 이 때 보조 벡터 B를 사용한다.

입력 : 정수 계수 ($a_{i,j}$)로 구성된 mxn행렬 A

데이터 : 보조 벡터 B

출력 : A의 HNF H

```
[1] k ← 1;
    for j ← 1 to n do
      for i ← (k+1) to n do
       if a_{i,j} ≠ 0 then
         // Euclidean step
         Compute (d,u,v) such that
              u a_{k,j} + v a_{i,j} = d = gcd(a_{k,j}, a_{i,j});
         B ← u A_k + v A_i;
         A_i ← (a_{k,j}/d) A_i − (a_{i,j}/d) A_k;
         A_k ← B;
    end if
      end for
      k ← k+1;
    end for

[2] // Final Reductions
    k ← 1;
    for j ← 1 to n do
     if a_{k,j} < 0 then
        A_k ← -A_k;
    end if
     b ← a_{k,j};
     if b = 0 then
       continue;
     else
       for i ← 1 to (k - 1) do
         q ← ⌊ a_{i,j}/b ⌉ ;
         A_i ← A_i - q x A_k;
       end for
    end if
     k ← k + 1;
    end for

    for i ← 1 to n do
[3]   H_i ← A_i;
    end for
```

Tourloupis 알고리즘 2는 Tourloupis 1과 다르게 보조 벡터를 활용하였고 Extended euclidean 공식을 사용해서 d, u, v를 계산하였으며 Final Reduction은 알고리즘 1과 동일하다.

Tourloupis 알고리즘 2의 진행을 예를 통하여 설명하겠다.

$$A=\begin{pmatrix} 0 & -1 & 1 & 0 \\ -2 & 3 & 2 & 1 \\ -6 & -1 & -2 & 0 \\ 4 & -2 & -2 & 10 \end{pmatrix}$$

k=1, i=2, j=1일 때 Extended Euclidean 알고리즘에 따라 $ua_{1,1}+va_{2,1}=d=\gcd(a_{1,1},a_{2,1})$ 이다.

$a_{1,1}$=0,$a_{2,1}$=-2이므로 gcd 값은 2이다. 즉 d=2, u=0, v=-1이다. 이 때 B=-A_2이므로 (2,-3,-2,-1) 이다. A_2=-A_1=(0,-1,1,0)이고 A_1은 B이다.

$$A=\begin{pmatrix} -2 & 3 & 2 & 1 \\ 0 & -1 & 1 & 0 \\ -6 & -1 & -2 & 0 \\ 4 & -2 & -2 & 10 \end{pmatrix}$$

k=1, j=1, i=3일 때 위와 같이 계산하면 d=2, u=1, v=0이고, B=A_1, A_3=A_3+3A_1=(0,10,-8,-3)이다.

$$A=\begin{pmatrix} -2 & 3 & 2 & 1 \\ 0 & -1 & 1 & 0 \\ 0 & -10 & -8 & -3 \\ 4 & -2 & -2 & 10 \end{pmatrix}$$

k=1, j=1, i=4일 때 위와 같이 계산하면 d=2, u=1, v=0이고 B=A_1, $A_4=A_4-2A_1$ = (0, 4, 2, 12) 이다.

$$A=\begin{pmatrix} -2 & 3 & 2 & 1 \\ 0 & -1 & 1 & 0 \\ 0 & -10 & -8 & -3 \\ 0 & 4 & 2 & 12 \end{pmatrix}$$

여기까지가 첫 번째 루프를 돌린 결과이다.

k=2, j=2, i=3일 때

위와 같이 계산하면 d=1, u=-1, v=0이고,

$B=-A_2=(0,1,-1,0)$ 이고, $A_3=-A_3+10A_2$

$=(0,0,18,3)$ 이 된다.

$$A=\begin{pmatrix} -2 & 3 & 2 & 1 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 18 & 3 \\ 0 & 4 & 2 & 12 \end{pmatrix}$$

k=2, j=2, i=4일 때

위와 같이 계산하면, d=1, u=1, v=0이고,

$B=A_2$, $A_4=-A_4-4A_2=(0,0,6,12)$ 가 된다.

$$A=\begin{pmatrix} -2 & 3 & 2 & 1 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 18 & 3 \\ 0 & 0 & 6 & 12 \end{pmatrix}$$

여기까지가 두 번째 루프이다.

k=3, j=3, i=4일 때

위와 같이 계산하면, d=6, u=0, v=1이고,

$B = A_4$, $3A_4 - A_3 = (0,0,0,33)$ 가 된다.

$$A = \begin{pmatrix} -2 & 3 & 2 & 1 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 18 & 3 \\ 0 & 0 & 0 & 33 \end{pmatrix}$$

여기까지가 세 번째 루프이다.

마지막으로 Final Reduction을 하면 다음과 같이 H를 구할 수 있다.

$$H = \begin{pmatrix} 2 & 0 & 1 & 11 \\ 0 & 1 & 5 & 12 \\ 0 & 0 & 6 & 12 \\ 0 & 0 & 0 & 33 \end{pmatrix}$$

Ⅲ. HNF 알고리즘 구현

3-1과 3-2는 Tourloupis 알고리즘 1, 2를 코드로 구현한 것이다. 여기서는 4×4 행렬에 대하여 구현하였으며 향후 $n \times m$ 행렬로 일반화한 구현을 진행할 계획이다.

3.1. Tourloupis 알고리즘 1 구현

```
#define roundoff(x, dig) (floor((x) * pow(10, dig) + 0.5) / pow(10,dig))
 for (j = 1; j <= n; j++){
      printf("\n**j=%d started**\n", j);
      //Choose Pivot
       int min = 1000;
          for (x = k; x <= n; x++){
               if ((abs(min) > abs(matrix[x][j])) &&
              matrix[x][j] != 0){
                    min = matrix[x][j];
                    row = x;
              } // if-end
          } // for-end
          int temp = 0;
          if (row >= k){
            // Exchange
              temp = matrix[k][1];
              matrix[k][1] = matrix[row][1];
              matrix[row][1] = temp;

              temp = matrix[k][2];
              matrix[k][2] = matrix[row][2];
              matrix[row][2] = temp;

              temp = matrix[k][3];
              matrix[k][3] = matrix[row][3];
              matrix[row][3] = temp;

              temp = matrix[k][4];
              matrix[k][4] = matrix[row][4];
              matrix[row][4] = temp;
                if (matrix[k][j] < 0){
                    //A_k=-A_k
                    matrix[k][1] = (-1)*matrix[k][1];
                    matrix[k][2] = (-1)*matrix[k][2];
                    matrix[k][3] = (-1)*matrix[k][3];
                    matrix[k][4] = (-1)*matrix[k][4];
                   } // if-end
          }//if-end

          //Reduced Rows
          b = matrix[k][j];
          for (i = (k + 1); i <= n; i++){
             if (matrix[i][j] != 0){
                    if (b == 0){
                       q = roundoff(matrix[i][j], 0.1);
                       printf("\nb is zero\n");
                    }
                    else{
                       q = matrix[i][j] / b;
                    } // if else-end
                    //A_i = A_i-(q*A_k)
                    matrix[i][j] = matrix[i][j] -
                                   (q*matrix[k][j]);
                    matrix[i][j + 1] = matrix[i][j+1]
                                - (q*matrix[k][j + 1]);
                    matrix[i][j + 2] = matrix[i][j+2]
                                - (q*matrix[k][j + 2]);
                    matrix[i][j + 3] = matrix[i][j+3]
                                - (q*matrix[k][j + 3]);
                           }//if-end
                    }//for-end
                    k++;
          }for-end

//Final Reductions
 k = 1;
 for (j = 1; j <= n; j++){
  printf("\n**j=%dstarted**\n", j);
  if (matrix[k][j] < 0){
   //A_k=-A_k
   matrix[k][1] = (-1)*matrix[k][1];
   matrix[k][2] = (-1)*matrix[k][2];
   matrix[k][3] = (-1)*matrix[k][3];
   matrix[k][4] = (-1)*matrix[k][4];
  }//if-end
```

```
    printf("if start\n");
    b = matrix[k][j];
    printf("\nb=%d\n", b);
    if (b == 0){ continue;
       printf("\nb is zero\n");
     } else{
       for (i = 1; i <= (k - 1); i++){
            q = myfloor(matrix[i][j], b);
            //A_i = A_i-(q*A_k)
           matrix[i][1] = matrix[i][1] -
                          (q*matrix[k][1]);
           matrix[i][2] = matrix[i][2] -
                          (q*matrix[k][2]);
           matrix[i][3] = matrix[i][3] -
                            (q*matrix[k][3]);
           matrix[i][4] = matrix[i][4] -
                            (q*matrix[k][4]);
           printMatrix();
         } // for-end
      }//if else-end
    k++;
} //for-end
for (i = 1; i <= 4; i++){
          for (j = 1; j <= 4; j++){
          finalMatrix[i][j] = matrix[i][j];//j=1~4
          } // for-end
} // for-end
// Output
printf("\nAfter\nprinted...\n");
for (i = 1; i <= 4; i++){ // column
          for (j = 1; j <= 4; j++){ // row
                printf("%d\t", finalMatrix[i][j]);
          } // for-end
          printf("\n");
 } // for-end
 fclose(in_file);
} // for-end
```

3.2. Tourloupis 알고리즘 2 구현

```
int k = 0;
for (int j=1; j <= 4; j++) {
  printf("\n**j=%d started**\n", j);
  for (int i=k+1; j <= 4; j++) {
    printf("\n**i=%d started**\n", i);
    if (matrix[i][j] != 0) {
          int x, y;
          int d = gcd(matrix[k][j], matrix[i][j]);
          int a = duv.u;
          int b = duv.v;
          int g = gcdExtended(a,b , &x, &y);

          vector[1][j] = a*matrix[k][j] +
                                b*matrix[i][j];
          matrix[i][j] = (matrix[k][j]/d)*matrix[i]
               [j] - (matrix[i][j] / d)*matrix[k][j];
          matrix[k][j] = vector;
    } //if-end
    min = 1000;
    for (x = k; x <= n; x++){
          if ((abs(min) > abs(matrix[x][j])) &&
          matrix[x][j] != 0){
                    min = matrix[x][j];
                    row = x;
          } // if-end
     } // for-end
```

이 후는 알고리즘 1과 코드가 같다.

여기서 myfloor 함수는 소수점 이하 모든 숫자를 버리는 것이고, gcd 함수는 최대공약수를 구하는 것이며, gcdExtended 함수는 Extended Euclidean 값을 구하기 위한 것이다.

Ⅳ. 결론 및 향후 연구

본 논문에서는 포스트 양자 암호로 기대되고 있는 격자 암호에서 유용하게 사용되는 Hermite Normal Form을 구성하는 기존 알고리즘들을 살펴보고 이를 구현한 내용을 소개하였다. 향후 Hermite Normal Form을 구성하는 성능이 개선된 알고리즘의 설계 및 구현에 대하여 연구할 계획이다.

Ⅴ. 참고문헌

[1] O. Goldreich, S. Goldwasser and S. Halevi, “Public-key cryptosystems from lattice reduction problems,” Crypto’97, LNCS 1294, Springer-Verlag, pp.112 - 131, 1997.

[2] P. Nguyen, “Cryptanalysis of the Goldreich-Goldwasser-Halevi cryptosystem from Crypto’97,” Crypto’99, LNCS 1666, Springer-Verlag, 1999.

[3] Daniel Micciancio, “Improving Lattice Based Cryptosystems Using the Hermite Normal Form,” In Proc. of Cryptography and Lattices ’01, LNCS 2146, pages 126 - 145. Springer, 2001.

[4] Vasilios Evangelos Tourloupis, Hermite Normal Forms and its Cryptographic Applications, Master’s Thesis, University of WOLLONGONG, 2013.

경량 블록 암호 SPECK에 대한 데이터 마스킹 기법 설계 및 구현

권 홍 필[1], 하 재 철[1†]

[1]호서대학교

Design and Implementation of Data Masking Method on Lightweight Block Cipher SPECK

Hong-Pil Kwon, Jae-Cheol Ha[1‡]

[1]Hoseo University

요 약

SPECK은 미국 NSA가 개발한 소프트웨어 기반의 경량 암호 알고리즘이다. 그러나 SPECK 암호 알고리즘을 디바이스에 구현할 경우 전력 분석이나 전자기파 분석과 같은 부채널 공격에 취약할 수 있다. 블록 암호에 대한 부채널 공격에 대한 대응책으로 마스킹 기법이 사용되고 있으나 마스킹을 설계하는 방식과 사용하는 알고리듬에 따라 연산 성능의 차이가 발생한다. 본 논문에서는 SPECK 암호 알고리즘에 마스킹 기법을 적용하기 위한 효율적인 설계 기법을 제시한다. 그리고 기존의 마스킹 알고리듬을 적용하여 부채널 공격에 안전한 SPECK 암호 시스템을 마이크로프로세서에 구현하고 마스킹 기법간의 효율성을 비교 분석한다.

I. 서 론

최근에는 모바일 기기나 IoT 장비들은 고성능화 되면서 점점 소형화 되고 있다. 하지만 디바이스가 경량화 되는 만큼 기존에 존재하는 암호 모듈을 적용하기에는 가용 자원이 제한되기 때문에 SIMON, SPECK, LEA 등과 같은 여러 경량 암호 알고리즘들이 제안되었다[1].

이렇게 제안된 경량 암호 알고리즘들은 가용 자원의 제한이 많은 소형 디바이스에 구현해야하기 때문에 물리적 공격에 대한 취약점을 내재한 채 구현될 가능성이 높다. 특히, 알고리즘이 디바이스에서 구현되어지는 동안에 발생하는 결함을 통해 중간 계산 값을 추출하고 취합하여 비밀 키를 알아내는 부채널 공격(side channel analysis attack)에 대한 연구가 많이 진행되어 지고 있다[2]. 이러한 경량 암호 알고리즘에 대한 부채널 공격에 대응하기 위해 사용되는 방법 중 하나가 중간 값을 랜덤화하여 공격자가 올바른 중간 값을 추출할 수 없도록 하는 마스킹(masking) 기법이다.

데이터에 대한 마스킹 기법은 알고리즘 내의 연산 종류에 따라 데이터는 부울(Boolean) 마스킹 또는 산술(Arithmetic) 마스킹이 적용된다. 하지만 대부분의 암호 알고리즘에는 부울 연산과 산술 연산이 복합적으로 존재하기 때문에 마스킹 데이터에 대한 변환 과정이 필요하다. 특히, 마스킹 변환 기법에는 부울-산술(Boolean-to-Arithmetic, BtoA) 마스킹 변환 기법과 산술-부울(Arithmetic-to-Boolean, AtoB) 마스킹 변환 기법이 있다[3-4]. 이렇게 서로 다른 마스킹 기법에 대한 변환 과정을 위해서는 많은 연산과 메모리가 필요하다. 이러한 한계를 극복하기

† 교신저자, jcha@hoseo.edu

위해 최근에는 마스킹 상호 변환 과정이 없이 부울 마스킹된 데이터를 바로 산술 연산 후 다시 부울 마스킹이 적용된 데이터로 출력하는 안전 덧셈(Secure Addition, 이하 SA 기법) 기법이 제안되기도 하였다[5-6].

그러나 암호 알고리즘에 적용하는 마스킹 기법의 설계 방식과 사용하는 알고리즘에 따라 연산 성능의 차이가 발생한다. 본 논문에서는 경량 암호 알고리즘인 SPECK에 마스킹 기법을 적용하기 위한 효율적인 설계 기법을 제시한다. 그리고 기존의 마스킹 알고리즘을 적용하여 부채널 공격에 안전한 SPECK 암호 시스템을 8비트 마이크로프로세서인 ATmega128 보드에서 구현하고 마스킹 기법간의 효율성을 비교 분석한다.

II. 데이터 마스킹 기법

데이터 마스킹 기법은 블록 암호 알고리즘이 동작하는 동안 발생하는 중간 값이 공격자에 의해 노출되지 않도록 하여 공격자가 올바른 중간 값을 알아낼 수 없도록 하는 부채널 공격 대응 기법이다. 마스킹이 적용되는 대부분의 알고리즘에는 부울 연산과 산술 연산으로 구성되기 때문에 마스킹 또한 내부 연산에 따라 다르게 적용되어진다.

일반적으로 입력 x에 대한 부울 마스킹과 산술 마스킹은 다음과 같이 적용된다.

- 부울 마스킹 : $x' = x \oplus r_x$
- 산술 마스킹 : $A = x - r_x \bmod 2^m$

여기서 x는 마스킹이 적용되기 전의 원래의 값이고, r_x는 랜덤 수로 마스킹을 위해 사용하는 값이다. 또한, m은 산술 마스킹 연산에서 처리하는 데이터의 비트 길이를 의미한다.

대부분의 블록 암호 알고리즘에는 부울 연산과 산술 연산을 혼용해서 사용하기 때문에 연산에 따라 적용된 마스킹 기법을 상호 변환해 주는 과정이 필요하다. 즉, 알고리즘이 구현되는 동안 부울-산술 마스킹 변환 알고리즘과 산술-부울 마스킹 변환 알고리즘을 이용하여 중간 값에 적용된 마스킹 연산이 변환되어야 한다. 하지만 마스킹 변환 과정에서 마스킹 처리되기 전의 원래 값이 노출되게 해서는 안 된다. 예를 들어 산술 마스킹된 $x-r$값을 부울 마스킹 $x \oplus r$로 변환하는 과정에서 x가 노출되면 부채널 공격에 취약할 수 있다.

2.1. 부울-산술 마스킹 변환 기법

부울-산술 마스킹 변환 기법은 부울 마스킹이 적용된 중간 값을 산술 연산하기 위해 산술 마스킹이 적용된 값으로 변환하는 기법이다. 지금까지 부울-산술 마스킹 변환 기법 가운데 Goubin이 제안한 부울-산술 마스킹 변환 기법은 연산량이 매우 적어 효율적으로 마스킹을 변환할 수 있어 많은 암호 알고리즘에서 사용되어 지고 있다. 다음 Fig. 1은 Goubin에 의해 제안된 부울-산술 마스킹 변환 기법을 나타낸 것으로서 부울 마스킹된 값 $x' = x \oplus r$과 난수 r을 입력으로 받고, 산술 마스킹된 $A = x - r$값을 출력한다.

Input : $x' = x \oplus r$, r
Output : $A = x - r$

1. $\Gamma \leftarrow \gamma$
2. $\Gamma \leftarrow x' \oplus \Gamma$
3. $\gamma' \leftarrow \gamma' - \Gamma$
4. $\Gamma \leftarrow \Gamma \oplus x'$
5. $\Gamma \leftarrow \Gamma \oplus r$
6. $A \leftarrow x' \oplus \Gamma$
7. $A \leftarrow A - \Gamma$
8. $A \leftarrow A \oplus \Gamma$

Fig. 1. Goubin's BtoA conversion method

2.2. 산술-부울 마스킹 변환 기법

2.2.1. Goubin 산술-부울 마스킹 변환 기법

산술-부울 마스킹 변환 기법은 산술 마스킹이 적용된 중간 값을 부울 연산하기 위해 부울 마스킹이 적용된 값으로 변환하는 기법이다[3]. 다음 Fig. 2는 Goubin이 제안한 산술-부울 마스킹 변환 기법(이하 Goubin 기법)으로 입력 값 A는 평문 x와 난수 r을 산술 연산한 $x-r$이고 출력 값은 x와 난수 r을 부울 연산한 $x' = x \oplus r$이다.

2.2.2. C-T 산술-부울 마스킹 변환 기법

Coron 등은 Goubin이 제안한 산술-부울 마스킹 변환 기법의 많은 연산량에 대한 개선을 위해 룩업 테이블(look-up-table) 기반의 산술-부울 마스킹 변환 기법(이하 C-T 기법)을 제안하였다[4]. 이러한 룩업 테이블 기법을 이용하면 필요한 임시 메모리는 늘어나지만 연산 속도를 높일 수 있다.

Input : $A=x-r$, r
Output : $x'=x\oplus r$

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** $i=1$ **to** $m-1$ **do**
    $\Gamma \leftarrow T \wedge r$
    $\Gamma \leftarrow \Gamma \oplus \Omega$
    $T \leftarrow T \wedge A$
    $\Gamma \leftarrow \Gamma \oplus T$
    $T \leftarrow 2\Gamma$
    end for
12. $x' \leftarrow x' \oplus T$

Fig. 2. Goubin's AtoB conversion method

III. Secure Addition 마스킹 기법

기존의 마스킹 변환 기법을 이용해 부울 마스킹된 두 데이터를 더하기 위해서는 부울-산술 마스킹 변환, 산술 연산, 산술-부울 마스킹 변환의 3단계를 거쳐야한다. 하지만 최근 이러한 기존의 마스킹 기법의 비효율적이고 많은 연산량을 개선하기 위해 SA 기법이 제안되었다.

3.1. KRJ SA 마스킹 기법

Karroumi 등은 부울 마스킹된 두 개의 데이터를 입력받아 새로운 값으로 부울 마스킹된 덧셈 결과를 출력하는 SA 마스킹 기법(이하 KRJ 기법)을 처음으로 제안하였다[5]. KRJ SA 기법은 논리적 AND, XOR, Shift 연산과 같은 기본적인 덧셈 알고리즘에 마스킹 기법을 적용한 것으로 Fig. 3은 KRJ 마스킹 기법을 나타낸 것이다.

3.2. V-G SA 마스킹 기법

Vadnala와 Groβschdl는 KRJ 기법의 연산량을 개선하기 위해 사전 테이블을 이용한 SA 마스킹 기법(이하 V-G 기법)을 제안하였다[6]. VG 기법의 개념은 k비트 단위의 $(x\oplus s_1)+(y\oplus s_2)$ 값을 계산할 때 발생하는 캐리를 미리 계산하여 실제 마스킹 연산 단계에서 이용하는 것이다.

Input : x', y', r_x, r_y
Output : z'

1. $C=\gamma$	10. $B=\Omega \ll 1$
2. $T=x' \wedge y'$	11. $C=C \ll 1$
3. $\Omega=C \oplus T$	12. $z'=x' \oplus y'$
4. $T=x' \wedge r_y$	13. $r_z=r_x \oplus r_y$
5. $\Omega=\Omega \oplus T$	14. $T=C \wedge z'$
6. $T=y' \wedge r_x$	15. $\Omega=\Omega \oplus T$
7. $\Omega=\Omega \oplus T$	16. $T=C \wedge r_z$
8. $T=r_x \wedge r_y$	17. $\Omega=\Omega \oplus T$
9. $\Omega=\Omega \oplus T$	
18. for $i=2$ to $k-1$ do	
18.1 $T=B \wedge z'$	18.4 $B=B \oplus T$
18.2 $B=B \wedge r_z$	18.5 $B=B \ll 1$
18.3 $B=B \oplus \Omega$	
19. $z'=z' \oplus B$	20. $z'=z' \oplus C$

Fig. 3. KRJ SA masking method

IV. SPECK 알고리즘 및 적용 마스킹 기법

4.1 SPECK 알고리즘

미국 NSA에서 개발한 SPECK 알고리즘에 입력되는 워드의 길이는 16~64까지이며 블록 사이즈는 32~128까지 선택할 수 있다[1]. 또한 키 사이즈는 64~256비트까지 선택하여 사용할 수 있다. SPECK 알고리즘에서 지원하는 여러 모드가 있지만 논문에서는 $n=32$와 키 길이 128비트의 환경으로 구현하였다.

SPECK 알고리즘은 두 개의 Feistel 구조로 이루어져 있으며 Addition, Rotate, XOR 연산으로 이루어진 ARX 구조로 설계되었다. 다음 Fig. 4는 SPECK 알고리즘의 라운드 함수를 나타낸 것이다. 본 논문에서는 좌측 순환 이동 연산을 $S^n(x)$과 같이 표현하며 이것은 입력 값 x를 왼쪽으로 n번 순환 이동 연산한다는 의미이다.

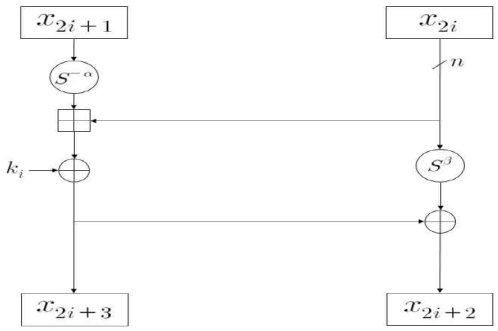


Fig. 4. SPECK round function

4.2 적용 마스킹 기법

본 논문에서는 SPECK에 여러 마스킹 기법을 적용하고 구현하여 성능을 비교하기 위해 부울-산술 상호 마스킹 변환 기법과 SA 마스킹 기법을 적용해 보고자 한다.

4.2.1 부울-산술 상호 마스킹 변환 기법 적용

다음 Fig. 5는 마스킹을 적용한 SPECK 라운드 함수에 부울-산술 상호 마스킹 변환 기법을 적용한 것이다.

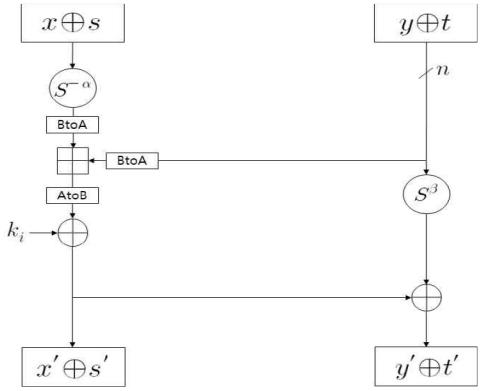


Fig. 5. SPECK round function applied with masking conversion method

위의 그림에서 왼쪽 입력 값 x의 마스킹을 위한 난수는 s이고, 오른쪽 입력 값 y의 마스킹을 위한 난수는 t로 표현하였다. 또한 라운드 함수를 통해 나온 출력 값을 각각 x', y', 그에 대한 각각의 난수를 s', t'으로 표현하였다. 먼저, 덧셈 연산을 위해 두 부울 마스킹된 입력에 대한 부울-산술 마스킹 변환(BtoA)이 필요하다. 두 변환 과정(BtoA)을 위한 입력 값에 추가 연산되는 마스킹 값은 각각 $\oplus S^{-\alpha}(s), \oplus t$이다.

그리고 부울-산술 마스킹 변환 과정 후의 출력 값의 산술 마스킹 값은 각각 $-S^{-\alpha}(s), -t$이며 덧셈 연산 후 중간 값의 산술 마스킹 값은 $-(S^{-\alpha}(s)+t)$가 된다. 덧셈 연산 후 산술-부울 마스킹 변환 과정을 통해 나온 결과 값의 마스킹 값은 $\oplus(S^{-\alpha}(s)+t)$가 되고 결국 이 값은 다음 라운드의 오른쪽 값(x')의 마스킹 값(s')이 된다. 또한 다음 라운드의 왼쪽 값(y')의 마스킹 값(t')은 $\oplus(S^{-\alpha}(s)+t)\oplus S^{\beta}(t)$가 된다. 여기서 $S^{\beta}(t)$는 $S^{\beta}(y \oplus t)$ 연산 결과로 나온 마스킹 값이다. 결과적으로 다음 라운드의 입력 값에 부울 마스킹되는 s', t'는 각각 $(S^{-\alpha}(s)+t)$, $(S^{-\alpha}(s)+t)\oplus S^{\beta}(t)$가 된다. 이러한 과정을 라운드 수만큼 반복한 후 마지막에 마스킹 값을 벗기면 중간 값이 노출되지 않고 최종 암호화된 값을 출력할 수 있다.

4.2.2 SA 마스킹 기법 적용

다음 Fig. 6은 마스킹을 적용한 SPECK 라운드 함수에 SA 마스킹 기법을 적용한 것이다.

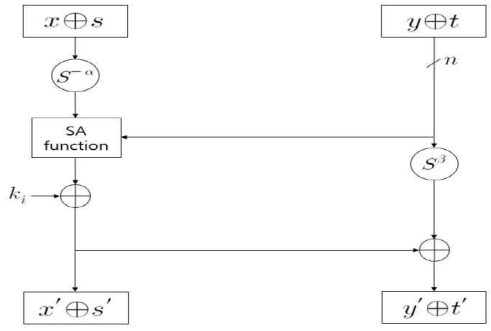


Fig. 6. SPECK round function applied with SA masking method

SA function의 두 부울 마스킹된 입력 값의 부울 마스킹 값은 각각 $\oplus S^{-\alpha}(s), \oplus t$이다. 또한 SA function을 통해 나온 중간 값의 부울 마스킹 값은 $\oplus(S^{-\alpha}(s) \oplus t)$가 되며 이 마스킹 값은 결국 다음 라운드의 오른쪽 입력 값(x')의 마스킹 값 s'가 된다. 특히, 이 시점에서 주의할 것은 SA 기법에서 s'이 부울-산술 상호 변환 기법에서의 s'과 서로 다른 값을 가진다는 점이다.

또한 다음 라운드의 왼쪽 입력 값(y')의 마스킹 값(t')은 $\oplus(S^{-\alpha}(s) \oplus t) \oplus S^{\beta}(t)$가 되며 $S^{\beta}(t)$는 $S^{\beta}(y \oplus t)$과정에서 난수 t의 결과 값이다. SA 마스킹 기법 또한 부울-산술 상호 마스킹 변환 기법과 같이 이러한 과정을 라운드 수만큼 반복하여 마지막에 마스킹 값을 벗겨 중간 값이 노출되지 않고 최종 암호 값을 출력할 수 있다.

V. 마스킹을 적용한 SPECK 구현 및 성능

본 논문에서는 기존의 마스킹 기법을 SPECK 암호 알고리즘에 적용하는 방법을 설계하였다. 설계 시 우선 고려할 것은 마스킹 값을 각 라운드마다 고정되게 사용하지 말고 그 값을 저장하여 최종 라운드까지 유지하는 것이다. 논문에서는 마스킹이 적용된 SIMON은 8비트 ATmega128 프로세서 플랫폼에서 구현하여 성능을 비교하였으며 컴파일러는 AVR Studio를 사용하였다.

마스킹이 정상적으로 설계되었는지 검증을 위해 블록 크기는 64비트, 비밀 키는 128인 SPECK 암호 알고리즘을 구현하였다. 각 마스킹 기법의 속도 측정 및 분석을 위해서 AVR Studio 컴파일러에서 제공하는 클럭 사이클 수를 측정하였다. Table 1은 각 마스킹 알고리즘을 적용하여 구현한 SPECK의 수행 속도이다.

Table 1. Performance comparison of Masking methods applied on SPECK

구분	마스킹 덧셈	테이블 사전계산	SPECK 암호
No-Masking	-	-	75,624
A2B(Goubin)	20,978	-	400,385
A2B(C-T)	5,624	19,131	249,794
SA(KRJ)	5,371	-	247,511
SA(V-G)	5,565	31,682	295,357

논문에서는 부울-산술 상호 마스킹 변환 기법으로 Goubin 기법과 C-T 기법을, SA 마스킹 기법으로 KRJ 기법과 VG기법을 SPECK 알고리즘에 적용하여 구현하였다. 실험 결과, 마스킹이 적용되지 않은 SPECK 암호 알고리즘을 수행하는데 75,624번 사이클에 해당하는 수행 시간 소요되었다. 마스킹 기법을 적용한 경우에는 동일 조건하에서 가장 빠른 것은 약 250,000번의 사이클이 소요되어 약 3.27배 정도의 추가 연산 시간만 필요하였다. 마스킹 방법 측면에서는 마스킹의 C-T 상호 변환 기법과 보다 KRJ SA 방법이 비교적 좋은 성능을 보였으나 C-T 기법은 약 256 바이트의 사전 계산 메모리가 필요하였다.

VI. 결 론

본 논문에서는 부채널 공격에 대응하는 SPECK 경량 암호 알고리즘을 구현함에 있어 마스킹 설계 기법을 제안하였다. 논문에서 설계한 마스킹 기법을 마스킹 상호 변환 알고리즘과 SA 마스킹 알고리즘을 적용하여 실제 마이크로프로세서에 SPECK을 구현한 결과, 약 3배 이상의 연산 기간과 256~512바이트 정도의 테이블 저장용 메모리 공간이 필요함을 확인하였다.

참고문헌

[1] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK Families of Lightweight Block Ciphers," Cryptology ePrint Archive, Report 2013/404, 2013.

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," CRYPTO'99, LNCS 1666, pp. 388-397, 1999

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

[4] J. Coron and A. Tchulkine, "A new algorithm for switching from arithmetic to Boolean Masking," CHES'03, LNCS 2779, pp. 89-97, 2003

[5] M. Karroumi, B. Richard, and M. Joye, "Addition with blinded operands," Constructive Side-Channel Analysis and Secure Design, COSADE'14, LNCS 8622, pp. 41-55, 2014.

[6] P. Vadnala and J. Großschadl, "Faster mask conversion with lookup tables," Constructive Side-Channel Analysis and Secure Design, COSADE'15, LNCS 9064, pp. 207-221, 2015.

양자 알고리즘 연구 동향*

김훈기[1†], 이동훈[1‡]

[1]고려대학교 정보보호대학원

A Study on Quantum Algorithms

Hunki Kim[1†], Dong Hoon Lee[1‡]

[1]Graduate School of Information Security, Korea University.

요 약

양자 컴퓨터에 관한 연구가 활발히 이루어지면서 적용 가능한 효율적인 양자 알고리즘이 제안되었다. 대표적인 알고리즘으로 1994년 Shor의 알고리즘, 1996년 Gorver의 알고리즘이 있다. 양자 컴퓨터가 현실화되면서 두 알고리즘을 통해 기존의 암호시스템 해독에 큰 영향을 미치게 되었고, 현실적으로 사용될 수 있는 연구가 이루어지고 있다. 본 논문에서는 두 알고리즘이 어떻게 기존의 암호시스템 해독에 영향을 미치는지 파악하고 양자알고리즘 연구 동향에 대해서 살펴본다.

I. 서론

최근 IBM, Intel, Google에서는 양자 컴퓨터에 관한 연구가 활발히 이루어지고 있다. 양자 컴퓨터가 현실화되면서 적용 가능한 효율적인 알고리즘들이 제안되었으며 암호 해독에 큰 영향을 미치는 알고리즘들이 존재하게 되었다.

대표적인 양자 알고리즘으로 1994년 Shor는 인수분해 문제를 다항시간에 풀 수 있는 양자 알고리즘[1]을 개발하였다. 이 알고리즘은 QFT(Quantum Fourier Transform)으로 함수의 주기를 구하고 이것을 이용하여 정수의 소인수 분해 총시간을 $O(\log^3 N)$안에 가능하도록 하는 알고리즘이다. 인수분해/이산대수 문제에 기반을 두는 공개키 암호시스템 공격에 사용할 수 있다. Shor알고리즘이 수행되기 위해서는 양자연산이 반복된다는 단점이 있지만, 2017년 Johnston등에 의해 양자연산의 반복을 피하는 연구 결과가 제시[4]되었다.

다른 대표적인 양자 알고리즘으로 1996년 Grover는 구조화되지 않은 데이터베이스에서 특정 조건을 만족하는 항목을 찾는 양자 알고리즘[2]을 개발하였다. 이 알고리즘은 정렬이 안 된 N개의 값 가운데 원하는 값을 $\sqrt{N}$번의 검색으로 찾아낼 수 있어 대칭키 암호시스템 공격에 사용할 수 있다. Gorver알고리즘은 원하는 값을 빠르게 찾을 수 있지만, 입력 Qubit수가 바뀌면 원하는 값을 찾는 확률이 변하기 때문에 응용이 제한되는 단점이 존재하였다. 이후 일정한 확률을 유지할 수 있는 연구가 이루어 졌으며 2018년 Morales등에 의해 Qubit수가 바뀌어도 일정 확률로 원하는 값을 빠르게 찾는 알고리즘[5]이 제시되었다.

이 논문에서는 암호 해독에 영향을 미치는 양자 알고리즘들과 최근동향을 살펴볼 것이며

* 본 연구는 고려대 암호기술 특화연구센터(UD170109ED)를 통한 방위사업청과 국방과학연구소의 연구비 지원으로 수행되었습니다.

† 주저자, hunki3882@korea.ac.kr

‡ 교신저자, donghlee@korea.ac.kr

본 논문의 구성은 다음과 같다. Ⅱ장에서는 양자 알고리즘의 이해에 필요한 배경지식을 설명한다. Ⅲ장에서는 대표적인 두 양자 알고리즘을 살펴본다. Ⅳ장에서는 현재 제안된 양자 알고리즘들의 연구동향에 대해 살펴본다. 마지막으로 Ⅴ장에서 결론을 맺는다.

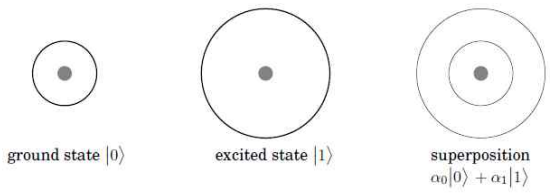
II. 배경지식

본 장에서는 양자 알고리즘을 살펴보기에 앞서 필요한 배경지식을 서술한다.

2.1 Quantum State

· Qubit

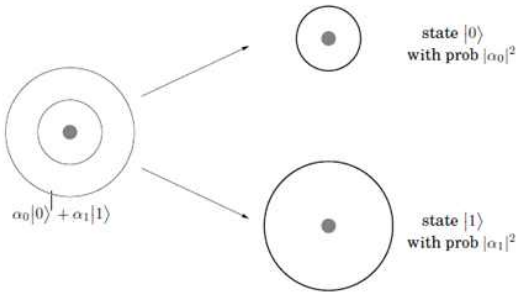
기존의 컴퓨터에서 전자는 '0' 또는 '1'의 상태를 갖는다. 반면 양자 컴퓨터에서 양자는 '0'의 상태를 가질 수도 '1'의 상태를 가질 수도 있게 된다. '0'일 때의 상태를 바닥상태라고 부르며 $|0\rangle$으로 표기한다. '1'일 때의 상태를 들뜬 상태라고 부르며 $|1\rangle$으로 표기한다. 하나의 양자가 어떤 상태인지 확인되지 않은 상태를 중첩상태라고 하며 바닥 상태와 들뜬 상태의 선형 결합으로 $\alpha_0|0\rangle+\alpha_1|1\rangle$표기한다. 이때 하나의 양자를 'Single Qubit'라고 한다.



[그림 1] Single Qubit

· Measurement (측정)

중첩상태의 qubit가 어떤 상태인지 확인하는 과정을 '측정'이라고 한다. $\alpha_0|0\rangle+\alpha_1|1\rangle$상태의 양자를 측정할 경우 $|\alpha_0|^2$의 확률로 바닥 상태($|0\rangle$)가 측정이 되고 $|\alpha_1|^2$의 확률로 들뜬 상태($|1\rangle$)가 측정된다. 두 상태가 측정될 확률의 합은 $|\alpha_0|^2+|\alpha_1|^2=1$이 된다.



[그림 2] Measurement

· Multiple Qubits

Single Qubit의 경우 '0' 또는 '1' 즉, 1bit의 정보만 저장을 할 수 있었다. Two Qubit의 경우 2bits의 정보를 저장할 수 있다. 따라서 $|\alpha\rangle=\alpha_{00}|00\rangle+\alpha_{01}|01\rangle+\alpha_{10}|10\rangle+\alpha_{11}|11\rangle$로 표기할 수 있으며 $2^2=4$개의 상태가 측정된다. Two Qubits를 측정하면 각 상태는 $|\alpha_i\alpha_j|^2$의 확률로 측정되며 $\sum_{j=0}^{1}\sum_{i=0}^{1}|\alpha_i\alpha_j|^2=1$이 된다.

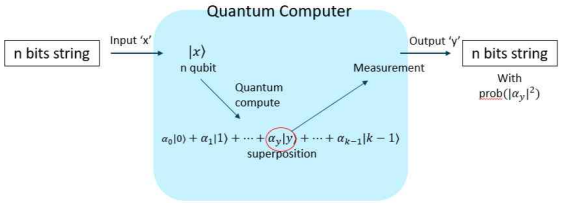
nbits의 정보를 저장하는 Multiple Qubits는 $|\alpha\rangle=\alpha_0|0\rangle+\alpha_1|1\rangle+\cdots+\alpha_{k-1}|k-1\rangle$로 표기할 수 있으며 $2^n=k$개의 상태를 갖게 된다. Multiple Qubits을 측정하면 각 상태는 $|\alpha_i|^2$의 확률로 측정되며 $\sum_{i=0}^{k-1}|\alpha_i|^2=1$이 된다.

· Entanglement (얽힘)

기존의 전자와는 다르게 양자는 '얽힘'이라는 특성을 갖는다. 서로 다른 두 개의 single Qubit $|\alpha\rangle=\alpha_0|0\rangle+\alpha_1|1\rangle$와 $|\beta\rangle=\beta_0|0\rangle+\beta_1|1\rangle$가 얽히면 two Qubits와 비슷한 형태인 $|\alpha,\beta\rangle=\alpha_0\beta_0|00\rangle+\alpha_0\beta_1|01\rangle+\alpha_1\beta_0|10\rangle+\alpha_1\beta_1|11\rangle$로 표현된다. 얽혀있는 Qubits를 측정하면 각 상태는 $|\alpha_i\beta_j|^2$의 확률로 측정되며 $\sum_{j=0}^{1}\sum_{i=0}^{1}|\alpha_i\beta_j|^2=1$이 된다. two Qubits와는 다르게 얽혀있는 Qubits의 경우 특정 Qubit의 상태를 측정할 수 있다. 나머지 Qubit은 먼저 측정한 Qubit과 관련된 상태만 측정 된다. 예를 들어 두 개의 single Qubit α,β가 얽혀있는 Qubits에서 특정 Qubit β를 측정하여 나온 상태가 1일 경우, α를 측정하면 $|01\rangle$ 또는 $|11\rangle$만 측정된다.

2.2 양자 알고리즘

양자 알고리즘에서 Quantum state의 동작 원리는 아래의 [그림3]에서 확인할 수 있다. 양자 컴퓨터는 n비트의 문자 'x'를 입력으로 받는다. 입력받은 'x'는 n Qubits, $|x\rangle$로 중첩 상태에서 양자 연산이 수행된다. 연산이 끝나면 측정을 하고 $|\alpha_y|^2$의 확률로 n비트의 문자 'y'를 출력한다. 이 과정을 양자 알고리즘이라고 한다.



[그림 3] 양자 알고리즘

III. Shor's & Grover's Algorithms

본 장에서는 기존의 암호시스템을 해독하는 데 영향을 주는 두 양자 알고리즘에 대해 살펴본다.

3.1 Shor's Algorithm [1]

Shor's Algorithm은 인수분해 문제를 다항시간 내에 풀 수 있는 양자 알고리즘이다.

- Reduction to Period-finding algorithm [3]

  홀수 'n'이 있을 때

  1. n보다 작은 x를 임의로 선택한다.

  2. $x^r \equiv 1 \bmod n$을 만족하는 주기 'r'을 구한다.

  3. 만약 r이 짝수라면 $p,q = \gcd(x^{\frac{r}{2}} \pm 1, n)$를 구한다.

  $(x^{\frac{r}{2}} - 1)(x^{\frac{r}{2}} + 1) = (x^r - 1) \bmod n \equiv 0$이기 때문에 $n = pq$가 된다. 만약 r이 홀수이거나 $x^{\frac{r}{2}} \equiv -1 \bmod n$이라면 x를 다시 뽑는다.

  따라서 $x^a \bmod n$의 주기 r을 안다면 n을 소인수분해 할 수 있음을 알 수 있다.

- Quantum Fourier Transform (QFT)

  · $M = 2^m$

  · $|\alpha\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_{M-1}|M-1\rangle$

  · 입력 : $(\alpha_0, \alpha_1, \cdots, \alpha_{M-1})$

  · 출력 : $(\beta_0, \beta_1, \cdots, \beta_{M-1})$

  · $\mathrm{QFT}(|\alpha\rangle) = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} \beta_y |y\rangle$

  양자 알고리즘 내에서 m qubits을 Fourier Transform으로 양자연산 하는 것을 QFT (Quantum Fourier Transform)이라고 한다.

  k를 주기로 l를 offset으로 갖는

  $|\alpha\rangle = \sum_{y=0}^{\frac{M}{k}-1} \sqrt{\frac{k}{M}} |j \cdot k + l\rangle$가 있을 때,

  QFT를 통해 다음과 같은 원리로 $|\alpha\rangle$의 주기를 구할 수 있다.

  1. $\mathrm{QFT}(|\alpha\rangle) = |\beta\rangle = \frac{1}{\sqrt{k}} \sum_{j=0}^{k-1} \omega^{\frac{ljM}{k}} \left| \frac{jM}{k} \right\rangle$

  2. 출력된 Qubits $|\beta\rangle$를 측정하면 $\frac{jM}{k}$ $(j = 0, \cdots, k-1)$의 값이 확률적으로 측정된다.

  3. 이를 반복하여 나온 값들의 최대공약수 $(\frac{M}{k})$가 $|\beta\rangle$의 주기가 된다.

  4. $|\beta\rangle$의 주기 $\frac{M}{k}$으로 $|\alpha\rangle$의 주기 k를 구한다.

  따라서 QFT에 주기를 갖는 Qubits를 입력으로 넣으면 출력을 통해 입력 Qubits의 주기를 알 수 있다.

- Shor's Algorithm [1]

  1. 홀수 n을 입력으로 받는다.

  2. n보다 작은 x를 임의로 선택한다. 만약 $\gcd(x,n)$이 1이라면 x를 다시 선택한다.

  3. 홀수 n을 양자 알고리즘의 입력으로 받고, $|n\rangle$을 QFT의 입력으로 하는 양자 연산을 반복 수행하여 관측된 값으로 n의 주기'r'을 찾는다.

  4. 만약 r이 홀수이거나 $x^{\frac{r}{2}} \equiv -1 \bmod n$일 경우 x를 다시 선택하고 아닐 경우

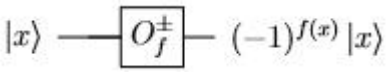
  $p,q = \gcd(x^{\frac{r}{2}} \pm 1, n)$을 출력한다.

Shor's algorithm[1]은 Quantum Fourier Transform으로 주기를 구하고, 주기를 구하면 인수분해를 할 수 있는 알고리즘을 통해 인수분해를 하였다. Quantum Fourier Transform에서 양자 연산함으로써 기존 컴퓨터에서 다항식 시간 내에 해결할 수 없던 N을 소인수분해 하는 문제를 $O(\log^3 N)$정도의 연산으로 해결할 수 있다. 따라서 Shor's algorithm[1]은 인수분해/이산대수 문제에 기반을 두는 공캐키 암호 시스템 공격에 사용 될 수 있다.

3.2 Grover's Algorithm [2]

Grover's algorithm은 구조화되지 않은 데이터베이스에서 특정 조건을 만족하는 항목을 찾는 양자 알고리즘이다. 즉, N개의 데이터베이스 $X=(x_1,x_2,\cdots,x_N)$에서 $f(x^*)=1$을 만족하는 유일한 x^*를 찾는 알고리즘 이라고 할 수 있다.

- $H^{\otimes n}$ (Hadamard) 회로
  $|\alpha\rangle=\alpha_0|0\rangle+\alpha_1|1\rangle+\cdots+\alpha_{N-1}|N-1\rangle$
  n($=\log N$) Qubits $|\alpha\rangle$를 입력으로 받으면
  $|\alpha\rangle=\frac{1}{\sqrt{N}}|0\rangle+\frac{1}{\sqrt{N}}|1\rangle+\cdots+\frac{1}{\sqrt{N}}|N-1\rangle$
  으로 일반화시킨 n Qubits을 출력한다.
- oracle $O_f^{\pm}$ 회로
  찾고자 하는 x^*의 부호를 바꿔준다.

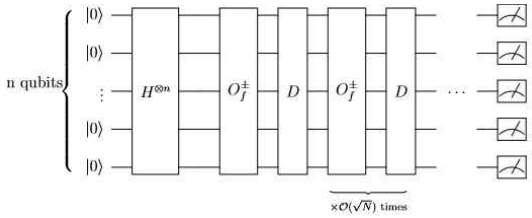


[그림 4] oracle $O_f^{\pm}$ 회로

- Grover 확산 회로
  $\sum_{x\in\{0,1\}} a_x|x\rangle \mapsto \sum_{x\in\{0,1\}^2}(2\mu-a_x)|x\rangle$
  이때 $\mu=\frac{1}{N}\sum_x a_x$이다. 즉, Grover 확산 회로는 중첩상태의 계수를 변경하는 회로이다.

Grover's algorithm[2]은 아래의 [그림5]와 같이 수행된다. 입력 qubits를 hardamad회로로 일반화를 시켜준 뒤 oracle 회로를 통해 찾고자 하는 x^*의 부호를 바꾸고, 확산 회로를 통해 계수를 확산시킨다. 두 개의 양자 회로를 $O(\sqrt{N})$만큼 반복한다. 반복 후 중첩상태의 Qubits을 측정하면 확산된 계수만큼의 높은 확률로 x^*가 측정된다.

기존 컴퓨터에서는 x^*를 찾기 위해 $O(N)$의 계산이 필요하였지만, Grover's algorithm[2]에서는 3개의 양자 회로를 사용하여 $O(\sqrt{N})$의 계산 내에 x^*를 찾을 수 있다.



[그림 5] Grover's algorithm[2]

IV. 양자 알고리즘 연구 동향

본 장에서는 양자 알고리즘의 최근 연구 동향에 대해 살펴본다.

4.1 Johnston등의 연구 [4]

Shor알고리즘이 수행되는 과정에서 만약 r이 홀수이거나 $x^{\frac{r}{2}}\equiv -1 \bmod n$일 경우 x를 다시 선택해야만 했다. x를 다시 선택하게 되면 양자연산이 반복 수행되어야 함으로 비용 낭비가 발생 할 수 있다.

2017년 Johnston등은 양자연산이 반복 수행되는 것을 방지하기 위해 만약 r이 홀수이거나 $x^{\frac{r}{2}}\equiv -1 \bmod n$일 경우에도 알고리즘이 수행 될 수 있는 알고리즘을 제시하였다. 만약 r이 홀수라면 r을 나누는 소수들(s)이 존재한다. 이를 통해 $\gcd(x^{\frac{r}{s}}-1, N)$을 구할 수 있고 이 때 출력되는 두 소수가 N의 소인수분해 값이 된다.

4.2 Morales등의 연구 [5]

Grover알고리즘은 양자연산을 반복 수행함으로서 찾고자 하는 값이 측정될 확률을 증가시킨다. 하지만 입력되는 Qubit수가 바뀌면 찾고자 하는 값이 측정될 확률이 바뀌게 된다. 2 Qubit일 때 높은 확률로 측정 되었지만, 3-4 Qubit일 때는 확률이 감소된다. Grover 알고리즘에서는 이러한 과정이

반복되게 된다.

2018년 Morales등은 oracle회로와 확산회로의 변수를 변경하여 항상 측정 확률이 떨어지지 않는 알고리즘(variational algorithm)을 제안하였다. 중첩상태의 계수가 복소수라는 점을 이용하여 두 회로를 통해 연산이 될 때 계수를 일정각도만큼 회전하여 측정확률이 떨어짐을 방지 하였으며, 두 회로의 회적 각이 같아야지만 알고리즘이 수행된다.

V. 결론

본 논문에서는 기존의 암호를 해독하는 데 영향을 주는 양자 알고리즘과 최근 연구 동향에 대해 살펴보았다. 양자 컴퓨팅 환경에서 지수연산 내에 인수분해 문제를 해결하는 Shor's algorithm [1] 은 기존의 공개키 암호시스템이 공격 될 수 있음을 보여준다. 또한, 양자 컴퓨팅 환경에서 지수연산 내에 특정 조건을 만족하는 항목을 찾을 수 Grover's algorithm [2]은 기존의 대칭키 암호시스템이 공격 될 수 있음을 보여준다.

이름	함수	기존암호	양자암호
대칭키 암호시스템			
AES-128	블록암호	128	64 (Grover)
AES-256	블록암호	256	128 (Grover)
SHA-256	해쉬함수	256	128 (Grover)
SHA-3	해쉬함수	256	128 (Grover)
공개키 암호시스템			
RSA	암호	128	broken (shor)
RSA	서명	128	broken (shor)
DH	키교환	128	broken (shor)
DSA	서명	128	broken (shor)

[표 1] 암호시스템 보안등급

[표 1]을 통해 대칭키 암호시스템의 보안등급이 2배 줄었으며, 공개키 암호시스템은 Shor's algorithm [1]으로 안전하지 않음을 확인할 수 있다.

이후 두 알고리즘의 단점을 보완하고, 효율성을 높이는 연구가 이루어지게 되었다. 2017년 Johnston 등의 연구를 통해 양자연산을 반복하지 않아 Shor 알고리즘의 효율을 높이는 연구가 이루어 졌으며, 2018년 Morales등의 연구를 통해 Qubit수와 상관없이 일정 확률로 Grover알고리즘을 수행 할 수 있는 연구가 제시되었다. 외에도 물리적으로 Qubit수를 증가하여 양자 알고리즘이 빠르게 수행되는 연구가 이루어지고 있다. 현재까지 나온 연구를 통해 양자알고리즘이 현실화되기 위해서는 알고리즘이 효율적으로 수행되는 기법들이 의미 있는 연구 주제가 될 것이다.

[참고문헌]

[1] P. W. Shor, "Algorithm for Quantum Computation: Discrete Logarithms and Factoring." in Foundations of Computer Science, pp. 124-134, 1994.

[2] L. K. Grover, "A fast quantum mechanical algorithm for database search." in Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pp. 212-219, 1996.

[3] G. L. Miller, "Riemann's hypothesis and tests for primality." in Journal of computer and system sciences 13.3, pp. 300-317, 1976.

[4] Johnston, Anna. "Shor's Algorithm and Factoring: Don't Throw Away the Odd Orders." IACR Cryptology ePrint Archive, 2017.

[5] Morales, Mauro ES, Timur Tlyachev, and Jacob Biamonte. "Variationally Learning Grover's Quantum Search Algorithm." arXiv preprint arXiv:1805.09337, 2018.

부채널 분석 공격에 대응하는 SIMON 암호 구현을 위한 마스킹 기법 제안

권 홍 필[1], 하 재 철[1†]

[1]호서대학교

Proposal of Masking Method for Block Cipher SIMON Resistant to Side Channel Analysis Attack

Hong-Pil Kwon, Jae-Cheol Ha[1‡]

[1]Hoseo University

요 약

SIMON은 미국 NSA가 개발한 하드웨어 기반의 경량 암호 알고리즘이다. 그러나 이 알고리즘도 전력 분석 공격과 같은 부채널 공격에 취약한 특성을 가지고 있다. 일반적으로 부채널 공격에 대한 대응책으로 마스킹 기법이 사용되고 있다. SIMON은 비트별 XOR, AND 그리고 좌측 순환 이동(Cyclic Shift) 연산을 주로 이용하는데 AND 연산에 대한 마스킹 처리가 쉽지 않다. 본 논문에서는 XOR 마스킹된 두 입력이 있을 때 안전하게 AND 연산을 처리하는 마스킹 기법을 제안한다. 그리고 제안된 마스킹 기법을 적용하여 부채널 공격에 안전한 마스킹 된 SIMON 암호 알고리즘을 구현한다.

I. 서 론

최근 IT 시장은 소형 모바일, IoT와 같은 경량화된 디바이스에 대한 소요가 꾸준히 증가하고 있다. 하지만 디바이스가 경량화되는 만큼 기존에 존재하는 암호 모듈을 적용하기에는 제한적이기 때문에 SIMON/SPECK과 같은 여러 경량 암호 알고리즘들이 제안되었다[1~2]

이러한 경량 암호 알고리즘들은 제한된 디바이스에 적합하게 설계되었기 때문에 물리적 취약성을 포함한 상태에서 구현될 가능성이 높다. 특히, 부채널 공격(side channel analysis attack)은 알고리즘이 디바이스에서 구현되어지는 동안에 발생하는 결함을 이용해 중간 계산 값을 추출하여 비밀 키를 알아내는 공격 방법으로서 최근 많이 연구되고 있다[3-4]. 블록 암호 알고리즘에 대한 부채널 공격이 대두됨에 따라 이를 방어하기 위한 대책으로 중간 값이 추출되지 않도록 하는 데이터 마스킹(masking) 기법을 사용하고 있다.

그러나 기존의 데이터 마스킹 기법들은 암호화에 사용된 연산이 부울(Boolean) 연산인지 산술(Arithmetic) 연산인지에 따라 각 연산에 대한 마스킹이 적용되어야 하기 때문에 마스킹 값에 대한 변환 과정이 필요하다. 이러한 마스킹 변환 기법에는 부울-산술(Boolean-to-Arithmetic) 마스킹과 산술-부울(Arithmetic-to-Boolean) 마스킹 기법이 있다[5-6]. 이러한 마스킹 상호 변환 과정을 위해서는 많은 연산량과 메모리가 필요하지만 경량화된 디바이스 환경에서는 이러한 마스킹 변환 과정을 위한 가용 자원이 부족하기 때문에 적용하기에 한계가 있다. 따라서 최근에는 이러한 마스킹의 변환과정 없이 부울 마스킹된 입력을 바로 산술 연산 후 부울 마스킹 값으로 출력하는 안전한 덧셈(Secure Addition, 이하

† 교신저자, jcha@hoseo.edu

S-ADD) 기법이 제안되기도 하였다[7].

지금까지 부울 연산은 대부분 XOR를, 그리고 산술 연산은 특정 길이에 대한 모듈러 덧셈(Addition) 연산을 가정하였다. 그러나 경량 암호 알고리즘 중 SIMON은 한 라운드 내에서 비트별 XOR, 비트별 AND 그리고 좌측 순환 이동(Cyclic Shift)을 주로 이용한다. 이 경우 비트별 AND 연산에 대한 마스킹 처리가 쉽지 않다.

본 논문에서는 XOR 마스킹된 두 입력이 있을 때 안전하게 AND 연산을 수행하는 마스킹 기법을 제안한다. 그리고 이를 적용하여 부채널 공격에 안전한 마스킹 된 SIMON 암호 알고리즘을 구현한다. 제안하는 SIMON 알고리즘은 각 라운드마다 두 번의 비트별 AND 연산의 추가만으로도 암호 중간 값에 대한 마스킹 연산을 처리할 수 있다.

II. 데이터 마스킹 상호 변환

부채널 공격을 대응하여 제안된 마스킹 기법은 블록 암호 알고리즘이 동작하는 동안 생성되는 중간 값에 랜덤한 값을 추가시켜 공격자가 올바른 중간 값을 알아낼 수 없도록 하는 기법이다. 암호 알고리즘은 대부분 부울 연산과 산술 연산으로 구성되어 있기 때문에 마스킹 또한 연산의 종류에 따라 적용되어진다. 입력 x에 대해 부울 마스킹과 산술 마스킹은 다음과 같이 표현된다.

- 부울 마스킹 : $x' = x \oplus r_x$
- 산술 마스킹 : $A = x - r_x \bmod 2^m$

여기서 x는 마스킹이 적용되기 전의 원래의 값이고, r_x는 난수로 마스킹에 적용된 값이다. 또한, m은 산술 연산에서 처리하는 데이터의 비트 크기를 의미한다.

대부분의 암호 알고리즘은 부울 연산과 산술 연산을 복합적으로 사용하기 때문에 마스킹 값을 상호 변환해 주는 과정이 필요하다. 즉, 알고리즘이 동작하는 동안 산술-부울 변환 알고리즘과 부울-산술 변환 알고리즘을 이용하여 중간 값들의 마스킹 연산이 변환되어야 한다. 단, 마스킹 값이 변환되는 과정에서 원래의 입력 값인 x값이 노출되어서는 안 된다. 예를 들어 $x-r$값을 $x \oplus r$로 변환하기 위해 $(x-r)+r \oplus r$식을 적용하면 되지만 $+r$과정에서 생성되는 중간 값이 원래 x가 되어 부채널 공격이 적용될 수 있다.

2.1 부울-산술 마스킹 변환 기법

부울-산술 마스킹 변환 기법은 부울 마스킹된 중간 값을 산술 마스킹된 값으로 변환하는 기법이다. 부울-산술 마스킹 변환 기법은 Messerges에 의해 처음 제안되었으며 그 이후 많은 마스킹 변환 기법들이 제안되었다. 그 중 Goubin에 의해 제안된 변환 기법은 연산량이 매우 적기 때문에 효율적으로 마스킹 변환 과정을 처리할 수 있어 많은 암호 알고리즘에서 사용되어지고 있다[5]. 부울-산술 마스킹 변환 기법은 부울 마스킹된 값 x'과 난수 r을 입력으로 받고, r로 산술 마스킹 된 A값을 출력한다. 다음 Fig. 1은 Goubin이 제안한 부울-산술 마스킹 변환 기법을 나타낸 것이다.

Input : $x' = x \oplus r$, r
Output : $A = x - r$

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. $A \leftarrow A \oplus T$

Fig. 1. Goubin's BtoA conversion algorithm

2.2 산술-부울 마스킹 변환 기법

산술-부울 마스킹 변환 기법은 원래 입력 값을 노출하지 않고 산술 마스킹된 중간 값을 부울 마스킹된 값으로 변환하는 알고리즘이다. Goubin이 제안한 산술-부울 마스킹 변환 기법[5]으로 입력 값 A는 평문 x와 난수 r을 산술 연산한 $x-r$이고 출력 값은 평문 x와 난수 r을 부울 연산한 $x' = x \oplus r$이다. Goubin기법 이외에도 C-T기법[6] 등 많은 산술-부울 마스킹 변환 기법들이 제안되었는데 실제 마스킹 연산량을 줄이기 위해 사전 테이블을 사용하기도 한다.

2.3 안전한 산술 덧셈 기법

부울 마스킹된 두 개의 메시지를 더하기 위해서는 부울-산술 마스킹 변환, 산술 연산, 산술-부

울 마스킹 변환의 3단계를 거쳐야 한다. 그러나 최근에는 이러한 마스킹 변환의 번거로움을 없애고 연산 속도를 개선하고자 안전한 덧셈이 제안되었다[7]. 2014년 Karroumi 등(이하 KRJ 기법)은 기존의 부울-산술 상호 마스킹 변환의 문제점을 해결하기 위해 부울 마스킹된 두 개의 메시지를 입력받아 새로운 값으로 부울 마스킹된 덧셈 결과를 출력할 수 있는 S-ADD 마스킹 기법을 처음으로 제안하였다.

Coron 등이 제안한 S-ADD 방법은 Kogge-Stone 올림수 예측 덧셈기 기반의 마스킹 기법으로서 KRJ 기법에 비해 효율적이라 할 수 있다. Vadnala와 Großschdl는 KRJ 기법을 개선하여 연산 효율성을 향상시키고자 사전 테이블을 이용한 SA 마스킹 기법을 제안하였다. VG 기법의 기본 개념은 k비트 단위의 $(x \oplus s)+(y \oplus t)$ 값을 계산할 때 발생하는 캐리를 미리 계산하여 실제 산술 연산 단계에서 이용하는 것이다.

III. SIMON 알고리즘 및 제안 마스킹 기법

3.1 SIMON 알고리즘

미국 NSA에서 개발한 SIMON 알고리즘은 하드웨어 기반의 디바이스 환경에서 구현될 수 있도록 개발된 경량 블록 암호 알고리즘이다[1]. SIMON 알고리즘의 입력 파라미터는 다양하게 적용할 수 있는데 워드의 길이가 n비트인 경우 블록 사이즈 $2n$로 나타낸다. 워드 길이는 16~64까지 이며 블록 사이즈는 32~128까지 선택할 수 있다. 그리고 키 사이즈는 64비트에서 256비트 까지 선택하여 사용할 수 있다. 본 논문에서는 $n=32$와 키 길이 128비트 SIMON을 구현하는 것으로 가정한다.

SIMON 블록 암호 알고리즘은 Feistel구조로 이루어져 있고 비트별 XOR, 비트별 AND 그리고 좌측 순환 이동(Cyclic Shift)을 통해 암호화가 이루어진다. 다음 Fig. 2는 SIMON 알고리즘의 라운드 함수를 나타낸 것이다. 본 논문에서는 좌측 순환 이동 연산을 $S^n(x)$과 같이 표기하며 이것은 입력 값 x를 왼쪽으로 n번 순환 이동 연산한다는 의미이다. 그림과 같이 2개의 워드를 입력받아 라운드 연산을 진행한다. 라운드 수는 평문의 크기와 키 사이즈에 따라 달라진다.

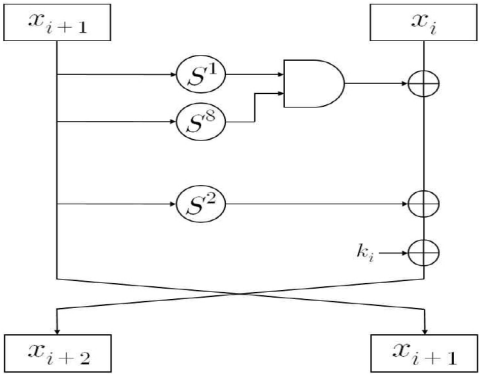


Fig. 2. SIMON round function

3.2 제안하는 마스킹 기법

SIMON 암호 알고리즘은 부채널 공격을 통해 비밀 키가 노출될 수 있는 취약점을 갖고 있다. 따라서 마스킹 기법을 적용하여 공격자가 올바른 중간 값을 획득할 수 없도록 함으로써 부채널 공격에 대응할 수 있다. SIMON 알고리즘의 라운드 함수에는 비트별 XOR와 AND 연산자가 부울 연산자로 사용되고 있다. 따라서 두 부울 연산자에 대한 상호 변환이 필요하다.

예를 들어 XOR로 마스킹 된 두 값이 AND 연산자를 통과하려면 XOR-to-AND 마스킹 변환 기법과 AND-to-XOR 상호 변환 기법이 필요하다. 즉, 일반적으로 Fig 3과 같은 상호 변환 기법을 사용하여야 한다. 그러나 이를 위해서는 별도의 XOR-to-AND 변환과 AND-to-XOR 변환 알고리즘이 개발되어야 한다.

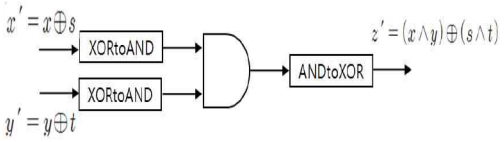


Fig. 3. General masking conversion

하지만 상기한 바와 같이 마스킹 변환 기법을 SIMON 알고리즘과 같은 경량 암호 알고리즘에 적용하면 연산량과 메모리양이 많이 늘어나 제한된 디바이스에 적용되기에 적합하지 않다. 이러한 문제점을 고려하여 본 논문은 XOR-AND 상호

마스킹 변환 과정 없이 적용되는 새로운 마스킹 기법을 SIMON 알고리즘에 적용하고자 한다.

먼저 Fig 2의 SIMON 라운드 함수의 입력이 $\hat{x}_i = x_i \oplus r$, $\hat{x}_{i+1} = x_{i+1} \oplus r$와 같이 난수 r로 마스킹 된 상태로 가정하자. 마스킹 된 값 $\hat{x}_{i+1}$은 좌측 순환 이동 S^1과 S^8을 거쳐 AND 연산을 수행하게 된다.

여기서 XOR로 마스킹된 두 값을 AND 연산한 결과를 정리하면 다음과 같다.

$$\begin{aligned} x' \wedge y' &= (x \oplus s) \wedge (y \oplus t) \\ &= (x \wedge y) \oplus (x \wedge t) \oplus (y \wedge s) \oplus (s \wedge t) \\ &= (x \wedge y) \oplus v \oplus (s \wedge t) \end{aligned}$$

단, $v = (x \wedge t) \oplus (y \wedge s)$를 의미한다. 따라서 AND 연산을 한 결과에 $(s \wedge t)$와 같은 값을 XOR 마스킹한 상태에서 출력할 수 있다. 제안하는 마스킹 기법을 도시한 것이 Fig. 4이다.

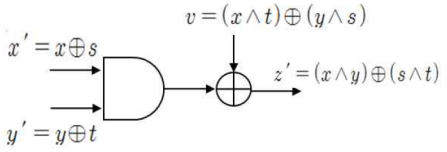


Fig. 4. Proposed masking method

따라서 AND 마스킹으로의 상화 변환과정 없이도 XOR 마스킹을 사용할 수 있게 된다. 제안하는 마스킹 기법은 입력 메시지의 노출없이 AND 연산을 수행한다는 의미에서 안전한 AND(Secure AND, 이하 S-AND) 마스킹 기법이라 할 수 있다. 이러한 원리를 바탕으로 실제 SIMON 암호 알고리즘의 마스킹을 적용한 것이 Fig. 5이다. SIMON 알고리즘의 각 라운드의 입출력 워드는 랜덤 수 r로 마스킹 되어 있다고 가정한다.

그림에서 보는 바와 같이 라운드 안의 $S^1(\hat{x}_{i+1}) \wedge S^8(\hat{x}_{i+1})$을 수행한 연산 결과에서 $v = (S^1(\hat{x}_{i+1}) \wedge S^8(r)) \oplus (S^8(\hat{x}_{i+1}) \wedge S^1(r))$를 XOR로 제거하면 $(S^1(r) \wedge S^8(r))$값만 XOR 형태로 마스킹 되어 남게 된다. 그리고 $S^2(\hat{x}_{i+1})$를 수행하게 되면 원래 $S^2(x_{i+1})$ 값에 $S^2(r)$값이 XOR 마스킹 되어 출력된다. 따라서 $(S^1(r) \wedge S^8(r))$과 $S^2(r)$를 제거하게 되면 모든 XOR 마스킹 값이 제거되고 $\hat{x}_i$에서 마스킹된 랜덤 수 r만 남게 되어 결국 라운드가 끝나는 시점의 중간 값은 모두 r로 XOR 마스킹된 상태가 된다.

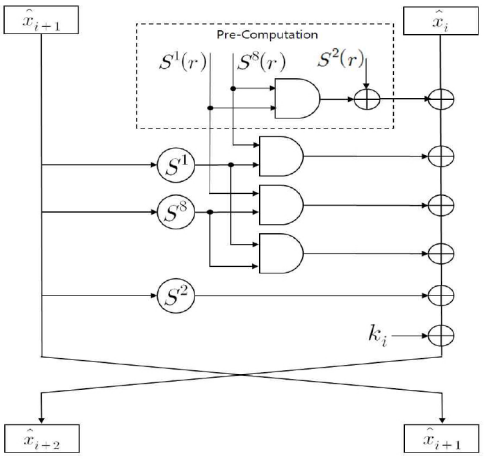


Fig. 5. SIMON round function applied with proposed masking method

특히, $(S^1(r) \wedge S^8(r))$과 $S^2(r)$는 난수 r이 정해진 상태에서는 미리 사전에 계산할 수 있어 구현 속도를 높일 수 있다. 즉, $\hat{x}_{i+1}$값에 대한 세 개의 좌측 순환 이동을 수행한 값에 랜덤 수 r을 XOR 마스킹하는 방법은 다음과 같이 정리할 수 있다.

$$\begin{aligned} & S^1(\hat{x}_{i+1}) \wedge S^8(\hat{x}_{i+1}) \oplus S^2(\hat{x}_{x+1}) \oplus r \\ &= S^1(x_{i+1} \oplus r) \wedge S^8(x_{i+1} \oplus r) \oplus S^2(x_{i+1} \oplus r) \oplus r \\ &= [S^1(x_{i+1}) \wedge S^8(x_{i+1})] \oplus [S^1(x_{i+1}) \wedge S^8(r)] \\ &\quad \oplus [S^1(r) \wedge S^8(x_{i+1})] \oplus [S^1(r) \wedge S^8(r)] \\ &\quad \oplus [S^2(x_{i+1})] \oplus S^2(r) \oplus r \\ &= [S^1(x_{i+1}) \wedge S^8(x_{i+1})] \oplus [S^2(x_{i+1})] \oplus r \\ &\quad \oplus [S^1(x_{i+1}) \wedge S^8(r)] \oplus [S^1(r) \wedge S^8(x_{i+1})] \\ &\quad \oplus [S^1(r) \wedge S^8(r)] \oplus S^2(r) \end{aligned}$$

여기서 $[S^1(x_{i+1}) \wedge S^8(r)], [S^1(r) \wedge S^8(x_{i+1})]$ 그리고 $[S^1(r) \wedge S^8(r)] \oplus S^2(r)$마스크를 XOR로 벗기면 다음과 같은 r값만 마스크 값으로 남게 된다.

$$[S^1(x_{i+1}) \wedge S^8(x_{i+1})] \oplus [S^2(x_{i+1})] \oplus r$$

IV. 제안 방식 검증 및 구현 분석

본 논문에서는 제안하는 마스킹 기법을 SIMON 암호 알고리즘에 적용하여 상용 마이크로프로세서에 구현하여 수행되는 성능을 분석하였다. 마스킹이 적용된 SIMON은 8비트 ATmega128 프로세서 플랫폼에서 구현하였으며 컴파일러는 AVR Studio를 사용하였다.

다음 Fig. 6은 ATmega128 마이크로프로세서에서 각 마스킹 기법을 구현한 실험 구성도이다. 검증을 위해 사용한 SIMON은 블록 크기는 64비트 비밀 키는 128인 암호 알고리즘을 구현하였다. 각 마스킹 기법의 속도 측정 및 분석을 위해서 AVR Studio 컴파일러에서 제공하는 클럭 사이클 수를 측정하였다.

실험 결과, 마스킹이 적용되지 않았을 경우, SIMON 암호를 수행하는데 157,491번 사이클에 해당하는 수행 시간 소요되었다. 제안하는 마스킹 기법을 적용한 경우에는 동일 조건하에서 166,305번의 사이클이 소요되어 약 5.6%정도의 추가 연산 시간만 필요하였다. 제안 마스킹 기법을 하드웨어로 구현한다 하더라도 두 번의 비트별 AND 연산과 세 번 정도의 XOR 연산을 수행(사전 계산 제외)하는 회로를 추가하면 되기 때문에 많은 추가요소 없이 구현이 가능하다.

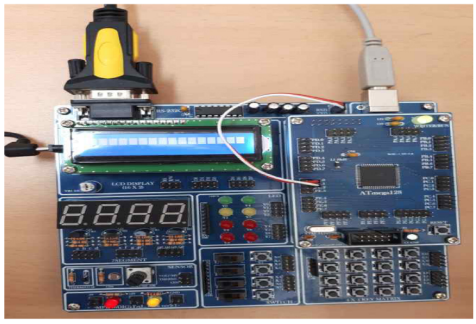


Fig. 6. ATmega128 implementation board

V. 결 론

본 논문에서는 SIMON 경량 암호 알고리즘을 구현함에 있어 부채널 공격에 대응하기 위해 사용할 수 있는 마스킹 기법을 제안하였다. 부울 연산 중 AND 연산을 비밀 값의 누설 없이 마스킹 처리할 수 있는 방법을 제안하였다. 이 방법을 SIMON에 적용하여 구현한 결과, 비교적 적은 연산량을 추가하는 것만으로도 충분히 마스킹된 상태에서 암호화 연산을 수행할 수 있음을 확인하였다.

참고문헌

[1] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK Families of Lightweight Block Ciphers," Cryptology ePrint Archive, Report 2013/404, 2013.

[2] G. Hatzivasilis, K Fysarakis, I. Papaefstathiou, and C. Manifavas, "A review of lightweight block ciphers," Journal of Cryptographic Engineering, Vol. 8, Issue 2, pp 141 - 184, 2018.

[3] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," CRYPTO'99, LNCS 1666, pp. 388-397, 1999

[4] T. Messerges, "Securing the AES finalists against power analysis attacks," FSE'00, LNCS 1978, pp. 150-164, 2001

[5] L. Goubin, "A sound method for switching between Boolean and arithmetic masking," CHES'01, LNCS 2162, pp. 3-15, 2001.

[6] J. Coron and A. Tchulkine, "A new algorithm for switching from arithmetic to Boolean Masking," CHES'03, LNCS 2779, pp. 89-97, 2003

[7] M. Karroumi, B. Richard, and M. Joye, "Addition with blinded operands," Constructive Side-Channel Analysis and Secure Design, COSADE'14, LNCS 8622, pp. 41-55, 2014.

부채널 분석에 안전한 스칼라 곱셈 알고리즘에 대한 단일 파형 비밀 키 비트 종속 공격

심보연* 강준기** 한동국*

*국민대학교 수학과, **ETRI부설 국가보안기술연구소

Key Bit-dependent Attack on Side-Channel Analysis-Resistant Scalar Multiplication Algorithm using a Single Trace

Bo-Yeon Sim*, Junki Kang**, Dong-Guk Han*

*Dept. of Mathematics, Kookmin University.

**The Affiliated Institute of ETRI.

요 약

스칼라 곱셈 알고리즘은 부채널 분석에 취약함이 보고되어 왔다. 이에 다양한 대응 기법이 연구되어 왔으나 주요 연산에 대한 대응 기법만 연구되어 왔을 뿐 비밀 키 비트 확인 단계에 대한 대응 기법은 연구되지 않았다. 이에 본 논문에서는 스칼라 곱셈 알고리즘에 대한 비밀 키 비트 종속 공격을 수행하여 전력파형으로는 100%, 전자파형으로는 98%이상의 성공률로 비밀 스칼라 비트를 찾을 수 있음을 보인다. 정교한 사전 전처리가 필요하지 않고 단일 파형만으로도 공격이 가능한 강력한 공격으로 이에 대한 대응 기법을 제시하고 이를 적용해야 함을 시사한다.

I. 서론

4차 산업 혁명을 이끄는 새로운 기술로 각광받고 있는 블록체인 및 FIDO(Fast Identity Online)는 ECDSA 알고리즘을 활용하여 사용자를 인증한다. 그러나 ECDSA의 주요 연산인 스칼라 곱셈 알고리즘은 부채널 분석에 취약하다.

따라서 다양한 부채널 대응 기법이 연구되어 왔으나, 주로 데이터 종속 분기 유형, 중간 값에 따른 통계 특성 또는 데이터 간의 상호 관계 기반 공격에 대한 대응 기법만 연구되어 왔을 뿐 비밀 키 비트 확인 단계에 대한 대응기법의 연구는 이루어지지 않았다. 비밀 키 비트 확인 단계에서는 비밀 키 비트 값이 추출되어 변수에 저장되기 때문에 취약점이 존재한다는 것이 밝혀지면 비밀 키가 노출될 수 있다.

이에 본 논문에서는 스칼라 곱셈 알고리즘에 대한 비밀 키 비트 종속 공격을 수행하여 취약함을 보이고 이에 대응할 수 있는 대응 기법을 제시한다.

II. 비밀 키 비트 종속 공격

2.1 비밀 키 비트 확인 단계

스칼라 곱셈 알고리즘은 [그림 1]과 같이 비밀 스칼라 비트 k_i값에 따라 동작이 결정되는 반복 연산으로 구성되어 있다. 따라서 각 반복 연산 시작 시에는 k_i값이 무엇인지 확인하는 단계가 있다. 즉, n비트열 스칼라 k로부터 i번째 비트인 k_i를 추출하여 해당 변수에 저장한다. 본 논문에서는 이 단계를 키 비트 확인 단계라고 정의한다.

2.2 비밀 키 비트 종속 특성

스칼라 곱셈 알고리즘의 키 비트 확인 단계에서는 n비트열 스칼라 $k=(k_{n-1},\cdots,k_0)_2$에서 i번째 비트인 k_i를 추출하여 해당 변수에 저장한다. 따라서 비밀 키 비트 확인 단계에서 소모되는 전력과 방출되는 전자파는 k_i 값과 연관되어 있다.

Left to Right

Input : $P=(x,y)$ a point on $\boldsymbol{EC}$,
an n-bit key $k=(k_{n-1},\cdots,k_0)_2$
Output : $Q=kP$

1: $R_0 \leftarrow \infty$, $R_1 \leftarrow P$
2: **for** $i=n-1$ down to 0 **do**
3: $R_{1-k_i} \leftarrow R_{k_i}+R_{1-k_i}$
4: $R_{k_i} \leftarrow 2R_{k_i}$
5: **end for**
6: **Return** R_0

Right to Left

Input : $P=(x,y)$ a point on $\boldsymbol{EC}$,
an n-bit key $k=(k_{n-1},\cdots,k_0)_2$
Output : $Q=kP$

1: $R_0 \leftarrow \infty$, $R_1 \leftarrow P$, $R_2 \leftarrow P$
2: **for** $i=0$ up to $n-1$ **do**
3: $R_{1-k_i} \leftarrow R_{1-k_i}+R_2$
4: $R_2 \leftarrow R_0+R_1$
5: **end for**
6: **Return** R_0

[그림 1] 단순 전력 분석에 안전한 규칙적인(Regular) 스칼라 곱셈 알고리즘

스칼라 곱셈 알고리즘에 대한 단순 전력 분석(또는 단순 전자파 분석)은 가장 기본적인 부채널 공격으로 대응 기법의 적용이 필수적이다. 따라서 [그림 1]과 같이 k_i값에 상관없이 항상 동일한 연산을 수행하여 단순 전력 분석에 안전하게 설계된 규칙적인(Regular) 스칼라 곱셈 알고리즘이 주로 사용된다. 하지만, 단계 3, 4 연산 수행 시 참조되는 레지스터의 주솟값이 k_i 값에 따라 결정되며, 이때 소모되는 전력과 방출되는 전자파는 참조되는 레지스터 주솟값과 연관되어 있다. 즉, k_i값에 종속된 전력이 소모되고 전자파가 방출된다.

특히 하드웨어로 구현된 암호 알고리즘의 경우, 연산이 병렬적으로 수행되기 때문에 비밀 키 비트 확인 단계에서 k_i값이 결정됨과 동시에 참조되는 레지스터의 주소가 결정된다. 따라서 비밀 키 비트 확인 단계에서 소모되는 전력과 방출되는 전자파는 k_i값뿐만 아니라 k_i값에 따라 참조되는 레지스터 주솟값과 연관된다.

하드웨어로 구현된 암호 알고리즘의 경우 전력 소비 모델(또는 전자파 방출 모델)이 주로 헤밍 디스턴스(HD, Hamming Distacne) 정보에 의존한다. 따라서 비밀 키 비트 확인 단계에서의 비밀 키 비트 종속 특성을 정리하면 [특성 1], [특성 2]와 같다.

[특성 1] 하드웨어로 구현된 스칼라 곱셈 알고리즘의 키 비트 확인 단계에서 소비되는 전력과 방출되는 전자파는 k_{i+1}과 k_i의 헤밍 디스턴스 정보에 의존한다. 즉, 만약 $k_{i+1}=k_i$이면 $k_{i+1}\oplus k_i=0$과 연관된 전력 소비와 전자파 방출이 발생한다. 그리고 만약 $k_{i+1}\neq k_i$이면 $k_{i+1}\oplus k_i=1$과 연관된 전력 소비와 전자파 방출이 발생한다. $(0\le i\le n-2)$

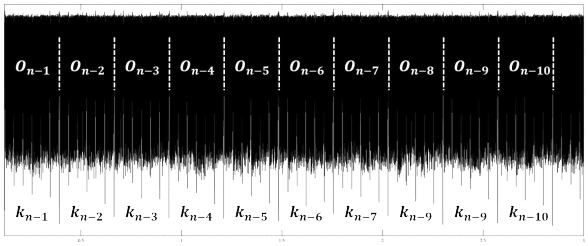
[특성 2] 하드웨어로 구현된 규칙적인(Regualr) 스칼라 곱셈 알고리즘의 키 비트 확인 단계에서 소비되는 전력과 방출되는 전자파는 k_{i+1}과 k_i의 헤밍 디스턴스 정보 뿐만 아니라 k_{i+1}과 k_i의 값에 따라 결정되는 레지스터 주솟값 $RegAddr_{k_{i+1}}$과 $RegAddr_{k_i}$의 헤밍 디스턴스 정보에도 의존한다. 즉, 만약 $k_{i+1}=k_i$이면 소비되는 전력과 방출되는 전자파는 $k_{i+1}\oplus k_i=0$, $RegAddr_{k_{i+1}}\oplus RegAddr_{k_i}=0$와 연관된다. 만약 $k_{i+1}\neq k_i$이면 $k_{i+1}\oplus k_i=1$, $RegAddr_{k_{i+1}}\oplus RegAddr_{k_i}\neq 0$과 연관된 전력 소비와 전자파가 방출된다. $(0\le i\le n-2)$

2.3 단일 파형 비밀 키 비트 종속 공격

본 논문에서는 차분 전력 분석 대응 기법으로 중간 값 랜덤화 기법이 적용된 규칙적인 스칼라 곱셈 알고리즘을 대상으로 한다. 따라서 공격자는 단일 파형을 이용한 비밀 키 비트 종속 공격을 수행해야 한다고 가정한다. 더불어 공격자는 수집된 파형에서 각 반복 연산을 식

별할 수 있다고 가정한다. 공격 단계는 다음 4단계로 구성되어 있다.

(전처리) 첫째, 스칼라 곱셈 알고리즘이 1회 수행되는 동안 수집한 파형을 T라고 했을 때, 이를 각 반복 연산에 해당하는 하위 파형 O_i로 나눈다. $(0 \le i \le n-1)$ 즉, T를 [그림 2]와 같이 n개의 하위 파형 $T = \{O_{n-1} \| O_{n-2} \| \cdots \| O_0\}$으로 나눈다. 그리고 n개 하위 파형의 정렬을 맞춘다.



[그림 2] 10회 수행된 반복 연산에 대한 전력파형

(공격 지점 선택) 만약 공격 대상 장비와 동일한 장비를 사용할 수 있다면, 알려진 입력 값에 대한 파형을 수집한 후 n개의 하위 파형 O_i에 대한 SOST(Sum Of Squared pairwise T-differences) 값을 계산하여 값이 가장 높은 위치를 공격 지점으로 쉽게 선택할 수 있다. 두 개의 그룹 G_1, G_2에 대한 SOST 값 계산 수식은 아래와 같다.

$$SOST = \left(\frac{E[G_1] - E[G_2]}{\sqrt{\frac{\sigma_{G_1}^2}{n_{G_1}} + \frac{\sigma_{G_2}^2}{n_{G_2}}}} \right)^2$$

(E는 평균, σ는 표준편차, n은 원소 개수)

만약 공격 대상 장비와 동일한 장비를 사용할 수 없다면, 대상 알고리즘이 어떻게 구현되어 있는지를 알아야 한다. 그리고 장비의 동작 주파수를 확인하여 비밀 키 비트 연산이 수행되는 클럭 위치를 공격 지점으로 선택한다. 일반적으로 비밀 키 비트 확인 연산은 각 하위 파형 O_i의 시작 클럭 인근에 위치한다.

(두 집합으로 분류 및 비밀 키 추출) 단순 전력 분석 또는 K-평균 군집화(K-means Clustering), 퍼지 K-평균 군집화(fuzzy K-means Clustering), EM(Expectation Maximization) 등과 같은 군집 알고리즘을 이용하여 n개의 하위 파형의 공격 지점 p_i를 두 개의 그룹 G_1, G_2로 나눈다. $(0 \le i \le n-1)$ G_1에 속한 p_i는 $k_{i+1} = k_i$일 때, 즉, 0과 연관된 누출이 발생하는 파형이고, G_2에 속한 p_i는 $k_{i+1} \neq k_i$일 때, 즉, 0이 아닌 값과 관련된 누출이 발생하는 파형이라고 가정한다. 그리고 비밀 키 k의 최상위 비트 값 k_{n-1}는 항상 1인 사실과 p_i가 속해있는 집합을 기준으로 k_i값을 찾을 수 있다. $(0 \le i \le n-2)$ 만약 G_1에 속한 p_i를 $k_{i+1} \neq k_i$, G_2에 속한 p_i를 $k_{i+1} = k_i$에 대한 파형이라고 가정할 때 앞서 찾은 비밀 키 비트열과 반전된 결과의 비트열을 얻을 수 있다. 즉, 후보 키는 총 2개로 입출력 값 확인을 통해 비밀 키를 찾을 수 있다.

III. 단일 파형을 이용한 비밀 키 비트 종속 공격 실험 결과

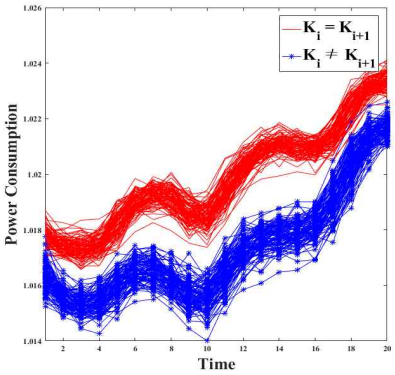
3.1 실험 환경

본 논문에서는 차분 전력 분석 대응기법으로 스칼라 랜덤화 기법이 적용된 Montgomery-López-Dahab ladder 스칼라 곱셈 알고리즘을 대상으로 한다. 따라서 공격자는 단일 파형을 이용한 공격을 수행해야 한다고 가정한다. 비밀 키 비트는 224비트이며, 부채널 분석 검증 보드로는 SASEBO-GII FPGA 보드를 이용하여 2.5 GS/s으로 전력 및 전자파형을 수집하였다. 전자파형 수집 시 사용한 프로브는 총 3종류로 Langer RF-U 5-2, LF-R 400과 Rohde & Schwarz RS-H 50-1이다.

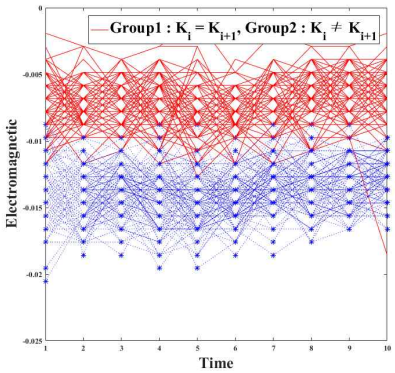
3.2 실험 결과

전력파형의 경우 [그림 3]과 같이 육안으로 쉽게 구분이 가능한 정보량이 존재한다. 따라서 단순 전력 분석을 통해 100%의 성공률로 비밀 스칼라 비트를 추출할 수 있었다.

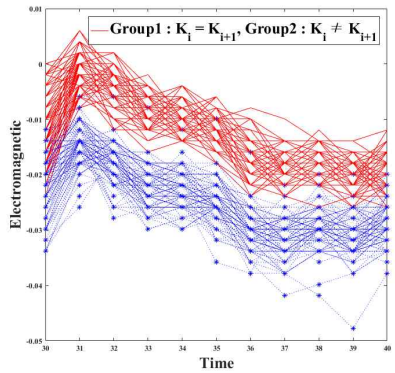
전자파형의 경우 전력파형과 달리 두 집합의 분포가 겹치기 때문에 군집 알고리즘을 적용하여 두 집합으로 분류하였다. K-평균 군집화 알



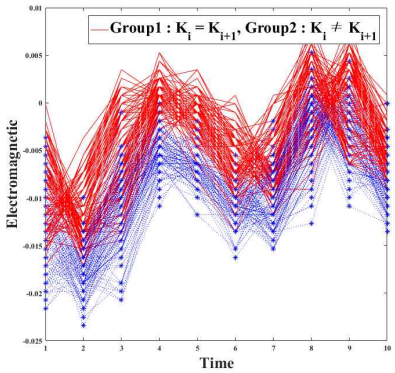
[그림 3] 전력파형



[그림 4] 전자파형 (RF-U 5-2)



[그림 5] 전자파형 (LF-R 400)



[그림 6] 전자파형 (RS-H 50-1)

고리즘을 적용하였을 때, 각각 98.45%, 99.50%, 99.32%의 성공률로 비밀 스칼라 비트를 추출할 수 있었다.

IV. 단일 파형을 이용한 비밀 키 비트 종속 공격 대응 기법

본 논문에서는 단일 파형을 이용한 비밀 키 비트 종속 공격 대응 기법으로 비밀 키 비트 확인 연산이 수행되기 전에 k_i 변수를 랜덤 값으로 초기화 하는 방법을 제안한다. 이는 k_{i+1}와 k_i 사이의 연관성을 제거 가능하며, 실험에 따르면 50%의 성공 확률로 비밀 스칼라 비트를 1/2의 확률로 랜덤하게 추정한 것과 동일하다.

V. 결론

본 논문에서 제시하는 비밀 키 비트 종속 공격은 단일 파형을 이용하여 공격이 가능하며, 정교한 사전 전처리 없이 전력파형의 경우 100%, 전자파형의 경우 98%이상의 성공률로 비밀 스칼라 비트를 추출할 수 있다. 이는 일반적으로 정교한 전처리 및 다중 파형을 필요로 했던 이전의 공격에 비해 상당한 이점을 보여준다. 또한 기존의 부채널 대응기법을 무력화 시킬 수 있는 강력한 공격으로, 본 논문에서는 ECC 스칼라 곱셈 알고리즘에 초점을 맞추었지만 RSA 모듈러 지수승 알고리즘에도 적용이 가능하다. 따라서 이에 대응할 수 있는 대응기법의 적용이 필수적이다.

[사사] "본 연구는 고려대 암호기술 특화연구센터(UD170109ED)를 통한 방위사업청과 국방과학연구소의 연구비 지원으로 수행되었습니다."

[참고문헌]

[1] B.-Y. Sim and D.-G. Han, Key Bit-Dependent Attack on Protected PKC Using a Single Trace, ISPEC 2017, LNCS 10701, pp. 168-185, December, 2017.

[2] D. Hankerson, A. Menezes, and S. Vanstone: Guide to Elliptic Curve Cryptography, Springer, ISBN 0-387-95273-X, 2003.

2018 한국정보보호학회 하계학술대회

B4 IoT보안 2

이 임 영 (순천향대학교)

- **탈취대응을 위한 상황인지 기반 드론 제어 메커니즘 설계**
  오윤석, 김애영, 서승현
- **CCTV 환경에서의 속성기반 프록시 재암호화를 사용한 영상데이터 접근제어 기술 연구**
  황용운, 이임영
- **스마트 축사 모니터링 시스템**
  박 환, 박용석, 김진보, 김미선, 서재현
- **자율주행 자동차 센서 신뢰도 향상 및 공격 탐지 알고리즘 분석**
  선현진, 이동훈
- **소프트웨어 난독화 기법 평가 기술 연구 동향**
  백은수, 석재혁, 이재융, 이동훈

탈취대응을 위한 상황인지 기반 드론 제어 메커니즘 설계

오윤석* 김애영** 서승현*†

* 한양대학교 대학원 전자공학과

** 한양대학교 공학기술연구소

Design of context-aware based drone control mechanism for countering physical capture attack

Yoon-Seok Oh* Ae-Young Kim** Seung-Hyun Seo*

*Dept. of Electrical Engineering, Graduate School, Hanyang University.

**Research Institute of Engineering & Technology, Hanyang University.

요 약

최근 다방면으로 활용되고 있는 드론은 무인 환경에서 동작하고 보안이 취약한 무선 통신을 사용하기 때문에 물리적 탈취 공격, 정보 유출 공격 등 다양한 보안 위협에 취약하다. 특히, 불법 드론 탈취로 인해 저장정보 유출 및 무단 도용 등의 피해를 예방하기 위한 연구가 필요하다. 이에 본 논문에서는 드론이 불법적으로 탈취당한 경우에, 저장된 내부 정보를 보호하고, 무단 도용을 예방할 수 있는 상황인지 기반 드론 제어 메커니즘을 제안하고, 제안 메커니즘의 실현성을 프로토타입 구현 및 실험으로 보였다.

I. 서론

드론(Drone)은 초기에 군사적 목적으로 이용되었으나 최근에는 관제, 배송, 방송촬영, 농업 등 점차 다양한 산업 분야에서 활용되고 있다. 그러나 드론은 무선 네트워크를 사용하여 통신하며 외부의 접근에 상시 열려있는 상태이기 때문에 상대적으로 사이버보안 공격에 취약하다. 또한 무인 환경에서 동작하기 때문에 불법 탈취되어 저장된 정보가 유출되거나, 제 3자에 의해 무단으로 도용되는 위협에 취약하다.

본 논문에서는 동작권한을 부여하지 않은 장소에서 드론의 작동이 불가능하도록 상황인지 기반 드론 제어 메커니즘을 제안한다. 제안 메커니즘은 드론 외부의 환경 정보와 드론 내부의 고유 잡음 정보를 동시에 이용하여, 드론의 동작 권한을 부여하거나 내부 정보를 암호화하는데 사용되는 비밀정보를 은닉한다. 또한, 드론의 동작 권한이 부여된 적법한 환경에서만 비밀정보가 복원되어 드론을 동작시킬 수 있도록 한다. 따라서, 제안하는 드론 제어 메커니즘을 적용한 드론은 불법적으로 탈취되었다 하더라도, 임의의 장소에서 동작되지 못하며, 내부에 저장된 정보들의 유출을 어렵게 만든다.

제안하는 메커니즘의 구현가능성을 검증하기 위하여, 본 논문에서는 상황인지기반 드론 제어 메커니즘의 비밀정보 은닉 알고리즘 및 복원 알고리즘을 설계하고, 프로토타입을 구현하여 실험 결과를 보였다.

이 성과는 2015년도 미래창조과학부의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2015R1C1A1A01052491).

II. 관련연구

드론은 각종 센서들을 탑재하여 모니터링하는 환경 및 주변 정보 등을 수집하는데 주로

이용된다. 하지만 무인 이동체로 상대적으로 보안이 취약한 무선 통신을 사용하여 정보를 전송하는 드론의 특성상 불법 탈취 및 저장정보 탈취 등의 물리적 보안 침해 위협과, 악성코드 감염으로 인한 오동작 및 전송되는 정보 유출 등의 사이버상의 보안 침해 위협이 공존한다.[1]

현재까지 안전한 드론 제어를 위한 보안 기법에 관한 연구로는 GPS 서브 프레임 데이터를 검증을 통해 GPS 스푸핑(spoofing)을 대응하는 방법이 있으며[2], Wi-Fi 등의 무선 네트워크를 통해 보안 취약점 악용과 그 대응책은 [3]에서 논의된 바가 있다. 그러나 네트워크 공격에 대한 대응이 아닌 물리적인 탈취와 정보 유출에 대응방안에 대한 연구가 미흡하다.

III. 상황인지기반 드론 제어 메커니즘

본 장에서는 드론이 불법적으로 탈취가 되었을 경우에도, 탈취된 드론이 정상적으로 동작할 수 없도록 하기 위해, 외부의 환경정보와 내부의 고유한 잡음정보를 이중 요소로 하는 퍼지 커미트먼트 기법[4] 기반의 드론 메커니즘을 설계한다. 제안하는 상황인지기반 드론 제어 메커니즘은 암호키 생성용 비밀정보 은닉단계, 비밀정보 복원 및 암호키 생성단계, 드론 제어 및 동작단계의 3단계로 구성된다.

3.1 암호키 생성용 비밀정보 은닉단계

본 단계에서는 드론 제어용 암호키를 생성하여, 이를 외부 및 내부 잡음원으로 은닉시키고, 키 복원단계에서 사용할 보조정보를 생성한다. 초기 비밀정보 r은 드론 제어용 암호키를 생성하는 시드(seed)로 이용되며, 외부 잡음원, 내부 잡원으로 은닉된 상태, h로 드론에 저장된다.

입력: 오류 정정 허용 t
결과: 보조정보 h
알고리즘:
1. 초기 비밀 정보 r을 랜덤하게 선택한다.
2. 오류 정정을 허용하는 파라미터 t를 설정한 후, r을 오류정정 코드로 인코딩하여 r'=Encode(t,r)를 생성한다.
3. 드론 카메라 센서를 이용하여, 드론 착륙장 주변 이미지 I_E를 획득한 후, I_E를 이진화하여 외부 잡음원 N_E으로 설정한다.
4. 드론 내부에 탑재된 PUF로 부터 내부 잡음원 N_I 획득한다.
5. 획득한 N_E와 N_I를 결합한 w=N_E⊕N_I를 계산한다.
6. r'와 w를 이용하여 보조정보 h=r'⊕w를 생성하여 드론에 저장한다.

3.2 비밀정보 복원 및 암호키 생성 단계

본 단계에서는 드론에 저장된 보조정보 h로부터 비밀정보 r을 복원하고, 복원된 r을 이용하여 드론 제어용 암호키를 생성한다.

입력: 오류 정정 허용 t
결과: 비밀정보 r, 암호키 k
알고리즘:
1. 드론 카메라 센서를 이용하여, 드론 착륙장 주변 이미지 I_E'를 획득한 후, I_E'를 이진화하여 N_E'를 생성한다.
2. 드론 내부에 탑재된 PUF로 부터 내부 잡음원 N_I' 획득한다.
3. 획득한 N_E와 N_I'를 결합한 w'=N_E'⊕N_I'를 계산한다.
4. 드론에 저장된 보조정보 h를 이용하여 r''=h⊕w'을 계산한다.
5. r''을 오류 정정 허용범위(t)내에서 디코딩하여 r=Decode(t,r'')을 복원한다.
6. r을 시드로 이용하여 드론 제어용 암호키 k를 생성한다.

외부 잡음원으로 사용되는 이미지는 조도의 차이, 카메라 렌즈의 잡음 등으로 동일한 장소에서 촬영했어도 약간의 오차를 가진다. 이 오차는 정상적인 상황에서 허용되는 오류정정 파라미터 범위 내에서 정정된다.

3.3 드론 제어 및 동작 단계

본 단계에서는 드론 제어용 암호키 k를 이용하여 드론을 동작시키는 단계이다. 드론을 동작시키기 위해서 이 k의 검증 결과 Validate(k)는 비밀정보 은닉단계에서 N_E를 획득한 환경 $a1$과 비밀정보 복원단계에서 N_E'를 획득한 환경 $a2$의 동일여부에 따라 다음과 같은 값을 갖는다.

$$Validate(k) = \begin{cases} True & (a1 \cong a2) \\ False & (a1 \neq a2) \end{cases}$$

*a2*가 *a1*과 동일한 정상적인 환경에서 생성된 값이라면 Validate(*k*)의 결과 값은 *True*로 드론을 제어할 수 있으며, *a2*가 탈취 등의 이상 상황에 따른 비정상적인 환경이라면 생성된 *k*의 검증 결과 *False*로 드론을 동작 시킬 수 없다.

IV. 드론 제어 메커니즘 구현

4.1 프로토타입 구현

제안하는 드론 제어 메커니즘을 실험하기 위하여 Raspberry pi 3(1.4Ghz, 메모리 1G) 보드를 탑재한 Pixhawk 4 비행 컨트롤러 드론을 사용하고, 내부잡음원을 획득하기위해 ICTK G1 PUF를, 외부이미지를 획득하기 위해 라즈베리파이 카메라 v2를 탑재하여 프로토타입을 구성하였다.

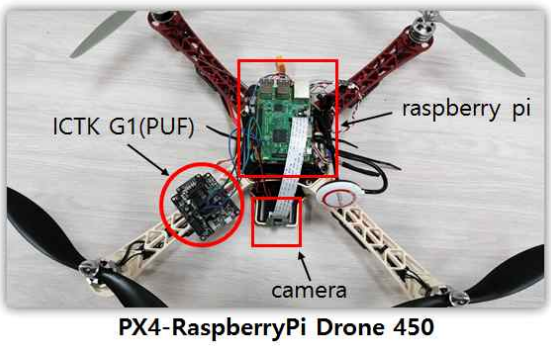


그림 1. 드론 제어 메커니즘 프로토타입

본 프로토타입의 구현은 라즈베리파이에 설치된 Dronekit-python API를 이용하여 C/C++ 및 Python으로 구현하였다. 상황인지기반 드론 제어 메커니즘의 비밀정보 은닉 알고리즘 및 복원 알고리즘을 구현하기 위해, 오류 정정 코드로는 BCH(Bose Chaudhuri Hocquenghem) 코드[9], 이진화 기법으로는 대표적인 이미지 전처리 기법인 Otsu 기법[8], 암호키 생성 기법은 의사난수 생성기를 구현하는데 활용되는 SHA-256 해시 알고리즘을 사용하였다.

4.2 실험 결과

실험 환경은 그림 2와 같다. 드론에 대한 동작권한을 부여한 장소 a1은 비밀정보 은닉 단계를 수행한 장소이다. 주어진 그림 2의 (a)와 (b) 장소에 대해, 비밀정보 복원 및 암호키 생성 단계를 수행하는 장소 a2로 (a)를 선택하면 동작권한을 가질 수 있는 비밀정보가 복원된다. 반면에 a2로 (b)를 선택하면 비밀정보 복원에 실패하여 드론을 작동시킬 수 없다.



(a) 동작권한을 부여한 장소	(b) 동작권한을 부여하지 않은 장소

그림 2. 실험 환경

실험을 위해 드론이 촬영한 외부이미지는 그림 3과 같다.

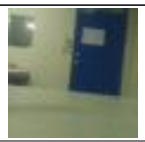
a1		드론이 비밀정보 은닉단계에서 촬영한 외부이미지
a2-a		그림2.(a)에 위치한 드론이 비밀정보 복원단계에서 촬영한 이미지
a2-b		그림2.(b)에 위치한 드론이 비밀정보 복원단계에서 촬영한 이미지

그림 3. 드론이 촬영한 외부 이미지

그림 4는 그림 3의 a2-a와 a2-b에 대하여 오류 정정 허용 파라미터 t의 값의 따라 비밀정보 복원률을 나타낸 것이다. 동작권한을 부여한 장소 a1에 대하여, 같은 장소 및 위치에서 드론이 외부 이미지를 촬영하여 그림 3의 a2-a를 얻었을 경우에는 비밀정보 복원률이 t=10부터 100%이다. 반면에 동작권한을 부여하지 않은

장소(그림 2.(b))에서 드론이 촬영한 외부 이미지 그림 3의 a2-b를 얻었을 경우에는 [4]에서 기술된 오류 정정 최대 허용 범위 t=26에서도 비밀정보 복원률은 0%이다.

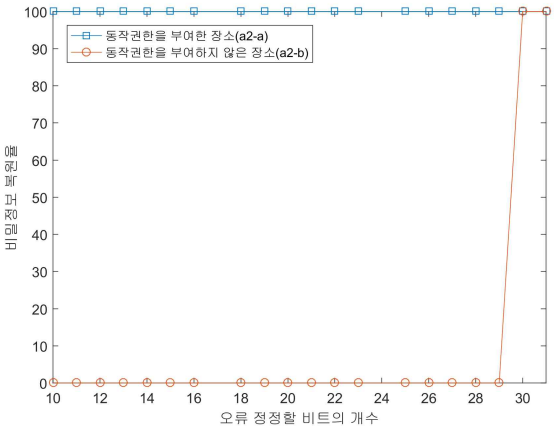


그림 4. 비밀정보 복원율

4.3 제안하는 드론 제어 메커니즘의 안전성

본 논문에서 제안하는 드론 제어 메커니즘의 안전성은 이중-요소 퍼지 커미트먼트 기법[4]의 안전성에 기반 한다. 드론 비밀 정보 은닉단계에서 생성된 보조정보 h=r′⊕N_E⊕N_I는 PUF 칩으로부터 추출된 N_I를 XOR하여 생성하였다. PUF가 출력하는 N_I는 균일분포(uniformly distribution)에서 선택된 난수[7]이기 때문에 h 또한 난수가 된다[4,6]. 따라서 드론에 저장된 h로부터 다항시간 내에 비밀정보 r을 추출하는 것은 불가능하다. 또한 임의의 이미지를 사용하여 복원을 시도하였을 경우, 비밀정보 복원 및 암호키 생성단계에서 오류 정정 허용 범위 내에 비밀정보가 복원되는 것이 불가능하다.

V. 결론

본 논문에서 탈취된 드론이 정상적으로 동작할 수 없도록 외부의 환경정보와 내부의 고유한 잡음정보를 이중 요소로 하는 상황인지 기반의 드론 제어 메커니즘을 제안하였다. 제안 메커니즘은 드론이 탈취될 경우에도 수집된 내부 정보가 유출되거나, 탈취된 드론이 무단 도용되는 피해 방지를 가능하게 한다. 본 논문에서는 제안 메커니즘을 구현하여 실험을 통해 위의 가능성을 보였다.

[참고문헌]

[1] Yousung Kang et al. “Security Requirements for Drone-based IoT Services”, IoTF, Feb. 2015

[2] Vishal Dey et al. “Security Vulner abilities of Unmanned Aerial Vehicles and Countermeasures: An Experimental Study”, 2018 31th International Con ference on VLSI Design and 2018 17th International Conference on Embedded Systems, IEEE, pp. 398-403, 2018

[3] Ji-Hyun Kim, Byung-Ki Kim, Yong-Tea Shin, “A Study on the Improvement of security vulnerabilities in Civilian Drone”, Korean Information Science Society, Jun, 2016

[4] Dooho Choi et al. “Two-Factor Fuzzy Commitment for Unmanned IoT Devices Security”, IEEE Internet of Things Journal, 2018

[5] J. R. Wallrabenstein, “Practical and Secure IoT Device Authentication Using Physical Unclonable Functions”, in IEEE 4th International Conference on Future Internet of Things and Cloud, 2016

[6] A. Juels, and M. Wattenberg, “A Fuzzy Commitment Scheme”, in ACM con ference on Computer and Comm unications Security, 1999, pp 28-36

[7] R. Maes et al. “Secure key generation from biased PUFs: extended version”, Journal of Cryptographic Engineering, vol. 6, no. 2, pp. 121-137, Jun. 2016

[8] N. Otsu, “A threshold selection method from gray-level histograms”, IEEE transactions on systems, man, and cybernetics, vol. 9, no. 1, pp.62-66, 1979

[9] R. Chien, “Cyclic decoding procedures for Bose-Chaudhuri-Hocquenghem codes ”, IEEE Transactions on Information Theory, vol. 10, no. 4, pp. 357-363, 1964

CCTV 환경에서의 속성기반 프록시 재암호화를 사용한 영상데이터 접근제어 기술 연구+

황용운, 이임영

순천향대학교 컴퓨터학과

A study on video data access control technology using attribute-based proxy re-encryption in CCTV environment

Yong-Woon Hwang, Im-Yeong Lee

Dept of Computer Science and Engineering, Soonchunhyang University

요 약

최근 CCTV는 과거 영상만을 기록하는 것과 달리 IoT 기술의 발달과 CCTV의 지능화 및 융합화에 따라 발전되었으며, 현재 다양한 분야에서 적용되어 활용하고 있다. 하지만 발전된 CCTV 환경에서 다양한 보안위협이 존재하는데, 공격자는 전송되는 영상데이터를 획득하여 CCTV에 찍힌 사용자의 정보를 획득할 수 있고, 이를 외부에 유출하거나 조작하여 영상데이터의 무결성을 훼손할 수 있다. 본 논문에서는 CCTV의 보안위협을 해결하고자 CCTV 환경에서 영상데이터를 속성기반 암호로 암호화하여 서버에서 관리함으로써 허가된 사용자만이 영상데이터에 접근할 수 있다. 또한 그 외에 다른 속성을 지닌 자가 영상데이터에 접근하고자 할 때, 접근자의 속성을 기반으로 프록시 재암호화 기법을 활용하여 영상데이터를 재암호화함으로써 안전하게 영상데이터에 접근 할 수 있다.

I. 서론

CCTV(closed circuit television)는 폐쇄 회로 텔레비전으로 과거 영상만을 기록하는 것과 달리 IoT 기술의 발달과 CCTV의 지능화 및 융합화에 따라 발전되었으며, 현재 일상생활 속에서 다양하게 적용되어 사용되고 있다. CCTV를 사용하는 이유는 교통상황이나 유치원, 공원 등 공공장소를 실시간 모니터링하는 경우와, 사건 사고시 현장을 관찰하거나 현장의 증거자료를 확인하기 위해 사용되며, 범죄 예방을 위한 수단으로 사용된다. 하지만 설치된 CCTV 환경에서도 다양한 보안위협이 존재한다. 특히 CCTV가 찍은 영상을 서버로 보내지는 구간의 보안상태가 취약하다[1]. 이를 통해 공격자는 전송되는 영상데이터를 획득하여 CCTV에 찍은 사용자의 정보를 획득할 수 있고, 이를 조작하여 사회에 혼란을 줄 수도 있다. 또한 다수의 카메라의 영상을 관리는 서버가 공격자에 의해 해킹당하면 다수의 CCTV는 공격자에 의해 제어 될 수 있다. 이러한 보안위협을 해결하기 위해 영상정보 암호화, 안전한 보안채널 구성 등 다양한 보안기술이 존재하지만, 결국 서버가 영상데이터를 볼 수 있으며, 키 분배도 별도로 고려하게 된다. 이를 해결하기 위해 본 논문에서는 CCTV 환경에 속성기반 암호와 이를 기반으로 하는 속성기반의 프록시 재암호화 기법(Attribute-based Proxy Re-Encryption)을 적용하여 인가된 사용자가 안전하게 영상데이터에 접근할 수 있는 접근제어 기술을 제안하고자 한다. 영상데이터를 속성기반 암호로 암호화하여 서버에서 관리함으로써 사용자는 자신의 속성이 암호화된 영상데이터의 속성에 해당되는 경우 영상데이터에 접근할 수 있다. 또한, 그 외 다른 사용자가 영상데이터에 접근하고자 하는 경우 관리자에 의해 인증된 사용자의 한

+ 이 논문은 연세대학교 바른ICT연구소의 지원을 받아 수행된 연구 결과입니다.

해 인증된 사용자의 속성을 기반으로 영상데이터를 재암호화하여 기존의 영상데이터에 접근할 수 있는 사용자 외에 추가로 인증된 사용자도 영상데이터에 안전하게 접근할 수 있다.

II. 관련연구

2.1 속성기반암호

속성기반암호는 각 개체의 속성(소속, 직무) 정보의 집합과 주어진 속성 집합에 접근을 할 수 있는지 없는지에 대한 접근구조를 바탕으로 암복호화를 실시하는 방식이다. 속성기반암호 중 CP-ABE(Ciphertext-Policy)는 암호문을 생성할 때 송신자가 접근구조를 지정하여 수신자에게 전송하고, 수신자는 자신의 속성 집합을 기반으로 암호문을 복호화 한다[2]. [그림 1]과 같이 영상데이터에 접근하려는 수신자가 [A구], [A 경찰서], [교통계]라는 속성을 가지고 있을 경우, 송신자는 암호문에 [A구, A경찰서, 교통계]라는 속성으로 접근구조 만들어 암호화하면 접근 구조를 만족하는 수신자만이 암호문을 복호화 할 수 있다.

2.3 속성기반의 프록시 재암호화 기법

속성기반의 프록시재암화 기법은 기존의 프록시 재암호화 기법에 속성기반 암호를 적용한 방식이다. 사용자(속성에 의해 식별된)들은 하나의 접근정책에서 다른 접근정책으로 암호문을 재암호화 하는 Proxy를 자유롭게 지정할 수 있다. 속성기반의 프록시 재암호화 기법 중 CP-ABPRE는 접근구조 AS로 암호화된 암호문 C를 다른 사용자의 속성에 맞는 접근구조 AS'로 변환하는 Proxy를 지정하여 변경된 접근구조로 암호문 C를 C'로 재암호화하는 방식이다[3][4].

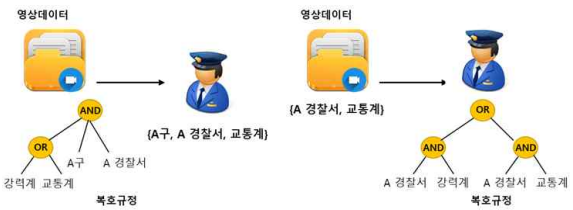


그림 1. 왼쪽 CP-ABE, 오른쪽 KP-ABE

III. 제안방식

본 장에서는 CCTV 환경에서 속성기반 암호화 속성기반 프록시 재암호화 기법을 활용한 영상데이터 접근제어 기법을 제안한다. [그림 2, 3]은 본 제안방식이 적용되는 환경을 시나리오로 나타낸 그림이다. [그림 2]에서 CCTV에 녹화된 영상은 A구의 A 경찰서 중 강력계와 교통계 부서의 속성으로 암호화되어 있기에, A구의 A 경찰서의 강력계와 교통계 부서만이 영상데이터를 확인할 수 있다. 이때 만약 범인이 청소년인 경우 청소년과 부서도 이 수사에 참여해야하며, CCTV를 볼 수 있는 권한이 주어져야한다. 하지만 청소년과 부서는 CCTV의 영상데이터를 복호화 할 수 있는 권한이 없기에, [그림 3]과 같이 속성기반 프록시 재암호화기법을 사용하여 부서별 접근구조를 변환시켜 영상데이터를 재암호화함으로써 청소년과 부서도 영상데이터를 복호화 할 수 있는 권한을 가질 수 있다.

3.1 시스템 계수

본 제안방식의 시스템 계수는 다음과 같다.

- TTP : 신뢰할 수 있는 3기관(관리자)
- $DVR Server$: CCTV 영상을 관리하는 서버
- pp, mk : 공개 파라미터, 마스터키
- AD_U, S : 접근자 속성데이터, 속성데이터 집합
- AS, AS' : 접근구조와, 변환된 접근구조

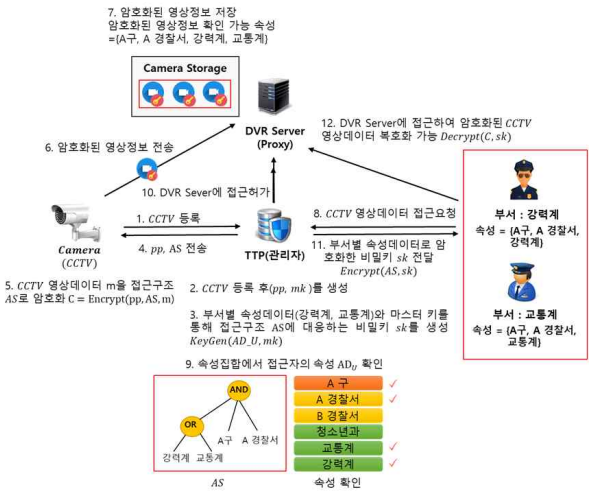


그림 2. 암호화된 영상데이터에 접근 시나리오

· rK, sk : 재암호화키, 접근자 비밀키
· C, C' : 암호데이터, 재암호화된 데이터
· $+d_i, -d_i$: 긍정 속성데이터, 부정 속성데이터

3.2 CCTV 영상암호화 단계

Step 1. CCTV는 TTP에게 등록메시지를 보내 등록을 요청하면 TTP는 CCTV 등록 후 공개파라미터와 마스터키 (pp, mk)를 생성한다.

• Setup단계 : 공개파라미터 pp, mk 생성

Step 2. 접근자 속성데이터와 마스터키를 통해 접근구조 AS를 생성하고 이에 대응하는 비밀키 sk를 생성한다. 이후 CCTV에게 공개파라미터와 사용자 접근구조(pp, AS)를 전송해준다.

• $KeyGen(S, mk)$: 속성의 집합 S와 마스터키를 통해 비밀키 sk를 생성

Step 3. CCTV는 영상데이터 m을 공개파라미터와 접근구조(pp, AS)로 암호화하여 DVR Server에게 전송한다. DVR Server는 CCTV별로 저장 공간을 생성해 실시간으로 전송받는 암호화된 영상데이터를 저장하며, 여기서 저장된 CCTV의 영상데이터는 A구, A경찰서, 강력계, 교통계의 속성을 가지고 있다.

• $Encrypt(pp, AS, m)$: 공개파라미터 pp와 접근구조 AS로 영상데이터 암호화 단계

3.3 속성을 가진 사용자 영상데이터 접근단계

Step 1. 영상데이터에 접근을 요청하는 접근자는 TTP에 접근하여 자신의 속성이 DVR Server에 접근 가능한지의 여부를 판단한다.

Step 2. TTP는 접근자의 속성을 확인후 DVR Server에 접근허가를 요청하고, 접근자 접근구조로 암호화한 비밀키 sk를 전송 해준다.

• $Encrypt(AS, sk)$: 접근자의 속성이 AS와 일치하면 비밀키 sk를 획득할 수 있는 단계

·만약 $+d_i$가 AS에 속한다면 sk 획득
·만약 $-d_i$가 AS에 속한다면 sk 획득실패

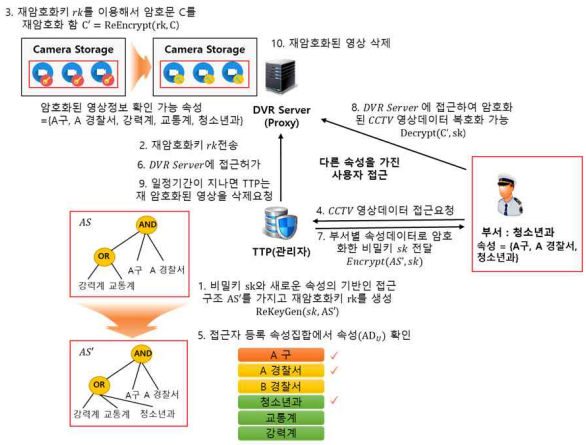


그림 3 다른 속성을 가진 사용자 접근단계

Step 3. 접근자는 DVR Server에 접근하여 암호화된 CCTV 영상데이터를 비밀키 sk로 복호화하여 볼 수 있다.

• $Decrypt(C, sk)$: 암호화된 영상데이터 C에 해당하는 속성을 지닌 자는 비밀키 sk로 복호화할 수 있는 단계

3.4 다른 속성을 가진 사용자 영상데이터 접근단계[그림 3]

Step 1. TTP는 새로운 속성(부서:청소년과)을 기반으로 접근구조를 $AS \rightarrow AS'$ 변환 후 비밀키 sk로 재암호화키 rk를 생성한다. 이후 재암호화키 rk를 DVR Server에 전송한다.

• $ReKeyGen(sk, AS')$: 새로운 접근구조 AS'와 비밀키 sk를 통해 재암호화키 rk 생성

Step 2. DVR Sever는 기존의 암호화된 영상데이터 C와 재암호화키 rk를 사용해 영상데이터를 재암호화한다. 재암호화된 영상데이터에는 청소년과 부서의 속성이 추가되었다.

• $ReEncrypt(rk, C)$: 기존의 암화화된 영상데이터 C를 재암호화키 rk를 통해 재암호화 하는 단계

Step 3. 청소년과 부서의 접근자가 영상데이터를 요청할 때, 3.4의 Step1~Step2를 통해 TTP로부터 자신의 속성이 DVR Server에 접근 가능한지의 여부를 접근자의 속성으로 확인 후, 접근구조로 암호화한 비밀키 sk를 전송해준다.

Step 4. 접근자는 DVR Server에 접근하여 재암호화된 CCTV 영상데이터를 비밀키 sk로 복호화 하여 볼 수 있다.

• $ReDecrypt(C', sk)$: 재암호화된 영상데이터 C'에 해당하는 속성을 지닌 자는 비밀키 sk로 복호화 할 수 있는 단계

Step 5. 접근자의 권한 기간이 만료되면 TTP는 DVR Server에게 재암호화된 영상데이터 삭제를 요청하며, DVR Server는 재암호화되어 저장된 영상데이터를 삭제한다. 이로써 공간의 효율을 높일 수 있으며, 기존에 암호화된 CCTV 영상 데이터의 속성을 지닌 접근자만이 영상데이터를 확인 할 수 있다.

IV. 제안방식 분석

다음과 같은 장에서는 CCTV 환경에서의 발생되는 보안요구사항을 만족시킨다.

· 재전송 공격 및 위장공격 : 재암호화된 영상데이터는 사용자의 속성과 사용자의 비밀키로 접근하여 복호화 할 수 있다. 이에 공격자는 영상데이터를 도청하여 획득하더라도 복호화 할 수 없음으로 재전송 공격이나 위장공격 등에 안전하다.

· 인가되지 않은 사용자의 접근제어 : 본 제안방식에서 사용자가 영상데이터에 접근하기 위해 초기에 TTP에서 인증절차를 거친다. 또한 DVR Server에 저장된 암호화된 영상데이터에 접근하기 위해서는 사용자의 속성과 암호화된 영상데이터의 속성을 비교하여 일치하면 접근할 수 있다. 이에 본 제안방식에서 인가되지 않은 사용자의 접근을 차단한다.

· 데이터 무결성 및 기밀성 보장 : 본 제안방식에서 CCTV 영상데이터를 속성기반으로 암호화하여 데이터의 기밀성을 강화하였으며, 암호화된 영상데이터의 속성과 일치하는 사용자의 속성과 비밀키로만 영상데이터를 복호할 수 있기에 영상데이터 무결성이 보장된다.

V. 결론

CCTV 환경에서 발생하는 보안위협을 해결하기 위해 본 논문에서는 속성기반 프록시 재암호화 기법을 활용한 영상데이터 접근제어 기법을 제안하였다. 제안방식은 영상데이터가 속성기반암호로 암호화되어 있기에 재전송공격이나, 위장공격과 같이 다양한 보안위협에 대해 안전하다. 또한 CCTV에서 녹화된 영상데이터에 인가된 사용자만이 접근 할 수 있어 안전하다.

향후 연구로는 속성기반 암호에서 사용자의 속성이 곧 개인정보이기 때문에 본 논문에서 제시된 속성기반 프록시 재암호화 기법에서 사용자의 속성에 익명성을 추가하여 사용자의 속성을 보호하는 연구가 필요할 것으로 사료된다.

[참고문헌]

[1] 박태성 외 2명. “Network CCTV 환경에서 악의적인 사용자를 차단하기 위한 RTSP 사용자 인증 프로토콜”, 한국산학기술학회, 2011.

[2] 박광용, 송유진. “속성기반 암호기술”, 정보보호학회지, 2010.

[3] Liang, Xiaohui, et al. "Attribute based proxy re-encryption with delegating capabilities", Proceedings of the 4th International Symposium on Information, Computer, and Communications Security. ACM, 2009.

[4] Chung, Pei-Shan, et al. "A Study of Attribute-based Proxy Re-encryption Scheme in Cloud Environments." IJ Network Security 16.1, 2014. pp. 1-13.

[5] Seo, Hwa-Jeong, and Ho-Won Kim. "Attribute-based proxy re-encryption with a constant number of pairing operations." Journal of information and communication convergence engineering 10.1, 2012. pp. 53-60.

스마트 축사 모니터링 시스템

박 환*, 박용석*, 김진보*, 김미선*, 서재현*
*목포대학교 정보보호학과

Smart Livestock Barn Monitoring System

Hwan Park*, Yong-Seok Park*, Jin-Bo Kim*, Mi-Sun Kim*, Jae-Hyun Seo*
*Division of information security, Mokpo National University.

요 약

IoT는 각종 센서가 부착된 사물에 통신 기술을 접목하여 인터넷에 연결하는 기술이다. 인터넷에 연결함으로서 다른 사물들과 연결되어 데이터를 주고받아 사용자가 활용할 수 있는 정보를 제공하기 때문에 스마트 홈, 스마트 팩토리, 스마트팜 등의 여러 환경에서 유용하게 사용되어진다. 본 논문에서는 축사에 IoT 기술을 접목하여 스마트 축사 환경을 구성하고 RTU와 게이트웨이를 통해 생성되는 센싱 데이터를 서버로 전달하여 해당 축사의 모니터링 서비스를 제공함으로써 IoT 디바이스를 관리할 수 있으며 화재 등의 사고를 예방할 수 있는 시스템을 설계하고 구현하였다.

I. 서론

IoT란 각종 센서가 부착되어져 있는 사물에 통신 기술을 접목하여 인터넷에 연결하는 기술이다. 이에 따라 많은 데이터들이 지속적으로 발생되고 교환됨으로서 빠른 연산을 통하여 데이터를 분석할 수 있다. 이를 통해 상황에 더욱 적합한 서비스를 제공할 수 있고 화재 등의 사고가 일어나기 전에 발생 가능성을 감지하여 사전에 예방 할 수 있기 때문에 의료, 산업 등의 분야에서 고편의 기능을 제공할 수 있다. 이러한 IoT는 환경에 따라 스마트 팜, 스마트 팩토리, 스마트 헬스, 스마트 홈 등으로 분류되어지며, 초연결 사회(Hyper Connected Society)를 가속화 시키고 있다.

본 논문에서는 IoT을 이용하여 축사에 대한 피해를 예방하기 위한 시스템을 개발하고자 한다. 대부분의 축사는 주인의 거주지와 먼 곳에 위치해 있기 때문에 실시간으로 직접적인 관리에 어려움이 있다. 이에 따라 화재 등의 사고에 취약할 수밖에 없으며, 사고가 발생 했을 시 막대한 자산 피해을 겪게 된다.

이러한 점을 고려하여 축사 내에 센서가 부착된 디바이스를 설치하고 지속적인 센싱(Sensing)를 통하여 축사 내의 상태 데이터를 생성하고 서버로 전송한 다음 데이터를 토대로 모니터링 서비스(Monitoring Service)를 제공하는 시스템을 설계하고 구현하였다. 이를 통해 실시간으로 축사를 간접적으로 관리 할 수 있도록 하고 화재 등의 사고를 예방 할 수 있도록 하였다.

II. 스마트 축사

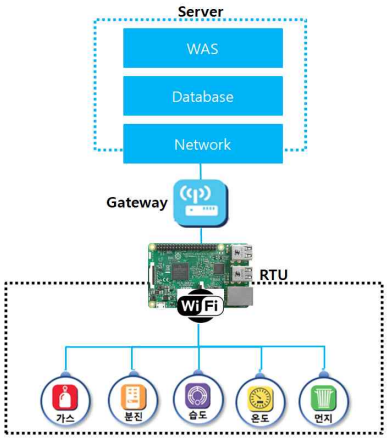
축산업은 변화하는 내·외부 환경에 적절히 대응하여 생산력을 향상시켜야 한다. 하지만 인구 감소 및 고령화로 인하여 축산업은 점점 쇠퇴하고 있다. 이를 위해 4차 산업 혁명과 관련된 기술을 축산업에 접목시켜 전통적인 축산업 방식에서 탈피하고 축산업의 생산성 및 효율성을 높이기 위한 스마트 팜(Smart Farm)의 필요성이 대두되고 있다. 스마트 축사는 스마트 팜의 모델 중 하나이며 IoT 등의 정보통신 기술을 활용하여 시간과 공간의 제약 없이 축사에 설치된 센서를 통해 내·외부 환경 상태를 측정하며, 수집된 정보를 네트워크를 통해 DB에 저장

하거나 분석하여 축사 관리자에게 축사 정보를 제공한다.[2] 이를 통해 먼지, 메탄가스 등에 의해 화재로 이어지는 사고를 예방할 수 있으며 적정한 축사 환경을 유지 및 관리하여 효율성을 높일 수 있다.

III. 스마트 축사 모니터링 시스템

본 논문에서는 IoT을 이용하여 축사에 대한 피해를 예방하기 위한 시스템을 개발하고자 한다. 대부분의 축사는 주인의 거주지와 먼 곳에 위치해 있기 때문에 실시간으로 직접적인 관리에 어려움이 있다. 이에 따라 화재 등의 사고에 취약할 수밖에 없으며, 사고가 발생 했을 시 막대한 자산 피해을 겪게 된다.

이러한 점을 고려하여 축사 내에 센서가 부착된 디바이스를 설치하고 지속적인 센싱(Sensing)를 통하여 축사 내의 상태 데이터를 생성하고 서버로 전송한 다음 데이터를 토대로 모니터링 서비스를 제공하는 시스템을 설계하고 구현하였다. 이를 통해 실시간으로 축사를 간접적으로 관리 할 수 있도록 하고 화재 등의 사고를 예방 할 수 있도록 하였다.

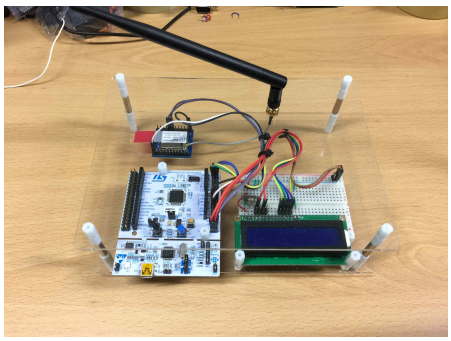


(그림 1) 시스템 구조

본 논문에서 제안한 시스템 구조는 (그림 1)과 같다. 엔드 디바이스(End Device)에 센서(Sensor)를 장착하여 센싱 데이터(Sensing Data)를 생성한다. 엔드 디바이스는 생성된 데이터를 RTU(Remote Terminal Unit)로 전송하여 데이터를 정규화 한다. 이때 두 노드는 WiFi 모듈을 이용하여 통신한다. 센싱 데이터를 전송 받은 RTU와 게이트웨이(Gateway)는 Wifi 통신을 사용하고, 데이터를 전송 받는 게이트웨이는 유선망을 이용한 TCP/IP 통신을 이용하여 서버로 데이터를 전송한다. 서버는 네트워크 서버(Network Server), 데이터베이스 서버(Database Server), 웹 어플리케이션 서버(Web Application Server)로 이루어져있으며, 네트워크 서버는 게이트웨이와 통신하여 데이터를 전송 받는다. 전송 받은 데이터를 데이터베이스 서버에 저장하며, 서비스를 위하여 웹 어플리케이션 서버에서 활용한다.

3.1 데이터 수집 및 정규화

엔드 디바이스는 센싱 데이터를 생성하기 위하여 센서를 부착한 임베디드 시스템(Embedded System)이다. 부착하는 센서의 종류에는 온도, 습도, 메탄 가스, 화재 감지 센서로 구성하였다. 그리고 각각의 센서와의 호환성을 고려하여 아두이노(Arduino) 또는 라즈베리파이3(Raspberry PI3)를 기반으로 개발하였으며, WiFi 모듈을 부착하여 RTU와의 통신을 가능하게 하고자 하였다.



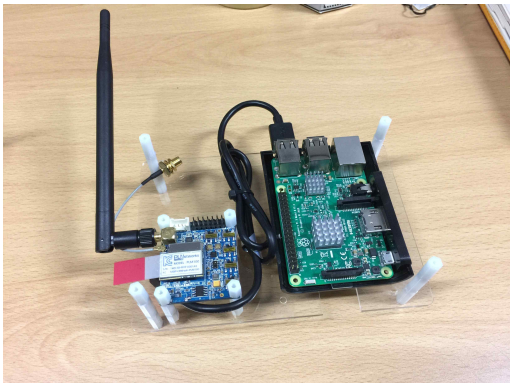
(그림 2) End Device

RTU는 마이크로 컴퓨터인 라즈베리파이3를 기반으로 개발하였다. 라즈베리파이3에 내장되어져있는 WiFi 모듈을 이용하여 엔드 디바이스로부터 센싱 데이터를 전송 받는다.

바이트	1	2	3	4	5	6	7	8
데이터	ED_ID				RTU_ID			
	Sensing_Data							
	DateTime							

(그림 3) 정규화 데이터 포맷

RTU는 센서들이 제조사와 종류가 달라서 각각의 센싱 데이터의 포맷(Format)을 가지고 있기 때문에 (그림 3)와 같은 포맷으로 정규화 하는 역할을 수행한다. 정규화 데이터 포맷은 해당 센싱 데이터를 생성한 엔드 디바이스의 관리를 위한 엔드 디바이스 아이디(ED_ID)와 정규화 및 전송을 하는 RTU의 아이디(RTU_ID), 생성된 센싱 데이터와 생성된 시간으로 구성하였다. 정규화 한 데이터를 WiFi 통신을 통하여 게이트웨이로 전송한다.[3]



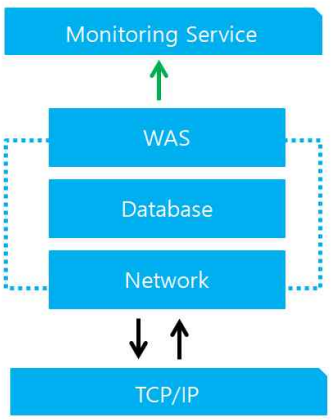
(그림 4) RTU

축사와 서버 간의 거리는 지역적으로 떨어져있다는 점으로 고려하여 RTU와 서버 간의 데이터 전달 역할을 하는 게이트웨이를 구축하였다. 게이트웨이는 미니 PC(Mini PC)인 브릭스(Brix)를 기반으로 개발하였으며, 내장되어져있는 WiFi 모듈을 이용하여 RTU와의 통신을 가능하게 하고자 한다. 그리고 유선망을 이용한 TCP/IP 통신을 통하여 RTU로부터 전송 받은 데이터를 네트워크 서버로전송한다.



(그림 5) Gateway

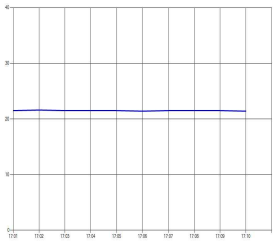
3.2 모니터링 서비스



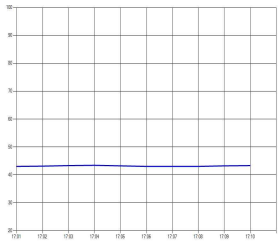
(그림 6) Server 구조

서버의 구조는 (그림 6) 와 같다. 네트워크 서버는 유선망을 통하여 게이트웨이와 TCP/IP 통신을 하여 데이터를 전송받는다. 전송받은 데이터를 데이터베이스로 전달되어 데이터베이스(Database)에 저장한다. 웹 어플리케이션 서버가 서비스를 위하여 데이터를 필요로 할 때, 데이터베이스 서버로부터 데이터를 요청하여 데이터를 전달받는다. 웹 어플리케이션 서버가 서비스를 위하여 데이터를 필요로 할 때, 데이터베이스 서버로부터 데이터를 요청하여 데이터를 전달받는다. 전달 받은 데이터를 기반으로 웹 어플리케이션 서버는 실시간 모니터링 서비스를 제공한다.

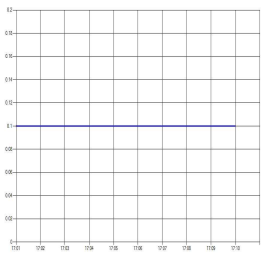
개발환경으로는 우분투 리눅스(Ubuntu Linux)를 기반으로 하였으며, 네트워크 서버는 C 언어를 이용하여 TCP/IP 프로토콜을 개발하였고 NoSql 데이터베이스인 몽고DB(MongoDB)를 이용하여 데이터베이스 서버를 개발하였다. 웹 어플리케이션 서버는 node.js와 HTML5를 이용하여 개발하였다.



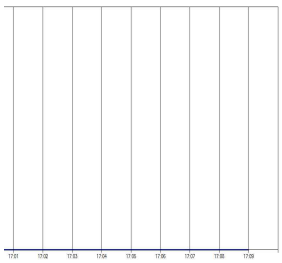
(그림 7-1) 온도 모니터링



(그림 7-2) 습도 모니터링



(그림 7-3) 메탄 가스 모니터링



(그림 7-4) 화재 감지 모니터링

(그림 7) 축사 모니터링

(그림 7)는 센서를 부착한 엔드 디바이스로부터 센싱 데이터를 실시간으로 전송 받아 모니터링 서비스를 위해 그래프의 형태로 표현한 것이다. 부착된 센서의 종류로는 온도, 습도, 메탄 가스, 화재 감지 센서로 구성하였다.[1]

IV. 결론

본 논문에서 구현한 시스템은 센서가 부착된 End Device가 생성하는 센싱 데이터를 토대로 서버에서

모니터링 서비스를 제공하여 관리 및 사고 예방을 할 수 있다. 하지만 일반적으로 서버는 축사와 먼 거리에 위치해있다. 그러기 때문에 짧은 통신 거리를 가지고 있는 Wifi를 이용하여 센싱 데이터를 서버까지 전달되기 위해서는 많은 게이트웨이를 필요로 한다. 이를 해결하기 위해서는 충분한 통신 거리를 가지고 있으면서 End Device와 같은 경량화 시스템에 적합한 통신 기술을 필요로 한다.

이를 위해 향후 연구에서는 LoRA라는 저전력 장거리 통신 기술을 시스템 적용하여 비교적 적은 게이트웨이로도 서버까지 데이터를 전달할 계획이다.

그리고 본 논문에서 구현한 시스템은 보안 취약점을 가지고 있기 때문에 무선 통신과 IoT 기기에 대해 암호화 통신, 무결성 보장 등의 보안적 요소를 접목하여 보다 안전한 서비스를 제공할 수 있는 방법을 연구할 것이다. 추가적으로 Alert 정책을 수립하여 알람 서비스를 제공하고 환경 유지 장치를 통해 자동적인 관리 서비스를 연구할 계획이다.

ACKNOWLEDGEMENT

본 논문(연구)는 중소벤처기업부의 재원으로 첫걸음기술개발사업의 지원받아 수행된 연구임.

[참고문헌]

[1] Ahmed Abdelgawad, Kumar Yelamarthi, and Ahmed Khattab. Iot-Based Health Monitoring System for Active and Assisted Living. 2017.

[2] 융합연구정책센터. Convergemce Resercj Review. March, 2018.

[3] Francis Enejo Idachaba. Review of Remote Terminal Unit and Gateways for Digital Oilfield delpoyments. 2012.

자율주행 자동차 센서 신뢰도 향상 및 공격 탐지 알고리즘 분석*

선현진*, 이동훈*

*고려대학교 정보보호학과

Analysis of Autonomous Vehicle Sensor Reliability Improvement and Attack Detection Algorithm*

Hyun Jin Sun*, Dong Hoon Lee*

*Graduate School of Information Security, Korea University

요 약

최근 자율주행 자동차에 대한 연구가 활발히 진행되고 있다. 자율주행 자동차는 주변의 물리적 환경을 정확하게 인식해야 하고 주행해야 한다. 이를 위해 자동차에 여러 개의 센서(Radar, Lidar, Ultrasonic sensor, camera, GPS 등)가 탑재되고 측정된 정보를 기반으로 주행 판단을 내린다. 이러한 환경에서 센서 정보의 위·변조 및 센서의 오작동은 탑승자에 안전에 큰 영향을 미친다. 본 논문에서는 특정한 물리량을 측정하기 위해 여러 개의 센서가 탑재된 상황에서 센서의 위·변조 공격을 탐지하고 위·변조 공격에 회복력을 가지는 센서 퓨전 알고리즘에 대한 연구를 소개한다.

I. 서론

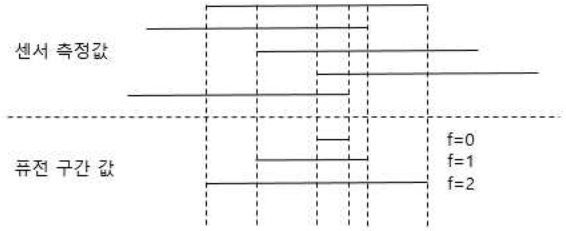
최근 여러 회사들이 자율주행 자동차 개발을 위해 연구를 진행하고 있다 [1]. 자율주행 환경에서 자동차가 스스로 주행하기 위해 외부환경의 인식은 필수 불가결 요소이다. 이러한 이유로 인해 외부환경을 인식하는 센서 정보의 위·변조 및 센서의 오작동은 탑승자의 안전을 위협하는 사고로 이어질 수 있다. 실제로 공격자가 자동차의 센서 정보를 위·변조하는 논문이 발표되었다 [3], [4], [5]. 이러한 공격에 안전하기 위해 센서 정보는 신뢰성을 보장해야 하며 위·변조 공격에 회복력을 가져야 한다. 이를 위해 센서 정보의 신뢰성을 보장하기 위한 센서 퓨전 알고리즘에 대한 연구가 진행되고 있다 [6], [7], [8].

* 이 논문은 2018년도 정보(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (R7117-18-0161, 자율주행 스마트자동차용 이상징후 탐지 핵심기술개발)

본 논문에서는 센서의 위·변조 공격을 탐지하고 위·변조 공격에 회복력을 가지는 센서 퓨전 알고리즘에 대해 소개한다. 자율주행 자동차는 특정한 외부환경의 물리량(전방 물체와의 거리, 전방 물체의 각도 등) 측정을 위해 여러 개의 센서(Radar, Lidar , camera, ultrasonic sensor 등)를 사용한다. 센서 퓨전 알고리즘의 목적은 N개의 센서 중 f(<N)개의 센서의 정보가 위·변조 되었을 때 이를 탐지하고 올바른 센서 정보의 범위를 추정해 안전한 주행 판단을 내릴 수 있는 정보를 제공하는 것이다.

또한 센서 퓨전 알고리즘은 센서 정보의 위·변조 공격뿐만 아니라, 날씨에 따른 센서의 오작동 상황에서도 필요하다.

본 논문에서는 2장에서 자율주행 자동차, abstract sensor model, Marzullo의 센서 퓨전 알고리즘의 개념에 대해 소개하고, 3장에서 기존의 센서 퓨전 알고리즘을 소개한다. 4장에서 기존의 센서 퓨전 알고리즘의 한계점을 분석하



<그림 1> N=5일 때 f값에 따른 퓨전 구간

고 마지막으로 4장에서 기존 센서 퓨전 알고리즘에 한계점을 보안할 수 있는 센서 퓨전 알고리즘 개발을 위한 연구 방향을 제시한다.

II. 배경지식

2.1 자율주행 자동차

인간의 운전 없이 센서(Radar, Lidar, GPS, camera)로 주위의 환경을 인식하여 목적지를 지정하는 것만으로 자동으로 주행할 수 있는 자동차를 의미한다 [2]. 많은 회사가 이를 연구하고 있으며 이 중에는 GM, Ford, BMW, Volkswagen등 완성차 업체들뿐 아니라 Google, Apple등과 같은 IT 업계와 Bosch와 같은 부품 업체도 존재한다 [1].

2.2 Abstract sensor model [9]

Abstract sensor model은 각각의 센서가 실제 값을 포함하는 구간을 컨트롤러에게 제공하는 것을 의미한다. 각각의 센서는 오류 임계치 δ를 가지고 있고, 시간 t에서 센서 i의 측정 값을 S(i,t)라고 하면 센서가 컨트롤러에게 제공하는 구간은 [S(i,t)-δ,S(i,t)+δ]가 된다.

2.3 Marzullo의 센서 퓨전 알고리즘 [9]

Marzullo는 abstract sensor model에서 센서 퓨전 알고리즘을 제안하였고 이는 많은 센서 퓨전 알고리즘에 기본 개념으로 사용되고 있다 [6], [8]. Marzullo의 센서 퓨전 알고리즘은 <그림1>과 같다. 여기서 f는 공격당한 센서의 개수를 의미한다. 이때 f는 $\frac{N}{2}$보다 작다는 가정이 있다(N: 센서의 개수). 이 방법에서 퓨전 구간 값은 적을수록 신뢰할 수 있는 측정값이고 f가 커질수록 일반적으로 구간의 길이는 길어진다.

III. 연구동향

3.1 센서 퓨전 알고리즘에 시스템 모델 및 공격자 모델 [6], [7], [8]

이번 절에서는 센서 퓨전 알고리즘에서 공통적으로 제안하는 시스템 모델과 공격자 모델을 정의한다.

3.1.1 시스템 모델

센서 퓨전 알고리즘에서는 공통적으로 다음과 같은 시스템 모델을 가정한다.

1. 하나의 물리량을 측정하기 위해 N개의 센서를 이용한다.
2. 센서는 공유된 버스로 연결되어 모든 측정값은 모든 노드에 broadcast 방식으로 전달한다.
3. 센서는 일정한 주기로 측정을 반복한다.
4. 컨트롤러는 매 라운드 마다 N개의 센서로부터 측정값을 받고 퓨전 알고리즘을 실행한다.

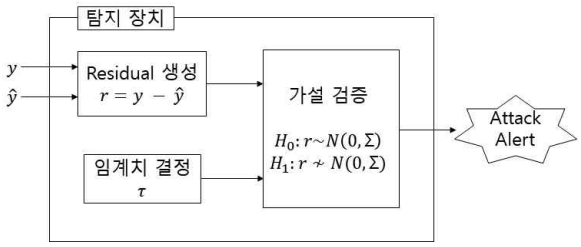
3.1.2 공격자 모델

1. 공격자는 공격에 성공한 센서의 출력 값만 위·변조가 가능하다.
2. 센서는 공유된 버스로 통신하기 때문에 공격자는 공격에 성공한 센서를 통해 다른 센서의 측정값을 알 수 있다.
3. 공격자는 몇 개의 센서 정보를 위·변조하여 퓨전 알고리즘의 출력 값(구간의 크기)을 최대화하는 것을 목표로 한다.

3.2 스케쥴링 기법을 이용한 센서 퓨전 알고리즘에 대한 연구 [6]

R. Ivanov 등은 Mazullo의 센서 퓨전 알고리즘[9]을 기본 개념으로 이용하여 공격자가 센서 측정값을 위·변조하였을 때 그 영향을 최소화하는 통신 스케쥴링 기법을 제안했다.

해당 논문에서는 센서 측정값의 구간 길이에 따라서 오름차순으로 정보를 전송하는 방식과



<그림 2> 탐지 알고리즘

내림차순으로 전송하는 방식을 비교했다. 공격자는 공유된 버스를 통해 자신이 위·변조한 정보를 주입하기 전 모든 측정값을 볼 수 있고 이를 기반으로 퓨전 구간의 크기가 최대가 되게 하는 위·변조한 정보를 주입한다. R. Ivanov 등은 많은 실험을 통해 오름차순으로 정보를 전송하는 방식이 더 공격의 영향을 줄일 수 있다는 것을 발견했다.

3.3 칼만 필터를 기반의 추정 기법을 이용한 센서 퓨전 알고리즘 [7]

S. Lee 등은 여러 개의 센서의 통합과 위·변조탐지 알고리즘을 위해 칼만 필터 기반의 추정기법을 제안하였다.

기존의 하나의 센서에 대한 추정값은 주어진 행렬 A, B, C에 대해 상태공간모델을 통해 식(1)과 식(2)로 나타낼 수 있다.

$$x(t+1) = Ax(k) + Bu(k) \quad (1)$$

$$y(k) = Cx(k) + w(k) \quad (2)$$

여기서 x는 상태벡터, y는 출력벡터, u는 제어입력벡터를 의미한다. 위에 식에 칼만 필터를 적용하여 여러 개의 센서를 통합하면 다음 상태의 추정값은 식(3)과 같이 나타낼 수 있다.

$$\hat{x}(t+1) = A\hat{x}(k) + Bu(k) + K[y(k) - \hat{y}(k)] \quad (3)$$

이를 이용하여 최종적으로 탐지 알고리즘은 <그림2>와 같은 방법으로 구한다. 해당 연구는 이전 상태를 바탕으로 현재의 상태에 대해 위·변조 탐지 할 수 있다는 점에서 의의가 있다.

3.4 history based pairwise inconsistency를 이용한 센서 퓨전 알고리즘 [8]

K. Yang 등은 Mazullo의 센서 퓨전 알고리즘[9]을 기본 개념으로 이용하여 퓨전 구간과 historical 측정을 사용하기 위해 가상의 센서를 추가하고 가상의 센서와 실제 센서 사이의 pairwise inconsistency를 사용하여 위·변조 공격을 탐지하는 기법을 제안했다.

해당 논문에서는 불일치 그래프를 이용하는 방법[10]을 기반으로 한 위·변조 공격 탐지 기법을 이용한다. 아래와 같은 3가지 상황을 약한 불일치로 판단한다.

1. 서로 다른 두 개의 센서의 측정 구간에 교집합이 없으면 두 개의 센서는 약한 불일치가 존재한다.
2. 각 센서의 측정 구간과 퓨전 구간에 교집합이 없으면 가상의 센서와 약한 불일치가 존재한다.
3. 각 센서의 이전 측정 구간과 현재 측정 구간에 교집합이 없으면 가상의 센서와 약한 불일치가 존재한다.

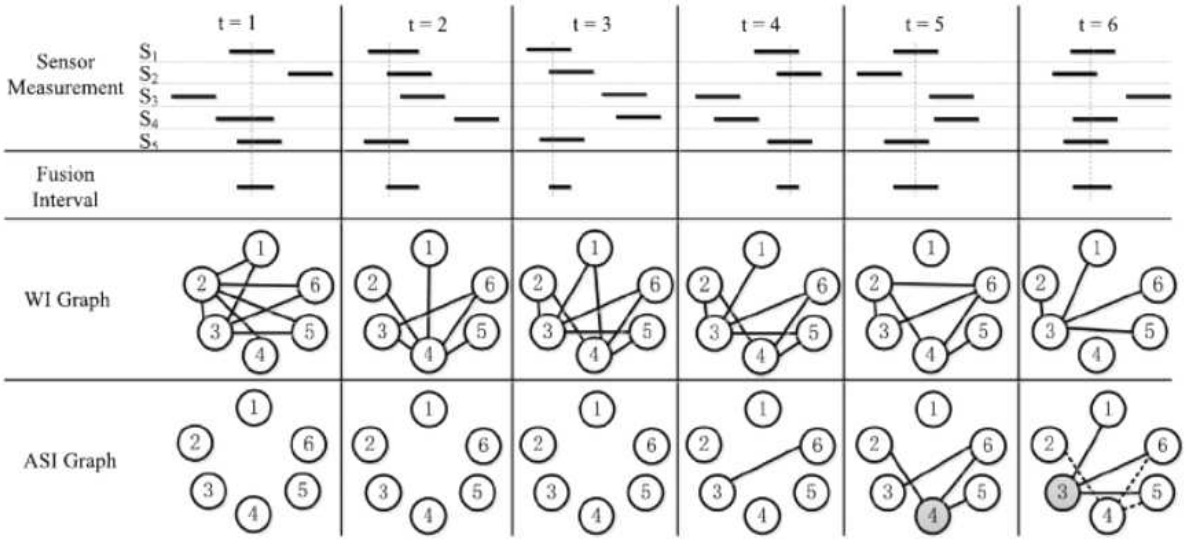
일정 기간동안 약한 불일치가 지속적으로 존재하면 이를 강한 불일치로 인식하고 최종적으로 특정 센서의 강한 불일치가 여러 개 존재할 경우 위·변조 공격을 당한 센서로 인식한다. 이를 도식화하면 <그림 3>과 같이 나타낼 수 있다. <그림 3>의 예제에서 t=5일 때 센서 4는 위·변조 공격을 당한 센서로 인식이 되고 t=6에서는 센서 3이 위·변조 공격을 당한 센서로 인식된다.

또한 해당 논문에서는 일정 기간동안 센서 측정값을 분석하여 특정 센서가 특정 시점 t에서 일시적 오류가 발생한 경우 이를 공격과 구분할 수 있는 알고리즘 [11]을 이용하여 위·변조 공격검출의 오탐율을 감소시켰다.

해당 연구는 기존의 센서 퓨전 알고리즘 여러 개를 융합하여 위·변조 공격에 대한 탐지의 성능을 개선 시킨 점에서 의의가 있다.

IV. 한계점 분석

기존의 기법 중 Mazullo의 센서 퓨전 알고리즘 [9]을 기반으로 설계된 기법 [6], [8]의 경우



<그림 3> 공격 탐지 예제 [8]

는 공격당한 센서의 수 f가 $\frac{N}{2}$보다 작은 경우에만 퓨전 구간의 신뢰성을 보장할 수 있다. 또한 스케쥴링 기법을 이용한 센서 퓨전 알고리즘 [6]의 경우 공격을 탐지하지 못하는 한계점을 가진다. 칼만 필터를 기반의 추정 기법을 이용한 센서 퓨전 알고리즘 [7]은 공격을 효율적으로 탐지하지만 실제 공격 상황에서 회복력을 가지지 못한다는 한계점을 가진다. 그리고 history based pairwise inconsistency를 이용한 센서 퓨전 알고리즘 [8]의 경우 공격자가 알고리즘을 잘 이해하고 있는 경우 주기적으로 공격한 센서에 올바른 측정값을 넣으면 강한 불일치를 피할 수 있으므로 공격당한 센서로 인식되지 않을 수 있다.

V. 결론

본 논문에서는 센서의 위·변조 공격에 회복력을 가지는 센서 퓨전 알고리즘에 대한 연구를 소개했다. 그러나 4장에서 분석한 대로 기존의 알고리즘들은 한계점을 가지고 있다. 향후 각각의 센서에서 전처리 과정에서 공격을 탐지하여 퓨전 알고리즘에서는 공격을 당한 센서를 배제함으로 올바른 센서값을 추정할 수 있는 센서 퓨전 알고리즘에 관한 연구를 진행할 예정이다.

[참고문헌]

[1] Navigant Reseach, https://www.navigantresearch.com/research/navigant-research-leaderboard-automated-driving-vehicles, Accessed: 2018-05-25

[2] Autonomous car, https://en.wikipedia.org/wiki/Autonomous_car, Accessed: 2018-05-25

[3] Shin H, Kim D, Kwon Y, Kim Y, “Illusion and Dazzle: Adversarial Optical Channel Exploits against Lidars for Automotive Applications”, Cryptographic Hardware and Embedded Systems – CHES 2017, pages 445-467, August 2017.

[4] Chen Yan, Wenyuan Xu, Jianhao Liu, “Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle”, DEF CON 24 Hacking Conference, August 2016.

[5] Petit J., Stottelaar B., Feiri M., Kargl F., “Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR”, Black Hat Europe 2015, November 2015.

[6] Radoslav Ivanov, Miroslav Pajic, and Insup Lee, "Attack-Resilient Sensor Fusion", Design Automation and Test in Europe Conference (DATE 2014) , pages 1-6. February 2014.

[7] Sangjun Lee, Yongbum Cho, Byung-Cheol Min, "Attack-Aware Multi-Sensor Integration Algorithm for Autonomous Vehicle Navigation Systems", 2017 IEEE International Confernce on Systems, Man, and Cybernetics (SMC), October 2017.

[8] Kang Yang, Rui Wang, Yu Jian, Houbing Song, "Sensor attack detection using history based pairwise inconsistency", Futer Generation Computer Systems, April 2018

[9] Keith Marzullo, "Tolerating failures of continuous-valued sensors", ACM Transactions on Computer Systems (TOCS), pages 284-304, November 1990.

[10] Junkil Park, Radoslav Ivanov, James Weimer, Miroslav Pajic, Insup Lee, "Sensor attack detection in the presence of transient faults", Proceedings of the ACM/IEEE Sixth International Conference on Cyber-Physical Systems (ICCPS), pages 1-10, April 2015.

[11] Ivanov, Radoslav Svetlozarov, "Context-aware sensor fusion for securing cyber-physical systems" Publicly Accessible Penn Dissertations, 2354, 2017.

소프트웨어 난독화 기법 평가 기술 연구 동향[1)]

백은수* 석재혁* 이재융* 이동훈*

*고려대학교 정보보호학과

Research Trend of Evaluation Technology on Software Obfuscation Technique

Eun-Su Baik*, Jae Hyuk Suk*, Jae Yung Lee*, Dong Hoon Lee*

*Korea University, Graduate School of Information Security

요 약

소프트웨어 난독화 기술의 공통적인 제약사항은 역공학에 대한 저항성을 측정하는 것이 어렵다는 점이다. 현재까지 제안된 소프트웨어 난독화 기법 평가에 대한 연구는 저조한 편이다. 난독화 기법 평가 기술의 부재는 보호 강도가 검증되지 않은 난독화 기법의 사용을 초래하고, 이는 소프트웨어의 중요 정보 유출의 위험성을 야기한다.

따라서 본 논문에서는 난독화 기법 평가 기술 연구의 필요성을 제시하고 최근 이의 연구 동향을 소개한다. 이를 바탕으로 난독화 기법 평가 기술의 요구사항과 보완사항을 정리하여 향후 연구계획을 제시한다.

I. 서론

소프트웨어 기술은 현대 사회에서 핵심적인 부분을 차지하고 있다. 그 결과 소프트웨어의 보호가 제대로 이루어지지 않으면 시스템의 치명적인 피해로 직결될 수 있다. 또한 소프트웨어의 지적재산권 침해 역시 큰 피해를 발생시킬 수 있기 때문에 소프트웨어의 보호 기술의 필요성은 늘 강조되고 있다. 난독화는 이러한 소프트웨어 보호 기술 중 하나로써 소프트웨어를 보호하는데 많이 활용되고 있다.

소프트웨어 난독화란 프로그램의 기능성은 유지하되 내부 로직을 이해하기 어렵도록 프로그램을 변형하는 기술이다. 난독화 기술은 합리적인 비용으로 소프트웨어를 보호할 수 있다는 장점이 있어 개발 업체에서 많이 사용하고 있다.

그러므로 과연 난독화 기술이 안전하게 소프트웨어를 보호하는지에 대한 의문점이 제기될 수 있다. 이를 검증하기 위해서는 난독화 기술에 대한 평가 기술이 함께 연구되어야 한다. 이에 [7]은 난독화 기술의 평가 지표로써 Potency(난독화된 코드를 사람이 이해하기 어려운 정도), Resilience(난독화된 코드를 자동화 기계가 분석하기 어려운 정도), Cost(난독화된 코드의 추가적인 시간/공간적 비용)를 제시하였다. 그러나 대부분의 난독화 기술을 제안하는 논문이나 도구들은 해당 기술의 Cost만을 평가 기준으로써 제시하며 보호 강도의 정량적인 값을 제시하지 않는다. 난독화 목적에 부합하는 지표는 Potency와 Resilience이기 때문에 이의 평가 기준도 수립되어야 한다. 또한 일반적이면서 객관적인 정량적 평가 모델이 있어야 난독화 기술의 보호 강도를 정확하게 평가할 수 있다. 그러나 다양한 환경과 난독화 기술들에 대한 평가를 할 수 있는 방법론의 부재로 아직 평가 기술에 대한 연구는 미흡한 실정이다.

대다수의 난독화 기술은 직관적으로 안전하게 보여질 뿐 보호 강도에 관한 가이드라인이 존재하는 것은 아니다. 그러므로 보호 강도가 검증되지 않은 난독화 기술을 사용하고 있는 실정이다. 따라서 난독화 기술의 보호 강도에 대한 가이드라인이 시급하다.

1) 본 연구는 고려대 암호기술 특화연구센터(UD170109ED)를 통한 방위사업청과 국방과학연구소의 연구비 지원으로 수행되었습니다.

clear.c

```
int main(){
  int a,b;

  a = 3;
  b = 5;

  printf("%d\n",a+b);
}
```

obfuscated.c

```
int main(){
  unsigned long x;

  /*  3L | (5L << 0x20) */
  x = 21474836483L;

  printf("%d\n",(int)(x&0xffff)+(int)(x>>0x20));
}
```

[그림 1] VarMerge 난독화 예시

본 논문에서는 현존하는 난독화 기술의 Potency와 Resilience에 대한 평가 기술 동향을 살펴보고 그들의 한계점을 분석한다.

본 논문의 구성은 다음과 같다. 2장에서는 난독화 기법 평가 기술 연구 동향을 이해하기 위한 배경지식을 설명한다. 3장에서는 최근 난독화 기법 평가 기술 연구 동향을 소개하고, 이를 바탕으로 4장에서 평가 기술 요구사항 및 보완사항을 정리한다. 마지막으로 5장에서 향후 연구계획을 제시하며 마무리한다.

Ⅱ. 배경지식

2.1 소프트웨어 난독화

소프트웨어 난독화란 프로그램의 기능성은 유지하되 내부 로직을 이해하기 어렵도록 프로그램을 변형하는 기술이다. 난독화는 크게 데이터 난독화, 제어흐름 난독화, 레이아웃 난독화 그리고 방지 난독화로 분류된다. 그 중에서 프로그램 분석시 대다수의 공격자가 목표로 하는 것은 데이터와 제어흐름 획득이므로 공격 대상은 데이터 난독화와 제어흐름 난독화에 초점을 맞춘다. 현재까지의 난독화 기법 평가 연구는 비교적 제어흐름 난독화에 대하여 많이 이루어진 편이다. 반면 데이터 난독화에 대한 평가 연구는 거의 이루어지지 않았다.

2.2 기호실행

기호실행[8](Symbolic Execution)은 프로그램의 입력값에 대한 실행 경로를 분석하기 위한 기법이다. 입력값을 기호화하여 이에 대한 실행 경로 획득이 가능하고, 역으로 특정한 실행 경로를 위한 입력값 생성도 가능하기 때문에 다양한 방법으로 활용 가능하다. 기호실행을 활용하는 대표적인 분야는 소프트웨어 테스트이다. 현재까지의 역난독화 연구는 기호실행을 기반으로 수행되는 경우가 많다. 기호실행을 수행할 수 있는 대표적인 도구에는 KLEE[6]가 있다.

Ⅲ. 난독화 기법 평가 기술 연구 동향

서론에서 언급하였듯이 이번 장에서는 난독화 기술 평가에 관한 최근 연구 동향을 제시한다. Potency와 Resilience에 대한 평가 기술에 관한 연구를 각각 두 가지씩 제시한다. 난독화된 프로그램의 Cost는 측정 방법이 매우 자명하기 때문에 별도로 평가 기술이 연구된 바 없으므로 본 논문에서는 해당 내용에 대하여 언급하지 않는다. 그 후 네 가지 연구의 기여도와 한계점을 바탕으로 향후 난독화 기술의 평가 연구 방향을 제시하고자 한다.

3.1 Potency 평가 기술에 대한 연구

이번 절에서는 데이터 난독화에 대한 Potency 평가 기법인 [1]과 제어흐름 난독화에 대한 Potency 평가 기법인 [2]를 소개한다. [1]의 경우 인간을 대상으로 하여 난독화 기술 분석의 어려움을 측정하는 방법을 제시하고, [2]의 경우 기계학습 알고리즘(ANN: Artificial Neural Networks)을 이용하여 난독화 기술 분석의 어려움을 측정하는 방법을 제시한다.

3.1.1 Assessment of Source Code Obfuscation Techniques[1]

[1]은 VarMerge[2)]([그림 1] 참고)라는 데이터 난독화 기술을 적용한 프로그램에 대하여, 이를 인간이 분석할 때 소요되는 시간을 측정함으로써 Potency를 제시하였다.

분석 대상 프로그램 2개와 이에 VarMerge 난독화를 적용한 프로그램 2개(총 4개)를 15명의 학생이 분

2) VarMerge란 여러 개의 스칼라 변수를 하나로 합치는 난독화 기법으로 적용 시 데이터 난독화 기법 중에서는 분석이 어렵다고 알려져 있음

석한 결과에 대하여 분석 성공 여부, 분석 수행 시간, 분석 수행 효율성을 측정함으로써 VarMerge가 프로그램 분석에 주는 영향을 통계 자료로 제시하였다.

본 논문은 데이터 난독화에 대한 Potency 평가를 시도한 최초의 연구이다. 기존에 제시되었던 [7]의 Potency 지표 표현방식은 프로그램 복잡도(Complexity, μ)를 수식으로 표현하였으나, 이는 실제 분석가의 난독화 분석 어려움 정도와는 다를 수 있다. 그렇기 때문에 본 논문의 실험 방식은 실제 공격상황과 유사한 환경에서 도출된 자료라는 점에서 의미가 있다고 볼 수 있다.

그러나 실험에 사용된 데이터 개수가 매우 적기 때문에 정확한 결과가 도출되지 않았을 확률이 높으므로 신뢰도가 떨어진다는 한계점이 있다.

3.1.2 Estimating Software Obfuscation Potency with Artificial Neural Networks[2]

[2]는 ANN을 이용한 원본 프로그램에 대한 제어흐름 난독화 기법 적용 후의 Potency 예측 모델을 제시한다. 본 논문은 앞서 언급하였던 프로그램 복잡도 수식 중 Cyclomatic Complexity(CC)와 Halstead Length(HL) 값을 예측할 수 있는 모델을 제시한다.

Diablo[5]가 제공하는 난독화 기법 중 제어흐름 난독화 기법 몇 가지를 분석 대상 프로그램에 적용하고, 기법 종류별로 CC와 HL의 변화량을 측정하여 데이터 셋을 생성하고 이를 ANN에 학습시킴으로써 예측 모델을 구성한다. 학습된 ANN을 이용하여 원본 프로그램의 CC와 HL 값으로부터 난독화 기법 적용 후의 각각의 값(CC, HL)을 예측할 수 있다.

본 논문에서 사용된 ANN은 실증적 결과에 근거하여 36 Feed-Forward Neural Networks로 구성되었다. 또한 Root Mean Square Error(RMSE) 값을 최소화하기 위하여 10-Fold Cross Validation을 이용하여 매개변수를 결정하였다.

본 논문의 ANN의 Potency 예측 결과는 실제 난독화 적용 후에 얻은 Potency의 데이터 분포와 매우 유사하게 나타났으며, 이러한 결과를 통하여 원본과 난독화가 적용된 프로그램의 Potency 관계를 선형적으로 표현할 수 있게 되었다. 또한 해당 ANN 모델을 활용하면, 프로그램의 난독화 적용에 소요되는 시간보다 100여 배 이상 빠르게 Potency 지표 수식 값을 예측할 수 있다. 또한 본 연구는 최적의 난독화 기법 결정에 활용할 수 있다.

그러나 본 논문에서 제시하는 예측 모델의 결과는 난독화 기법이 단일 적용되어있는 경우 정확하지만, 다중 적용된 경우에는 예측 정확도가 급격하게 떨어진다는 한계점이 있다. 실질적으로 난독화 기법은 다중 적용되는 경우가 많기 때문에 본 연구 결과를 이용하여 현실적인 최적의 난독화 기법 결정에 활용하기에는 무리가 있을 것으로 보인다.

3.2 Resilience 평가 기술에 대한 연구

이번 절에서는 자동화 공격에 대한 Resilience 평가 방법론을 제시한 [3], [4]의 연구를 제시한다.

3.2.1 A Framework for Measuring Software Obfuscation Resilience against Automated Attacks[3]

[3]은 임의의 난독화 기법에 대하여 공격자 모델과 난독화 기법의 안전성에 대한 개념을 정의하여 Resilience 평가 방법론을 제시한다. 그 후 이전의 역난독화 연구를 해당 방법론에 대응시킨 결과를 제시하였다.

본 연구의 방법론은 원본 프로그램의 제어흐름과 이의 데이터 획득을 목표로 하는 공격자에 대한 개념을 각각 정의한다. 그 중 가장 능력이 좋은 Best Attacker의 개념을 정의하고 Best Attacker의 공격 수행능력을 기준으로 안전함이 보장되는 개념을 정의한다. 이를 바탕으로 특정 난독화 기법의 안전성 보장을 확인한다. 본 연구에서는 Tigress Diversifying C Virtualizer[3]에서 제공하는 몇 가지 난독화 옵션으로 라이센스 검증 루틴을 난독화하며, 이를 제안하는 방법론에 적용함으로써 안전성 검증을 수행하였다.

본 연구에서의 공격자 목표는 라이센스 검증을 통과하는 것이다. 공격자는 KLEE Symbolic Execution Engine을 사용함을 가정하고 공격 수행에 소요되는 시간을 측정한다.

본 연구 수행결과로써 KLEE에 대한 Resilience를 실험적으로 평가하였다. 타 연구의 Resilience 평가는 공격 성공 여부만을 제시하였지만, 본 연구에서는 공격의 기준 시간을 정의하는 방법론을 추가적으로 제시하여 상호비교가 가능한 평가 체계를 구축하였다. 해당 결과는 KLEE가 아닌 타 분석도구에 대해서도 적용이 가능하여 일반성을 가지고 있다.

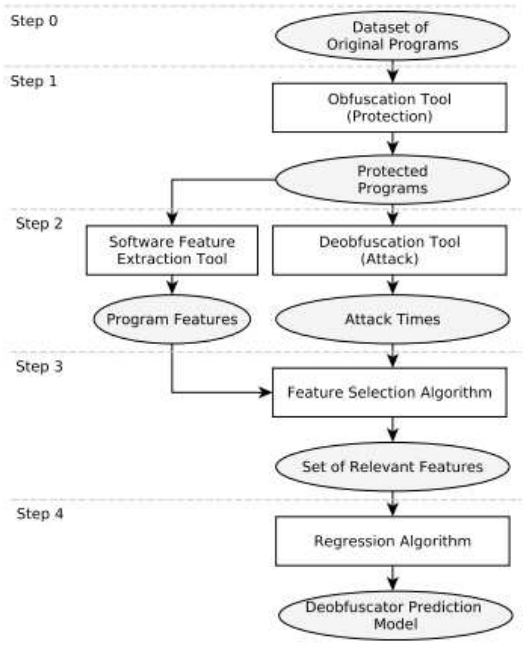
3) http://tigress.cs.arizona.edu/

그러나 해당 논문에서는 Best Attacker로써 KLEE를 지정하였는데, 이의 타당성이 별도로 검증되지 않았다. 또한 수행한 실험 결과 중에서 KLEE가 공격에 실패했던 경우가 존재하였고 이 경우, 안전성 보장의 기준 시간을 설정하지 못한다는 한계를 보였다.

3.2.2 Predicting the Resilience of Obfuscated Code against Symbolic Execution Attacks via Machine Learning[4]

[4]는 난독화 기술의 Resilience를 측정하며, 해당 지표에 영향을 크게 주는 소프트웨어 특성을 찾는 방법론을 제시한다. 추출된 소프트웨어 특성에 대한 회귀 분석 모델을 적용하여 자동화된 공격에 대한 Resilience를 예측한다.

우선 해당 연구에서 사용하기 위한 원본 프로그램 데이터 셋을 생성한다. 그 후 원본 프로그램을 평가 대상 난독화 도구를 이용하여 난독화 기법을 적용한다. 난독화된 프로그램에 대하여 자동화된 공격에 소요되는 시간을 기록한다. 동시에 난독화된 프로그램의 소프트웨어 특성 값을 추출한다. 추출된 특성 값에 특성 선택 알고리즘을 적용하여 자동화된 공격 소요시간에 영향을 주는 특성 셋을 추출한다. 마지막으로 추출된 특성 셋을 기계학습 알고리즘에 적용하여 Resilience를 예측하는 회귀 분석 모델을 설계한다. 이의 전체적인 프로세스는 [그림 2]와 같다.



[그림 2] Resilience 예측 모델 생성 과정

해당 논문이 제시한 방법론으로 난독화된 프로그램의 Resilience를 예측한 결과를 제시하였으며, 이의 정확도는 80% ~ 90%에 달한다. 또한 Resilience를 예측하기 위한 일반적인 방법론을 제시했다는 점에서 타 연구와의 차별점을 가진다.

그러나 해당 결과는 자신들이 생성한 데이터 셋[4]에 대해서만 해당 정확도를 가지며, 실제적인 프로그램에 대해서는 Resilience 예측 정확도가 많이 떨어짐이 제시되었다. 따라서 해당 예측 모델의 정확성을 높이기 위해서는 학습 과정에도 실제적인 프로그램이 활용되어야 할 것으로 보인다.

Ⅳ. 평가 기술 요구사항 및 보완사항

본 논문에서는 Potency와 Resilience 평가 기술에 관한 연구를 제시하였다. 이번 장에서는 평가 기술 요구사항을 정리함으로써 향후 평가 기술 연구를 위하여 보완되어야 하는 사항을 정리하고자 한다. [표 1]은 기존 연구에서 제시된 평가 기술 연구의 요구사항을 정리하며, 더불어 평가 기술 연구를 위한 보완사항을 함께 제시한다.

4.1 기존 연구의 평가 기술 요구사항

기존 난독화 기술 평가 연구를 살펴보았을 때 정확한 평가를 하기 위해서 고려할 점은 데이터 수집, 기술 검증 그리고 평가 요인 등으로 볼 수 있다.

데이터 수집 면에서는 다양한 실 데이터의 특성을 반영한 충분한 수의 데이터 셋 수집이 이루어져야 정확한 분석결과를 도출해 낼 수 있다. 또한 이러한 데이터 셋의 수집을 위한 방안 또는 기준이 제시되어야 평가 주체와 무관하게 객관적인 결과가 나올 것이다. [4]에서는 라이센스 검증 루틴으로 이루어진 데이터 셋을 생성하기 위한 C Program Generator 구현 방법/결과를 제시한다.

또한 향후 연구될 난독화 평가 기술은 일반성을 가지면서 이의 검증 결과도 제시되어야 신뢰할 수 있다. [3], [4]는 일반화시킨 난독화 평가 기술을 제시하였으므로 환경에 무관하게 적용될 수 있다.

그리고 평가 대상 지표에 영향을 주는 요인은 유일하지 않기 때문에 이를 다양하게 구성하여 복합적으로 지표를 측정하여야 한다. [1]의 경우 Potency에 대한 평가 요소로 공격 성공 여부와 시간, 효율성을

4) C Program Generator, 본 논문 저자들이 구현한 간략화된 프로그램 랜덤 생성기가 생성한 데이터 셋임

항목		해당 연구	미해당 연구
데이터 수집	충분한 수의 데이터 셋 수집	[2], [4]	[1], [3]
	실 데이터의 특성을 반영한 다양한 데이터 셋 수집	[1]	[2], [3], [4]
	데이터 셋 수집 방안 제시	[4]	[1], [2], [3]
기술 검증	제안하는 평가 기술 검증 결과 제시	[1], [2], [4]	[3]
	제안하는 평가 기술 일반성 제시	[3], [4]	[1]. [2]
평가 요인	평가 대상 지표의 평가 요인 다양화	[1]	[2], [3], [4]
보완사항	**다양한 공격 기법 및 난독화 기술 간의 비교 평가 방안 제시**	**(현존하는 연구 중에서는 해당사항 없음)**	
	대상 프로그램 특성에 따른 평가 점수 보정 방안 제시		
	평가 대상 지표 간 종합적 평가 점수 제시		
	평가 기술 제안에 활용되는 분석 모델 적합성 검증		

[표 1] 평가 기술 요구사항 및 보완사항

함께 고려하였다. [1]을 보완하여 향후 연구에서는 Potency 지표를 고려할 때, 인간의 공격 수행 결과/시간과 [2]의 프로그램 복잡도를 복합적으로 고려하여 나타내는 것이 다방면의 특징을 고려하므로 객관적인 평가를 나타낼 수 있을 것으로 예상된다.

4.2 기존 연구의 평가 기술 보완사항

4.1에서 제시한 평가 기술 요구사항은 보완해야 할 점이 있으며 이를 [표 1]의 보완사항에 제시하였다.

우선 다양한 공격 기법 및 난독화 기술 간의 비교 평가 방안이 제시되어야 한다. 난독화 평가 기술의 목적 중 하나는 평가 대상 난독화 기술이 타 난독화 기술에 비해 얼마나 우수한지를 입증하는 것이다. 따라서 난독화 기술간의 지표 비교가 가능하여야 한다.

또한 대상 프로그램 특성에 따른 평가 점수 보정 방안과 평가 대상 지표 간 종합적 평가 점수도 제시되어야 한다. 예를 들어, 문자열 암호화 기법의 경우 해당 프로그램에 문자열이 많은 경우 난독화 적용 범위가 넓어져서 해당 기법이 적용된 프로그램의 분석에 더 많은 시간이 소요될 수 있다. 그러나 이는 프로그램 고유의 특성으로 인한 결과이므로 이에 대한 보정을 하여야 정밀한 평가 결과를 제시할 수 있을 것으로 예상된다.

평가 대상 지표 간 종합적 평가 점수 제시가 필요한 이유는, 예를 들어, 실제 프로그램 분석은 인간이 자동화된 도구를 활용하여 분석을 시도하는 경우도 있으므로 Potency와 Resilience를 동시에 고려한 평가 점수를 제시할 수 있어야 전반적인 평가 및 활용이 가능할 것으로 보인다.

마지막으로 평가 기술 제안에 활용되는 분석 모델의 적합성 검증이 필요하다. [1]의 경우 다량의 데이터를 대상으로 하는 분석 모델을 이용하여 실험 결과를 분석하였다. 그러나 [1]의 데이터의 개수는 해당 분석 모델을 적용하기에는 매우 부족하므로 적절한 모델을 사용했다고 볼 수 없고, 실험 결과 또한 신뢰하기 어려울 수 있다.

Ⅴ. 결론

본 논문에서는 최근 난독화 기법 평가 기술 동향을 소개하고 이들의 기여도와 문제점을 분석하였다. 그리고 이를 바탕으로 현재 난독화 기법 평가 기술의 요구사항을 정리하고 이에 따른 보완사항을 제시하였다. 본 논문은 기존의 난독화 평가 기술을 정리하고 이의 향후 연구방향을 제시하였다는 점에서 의미가 있다고 볼 수 있다.

본 논문에서 제시하는 내용을 바탕으로 하여 보완사항을 만족하는 난독화 기법 평가 기술 연구를 수행할 예정이다. 이러한 평가 기술의 연구는 추후 더욱 강화된 난독화 기술을 연구함에 있어 기준과 지표가 될 것으로 기대하는 바이다

[참고문헌]

[1] Viticchié, Alessio, et al. "Assessment of source code obfuscation techniques." Source Code Analysis and Manipulation (SCAM), 2016 IEEE 16th International Working Conference on. IEEE, 2016.

[2] Canavese, Daniele, et al. "Estimating Software Obfuscation Potency with Artificial Neural Networks." International

Workshop on Security and Trust Management. Springer, Cham, 2017.

[3] Banescu, Sebastian, Martín Ochoa, and Alexander Pretschner. "A framework for measuring software obfuscation resilience against automated attacks." Proceedings of the 1st International Workshop on Software Protection. IEEE Press, 2015.

[4] Banescu, Sebastian, Christian Collberg, and Alexander Pretschner. "Predicting the resilience of obfuscated code against symbolic execution attacks via machine learning." Proceedings of the 26th USENIX Security Symposium. 2017.

[5] Van Put, L., Chanet, D., De Bus, B., De Sutter, B., De Bosschere, K.: Diablo: a reliable, retargetable and extensible link-time rewriting framework. In: 5th IEEE International Symposium on Signal Processing and Information Technology, pp. 7 - 12 (2005)

[6] C. Cadar, D. Dunbar, and D. R. Engler. Klee: Unassisted and automatic generation of high-coverage tests for complex systems programs. In OSDI, 2008.

[7] Collberg, Christian, Clark Thomborson, and Douglas Low. A taxonomy of obfuscating transformations. Department of Computer Science, The University of Auckland, New Zealand, 1997.

[8] Symbolic Execution. https://en.wikipedia.org/wiki/Symbolic_execution

2018 한국정보보호학회 하계학술대회

B5 관리정책교육 2

이 경 헌 (부경대학교)

- **ICT 기반 보안 개념과 영역에 관한 조사 연구**
  전민서, 나원철, 장항배
- **보안성숙도 모델을 활용한 정보보호 관리수준 점검방안에 관한 연구**
  이상규, 김인석
- **가상화폐 거래소의 보안성 확보를 위한 정보통신망 이용촉진 및 정보보호 등에 관한 법률 개정(안) 제시**
  전형율, 오장욱, 서정택
- **데이터베이스 삭제 방법과 관련 법률의 지시사항 격차 확인을 통한 개선방향 제시**
  임창완, 조성영
- **딥 러닝을 활용한 CVSS 점수 예측에 관한 연구**
  김현우, 송기범, 류승진, 윤한준, 이만희

ICT 기반 보안 개념과 영역에 관한 조사 연구

전민서*, 나원철**, 장항배***

*더존비즈온 포렌식센터

**중앙대학교 일반대학원 융합보안학과

***중앙대학교 경영경제대학 산업보안학과

Research on ICT-Based Securty Concepts and Domains

Minseo Jeon*, Onechul Na**, Hangbae Chang***

*Forensic Center, Duzon Bizon

**Department of Security Convergence, Chung-Ang University.

***Department of Industrial Security, Chung-Ang University

요 약

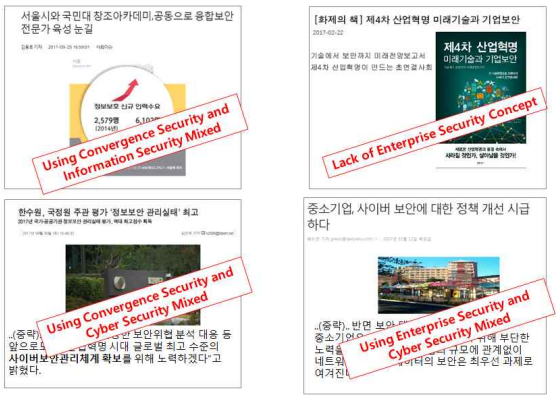
꾸준히 발생하는 보안 사고와 그에 따른 피해의 규모가 커짐에 따라 사회의 보안에 대한 관심이 커지고 있으며 학문적 관심과 연구의 양도 지속적으로 증가하고 있다. 하지만 이러한 관심과 연구의 양적 증가에도 불구하고 '보안'과 '안전'에 대한 용어가 혼용되고 있으며 다양한 보안 용어들의 개념적 정의가 명확하게 이루어지지 않은 채 연구가 이루어져 왔다. 이로 인하여 보안은 학문적 정체성을 확보하지 못한 실정이다. 따라서 본 연구에서 혼용하고 있는 다양한 보안 용어를 선정하고 그 용어들의 개념을 국내외 문헌 분석을 기반으로 개념을 정리한 후, 정리한 결과에 대한 전문가들의 합의를 도출하고자 하였다. 본 연구를 통하여 관련 연구자들에게 용어의 혼용으로 인하여 발생할 수 있는 오류를 방지하고 더 나아가 보안의 학문적 정체성 확립에 조금이나마 기여하고자 한다.

I. 서 론

ICT융합 新산업이 확산됨에 따라 경제와 산업 발전에 많은 이익을 가져다주었지만 동시에 보안 측면에서 양날의 검으로 큰 재앙이 되어 다가올 수 있다. 보안 사고에 활용되는 공격수법이 지능화되고 피해 규모 또한 큰 사건들이 발생하고 있다. 이러한 보안 위협에 맞서 산업계에서는 보안이 더 이상 선택이 아닌 필수로 인지하고 비즈니스 영역 전반에 걸친 보안 대책을 강구할 필요성을 느끼고 있으며 이에 필요한 보안 전문 인력에 대한 수요가 늘고 있다. 학계에서는 보안을 하나의 학문으로서 연구하고 보안 전문 인력을 양성해내는 보안 관련 학과가 신설되어 운영되고 있다. 하지만 보안의 중요성과 나날이 증가하는 사회의 관심에도 불구하고'보안'과 '안전'에 대한 용어가 혼용되고 있으며 다양한 보안 용어들의 개념적 정의가 명확하게 이루어지지 않은 채 연구가 이루어져 왔으며 이로 인하여 보안의 학문으로서의 독자적인 정체성을 확보하지 못하였다.

실제로 보안 개념을 혼용하고 있거나 명확한 정의가 부재된 상태로 보안 개념을 사용하고 있는 사례를 다음 그림과 같이 기사와 도서에서 쉽게 찾아볼 수 있었다. 기사 제목에서 융합보안 전문가를 명시하였지만 기사의 내용은 융합보안이 아닌 정보보안 인력수요 통계자료를 사용하며 정보보안의 개념을 사용하고 있었다(상단 좌측). 다른 기사에서 정보보안과 사이버보안의 개념을 동일하게 여겨 기사 제목과 내용에서 둘의 개념을 혼용하고 있음을 알 수 있었다(하단 좌측). 또한 기업보안의 명확한 개념이 정립되지 않아서 정보보안과 사이버보안 자료를 근거 자료로 잘못 사용되고 있었다(하단 우측). 기사뿐만 아니라 도서에서도 보안 개념

의 남용 사례를 찾아 볼 수 있었다(상단 우측). '기업보안'이 도서의 제목에 포함되어 있으므로 굉장히 중요한 개념임에도 불구하고 실제 도서 내용에 기업보안 개념에 대한 명확한 제시되지 않았다.



<그림 1> Exaples of Using Security Concepts Mixed

이러한 관점에서 보안이 학문으로서 정체성을 확립하기 위해서 보안에 대해 연구자들의 동일한 개념을 합의하는 것이 필요하다고 생각된다. 현재 보안의 성격 상 같은 연구주제라 하더라도 다양한 학문분야에 걸쳐 진행되고 있으며 동일한 용어에 대하여 서로 다른 의미로 사용하고 있어 학문적 교류와 발전에 어려움을 겪고 있다.

따라서 본 연구에서 혼용하고 있는 다양한 보안 용어를 제시하고 그 용어들의 개념을 국내외 문헌 분석을 기반으로 개념을 정리한다, 마지막으로 전문가 델파이조사와 라운드테이블 회의를 통하여 정리한 결과에 대한 전문가들의 합의를 도출하고자 하였다.

II. 선행연구

2.1 보안 개념 관련 연구

앞서 언급한 바와 같이 본 연구에서는 혼용하고 있는 보안 용어를 선정하고 그 개념을 정리하고자 한다. 국립국어원의 표준국어대사전과 옥스퍼드 사전에서 정의하고 있는 안전(Safety)과 보안(Security)의 의미를 살펴본 바, 두 단어 모두 공통적으로 '위험'과 '보호'라는 단어를 내포하고 있었다. 하지만 안전(Safety)은 단순히 상태를 말하고 있는 반면에 보안(Safety)은 보호하는 활동이라 정의하며 좀 더 적극적인 의미를 내포하고 있었다. 또한 주체로 둘의 차이가 나타났는데, 안전(Safety)은 위험과 사고가 나지 않는 상태로 만들 주체가 명시되지 않았다. 하지만 보안(Security)은 사회의 안녕, 국가, 건물 등 보호대상을 명시함으로써 보호하는 활동에 중점을 두며 책임의 주체를 유추해 볼 수 있었다.

정필운[1]은 그의 연구에서 사이버보안, 정보보안, 정보보호, 사이버안전 등의 개념이 어떻게 정의될 수 있으며 서로 어떤 상관성이 있는지 정리하고, 정보통신기술로 모든 것이 연결되는 세상에서 정보통신에 대한 침해행위에 대응하는 것을 지시하는 개념으로 어떠한 개념을 사용하는 것이 가장 적합한지 탐색하고자 하였다.

김정덕 외[2]는 융합보안에 대한 국외의 연구를 참고하여 국내에서 혼용되고 있는 융합보안의 개념을 재정립하고 융합보안을 통합보안과 복합보안 측면에서 분석함으로써 향후 융합보안 적용 시 고려해야할 접근 방법을 제시하였다. 융합보안에 대한 정의를 위해 국외의 다양한 연구기관에서 제시된 융합보안 개념을 참고하였다.

또한 이창무[3]는 보안이라는 개념의 모호성이라는 문제점을 파악하고 산업보안을 제목으로 설정한 모든 학술지 논문을 대상으로 조사를 했다는 점에서 의미가 있다. 또한 국내외 문헌과 표준문서에서 제시한 개념을 종합한 다른 연구와 달리 이론화와 개념화에 대해 깊은 고민을 하였던 연구였다.

2.2 개념 정립 관련 연구

본 연구의 가장 중요한 목표는 보안 개념을 정리함으로써 보안의 학문적 정체성 확립에 기여하는 것이다. 어떠한 분야가 학문으로 성립되기 위해서는 첫째, 고유한 분석의 단위가 존재하고 둘째, 인접 분야와는 구별되는 목표와 그에 따른 방법론이 정당하여야 한다고 하였다[4]. 이러한 이론의 연장선상에서 개념에 대한 연구를 용어 이론의 중심이자 출발점[5]이라고 볼

수 있을 것이다.

III. 용어작업

3.1 용어작업 기준 선정

용어작업 기준으로 제시된 ISO 704 및 남북통일 표준화 원칙은 절대적인 원칙은 아니지만 용어 작업에 있어 중요한 정보를 제공하고 있으므로 용어작업 기준 선정에 충분히 고려되어야 한다. 따라서 위 원칙들을 존중하면서 현재 실정에 맞게 수정하여 기준을 '명료성', '배타성', '포괄성'으로 선정하였다.

명료성의 경우 ISO 704와 남북통일 표준화 원칙에서 가장 첫 번째로 꼽는 투명성(Transparency)과 개념표현의 정확성을 참고하였다. 개념의 가장 주된 특징을 반영하고 애매혹은 모호한 표현 없이 개념을 표현하고 있다면 명료성이 높은 점수로 나올 것이라 예상하였다.

배타성은 전통적 용어 이론의 원리 중 '제4원칙 일의성 원칙'이 이론적 배경이 되었다. 전통적 용어 이론의 원칙은 다음 표와 같이 크게 다섯 가지로 볼 수 있다. 배타성의 이론적 배경이 된 '제4원칙'은 인지 용어론자들로부터 용어의 자율적인 발전과 변화를 규제한다는 비판을 받는다. 하지만 대표적인 사회 인지 용어론자인 Temmerman[6]은 '제4원칙'이 전문용어에 효과적이라 관찰하였다.

포괄성의 경우 현재 보안 개념이 혼용되는 원인 중 하나인 외국어로 된 개념을 국내로 받아들이면서 번역의 오류로 인한 개념상의 혼란이 야기하는 점을 새로 제시하는 개념에서 바로잡고자 하였다. 따라서 적합성(Appropriateness), 학술적 체계성 및 원어와의 대응관계 등을 고려하여 본 기준을 선정하였다.

3.2 용어작업을 위한 보안 개념 선정

기사 검색 DB를 통하여 수집된 총 2,193건의 기사에서 NetMiner를 통한 키워드 '보안'과의 연관성 분석을 진행하였으며 그 결과는 다음과 같다. 보안과 미국, 국가정보원, 청와대가 연관성이 매우 높은 것을 알 수 있었다. 하지만 본 연구의 주제인 보안 개념과 관계가 낮은 인물, 기관, 장소를 제외한 결과 보안 관련 개념은 '정보보안', '사이버보안', '기업보안', '산업보안', '연구보안', '융합보안'으로 나타났다. 또한 보안 개념 노드의 사이즈, 밀도, 연결 분포 등을 미루어보아 보안 개념 자체에 대한 관심이 미미하다고 볼 수 있다.

선정된 보안 개념에 대하여 새로운 개념 제시를 위하여 국내외 문헌연구 분석을 통하여 아래와 같이 정리하였다. 제시한 개념이 적절성 평가 기준에 부합하고자 명료성, 배타성, 포괄성 기준을 참고하여 정리하였다. 또한 설문에 참여하는 전문가들의 이해를 돕고자 개념과 함께 개념을 도식화한 그림을 함께 첨부하였다.

<표 1> Summary of Security concept(Primary)

Terms	Concept
Security	Activities that maintain order and well being by protecting the objects in the environment from risk
	$\frac{\text{Object}}{\text{Environment}}$
Information Security	Activities to protect assets that have information from the viewpoint of information life cycle (generation ~ distribution ~ destruction)
	$\frac{\text{Information}}{\text{Environment}}$
Cyber Security	Activities to protect the object of cyberspace from threats
	$\frac{\text{Object}}{\text{Cyber Space}}$
Enterprise Security	Activities to protect assets (object) from threats for stable business activities of

	corporations (organizations) Asset / Organization
Industrial Security	① As a non-broad concept, industrial security means protecting an organization's technology. ② As a broad concept, industrial security means "security of the industry" that reflects the business characteristics of each industry
	Technology (1) / Organization + Value Chain (2)
Research Security	Activities to prevent leakage or infringement of major R&D outcomes that occurred during the entire implementation process of national R&D projects
	Research Contents / Research Organization + Time Dimension
Convergence Security	① Integration of security measures (physical security + information security) ② Creation of new value through fusion of security technology and other industries

IV. 연구결과

4.1 1차 전문가 조사 분석

상기 선정한 보안 용어와 그에 대한 개념에 대해 전문가들이 어떻게 평가하는지를 확인하기 위해 델파이조사를 실시하였다. 1차 전문가 조사지에서는 전문가 의견을 종합적으로 수집하는 차원에서 폐쇄형 및 개방형 형태로 질문지를 설계하였다. 예를 들어 "제시된 개념 외에 더욱 적절하다고 생각하는 개념과 그에 대한 이유를 적어주시기 바랍니다."와 같이 선정된 각각의 용어와 제시한 개념에 대해 개방형의 질문 형태를 제시함으로써 전문가들의 대표적 견해를 자유로운 분위기에서 수집하고자 하였다. 또한 필요시 전문가의 이해와 응답의 용이성을 위하여 개념을 도식화한 그림을 함께 제시하였다. 1차 조사를 실시한 결과 다음과 같은 응답을 얻을 수 있었으며 다음 표는 그 중 '보안'에 대한 결과를 정리한 것이다.

<표 2> Results of the experts evaluation of 'Security'(1st)

Terms	Respondent(n=15)				
	Evaluation	Frequency		Average	Standard-Deviation
Security	Clarity	Not very right	0	4.73	0.44
		Not right	0		
		General	0		
		Right	4		
		Very right	11		
	Exclusivity	Not very right	0	4.13	0.18
		Not right	0		
		General	4		
		Right	5		
		Very right	6		
	Inclusivity	Not very right	0	4.40	0.71
		Not right	0		
		General	2		
		Right	5		
		Very right	8		

조사 결과, '보안', '정보보안', '사이버보안', '기업보안', '산업보안', '연구보안', '융합보안'에 대한 명료성, 배타성, 포괄성 모두 평균값(표준편차)이 평균 이상으로 높게 도출되어, 선정한 보안 용어와 그에 대한 개념의 타당성이입증되었다.

4.2 2차 전문가 조사 분석

2차 전문가 조사는 라운드테이블 회의 방식으로 진행하였으며, 참가자 간 상하 구별 없이

자유롭게 의견을 나누며 수평적인 자유 토론을 거쳐 합의에 이르고자 하였다. 2차 전문가 조사는 1차 조사에 응답한 인원 중 전문성과 경력을 감안하여 6명을 선정하여 심층 논의가 이루어졌다. 1차 조사 결과의 자신의 의견을 서면으로 작성하고 상호 확인을 거친 후 토론 형식으로 진행되었다.

2차 조사 때 가장 심도 있는 이야기가 진행된 부분은 보안의 주체와 범죄 연관성 여부였다. 3차 조사에서는 이를 반영하여 보안의 주체와 범죄 연관성이 포함된 보안의 개념으로 수정하여 회의가 진행되었다. 또한 '보안'이라는 중심이 되는 개념에서 파생된 개념이 많기 때문에 '보안'의 명확한 개념을 정리하는 것이 그 무엇보다 우선시 되었다고 생각된다. 2차 조사 결과를 바탕으로 보안이 안전과 구별되는 부분은 인간의 개입 여부라고 생각된다. 더불어 피해 여부와 상관없이 인간의 실수에 의한 오용과 의도적 남용 모두 보안의 범주 안에 속한다고 보여진다.

또한 2차 조사 때 보안과 안전의 차이점 다음으로 많이 언급된 문제는 정보보안과 사이버보안, 기업보안과 산업보안의 차별성이 뚜렷하지 않다는 것이었다. 지적된 문제점을 반영하여 3차 조사 때 수정된 개념을 제시하고 회의가 진행되었다.

연구보안의 경우 지적된 사항을 반영하여 개념을 국가연구개발사업에 한정하지 않고 연구개발사업(R&D)을 진행하는 기업과 조직에도 적용이 되어 광의의 개념을 갖는 수정된 개념을 반영하여 3차 조사 때 수렴된 의견을 도출하고자 하였다.

4.3 3차 전문가 조사 분석

2차 조사 때 수렴된 전문가들의 의견을 반영하여 수정된 개념을 제시하고 2차 조사와 같은 방식으로 3차 라운드테이블 회의가 진행되었다.

회의가 진행되면서 제시된 개념의 배타성에 대한 문제점과 지적이 지속적으로 언급되었다. 하지만 3차 회의를 통하여 보안의 개념을 명확히 함으로써 각 개념이 보안에서 파생된 개념인 점을 미루어보아 각각의 개념이 완벽하게 배타적일 수 없다는 결론을 도출할 수 있었다. 더불어 보안은 사람의 범죄행위(실수에 의한 오용, 의도적 남용을 모두 포함)로부터 보호대상의 안녕과 질서를 유지하는 것이라는 개념을 도출할 수 있었으며 사람의 범죄행위라는 보안이 안전과 명확하게 구별되는 점을 전문가들의 의견 교환을 통해 도출할 수 있었다.

사이버보안과 정보보안의 모호성을 보호대상과 보호환경을 명확히 함으로써 전문가들의 합의를 이끌어낼 수 있었다. 하지만 기업보안과 산업보안의 모호성을 완벽하게 해소하기엔 다소 아쉬움이 남는 결과였다. 보안 개념의 연구가 활성화 되어 이 부분에 대해 좀 더 집중적으로 다루었으면 좋겠다는 전문가들의 의견이 있었다.

V. 결 론

본 연구를 통하여 '보안'과 '안전'이 갖는 차별성에 대해 전문가들은 의견을 주고받으며 다음과 같은 의견을 수렴할 수 있었다. 보안은 사람의 실수에 의한 오용과 의도적 남용으로 인한 범죄행위로부터 보호대상의 안녕과 질서를 유지하는 것이라는 개념을 도출할 수 있었으며, 여기서 사람의 실수 즉, 인위성이 안전과 구별되는 점이라 할 수 있다.

또한 보안과 그 외의 보안 개념들이 보안으로부터 파생된 점을 감안하여 각각의 개념이 완벽하게 배타적일 수 없다는 의견을 도출할 수 있었다. 하지만 보호대상과 환경의 차별성을 명확히 함으로써 개선된 개념으로 정리하였다.

본 연구의 방법이 전문가 델파이조사로 진행된 만큼 비교적 오랜 기간을 두고 지속적으로 살펴보았어야 했지만 조사 기간이 짧았던 점, 연구 주제에 대한 연구자의 역량이 부족하다는 점으로 인해 한계가 있다. 하지만 용어학의 용어작업 기준에 의하여 보안 개념을 정리하고 이에 대해 전문가들의 합의를 도출했다는 점에서 의의를 가진다. 또한 향후 연구에서는 현재 산업보안의 협의적 개념이 지나치게 한정되어 있다는 점에서 산업보안의 영역을 넓히는데 기여하고자 광의적 개념에 대한 추가적인 연구를 진행하고자 한다.

감사의 글

"본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음" (IITP-2018-2014-1-00636)

[참고문헌]

[1] Pil-woon Jung, "A Crictical Analysis on the Concept of Cyber Security," Yonsei Journal of Medical and Science Technology Law, 2(2), pp. 1-25, 2011.

[2] Jung-duk Kim, Kun-woo Kim, Yong-duk Lee, "The concept of convergence security and approach," Review of KIISC, 19(6), pp. 68-74, 2009.

[3] Chang-moo Lee, "A Critical Review of Industrial Security Concepts," Korean Security Science Association, 50, pp. 285-303, 2017.

[4] Cabré Castellví, M. T., "Theories of terminology: Their description, prescription and explanation," Terminology, 9(2), pp. 163-199, 2003.

[5] Felber, H., "Manuel de terminologie," Organisation des Nations Unies pour l'Education, la Science et la Culture, 1987.

[6] Temmerman, M., "Towards new ways of terminology description: The sociocognitive-approach," John Benjamins Publishing Company, 2000.

[7] Brinkley, D. L., and Schell, R. R., (1995). "Concepts and terminology for computer security,". Information security: An integrated collection of essays, pp. 40-97, 1995.

[8] Brooks, D. J., "What is security: Definition through knowledge categorization," Security Journal, 23(3), pp. 225-239, 2010.

[9] Castellví, M. T. C., and Cormier, M. C., "La terminologie: théorie, méthode et applications," A. Colin; Ottawa: Presses de l'Université d'Ottawa, 1998.

[10] Laprie, J. C., "In Dependability: Basic Concepts and Terminology," pp. 3-245, 1992.

[11] Mokkink, L. B., et al., "The COSMIN checklist for assessing the methodological quality of studies on measurement properties of health status measurement instruments: an international Delphi study," Quality of life research, 19(4), pp. 539-549, 2010.

보안성숙도 모델을 활용한 정보보호 관리수준 점검방안에 관한 연구

이 상 규[1]*, 김 인 석[2]†
고려대학교 정보보호대학원

A Study on the Level of Information Security Management using Security Maturity Model

Sang-kyu Lee,[1]† , In-seok Kim[2]‡
Graduate School of Information Security , Korea University.

요 약

최근 다양한 산업에 속하는 많은 기업에서 디지털 트랜스포메이션을 지향하며 디지털화를 급격히 진행하고 있고 이러한 현상으로 인해 더욱 다양한 정보보호 위협에 직면하게 되었다. 기업은 정보보호 관리체계 인증을 통해 정보보호에 대한 신뢰를 보장받고 있으나 세부영역에 대한 수준의 진단과 활용이 제한적이다. 보안 성숙도 모델은 기업의 정보보호 수준을 단계적으로 진단할 수 있고 개선해야 할 영역을 판단할 수 있음은 물론 기업의 특성과 수준에 맞는 목표 설정을 지원하는 도구가 된다. 본 논문에서는 보안 성숙도 모델인 O-ISM3과 C2M2를 비교하여 특징을 소개하고 ISMS의 통제항목과 성숙도 모델을 통해서 기업의 정보보호 관리체계 수준을 효과적으로 진단할 수 있는 방안과 활용방법을 살펴본다.

I. 서론

금융위원회는 2018년 3월 금융분야 데이터 활용 및 정보보호 종합방안을 발표한 바 있다. 인공지능, 사물인터넷과 함께 4차 산업혁명의 핵심기술로 손꼽히는 빅데이터의 안전한 활용을 보장하기 위한 보호조치로 정보활용과 관리 실태에 대한 상시평가 제도를 도입하겠다는 취지가 담겨있다[1]. 금융업뿐만이 아니라 전통적인 산업군에 속하는 많은 기업에서도 이른바 '디지털 트렌스포메이션'을 지향하며 비즈니스 모델의 전환을 준비하고 있다. 이와 같이 다양한 산업에서 디지털화가 급격히 진행되면서 기업은 더욱 많은 정보보호 위협에 직면하게 되었다. 그럼에도 불구하고 여전히 기업의 보안 관리자는 제한된 예산으로 효과적인 투자를 통해 끊임없이 발생하는 보안 문제를 해결해야 한다는 중대한 과제를 안고 있다.

기업들은 정보보호 관리체계(Information Security Management System)인증을 받음으로써 고객에게 보안관리 체계 구축과 정보보호 활동에 대한 신뢰를 보장받고 있다. 국제적으로는 ISO/IEC 27001과 같은 표준인증을 통해서 정보보호 관리체계를 구축, 운영하고 있으며 국내에서는 "정보통신망 이용촉진 및 정보보호 등에 관한 법률" 제47조, "정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령" 제47조에

* 주저자, sk239@korea.ac.kr
† 교신저자, iskim11@korea.ac.kr(Corresponding author)

서 제54조에 의거 평가 및 인증제도를 운영하고 있다[2].

이러한 인증제도는 기업의 정보보안 강화 활동을 위한 준비와 대응을 가능하게 하는 한편 인증제도 특성상 결과가 인증 또는 미인증으로 제한됨으로 관리체계를 구성하는 세부 영역에 대한 수준별 평가 결과 도출에 한계를 가진다[3]. 또한 이를 통한 세부적인 보안 수준측정과 분석이 어렵고 기업에서 투자를 결정하는 경영진과의 의사소통을 위한 도구로서의 활용성이 부족함에 따라 효과적인 정보보안 투자를 이끌어 내는 데에 한계가 될 수 있다.

이에 반해 보안 성숙도 모델의 대표적인 사례인 정보보안 관리 성숙도 모델 (Open Information Security Management Maturity Model : O-ISM3), 정보보호역량 성숙도 모델 (Cyberspace Capability Maturity Model :C2M2)은 기업의 정보보호 수준을 단계별로 진단할 수 있고, 기업 전반의 정보보호 역량 강화를 위해 시급히 개선해야 할 영역을 판단할 수 있음은 물론 각 기업의 특성과 수준에 맞는 목표 설정을 지원하는 효과적인 도구가 될 수 있다.

이에 본 논문에서는 성숙도 모델을 기반으로 하는 O-ISM3과 C2M2를 국내 정보보호 관리체계 인증(ISMS)과 비교, 분석하여 기업의 정보보호 관리체계를 영역별로 점검하고 그 수준을 측정할 수 있는 방법을 제안한다. 기업은 개선된 정보보호 관리수준 진단 방법을 통해 정보보호 수준을 단계적으로 평가할 수 있으며 이를 통해 효과적인 대책을 수립하고 발전시켜 나갈 수 있을 것이라 기대한다.

II. 관련연구

정보보호 관리체계란 조직이 보존해야 할 정보자산의 기밀성, 무결성, 가용성을 확보하기 위한 보호대책을 마련하고 위험기반 접근 방법에 기초하여 구축, 구현, 운영, 모니터링, 검토, 개선 등의 주기를 거쳐 정보를 체계적으로 관리하고 운영하는 전반적인 체계를 말한다[4]. 국제적으로는 ISO 27001:2013이 표준인증으로 인정받고 있으며 국내에서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」개정을 통해 2001년 7월부터 정보보호 관리체계 인증 제도를 도입한 후 현재까지 정보보호 관리체계(Information Security Management System) 인증 제도를 운영하고 있다.

2.1 정보보호 관리체계 인증제도(ISMS)

ISMS는 5단계 정보보호 관리과정과 13개 분야 정보보호 대책 총 104개의 통제항목으로 구성된다. 정보보호 관리체계 인증은 정보보호 관리체계의 구축과 유지, 지속적인 개선을 위한 요구사항을 제공하기 위해 개발되었으며 상세적인 항목의 점검을 통해 기업은 정보보호 정책과 활동의 일관성을 확보하여 보다 효과적인 정보보호 체계를 구축할 수 있다[5].

ISMS 인증을 획득한 기업은 지속 가능한 정보보호 관리와 운영을 위해 필요한 경영진의 지원을 이끌어 낼 수 있고 보유한 자산과 특정 상황에 적합한 통제수단을 도입하여 상황을 개선시킬 수 있다. 무엇보다 인증을 통해 얻을 수 있는 가장 큰 이점은 이해관계자들에게 신뢰성을 제공할 수 있다는 것이다. 이러한 이해관계자 신뢰를 바탕으로 정보보호 투자에 대한 효과적이고 경제적인 관리가 가능해 질 수 있다.

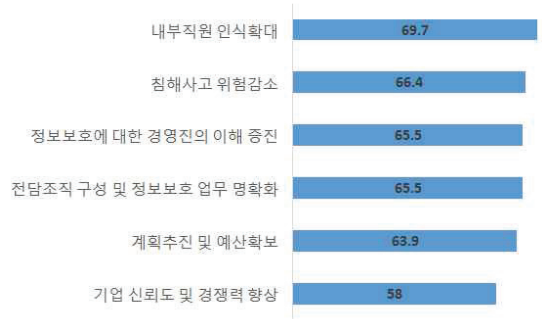


Fig 1. ISMS 인증효과

정보보호 관리체계 인증 의무 대상자 지정에 따라 ISMS 인증을 받은 사업자는 해마다 증가하고 있으나 의무 대상에 속하지 않는 업종과 기업의 인증은 활발하지 못한 실정이다.

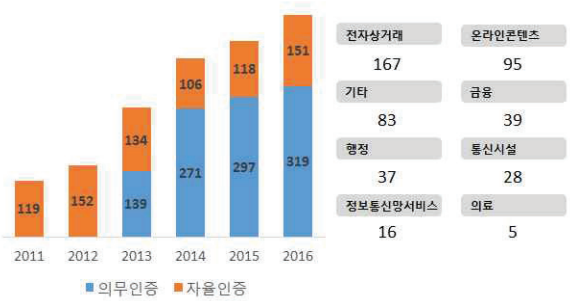


Fig 2. ISMS 인증 현황

2.2 정보보호 관리체계 인증의 시사점

기존의 정보보호 관리체계 인증제도는 정보보호 대책을 수립하고 시스템 및 서비스의 취약점을 점검하는 등 여러 가지 보안활동을 수행하지만 각각의 세부 활동이 포함된 영역에 대한 보안관리 수준이 명확하게 표현되지 못함에 따라 상세한 보안수준측정이 어렵다는 문제점을 안고 있다. 따라서 본 논문에서는 정보보호 관리체계를 구축하고 운영하는 기업이 정보보호 관리를 위한 영역별 상태를 수준별로 점검할 수 있고 더 나아가 이를 지속적으로 개선해 나갈 수 있도록 보안 성숙도 모델을 활용한 방안을 제안한다.

III. 보안성숙도 모델 분석

3.1 성숙도 모델 적용 방법 및 효과

성숙도 모델이란 특정 분야의 능력과 발전 정도를 나타내는 특성, 속성, 지표들의 집합이다. 예를 들어, 인증방법에 대한 성숙도 진행은 단순한 패스워드의 사용으로 시작하여 복잡한 패스워드 규칙의 적용, 주기적인 패스워드 변경 정책 적용, Two-factor 인증, Three-factor 인증과 같은 단계로 인증방법을 성숙시킬 수 있다.

A Maturity Progression for Authentication
Three-factor authentication
Two-factor authentication
Addition of changing every 60 days
Use of strong passwords
Use of simple passwords`

Fig 3. 인증 성숙도 단계

성숙도 모델에서 제공하는 내용은 일반적으로 우수사례의 기준이 되어 실제 구현 및 적용에 참고가 될 수 있으며 다른 표준이나 실무 규칙과 접목되어 통합될 수 있다. 또한 성숙도 모델을 통해 기업의 업무 내용, 절차 및 방법에 대한 현재 수준을 진단하고 개선을 위한 목표와 우선순위를 설정할 수 있는 가이드를 제공한다.

보안 성숙도 모델을 사용하여 얻을 수 있는 이점은 다음과 같다.

- 기업의 정보보호 관리 역량을 강화시킨다.
- 정보보호 관리체계를 효과적이고 일관성 있게 평가하고 벤치마크 할 수 있다.
- 정보보호 역량을 향상시키기 위한 수단으로 지식, 우수사례 및 관련 참고 자료를 공유할 수 있다.
- 정보보호 활동과 투자의 우선순위를 정하여 기업 보안 수준을 향상 시킬 수 있다.

보안성숙도 모델은 조직에서 일관된 정보보호 관리 수준을 진단하고 이를 의미 있는 방식으로 전달하며 정보보호 관리를 위한 투자의 우선순위를 선정하기 위해 사용된다.

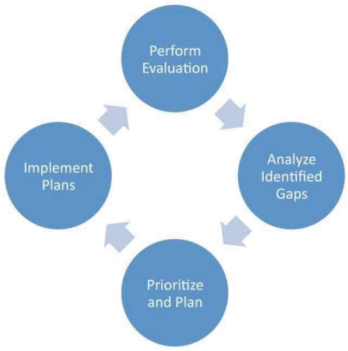


Fig 4. 성숙도 모델 활용 방법

정보보호 성숙도 목표 수준을 설정한 기업은 세부영역에 대한 수준 점검을 수행하고, 평가결과를 활용하여 목표한 수준과의 차이를 파악한다. 이후 차이를 극복하기 위한 계획을 수립하고 계획을 실행한다. 사업의 목표가 변경되고 위험 환경이 진화되면 이 프로세스는 다시 반복된다.

3.2 O-ISM3(Open-Information Security Management Maturity Model)

O-ISM3(Information Security Management Maturity Model)은 정보보호관리 성숙도 모델로 2011년 개방형 시스템 관련 컨소시엄 표준 단체인 오픈 그룹(The Open Group)에 의해 만들어 졌다. ISO/IEC 27001 정보관리체계의 이론과 실무 간의 격차를 좁히고 정보보호 관리와 성숙도 모델을 연계하고자 개발되었고 조직 내 ISO/IEC27001 구현을 최적화하기 위해 ISM3 모델을 사용할 수 있다[8].

3.2.1 O-ISM3 구성

ISM3은 일반적(generic), 전략적(strategic), 전술적(tactical), 운영(operational) 프로세스 영역으로 구분하고 45개 프로세스 활동을 구성하고 있다. 전략적 실무 활동을 통해 제시된 방향과 자원 제공을 바탕으로 전술적인 실무활동을 통해 정보보호 관리체계를 구현하고 최적화 한다. 이러한 과정은 지속적인 방법을 통해 개선되고 이를 통해 높은 수준의 보안 역량 성숙도를 달성 할 수 있게 된다.

가. 일반 프로세스(GP: Generic Processes) - 정보보호 관리체계를 구축하고 문서화하며 지속적으로 개선하기 위한 전반적인 관리과정을 다룬다.

나. 전략적 프로세스(SSP : Strategic-Specific Processes) - 정보보호 목적과 조정, 자원의 제공과 같은 정보보호 관리체계의 방향성을 다룬다.

다. 전술적 프로세스(TSP : Tactical-Specific Processes) - 정보보호 관리체계의 설계와 구현, 목표 정의, 자원관리 등 정보보호 관리체계를 구현하고 최적화하는 프로세스를 다룬다.

라. 운영 프로세스(OSP : Operational-Specific Processes) - 기술적인 처리수단에 대하여 정의된 목표의 달성을 위한 실행과 보고를 다룬다. 운영 프로세스는 운영 관리, 생명주기 통제, 접근과 환경 통제, 가용성 통제, 감사, 모니터링, 사고처리 등으로 구분된다.

3.2.2 O-ISM3 성숙도 단계

ISM3의 성숙도 단계는 Level1:초기(initial), Level2:관리되는(managed), Level3:정의된(defined), Level4:통제되는(controlled), Level5:최적화된(optimized) 단계로 구분된다. 각 단계에서 판단하는 관리 활동의 기준은 문서화 활동을 기본으로 실제 수행활동과 범위, 품질과 효율성 등이 기준이 된다.

Capability Level		Initial	Managed	Defined			Controlled	Optimized
Management Practices Enabled		Audit, Certify	Test	Monitor	Planning	Benefits Realization	Assessment	Optimization
Documentation		*	*	*	*	*	*	*
Metric Type	Activity		*	*	*	*	*	*
	Scope		*	*	*	*	*	*
	Unavailability[1]		*	*	*	*	*	*
	Effectiveness		*	*	*	*	*	*
	Load			*	*	*	*	*
	Quality						*	*
	Efficiency							*

Table 1. O-ISM3 성숙도 단계

3.3 C2M2(Cybersecurity Cpability Maturity Model)

정보보호 역량 성숙도 모델(C2M2, Cyber security Capability Maturity Model)은 지속되고 있는 모든 형태의 조직에 대한 정보 위협을 감소시키기 위해 2014년 2월 미국 국토안보부(DHS)와 에너지부(DOE)에 의해 개발되었다[11]. C2M2는 정보기술 및 운영기술에 필요한 자산과 운영환경과 관련한 정보보호 관리체계의 구현과 관리에 중점을 두고 있다.

3.3.1 C2M2의 구성

C2M2모델은 10개의 영역으로 구성되어 있고 각 영역은 정보보호 관리 수준과 기업이 해당 영역에서 갖춰야 할 능력, 그리고 이를 성숙시키기 위해 필요한 수행 활동으로 정의된다. 각 영역이 달성해야 하는 목표는 수행 활동을 포함하여 MIL(Maturity Indicator Level)를 기준 지표로 하여 성숙도 수준이 정의된다.

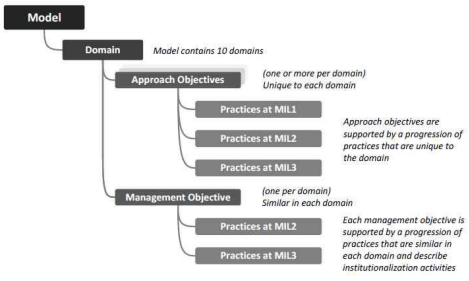


Fig 5. C2M2 모델과 영역 관계

모델을 구성하고 있는 영역은 아래와 같다

- 위험관리(RM) : 조직의 정보보호 위험을 식별, 분석 및 완화하기 위한 정보보호 관리 체계를 수립 운영하고 유지 한다.

- 자산, 구성 및 변경 관리(ACM) : 조직의 정보기술(IT) 및 운영기술(OT) 자산을 관리하여 중요한 인프라 및 조직 목표에 대한 위험에 대비한다.

- 계정 및 접근 관리(IAM) : 조직의 자산에 대한 접근을 제어하고 중요한 인프라 및 조직 목표에 대한 위험에 대비한다.

- 위협 및 취약점 관리(TVM) : 정보보호 위협 및 취약점을 탐지, 식별, 분석, 관리하고 이에 대응하기 위한 계획, 절차 및 기술을 수립하고 유지 관리한다.

- 상황인식(SA): 운영과 정보보호에 필요한 정보를 수집, 분석, 경보, 제시, 사용하기 위한 활동과 기술을 수립하고 유지 관리한다.

- 정보공유 및 의사소통(ISC) : 정보보호 자료를 수집하고 이를 제공하기 위해 내·외부 기관과의 관계를 수립하고 유지한다.

- 이상징후 탐지 및 사고대응, 업무연속성 관리(IR) : 정보보호 이벤트를 탐지, 분석, 대응하고 정보보호 이벤트 전반에 걸쳐 운영을 유지하기 위한 계획과 절차, 기술을 수립하고 유지 관리한다.

- 공급망 및 외부 의존성 관리(EDM) : 외부기관에 의존하는 서비스 또는 자산과 관련된 정보보호 위험을 관리하기 위해 통제방안을 수립하고 유지 관리한다.

- 인력 관리(WM) : 정보보호 문화를 창출하고 직원의 지속적인 적합성과 역량을 보장한다.

- 정보보안 프로그램 관리(CPM) : 정보보호 활동에 대한 관리, 전략 계획 및 지원을 제공하는 전사적인 정보보호 프로그램을 수립하고 유지 관리한다.

3.3.2 C2M2 성숙도 단계

C2M2 모델은 각 영역에 독립적으로 적용되는 4개의 성숙도 레벨인 MIL0에서부터 MIL3까지를 정의한다. MIL(Maturity Indicator Level)은 각 영역이 성숙된 정도를 의미한다.

IV. ISMS와 보안성숙도 모델 비교

비교 분석을 위해서 정보보호 관리체계 인증 기준의 관리과정 상세내용과 정보보호대책의 통제항목과 통제목적을 기준으로 하였다. ISM3은 정보보호 관리 활동에 대한 설명과 관리활동이 가지는 가치를 기준으로 항목을 비교하였고 관련한 문서를 통해 세부적으로 분석하였다. C2M2는 정보보호 관리 영역의 목적과 이를 바탕으로 달성해야 하는 목표를 기준으로 항목을 비교하였고 성숙도 수준(MIL) 별로 수행해야 하는 활동을 세부기준으로 분석하였다.

4.1 ISMS와 성숙도 모델 세부영역 비교

ISMS 정보보호 관리과정	O-ISM3	C2M2
정보보호정책수립 및 범위설정	TSP-3:보안대상과 목적 정의	자산, 구성 및 변경 관리(ACM)
경영진 책임 및 조직 구성	SSP-1:이해관계자 보고 SSP-6:자원할당	인력관리(WM)
위험관리	TSP-2:자원관리	위험관리(RM)
정보보호 대책구현	TSP-1:전략적 관리보고 OSP-1:전술적 관리보고 TSP-11:보안인식	정보공유 및 의사소통(ISC)
사후관리	GP-2:ISMS와 비즈니스감사 OSP-21:정보품질 및 규정준수 평가 GP-3:ISM설계 및 발전	

Table 2. 정보보호 관리과정과 성숙도 모델 비교

대표적인 보안 성숙도 모델인 O-ISM3과 C2M2를 국내 정보보호 관리체계 인증인 ISMS와 비교 분석한 결과 세부 항목에 대한 분류에 차이가 있지만 대부분의 관리 영역이 ISMS의 통제 분야 및 세부항목에 포함됨을 알 수 있다. 오히려 성숙도 모델에 따라서 외부자와 관련한 보안관리 항목이 포함되지 않거나 물리환경에 대한 점검이 부족한 측면도 발견되었다. 특히 암호통제 영역은 두 가지 성숙도 모델 모두 직접적으로 정의된 절차나 활동이 존재하지 않았으며 운영보안 영역에서의 원격운영, 스마트워크, 무선네트워크, 공개서버, 전자거래, 휴대용 저장매체 관리와 같이 세부적인 매체에 대한 보안 관리 활동 정의는 제공되지 않고 있다.

ISMS 정보보호대책	O-ISM3	C2M2
정보보호정책	GP-1:지식관리	
정보보호조직	SSP-4:직무규칙 정의 SSP-2:조정	인력관리(WM)
외부자보안		공급망 및 외부 의존성 관리(EDM)
정보자산분류	OSP-3:자산관리	자산, 구성 및 변경 관리(ACM)
정보보호교육	TSP-11:보안인식 TSP-9:보안인력 교육	인력관리(WM)
인적보안	SSP-4:직무규칙 정의 TSP-8:인적보안 TSP-10:징계절차	인력관리(WM) 계정 및 접근 관리(IAM)
물리적보안	OSP-14:물리환경 보호관리	이상징후 탐지 및 사고대응, 업무연속성 관리(IR) 자산, 구성 및 변경 관리(ACM)
시스템개발보안	OSP-8:소프트웨어 개발 생명주기 통제	정보보안프로그램관리(CPM) 상황인식(SA) 계정 및 접근 관리(IAM) 정보보안프로그램관리(CPM) 공급망 및 외부 의존성 관리(EDM)
암호통제		
접근통제	OSP-16:분리와 필터링 관리 OSP-11:접근통제	계정 및 접근 관리(IAM)
운영보안	OSP-4:정보시스템IT관리영역 변경통제 OSP-2:보안조달 TSP-6:보안 아키텍처 OSP-9:보안조치변경제어 OSP-26:안정성 및 가용성 향상 관리 OSP-10:백업관리 OSP-27:보관관리 OSP-19:내부기술 감사 OSP-6:IT관리영역 청산 OSP-17:악성소프트웨어 방지 OSP-5:IT관리영역 패치 OSP-23:내부 이벤트 탐지 및 분석 OSP-22:경고 모니터링 OSP-28:외부 이벤트 탐지 및 분석	정보보안프로그램관리(CPM) 자산, 구성 및 변경 관리(ACM) 상황인식(SA) 이상징후 탐지 및 사고대응, 업무연속성 관리(IR) 위협 및 취약점 관리(TVM) 계정 및 접근 관리(IAM)
침해사고관리	OSP-20:사고대응 OSP-24:사건과 사고처리 OSP-25:포렌식	이상징후 탐지 및 사고대응, 업무연속성 관리(IR) 위협 및 취약점 관리(TVM) 정보공유 및 의사소통(ISC)
IT재해복구	OSP-15:업무연속성 관리	이상징후 탐지 및 사고대응, 업무연속성 관리(IR)

Table 3. 정보보호대책분야와 성숙도 모델 비교

성숙도 모델간에도 평가결과의 표현방식과 활용성에 대한 특징과 차이점을 확인할 수 있다.

성숙도 모델은 적용과 평가 방식에 따라 Staged 또는 Continuous한 방식으로 구분 가능하다. Staged 방식은 조직 차원의 성숙도를 평가하는데 적합하며 각 성숙도 단계별로 달성해야 할 프로세스 영역이 별도로 정의되어 있다. 전체 영역에 대한 종합적인 성숙도 수준을 중심으로 조직간 비교가 가능하다. ISM3의 경우가 이에 해당한다. Continuous 방식의 경우는 영역별 성숙도를 평가할 수 있으며 모든 프로세스 영역별로 각각의 수준이 존재한다. 각 영역을 개별적으로 측정, 개선할 수 있는 장점이 있고 사업 목표에 맞도록 개선의 순서를 설정할 수 있다. 또한 프로세스 영역을 중심으로 비교가 가능하다. C2M2는 Continuous 방식에 해당된다.

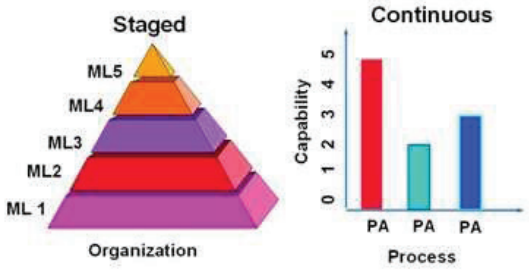


Fig 6. Staged와 Continuous 방식 표현 비교

V. 정보보호 관리수준 점검 방안

정보보호 관리체계 인증과 보안 성숙도 모델은 기업의 정보보안과 이를 구현하는 방법을 제공한다는 공통점을 가진다. 그러나 모든 기업은 상이한 수준의 정보보안 목표를 가지고 있으며 사업 환경과 보유한 자원에 차이가 존재한다. 즉, 특정 기업의 정보보호 거버넌스를 충족하는 범위에서 프로세스를 적절하게 선택하여 단계적으로 개선시켜 나아갈 때 효과적인 결과를 얻을 수 있다. 따라서 기업이 달성하고자 하는 정보보안 목표 수준에 대한 성숙도를 평가할 수 있도록 구조적으로 관리체계를 구현하고 평가할 수 있어야 하며, 이러한 점에 있어서 성숙도 모델은 인증제도와 차이를 가진다.

이미 정보보호 관리체계의 구축과 평가분야에서 효과성이 충분히 검증된 ISMS 통제항목과 Continuous방식의 보안성숙도 모델인 C2M2를 활용하면 기업의 정보보호 성숙도 수준을 효과적으로 점검할 수 있다.

위협 및 취약점 관리	침해사고 관리	정보공유
구성 및 변경 관리	정보시스템 개발 및 운영 관리	로깅 및 모니터링
권한관리	접근통제	암호화 관리
물리환경 보호관리	저장매체 관리	업무연속성 관리
자산 및 위험 관리	인적자원 관리	외부자원 관리

Table 4. 정보보호 관리체계 점검영역 분류

정보보호 관리 수준 점검체계는 15개의 논리 영역으로 구분된다. 암호화 관리 영역과 같이 보안성숙도 모델에 정의되어 있지 않은 영역들은 ISMS를 참고하여 유지하였고 정보보호 정책과 같이 모든 영역의 수준별 세부 점검항목에 포함되는 영역은 논리영역에서 제외하였다. ISMS의 운영보안영역과 같이 폭넓은 범위에 걸쳐 점검항목이 정의된 경우 세부항목에 따라 분리하여 논리영역을 구분하였다. 반대로 정보보호교육과 인적보안의 일부 항목의 경우 인적자원 관리영역으로 통합하여 분류하였다.

논리영역의 하위에는 개별 평가항목들이 존재하며 평가항목에 대한 성숙단계는 Lv0-Lv3로 구분된다. Lv0은 정보보안에 대한 활동이 전혀 없는 수준으로 별도 정의하지 않는다. Lv1은 자산목록 구성과 같이 정보보호 활동에 필요한 기본적인 준비사항이 갖추어져 있는지 여부를 점검한다. Lv2는 기준정의, 문서화와 같이 정형화된 체계와 활동이 갖추어져 있는지를 확인하고 Lv3보다 수동적인 개념의 활동들이 포함된다. Lv3은 전담인력, 주기적 모니터링과 필요한 기술 확보와 같이 구조적이고 적극적으로 진행되는 활동이 포함된다.

Lv1	식별된 정보자산을 다음 항목이 포함된 별도 목록으로 관리하고 있는가?
	기밀성, 무결성, 가용성, 법적요구사항 등을 고려하여 정보자산의 중요도를 평가하기 위한 기준을 수립하고 있는가?
	정보자산별로 중요도를 평가하고 각 자산별 특성에 적합한 보안등급 부여하고 보안등급을 쉽게 확인할 수 있도록 하고 있는가?
Lv2	정보보호 및 개인정보보호를 위한 관리적, 물리적, 기술적, 법적 분야 등 다양한 측면에서 발생할 수 있는 위험을 식별하고 평가할 수 있는 방법을 정의하여 문서화하고 있는가?
	정보보호 관리체계 통제항목 또는 별도의 기준으로 관리적, 운영적, 물리적 위험을 식별하고 있는가?
	정보보호 관리체계 인증범위 내의 정보시스템 자산에 대해 취약점 점검을 통한 기술적 위험을 식별하고 있는가?
	식별된 위험에 대한 위험도를 산정하고 있는가?
	조직에서 수용 가능한 목표 위험수준을 정하고 그 수준을 초과하는 위험을 식별하고 있는가?
	정보자산(정보시스템, 정보보호시스템, 정보)
	의 분류기준을 수립하고 정보보호 관리체계 범위 내 모든 정보자산을 식별하고 있는가?
Lv3	매년 위험관리를 수행하기 위하여 전문인력 구성, 기간, 대상, 방법, 예산 등을 구체화한 위험관리계획을 수립 • 이행하고 있는가?
	정보보호 관리체계 범위 전 영역에 대한 위험식별 및 평가를 연 1회 이상 수행하고 있는가?
	위험 식별 및 평가 결과를 정보보호 최고책임자 등 경영진이 이해하기 쉽게 작성하여 보고하고 있는가?
	정기적으로 정보자산 현황을 조사하고 정보자산목록을 최신으로 유지하고 있는가?
	식별된 정보자산에 대한 책임자 및 관리자(또는 담당자)를 지정하고 있는가?
	정보자산의 보안등급에 따른 취급절차(생성, 저장, 이용, 파기 등)를 정의하고 이행하고 있는가?

Table 5. 자산 및 위험관리영역 세부 점검항목

정보보호 업무를 담당하는 관리자는 논리적으로 구분된 영역에서의 성숙단계별 점검 항목들을 평가하여 기업이 위치한 현재수준을 파악할 수 있다. 이때 각 항목을 평가하는 기준은 시행여부에 따라 미시행, 부분시행, 완전시행으로 평가할 수 있으며 영역별 특정 성숙도 수준에 포함되는 모든 평가 항목에 대하여 완전시행인 경우 해당 성숙도를 달성했다고 판단할 수 있다.

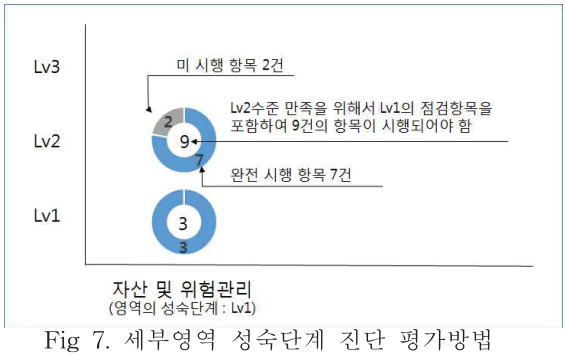


Fig 7. 세부영역 성숙단계 진단 평가방법

예를 들어, 자산 및 위험관리 영역의 Lv1에는 3개의 점검항목이 존재한다. Lv2의 경우에는 Lv1의 점검항목을 포함하여 9개의 점검항목으로 구성되어 있고 그 중 2개 항목이 미시행 상태이고 나머지 7개 항목이 완전시행되고 있는 상태임을 의미한다. 또한 Lv1을 포함하고 있는 Lv2의 모든 점검 항목 중에 2개의 항목이 미시행 중임으로 해당영역에 대한 최종적인 성숙도는 Lv1으로 평가된다.

논리적으로 구분된 영역 전체에 대한 단계별 수준 점검이 모두 완료되면 각 영역별 수준을 포함한 정보보호 관리체계에 대한 전체적인 수준을 판단할 수 있다.

VI. 결론

기업의 성공적인 운영은 각 조직이 가지는 고유한 위험이 효과적으로 관리될 때에야 비로소 달성될 수 있다. 따라서 기업의 위험관리 전략에 부합하는 정보보호 관리체계의 수립과 운영이 필요하다. 이를 위해 기업은 정보보호를 위해 시행중인 보안활동과 현재의 역량 상태를 세밀히 평가하고 달성해야할 목표수준을 설정한 후 목표까지의 격차를 식별하여 투자 우선순위를 결정해야 한다. 보안 성숙도 모델과 이를 활용한 정보보호 관리수준 점검방안을 사용하는 산업 또는 기업이 가진 특수성을 감안하여 세부 영역과 점검항목을 새롭게 구성할 수 있다. 보안 성숙도 모델과 이를 활용한 정보보호 관리수준 점검방안은 이러한 결정을 위한 유용한 도구로 활용될 수 있고 최종적으로 기업의 리스크 관리 전략 및 활동에 반영되어 실제적인 도움이 될 수 있을 것이라 기대한다.

앞으로의 연구를 통해 개별 산업이 가지는 고유한 특성이 반영될 수 있도록 적합한 영역을 정의하고 세부 점검항목을 추가적으로 개발하여 점검체계를 개선하고 유사 업종 및 기업별 수준 비교를 통해 효과성을 분석할 수 있을 것이다.

[참고문헌]

[1] 금융위원회, 금융분야 데이터활용 및 정보보호 종합방안, 2018

[2] Sumin Sin, "A study on the impact of the project management knowledge area on the ISMS Project Performance : The Case of ISMS project", Dongguk University, 2016

[3] Sengsik Son, "The Study on the Improved Assessment Methodology for Information Security Level Using 27001", Sungkyunkwan university, 2014

[4] YoungSik Bae, "A Study of Effect of Information Security Management System[ISMS] Certification on Organization Performance", Korea Acadevy Industrial Cooperation Society, 13(9), pp.4224-4233, 2012

[5] KISA, ISMS 인증제도 안내서, 2017

[6] KISA, 정보보호 관리체계(ISMS) 인증 추진계획, 2017

[7] Open Group Standard, 『Open Information Security Management Maturity Model (O-ISM3)』, 2011.

[8] Soo Hyun Lee, "A Study on Maturity Model for Improving Security Check in Information System Audit", Konkuk University, Dec 2014.

[9] U.S Department of Energy(DOE), Cybersecurity capability maturity model, 2014

[10] Katie Stewart, Evaluating and Improving Cybersecurity Capabilities of the Electricity Critical Infrastructure, Carnegie Mellon University, 2015

[11] Sungmoon Kwon, "Cyber Security Framework for Critical Infrastructure:, Journal of The Korea Institute of Information Security & Cryptology, VOL.27, No.2, Apr. 2017

[12] YeonSuk Hwang, "A Study on Improvement of SECU-STAR through Comparative Analysis with Cybersecurity Capability Maturity Model, Soonchunhyang University, 2016

<저 자 소 개>



이 상 규 (Sang-kyu Lee) 정회원
1999년 2월: 명지대학교 컴퓨터소프트웨어학과 졸업
2017년 3월~현재: 고려대학교 금융보안학과 석사과정
2007년 3월~현재: 신한아이타스(주) 차장
<관심분야> 금융보안, 정보보호 관리체계, 보안성숙도



김 인 석 (In-seok Kim) 정회원
1980년 5월 ~ 1998년 12월: 한국은행 과장
1999년 1월 ~ 2011 3월: 금융감독원 부국장
2011년 3월~현재: 고려대학교 정보보호대학원 교수
<관심분야> 금융보안, 전자금융 정책, 전자금융 법규

가상화폐 거래소의 보안성 확보를 위한 정보통신망 이용촉진 및 정보보호 등에 관한 법률 개정(안) 제시

전 형 율, 오 장 욱, 서 정 택

순천향대학교 정보보호학과

Proposal of a revision to the Act on Promotion of Information and Communications Network Utilization and Information Protection for Security of Virtual Money Exchange

Hyung Youl Jeon, Jang Wook Oh, Jung Taek Seo

Department of Information Security Engineering, Soonchunhyang University.

요 약

최근 가상화폐인 비트코인의 가격 변동성이 커지면서 가상화폐에 대한 관심도가 증가하였고, 다수의 가상화폐 거래소들이 생겨났다. 그러나 대부분의 가상화폐 거래소들이 보안 대비를 소홀히 함에 따라 사이버 공격의 주 표적으로 떠 올랐다. 2018년 1월에는 일본의 주요 암호화폐 거래소인 코인체크가 해킹을 당해 약 5700억 원 상당의 암호화폐가 도난당하였고, 국내에서 한 가상화폐 거래소가 개인정보 유출 및 가상화폐 도난을 당한 사례가 있다. 현재 정보통신망법 제49조에서 이용자 수를 기준으로 하여 큰 규모의 가상화폐 거래소는 올해부터 ISMS 인증 대상에 들어가지만, 중소규모의 가상화폐 거래소는 여전히 법의 테두리에 들어 있지 않다. 본 논문에서는 소규모의 가상화폐 거래소의 보안관리가 이루어질 수 있도록 관련 조항에 대한 개정안을 제시하고자 한다.

I. 서론

최근 큰 논쟁거리로 떠올랐던 가상화폐 거래소인 빗썸이 개인정보 유출사건이 있었고, 과학기술정보통신부에서 국내 가상화폐 거래소 10개를 대상으로 보안점검 및 개인정보보호체계 점검 시행한 결과로 접근통제장치 설치·운영, 개인정보 취급자의 비밀번호 작성규칙 수립 등 기본적인 보호조치조차 준수하지 않는 등의 이용자 보호조치가 전반적으로 매우 미흡한 것으로 나타났다[1][2].

그러나 현재 국내 암호화폐 거래소에 대한 보안과 관련된 기준을 강제할 법규나 제도 등이 마련되어 있지 않고, 정보통신망법 49조에 의해 정보보호 평가인증을 받는 기준이 있지만, 그 기준이 높은 탓에 중소규모의 가상화폐 거래소는 아직 개인정보 보호에 대해 크게 신경 쓰지 않고 있다[2].

해외의 경우 일본을 볼 수 있는데 일본의 주요 암호화폐 거래소인 코인체크가 해킹을 당해서 약 5700억 원 상당의 뉴이코노미무브먼트(NEM)를 도난당했고 이탈리아에서는 가상화폐 거래소인 비트그레일(BitGrail)은 신생 가상화폐인 나노(Nano) 1700만 개가 무단 인출되어서 1840억 원 상당에 피해를 본 것으로 나타났다[2].

본 논문에서는 앞으로 디지털 기술의 발달로 인해서 다양한 가상화폐가 발행되고 이를 거래하는 거래소도 늘고 있는 상황에서 보안대책을 마련하지 않는 거래소가 많아짐에 따라서 현재 가상화폐 거래소 관련 법률을 해외 법률과 비교 분석하여서 국내 현황에 맞게 보안 관련 법률을 제시한다.

본 논문의 구성은 다음과 같다. II 장에서는 국내외의 가상화폐 거래소 사이버 공격에 대한 사례를 분석하고, III 장에서는 국내외의 가상화폐 관련 제도 및 시장현황을 비교 분석을 진행한다. IV 장에서는 국내 현황에 맞게 가상화폐 거래소의 개인정보보호를 위한 법률과 그에 따른 기대효과를 제안한다.

마지막으로 V 장에서는 앞서 진행된 비교 분석의 결과를 바탕으로 가상화폐 거래소에 대하여 법규 강화의 필요를 강조하고 향후 법 개정에 있어서 중요한 사항에 대해 제시하면서 결론을 맺는다.

II. 국내·외 가상화폐 거래소 사이버 공격 사례 분석

2.1 국내 가상화폐 거래소 공격 사례 분석

국내 가상화폐 거래소인 빗썸이 사이버 공격을 받아 회원 정보 3만 1000여 명의 개인정보를 유출한 사건이 있었다. [그림1] 은 개인정보가 유출되는 과정을 도식화한 것으로 써 빗썸의 직원 PC로 악성코드를 심은 입사 지원서를 이메일로 제출했고, 이를 통해 내부 PC로 감염되어 개인정보 유출이 일어나게 되었다. 이 사례를 통해 개인정보보호가 필요하다는 것을 알 수 있게 해주었다[3].



[그림1] 빗썸 개인정보 유출경로

2.2 해외 가상화폐 거래소 공격 사례 분석

해외 사례로는 일본의 코인체크 해킹 사건을 볼 수 있는데 이 사건은 NEM 이라는 가상화폐가 해킹으로 인해 탈취되었고, 피해액은 580억 엔(한화 5천 6백억) 규모로 적지 않은 피해를 보았다. 이 사건의 원인은 보안 시스템을 유지하기 위해 가상화폐 지갑을 인터넷과 차단되는 거래 시스템인 '콜드 월렛'을 따로 확보하고 관리해야 하는데 코인체크에서는 이를 갖추지 않았고, 전체거래 시스템을 24시간 인터넷에 연결해 놓았기 때문에 해킹에 노출이 되었다. 결국, 이러한 관리 소홀로 가상화폐 탈취라는 결과를 가져왔다. 이 사례 또한 가상화폐 거래소가 보안 조치를 하지 않았기 때문에 공격을 당한 것으로 국내 가상화폐 거래소에 대한 개정(안)이 필요하다.

III. 국내·외 가상화폐 관련 제도 및 시장현황 비교 분석

3.1 국내 가상화폐 관련 제도 분석

현재 국내의 가상화폐 거래소는 금융업이 아닌 전자화폐(문화상품권, 전자화폐 등)와 같이 통신판매사업자로 취급되며, 전자상거래 등에서의 소비자보호에 관한 법률(약칭 전자상거래법)을 적용을 받는다. 아래 [표1] 과같이 정보통신망 이용촉진 및 정보보호 등에 관한 법률 (약칭 정보통신망법) 제47조2항(정보보호 관리체계의 인증)의 2, 3번의 내용인 전년도 매출액 100억 원 이상 이거나, 전년도 말 3개월 평균 일일 이용자 수가 100만 명 이상인 자에 해당하지 않으면, 정보보호 관리체계 인증 대상이 되지 않는다.

[표 1] 대한민국 법제처,"정보통신망 이용촉진 및 정보보호 등에 관한 법률"

정보통신망 이용촉진 및 정보보호 등에 관한 법률(약칭 : 정보통신망법)
제 47조 2항 ② 「전기통신사업법」 제2조 제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신 역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다. <신설 2012.2.17., 2015.12.1.> 1. 「전기통신사업법」 제6조제1항에 따른 허가를 받은 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자 2. 집적정보통신시설 사업자 3. 연간 매출액 또는 세입 등이 1,500억 원 이상이거나 정보통신서비스 부문 **전년도 매출액이 100억 원 이상 또는 3개월간의 일일 평균 이용자 수 100만 명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자**

정부가 발표한 가상통화 관련 긴급대책에서는 올해부터 다음 [표 1]의 2항의 3번의 내용을 만족하는 4개의 대형 거래소(업비트, 빗썸, 코인원, 코빗)들이 정보보호 관리체계인증 대상자로 인증을 이행하여야 하지만, 반면에 그 기준을 만족하지 못하여 인증 의무대상에서 제외된 중소규모의 거래소는 개인정보 관리체계(Personal Information Management System) 및 개인정보보호 인증마크(ePRIVACY Mark)를 획득할 수 있도록 하여서 가상화폐 거래소에 대한 보안을 높이도록 마련하였다. 그러나 이 두 가지의 조치는 강제성이 없고, 자율인증 제도이기 때문에 가상화폐 거래소들이 이행한다는 보장이 없다[5].

3.2 해외 가상화폐 관련 제도 분석

본 장에서는 앞서 살펴보았던 국내 가상화폐 관련 제도의 미비점을 바탕으로 해외의 가상화폐 관련 제도를 분석함으로써 국내 가상화폐 관련 제도를 보완해 보고자 한다.

3.2.1 미국

해외의 가상화폐 관련 제도를 살펴보았을 때, 미국의 경우 연방정부 차원에서는 가상화폐 규제안을 별도로 마련되어 있지 않지만, 뉴욕주에서는 비트라이센스(BitLicense)를 도입하여 가상화폐에 대한 규제를 적용하였다. 비트라이센스에 따르면 디지털화폐 거래소, 디지털화폐 교환소, 디지털화폐 보관/관리 업체 등 디지털통화사업자는 해당 감독규정을 만족시켜 취득해야 하지만 영업할 수 있고, 허가를 위해서는 고객 자산 보호, 디지털화폐 거래 영수증 발급, 디지털화폐 거래의 위험성에 대한 고지, 자금세탁 방지 규정 준수, CISO(정보보호 최고책임자) 지정 등의 사항을 충족해야만 한다. [6]

3.2.2 일본

일본의 경우 다음의 [표2], [표3] 와 같이 자금결제법 내에 가상통화교환업자에 대한 업무를 규제하고 있고, 가상화폐 교환 업체에 관한 내각 부령에 따라 개인 이용자 정보의 안전관리 조치를 시행하고 있다. Ⅱ 장에서 다루었던 코인체크 해킹 사건 또한 자금결제법을 적용받았기 때문에 일본 정부에서 해당 가상화폐 거래소에 대해 행정조치가 가능했고, 결과적으로 피해자들에 대한 보상이 이루어졌다[7].

[표 2] 일본 총무성,"자금결제에 관한 법률"

일본 자금결제법 가상통화교환업자에 대한 업무 규제(제63조11)
제63조의11 가상화폐 거래소는 가상 화폐교환업에 관해서 내각 부령으로 정하는 바에 의한 가상화폐 거래소 이용자의 재산과 가상화폐를 거래소의 재산 또는 가상화폐와 구분하여 관리해야 한다. **2** 가상화폐 거래소는 전항의 규정에 따른 관리 상황에 대해서 내각 부령으로 정하는 바에 의한 정기에 공인 회계사(공인 회계사 법(쇼와 이십삼년 법률제103호) 제16조의 두 다섯항에 규정하는 외국 공인 회계사를 포함한다. 제63조14의3항에서는 동일) 또는 감사 법인의 감사를 받아야 한다.

[표 3] 일본 총무성," 가상화폐 교환업체에 관한 내각부령"

가상화폐 교환업체에 관한 내각부령
제12조 가상 화폐 교환 업체는 그 행적을 가상화폐 교환업의 업무 내용 및 방법에서 가상 화폐 교환업에 관련된 전자 정보 처리 조직 관리를 제대로 수행하려는 조치를 마련해야 한다. (개인 이용자 정보의 안전관리 조치 등) **제13조** 가상화폐거래소는 취급하는 개인 가상화폐 교환업체 이용자에 관한 정보 안전관리, 종업원의 감독 및 해당 정보의 취급을 위탁하는 경우에는 그 위탁처의 감독에게 해당 정보의 누설, 멸실 또는 훼손방지를 도모하기 위해서 적절한 조치를 마련해야 한다.

이처럼 일본과 미국처럼 암호화폐 거래소에 관한 법이 마련되어 있고 이를 시행하고 있다. 이러한 사항을 보았을 때 국내에서도 가상화폐 거래소의 보안에 대한 규제를 할 수 있는 법이 개정되어야 한다.

IV. 국내 가상화폐 관련 정보통신망법 법률 개정(안) 제시 및 기대효과

4.1 국내 가상화폐 관련 정보통신망법 법률 개정(안) 제시

본 논문에서는 정보통신 이용촉진 및 정보보호 등에 관한 법률을 가지고 개정(안)을 제시하게 되는데, 그 이유는 현재 가상화폐 거래소는 금융권이 아닌 통신판매사업자로 지정되기 때문에 정보통신서비스로 볼 수 있고 정보통신망법에서는 정보통신서비스를 이용하는 자에 대해 보호하기 때문에 선정하게 되었다.

앞서 정보통신망법 제49조의 ISMS의 인증기준에 해당하는 4개의 대형거래소처럼 ISMS 인증의 기준을 낮추어서 중소규모 거래소들도 인증을 받게 만들면 될 것으로 생각을 할 수 있을 것이다. 하지만 그렇게 되면 다른 통신판매업 업종까지도 영향을 미치기 때문에 본 논문에서는 다음[표 4] 와 같이 정보통신망법을 개정하여 가상화폐 거래소가 안전하게 거래될 수 있도록 개정(안)을 제시한다.

[표 4] 가상화폐 관련 정보통신망 법률 개정(안) 요약

정보통신망법 시행령 36조의 6	암호화폐의 거래 중계 및 유통을 취급하는 통신판매업자(이하 암호화폐 거래소) 및 가상통화 관련 사업자(추가)
정보통신망법 시행령 49조	암호화폐의 거래 중계 및 유통을 취급하는 통신판매업자(이하 암호화폐 거래소)는 법 제47조제2항제2번, 제3번과 관계없이 대상에 포함한다. (추가)
정보통신망법 시행령 17조	암호화폐 거래소는 법 제30조의2제1항에 따라 이용자에게 시행령 제17조제2항에 해당하는 명세 및 외부감사결과에 대한 자료도 같이 통지하여야 한다. (추가)

[표 4]는 본 논문에서 제시하는 정보통신망 법률 개정을 제안하는 안이다. 개정안은 정보통신망법의 정보보호 최고책임자를 지정하는 안, 정보보호 관리체계 인증의 범위를 확대하는 안, 개인정보 이용통지에 관한 법률을 개정하는 안을 제안하였다.

[표 5] 대한민국 법제처,"정보통신망 이용촉진 및 정보보호 등에 관한 법률" 개정(안)

정보통신망 이용촉진 및 정보보호 등에 관한법률 시행령 개정(안)
제36조의6 (정보보호 최고책임자 지정·신고 대상자의 범위) 1. 법 제41조제1항제1호에 따른 내용 선별 소프트웨어를 개발 및 보급하는 사업자 2. 법 제47조제2항에 따라 정보보호 관리체계 인증을 받아야 하는 자 3. 「저작권법」 제104조제1항에 따른 특수한 유형의 온라인서비스제공자로서 상시 종업원 수가 5명 이상이거나 전년도 말 기준 직전 3개월간의 일일평균 이용자 수가 1천명 이상인 자 4. 「전자상거래 등에서의 소비자보호에 관한 법률」 제2조제3호에 따른 통신판매업자(통신판매중개업자를 포함한다)로서 상시 종업원 수가 5명 이상인 자 5. 「게임산업진흥에 관한 법률」 제2조제7호에 따른 인터넷컴퓨터 게임시설 제공업을 꾸려나가는 자에게 같은 법 제28조제6호에 따라 고시된 음란물 및 사행성 게임물 차단 프로그램을 제공하는 사업자 6. 상시 종업원 수가 1천 명 이상인 자 **(추가) 7. 암호화폐의 거래 중계 및 유통을 취급하는 통신판매업자(이하 암호화폐 거래소) 및 가상통화 관련 사업자**

위의 [표 5]는 정보통신망법 시행령 제36조의6의 정보보호 최고책임자 지정 및 신고 대상자의 범위에 대해 개정하는 안을 제시한 것이다. 가상화폐 거래소의 특성상 소규모의 사업자라도 하더라도 고객의 자산 안전과 개인정보보호를 위해 정보보호 최고책임자를 지정하여 침해사고 예방에 특히 신경쓸 수 있도록 법적인 규제가 필요하다.

암호화폐를 취급하는 거래소에 대하여 신규진입 또는 소자본으로 운영되더라도, 정보보호 최고책임

자를 지정을 의무화할 수 있도록 정보통신망법 시행령 제36조의6 신고 대상자의 범위에 대해 위의 [표 5]와 같이 대상을 신설할 것을 제안한다.

이처럼 신고 대상자의 범위에 '암호화폐 거래소 등 가상통화 관련 사업자'를 추가함으로써 사업장의 규모 또는 이용자 수에 상관없이 정보보호 최고책임자를 지정하도록 하여 안전한 암호화폐 거래시장을 운영할 수 있도록 법적 환경을 마련할 수 있다.

또한, 규제의 사각지대에 있었던 가상화폐 거래소의 소규모 사업자 및 신규진입하는 사업자에 대해 고객의 자산 보호 및 개인정보보호를 위해 보안체계를 필수적으로 갖출 수 있도록 법적인 조치가 필요하다.

[표 6] 대한민국 법제처,"정보통신망 이용촉진 및 정보보호 등에 관한법률" 개정(안)

정보통신망 이용촉진 및 정보보호 등에 관한법률 시행령
제49조(정보보호 관리체계 인증 대상자의 범위) ① 법 제47조제2항제1호에서 "대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자"란 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자를 말한다. ② 법 제47조제2항제3호에서 "대통령령으로 정하는 기준에 해당하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다. <개정 2016.5.31.> 1. 연간 매출액 또는 세입이 1,500억원 이상인 자로서 다음 각 목의 어느 하나에 해당하는 자 가. 「의료법」 제3조의4에 따른 상급종합병원 나. 직전연도 12월 31일 기준으로 재학생 수가 1만명 이상인 「고등교육법」 제2조에 따른 학교 2. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자. 다만, 「전자금융거래법」 제2조제3호에 따른 금융회사는 제외한다. 3. 전년도 말 기준 직전 3개월간의 일일평균 이용자 수가 100만명 이상인 자. 다만, 「전자금융거래법」 제2조제3호에 따른 금융회사는 제외한다. **4. 암호화폐의 거래 중계 및 유통을 취급하는 통신판매업자(이하 암호화폐 거래소)는 법 제47조제2항제2번, 제3번과 관계없이 대상에 포함한다.**

위의 [표 6]은 정보통신망법 시행령 제49조로 정보보호 관리체계(약칭 ISMS) 인증 대상자의 범위를 나열한 것으로, 현행법에서 가상화폐 거래소의 경우 제49조의2항 2번 및 3번의 조건에 부합되는 거래소는 4곳뿐이며 조건에 부합하지 않으면 ISMS 인증을 받을 의무가 없다. 더불어 [표 7]의 개인정보이용내역의 통지에 대한 의무가 없기 때문에 전년도 매출액이 100억 원 미만이거나, 일일평균 이용자수가 100만 명 미만인 소규모의 가상화폐 거래소는 정보보호 관리체계에 대한 강제성이 없어 보안대책에 대해 미흡해지는 상황이 발생하게 된다.

소규모 가상화폐 거래소 및 신규 진입을 준비하고 있는 거래소에게 보안에 대한 대비 및 책임을 질 수 있는 법적인 환경을 만들고자 아래 [표 6] 및 [표 7]와 같이 법안 개정(안)을 제안한다.

[표 7] 대한민국 법제처,"정보통신망 이용촉진 및 정보보호 등에 관한법률" 개정(안)

정보통신망 이용촉진 및 정보보호 등에 관한법률 시행령
제17조(개인정보 이용내역의 통지) ① 법 제30조의2제1항 본문에서 "대통령령으로 정하는 기준에 해당하는 자"란 **암호화폐의 거래 중계 및 유통을 취급하는 통신판매업자(이하 암호화폐 거래소) 및** 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자등을 말한다. ② 법 제30조의2제1항에 따라 이용자에게 통지하여야 하는 정보의 종류는 다음 각 호와 같다. <개정 2016.9.22.> 1. 개인정보의 수집·이용 목적 및 수집한 개인정보의 항목 2. 개인정보를 제공받은 자와 그 제공 목적 및 제공한 개인정보의 항목. 다만, 「통신비밀보호법」 제13조, 제13조의2, 제13조의4 및 「전기통신사업법」 제83조제3항에 따라 제공한 정보는 제외한다. 3. 법 제25조에 따른 개인정보 처리위탁을 받은 자 및 그 처리위탁을 하는 업무의 내용 ③ 법 제30조의2제1항에 따른 통지는 전자우편·서면·모사전송·전화 또는 이와 유사한 방법 중

어느 하나의 방법으로 연 1회 이상 하여야 한다.
④ 암호화폐 거래소는 법 제30조의2제1항에 따라 이용자에게 시행령 제17조제2항에 해당하는 내역 및 외부감사결과에 대한 자료도 같이 통지하여야 한다.
[본조신설 2012.8.17.]

이와 같이 암호화폐 거래소는 전년도 매출액이나 일일평균 이용자 수와 상관없이 ISMS 인증 대상자로 정하여, 규모에 상관없이 암호화폐 거래소의 보안에 대한 법적 장치를 만들 수 있으며, 개인정보 이용내역 통지할 때 외부감사결과에 대한 자료도 통지하게 하여 전자상거래법 으로는 부족한 가상화폐 거래소의 투명성을 증대할 수 있다.

4.2 기대효과

본 논문의 개정안을 통해서 앞으로 가상화폐 거래소는 보안규제를 통해 대형 거래소뿐만 아니라 중소규모의 거래소들도 정보보호책임자 지정해서 보안에 대비할 수 있게 되고 또한 개인정보 보호 및 이용 통지하게 하게 하여서 이용자의 개인정보를 보호할 수 있는 효과도 가져온다.

V. 결론

본 논문에서는 가상화폐 거래소의 보안 규정에 대해 법적 기준이 마련되어 있으나 그것은 대형 규모의 가상화폐 거래소만 해당되며 중소규모 거래소의 경우 개인정보보호에 큰 문제점이 있음을 알아보았고 국내외 가상화폐 거래소 해킹사례를 분석하고 그에 따라 정보통신망법과 해외 관련법을 분석하여서 국내 현황에 맞게 기존 법률의 개정(안)을 제안하였다. 본 개정(안)은 정보통신망법에서 가상화폐 거래소를 규정하고 ISMS인증과 정보보호최고책임자 임명, 개인정보이용내역 등을 통지하여서 이용자의 개인정보를 보호하고 가상화폐 도난을 방지 할 수 있도록 법 규제를 제안하였다. 따라서 앞으로 가상화폐 거래소가 개인정보보호를 소홀히 하지 않기를 기대하고 입법 후에도 생길 수 있는 문제에 대하여 지속적으로 논의 되어야 할 것이다.

[참고문헌]

[1] 아이뉴스, “보안점검 기준통과 가상화폐거래소 단 한곳도 없다” http://news.inews24.com/php/news_view.php?g_serial=1073431&g_menu=020200&rrf=nv

[2] 연합뉴스, “가상화폐 거래소 또 해킹…이탈리아서 1천800억원 무단인출” http://www.yonhapnews.co.kr/bulletin/2018/02/11/0200000000AKR20180211035000009.HTML?from=search

[3] 네이버 지식 백과, “빗썸 해킹사건” https://terms.naver.com/entry.nhn?docId=4351487&cid=43667&categoryId=43667

[4] 티스토리, “일본 가상화폐 NEM 해킹사건”
http://youngwizard.tistory.com/138

[5] 금융감독원, “정부, 가상통화 관련 긴급대책(12.13) 후속조치 추진”

[6] 금융보안원, “해외 주요국 디지털화폐 관련 제도 및 시장현황”

[7] 동아일보 “유출 코인 추적 포기… 해커가 이겼다” http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=104&oid=020&aid=0003135387

[표 1] 및 [표 4] 대한민국 법제처, “정보통신망 이용촉진 및 정보보호 등에 관한법률”

[표 2] 일본 총무성, “자금결제에 관한 법률”

[표 3] 일본 총무성, “가상화폐 교환업체에 관한 내각부령”

[표 5]부터 [표 7] 대한민국 법제처, “정보통신망 이용촉진 및 정보보호 등에 관한법률”

데이터베이스 삭제 방법과 관련 법률의 지시사항 격차 확인을 통한 개선방향 제시

임 창 완, 조 성 영

국방과학연구소

Suggest improvement direction through identified gap between method of delete database and instruction for related laws

Changwan Lim, Sungyoung Cho

Agency for Defense Development

요 약

기업의 서비스를 이용하기 위해서 사용자들은 자신의 개인정보를 기업에게 제공하여야 하고 이러한 개인정보를 관리하는 기업은 법을 준수하여야 한다. 개인정보 보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 같은 여러 법적 기준이 마련되어 있으며 정보보호 관리체계(ISMS), 개인정보보호 관리체계(PIMS) 등을 기업이 의무적으로 인증 취득하도록 요구한다. 하지만 현실적인 문제로 일부 업무에 대해선 법 준수가 되고 있지 않으며 각종 정보유출 사고가 빈번한 현 상황에서 큰 문제라고 할 수 있다. 본 논문에서는 개인정보 관리 업무 중 개인정보 삭제에 대해 집중하여 현행 파기 방법과 법적 요구조건을 비교해보고 이를 위한 정책제안을 해보고자 한다.

Ⅰ. 서 론

기업은 사용자의 개인정보를 데이터베이스화하여 관리하고 있다. 선택적으로 데이터를 파기하여야할 경우 저장매체 전체를 보안 삭제하는 방법을 사용하지 못하게 되고 파기된 데이터가 다시 복구될 수 있는 가능성이 존재하게 된다. 데이터베이스 관리 시스템에서 제공하는 삭제명령은 기술적 접근에서 업무 효율성을 높이기 위한 것으로 법률의 요구사항을 만족할 수 없는 수준이다.(1)

기업의 정책을 관리, 감독하는 정부에선 관련 사항을 법률로 제정하여 기업이 이를 준수하도록 하고 있다. 하지만 기술적 접근에 대한 이해 없이 법률용어로 명시되어 있는 요구사항은 개인정보 관리를 위한 지표로는 현장과의 간극이 클 수밖에 없다. 이행 불가능한 개인정보 관리 관련 법률을 기업들이 실제로 지키지 못하고 있는 상황에서 데이터의 파기에 대한 현행 법률과 기업의 실제 관리 환경을 비교하여 기술적 증적으로 법률 요구사항을 만족하지 못하는 것을 증명하고, 문제점 해결을 위한 향후 정책 방향을 제시한다.

개인정보 관리에 관련된 현행 법률을 알아보고 실제 기업에서의 데이터베이스 파기 작업 수행 시 파기된 데이터의 복구가능여부를 확인하기 위해 많은 기업에서 사용하는 데이터베이스 관리 시스템인 MySQL을 이용하여 유사환경을 구성한다. MySQL에서 제공하는 삭제명령을 수행하여 데이터베이스를 삭제한 후 모니터링 툴을 통해 파기된 데이터를 복구할 수 있는가를 알아낸다. 이러한 기술적 증적을 통해 기업이 법률 요구사항을 준수하지 못하고 있는 것을 밝히고 법적 접근과 기술적 접근의 격차를 해소하기 위한 정책 방향을 제시한다.

Ⅱ. 개인정보 파기의 법적 접근

2.1 정보시스템 불용처리 지침

국가정보원이 지난 2006년 중앙 행정 기관 등에 배포한 규정으로서 「국가정보보안기본지침」제39조 제3항의 규정에 의하여 정보시스템 저장매체에 수록된 자료의 삭제방법과 세부 처리절차를 규정한 내용을 담고 있다. 이 지침에서 논하는 데이터 파기는 파쇄조각의 크기가 0.25mm 이하로 잘게 부수는 완전파괴, 전용 소자장비를 이용한 저장자료 삭제, 저장매체 전체를 난수나 0, 1로 중복 저장하는 완전포맷의 방법을 지시한다. 하지만 이 방법은 2006년 이후 개정되지 않고 있어 현재 기술을 따라가지 못하고 있다. 완전포맷과 같은 방법의 파기는 결코 안전하지 않다는 것이 1996년 Gutmann의 연구를 통해 알 수 있으며 선택적인 데이터를 파기하는 것에 대해선 전혀 방법제시가 없다.

2.2 개인정보 보호법

개인정보 보호법 제21조 2항 4항에 관련 내용을 서술하며 "개인정보처리자가 제1항에 따라 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.", "개인정보의 파기방법 및 절차 등에 필요한 사항은 대통령령으로 정한다."의 내용을 담고 있다. 개인정보 보호법 시행령 제16조 1항에는 "개인정보처리자는 법 제21조에 따라 개인정보를 파기할 때에는 다음 각 호의 구분에 따른 방법으로 하여야한다. 1. 전자적 파일 형태인 경우: 복원이 불가능한 방법으로 연구 삭제"의 내용을 담고 있다.

2.3 개인정보의 안정성 확보조치 기준

개인정보의 안정성 확보조치 기준 제13조 2항은 "개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다. 1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독"의 내용을 담고 있다.

2.4 정보통신망 이용촉진 및 정보보호 등에 관한 법률

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제29조 1항은 "정보통신서비스 제공자등은 다음 각 호의 어느 하나에 해당하는 경우에는 지체 없이 해당 개인정보를 복구·재생할 수 없도록 파기하여야 한다. 다만, 다른 법률에 따라 개인정보를 보존하여야 하는 경우에는 그러하지 아니하다."의 내용을 담고 있다.

Ⅲ. 데이터베이스 관리 시스템

MySQL은 가장 많이 쓰이는 오픈 소스 기반의 관계형 데이터베이스 관리 시스템이다. 크기가 작고 간결하여 중소규모의 데이터베이스 서버로 적합하며, 플랫폼 독립적이다. 또한 MySQL은 다른 상용 데이터베이스보다 단순한 쿼리를 지원하여 빠른 처리가 가능하다는 장점을 갖는다.[2]

MyISAM 스토리지 엔진은 MySQL 5.5 버전 이전의 기본 스토리지 엔진이다. 테이블은 디스크에 3개의 파일로 저장이 되는데 .frm 확장자를 쓰는 테이블 정의 파일, .MYD 확장자를 쓰는 데이터 파일, .MYI 확장자를 쓰는 인덱스 파일이 있다. 데이터 저장에 제한이 없고 효율적이어서 속도가 빠른 편이고 B-Tree, R-Tree, Full-Text 인덱스를 지원한다. 테이블 락 사용으로 읽기에는 어울리지만 자주 쓰기가 이루어져야 할 때는 적합하지 않다.

Ⅳ. 개인정보 파기의 기술적 접근

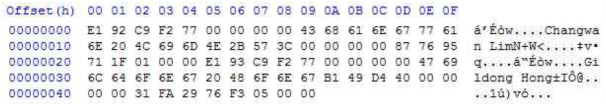
테스트 환경은 MySQL 5.7 버전의 MyISAM 스토리지 엔진을 사용하여 데이터베이스를 구성하였고 모니터링 툴로 HxD를 사용하였다. 시뮬레이션은 간단한 개인정보 데이터베이스를 구성해보고 삭제 명령을 통해 이 데이터베이스를 파기한 후 모니터링 툴을 이용하여 파기한 데이터를 복원할 수 있는지 확인하는 형식으로 진행된다.

4.1 정적 테이블

```
CREATE DATABASE Personal_Data;
CREATE TABLE `Personal_Data_1` (
`Custom_Number` bigint DEFAULT NULL,
`Name` char(12) DEFAULT NULL,
`Phone_Number` bigint DEFAULT NULL,
`Registration_Number` bigint DEFAULT NULL
) ENGINE=myisam ROW_FORMAT=fixed DEFAULT CHARSET=binary;
insert into Personal_Data_1 values (2012400018, 'Changwan Lim', 01012345678, 1234561234567);
insert into Personal_Data_1 values (2012400019, 'Gildong Hong', 01087654321, 6543217654321);
```

그림 1 정적 테이블 생성 명령어

그림 1의 명령어를 사용하여 두 명의 개인정보를 갖고 있는 정적 테이블을 생성하였다.



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	E1	92	C9	F2	77	00	00	00	00	43	68	61	6E	67	77	61	á'Éòw....Changwa
00000010	6E	20	4C	69	6D	4E	2B	57	3C	00	00	00	00	87	76	95	n LimN+W<....‡v•
00000020	71	1F	01	00	00	E1	93	C9	F2	77	00	00	00	00	47	69	q....á"Éòw....Gi
00000030	6C	64	6F	6E	67	20	48	6F	6E	67	B1	49	D4	40	00	00	ldong Hong±IÔ@..
00000040	00	00	31	FA	29	76	F3	05	00	00							..1ú)vó...

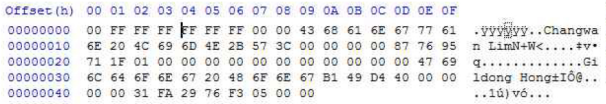
그림 2 정적 테이블 삭제 명령 전

생성된 Personal_Data_1.MYD 파일을 모니터 툴인 HxD를 이용하여 데이터를 보았을 때 입력한 값들이 16진수로 저장되어 있는 것을 확인할 수 있다. offset (00, 00)의 E1과 (20, 05)의 E1이 각 데이터의 시작지점인 것을 확인할 수 있다.

```
delete from Personal_Data_1 where Custom_Number=2012400018;
delete from Personal_Data_1 where Custom_Number=2012400019;
```

그림 3 정적 테이블 삭제 명령어

그림 3의 delete 명령어를 통해서 두 개의 데이터를 모두 삭제하였다.



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	00	FF	FF	FF	FF	FF	FF	00	00	43	68	61	6E	67	77	61	.ÿÿÿÿÿÿ..Changwa
00000010	6E	20	4C	69	6D	4E	2B	57	3C	00	00	00	00	87	76	95	n LimN+W<....‡v•
00000020	71	1F	01	00	00	00	00	00	00	00	00	00	00	00	47	69	q.............Gi
00000030	6C	64	6F	6E	67	20	48	6F	6E	67	B1	49	D4	40	00	00	ldong Hong±IÔ@..
00000040	00	00	31	FA	29	76	F3	05	00	00							..1ú)vó...

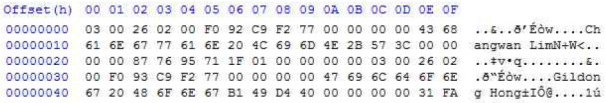
그림 4 정적 테이블 삭제 명령 후

삭제 명령어 실행 후 Personal_Data_1.MYD 파일을 HxD를 이용하여 데이터를 보았을 때 각 데이터의 시작지점부터 7 바이트가 삭제된 것을 확인할 수 있었다. 하지만 Custom_ Number 부분을 제외한 나머지 뒷부분들은 완벽히 복원할 수 있는 것을 확인할 수 있다.

4.2 동적 테이블

그림 5 동적 테이블 생성 명령어

그림 5의 명령어를 사용하여 두 명의 개인정보를 갖고 있는 동적 테이블을 생성하였다.



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	03	00	26	02	00	F0	92	C9	F2	77	00	00	00	00	43	68	..&..ð'Éòw....Ch
00000010	61	6E	67	77	61	6E	20	4C	69	6D	4E	2B	57	3C	00	00	angwan LimN+W<..
00000020	00	00	87	76	95	71	1F	01	00	00	00	00	03	00	26	02	..‡v•q........&.
00000030	00	F0	93	C9	F2	77	00	00	00	00	47	69	6C	64	6F	6E	.ð"Éòw....Gildon
00000040	67	20	48	6F	6E	67	B1	49	D4	40	00	00	00	00	31	FA	g Hong±IÔ@....1ú
00000050	29	76	F3	05	00	00	00	00									)vó.....

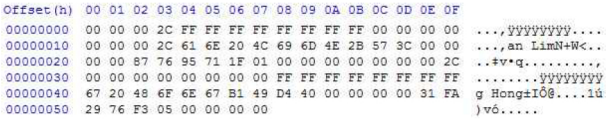
그림 6 동적 테이블 삭제 명령 전

생성된 Personal_Data_2.MYD 파일을 HxD를 이용하여 데이터를 보았을 때 offset (00, 00)의 03과 (20, 0C)의 03이 각 데이터의 시작지점인 것을 확인할 수 있다.

```
delete from Personal_Data_2 where Custom_Number=2012400018;
delete from Personal_Data_2 where Custom_Number=2012400019;
```

그림 7 동적 테이블 삭제 명령어

그림 7의 delete 명령어를 통해서 두 개의 데이터를 모두 삭제하였다.



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	00	00	00	2C	FF	FF	FF	FF	FF	FF	FF	00	00	00	00		...,ÿÿÿÿÿÿÿ....
00000010	00	00	00	2C	61	6E	20	4C	69	6D	4E	2B	57	3C	00	00	...,an LimN+W<..
00000020	00	00	87	76	95	71	1F	01	00	00	00	00	00	00	00	2C	..‡v•q.........,
00000030	00	00	00	00	00	00	00	00	FF	FF	FF	FF	FF	FF	FF	FF	........ÿÿÿÿÿÿÿÿ
00000040	67	20	48	6F	6E	67	B1	49	D4	40	00	00	00	00	31	FA	g Hong±IÔ@....1ú
00000050	29	76	F3	05	00	00	00	00									)vó.....

그림 9 동적 테이블 삭제 명령 후

삭제 명령어 실행 후 Personal_Data_2.MYD 파일을 HxD를 이용하여 데이터를 보았을 때 각 데이터의 시작지점부터 20 바이트가 삭제된 것을 확인할 수 있다. 하지만 일부 Name 부분부터 나머지 뒷부분들은 완벽히 복원할 수 있는 것을 확인할 수 있다.

기술적 접근에서 확인한 데이터베이스의 삭제 명령은 데이터 전체를 삭제하는 것이 아니라 각 데이터의 시작지점을 삭제하여 시스템이 해당 데이터를 참조할 수 없도록 만들어주는 역할을 할 뿐이었다. 이는 데이터 삭제가 법에서 요구하는 파기를 만족시키지 못함을 보여준다. 시뮬레이션 환경과 달리 실제 기업에서 운영하고 있는 개인정보 데이터베이스는 작게는 천만에서 억 단위의 사람들의 개인정보를 저장하고 있기 때문에 삭제를 하기 위해서 상당한 자원이 소비되어야한다.

Ⅴ. 결 론

기술적 접근에서의 데이터 삭제와 법적 접근에서의 파기는 서로 일치하지 않는 개념이다. 실제 데이터 전

체를 삭제하는 것이 아닌 시스템에서 참조하지 못하도록 데이터 시작부분만 덮어쓰는 방식이 현재 데이터베이스 관리 시스템에서 제공하고 있는 삭제 명령어이며 기업들이 개인정보를 삭제할 때 사용되고 있는 방식이기도 하다. 하지만 법에서 요구하고 있는 전체 데이터를 복원 불가능할 정도로 없애는 것과는 상당한 차이가 있는 것을 확인하였다. 이러한 방식은 법에서는 유효하지 않으며 따라서 기업이 법을 준수하고 있지 않고 법 또한 실제 개인정보 관리 현장에 동떨어진 개념을 요구하고 있다는 것을 말해준다.

현재 기업 데이터베이스에는 작게는 수백만에서 크게는 수억에 이르는 사람들의 개인정보가 있다. 원활한 업무가 가능하도록 방대한 용량의 데이터베이스를 관리하려면 신속이 명령이 처리되는 최적화가 필요하다. 법이 요구하는 파기의 개념을 준수하기 위해서는 근본적인 시스템 수정이 이루어져야하지만 소비되는 비용이 엄청나기 때문에 이행이 불가능한 사항이고 강제하기에는 현장에서 큰 어려움이 따른다. 그렇기에 우선적으로 법률이 개정되어 파기에 대한 항목은 현재 기업의 상황에 맞춰 예외상황을 포함하도록 하여 기업이 제도개선을 위한 유예기간을 가질 수 있도록 하고 법률에 사용되는 개념을 현장에서 사용하는 개념과 일치하도록 수정할 필요가 있다. 기술적 전문가가 참여하여 발전하는 기술의 수준에 맞는 법적 접근을 돕고 실제 현장과 법의 간극을 좁혀 추상적 개념만 존재하는 실용성 없는 현재 법률을 개정하는 것이 요구된다.

현 수준에서는 기술적으로 데이터베이스의 데이터를 선택적으로 완전 파기할 수 없기 때문에 이를 뒷받침할 수 있는 항목이 추가되어야 한다. 기존의 법률을 삭제하고 수정하는 것보다 관리 및 감독에 대한 항목을 추가하는 것이 바람직하다. 선택적 완전 파기에 대한 기술이 추후에 개발될 수 있기 때문에 현시점만을 위해 관련 항목을 삭제하는 것은 다시 개정을 필요로 하는 결과를 낼 것이며 '개인정보처리자는 개인정보의 완전 파기가 불가능할 경우, 관리 및 감독을 통해 삭제한 정보가 복구 및 재생되지 않도록 해야 한다.'라는 항목을 개인정보의 안정성 확보조치 기준 이외의 다른 법률에도 추가하여야한다.

참 고 문 헌

〔1〕 황성환, "기업의 디지털 데이터 파기 신뢰성 요인에 관한 연구", 동국대학교 국제정보대학원 석사학위논문, 2012

〔2〕 장성민, "MySQL InnoDB의 삭제된 레코드 복구 기법 연구", 고려대학교 정보보호대학원 석사학위논문, 2014

딥 러닝을 활용한 CVSS 점수 예측에 관한 연구

김현우*, 송기범*, 이만희*
*한남대학교 컴퓨터공학과

A Study on Predicting CVSS Score Utilizing Deep Learning

Hyeon-Woo Kim*, Gi-Beom Song*, Man-Hee Lee*
*Department of Computer Engineering, Hannam University

요 약

네트워크의 비약적인 발전과 IT산업의 꾸준한 성장에 따라 새롭게 발견되는 취약점도 기하급수적으로 증가하고 있다. 취약점은 존재하고 있는 대상에 관계없이 악의적인 목적을 가진 공격자에 의해 악용될 경우 큰 보안 사고로 이어질 수 있기 때문에 조기에 취약점을 발견하고 패치를 통해 예방하는 것이 가장 중요하다. 하지만 보안 관리자 입장에서 패치를 진행할 취약점의 우선순위를 결정하는 것은 매우 어려운 작업이다. 이에 따라, 본 연구에서는 식별된 취약점의 위험도를 평가하는 지표로 사용되는 CVSS의 점수를 평가되기 전에 미리 예측하기 위한 방안으로 딥 러닝의 활용을 제시한다.

I. 서론

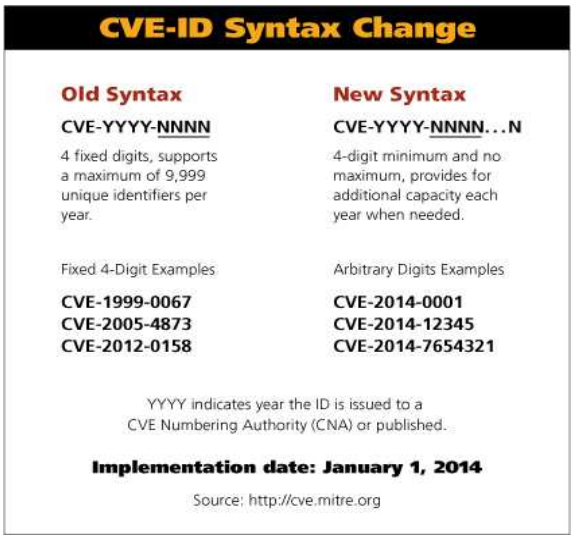
최근 네트워크의 비약적인 발전과 IT 산업의 꾸준한 성장으로 인해 발견되는 보안 취약점의 수 또한 기하급수적으로 증가하고 있다. 트렌드마이크로 社의 “2017년 연간 위협 보고서”에 따르면 2017년의 제로데이 취약점은 2016년보다 98%증가하였고 기존 취약점에 대한 악용 사례도 더 증가하였다고 밝혔다[1]. 취약점은 소프트웨어, 하드웨어를 구분하지 않고 존재할 수 있고 여부에 따라 악의적인 목적을 지닌 공격자에 의해 악용될 수 있기 때문에 취약점의 유무를 점검하고 패치하는 작업은 매우 중요하다.

국내·외에서 취약점을 악용함으로써 발생된 대표적인 보안 사고로 워너크라이(WannaCry)가 존재한다[2]. 워너크라이는 랜섬웨어(Ransomware)의 일종으로 마이크로소프트 윈도우의 파일 공유에 사용되는 서버 메시지 블록 원격코드의 취약점을 악용함으로써 하루 만에 전 세계 100개국의 컴퓨터 10만대를 감염시켜 막대한 피해를 입히며 전 세계적으로 보안 취약점에 대한 사전 예방의 경각심을 불러 일으켰다.

취약점에 대한 악용을 예방하는 가장 효과적인 방법은 사전에 취약점의 존재 여부를 점검하고 패치를 통해 사전에 예방하는 것이다. 하지만 존재하는 취약점이 많을 경우 보안 관리자 입장에서 모든 취약점들을 식별하고 패치해야 하는 우선순위를 정하는 것은 매우 어려운 작업이다. 이와 같은 어려움을 해결하기 위해 MITRE사에서 1999년 만든 체계인 CVE(Common Vulnerabilities and Exposure)와 FIRST에서 만든 CVSS(Common Vulnerability Scoring System)가 존재한다[3][4].

CVE는 공개적으로 알려진 정보보안 취약점 및 노출에 대한 참조 방법을 제공하는 고유 표기번호로써 CVE라는 문자에 취약점이 발견된 년도와 취약점 보고 순서를 의미하는 번호로

아래 [그림 1]의 좌측에 기재되어 있는 내용처럼 표현되었으나 기하급수적으로 증가하는 취약점들을 모두 표현하기에 제약적인 고정길이 방식으로 인해 가변길이를 가지는 새로운 CVE 형식으로 14년 1월 변경되어 현재까지 사용되고 있다[5][6].



[그림 1] CVE 형식

CVSS는 고유 식별 형식인 CVE형태로 제공되는 취약점에 대해 개방적이고 정량화된 위험도를 평가하고 제공하기 위해 설계된 오픈 프레임워크로써 보안 관리자에게 취약점들의 우선순위를 결정하고 가장 큰 위험성을 지닌 취약점부터 패치 할 수 있도록 수치화된 위험도 정보를 제공한다[7].

CVE를 통해 취약점을 식별하고 CVSS에 의해 측정된 위험도 점수를 통해 보안 관리자는 우선적으로 제거해야 할 취약점을 구분할 수 있다. 하지만 새롭게 등록되는 CVE에 대해서는 CVSS 점수가 바로 측정되어 등록되는 것이 아니기 때문에 보안 관리자 입장에서는 새롭게 등록된 CVE에 대한 위험도를 판단하기에 어려움이 존재한다.

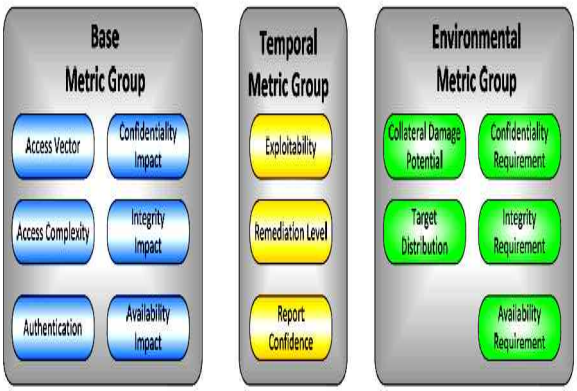
이러한 어려움을 극복하기 위한 연구로 Fuzzy-System을 활용한 연구가 진행된 바 있다[10]. 해당 연구에서는 CVSS 점수를 예측하기 위해 OSVDB에 존재하는 CVE Description과 CVSS 점수를 가진 CVE들을 수집하고, 불용어 제거, 어간 추출, TF-IDF(Term Frequency - Inverse Document Frequency)를 통해 특징 벡터를 추출한 뒤 LDA(Linear Discriminant Analysis), PCA(Principal Component Analysis)를 사용하여 차원을 축소하고 Fuzzy-system을 활용하여 예측했다[10].

이전의 연구는 머신 러닝 알고리즘과 자체적으로 설계한 Fuzzy-system을 활용하여 CVSS 점수를 예측하였으나, 최근 예측 연구에 많이 사용되는 딥 러닝(Deep Learning) 기법을 이용한 CVSS 점수 예측 연구는 없었다. 이에 따라 딥 러닝을 이용한 CVSS 점수 예측 기법을 소개한다.

II. 관련연구

2.1 CVSS

CVSS는 CVE형태로 표현되는 취약점에 대하여 수치화된 위험도를 제공하기 위해 설계된 오픈 프레임워크로써 아래 [그림 2]와 같이 기본 메트릭(Metric) 그룹, 임시 메트릭 그룹, 환경 메트릭 그룹 총 3가지의 메트릭 그룹으로 구성되어 있다.



[그림 2] CVSS 측정기준 그룹

기본 매트릭스는 시간과 사용자 환경에 의해 변하지 않는 본질적이고 근본적인 특징들을 나타내며 임시 메트릭은 사용자들의 환경에 의한 것이 아닌 시간의 흐름에 따라 변경되는 취약점의 특징을 나타낸다. 마지막으로 환경 메트릭은 특정한 사용자의 환경과 관련되어 있는 취약점의 특징을 나타낸다. 이에 따라, CVSS 기본 메트릭 그룹은 취약점의 근본적인 특징을

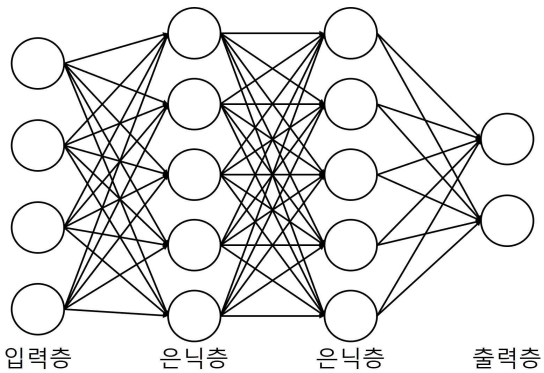
정의하고 전달하는 것을 목적으로 취약점에 특징을 부과하는 목적을 가진 사용자들에게 분명하고 직관적으로 취약점의 정보를 제공한다.

만일 CVSS를 이용하는 관리자가 매우 정확하게 자신들의 환경에 존재하는 위험이 반영된 정보를 얻고자 할 때 임시 매트릭스와 환경 매트릭스 그룹을 사용하여 평가할 수 있다. 이러한 모든 메트릭이 정해지면 CVSS만의 정해져 있는 수식을 거쳐 CVSS의 점수가 산정된다.

2.2 딥 러닝

딥 러닝(Deep Learning)은 머신러닝의 한 분야로 심층 인공신경망에 학습 알고리즘과 방대한 양의 데이터를 이용하여 학습 능력을 지속적으로 개선시키는 기법으로 인공신경망의 깊이가 깊어질수록 성능이 향상되는 구조를 지닌다. 인공 신경망(Artificial Neural Network)은 수많은 뉴런이 시냅스에 의해 복잡하게 얽혀 신경 네트워크를 구성하고 각 뉴런의 학습으로 인해 변화되는 시냅스의 가중치를 통해 문제 해결 능력을 가지는 구조로 인간 두뇌에서 영감을 얻은 컴퓨팅 시스템 모델 전반을 의미한다[9].

인공 신경망의 각 뉴런들은 여러 층에 구성되어 있는 서로 다른 뉴런들 간의 시냅스에 의해 아래 [그림 3]과 같이 완전 접속망(Fully Connected Network)구조를 이루며, 이 구조에 나타나는 뉴런과 계층의 수는 신경망을 설계하는 설계자에 따라 혹은 학습하고자 하는 데이터의 크기에 따라 달라질 수 있다.



[그림 3] 인공 신경망 구조

입력층의 뉴런은 학습을 위해 입력되는 데이터들의 값이 할당되며 은닉층의 뉴런들은 입력층의 뉴런들이 가진 값과, 연결된 시냅스의 가중치의 값을 곱한 뒤 지정된 활성화 함수를 통하여 도출된 값을 가진다. 이러한 과정을 존재하는 계층의 수만큼 반복하면 출력층에는 최종 값이 도출되어 훈련 데이터의 정답과 비교를 통해 오차를 계산할 수 있게 된다. 입력층에 입력된 학습용 데이터로부터 출력층에 도출되는 값의 오차를 계산하는 과정을 순전파(Forward propagation)라고 하며 계산된 오차를 출력층에서 입력층 방향으로 전파시키면서 각층의 가중치를 변경 하는 과정을 역전파(Back propagation)라고 한다.

도출된 오차의 값이 역전파와 순전파의 반복을 통해 0에 가까워질수록 정확도가 높은 신경망으로 학습이 진행된다.

2.3 Fuzzy-System을 활용한 CVSS 점수 예측 연구

CVSS 점수 예측을 위해 Fuzzy-System을 활용한 연구에서는 OSVDB에 존재하는 CVE의 Description과 CVSS 점수를 가진 CVE를 19,320개 수집했다[8][10]. 수집된 데이터 중 CVSS 점수는 정답 레이블로 활용하고 Description은 특징으로써 활용하기 위해 Description으로부터 단어를 추출하고 불용어를 제거한 뒤 어간 추출 알고리즘을 통해 어형이 변형된 단어로부터 어간을 분리해낸 후 추출되는 단어들을 TF-IDF를 사용하여 단어의 빈도수를 계산했다.

TF-IDF는 전체 문서에서 등장하는 모든 단어들이 특정 문서 내에서 갖는 중요도를 나타내는 통계적 수치로써, 문서의 핵심어를 추출하는데 사용된다. TF는 특정 단어가 한 문서 내 나타나는 빈도수 값이며, IDF(Inverse Document Frequency)는 DF(Document Frequency)의 역수로 DF는 특정 단어가 전체 문서 내에서의 나타나는 빈도수 값이다[11].

TF-IDF는 TF와 IDF의 곱으로 이루어지며 특정 문서 내에서 단어 빈도가 높을수록, 전체 문서들 중 그 단어를 포함한 문서가 적을수록

TF-IDF값이 높아지기 때문에 TF-IDF를 사용하여 흔하게 나타나는 단어들을 제거했다.

그 후 WVT(Word Vector Tool)를 사용해서 특징 벡터를 생성하고 고차원의 데이터를 LDA 및 PCA를 통해 차원을 축소함으로써 훈련 속도와 분류 기준의 정확성을 높였다. 차원이 축소된 데이터의 3분의2를 학습용 데이터로 사용하고 나머지를 테스트 위한 데이터로 구성하여 SVM, Random-Forest와 전문 지식과 수치적 데이터를 기반으로 설계된 Fuzzy-System을 활용하여 학습 데이터와 테스트 데이터의 정확도를 비교한 결과 Fuzzy-System이 88.01%의 학습 데이터 정확도와 88.37%의 테스트 데이터 정확도로 가장 좋은 정확도를 도출했다.

하지만 체계적인 설계법이 존재하지 않는 Fuzzy-System으로부터 도출되는 결과는 불확실한 데이터들을 기반으로 설계자가 정한 규칙과 정확한 추론이 아닌 합리적인 추론을 거쳐 얻어짐으로써, 잘못된 예측을 유발할 수 있다고 판단된다[12]. 또한 머신러닝 알고리즘과 자체적으로 설계한 Fuzzy-System을 통해서만 CVSS 점수가 예측되고, 본 연구 외에 딥 러닝을 활용하여 CVSS 점수 예측을 시도한 연구는 없는 것으로 판단됨에 따라 우리는 딥 러닝의 활용을 통해 CVSS 점수를 예측하는 기법을 제시한다.

III. 딥 러닝을 활용한 CVSS 점수 예측 기법

CVSS 점수가 평가되지 않은 CVE의 점수를 예측하기 위해 우리는 CVE-details에 존재하는 모든 CVE들의 ID와 CWE ID, 악용 수, 취약점 타입, 영향을 받는 제품, Description, CVSS 점수 데이터를 수집하였다. 총 수집한 데이터의 수는 약 95,860개로 정답 레이블 역할을 하는 CVSS 점수와 데이터 식별을 위한 CVE ID를 제외한 나머지 데이터는 학습을 위한 특징으로 활용된다[13].

각 CVE ID마다 특징 행렬을 만들기 위해 Description을 제외한 데이터는 종류의 수를 추출한다. 추출 된 데이터 중 제품의 경우 존재하는 종류의 수가 약 38,004개에 이르지만 특징 행렬의 크기와 자주 등장하지 않는 종류들을 고려하여 Description의 크기에 맞춰 유동적으로 구성된다.

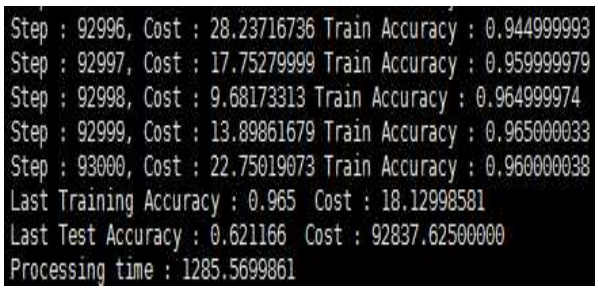
Description은 파이썬의 자연어처리 모듈을 이용하여 불용어 제거, 명사만 추출한 뒤 가장 많이 등장한 단어의 순위를 기준으로 각 1000개, 500개를 추출하였다. 추출된 Description의 개수에 맞춰 아래 [표 1]과 같이 A와 B의 모델과 같은 크기의 특징 행렬이 구성된다.

	A 모델	B 모델
CWE-ID	106	106
Of Exploit	1	1
Vulnerability Type	14	14
Vendor_Product	175	675
Description	1000	500
Total	1296(36x36)	1296(36x36)

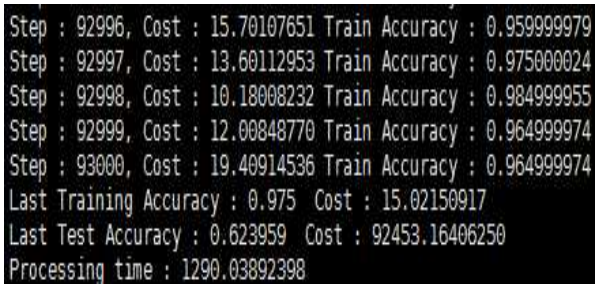
[표 1] 특징 행렬 구조

구성된 특징 행렬을 기반으로 수집한 데이터의 학습을 위해 주로 이미지를 인식하는데 사용되며 2012년 세계적인 이미지 인식 경연 대회 우승 모델인 CNN(Convolutional Neural Network)을 사용하였다. CNN의 구조상 입력 데이터를 이미지로 입력받기 때문에 1296크기의 1차원 행렬로 구성되어 있는 데이터를 36x36 크기의 그레이 스케일 이미지로 변환한다.

변환된 전체 이미지 중 70%는 학습용 데이터 셋으로 구성하고 나머지 30%는 테스트를 위한 데이터 셋으로 구성하여 A, B 모델에 대해 각각 200 에폭 만큼 학습을 진행한 결과 Description에 대한 특징이 더 많았던 A모델은 아래 [그림 4]와 같이 Training Accuracy 96%, Test Accuracy 62%를 도출하였고 제품의 특징이 더 많았던 B모델은 [그림 5]와 같이 Training Accuracy 97%, Test Accuracy 62%를 도출하였다.



[그림 4] A 모델 학습 결과



[그림 5] B 모델 학습 결과

IV. 결론

본 논문에서 우리는 딥 러닝을 활용하여 취약점의 위험도를 나타내는 CVSS 점수를 예측하기 위해 기존에 평가되어 있는 CVE들의 정보를 수집하여 특징으로 CWE-ID, 악용 수, 취약점 타입, 제품, Description을 선정하고 딥 러닝을 활용하여 학습을 진행하였다. 실험 결과 96~97%의 학습 데이터 정확도와 62%의 테스트 데이터 정확도를 도출하였다.

88.01%의 학습 데이터 정확도와 88.37%의 테스트 데이터 정확도를 도출한 Fuzzy-System을 활용한 논문과 비교할 때, 아직 테스트 데이터 정확도가 낮은 것을 알 수 있었다. 이러한 결과의 차이는 수집된 데이터에서 선정된 특징들이 활용되기에 아직 가공되지 않고 정형화되지 않아 도출된 결과라고 판단된다.

이에 따라 향후 연구로 정형화된 특징을 도출할 수 있는 방안을 연구하여 더 나은 정확도를 도출하는 모델을 만들고 검증하고자한다. 이를 통해 평가되지 않은 취약점의 위험도를 예측하여 긴급한 취약점은 우선적으로 패치되고 예방될 수 있도록 컴퓨터 시스템 보안에 기여하고자 한다.

[참고문헌]

[1] Trendmicro, 2017년 연간 위협 보고서:사이버위협의 역설, https://resources.trendmicro.com/rs/945-CXD-062/images/2017_Annual_Security_Roundup_kr.pdf, Feb, 2018

[2] Wikipedia, “워너크라이”, https://ko.wikipedia.org/wiki/워너크라이

[3] MITRE, CVE-Common Vulnerabilities and Exposures (CVE), https://cve.mitre.org/

[4] FIRST, Common Vulnerability Scoring System SIG, https://www.first.org/cvss/

[5] Wikipedia, Common Vulnerabilities and Exposures, https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures

[6] Common Vulerabilities and Exposures, https://cve.mitre.org/cve/identifiers/syntaxchange.html

[7] Wikipedia, Common Vulnerability Scoring System, https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System

[8] OSVDB, Open Source Vulnerability Database, https://blog.osvdb.org/

[9] N. Gupta, Artificial Neural Network, Network and Complex System, vol. 3, No. 1, pp.24-28, March, 2013.

[10] K. Atefeh, An automatic method for CVSS score prediction using vulnerabilities description, Journal of Intelligent & Fuzzy Systems, vol. 30, no. 1, pp. 89-96, 2016

[11] Wikipedia, tf-idf, https://en.wikipedia.org/wiki/Tf-idf

[12] Wikipedia, Fuzzy Control System, https://en.wikipedia.org/wiki/fuzzy_control_

system

[13] CVE Details, CVE security vulnerability database. Security vulnerabilities, exploits, references and more, https://www.cvedetails.com/

2018 한국정보보호학회 하계학술대회

B6 취약점 분석

박 창 섭 (단국대학교)

- **무인 복합 출력기 솔루션의 취약성 분석**
  지우중, 김형식
- **Most Significant Bit가 Most Significant Power이다 – Case Studey: Chip Whisperer**
  이지우, 김주환, 이종혁, 한동국
- **평창 올림픽 악성코드 분석을 통한 향후 공격 예측**
  김찬진, 탁현주, 김민서, 임수민, 염흥열
- **안드로이드 모바일 게임 어플리케이션 보호 솔루션에 대한 분석 및 공격 기법 연구**
  조동민, 최형기
- **임베디드 디바이스의 펌웨어 리버스 엔지니어링 방법 연구**
  박재현, 김승주

무인 복합 출력기 솔루션의 취약성 분석

지우중, 김형식

성균관대학교 전자전기컴퓨터공학과

A Security Vulnerability Analysis for Printer Kiosks

Woojoong Ji, Hyoungshick Kim

Department of Computer Science and Engineering,
Sungkyunkwan University

요 약

무인 복합 출력기는 각종 저장매체나 이메일로 받은 각종 문서나 사진 등을 길거리, 지하철, 학교, 도서관 등에서 바로 인쇄 할 수 있고 여러 가지 작업을 복합적으로 사용할 수 있는 기기이다. 사용자들이 때로는 무인 복합기를 통하여 민감한 정보가 포함된 문서를 출력할 수 있기 때문에 무인 복합 출력기에서 안전하게 문서가 저장 및 관리되어야 한다. 본 논문에서는 무인 복합 출력기에 대한 다양한 보안 위협 가능성을 분석하고, 실현 가능한 다양한 공격 시나리오를 제시하였다. 제시한 공격의 실현 가능성을 검증하기 위하여, 실제 사용 중인 상용 무인 복합 출력기의 네트워크 트래픽을 분석한 결과, 다른 사용자의 인증 정보를 탈취할 수 있으며 이를 이용하여 해당 사용자의 민감한 개인 정보 또한 획득할 수 있음을 확인하였다.

I. 서론

최근 고가의 프린터 장비와 이를 유지하기 위해 드는 유지 관리 비용 등 여러 가지 비용 측면에서 프린터 장비를 사지 않고 일정한 금액을 지불하고 무인 복합 출력기를 많이 사용하고 있는 추세이다. 무인 복합 출력기는 각종 저장매체나 이메일로 받은 각종 문서나 사진 등을 길거리, 지하철, 학교, 도서관 등에서 바로 인쇄 할 수 있고 문서작업은 물론, 인터넷 사용, 필요한 문서나 사진을 스캔하여 전송하는 기능 등 여러 가지 작업을 복합적으로 사용 할 수 있는 기기이다. 이렇게 무인 복합 출력기가 사람들에게 많은 인기가 있는 이유는 언제 어디서나 원하는 문서 작업을 할 수 있고 또 여러 가지 기능을 가진 무인 복합 출력기를 이용하고자 하는 사용자들의 동선을 미리 파악하여 해당하는 곳에 설치하여 별도의 시설을 찾아다닐 필요없이 평소 동선상에서 간편하게 이용할 수 있도록 사용자들에 대한 접근성을 높여 많은 사용자들이 쉽고 빠르게 무인 복합 출력기를 사용할 수 있도록 하여 많은 사람이 사용하고 있는 추세이다.

그러나 많은 기업에서 이러한 무인 복합 출력기를 개발할 때 외적인 부분과 사용자 인터페이스 등 보안적인 관점이 아닌 다른 외적인 부분에 대해 더 많은 노력과 시간을 투자하기 때문에 자연스럽게 사용자의 개인정보나 사용자들이 무인 복합 출력기를 사용함으로써 이로 인해 생기는 보안적인 문제점을 가질 확률이 다소 높다. 예를 들어 사용자들이 무인 복합기를 통하여 민감한 정보가 포함된 문서를 출력할 수 있기 때문에 무인 복합 출력기에서 안전하게 문서가 저장 및 관리되어야 한다. 무인 복합 출력기 특성상 일반 사용자와 악의적인 사용자를 구분 할 수가 없기 때문에 특히 보안에

* 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음(IITP-2018-2015-0-00403)

신경을 많이 써야한다. 예를 들어 악의적인 사용자가 무인 복합 출력기에 일반적인 사용자로 위장하여 악의적인 행동이나 악성프로그램을 설치하여 수행하게 된다면 무인 복합 출력기를 사용하는 사용자의 모든 정보가 악의적인 사용자에게 전송되어 많은 문제점을 발생시킬 수 있다. 본 논문에서는 무인 복합 출력기에 대한 다양한 보안 위협 가능성을 분석하고, 실현 가능한 다양한 공격 시나리오를 제시하였다. 이러한 문제 때문에 보안적인 부분에 더욱 신경을 써야한다. 그래서 본 논문에서는 이러한 보안적인 문제점과 앞의 문제점으로 인해 실제 사용중인 상용 무인 복합 출력기의 네트워크 트래픽을 분석한 결과, 다른 사용자의 인증 정보를 탈취할 수 있으며 이를 이용하여 해당 사용자의 민감한 개인 정보 또한 획득할 수 있음을 확인하였다.

본 논문의 구성은 다음과 같다. 2장에서는 무인 복합 출력기에 대한 공격 방법에 대해 설명하고 3장에서는 2장에서 설명한 공격 방법을 적용하여 실제 사용자의 개인정보 유출 사례를 소개한다. 4장에서는 취약점 개선방안, 마지막으로 5장에서는 결론을 제시한다.

II. 메타 데이터를 이용한 공격

2.1 메타 데이터

메타 데이터란 일반적으로 데이터에 대한 데이터라는 추상적 개념으로 정의가 되지만, 구체적인 의미를 갖기 위해서는 메타 데이터를 활용하는 집단이 다시 정의를 내릴 필요가 있다. ISO 15489에서는 메타 데이터를 기록의 맥락과 내용, 구조와 기록관리 전 과정을 기술한 데이터로 정의하고 있다. 즉, 기록에 대하여 맥락, 내용, 구조, 관리내력 이라는 4가지 영역을 기술하는 데이터라고 이해할 수 있다.

이런 메타 데이터의 많은 유형 중 HTTP URL이라는 메타 데이터는 URL에 특정 데이터를 저장하는데 사용이 된다. 예를 들어 URL 메타 데이터 소스에 대한 입력은 RFC 표준에 의하면 http://host:port/path?query의 형식으로 이루어져 있다.

본 논문에서 이러한 URL 메타 데이터의 정보를 이용해 취약하게 관리되고 있는 상용 무인 복합 출력기 A사에 대해 분석해 보았고 실제 공격 사례는 3장에서 설명하겠다.

2.2 재전송 공격

재전송 공격[1]이란, 사용자의 인증을 쿠키에만 의존해 공격자는 단순한 네트워크 도청을 통해 해당 쿠키 정보를 쉽게 탈취가 가능하다. 이렇게 탈취한 쿠키 정보를 그대로 해당 사이트에게 다시 보내게 되면 해당 사이트는 쿠키만 가지고 사용자를 인증하기 때문에 그대로 탈취당한 사용자의 계정으로 로그인이 되거나 해당 쿠키 정보가 적용된 타 사이트까지 이동이 가능하기 때문에 사용자의 민감한 데이터까지 탈취가 가능하다. 또 이렇게 사용자의 로그인에 관해 생성되는 쿠키 정보가 매번 로그인 할 때마다 생성되는 정보가 아니라 바뀌지 않는 고정된 쿠키 정보이면 탈취 당한 쿠키를 가지고 악의적인 사용자는 해당 사용자의 권한을 항상 가지고 있는 것이다. 이렇게 탈취당한 쿠키를 이용해서 인증이 되는 이유는 요즘 웹 서비스들은 그룹 단위로 통합하는 곳이 늘어감에 따라 이를 위해 다양한 솔루션이 개발되었지만 솔루션들의 보안성은 대부분 쿠키에만 의존하기 때문이다.

본 논문에서는 쿠키 정보를 이용한 공격 방법은 아니지만 위에서 언급한 것처럼 바뀌지 않는 쿠키를 공격에 이용한 것처럼 URL안의 메타 데이터에 존재하는 특정 사용자를 나타내는 값이 바뀌지 않는 정보라는 점이 같아 해당 URL의 메타 데이터에 대해 조작하거나 재전송 한다면 악의적인 공격이 이루어진다.

2.3 추측공격

본 논문에서는 해당 사용자를 나타내는 URL 메타 데이터를 탈취하여 해당 사용자뿐만 아니라 추측 공격으로 다른 사용자의 개인 정보까지도 탈취가 가능한 것을 실제 사례로 소개한다.

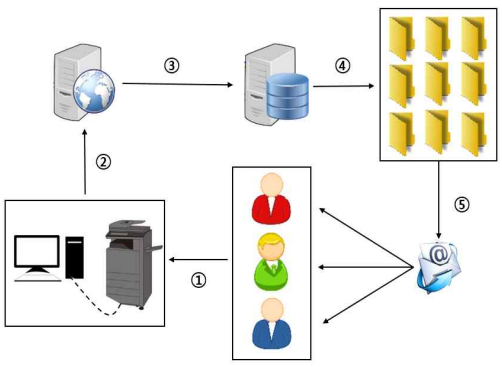
추측 공격[2]이란(Guessing Attacks), 공격자

가 설계자의 의도보다 비교적 작은 키 공간에서 키에 대한 추측 및 검증을 반복하는 것을 말하며, 불법적으로 키 또는 패스워드를 알아내고 이를 이용하여 인증 및 암호키 분배의 안정성을 파괴하는 목적으로 한다.

하지만 본 논문에서는 추측 공격을 암호분석(cryptanalysis) 측면에서 보는 것이 아니라 제한된 작은 키 공간에서 사용자를 나타내는 특정값을 추측 하는 공격으로 설명한다. 다시 말해, URL 메타 데이터에서 사용자의 고유한 정보를 나타낸 정보를 이용하여 다시 재전송 공격을 수행하거나 사용자를 나타내는 공간이 제한적이기 때문에 악의적인 공격자는 제한된 공간만큼만 추측 공격을 하게 된다면 다른 사용자의 데이터까지 얼마든지 접근이 가능하다.

2.4 공격 시나리오

본 논문의 전체적인 공격 시나리오는 다음과 같다. 먼저 이 공격이 이루어지려면 무인 복합 출력기만 가지는 특징을 이용한다. [그림 1]에서는 일반 사용자와 악의적인 사용자가 함께 존재한다. 하지만 무인 복합 출력기 솔루션에는 이를 회원가입을 통해 구분하려고 하지만 A사의 경우 비회원도 이용이 가능하기 때문에 악의적인 사용자는 자신의 신분을 노출하지 않고도 악의적인 행동을 수행할 수 있다.



[그림 1] A사의 무인 복합 출력기 솔루션 구조

[그림 1]에 대해서 설명하자면 ①에서 일반 사용자는 회원가입을 통해 회원으로 해당 솔루션을 이용하거나 비회원으로 선택하여 일정한 금액을 지불하고 해당 서비스를 이용하기 시작한다. 그런 다음 사용자는 자신이 원하는 문서 작업, 인터넷 서핑, 스캔, 인쇄 등 여러 작업 중 사진을 스캔하는 작업을 한다고 가정하자. 그러면 스캔파일은 ②처럼 해당 솔루션 서버에게 보내게 된다. 그런 다음 ③처럼 사용자에게 받은 스캔파일을 다시 자신만이 가지고 있는 파일 서버에 전송하여 ④처럼 각 사용자별로 파일이름을 지정하여 저장한다. 해당 솔루션은 이렇게 파일 서버에 저장된 파일을 ⑤사용자가 회원가입을 할 때 입력했던 이메일로 해당 URL 정보를 평문의 값으로 넘겨주게 된다. 그 후 사용자는 평문으로 된 URL을 통해 솔루션 파일 서버에 스캔 파일을 다운로드 받는 전체적인 과정이다.

하지만 여기서 취약점이 발견이 되었는데 [그림 2]는 해당 사용자의 이메일로 전송된 평문의 URL로 해당 파일을 다운로드 받을 때 WireShark[3]로 패킷을 캡쳐한 패킷 내용이다.

```
GET /?IDX=253744&USERID=GUEST HTTP/1.1
Host:
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.6,en;q=0.4
Cookie: ASPSESSIONIDSASRQABA=NMKBPCGCIDHNKAPMCEOBNMJF
Range: bytes=2361-2361
If-Range: "0CEDD16FFFEF49399FA67B3B421FCD24"
```

랜덤 값 / 사용자 유형 / 다운로드 패킷 캡쳐

[그림 2] 비회원 스캔 파일 다운로드 요청 패킷

위의 [그림 2]를 보면 해당 HTTP URL 메타 데이터에 대해 암호화가 전혀 적용되어 있지 않고 조금만 분석하더라도 http://해당 솔루션 파일 서버의 host 주소/?IDX=특정한 랜덤 값&USERID=해당 유저의 타입 이라는 것을 알 수가 있다.

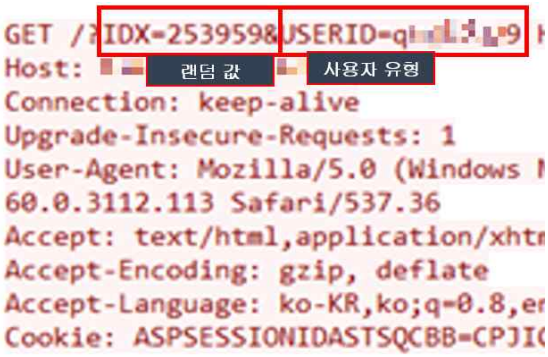
위의 패킷 데이터를 얻기 위해서 공격자는 일반 사용자로 위장하여 일반사용자와 똑같이 해당 무인 복합 출력기 솔루션 이용한다. 그런 다음 [그림 2]처럼 HTTP URL 메타 데이터를 획득한 다음 공격을 진행한다. 자세한 내용은 3장에서 설명하겠다.

III. 무인 복합 출력기 공격 실험 결과

본 절에서는 위에서 설명한 공격시나리오를 바탕으로 무인 복합 출력기 솔루션 A사에 대해 실제 공격에 대한 결과를 설명한다.

3.1 무인 복합 출력기 회원 공격

먼저 해당 솔루션에 회원가입이 되어 있을 경우를 살펴보자. [그림 2]에서는 비회원으로 USERID=GUEST로 되어 있지만 [그림 3]을 보면 USERID=해당 유저 아이디를 볼 수가 있다. 유저 ID는 해당 솔루션 자유게시판 [그림 4]에서 보는 것처럼 쉽게 얻을 수가 있다. 이런 방식으로 악의적인 공격자는 자유게시판이나 다른 사용자가 올린 게시물에서 다른 사용자의 ID를 얻어와 해당 값을 변조하는 프로그램을 실행하여 악의적인 사용자는 IDX값과 USERID를 각각 변조해 변조된 HTTP URL 메타 데이터를 파일서버에게 재전송 공격을 수행하면 파일 서버는 이를 검증하지 않고 그대로 해당 스캔 파일을 넘겨주게 된다.



[그림 3] 회원 스캔 파일 다운로드 요청 패킷



[그림 4] 자유게시판 유저 ID 노출

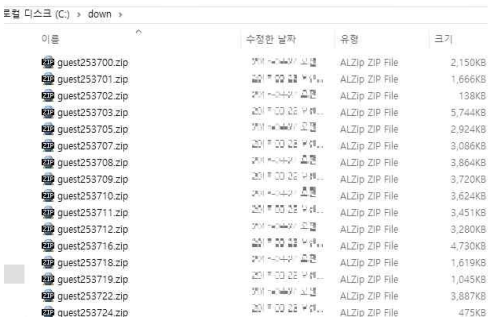
3.2 비회원 공격

A사의 경우 회원가입을 하지 않고 회원가입 했을 때와 동일하게 서비스를 이용 할 수 있다. 다른점은 USERID에 회원 ID가 아닌 GUEST로 설정된다. IDX는 최대 10자리를 가지는 0부터 9까지의 수이다. 많이 사용되는 값은 분석한 결과 6자리를 가장 많이 사용하여 길이는 더 작아진다.

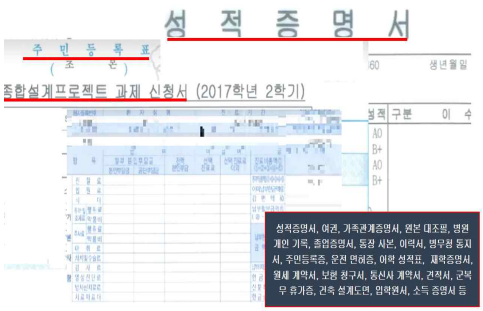


[그림 5] 다른 사용자의 스캔파일

또 파일 서버 특성상 모든 파일을 계속해서 저장할 수 없기 때문에 일정한 시간이 지나면 해당 파일을 삭제해 더 이상 다운로드 할 수가 없다. 따라서 IDX가 가지는 전체적인 공간은 더 줄어들어 추측공격과 무차별공격[4]으로 인해 빠른 시간에 회원/비회원의 스캔 파일[그림 5]에 접근할 수가 있고 해당 스캔파일에는 여러 가지 개인정보들이 포함된 많은 문서[그림 6]들이 유출되었음을 확인하였다.



[그림 6] 회원/비회원 스캔 파일



[그림 6-1] 회원/비회원 스캔 파일

또 해당 파일의 이름이 생성될 때 사용자가 사용한 무인 복합 출력기의 기기 번호와 스캔한 시간으로 기본적으로 설정되어 스캔 파일 이름과 해당 개인정보가 유출된다면 사용자의 위치도 함께 노출이 때문에 각종 범죄의 대상이 될 우려가 높다.

IV. 취약점 개선방안

발견된 2가지 취약점은 솔루션 개발 업체에서 조금만 보안에 관심만 있었어도 막을 수 있는 간단한 취약점이다. 이러한 공격을 제일 간단하게 방어할 수 있는 기법은 해당 HTTP URL 정보를 해시함수를 통해 악의적인 사용자가 일반적인 사용자로 위장하여 위와 똑같은 방법을 사용하더라도 URL에는 해시값이 들어가 있기 때문에 큰 비용없이 간단한 코드 몇 줄로 해당 취약점에 대한 공격을 막을 수가 있다.

V.결론

본 논문은 무인 복합 출력기에 대한 취약성을 알아보았다. 하지만 우리나라의 중, 소규모 기업들은 이런 취약점이 발견되었다고 하더라도 보안인력과 취약점을 개선할 때 발생하는 비용적인 측면 때문에 이를 확인하고도 묵인하고 있는 경우가 많다. 이와 마찬가지로 본 논문에서 소개한 무인 복합 출력기에 대한 취약성을 해당 기업에게 2017년 9월 20일에 해당 취약점을 발견하여 제보를 하였지만 2018년 5월 25일 현재까지도 패치가 되어있지 않은 상황이다. 해당 취약점은 HTTP URL 메타 데이터를 악의적인 사용자가 마음대로 조작할 수 있다는 점과 파일 서버에서 아무런 사용자의 인증을 거치지 않고 해당 스캔파일을 다운로드 할 수 있는 간단한 2가지의 취약점인데 해당 개선방안까지 제시하여 제보를 하였지만 아직까지 취약점에 패치를 하지 않는 것으로 보아 아직도 기업에서는 보안의식이 심각하게 낮다는 것을 보여주는 사례이다.

[참고문헌]

[1] 맹영재, 양대헌. (2008). Single Sign-On 솔루션의 재전송 공격 취약점 분석. 정보보호학회논문지, 18(1), 103-114.

[2] 권태경, 송주석. (1997). 추측 공격에 대해서 안전하고 효율적인 패스워드 기반 인증 프로토콜. 정보과학회논문지(A), 24(8), 795-806.

[3] https://www.wireshark.org/download.html

[4] "Implementation of tools for brute forcing touch inputted passwords," 2012 International Conference for Internet Technology and Secured Transactions, London, 2012, pp. 807-808.

Most Significant Bit가 Most Significant Power이다
- Case Study : ChipWhisperer

이지우*, 김주환**, 이종혁*, 한동국*,***

*국민대학교 금융정보보안학과, **국민대학교 수학과, ***국민대학교 정보보안암호수학과

Most Significant Bit is Most Significant Power
- Case Study : ChipWhisperer

Ji-Woo Lee*, Ju-Hwan Kim**, JongHyeok Lee*, Dong-Guk Han*,***

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

요 약

부채널 분석이란 실제 장비에서 암호 알고리즘이 동작할 때 발생되는 소비 전력, 전자기파 등의 부가적인 정보를 이용하여 암호키와 같은 비밀 정보를 분석하는 공격 방법이다. 부채널 분석 방법 중 전력 분석의 경우 선택하는 소비 전력 모델에 따라 분석 결과가 크게 달라질 수 있는데, 일반적으로 대상 암호 알고리즘이 사용하는 연산 단위의 모든 비트 값을 이용하여 전력 소모량을 추측하는 해밍 웨이트 모델이나 해밍 디스턴스 모델을 이용한다. 하지만 특정 위치의 비트가 다른 비트들에 비해 전력 소모량에 미치는 영향이 크다면 모든 비트의 값을 이용하여 전력 소모량을 추측하는 것보다 특정 위치의 비트 값만을 이용하여 전력 소모량을 추측하였을 때 분석 성능이 높게 나올 수 있다. 본 논문에서는 NewAE Technology 사에서 제작한 ChipWhisperer 전력 수집 보드를 이용하여 AES 암호 알고리즘이 동작할 때 소모되는 전력량을 측정하고, 최상위 비트(MSB)의 정보만을 이용하여 전력 소모량을 추측한 후 분석을 수행하는 경우가 바이트 전체를 활용한 경우보다 분석 성능이 높음을 보인다. 따라서 ChipWhisperer 전력 수집 보드가 사용하는 Atmel XMEGA128 Chip을 대상으로 차분 전력 분석을 수행할 경우 바이트 기반의 분석보다 최상위 비트(MSB) 기반 분석이 물리적 취약성 검증 모델로 더 적합하다.

I. 서론

최근 정보 보안의 중요성이 부각되면서 IT 제품, 금융 IC 카드 등 다양한 분야에서 수학적으로 안전한 암호 알고리즘을 사용하고 있다. 하지만 실제 장비에서 암호 알고리즘이 동작할 때 발생되는 소비 전력, 전자기파 등의 부가적인 정보들을 이용하여 비밀 정보를 분석하는 부채널 분석(Side Channel Analysis, SCA)[1]을 이용하여 암호키가 노출될 수 있다. 부채널 분석 방법 중 전력 분석은 암호 알고리즘이 수행되는 동안 발생되는 소비 전력을 이용하여 비밀 정보를 분석하는 방법이다. 전력 분석은 소량의 파형만을 이용하여 분석을 수행하는 단순 전력 분석(Simple Power Analysis, SPA)과 다량의 파형을 두 집단으로 나누어 그 차분을 이용하는 차분 전력 분석(Differential Power Analysis, DPA)[2]으로 나누어진다. 차분 전력 분석은 부채널 파형과 암호 알고리즘의 중간 값 간의 상관도를 이용하는 상관관계 전력 분석(Correlation Power Analysis, CPA)[3]으로 발전되었다.

실제 암호 알고리즘이 동작할 때 발생되는

전력 소모량은 장비에 따라 다르기 때문에 전력 분석에서 선택하는 소비 전력 모델에 따라 분석 결과가 크게 달라질 수 있다. 일반적으로 사용되는 소비 전력 모델에는 모든 비트의 가중치가 동일하다는 가정으로 전력 소모량을 추측하는 해밍 웨이트(Hamming Weight, HW) 모델과 해밍 디스턴스(Hamming Distance, HD) 모델이 있다. 실제 장비에서 연산이 수행될 때 여러 비트가 동시에 전력 소모량에 영향을 미칠 수 있기 때문에 대부분의 전력 분석에서는 대상 암호 알고리즘이 사용하는 연산 단위의 모든 비트를 이용하여 전력 소모량을 추측하는 방법을 선택한다. 하지만 특정 위치의 비트가 다른 비트들에 비해 전력 소모량에 미치는 영향이 현저히 크다면 모든 비트를 이용하는 것보다 특정 위치의 비트만을 이용하여 전력 소모량을 추측하였을 때 분석 성능이 높게 나올 수 있다.

본 논문에서는 NewAE Technology 사에서 제작한 ChipWhisperer 전력 수집 보드[4]를 이용하여 AES 암호 알고리즘이 동작할 때 발생되는 소비 전력량을 측정하고, 최상위 비트(Most Significant Bit, MSB)의 정보만을 이용해 전력 소모량을 추측하여 분석을 수행할 때 바이트 전체를 활용한 경우보다 분석 성능이 높음을 보인다. DPA에서 암호키의 첫 번째 후보에 대한 차분 값과 두 번째 후보에 대한 차분 값의 비율이 1.2 이상일 때 첫 번째 후보가 올바른 키로 분석되었다고 가정하면, MSB의 정보만을 이용한 경우 약 90개의 파형에서 암호키의 모든 바이트가 올바르게 분석되지만 바이트 전체를 활용한 경우 1,000개의 파형을 이용하여도 암호키의 일부 바이트가 분석되지 않았다. 따라서 ChipWhisperer 전력 수집 보드가 사용하는 Atmel XMEGA128 칩을 전력 기반 부채널 분석할 경우 바이트 기반 DPA 보다는 MSB 기반 DPA가 물리적 취약성 검증 모델로 더 적합하다.

II. 관련 연구

실제 장비에서 연산이 수행될 때 발생하는 총 전력 소모량은 다음과 같이 나타낼 수 있다.

$$P_{total} = \epsilon \bullet g(S_1, S_2) + P_{noise}$$

전력 분석을 수행하기 위해서는 실제 소비 전력과 유사한 P_{total} 값을 획득해야 하지만 ϵ과 P_{noise}의 추측이 어렵기 때문에 알고리즘의 중간 계산 값 S_1, S_2에 대한 소비 전력 모델 $g()$의 선택에 따라 P_{total}을 추측한 후 분석을 수행한다. 주로 쓰이는 소비 전력 모델에는 모든 비트의 가중치가 동일하다고 가정하여 전력 소모량을 추측하는 해밍 웨이트 모델과 해밍 디스턴스 모델이 있다. 해밍 웨이트 모델의 경우 전력 소모량이 1의 값을 갖는 비트의 개수에 비례하다고 보며, 해밍 디스턴스 모델의 경우 변화가 일어나는 비트의 개수에 비례하여 전력 소모량이 발생한다고 예상한다. 이때 각 모델에 대한 총 전력 소모량은 다음과 같이 나타낼 수 있다.

(1) $P_{total} = \epsilon \bullet HW(S_2) + P_{noise}$

* $HW(x)$: x의 비트표현시 1의 개수

(2) $P_{total} = \epsilon \bullet HD(S_1, S_2) + P_{noise}$

$= \epsilon \bullet HW(S_1 \oplus S_2) + P_{noise}$

* $HD(x,y)$: x에서 y로 변할 때 변한 비트의 개수

실제 장비에서 연산이 수행될 때 여러 비트 값이 동시에 전력 소모량에 영향을 미칠 수 있기 때문에 대부분의 전력 분석에서는 해밍 웨이트나 해밍 디스턴스 모델과 같이 모든 비트의 값을 이용하여 전력 소모량을 추측한다.

III. ChipWhisperer 전력 분석

본 절에서는 NewAE Technology 사에서 제작한 ChipWhisperer 전력 수집 보드를 이용하여 AES 암호 알고리즘이 동작할 때 발생되는 소비 전력량을 측정하고, MSB의 정보만을 이용해 전력 소모량을 추측하여 분석을 수행할 때 바이트 전체를 활용한 경우보다 분석 성능이 높음을 보인다. ChipWhisperer 전력 수집 보드가 사용하는 Atmel XMEGA128 칩의 사양

은 Table. 1.과 같다.

Table. 1. Specifications of Atmel XMEGA128 Chip

Operating Voltage Range (V)	1.6 ~ 3.6
Flash Memory (KB)	128
SRAM (bytes)	8
EEPROM (bytes)	2048
CPU Speed (MIPS/DMIPS)	32

실험을 위해 8비트 기반 소프트웨어로 구현된 AES-128 암호 알고리즘이 ChipWhisperer에서 1,000번 동작할 때 소비되는 전력량을 측정하였으며, 1라운드 SubBytes 함수의 출력을 분석 위치로 하여 DPA와 CPA를 각각 수행하였다. 소비 전력 모델은 특정 위치의 비트만을 이용하는 방법을 선택하였으며, 여기서 특정 위치란 8비트 중 MSB부터 최하위 비트(Least Significant Bit, LSB)까지를 의미한다. 또한 모든 비트 값을 이용하여 전력 소모량을 추측할 때와의 성능 비교를 위해 일반적으로 많이 사용되는 해밍 웨이트 모델을 추가적으로 선택하였다.

3.1 DPA 결과

본 논문에서는 특정 위치의 비트만을 이용하여 전력 소모량을 추측하기 위해 다음과 같은 시나리오를 이용하여 DPA를 수행하였다.

① 1,000개의 평문 p_i에 대하여 전력 소모량을 측정한다.

② 추측하는 비밀 정보 값 k에 따라 암호 알고리즘의 중간 값 $s[p_i \oplus k]$를 계산한다.

③ 8비트의 중간 값 중 대상으로 하는 비트의 값이 1인지 0인지에 따라 측정한 전력 소모량을 두 집합으로 분류한다.

④ 두 집합 간의 차분 값을 최댓값으로 갖는 k를 산출한다.

모든 비트의 값을 이용하여 전력 소모량을 추측한 경우 ③에서 8비트 중간 값의 해밍 웨이트가 4 이상인지 미만인지에 따라 파형을 두 집합으로 분류하여 분석을 수행하였다.

수집한 분석 파형 중 실제 분석에 사용되는 파형의 개수를 각각 1,000, 700, 400, 100개로 하였을 때의 분석 결과는 다음과 같다. 암호키의 첫 번째 후보에 대한 차분 값과 두 번째 후보에 대한 차분 값의 비율이 1.2 이상이면 첫 번째 후보가 올바른 키로 분석되었다고 간주한다. Fig. 1.은 올바른 키로 분석된 바이트 수를 나타낸다. MSB를 이용해 전력 소모량을 추측하였을 때 100개의 파형에서 모든 바이트 값이 올바르게 분석되지만 다른 위치의 비트 값을 이용하거나 해밍 웨이트 모델을 이용한 경우는 1,000개의 파형 모두를 사용하여도 분석되지 않은 바이트가 존재하였다.

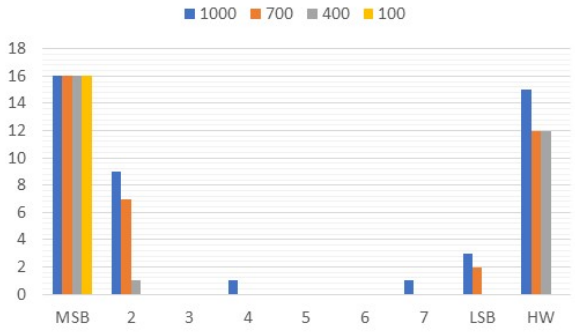


Fig. 1. Number of correctly analyzed bytes (DPA)

따라서 ChipWhisperer 전력 수집 보드가 사용하는 Atmel XMEGA128 칩을 전력 기반 부채널 분석할 경우 바이트 기반 DPA 보다는 MSB 기반 DPA가 물리적 취약성 검증 모델로 더 적합하다.

3.2 CPA 결과

본 논문에서는 특정 위치의 비트만을 이용하여 전력 소모량을 추측하기 위해 다음과 같은 시나리오를 이용하여 CPA를 수행하였다.

① 1,000 개의 평문 p_i에 대하여 전력 소모량을 측정한다.

② 추측하는 비밀 정보 값 k에 따라 암호 알고리즘의 중간 값 $s[p_i \oplus k]$를 계산한다.

③ 8비트의 중간 값 중 대상으로 하는 비트와 측정한 전력 소모량의 피어슨 상관계수 $corr_k$를 계산한다.

④ $corr_k$을 최댓값으로 갖는 k를 산출한다.

모든 비트를 이용하여 전력 소모량을 추측한 경우 ③에서 8비트 중간 값의 해밍 웨이트와 측정한 전력 소모량의 피어슨 상관계수를 계산하여 분석을 수행하였다.

수집한 분석 파형 중 실제 분석에 사용되는 파형의 개수를 각각 1,000, 700, 400, 100개로 하였을 때의 분석 결과는 다음과 같다. 암호키의 첫 번째 후보에 대한 상관계수와 두 번째 후보에 대한 상관계수의 비율이 1.2 이상이면 첫 번째 후보가 올바른 키로 분석되었다고 간주한다. Fig. 2.는 올바른 키로 분석된 바이트 수를 나타낸다. DPA와 다르게 MSB를 이용해 전력 소모량을 추측하였을 때와 해밍 웨이트 모델을 이용한 경우 모두 100개의 파형에서 모든 바이트 값이 올바르게 분석되었다. 따라서 두 소비 전력 모델의 성능을 비교하기 위해 100개의 파형에서 첫 번째 후보에 대한 상관계수와 두 번째 후보에 대한 상관계수의 비율을 Fig. 3.과 같이 나타내었으며, MSB만 이용한 전력 소비 모델이 더 좋은 분석 성능을 보였다. 또한 모든 바이트가 올바르게 분석되는 최소 파형수도 각각 약 60개, 40개로 MSB만 활용하는 경우가 더 적은 수의 파형으로 분석이 가능하였다.

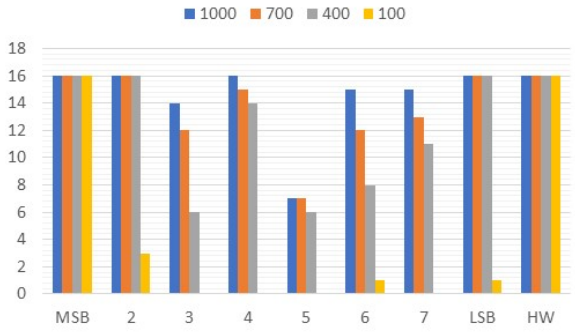


Fig. 2. Number of correctly analyzed bytes (CPA)

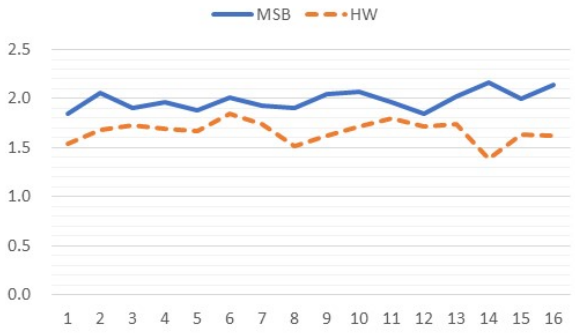


Fig. 3. Ratio of correlation with 100 traces (CPA)

따라서 ChipWhisperer 전력 수집 보드가 사용하는 Atmel XMEGA128 칩을 전력 기반 부채널 분석할 경우 바이트 기반 CPA 보다는 MSB 기반 CPA가 물리적 취약성 검증 모델로 더 적합하다.

IV. 결론

부채널 분석에서 DPA와 CPA를 수행할 때, 선택하는 소비 전력 모델에 따라 분석 성능이 달라진다. 실제 장비에서 연산이 수행될 때 여러 비트가 동시에 전력 소모량에 영향을 미칠 수 있기 때문에 대부분의 전력 분석에서는 모든 비트를 이용하여 전력 소모량을 추측하는 방법을 선택한다. 하지만 특정 위치의 비트가 다른 비트들에 비해 전력 소모량에 미치는 영향이 크다면, 모든 비트를 이용하는 것보다 특정 위치의 비트만을 이용하여 전력 소모량을 추측하였을 때 분석 성능이 높게 나올 수 있다.

본 논문에서는 NewAE Technology 사에서 제작한 ChipWhisperer 전력 수집 보드를 이용하여 AES 암호 알고리즘이 동작할 때 발생되는 전력 소모량을 측정하고, MSB의 정보만을 이용하여 분석을 수행한 경우가 바이트 전체를 활용한 경우보다 분석 성능이 높음을 보였다. 따라서 ChipWhisperer 전력 수집 보드가 사용하는 Atmel XMEGA128 칩을 대상으로 전력 기반 부채널 분석을 수행할 경우 바이트 기반의 분석보다 MSB 기반 분석이 물리적 취약성 검증 모델로 더 적합하다.

[사사] 본 연구는 고려대 암호기술 특화연구센터(UD170109ED)를 통한 방위사업청과 국방과학연구소의 연구비 지원으로 수행되었습니다.

[참고문헌]

[1] P.Kocher, J.Jaffe, and B.Jun, “Introduction to differential power analysis and related attacks”, White Paper, Cryptography Research. Available : http://www.cryptography.com, 1998.

[2] P.Kocher, J.Jaffe, and B.Jun, “Differential power analysis”, Advances In Cryptology CRYPTO′ 99, LNCS 1666, pp. 388-397, 1999.

[3] E.Brier, C.Clavier, and F.Olivier, “Correlation power analysis with a leakage model”, Cryptographic Hardware and Embedded Systems, LNCS 3156, pp.16-29, 2004.

[4] ChipWhisperer, “http://newae.com/tools/chipwhisperer/”, Last accessed 2018/05/27.

평창 올림픽 악성코드 분석을 통한 향후 공격 예측

김찬진*, 탁현주*, 김민서*, 임수민*, 염흥열*

*순천향대학교 정보보호학과

Prediction of future attacks through malicious code analysis at the Pyeongchang Olympics

Chan-Jin KIM*, Hyun-Ju TAK*, Min-Seo KIM*, Su-Min LIM*, Heung-Youl YOUM*

*Division of information security, Soonchunhyang University.

요 약

2018 평창 올림픽이 성황리에 막을 내렸다. 세계적인 축제인 만큼 많은 사람들의 이목을 끌었지만 해커들 역시 기승을 부렸다. 개막식 당일 올림픽을 방해하기 위한 목적으로 악의적인 해커들의 공격을 받아 미디어센터 IPTV 중단, 현장 유무선 네트워크 시스템 마비, 올림픽 관련 웹사이트가 마비되었다. 유동적인 대처에 의해 12시간 만에 복구되었지만 전 세계적으로 주목하는 올림픽 개막식에서 이러한 피해는 결코 적다고 말할 수 없다. 평창 올림픽 공격은 이전 올림픽과는 달리 파괴형 악성코드를 사용하여 더욱 집중 받고 있다.

본 논문에서는 올림픽에서 발생한 파괴형 악성코드에 대한 분석을 통해 공격에 따른 피해를 알아보고 그에 대한 대응방안과 향후 공격을 제시하고자 한다.

I. 서론

2018년 2월 9일 평창 동계올림픽이 개막되어 25일 폐막식과 함께 끝이 났다. 성공리에 개최되었던 평창 동계올림픽에서는 한 차례의 사이버 공격이 존재했다. 2월 9일 개막식을 노린 사이버 공격은 랜섬웨어와 같이 시스템 데이터를 볼모로 이익을 얻으려는 것이 아닌 시스템을 망가뜨려 IT 기반 서비스 가동이나 운영을 방해하려는 목적의 파괴형 악성코드였다. 심지어 해당 악성코드는 악성코드 분석 공유 사이트인 VirusTotal에 2018년 2월 9일에 올라와 2018년 2월 12일에 분석되어 공격자가 사전에 공격 시나리오를 세우고 범행을 저질렀을 가능성 또한 보여주고 있다.[1]

올림픽을 겨냥한 사이버 공격은 과거에도 여러 차례 존재했다. 2008년 베이징올림픽 당시 보고된 사이버 공격 건수는 약 1,900건, 2012년 런던 올림픽에서는 2억 회가 넘는 올림픽 공식 웹 사이트 공격 시도가 발생했으며, 소치동계올림픽에서는 3억 2,200만 건, 2016년 리우올림픽에서는 5억7000만 건의 사이버 공격이 보도된 바 있다.

지금껏 발생했던 올림픽 사이버 공격 유형은 DDoS 공격을 통한 올림픽 웹사이트 접근을 차단하거나, 올림픽 콘텐츠로 위장한 이메일 피싱 공격이 많이 발생했다. 하지만 런던올림픽 당시 나타났던 PDF 형식의 악성코드를 필두로 유형이 많이 변화하고 있다. 그 결과로 이번 평창올림픽은 유례를 찾아보기 힘든 APT(지능형지속위협) 공격이었다. 위와 같은 사실은 앞으로 개최될 도쿄와 파리에서의 올림픽도 공격이 발생할 가능성이 크다는 것을 보여준다. [2][3][4]

본 논문의 구성은 다음과 같다. 제2장에서는 본 논문에서 소개한 올림픽 디스트로이어의 분석과정을 서술하고 분석 결과를 토대로 대응방안을 기술하며, 제3장에서는 향후 공격 예측을 논한다.

II. 본론

2.1 평창올림픽 악성코드 분석

본 악성코드는 Windows 7 64bit 환경에서 OllyDBG[5]와 IDA[6]라는 툴을 이용하여 분석했다.

올림픽 악성코드는 시스템 정보 탈취 프로그램, 브라우저 정보 탈취 프로그램, 원격제어 프로그램, 시스템 파괴 프로그램을 드롭한다. 그 중, 원격제어 프로그램은 정상적인 프로그램으로 원격제어기능을 악용하는데 사용한다. 각각 드롭된 파일들의 행위는 [표 1]과 같다.

[표 1] 올림픽 악성코드 드롭파일 및 행위

구분	행위
올림픽 악성코드	파일 드롭
브라우저 정보 탈취 프로그램	브라우저 정보 탈취
시스템 정보 탈취 프로그램	시스템 정보 탈취
원격제어 프로그램	원격제어
시스템 파괴 프로그램	시스템 파괴

2.1.1 올림픽 악성코드 분석

올림픽 악성코드는 파일을 드롭할 때, 암호화된 리소스를 추출하고, AES 알고리즘으로 복호화를 한다. 이때, AES 알고리즘을 복호화하기 위한 키는 “123”을 MD5로 해시한 값이다. 각 파일을 드롭한 이후, [그림 1]과 같이 드롭한 파일들과 통신하기 위해 드롭한 파일들에 각각 인자 값을 “123”과 파이프 이름으로 설정한다.

```
0062D4B4  000EAABE  CALL to CreateProcessW from EDB1FF25.000EAAB8
0062D4B8  0039A348  ModuleFileName = "C:\Users\ADMINI~1\AppData\Local\Temp\srqqv.exe"
0062D4BC  0062D5D0  CommandLine = " 123 \\.\pipe\50B4B481-BC12-4EEC-BB6A-199139767DC1"
0062D4C0  00000000  pProcessSecurity = NULL
0062D4C4  00000000  pThreadSecurity = NULL
0062D4C8  00000000  InheritHandles = FALSE
0062D4CC  00000000  CreationFlags = 0
0062D4D0  00000000  pEnvironment = NULL
0062D4D4  00000000  CurrentDir = NULL
0062D4D8  0062D510  pStartupInfo = 0062D510
0062D4DC  0062D500  pProcessInfo = 0062D500
```

[그림 1] 실행 시 파이프 인자 값

원격제어를 할 때, [그림 2]와 같이 하드코딩된 44개의 도메인과 계정을 사용한다. 이러한 특징들을 통해 평창 올림픽 때 APT 공격이 진행되고 있었고, 악성코드에 명령을 내려 내부 네트워크와 주변 기기들을 감염시키도록 명령을 내리는 단계[7]인 Lateral Movement일 때 발견된 악성코드라는 것을 유추할 수 있다.

```
.data:0042891E  0000001C  C  Pyeongchang2018.com\\pcadmin
.data:0042893A  0000000D  C  [illegible]
.data:0042894B  00000021  C  Pyeongchang2018.com\\PCA.GMSAdmin
.data:0042896C  0000000C  C  [illegible]
.data:0042897C  0000001B  C  Pyeongchang2018.com\\cert01
.data:00428997  0000000A  C  [illegible]
.data:004289A5  00000016  C  g18.internal\\minadmev
.data:004289BB  00000009  C  [illegible]
.data:004289C8  0000001E  C  g18.internal\\adm.adam.wollman
.data:004289E6  0000000B  C  [illegible]
.data:004289F5  00000021  C  g18.internal\\adm.vadim.antonenko
.data:00428A16  0000000A  C  [illegible]
```

[그림 2] 하드코딩된 도메인 및 계정

2.1.2 브라우저 정보 탈취 프로그램 분석

브라우저 정보 탈취 프로그램은 [그림 3]과 [그림 4]와 같이 크롬이나 파이어폭스 등의 브라우저 관련 정보를 탈취하여 [그림 5]와 같은 쿼리문을 통해 저장한다. 탈취되는 정보는 브라우저 내에 로그인되어있는 프로필이나 저장된 아이디와 패스워드 등이 있다.

```
SHGetFolderPathA(0, 28, 0, 0, pszPath);
v2 = &pszPath[lstrlenA(pszPath)];
v3 = lstrlenA("\\Google\\Chrome\\User Data\\Default\\Login Data");
sub_10081E70(v2, "\\Google\\Chrome\\User Data\\Default\\Login Data", v3);
```

[그림 3] 크롬 브라우저 탈취

```
v3 = lstrlenA("\\Mozilla\\Firefox\\");
sub_10081E70(v2, "\\Mozilla\\Firefox\\", v3);
v2[v4] = 0;
sub_100821C0(&FileName, 261, (int)"%s\\profiles.ini",
GetPrivateProfileStringA("Profile0", "Path", Default,
```

[그림 4] 파이어폭스 브라우저 탈취

```
sub_1005C930(
  (int)"SELECT origin_url, username_value, password_value FROM logins;",
```

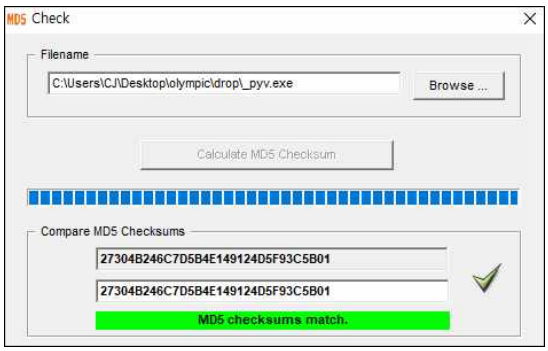
[그림 5] 저장되는 쿼리문

2.1.3 원격제어 프로그램 분석

원격제어 프로그램은 [그림 6]과 [그림 7]과 같이 해당 프로그램의 디지털 서명이나 해시를 통해 정상적인 파일이라는 것을 알 수 있다. 또한, 올림픽 악성코드가 해당 프로그램을 통해 원격제어기능을 악용한다는 것을 알 수 있다.



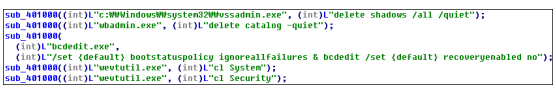
[그림 6] 디지털 서명



[그림 7] MD5Check[8]를 통한 해시값 비교

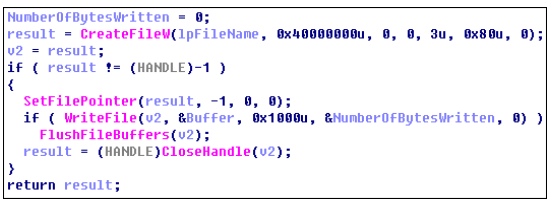
2.1.4 시스템 파괴 프로그램 분석

시스템 파괴 프로그램은 [그림 8]과 같이 사용자가 컴퓨터를 복구하는 것을 막기 위해 볼륨 쉐도우 카피 및 카탈로그를 삭제하고, Windows 오류 복구 알림창 표시를 하지 않음으로 설정하며, 복구모드를 사용하지 않도록 설정하고, 이벤트 로그들을 삭제한다. 또한, 서비스들의 Start Type을 SERVICE_DISABLED 상태로 변경해 서비스들을 중지시키고, [그림 9]와 같이 파일 내용들을 공백으로 덮어씌움으로써 시스템들이 정상적으로 동작하지 못하게 한다.



```
sub_A01000((int)L"c:WWindowsWWsystem32WWvssadmin.exe", (int)L"delete shadows /all /quiet");
sub_A01000((int)L"wbadmin.exe", (int)L"delete catalog -quiet");
sub_A01000(
  (int)L"bcdedit.exe",
  (int)L"/set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no");
sub_A01000((int)L"wevtutil.exe", (int)L"cl System");
sub_A01000((int)L"wevtutil.exe", (int)L"cl Security");
```

[그림 8] 복구 차단 루틴



```
NumberOfBytesWritten = 0;
result = CreateFileW(lpFileName, 0x40000000u, 0, 0, 3u, 0x80u, 0);
v2 = result;
if ( result != (HANDLE)-1 )
{
  SetFilePointer(result, -1, 0, 0);
  if ( WriteFile(v2, &Buffer, 0x1000u, &NumberOfBytesWritten, 0) )
    FlushFileBuffers(v2);
  result = (HANDLE)CloseHandle(v2);
}
return result;
```

[그림 9] 파일 손상 루틴

2.2 올림픽 멀웨어 공격에 대한 대응방안

파괴형 악성코드는 데이터를 복구할 수 있는 Ransom-ware와는 다르게 기존에 있던 데이터를 완전히 지우기 때문에 데이터 복원이 불가능하다. 평창 동계 올림픽대회 및 동계 패럴림픽 대회 조직위원회가 대회 기간 사이버 공격에 대비하기 위해 '사이버 침해 대응팀'을 운영하여 사이버 공격에 대비·대응을 진행하였고, 이에 따라 개막식 중 발생한 사이버 공격에 대해 12시간 이내에 인지·대응하였다[9][10]. 이때 발생한 악성코드 샘플을 분석한 결과 공격자들이 정상적인 소프트웨어(PsExec 원격 관리 툴, WMI 윈도우 관리 도구)를 통해 접근 하였으며, 시스템에 침투한 후 정상 툴을 이용해 네트워크 내부에서 활동하였다[11]. 이러한 사이버 공격에 대한 대응 방안에는 여러 방안들이 존재한다.

2.2.1. 백신과 OS를 정기적으로 업데이트한다. 이는 중요한 예방법 중 하나로, 악성코드 감염 방지를 위해 백신과 OS를 정기적으로 업데이트 하는 방안이 있다. 알려지지 않은 악성코드에 대한 탐지가 어렵다는 단점이 존재하지만, 가장 우선적으로 권장되는 방안이다[11].

2.2.2 신뢰할 수 없는 발신자에 대한 메일 열람에 주의한다. 출처가 확실하지 않은 신뢰할 수 없는 스팸, 광고성 메일에는 악성코드 및 여러 바이러스가 숨겨져 있을 가능성이 크기 때문에 의심되는 메일에 대한 열람을 자제하는 것은 사이버 공격에 대한 감염 사고 발생률을 감소시킬 수 있는 하나의 방안이다[12].

2.2.3. 비 권한 프로세스에 대한 실행을 차단할 수 있는 프로그램을 사용한다. 파괴형 악성코드는 서버를 대상으로 발생하는 공격으로 복구 불가능하게 만든 후 시스템을 파괴 시킨다. 비 권한 프로세스에 대한 실행이 차단 될 경우 올림픽 사례와 같은 악성행위가 불가능 하다. VMM OS 단에서 동작하는 프로그램을 사용하는 것은 파괴형 악성코드의 보안 방안 중 하나이다[12].

III. 결론

IT기술의 발전에 따라 올림픽뿐만 아니라 여러 스포츠 경기에 사이버기술이 도입되는 추세이다. 다양한 기술이 도입되는 만큼 여러 가지 공격을 예측할 수 있다.

비디오 판독 시스템 공격이 가능하다. 최근 다양한 스포츠 종목에서 사람이 보지 못한 부분들을 판독해 줄 수 있는 비디오 판독 시스템의 도입이 일반화되고 있다. 판독을 통한 1점에 승패가 갈릴 수 있는 스포츠에서는 판독이 매우 중요한 요소 중 하나이기 때문이다. 이를 악용해 자신이 응원하는 팀이나 선수에게 유리하게 작용시키기 위해 판독 시스템을 공격할 수 있다.

로봇류 관련 공격도 가능하다. 앞으로 오심과 편파성 우려가 없는 로봇을 스포츠 심판으로 대체할 확률이 높다. 일본체조협회에서는 2020 도쿄올림픽 체조경기 심판을 로봇으로 대체하기 위해 로봇을 개발 중이라고 발표했다. 테니스경기에서도 10명 중 9명이 로봇 심판으로 대체되는 상황이다. 때문에 로봇류 관련 공격도 많을 것으로 예상한다.[13][14]

선수 모니터링 즉, 도핑테스트에 관한 공격도 가능하다. 도핑은 산소를 운반하는 적혈구를 늘리거나 근육을 강화하는데 앞으로 도핑 기술이 기존 약물 복용에서 유전자 조작으로 전환되어 도핑 테스트가 어려워질 것으로 예상된다. 일본에서는 이러한 어려움을 막기 위해 새로운 도핑테스트를 하는 기술을 개발 중이며 이에 따른 공격도 가능할 것이다.[15]

본 논문에서는 평창 올림픽에서 사용된 파괴형 악성코드에 대해 알아보고 그에 대한 피해와 대응 방안을 제시하였다. 본 논문을 통해 향후 공격을 예측할 수 있으며 향후 공격기법에 관한 지속적인 연구와 효과적인 대응방안 마련이 필요하다.

[참고문헌]

[1] MSN news, "평창대회 노린 사이버 공격 잇따라", https://www.msn.com/ko-kr/news/techandscience/올림픽-평창대회-노린-사이버-공격-잇따라…주의보-종합/ar-BBIQchk

[2] boannews, "평창올림픽 홈피 공격",http://www.boannews.com/media/view.asp?idx=66756&page=3&kind=1&search=title&find=%BF%C3%B8%B2%C7%C8

[3] zdnet, "파괴형 악성코트, 올림픽 개회식 방해 목적". http://www.zdnet.co.kr/news/news_view.asp?artice_id=20180214161813

[4] inews24, "평창올림픽 사이버 공격 시작",http://news.inews24.com/php/news_view.php?g_menu=020200&g_serial=1066807

[5] OllyDBG, http://www.ollydbg.de/

[6] IDA, https://www.hex-rays.com/products/ida/index.shtml

[7] 수산INT 기술 연구소(CERT), 월간 악성코드 분석 보고서 (2018-02) UBoat Rat 분석 보고서, 2018, 5p

[8] MD5Check Utility, http://www.angusj.com/delphi/md5check.html

[9] Pyeongchang2018, “평창올림픽 디스트로이어”, https://www.pyeongchang2018.com/ko/news, (2018.05.25.)

[10] ZDNet Korea, “파괴 형 악성코드”, http://www.zdnet.co.kr/news/news_view.asp?artice_id=20180214161813, (2018.05.25.)

[11] 보안뉴스, “파괴형 멀웨어”, http://www .boannews.com/media/view.asp?idx=66776&kind=1&search=title&find=%C6%C4%B1%AB%C7%FC, (2018.05.25.)

[12] SOOSAN INT 월간 악성코드 분석 보고서 (2018-03), “평창올림픽 파괴 악성코드 분

석", http://www.soosanint.com/wordpre ss/wp-content/uploads/2018/03/eWalker-MonthlyReport_3_ko.pdf, (2018.05.25.)

[13] 한국일보, "도쿄올림픽 체조, AI 심판이 100% 채점한다", http://hankookilbo.com/v/4dbdcc0d9231496da664375b7ca2f573, (2017.12.18.)

[14] 조선뉴스, "테니스에 로봇 심판… 인간 심판 10명 중 9명 짐싸다", http://news.chosun.com/site/data/html_dir/2017/09/20/2017092000135.html?Dep0=twitter&d=2017092000135, (2017.09.20.)

[15] 로봇신문, "일본 츠쿠바대, 도핑 검사용 바이오 실험 로봇 개발", http://www.irobotnews.com/news/articleView.html?idxno=14038, (2018.05.25.)

안드로이드 모바일 게임 어플리케이션 보호 솔루션에 대한 분석 및 공격 기법 연구

조동민, 최형기*

성균관대학교

Study on Mechanism and Attack Technique of Android Mobile Game Application Packer

Dongmin Jo, Hyoung-Kee Choi

Sungkyunkwan University.

요 약

안드로이드 어플리케이션이 역공학되는 것을 방지하고자 많은 어플리케이션 보호 솔루션들이 등장하고 있다. 그러나 모바일 게임 어플리케이션은 기존 솔루션들에 의해 보호될 수 없어 역공학의 위험에 쉽게 노출되어 있다. 이로 인해 모바일 게임만을 보호하는 게임 보호 솔루션들이 등장하고 있지만, 이들에 대한 연구는 일반 어플리케이션 보호 솔루션에 비해 매우 부족하다. 이에 본 논문은 모바일 게임 어플리케이션 보호 솔루션을 분석하여 일반 보호 솔루션과의 차이를 밝히고, 솔루션에 공격을 시도하여 보호 기법의 효과성 및 공격에 대한 대응 방안을 보인다.

I. 서론

안드로이드 어플리케이션 시장이 폭발적으로 증대되면서 어플리케이션 역공학의 위험성이 대두되고 있다. 이에 대한 근거로 2016년 OWASP에서는 모바일 보안 위협 중 어플리케이션이 쉽게 분석되어 발생할 수 있는 위험성에 대해 발표하였다[1]. 이러한 위험성으로 인해 어플리케이션이 쉽게 분석되는 것을 최대한 방지하고자 다양한 어플리케이션 보호 솔루션들이 등장하고 있다.

한편, 안드로이드 모바일 게임 시장이 폭발적으로 성장하고 있다. 현재 모바일 게임이 전 세계 어플리케이션 총 소비자 지출의 80% 이상을 차지하고 있고, 모바일 게임 시장 규모는 지속적인 상승세를 보이고 있다[3]. 그런데 게임 어플리케이션 시장에서의 보안 허점은 기존의 안드로이드 어플리케이션 보호 솔루션들이 게임 어플리케이션은 보호하지 못한다는 점이다. 기존 솔루션들이 모바일 게임을 이루는 Unity 엔진의 DLL(Dynamic Link Library) 파일을 고려하지 않아 게임 어플리케이션은 기존 솔루션들에 의해서는 보호 받기 어렵다[12]. 그런데 모바일 게임에 대한 위변조율이 95%에 육박하고 있어 게임 개발사들이 겪는 피해가 적지 않다[4].공격자들은 게임 어플리케이션을 무단 수정 후 재배포하여 게임 개발사의 이익을 침해하거나 사용자의 기기에 신뢰할 수 없는 게임 어플리케이션 설치를 유도하는 안드로이드 게임 블랙 마켓을 구성하고 있다.

이렇듯 게임 어플리케이션을 보호하고자하는 요구가 증가하면서 안드로이드 게임 어플리케이션만을 보호하는 솔루션들이 등장하고 있다. 게임 어플리케이션만을 보호하는 업체들이 새로 등장하거나 기존에 존재하는 어플리케이션 보호 전문 업체들이 게임 어플리케이션에 대한 솔루션을 추가적으로 제공하는 형식이다

* 교신저자(Corresponding author)

[5][6][14].

그러나 일반 어플리케이션 보호 솔루션에 대한 연구는 다양하여 보호 기법들의 효과성 및 공격 방법 등에 대한 연구가 존재하지만, 안드로이드 게임 어플리케이션 보호 솔루션에 대해서는 전혀 연구된 바가 없다[2][7][8]. 따라서 본 논문에서는 특정한 게임 어플리케이션 보호 솔루션에 대해 분석하여 기존 일반 어플리케이션 보호 솔루션과의 차이점에 대해 설명하고, 게임 어플리케이션만이 이용하고 있는 보호 기법과 이에 대한 공격 기법, 결과를 보인 후 대응 방안을 제시한다.

II. 배경지식

2.1 안드로이드 어플리케이션 보호 기법

안드로이드 어플리케이션을 보호하기 위해 보호 솔루션들이 취하는 기법은 크게 동적 실행 코드 수정, 동적 실행 코드 로딩, 안티 디버깅, 난독화, 안티 리패키징으로 구분할 수 있으며 이 기법들은 게임 보호 솔루션에도 동일하게 적용된다. 난독화 기법은 생략하였다.

2.1.1 동적 실행 코드 수정(Dynamic Code Modification)

실행 압축이라고도 하며 어플리케이션의 특정 실행 코드 부분을 암호화 한 후, 어플리케이션을 실행되면 어플리케이션 스스로 해당 부분을 복호화 방식이다. 실행 부분이 암호화가 되어 있어 역공학자의 정적분석을 어렵게 한다. 그러나 암호화가 되어있더라도, 암호화된 부분이 실행되기 이전에는 반드시 해당 부분을 복호화하는 기능이 먼저 수행되므로 동적 분석에는 취약한 것이 특징이다. 보호 솔루션에서 주로 dex 파일의 실행 부분을 보호하기 위해 이용되며, 추가로 삽입되는 네이티브 라이브러리에도 적용될 수 있다[2].

2.1.2 동적 실행 코드 로딩 (Dynamic Code Loading)

안드로이드는 메인 엔트리 파일인 classes.dex가 아닌 다른 경로에 있는 dex 파일을 실행할 수 있는 동적 실행 코드 로딩이라는 기법을 지원한다. DexClassLoader 등의 클래스에 dex 파일의 경로를 인자로 하여 동적 실행 코드 로딩을 사용할 수 있다. dex 파일을 네트워크에서 다운로드하여 로드하는 경우도 적지 않으며, 어플리케이션 자체 코드 업데이트, 제3자 SDK 이용, APK 파일 경량화, 어플리케이션 보호 기법 등에 이용된다[9]. 보호 기법으로 이용될 경우에는 주로 메인 로직이 담긴 main.dex 파일을 암호화하여 다른 경로에 두고, classes.dex 파일이 main.dex 파일을 복호화하고 로드하도록 하여 역공학을 어렵게 한다.

2.1.3 안티 디버깅 (Anti-debugging)

어플리케이션이 동적으로 분석되는 것을 막는 기법이다. 안드로이드는 Linux 운영체제를 기반으로 하여, 일반적으로 디버깅은 ptrace 시스템 콜을 이용한다. 따라서 안티 디버깅 기법으로는 어플리케이션 프로세스가 자기 자신을 ptrace 하여 타프로세스의 ptrace 접근을 막는 방법, 주기적으로 /proc/self/status를 확인하여 tracerpid를 확인하는 방법, 일정 간격마다 경과된 시간을 측정하여 디버깅 되었을 경우를 감지하는 방법 등이 있다.

2.1.4 안티 리패키징 (Repackage-proofing)

공격자는 사용자에게 악성 어플리케이션을 쉽게 배포하기 위해 유명한 어플리케이션에 페이로드를 삽입하여 배포하려는 경우가 많다. 이 경우 유명한 어플리케이션들은 자신이 리패키징되어 피해자의 기기에서 실행되는 것을 막고자하여 적용하는 기법이 안티 리패키징이다. 어플리케이션 내부에 원본 코드의 해시 값을 저장해놓고 어플리케이션 실행시 어플리케이션은 자신의 파일을 해시하여 저장해놓은 해시 값과 비교한다. 비교하여 일치하지 않을 경우 리패키징 되었다고 판단한다. 리패키징이 되었다고 판단할 경우 어플리케이션을 바로 종료하거나, 혹은 역공학을 어렵게 하기 위해 이상행위를 일으켜 어플리케이션 이용을 어렵게 할 수 있다[10].

2.2 기존 솔루션의 어플리케이션 보호 범위

2.2.1 apk 파일 구성

apk 파일의 기능을 담당하는 핵심 파일 및 폴더에는 classes.dex 파일과 AndroidManifest.xml 파일, /lib, /assets, /res 등의 폴더들이 있다. AndroidManifest.xml 파일은 어플리케이션의 각종 컴포넌트 정보 및 권한 정보 등 다양한 어플리케이션 메타 데이터들을 포함하고 있다. /lib 폴더에는 어플리케이션에서 네이티브 함수를 이용할 경우 필요한 네이티브 라이브러리(shared object)를 담고 있고 /res 폴더에는 어플리케이션의 Activity 컴포넌트를 구성하는 화면 구성 오브젝트들이 저장되어 있다. /assets 폴더는 이외의 경우에 개발자가 필요하여 직접 포함한 파일들이 담겨 있다.

2.2.2 기존 솔루션의 보호 범위

기존 보호 솔루션들은 소스 코드가 담긴 classes.dex를 최우선적으로 보호한다. 또한 /res 폴더의 파일들을 보호하여 사용자가 조작된 화면을 통해 피해를 받을 수 있는 확률을 줄인다. /lib 폴더의 네이티브 라이브러리를 보호하는 솔루션은 존재하지만 상대적으로 그 수가 적다[8]. /aseets 폴더에 대해서는 어플리케이션 마다 해당 폴더 안의 파일을 사용하는 방법이 다르므로 솔루션들이 이 폴더안의 파일을 사용하는 코드 부분을 찾아 복호화하는 로직을 삽입하기 어렵다. 따라서 기존 솔루션들은 일반적으로 /assets 폴더의 내부는 보호하지 않는다.

2.3 Unity 게임 어플리케이션

2.3.1 Unity 기반 모바일 게임 시장

Unity 게임 어플리케이션이 모바일 게임 시장을 차지하는 비율은 상당하다. Unity 사가 제시하는 자료에 따르면 상위 무료 모바일 게임 1000개 중 34%가 Unity 엔진으로 개발한 작품이다[11]. 그러나 해당 자료에서 1위를 차지하는 게임 엔진은 게임 개발사의 비공개 엔진이므로, Unity는 상용 모바일 게임 엔진으로서는 1위로 확인된다. 이렇듯 많은 비율의 모바일 게임이 Unity로 작성되는 것을 알 수 있고. 보호 솔루션이 모바일 게임을 보호하려면 Unity로 제작된 어플리케이션을 보호할 수 있어야 한다.

2.3.2 Unity 어플리케이션 실행 메커니즘

Unity는 모든 플랫폼에 동일하게 Microsoft가 발표한 언어인 C#을 통해서 프로그램이 작성된다. 안드로이드 어플리케이션의 경우 Linux의 C# 가상 머신인 Mono Runtime에 의해 실행된다[13]. 안드로이드에서 Unity 어플리케이션을 실행할 경우 DVM(Dalvik Virtual Machine) 혹은 ART(Android Runtime) 환경으로 dex 파일을 실행하면 dex 파일에서 어플리케이션 내부에 포함된 Mono Runtime을 로드하고, Mono Runtime이 게임 어플리케이션을 실행한다.

Unity에서 안드로이드 어플리케이션을 빌드할 경우 /lib 폴더 안에 세 가지의 네이티브 라이브러리를 포함하는데 Mono Runtime인 libmono.so 파일, Unity engine인 libunity.so 파일 그리고 Unity engine을 초기화하는 libmain.so 파일이다. 또한 게임 주요 로직인 C# 소스 코드를 /assets 폴더 안의 DLL 파일의 형태로 담는다. 해당 DLL 파일들은 C#의 중간 언어 형태인 CIL(C# Intermediage Language)로 구성되어 있다.

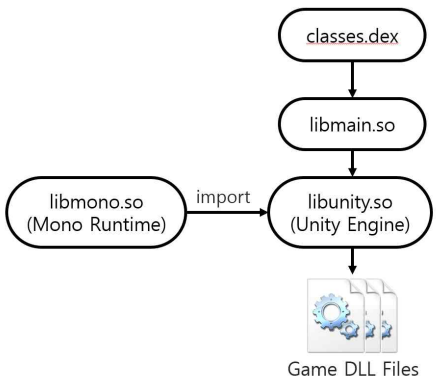


그림 1. Unity Runtime의 실행 구조

Unity 어플리케이션의 실행 구조는 위 [그림 1]에 표현되어 있다. Java 소스가 담겨있는 classes.dex에서 libmain.so 를 로드하고, libmain.so의 JNI_OnLoad 함수에서는 libunity.so 파일의 JNI_OnLoad 함수를 호출한다. libunity.so 에서는 DLL 파일을 로드하기 위해 필요한 Mono Runtime 함수들을 libmono.so 에서 import 한 후, DLL 파일을 실행하여 게임을 구동한다.

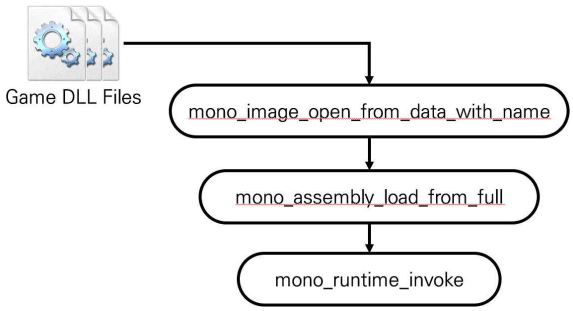


그림 2. Mono Runtime의 실행 구조

libunity.so 파일이 DLL 파일을 읽어 DLL 파일 안의 클래스 및 메소드를 호출하는 구조는 위 [그림 2]와 같다. 우선 mono_image_open_from_data_with_name 함수를 호출한다. 해당 함수 내에서는 DLL 파일의 내용을 파싱하여 MonoImage 구조체에 담는다. 이후 mono_assembly_load_from_full 함수를 호출하여 MonoImage 구조체로부터 각 클래스 및 메소드가 호출되는 컨텍스트를 구분하여 여러 MonoAssembly 구조체로 초기화하여 저장한다. 이 후 mono_class*, mono_method*등의 함수들을 호출하여 DLL 파일내의 클래스 및 메소드를 메모리에 초기화한다. 마지막으로 초기화한 오브젝트를 호출하는 함수인 mono_runtime_invoke를 호출하여 DLL 파일 안의 메소드나 클래스를 기기의 CPU 구조에 맞게 컴파일하여 호출하게 된다.

III. 본론

3.1 기존 보호 솔루션과의 보호 범위 차이

	DLL 파일 보호 여부
Baidu	게임 보호 솔루션 제공
Ali	보호하지 않음
Bangcle	보호하지 않음
ijiami	보호하지 않음
Qihoo	보호하지 않음
apkprotect	보호하지 않음
Tencent	보호하지 않음

표 2. 기존 솔루션들의 DLL 파일 보호 여부

기존 연구의 자료로 쓰였던 보호 솔루션들의 DLL 파일 보호 여부를 조사하였다[8]. 분석 결과 위 표와 같이 Baidu의 솔루션을 제외하고 /assets 폴더를 전혀 보호하지 않고 있는 것을 확인하였다. 따라서 게임 어플리케이션이 기존의 보호 솔루션을 채용하였을 경우 /assets 폴더 안의 DLL 파일이 전혀 보호되지 않으므로 위험에 노출되기 쉽다. 게임의 로직이 그대로 공격자에게 노출되며 공격자는 보호 솔루션이 안티 리패키징으로 보호되고 있음에도 불구하고 해당 DLL 파일만을 추출하여 원하는 로직을 수정 후 같은 Unity 어플리케이션을 만들어 낼 수 있다.

3.2 게임 어플리케이션 보호 기법

협업하고 있는 특정 게임 보호 솔루션사의 솔루션이 적용된 게임을 분석하였다. 기존 보호 솔루션들이 적용하는 기법은 게임 보호 솔루션들도 적용하고 있으나 여기서는 기존 보호 솔루션은 적용하지 않고 게임 보호 솔루션만 적용하는 보호 기법을 다룬다.

3.2.1 DLL 파일 암호화

게임 보호 솔루션은 기본적으로 /assets 폴더 안의 DLL 파일을 암호화한다. 일반적으로 DLL 파일은 PE(Portable Executable) 형식을 가지므로, 만약 DLL 바이너리가 이러한 PE 형식을 가지지 않을 경우 암호화되지 않은 것으로 판단할 수 있다. 이로 인해 단순한 정적 분석으로는 DLL 파일의 원본을 탈취하기 어렵다. Mono Runtime 역시 PE 형식을 검증하고, 암호화되어 있을 경우 DLL 파일을 실행할 수 없다. 따라서 게임 어플리케이션이 실행되면서 복호화 과정이 수행되어야 Mono Runtime이 DLL 파일을 실행할 수 있게 된다.

3.2.2 DLL 동적 실행 코드 수정

DLL 파일 안의 C# 클래스 및 메소드 안에서 동적 실행 코드 수정 기법이 도입되어 있는 것을 확인하였다. 이는 DLL 파일이 PE 형식을 갖도록 복호화 한 이후에 확인한 결과이며 이 과정은 공격 기법에서 설명한다. Java와 동일하게 C# 클래스 및 메소드들이 암호화되어 있고, 암호화되지 않은 특정 클래스 생성자가 실행될 경우 해당 정보들을 복호화한다. 따라서 게임 어플리케이션을 실행해야만, 복호화 생성자들이 수행되면서 게임의 로직이 복호화되고 실행된

다.

3.2.3 Custom Mono Runtime

Mono Runtime은 오픈 소스 기반 프로젝트이므로, 일반 사용자가 내용을 고쳐 컴파일할 수 있다. 그런데 보호 솔루션이 적용된 게임 어플리케이션의 libmono.so 파일은 보호 솔루션이 적용되지 않은 파일과 다르다는 점을 확인하였다. DLL 파일이 암호화되어 있기에 이를 복호화하는 과정이 필요하여 DLL 파일을 로드하는 과정 직전에 복호화 루틴이 삽입된 것을 확인하였다.

3.2.4 so(Shared Object) 파일 보호

게임 보호 솔루션에서 네이티브 라이브러리를 보호하고 있는 것을 확인하였다. 핵심적인 3개의 so 파일을 보호하고 있으며 기법으로는 동적 실행 코드 수정 기법을 이용하고 있다.

3.3 공격 기법 제안 및 시도 결과

공격의 목표는 DLL을 완전 복호화한 후 게임 로직을 변경하여 새로운 게임 어플리케이션으로 리패키징하는 것이다.

3.3.1 분석 환경

환경은 윈도우용 안드로이드 상용 에뮬레이터를 사용하였으며 공격 기법은 hooking을 이용하였다. hooking 기법으로는 어플리케이션 실행시 환경 변수에 LD_PRELOAD를 삽입하여 특정 함수를 hooking 할 수 있도록 하였다.

3.3.2 DLL 원본 추출

Mono Runtime에서 DLL 파일의 내용을 처음으로 파싱하는 부분은 mono_image_open_from_data_with_name 함수이므로 해당 함수 부분을 분석하였다. 해당 함수는 동적 실행 코드 수정이 적용되어 있어 어플리케이션을 실행 후 메모리에서 추출하여 함수의 원본을 얻을 수 있었다. 함수 안에서 mono_image_init 함수 직전에 DLL 파일을 복호화하는 부분을 발견하였다. 이를 공격하여 DLL 원본을 추출하기 위해 mono_image_init 함수를 후킹한 후 DLL 파일의 내용이 담긴 인자를 찾아 파일로 추출하였다. 추출한 파일은 PE 형식을 갖추고 있고, C# 디컴파일러를 이용해 성공적으로 복호화가 수행된 것을 확인할 수 있었다. 그러나 동적 실행 코드 수정 기법이 적용되어 있어 완전 복호화된 C# DLL 파일이라고는 할 수 없다.

3.3.3 DLL 동적 실행 코드 수정 대응

DLL 내부에 적용된 동적 실행 코드 수정 기법들을 파훼하기 위해 mono_runtime_invoke 함수를 hooking하였다. mono_runtime_invoke 함수는 C# 메소드를 최종적으로 호출할 경우 불리는 함수이다. 그런데 동적으로 실행 압축된 메소드나 클래스가 실행되는 순간에는 압축이 풀려야 한다. 따라서 mono_runtime_invoke 함수를 hooking하여 암호화된 메소드가 실행되는 순간 메소드의 내용을 추출한다. DLL 파일에 추출한 메소드와 대응하는 메소드를 지우고 추출한 메소드로 대체하여 완전 복호화된 DLL 파일을 얻을 수 있었다.

3.3.3 리패키징

완전한 DLL 파일에서 점수를 표시하는 부분을 항상 1이라는 숫자를 표시하도록 수정하였다. 그 후 메모리에서 세 개의 so 파일과 dex 파일의 원본을 추출하고 수정한 DLL 파일을 포함하여 새로운 APK 파일을 구성하였다. 새로운 APK 파일을 기기 및 에뮬레이터에서 실행하자 점수를 표시하는 부분이 수정된 로직으로 동작하는 것을 확인할 수 있었다.

3.3 대응 방안

본 단락에서는 위와 같은 공격을 막기 위해 필요한 기법들을 소개한다.

3.3.1 C# 난독화

Java의 클래스와 메소드를 알기 어려운 이름들로 대치하는 것과 동일하게 C#의 클래스와 메소드 이름들도 의미없는 문자열로 대치해야 한다. 다만 더미 메소드나 클래스를 삽입하는 것은 지양하여 성능 저하를 막아야 한다는 점은 Java 난독화와 다를 수 있다. 의미없는 클래스와 메소드 이름으로 인해 공격자는 수정하고

자 하는 특정 게임 로직을 찾는 시간이 지연될 것이다.

3.3.2 Unity의 il2cpp 빌드 옵션

2015년 Unity에서 iOS 64bit에 Mono Runtime 대신 처음 적용한 빌드 방법으로 가상 머신에 의지하지 않으며 C# 코드가 DLL 파일이 아닌 so 파일로 컴파일된다.. Mono Runtime과 같이 C#을 굳이 실행시마다 컴파일할 필요가 없어 성능이 향상되고, 게임 로직이 이미 컴파일되어 있기에 C#과 같은 소스 코드를 볼 수 없어 보안적으로 안전하다. 그러나 안드로이드의 여러 아키텍처에 대해 컴파일 해야할 경우 어플리케이션의 용량이 크게 증가하고, .NET이 제공하는 C#의 다양한 기본 함수들을 지원하지 못하는 호환성 문제가 있다. 따라서 il2cpp를 적용하여 빌드할 경우 위와 같은 방식의 공격 기법은 효력을 발휘할 수 없다.

IV. 결론

본 논문에서는 기존의 안드로이드 어플리케이션 보호 솔루션들이 DLL 파일을 고려하지 못하여 게임 어플리케이션을 보호하지 못하고 있다는 점을 밝혔다. 그리고 게임 어플리케이션 전용 보호 솔루션만이 적용하는 보호 기법들을 분석하고 이들을 우회하는 공격 기법들을 제시하고 공격에 성공한 결과를 보였다. 그리고 마지막으로 성공한 공격 기법에 대응할 수 있는 방어 기법들을 제시하였다.

Acknowledgement

이 논문은 2016년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2016R1D1A1B03936211).

[참고문헌]

[1] OWASP 2016 Mobile Top 10 Security Risks,https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

[2] Zhang, Yueqian, Xiapu Luo, and Haoyang Yin. "Dexhunter: toward extracting hidden code from packed android applications." European Symposium on Research in Computer Security. Springer, Cham, 2015.

[3] App Annie 2016 Special IDC Report, https://www.appannie.com/kr/insights/mobile-gaming/gamings-mobile-growth-special-idc-report/.

[4] C. Davies, http://www.slashgear.com/95-android-game-piracyexperience-highlights-app-theft-challenge-15282064/.

[5] Baidu, http://app.baidu.com/.

[6] AppSealing, https://www.appsealing.com/.

[7] Yang, Wenbo, et al. "Appspear: Bytecode decrypting and dex reassembling for packed android malware." International Workshop on Recent Advances in Intrusion Detection. Springer, Cham, 2015.

[8] Duan, Yue, et al. "Things You May Not Know About Android (Un) Packers: A Systematic Study based on Whole-System Emulation."

[9] Qu, Zhengyang, et al. "DYDROID: Measuring Dynamic Code Loading and Its Security Implications in Android Applications." Dependable Systems and Networks (DSN), 2017 47th Annual IEEE/IFIP International Conference on. IEEE, 2017.

[10] Luo, Lannan, et al. "Repackage-proofing Android apps." Dependable Systems and Networks (DSN), 2016 46th Annual IEEE/IFIP International Conference on. IEEE, 2016.

[11] Unity Fast Fact, https://unity3d.com/kr/public-relations.

[12] Unity3d, http://unity3d.com/.

[13] Mono Runtime, https://www.mono-project.com/.

[14] NSHC, http://www.nshc.net/.

[15] Unity il2cpp, https://docs.unity3d.com/Manual/IL2CPP.html.

임베디드 디바이스의 펌웨어 리버스 엔지니어링 방법 연구*

박재현, 김승주

고려대학교 정보보호대학원

Research of Firmware Reverse Engineering Method for Embedded Device

Jaehyeon Park, Seungjoo Kim

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

요 약

임베디드 디바이스가 산업, 군사 등 다양한 영역에서 활용되고 보급량이 증가될 것으로 전망된다. 임베디드 디바이스의 보안성 검증, 관련 법률 자문 등 다양한 분야에서 리버스 엔지니어링이 활용되는데, 민간 차원의 불법 복제 및 지적 재산권 침해 등의 문제만이 아니라 무기기술의 국외유출과 같은 국가 안보에 직결되는 문제가 발생할 수 있다. 그렇기에 임베디드 디바이스에 대한 연구가 필요하며, 그 중 디바이스의 전반적인 기능을 제어하는 펌웨어에 대한 리버스 엔지니어링 기술 연구가 필요하다. 그러나 기존 연구는 각 연구의 대상 디바이스에 한정되어 있어 전체적인 펌웨어 리버스 엔지니어링 기술에 대한 이해에 어려움이 있다. 그래서 본 논문은 기존 연구 사항들을 분석하여 개괄적인 펌웨어 리버스 엔지니어링의 작업 프로세스를 파악하고 세부 프로세스에서 실시사항과 사용 도구에 대하여 분석하였다.

I. 서론

임베디드 디바이스는 특정 기능을 제어하기 위해서 마이크로프로세서 기반의 시스템인 임베디드 시스템을 포함하고 있는 기기를 의미한다[1]. 리버스 엔지니어링의 정의는 대상 시스템의 구성요소와 각 요소 간의 상호작용을 분석하고 이를 다른 형태로 표현하는 과정이다[2]. 상기 정의를 통해 임베디드 디바이스 리버스 엔지니어링을 정리하면 임베디드 시스템과 디바이스의 하드웨어 요소를 파악하고 시스템과 요소 간의 상호작용을 분석하여 다른 형태로 표현하는 과정이라고 할 수 있다.

리버스 엔지니어링을 실시하는 목적은 크게 'honest'한 목적과 'dishonest'한 목적으로 분류할 수 있다. honest한 목적은 검증, 취약점 분석, 시장 조사, 지적 재산권 침해 여부 확인 그리고 기술 연구 등이 포함된다. 반면, dishonest한 목적은 취약점 공격, 불법 복제, 지적 재산권 침해, 공격 기법 개발 등 타인의 자산에 피해를 입히는 목적이다[3].

honest한 목적의 예로 국내 기업 중 SNTWORKS가 있다. 해당 기업은 임베디드 디바이스의 보안성을 분석하기 위해 리버스 엔지니어링을 실시한다. 그리고 대상 디바이스 펌웨어의 코드를 재구성하고 분석하여 지적 재산권 침해 여부를 확인하는 서비스도 제공한다[4].

한편, dishonest한 목적의 사례로 이란의 경우가 있다. 이란은 2011년 미국의 스텔스 무인항공기를 획득하여 리버스 엔지니어링을 실시하였다. 이란은 리버스 엔지니어링을 통해 미국 무인항공기 하드웨어와 펌웨어의

* 본 연구는 고려대 암호기술 특화연구센터(UD170109ED)를 통한 방위사업청과 국방과학연구소의 연구비 지원으로 수행되었습니다.

설계이론을 습득하였고, 이를 통해 자국의 무인항공기 기술을 향상시켰다[5][6][7].

상기 이란의 사례와 같이 리버스 엔지니어링은 단순히 자산 피해 문제만이 아니라 국가 안보와 직결된 문제와 연관될 수 있다. 한국인터넷진흥원에서 발표한 자료에 따르면 2020년까지 약 409억 개의 사물인터넷 기기가 보급되며 산업 현장, 군사 영역 등에 다양한 분야에서 활용될 것으로 전망하고 있다[8]. 민간 자산의 보호뿐만 아니라 국가 기반 시설이나 군사 영역에서 활용되는 임베디드 디바이스에 대한 보호를 위하여 리버스 엔지니어링을 실시하는 기술과 방지하는 기술에 대한 연구가 필요하다.

본 논문은 임베디드 디바이스의 전반적인 기능을 통제하는 펌웨어에 대한 리버스 엔지니어링에 대하여 연구하고자 한다. 펌웨어 리버스 엔지니어링의 개괄적인 작업 프로세스를 파악하고 세부 프로세스의 실시사항과 사용 도구에 대해 분석하였다.

II. 관련 연구

펌웨어 리버스 엔지니어링에 대한 연구는 펌웨어를 획득하는 과정과 분석하는 과정을 중심으로 실시된다.

2.1. 펌웨어 획득

펌웨어 획득 방법은 장비 외적 방법과 장비 내적 방법으로 분류된다. 장비 외적 방법은 하드웨어 디버깅 포트를 이용하거나 플래시 메모리에 직접 접근하여 획득하고, 장비 내적 방법은 펌웨어 업데이트 기능을 이용하여 획득한다.

하드웨어 디버깅 포트를 이용한 연구로 2006년 M.F. Breeuwsma는 JTAG을 이용하여 펌웨어를 획득하는 논문을 발표하였다. 데이터시트와 같은 사전 정보가 없을 때, JTAG TAP(Test Access Port)를 식별 및 연결하고 JTAG 명령어를 통해 펌웨어를 획득하는 과정을 서술하였다[9].

2013년 NDSS(Network and Distributed System Security Symposium) 2013에서 Ang Cui 등 3명은 HP사의 프린터에 대한 펌웨어 변조 공격에 대한 논문을 발표하였다. 펌웨어가 포함된 플래시 메모리에 직접 접근하여 이미지를 획득하고 펌웨어의 기능을 분석하는 과정을 제시하였다[10]. 그리고 Black Hat USA 2011에서 Charlie Miller는 Macbook의 배터리를 관리하는 smart battery controller에 직접 연결하여 해당 펌웨어를 획득하고 디스어셈블러를 이용하여 펌웨어를 분석하는 과정을 발표하였다[11].

펌웨어 업데이트 기능을 이용하여 펌웨어를 획득하는 연구도 진행 중이다. Jacob Maskiewicz 등 4명은 마우스의 펌웨어 업데이트 기능을 이용하여 펌웨어를 획득 및 변조하는 논문을 발표하였다. 펌웨어 업데이트 시 전송되는 패킷을 스니핑하여 펌웨어 구조와 정보를 식별하고 변조하는 공격 과정을 제시하였다[12]. 그리고 DFRWS(Digital Forensics Research WorkShop) 2015 USA에서 Seung Jei Yang 등 4명은 스마트폰의 펌웨어 업데이트 기능의 업데이트 명령어을 이용하여 펌웨어를 획득하는 방법을 발표하였다[13].

2.2. 펌웨어 분석

2013년 Critical Infrastructure Protection 저널에서 미국 공군 기술연구소의 Zachry Basnight 등 4명은 산업 현장 시스템의 작동을 제어 및 감독하는 Programmable Logic Controller(PLC)를 대상으로 펌웨어 분석 프로세스를 제시하였다[14]. 펌웨어의 분석 과정을 펌웨어 획득, 펌웨어 이진 이미지를 분석, 이진 이미지를 디스어셈블리, 펌웨어 인증 과정 분석의 4가지 단계로 분할하고 세부 과정을 제시하였다. 2016년 Digital Investaigation 저널에서 Ruijin Zhu 등 4명은 ARM 프로세서의 펌웨어 분석에 관한 방법론을 서술하였다. FIND-LP와 DBMLP라는 알고리즘을 제시하고 이를 통해 펌웨어의 포맷을 파악하는 과정을 제시하였다[15].

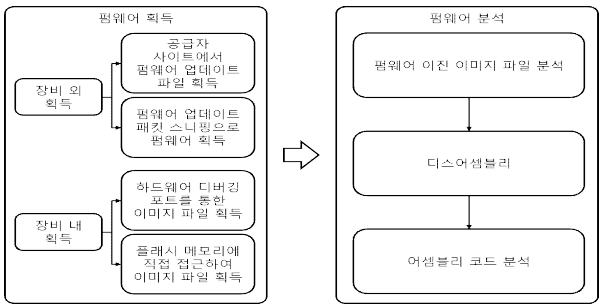
기존의 펌웨어 리버스 엔지니어링에 대한 연구는 연구 대상 디바이스의 종류에 한정되어 있으며, 그리고 전반적인 프로세스가 아닌 연구에서 실시한 일부 프로세스에 대해서만 논하고 있다. 그래서 본 논문은 개괄적인 펌웨어 리버스 엔지니어링 작업 프로세스와 그 세부사항에 대하여 분석하였다.

III. 펌웨어 리버스 엔지니어링 프로세스

펌웨어 리버스 엔지니어링 과정은 2단계로 진행된다. 첫째, 펌웨어를 획득하는 단계와 둘째, 획득한 펌웨어를 분석하는 단계이다. 각 단계의 세부 진행과정의 개괄적인 도식은 [그림 1]과 같다.

펌웨어를 획득하는 단계는 장비 외적으로 획득하는 방법과 장비 내적으로 획득하는 방법 두 가지로 나뉜다. 장비 외적으로 획득하는 방법은 대상 장비의 펌웨어 업데이트를 공급자 사이트에서 다운로드받거나, 원격 펌웨어 업데이트 시 패킷 스니핑으로 획득하는 방법이다. 장비 내적으로 획득하는 방법은 하드웨어 디버깅 포트를 이용하여 펌웨어를 획득하거나, 펌웨어가 포함되어 있는 플래시 메모리 등에 직접 접근하여 펌웨어 이미지를 추출하는 방법으로 분류된다.

펌웨어를 분석하는 방법은 먼저 기존의 이진 이미지 파일을 분석하여 펌웨어의 구조 및 구성요소를 파악하고, 디스어셈블러를 이용하여 어셈블리 코드를 도출한다. 도출된 어셈블리 코드를 분석하여 해당 펌웨어의 기능 및 취약점을 분석한다.



[그림 1]. 펌웨어 리버스 엔지니어링 프로세스

IV. 프로세스 상세 및 사용 도구

4장에서는 3장에서 제시한 분석 프로세스 별 세부 작업사항에 대해 서술하고 각 과정에서 사용가능한 도구들에 대해 서술한다. 세부 단계별 운용하는 도구는 [표 1]에 정리하였다.

2.3. 펌웨어 획득

펌웨어를 획득하는 방법은 장비 외적 요소로부터 획득하거나 장비 내부의 자체 요소에서 획득하는 2가지로 분류된다. 펌웨어 획득을 위해 필요한 작업량은 장비 외적으로 획득하는 방식이 내적으로 획득하는 방식보다 작업 소요가 적고 실패율이 적다. 하지만 펌웨어 관련 이슈들이 등장함에 따라 펌웨어 업데이트 파일을 사용자에게 제공하지 않는 경우가 증가하고 있는 추세로 장비 내적으로 획득하는 방법의 수요는 증가하고 있다.

2.3.1. 장비 외 획득

장비 외적으로 펌웨어를 획득하는 가장 간단한 방법은 제품 공급자 사이트에서 해당 펌웨어를 획득하는 방법이다. 펌웨어 업데이트 파일을 제공하는 공급자에게서 손쉽게 펌웨어를 획득하는 것이 가능하지만, 최근 펌웨어 업데이트 파일을 사용자에게 제공하지 않는 경우가 증가하고 있다.

다른 방법으로는 원격으로 펌웨어 업데이트를 지원하는 장비가 펌웨어 업데이트를 실시하는 동안 와이어샤크(Wireshark)와 같은 패킷 분석 프로그램을 이용하여 펌웨어의 정보를 습득하는 방법이 있다. 공급자가 펌웨어를 추가적으로 제공하지 않아도 펌웨어를 획득할 수 있으나, 대상 장비가 자동으로 펌웨어 업데이트 기능을 지원하지 않거나, 네트워크상에서 암호화 혹은 난독화가 되어 있을 경우에 해당 펌웨어 정보를 분석하는 것이 제한된다.

2.3.2. 장비 내 획득

장비 외적으로 펌웨어 획득이 제한되는 경우, 장비 내부에 설치되어 있는 펌웨어가 포함되어 있는 메모리에 접근하여 덤핑하는 것으로 펌웨어 정보를 획득한다. 해당 방법의 경우, 장비 내부의 보드 특성에 따라 다양한 방법이 있지만 대표적으로 하드웨어 디버깅 포트를 통한 덤핑과 플래시메모리에 직접 접근하여 덤핑하는 방법이 있다.

2.3.2.1. 하드웨어 디버깅 포트

하드웨어 디버깅을 위한 수단은 대표적으로 UART와 JTAG 두 가지 방식이 있다. UART는 Universal Asynchrounous Receiver /

Transmitter의 준말로 직렬 데이터를 전송하는 방식으로 하드웨어에 직접 연결하여 디버깅을 실시하는데 사용되는 통신방식 중 하나이다. UART 포트를 식별하고 연결을 위하여 핀 기능을 확인하는 과정에서 전압을 측정하는 존재한다. 물리적으로 UART 및 JTAG Port를 제거한 경우와 논리적으로 해당 통신방식의 명령어 기능을 소거한 경우로 하드웨어 디버깅 포트를 이용하여 펌웨어를 획득하는 것은 제한된다. 그래서 펌웨어가 저장되어 있는

분석 단계	분석 과정			필요 도구	
				하드웨어	소프트웨어
펌웨어 획득	장비 외 획득	패킷 스니핑		-	Wireshark, Tcpdump[17]
	장비 내 획득	하드웨어 디버깅 포트	UART	UART to USB Bridge, Multi-meter, Logic Analyzer	Putty, XShell
			JTAG	JTAGulator[19], Riff Box[20]	OpenOCD[21], ScanExpress[22]
		플래시 메모리 접근		De-soldering Device, MINIPRO TL866[23]	MINIPRO TL866 드라이버 및 응용 프로그램[23]
펌웨어 분석	이진 이미지 분석			-	Binwalk[24], HxD Binary file editor[25]
	디스어셈블리, 어셈블리 코드 분석			-	IDA Pro[26], OllyDbg[27], Radare2[28]

[표 1] 각 세부 과정별 사용 도구

Multi-meter와 Logic Analyzer가 필요하다. 그리고 UART포트와 분석 PC를 연결할 수 있는 PL2303과 같은 Bridge와 분석 PC에서 명령어를 확인 및 구동시킬 수 있는 Putty나 XShell과 같은 직렬 터미널 프로그램이 필요하다.

JTAG은 IEEE 1149.1에서 지정된 국제표준으로 하드웨어 회로 내부에서 특정 부분의 입력 및 출력을 위하여 데이터를 송, 수신하는 방식을 의미한다[16]. JTAG Test Access Port(TAP)를 이용하여 분석하고자 하는 PC와 연결을 실시한다. 이 과정에서 데이터시트가 제공되는 경우, JTAG TAP를 쉽게 찾고 분석하는 것이 가능하나, 없을 경우에는 회로 분석을 통하여 JTAG TAP로 의심되는 Port를 식별하고 모두 점검하는 것으로 JTAG TAP를 찾는다[9]. 연결 후 JTAG 명령어를 통하여 펌웨어를 포함하는 메모리에 접근 및 복사가 가능하다. 해당 과정에서 JTAG TAP를 연결하기 위한 Bridge로 JTAGulator나 RiffBox 등을 이용하여 연결한 후, JTAG 디버깅 툴을 사용하여 JTAG 명령어로 메모리의 이미지를 획득한다.

이 두 가지 획득 방식이 불가능한 경우가 플래시 메모리에 직접 접근하여 펌웨어를 획득하는 방법을 사용한다.

2.3.2.2. 플래시 메모리 접근

플래시 메모리에 각 핀별로 직접 연결이 가능한 경우, 플래시 메모리를 분리하지 않아도 무방하나, 불가능하다면 해당 메모리를 결합되어 있는 PCB에서 분리해야 한다. 해당 과정에서 주의할 점은 분리하는 과정에서 디솔더링을 실시할 때, 해당 Chip의 회로가 타버리지 않도록 주의해야 한다. 사고를 방지하기 위하여 디솔더링 전용 장비가 제공되고 있으며, 이를 이용하는 것으로 쉽게 디솔더링이 가능하다.

디솔더링을 통하여 대상이 되는 메모리를 분리한 후, MINIPRO TL866과 같이 칩과 분석 PC를 연결하는 용도의 어댑터 및 분석 프로그램을 통해 연결한다.

2.4. 펌웨어 분석

4.1장의 과정을 통하여 획득한 펌웨어는 아래의 4.2.1, 4.2.2, 4.2.3의 과정을 순차적으로 수행하여 분석을 실시한다. 해당 과정은 [12]의 참고 문헌을 참조하여 수립하였다.

2.4.1. 이진 이미지 분석

먼저, 획득한 펌웨어 이진 이미지부터 분석을 실시한다. 이 과정에서는 VBinDiff (Visual Binary Diff)나 Binwalk와 같은 도구를 이용하여 대상이 되는 파일의 구조를 분석한다. 이를 통하여 펌웨어 영역과 펌웨어가 저장된 포맷을 식별하는 것이 가능하다.

펌웨어 파일 구조를 더 정확하게 식별하기 위하여 버전이 다른 펌웨어 파일을 획득하고 이를 비교한다. 가장 최신 버전의 파일과 인접 버전의 파일을 비교하는 것으로 동적으로 변동되는 부분을 식별하여 펌웨어 검증 영역을 식별한다. 반면, 가장 오래된 버전과 비교하는 것으로 변동되지 않는 부분을 식별하여 펌웨어의 구조를 식별한다.

2.4.2. 디스어셈블리

펌웨어 이진 이미지를 디스어셈블하여 어셈블리 코드를 획득한다. 디스어셈블러는 대표적으로 IDA Pro, OllyDbg 등이 있으며, 해당 도구를 이용하여 어셈블리 코드를 획득하는 것뿐만 아니라 분기 지점 및 함수 영역에 대한 프로그램의 논리를 파악하는데 용이하다.

디스어셈블러는 모든 이진 이미지를 디스어셈블리 하는 것은 불가능하다. 그래서 이진 이미지 분석 과정에서 파악한 펌웨어 구조를 참고하여 어셈블리 코드로 변환되지 않은 부분을 분석가가 임의로 디스어셈블리 코드를 수정하여 디스어셈블을 실시한다.

2.4.3. 어셈블리 코드 분석

분석하고자 하는 펌웨어 이미지를 어셈블리 코드로 변환한 후에 해당 코드의 기능 및 특성을 분석한다. IDA Pro의 경우, 해당 어셈블리 코드의 함수와 같은 분기 지점을 그래픽 형태로 분석이 가능하다. 프로그램의 논리를 분석하여 해당 펌웨어의 기능을 식별한다.

해당 어셈블리 코드에서 특정 문자열을 검색하여 식별하는 것으로 검증 기능에 사용하는 변수임을 식별하거나, API를 실행하여 접근하는 주소를 식별하는 것으로 주요 변수를 확인한다.

V. 결론 및 차후연구

시장 조사, 지적 재산권 침해 확인과 같은 상업적 목적 외에 타국의 군사 장비 분석 등 다양한 분야에서 활용되는 펌웨어 리버스 엔지니어링에 대한 연구를 진행하고자 하였다. 기존의 연구는 대상 디바이스에 한정된 방법론으로 연구를 진행하여 전체적인 펌웨어 리버스 엔지니어링에 대한 이해가 어려웠다. 그래서 본 논문은 개괄적인 펌웨어 리버스 엔지니어링 프로세스를 파악하고, 프로세스 세부사항과 사용 도구에 대하여 서술하였다.

차후 연구로는 다양한 리버스 엔지니어링 기법에 대한 연구를 통해 작성한 프로세스를 개선하고자 한다. 그리고 펌웨어 리버스 엔지니어링을 방지하기 위해 적용된 암호화, 난독화 등의 기법을 우회하여 펌웨어를 획득하는 방법론을 연구하고자 한다. 그리고 본 논문의 펌웨어 리버스 엔지니어링 작업 흐름의 실효성을 확인하고자 실제 디바이스를 대상으로 사례 분석을 실시할 예정이다.

[참고문헌]

[1] Heath Steve, Embedded systems design, Newnes, ISBN, 2003.

[2] Eilam Eldad, Reversing: secrets of reverse engineering, John Wiley & Sons, 2011

[3] Shaahed E. Quadir, Junli Chen, Domenic Forte, Navid, Sina Shahbazmohamadi, Lei Wang, John Chandy, and Mark Tehranipoor, A Survey on Chip to System Reverse Engineering, ACM journal on emerging technologies in computing systems (JETC), vol.13(1):6, December, 2016.

[4] SNTWORKS, SERVICES, http://www.sntworks.kr/

[5] Arie Egozi, iHLS, Egozi: The Iranian Reverse Engineering Effort, https://i-hls.com/archives/81306, 2018

[6] National Post, Iran to 'reverse-engineer' seized U.S. stealth drone after hacking operating system, http://nationalpost.com/news/iran-to-reverse-engineer-u-s-stealth-drone, 2011

[7] 연합뉴스, 이란 "5년 전 포획한 美드론" 본떠 공격용 드론 개발, http://www.yonhapnews.co.kr/bulle-

tin/2016/10/01/0200000000AKR20161001052900111.HTML, 2016

[8] 한국인터넷진흥원, 사물인터넷 보안 위협 동향, https://www.kisa.or.kr/public/library/PR_View.jsp?mode=view&p_No=160&b_No=160&d_No=86&ST=TC&SV=, 2014

[9] M. F. Breeuwsma, Forensic imaging of embedded systems using JTAG (boundary-scan), Digital Investigation vol. 3(1), pp.32-42, March, 2006.

[10] Ang Cui, Michael Costello and Salvatore J. Stolfo, When firmware modification attack: a case study of embedded exploitation, The Network and Distributed System Security Symposium (NDSS) 2013, February, 2013.

[11] Charlie Miller, battery firmware hacking, black hat USA, July, 2011

[12] Jacob Maskiewicz, Benjamin Ellis, James Mouradian and Hovav Shacham, Mouse Trap: Exploiting Firmware Updates in USB Peripherals, WOOT, 2014.

[13] Seung Jei Yang, Jung Ho Choi, Ki Bom Kim and Taejoo Chang, New acquisition method based on firmware update protocols for Android smartphones, Digital Investigation, vol. 14, pp. 68-76, 2015.

[14] Zachry Basnight, Jonathan Butts, Juan Lopez Jr. and Thomas Dube, Firmware Modification Attacks on Programmable Logic Controller, International Journel of Critical Infrastructure Protection, vol. 6(2), pp. 76-84, June, 2013.

[15] Ruijin Zhu, Yu-an Tan, Quanxin Zhang, Yuanzhang Li and Jun Zheng, Determining image base of firmware for ARM devices by matching literal pools, Digital Investigation, vol. 16, pp. 19-28, 2016.

[16] Institute of Electrical and Electronics Engineers. IEEE Standard Test Access Port and Boundary-scan Architecture: Approved February 15, 1990, IEEE Standards Board; Approved June 17, 1990, American National Standards Institute. IEEE, 1990.

[17] Pallavi Asrodia and Hemlata Patel, Analysis of Various Packet Sniffing Tools for Network Monitoring and Analysis, International Journal of Electrical, Electronics and Computer Engineering, vol. 1(1), pp. 55-58, May, 2012.

[19] Grand. J., JTAGulator: assisted discovery of on-chip debug interfaces, 21st DefCon Conference, Las Vegas, August, 2013.

[20] Team Rocker, RIFF Box JTAG Revolution, http://www.riffbox.org/jtag-news/riff-news/, July, 2010.

[21] Dominic Rath, OpenOCD: Open on-chip debugger, http://openocd.org/, January, 2017.

[22] CORELIS, ScanExpress Boundary-Scan Test Software, https://www.corelis.com/products/jtag-products/jtag-software/, October, 2017.

[23] XG autoelectric, XGecu TL866II Plus USB High Performance Programmer, http://www.autoelectric.cn/en/tl866_main.html, April, 2018.

[24] Craig Heffner, Binwalk: Firmware analysis tool, https://code.google.com/p/binwalk/, March, 2013.

[25] mh-nexus, HxD - Freeware Hex Editor and Disk Editor, https://mh-nexus.de/en/hxd/, May, 2018.

[26] Hex-Rays, IDA about, https://www.hex-rays.com/products/ida/, May, 2015.

[27] Oleh Yuschuk, OllyDbg, http://www.ollydbg.de/, February, 2014.

[28] pancake and the core-contributors, Radare 2 book, https://www.gitbook.com/download/pdf/book/radare/radare2book, November, 2016.

2018 한국정보보호학회 하계학술대회

B7 산업보안

오 희 국 (한양대학교)

- **S7CommPlus 제어 프로토콜 통신 보안 위협을 통한 기계학습 기반의 이상징후 탐지 방안 연구**
  홍기섭, 김효빈, 서정택
- **풍력발전 제어시스템의 사이버 보안위협 분석을 통한 공격 가능시나리오 도출 및 대응방안 제시**
  송진우, 윤 건, 전형율 ,서정택
- **산업제어시스템 보호를 위한 ICS DPI Firwall 개발**
  노권수, 한상헌, 박혜용, 김기현
- **SCADA 프로토콜 보안위협 및 보안요구사항 분석**
  위한샘, 이옥연
- **쇼단을 이용한 제어시스템 공격 사례분석 및 대응방안**
  박현진, 박재용, 김인수, 서정택

S7CommPlus 제어 프로토콜 통신 보안 위협을 통한 기계학습 기반의 이상징후 탐지 방안 연구

홍기섭*, 김효빈*, 서정택**

*순천향대학교 정보보호학과 사이버물리시스템보안연구실

**순천향대학교 정보보호학과

Study on Anomaly Detection based on Machine Learning through S7CommPlus Control Protocol Communication Security Threat

Ki-Seob Hong*, Hyo-Bin Kim*, Jung-Taek Seo**

*CPSS Lab., Department of Information Security Engineering, Soonchunhyang University.

**Department of Information Security Engineering, Soonchunhyang University.

요 약

최근 제어시스템을 대상으로 하는 악성코드를 통한 공격들이 고도화되고 정교해지고 있다. 제어시스템 환경에서 사이버 공격을 탐지하고자 화이트리스트 기반의 침입탐지시스템을 적용 및 연구 중에 있으나, 높은 오탐율 문제와 새로운 공격 탐지에 대한 어려움이 있다. 새로운 악성코드에 감염된 내부 PC를 통해 제어기기에 대한 제어명령 위변조 공격이 발생할 수 있으며 이는 제어시스템에 큰 피해를 야기할 수 있다. 따라서 제어시스템 내의 제어망에서의 이상징후 탐지 방안 연구가 필요하다. 본 논문에서는 Siemens 社의 S7CommPlus 제어 프로토콜을 분석하여 보안 위협을 재현하고, 효과적인 보안 위협 탐지를 위해 기계학습 기반 이상징후 탐지 방안을 제안한다.

I. 서론

최근 국가기반시설, 제조 기업 등의 제어시스템을 대상으로 사이버 공격이 증가하고 있다. 실제로 2010년 이란의 우라늄 추출 시설의 가동을 중단시키기 위해 Microsoft 社의 제로데이 취약점을 통해 내부 네트워크를 감염시켜 PLC(Programmable Logic Controller, 이하 PLC)의 제어명령 위변조 공격을 수행한 Stuxnet[1], 2011년 MS-Word 취약점을 이용하여 피해 기관이나 기업을 대상으로 내부정보를 수집하는 Duqu[2], 2012년 이란 및 중동 국가의 전력 제어시스템의 피해를 주기 위해 Windows 시스템을 감염시켜 내부 문서, 모니터 스크린샷, 네트워크 기록 등을 훔치며 백도어를 설치한 Flame[3], 이외에도 Dragonfly, BlackEnergy, Industroyer 등이 대표적인 사이버 공격 사례들이다[4][5][6].

제어시스템 대상 사이버 공격의 특징 중 하나는 피해 대상 기관이나 기업에서 사용중인 산업 제어시스템의 제조사를 파악하여 PLC나 HMI,(Human Machine Interface, 이하 HMI), 소프트웨어의 취약점과 제조사의 독자적인 제어 프로토콜의 취약점을 사전에 분석하여 사이버 공격을 수행한다는 점이다. 글로벌 산업 제어기기 및 플랫폼 시장에서 높은 시장점유율을 차지하고 있는 독일의 Siemens 社는 이더넷 기반의 독자적인 S7CommPlus 제어 프로토콜을 개발하여 상용화하고 있다. 하지만 최근 연구를 통하여 다양한 보안 위협 시나리오 및 취약점 관련 연구가 발표되었다[7][8][9]. 이에 따라 폐쇄망으로 운영되고 있는 제어시스템 환경에서 사

이버 공격을 탐지 및 대응하고자 화이트리스트 기반 침입탐지시스템 적용에 대한 논의 및 연구가 진행 중에 있지만, 제어시스템에서 새로운 사이버 공격과 제어명령 재전송 공격 등에 대해 탐지하지 못하는 한계점이 있다. 본 논문에서는 S7CommPlus 제어 프로토콜의 통신 패킷을 대상으로 기계학습을 통한 이상징후 탐지 방안을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 S7CommPlus 제어 프로토콜 보안 위협 관련 연구와 제어시스템에서의 기계학습을 통한 이상 징후 탐지 관련 연구들에 대해 소개한다. 3장에서는 본 논문에서 대상으로 하는 S7CommPlus 제어 프로토콜의 통신 과정 및 서비스 거부 공격(Denial of Service)과 재전송 공격을 통한 보안 위협들을 재현하고, 제안하는 탐지 방안을 제시하며 4장에서는 실험 결과를 분석한다. 5장에서는 본 논문의 결론과 향후 연구 방향에 대해 기술한다.

II. 관련 연구

2.1 S7CommPlus 제어 프로토콜 보안 위협

최근 3년 동안 Siemens 社의 독자적인 S7CommPlus 제어 프로토콜에 대한 보안 위협 연구가 진행되었다. Johannes Klick 등[7]은 사물인터넷 검색 엔진인 쇼단(Shodan)을 이용하여 외부 인터넷과 연결되어있는 PLC를 검색하여 S7CommPlus 제어 프로토콜의 이전 버전인 S7Comm 제어 프로토콜의 인증 취약점을 통해 악의적인 논리 코드 블록을 다운로드하여 내부 네트워크를 감염시키는 공격 시나리오 연구를 진행하였다. 이는 제어시스템이 완벽하게 폐쇄된 네트워크 환경으로 구성되어 운영되지 않는 점을 이용하여 외부에서 접근을 통해 제어 프로토콜의 취약점을 이용해 악의적인 통신 패킷을 발생시킬 수 있다는 것을 입증하였다. 프로토콜 취약점을 보완하기 위해 다음 버전인 S7CommPlus 제어 프로토콜이 개발되었지만, Ralf Spenneberg 등[8]은 S7CommPlus 제어 프로토콜의 분석을 통하여 재전송 공격 방지 기능을 우회하여 PLC 간 통신을 이용한 악의적인 코드 블록을 전파하는 웜을 통한 공격 시나리오 연구를 진행하였다. 이에 따라, 암호화 기능이 보완된 새로운 S7CommPlus 제어 프로토콜이 개발되었지만, Cheng Lei 등[9]은 PLC 관리 제어 소프트웨어인 TIA Portal을 역공학을 통하여 암호화된 새로운 S7CommPlus 제어 프로토콜을 복호화하여 재전송 공격을 통해 정상적인 통신 패킷을 임의로 생성하여 제어 명령이 가능함을 입증하였다. 이러한 보안 위협 연구를 통한 보안 대책으로 제어 프로토콜 통신 패킷 전체 암호화 방안과 관리 소프트웨어의 역공학 방지 기술 방안 제시를 했지만, 가용성을 중시하는 제어시스템의 특성 상 업데이트 문제 및 고비용의 제어기기 교체 등의 경제적인 문제가 있다. 따라서 사이버 공격을 탐지하여 조치할 수 있는 실질적인 방안이 필요하다.

2.2 제어시스템에서의 기계학습을 통한 이상징후 탐지 방안

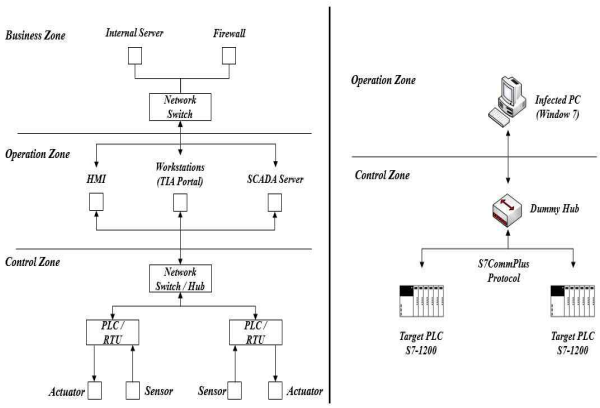
최근 제어시스템의 화이트리스트 기반 침입탐지시스템 적용 연구가 진행 중에 있으나, 새로운 사이버 공격 탐지에 어려움을 가지고 있다. 이에 따라, 기계학습을 통한 이상징후 탐지에 대한 연구가 진행 중에 있다. Leandros A. Maglaras 등[10]은 SCADA(Supervisory Control and Data Acquisition) 시스템에 기계학습 모델인 OCSVM(One-Class support vector machine)을 통하여 정상적인 트래픽과 비정상적인 트래픽을 클러스터링하여 분류하는 연구를 진행하였다. 하지만 제어시스템에서 사용하는 대부분의 제어 프로토콜이 단일 통신 패킷 구조를 가지고 있어 트래픽을 분류하기 위한 분석에 용이하며, 재전송 공격 방지 기능 등이 있는 특정한 이더넷 기반의 제어 프로토콜을 대상으로 비정상 트래픽 분류에 한계가 있다. F. Schuster 등[11]은 PROFINET 제어 프로토콜을 대상으로 통신 패킷의 출발/목적지 주소, 프로토콜 타입, 패킷 타입, 패킷의 데이터를 feature로 선정하여 n-grams 모델을 통해 외부로 부터의 침입을 탐지하는 연구를 진행하였다. 하지만, 외부 침입이 아닌 내부자의 USB를 통한 악성코드 전파와 같은 의도되거나, 의

도되지 않은 다양한 공격 방법을 이용하여 감염된 내부 PC를 통해 제어기기인 PLC로의 재전송 공격 탐지에 대한 어려움이 존재한다.

III. 보안위협 분석을 통한 탐지 방안

본 장에서는 S7CommPlus 제어 프로토콜 통신 과정에서 발생할 수 있는 보안 위협들을 재현하고, 이를 탐지 할 수 있는 방안을 제안한다.

제어시스템 운영 보안 상, 기관이나 기업의 실제 제어 데이터 셋을 구하는 것은 한계점이 있다. 따라서 제안하는 탐지 방안에 활용 가능한 데이터 셋 수집을 위해 [그림 1]과 같이 PC 및 PLC 실험환경을 구축하였다. 운영체제는 Windows 7 환경에서 PLC 관리, 제어 소프트웨어 TIA Portal 11을 설치하였고, 통신 패킷 분석을 위해 Dummy Hub를 사용하였으며, PLC는 Siemens 社의 S7-1200 모델로 구성하였다.

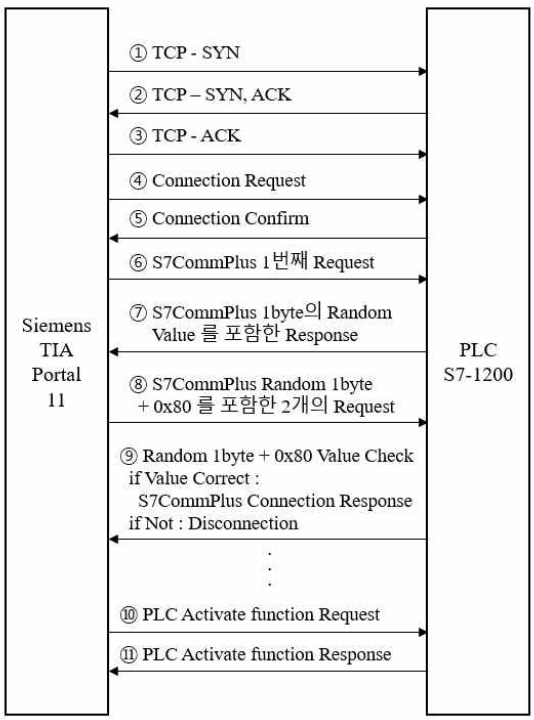


[그림 1] 일반적인 제어시스템 구조와 실험환경 구축 네트워크 구성도

[그림 1]의 제어시스템 내 제어망인 Operation Zone의 PLC를 관리, 제어하는 PC가 악성코드에 감염되었다는 가정하에 재전송 공격 및 서비스 거부 공격을 재현한다.

3.1 S7CommPlus 제어 프로토콜 분석 및 보안 위협

S7CommPlus 제어 프로토콜은 이더넷 기반으로 동작한다. 각 PLC는 IP를 지정할 수 있으며 서비스 포트는 102번을 통해 관리 제어 소프트웨어인 TIA Portal과 서로 통신한다. [그림 2]와 같이 TCP 3-way 핸드 쉐이크 과정을 거치며, ⑦에서 PLC는 S7CommPlus 통신 패킷 데이터에 Random Value를 포함한 1바이트를 전송한다. ⑧에서 TIA Portal은 Random Value에 0x80을 더한 값을 통신 패킷의 17번째 22번째 데이터 필드에 넣어 전송한다. ⑨에서 PLC는 수신 받은 값을 검사하고 올바른 값이면, 연결을 맺으며 올바르지 않을 시, 연결을 끊는다. 연결이 성립되면 ⑩에서 PLC 시작, 정지 등의 기능을 하는 제어 명령 패킷을 전송한다.

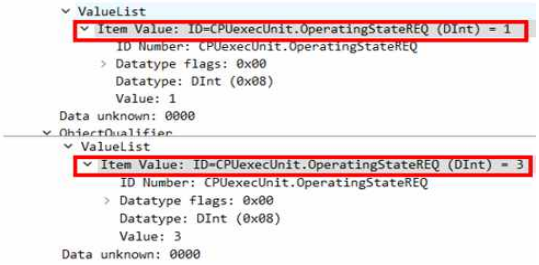


[그림 2] S7CommPlus 제어 프로토콜 통신 과정

3.1.1 제어 명령 재전송 공격

제어시스템은 임의로 PLC 시작, 정지 제어 명령만으로도 센서와 엑추에이터의 정상적인 기능을 방해할 수 있다. 만약 PC가 악성코드에 감염되어 악의적인 스크립트가 실행된다면 큰 피해를 줄 수 있다. 따라서 본 연구에서는 기본적인 PLC 시작, 정지 제어명령만 재전송 공격을 재현하였다. PLC 시작, 정지 제어명령 패킷은 항상 동일하게 18개의 Request, Response

패킷 프레임이 발생하며, 분석을 통하여 [그림 3]과 같이 18번째 패킷 프레임의 28번째 데이터 필드 값인 Item Value가 0x01이면 PLC 시작, 0x03이면 정지하게 된다. 정상적인 PLC 시작, 정지 제어 패킷을 캡처하여 스크립트를 통해 [그림 2]의 과정 ①부터 ~ ⑨까지 Random Value를 연산을 통해 재전송 공격이 가능하다.



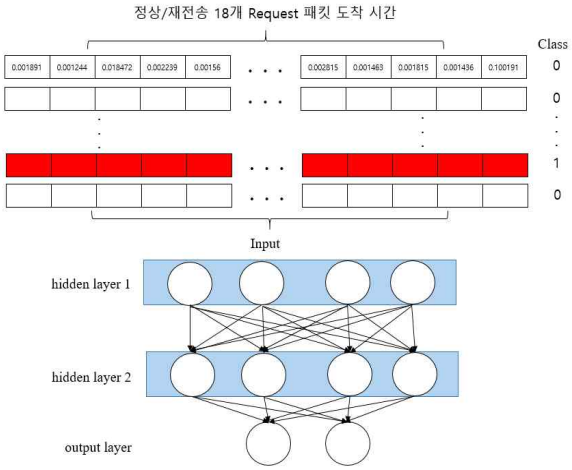
[그림 3] PLC 시작, 정지 패킷 데이터 필드

3.1.2 서비스 거부 공격

S7CommPlus 제어 프로토콜은 TCP 기반으로 동작하고 102번 포트로 서비스 거부 공격이 가능하다. 실시간성이 중요한 제어시스템에서 센서의 값에 따라 엑추에이터를 제어하는 PLC의 논리 프로그램 동작을 서비스 거부 공격을 통해 방해할 수 있다.

3.2 제안하는 탐지 방안

앞 절을 통해 PLC의 서비스 거부 공격의 경우, 단위 초당 트래픽의 양을 실시간 모니터링을 통해서 탐지가 쉽게 가능하다. 하지만 악성코드에 감염된 TIA Portal이 설치된 PC의 경우 동일한 IP와 서비스 포트를 사용하고 있어, 일반적인 화이트리스트를 통한 탐지가 어렵다. 기계학습을 통한 재전송 공격 탐지의 경우, 분별력 있는 feature 선정이 제한적이지만, 본 연구에서 제안하는 방법은 항상 서로 다른 18개의 패킷 시퀀스가 발생하는 PLC 시작, 정지 제어 명령의 각 Request 패킷을 분석하여 정상과 재전송 공격 간의 Request 패킷 도착 시간 간격 차이를 feature로 이용한다. 따라서 [그림 4]와 같이 각 시퀀스마다 패킷의 크기에 따른 미세한 패킷 전송 시간차이를 입력 값으로 사용하여 기계학습을 통한 재전송 공격 탐지 방안을 제안한다.



[그림 4] Request 패킷 도착 시간 차이를 이용한 기계학습 기반 탐지 방안

3.3 실험 방법

3.3.1 실험 데이터 수집

TIA Portal를 통한 정상적인 PLC 정지 패킷을 약 5시간 동안 수집하여, 2464개의 패킷 플로우와 재전송 공격을 통해 30분 동안 99개의 패킷 플로우를 수집하였다. [그림 5]와 같이 수집된 .pcapng 파일을 파이썬 스크립트를 통해 각 18개의 패킷으로 나누어 패킷 도착 시간을 .csv 파일에 저장하였다.

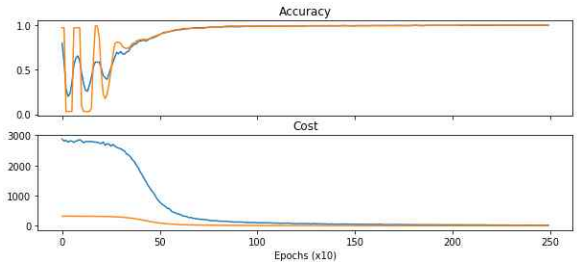
```
frame_length = 18
pcap_name = '0524_replay.txt'
csv_name = pcap_name.split('.')[0] + '_result.csv'

tmp_path = 'D:₩paper/'

csvfile = open( tmp_path + csv_name, 'wb' )
fieldnames = [ 'frame[' + str(i) + ']' for i in range(1, frame_length + 1) ]
writer = csv.writer( csvfile )
writer.writerow( fieldnames )

filepath = tmp_path + pcap_name
Packet_Tree = open( filepath, 'rb' ).read()

pattern = re.compile('(Frame ₩d+: ₩d+ bytes)')
frame_number = pattern.findall(Packet_Tree)

def split_frame(_Packet_Tree):
    loop = 0
    result = []

    while loop < len(frame_number) - 1:
        index = _Packet_Tree.find(frame_number[loop + 1])
        frame = _Packet_Tree[:index].rstrip()
        result.append(frame)

        _Packet_Tree = _Packet_Tree[index:]
        loop += 1

    return result

def COTP_packet(_split_frame):
    result = []

    for frame in _split_frame:
        if frame.find('S7 Communication Plus') != -1:
            result.append(frame)

    return result


def find_field( _packet, _field_name ):
    for field in _packet.split( '₩n' ):
        if field.find( _field_name ) != -1:
            return field.split( _field_name )[-1].strip()

def save_csv( _result ):
    #fieldnames = [ 'frame[' + str(i) + ']' for i in range(1, 19) ]
    loop = 0
```

[그림 5] S7CommPlus Request 패킷 도착 시간 값 파싱 및 ,csv 파일 저장 스크립트

전체 패킷 플로우 대비 재전송 패킷 플로우의 구성비는 0.0386%로 구성하였으며, 재전송 공격 패킷의 경우, 정상적인 데이터와 미세하게 시간 값의 차이가 있음을 확인할 수 있었다. 이를 통해 기계학습 데이터로 활용한다.

3.3.2 데이터 학습

본 실험에서는 Google에서 만든 오픈소스 라이브러리인 TensorFlow를 이용하였다. 고차원적인 데이터를 처리하는 것이 아니기에 일반적인 인공 신경망(Neural Network)를 활용하였다. 전체 데이터의 80%는 훈련 데이터로 활용하고 나머지 20%는 테스트하기 위한 데이터로 활용하며, 데이터 셔플링을 한다. 정상/비정상 데이터의 불균형 문제를 해결하기 위해 전체 데이터 수를 비정상 데이터 수로 나눈 비율을 학습모델에 적용한다. 입력 노드로는 [그림 4]와 같이 18개이며, Hidden Layer를 포함한 전체 Layer를 4개 층으로 구성하였다. 출력 노드의 경우, 정상과 비정상을 나누기 위해 2개로 구성하였다. 학습된 모델의 성능을 높이기 위한 파리미터 설정값과 activation function 등에 관련된 구체적인 기계학습 모델의 구성에 대한 논의는 본 논문의 취지와 맞지 않기에 생략한다. 수집된 데이터로 모델을 학습시킨 결과 [그림 6]과 같이 Epoch를 200을 주었을 때, 학습된 모델의 정확도가 99.65%의 결과가 나왔으며 비용이 수렴하는 것을 확인할 수 있다.

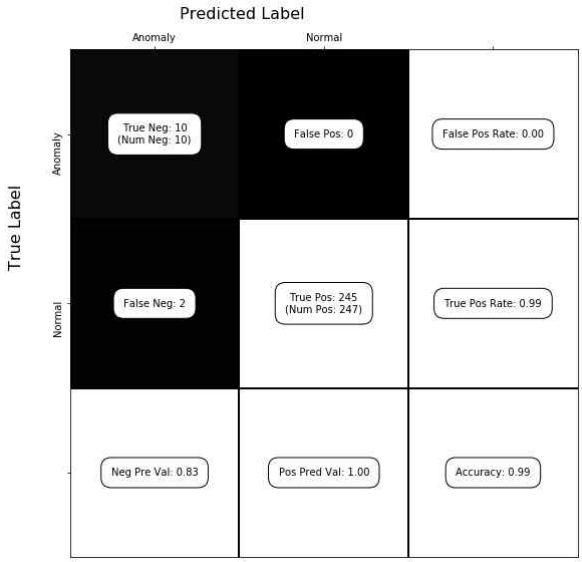


[그림 6] 수집된 데이터를 이용한 제안하는 학습된 모델의 정확도와 비용

훈련된 학습 모델을 활용하여 따로 분류하였던 테스트 데이터 셋에 적용하여 실험 결과를 분석한다.

IV. 실험 결과

앞 절의 과정을 통해 학습된 모델을 이용하여 테스트에 활용할 데이터를 실험을 통해 다음 [그림 7]과 같은 결과를 보였다.



[그림 7] Confusion matrix을 통한 모델 평가[12]

F1 Score는 기계학습 모델의 정탐과 오탐에 대한 분류 성능을 나타낼 때 주로 사용한다. F1 Score의 계산식은 식(1)과 같다.

$$F1\ Score = \frac{2 * TP}{2 * TP + FP + FN} \quad (1)$$

- TP(True Positive) : 실제 정탐을 모델이 정탐으로 분류
- FP(False Positive) : 실제 오탐을 모델이 정탐으로 분류
- FN(False Negative) : 실제 정탐을 모델이 오탐으로 분류

분류 정확도는 99.22%, F1 Score는 0.9959의 결과를 보였다. 247개의 정상 데이터 중 245개를 정상으로 판별하였으며, 나머지 2개를 오탐으로 판별하였다. 실제 오탐을 모델이 오탐으로 분류하는 TN(True Negative)의 경우, 모두 탐지하는 결과를 보였다.

V. 결론

본 논문에서는 S7CommPlus 제어 프로토콜의 분석을 통한 보안 위협을 재현하였다. 그중 화이트리스트를 통한 재전송 공격 탐지의 어려움에 따라 3장의 제안하는 기계학습 기반 탐지 방안 연구를 통해 99.22%의 분류 정확도가 나왔다. 본 연구의 제한사항으로 실제 제어시스템에서 사용하는 대량의 데이터 셋 수집 및 분석의 한계가 있었다. 향후 연구로는 최적화된 모델의 성능을 위해 최적화된 기계학습 알고리즘 모델 개발과 정상적인 데이터만을 활용한 비지도학습 모델 적용 연구 및 실시간 탐지에 대해 연구가 필요하다.

ACKNOWLEDGEMENT

본 연구는 2018년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 논문입니다(No. 2016M2A8A4952280).

[참고문헌]

[1] Nicolas Falliere, Liam O Murchu, and Eric Chien, “W32.Stuxnet Dossier,” Symantec, verseion 1.3 edition, November 2010.

[2] Nikos Virvilis, Dimitris Gritzalis, “The Big Four – What We Did Wrong in Advanced Persistent Threat Detection?,” IEEE Availability, Reliability and Security(ARES), pp.248 - 254., September 2013.

[3] Bencsath, B., Pek G., Buttyan L. and Felegyhazi M. “The Cousins of Stuxnet: Duqu, Flame, and Gauss,” in Proc. Of Future Internet, Vol. 4, No.4, pp. 971-1003, November 2012.

[4] R. Piggin, “Critical Infrastructure Under Attack,” ITNOW, vol. 56(4), pp. 30-33., December 2014.

[5] R. Khan, P. Maynard, K. McLaughlin, D. Laverty and S. Sezer, “Threat analysis of BlackEnergy malware for synchrophasor based real-time control and monitoring in smart grid,” Proc. 4th Int. Symp. ICS SCADA Cyber Secur. Res. (ICS-CSR), pp. 53-63, Aug. 2016.

[6] A. Cherepanov, "Win32/industroyer-a new threat for industrial control systems," Tech. Rep., 2017, [Online] Available: https://www.welivesecurity.com/wp content/uploads/2017/06/Win32_Industroyer.pdf.

[7] Johannes Klick, Stephan Lau, Daniel Marzin, Jan-Ole Malchow and Volker Roth, “Internet-facing PLCs - A New Back Orifice,” In Blackhat USA 2015, Las Vegas, USA, 2015.

[8] R. Spenneberg, M. Brüggemann, H. Schwartke, “Plc-blaster: A worm living solely in the plc,” In Blackhat ASIA 2016, Singapore, 2016.

[9] Cheng Lei, Li Donghong and Ma Liang, “The spear to break the security wall of S7CommPlus,” In Blackhat USA 2017, Las Vegas USA, 2017.

[10] L. A. Maglaras, J. Jiang, T. Cruz, "Combining ensemble methods and social network metrics for improving accuracy of OCSVM on intrusion detection in SCADA systems", J. Inf. Security Appl., 2016, [online] Available: http://dx.doi.org/10.1016/j.jisa.2016.04.002.

[11] F. Schuster, A. Paul, H. Konig, "Towards learning normality for anomaly detection in industrial control networks" in Emerging Management Mechanisms for the Future Internet, Berlin, Germany:Springer, vol. 7943, pp. 61-72, 2013.

[12] Matt Hancock, [Online] http://notmatthancock.github.io/2015/10/28/confusion-matrix.html

풍력발전 제어시스템의 사이버 보안위협 분석을 통한 공격 가능시나리오 도출 및 대응방안 제시

송진우, 윤건, 전형율, 서정택

순천향대학교 정보보호학과

A Study on Detecting Attackable Scenarios and Analyzing Countermeasures through Analysis of Cyber Security Threats in Wind Power Generation Control System

Jin Woo Song, Keon Yun, Hyung Youl Jeon, Jung Taek Seo

Department of Information Security Engineering, Soonchunhyang University.

요 약

최근 4차 산업혁명의 발전으로 인해 에너지 안보를 위한 신재생 에너지 개발이 추진되고 있으며 그 중 높은 기술적 완성도와 상대적인 원가 경쟁력을 갖춘 풍력발전 제어시스템이 각광받고 있다. 하지만 풍력발전 제어시스템은 사이버보안이 중요한 요소임에도 불구하고 설계적 결함, 외부 인터넷망과의 연계를 통한 취약점, 안전하지 않은 원격관리서비스(ex. telnet, FTP, SNMP 등)를 사용하는 등의 여러 취약점들이 존재할 수 있다. 이러한 풍력발전 제어시스템이 사이버 공격에 노출될 경우 발전기 손상 및 파괴에 따른 전력 공급 중단뿐 아니라 경제적 손실 및 인명피해를 발생시키는 등의 심각한 보안 사고를 일으킬 수 있다. 따라서 본 논문에서는, 풍력발전 제어시스템의 사이버 보안위협을 분석하여 공격가능시나리오를 도출하고 대응방안을 제시하였다.

I. 서론

에너지 수요의 급증과 고갈에 대한 대책의 일환으로 신재생 에너지가 개발이 추진되고 있다. 특히 높은 기술의 완성도와 상대적으로 저비용 등의 이점을 가진 풍력발전 시스템은 급속한 신장 추세를 보이고 있으며, 국내 풍력 발전설비 또한 최근 5년(12~16년)간 연평균 21.4% 증가하는 등 지속적인 발전을 거듭하고 있다[1].

풍력발전기가 증가하면서 이와 관련된 사고 또한 증가하고 있다. 2016년 8월 기준 국내 풍력발전기 사고로 인한 발전기 정지사례는 60건이다. 또한 풍력발전 시스템 설계 및 구현적 결함으로 인해 풍력발전기의 가동이 중단되거나 블레이드 과회전으로 인해 과열로 인한 파손 및 화재가 발생하는 경우 또한 빈번하게 발생하고 있다[2].

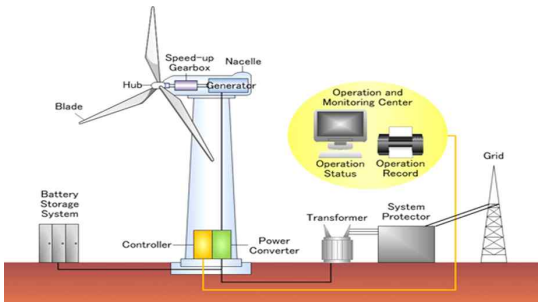
현재까지는 풍력발전기의 제어시스템에 대해 사이버공격으로 인한 사고사례는 보고된 바 없지만, 풍력발전기 또한 해킹 사고로부터 자유로울 수 없다. 2015년 북미의 풍력발전기 전문 제조업체인 XZERES 제품에서 CRSF(Cross Site Request Forgery) 취약점이 발견되었고 2017년 blackhat 및 DEFCON 컨퍼런스에서 Tulsa대학교의 보안 전문가인 Jason Staggs는 풍력발전기의 취약점에 대해 발표한 사례가 있다[3][4].

따라서 본 논문에서는 풍력발전 제어시스템의 사이버보안 취약점을 분석하고 공격가능시나리오를 도출하여 그에 따른 대응방안을 제시하였다.

본 논문의 구성은 다음과 같다. Ⅱ장에서 풍력발전 제어시스템의 구조 및 구성요소에 대해 살펴본다. Ⅲ장에서 풍력발전 제어시스템에 대한 보안위협을 분석한다. Ⅳ장에서는 앞서 분석한 보안위협을 바탕으로 풍력발전 제어시스템에 대한 공격가능시나리오 및 그에 따른 파급효과를 도출한다. Ⅴ장에서는 앞서 분석한 보안위협을 바탕으로 도출된 공격가능시나리오에 대한 대응방안을 제시한다. 마지막으로 Ⅵ장에서 본 논문의 결론 및 향후 연구방향을 제시한다.

II. 풍력발전 제어시스템 구조

풍력발전기는 풍력을 이용하여 전기를 발생시킨다. 풍력은 각 발전기에 설치된 블레이드를 회전시키며, 로터는 발전기에 동력을 공급하고 발전기는 로터 블레이드로 획득하는 기계적 에너지를 전기적 에너지로 변환하여 전기를 생산한다. 풍력발전 제어시스템은 풍력발전기로부터 각종 데이터 (ex. 바람속도, 전력생산량, 상태정보, 로터RPM, 나셀 내부온도 등)을 전송받고, 풍력발전기에 대한 제어명령 (ex. 최대 발전생산량 변경, 풍력터빈 작동상태변경, 비상정지 등)을 전송하여 풍력발전기를 제어한다. 아래 [그림 1]은 풍력발전 제어시스템의 전체적인 구성요소이며, [표 1]은 구성요소에 따른 용어정리이다.



[그림 1] 풍력발전 제어시스템 구조

[표 2] 풍력발전 시스템 구성요소 용어정리

용어	정의
블레이드 (Blades)	대부분의 터빈에는 2~3개의 블레이드가 존재하며 바람이 불 경우 회전
로터 (rotor)	블레이드를 결합한 풍차를 의미
브레이크 (Brake)	비상 시 로터를 기계적, 전기적 또는 유압적으로 정지시킴
컨트롤러 (Controller)	시간당 약 8 ~ 16 마일의 풍속일 경우 기계를 작동시키고 약 55mph 이상의 풍속에서 기계를 정지시킴 터빈은 풍속에 의해 손상될 수 있기 때문에 약 55mph 이상의 풍속에서 작동하지 않음
기어박스 (Gear Box)	저속 축을 고속 축에 연결시키고 분당 60~80회의 회전속도를 약 1,000 ~ 1,800으로 높이는 역할을 수행
발전기 (Generator)	로터 블레이드로 획득하는 기계적 에너지를 전기적 에너지로 변환하여 AC전기를 생성
풍속계 (Anemometer)	풍속을 측정하고 해당데이터를 제어기로 전송
나셀 (Necelle)	기어박스, 고속 축, 생성기, 컨트롤러, 브레이크를 모두 포함하는 구조물
Pitch	날개를 바람 밖으로 돌려 로터 속도를 제어하고, 너무 높거나 너무 낮은 바람이 전기를 생산하지 못하도록 로터를 회전시킴
Tower	터빈의 구조를 지지하고, 더 많은 전기를 생산할 수 있도록 도움
Yaw Drive	방향이 바뀔 경우 바람이 불어오는 방향의 터빈이 바람을 바라볼 수 있도록 조정
Yaw motor	Yaw Drive에 동력을 공급

III. 풍력발전 제어시스템 보안위협

풍력발전 제어시스템은 설계 및 구현의 결함으로 인해 공격에 취약한 구조를 유지하고 있으며, 다음과 같은 취약성이 존재한다[3][4].

- 제어 메시지의 인증 또는 암호화 없음
- 안전하지 않은 원격 관리서비스 사용 (ex. telnet, FTP, SNMP 등)
- 공급업체 기본암호 또는 추측하기 쉬운 암호 사용
- 현장 발전기기 및 제어시스템의 물리적 보안이 매우 취약
- 풍력 터빈 간의 네트워크분할이 없음
- Legacy 운영체제 사용

이러한 취약성을 통해 공격자는 전송된 데이터의 기밀성 및 무결성을 손상시키며 서비스 사용을 불가능하게 할 수 있다[5][6]. 따라서 본 장에서는 풍력발전 제어시스템의 보안위협을 분석하고 [표 3]을 통해 정리하였다.

[표 3] 풍력발전 제어시스템 보안위협

보안위협	정의
메시지 변조	서버의 취약점을 이용하여, 공격자가 제어메시지를 원하는 메시지로 변조
악의적인 소프트웨어 삽입	바이러스나 웜, 스파이웨어와 같이 컴퓨터 또는 네트워크에 피해를 입히거나 보안을 무력화하게 하는 소프트웨어 삽입

비인가 접근	인가를 받지 않은 사용자가 제어시스템에 접근
DDoS 공격	여러 대의 공격자를 분산 배치하여 서비스 거부 공격을 함으로써 정상적인 서비스 제공을 어렵게 함
제로데이 공격	보안 취약점이 발견되었을 때 해당 취약점이 공식화되기 전에 악용하여 이루어지는 공격
랜섬웨어	시스템을 잠그거나 데이터를 암호화하여 사용할 수 없도록 만들어 이를 인질로 금전을 요구하는 악성 프로그램

IV. 풍력발전 제어시스템 공격가능 시나리오 및 파급효과

4.1 Use-after-free 취약점을 이용한 공격가능 시나리오

트랜드마이크로와 제로데이이니셔티브(ZDI)가 발행한 'SCADA HMI 보안 취약점 동향보고서'에 따르면 2016년 동안 SCADA 시스템 보안 취약점 패치가 나오는데 143일이 소요되었다. 대부분의 HMI는 Windows를 기반으로 하고 있기 때문에, 아래 [그림 2]와 같이 풍력발전기의 제어시스템으로 사용되고 있는 YOKOGAWA사의 FAST/TOOLS의 경우에도 이에 해당된다[7][8].

● Web HMI Server

Items	Specifications	
CPU	Microsoft	Intel © Core™ i7, 3.40 GHz or better
RAM	At least 8 GB (for ASPA 16 GB)	
Hard Disk	1TB (7200 rpm) At least 200 Mbytes of free space is required. Additional space is required for display and symbols.	
Ethernet adapter	An Ethernet adapter that is supported by the operating system specified is required at installation.	
DVD-ROM Drive	A DVD-ROM drive that is supported by the operating system is required.	
Peripherals	Sound card and speaker are required for audible messages.	
Web browser	Microsoft EDGE Mozilla Firefox 53 Google Chrome 58	

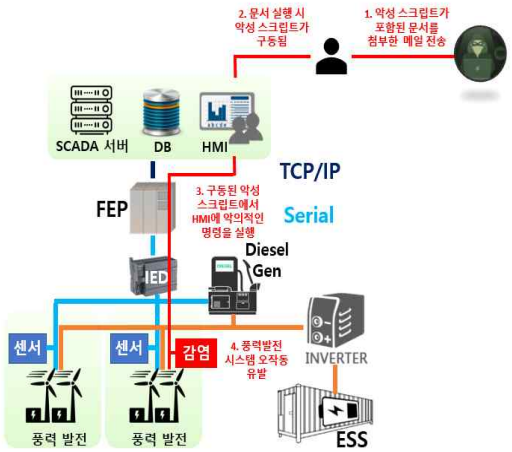
● Web HMI Client

Items	Specifications	
CPU	Microsoft	Intel © Core™ i5, 2.50 GHz or better
RAM	At least 4 GB	
Hard Disk	500 GB (7200 rpm) At least 1 GB of free space is required.	
Ethernet adapter	An Ethernet adapter that is supported by the operating system specified below is required at installation.	
DVD-ROM Drive	A DVD-ROM drive that is supported by the operating system is required.	
Peripherals	Sound card and speaker are required for audible messages.	
Web browser	Windows 10 Pro (64 bit) Windows 10 Enterprise (64 bit) Windows 10 Enterprise 2016 LTSB (64 bit) Windows 10 IoT Enterprise 2016 LTSB (64 bit) Windows 7 Professional SP1 (64 bit)	Microsoft EDGE Mozilla Firefox 53 Google Chrome 58

[그림 2] YOKOGAWA사 FAST/TOOLS 구성 및 사양

이 경우 Windows의 알려지지 않은 취약점이나 최신의 취약점을 이용한 공격이 가능하다.

최근에 알려진 Use-after-free 취약점은 DRM(Direct Rendering Manager) 관련 메소드의 취약점으로, Use-After-Free 취약점을 이용한다. 워드나 엑셀 문서를 열 때 플래시를 구동하여 어도비 플래시 프로그램에서는 콘텐츠의 저작권 정보를 처리하는 DRM 기능을 통해 특정 함수를 호출하게 되고, DRM 정보를 처리하는 과정에서 지정한 변수의 적절성을 검증하지 않고 메모리를 해제하게 된다. 이 때 버그가 발생되고, 공격자는 이를 통하여 원하는 명령어를 실행할 수 있게 된다. 아래 [그림 2]는 Use-after-free 취약점을 이용한 공격가능시나리오를 나타낸다.



[그림 3] Use-after-free 취약점을 이용한 공격가능시나리오

[표 4] Use-after-free 취약점을 이용한 공격가능시나리오 단계별 세부 내용

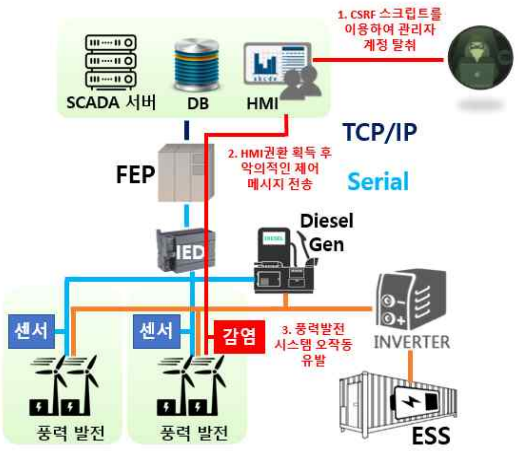
단계	세부내용
Step 1	공격자는 Use-after-free 취약점을 활용하여 악성 스크립트를 첨부한 문서를 메일로 전송
Step 2	사용자가 문서 파일을 실행하게 되면 악성 스크립트가 구동됨
Step 3	구동된 악성 스크립트를 통해 HMI에 악의적인 명령을 실행
Step 4	풍력 발전기기 오작동 유발

[그림 3]을 통한 파급효과는 다음과 같다.

- 악의적인 명령을 실행하여 시스템 피해 유발
- 구동된 플래시를 통해 명령어를 실행하여 내부자료 외부 유출가능
- 취약점 패치되기 전까지 다양한 공격 수행 가능

4.2 CSRF 취약점을 이용한 공격가능 시나리오

CRSF(Cross-Site Request Forgery) 공격은 웹사이트의 취약점을 이용한 공격으로, 사용자의 의지와는 무관하게 공격자가 의도한 행위를 특정 웹사이트에 요청시키는 공격을 의미한다. 아래 [그림 4]는 CSRF취약점을 이용한 공격가능 시나리오를 나타낸다.



[그림 4] CSRF취약점을 이용한 공격가능시나리오

[표 5] CSRF 취약점을 이용한 공격가능시나리오 단계별 세부 내용

단계	세부내용
Step 1	공격자는 Web client에 CSRF 스크립트가 포함된 게시물 또는 파일 등을 게시하여 관리자가 CSRF 스크립트가 포함된 게시물을 확인하도록 만들어 관리자 계정 탈취
Step 2	관리자 계정을 통해 제어발전시스템 내 시스템의 관리자 ID, PW 정보를 탈취해 HMI 권한을 획득하여 악의적인 제어 메시지를 기기에 전송
Step 3	풍력 발전기기 오작동 유발

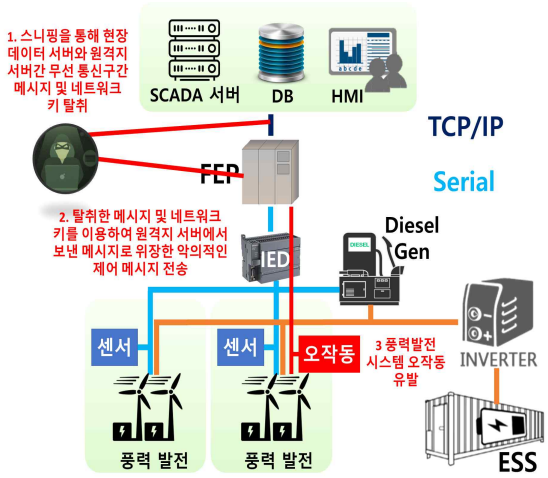
[그림 4]을 통한 파급효과는 다음과 같다.

- HMI 이외의 시스템 관리자 정보를 획득하여, 시스템 조작 및 피해 유발
- 악성코드를 이용한 봇넷을 구성하여 제어 시스템 망 서버자체에 DDoS 공격 및 시스템 마비
- 악성코드를 이용한 봇넷을 구성하여 새로운 공격 형태의 악성코드 삽입 가능

4.3 무선통신 구간 스니핑을 통한 메시지위조 공격가능시나리오

스니핑 공격은 무선LAN 신호를 잡아내 네트워크상의 데이터를 도청하는 행위를 의미한다. 공격자는 스니핑도구를 통하여 무선 통신의 ID, PW를 획득이 가능하며, 이를 통하여 네트워크에 접속이 가능하다.

아래 [그림 5]은 스니핑을 통한 메시지위조 공격가능시나리오를 나타낸다.



[그림 5] 스니핑을 통한 메시지위조 공격가능시나리오

[표 6] 스니핑을 통한 메시지변조 공격가능시나리오 단계별 세부 내용

단계	세부내용
Step 1	공격자는 현장 데이터 서버와 원격지 제어 및 모니터링 서버간 무선 통신구간에 스니핑 도구를 통해 통신을 분석하여 메시지 및 네트워크 키 획득
Step 2	습득한 메시지와 네트워크 키를 이용하여 현장 데이터서버에 원격지 서버에서 보낸 메시지로 위장한 악의적인 제어명령 전송
Step 3	풍력 발전기기 오작동 유발

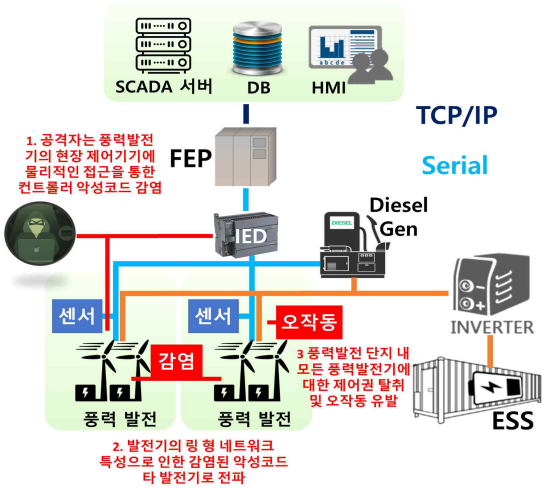
[그림 5]을 통한 파급효과는 다음과 같다.

- 공격자는 무선 통신구간의 통신 권한을 통하여 기기 내 악성코드 삽입 가능
- 현장데이터 서버에서 원격 모니터링 서버로 전송하는 데이터를 위·변조 가능

4.4 물리적 접근을 통한 공격가능시나리오

제어시스템의 특성상 넓은 설치 공간을 가지며 발전기와 같은 구성요소는 물리적 접근이 가능한 외부에 존재하며, 이는 발전기 시스템의 물리적 보안이 취약해 질 수 있는 요소 중 하나이다[6].

아래 [그림 6]을 통해 공격자의 물리적 접근을 통한 공격가능시나리오를 나타내었다.



[그림 6] 물리적 접근을 통한 공격가능시나리오

[표 7] 물리적 접근을 통한 공격가능시나리오 단계별 세부 내용

단계	세부내용
Step 1	공격자가 외부에 존재하는 발전기에 물리적인 접근을 통해 컨트롤러에 악성코드 감염
Step 2	발전기는 링 형 네트워크망으로 구성되어 있으며, 해당 네트워크의 구조적 특성으로 인해 감염된 악성코드를 다른 발전기로 전파
Step 3	공격자는 풍력발전 단지 내 모든 발전기들에 대한 제어권 탈취 및 발전기의 오작동 유발 가능

[그림 6]을 통한 파급효과는 다음과 같다.

- 발전기 제어권 탈취를 통한 시스템 파괴 및 오작동 유발
- 감염된 발전기의 악성코드 전파를 통한 피해 확산

V. 대응방안

본 논문에서는 Ⅲ,Ⅳ장을 통하여 풍력발전 제어시스템의 보안위협 및 공격 시나리오별 파급효과에 대해 정리하였고, 본 장에서는 이에 대한 대응방안을 제안한다.

5.1 기술적 대응 방안

- 네트워크 간의 격리를 구현하여 시스템간의 위협 전파 방지
- 보안장비(방화벽, IPS 등)를 이용하여 네트워크 보안 구조 강화
- HMI의 최신 윈도우 운영체제 업데이트 적용
- 지속적인 보안패치 적용
- 비인가 어플리케이션이 구동되는 장치들을 네트워크에서 분리 및 격리
- 정기적인 보안 점검을 통한 침해사고 예방

5.2 물리적 대응 방안

- 물리적 접근 보안을 위한 안티템퍼링 기술 구현
- 풍력발전기 내부 비인가자의 접근 통제 강화
- 내부(제어시스템)와 외부간(인터넷) 물리적 망 분리

VI. 결론 및 향후연구방향

본 논문에서는 풍력발전 제어시스템의 사이버 보안 취약점 분석 및 공격가능시나리오를 도출하고 그에 따른 대응방안을 제시하였다. 하지만, 본 논문에서 제시한 대응방안은 논리적인 측면이며, 실제 국내에 적용된 풍력발전 제어시스템에 대한

직접적인 취약점 분석에 따른 사이버보안 개선 방안을 제시하지 못한 한계점이 존재한다.

따라서, 향후 연구로는 현재 운영 및 개발 중인 풍력발전 제어시스템에 대한 직접적인 사이버보안 취약점 평가 및 테스트를 통한 사이버보안 개선 방안에 대한 연구가 진행되어야 한다.

[논문사사]

본 연구는 2018년도 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 과제입니다. (No. 20162220200010)

[참고문헌]

[1] 황정환, "최근 국내 풍력산업 변화와 시사점", 산업기술리서치센터, 이슈브리프, 2017.6.19.

[2] 2016년 산업통상자원위원회 국회의원 김정훈 의원실 국정감사 보도자료.

[3] Black Hat USA 2017 - Jason Staggs, Adventures in Attacking Wind Farm Control Networks.

[4] DEFCON 25 conference - Jason Staggs, breaking wind: adventures hacking wind farm control networks.

[5] Apurva Mohan, Himanshu Khurana. Implementing Cyber Security Requirements and Mechanisms in Mcrogrids. 9th International Conference on Critical Infrastructure Protection (ICCIP), Mar 2015.

[6] Anibal Sanjab, Walid Saad, Ismail Guvenc, Arif Sarwat, and Saroj Biswas. Smart Grid Security: Threats, Challenges, and Solutions. ARXIV, June 2016.

[7] Hacker Machine Interface : The State of SCADA HMI Vulnerabilities (Trend Micro, 2017).

[8] YOKOGAWA FAST/TOOLS SCADA and Enterprise Automation Solution (EAS) General Specifications.

산업제어시스템 보호를 위한 ICS DPI Firwall 개발†

노권수*, 한상헌*, 박혜용*, 김기현*††
*㈜앤앤에스피 부설연구소

Development ICS DPI Firewall to Protect Industrial Control System

Kwon Su Ro*, Sang Heon Han*, Hye Yong Park*, Ki-Hyun Kim*
*R&D Center, NNSP Co., Ltd.

요 약

시리얼 통신의 필드버스로 폐쇄적으로 운영되던 산업제어망 환경이 이더넷 기반으로 변화하고 스마트공장과 같이 본사 등 외부망과 연결되면서 방화벽과 같은 경계 보안이 필요하지만 일반 IT 방화벽은 산업용 이더넷 프로토콜에 대한 필터링을 제공하지 못한다. 본 논문에서 Ethernet/IP(CIP), Profinet, Modbus, DNP3 등 다양한 산업용 이더넷 프로토콜을 분석하고 DPI 기반의 ICS 방화벽을 개발하였다. 이더넷 프로토콜별 세부 Function Code를 알지 못하는 관리자를 위해 읽기, 쓰기, 읽기/쓰기별로 Function Code를 분류하여 보다 쉽게 규칙을 적용할 수 있도록 개발하였으며 ICS 방화벽과 일반 IT 방화벽을 비교 시험하여 본 논문에서 개발한 ICS 방화벽이 산업제어시스템 환경에 보다 효율적으로 사용될 수 있음을 검증하였다.

I. 서론

스마트공장과 같은 ICS(Industrial Control System) 환경에서는 IT 환경과 달리 필드버스(Fieldbus), 산업용 이더넷(Industrial Ethernet) 등 산업용 프로토콜이 사용된다.

산업용 프로토콜은 오래전부터 생산에 필요한 각종 장비/설비(Sensor, Actuator, Control Device 등)들의 운영 및 운전이 이루어지는 현장에서 데이터를 전송하기 위해 디지털 직렬 통신망으로 다양한 필드버스들이 사용되었다.

산업 현장의 제어기기(PLC)의 Master & Slave 사이 통신에 인터넷 통신 개념이 도입되면서 2006년 ISO TC 184 SC5 전문위원회에서 ISO 15745 Open Systems Application Integration Frameworks의 Part 4인 Ethernet-based Control System에서 규격이 제정되면서 산업용 이더넷(Industrial Ethernet)을 사용하게 되었다.

시리얼 통신의 필드버스로 폐쇄적으로 운영되던 산업제어망 환경이 이더넷 기반으로 변화하고 스마트공장과 같이 본사 등 외부망과 연결되면서 방화벽과 같은 경계 보안이 필요하게 되었다.

IT 방화벽은 IP 헤더와 TCP 헤더의 네트워크 정보를 기반으로 필터링 기능을 수행하지만 응용계층에서 산업용 이더넷 프로토콜 헤더를 가지고 있는 ICS 환경에 적용하기에는 한계가 있다.

본 논문에서는 다양한 산업용 이더넷 프로토콜을 분석하고 ICS 환경에 적용하기 위한 DPI 기반의 산업용 방화벽을 설계하고 개발한다.

II. 산업용 이더넷 프로토콜 고찰

본 논문에서는 산업용 프로토콜에서 시리얼

† 본 논문은 중소벤처기업부의 재원으로 지원을 받아 수행된 “안전한 스마트팩토리 연계를 위한 산업용 통합보안장치 개발” 사업의 연구결과입니다.
†† 교신저자 : khkim@nnsp.co.kr

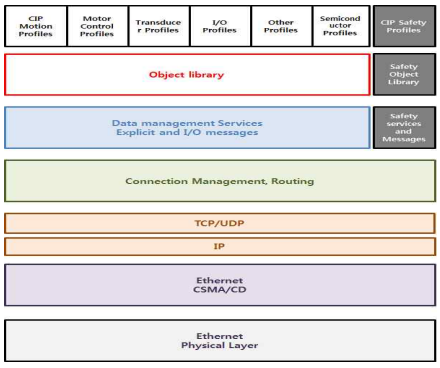
통신으로 사용하는 필드버스는 제외하고 이더넷 환경에서 사용되는 산업용 이더넷 프로토콜을 분석하고 경계 보안을 위한 산업용 방화벽을 설계하고 개발한다.

Ethernet/IP(CIP), Profinet, Modbus 등 산업용 이더넷은 국제표준으로 EC 61158과 IEC 61784에 정의되어 있으며 국내 표준에서도 이를 참조하고 있다.

본 논문에서는 스마트공장 표준으로 많이 사용되고 있는 EtnerNet/IP과 Profinet, 산업제어 시스템 전반에서 사용되고 있는 Modbus-TCP, 전력제어에 사용되고 있는 DNP3에 대한 산업용 방화벽을 개발하기 위해 해당 프로토콜을 분석한다. 주요 산업용 이더넷 프로토콜 별 특징과 보안 대응에 분석하면 다음과 같다[1].

2.1 EtherNet/IP-CIP 분석

EtherNet/IP-CIP는 ODVA에서 산업자동화를 위해서 만든 산업제어용 프로토콜중 이더넷을 기반으로 운용되는 프로토콜이다[2]. CIP는 두 가지 접속 방식을 사용한다. explicit messages는 TCP를 이용하여 요청-응답방식으로 데이터가 전송된다. implicit messages 는 UDP를 사용하며 주요 데이터 전송을 위해서 사용되며 멀티 캐스트방식을 이용하여 데이터를 전달한다[6]. IP-CIP는 별도의 보안이 고려되어 있지 않고 이더넷이 가지는 보안취약점을 안고 있다. 또 프로토콜 특성상 멀티캐스트와 실시간 응답을 요구하는 프로토콜 특성상 암호 처리는 제한적이다.

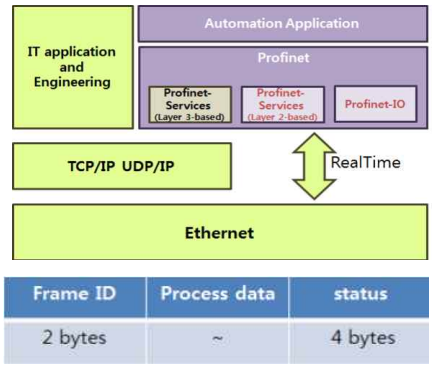


command	length	Session handle	Status	Sender context	options	Command specific data
2 bytes	2 bytes	2 bytes	2 bytes	8 bytes	4 bytes	~

(그림 1) IP-CIP 구조도

2.2 Profinet 분석

Profinet은 물리계층을 Profibus가 주력으로 사용하는 RS485 시리얼 대신 이더넷에 맞춰진 프로토콜이다[3]. 속도와 용도에 따라서 3개의 프로토콜이 정의되어 있다[7]. profibus는 일반적으로 토큰을 기반으로 동작하며 프로토콜 자체의 보안 기능이 결여되어서 트래픽 주입이나 서비스 거부 공격에 취약하다. 프로토콜내에서 인증이나 보안이 부족하므로 시스템의 가용성과 운용 안정성을 확보하기 위해서는 DMZ나 VLAN을 이용하여 네트워크를 분리하고 IT방식을 이용한 암호화통신의 이용 그리고 네트워크 감시를 통한 미인증 혹은 비정상 트래픽에 대한 감시를 강화해야 한다.



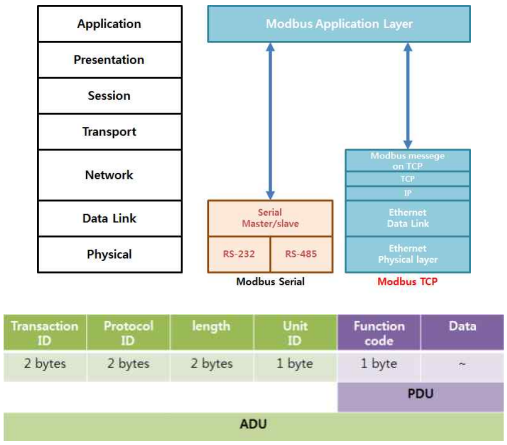
(그림 2) Profinet 구조도

2.3 Modbus 분석

Modbus는 1979년에 산업 제어용 프로토콜로 PLC와 상호 작용하기 위해서 개발되었다[8].가장 널리 사용되는 산업용 프로토콜 중 하나로 응용 계층에 위치하고 있으며 시리얼을 비롯한 다양한 물리적 매체에서 동작할 수 있다. Modbus-TCP 프로토콜은 TCP 프로토콜에 영향받지 않도록 구현되며 이전 프로토콜과의 호환성을 위해서 추가적인 보안 특성은 고려되지 않았다[5].

응용 계층에서 동작하는 시스템으로 Modbus는 보안적 특성은 고려되지 않았다. 주소와 기능코드는 프로토콜에 공개되어 노출되어 있고 동작상에서 암호화정보도 지원하지 않는다. 시리얼의 경우 브로드캐스트가 가능해서 DoS공격에도 취약하다. 이 때문에 Modbus를 보호하기 위해서는 트래픽 모니터링을 통해서

특정 명령어를 가진 데이터의 처리 빈도와 내용을 확인하는 과정이 필요하다.

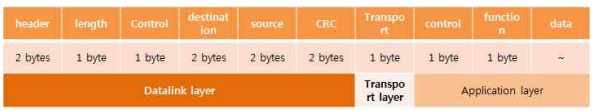


(그림 3) Modbus-TCP 구조도

2.4 DNP3 분석

1993년에 개발된 통신 프로토콜로 북미의 전력부분에서 광범위하게 사용되고 있다. 프로토콜은 총 3개 계층으로 구분되어 있지만 프로토콜 표준 7계층과 직접적으로 관련은 적다.[9]

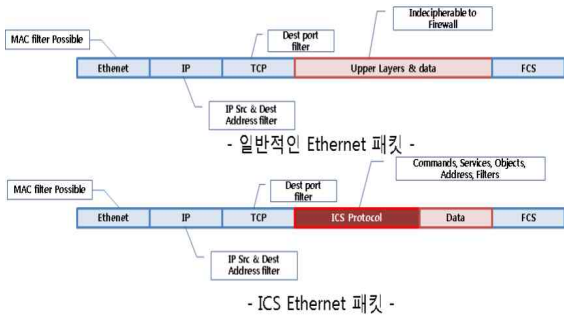
DNP3는 시스템의 이용성을 극대화하려 설계되었기 때문에 신뢰성이나 데이터 무결성 관련 내용은 부족하다. 프로토콜내에서 CRC로 데이터를 검증할 수 있지만 CRC 계산방식은 이미 공개되어 외부 공격에 취약하다. 이에 대해서 DNP3측은 secureDNP라고 하는 보완된 프로토콜을 추가했다[4]. 이 표준은 요청-응답을 기반으로 하는 방식이고 인증이 필요한 명령에 대해서는 인증요청이 해결되지 않으면 처리를 지연시킨다. 이 보완 프로토콜은 사용자 인증과 메시지의 변조 등을 막을 수 있지만 처리 지연과 네트워크 부하를 함께 수반한다.



(그림 4) DNP3 구조도

III. DPI 기반 ICS 방화벽 설계 및 개발

ICS 패킷의 대부분은 프로토콜의 동작 목적에 따라서 각 계층이 구분되어 있고 각각의 구조에 대응하는 데이터가 다르기 때문에 이더넷 환경에서는 이질적으로 동작해야 하는 것 처럼 보이지만 실제의 운용은 대부분 정상적으로 이루어진다. 실 시스템의 운용은 TCP/IP 시스템 위에 구축되어 ICS프로토콜을 운용하기 위해서는 프로토콜 자체를 네트워크의 응용계층에 올려서 사용하는 방식을 취하고 있다. 이러한 이유로 ICS 패킷에 대한 분석을 위해서는 Ethernet 패킷의 일반적인 구조를 감안하고 다시 한번 ICS 프로토콜에 맞춰서 검사하는 DPI(Deep packet Inspection) 기반의 검사과정이 이루어지도록 설계하였다.

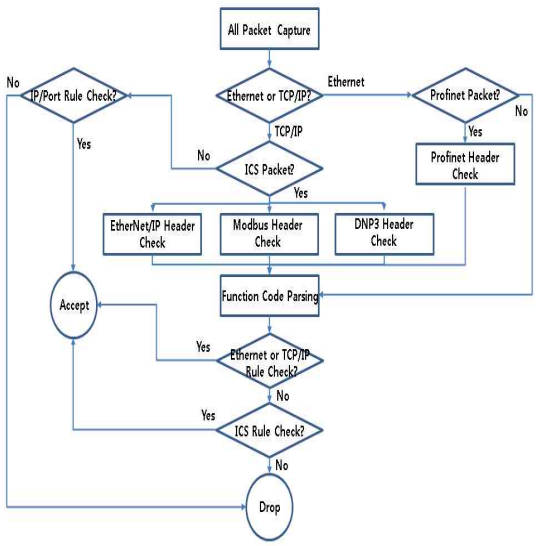


(그림 5) 이더넷 패킷과 ICS 패킷의 분석[10]

3.1 DPI 기반의 ICS 방화벽 설계

EtherNet/IP, Modebus-TCP, DNP3 등은 TCP Layer(4계층)에서 동작하지만 Profinet과 같은 산업용 이더넷은 Ethernet Layer(2계층)에서 동작한다.

다음은 DPI 기반의 ICS 방화벽의 플로우 차트를 나타내고 있다.



(그림 6) DPI 기반 ICS 방화벽 설계

본 논문에서는 TCP Layer(4계층)에서 동작하는 산업용 이더넷과 Ethernet Layer(2계층)에서 동작하는 산업용 이더넷을 모두 수용할 수 있도록 DPI 기반의 ICS 방화벽을 설계하였다.

ICS 방화벽은 DPI 기반으로 동작하며 방화벽으로 들어와서 나가는 모든 패킷을 검사한다.

먼저 해당 패킷이 Ethernet 패킷인지 TCP/IP 패킷인지 확인한다. Ethernet 패킷일 경우 Profinet 패킷 필터링과정을 별도로 수행한다.

TCP/IP 패킷일 경우 일반 IT 패킷인지 ICS 패킷인지 확인한다. 일반 IT 패킷인 경우 IP와 Port에 대한 인가/거부 규칙에 따라 필터링 과정을 수행한다.

ICS 패킷인 경우 EtherNet/IP, Modbus, DNP3 등 산업용 이더넷 프로토콜별로 헤더의 필드 구성 및 필드 값을 검사하여 Malformed Data와 Invalid Data를 패킷을 차단한다.

본 논문에서는 다양한 산업용 이더넷 프로토콜에 공통적으로 적용할 수 있는 ACL 규칙을 사용하고 있으며 이를 위하여 EtherNet/IP, Modbus, DNP3, Profinet 패킷의 헤더 정보에서 Function Code(명령어)를 파싱하고 Rule의 Action 값에 따라 필터링 대상 패킷을 Accept 또는 Drop 한다.

3.2 DPI 기반의 ICS 방화벽 개발

개발된 ICS 방화벽은 일반 IT 프로토콜에 대한 IP/Port 필터링과 TCP/IP를 사용하는 이더넷 프로토콜 필터링을 위해 IP 보안정책으로 개발되었으며 2계층에서 동작하는 이더넷 프로토콜 필터링을 MAC 보안정책으로 개발하였다.

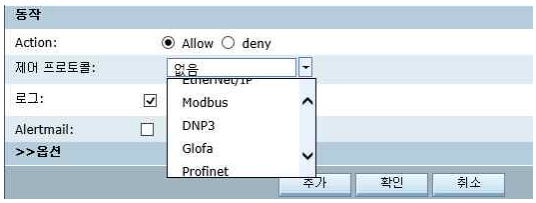


(그림 7) IP 보안정책

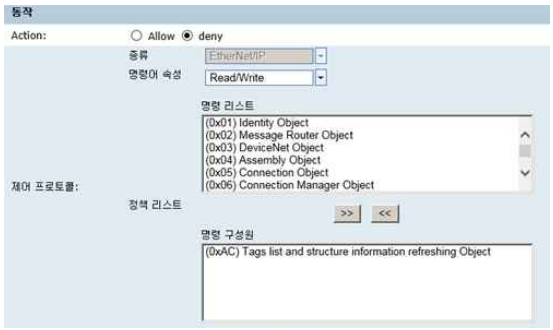


(그림 8) MAC 보안정책

대부분 산업제어시스템 관리자들이 프로토콜별 세부적인 Function Code까지 알지 못하므로 관리자들의 정책 설정의 편리성을 위하여 해당 프로토콜을 선택하고 Function Code를 읽기, 쓰기, 읽기/쓰기로 구분하여 ACL Rule을 제공하도록 구현하였다.



(그림 9) 이더넷 프로토콜 선택 예



(그림 10) EtherNet/IP 정책 구성 예

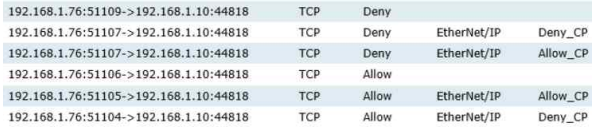
3.3 DPI 기반의 ICS 방화벽 시험 및 고찰

개발된 DPI 기반 ICS 방화벽에 대하여 다음과 같은 패킷을 전송하고 패킷 필터링 여부를 시험하였다.

[표 1] 필터링 테스트 패킷 종류

	Rule 유형	패킷 종류
1	비인가 IP/PORT	일반 패킷
2		인가 ICS 명령 패킷
3		비인가 ICS 명령 패킷
4	인가 IP/PORT	일반 패킷
5		인가 ICS 명령 패킷
6		비인가 ICS 명령 패킷

상기 표의 Rule 순서에 따라 테스트한 결과는 다음과 같다.



(그림 11) ICS 방화벽 테스트 결과

본 논문에서 개발한 ICS 방화벽과 일반 IT 방화벽을 비교하면 다음과 같다.

[표 2] 본 논문과 IT 방화벽 기능 비교

구분	본 논문	IT 방화벽
IP 및 Port 필터링	○	○
산업용 이더넷 MAC 필터링	○	X
산업용 이더넷 헤더 필터링	○	X
제어명령어 필터링	○	X

일반 IT 방화벽은 IP/Port에 기반한 필터링 기능을 제공하지만 본 논문에서 개발한 ICS 방화벽은 산업용 이더넷 MAC 필터링, 산업용 이더넷 헤더 필터링, 제어명령어 필터링 등 산업제어시스템 환경에 적합한 다양한 필터링 기능을 제공하고 있다.

IV. 결론

본 논문에서는 EtherNet/IP, Profinet, Modbus, DNP3 등 산업용 이더넷 프로토콜을 분석하고 DPI 기반의 ICS 방화벽을 개발하였다.

DPI 기반의 ICS 방화벽은 IP/PORT 기반의 필터링 기능을 제공하는 IT 방화벽과 달리 Function Code(제어명령어) 기반의 필터링을 추가로 제공함으로써 산업제어시스템 보호에 적합하도록 개발되었다.

또한 이더넷 프로토콜별 세부 Function Code를 알지 못하는 관리자를 위해 읽기, 쓰기, 읽기/쓰기별로 Function Code를 분류하여 보다 쉽게 규칙을 적용할 수 있도록 개발하였다.

DPI 기반의 ICS 방화벽과 일반 IT 방화벽을 비교 시험하여 본 논문에서 개발한 ICS 방화벽이 산업제어시스템 환경에 보다 효율적으로 사용될 수 있음을 검증하였다.

향후 EtherNet/IP, Profinet, Modbus, DNP3뿐만 아니라 EtherCat, CC-Link, SERCOS 등 다양한 이더넷 프로토콜로 ICS 방화벽을 기능을 확장할 예정이다.

[참고문헌]

[1] Miguel Herrero Collantes. Antonio Lopez Padilla, "Protocols and network security in ICS infrastructures", incibe, 2015.

[2] https://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00138R6_Tech-Series-EtherNetIP.pdf

[3] https://us.profinet.com/technology/profinet/

[4] Grant Gilchrist, "Secure Authentication for DNP3", IEEE, 2008.

[5] http://www.modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf

[6] IEC 61784-5-2, Industrial communication networks : Installation of fieldbuses Installation profiles for CIP (ControlNet, EtherNet/IP, DeviceNet)

[7] IEC 61784-5-3, Industrial communication networks : Installation of fieldbuses Installation profiles for PROFIBUS/PROFINET

[8] IEC 61784-5-15, Industrial communication networks : Installation of fieldbuses Installation profiles for Modbus-TCP

[9] IEEE 1815-2012, IEEE Standard for Electric Power Systems Communications -Distributed Network Protocol (DNP3)

[10] Eric Byres, Erik Schweigert, Michael Thomas. "Securing EtherNet/IP Using DPI firewall Technology", ODVA conference, 2014.

SCADA 프로토콜 보안위협 및 보안요구사항 분석

위한샘, 이옥연*

*국민대학교 금융정보보안학과

Analysis of SCADA protocol security requirements

Hansaem Wi , Okyeon Yi*

*Dept, of Financial Information Security, Kookmin University

요 약

산업제어시스템은 현장장치를 제어, 감시하기 위해 설계된 시스템으로써 국가의 기반시설인 가스, 원자력, 상하수도 등의 시스템에서 사용되고 있다. 산업제어시스템은 외부에 대해 폐쇄적인 구조로 설계되었기 때문에 산업제어시스템에서 제어, 감시 데이터 통신에 사용되는 SCADA 프로토콜 역시 보안에 관한 규격 없이 설계되었다. 따라서 본 논문에서는 SCADA 프로토콜에 존재하는 보안 취약점으로 인해 발생할 수 있는 보안위협과 보안위협에 대응하기 위한 SCADA 프로토콜 보안 요구사항을 분석한다.

I. 서론

산업제어시스템은 산업시설의 공정을 효율적으로 운영하기 위하여 설계된 시스템이다. 산업제어시스템에 설치된 제어 S/W, 제어 H/W간의 데이터 통신을 수행하여 산업현장의 현장장치들을 제어하고 장치들의 상태를 감시한다. 산업제어시스템은 보다 효율적인 공정 운영을 위해 IT 시스템을 도입하였고 시스템 구조의 변화로 인해 기존에 유지하던 폐쇄적인 구조에서 점차 개방형 구조로 변화하고 있다. [2]

IT 시스템의 도입으로 인해 산업제어시스템 자체의 운영 효율성이 증가하였지만 이와 더불어 IT 시스템에 존재하던 보안 취약성이 산업제어시스템에도 존재하게 되는 상황이 되었다. 기존의 폐쇄적인 구조와는 달리 IT시스템을 사용함으로써 외부와의 연결점이 증가하였고 제어시스템의 규모 또한 확장되었다. 이에 대해 산업제어시스템은 더 이상 폐쇄적인 구조와 물리적인 보안만으로는 시스템의 자원, 데이터 보안을 유지하기가 어려운 상황이 되었다.

산업제어시스템은 보통의 IT시스템에 비해 가지고 있는 자원의 특수성과 규모 그리고 인명과 관련된 시설 요소들이 많기 때문에 보안사고가 발생 했을 때 감수해야하는 경제적, 인명피해 규모 역시 IT시스템에 비해 크다. 따라서 변화하고 있는 산업제어시스템에서 생겨난 보안 취약성에 대한 보안요구사항과 보안요구사항이 반영된 보안 솔루션이 필수적이다.

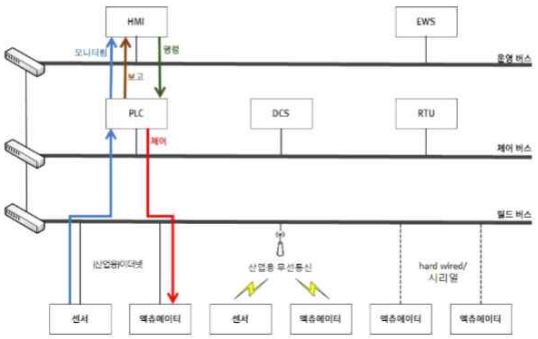
본 논문에서는 SCADA 프로토콜의 취약점, 프로토콜의 취약점과 관련된 보안사고에 대해 분석하고 [4]에서 수행한 SCADA 프로토콜의 데이터 보안 취약성을 이용한 모의공격에 대해 소개한 후 산업제어시스템에서의 통신 프로토콜 데이터에 대한 보안을 제공하기 위해 요구되는 보안 요구사항을 분석한다.

II. 본론

본 장에서는 산업제어시스템의 네트워크 구조와 시스템 내의 제어 S/W, 제어 H/W, 현장장치간의 제어, 감시 데이터 통신 과정을 살펴보고 SCADA 프로토콜의 보안 취약성으로 인해 데이터 통신 시 발생할 수 있는 보안 위협, 보안사고 사례를 설명한다. 끝으로 통신 데이터에 대한 보안 요구사항을 제시하며 장을 마무리 한다.

2.1 산업제어시스템 네트워크 구조 [1]

산업제어시스템은 운영계층, 제어계층, 현장장치 계층 총 3계층으로 구성된다. [그림 1]은 산업제어시스템의 각 계층이 이루고 있는 네트워크를 나타내는 그림이다.



[그림 1] 산업제어시스템 네트워크 구성

운영계층은 산업제어시스템 관리자가 산업현장을 모니터링하거나 현장 장치로 제어 명령을 전송한다. 운영계층이 포함하는 요소로는 HMI(Human Machine Interface), MMI(Man Machine Interface), EWS(Engineering Workstation)등의 제어 S/W들이 있으며 제어 명령을 제어 H/W와 현장장치로 전송하거나 제어, 감시 데이터 포맷을 생성하는 역할을 담당한다.

제어계층은 운영계층의 제어 명령을 전달받아 산업현장에 있는 액추에이터, 센서 등을 제어하고 제어에 대한 결과를 운영계층의 제어 S/W에게 보고하는 역할을 한다. 또한 현장장치들의 상태 정보를 주기적으로 수집하여 운영계층에 전달하여 운영계층의 관리자가 현장장치들의 상태를 모니터링 할 수 있도록 한다. 제어계층이 포함하고 있는 요소로는 PLC(Programmable Logic Controller), DCS(Distributed Control System), RTU(Remote Terminal Unit)등의 제어 H/W들이 있다. 운영계층에 위치한 제어 S/W와 제어계층에 위치한 제어 H/W 간 제어, 감시에 관련된 데이터를 통신 할 때에는 산업제어프로토콜 또는 SCADA 프로토콜이 사용된다.

현장장치 계층은 센서, 액추에이터 등의 산업현장에서 현장의 상태 값을 수집하거나 현장에서 공정을 위해 동작하는 현장장치들을 포함한다. 운영계층의 관리자는 제어 S/W를 이용하여 현장 장치로 제어명령 또는 상태 값 수집 요청을 전송하고 이를 전달 받은 제어 H/W는 연결된 현장 장치들과의 통신을 통해 현장장치의 제어 결과, 수집된 상태 값 데이터를 운영계층의 제어 S/W가 설치된 장치로 전송한다.

2.2 SCADA 프로토콜 취약성

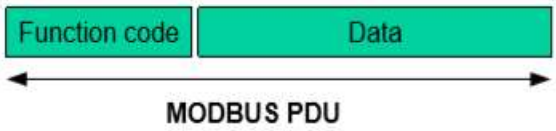
산업제어시스템은 설계 시 폐쇄적인 구조 아래 운영되도록 설계되었다. 또한 제어시스템 내에서 제어, 감시 데이터 전송을 위해 사용되는 SCADA 프로토콜 역시 보안에 대한 규격이 고려되지 않은 채 설계되었다. MODBUS, DNP 3.0은 우리나라를 비롯한 해외의 여러 산업제어시스템에서 사용되고 있는 SCADA 프로토콜이다. 본 절에서는 MODBUS, DNP3의 취약점에 대해 진행되었던 연구들을 소개함으로써 현재 산업제어시스템에서 사용되고 있는 SCADA 프로토콜들에 대한 보안 취약점을 도출한다.

2.2.1 MODBUS 취약점 및 보안위협

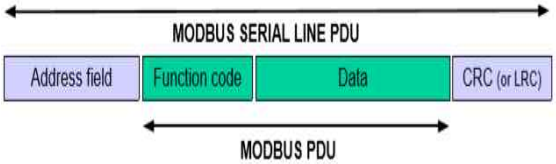
MODBUS는 1979년 자사의 PLC 제어를 위해 modicon에서 개발 하였으며 이 후 de facto 표준으로 제정되어 현재까지 산업제어시스템에서 널리 쓰이고 있는 SCADA 프로토콜이다. MODBUS의 사용 형태는 통신 방식에 따라 크게 시리얼 라인에서 사용되는 MODBUS over serial line과 Ethernet/IP 기반으로 동작하는 MODBUS/TCP가 있다. [8]

MODBUS 프로토콜을 사용함으로써 발생하는 데이터 보안 취약점은 크게 통신 3가지로

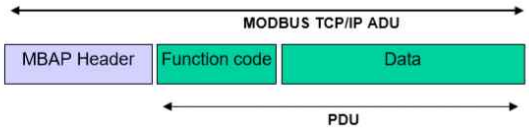
분류할 수 있다. 먼저 데이터 통신 이전 장치 간 상호 인증이 진행되지 않은 상태로 데이터 통신이 이루지는 것이다. 다음 [그림 2], [그림 3], [그림 4]는 순서대로 MODBUS 어플리케이션 프로토콜 데이터 포맷, MODBUS over serial line과 MODBUS/TCP의 프로토콜 데이터 프레임을 나타낸다.



[그림 2] MODBUS 어플리케이션 프로토콜 데이터 포맷



[그림 3] MODBUS over serial line 데이터 프레임



[그림 4] MODBUS/TCP 데이터 프레임

시리얼 라인을 사용한 MODBUS 데이터 프레임과 Ethernet/IP를 사용한 MODBUS/TCP 데이터 프레임 모두 데이터를 전송하는 주체에 대한 인증과 관련된 데이터 필드가 존재하지 않는다. 장치를 인식할 수 있는 필드는 [그림 3]의 주소필드와 [그림 4]의 MBAP Header에 존재하는 Unit Identifier가 있지만 이는 상호간에 암호학적인 인증과정을 통해 나눠가진 비밀정보가 아니라 운영계층에서 제어, 감시 데이터 통신을 구현하는 프로그램으로 할당한 ID 값이다. 통신 이전에 암호학적인 식별 및 인증과정을 거치지 않고 통신을 진행할 경우 관련 연구로 진행된 [4]에서 볼 수 있듯이 MODBUS 프로토콜을 사용하는 환경의 장치들의 통신 간 중간자 공격을 수행하는 기기를 구현하여 데이터 위/변조, 재전송 공격이 가능함을 볼 수 있다. 이는 MODBUS를 장치 간 데이터 통신에 사용하는 산업제어시스템의 가용성에 큰 영향을 미칠 수 있는 보안 위협이다.

두 번째로 MODBUS는 데이터 기밀성을 보장하지 않는다. 암호알고리즘을 이용한 암호화를 수행하지 않기 때문에 데이터 스니핑을 통하여 데이터 유출이 가능하고 평문 값을 모두 확인 할 수 있기 때문에 공격자가 이를 분석하여 2차적 공격을 수행할 수 있다. 이에 대해 관련 연구인 [4]에서 데이터 유출 및 유출된 데이터를 분석하여 공격이 가능하였다.

세 번째로 MODBUS는 데이터 무결성에 대한 검증을 수행하지 않는다. [그림 2]에 있는 데이터 전송 시 오류를 검출하기 위한 CRC(Cyclic Redundancy Check), LRC(Longitudinal Redundancy Check)만으로는 데이터를 전송한 출처와 데이터 위/변조에 대한 무결성을 모두 검증할 수 없다. 이 역시 관련 연구인 [4]에서 수행한 모의공격을 통해 공격자가 임의로 위조한 데이터를 PLC로 전송하여 현장장치를 제어하고 HMI가 PLC로 전송한 제어명령을 가로챈 공격자의 규칙대로 변조하여 CRC 값을 다시 계산하는 방식으로 데이터를 재생성하여 오작동 시키는 것이 가능하였다

2.2.2 DNP3 취약점 및 보안위협 [5]

DNP3는 1993년에 상세 규격이 정의되어 2003년 기준으로 전 세계 사용 비율이 88%에 이르는 널리 쓰이는 de facto 표준 SCADA 프로토콜이다. 사용하는 통신 종류에 따라 시리얼 통신에서의 DNP3, Ethernet/IP 기반으로 한 DNP3 TCP 버전이 있다.

DNP3 프로토콜 역시 MODBUS와 마찬가지로 프로토콜 설계상의 장치 간 상호인증과정, 데이터 기밀성 제공, 데이터 무결성 검증 등의 과정이 존재하지 않는다.

[5]에서 수행한 DNP3 프로토콜의 취약점을 이용한 공격 실험 결과에 따르면 DNP3 프로토콜이 가지고 있는 데이터 보안 취약점에 대한

공격 12가지를 시도하였고 이 중 5개 항목에 대한 취약점 공격이 가능하였다. 실험 환경은 운영계층과 제어계층 사이에 DNP3의 패킷을 생성하고 수집할 수 있는 시뮬레이터 장치를 연결하고 공격실험을 수행하였다.

먼저 인증되지 않은 공격자가 제어시스템의 운영계층에 위치한 제어서버 혹은 제어 시스템 운영자가 처리할 수 없을 정도의 다량의 정상적인 응답 패킷을 전송하여 가용성을 해치는 공격을 수행하였다. 이는 DNP3 프로토콜 설계 상의 인증과정이 없기 때문에 네트워크상에 존재할 수 있는 임의의 공격자의 패킷을 정상적인 패킷으로 인식하는 취약점을 이용한 것이다.

두 번째로 시뮬레이터 장치를 이용하여 현장장치의 상태 값을 수집하는 것이 가능하였다. 이는 DNP3 설계 상 데이터 기밀성 제공에 대한 부분이 결여되어 있기 때문에 공격자가 네트워크상에 장치 간 통신되는 데이터의 평문을 획득할 수 있다는 취약점을 이용한 것이다.

세 번째로 시뮬레이터 장치를 이용하여 현장장치의 상태를 변경하고 제어명령 데이터에 설정된 현장장치의 ID값을 변경하여 제어서버에서 변경하려고 했던 현장장치와는 다른 장치의 상태 값을 변경시키는 공격이 가능하였다.

본 장에서는 MODBUS, DNP3 이외에도 SCADA 프로토콜은 공통적으로 인증과정, 데이터 무결성 검증, 데이터 기밀성, 가용성에 대한 확인 절차 등이 상세규격에 포함되지 않은 상태이며 해당 보안기능의 부재로 인한 취약점을 살펴보았다. 또한 2.2.1, 2.2.2절에서 소개한 보안 위협을 이용한 모의공격 실험을 통하여 실제 산업현장을 대상으로 한 공격의 가능성을 확인하였다. SCADA 프로토콜의 공통적인 데이터 보안 위협과 관련된 보안기능은 [표 1]과 같이 정리할 수 있다.

[표 1] SCADA 프로토콜 데이터 보안 취약점

항목	설명
제어시스템 서비스 방해 (무결성, 가용성)	인증되지 않은 공격자는 고의적으로 다량의 정상적인 패킷이 발생할 수 있고 운영계층, 제어계층의 장치들이 처리하기 어려울 정도의 패킷이 발생되었을 시 시스템의 가용성에 큰 영향을 끼친다.
데이터 유출 및 분석 (기밀성)	데이터 기밀성에 대한 부재로 인하여 네트워크상의 공격자에게 제어 , 감시 데이터의 평문이 유출 될 수 있고 공격자는 이를 분석하여 2차적인 공격에 활용할 수 있다.
데이터 위/변조 (무결성, 가용성)	유출된 제어, 감시 데이터를 활용하여 공격자는 원하는 데이터를 위조 또는 스니핑 된 데이터를 변조하여 현장장치의 상태 값을 임의적으로 변경할 수 있다.
데이터 재사용 (무결성, 가용성)	공격자는 유출 후 저장된 제어, 감시데이터를 재사용하여 현장장치의 상태 값을 변경시킬 수 있다.

DNP3와 같이 인증과정의 사용을 권고사항으로 추가한 SCADA 프로토콜도 존재하지만 이마저도 보안기능 중 일부만을 권고사항으로 추가한 것이며 MODBUS와 같은 경우 보안에 관한 권고사항이나 프로토콜 상세 규격 수정이 이루어지고 있지 않다. 이에 대해 SCADA 프로토콜의 취약점에 대한 보안요구사항이 필수적이다. 2.4절에서는 SCADA 프로토콜의 취약점에 대한 보안위협을 기준으로 한 보안 요구사항을 도출한다.

2.4 SCADA 프로토콜 보안 요구사항

2.3에서 살펴본 SCADA 프로토콜의 데이터 보안 취약점은 인증, 데이터 기밀성, 데이터 무결성, 가용성의 부재로 인하여 생겨난 것이다.

이에 대하여 SCADA 프로토콜에 요구되는 보안 요구사항은 [표 2]과 같다. [1][2]

[표 2] SCADA 프로토콜 데이터 보안 요구사항

항목	설명
장치 식별 및 인증	장치의 신원을 검증하기 위해 서비스 제공 이전에 식별 및 인증 기능을 제공해야 한다.
전송 데이터 무결성	민감한 전송 데이터에 대해 위/변조 야부와 재사용 공격에 대비한 최신성 여부를 확인할 수 있도록 무결성 보장 기능을 제공해야 한다.
전송 데이터 기밀성	민감한 전송 데이터에 대해 기밀성 보장 기능을 제공해야 한다.
통신세션 자동 종료	일대일 통신에 있어 설정 시간을 초과한 세션, 설정시간 동안 미사용중인 세션, 사용목적을 달성한 세션에 대해서는 종료하는 기능을 제공해야 한다.
암호연산	암호연산을 사용하는 경우 안전한 암호 알고리즘 및 암호 키 길이를 사용하여 암호연산이 수행되어야 한다.
암호 키 관리	암호 연산을 위해 사용하는 암호키에 대해 안전한 키 생성/설정/저장/파기 방법을 사용해야 한다.

2.4.1 장치 인증 및 키 일치

통신에 참여하는 장치는 실제 제어, 감시와 관련된 통신이 이루어지기 전 상호 간 인증을 수행하여야 한다. 상호간에 사전에 공유된 키 혹은 인증서를 기반으로 하는 상호 인증을 수행한 뒤 인증이 성공 할 시 통신세션을 생성하고 정해진 세션 시간동안 통신함으로써 제어시스템의 정상적인 장치 이외의 인증되지 않은 장치와의 통신을 방어할 수 있다.

2.4.2 데이터 기밀성

제어, 감시와 관련된 데이터는 산업제어시스템에서 민감한 데이터로 분류 된다. 인증 및 키 일치 과정 이 후 정해진 세션동안 데이터 통신 시 세션 키를 이용한 데이터 암호화를 통하여 데이터 기밀성을 제공함으로써 공격자에 대하여 제어, 감시 데이터의 평문 유출을 방어할 수 있다.

2.4.3 데이터 무결성

제어, 감시와 관련된 데이터는 재사용 여부, 또는 위/변조에 대하여 데이터의 무결성 즉, 데이터의 출처와 위변조 여부 그리고 데이터의 최신 성을 확인해야한다. 이를 통해 데이터 위/변조와 데이터 재사용 공격을 방어할 수 있다.

산업제어시스템은 IT시스템과는 다르게 운영의 연속성이 가장 중요시 된다. 산업제어시스템이 보유하고 있는 자원의 특수성, 규모 그리고 인명과 관련된 요소가 많기 때문에 운영이 중단 되었을 시 일어날 수 있는 경제적, 인명피해가 기존의 IT시스템에 비해 클 수 있기 때문이다. 정보보호의 우선순위 역시 시스템의 가용성이 가장 중요시 된다. [1]

산업제어시스템의 장치의 경우 S/W, H/W의 업데이트 주기는 15~20년으로 IT 시스템의 주기인 3~5년에 비해 매우 길기 때문에 보안을 위한 즉각적인 패치나 교체가 현실적으로 어려운 상황이다. [1] 그렇기 때문에 패치를 부분적으로 진행하여 시스템 전체의 가용성이 받는 피해를 최소화 하거나 기존 제어와 관련된 장치 외부에 따로 보안장비를 설치함으로써 보안 시스템의 도입에 걸리는 시간을 줄이는 방법도 고려해야할 필요가 있다. 즉, 세션의 생명주기,

인증서버의 운영 등의 보안 정책 수립뿐만 아니라 보안 적용 방법에 대한 정책도 수립해야 할 필요가 있다.

III.결론

본 논문에서는 산업제어시스템 내에서 데이터 통신에 중요한 역할을 하는 SCADA 프로토콜의 취약점과 그로 인해 발생할 수 있는 보안 위협을 살펴보았고 보안위협에 대응할 수 있는 보안 요구사항을 도출하였다.

산업제어시스템의 보안 요구사항의 전체적인 항목은 IT 시스템과 크게 다르지 않지만 보안을 적용할 때 가용성을 IT 시스템에 비해 신중하게 고려해야 한다는 차이점을 보였다. 또한 산업제어시스템에 실제적으로 보안이 적용된 S/W 또는 보안기능을 수행하는 보안장비를 도입할 때의 방법에 관한 정책도 고려해야 한다는 결과도 얻을 수 있었다.

[참고문헌]

[1] TTA, “산업제어시스템 보안요구사항”- TTAK.KO-12.0307

[2] NIST SP 800-82r2, “Guide to Industrial Control System(ICS) Security”

[3] NCCIC_ICS-CERT_FY 2016_Annual_Vulnerability_Coordination_Report

[4] 위한샘, 이재훈, 이옥연. "Modbus RTU 프로토콜의 보안 취약점 모의 공격을 통한 산업제어시스템 데이터 보안 연구." 한국통신학회 학술대회논문집, (2018.1): 78-80.

[5] 장문수, 이건희, 김신규, 민병길, 김우년, 서정택.“DNP 제어시스템 프로토콜 취약점 실험.” 보안공학연구논문지, 제 7 권 제 1 호 2010년 2월.

[6] 장지웅, 김휘강. “전력 제어시스템의 시리얼 기반 DNP통신 취약점에 관한 연구.” Journal of The Korea Institute of Information Security & Cryptology VOL.23, NO.6, Dec. 2013

[7] Gabor JAKABOCZKI, Eva ADAMKO. “VULNERABILITIES OF MODBUS RTU PROTOCOL.” ANNALS OF THE ORADEA UNIVERSITY

[8] modbus.org. “MODBUS Application Protocol Specification V1.1b3”

쇼단을 이용한 제어시스템 공격 사례분석 및 대응방안

박현진, 박재용, 김인수, 서정택

순천향대학교 정보보호학과

An Attack Case Analysis Of The Control Systems And Countermeasure Through A Shodan

Hyun Jin Park, Jae Yong Park, In Soo Kim, Jung Taek Seo

Department of Information Security Engineering, Soonchunhyang University.

요 약

최근 제어시스템에 대한 사이버 공격이 지속적으로 증가하고 있지만 이에 대한 제어시스템 보안 관리 및 대응방안 적용은 미흡한 상태이다. 특히 쇼단(Shodan)으로 검색한 정보를 활용하여 공격하는 사례가 증가하고 있다. 제어시스템을 공격하면 제어시스템은 정상적인 동작을 할 수 없게 되고 시민들은 불안감과 혼란이 일어나게 된다. 이에 따라 본 논문에서는 쇼단을 이용한 제어시스템 공격 사례분석과 이에 대한 대응방안을 제시한다.

I. 서론

제어시스템은 기기마다 외부기기 또는 상호간 연결하여 장치에 대한 원격접근과 제어가 가능하고, 다양한 조작 및 명령이 가능할 수 있게 양방향 통신서비스 환경을 만들고 있다. 목적과 사용 환경에 따라 산업제어시스템(ICS, Industrial Control System), 분산제어시스템(DCS, Distributed Control System) 또는 원방감시제어시스템(SCADA, Supervisory Control And Data Acquisition) 이라고 한다[1].

제어시스템에 대한 공격은 통신 체계, 금융체계, 교통체계, 에너지체계가 마비되고 결과적으로 국가혼란사태를 유발하게 된다. 국내의 경우 2009년 7·7 DDoS 공격, 2011년 농협 전산망 사이버 테러, 2013년 3· 20 전산망 장애, 2014년 한수원 해킹 공격 등 제어시스템에 대한 보안 위협은 나날이 증가하고 있다[2]. 이러한 보안위협 중 검색엔진인 쇼단을 이용하여 국내 가스 측정 시스템 정보, 인천국제공항공사 내부정보, 국내 기업 IT 인프라 정보 등이 노출되는 사례가 발생하였다[3][4][5]. 본 논문에서는 이러한 사태에 대응하기 위해 쇼단을 이용한 취약점 공격 사례를 분석하고 취약점 공격으로 인한 피해 분석 및 대응방안을 제시한다.

본 논문은 2절에서 쇼단에 대한 정의와 쇼단 웹 사이트를 이용한 검색 방법을 설명하며, 3절에서 쇼단을 이용하여 찾은 제어시스템, 빌딩시스템, 웹캠 등에 대한 취약점 공격 사례를 분석한다. 4절에서는 3절에서 발견된 취약점 공격으로 발생할 수 있는 피해 범위와 대응방안을 제시하며 마지막 5절에서는 결론과 차후 연구 방안에 대하여 제시하고자 한다.

II. 쇼단(Shodan)

2.1 쇼단의 정의

쇼단과 일반적인 검색엔진의 차이점은 웹사

이트의 정보를 가져오는 것이 아닌 웹캠, 라우터, 발전소, 아이폰, 풍력 발전, 냉장고, 그리고 VoIP 전화기 등 사물 인터넷(IoT, Internet of Things)정보와 제어시스템에 대한 정보를 수집할 수 있는 검색 엔진이다. 쇼단은 웹(Web) 사이트를 기반으로 한 검색을 제공하고 있다[6].

2.2 쇼단 웹 사이트를 이용한 검색 결과

쇼단의 웹 사이트(https://www.shodan.io)로 접속하여 검색엔진에 키워드를 입력하면 해당 키워드를 포함한 장치의 국가와 도시, IP주소, MAC 주소 등 다양한 정보를 표시해준다. 그림 1은 쇼단 웹 사이트에서에서 'CCTV'를 키워드로 입력하여 얻을 수 있는 정보이다.



[그림 1] 쇼단 웹사이트를 이용한 검색 결과

쇼단은 많은 양의 정보를 검색할 수 있지만 웹 사이트에서 검색 시 입력어에 더해서 검색 결과의 범위를 축소시킬 수 있는 필터들을 제공한다. 필터를 이용하여 필요한 키워드만 찾을 수 있다. 표 1은 쇼단에서 사용할 수 있는 필터이다.

필터	설명
city	입력된 키워드를 한정된 도시내로 검색 결과를 보여준다. (ex. cctv city:"Busan")
country	입력된 키워드를 한정된 국가내로 검색 결과를 보여준다. (ex. SCADA country:KR)
geo	지정한 위도/경도 정보를 참고 후, 주변에 있는 검색 결과를 보여준다. (ex. cctv geo:42.9692,-74.1224)
hostname	호스트 네임과 일치하는 검색 결과를 보여준다. (ex. "Server: gws" hostname:google)
net	지정한 Class에 제한하여 검색 결과를 보여준다. (ex. net:216.219.143.0/24)
os	지정한 OS에 관한 검색 결과를 보여준다. (ex. microsoft-iis os:"windows 2008")
port	지정한 포트에 관한 검색 결과를 보여준다. (ex. proftpd port:21)
before/after	지정한 날짜 전/후로 검색 결과를 보여준다. (ex. nginx after:18/01/2012)

[표 1] 쇼단 웹 사이트에서 제공하는 필터[7]

Ⅲ. 쇼단을 이용한 공격 사례분석

3.1 특정 프로토콜의 포트번호를 이용한 산업제어시스템 접속사례

산업제어시스템은 해당 시스템의 제조사 고유의 프로토콜을 사용하는 경우가 많다. 이를 이용한 시스템 접속 과정은 다음과 같다. 먼저 해당 프로토콜이 사용하는 고유의 포트번호를 쇼단에서 검색한다. 이후 해당 포트를 사용하는 장비들의 IP가 검색결과로 나오게 된다. 이를 이용해 해당 IP로 접속하게 되면 취약한 시스템의 경우 해당 서버가 사용하는 PLC나 기타 장비의 정보를 획득할 수 있고, 이를 통해 해당 서버가 어떤 서비스를 제공하는지 알 수 있으며, 해당 사례의 경우 로그인 웹페이지로 접속할 수 있게 되어 있었다. 추가적으로 통상서버

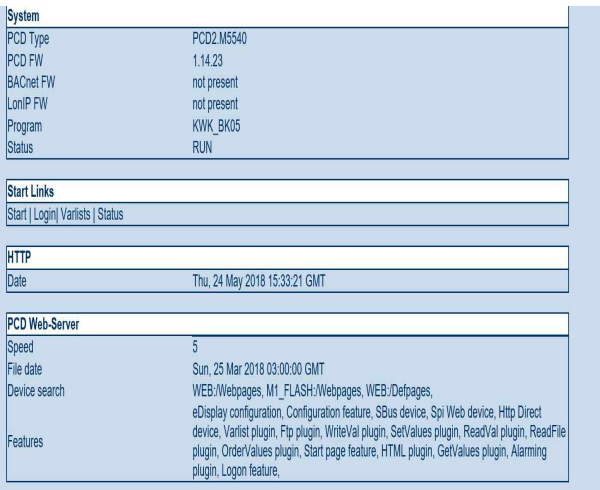
의 경우 여러 번의 접근시도가 요청되면 일정 시간 로그인을 진행할 수 없게 하는 별도의 접근제어가 이루어지는 반면, 해당 사례의 경우 별도의 제어과정이 없어 Brute-Force 공격에 매우 취약한 환경임을 확인할 수 있었다.

3.2 특정 장비 모델명/제조사명을 이용한 장비 접속사례

3.1의 사례처럼 해당 서비스 프로토콜이 사용하는 포트번호로 검색할 수도 있지만, 해당 시스템이 사용하는 장비 모델명이나 해당 장비의 제조사 이름을 통해서도 검색이 가능하다. [그림 3]의 경우 VIVOTEK 사의 웹캠에 접속한 사례인데, 해당 웹캠의 경우 관리자 계정과 비밀번호가 모두 기본 값으로 설정되어 있어 손쉽게 접근이 가능하였다. 카메라를 움직일 수 있을 뿐만 아니라 해당 페이지의 계정관리 및 관리자 계정의 비밀번호 변경도 가능하여, 매우 취약한 상황이었다. 표 2는 웹캠 제조사에서 초기로 설정하는 계정 및 비밀번호이다.

계정 취약점을 가지고 있는 장비들의 경우 초기 관리자 계정과 비밀번호가 admin으로 설정되어 있거나 추측 가능한 경우가 많아 손쉽게 접속이 가능하고, 접속이 성공하면 해당 기기의 접속 계정 관리도 가능해지기 때문에 관리자 계정의 비밀번호를 임의로 변경하거나 삭제할 수 있다.

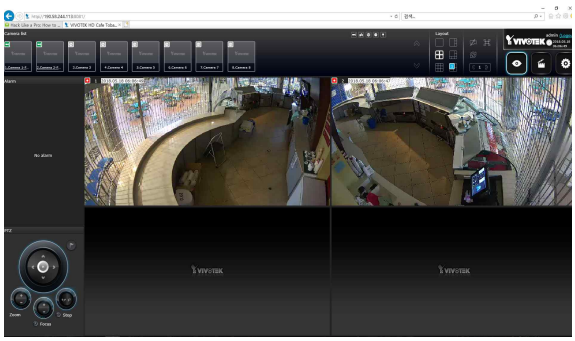
이렇게 되면 해당 장비를 사용하기 위해서는 부득이하게 장비의 재기동절차를 거쳐야하기 때문에 장비가 수집했거나 보유하고 있는 데이터들이 손실될 수 있다.



[그림 2] Modbus가 사용하는 포트를 이용한 제어시스템 웹 서버 접속

웹캠 제조사	초기아이디/비밀번호
ACTi	admin,Admin/123456
Axis(Old)	root/pass
Axis(New)	초기 패스워드 설정 필요
Cisco	admin/admin
Grandstream	admin/admin
IQinVision	root/system
Mobotix	admin/meinsm
Panasonic	admin/12345
삼성전자	root/root or admin/4321
삼성테크윈(Old)	admin/1111111
삼성테크윈(New)	admin/4321
Sony	admin/admin
TRENDnet	admin/admin
Toshiba	root/ikwd
Vivotek	root/<blank>
WebcamXP	admin/<blank>

[표 2] 웹캠 제조사별 초기 관리자 계정/비밀번호[9]



[그림 3] 초기 관리자 계정을 이용한 웹캠 접속

3.3 노출된 IP 주소를 이용한 서버 접속사례

[그림 4]의 경우 Schneider Electric사의 서버를 이용하는 산업제어시스템에 접속한 사례이다. 해당 서버를 SSH 연결을 사용해 접속하였는데, 초기에 설정된 아이디와 비밀번호를 사용해 접속이 가능하였다. 취약점을 가진 많은 서버에 SSH로 접속하게 되면 초기화면에서 관리자 계정의 아이디와 비밀번호가 그대로 노출되어 있으며, 이를 통해 해당 장비에 접속이 가능하였다. 또한 Karn Ganeshen이 공개한 취약점을 이용한 해당 서버의 공격도 가능하였다.[10]



[그림 4] 계정 취약점을 이용한 SSH 접속

Ⅳ. 피해 분석 및 대응방안

4.1 쇼단 검색 결과를 활용한 공격 피해 분석

(1) 산업제어시스템

산업제어시스템의 경우 일반적인 전산 서버와 다르게 운영이 중지되었을 경우 경제적인 피해나 인명 피해가 발생할 수 있다. 특히 다수의 제어시스템의 관리자 계정이 초기 값으로 설정되어 있다. 따라서 해커가 손쉽게 제어시스템의 관리자 권한을 획득하여 취약점을 이용해 시스템의 가동을 중지하는 등 심각한 피해를 발생시킬 수 있고, 전력제어시스템 및 사회 인프라 시설을 운영하는 시스템들은 해킹으로 인해 피해를 입을 경우 해당 시스템과 연계되어 있는 다른 제어시스템에도 영향을 미칠 수 있기 때문에 그 피해는 더 심각할 수 있다.

(2) 빌딩제어시스템

BAS시스템의 경우 산업제어시스템과 마찬가지로 기본값으로 설정된 시스템이 다수 존재했다. 대부분의 BAS시스템이 자동화 되어 있는데 악의적 목적을 가진 공격자가 쇼단을 통해 IP주소, 라우터 등의 정보를 탈취해 공격한다면 전력제어, 배기제어, 출입제어 등의 시스템이 정상적으로 동작하지 않게 된다. 더불어 사이버상의 공격뿐만 아니라 허가되지 않은 인원의 출입 같은 2차적 피해까지 발생할 수 있다.

(3) 웹캠

웹캠의 경우 치안이나 도로의 교통정보 제공을 위한 목적으로 설치되어 있는 경우가 많은데, 개인이 치안목적으로 설치한 경우 해커가 관리자 권한을 획득해 접속하게 되면 개인의 프라이버시를 침해하거나 사회공학적 공격을 위한 자료수집의 타겟이 될 수 있다. 타인의 주거정보 등을 무단으로 수집할 수 있고 이를 이용해 2차 범죄로 이어질 수 있다.

4.2 대응방안

본 논문에서 산업제어시스템, 빌딩제어시스템, 웹캠에 대한 취약점 공격으로 인한 피해를 방지하기 위해 제시하는 대응방안은 아래와 같다.

(1) 관리자 계정에 대한 Default 값 변경

많은 장비들이 초기 관리자계정(admin)과 비밀번호를 사용하고 있다. 이에 대응하기 위해 기본값으로 설정되어 있는 초기비밀번호 변경이 요구된다. 또한 기존 admin으로 설정되어 있는 계정을 삭제하는 등의 대응방법도 있다.

(2) 제어시스템의 모의해킹을 통한 취약점 분석

산업제어시스템 분야는 기존 Web, 모바일과 같은 시스템에 비해 모의해킹을 통한 취약점분석 연구가 활발히 이루어지지 않았다. 따라서 ICS 및 BAS 시스템 또한 모의해킹을 통한 취약점분석과 침해사고 대응이 필요하다.

(3) 내부망과 외부망의 망분리

ICS 시스템 및 BAS 시스템은 내부망과 외부망에 대한 철저한 망분리가 요구된다.

(4) 주기적인 서버 보안 패치

새로운 취약점들이 발견되고 있고, 이에 따른

취약점 패치가 제공되고 있다. 제어시스템을 운용하는 기업/공공기관에서는 주기적인 서버 취약점 패치를 진행해야 한다.

(5) 주기적인 관리자 계정비밀번호 변경

취약한 시스템의 경우 오랫동안 비밀번호를 변경하지 않는 것이 일반적이다. 따라서 주기적으로 해당 계정에 대한 비밀번호를 변경함으로써 공격자가 손쉽게 계정을 탈취하지 못하도록 할 수 있다.

Ⅴ. 결론

본 논문에서는 쇼단(Shodan)을 통한 산업제어시스템, 빌딩제어시스템에 대한 취약점 분석을 하였으며, 더불어 웹캠과 같은 IoT 기기에 대한 보안 위협도 알아보았다. 그리고 사례에 관한 피해분석 및 대응방안도 제시하였다. 쇼단의 근본적인 기능은 보안을 강화하기 위해 그 취약점을 찾아내는 것에 있다. 보안 취약점은 그 취약성이 공개될수록 조치를 통해 발전하는 분야이기 때문에 쇼단이 드러내는 보안 취약점을 통해 보안수준이 한층 더 높아질 수 있는 계기가 되어야 할 것이다. 이를 위해 기본적인 보안원칙을 준수하고 제어시스템 또한 모의해킹을 통해 다양한 취약점분석 연구가 향후 요구된다.

본 연구는 2018년도 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 과제입니다.(No. 20162220200010)

[참고문헌]

[1] 조평현, “주요정보통신기반시설에 대한 보안 취약점 개선방안에 관한 연구 : 교통신호제어시스템 중심으로”, 高麗大學校 情報經營工學專門大學院, 2013

[2] 오준형, 유영인, 이경호, “기반시설 침해사고 및 제어시스템 표준 동향”, 정보보호학회지, 27(2), pp. 5-11, 2017

[3] 검색엔진 쇼단에 국내 가스측정 시스템 정보 노출, 2016
http://www.boannews.com/media/view.asp?idx=49636

[4] 인천국제공항공사 내부정보, 검색엔진에 노출돼 '말썽' , 2016
http://www.boannews.com/media/view.asp?idx=50441

[5] 쇼단에 국내 기업 IT 인프라 정보 무방비 노출.. 해킹 공격에 이용, 2017
http://www.dailysecu.com/?mod=new&act=articleView&idxno=21388

[6] The search engine Shodan, https://www.shadon.io/

[7] 고윤성, “보안 취약서 IoT 디바이스의 IP 노출 위협 예방 시스템 연구”, 부경대학교 대학원, 2016

[8] SCADA Hacking : Finding SCADA Systems Using Shodan
https://www.hackers-arise.com/single-post/2016/06/30/Hacking-SCADA-Finding-SCADA-Systems-using-Shodan

[9] How to Find Vulnerable Webcams Across the Globe Using Shodan, https://null-byte.wonderhowto.com/how-to/hack-like-pro-find-vulnerable-webcams-across-globe-using-shodan-0154830/

[10] CVE-2016-2278
https://www.exploit-db.com/exploits/39522

2018 한국정보보호학회 하계학술대회

B8 악성코드

하 재 철 (호서대학교)

- **금융권 보안 사고 악성코드 간 유사도 분석**
  김예준, 이재경, 류기백, 이유정, 염흥열
- **난독화된 자바 악성코드에 대한 탐지 프로세스 제안**
  김광훈, 염흥열
- **해양 산업에서 사이버 해적의 위협 분석**
  조용현, 강준모, 차영균
- **매그니튜드 익스플로잇 킷을 통해 유포되는 마이랜섬의 변화 동향 분석**
  김동현, 임명은, 양준호, 염흥열
- **랜섬웨어 Native API 정보 분석을 통한 탐지 방법 연구**
  장준영, 김우재, 옥정윤, 임을규

금융권 보안 사고 악성코드 간 유사도 분석

김예준*, 이재경*, 류기백*, 이유정*, 염흥열*
*순천향대학교 정보보호학과

Analysis of the similarity between malicious codes of finalcial security accidents

Ye-Jun Kim*, Jae-Kyeong Lee*, Ki-Baek Ryu*, Yu-Jeong Lee* , Heung-Youl Youm*
*Department of information security, Soonchunhyang University.

요 약

과거 발생한 보안 사고는 단순 개인 정보의 무단 복제 및 유출이 주된 목적이었으나, 최근 다양한 공격 기법이 개발됨에 따라 금융권을 타깃으로 한 공격 형태로 확대되었다. 즉, 해커의 패러다임이 고객 정보 유출에서 막대한 이익을 얻을 수 있는 형태로 진화하였다. 이러한 변화로 인하여 랜섬웨어와 같은 악성코드의 공격이 해커들의 주요 공격 수단으로 사용되고 있다. 이러한 악성코드를 이용한 공격 빈도가 높아지면서 금융권을 대상으로 하는 공격 또한 증가하고 있다. 여러 금융권 대상 공격 중 SWIFT(Society for Worldwide Interbank Financial Telecommunication, 이하 SWIFT) 시스템 해킹사고의 경우 기타 악성코드와 함께 최근 유포되고 있는 헤르메스 랜섬웨어(Hermes Ransomware)가 같이 사용된 바가 있다. 따라서 본 논문에서는 과거 금융권 사고에서 쓰인 악성코드와 현재까지 유포되고 있는 랜섬웨어의 특징을 추출하여 서로의 연관성을 찾는 악성코드 유사도 분석 기법을 활용하여 악성코드 간의 그룹을 식별하고자 한다.

I. 서론

과거 국내 보안 침해 사고들의 목적은 개인 정보의 무단 복제 및 해킹으로 인한 개인 정보 유출입니다. 그러나 [표 1]과 같이 해킹으로 인한 정보 유출, 디도스(DDoS) 공격, 홈페이지 위변조, 악성코드 감염 등 악의적인 범죄가 지속적으로 발생하였다. 최근 랜섬웨어, 스피어 피싱, ATM 스키밍(Skimming), 모바일 해킹과 같은 새로운 공격 기법이 개발되어 금융권을 직접적으로 공격하는 형태로 진화하였다[1][2]. 이를 비추어 보아 해커들의 패러다임이 개인 정보 유출에서 직접적인 수익을 얻을 수 있는 형태로 진화하였다. 그중 랜섬웨어와 같은 악성코드 공격은 지속적으로 이루어지고 있으며 점차 발전된 형태로 공격을 시도하고, 그 피해 또한 증가하고 있다. 발전된 형태의 공격은 금융권을 타깃으로 한 랜섬웨어 공격과 SWIFT를 겨냥한 공격을 발생시켰다. 이처럼 더욱더 고도화되고 지능화되는 악성코드들의 피해를 막기 위한 빠른 대응이 필요한 현실이다. 악성코드 유사도 측정 기법을 활용하여 새로운 악성코드 발생 시, 기존 악성코드와의 유사도를 분석하여 분류함에 따라 악성코드에 대하여 보다 신속한 대응이 가능하다.[3]

[표 1] 금융회사 전자 금융사고 보고 현황[4]

유형	'13년	'14년	'15년	'16년	'17년 1~8월	합계
IT보안 사고	11	5	7	6	21	50
정보기술사고	363	366	294	276	157	1,456
IT사고 소계	374	371	301	282	178	1,506

따라서 본 논문에서는 SWIFT 전산망 해킹 사고를 분석하며 금융권을 겨냥한 악성코드와 SWIFT 전산망 해킹에 사용된 악성코드들을 비교 분석하여 악성코드 간의 유사도를 찾아 향후 발생 가능한 악성코드들에 대하여 신속한

대응을 위한 연구를 실시한다. 본 논문의 2장에서는 SWIFT 공격 사례를 분석하고 해당 악성코드의 바이너리를 분석하며 악성코드 간 유사도를 찾는다. 본 논문의 3장에서는 결론을 맺는다.

II. 본론

본 논문에서는 세계적으로 이슈가 되었던 2016년 방글라데시 중앙은행 해킹 사건과 2017년 대만 극동 국제 은행 해킹 사건을 분석하며 2017년 SWIFT에 사용된 헤르메스 랜섬웨어를 분석하여 SWIFT 악성코드와 헤르메스 랜섬웨어의 유사도를 분석한다.

2.1 2016년 2월 SWIFT 시스템 해킹사고[5]

2016년 2월, 방글라데시 은행의 SWIFT 코드를 사용한 이체 요청이 뉴욕 연방 은행에 접수되었다. 4회의 이체 요청으로 인하여 약 8,100만 달러가 필리핀으로 이체되었으며 5회 이체 요청에서 해커들의 수령인 철자 실수로 인하여 불법 자금 인출 시도임이 밝혀졌다. 이번 해킹에 사용된 악성코드는 8개의 은행의 특정 조건에 해당할 경우, SWIFT 코드를 조작하여 송금한 후 부정 거래 내역을 은폐하는 악성코드이다.[6]

위에서 다루었던 SWIFT 시스템 해킹사고에 이어서 약 1년 8개월 후, 대만의 상업회사인 극동 국제 은행을 목표로 한 공격이 수행되었다. 해당 공격은 SWIFT 메시지 유형에 속하는 MT103, MT202COV 거래 코드를 사칭하는 방식으로 수행되었다. 이 과정에서 공격자가 MT202COV 코드를 잘못 사용함에 따라 공격 사실을 감지하였다. 그러나 공격자가 이를 알아차려 헤르메스 랜섬웨어를 업로드하였던 해킹사고이다.

2.2 헤르메스 랜섬웨어[7]

2017년 10월 대만은행 공격 사건에서 알려진 랜섬웨어 공격이다. 익스플로잇 킷의 일종인 선다운을 사용하여 악성코드를 drive by download 방식으로 웹사이트에 업로드하여 배포하는 방식이다.



[그림 1] 헤르메스 랜섬웨어 감염 화면[8]

최초의 SWIFT 공격에 사용된 헤르메스 랜섬웨어는 랜섬웨어의 기능보다 시스템 파괴용 행위를 일으키는 악성코드였으나 선다운 익스플로잇 배포 방안을 채택한 이후 랜섬웨어로 활동하였다. 헤르메스 랜섬웨어의 감염 경로는 플래시 취약점을 통하여 시스템을 감염시킨다. 감염 시 HRM 확장명으로 중요 파일을 암호화하며, 복호화 비용으로 약 266만 원 상당의 가상화폐를 요구한다.

2.3 SWIFT 악성코드와 헤르메스 랜섬웨어 분석

위 2.1에서 다룬 SWIFT 시스템 해킹사고에서 공격 이후 사용된 랜섬웨어는 Hermes로, 현재까지도 활발히 유포되고 있다. 이때, 공격에 사용된 악성코드와 Hermes Ransomware의 특징점 및 연관성은 아래와 같다.

아래 그림은 Hermes Ransomware에서 각각의 API를 Mapping 하기 위하여 사용되는 Assembly code이다.

[그림 2]를 보면 각각의 난독화된 문자열을 복호화하여 본래의 문자열을 추출한 후, API를 매핑시키기 위하여 사용되는 코드이다.

```
.text:00411635 024                mov     eax, dword_41C2E4
.text:0041163A 024                cmp     eax, ebx
.text:0041163C 024                jz      short loc_41168D
.text:0041163E 024                cmp     dword_41C2E8, ebx
.text:00411644 024                jz      short loc_41168D
.text:00411646 024                push    eax
.text:00411647 028                call    __decode_pointer
.text:0041164C 028                push    dword_41C2E8
.text:00411652 02C                mov     esi, eax
.text:00411654 02C                call    __decode_pointer
.text:00411659 02C                pop     ecx
.text:0041165A 028                pop     ecx
.text:0041165B 024                mov     edi, eax
.text:0041165D 024                test    esi, esi
.text:0041165F 024                jz      short loc_41168D
.text:00411661 024                test    edi, edi
.text:00411663 024                jz      short loc_41168D
.text:00411665 024                call    esi
.text:00411667 024                test    eax, eax
.text:00411669 024                jz      short loc_411684
.text:0041166B 024                lea     ecx, [ebp+var_8]
.text:0041166E 024                push    ecx
.text:0041166F 028                push    0Ch
.text:00411671 02C                lea     ecx, [ebp+var_14]
.text:00411674 02C                push    ecx
.text:00411675 030                push    1
.text:00411677 034                push    eax
.text:00411678 038                call    edi
.text:0041167A 024                test    eax, eax
.text:0041167C 024                jz      short loc_411684
.text:0041167E 024                test    [ebp+var_C], 1
.text:00411682 024                jnz     short loc_41168D
```

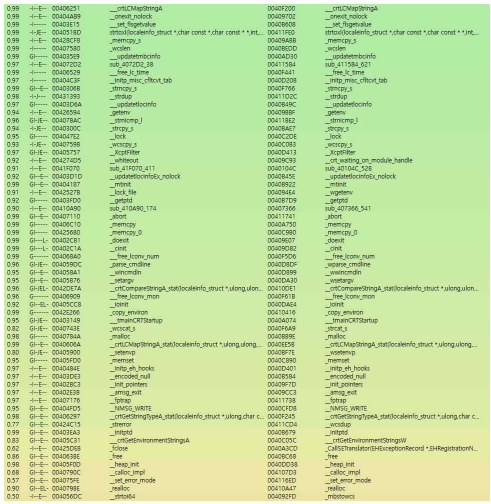
[그림 2]Hermes Ransomware Assembly code

```
.text:00407385 034                mov     eax, dword_43907C
.text:0040738A 034                mov     ecx, [ebp+var_18]
.text:0040738D 034                mov     esi, ds:DecodePointer
.text:00407393 034                cmp     eax, ecx
.text:00407395 034                jz      short loc_4073DE
.text:00407397 034                cmp     dword_439080, ecx
.text:0040739D 034                jz      short loc_4073DE
.text:0040739F 034                push    eax             ; Ptr
.text:004073A0 038                call    esi ; DecodePointer
.text:004073A2 034                push    dword_439080    ; Ptr
.text:004073A8 038                mov     edi, eax
.text:004073AA 038                call    esi ; DecodePointer
.text:004073AC 034                mov     ebx, eax
.text:004073AE 034                test    edi, edi
.text:004073B0 034                jz      short loc_4073DE
.text:004073B2 034                test    ebx, ebx
.text:004073B4 034                jz      short loc_4073DE
.text:004073B6 034                call    edi
.text:004073B8 034                test    eax, eax
.text:004073BA 034                jz      short loc_4073D5
.text:004073BC 034                lea     ecx, [ebp+var_24]
.text:004073BF 034                push    ecx
.text:004073C0 038                push    0Ch
.text:004073C2 03C                lea     ecx, [ebp+var_10]
.text:004073C5 03C                push    ecx
.text:004073C6 040                push    1
.text:004073C8 044                push    eax
.text:004073C9 048                call    ebx
.text:004073CB 034                test    eax, eax
.text:004073CD 034                jz      short loc_4073D5
.text:004073CF 034                test    [ebp+var_8], 1
.text:004073D3 034                jnz     short loc_4073DE
```

[그림 3] SWIFT 공격 악성코드 Asembly code

[그림 2]와 [그림 3]을 비교하면 사용되는 어셈블리 코드의 유사한 부분을 확인할 수 있다. 2017년 SWIFT 공격에 사용된 악성코드와 함께 사용되었던 Hermes Ransomware는 전혀 다른 종류의 악성코드이지만, [그림 2]의 .text:0041165B 부분 어셈블리 코드와 [그림 3]에서의 .text:004073AC 부분 어셈블리 코드를 확인하면 악성코드에서 사용하는 코드가 재사용되어 서로의 유사함을 볼 수 있다.

이처럼 각 악성코드마다 사용되는 code의 경우에는 공격자 및 공격 그룹마다 동일하게 삽입되어있는 부분이 존재하기 때문에 바이너리를 이용하여 각 악성코드의 연관성을 비교할 수 있다. Bindiff[9]를 이용하여 2017년 Swift 시스템 해킹에 쓰인 악성코드와 Hermese Ransomware 에 대한 바이너리를 비교한 결과로 대부분 일치하는 결과를 볼 수 있다.



[그림 4] 유사도 분석 결과

[그림 4]은 Bindiff를 사용하여 비교한 결과이다. 함수 간 바이너리의 유사성을 파악하여 순차적으로 정렬된 형태로 나타내는데 초록색에 가까울수록 높은 유사도를 갖고 있음을 보인다. 특히 2017년 SWIFT 공격 당시 사용되었던 Hermese Ransomware와 그 이전 SWIFT 공격에 사용된 “97aaf130cfa251e5207ea74b2558293d” (splwow32.exe) 악성코드와 바이너리를 비교하였을 때, 비교 가능한 총 363개 함수 중 213개의 함수가 유사하여 약 70% 이상 유사도가 일치한다. 이처럼 같은 코드가 절반 이상같이 사용되었음을 볼 수 있다. 문자열과 API를 이용하여 악성코드의 유사도를 측정한 논문[10]의 결과 목표 악성코드 간의 유사도가 평균 70% 이상의 높은 유사성을 보인 결과가 존재한다. 따라서 본 논문에서도 약 60% 이상의 높은 유사도를 보인다.

III. 결론

본 논문에서는 2016년 SWIFT 시스템 해킹사고와 2017년 SWIFT 시스템 해킹사고에 사용된

Hermes Ransomware와의 연관성을 분석하였으며 바이너리 비교 분석 결과 악성코드 간에 약 60%의 높은 유사성을 보임을 확인하였다. 현재 SWIFT 시스템 해킹사고에만 한정하여 분석을 하였으나, 과거 사용되었던 APT 악성코드와 새롭게 유포되고 있는 악성코드와의 연관성을 도출하는 것도 중요하다.

따라서 향후 연구 과제로서 과거 발생한 APT 사고와 최근 발생한 APT 사고와의 연관성을 도출하는 연구가 필요하다.

[참고문헌]

[1] KB금융지주 경영연구소, KB 지식 비타민 : “국내외 금융권의 정보보안 최근 동향과 전망”, pp. 3, 2015.03

[2] 우리금융경영연구소 김종현 연구위원, “신종 금융보안사고의 확산 및 시사점”, pp. 1-2, 2014.01

[3] 한국인터넷진흥원 강홍구 외 4명, “악성코드 행위기반 유사도 측정 기법 연구“, 한국통신학회 2017년도 추계종합학술발표회, pp. 1, 2017.

[4] 석지헌 기자, 글로벌이코노믹, “[2017 국정감사] 금융사 전자금융사고, 5년간 1500건 넘어… ″보안에 취약”, 2017.

[5] 한국인터넷진흥원, “2016년 2분기 사이버 위협 동향 보고서”, pp. 40-45 2016.08

[6] 고려대학교 이경호, “사이버 보안 미래 과제”, pp. 46-48, 2016.09

[7] 수산INT 기술 연구소, “사이트 접속만으로 감염되는 ‘헤르메스’”, 월간 악성코드 분석 보고서, pp. 3-4, 2018.04

[8] 디지털데일리 “최신 플래시 취약점 이용한 ‘헤르메스’ 랜섬웨어 감염 주의, 2018.03

[9] SABRE-Security.com, Using SABRE BinDiff v1.6 for Malware analysis

[10] 박재우 외 6명, “문자열과 API를 이용한 악성코드 자동 분류 시스템”, 보안공학연구논문지(Journal of Security Engineering), 제 8권 제 5호, pp. 622-623, 2011.10

난독화된 자바 악성코드에 대한 탐지 프로세스 제안*

김광훈*, 염흥열**

*순천향대학교 융합서비스보안학과,**순천향대학교 정보보호학과

Proposal for detecting obfuscated Java malwares

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 증가하여 현재 모든 악성코드를 분석하는데 한계가 있다. 또 악성코드의 지능적인 기술 발전으로 인해 기존의 악성코드에 변형된 변종 악성코드 또한 증가하고 있어, 기존의 안티 바이러스 솔루션의 분석, 탐지 메커니즘으로는 이에 대응하기 어려운 상황이다. 따라서 본 논문에서는 자바 플랫폼 기반의 난독화가 적용된 악성코드를 효과적으로 탐지하기 위한 프로세스 모델을 제안하여 안티 바이러스 또는 악성코드 분석가가 효율적으로 악성코드의 심층 분석과 탐지를 수행할 수 있도록 지원하고자 한다.

I. 서론

오늘날 악성코드는 날이 지날수록 기하급수적으로 증가하고 있어 현재 모든 악성코드를 분석하기에는 한계가 있다. 또 악성코드의 지능적인 기술 발전으로 인해 기존의 악성코드에 변형된 변종 악성코드 또한 증가하고 있어, 기존의 안티 바이러스 솔루션의 분석, 탐지 메커니즘으로는 이에 대응하기 어려운 상황이다. 현재 자바 플랫폼에서 기승하고 있는 애드윈드 악성코드는 여러 난독화 기법[1]을 사용하여 안티 바이러스에 의한 탐지를 회피 또는 악성코드 분석가가 코드를 역공학하여 분석하는 것을 어렵게 한다. 난독화가 적용된 변종 악성코드에 대응하기 위한 방법 중 하나는 해당 프로그램의 난독화 해제 시점을 추적, 파싱하여 해당 실행 단위별 코드(함수)를 동적으로 재실행해봄으로써 난독화가 해제된 문자열을 얻는 것이다. [2] 해당 문자열은 악성코드를 식별하기 위한 주요 탐지 시그니처로 사용될 수 있다. 따라서 본 논문에서는 자바 플랫폼 기반의 난독화가 적용된 악성코드를 동적(부분별)으로 탐지하기 위한 프로세스 모델을 개발, 제안하여 안티 바이러스 또는 악성코드 분석가가 효율적으로 악성코드의 심층 분석과, 탐지를 수행할 수 있도록 지원하고자 한다.

* 본 연구는 미래창조과학부 및 한국인터넷진흥원의 “고용계약형 정보보호 석사과정 지원사업”의 연구결과로 수행되었음

II. 제안 배경

2.1 자바 플랫폼에 대한 위협

Java는 이식 가능하고 아키텍처 중립적인 성격을 가진다. 이는 환경에 관계없이 JVM 코드가 동일하게 실행되므로 아키텍처 중립적이라고 볼 수 있다. [3]

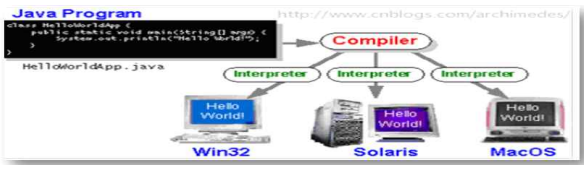


그림 1. 자바 어플리케이션과 런타임 환경

아키텍처 중립은 C / C ++와 같은 언어에 비해 큰 이점을 제공하지만 중요한 보안 위협이 된다. [4] 최근 이러한 자바 플랫폼의 특성을 이용하여 공격자들은 JVM의 취약점을 찾고 이에 해당하는 익스플로잇 공격을 다양한 방면으로 시도하고 있다. 익스플로잇 공격이 JVM 취약점을 악용할 경우 취약점을 패치 하지 않은 JVM의 모든 버전과 이를 사용하는 모든 사용자에게 영향을 미친다. 반면에 아키텍처 중립적인 특성은 보안적인 측면에서도 이용될 수 있다. 이는 해당 JVM 버전의 취약점을 악용하는 모든 익스플로잇 공격에 대한 대응 또한 가능하다는 의미이다. 따라서 본 논문의 목적은 이러한 자바 플랫폼의 특성에 적합한 보안 솔루션(AV)을 고려하여, 자바 악성코드에 대한 통합적 관리측면의 모니터링이 가능하도록 지원하는데 의의를 둔다.

2.2 자바 악성코드의 공격 전략

자바 플랫폼에 대한 안티 바이러스(AV) 성능이 발전함에 따라 공격자들은 자신의 익스플로잇 코드가 AV에 의해 탐지되는 것을 피하기 위해 해당 코드에 난독화(문자열, 리플렉션)를 적용하고 있다. [4]

2.2.1 문자열 난독화

악성코드는 런타임 시에 문자열을 인코딩 하거나 디코딩 할 수 있다. 인코딩 또는 디코딩 어느쪽을 사용하더라도 스트링을 숨기므로 클래스와 메소드 이름을 인식하기가 더 어려워지며 시그니처 기반 안티 바이러스를 우회 할 가능성을 높일 수 있다. [2]

(1). 재구성을 위해 문자열 java.lang. SecurityManager는 실행시에 제거되는 숫자로 채워진다.

(2). 인코딩 된 문자열은 런타임 시에 디코딩 된다.

```
public static String getStr(String input) {
  StringBuilder sb = new StringBuilder();

  for(int i = 0; i < input.length(); i++) {
    if(!(input.charAt(i) >= '0' && input.charAt(i) <= '9')) {
      sb.append(input.charAt(i));
    }
  }
  return sb.toString();
}

String str = "1j2a34v234a.3241324an324g23.4
   S234e3c24u324r3i4t324y23M4a23n4ag234er";

Class<?> c = Class.forName(getStr(str));
```

그림 2. 자바 플랫폼에서의 문자열 난독화

2.2.2 리플렉션 난독화

AV 필터는 알려진 취약한 라이브러리 함수의 호출을 검사 할 수 있으며 이를 막기 위해 악성 애플릿은 리플렉션을 사용하여 취약한 메소드를 호출한다. [4]

(1). Class.forName 정적 메소드를 사용하여 Class 유형의 객체 c를 생성한다.

(2). 객체 c는 작성자가 Java 클래스 java에 관한 정보에 액세스 할 수 있게 한다. security.Permissions, 특히 java.security.Permissions 형의 객체를 작성한다. 또한 c를 사용하여 객체를 만들 수 있다.

(3). m은 객체 o에 대한 메소드 호출의 세부 사항을 캡슐화 한다. 호출은 o를 매개 변수로 사용하여 m에 호출을 적용하여 실현된다. 이러한 일련의 리플렉션 작업은 메서드를 직접 호출하는 방법을 위장하는 역할을 수행 한다.

```
java.security.Permissions o = new java.security.Permissions();
o.add(new AllPermission());

Class<?> c = Class.forName("java.security.Permissions");
Object o = c.newInstance();
Method m = c.getMethod("add", Permission.class);
m.invoke(o, new AllPermission());
```

그림 3. 자바 플랫폼에서의 리플렉션 난독화

리플렉션 및 문자열 난독화를 함께 사용할 수 있으며 이외에도 다양한 난독화 기법의 등장으로 AV의 탐지 성능이 위협을 받고 있다.

본 논문에서는 해당 난독화 기법이 적용된 악성코드를 대상으로 난독화 해제 연구를 진행하고 그 결과 값으로부터 악성코드로 식별 가능한 문자열을 추출하여 탐지 시그니처로 활용하는 방안을 제안한다.

III. 탐지 프로세스

3.1 개요

본 논문에서 제안하는 난독화된 자바 악성코드를 탐지하기 위한 프로세스는 다음과 같다.

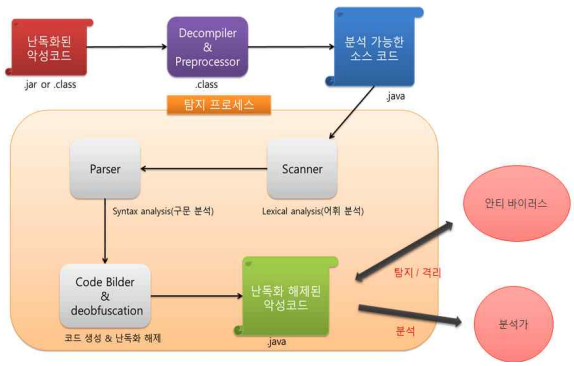


그림 4. 난독화된 악성코드의 탐지 프로세스

본 논문과 기존 논문의 탐지 메커니즘[4]에 대한 차이점은 다음과 같다.



그림 5. 기존 논문의 Partial Evalutation을 이용한 탐지

표 1. 본 논문과 기존 논문[4]의 탐지 메커니즘 차이

	본 논문	기존 논문
탐지 방법	정적, 동적(부분)	정적
런타임 성능	느림	빠름
난독화 해제	자바 런타임 환경을 이용한 정확한 해제	자체 컴파일러를 이용한 부분적 해제(문법 지원 여부에 따라 비율이 다름)
분석용 소스	java(실행 가능)	jimple(실행 불가능)

3.2 악성코드 샘플

먼저 연구에 사용된 악성코드 샘플은 현재 기하급수적으로 증가하고 있는 난독화가 적용된 자바 실행 파일(JAR) 기반의 애드윈드를 대상으로 하였다. 해당 샘플의 주요 행위는 다음과 같다.



그림 6. 자바 악성코드 - 애드윈드의 주요 행위

3.3 디컴파일 & 전처리 [5]

JAR 파일로된 자바 악성코드의 바이트 코드를 디컴파일 하기 위한 도구로는 바이트 코드 뷰어를 사용하였다. 전처리 단계에서는 디컴파일로부터 분할된 자바 소스코드를 컴파일하고, 메인 함수가 포함된 소스의 경로를 추출한다. 컴파일된 소스코드는 그 자체로 분석이 가능하며 탐지 프로그램의 입력 값으로 사용된다.

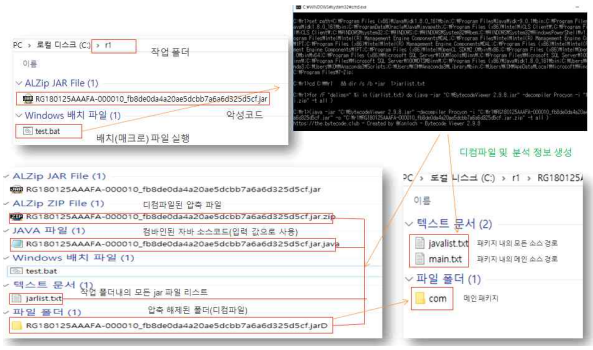


그림 7. 디컴파일과 전처리 과정

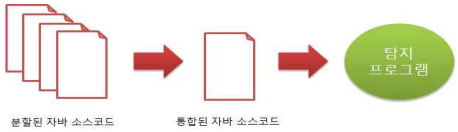


그림 8. 디컴파일된 자바 소스코드의 통합

3.4 스캐너 [5]

스캐너 루틴에서는 입력된 소스 코드로부터 함수 호출에 대한 시퀀스와 변수 선언과 정의된 상태를 추적하여 얻은 디버깅 정보를 기록한다. 해당 정보는 난독화 해제를 위한 3.5 루틴에서 참조한다.

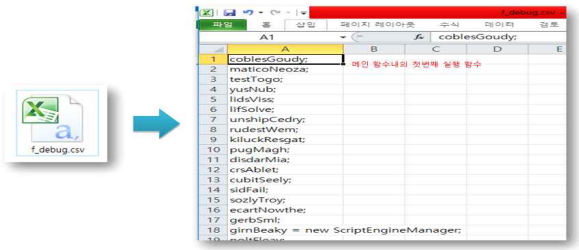


그림 9. 함수의 콜 시퀀스 트레이싱



그림 10. 변수의 선언, 정의된 상태 트레이싱

3.5 파서 [5]

리플렉션 및 문자열 난독화를 사용하기 위해 호출되는 함수(getDeclaredMethod, getMethod)와 변수가 존재할 경우 해당 함수의 인자와 내부 변수의 값을 순차적으로 파싱한다. 여기서 인자가 함수일 경우 문자열 난독화 해제를 위한 디코딩 루틴일 가능성이 높다. 따라서 함수 내부 또한 재귀함수에 의해 의미 있는 리턴 값을 추출, 트레이싱한다.

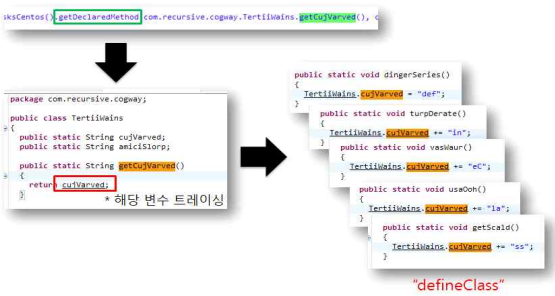


그림 11. 난독화 해제를 위한 디코딩 루틴 파싱 과정

3.6 코드 빌더 & 난독화 해제

코드 빌더 루틴은 3.4 파서로부터 추출된 값을 3.2 전처리 단계에서 구한 메인 함수가 포함된 소스 코드에 삽입한다. 이 때 원래의 메인 코드는 초기화되며 문자열 분할 유형의 난독화[2]를 해제하기 위해 3.3 스캐너의 디버깅 정보를 참조해 정의된 함수와 변수의 시퀀스를 끼어 맞추는 작업이 선행된다. 이 후 패키지 전체를 다시 컴파일하여 실행함으로써 결과적으로 난독화 해제된 문자열을 얻게 된다. 이는 기존의 악성코드 전체를 실행하여 난독화를 해제하는 방법[2]이 아닌 해당 디코딩 루틴만 가져와서 부분적으로 재실행함으로써 악성코드의 감염을 피하고 런타임 오버헤드를 줄일 수 있다는 장점을 가진다.



그림 12. 리플렉션 난독화 해제 과정



그림 13. 문자열 난독화 해제 과정

3.7 난독화 해제된 악성코드의 탐지

본 논문에서 제안한 탐지 프로그램을 사용하여 난독화 해제를 수행한 결과는 다음과 같다.

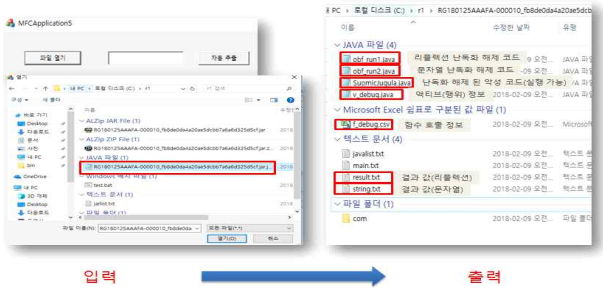


그림 14. 탐지 프로그램의 실행 결과

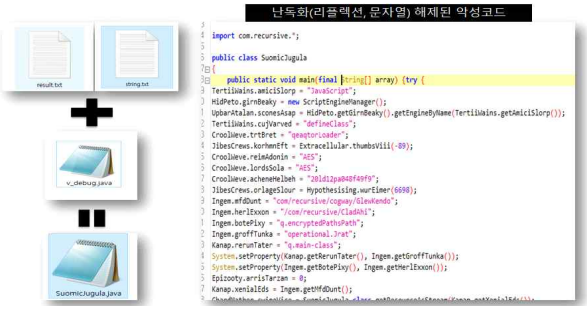


그림 15. 리플렉션, 문자열 난독화가 해제된 악성코드의 소스

입력된 파일은 3.2 디컴파일 후 전처리 단계에서 추출한 통합된 자바 악성코드(애드윈드)의 소스이다. 최종적으로 출력된 SuomicJugula.java 파일은 스캐너에 의해 추출된 변수 액티브 상태를 기록한 파일(v_debug)과 코드 빌더기에 의해 추출된 리플렉션, 문자열 난독화 해제 결과를 기록한 파일(result, string)을 컴바인 한 결과물이다. 이는 난독화가 해제된 악성코드의 소스 코드로 그 자체로 실행이 가능하며 악성 행위 또한 원본과 동일하다. 따라서 해당 소스 코드는 샌드박스 환경의 분석에서 유용하게 사용될 수 있으며 악성코드로 식별 가능한 문자열을 선별하여 탐지 시그니처로 활용한다면 더욱 효율적으로 변종 악성코드에 대응할 수 있을 것이다.

IV. 결론

본 논문에서는 난독화된 자바 악성코드를 효율적으로 식별하는 탐지 프로세스를 제안하였다. 해당 프로세스를 통해 리플렉션 및 문자열 난독화 해제를 수행하고 그 과정에서 디코딩 루틴만 부분적으로 재실행함으로써, 악성코드의 감염과 런타임 시 오버헤드를 감소시켰다. 최종 출력된 분석용 소스는 샌드박스 환경에서 리패키징하여 실행함으로써 특정 행위에 대한 분석과 탐지 또한 가능하다. 이로써 안티 바이러스 또는 악성코드 분석가 입장에서 더욱 효율적으로 악성코드에 대한 심층 분석과 탐지를 수행할 수 있을 것으로 기대하며, 또 앞으로 계속 증가하는 신종, 변종 악성코드 수와 식별 가능한 악성코드 수의 격차를 줄여 신속한 침해 대응이 가능할 것으로 예상된다.

[참고문헌]

[1] "애드윈드 악성코드의 역습", Ahnlab, http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=25778
[2] "자바 스크립트 난독화 이해하기", Ahnlab, http://image.ahnlab.com/file_upload/tech/javascript.pdf
[3] "The JavaTM Platform A White Paper" JAVASOFT, ftp://me.psu.ac.th/pub/linux/java/JavaPlatform.pdf
[4] Ranjeet Singh, Andy King "Partial Evaluation for Java Malware Detection", University of Kent, 2017년
[5] 아오키 미네로우, "컴파일러 구조와 원리", 2010년

해양 산업에서 사이버 해적의 위협 분석

조용현*, 강준모**, 차영균***
*고려대학교 정보보호대학원

Cyber Piracy Threat Analysis in Maritime Industry

Yong-Hyun Jo*, Jun-Mo Kang**, Young-Kyun Cha***
*Graduate School of Information Security, Korea University

요 약

해양 산업은 대표적으로 조선, 해운, 항만업으로 분류되며 국가 경쟁력에 큰 비중을 차지하는 중추적인 영역이다. 2017년 국제해사기구(IMO)의 해양안전위원회(MSC)에서는 해양 산업을 대상으로 한 사이버 공간에서의 위협이 증가함에 따라 해양 사이버보안에 대한 논의가 본격화 되었다. 본 논문에서는 해양 사이버보안 사례와 국제 해양기구의 사이버보안 가이드라인 동향을 살펴보고 그 의미를 고찰하고자 한다.

I. 서론

지구의 70%를 차지하고 있는 바다를 통한 해양 산업은 국가간 교역의 90% 이상이 이뤄지고 있으며, 전세계 해운 시장은 2010년 7,200억 달러 규모에서 2030년에는 1조 2,300억 달러로 전망하고 있다. 국내 해양 산업의 규모는 2016년 기준 127조원으로 해운업은 2016년 기준 연간 총 수입이 26조원으로 국내 산업 중 7번째로 많은 매출을 기록했다. 정부에서는 2018년부터 조선 및 해운업 발전을 위한 계획을 발표하고 새로운 선박 건조와 해운업 발전을 위한 전략을 추진 중이다. 해양 산업에도 정보통신 기술이 적용되어 선박에서 운영 중인 각종 항해장치들이 디지털화되거나 선박과 선박, 선박과 항만, 선박내 장치와 장치들이 통신망으로 연결되고 있다. 이와 같은 변화는 ICT 기반의 Smart Ship 환경으로 변화되기 때문인데 이는 법/규제 이행요구, 화주의 요구사항 증가, 선박의 위치, 운항정보, 연료사용 실적 분석, 환경규제의 이행을 위한 IT 기술 적용, 선박의 위성통신 적용, 선원 복지를 위한 개인 e메일과 인터넷 사용을 위한 해상 네트워크 통신망 보편화, 선박 건조시 선박내 엔진, 항로조정 장치 등이 네트워킹 구성, 선주-선박-운영사 간의 IT 기반의 선박관리 시스템 적용이 요구되기 때문이다.

기존의 전통적인 해적은 총기, 폭발물 등으로 무장하고 선박 또는 선원, 화물을 납치, 탈취하여 인질로 삼고 해운회사, 정부와 협상하여 석방의 대가를 지불받는 무장단체를 일컬었으나 최근에는 정품 소프트웨어를 대량으로 무단 유포, 판매하는 사람을 사이버 해적으로 불러왔다. 하지만 선박, 조선, 해운 등 해양 관련 산업이 IT기술 기반으로 변화함에 따라 해상에서의 납치/탈취 행위가 아닌 해양 산업에서의 해킹, 정보유출 또는 범죄조직과 해커가 연계한 사이버범죄 사건이 발생하여 이러한 해양 산업을 대상으로 한 사이버 공격자를 본 고에서는 사이버 해적으로 정의하고자 한다.

해양 산업에서는 국제 항해 선박 및 항만시설의 보안에 관한 법률에 따라 선박이나 항만에 폭발물 또는 무기류의 반입, 은닉 등을 주요한 위협으로 정의하였으나 디지털화 되면서 선박, 항만 등에 해킹, 악성코드 감염, 시스템 파괴와 같은 사이버보안의 이슈가 대두되고 있다.

2016년 국제해사협회(BIMCO)에서 해양 업

계 종사자를 대상으로 조사한 자료에 따르면 응답자 5명중 1명은 사이버공격의 피해를 입었고, 응답자중 40%만이 예방조치를 하였다고 응답하였다.

이와 같이 해양 사이버보안 위협에 대응하기 위해 ENISA에서는 해양 분야를 ICS SCADA, Smart Grid, Financial, Health와 함께 Critical Infrastructure로 분류하였다.

국제해사기구(IMO) 해양안전위원회(MSC)에서는 이러한 사이버보안의 위험증가에 따라 해양 사이버위험을 관리하기 위한 방안을 제시하고 2021년 1월 1일부터 시행키로 하였다.

본 고에서는 해양 산업의 사이버보안 사례와 해양 산업의 글로벌 보안 표준 및 가이드를 분석하고자 한다.

II. 해양 사이버 보안 동향

2.1 보안 이슈사례

[표 1]의 해양 사이버 보안의 이슈 사례를 살펴보면 다음과 같다.

사례번호 1은 기존에 서아프리카 해역에서 무장하고 선박과 선원을 납치하던 나이지리아 범죄조직이 해킹그룹과 연계하여 한국, 일본, 노르웨이 등의 해운 회사를 대상으로 임직원 개인정보(User ID, password)를 탈취하여 비즈니스 스캠(Business SCAM)을 시도하는 사례가 발생하였는데 이는 전통적인 해적이 사이버 공격 기술을 활용하는 사이버 해적(Cyber Pirate)화 되는 대표적인 사례이다.

사례번호 2는 네덜란드 해운회사의 e메일 시스템이 자동전달 기능을 통해 외부 공격자에게 최소 11개월 동안 포워딩되어 호주 국적 임직원 개인정보 500여건의 민감정보가 유출된 것으로 확인되었다.

사례번호 3,4는 영국과 싱가포르의 글로벌 해운 회사들이 해킹으로 인하여 데이터가 유출되거나 시스템 다운된 사례이다.

사례번호 5는 선박에서 이용되는 위성 통신 장치 시스템에서 심각한 취약점이 발견되어 해당 취약점을 이용하여 공격자가 해상에서 운항중인 선박의 위성 통신 시스템과 내부 엔진장치, 운항장치 등에 침투 할 수 있다. 그러나, 이 시스템은 2017.6월부로 EoS(End Of Services)되어 취약한 시스템을 탑재한 선박은 패치 전까지 위협을 내재하고 있으나 선박 시스템의 경우 수명연한이 20~30년 이상으로 폐기 전까지는 내부 시스템을 업그레이드 하거나 패치하기 어려운 문제점을 내포하고 있다.

사례번호 6는 2017년 8월 미 해군함정이 싱가포르 해협에서 유조선과 충돌하여 승조원 10명이 사망한 사건이 발생하였는데, 이후 언론에서는 사이버공격에 의한 개연성을 제기하였다.

사례번호 7은 2017년 글로벌 보험사인 알리안츠에서 선박 안전과 위험 보고서에 따르면 2016년 3월 북한의 사이버공격으로 한국 선박의 GPS 시스템이 무력화된 사건을 계기로 선박 안전에 사이버보안이 영향이 증대할 것으로 예상하였다.[1]

사례번호 8은 세계 최대의 해운회사인 머스크 라인의 우크라이나 지점에서 사용 중인 회계소프트웨어의 취약점을 통해 감염된 NotPetya 랜섬웨어가 전세계 지점과 항만 등에 전이 되어 추가 피해 방지를 위해 전체 IT시스템을 강제 다운 시키고 시스템 복원을 위해 3개월간에 걸쳐 45,000대의 PC, 2,500개의 Application 재설치한 사건이 발생하였다. 이 때문에 머스크 라인의 총 피해 추산액은 약 3,000억으로 집계되었다. 감염 및 전파 증상이 발견된 초기에 거대 기업이 추가 피해 방지를 위해 IT시스템을 강제 다운했던 신속한 판단과 트위터 등을 통해 피해 및 복구활동 조치 사항을 전파함으로써 고객 이탈을 방지하였다.

사례번호 9은 독일 소유의 컨테이너선(8,250 TEU급)이 해킹 되어 10시간동안 선박의 통제권을 잃어버리는 사건이 발생하였는데 이를 원상 복구하기 위해서 선박은 운항을 중단하고 IT시스템 복구 작업을 실시하였다. 컨테이너선의 경우 대량의 화물을 운송하고 있어 화물운송 지연 및 선박 연료비의 증가 등으로 인한 경제적 손실이 발생할 수 있는 사건이다.

사례번호 10는 2016.11월 미 해군 승조원의 개인정보가 유지보수 회사의 Labtop을 통해 외부로 유출된 사건으로 해군 정보의 유출로 인

한 사고이다.

사례번호 11은 2016.08월 미국 및 전 세계 13개 항만에서 사용중인 미국의 Cargotec 주식회사의 선박 Navis 웹 기반 시스템에 Zeroday 취약점인 sql-injection(CVE-2016-5817)이 공개된 건으로 선박 시스템의 패치 관리에 대한 이슈가 제기되었다.[2]

사례번호 12는 2016. 프랑스 방산 회사에서 스텔스 기술 등 해군 잠수함 관련 자료 22,400 페이지가 전직 해군 장교에 의해 유출되었다.

사례번호 13은 2016. 3월 해적이 글로벌 해운사의 선박을 납치한 후 특정화물이 적재된 컨테이너만을 탈취하고 이탈한 사건 발생. 해적 피해를 입은 해운회사의 선적화물 관리시스템과 선하 증권 관리 시스템을 조사한 결과, 해운사 시스템에서 악성코드가 발견된 사건이다. 해적이 해커를 고용하여 해운사의 전산시스템을 이용한 범죄행위를 유발하였다는데 특징이 있고 해운사의 보안관리 체계는 화물과 선박, 회사 전산관리시스템 등으로 범위를 광의적으로 해야 하는 의미를 가지고 있다.

사례번호 14은 2015년에 발견된 선박에서는 항공기의 BlackBox 역할을 하는 VDR(Voyage Data Recorder) 시스템에서 취약점이 발견되어 원격에서 VDR에 기록된 데이터의 삭제 및 변조가 가능한 것이 발표되었다. 이에 따라 선박 사고 조사시 해당 취약점의 패치 여부와 해당 취약점에 의한 원격에서의 VDR 데이터 위변조 여부를 확인하여야 디지털증거의 무결성을 증명할 것이라고 판단된다.

사례번호 15는 2014년 10월에 선박 등에 연료를 공급하는 해상급유 주요 기업인 WFS(World Fuel Services)가 Email SCAM으로 1,800만 달러의 사기 피해를 입은 사건으로 이후에도 Business SCAM이 꾸준히 지속되었고 2018년 4월에는 해운사를 타켓으로 한 집중 공격이 발견되었다.[3]

사례번호 16는 2013년 10월 마약 밀매업자들이 해커를 고용하여 벨기에 Belgian port of Antwerp 항만 제어 시스템에 침입하여 코카인과 헤로인을 선적한 컨테이너를 확인하고 합법적 화물주가 도착하기 전에 반출하였다.[4]

사례번호 17은 2012년 범죄조직에서 고용한 해커가 호주 세관과 Cargo System에 침입하여 세관 당국이 의심하는 선적 컨테이너(선적화물) 정보를 파악하는 사건이 발생하였다.[5]

사례번호 18은 2011년 8월 Iranian Shipping Line 서버에 해커가 침입하여 요금, 적재화물, 화물번호, 운송날짜와 장소 데이터를 손상하였다.[6]

사례번호	시기	내용
1	2018.04	나이지리아 해킹그룹이 한국, 일본, 노르웨이 등 해운 회사를 대상으로 공격. 이 중 한국 해운 회사 3개의 임직원 개인정보를 탈취하여 BEC(Business Email Compromise) 공격에 활용
2	2018.03	네덜란드 해운회사의 e메일 시스템이 자동전달 기능을 통해 외부 공격자에게 최소 11개월 동안 포워딩되어 호주 국적 임직원 개인정보 500여건의 민감정보가 유출된 것으로 확인
3	2017.12	싱가포르 해운회사 BW그룹의 컴퓨터 시스템이 해킹으로 오프라인 상태로 전환
4	2017.12	영국 Clarksons, 해커들이 요구한 금액 지불을 거부했다가 데이터 유출 협박받음
5	2017.10	위성 서비스 회사의 관련 시스템에서 심각한 취약점 발견
6	2017.08	미 해군함정 John S.McCain호가 충돌 사고로 10여명의 승무원이 사망하거나 실종되는 사건 발생, 이후 일부에서 사이버 공격 또는 사이버 침해로 인한 개연성을 제기
7	2017.08	보험사의 선박 안전과 위험 보고서에 따르면 선박 안전에 사이버보안이 영향이 증대할 것으로 예상
8	2017.06	세계 최대 해운사 머스크 라인 Ransomware (NotPetya) 공격으로 4,000대 서버, 45,000대 PC, 2,500개의 Application 재설치. 총 피해 추산액은 약 3,000억
9	2017.02	독일 소유의 Cyprus에서 djbouti까지 항해하는 8,250 teu급 선박의 항법장치

		(Navigation System)를 10시간 동안 해커가 장악
10	2016.11	미해군 134,386명의 사회보장번호 등의 민감정보가 IT 외주직원(**사)의 랩탑이 해킹되어 유출
11	2016.08	미국 및 전세계 13개 항만에서 사용중인 미국의 Cargotec 주식회사의 선박 Navis 웹 기반 시스템에 Zeroday sql-injection(CVE-2016-5817) 취약점 공개
12	2016	프랑스 방산 회사에서 스텔스 기술 등 잠수함 관련 자료 22,400페이지 유출
13	2016.03	해적이 글로벌 해운사의 선박을 납치한 후 특정화물이 적재된 컨테이너만을 탈취하고 이탈한 사건 발생. 해적 피해를 입은 해운회사의 선적화물 관리시스템과 선하 증권 관리 시스템을 조사한 결과, 해운사 시스템에서 악성코드가 발견됨
14	2015	선박의 blackbox 기능인 VDR시스템의 취약점 발견. 원격에서 VDR에 기록된 데이터의 삭제/변조 가능
15	2014	선박 등에 연료를 공급하는 해상급유 주요 기업인 WFS(World Fuel Services)는 Email SCAM으로 1,800만 달러의 사기 피해 발생
16	2013.10	마약 밀매업자들이 해커를 고용하여 벨기에 항만 제어 시스템에 침입하여 코카인과 헤로인을 선적한 컨테이너를 확인하고 합법적 화물주가 도착하기 전에 반출. 해커는 Trojans 첨부파일 이메일을 통해 관련 pc를 감염시키고, 사무실에 침입하여 비밀번호를 탈취하는 usb를 설치
17	2012	2012년 범죄조직에서 고용한 해커가 호주 세관과 Cargo System에 침입하여 세관 당국이 의심하는 선적 컨테이너(선적화물) 정보를 파악
18	2011.08	Iranian Shipping Line 서버에 해커가 침입하여 요금, 적재화물, 화물번호, 운송날짜와 장소 데이터를 손상

[표 1] 해양 사이버 보안 사례

사례를 IT Infra 측면, 항만 및 화물 관리 시스템 측면, 선박 측면으로 보안 위협을 분류하면 다음 [표 2]와 같다.

분류	보안 위협
IT Infra	Email Scam 무역대금 사기
	임직원 개인정보 유출
	비인가 화물정보 열람
	IT 시스템 다운
항만 및 화물 관리 시스템	항만 제어 시스템 중단 및 파괴
	비인가 화물 데이터 열람
	운송장 데이터 위/변조
선박	VDR 데이터 삭제/위변조
	선박 위성 시스템 해킹
	선체 내부 시스템 악성코드 감염
	선박 GPS 시스템 Jamming
	위치 정보 위/변조
	디지털 항법장치 제어권 탈취

[표 2] 해양 사이버 보안 위협

2.2 선박 및 항만 시설에 필요한 보안조치

2001. 9. 11 미항공기 테러 이후 테러대응체제 구축 필요성을 인식한 국제해사기구(IMO)가 선박 및 항만시설에 필요한 보안조치(ISPS, International Ship and Port facility Security)를 규정하여 '02. 12월 제정한 협약으로 『국제선박 및 항만시설 보안규칙』이라 번역되며 '04. 7. 1 발효되었다.

선박은 자체 보안계획을 수립하여 정부의 승인을 득하여야 하며, 정부의 보안심사를 받은 후 국제 선박보안증서(ISSC, 유효기간 5년)를 비치하고 운항하여야 한다. 선박마다 고유식별번호(IMO 번호)를 선체에 영구표시토록 강제화하고 있으며, 선박보안증서 미소지 선박은 입항거부 또는 출항정지 등 국제항해가 불가하며, 항만은 항만시설보안책임자를 임명하고 항만보안평가를 실시한 후 보안계획을 수립하여 정부의 승인을 받아야 한다.

2.3 국제 해양 기구 동향

해운과 조선에 관한 국제적인 문제들을 다루기 위해 설립된 국제 기구인 IMO(International Maritime Organization)에서는 선박간, 육·해상간 전자·통신장비 장착 및 가동이 확산되면 육

상에서와 마찬가지로 해킹, 정보유출, 사이버테러 등 심각한 해상안전 문제가 발생할 것으로 경고하였다.

이에 산하 조직인 MSC(Maritime Safety Committee) 94차에서 미국, 캐나다는 항만, 선박 해사 시설물 및 해운물류 시스템의 다양한 해사 분야에 사이버보안을 강화할 것을 제안하였고,

MSC 95차에서 미국, 캐나다 등은 선박 외의 항만, 해사시설물, 장비의 사이버보안 관련 통합지침 개발이 시급함을 주장하였으나,

MSC 96차에 제출한 안에는 MSC 95에서의 다른 국가들의 의견을 반영하여 우선 선박 사이버보안 지침안만 포함되었다. 이 지침에는 사이버위험의 이해, 사이버위험 관리의 필요성과 목적, 위험관리 절차 파악, 선주 및 운항자가 위험/보안 관리 시스템에 추가할 활동 목록 제안 등의 내용이 포함되었다.

MSC 98차 회의(2017년 6월 20일)를 통해 사이버 보안에 대한 가이드라인을 규정하고 2021년 1월 1일부터 안전관리 시스템에 사이버 보안 관리 분야(Maritime Cyber Risk Management)를 포함하는 것을 의무화 하였고, 이 지침은 업계의 모든 조직을 대상으로 적용된다.

III. 해양 사이버보안 지침 및 가이드

3.1 IMO

IMO cyber security risk management guideline에서는 선박의 취약한 시스템으로 선박 운항 및 화물관리, 승객 관리, 엔진 및 통신 시스템 등을 제시하고 있다.

이 가이드라인에서는 식별-보호-탐지-대응-복구 5단계의 기능으로 효율적인 risk 관리 프레임워크를 제시하고 있다. 이 프레임워크는 NIST의 cyber security framework[7]이다.

최상의 risk 관리를 위해서는 BIMCO(발틱국제해사기구협의회)의 지침, ISO/IEC 27001, NIST cyber security framework 등 모든 관련 지침 및 표준의 최신 버전을 참조하도록 권고하고 있다.

3.2 BIMCO

2016년 2월 1.1버전의 THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS[8]에 이어 2017.6월에 2.0 버전을 발표하였다. 이 버전에는 사이버 침입사고에서 연속성 계획과 대응 및 복구 계획 챕터에서는 선박의 원격 환경을 고려하여 지침이 구체화 되었다. 이 가이드는 사이버 안전관리에 대한 필수 지침을 제공하는 것을 목적으로 하고 있다.

제1장에서는 사이버보안과 안전관리를 다루고 있으며 해양 사이버보안은 탑승한 인원(승객 및 선원), 선박과 화물을 무단 접속과 조작/중단, 데이터의 유실로부터 보호한다고 정의하고 있다. 주요 우려사항으로 선박의 전자파트 디스플레이 및 정보시스템(ECDIS)의 무결성 훼손, 선박용 소프트웨어의 유지관리 및 패치로 발생할 수 있는 장애, 선박의 중요한 센서의 손실 또는 조작으로 위성 네비게이션 시스템을 포함하고 있다.

제2장에서는 해양 사이버보안의 위협을 회사, 선박, 운영과 거래로 식별하고 있으며 금융기관, 공공기관 등 다른 산업에서의 경험이 성공적인 사이버공격의 경감 사례가 될 수 있음을 제시하고 있다. 또한 회사의 직원이 해상과 육상에 있을 때 각각 사이버 공격에 노출 될 수 있음을 제기한다.

제3장에서는 선박에서 취약점에 노출될 수 있는 시스템을 식별하고 있는데 본 고의 3.1 IMO에서 제시하고 있는 선박 시스템과 동일하다. 다만 선박과 육상(항만 또는 선박 운영회사, 해운 회사 등)과의 통신이 이뤄지는 시스템인 엔진 성능 모니터링 시스템, 선박 유지관리 시스템, 화물과 승선원 관리 시스템, 항해 관리 시스템 등 육상에서 선박의 운항을 점검하고 관리하기 위해 통신 하는 시스템을 추가로 식별하고 있다.

제4장에서는 위험 평가에 관한 것으로 K-ISMS, ISO27001 등에서 제시하고 있는 위험평가 가이드 및 통제항목과 동일하게 위험평가의 책임은 고위 경영진에 있음을 명시하고 있다. 영향 평가를 위해서는 CIA Model[9]을 통해 평가하나 해양 산업과 선박의 환경을 고려

하여야 한다. 예를 들면 민감한 정보에는 선박 위치, 시스템의 상태 및 판독 값, 화물의 세부 사항, 권한, 인증서 등을 포함하도록 하고 있다. 선박의 전력관리 시스템은 SCADA 시스템을 포함하고 있고 선박 전체의 전력 분배와 제어를 담당한다. 이 시스템은 선박의 통신 시스템과 연결되어 육상의 회사에서 모니터링 하도록 구성되어 있다.

제5장에서는 보호대책에 관한 것으로 위험평가 결과 나타난 위험에 대해 고위경영진의 책임 하에 보호대책을 이행하여야 한다. 보호조치는 절차과 지침으로 구성하고 기술적인 수단과 관리적인 수단을 제시하고 있다. 특히, 보호대책으로 선박이 위성 및 무선 통신을 이용할 때 위성통신 시스템과 사양을 고려하고, 운항 선박의 불법적인 접속을 방지하는 방법을 고려하여야 한다. 제어 소프트웨어와의 관리 인터페이스는 주로 웹 기반 사용자 인터페이스의 형태로 제공되는데 그러한 인터페이스의 보호는 선박에 설치될 때부터 고려해야 한다.

제6장에서는 업무연속성 계획에 관한 것으로 선박의 경우 전자 항법 장비의 가용성 또는 탐색의 무결성 데이터 손실, 글로벌항법위성시스템(GNSS)의 가용성 또는 무결성 손실, 해안과의 필수적인 통신의 손실, 세계 해상 조난 안전 시스템(GMDSS) 통신 두절, 선박의 추진 시스템, 보조 시스템 및 산업 제어 시스템을 포함한 산업 제어 시스템의 가용성 손실, 기타 데이터 관리 및 제어 시스템의 무결성 손실, 랜섬웨어 또는 서비스 거부공격(DoS)에 대한 손실 등을 고려하여야 한다.

제7장에서는 사고대응 계획에 관한 것으로 예를 들면 전자해도시스템(ECDIS)가 악성코드에 감염되었을 때 원복하는 복구계획, 사고대응 계획, 조사 계획 등을 수립하여야 한다.

IV. 결론

본 논문에서는 조선, 해운 회사, 항만 등 해양 산업을 대상으로 한 사이버 공격자를 사이버 해적으로 정의하고 그 피해 사례를 살펴보았다. 해양 산업은 선박-항만-지원시설-회사(선주사, 선박운영회사)-화주(고객) 등으로 구성되는데 이러한 구성체계가 사이버 공격에 노출될 경우 선박과 화물, 승선원의 물질적, 인명의 피해로 야기될 수 있다. 이에 따라 관련 국제기구에서는 해양 산업의 사이버 보안 리스크 관리 체계를 마련하도록 결의하였고 영국 정부의 교통부 장관은 2017. 9월 해양 산업(선박 운영 자, 선주, 승무원 등)에서 사이버 위협에 대처 할 수 있는 지침 Code of practice: cyber security for ships)을 제시하였다.[10] 이러한 제도적 움직임은 한국 해양산업에도 밀접한 영향을 끼칠 것으로 판단된다. 또한, 향후 자율운항 선박의 등장과 해양 산업에서의 IT 적용이 증가될 것이 예상됨에 따라 해양 사이버 보안 체계가 증가할 것으로 사료된다.

[참고문헌]

[1] Allianz Global Corporate & Specialty, Safety and Shipping Review 2017, Aug, 2017

[2] https://ics-cert.us-cert.gov/advisories/ICSA-16-231-01

[3] https://shipandbunker.com/news/world/670152-wfs-in-court-over-18m-bunker-scam-claim

[4] https://motherboard.vice.com/en_us/article/bmjgk8/how-traffickers-hack-shipping-containers-to-move-drugs

[5] https://www.kaspersky.com/blog/maritime-cyber-security/8796/

[6] https://www.csoonline.com/article/3245803/security/defeating-21st-century-pirates-the-maritime-industry-and-cyberattacks.html

[7] NIST, Cyber Security Framework, April, 2018

[8] https://www.bimco.org/news/press-releases/20170705_cyber-g

[9] NIST, Standards for Security Categorization of Federal Information and Information Systems, Feb, 2004

[10] UK Department for Transport, Ship security: cyber security code of practice, Sep, 2017

매그니튜드 익스플로잇 킷을 통해 유포되는 마이랜섬의 변화 동향 분석

김동현*, 임명은*, 양준호*, 염흥열*
*순천향대학교 정보보호학과

An Analysis of the Trend of Variation in MyRansom

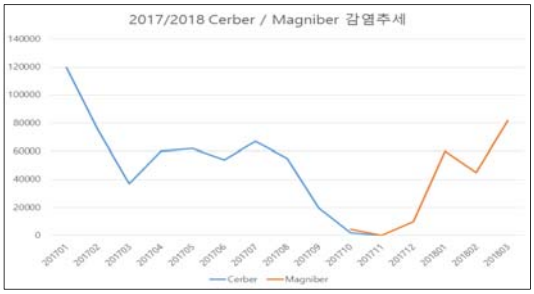
Donghyun Kim*, Myeongeun Im*, Junho Yang*, Heung-Youl Youm*
*Department of Information Security Engineering,
Soonchunhyang University

요 약

마이랜섬 랜섬웨어(MyRansom Ransomware)는 2017년 하반기부터 국내에 활발하게 유포된 랜섬웨어로 사용자의 파일을 암호화하고 이를 복호화해주는 댓가로 금품을 요구하는 악성코드이다. 마이랜섬은 매그니튜드 익스플로잇 킷(Magnitude Exploit Kit)을 통해 유포되며 케르베르(Cerber) 랜섬웨어와 유사하다는 특징이 존재하여 매그니버(Magniber)라고 불리기도 한다. 마이랜섬 랜섬웨어는 다양한 방식으로 유포되는데, 주로 멀버타이징(Malvertising)기법으로 불특정 다수를 감염시키며 공격자에 대한 추적이 어렵다. 마이랜섬은 처음 등장한 이후 감염 방식 등 많은 부분이 계속적으로 변화하였고, 상당한 감염률을 유지하여 국내에 많은 피해를 입힌 후 현재는 유포가 중지된 상태이다. 본 SCH사이버보안연구센터는 마이랜섬의 약 7개월 동안의 유포 과정 중 많은 변형을 탐지 및 분석하였으며, 이러한 사항들을 본 논문에서 서술하고자 한다.

I. 서론

마이랜섬 랜섬웨어는 2017년 하반기에 처음 발견된 랜섬웨어의 한 종류로 사용자의 파일을 암호화하고 랜섬노트를 통해 이를 복호화해주는 댓가로 금품을 요구하는 악성코드[1]이다. 감염방식 및 감염경로 등의 특징이 기존에 활발히 유포되던 케르베르 랜섬웨어와 매우 유사하고, 마이랜섬이 등장한 시점부터 케르베르 랜섬웨어가 활동을 멈춘 것으로 미루어볼 때 케르베르 랜섬웨어의 변종으로 추정된다.



[그림 1 : 2017/2018 Cerber/Magniber 감염추세[2]]

마이랜섬은 감염 대상 PC가 한국어일 경우에만 감염시키는 한국을 대상으로 한 랜섬웨어이다. 랜섬노트에 출력되는 제목인 “My Decryptor”를 참고하여 마이랜섬이라 명명되었고, 매그니튜드 익스플로잇 킷을 통해 감염되고 케르베르 랜섬웨어의 후속 버전이라는 점에서 이 둘의 합성어인 매그니버라는 이름으로 불리기도 한다.

마이랜섬은 2018년 1분기에 국내에서 유포되는 주요 랜섬웨어 중 62%의 점유율[2]을 차지할 정도로 영향력이 컸으며 국내 인터넷 사용자들에게 많은 피해를 입혔다.



[그림 2 : 2018년 1분기 주요 랜섬웨어 현황[2]]

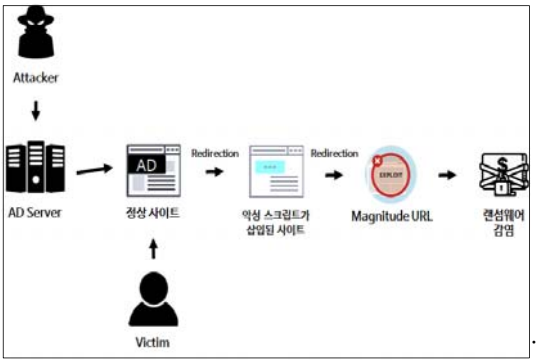
마이랜섬은 온라인 광고를 통해 악성코드를 유포시키는 기법(이하 멀버타이징(Malvertising))으로 2017년 10월부터 2018년 4월까지 약 7개월간 활발하게 유포되었다. 멀버타이징 기법은 악성코드인 'Malware'와 광고를 뜻하는 'Advertising'의 합성어로써 온라인 광고배너에 악성 스크립트를 삽입하여 사용자가 인지하지 못하게 악성코드를 유포시키는 행위[3]를 말하며 대다수의 웹 사이트에서 광고배너를 사용하고 있기 때문에 짧은 시간 동안 많은 사용자가 감염될 수 있다. 과거에 케르베르 랜섬웨어를 유포했었던 다수의 국내 사이트들이 마이랜섬의 유포지로 사용되며 많은 감염자가 발생했다.

마이랜섬은 약 7개월간의 유포 과정 중 실행파일의 확장명, 파일의 저장방식, 실행방식, 사용하는 취약점 등의 변화가 매우 활발하였다.

본 논문에서는 마이랜섬의 유포 과정을 크게 익스플로잇 킷 부분과 실행파일 부분으로 나누어 변화점을 분석하고, 변화의 의도와 그에 대한 결론을 모색해보고자 한다.

II. 마이랜섬의 변화

마이랜섬 랜섬웨어는 멀버타이징 기법을 이용하여 익스플로잇 킷이 설치된 웹 사이트로 사용자의 접속을 유도하고, 사용자가 접속하게 되면 익스플로잇 킷이 사용자 컴퓨터 환경의 취약점을 공격하여 사용자 모르게 악성코드가 자동으로 다운로드되고 실행되는 드라이브 바이 다운로드(Drive-By-Download)기법을 통해 감염된다. 본 장에서는 마이랜섬을 실행파일과 익스플로잇 킷으로 나누어 분석 결과와 변화점에 대해 서술한다.



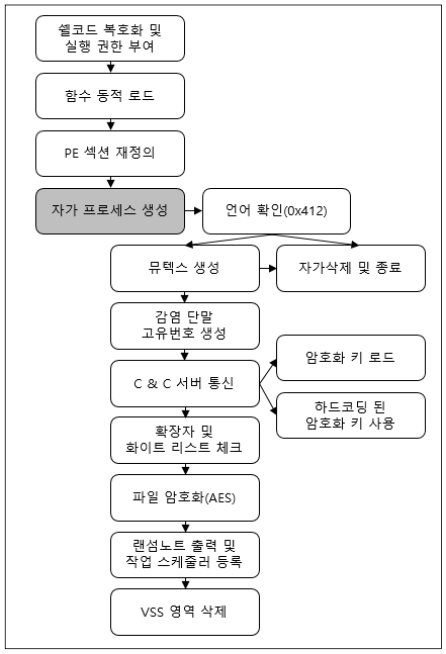
[그림 3 : 마이랜섬 감염과정]

2.1 마이랜섬 실행파일 분석

마이랜섬 분석은 초기 샘플을 기준으로 하며, 변화 사항들은 다음 절에 추가적으로 서술한다.

마이랜섬이 실행되면 먼저 감염 PC의 로케일 언어를 확인하여 그 값이 한국어(0x412)인지 확인하고 아닐 경우 자가 삭제한다. 한국어일 경우에만 암호화를 진행하기 때문에 명확히 한국을 대상으로 유포되는 랜섬웨어임을 알 수 있다. 이후 중복실행을 방지하기 위한 뮤텍스(Mutex)를 생성한다. 파일 실행 시에 중복 실행되어 감염 및 암호화 작업이 원활히 수행되지 못하는 상황을 방지하고 내부에 하드코딩 된 약 800여 개의 확장자를 로드한 뒤 AES 방식으로 암호화한다. AES 암호화는 초기화 벡터(Initialization Vector)와 암호화키를 이용하는 블록암호화 방식이다. 암호화 수행 전에 C&C(Command & Control) 서버로부터 암호화 키를 받아오도록 시도하며, 키를 받아오는데 실패할 경우 내부 하드코딩 된 키와 초기화 벡터를 가지고 암호화를 수행한다.

대부분의 랜섬웨어는 파일을 암호화 할 시 암호화 파일의 확장자가 고정되어 있지만 마이랜섬의 경우 유포 기간별로 암호화 확장자가 랜덤하게 변화하였다. 암호화가 완료되면 볼륨쉐도우 복사본(Volume Shadow Copy)이 삭제되어 복구기능이 동작하지 않도록 하고 레지스트리 변조작업을 통해 작업스케줄러에 랜섬노트를 등록하고 주기적으로 랜섬노트가 출력되도록 한다. 최종적으로 모든 감염 작업을 마치면 자가 삭제하여 자신의 흔적을 제거하고 분석 및 추적이 어렵게 한다.



[그림 4 : 초기 마이랜섬 샘플 동작 순서도]

2.2 Magnitute EK의 변화점

익스플로잇 킷(Exploit Kit)은 소프트웨어(Internet Explorer, Adobe Flash, Java 등)에서 발견되는 보안 취약점을 악용해 악성코드를 유포한다.[4] 특히, 마이랜섬을 유포 시킬 때 사용되는 매그니튜드 익스플로잇 킷(이하 매그니튜드 EK)는 2013년에 최초로 등장하여 다양한 악성코드를 유포하는데 사용되어 왔다. 마이랜섬 유포 시 탐지되는 매그니튜드 EK의 실행 단계로는 크게 3단계로 구성되어 있다.

1. “Magnigate”[5]로 불리는 2단계의 리다이렉션(Redirection) 과정을 거친 후 매그니튜드 EK에 도착함.
2. EK 내부에서 소프트웨어 취약점이 발생하면 공격자가 지정한 원격 코드(Arbitrary Code)를 실행함.
3. 원격 코드 내부에서 C & C 서버로부터 악성코드 다운로드 후 실행함.

마이랜섬 유포 시에는 난독화 방식, 원격 스크립트 로드 방식 등의 다양한 변화를 통해 지속적으로 바뀌어 왔다.

매그니튜드 EK는 마이랜섬 유포 초기에 IE(Internet Explorer) 취약점을 이용하였으나 최신 취약점이 발표되면 매그니튜드 EK에 최신 취약점을 반영하는 동향을 보였다. 또한 그 외에 스크립트 로드방식, 실행 방식 등이 변경되었다.

[표 1 : 매그니튜드 EK 변화점]

변화점	최초	변화
Base64 인코딩 방식	X	O
스크립트 로드 방식	rundll32	rundll32 regsvr32 mshta wscript
확장자	.exe	.com, .cmd, .exe, ADS 등
실행 방식	ShellExecute()	WMIC, forfiles TSWbprxy 등
소프트웨어 취약점	CVE-2016-0189	CVE-2016-0189 CVE-2018-4878

2.3 마이랜섬 실행파일의 변화

마이랜섬 초기버전에서는 “.exe” 파일을 다운받아 실행시켰다. 하지만 얼마 지나지 않아 “.com” 확장자로 변화하였고 그 밖의 “.cmd”, “.[랜덤문자열]” 등으로 주기적으로 변경되며 사용되었다. 이렇듯 초기에는 실행파일을 다운로드 후 단순히 실행하는 방식으로 감염이 이루어 졌지만 이후에는 라이브러리 파일을 다운로드 받아 다른 프로세스를 통해 실행하여 감염시키는 방식을 사용하였다. 랜덤한 이름과 확장자로 DLL 파일을 다운로드 한 뒤 “rundll32.exe” 등 운영체제가 기본적으로 제공하는 응용프로그램을 통해 라이브러리 파일을 로드하여 실행하였다. 또한 ADS(Alternative Data Stream)으로 파일 데이터를 저장하여 일반 사용자의 눈에 띄지 않게 은닉하기도 했다. ADS는 NTFS에서 지원하는 파일에 데이터 스트림 저장 할 수 있는 기능으로 파일명 뒤에 “:” 를 붙이고 데이터 스트림을 지정하는 방식[6]으로 파일을 저장하거나 접근하여 실행할 수 있지만, 탐색기 등 일반적인 방법으로는 파일의 존재를 확인할 수 없기 때문에 파일을 은닉할 수 있다.

파일의 저장과 실행 관련 변화점 이외에 내부 암호화 과정의 기능적인 부분에서도 많은 변화가 존재하였다. 우선, 암호화 대상 확장자를 확인하는 방법을 코드 내부 하드 코딩된 확장자들과 비교하는 방식에서 확장자를 Checksum 형태로 저장하여 비교하는 방식으로 변경하여 구체적으로 어떤 파일확장자를 암호화하는지 분석하기 어렵게 하였고, 암호화 키를 로드하는 부분을 C&C 서버에서 키를 받아온 후 암호화를 진행하는 방식에서 내부 하드 코딩된 키를 이용하는 방식으로 변화하였다.

[표 2 : 마이랜섬 변화점]

특징	최초	변화
암호화 대상 확장자 확인 방법	내부 하드코딩	Checksum 형태 확인
암호화 키 로드 방식	C & C 서버 (실패 시, 하드코딩 된 키 사용)	내부 하드코딩
파일 포맷	exe	exe, dll
랜섬노트	READ_ME_FOR_DECRYPT.txt	READ_ME.txt
암호화 방식	AES 암호화 방식	
개발 언어	C/C++, Windows Programming	

III. 결론

본 논문에서는 매그니튜드 익스플로잇 킷으로 유포되는 마이랜섬의 변화 및 동향을 분석하였다. 마이랜섬은 국내를 타겟으로 한 랜섬웨어로 국내 백신업체의 대응에도 발 빠르게 변화하며 국내 인터넷 사용자를 위협해왔다. 마이랜섬은 현재 암호화에 사용되는 키를 코드 내부에 하드 코딩 해놓은 문제로 복호화 툴이 개발되어 피해를 줄일 수 있게 되었고 복호화 툴이 공개된 시기에 맞물려 현재는 유포가 중지된 상태지만 초기 버전처럼 C&C 서버에서 키를 다운받아 암호화를 진행하도록 변경되거나 공개키 암호화 방식을 도입하는 등으로 변화할 경우 복호화가 원천적으로 불가능하게 될 수 있다. 또한 매그니튜드 EK에 새로운 취약점이 지속적으로 추가될 가능성이 있고, 마이랜섬의 유포가 중단되기 직전까지 변화가 활발했던 점에서 지금까지 발견된 문제점들이 해결된다면 더욱 강력한 랜섬웨어로 변화하여 다시 유포될 수 있다.

국내 인터넷 사용자를 위협하는 랜섬웨어는 나날이 진화하며 지능화되고 있다. 이러한 랜섬웨어의 위협을 좀 더 발 빠르게 탐지하고 대응하여 피해를 최소화 할 수 있는 보안체계가 필요한 시점이다.

[참고문헌]

[1] 한국인터넷진흥원, 랜섬웨어 정의 및 감염경로, https://www.krcert.or.kr/ransomware/information.do

[2] 안랩, 2018년 1분기 랜섬웨어 동향 2018.4, http://asec.ahnlab.com/1132

[3] 한국정보보호진흥원, 온라인 광고배너를 통한 악성코드 유포대응 보안 가이드 2p, 2016.10

[4] PaloAlto Network, What is an Exploit Kit?, https://www.paloaltonetworks.com/cyberpedia/what-is-an-exploit-kit

[5] ProofPoint, Magnitude Actor Adds a Social Engineering Scheme for Windows 10, https://www.proofpoint.com/us/threat-insight/post/magnitude-actor-social-engineering-scheme-windows-10

[6] Microsoft, How To Use NTFS Alternate Data Streams, https://support.microsoft.com/en-ca/help/105763/how-to-use-ntfs-alternate-data-streams

랜섬웨어 Native API 정보 분석을 통한 탐지 방법 연구

장준영 김우재* 옥정윤** 임을규***

*한양대학교 컴퓨터 공학과

**한양대학교 정보보안학과

***한양대학교 컴퓨터소프트웨어학부

Research on ransomware detection through Native API information analysis

Jun-Young Chang Woo-Jae Kim* Jeong-Yun Oak** Eul-Gyu Im***

*Division of Computer Science, Hanyang University.

**Department of Information Security, Hanyang University

***Department of Computer and Software, Hanyang University

요 약

최근 파일을 암호화하는 악성코드인 랜섬웨어(ransomware)가 유행하고 있다. 비트코인(bitcoin)의 등장으로 해커는 손쉽게 사용자에게 금전을 요구할 수 있게 되었기 때문에 앞으로도 랜섬웨어는 꾸준히 유행할 것으로 보인다. 랜섬웨어가 파일을 암호화할 때 일반적인 프로그램과 마찬가지로 프로세스(process)를 생성하고, API(Application Programming Interface)를 호출한다. 본 논문에서는 프로세스 API 중에서 실제 시스템 영역에 접근하는 윈도우 Native API[1]들을 서열과 빈도수를 중심으로 분석하여 랜섬웨어의 특징을 추출, 분류한다. 결과적으로 파일의 프로세스 API 정보를 주었을 때 해당 파일이 랜섬웨어인지, 안전한 실행 파일인지 정확히 판별하는 것이 목표이다.

I. 서론

IT 기술은 시대가 거듭할수록 점점 발달 되고, 그 영향도 커지며 많은 분야에 적용되고 있다. 이에 따른 부작용들도 나타나고 있으며, 그 중 하나가 공격 대상 증가에 따른 사이버 공격의 증가이다. 과거 대부분의 사이버 공격의 경우, 개인의 해킹 기술을 과시하거나 호기심이 목적이지만 오늘날에는 금전적인 이득을 취하기 위한 수단으로 사이버 공격이 행해진다.

금전적 이득을 위한 대표적인 사이버 공격이 랜섬웨어이다. '몸값(ransom)'과 '소프트웨어(software)의 합성어인 랜섬웨어는 시스템 및 데이터를 암호화하여 사용할 수 없도록 만든 후, 이를 인질로 삼아 금전을 요구하는 악성 프로그램이다. 2005년에 본격적으로 알려지기 시작했지만, 이 시기에는 낮은 암호화 수준으로 복호화 방법을 통해 쉽게 데이터를 복구할 수 있었다. 하지만 2013년 거래가 쉬운 비트코인이 개발되어 직접적인 금품요구가 쉬워지고, 강력한 암호화 알고리즘을 이용한 랜섬웨어가 등장하면서 전 세계적으로 공공기관, 기업, 개인 PC 등을 향한 공격이 매년 늘어나는 추세이다. 이스트소프트에서 발표한 2016년 랜섬웨어 동향 결산[2]에 따르면 국내의 경우 2016년 한해 알약 백신을 통해 사전 차단된 랜섬웨어 공격이 총 397만 4,658건으로 적지 않은 수의 랜섬웨어 공격 시도가 발생한다는 것을 알 수 있다.

이처럼 매년 수가 급격히 증가하고 그 수법도 매우 고도화되는 랜섬웨어를 분석하고 그

특징을 도출해내려는 시도는 이전부터 있었다. 하지만 빠른 속도로 변종이 생성되기 때문에 이미 검출된 악성코드의 특징을 이용해 유사한 악성코드를 검출하는 방식으로 탐지하기는 어렵다[3]. 따라서 분석가들이 직접 로그(log) 파일을 살펴보며 랜섬웨어의 특징들을 찾아내야 한다. 이 과정에 Cuckoo sandbox[4]라는 분석 도구가 많이 사용되는데, 이는 가상머신 환경에서 직접 악성코드를 실행하며 발생하는 프로세스, 메모리, 네트워크 등을 동적 분석할 수 있게 해주는 시스템이다.

본 논문에서는 이 Cuckoo sandbox의 분석 결과로 생성된 로그 파일에서 프로세스 API, 그중에서 Native API에 집중해 실제로 랜섬웨어가 사용자의 컴퓨터를 암호화하는 과정에서 사용되는 API들의 상관관계를 서열과 빈도수를 중심으로 분석할 것이다.

II. 배경지식

2.1 랜섬웨어

랜섬웨어는 크게 사용자 화면을 장악하는 Lock Screen 랜섬웨어, 데이터를 암호화하는 Encryption 랜섬웨어, boot 영역을 훼손하는 Master Boot 랜섬웨어, 안드로이드 기기를 대상으로 하는 Mobile Device 랜섬웨어[5]로 나누어지며, 2017년 기준으로 우리나라에 보고된 랜섬웨어는 275종에 이른다[6]. 본 논문에서는 이 중에서도 2017년 5월 전 세계 90개국 이상에 대규모로 전파된 WannaCry(또는 WannaCrypt)[7] 랜섬웨어를 주요 대상으로 한다. 이 랜섬웨어는 마이크로소프트 윈도우 운영체제에서 파일 공유에 사용하는 서버 메시지 블록(Server Message Block)의 취약점을 이용한 Encryption 랜섬웨어로, 최신 윈도우 보안 패치를 적용하지 않아 보안이 취약한 PC로 전파되며 PC 내 다양한 문서파일과 압축파일, DB 파일 등을 암호화하여 사용할 수 없게 만든다. 이메일 첨부파일을 통해 유포되는 일반적인 랜섬웨어와 달리 인터넷 네트워크 접속만으로 감염되는 특징을 가진다.

2.2 Cuckoo sandbox

프로그램의 행위 분석은 크게 정적 분석과 동적 분석으로 나뉜다. 정적 분석은 실제 실행 없이 소프트웨어를 분석하는 방식으로, 코드 분석을 통해 프로그램의 실행 방향을 예측한다. 하지만 대부분의 악성 프로그램들은 난독 화 과정을 거치기 때문에 분석이 어렵다. 따라서 악성코드는 주로 동적 분석을 한다. 행위 자체를 탐지하기도 쉽고, 무엇보다 행동 과정을 실제로 지켜볼 수 있기 때문이다. 하지만 동적 분석을 시행하려면 실제로 악성코드를 작동시켜야 하기 때문에, 실험 장비가 감염될 가능성이 있다. 본 실험에서는 Cuckoo sandbox 오픈소스 악성코드 분석 시스템을 사용한다. 이 시스템에 악성 프로그램을 입력하면 Cuckoo sandbox가 관리하는 독립된 가상 환경에서 실제로 악성코드를 실행하고, 이때 발생하는 프로세스, 메모리, 네트워크 변화를 기록한다. 이 분석 결과 보고서는 JSON 등의 형식으로 저장되는데, 사용자는 이 분석 보고서만으로 안전한 환경에서 악성 프로그램을 살펴볼 수 있다.

2.3 Native API

프로그램은 실행 과정에서 프로세스를 생성하고, 다양한 API를 호출한다. 이 중에서 Native API는 일반적으로 사용자가 접근하지 못하는 OS의 기능들을 간접적으로 호출할 수 있는 도구로, 그 이름과 역할이 정해져 있다. 따라서 이전까지 없던 변종 프로그램이 등장하더라도 미리 알려진 Native API를 사용할 수밖에 없다. 본 논문에서는 랜섬웨어가 실행될 때 호출되는 프로세스 API를 추출, 그중에서 Native API만을 추려내어 변종에 대응할 수 있는 탐지 방법을 목표로 진행한다.

III 실험설계

3.1 샘플 분석 방식

총 두 가지 기준으로 API를 분석하는데, 호출된 모든 API를 서열화하여 순서대로 나열한 후 특정 그룹의 API 출현 정도 등을 조사하는 서열 중심 분석 N-gram 방식[8]과 어떤 종류의

API가 등장하고, 어떤 API가 빈번히 호출되는지를 빈도수 중심으로 분석하는 TF-IDF 방식[9]을 사용한다.

3.1.1 서열 중심 분석 (N-gram)

N - gram은 문서 간의 유사함을 찾기 위해 처음 제안된 기법으로, 연속한 N개의 단어나 텍스트를 하나의 하위 문자열로 나누어 통계학적으로 사용하는 방법을 말한다. N의 단위는 1bit, 1byte부터 하나의 단어나 음절까지 필요에 맞는 기준에 따라 자유롭게 선택할 수 있으며, N-gram으로 생성된 하위 문자열의 빈도수를 이용하여 문자의 유사도를 측정한다. 예를 들어 "랜섬웨어"라는 문자열에 2-gram을 적용하는 경우 "랜섬", "섬웨", "웨어"라는 3가지 하위 문자열이 생성되며, 각각 하위 문자열의 빈도수는 1이다.

본 논문에서는 각각의 Native API 이름을 그대로 사용하지 않고, Native API 이름을 각각 A1, B1 등과 같이 고유한 문자에 대응시켜, 이를 N - gram에 적용하였다.

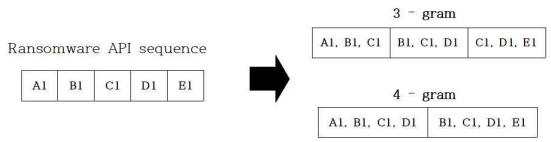


그림 1 서열 정렬 예시

N-gram의 경우 단순한 형태의 분석법이기 때문에, 결과를 가공할 필요가 있다. 가장 대표적으로 사용하는 방법이 의미가 없이 사용되는 조사나 연결어인 불용어를 제거하는 것이다. 이를 본 실험에 적용하여 일반 파일의 특징 서열을 불용어로 설정하여, 불용어를 제거한 경우와 아닌 경우를 나누어서 실험을 진행했다.

3.1.2 빈도수 중심 분석(TF-IDF)

TF-IDF는 문서에서 특정 단어가 얼마나 자주 나타나는지에 대한 정보(TF)와 특정 단어가 얼마나 많은 문서에서 등장하는지, 즉 얼마나 흔한 단어인지에 대한 정보의 역수(IDF)를 이용하여 문서와 단어 간의 관련성을 비교한다. 이를 계산하는 식은 분석 대상에 따라 다양하게 적용할 수 있다[10].

$$TF\text{-}IDF = TF * IDF \quad (1)$$

TF는 Term Frequency의 약자로, 한 문서 내에서 특정 단어가 얼마나 빈번히 등장하는지를 계산한 식이다. 단순히 전체 단어 개수로 특정 단어 개수를 나눈 값을 이용하거나, 문서 내 등장 여부만을 기록하는 Boolean 빈도 계산법, 또는 가중치를 적게 주고 싶을 때 로그를 취한 값을 사용할 수도 있다.

IDF는 Inverse Document Frequency의 약자이다. 특정 단어가 모든 문서에서 등장한다면 이 단어는 문서를 분류하는 특징이 부족하다고 할 수 있는데, 이런 사실을 이용해 전체 문서 중 특정 단어가 나타난 문서 수를 세어 이를 역수로 계산한다. TF 계산과 마찬가지로 주고 싶은 가중치에 따라 단순 개수 계산부터 로그 취한 값 계산까지 다양하게 적용할 수 있다.

본 논문에서는 이러한 특징 추출 방식을 프로그램과 API로 확장해서, 특정 API와 프로그램과의 연관성을 나타낼 수 있는 지표로 사용한다. 하지만 보통의 문서와 단어의 관계는 프로그램과 API의 관계와 차이점이 있다. 첫째, 본 논문에서 대상으로 삼는 Native API는 단어와는 다르게 그 수가 매우 제한적이다. 따라서 같은 API가 훨씬 빈번히 사용된다. 둘째, 악성코드는 탐지를 피하려고 의도적으로 불필요한 기능을 여러 번 수행해 본연의 목적을 숨기거나 전혀 불필요한 행동을 하기도 한다. 따라서 같은 기능을 수행하는 샘플이 더라도 전혀 다른 API를 추가로 사용할 수도 있다.

이러한 어려움 때문에 랜섬웨어를 다른 프로그램과 구별하기 위해 TF, IDF 어느 쪽에 가중치를 더 부여해야 하는지에 대한 정확한 기준을 세우기가 힘들다. 이 때문에 실험을 다양하게 설계하여 진행하였다. 수식을 선형적으로 또는 지수적으로 설정하기도 했고, 특정 요소를 아예 제외하기도 했다.

3.2. 유사도 측정 방식

샘플을 분석하여 나온 결과값과 분석하려는 대상의 유사도를 측정하는 방식에는 여러 가지

가 있지만 본 논문에서는 코사인 유사도(cosine similarity)를 사용하였다. 코사인 유사도는 두 벡터의 유사도를 측정하기 위한 간단한 공식이다. 이때 벡터의 크기가 아닌 방향성의 유사도를 판단한다. 코사인 유사도를 구하기 위한 공식은 다음과 같다.

$$\text{Similarity} = \frac{\sum_{i=1}^{n} A_i B_i}{\sqrt{\sum_{i=1}^{n} A^2 \sum_{i=1}^{n} B_i^2}} \qquad (2)$$

일반적으로 방향이 완전히 일치하면 1, 완전히 반대이면 -1의 값을 갖지만, TF-IDF처럼 값이 음수를 갖지 않는 경우는 0에서 1 사이의 범위의 값만을 가진다. 샘플들과 분석하려는 대상의 코사인 유사도를 계산하여 두 대상 사이의 유사도를 측정할 수 있다.

Ⅳ 실험내용

본 논문에서는 서열 중심 분석과 빈도수 중심 분석을 위해 Cuckoo sandbox를 활용하여, 'report.JSON' 파일을 생성하여 분석했다.

4.1 서열 중심 분석

서열 중심 분석을 하기 위해 500개의 랜섬웨어의 모든 Native API를 추출하여 고유한 문자표를 생성했다. 중복된 값은 삭제하고 하나의 Native API에 하나의 고유한 문자를 배정했다.

표 1 고유한 문자로 변환된 Native API

Native API	Unique code
NtQueryAttributesFile	A0
NtResumeThread	A1
NtOpenKeyEx	A2
RtlDecompressBuffer	A3
…	…
NtEnumerateValueKey	F6

총 57개의 Native API가 추출되었다. 이렇게 변환된 Native API 고유 문자를 하나의 N으로 하여, 4개의 고유 문자가 묶여 하위 문자열을 생성하는 4-gram으로 실험을 진행했다[11]. 유의미한 결과를 도출하기 위해 4-gram의 모든 하위 문자열의 빈도수가 1인 결과는 제외하였다. 위의 결과를 통해 나온 결과를 바탕으로, 랜섬웨어 특징 Native API 서열 찾기 위해 TF-IDF 식에서 TF 값만을 이용했다. 전체 빈도수를 TF를 통해 빈도수를 측정하지 않고, 각각의 파일에 대해서 TF를 적용하여 빈도수를 측정했다. 이는 똑같은 서열이 특정 파일에서 많이 측정되어 전체 결과값에 영향을 미칠 수 있기 때문이다. TF에 따라 랜섬웨어의 특징이 되는 서열이 결정되므로 적당한 크기를 가지며 랜섬웨어의 특징을 가지는 TF 값을 결정해야 한다. 그림 2 을 보면, TF 값을 0.01 이상의 TF 값만을 사용하는 경우 1760개의 서열이 특징 서열로 선택되기 때문에 올바르지 않다. 0.04 보다 큰 값으로 하는 경우 28개의 서열이 선택되지만, 랜섬웨어를 대표하는 특징이 부족했다. 실험을 통해 최적의 TF 값 0.038 이상을 이용하여 32개의 랜섬웨어 특징 서열을 도출했다.

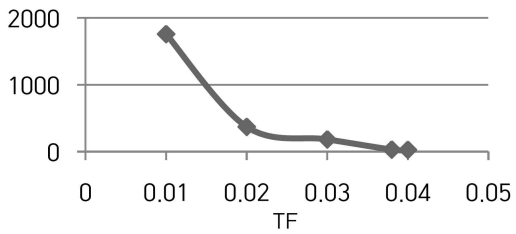


그림 2 TF에 따른 특징 서열의 개수 변화

이를 이용하여, 각각 랜섬웨어 파일 165개, 일반 파일 123개를 이용하여 실험을 진행했다.

4.1.1 랜섬웨어 특징 서열 이용

랜섬웨어 특징 서열만을 이용하여 실험을 진행하였다. 165개의 랜섬웨어 파일을 각각 65개의 랜섬웨어 파일 R1, 100개의 랜섬웨어 파일 R2로 나누고, 123개의 일반 파일을 77개의 일반 파일 N1, 46개의 일반 파일 N2로 나누어 실험을 진행하였다. R은 랜섬웨어 특징 서열을 가지고 있어 랜섬웨어로 분류된 것을 나타내고 'No R' 특징 서열이 없어서 일반 파일로 분류된 것이다. 실험 결과는 아래 그림 3이다.

.

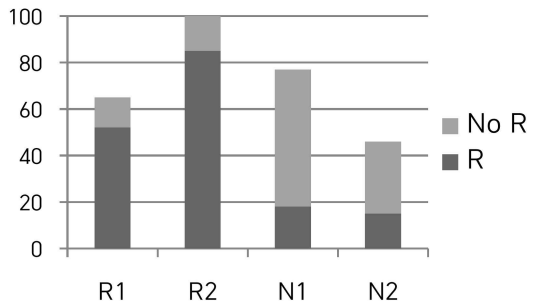


그림 3 랜섬웨어 특징 서열을 이용한 실험 결과

그림 3에서 알 수 있듯이 R1은 80%, R2는 85%의 확률로 랜섬웨어 파일을 랜섬웨어로 분류했다. 하지만 일반 파일의 경우 N1은 27%, N2는 32%의 확률로 일반 파일을 랜섬웨어로 분류했다.

4.1.2 일반 파일 특징 서열을 제거

랜섬웨어 특징 서열 32개에서 일반 파일 특징 서열 28개 중 중복되는 값을 제거하여, 18개의 특징 서열만을 가지고 실험을 진행했다. 실험 결과는 아래 그림 4와 같다.

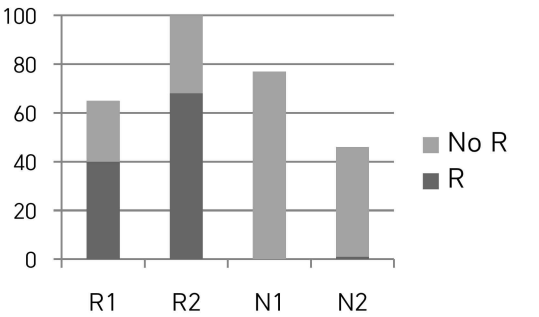


그림 4 일반 특징 서열을 제거한 실험 결과

랜섬웨어를 일반 파일로 분류하는 오류가 증가했지만, 일반 파일을 랜섬웨어로 분류하는 오류는 1% 내외로 측정된다.

4.2 빈도수 중심 분석

분석 대상 파일 종류에 따른 특징을 분석하기 위해, 유해하지 않은 실행 파일과 랜섬웨어가 아닌 악성코드, 랜섬웨어 샘플 각 400, 400, 800개를 대상으로 실험을 진행하였다. 여러 가지 고려해야 할 조건들이 혼합되어 있으므로 어떤 수식을 사용해야 가장 바람직한 결과를 도출해낼 수 있는지 알아내기가 힘들므로 여러 조건에서 실험을 진행했다.

실험 진행 순서는 다음과 같다.

(1) 각 분석 샘플의 Cuckoo sandbox 분석 보고서에서 Native API의 이름과 개수만을 추출한다.

(2) 샘플 별로 API별 TF 값을 계산하여 저장한다.

(3) API별 IDF 값을 계산하여 샘플별 TF-IDF 값을 저장한다.

(4) 샘플 전체에 대한 TF-IDF 평균을 구한다.

(5) 비교하려는 대상의 TF-IDF 값을 구한다.

(6) 두 TF-IDF 값으로 코사인 유사도를 측정한다.

이때 각 문서의 TF 값 계산, 샘플 전체의 IDF 값 계산에서 수식을 변화시킬 수 있다. 식의 항등원을 이용해서 특정 값을 아예 계산식에서 제외하거나, 선형적으로 계산하거나, 로그 취한 값으로 계산하여 실험을 진행하였다. 계산에 이용한 식은 다음과 같다.

$$TF = w / d \quad (3)$$

$$TF = \log(1 + w / d) \quad (4)$$

w를 문서 내 특정 API의 등장 횟수, d를 문서 내 전체 API의 수라고 했을 때 TF 값은 수식 (3)처럼 비율로 계산할 수도 있고, 이 값에 계산할 수도 있다. 이때 특정 샘플에서는 아예 계산하려는 API가 등장하지 않을 수 있으므로 수식(4)에서 로그 계산식에 1을 더해주었다.

$$IDF = 1 \quad (5)$$

$$IDF = \log(N / n) \quad (6)$$

$$IDF = N/n \quad (7)$$

IDF의 계산식도 TF와 유사하다. 전체 문서 수를 N, 특정 API가 등장하는 문서 수를 n이라고 했을 때 비율의 역수 또는 그것의 로그 값으로 계산할 수 있다. 또 아예 IDF의 값을 1로 지정해 TF 값 비교만으로도 유의미한 결과가 나오는지 실험을 진행했다.

분석하려는 대상은 그 개수가 하나이므로 IDF 값을 어떻게 부여해야 할지도 정해야 한다. IDF 값에 1을 부여하여 계산식에서 제외하거나, 샘플의 IDF와 같은 값을 사용하는 두 가지 방법을 채택했다.

동일한 샘플을 대상으로 위의 다각적 실험을 진행한 결과 랜섬웨어가 아닌 경우와 랜섬웨어인 경우 탐지율은 다음과 같았다. (ⅰ)는 검사하려는 파일의 IDF 값을 1로 준 경우이고, (ⅱ)는 샘플과 같은 IDF 값을 사용한 경우이다.

표 2 코사인 유사도 실험 결과

input / sample	수식 (3)	수식(4)
수식 (5)	(ⅰ)98.75%, 34.375% (ⅱ)98.75%, 34.375%	(ⅰ)98.75%, 41.5% (ⅱ)98.75%, 41.5%
수식 (6)	(ⅰ)90.5%, 58.25% (ⅱ)85.375%, 55.0%	(ⅰ)90.5%, 60.25% (ⅱ)85.125%, 56.875%
수식(7)	(ⅰ)97.75%, 48.625% (ⅱ)97.5%, 65.25%	(ⅰ)97.75%, 52.25% (ⅱ)97.625%, 68.25%

실험 결과로 보아 TF의 값은 로그를 취해 계산하고, IDF의 값은 선형적으로 계산하는 것이 랜섬웨어의 탐지율을 높일 수 있었다. 즉 랜섬웨어 탐지는 TF보다는 IDF에 더 의존적으로 나타났다. 수가 한정된 Native API라고 할지라도, 특정 API가 결과물에 등장하는지 아닌지의 정보가 중요하다고 판단할 수 있다. 또한 검사하는 파일의 IDF 값 설정에 따라서 결과가 크게 차이가 나는 것으로 보아, 해당 값을 적절하게 부여한다면 높은 탐지율을 얻을 수 있을 것으로 기대된다.

Ⅴ 결론

서열, 빈도수 두 가지 요소를 기준으로 악성코드를 탐지한 결과 랜섬웨어 탐지 면에서는 랜섬웨어의 특징 서열만 이용한 N-gram 분석 방식이 더 높은 탐지율을 보였고, 랜섬웨어가 아닌 파일을 탐지할 때는 TF-IDF 식을 사용한 방식이 높은 탐지율을 보였다. 따라서 이 두 방식을 혼합하여 사용한다면 높은 정확도로 파일을 랜섬웨어인지 아닌지 구별해낼 수 있을 것이다. 본 논문에서 사용한 프로그램 샘플은 한정적이지만, 좀 더 다양하고 많은 수의 샘플을 사용하여 특징을 추출한다면 더 높은 정확도로 파일을 분류해 낼 수 있을 것으로 기대된다.

[참고문헌]

[1] Native API, https://en.wikipedia.org/wiki/Native_API

[2] 2016년 랜섬웨어 동향 결산, https://www.estsecurity.com/

[3] 주정욱, “회피기법이 있는 악성코드 분석을 위한 샌드박스용 사용자 이벤트 발생기 설계”, 목포대학교 대학원, 2015

[4] Cuckoo Sandbox 공식 홈페이지, http://www.cuckoosandbox.org/

[5] No More Ransom, Types of Ransomware, https://www.nomoreransome.org/ransomware-qa.html

[6] 한국인터넷진흥원, 사이버 위협 동향 보고서, http://www.kiise.or.kr/academy/main

[7] 김소람, “최신 랜섬웨어에 대한 암호키 복구 방안 연구”, 국민대학교, 2017

[8] 심유진, “API 호출 시퀀스 기반 악성코드 탐지 및 분류 시스템”, 한양대학교, 2016

[9] Christopher D. Manning, Prabhakar Raghavan, "An Introduction to Information Retrieval", Cambridge University Press, pp. 117-128, April, 2009

[10] Amit Singhal, “Modern Information Retrieval: A Brief Overview”, Bulletin of the IEEE Computer Society Technical Committee on Data Engineering, 2001

[11] 권희준, 김선우, 임을규, “Multi N-gram을 이용한 악성코드 분류 시스템”, 보안공학연구논문지 제 9권 제 6호, pp. 531-542, 2012

2018 한국정보보호학회 하계학술대회

C1 암호화폐/블록체인 3

유 일 선 (순천향대학교)

- **스마트 컨트랙트의 취약점과 취약점 분석 도구에 대한 연구**
  민정기, 김승주
- **비트코인 거래 생성 시간 필드를 추가한, 이기적 채굴 대응방안 개선**
  이지혜, 김윤정
- **국외 블록체인 기반 전력 시스템 보안 연구 동향 및 국내 블록체인 기반 전력시스템 적용 방안**
  김효빈, 홍기섭, 서정택
- **블록체인 확장성 문제에 대한 분석과 고찰**
  노시완, 이경현

스마트 컨트랙트의 취약점과 취약점 분석 도구에 대한 연구

민정기, 김승주

고려대학교 정보보호대학원

A Survey on Smart Contract Vulnerabilities and Vulnerability Analysis Tools

Jungki Min, Seungjoo Kim

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

요 약

이더리움 스마트 컨트랙트가 사용되면서, 스마트 컨트랙트의 취약점 때문에 많은 사건이 발생하고 있다. 대부분의 스마트 컨트랙트의 취약점은 프로그래머가 의도한 바와는 다르게 스마트 컨트랙트가 작동하는 의미론적 차이에 의해 발생한다. 이러한 취약한 스마트 컨트랙트는 금전적인 피해를 야기한다. 본 논문에서는 스마트 컨트랙트의 취약점을 조사해 분류하고, 예시를 들어 설명하였다. 또한 스마트 컨트랙트 취약점 분석 도구들을 조사하고, 각 도구들이 커버할 수 있는 취약점을 비교하였다.

I. 서론

스마트 컨트랙트[1]는 1994년 Nick Szabo에 의해 제안된 개념으로, 디지털 명령어로 작성된 계약 프로그램을 말한다. 기존의 자연어로 된 계약서의 경우, 계약 조건을 이행하기 위해서는 계약 내용에 대해 이해한 후, 계약서에 쓰인 내용을 사람이 실제로 이행해야하지만, 스마트 컨트랙트는 규칙이 프로그래밍 언어로 코딩되어 있어 계약 조건에 따른 계약 결과가 명확하고, 계약 내용을 즉각 이행할 수 있다는 편리함이 있다. 계약에 참여[1]하는 당사자들이 직접 만나지 않고 서로 언어가 통하지 않더라도, 스마트 컨트랙트에 프로그래밍 언어로 명시된 계약 내용은 컴퓨터가 자동으로 처리해주기 때문에 기존의 계약을 이행하는데 필요한 복잡한 프로세스를 간소화할 수 있다는 장점이 있다. 그러나 스마트 컨트랙트가 제안된 당시에는 디지털로 된 스마트 컨트랙트는 쉽게 조작될 수 있다는 문제점이 제시되어 개념상으로만 존재하고 실제 서비스로 사용되지는 않았다.

이더리움[2]은 이러한 기존의 스마트 컨트랙트의 문제점을 블록체인으로 보완한 분산 컴퓨팅 플랫폼이다. 이더리움 가상머신에서 돌아가는 튜링 완전 언어를 이용해, 사용자들은 자신이 원하는 스마트 컨트랙트를 구현할 수 있고, 이를 이더리움 블록체인 상에 저장해 계약 내용과 상태 정보의 무결성을 보장할 수 있다. 스마트 컨트랙트의 내용과 상태 정보가 공격자에 의해 조작될 경우, 스마트 컨트랙트에 저장되어 있는 암호 화폐가 컨트랙트에 묶여서 사용 불가능해지거나, 공격자의 손으로 흘러들어갈 수 있기 때문에, 스마트 컨트랙트의 무결성을 지키는 것은 컨트랙트가 제 기능을 하기 위해서 달성되어야 할 필수 조건이다.

그러나 최근 몇 년간 발생한 이더리움 스마트 컨트랙트에 대한 공격 사례를 보면, 단순히 컨트랙트의 무결성의 문제가 아니라,

1) 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2018-2015-0-00403)

컨트랙트 코드의 취약점이 심각한 문제를 야기한다는 것을 알 수 있다. 2016년 발생한 DAO(Decentralized Autonomous Organization) 공격은 스마트 컨트랙트의 reentrancy 취약점을 이용한 공격으로, 당시 1500억원 가량의 피해액을 발생 시켰고, 2017년 발생한 Parity Multisig Wallet 사건은 스마트 컨트랙트의 초기화 부재로 인한 컨트랙트 권한 문제로 600억원 가량의 피해액을 발생 시켰다. 스마트 컨트랙트의 취약점은 대부분 프로그래머의 의도와 스마트 컨트랙트 언어상의 의미론적 차이 때문에 발생한다. 프로그래머가 의도한대로 스마트 컨트랙트가 동작하지 않을 경우 위의 공격 사례와 같은 심각한 금전적 피해를 불러올 수 있다. 또한, 스마트 컨트랙트는 그 특성상 한번 블록체인에 저장되면 그 내용을 수정할 수 없기 때문에, 취약한 스마트 컨트랙트 코드를 패치하는 것이 불가능하다. 따라서 스마트 컨트랙트 프로그래머들은 블록체인에 스마트 컨트랙트를 저장하기 전에 신중하게 스마트 컨트랙트의 안전성을 검토할 필요가 있다. 이를 위해 스마트 컨트랙트 코드 상의 취약점을 발견할 수 있는 여러 도구들[3,4,5]이 개발되었다.

본 논문에서는 이더리움 스마트 컨트랙트의 취약점들을 분류하고 각각에 대한 예시를 들어 설명한다. 또한 현존하는 스마트 컨트랙트 취약점 분석 도구 총 3종(Oyente[3], Zeus[4], Maian[5])에 대해 소개하고, 분류된 취약점을 얼마나 커버할 수 있는지를 비교한다.

II. 스마트 컨트랙트 취약점

스마트 컨트랙트의 취약점은 크게 5가지로 reentrancy, integer over/underflow, mishandled exception, timestamp dependence, suicidal contract 가 있다.

2.1 Reentrancy

Reentrancy 취약점은 2016년 발생한 DAO 공격의 원인이 된 취약점으로, 스마트 컨트랙트의 폴백 함수 내부에서 다른 스마트 컨트랙트를 호출할 수 있다는 것을 이용한 취약점이다. [그림 1]을 보면, attacker 컨트랙트의 attack 함수가 victim 컨트랙트의 withdraw 함수를 호출하고, withdraw의 call.value 함수가 다시 attacker 컨트랙트의 폴백 함수를 호출한다. 이는 다시 victim 함수의 withdraw 함수를 호출하는데, 이 때 아직 victim 컨트랙트의 7번째 줄이 실행되지 않은 상태기 때문에, 공격자의 잔고가 업데이트되지 않았으므로 조건문의 결과가 참이 되어 다시 공격자에게 돈을 보내게 되고, 이는 또 다시 attacker 컨트랙트의 폴백 함수를 호출하게 된다. 이러한 호출이 반복되는 이유는 victim 컨트랙트의 잔고가 업데이트 되지 않은 상태에서 계속해서 조건문을 검사하기 때문에, 설령 의미론적으로는 조건문이 거짓이라 하더라도, 실제 코드 흐름상으로는 조건문이 항상 참이 될 수밖에 없기 때문이다.

```
1  contract victim {
2      mapping (address => uint) balances;
3      function save(){balances[msg.sender] += msg.value;}
4      function withdraw(uint amount){
5          if(balances[msg.sender]>=amount){
6              msg.sender.call.value(amount)();
7              balances[msg.sender]-=amount;
8  }}}
9
10 contract attacker {
11     function(){ victim.withdraw(1); }
12     function attack(){ victim.withdraw(1); }
13 }
14 contract attacker2 {
15     bool trigger = true;
16     function(){
17         if(trigger){
18             trigger=false;
19             victim.withdraw(1);
20         }}
21     function attack(){
22         victim.save.value(1)(this);
23         victim.withdraw(1);
24 }}
```

[그림 1] reentrancy, integer underflow 취약점 코드

2.2 Integer Over/Underflow

Integer over/underflow 취약점은 스마트 컨트랙트 언어가 암시적인 타입 확장을 허용하지 않기 때문에 발생하는 취약점이다. 따라서 프로그래머는 이를 염두에 두고 경계값 체크를 반드시 해야 한다. [그림 1]의 attacker2 컨트랙트는 이러한 integer underflow 취약점과 reentrancy 취약점을 결합한 공격이다. attacker2 컨트랙트는 처음에 1 wei를 저축해 잔고를 1 wei로 만들고, 다시 그만큼 인출한다. 이 때, withdraw 함수 내부의 call.value 함수가 호출되고, 그에 따라 attacker2의 폴백 함수가 호출되는데, 이 안에서 또 다시 1 wei만큼 인출을 시도한다. 이 때, reentrancy 공격 때와 마찬가지로 잔고 업데이트가 아직 되지 않았기 때문에 또 다시 인출이 가능해진다. 이 때, trigger 값을 통해 공격을 멈추고 나면, attacker2의 잔고의 최종 상태는 최초 상태(0)에서, attack 함수 내의 save로 +1, attack 함수 내의 withdraw로 -1, 폴백 함수 내의 withdraw로 -1이 되어 최종적으로 -1이 된다. 그러나 잔고의 타입은 uint 인데, 이는 unsigned integer 값으로 32비트 환경에서 0부터 $2^{32}-1$의 값을 가지기

때문에 underflow가 발생해 attacker2의 잔고가 $2^{32}-1$이 된다.

```
contract KotET {
    address public king;
    uint public claimPrice=100;
    address owner;

    function kotET(){ owner=msg.sender; king=msg.sender; }
    function sweepCommision(uint amount){ owner.send(amount); }
    function (){
        if(msg.value<claimPrice) throw;
        uint compensation=calculateCompensation();
        king.send(compensation);
        king=msg.sender;
        calimPrice=calculateNewPrice();
}}
```

[그림 2] 간소화된 King of Ether Throne[6] 취약점 코드

2.3 Mishandled Exception

Mishandled exception은 스마트 컨트랙트 언어상에서 예외처리를 하는 방식이 일관되지 않기 때문에 발생하는 취약점이다. 예외가 발생하는 경우에 따라 예외를 처리하는 방식이 다른데, 컨트랙트 내부에서 다른 컨트랙트의 함수를 직접 호출했을 때 예외가 발생할 경우, 호출한 컨트랙트 내부의 모든 진행 상황이 함수를 호출하기 전으로 복구되는데, 직접 호출이 아닌 call 함수나 delegatecall 함수를 통해 간접적으로 호출하거나, send 함수를 사용했을 때 예외가 발생할 경우에는, 해당 호출된 함수의 컨트랙트의 상태만 복구되고, 호출한 함수의 컨트랙트의 상태는 복구되지 않고 단지 함수의 결과로 0이 반환된다. 이렇게 일관되지 못한 예외처리가 프로그래머가 의도한대로 동작하지 않는 원인이 된다. [그림 2]는 실제 존재하는 유명한 컨트랙트인 King of Ether Throne[6]이다. 이 컨트랙트는 정해진 금액을 이전 왕에게 지불하고 본인이 왕이 되는 컨트랙트이다. 11번째 줄을 보면, send의 반환 값을 확인하지 않고 있는데 이는 만약 send가 실패할 경우, 이전 왕에게 제대로 금액이 지불되지 않았음에도 불구하고 컨트랙트는 예외가 발생하지 않고 계속 실행되어 왕이 바뀌게 되고, 컨트랙트 소유주가 지불되지 않은 금액을 가로챌 수 있는 악의적인 컨트랙트이다.

2.4 Timestamp Dependence

Timestamp dependence 취약점은 스마트 컨트랙트 코드 내에서 블록의 타임스탬프 값을 이용할 때 생기는 취약점이다. [그림 3]은 실제 존재하는 The Run[7]이라는 컨트랙트이다. 이 컨트랙트는 블록 넘버와 이전 블록의 해시, 그리고 블록의 타임스탬프 값을 시드 값으로 임의의 값을 생성해 누가 돈을 획득할지를 결정하는 컨트랙트이다. 이 때 블록 넘버와 이전 블록의 해시는 미리 계산할 수 있고, 블록의 타임스탬프 값은 채굴자의 로컬 시간 값에서 900초의 오차 범위 이내로 조작이 가능하기 때문에, 공격자는 직접 채굴자가 되어 자신이 돈을 얻을 수 있는 타임스탬프 값을 미리 계산해 채굴을 하면 돈을 얻을 수 있게 된다.

```
contract theRun{
    uint private Last_Payout=0;
    uint256 salt=block.timestamp;
    function random returns (uint256 result){
        uint256 y=salt*block.number/(salt%5);
        uint256 seed=block.number/3 + (salt%300)+Last_Payout+y;
        uint256 h=uint256(block.blockhash(seed));
        return uint256(h%100)+1;
}}
```

[그림 3] 간소화된 The Run[7] 취약점 코드

2.5 Suicidal Contract

Suicidal contract 취약점은 해당 스마트 컨트랙트를 누구든지 종료시킬 수 있는 취약점이다. 이 취약점은 2017년 발생한 Parity Multisig Wallet 사건에서 발견된 취약점이다. [그림 4]는 Parity 사건의 컨트랙트에서 사용하는 라이브러리 코드인데, initMultiowned 함수를 통해 복수의 소유주를 초기화하고, kill 함수를 통해 소유주중 일부가 동의할 시 컨트랙트를 종료시킬 수 있다. 두 번째 줄을 보면 한번 초기화를 하고나면 더 이상 초기화를 할 수 없도록 예외를 발생시키는데, 해당 Parity 사건의 라이브러리 컨트랙트는 초기화를 제대로 하지 않은 상태여서 누구나 초기화를 하고, kill 함수를 통해 컨트랙트를 종료 시킬 수 있는 상태였다. 그런 상태에서 악의 없는 유저가 실수로 초기화 후 kill 함수를 호출하여 해당 라이브러리 컨트랙트를 사용하는 모든 컨트랙트들의 잔액이 사용 불가능하게 된 사건이었다. 이처럼 부주의하게 초기화를 제대로 하지 않아서 컨트랙트를 임의로 종료시킬 수 있는 취약점이 발생했다.

```
function initMultiowned(address[] _owners, uint _required){
    if(m_numOwners > 0) throw;
    m_numOwners=_owners.length+1;
    m_owners[1]=uint(msg.sender);
    m_ownerIndex[uint(msg.sender)]=1;
    m_required=_required;
}
function kill(address _to){
    ...
    var pending = m_pending[sha3(msg.data)];
    if(pending.yetNeeded == 0){
        pending.yetNeeded=m_required;
        pending.ownersDone=0;
    }
    ...
    if(pending.yetNeeded <= 1)
        suicide(_to);
    else{
        pending.yetNeeded--;
        pending.ownersDone|=ownerIndexBit;
    }
}
```

[그림 4] Parity 라이브러리 취약점 코드

	Reentrancy	Integer over/underflow	Mishandled Exception	Timestamp Dependence	Suicidal Contract
Oyente	O	X	O	O	X
Zeus	O	O	O	O	O
Maian	O	X	O	X	O

[표 1] 취약점 분석 도구가 커버하는 취약점 비교

III. 스마트 컨트랙트 취약점 분석 도구

스마트 컨트랙트 취약점 분석 도구는 프로그래머들이 자신이 만든 컨트랙트의 취약점을 확인하고, 또한 사용자들이 자신이 이용할 컨트랙트의 안전성을 확인하기 위해 사용될 수 있다. 현재 대량의 스마트 컨트랙트에 대해 취약점 분석 결과가 정리 되어 있는 분석 도구는 총 3종으로, Oyente[3], Zeus[4], Maian[5]이다. 이 도구들에 대해 소개하고, 각 도구가 커버할 수 있는 취약점을 [표 1]에 정리 했다.

3.1 Oyente

Oyente는 싱가폴 국립대학의 연구진들이 만든 취약점 분석 도구로, 기호 실행(Symbolic Execution)을 기반으로 하는 스마트 컨트랙트 정적 분석 도구이다. 기호 실행이란, 컴퓨터 프로그램의 입력에 대한 실행 경로를 분석하기 위한 기법이다. Oyente는 총 네 모듈로 구성되는데, CFGBuilder, Explorer, CoreAnalysis, Validator이다. Oyente는 컨트랙트 바이트코드를 입력 받아 CFGBuilder를 통해 프로그램의 실행 흐름을 나타내는 제어 흐름 그래프를 만들고, 이를 바탕으로 Explorer에서 기호 실행을 한다. 기호 실행의 결과를 통해 CoreAnalysis 모듈에서 Oyente가 찾고자 하는 취약점인 reentrancy, mishandled exception, timestamp dependence를 찾고, 마지막으로 Validator에서 거짓 양성(False Positive) 케이스를 걸러내 사용자에게 보고한다. Oyente는 총 19,366개의 스마트 컨트랙트를 대상으로 분석을 진행 했고, 그 중 8,833개의 컨트랙트가 적어도 하나의 취약점을 갖고 있음을 발표했다.

3.2 Zeus

Zeus는 IBM 연구진들이 개발한 취약점 분석 도구로, 정형 검증을 기반으로 하는 도구이다. Zeus는 Policy Builder, Source Code Translator, Verifier로 구성되어 있다. Oyente와는 다르게, Zeus는 스마트 컨트랙트의 상위 레벨 소스 코드와 스마트 컨트랙트의 보안 정책을 입력 받는다. 우선 Policy Builder에서 입력 받은 보안 정책을 assert 함수의 형태로 스마트 컨트랙트 소스 코드의 검증하고자 하는 부분에 삽입하고, Souce Code Translator가 이를 입력 받아 LLVM(Low Level Virtual Machine) 비트코드로 변환시켜준다. 마지막으로 Verifier가 비트코드 레벨에서 해당 보안 정책을 만족하는지를 검증한다. Zeus는 총 22,493개의 스마트 컨트랙트를 대상으로 분석을 진행 했고, 그 중 21,281개의 컨트랙트가 적어도 하나의 취약점을 갖고 있음을 발표했다.

3.3 Maian

Maian은 Oyente와 마찬가지로 싱가폴 국립대학의 연구진들이 만든 취약점 분석 도구로, 기호 실행에 기반을 둔 도구이다. Maian은 스마트 컨트랙트의 안전성을 만족하는지를 검사하는 도구로, 기호 실행에 사용될 커스텀 이더리움 가상 머신을 직접 개발해, 스마트 컨트랙트 바이트코드에 대한 기호 실행을 한다. 이러한 실행 흔적들을 분석해 특정 속성을 만족하지 않는 실행 흔적을 뽑아내고, 기호에 대한 실제 값을 예시로 출력한다. 이를 이용해 실제로 컨트랙트를 실행해봄으로써 거짓 양성 케이스를 걸러낼 수 있다. Maian은 총 970,898개의 스마트 컨트랙트를 대상으로 분석을 진행 했고, 그 중 34,200개의 컨트랙트가 적어도 하나의 취약점을 갖고 있음을 발표했다.

[표 1]에는 각 도구들이 커버할 수 있는 취약점을 비교해 놓았다. Oyente의 경우, 저자들이 고려한 취약점에 Integer over/underflow와 Suicidal Contract가 포함되지 않았기 때문에 이를 찾아낼 수 없었다. Maian의 경우, Oyente와 마찬가지로 저자들이 고려한 취약점에 Integer over/underlfow와 Timestamp Dependence가 포함되지 않았기 때문에 이를 찾아낼 수 없었다. 이 두 정적

분석 도구는 각각 취약점 패턴을 탐지하는 모듈에 탐지하고자 하는 취약점 패턴을 추가함으로써 다른 취약점을 찾을 수 있도록 확장성을 고려했다. Zeus의 경우, 다른 두 가지 도구와 가장 차별화된 부분은 보안 정책을 XML의 형태로 코딩해 사용자가 스마트 컨트랙트가 만족했으면 하는 보안 정책을 골라서 검증할 수 있었고, 위에서 분류된 취약점 모두를 찾아낼 수 있었다.

IV. 결론

본 논문에서는 스마트 컨트랙트의 취약점을 그에 대한 예시와 함께 설명하고, 스마트 컨트랙트의 취약점을 탐지할 수 있는 도구에 대해서 소개하고 비교 분석하였다. 대부분의 스마트 컨트랙트 취약점은 프로그래머가 생각한 컨트랙트의 작동 방식과, 실제 이더리움 가상 머신 상에서 돌아가는 코드 사이에 의미론적인 차이 때문에 발생한다고 볼 수 있다. 따라서 스마트 컨트랙트를 작성할 때는 프로그래머가 주의해서 작성할 필요가 있다. 그리고 취약점 분석 도구를 활용해 컨트랙트를 블록체인에 저장하기 전에 반드시 취약점 검사를 진행할 필요가 있다. 마찬가지로 사용자의 경우에도, 자신이 사용하고자하는 스마트 컨트랙트의 바이트코드를 블록체인에서 쉽게 다운로드 받을 수 있기 때문에, 취약점 분석 도구를 이용해 자신이 사용하고자하는 스마트 컨트랙트의 안전성을 확인하고 사용할 필요가 있다.

[참고문헌]

[1] N.Szabo, Smart Contracts. http://szabo.best.vwh.net/smart.contracts.html, 1994.

[2] G.Wood, Ethereum: A secure decentralised generalised transaction ledger. https://ethereum.github.io/yellowpaper/paper.pdf, 2014.

[3] L.Luu, D.H.Chu, H.Olickel, P.Saxena, A.Hobor, Making smart contracts smarter. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security ACM, 2016.

[4] S.Kalra, S.Goel, M.Dhawan S.Sharma, Zeus: Analyzing safety of smart contracts. NDSS, 2018.

[5] I.Nikolic, A.Kolluri, I.Sergey, P.Saxena, A.Hobor, Finding The Greedy, Prodigal, and Suicidal Contracts at Scale. arXiv preprint arXiv:1802.06038, 2018.

[6] KingOfTheEtherThrone smart contract. https://github.com/kieranelby/KingOfTheEtherThrone

[7] The Run smart contract. https://etherscan.io/address/0xcac337492149bdb66b088bf5914bedfbf78ccc18

비트코인 거래 생성 시간 필드를 추가한, 이기적 채굴 대응방안 개선*)

이지혜, 김윤정

서울여자대학교 정보보호학과

Improvement of the Selfish Mining Countermeasures by adding Bitcoin Transaction Creation Time Field

Jihye Lee, Yoonjeong Kim

Dept. of Information Security, Seoul Women's University

요 약

비트코인은 블록체인을 기반으로 한 암호화폐로 블록체인에 모든 거래가 기록되고 공유되어 거래의 유효성을 보장받으며 이 행위를 채굴이라고 한다. 채굴 시, 정직한 채굴자는 전체 네트워크에서 본인의 컴퓨팅 파워에 따라 보상을 받는다. 그러나 이기적 채굴을 통해 채굴자가 컴퓨팅 파워 이상의 이익을 얻을 수 있다는 것이 증명되었다. 이기적 채굴은 블록체인의 의도적인 블록 분기를 의도하며 정직한 채굴자의 컴퓨팅 파워를 낭비시킨다. 본 논문에서는 이기적 채굴과 기존 대응 방안에 대해 분석하였으며, 거래 자료구조에 거래 생성 시간을 추가하고, 블록의 거래 생성 시간 평균을 이용하여 이기적 채굴을 막는 새로운 방법을 제시한다. 제안하는 방법은 이기적 채굴이 성공하기 위해 필요한 임계값을 33%로 하는 것으로 기존 방안들과 비교하여 가장 높은 임계값이다. 이 값은 또한 정직한 채굴자가 이기적 채굴풀에 채굴할 확률을 0으로 설정한 것으로 가장 최적화된 결과이다.

I. 서론

비트코인(bitcoin)은 2008년 사토시 나카모토(Satoshi Nakamoto)라는 프로그래머가 개발한 암호화폐로 블록체인 기술을 기반으로 하고 있다 [1]. 블록체인(blockchain)은 거래를 블록에 저장하여 노드(node)끼리 공유하는 P2P 기반의 분산화 된 데이터 저장 구조를 가지고 있어 비교적 경제적으로 데이터의 안전성과 무결성을 보증할 수 있다는 장점이 있다 [2,3]. 이 때문에 비트코인뿐만 아니라 다양한 분야에 블록체인 기술이 활용되고 있다.

*) 본 연구는 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원(No. NRF-2016R1A2B4011984)과 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2018-2014-1-00636)

비트코인은 중앙에서 관리하는 서버가 없기 때문에 특정 조건을 만족하는 블록을 찾아 블록의 유효성을 증명 받는 작업증명(proof of work)를 통해 거래의 유효성을 보장받는다. 먼저, 거래가 발생하면 네트워크를 통해 거래를 모든 노드에게 전송한다. 노드는 받은 거래들을 하나의 블록에 넣는다. 컴퓨팅 파워를 이용해 이전 해시값, 거래 내역 해시값, 임의 값(nonce) 세 정보를 결합하여 정해진 해시값보다 작은 블록 해시값을 찾는다. 특정 값을 만족하는 블록을 찾으면, 그 블록을 네트워크에 공개하고 다른 노드에게 검증받는다. 유효한 블록이면 블록체인의 끝에 이으며, 가장 먼저 유효한 블록을 찾는 노드에게 보상이 주어진다 [3]. 작업증명부터 보상을 받기까지의 과정을 채굴(mining)이라고 하며, 채굴을 하는 노드를 채굴자

(miner)라고 한다.

비트코인 전체 네트워크의 51% 이상을 장악하고 있는 그룹이 있다면 블록체인 네트워크를 마음대로 제어가 가능하고 비트코인의 무결성이 파괴될 수 있다 [2]. 이를 “51% 공격”이라고 한다. 그러나 2014년에 더 적은 네트워크 장악력으로도 네트워크 공격을 할 수 있음을 증명하였고 이 공격을 이기적채굴이라고 하였다 [4].

본 논문에서는 이기적 채굴과 기존에 공개된 이기적 채굴 대응방안을 분석을 하고, 이기적 채굴을 방어할 수 있는 새로운 대응 방안을 제시하였다. 제시하는 방법은 두 개 이상의 블록이 동시에 도착할 경우, 블록에 담긴 거래 생성 시간의 평균값을 이용하여 채굴자가 어떤 블록을 선택할지 기준을 제시하는 방안이다.

II. 이기적 채굴 분석

비트코인 표준 프로토콜에서는 작업증명을 통해 블록을 생성하고, 유효한 블록을 찾으면 바로 네트워크에 공개해 유효성을 증명 받아 블록체인을 확장한다. 두 개 이상의 블록이 동시에 도착할 경우, 먼저 온 블록에서 작업증명을 하고 한쪽 체인이 더 길어질 때까지 경쟁이 이어진다. 이 현상을 블록 분기가 발생했다고 한다 [3]. 이 프로토콜을 따르는 채굴자를 정직한 채굴자(honest mimer)라고 한다.

채굴자의 블록 보상 이익은 채굴자가 전체 네트워크에서 차지하고 있는 컴퓨팅 파워와 동일하다. 예를 들어, 전체 네트워크의 40% 컴퓨팅 파워가 있으면 40%의 확률로 채굴 보상을 얻을 수 있다. 비트코인 네트워크가 커지면서 개인 채굴자가 블록 보상을 가져가기가 힘들어졌다. 이에 따라 개인 채굴자들이 모여 함께 채굴을 하고 기여도에 따라 채굴 보상을 나눠가지는 채굴 풀(pool)을 형성하기 시작하였다.

Eyal과 Sirer는 상대적으로 큰 컴퓨팅 파워를 보유한 채굴풀이 이익을 더 많이 가져가기 위해 기존 프로토콜을 우회할 수 있음을 연구하고 증명하였다 [4]. 이기적 채굴 프로토콜에서는 정직한 채굴자의 체인인 공개 체인(public branch)과 이기적 채굴풀이 공격을 위해 만든 비공개 체인(private branch)이 존재한다. 이기적 채굴풀은 유효한 블록을 찾아도 바로 네트워크에 공개하는 것이 아니라 비공개 체인에 연결하였다가, 이기적 채굴풀에게 유리한 순간에 비공개 체인에 있는 블록을 선택적으로 공개한다.

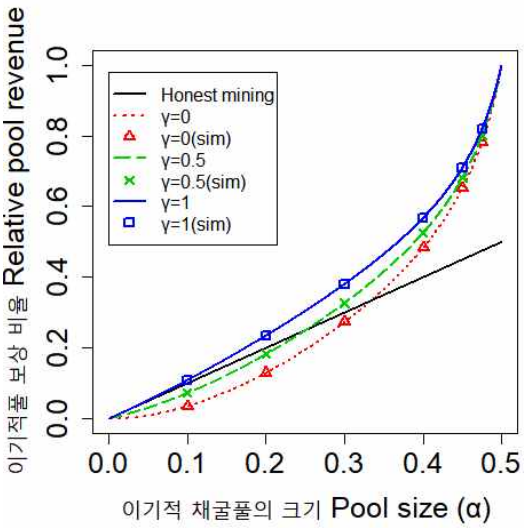


그림 1. 정직한 프로토콜과 이기적 채굴 프로토콜 사용 시 이익 비교 그래프 [4]

Eyal과 Sirer은 상태머신(state machine)을 이용해 기존 프로토콜과 이기적 채굴 프로토콜 사용 시 나타나는 이익 비교 그래프를 그림 1과 같이 도출했다. α는 이기적 채굴풀의 크기(컴퓨팅 파워), γ는 정직한 채굴자가 이기적 채굴풀에서 채굴하는 확률을 의미한다. 그림 1에서 이기적 채굴을 하지 않고 정직한 프로토콜을 따를 경우 이기적 채굴풀의 크기와 이익이 서로 비례하는 것을 볼 수 있다. 이기적 채굴 전략을 따르게 되면 이기적 채굴 풀이 일정 크기(임계치) 이상이 되어야 이익을 얻고, γ에 따라 이익이 달라진다.

$$\frac{1-\gamma}{3-2\gamma} < \alpha < \frac{1}{2} \qquad \text{(식 1) [4]}$$

식 1은 γ에 따른 이기적 채굴풀이 이익을 얻을 수 있는 풀의 크기 범위를 보여준다. γ가 0%이면 이기적 채굴풀이 보상을 얻기 위해 필요한 최소한의 풀 크기가 33%이고, γ가 $\frac{1}{2}$이면 25%, γ가 1이면 0%이다. 그림 1과 식 1을 통해 γ가 클수록 더 낮은 임계치(α 최솟값)로 많은

표 1. 이기적인 채굴에 대한 기존 대응방안 및 새로운 대응방안 비교

특징 / 대응	개념	한계점	임계치 (α 최솟값)
블록 랜덤 선택 기법 [4]	분기 시, 두 개의 블록 중 채굴할 블록 한개를 랜덤하게 선택하는 방법	현재 채굴풀이 임계치를 넘었으며, 작은 컴퓨팅 파워로 이기적 채굴이 가능	25%
블록 신선도를 이용한 기법 [5]	분기 시, 블록 타임스탬프를 보고 더 나중에 생성된 블록을 채굴하는 방법	타임스탬프 발행 및 관리 기관이 필요하며, 타임스탬프를 이용한 공격 가능	32%
블록선택조건 추가 방법 [6]	분기 시, 두 개의 블록 중 한 개를 선택하거나 두 개 모두 채굴하지 않는 방법	계속해서 어느 블록도 선택하지 않는 경우 진행 불가	28%
블록 만료 시간을 이용한 방법 [7]	제한 시간 내에 블록이 수신되거나 생성될 경우만 유효한 것으로 판별	의미 없는 블록이 생성될 가능성이 있음	-
가중치를 이용한 방법 [8]	체인에 가중치를 주어 더 높은 가중치를 가진 체인에서 채굴하도록 하는 방법	가장 긴 체인 법칙과 가중치 체인 법칙을 따르는 채굴자 사이의 일시적인 불일치를 이용한 공격이 가능	-
제안방안: 거래 생성 시간 평균값을 이용한 기법	블록 내 거래 생성 시간의 평균을 구해 분기 시 평균 시간이 더 최신인 블록을 선택하는 방법	소수의 거래만 넣거나 최신의 거래만 선택하려는 현상 발생 가능	33%

이익을 가져갈 수 있음을 알 수 있다.

이처럼 이기적 채굴은 노드가 전체 네트워크에서 차지하고 있는 컴퓨팅 파워 보다 더 많은 보상을 가져갈 수 있으며, 이것은 다른 정직한 노드의 컴퓨팅 자원을 낭비시키는 문제점을 야기한다.

III. 이기적 채굴에 대한 기존 연구

이기적 채굴 발표 이후, 이기적 채굴 대응방안에 대한 연구가 활발히 이루어졌다. 분기 시, 먼저 온 블록 선택하는 프로토콜을 수정해 랜덤하게 선택 하는 방법, 시간을 이용하여 선택 기준을 주는 방법, 체인에 가중치를 주어 높은 가중치를 선택하는 방법들이 제시되었다.

3.1 블록 랜덤 채택 방법 [4]

Eyal과 Sirer는 이기적 채굴 분석과 함께 대응방안에 대해서도 연구하였다. 두 개의 블록이 동시에 도착해 경쟁이 일어날 경우 두 개의 블록을 다시 전송해 두 개의 블록 중 하나를 랜덤하게 선택하게 하는 대응방법을 제시했다. 어떤 블록이 이기적 채굴풀의 블록인지 알 수 없기 때문에 정직한 채굴자는 채굴할 블록을 랜덤하게 선택할 수밖에 없다. 이 때, 정직한 채굴자가 이기적 채굴풀에서 채굴하는 확률 γ는 $\frac{1}{2}$이 되고 식 1에 따르면 임계치(α의 최솟값)는 $\frac{1}{4}$이 된다. BTC.com 채굴풀이 전체 네트워크의 25.8%를 차지하고 있다는 점을 봤을 때 좀 더 높은 임계치가 필요하다.*)

3.2 블록 신선도(Freshness Preferred)에 따른 블록 선택 방법 [5]

이 방법은 일정 시간 내에 두 개의 블록이 도착할 경우 블록의 타임스탬프를 보고 더 최근에 생성된 블록을 선택하도록 하는 방법이다. 만약 타임스탬프가 동일하다면 먼저 도착한 블록을 선택한다. 이 방법은 랜덤 비콘을 이용하여 위조할 수 없는 타임스탬프를 이용한 방법으로 임계치(α의 최솟값)을 32%까지 끌어올렸다. 다만, 신뢰할 수 있는 타임스탬프 발행 및 관리가 필요하며, 타임스탬프를 이용한 공격이 있을 수 있다는 단점이 있다.

*) https://blockchain.info/ko/pools (2018년 5월 22일 기준)

3.3 블록 선택 조건 추가하는 방법 [6]

이 방법은 3.1의 방법을 수정한 것으로 블록 분기 후 채굴할 블록을 선택할 때 “블록을 선택하지 않는다” 라는 조건을 추가하였다. 채굴자가 두 개의 블록을 발견할 경우 두 개의 블록 중 한 개를 선택하거나 두 개의 블록 모두 선택하지 않도록 하여 $\gamma = \frac{1}{3}$로 낮췄으며, 식 1에 따라 계산하면 임계치(α의 최솟값)는 $\frac{2}{7}$(약 28%)이다. Eyal과 Sirer의 대응 방법보다 약 3% 개선된 수치이다. 이 방법 또한 좀 더 높은 임계치가 필요하며, 채굴자들이 계속해서 아무 블록도 선택하지 않으면 블록체인이 진행이 되지 않는다는 문제점이 있다.

3.4 블록 만료 시간을 이용한 방법 [7]

이 방법은 각 노드의 로컬타임을 이용해 예상시간(expected time)을 두어 제한 시간 내에 수신된 블록 혹은 채굴한 블록만 유효한 블록으로 간주하는 방법이다. 만약 예상시간 내에 블록을 수신하지도 못하고 블록 채굴에도 실패한다면 이전 블록 해시값과 예상타임을 이용하여 더미블록(dummy block)을 생성하여 블록체인을 이어나갈 수 있다. 정직한 채굴자의 체인에서 블록이 생성된 후 이기적 채굴풀이 이전 블록 해시가 같은 블록을 공개하더라도 정직한 채굴자의 체인에는 이미 해당 블록 존재하기 때문에 정직한 채굴자는 그 블록을 받아들이지 않는다.

3.5 가중치에 따른 체인 선택 방법 [8]

이 방법은 분기 이후 체인에 가중치를 주어 더 높은 가중치를 가진 체인의 블록에서 채굴하도록 하는 방법이다. 한 블록이 수신된 이후 일정 시간 내에 수신되고, 블록 채굴 시 이전 블록과 경쟁하는 블록의 해시를 추가한 블록이 있는 체인이 높은 가중치 값을 받을 수 있다. 이기적 채굴풀이 의도적 분기를 일으켰을지라도 이기적 채굴풀은 이전 블록과 경쟁하는 블록의 해시값을 예상할 수 없기 때문에 가중치가 높은 블록을 미리 생성할 수 없다. 즉, 정직한 채굴자가 이기적 채굴풀의 블록에서 채굴할 확률이 낮아진다.

IV. 본 연구의 대응방안

4.1 제안방안 개요

본 논문에서는 블록에 들어있는 거래의 생성 시간 평균을 이용해 현재와 더 가까운 시간을 가진 블록을 선택하도록 하는 대응방안을 제안한다.

이기적 채굴풀은 미리 블록을 채굴 해 비공개 체인에 이어나가기 때문에, 공개 체인과 비공개 체인에서 동일한 인덱스의 블록을 채굴한다고 했을 때 비공개 체인에 있는 블록이 먼저 채굴된다. 비공개 체인의 블록에 들어있는 거래 또한 정직한 채굴자 블록에 들어있는 거래 보다 더 오래될 수밖에 없다. 이 점을 이용해 두 개 이상의 블록이 도착 시, 채굴자가 블록 내에 있는 거래들의 생성 시간 평균을 보고 현재에 더 가까운 값을 가진 블록을 채택해 채굴을 계속하도록 하는 방법을 제안한다.

이 방법은 비공개 체인에 블록을 오래 숨겨둘수록 블록 내 거래 생성 시간이 오래되기 때문에 이기적 채굴풀에게 불리해지며 블록 채굴 후 바로 네트워크에 공개를 유도할 수 있다는 장점이 있다.

그러나 비트코인 거래 구조에는 거래 생성 시간 정보가 없기 때문에 본 논문에서 제안하는 아이디어 구현을 위해서는 거래 구조 수정이 필요하다. 이 장의 나머지 부분에서는 거래 구조 수정과 그에 대한 영향을 논한다.

4.2 비트코인 거래(transaction) 구조 수정

현재의 비트코인 거래에서는 거래 생성 시간이 사용되지 않으며 거래 생성 시간을 저장하지 않는다. 이중지불 공격을 막기 위해서 블록체인의 가장 긴 체인 규칙을 따르고 있기 때문에 거래 생성 시간이 중요하지 않다. 그러나 본 논문에서 제안하는 아이디어 구현을 위해서는 거래 생성 시간이 필요하며 소스코드에서 거래 자료구조를 찾아 수정하는 방안이 필요하다.

표 2는 기존 비트코인 거래 구조에

표 2. 비트코인 거래(transaction) 구조

필드	크기	설명	비고
Version	4bytes	거래가 따르고 있는 룰 명시	기존 필드
Input Counter	1-9 bytes(VarInt)	포함된 입력 값의 수	기존 필드
Inputs	Variable	하나 이상의 거래 입력 값	기존 필드
Output Counter	4bytes	포함 된 출력 값 수	기존 필드
Outputs	Variable	하나 이상의 거래 출력 값	기존 필드
Lock_time	4bytes	유닉스 타임 스탬프 또는 블록 번호	기존 필드
transTime	4bytes	거래 생성 시간	추가한 필드

'transTime' 필드를 수정하여 나타낸 것이다. 기존 필드 Version은 거래가 따르는 규칙, Inputs는 거래 입력값이 참고하고 있는 거래들, Outputs는 거래 출력값으로 거래가 도착할 주소를 의미한다. Lock_time 필드는 거래를 지연시키고자할 때 사용한다. 추가된 'transTime' 필드는 거래가 언제 생성되었는지에 대해 알 수 있는 타임 정보를 담고 있다.

'transTime'을 추가한 거래의 자료구조를 비트코인 소스로 나타내면 그림 2와 같다. 이 자료구조는 비트코인 소스 primitives/transaction.h 에 들어있는 것을 수정한 것으로, 'transTime' 변수에 거래 생성 시간을 저장한다.

거래 생성 시간 정보를 이용하는 수정 된 비트코인 프로토콜을 살펴보면 다음과 같다. 먼저, 거래가 발생할 때 버전, 입력값 정보, 출력값 정보, 글로벌타임을 기준으로 한 거래 생성 시간 정보를 저장한다. 생성된 거래는 네트워크를 통해 노드에게 전달되고, 노드는 받은 거래들을 하나의 블록에 넣는다. 컴퓨팅 파워를 이용해 기존과 동일하게 블록의 해시값을 찾는다. 유효한 블록을 찾으면 블록을 네트워크에 공개하고 다른 노드에게 검증받는다. 유효한 블록이면 블록체인의 끝에 연결하며, 가장 먼저 유효한 블록을 찾은 노드가 보상을 받는다. 그러나 두 개 이상의 블록이 동시에 도착하면 블록 내에 있는 거래 'transTime'의 평균을 확인하여 현재 시간과 더 가까운 블록을 선택한다. 이후 경쟁이 끝나면 이긴 체인에 있는 블록의 주인이 보상을 받는다.

```
class CTransaction {
  static const int32_t CURRENT_VERSION=2;
  static const int32_t MAX_STANDARD_VERSION=2;
      const std::vector<CTxIn> vin;
      const std::vector<CTxOut> vout;
      const int32_t nVersion;
      const uint32_t nLockTime;
      const uint32_t transTime;
}
```

그림 2. 수정한 비트코인 거래 자료구조

4.3 제안 방안 성능 분석

이기적 채굴풀의 블록에 들어있는 거래가 정직한 채굴자 블록에 들어있는 거래 보다 더 이전에 발생한 거래들이기 때문에, 이 방법을 사용하면 정직한 채굴자가 이기적 채굴 풀의 블록에서 채굴할 확률이 0에 가까워진다. γ가 0일 때, 식 1을 활용하면 임계치(α 최솟값)는 33%가 된다. 따라서 이기적 채굴 전략을 취했을 때 이기적 채굴 풀의 크기가 33% 이상인 경우에만 더 많은 이익을 볼 수 있다. 이 33%는 현재 나와 있는 임계값 중 가장 좋은 값이다.

4.4 거래 구조 수정으로 인한 영향 분석

거래 구조 수정으로 인해 몇 가지 현상이 발생할 수 있다. 기존 비트코인 프로토콜에서는 채굴자가 블록에 거래를 넣을 때 수수료가 높은 거래를 넣으려고 한다. 그러나 우리가 제안하는 프로토콜에서는 채굴자가 블록 생성 시 분기 상황을 고려해 소수의 거래만 넣거나 최신의 거래만 선택해 'transTime' 평균을 높이려고 할 수 있다. 소수의 거래만 넣을 경우 'transTime' 평균이 높아질 수는 있겠지만 수수

료가 적어지므로 채굴자 입장에서 선호하지 않을 것이다. 최신의 거래만 채굴한다면 오래된 거래는 처리지연이 발생할 수 있다. 이는 거래 소유자가 거래를 재전송하여 해결하면 된다. 수수료를 기준으로 거래를 선택할 때, 낮은 수수료의 거래가 늦게 처리되는 현상이 발생했으며, 더 높은 수수료로 거래를 재전송하여 해결했다. 이처럼 거래가 오랜 시간이 지나도록 처리가 되지 않을 경우, 거래 소유자가 거래 재전송을 통해 거래 생성 시간을 최신의 것으로 만들어 해결할 수 있다.

4.5 공격 가능성 분석

거래 구조 변화로 'transTime'을 이용한 공격이 있을 수 있다. 채굴 시, 블록 내 거래 'transTime' 평균을 최신의 것으로 만들기 위해 거래 내 'transTime'을 위변조하려고 시도할 수 있다. 그러나 비트코인은 스패밍(spamming), 서비스거부(Dos) 등 네트워크에 영향을 주는 공격을 사전에 방지하기 위해 각 노드에서 독립적으로 모든 거래를 유효화하고 해당 거래를 다른 노드에게 전파한다 [9]. 즉, 모든 거래 생성 시간을 위변조하기 위해서는 비트코인 네트워크의 51% 이상의 노드의 거래의 'transTime'을 위변조해야 하므로 거래 'transTime'을 위변조 공격 성공 가능성이 적다고 볼 수 있다.

V. 결론 및 향후연구

본 논문에서는 비트코인 취약점 중 하나인 이기적 채굴과 대응방안에 대해 분석하고 새로운 방법을 제시했다. 이기적 채굴 전략을 취하지 않더라도 블록 분기가 일어나며 블록의 자원이 낭비된다. 그러나 이는 자연적인 분기로 채굴자가 의도하지 않은 상황에서의 자원 낭비이다. 이기적 채굴풀이 블록을 바로 공개한다면 다른 채굴자들은 해당 인덱스의 블록을 계속적으로 채굴 하지 않았을 것이다. 즉, 이기적 채굴에서 표준 프로토콜을 따르는 정직한 채굴자의 의도적인 자원 낭비를 유도하고 있다.

이런 문제를 해결하기 위해 블록 내 거래 생성 시간 평균을 이용하여 블록을 선택하는 방법을 제시했다. 이 방법은 블록을 비공개로 둘 때의 이점을 없앨 수 있다.

향후에는, 본 논문에서 제시한 'transTime' 필드 추가로 인한 오버헤드 등에 대한 분석을 진행하여 제안 방법의 효율성을 좀 더 심도있게 분석할 계획이다.

[참고문헌]

[1] 비트코인 (위키피디아), https://ko.wikipedia.org/wiki/%EB%B9%84%ED%8A%B8%EC%BD%94%EC%9D%B8, 2018년 5월 22일 확인.

[2] 블록체인 (위키피디아), https://ko.wikipedia.org/wiki/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8, 2018년 5월 22일 확인.

[3] Satoshi Nakamoto, "Bitcoin: A peer-to- peer electronic cash system," 2008.

[4] Ittay Eyal and Emin Gün Sirer. "Majority is not enough: Bitcoin mining is vulnerable," International Conference on Financial Cryptography and Data Security, Springer, Berlin, Heidelberg, 2014.

[5] Ethan Heilman, "One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner," International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2014.

[6] 양지연, 김소희, 김윤정, "비트코인 블록체인의 이기적인 채굴 대응방안 개선", 2015 한국정보보호학회 동계종합학술발표회, 서울여자대학교, 2015.

[7] Siamak Solat and Maria Potop-Butucaru, "Zeroblock: Preventing selfish mining in bitcoin," arXiv preprint arXiv:1605.02435 (2016).

[8] Ren Zhang and Bart Preneel, "Publish or perish: A backward-compatible defense against selfish mining in bitcoin," Cryptographers' Track at the RSA Conference, Springer, Chaum, 2017.

[9] Andreas M. Antonopoulos, "Mastering Bitcoin: Unlocking Digital Cryptocurrencies," O'REILLY, 2014.

국외 블록체인 기반의 전력 시스템 보안 연구 동향분석 및 국내 적용 방안 연구

김효빈*, 홍기섭*, 서정택**

*순천향대학교 정보보호학과 사이버물리시스템보안연구실

**순천향대학교 정보보호학과

Block Chain Based Power System Security Research Trend

Hyo-Bin Kim*, Ki-Seob Hong*, Jung-Taek Seo**

*CPSS Lab., Department of Information Security Engineering, Soonchunhyang University

**Department of Information Security Engineering, Soonchunhyang University

요 약

4차 산업혁명의 핵심요소기술로 유엔 미래 보고서에서는 블록체인을 꼽았다. 해당 기술은 여러 분야에 활용을 위해 연구되고 있는 실정이다. 이에 본 논문에서는 블록체인 기반 전력 시스템에 대해 알아보고, 해당 시스템의 보안성 강화를 위한 보안 기술 연구 동향을 살펴보고, 국내 전력 시스템에 블록체인 적용 방안을 제시한다.

I. 서론

기존 전력망에 ICT(Information & Communication Technology)를 접목한 스마트그리드는 전력 공급자와 소비자 간 실시간 정보 교환으로 향상된 에너지 효율을 목표로 하는 기술이다. 이는 우리 생활에 더욱 밀접하게 다가올 것이며, 효율적인 에너지 소비를 끌어낼 것이다. 향후에는 고용량, 고효율성, 고가용성을 보장하기 위한 여러 신기술이 도입것으로 전망된다.

4차 산업혁명의 핵심요소기술로 유엔 미래 보고서에서는 블록체인을 꼽았다. 이는 공공 거래 장부로 보안성을 제공하는 기술로 2016년 초 한국은행에서 블록체인을 "P2P 네트워크에 거래정보를 기록한 장부를 분산해 관리하는 기술로 소개되었다[1]. 더불어 미국 IT 리서치 기업인 가트너의 발표에 따르면 미래 유망 전략 기술로 블록체인을 선정하여 블록체인 기반 사업 가치는 2022년에 100억 달러에 이를 것으로 전망하였다[2]. 현재 기존 에너지 분야에서 겪고 있는 어려움을 디지털화하면 많은 문제점을 해결할 수 있는데 특히 블록체인 기술을 활용한 방안에 관해 많은 연구가 진행되고 있다. 에너지 분야산업에서 낭비되는 에너지를 효율적으로 활용하려는 방안으로 스마트그리드, 마이크로 그리드가 있는데 이 기술과 블록체인이 결합하면 효율적이며 안전, 보안이 강화된 에너지 거래 시장 플랫폼을 형성할 수 있다. 스마트그리드의 정교한 소비 모니터링을 제공할 뿐만 아니라 분배 에너지 거래(예: 마이크로 그리드)로 점점 더 많은 가정용 발전 사이트가 구성될 것으로 예상된다.

현재 대부분의 결재 및 금융 인프라는 중앙 집중식으로 관리되고 있으며, 이는 계정 및 수수료를 처리하고 보안을 제공하는 신뢰할 수 있는 제3자의 참여를 의미한다. 중앙 집중식 에너지 거래는 확장성 및 보안 문제를 겪고 있다. 예를 들어 중앙 소비형 중개인은 전력 소비 프로파일링 접근법의 Wood의 행동 모델링에 따라 에이전트(전력 거래에 대한 자격을 갖추고 허가를 받아서 업무를 중개하거나 대행하는 사람)의 에너지 생성 패턴을 밝혀내고 에이전트의 일상 활동을 예측할 수 있다[3]. 그러므로 프라이버시와 익명성이 결여되어 보안 위협으로 이어진다. 따라서 스마트그리드에서 거래자 간 계약을 수행하고 입찰, 협상 및 거래를 처리하면서 신원 정보의 프라이버시와 거래 데이터를

보호할 수 있는 안전한 에너지 거래 인프라를 갖추는 것이 중요하다.

본 논문에서는 블록체인 기반의 전력 시스템 기술 동향을 살펴보고, 국내 전력 시스템에 블록체인 기반의 전력 시스템 적용 방안을 제시한다.

2장에서는 블록체인 기반 전력 시스템에 대해 살펴보며, 3장에서는 블록체인 기반 전력 시스템에서 프라이버시와 익명성을 보장하는 기술과 거래 데이터를 보호하는 프레임 워크를 포함한 최근 연구 동향을 살펴본다. 4장에서는 국내 전력 시스템에 블록체인 기술 적용 방안을 제시하고, 마지막으로 5장에서는 본 논문의 결론을 맺는다.

II. 블록체인 기반 전력 시스템 개요

블록체인 기술은 암호통화에 대한 검증 메커니즘으로 개발되었지만 최근 많은 분야에서 블록체인 기술을 활용하여 다양한 응용 프로그램을 구현하고 있다. 블록체인 기반 시스템은 기본적으로 원장이라는 분산 레지스터, 분산된 합의 메커니즘 및 일부 암호화 보안 조치를 결합한 것이다. 이러한 시스템은 스마트 계약과 함께 거래 시스템의 기능에 혁명을 일으키고 완전히 분산된 시장 플랫폼을 가능하게 한다.

현재 블록체인 기반 전력 시스템은 국내외 선행자료 조사와 과학기술정책연구원의 “에너지 블록체인 도입방안 연구”에 따르면 에너지 블록체인 유형은 총 5가지(△P2P 전력거래, △EV 충전 및 공유, △에너지 데이터 활용, △에너지 공유, △탄소자산 거래)로 분류된다.

<표 1>과 같이 여러 유형의 에너지 블록체인이 존재하지만 현재 개발된 대부분의 블록체인 기반 전력 시스템은 P2P 전력거래가 많은 상태이다.

<표 1> 에너지 블록체인 유형 및 내용 [4]

유형	내용	사례
P2P 전력 거래	개인 간 전력거래의 비용을 줄이고, 투명한 전력거래를 위해 블록체인 기술을 활용함	Brooklyn Microgrid Project(미국), Energo(중국), Power Ledger(호주) SolarCoin(미국)
EV 충전 및 공유	전기차를 충전 및 결제할 때 블록체인 기술을 활용해서 신뢰성 및 비용 절감 효과를 가져올 수 있음	Slock.it&RWE(독일) Energo(중국)
에너지 데이터 활용	블록체인에 에너지 데이터를 공유하여 새로운 비즈니스 모델을 구축함	Grid Singularity (오스트리아)
에너지 공유	에너지 공급이 필요한 개발도상국에 신재생에너지 설비를 공유할 수 있도록 블록체인을 활용함	Bankymoon(남아공), M-PAYG(덴마크)
탄소 자산 거래	탄소배출권 거래제와 같은 탄소자산 거래를 활성화하기 위해 블록체인 기술을 도입함	IBM & Smart Blockchain Lab (중국)

블록체인 기반 P2P 전력거래에서는 시스템의 구성요소가 서로 상호 작용하기 위해 각 스마트 미터는 아래 항목과 같은 필수 기능을 갖추어야 한다.

<표 2> P2P 전력거래를 위한 스마트 미터 필수 기능

- ■ 미터별 고유한 주소로 식별
- ■ 공개키 및 개인키의 생성을 지원하는 특정 소프트웨어 설치
- ■ RAM, 연산 하드웨어, 데이터 수집 장치, 신호 송신기, 신호 수신기 및 데이터 처리 장치
- ■ 유선 또는 무선 통신 채널을 통해 서로 통신

블록체인 기반 전력 시스템에서 퍼블릭 블록체인은 확장의 제한성, 높은 가치 변동성 등의 한계점이 있기에 안정적으로 전력을 공급해야 하는 에너지 분야에서는 신뢰할 수 있는 인증된 사용자들이 해당 네트워크에 참여할 수 있는 프라이빗 블록체인을 기반으로 한 서비스가 대다수이다. <표 3>은 블록체인 기반 전력 시스템에서의 퍼블릭 블록체인과 프라이빗 블록체인의 특성을 보여준다.

<표 3> 블록체인 유형 및 특성 [5, 6]

- ■ (퍼블릭 블록체인) 누구든지 네트워크에 참여하여 블록체인 내 정보를 읽고, 쓰고, 검증할 수 있지만, 데이터 기록에 문제 발생 시 중재 방법이 없음

- 퍼블릭 블록체인의 대표 격인 비트코인은 블록체인 기술을 화폐 발행 및 거래에만 적용한 사례로써 기존 은행 거래에 비해 높은 보안성, 낮은 이체수수료, 거래 투명성, 계좌생성 편의성 등 장점이 있지만, 높은 가치 변동성, 검열 저항성, 제한된 확장성, 익명성 등 불안요소가 존재함
- 블록체인 2.0 중의 하나인 Ethereum은 튜링완전언어를 스마트 계약에 사용해서 화폐거래 정보뿐만 아니라 에너지 정보나 무역거래 정보를 분산 원장에 공유할 수 있는 플랫폼을 제시했지만, 여전히 무제한 코딩 공격에 대한 보안이 취약하고, 코드가 잘 실행되는지를 검증할 수 있는 체계가 미흡함

■ (프라이빗 블록체인) 중앙기관이 네트워크 참여에 대한 권한을 가지고, 신뢰할 수 있는 사용자들만 네트워크에 참여해서 분산 원장 데이터를 공유하고 검증하는 시스템

- 프라이빗 블록체인은 네트워크 내에 있는 데이터의 열람, 검증 권한을 차등적으로 부여할 수 있어 데이터 프라이버시를 보호할 수 있음
- 퍼블릭 블록체인은 검열 저항성이 강하기 때문에 산업에 적용하기 어렵지만, 프라이빗 블록체인은 불의의 사고나 악의적인 공격이 발생 시 미리 정한 규약이나 동의서에 따라 법적 책임을 물을 수 있음

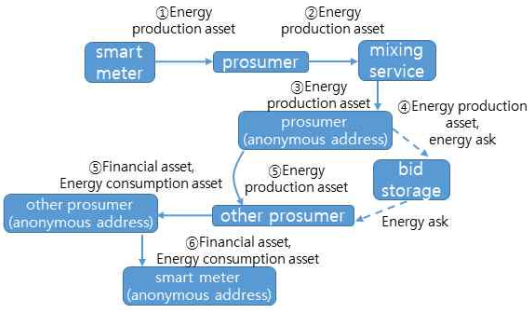
블록체인 기술을 활용하여 많은 응용 프로그램을 구현하지만 아직 초기 단계에 있고 다양한 보안적 문제(예 : 51% 공격, 사용자 ID 및 데이터 추적 등)가 존재한다. 이러한 문제를 해결하기 위해 다양한 연구가 이루어지고 있다.

III. 블록체인 기반의 전력 시스템 보안 연구 동향

전력 시스템 보안은 학계와 산업계 모두에서 주목을 끌고 있고 있다. 따라서 현대 전력 시스템의 견고성을 높이기 위해 보호 프레임 워크 및 프라이버시 솔루션, 데이터 보안 등의 연구가 활발히 이루어지고 있다. 이번 장에서는 블록체인 기반 전력 시스템 보안 연구 동향을 살펴보고, 비교 분석한다.

3.1 프라이버시 및 익성명 보안

Aron Laszka 등은 분산 원장을 사용하는 IoT 기반의 Transactive 에너지 시스템에서 개인 정보, 안전 및 보안 제공에 대해 제안한다[7]. 이는 소비자가 프라이버시를 희생하지 않고도 에너지를 교환할 수 있게 하는 Transactive 마이크로그리드의 안전한 솔루션인 프라이버시 보존 에너지 거래(PETra, Privacypreserving Energy Transactions)에 대해 설명한다. PETra는 블록체인과 같은 분산 원장을 기반으로 하며 통신, 입찰 및 거래에 대한 익명성을 제공하여 전력 시스템에서 프로슈머에게 프라이버시를 제공한다. <그림 1>과 같은 절차를 따르며 프로슈머는 익명으로 에너지 거래를 할 수 있다.



<그림 1> 에너지를 판매하는 프로슈머의 관점에서 자산 흐름의 간략한 개요

생산 자산에 대한 익명성을 얻기 위해 프로슈머는 CoinShuffle [8] 또는 Xim [9]과 같이 분산형 프로토콜로 구현될 수 있는 Mixing Service를 사용한다. 이는 다수의 요청 및 전송을 함께 혼합하여 소유자 자산의 추적을 방지한다. 따라서 Mixing Service는 프로슈머와 익명 주소 간의 연결을 숨긴다. Mixing Service는 여러 접근법을 사용하여 구현할 수 있다. 가장 간단한 방법은 자산을 송수신 할 수 있는 Cryptocurrency Tumbler라고 하는 신뢰할 수 있는 제3자를 이용하는 것이다. 그러나 이 경우 익명성은 주소의 이름을 변경가능한 제3자의 신뢰성에 달려 있다. 보다 안전한 접근 방법은 CoinShuffle [22] 또는 Xim [2]과 같은 분산화된 프로토콜을 사용하는 것이다. 이 프로토콜을 사용하면 제3자의 필요성을 없애준다. PETra는 익명 서비스가 구축되는 인프라이기에 익명 통신 계층에서 통신이 이루어진다. 그러므로 익명 통신 계층이 없으면 소스 및 네트워크 식별자(예 : IP 또는 MAC 주소)를 기반으로 거래 및 입찰가

를 쉽게 익명화 할 수 있다. 익명 통신에서는 Onion Routing과 같은 익명 통신에 잘 알려지고 널리 사용되는 기술을 사용할 수 있다[10]. 해당 연구는 이론적으로 제시가 되었으며 추가적으로 증명이 필요하다.

Nurzhan Zhumabekuly Aitzhan 등은 다중 서명, 블록체인 및 익명 메시징 스트림을 통한 분산 에너지 거래의 보안 및 개인 정보보호에 대해 제안했다[11]. 익명으로 에너지 가격을 협상하고 거래를 안전하게 수행할 수 있게 해주는 토큰 기반 Private 분산 에너지 거래 시스템인 PriWatt을 구현했다. PriWatt 시스템은 거래가 모든 노드 간에 복제되기 때문에 트랜잭션이 장애로부터 보호되는 P2P 커뮤니티 기반 데이터 복제 방법을 사용한다. 또한 PriWatt 디지털 서명은 타원 곡선 암호화(ECC)를 사용하여 구현하였다. 같은 유형의 비대칭 암호화와 비교할 때 ECC의 주요 이점은 ECC가 더 짧은 키 길이를 요구하지만 비슷한 보안 레벨을 제공한다.

<표 4> ECC와 RSA/DSA/DH 비교

보안 강도	Key size	
	ECC	RSA/DSA/DH
80 bits	160 bits	1024 bits
112 bits	224 bits	2048 bits
128 bits	56 bits	3072 bits
192 bits	384 bits	7680 bits
256 bits	521 bits	15360 bits

이 시스템에서 블록체인 기술, 멀티 서명 및 익명 메시징 전파 스트림의 적절한 조합은 기존의 중앙 집중식 거래 솔루션에 비해 높은 개인 정보보호 및 보안으로 분권화된 P2P 전력거래에 대한 실현 및 신뢰할 수 있는 방향을 제시했다.

3.2 보안 프레임워크

Gaoqi Liang 등은 사이버 공격에 대한 최신 전력 시스템의 자기 방어 능력을 향상시키기 위해 분산 된 블록체인 기반의 새로운 보호 프레임 워크를 제안한다. 제안된 프레임 워크에서 수집된 모든 데이터는 각 미터의 메모리에 분산 형태로 존재하는 연결된 블록의 형태로 원장에 저장된다. 저장하기 전에 데이터 정확성을 보장하기 위해 데이터 브로드캐스트, 투표 메커니즘을 통한 데이터 검증, 블록 데이터 누적, 마이닝 프로세스, 투표 메커니즘을 통한 마이닝 결과 확인, 분산 원장 동기화 등의 각 절차를 거친다. 제안된 프레임워크는 기존 비트 코인 시스템과 기술 비교를 통해 정보 수집 및 저장에 있어, 보다 안전한 환경을 제공함을 증명했다.

Jianbin Gao 등은 투명성과 출처를 제공하는 독립(sovereign) 블록체인을 활용하여 GridMonitoring 시스템을 구현했다. 독립 블록체인은 블록의 체인을 통해 서로 연결되어있는 정렬된 레코드 목록을 포함하는 분산 데이터베이스이다. 해당 시스템은 정보 공유, 효율적 데이터 관리 기능을 포함한 데이터의 무결성 및 기밀성을 제공하여 기타 관련 시스템과의 비교를 통해 증명하였다.

이처럼 기존 전력 시스템의 보안성 강화를 위해 블록체인 기술을 통한 전력 시스템관련 보안 연구 동향이 활발하게 진행되고 있다. 이들 연구들 중 상대적으로 보안성이 높은 연구를 찾고자 지표를 통해 <표 5>와 같이 제시한다.

<표 5> 분석된 연구 동향 비교

지표	설명
정보 공유	전력 회사가 연구 목적으로 제3자에게 생성된 데이터를 제공할 수 있는 능력
효율적인 데이터 관리 기능	데이터 소유자가 제3자와 공유하는 데이터를 완벽하게 제어할 수 있는 능력
데이터 불변성	데이터 변경 불가능
데이터 무결성	데이터에 대한 무결성
데이터 기밀성	네트워크의 관리자 및 거래 당사자만 정보 자산에 접근할 수 있는 기능
데이터 출처 및 감사	데이터 사용을 설명 할 수 있는 기능
데이터 변조 탐지	데이터에 대한 무단 수정을 탐지하는 기능

<표 6> 분석된 연구 동향 비교

지표	[7]	[11]	[12]	[13]
정보 공유	Y	Y	Y	Y
효율적인 데이터 관리 기능	-	-	-	Y
데이터 불변성	Y	Y	Y	Y
데이터 변조 탐지	-	-	Y	Y
데이터 무결성	Y	Y	Y	Y
데이터 기밀성	Y	Y	Y	Y
데이터 출처 및 감사	Y	Y	Y	Y

연구 동향 비교를 통해 블록체인 기반 전력 시스템은 해당 데이터에 대한 불변성, 무결성, 기밀성을 필수 보안 요구사항으로 제공해야 됨을 보여준다.

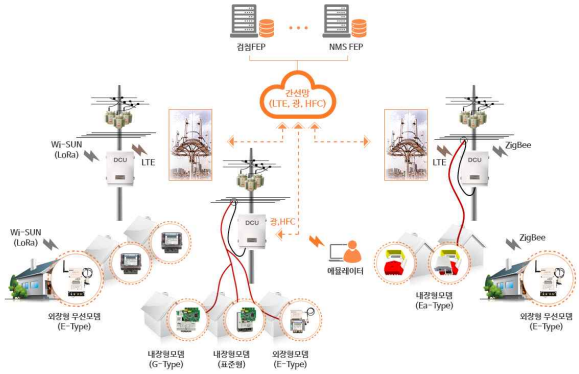
IV. 국내 전력 시스템 적용 방안

4.1 법적 규제 완화

2017년 1월 산업통상자원부가 에너지신산업 수출동력화와 신재생에너지 보급 확대에 집중할 것임을 강조하였다. 주요 정책으로는 신재생에너지 전력생산량 2030년까지 20% 추진 및 발전사업자들의 신재생에너지 의무 공급량 비율 높이는 정책이 발표 되었다. 해당 정책으로 인해 프로슈머의 수가 늘어날 것이다. 하지만 국내에서는 전기사업법에 의하여 전기판매 사업자는 한국전력 구역전기 사업 외에는 불가능하다[14]. 따라서 국외에서 활발하게 진행되고 있는 P2P 전력거래는 현 시점에서 국내에 적용하기 힘들다. 따라서 개인 간의 거래를 위해 법적 규제 완화가 필요하다.

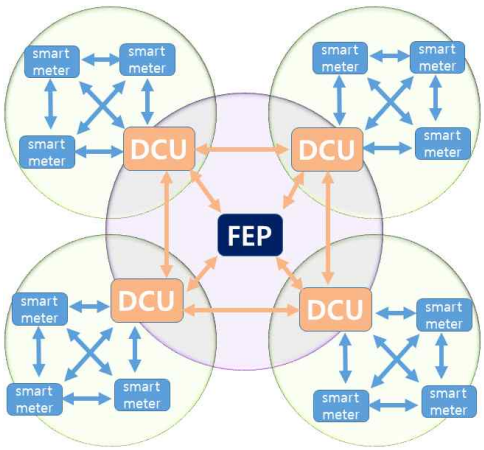
4.2 AMI 시스템에 블록체인 기술 적용

현재 국내 전력 시스템에서 법적 규제를 벗어나 블록체인 기술을 적용하기 위해서는 P2P 전력거래가 아닌 AMI 시스템에 적용해야 하는 실정이다. AMI는 스마트 미터에서 측정한 데이터를 원격 검침기를 통해 측정하여 전력 사용 분석을 자동으로 진행하는 기술이다[15]. 현재 국내 AMI 구조는 <그림 2>와 같이 트리형 구조로 이루어져 있다.



<그림 2> 지능형 전력계량 인프라, 출처:한전KDN, https://www.kdn.com/menu.kdn?mid=a10204070100

이에 법적 문제를 해결하여 블록체인 기술을 적용하기 위해 네트워크 구조를 하나의 중앙기관이 네트워크에 참여하는 것에 대한 권한을 가지고, 신뢰할 수 있는 사용자(스마트 미터, DCU)들만 네트워크에 참여해서 분산원장 데이터를 공유하고 검증하는 시스템인 프라이빗 블록체인 유형을 적용하며, 노드의 오버헤드를 방지하기 위해 행정구역별 사이드체인을 이용하여 구성할 수 있다.



<그림 3> 제안하는 AMI 시스템에 블록체인 기술 적용 구조(예)

프라이빗 블록체인에서는 네트워크 내에 있는 데이터를 사용하고, 검증하는 권한을 차등적으로 부여할 수 있기 때문에 중앙 기관의 관리가 가능하며, 데이터 프라이버시를 보호할 수 있다. 더불어 조사된 동향의 보안 기술을 적용하게 된다면 보다 강화된 신원 정보의 프라이버시와 전력사용량 데이터를 보호할 수 있는 안전한 인프라를 구성할 수 있다.

V. 결론

지금까지 국외 블록체인 기반 전력 시스템 보안 연구 동향을 살펴보았다. 국외는 전력 시스템에서 P2P 전력거래에 대한 서비스 및 관련 보안 연구가 활발하게 진행되고 있다. 대부분 공통적으로 P2P 전력거래 데이터에 대한 보안을 제공하며 프라이버시를 보장하는 연구들이 주를 이루고 있다. 이를 통해 블록체인은 최신 전력 시스템의 데이터 보안을 위한 유망한 솔루션으로 간주 될 수 있다. 이에 따라 국내 기업 또한 국외 사례들을 정확히 파악하여 블록체인 기술을 활용하여 국내 시스템 환경에 적합한 새로운 보안 기술 연구개발이 필요하다.

ACKNOWLEDGEMENT

본 연구는 2018년도 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 과제입니다. (No. 20162220200010)

[참고문헌]

[1] Bank of Korea, Development strategy of digital innovation and payment service, 2016 Bank of Korea payment and settlement system conference, 2016.

[2] gartner symposium, http://www.gartner.com/events/na/orlando-symposium, March, 2016.

[3] G. Wood and M. Newborough, “Dynamic energyconsumption indicators for domestic appliances: environment, behaviour and design,” Energy and Buildings, vol. 35, no. 8, pp. 821 - 841, 2003.

[4] 우청원, 에너지 블록체인 도입방안 연구, STEPI Insight, Vol. 222, April, 2018.

[5] finector, 피넥터 보고서 제1호 ‘블록체인 기술의 발전과정과 이해’, 2016.

[6] finector, 피넥터 보고서 제2호 ‘금융기관을 위한 블록체인의 이해’, 2016.

[7] Aron Laszka, Abhishek Dubey, Michael Walker, Doug Schmidt, Providing Privacy, Safety, and Security in IoT-Based Transactive Energy Systems using Distributed Ledgers, IoT '17 Proceedings of the Seventh International Conference on the Internet of Things Article No. 13, 22, Octover, 2017

[8] Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate, CoinShuffle: Practical decentralized coin mixing for Bitcoin. In 19th European Symposium on Research in Computer Security (ESORICS). Springer, 345 - 364, 2014.

[9] George Bissias, A Pinar Ozisik, Brian N Levine, and Marc Liberatore, Sybil-resistant mixing for Bitcoin. In Proc. of 13th Workshop on Privacy in the Electronic Society. ACM, 149 - 158, 03, November, 2014

[10] Michael G Reed, Paul F Syverson, and David M Goldschlag. Anonymous connections and onion routing. IEEE Journal on Selected areas in Communications 16, 4 (1998), 482 - 494, May, 1998.

[11] Nurzhan Zhumabekuly Aitzhan and Davor Svetinovic, Security and Privacy in Decentralized Energy Trading through Multi-Signatures, Blockchain and Anonymous Messaging Streams, IEEE Transactions on Dependable and Secure Computing (Early Access), 12, October, 2016

[12] Gaoqi Liang, Steven R. Weller, Fengji Luo, Junhua Zhao, Zhao Yang Dong, Distributed Blockchain-Based Data Protection Framework for Modern Power Systems against Cyber Attacks, 27, March, 2018.

[13] Jianbin Gao, Kwame Omono Asamoah, Emmanuel Boateng Sifah, Abla Smahi, Qi Xia, Hu Xia, Xiao-Song, Zhang and Dong Guishan, GridMonitoring: Secured Sovereign Blockchain Based Monitoring on Smart Grid, IEEE Access(Volume: 6), 27, February, 2018.

[14] 전기사업법 시행령, 대통령령 제28212호, 26, July, 2017.

[15] 한국에너지공단, 스마트 그리드란 무엇일까?, 27, May, 2016

블록체인 확장성 문제에 대한 분석과 고찰

노시완*, 이경현**

*부경대학교 일반대학원 정보보호학협동과정
**부경대학교 IT융합응용공학과

Analysis and Implications on the Blockchain Scalability

Siwan Noh* and Kyung-Hyune Rhee**

*Interdisciplinary Program of Information Security, Graduate School, Pukyong National University.
**Department of IT Convergence and Application Engineering, Pukyong National University

요 약

비트코인의 등장과 함께 그 기반기술인 블록체인에 대한 국내외의 관심이 증가하는 가운데 국외에서는 블록체인의 확장성 문제에 대한 논의가 활발히 이루어지고 있다. 블록체인은 시스템을 관리하는 중앙기관 대신 네트워크의 사용자들의 합의에 기반하여 시스템을 유지한다. 하지만 신뢰할 수 없는 사용자 간의 합의를 위해 작업증명이라는 신뢰보장을 위한 기술을 사용하였고 이로 인해 비트코인과 같은 공개 블록체인은 제한된 처리량을 가지게 되었다. 하지만 현재까지 알려진 대부분의 공격들이 제한된 처리량으로 인한 처리 지연으로 공격 성공률이 증가하기 때문에 이에 대한 연구가 필요한 실정이다. 때문에 본 논문에서는 이러한 확장성 문제와 함께 현재 알려진 솔루션에 대한 분석과 고찰을 수행하였다.

I. 서론

비트코인[1]은 종래의 은행과 같은 제3자의 개입 없이 개인 간의(Peer-to-Peer, P2P) 안전한 거래가 가능한 결제 시스템으로서 블록체인 기술을 사용한 첫 사례이다. 비트코인 결제 시스템에 참여하고 있는 모든 사용자들은 시스템에서 발생하는 모든 거래에 대한 기록(transaction)을 자신의 블록체인에 저장하고 저장된 기록을 토대로 시스템에서 발생하는 모든 거래를 검증하여 유효한 거래만 자신의 블록체인에 새롭게 추가한다. 이 동작을 시스템의 모든 사용자가 개별적으로 수행하여 최종적으로 시스템의 모든 사용자들이 하나의 동일한 블록체인(거래장부)을 유지·보관하는 분산원장기술(Distributed ledger technology)이다.

신뢰할 수 없는 사용자들 간에 하나의 원장을 선택토록 해야 하는 비잔틴 장군 문제(Byzantine fault tolerance)를 비트코인에서는 작업증명(P

roof-of-Work, PoW)를 사용하여 해결하고 있다. 하지만 이로 인해 하나의 새로운 블록(거래기록의 집합)을 블록체인에 추가하는 것에는 상당한 시간을 필요로 하게 되었고 결과적으로 시간당 처리 가능한 거래의 수는 제한되게 되었다.

이러한 제한된 시간당 처리량으로 인한 확장성 문제(Scalability problem)을 해결하고자 국외에서는 많은 연구가 이루어지고 있으나 국내에서는 관련 연구가 미흡하여 본 논문에서는 이러한 확장성 문제 해결의 필요성과 대표적인

이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구(No.2017-0-00156, 블록체인의 정보보호 프레임워크 및 평가 방법 개발)이며, 일부는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터 육성 지원사업의 연구결과로 수행되었음 (IITP-2018-2015-0-00403)

해결방법들을 소개하고자 한다.

II. 블록체인 확장성

7년전 비트코인의 하루 트랜잭션 처리 수는 5,357개('11.12.31.기준)였지만 최근에는 340,980개('17.01.02.기준)으로 60배 이상 증가하였다[2]. 비트코인 시스템이 평균적으로 10분에 하나의 블록을 처리하고 각 블록은 최대 1MB의 크기를 가지며 포함되는 트랜잭션이 2개의 입력과 3개의 출력을 가진다고 가정할 때 시스템이 하루에 처리 가능한 트랜잭션의 수는 약 305,085개(시간당 약 12,712개)로서 만약 특정 시간대에 처리를 기다리는 트랜잭션의 수가 시간당 최대 처리량을 초과할 경우 처리되지 못한 트랜잭션은 평균 대기시간보다 더 오랜 시간을 대기하거나 처리되지 못할 가능성이 존재한다. 때문에 IoT와 같은 방대한 데이터를 처리하는 분야에 이러한 시스템을 그대로 적용할 경우 확장성 문제에 직면할 수 있다. 현재까지 알려진 많은 공격들[3-5]이 이러한 트랜잭션 처리 지연 혹은 분기로 인한 트랜잭션의 폐기에 기반하고 있고 지연이나 분기의 증가에 따라 공격확률이 증가하므로 이러한 확장성 문제의 해결이 시급한 상황이다.

2.1 파리미터 재설정(Reparameterization)

비트코인의 경우 이러한 확장성 문제에 대한 논의가 개발자들 간에 오래전부터 이루어져왔다. 대표적으로는 현재 비트코인 클라이언트에서 제한해놓은 블록 크기 제한(1MB)을 수정하여 블록에 포함될 수 있는 트랜잭션의 수를 증가시키자는 의견이 대다수였으나 개발자들 간의 합의점을 찾지 못해 기존 시스템과 다른 독립된 블록체인을 만드는 하드포크(Hard fork)를 통해 기존 비트코인 클라이언트에서 파라미터를 재설정하여 시간당 처리량을 증가시킨 비트코인 캐시, 비트코인 클래식, 비트코인 언리미티드와 같은 암호화폐들이 만들어졌다.

블록의 최대크기를 증가시켜 블록에 포함되는 트랜잭션의 수를 증가시키거나 새로운 블록의 추가에 필요한 시간을 감소시킴으로써 시간당 처리량을 증가시킬 수 있지만 이로 인해 또 다른 문제가 발생할 가능성이 증가한다. 그림1.은 네트워크 노드의 수가 100개일 때 블록 크기의 증가에 따른 전파 지연을 나타낸 것으로 블록의 크기가 증가할수록 모든 네트워크의 노드가 블록을 수신하는데 걸리는 시간이 증가함을 확인할 수 있다.

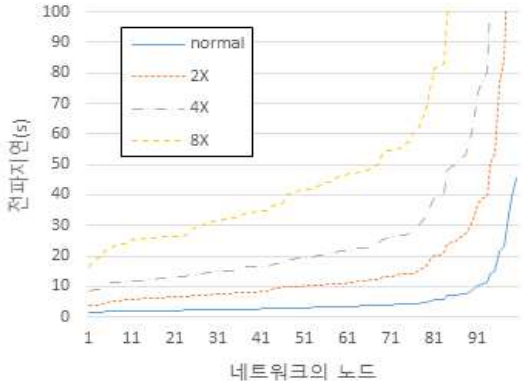


그림 1 블록의 크기에 따른 전파지연
(nodes=100, interval=10m, noBlocks=100)

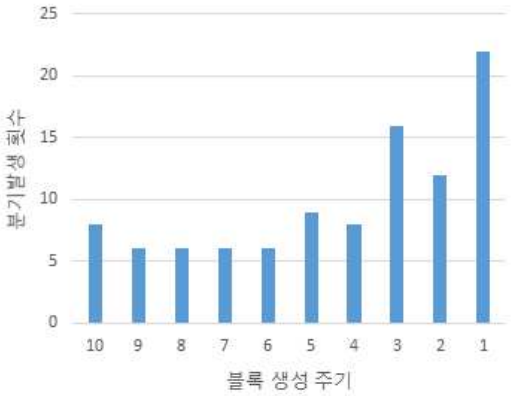


그림 2 블록 생성 주기에 따른 분기 횟수
(nodes=100, blockSize=1MB, noBlocks=1000)

지연시간의 증가는 하나의 블록이 네트워크에 전파되는 도중에 새로운 블록의 전파가 발생하는 분기의 발생 확률이 증가함을 의미한다. 즉, 이러한 전파 지연의 증가는 이를 기반으로 하는 공격의 성공률 또한 증가시킴으로 단순히 블록의 크기를 증가시키는 방식은 보안적 측면에서 적절하지 못하다고 볼 수 있다. 또한 블록 생성 주기를 감소시킬 경우 시간당 처리량은 일정하지만 블록의 생성 주기가 감소하므로 실

질적으로 전체 처리량을 증가시킬 수 있다. 하지만 생성주기의 감소를 위해서는 PoW의 난이도(difficulty)를 감소시켜야하므로 블록의 크기와 마찬가지로 새로운 블록의 발견 확률이 증가하므로 분기의 발생 가능성이 증가한다(그림 2). [6]에서 Croman 등은 이러한 파리미터 재설정에 대해 네트워크 상황에 따른 재설정 한계치를 계산하여 네트워크의 전파지연을 예상하여 전체 노드 중 X%의 노드가 블록을 전파받을 효과적인 처리량(effective throughput)을 구하는 공식을 다음과 같이 구하였다. 본 논문에서는 현재 네트워크 상황에 맞춰 실험을 통해 전파지연을 측정하여 표1과 같이 효과적인 처리량을 계산하였다.

X% effective throughput :=
(block size) / X% block propagation delay

이에 대한 처리량 한계치(throughput limit)는 다음과 같다.

block size / X% effective throughput
< block interval

표 1. X% 노드에 대한 효과적인 처리량
(intreval=10m, nodes=10,000)

X%	effective throughput	translated to transaction/sec
25%	703 Kbps	351 tx/sec
75%	318 Kbps	159 tx/sec
90%	166 Kbps	83 tx/sec

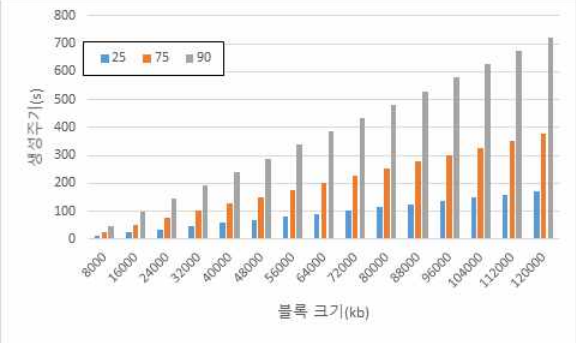


그림 3 블록크기에 따른 X%의 처리량 한계치

위와 같이 정의된 공식에 대해 시뮬레이션[1] 한 결과 그림 3과 같이 블록 크기의 경우 90%의 효과적인 처리량에서 최대 12MB이며 생성주기의 경우 1MB 블록에 대해 최소 48초로 확인되었다. 이는 전파되는 네트워크 대역폭과 같은 네트워크 성능에 의해 변동되므로 시스템 환경을 고려하지 않은 파라미터 재설정은 위험성을 내포하고 있음을 알 수 있다.

2.2 페이먼트 채널(Payment Channel)

페이먼트 채널[7-9]은 특정한 사용자 간에 트랜잭션을 자주 주고받는 상황에서 생성되는 모든 트랜잭션이 아닌 일부만을 블록체인 상에(on-chain)에 저장하고 나머지는 해당 사용자 간(off-chain)에 보관하는 형태로 특정 사용자 간에 하나의 채널을 형성하여 채널 간 거래는 블록체인 외부에서 처리하는 형태이다. [7]에서 제안한 양방향(bidirectional) 채널의 생성은 다음과 같이 이루어진다(그림4,5).

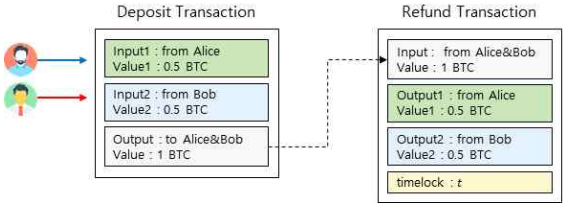


그림 4 페이먼트 채널 초기 상태(on-chain)

1) 채널을 생성하기를 원하는 사용자 A와 B는 자신이 보유한 미사용 출력(unspent transaction output)을 사용하여 하나의 2-of-2 다중서명(multi-signature) 출력을 생성하는 담보(deposit) 트랜잭션을 생성한다.

2) 담보 트랜잭션의 출력을 사용하여 1)에서 각 사용자가 소비한 출력을 원래 사용자에게로 반환하는 반환(refund) 트랜잭션을 timelock t와 함께 생성한다.

3) A는 1)의 담보 트랜잭션의 출력을 사용하여 A와 B에게 금액를 배분하는 커밋먼트(commitment) 트랜잭션 tx_1을 timelock

1) 실험은 http://arthurgervais.github.io/Bitcoin-Simulator에서 배포한 오픈소스 시뮬레이터를 사용하였으며 비트코인 테스트넷에서 10,000개의 네트워크 노드를 가정하고 수행함

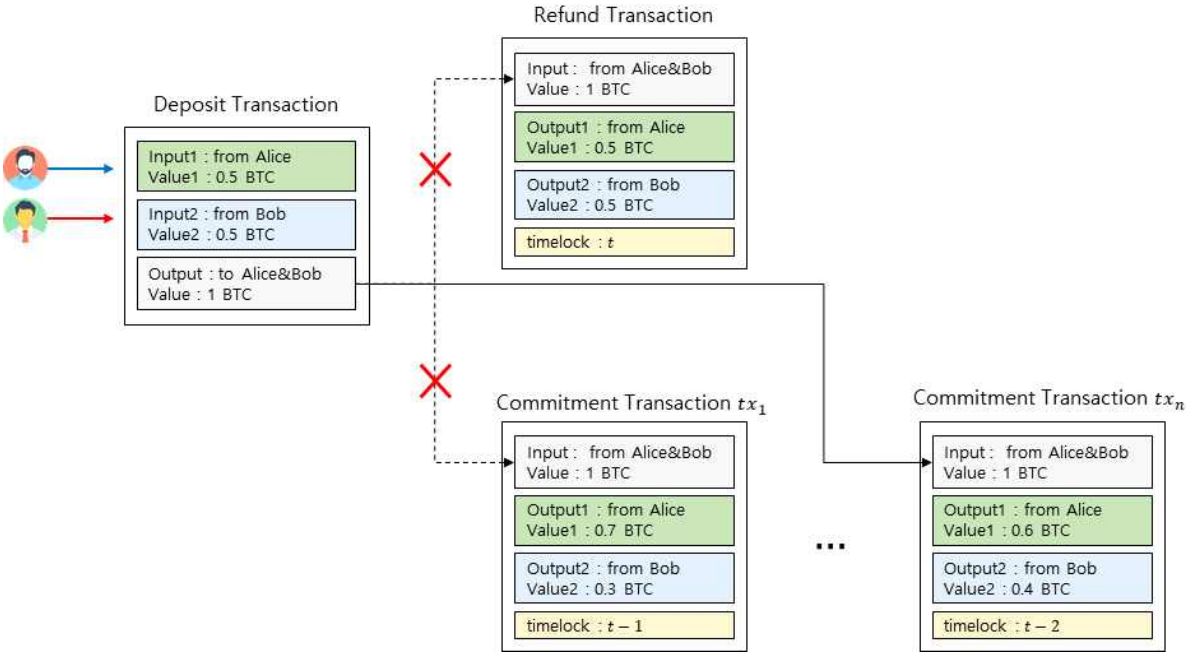


그림 5 n차 업데이트 후 채널 종료 시의 트랜잭션 상태

$t-1$과 함께 생성하여 서명 후 B에게 전달한다.

4) B는 3)에서 생성된 tx_1의 내용에 동의할 경우 tx_1에 대한 자신의 서명을 첨부하여 A에게 전달한다.

5) 3)~4)의 과정을 더 이상 거래가 필요하지 않다고 판단될 때까지 반복하여 tx_1을 수정하여 최종적으로 생성된 tx_n을 시간 t 이전에 블록체인에 전파한다.

이와 같이 생성된 트랜잭션은 최초의 담보 트랜잭션과 이를 반환하는 반환 트랜잭션, A와 B사이에 주고받는 $\{tx_1,...,tx_n\}$와 같이 $n+2$개 이지만 실제 블록체인 상에는 담보 트랜잭션과 최종적으로 업데이트된 tx_n만이 추가된다. 담보 트랜잭션의 출력을 반환하는 반환 트랜잭션은 최종적으로 합의된 트랜잭션 tx_n이 시간 t 이전에 블록체인에 추가될 경우 동일한 출력을 사용하는 반환 트랜잭션은 이중지불로 인해 네트워크의 노드들에 의해 폐기된다.

페이먼트 채널은 네트워크에 전파되는 트랜잭션의 수를 감소시킬 뿐 아니라 전파된 트랜잭션이 블록에 포함되어 추가되는 것을 기다릴 필요가 없기 때문에 매우 빠른 처리속도를 보장 받을 수 있다. 또한 채널에 속한 사용자 간에만 트랜잭션을 주고받음으로써 사용자의 프라이버시 또한 보장받을 수 있지만 네트워크의 모든 사용자들 사이에 채널을 생성할 경우 $O(N^2)$의 담보 트랜잭션의 생성이 필요하기에 [7]에서는 일부 사용자들이 몇몇 불특정다수의 사용자와 채널을 형성하고 있을 경우 A와 B 사이에 이러한 여러 페이먼트 채널을 경유하여 통신하는 페이먼트 네트워크가 제안되었다.

하지만 페이먼트 채널의 경우 사전에 생성한 담보 트랜잭션에 포함된 담보 금액만큼의 트랜잭션만을 생성 가능하기에 담보 트랜잭션에서 정의한 금액을 초과하여 사용해야할 경우 발생하는 고갈문제가 존재한다. 이러한 담보를 초과하는 트랜잭션의 생성을 위해서는 채널을 닫고(close) 새로운 담보 트랜잭션을 생성할 수밖에 없으며 off-chain에서 생성된 트랜잭션은 채널이 종료되어 블록체인에 포함될 때까지 제3자에게 트랜잭션의 유효성을 인정받을 수 없다는 문제가 존재한다. [10]에서는 채널의 종료없이 담보 트랜잭션의 값을 변경하는 방법과 함께 [7]에서 제안한 페이먼트 네트워크에서 채널에 필요한 시간비용을 줄이는 상태 채널(State

Channel)에 대한 개념를 제안하였다.

앞서 분석한 파리미터 재설정과 페이먼트 채널은 확장성 문제를 해결하기 위해 제안되었으나 현재까지 이를 완전하게 해결할 수 있는 단일 솔루션은 존재하지 않는다. 블록체인 어플리케이션을 적용하고자하는 시스템의 특성과 사용하는 네트워크의 성능에 따라 현재 존재하는 여러 솔루션을 복합적으로, 혹은 단일로 사용하여 시스템 환경에 맞는 방법을 적용하는 방법이 블록체인 시스템 구축 전에 필요할 것으로 보인다.

III. 결론

본 논문에서는 블록체인 확장성 문제에 대해 가장 대중적인 솔루션인 파라미터 재설정과 페이먼트 채널에 대해 기술하고 실험을 통해 이를 검증하였다. 현재 국내 블록체인 관련 산업은 증가하고 있지만 기반기술에 대한 연구보다는 응용에 초점을 맞추고 있기에 추후 국내 기술이 국외에 종속될 위험이 높다. 국가 경쟁력 제고 및 안전한 블록체인 어플리케이션의 개발을 위해서도 확장성 문제와 같은 블록체인 기반기술에 대한 연구가 필요하다.

[참고문헌]

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

[2] https://blockchain.info/charts/n-transactions

[3] Eyal, I., and Sirer, E. G. “Majority is not enough: Bitcoin mining is vulnerable,” In International conference on financial cryptography and data security, Springer, pp.436-454, 2014.

[4] Heilman, E., Kendler, A., Zohar, A., and Goldberg, S. “Eclipse Attacks on Bitcoin's Peer-to-Peer Network,” In USENIX Security Symposium, pp.129-144, 2015

[5] Bahack, L. “Theoretical Bitcoin Attacks with less than Half of the Computational Power (draft),” arXiv preprint arXiv:1312.7013. 2013.

[6] Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., ... & Song, D. (2016, February). On scaling decentralized blockchains. In International Conference on Financial Cryptography and Data Security (pp. 106-125). Springer, Berlin, Heidelberg.

[7] J. Poon and T. Dryja. “The bitcoin lightning network.”, https://lightning.network/lightning-network-paper.pdf, retrieved Nov 26, 2015.

[8] Christian Decker and Roger Wattenhofer. A fast and scalable payment network with bitcoin duplex micropayment channels. In Symposium on Self-Stabilizing Systems, pages 3 – 18. Springer, 2015.

[9] Burchert, Conrad, Christian Decker, and Roger Wattenhofer. "Scalable Funding of Bitcoin Micropayment Channel Networks." International Symposium on Stabilization, Safety, and Security of Distributed Systems., 2017.

[10] Miller, A., Bentov, I., Kumaresan, R., Cordi, C., & McCorry, P. (2017). Sprites and State Channels: Payment Networks that Go Faster than Lightning.arXiv preprint arXiv:1702.05812.

2018 한국정보보호학회 하계학술대회

C2 암호화폐/블록체인 4

현 상 원 (조선대학교)

- **블록체인을 활용한 공동인증서비스 기술 분석**
  이연수, 이가영, 이혜지, 염홍열
- **(D)PoS 기반 블록체인의 거래 및 합의 방식 분석**
  한성호, 홍동연, 최낙준, 이나비, 김광조
- **IoT 환경의 확장성을 위한 블록체인을 이용한 키 교환 프로토콜**
  이정호, 최형기
- **비트코인 탈익명화 사례 분석**
  홍지형, 김윤정

블록체인을 활용한 공동인증서비스 기술 분석

이연수, 이가영, 이혜지, 염흥열

*순천향대학교 정보보호학과

Analysis of joint authentication service technology using block chain

Yeun-Su Lee, Ga-Young Lee, Hye-Ji Lee, Heung-Youl Youm

*Department of Information Security Engineering, Soonchunhyang University.

요 약

최근 블록체인 기술은 국내외 여러 산업 분야에서 혁신적인 기술로 주목받고 있다. 특히 금융 분야에서 기존 시스템을 개선하기 위하여 블록체인을 도입하려는 시도가 활발히 이루어지고 있다. 따라서 본 논문에서는 블록체인을 활용한 새로운 금융 인증 서비스인 공동인증서비스에 대해 정의하고 설명한다. 또한 공동인증서비스가 가지는 안정성 및 효율성을 통해 기존 금융 인증 서비스에 대한 한계점을 시사하고 공동인증 서비스를 이용하기 위한 인증서 생성 및 등록 과정, 인증 과정, 데이터 처리과정을 단계적으로 자세하게 분석하고자 한다.

I. 서론

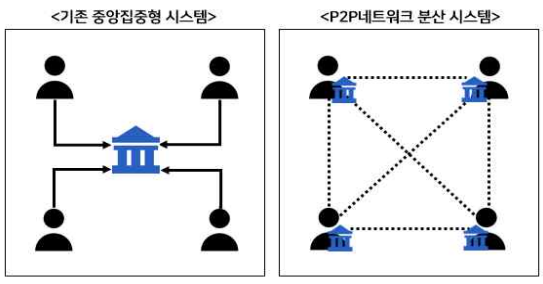
거래 데이터를 분산 저장하여 위·변조를 방지하는 기술인 블록체인(Blockchain)은 2008년도에 개발된 비트코인(Bitcoin)의 기반 기술로 시작되어 현재까지 혁신적인 기술로 주목받고 있다[1]. 실제로 2015년부터 블록체인에 대한 투자 건수와 규모가 증가 하고 있으며[1], 이미 미국, 호주, 영국 등 여러 국가에서 블록체인 기술 도입을 위한 시도가 이루어지고 있다[1].

블록체인 기술은 기존의 인프라에 비해 높은 보안성, 확장성, 투명성 등을 보장하며[2] 교육, 의료, 자율주행자동차 등 다양한 분야에 적용이 가능하다[3]. 특히 금융 분야에서는 기존 시스템의 신뢰성, 보안성, 경제성 등을 개선하기 위한 블록체인 활용 사례가 등장하고 있다[1][4].

따라서 본 논문에서는 블록체인을 활용한 새로운 금융 인증방식인 공동인증서비스를 분석하기 위해 관련 논문인 '클라우드 기반의 분산원장기술을 활용한 전자금융기반시설 간의 공동인증서비스에 대한 보안 프레임워크 제안[5]'을 기반으로 공동인증서비스 사용자에 대한 신규 등록 및 인증절차, 데이터 처리과정을 재분석하고 블록체인에 대한 연구를 진행했다.

II. 관련 연구

2.1 블록체인 정의 및 특징

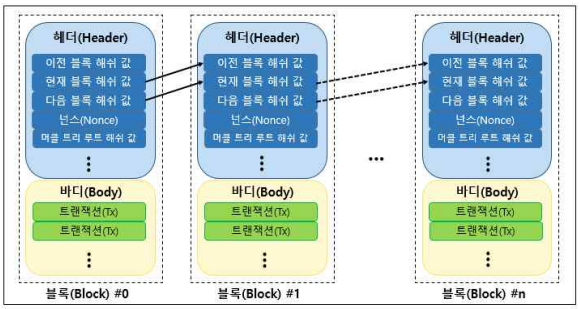


[그림 1] 기존의 중앙집중형 방식과 블록체인 방식

블록체인(Blockchain) 기술은 데이터 거래 시 P2P네트워크의 모든 참여자들이 거래 내용을

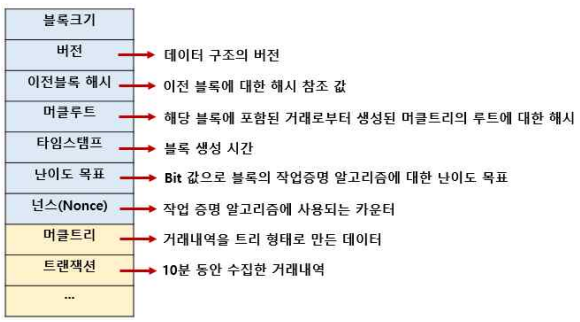
공동으로 기록·저장·관리하는 분산화된 공개 장부 관리 기술을 가리킨다[6]. 신뢰할 수 있는 제 3 기관을 설립하여 데이터를 중앙집중형으로 관리하는 기존의 시스템과 달리 블록체인은 P2P네트워크에 공동으로 데이터를 분산하고 관리하는 구조상 제 3의 기관이 불필요하므로 기존 중앙집중형의 운영 및 유지보수, 보안 등에 필요한 비용을 절감할 수 있다[4].

또한 블록체인은 각각의 블록이 이중 연결 리스트로 이루어진 데이터베이스이며, 블록체인을 구성하고 있는 블록은 거래별로 데이터가 기록되는 단위를 의미한다[7]. 블록체인의 기본 구조는 다음 [그림 2]과 같다[7].



[그림 2] 블록체인 연결 구조

해당 블록은 크게 헤더(Header)와 바디(Body)로 나뉘고[7], 헤더와 바디에 포함되고 있는 정보는 다음 [그림 3]와 같다.



[그림 3] 블록 구조

상기와 같이 블록체인을 구성하고 있는 블록은 이전 블록의 정보, 현재 거래 정보, 해시 값과 같은 데이터들을 포함하며 해당 블록을 P2P 네트워크에 분산처리 방식으로 기록 및 관리하며 블록체인은 다음과 같은 특성을 지닌다[4].

[표 1] 블록체인 특성

구분	내용
분산성	신뢰하는 제3기관 없이 P2P네트워크 환경에서 거래 가능
확장성	공개된 소스에 의해 네트워크의 모든 참여자가 구축·연결·확장 가능
투명성	모든 데이터 거래 기록에 공개적으로 접근이 가능
보안성	데이터 거래 내역을 네트워크의 모든 참여자가 공동으로 기록함으로써 거래 조작 방지 및 무결성 보장
안정성	참가 시스템 중 일부가 오류 또는 성능 저하 발생 시 전체 네트워크에 영향 미미

상기와 같은 특성을 기반으로 블록체인은 암호화 화폐, 주식거래(장외시장), 금융거래, 스마트 계약 등의 다양한 분야에서 활용된다[2].

2.2 블록체인 종류별 특징

블록체인은 참여하고 있는 네트워크의 특징, 범위 등에 따라 크게 퍼블릭, 프라이빗, 컨소시엄 블록체인으로 구분된다[4].

[표 2] 블록체인 종류별 특징

요소	퍼블릭	프라이빗	컨소시엄
관리주체	모든 거래 참여자	하나의 중앙기관	컨소시엄에 참여하는 사용자
거래속도	느림	빠름	빠름
데이터 접근	제한 없음	허가받은 사용자	허가받은 사용자
식별성	익명성	식별가능	식별 가능
거래증명	검증 알고리즘에 따라 거래 증명자 결정(사전에 알 수 없음)	중앙기간에 의하여 거래증명이 이루어짐	거래 증명자가 인증을 거쳐 알려짐
활용사례	비트코인	링크(Linq)	RSCEV, CASPER

공동인증서비스는 컨소시엄 블록체인을 활용하고 있으며, 자세한 설명은 본 논문의 연구내용에서 다루고자 한다.

Ⅲ. 연구내용

3.1 공동인증서비스 정의

공동인증서비스는 온라인 거래, 자금 이체 등을 이용하기 위하여 사용자 인증 과정에서 블록체인의 원리 및 특성을 이용해 인증서 및 인증 데이터를 컨소시엄 블록체인 인프라에 저장하는 인증 서비스이다[8]. 인증서 및 인증 데이터가 컨소시엄 블록체인 네트워크 내에 분산되어 저장되므로 데이터의 위·변조 위험이 감소하며, 제 3자의 도움 없이 사용자 인증이 이루어진다[9]. 또한 블록체인 네트워크 내에 인증서 및 인증 데이터가 보관되기 때문에 인증서 및 인증 데이터를 관리하는 중앙 기관이 불필요하게 되어 유지 및 생성 비용이 감소한다[10].

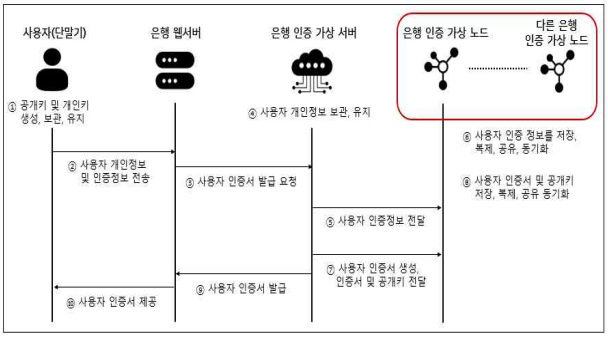
기존의 온라인 거래, 자금 이체 등을 이용하기 위한 사용자 인증은 대표적으로 공인인증서를 이용한 인증 방식이 있다. 공인인증서를 이용한 인증 방식은 은행에서 서비스를 받기 위해 사용자 인증서 생성 및 인증 과정을 거치며 은행 서버 내에 데이터가 저장된다[9]. 은행 간에 사용자 인증정보가 공유되지 않으므로 다른 은행에서 서비스를 받기 위해서는 이전에 진행한 인증 과정을 반복해야 한다[9]. 공동인증서비스는 컨소시엄 블록체인 인프라를 통하여 상기의 문제점을 해결하고 사용자 및 은행에게 편리성과 효율성을 제공한다[9]. 실제로 인증이 이루어지는 방식은 기존 PKI(Public Key Infrastructure) 방식의 인증 과정과 동일하며 PKI 방식에 대한 자세한 설명은 본 논문 3.3.1에서 설명하고자 한다.

3.2 인증서 생성 및 등록

[표 3] 개인 및 인증 정보 구성 내용

구분	이름
개인정보	고유식별정보
	생년월일
	휴대전화 번호
	이름
인증정보	이용자ID, 비밀번호
	계좌번호, 계좌 비밀번호
	PIN
	생체정보 검증 결과

인증서 생성 및 등록 과정에서 전송되는 개인정보와 인증정보의 구성내용은 [표 3]과 같다[5]. 인증정보에 포함되는 비밀번호와 계좌 비밀번호는 해쉬함수를 통하여 해싱된 값으로 블록체인 네트워크 내에 저장된다.



[그림 4] 공동인증서비스의 인증서 생성 및 등록 과정

공동인증서비스를 활용한 인증을 이용하기 위해서는 사용자에 대한 인증서 생성 및 등록 과정이 필수적이다. 인증서 생성은 은행 인증 가상 서버에서 이루어지며 생성된 인증서는 컨소시엄 블록체인 네트워크에 저장된다. 생성 및 등록 과정은 기존 관련 논문[5]을 참고하여 재해석을 진행하였으며 [그림 4]와 같은 과정을 거친다. 자세한 설명은 단계별로 아래에서 설명하고자 한다.

STEP 1. 공동인증서비스를 이용하고자 하는 사용자는 자신의 공개키 및 개인키를 생성하고 보관 및 유지한다.

STEP 2. 사용자는 자신의 개인정보 및 인증정보를 은행 웹서버에 전송한다.

STEP 3. 은행 웹서버는 은행 인증 가상 서버에게 사용자로부터 전달 받은 개인정보 및 인증정보를 포함하여 인증서 발급 요청 신호를 전송한다.

STEP 4. 은행 인증 가상 서버는 은행 웹서버로부터 전달 받은 사용자 개인정보를 자신의 서버에 보관 및 유지한다.

STEP 5. 은행 인증 가상 서버는 은행 웹서버로부터 전달 받은 사용자 인증정보를 은행 인증 가상 노드에게 전달한다.

STEP 6. 은행 인증 가상 노드는 은행 인증 가상 서버로부터 전달받은 사용자 인증정보를 블록체인 네트워크 내에 저장하고 복제, 공유, 동기화를 한다.

STEP 7. 은행 인증 가상 서버는 사용자 인증서를 생성하여 은행 인증 가상 노드에게 인증서 및 공개키를 전달한다.

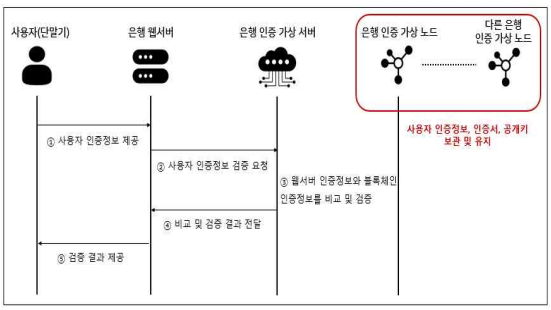
STEP 8. 은행 인증 가상 노드는 은행 인증 가상 서버로부터 전달받은 사용자 인증서 및 공개키를 블록체인 네트워크 내에 저장하고 복제, 공유, 동기화를 한다.

STEP 9. 은행 인증 가상 서버는 은행 웹서버에게 생성된 사용자 인증서를 전달한다.

STEP 10. 은행 웹서버는 은행 인증 가상 서버에게 받은 사용자 인증서를 사용자에게 제공한다.

상기의 모든 과정이 정상적으로 이루어지면 인증서가 생성되고 블록체인 네트워크에 등록이 된다. 이후 블록체인 네트워크에 저장된 인증정보 및 인증서를 통하여 사용자 인증이 이루어진다.

3.3 사용자 인증



[그림 5] 공동인증서비스의 사용자 인증 절차 과정

사용자는 공동인증서비스 이용 전 3.2에서 등록한 인증정보에 대한 인증 과정을 거쳐야한다. 사용자 인증에서는 은행 인증 가상 노드에 보관중인 인증정보와 사용자가 제공한 인증정보를 비교 및 검증하는 과정을 포함하고 있으며 인증정보의 구성요소는 3.2에서 언급한 것과 동일하다. 사용자 인증 절차는 기존 논문[5]을 바탕으로 재해석을 진행하여 [그림 5]와 같은 과정을 거친다. 또한 추가적으로 기존 인증과정에서 인증정보를 비교 및 검증하는 과정을 3.3.1에 서술하였다. 사용자 인증과정에 대한 자세한 설명은 아래 단계별로 설명하고자 한다.

STEP 1. 사용자(단말기)는 사용자 인증정보를 은행 웹서버에게 제공한다.

STEP 2. 은행 웹서버는 은행 인증 가상 서버에게 사용자 인증정보 검증을 요청한다.

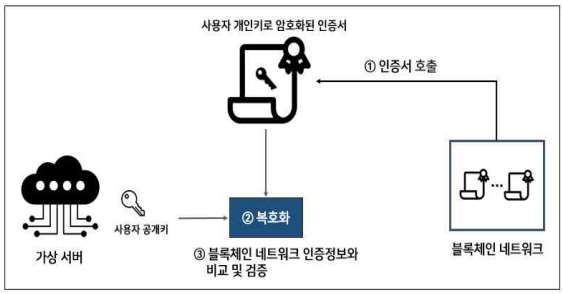
STEP 3. 은행 인증 가상 서버는 은행 웹서버로부터 전달받은 웹서버 인증정보와 블록체인 인증정보를 비교 및 검증한다. 이때 검증은 PKI 기반으로 진행하며 자세한 설명은 3.3.1에서 하고자 한다.

STEP 4. 은행 인증 가상 서버와 은행 인증 가상 노드에서 인증정보에 대한 비교 및 검증한 결과를 은행 웹서버에게 전달한다.

STEP 5. 은행 웹서버는 사용자(단말기)에게 결과를 전달한다.

3.3.1 PKI

인증기관 및 등록기관으로 구성되어 인증서의 발급 및 유효성을 검증하는 체계를 말하는 PKI(Public Key Infrastructure), 공개키 기반구조는 인증기관을 기반으로 공개키 암호 시스템이 원활히 응용될 수 있도록 하는 암호기법이다[11]. 인증기관에서 인증된 공개키를 사용함으로써 공개키의 안전성을 보장하고 위장 공격을 예방할 수 있는 보안성을 지니고 있으며[12]. 복호 시, 사용자만이 소유하고 있는 개인키로만 복호화가 가능하다.



[그림 6] PKI 기반 인증정보 비교·검증 과정

공동인증서비스 모델은 위와 같은 PKI 기법을 기반으로 사용자 인증을 거치며 과정은 [그림 6]과 같다.

STEP 1. 블록체인 네트워크 내에 저장되어 있는 사용자 인증정보는 가상노드를 통해 호출한다.

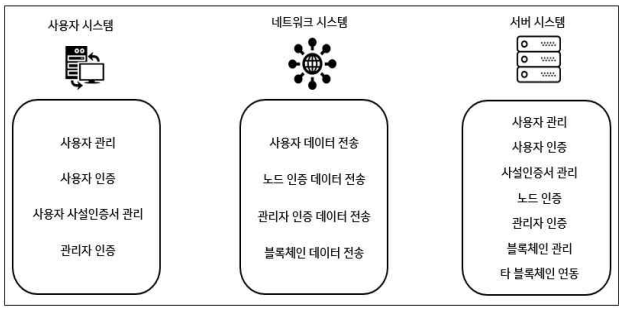
STEP 2. 가상 서버는 사용자의 공개키로 사용자의 개인키로 암호화된 인증서를 복호화 한다.

STEP 3. 복호화된 블록체인 네트워크 인증정보와 사용자가 제공한 인증정보와 비교 및 검증을 진행한다.

인증서 생성 및 등록, 사용자 인증과정의 절차를 3.2와 3.3에서 설명하였다. 3.4에서는 사용자 개인정보 및 인증정보, 관리자 인증정보, 노드 인증정보의 데이터 처리 과정에 대한 분석을 진행하였다.

3.4 데이터 처리

공동인증서비스의 데이터 처리에 필요한 구성요소는 [그림 7]과 같이 3개의 시스템과 하위에 내장된 서브시스템으로 구성되며 해당 과정은 기존 논문을 바탕으로 분석하였다[5].



[그림 7] 데이터 처리 과정 구성 요소

데이터 처리 과정은 서브시스템 간의 데이터 전달과정을 통하여 진행되며 데이터로는 사용자, 관리자, 노드의 개인정보 및 인증정보가 해당된다. 포함되는 정보는 [표 4]에 나타내었다[5].

[표 4] 서브시스템 개인·인증정보 구성요소

구분	이름
이용자 개인정보	고유식별정보
	생년월일
	휴대전화 번호
	이름
이용자 인증정보	이용자ID, 비밀번호
	계좌번호, 계좌 비밀번호
	PIN
	생체정보 검증 결과
관리자 인증정보	관리자 ID, 비밀번호
노드 인증정보	MAC 주소
	사용자·서버용 인증서

상기와 같은 데이터에 대한 처리법은 각 사용자 시스템, 네트워크 시스템, 서버시스템 별로 나누어 설명하고자 한다.

3.4.1 사용자 시스템

사용자 시스템에 포함된 서브시스템은 4개이며 데이터 처리법은 다음 [표 5]와 같다.

[표 5] 사용자 시스템 데이터 처리법

서브시스템	처리법
사용자 관리	사용자 개인·인증 정보 네트워크 시스템에 전송
사용자 인증	사용자 인증정보 네트워크 시스템에 전송
사용자 사설 인증서 관리	공개키 및 사설인증서 네트워크 시스템에 전송
관리자 인증	관리자 인증정보 네트워크 시스템에 전송

3.4.2 네트워크 시스템

네트워크 시스템에 포함된 서브시스템은 4개이며 데이터 처리법은 다음 [표 6]과 같다.

[표 6] 네트워크 시스템 데이터 처리법

서브시스템	처리법
사용자 데이터 전송	사용자 인증결과, 사설인증서 사용자 시스템에 전송
	사용자 개인·인증정보, 공개키 서버 시스템에 전송
노드 인증	노드별 MAC 주소 수집

데이터 전송	인증정보 서버 시스템에 전송
관리자 인증 데이터 전송	관리자 인증결과 사용자 시스템에 전송
	관리자 인증정보 서버 시스템에 전송
블록체인 데이터 전송	사용자 인증정보, 공개키, 사설 인증서 서버 시스템에 전송

3.4.3 서버 시스템

서버 시스템에 포함된 서브시스템은 7개이며 데이터 처리법은 다음 [표 7]과 같다.

[표 7] 서버 시스템 데이터 처리법

서브시스템	처리법
사용자 인증	사용자 인증결과, 사설인증서 네트워크 시스템에 전송
사설인증서 관리	인증결과 네트워크 시스템에 전송
노드 인증	노드 인증결과 네트워크 시스템에 전송
관리자 인증	관리자 인증결과 네트워크 시스템에 전송
블록체인 관리 타 블록체인 연동	이용 시, 사용자 인증정보, 공개키, 사설인증서 네트워크 시스템에 전송

공동인증서비스에서의 인증서 생성 및 등록, 사용자 인증, 데이터 처리 과정을 분석하였다. 공동인증서비스는 기존 인증방식인 공인인증서에서 활용하는 PKI 기법을 기반으로 인증정보를 비교 및 검증하는 방식을 취하고 있다. 따라서 공개키의 안전성을 보장할 뿐만 아니라 블록체인을 활용함으로써 거래 내역의 투명성과 데이터의 조작을 방지하고 무결성을 보장하는 등 기존 인증 방식의 한계점을 해결할 수 있을 것으로 기대된다.

Ⅳ. 결론

최근 블록체인은 거래 데이터를 분산 저장하여 위·변조를 방지하는 기술로써 금융 분야에서 많은 활용을 하고 있다. 따라서 본 논문에서는 블록체인을 활용한 새로운 인증방식인 공동인증서비스에 대한 인증서 생성 및 등록, 사용자 인증과정, 데이터 처리과정을 분석하였다. 그 결과, 해당 서비스에 적용된 기법 및 처리 과정을 확인할 수 있었다.

블록체인을 활용한 다양한 응용사례가 나오는 시점이지만 여전히 기술적, 관련 법규에 대한 개선점 및 블록체인의 보안위협에 대한 해결법이 요구되고 있다. 따라서 향후 공동인증서비스에서 나타날 수 있는 보안위협을 분석하고 이와 관련된 해결법에 대한 연구가 추가로 필요하다.

[참고문헌]

[1] 서영희, 송지환, 공영일, 블록체인(Blockchain) 기술의 산업적·사회적 활용 전망 및 시사점, 소프트웨어정책연구소, pp. 3-7, 2017.09.

[2] 한승우, 블록체인 활용사례로 알아보는 금융권 적용 고려사항, 전자금융과 금융보안 제3호, pp. 22-34, 2016.01.

[3] 서영희, 블록체인 기술의 다양한 활용 사례, 소프트웨어정책연구소, 2017.11.

[4] 홍승필, 금융권 블록체인 활용 방안에 대한 정책 연구, 전자금융과 금융보안 제6호, pp. 12-18, 2016.04.

[5] 박근덕, 클라우드 기반의 분산원장기술을 활용한 전자금융기반시설 간의 공동 인증 서비스에 대한 보안 프레임워크 제안, 순천향대학교 대학원, 2018.02

[6] 김동섭, 분산원장 기술과 디지털통화의 현황 및 시사점, 한국은행, pp. 1-6, 2016.01.

[7] 박강희, 블록체인의 이해와 금융업의 활용에 대한 고찰, IBK경제연구소, pp. 1-4, 2017.07.

[8] 이상기, 증권플랫폼에서의 블록체인 활용과 시사점, 코스콤 R&D, 2017.07.

[9] 강송희, 유호석, 김준연, 공인인증과 전자서명의 미래, 소프트웨어정책연구소, pp. 12, 2017.12.

[10] 유성민, 블록체인을 활용한 효율성 향상 적용 사례, 정보통신기술진흥센터, pp. 22, 2018.02.

[11] 정소윤, 공개키 기반(PKI)의 전자서명 인증제도 활성화 방안 연구, 연세대학교 대학원, 2002.

[12] 조원희, 임재홍, PKI 기반의 암호화 통신 컴포넌트 설계 및 구현, 한국정보통신학회논문지 제 9권 제 6호, pp. 1-2, 2005.05.

(D)PoS 기반 블록체인의 거래 및 합의 방식 분석1)

한성호* 홍동연* 최낙준* 이나비* 김광조*
*카이스트 정보보호대학원

Analysis of Consensus and Transaction of (D)PoS-based Blockchains

Seongho Han* Dongyeon Hong* Nakjun Choi* Nabi Lee* Kwangjo Kim*
*Graduate School of Information Security, KAIST.

요 약

블록체인은 데이터 위조 방지와 데이터의 분산 저장을 제공하는 분산원장 기술이다. 블록체인에서 각 노드는 데이터가 기록된 블록을 분산 저장한다. 하지만 데이터를 분산 저장할 경우 동일한 데이터베이스를 유지하지 못하는 문제가 발생한다. 여러 노드에 동일한 데이터를 분산저장하기 위해 고안된 방식이 합의 알고리즘이다. 최초의 암호화폐인 비트코인은 PoW를 합의 알고리즘으로 채택하였다. 그러나 PoW 알고리즘은 불필요한 자원과 에너지가 소모된다는 단점을 가지고 있다. 이 문제를 해결하기 위해 등장한 합의 알고리즘이 PoS이다. 그리고 PoS에 위임의 형식을 추가한 것이 DPoS이다. 본 논문에서는 (D)PoS를 채택한 대표적인 블록체인 어플리케이션인 QTUM, ADA, EOS, LISK의 합의 알고리즘을 분석한다. 또한 각 코인의 블록 구조 및 거래 방식을 분석한다. 본 논문의 분석 결과를 추후 각 블록체인의 신뢰성 검증에 활용할 수 있는 가능성을 제시한다.

I. 서론

암호화폐와 기반 기술인 블록체인에 대한 관심이 높아지고 있다. 블록체인은 데이터 위조 방지와 데이터의 분산 저장을 제공하는 분산원장 기술이다. 블록체인에서 각 노드는 데이터가 기록된 블록을 저장한다. 하지만 데이터를 분산 저장할 경우 동일한 데이터베이스를 유지하지 못하는 문제가 발생한다. 여러 노드에 동일한 데이터를 분산저장하기 위해 고안된 방식이 합의 알고리즘이다.

최초의 암호화폐인 비트코인[1]은 작업 증명 방식(Proof of Work, PoW)을 합의 알고리즘으로 채택하였다. 그러나 PoW 알고리즘은 불필요한 자원과 에너지가 소모된다는 단점을 가지고 있다. 이 문제를 해결하기 위해 등장한 합의 알고리즘이 지분 증명 방식(Proof of Stake, PoS)[5]이다. 그리고 PoS에 위임의 형식을 추가한 것이 위임 지분 증명 방식[4](Delegated Proof of Stake, DPoS)이다.

본 논문에서는 (D)PoS방식에 대하여 설명하고, (D)PoS를 합의 프로토콜로 채택한 대표적인 블록체인 어플리케이션인 QTUM[2,9], ADA[11], EOS[7], LISK[8]의 합의 알고리즘을 분석한다. 세부적으로 각 코인을 블록 구조 및 거래 방식의 관점에서 분석한다.

1.1 논문의 구성

본 논문의 구성으로 Ⅱ장에서는 각 코인과 PoS 및 DPoS에 대하여 간략히 설명하고, Ⅲ장은 각 코인의 합의 알고리즘을 분석한다. Ⅳ장에서는 각 코인의 블록 구조 및 거래 방식을 분석한다. 마지막으로 Ⅴ장에서는 결론과 본 논

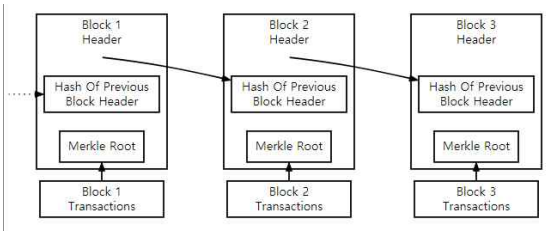
1) 본 연구는 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행되었습니다. (No.2017-0-00555, 양자 컴퓨터 환경에서 래티스 문제를 이용한 다자간 인증키교환 프로토콜 연구)

문 성과를 이용한 추후 연구에 대한 가능성을 제시한다.

II. 배경지식

2.1 블록체인 어플리케이션

이 절에서는 QTUM, ADA, EOS, LISK에 대해 설명한다. [그림 1]은 블록체인의 기본적인 구조를 나타낸다.



[그림 1] 블록체인의 구조

QTUM[2,9] QTUM은 비트코인과 이더리움[6]을 합친 암호화폐로 볼 수 있다. 비트코인은 Unspent Transaction Output(이하 UTXO)을 기반으로 state를 관리하는 반면 이더리움은 Account를 기반으로 state를 관리한다. 두 암호화폐는 서로 호환이 되지 않는 구조이기 때문에 QTUM은 Account Abstraction Layer(이하 AAL)을 통해 둘 사이에 연결 다리를 놓았다. QTUM의 목표는 최초의 UTXO 기반의 스마트 컨트랙트 시스템을 구현하는 것이다.

ADA[11] ADA는 모바일에 최적화된 플랫폼인 Cardano를 통해 만들어진 암호화폐이다. 2015년에 IOHK에 설계됐고 2017년 10월에 공식 발표됐다. ADA는 DPoS를 채택한 암호화폐 중 하나이며 Ouroboros 프로토콜을 적용하면서 신뢰성이 상승하고 화폐의 가치가 증가했다.

EOS[7] EOS는 분산화된 어플리케이션의 확장성을 위해 고안된 블록체인 플랫폼 혹은 운영체제로 볼 수 있다. 계정, 인증, 데이터베이스, CPU 스케줄링 등 많은 기능들을 제공한다. 거래 처리량을 초당 백만 개로 유지하여 기존 암호화폐의 단점을 개선하는 것과 무료로 사용하는 것 등을 목표로 하고 있다.

LISK[8] LISK는 이더리움[6]처럼 블록체인 어플리케이션의 플랫폼을 제공하는 걸 목표로 한다. 이더리움과의 차이는 자바 스크립트를 기반으로 블록체인 어플리케이션의 플랫폼을 제공한다는 점이다. 다른 플랫폼들과 달리 개발자들은 메인 체인에 저장할 필요 없이 사이드 체인에 저장할 수 있다. 따라서 개발자들은 자신들의 체인을 구성하고 관리할 수 있다.

2.2 합의 알고리즘

지분 증명 방식(PoS)[5] 현재 가장 많이 사용되는 합의 알고리즘은 PoW이다. 하지만 PoW는 자원과 에너지가 과도하게 소모된다는 단점을 갖고 있다. 이를 대체하는 방법으로 PoS가 고안되었다. PoS는 PoW와 달리 채굴자가 없고 검증자가 존재한다. 검증자 선발 과정은 두 단계로 나뉜다. 우선 참가자들은 시스템을 통해 보증금을 예치한다. 이후 특정 규칙에 따라 최종적으로 검증자를 선발한다. 검증자가 된 사람은 거래의 유효성을 확인하고 블록을 생성한다. 검증자로 있는 기간이 길어질수록 받는 인센티브가 증가한다. 검증자는 유효하지 않은 거래를 거짓으로 유효하다고 할 수 없다.

위임 지분 증명 방식(DPoS)[4] DPoS는 PoS와 달리 누구에게나 검증자가 될 기회가 주어지지 않는다. 검증자가 되기 위해선 투표를 거쳐야 한다. 이때 명칭이 바뀌는데 투표를 통해 선출된 검증자를 대표자라고 한다. 선출된 대표자들은 블록을 생성한다. 블록을 확정하기 위해선 2/3 이상의 승인이 필요하다. 대표자의 지위는 일정 시간 이내에 블록 생성에 참여해야 유지된다. PoS와 달리 같은 시간에 훨씬 더 많은 거래를 처리할 수 있다는 점과 수수료가 없다는 장점이 있다.

III. 각 코인의 (D)PoS 합의 알고리즘 분석

QTUM PoS 2.0[9]에서 새 블록의 생성은 다음 조건을 충족해야 한다.

$$ProofHash < coins \times age \times target$$

ProofHash는 계산할 때 사용되지 않은 출력과 현재 시간을 고려하게 된다. 그러나 이 경우

double spending attack, coin age attack 등에 취약하기 때문에 QTUM은 최신 QTUM 코어에 PoS 3.0[10]을 채택하여 age를 제거하였다.

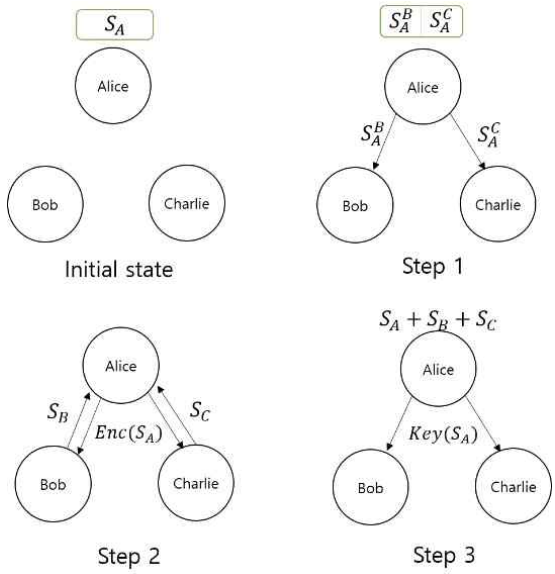
$$ProofHash < coins \times target$$

QTUM에서 블록 생성 권한은 지분 소유자가 보유한 코인의 양에 따라 결정된다. 지분 소유자들은 고정된 입력에 대해 그들이 제어하는 UTXO마다 하나의 해시를 수행하여 결과가 가중된 임계값 이하인지 여부를 확인한다. 해시되는 UTXO가 보유한 양이 많을수록 임계값에 가중치가 적용되므로 UTXO가 보유한 양이 많으면 더 높은 확률로 승리 할 수 있다. 조건을 충족시키는 해시가 생성되면 사용자는 블록을 전파한다. 그렇지 않다면 해시를 중지하고 다음 번 재생까지 기다린다.

16초마다 고정 입력 값이 변경되므로 지분 보유자들은 UTXO에 대한 새로운 해시 값을 생성하고 승자인지 확인할 수 있는 기회가 생긴다. 이것은 매 16초마다 추첨을 하는 것과 유사하다. UTXO에 의해 계산된 해시는 가중치가 있는 티켓을 나타낸다. 이 때 티켓에 가중치를 부여하는 것은 높은 가치의 UTXO를 여러 개의 작은 값으로 나눈 사용자가 더 많은 티켓을 얻지만 우승 확률은 증가하지 않도록 하기 위함이다. 난이도는 당첨된 티켓이 평균적으로 128초당 한 번만 발견되도록 설정된다.

ADA ADA는 DPoS 합의 알고리즘을 채택하였다. Ouroboros[3]를 이용하여 블록을 생성한다.

- Ouroboros: Ouroboros는 기존 PoS 합의 알고리즘의 문제를 해결하도록 설계되었다. 특히 Stake-Grinding Attack에 대응하는 것이 주요 목표이다. 현재 대부분의 PoS 프로토콜은 마지막 블록의 정보를 기반으로 무작위 변수를 계산한다. 그러나 마지막 블록 작성자는 사용자에게 유리한 랜덤 변수를 얻을 때까지 의도적으로 전송 세부 정보를 삭제하거나 포함할 수 있다. 따라서 Ouroboros는 Coin Tossing Protocol을 통해 위 문제를 해결하였다. Coin Tossing Protocol의 진행 과정은 [그림 2]와 같다.



[그림 2] Coin Tossing Protocol의 단계

[초기 상태] Alice, Bob 및 Charlie가 각각 랜덤 변수를 만든다.

[단계 1] 참가자들은 참가자 수만큼 랜덤 변수를 잘라서 모두에게 보낸다.

[단계 2] 각 랜덤 변수를 암호화하여 다른 참가자에게 보내면 받는 사람은 원래 랜덤 변수를 반환한다.

[단계 3] 다른 참가자의 랜덤 변수를 수신하자마자 수신자는 암호화 된 변수를 해독하기 위한 키를 보낸다. 키를 받은 참가자가 받은 키를 통해 암호를 해독하면 모든 사람이 랜덤 변수를 공유하게 된다.

위의 프로토콜을 사용하면 무작위로 분산된 변수 조각을 수집하고 복원할 수 있기 때문에 랜덤 변수를 안전하게 생성할 수 있다. 기존의 PoS 합의 알고리즘은 블록체인 참가자의 정보를 알 수 있는 경우에만 참여할 수 있는 보안상의 단점이 있었다. Ouroboros Genesis 프로토콜은 이를 해결하여 PoW와 유사한 수준의 보안을 제공할 것으로 예상되고 있다.

EOS EOS는 DPoS 합의 알고리즘을 사용한다. EOS는 지속적인 승인 투표 시스템을 통해 대표자라고 불리는 블록 생산자를 선택한다. 누구나 블록 생산에 참여할 수 있으며 일정 수준

의 토큰을 얻을 경우 대표자가 될 수 있다. EOS는 블록을 생성하고 네트워크에 영향력을 행사하는 21명의 대표단을 임명한다.

126라운드 동안 블록들이 생성된다. 21명의 대표는 6개의 블록을 각각 생성한다. 각 라운드가 시작할 때 토큰 소지자가 투표한 결과에 따라 21명의 고유한 대표자가 선정된다. 대표자는 15명 이상의 대표자가 합의한 순서대로 계획을 수행한다. 블록은 정확히 0.5초마다 생성되며 어느 시점이든 정확히 한 명의 대표자만 블록을 생성 할 권한이 있다. 블록이 예정된 시간에 생성되지 않으면, 그 시간 슬롯에 대한 블록은 생략된다. 하나 이상의 블록을 건너 뛸 때 블록 체인에 0.5 초 이상의 간격이 존재한다.

대표자가 블록을 놓치고 24시간 내에 블록을 생성하지 않을 경우 블록 생성을 다시 시작할 의사가 있음을 알릴 때까지 대표자 목록에서 제거된다. 이를 통해 누락되는 블록을 최소화하여 네트워크를 원활하게 작동시킬 수 있다.

EOS는 대표자들이 정상적인 조건 하에서 블록을 생산하기 위해 협력하기 때문에 어떤 포크도 일어나지 않는다. 포크가 발생하면 합의는 자동으로 가장 긴 체인으로 전환된다. 이 방법은 블록이 블록체인 포크에 추가되는 비율이 동일한 합의를 공유하는 대표자의 비율과 직접적으로 연관되기 때문에 가능하다.

이에 더해 대표자는 동시에 2개의 포크에 블록을 생산할 수 없다. 대표자는 이중지불을 하면 지위가 박탈된다. 이중지불에 대한 암호학적 증거는 악용하는 사람을 자동으로 제거하는 데 사용할 수 있다.

LISK LISK 또한 DPoS를 사용한다. 블록을 생성하는 대표자 N명(현재 N=101)은 모든 참여자에 의해 선출된다. 모든 참여자는 대표자가 될 수 있지만 필요한 지분을 보유한 참여자만 블록을 생성 할 수 있다. 각 참여자는 최대 101명까지 투표 할 수 있으며 표의 영향력은 참여자가 소유하는 토큰 양에 따라 달라진다.

시스템 내에서 한 라운드는 대표자 수와 동일한 N블록으로 구성된다. 각 라운드의 시작 부분에서 각 대표는 블록 생성 프로세스에서 그들의 위치를 나타내는 슬롯에 지정되어 있다. 각 대표는 한 라운드 동안 정확히 하나의 블록을 생성한다. 블록은 10초마다 생성된다. 각 블록에는 25개의 거래 내역이 포함된다. 각 블록은 서명 된 후 대표자에 의해 네트워크로 전파된다. 블록이 네트워크에 도달하면 다음 대표자가 할당된 슬롯에서 블록을 생성한다. 선출 된 대표자가 라운드 도중 블록을 생산할 수 없다면, 다른 대표자가 블록을 대신 생성한다.

블록 생성을 위해서 51%의 동료가 broadhash 합의를 유지해야한다. 포크를 막기 위해서 broadhash 합의가 필요하다. Broadhash는 데이터베이스에 있는 지난 5개 블록에 집계된 롤링 해시로 설정된다. 동일한 블록을 가진 모든 노드는 시스템 헤더를 통해 동일한 정보를 생성하고 해당 정보를 전파한다. 이를 통해 유효한 노드 중 대다수가 블록을 생산하는 것에 동의하게 된다.

IV. 각 코인의 블록 구조 및 거래 방식 분석

QTUM

- 블록구조: 비트코인의 UTXO 모델을 기반으로 하기 때문에 비트코인 블록구조[그림 3]와 유사하다.

version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c817010000000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833
transaction count	63
coinbase transaction	
transaction	
...	

[그림 3] 비트코인의 블록 구조

- 거래 방식: 거래의 전체적인 흐름은 비트코인과 유사하다고 볼 수 있다. 그러나 OP_EXEC, OP_EXEC_ASSIGN, OP_TXHASH 3가지의 명령어의 추가로 차이가 발생한다. 3가지의 명령어는 비트코인의 명령어와 이더리움의 명령어를 이어주는 매개체로 볼 수 있는데 AAL과 연관이 있다. 채굴 과정에서 거래를 추가할 때 EXEC의 유무에 따라 절차가 달라진다. EXEC이 있으면 수수료를 계산하는 작업을 한 후 bytecode를 실행시켜 특정 프로세스를 실행한다. 이후 블록을 생성하고 연결하는 작업에서 같은 EXEC의 bytecode를 실행하고 생성된 거래를 queue에 추가한다. 그리고 TXHASH 명령어를 통해 검증 작업을 거친다. 거래가 유효하다면 블록을 승인한다.

ADA

- 블록구조: 메인 블록과 제네시스 블록으로 나뉜다. 각 블록은 헤더와 바디로 구분된다. 헤더에는 4가지의 항목이 있다. 이전 블록의 서명, 바디의 증명, 합의 알고리즘에 필요한 데이터와 그 외 데이터로 나뉜다. 바디 부분에는 총 4가지의 페이로드가 있는데, transaction, SSC(Shared Seed Computation), delegation와 update가 있다. 제네시스 블록에는 3가지의 정보가 더 존재한다. 현재 epoch의 index와 slot leader의 리스트, 체인을 연결하기 위한 난이도이다.

- 거래 방식: 거래 내역은 자금 전송 시점에 생성된다. 거래의 전체적인 흐름은 다음과 같다. (1) 거래를 만들고 개인 비밀키로 서명한다. (2) 자신의 주변에 거래를 전송한다. (3) Slot leader가 검증한 이후 로컬 데이터에 저장한다.

거래는 간단히 input과 output data로 나뉜다. Input은 현재 거래의 ID와 대응되는 output의 index 정보와 금액을 갖고 있다. Output은 받는 노드의 주소와 금액 정보를 갖고 있다. 돈을 전송할 때 거래에 있던 output이 다른 거래의 input으로 들어간다. 이때 UTXO(Unspent Transaction Output)라는 개념이 필요하다. A의 주소로 향하는 거래가 B의 주소로 간다고 가정하면, A의 주소를 가리키던 output이 거래의 input으로 들어가고 B의 주소를 가리키는 output이 된다. 이후 slot leader가 검증하면 거래가 성립된다.

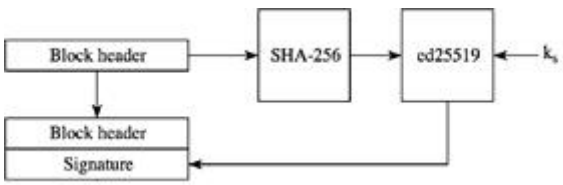
EOS

- 블록구조: EOS의 거래 방식은 Steem, BitShare와 유사하다. 따라서 EOS의 블록구조는 BitShare의 블록구조와 유사할 것으로 추정된다. BitShare의 블록은 헤더와 바디로 구성된다. 헤더 부분에는 이전 블록 ID, 블록 번호, 타임스탬프, transaction 요약, 다음 비밀 해쉬, 이전 비밀이 포함된다. 바디에는 블록 ID, 공개키, 헤더 서명, 블록 크기, 서명된 거래들이 포함된다. 데이터와 코드가 분리되어있어 계약에서 병목 현상을 해결할 수 있는 것이 특징이다.

- 거래 방식: 거래 방식은 총 3가지 필드로 구성된다. 범위(Scope), 메시지(Message), 스케쥴링이다. Scope는 읽히거나 쓰여질 데이터의 범위를 구체화한다. 만약 메시지가 범위 밖에 있는 데이터를 읽거나 쓰려고 시도하면 거래는 실패한다. Message는 코드, 타입, 수신자, 권한, 데이터 정보를 포함한다. EOS에서는 권한이 명시적으로 정의되므로 필요한 서명 전부를 자동으로 확인한다. 스케쥴링은 블록을 병렬적으로 실행할 수 있는 기회를 제공한다.

LISK

- 블록구조: LISK의 블록 헤더는 블록 버전, 타임스탬프, 이전 블록 ID, 거래량, 전송된 총 LISK 양, 총 수수료 금액, 대표자에 대한 보상, 페이로드 길이, 페이로드 해시값, 대표자의 공개키로 구성된다. 블록 헤더는 서명이 필요하다. 서명 과정은 [그림 4]와 같다. 블록 헤더의 SHA-256 해시를 생성하고 대표자의 키 암호를 사용하여 서명한다.



[그림 4] 블록헤더의 서명 과정

- 거래 방식: LISK에서 주로 사용되는 거래 유형은 총 5가지가 있다. 지정된 LISK 주소로 자금 전송, 두 번째 암호 등록, 대표자 등록, 대표자를 위한 투표 등록, 다중 서명 등록 유형이다. 유형에 관계없이 모든 거래는 네트워크에서 승인되기 전에 발신자가 서명해야한다. 거래에 서명하는 과정은 모든 거래에서 동일하며 블록 헤더의 서명 과정과도 동일하다. 단 데이터 블록에 포함 된 추가 정보는 거래 유형에 따라 다르다.

모든 거래는 3가지 단계로 구성된다. (1) 거래에 필요한 필드 지정 후 거래 객체를 작성한다. (2) 객체에 서명한다. (3) 거래 수수료를 계산한다.

자금을 전송하는 유형의 경우에는 대표자가 해당 거래를 처리하는 과정이 추가된다.

V. 결론

본 논문에서는 PoS방식과 DPoS방식에 대하여 설명하고, (D)PoS를 합의 프로토콜로 채택한 대표적인 블록체인 어플리케이션인 QTUM, ADA, EOS, LISK의 합의 알고리즘을 분석하였다. 세부적으로 각 코인을 블록 구조 및 거래 방식의 관점에서 분석했다. 이를 통해 (D)PoS 방식이 가질 수 있는 한계를 발견하고 개선 방안을 탐구할 수 있다. 향후 연구로 (D)PoS의 단점을 개선한 합의 알고리즘을 제안할 수 있을 것이다.

한편 블록체인의 신뢰성 검토에 본 논문을 활용할 수 있다. 블록체인의 합의 알고리즘은 이중지불을 방지하므로 블록체인의 신뢰도와 직결되어있다. 따라서 블록체인에 한층 더 높은 신뢰성을 제공하기 위한 연구에 활용할 수 있다.

[참고문헌]

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system” 2008.

[2] P. Dai, N. Mahi, J. Earls, A. Norta, “Smart-Contract Value-Transfer Protocols on a Distributed Mobile Application Platform”

[3] Kiayias, Aggelos, et al. "Ouroboros: A provably secure proof-of-stake blockchain protocol" Annual International Cryptology Conference. Springer, Cham, 2017.

[4] Larimer, Daniel. "Delegated proof-of-stake (dpos)" Bitshare whitepaper, 2014.

[5] King, Sunny, and Scott Nadal. "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake" self-published paper, 2012.

[6] https://github.com/ethereum/wiki/wiki/White-Paper

[7] https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md

[8] https://lisk.io/documentation

[9] https://qtum.org/en/

[10] https://blackcoin.co/

[11] https://whycardano.com/

IoT 환경의 확장성을 위한 블록체인을 이용한 키 교환 프로토콜

이정호, 최형기*
성균관대학교

Key Exchange Protocol Using Blockchain for Scalable IoT Environment

Jeongho Lee, Hyoung-Kee Choi
Sungkyunkwan University

요 약

블록체인이 쟁점이 됨에 따라 블록체인을 이용한 다양한 플랫폼에 대한 개발 및 연구에 대한 진행이 급속도로 이루어지고 있다. IoT 역시 블록체인을 응용하는 분야로 떠오르고 있다. 본 논문에서는 블록체인을 이용하여 IoT의 보안 문제 중 하나인 확장성을 해결하기 위한 새로운 프로토콜을 제시하고 제시하는 프로토콜의 장점과 한계점에 대해 논의한다.

I. 서론

최근 블록체인이 많은 쟁점이 됨에 따라 블록체인을 이용한 기술 구현 혹은 플랫폼 개발은 국외는 물론 국내에서도 활발히 진행되는 연구 중 하나이다[1]. 블록체인의 적용 대상이 되는 분야 중 Internet of things(IoT)는 블록체인이 가지는 확장성과 보안성을 이유로 그 가치를 높이고 있다. 블록체인 관련 기업과 포춘 선정 500대 기업이 참여하여 2016년 12월 IoT 블록체인 컨소시엄이 결성되는 등 블록체인 기반 사물인터넷의 중요성은 더욱 주목받고 있으며 블록체인 기반 사물인터넷 프로토콜 개발과 연구를 위한 협업이 꾸준히 진행되고 있다[2].

IoT 센서들이 더 저렴하고 가볍게 발전함에 따라 다양한 적용 사례와 함께 관련 산업의 발전을 이끌고 있다. 이러한 IoT 기기들은 사용자에 밀접한 정보들을 주고받기 때문에 이에 대한 보안은 IoT 환경에서 주요한 고려사항 중 하나이다. 새로운 기기의 추가나 기존 기기의 이동이 잦은 IoT의 특성에 의해 확장성은 IoT 보안을 고려하는 중요한 요소 중 하나로 여겨진다.

본 논문에서는 블록체인을 이용하여 IoT 환경에서 확장성을 보장할 수 있는 새로운 프로토콜을 제시하려 한다. 또 본 프로토콜이 어떻게 확장성을 이룰 수 있는지에 대해 설명하고 장점과 한계점에 대해 논의하고자 한다.

* 교신저자(Corresponding author)

II. 관련 연구

2.1 블록체인

블록체인은 시스템은 분산형 데이터베이스 플랫폼으로 비트코인과 같은 암호화폐에 대표적으로 사용된다. 블록 간 관계가 해시에

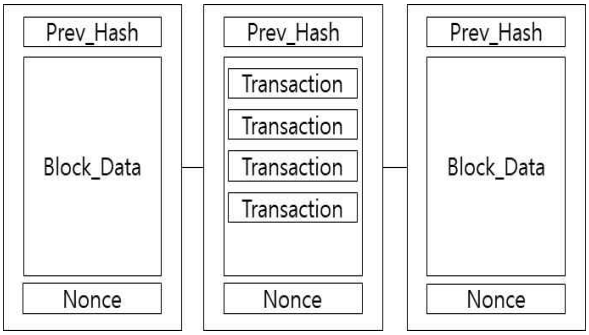


그림 1. 블록체인 구조

의해 묶여 있으며 이를 통해 무결성과 신뢰성을 제공한다. 사토시 나카모토가 쓴 비트코인 백서에는 이러한 블록체인의 기본 개념에 대해 상세히 기술되어 있다[3]. 본 논문에서는 프로토콜에서 제안하는 블록체인 기반 키 교환 방식에 대한 설명을 위해, 비트코인 백서 내용을 기반으로 블록체인 구조에 대해 상세히 설명하려 한다.

2.2.1 블록체인 구조

블록체인은 트랜잭션으로 이루어진 블록들이 해시에 의해 체인처럼 묶여 있는 구조로써 공개키 서명과 합의 알고리즘에 의해 무결성이 보장된다. 그림 1은 블록체인의 구조를 그림으로 나타낸 것이다. 블록은 크게 이전 블록의 해시와 블록이 가지는 트랜잭션 데이터 그리고 특정 조건을 만족하는 넌스(nonce) 값으로 이루어져 있다.

그림에서 볼 수 있듯이 블록체인의 블록은 이전 블록의 해시를 가지고 있으므로 한번 체인에 올라간 블록에 대한 변조가 불가능하다는 특징을 가진다. 그 이유는 데이터에 대한 변조를 시도하는 경우 해시값이 달라지고 체인에 대한 검증을 통해 이를 알 수 있기 때문이다. 또한, 사용자들은 블록체인에 있는 전체 트랜잭션에 대한 검증을 통해 블록체인을 통해 일어난 거래 전반에 대해 신뢰할 수 있게 된다.

2.2.2 블록 합의

블록이 블록체인에 올라가기 위해서는 블록 합의하는 과정을 거쳐야 한다. 블록체인은 크게 퍼블릭 블록체인과 프라이빗 블록체인으로 나뉘고 이에 따라 합의 방식도 변하게 된다. 퍼블릭 블록체인의 경우 네트워크에 어떠한 참여자라도 블록을 만들 수 있고 이에 대한 합의를 proof of work(PoW) 혹은 proof of steak(PoS)라는 방식을 통해 합의 한다. 이 중 PoW 방식은 비트코인에 사용되는 방식으로 사용자는 해당 블록의 해시 값을 현재 네트워크의 난이도에 맞게 출력해주는 넌스 값을 찾는 것으로 블록에 대한 증명을 수행한다.

2.2.3 블록 전파

합의가 완료된 블록은 다른 블록체인 노드들에 전파되어 메인 체인에 올라가게 된다. 노드들은 가장 먼저 도착한 블록을 자신이 가지고 있는 메인 체인 뒤에 이어 붙이며 이를 수행하기 전 보내온 블록에 대한 서명 검사와 트랜잭션 검사를 우선으로 수행한다.

2.2 기존에 제안된 키 교환 방식

2.2.1 사전에 공유된 키를 이용한 인증

키 교환을 위해 가장 쉽게 생각할 수 있는 방법으로 사전에 공유된 대칭 키를 이용해서 키를 주고받는 방식이 있다. 네트워크 참여자는 네트워크 관리자 혹은 신뢰할 수 있는 서드파티와 키를 미리 공유하고 있으며 대칭 키를 공유하고 있는 주체를 이용하여 통신하고자 하는 네트워크 참여자와 세션 키를 교환하는 방식이다.

하지만 사전에 키를 공유하는 방식은 다음과 같은 문제에 의해 확장성을 떨어뜨릴 수 있다. 하나는 네트워크 참여자가 신뢰할 수 있는 관리자 혹은 서드파티를 사전에 합의해야 한다는 점이고 다른 하나는 네트워크 참여 시에 이러한 신뢰 주체에 의해 인증을 받아야 한다는 점이다.

2.2.2 Public key infrastructure(PKI) 기반 인증

PKI를 기반으로 한 인증은 네트워크 참여자 간에 키를 공유하는 것이 아닌 인증서를 주고받아 통신을 수행한다. 인증서를 통해

통신하고자 하는 네트워크 참여자의 공개키를 알 수 있고 이를 통해 세션 키를 암호화하여 전달하는 방식이다[4].

PKI를 기반으로 한 인증 역시 사전에 공유된 키를 이용한 인증과 마찬가지로 PKI 사용을 위한 신뢰 관계를 미리 구축해야 한다는 한계가 존재한다. 많은 수에 기기가 존재하는 IoT 환경에서 이에 대한 인증서를 발급 및 관리하는 데 문제가 존재한다.

III. 프로토콜 제안

이 절에서는 IoT 환경을 위해 게이트웨이 노드 간 블록체인을 도입한 새로운 프로토콜에 대해 제안한다.

3.1 네트워크 환경

제안하는 프로토콜에서 가정하는 네트워크 환경은 네트워크 참여자를 센서와 게이트웨이 노드 사용자 세 분류로 나눈다. 센서는 IoT 기기를 의미하면 게이트웨이 노드는 충분한 계산능력을 갖추고 있으며, 센서들을 관리하는 홈 라우터와 같은 기기를 의미한다. 사용자의 경우 센서들로부터 정보를 얻어오려 하는 네트워크 참여자이다. 제안하는 프로토콜에서 게이트웨이 노드들은 블록체인을 통해 센서의 정보를 공유한다.

3.2 블록체인을 통한 세션 키 교환

3.2.1 게이트웨이 노드 등록과정

게이트웨이 노드가 최초 네트워크 참여시 자신의 정보를 다른 게이트웨이 노드에 알리는 것으로 참여를 시작한다. 게이트웨이 노드는 다른 게이트웨이 노드들에 자신의 주소와 공개키 그리고 자신의 주소를 개인 키로 서명한 서명 값을 전달한다. 이를 전달받은 게이트웨이 노드들은 자신들의 게이트웨이 노드 목록을 보고 중복된 주소가 있는 경우, 해당 요청을 폐기한다. 중복된 주소가 없는 경우, 새로이 해당 게이트웨이 노드를 목록에 추가하는 것으로 작업을 마친다.

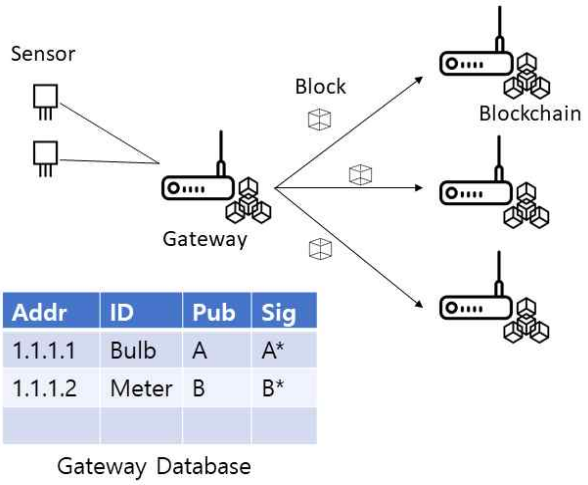


그림 2. 제안하는 프로토콜 구조

3.2.2 센서 등록과정

그림 2는 제안하는 프로토콜의 전체 개요를 나타내고 있다. 센서는 게이트웨이와의 안전한 통신을 위해 게이트웨이와의 최초 통신 시 센서는 개인 키 공개키 쌍을 생성한 후 공개키 값, 센서에 대한 설명, 이에 대한 서명 값을 게이트웨이 노드에 전달한다. 게이트웨이 노드는 센서의 주소와 전달받은 값들을 매핑하여 가진다. 센서 등록 시 센서로부터 전달받은 값을 게이트웨이 주소와 함께 네트워크 내 다른 게이트웨이 노드들에 트랜잭션 형태로 전달한다.

트랜잭션을 전달받는 게이트웨이는 자신이 등록해놓은 게이트웨이 노드 목록으로부터 주소와 공개키를 검색하여 해당 서명에 대한 검증을 수행한다. 목록에 없는 경우 트랜잭션을 폐기하며 게이트웨이가 등록과정을 선행해야 함을 메시지로 전달한다.

전달된 트랜잭션들은 게이트웨이 노드들에 의해 블록으로 만들어지며 검증을 통해 주 체인에 올라가게 된다. 블록에 대한 검증은 서명에 대한 검증과 이미 체인에 존재하는 센서 인지에 대한 검증으로 나누어 진행된다. 두 경우 모두 위배되는 경우 트랜잭션은 폐기되며 위배되는 트랜잭션을 보낸 게이트웨이 노드에 대해서는 전달 받은 횟수에 따라 요청을 일정 시간 동안 받지 않는다. 그림 2는

위에 과정을 통해 생성된 블록체인을 그림으로 나타내고 있다.

3.2.3 사용자와 센서의 키 교환

사용자는 센서 노드로부터 정보를 전달받기를 원하며 안전한 통신을 위한 세션 키 설립을 원한다. 이를 위해 사용자는 블록체인을 직접 찾아보거나 혹은 게이트웨이 노드에 찾을 것을 요청하여 정보를 전달받길 원하는 센서가 속해 있는 게이트웨이 노드의 주소와 센서의 공개키를 알 수 있다. 사용자는 새로운 대칭 키를 생성한 후 이 키와 자신의 주소를 센서의 공개키로 암호화하여 해당 센서의 서명 값과 함께 게이트웨이 노드 주소로 전달한다. 암호화된 키를 전달받은 게이트웨이 노드는 서명 값에 매핑되는 센서로 전달한다. 센서는 이를 자신의 개인 키로 복호화하여 전달받은 키와 주소를 가지고 사용자와 통신할 수 있다.

3.3 제안하는 프로토콜의 장점

제안하는 프로토콜은 게이트웨이 간 블록체인을 통해 키 교환을 이루기 때문에 게이트웨이 간 신뢰 관계를 미리 구축할 필요 없다는 장점이다. 이는 각기 다른 제조사들이 구성하는 실제 IoT 환경에서 알 수 없는 게이트웨이로부터의 연결을 받을 수 있다는 점에서 확장성을 크게 높일 수 있다. 또한, 센서 역시 네트워크 참여 시에 게이트웨이에 인증받으므로 전체 네트워크에 참여할 수 있다는 장점이 있다.

3.4 제안하는 프로토콜의 한계점

제안하는 프로토콜은 블록체인 합의 알고리즘 중 PoW 방식을 사용하여 게이트웨이 노드에 상당한 부하를 가져올 수 있다. 또한, 센서의 성능이 아주 낮은 경우 공개키를 이용한 연산이 부담될 수 있다. 이를 해결하기 위해서는 합의 알고리즘에 대한 개선과 공개키 방식보다 경량화된 암호 방식에 관한 향후 연구가 필요하다.

IV.결론

블록체인에 관한 관심이 커짐에 따라 이를 이용한 연구 역시 활발히 적용되고 있으며 IoT 역시 중요한 주제로 떠오르고 있다. 본 논문에서 IoT의 보안 문제 중 확장성을 해결할 수 있는 새로운 프로토콜에 대해 제안하였으며 이에 대한 장점과 한계점에 대해 다루어 보았다.

ACKNOWLEDGEMENT

이 논문은 2016 년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No.2016R1D1A1B03936211).

[참고문헌]

[1] 민경식, 한국인터넷진흥원, 블록체인 최신 기술 동향 Vol. 49, 3월, 2018.

[2] 보안기술연구팀, 금융보안원, 국내·외 블록체인 기반 사물인터넷 동향, 6월, 2017.

[3] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, October, 2008.

[4] Brian Knopf, Neustar Inc, Redesigning PKI to Solve Revocation Expiration and Rotation Problem, March, 2017.

비트코인 탈익명화 사례 분석*)

홍지형, 김윤정
서울여자대학교 정보보호학과

De-anonymity Case Analysis in Bitcoin

Jihyung Hong, Yoonjeong Kim
Department of Information Security, Seoul Women's University

요 약

중앙에 서버를 두고 거래가 이뤄지는 일반적인 금융거래패턴이 아닌, 공동 분산장부를 투명하게 공유하는 방식의 비트코인은 2008년에 제안된 전자 화폐이다. 비트코인의 특성 중 하나는, 익명성을 보장하는 화폐거래라는 점이다. 그러나, 비트코인 거래가 탈익명화가 가능할 것이라는 의견도 있어왔다. 본 논문에서는 비트코인 익명성 강화를 위해 제안된 기존연구를 정리하고, 비트코인 익명성을 탈익명화 관점에서 실제 조사한 예를 소개한다. 조사 및 분석 결과, 비트코인 주소 소유자가 언론에 공개된 전력이 있는 경우, 이 소유자의 거래 패턴이 탈익명 상태로 모두 공개됨을 확인할 수 있었다.

I. 서론

비트코인(Bitcoin)이란 2008년 사토시 나카모토(Satoshi Nakamoto)라는 익명의 프로그래머 혹은 집단에 의해 처음 제안된 피어 투 피어(peer-to-peer) 방식을 사용한 전자 화폐이다[1,2]. 비트코인 등장 이후, 디지털 시대의 새로운 화폐로써 큰 각광을 받았다. 모든 비트코인 거래(transaction)는 장부(ledger)에 공개되어 투명성을 유지하면서도, 동시에 비트코인 사용자들은 자신의 이름을 공개하지 않아도 거래가 가능한 익명성(anonimity)이라는 특징을 갖고 있다. 그러나 비트코인 거래소, 상점 등을 이용하려면 이용자의 신분을 추정할 수 있는 정보를 거래소에 알려야 한다. 비트코인은 이전의 모든 블록이 체인의 형태로 이어져 있어, 개인키를 소유한 사용자가 드러나게 되면 링크된 체인을 통해 동일한 소유자의 다른 거래가 노출될 수 있는 특성도 있다.

본 논문에서는, 우선 비트코인 및 비트코인 익명성에 관한 기존 연구를 정리한다. 다음으로, 실제 운영되는 비트코인에 대하여 탈익명화가 가능한지를 블록체인인포 사이트를 이용하여 실례를 통하여 분석한 결과를 소개한다. 분석 결과, 해당 사용자의 실제 이름이 언론에 공개된 적이 있는 경우 탈익명화가 가능함을 알 수 있었다.

II. 비트코인

비트코인은 두 명의 개체 사이에서 이루어지는 유형의 자금거래로, 제 3자의 신뢰성 있는 중앙기관의 역할을 비트코인 네트워크 안에 속한 노드들이 하면서 거래를 인증하는 방식이다. 기존 금융방식과 비교했을 때 비트코인은 비교

*) 본 연구는 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원(No. NRF-2016R1A2B4011984)과 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2018-2014-1-00636)

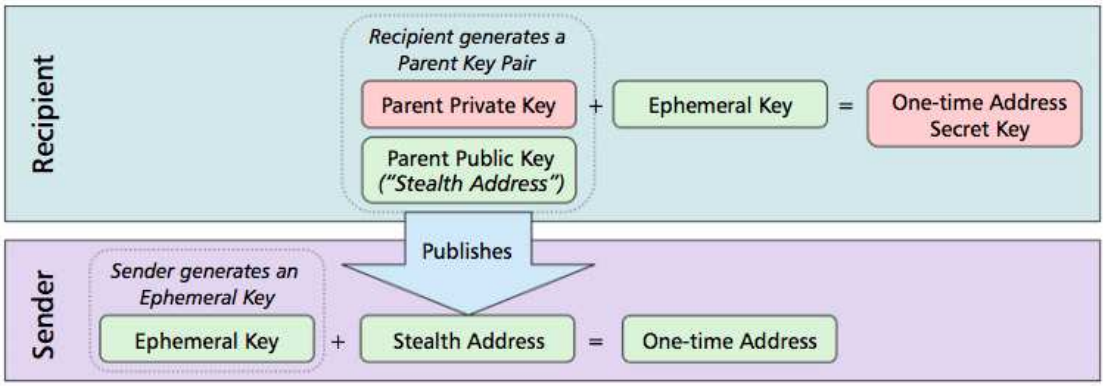


그림 1 . 스텔스 주소 [5]

적 규제 또는 감독이 적은 화폐로, 거래시각, 국가 등의 제약 없이 자유로운 거래가 가능하다는 점이 장점 중 하나로 꼽힌다. 비트코인은 사용자 사이에서 일어나는 모든 거래가 블록체인에 기록된다. 이후 채굴(마이닝, mining)을 통하여 비트코인 거래시스템을 유지하는 것이 핵심 메커니즘이며, 이것은 비트코인 화폐 공급 역할을 한다. 채굴에 참여하는 노드들을 마이너 혹은 채굴자라고 부르며, 평균적으로 10분마다 생성되는 블록을 채굴하기 위한 작업을 한다. 채굴에 성공하게 되면 이전 거래들이 다 포함되어 있는 블록체인에 새로 연결된다. 이러한 블록체인은 작업증명(Proof-of-work) 시스템과 피어 투 피어 네트워크를 통해 노드들에게 공유된다.

III. 비트코인 익명성 관련 기존연구

P2P 전자 화폐 시스템 비트코인의 익명성을 분석한 연구가 있어왔다 [3,4,5,6,7,8]. 비트코인 네트워크에 존재하는 사용자들은 임의의 암호화된 공개키와 비밀키 키 쌍이 저장된 지갑을 갖는다. 공개키는 비트코인 수신자의 주소로 쓰인다. 비밀키(개인키)는 송금 거래내역을 작성하고 거래내역에 서명을 할 때 사용한다. 비트코인 주소에는 소유자에 대한 개인정보가 포함되어 있지 않아 익명성을 보장한다. 비트코인 사용자는 공개키로 사용하는 주소를 새로 여러 개 생성할 수 있다. 이렇게 쉽게 주소를 생성해 수시로 바꿔서 사용한다면 익명성이 보장될 수 있다. 비트코인은 모든 거래내역이 블록체인으로 이어져 투명하게 공개되기 때문에 안전하게 익명성을 보장해야 한다. 익명성을 강화하기 위한 기법인 스텔스 주소, 믹스코인에 대해 살펴보면 다음과 같다.

3.1 스텔스 주소

비트코인 익명성 강화 관점에서는 주소의 재사용을 권장하지 않는다. 따라서 스텔스 주소를 비트코인 거래에 적용하는 방식이 제안되었다. 수신자는 부모 키 쌍을 생성하고, 공개키를 알리는데 이때 이 공개키를 스텔스 주소로 한다 [5]. 송신자는 이 스텔스 주소를 원타임 지불 주소를 생성하는데 활용한다. 오직 수신자만이 자신의 개인키를 가지고, 발신자의 원타임 지불 주소의 비밀키를 계산하는데 쓸 수 있다.

3.2 믹스코인

믹스코인(Mixcoin)은 2014년 Joseph Bonneau 등이 제안한 프로토콜로, 비트코인과 암호화폐에 있어서 익명 지불이 가능하도록 제안된 프로토콜이다 [6]. 믹스코인은 책임성 메커니즘을 추가하여 도난과 같은 일이 일어나면 그것을 노출시킨다. 이름에서 알 수 있듯 코인을 믹싱하고자 하는 사용자와 믹싱을 하는 사용자가 존재하여, 믹싱 전에 서명이 적힌 보증서를 받아 거래에 책임성을 부여한다.

믹스코인의 구현은 현재의 비트코인 거래 방식을 변경할 필요가 없으므로 일반 비트코인 사용자가 쉽게 이용할 수 있다는 장점이 있다.

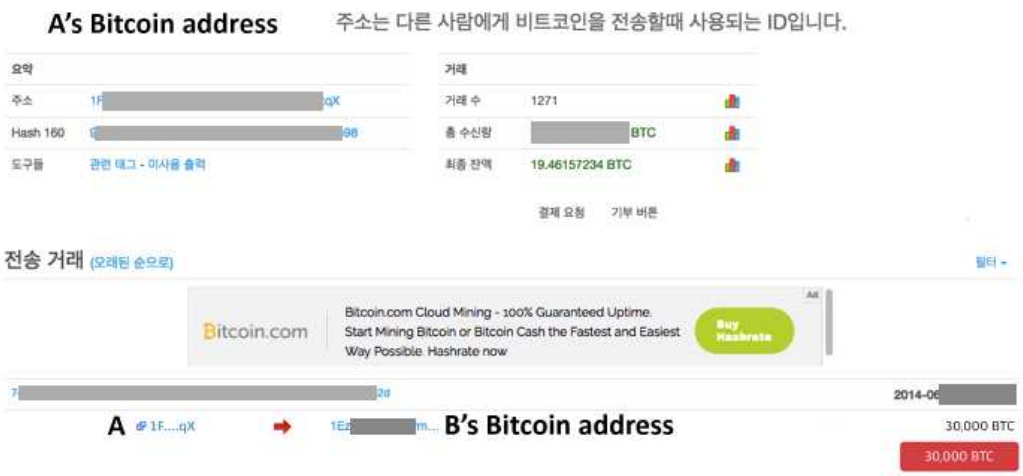


그림 2. 블록체인인포[9] 내 비트코인 주소 A 상세검색화면

IV. 비트코인 운영 사례 분석

본 논문에서는, 블록체인 탐색기 중 블록체인인포를 통하여 [9], 특정 블록을 선정하여 해당 주소에 연결된 거래들이 어떤 패턴을 이루고 있는지 직접 사례를 분석하였다.

그림 2는 블록체인 탐색기 중 하나인 블록체인인포에 특정 비트코인 주소 A를 검색했을 때 대면하게 되는 화면을 캡쳐한 것이다. 여기서, A는 실제 현실에 존재하는 주소를 말하며, 본 논문에서는 이 실제 주소를 A로 가명 처리하였다. 해당 비트코인 주소가 공개키로 사용됨을 알 수 있고 거래가 얼마나 일어났는지에 대한 거래 수, 총 수신한 비트코인 양인 BTC 정보, 현재 잔액, 관련 거래 등을 파악할 수 있다. 그림 2의 하단에 A의 주소에서 B의 비트코인 주소로 30,000 BTC이 송금되는 것을 확인할 수 있다. B의 비트코인 주소를 클릭하게 되면 해당 주소와 연결된 거래들을 추적할 수 있다. 분석을 위해 블록체인 탐색기를 활용하여 특정 주소와 연결되어 있는 거래를 분석하여 사용자의 정보를 추정해나가는 단계를 계속 수행하였다.

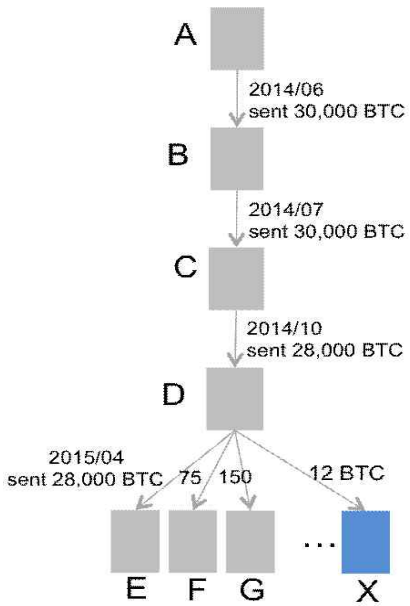


그림 3. 비트코인 거래들

그림 3은 비트코인 주소끼리 일어나는 거래에 대한 사례를 도식화하여 표현한 것이다. A부터 X는 비트코인 주소이다. X는 다수 개의 거래가 포함되어 있는 형태이다. 보통, 포함되는 거래의 수는 1개일 수도 있고 1000개가 될 수도 있다. A에서 B로 30,000 BTC이 송금되어 거래가 하나 발생하였다. B는 C의 주소로 28,000 BTC을 송금하여 B와 C 사이에 거래가 생성되었다. D의 한 거래에는 E에서 X까지 여러 비트코인 주소에 비트코인을 각기 다른 양으로 송금한다. 많게는 28,000 BTC부터 12 BTC 까지이다.

그림 4는 그림 3의 가명 주소 X에서 보여지는 송금패턴을 분석한 결과이다. 비트코인 주소 X에는 거래가 2개 존재하는데, D로부터 12 BTC을 받는 것 하나와 각기 다른 주소 8개로

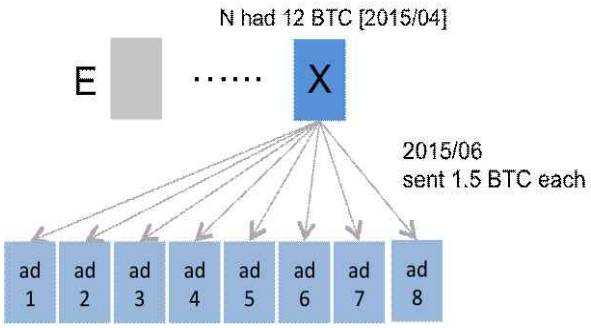


그림 4. 특정 비트코인 주소의 송금패턴

송금하는 거래 하나가 존재한다. 비트코인 주소 X의 경우 동일한 날짜와 시각에 1.5 BTC을 동일하게 8개의 각기 다른 주소로 송금하였다.

거래가 이루어진 2014년 6월 당시 1 BTC의 가치는 US $580로, 1.5 BTC이면 US $870이다. 8개의 주소에는 일정한 공통점을 가지고 있는데 첫째로 거래의 양이 400개에서 500개 사이라는 점, 둘째로 2015년 9월 중순의 거래가 마지막 거래이고 그 이후에는 사용하지 않았다는 점이다. 또한 현재 잔액은 모두 0 BTC로 모든 금액을 소진한 상태였다.

V. 비트코인 탈익명화 분석

4.1 주소 소유 기관 공개에 따른 탈익명화

4 장에서 분석한 사례에서, 공개주소 A를 소유한 기관의 이름이 공공연히 언론에 드러난 바 있다. 따라서 분석한 공개주소의 소유주가 수행한 거래 내역을 충분히 파악할 수 있었다. 또한 거래 추적 중의 마지막 8개 주소는 동일한 값의 비트코인을 받고난 후 일정 기한 이후에는 아무런 거래가 일어나지 않았다. 즉, 해당 주소는 특정 목적을 위해 사용된 이후 버려진 주소임을 추측할 수 있다.

4.2 거래소 신분확인을 통한 탈익명화

한편, 거래소의 경우 사용자의 회원가입시 사용자 신원이 파악된다. 따라서, 비트코인 거래 중 거래소를 이용하는 거래가 포함된 경우에도 소유자의 탈익명화가 가능하다.

VI. 결론

본 논문에서는 비트코인의 익명성에 대한 기존 연구와 비트코인 운영사례의 실제 분석을 통하여 비트코인의 탈익명화 가능성을 실증하였다. 비트코인 운영사례의 분석에는 블록체인 탐색기 중 블록체인인포를 활용하였다.

분석 결과, 비트코인 공개주소의 소유주가 언론에 드러난 바 있는 경우 이를 이용하여 이 소유주의 거래 흐름을 파악하는 탈익명화가 가능함을 알 수 있었다. 또한, 거래소 등 신원 확인을 필요로 하는 중개소를 거치는 경우에도 탈익명화가 가능하다.

[참고문헌]

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

[2] Tobias Bamert, Christian Decker, Lennart Elsen, Roger Wattenhofer and Samuel Welten, “Have a Snack, Pay with Bitcoins,” 13-th IEEE International Conference on Peer-to-Peer Computing, 2013.

[3] 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.

[4] 김승민, 이지혜, 김윤정, “비트코인 익명성 분석 및 전망”, 정보기술논문지, 15(1), 2017.

[5] Danny Yang, Jack Gavigan and Zooko Wilcox-O’Hearn, Survey of Confidentiality and Privacy Preserving Technologies for Blockchains, 2016.

[6] 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.

[7] 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.

[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] 블록체인 인포(Blockchain info), https://blockchain.info/, 2018년 5월에 확인.

2018 한국정보보호학회 하계학술대회

C3 관리정책교육 3

김 인 석 (고려대학교)

- **정보통신망 이용촉진 및 정보보호 등에 관한 법률 제49조 “비밀” 의 분류 및 정의**
  윤우석, 박재용, 서정택
- **내부 정보 유출 경로별 통합 시나리오 점검 방법 연구**
  권현우, 이익준, 염홍열
- **블록체인 기술 적용과 개인정보 삭제 및 제3자 제공의 법적 문제에 관한 연구**
  최용혁
- **공공의 이익을 위한 의료 빅데이터의 활용관련 법률 분석 및 의료법 개정(안)제시**
  한종찬, 박지환, 서정택

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제49조 “비밀”의 분류 및 정의

윤우석, 박재용, 서정택

순천향대학교 정보보호학과

Classification and definition of “Secret” in Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.

Woo seok Yun, Jae Yong Park, Jung Taek Seo

Department of Information Security Engineering, Soonchunhyang University.

요 약

최근 판례 2017도4240에서 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 “정보통신망법”) 제49조의 타인의 비밀은 “일반적으로 알려져 있지 않은 사실을 다른 사람에게 알리지 않는 것이 본인에게 이익인 경우를 말한다.”라고 판결하였다. 특히 기업 내부 정보는 비밀에 해당하지 않아 무죄를 선고받았다. 하지만 판례2005도7309 에서는 비밀이란 개인정보만 포함하는 것이 아닌 기업·국가·공공 영역에서의 개인정보 및 일반적으로 알려지지 않은 정보 또한 포함해야 한다고 판결하였다. 두 판례의 사례로 미루어봤을 때 동 법 제49조에서 규정하고 있는 비밀에 대한 명확한 정의와 범위가 명시되어 있지 않아 판례마다 해석의 상충되는 부분이 발생한다. 이에 따라 본 논문에서는 해결방안으로 정보통신망법 제49조의 “비밀”에 대한 분류 및 정의를 제시한다.

I. 서론

정보통신망법 제49조는 “누구든지 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하여서는 아니 된다.” 라고 규정되어 있다[1]. 하지만 가장 중요한 “비밀”에 대한 분류 및 정의가 명확하지 않아 판례2005도 7309와 판례 2017도4240 등 상충되는 부분이 많고, 개인정보보호법, 위치정보의 보호 및 이용 등에 관한 법률과 중복되는 부분 또한 많아 판례마다 견해 차이가 있다. 위와 같이 “비밀”이 정확히 규정되어있지 않기 때문에 확실한 정립이 필요하다. 이는 발전하는 정보통신기술로 인하여 그림 1과 같이 인터넷 사용자가 증가함에 따른 개인·국가·기업 등의 정보통신망 인프라 구축에도 필요한 사항이다[2]. 본 논문에서는 정보통신망법 제49조의 “비밀”과 동 법에 상충되는 판례를 설명하고, 문제해결을 위한 “비밀”에 대한 범위를 국가, 공공, 기업, 개인 정보로 넓혀 분류 및 정의를 하고 결론 및 향후 연구 방안을 제시한다.

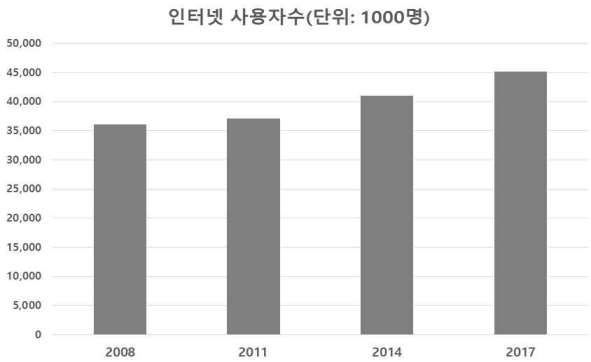


그림 1. 국내 인터넷 사용자수 추이

II. 정보통신망법 제49조의 “비밀”

정보통신망법 제49조는 정보를 다운받아 탈취하는 행위인 ‘침해’와 타인의 비밀로 인터넷 사이트에 로그인하는 행위 등을 ‘도용’, 불법으로 탈취한 정보를 제3자에게 판매한 행위를 ‘누설’이라 칭하고 있다. 하지만 타인의 비밀에 대

한 범위가 정의되어있지 않다. 정보통신망법에서는 “비밀”을 개인정보에 한하여 표 1과 같이 분류하였다.

비밀 정보	유형 구분	
개인 정보	인적 사항	
	신체적 정보	신체 정보
		의료, 건강정보
	정신적 정보	기호, 성향정보
		내면의 비밀 등
	재산적 정보	개인금융정보
		신용정보
	사회적 정보	교육정보
		법적정보
		근로정보
		병역정보
	기타	

표 1. 정보통신망법의 개인정보에 대한 항목

현행 법제의 개인정보 관련 정의 규정에서의 개인정보는 살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보와 쉽게 결합되어 개인정보가 될 수 있는 정보까지 포함한 정보를 말한다. 표 1에서의 기타 항목은 전화통화내역, 웹사이트 접속 내역, GPS 등에 의한 위치정보 등은 위에서 말한 바와 같기에 개인정보로서 인정된다.

Ⅲ. 동 법에 상충되는 판례

대법원은 표 2에서의 판례에 비추어 기업 정보는 비밀에 해당하지 않아 범죄 성립이 어렵다고 판결한 바 있다[5]. 하지만 표 3과 같은 판

<대법원 2017.6.19. 선고 2017도4240> 판결 정보통신망법 제49조에 규정된 '정보통신망에 의하여 처리,보관 또는 전송되는 타인의 비밀 누설'이란 타인의 비밀에 관한 일체의 누설 행위를 의미하는 것이 아니라, 정보통신망에 의하여 처리,보관 또는 전송되는 타인의 비밀을 정보통신망에 침입하는 등의 부정한 수단 또는 방법으로 취득한 사람이나, 그 비밀이 위와 같은 방법으로 취득된 것임을 알고있는 사람이 그 비밀을 아직 알지 못하는 타인에게 일를 알려주는 행위만을 의미하는 것으로 제한하여 해석함이 타당하다.

표 2. 대법원 2017.6.19. 선고 2017도4240 판결

례에서는 “정보통신망 이용촉진 및 정보보호 등에 관한 법률 제49조에서 말하는 타인의 비밀이란 일반적으로 알려져 있지 않은 사실로서 이를 다른 사람에게 알리지 않는 것이 본인에게 이익이 있는 것을 의미한다.” 라고 판결하여 일반적으로 알려져 있지 않은 기업 내부 정보에 대한 의미에 대한 견해 차이가 존재한다[6].

<대법원 2006.3.24. 선고 2005도7309> 판결 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제49조에서 말하는 타인의 비밀이란 일반적으로 알려져 있지 않는 사실로서 이를 다른 사람에게 알리지 않는 것이 본인에게 이익이 있는 것을 말한다.

표 3. 대법원 2006.3.24. 선고 2005도7309 판결

위와 같이 비밀이란 개인정보만 포함하는 것이 아닌 기업, 국가, 공공 영역에서의 개인정보 및 일반적으로 알려져 있지 않은 정보 또한 포함해야하는 것이 옳다.

Ⅳ. 문제해결을 위한 정보통신망법 제49조 “비밀”의 분류 및 정의

본 장에서는 3장에서 다루었던 문제에 대한 해결방안인 정보통신망법 제49조 “비밀”의 분류 및 정의와 그에 따른 기대효과를 제시한다.

1. 국가·공공 정보

비밀 정보	유형	항목
국가 정보	기밀 정보	연구 과제, 작전
	군사 정보	군사력, 군사 작전, 통신망, 지휘체계
	교통 정보	항공, 항해, 철도, 수송, 운반에 대한 정보

	위치 정보	주요통신기반시설, 국가 기관의 지리적 위치
	지역 정보	지역 별 인구 수, 생활 수준 정보, 지원금, 에너지
	재산 정보	세금, 무역품에 대한 정보
	교육 정보	국가 시험

표 6. 국가・공공 정보 분류 및 정의 제시

국가·공공 정보는 국가와 관련된 정보로 유출될 경우 국가적 손실 혹은 국민의 혼란을 야기할 수 있는 정보를 뜻하며 표 6와 같이 정의했다. 기밀 정보는 국가 기밀 사항들의 유형으로 국가가 주도하여 실시하는 연구 및 작전 등을 의미한다. 기밀 정보가 노출될 경우 해당 연구 과제 및 작전에 대하여 국민들의 불안감 및 혼란을 야기 할 수 있다. 군사 정보는 국가의 군사력에 관한 정보로써, 부대 병력, 지휘 체계, 보유한 무기에 대한 정보, 통신망에 대한 정보이다. 군사 정보가 누출 될 경우 군사가 이용하는 통신망에 대한 도청을 당할 위험성과 적대국이 우리나라가 보유한 첨단 무기에 대한 대책을 마련할 수 있게 된다. 교통 정보는 배, 비행기, 자동차, 신호등 등 교통에 관련된 정보이다. 교통 정보가 노출될 경우 신호등이나 항공에 관하여 악의적인 방해 공작 및 혼란을 유도하여 시민들의 안전을 위협하고 혼란을 야기할 수 있다. 위치 정보는 주요통신기반시설 및 국가와 연관된 기관의 위치 정보를 의미한다. 위치 정보가 노출될 경우 해당 기관에 대한 테러의 위험성이 높아지며 이로 인한 국민들의 불안감이 조성될 가능성이 높다. 지역 정보는 우리나라 지역 별 인구 분포도와 생활 수준에 대한 정보이다. 지역 정보의 비밀이 노출될 경우 지역별 생활 수준 차이로 인한 타 지역에 대한 천대 및 무시가 생길 수 있어 지역 간의 발전이 아닌 과도한 경쟁구도로 지역 감정이 악화될 가능성이 있다. 재산 정보는 현재 국가의 세금과 교류하고 있는 타국과의 무역품에 대한 원가 및 수출 시세에 대한 정보이다. 재산 정보가 누출될 경우 우리나라의 경제력 수준을 타국이 알게 되고 이를 이용하여 무역 협상 단계에서 불리한 입장으로 진행하게 된다. 교육 정보는 국가가 실시하는 시험에 대한 정보로 수학능력시험, 공무원 시험 등이 예시이다. 교육 정보가 노출될 경우 해당 시험 결과에 대한 신뢰성을 상실하게 되고 응시자들에게 국가 시험에 대한 신뢰도를 상실하게 될 것이다.

2. 기업 정보

기업 정보는 표 7와 같이 정의된다. 사원에 대한 개인정보 또한 포함된다. 호봉, 연봉, 상여금 같은 경우는 일반적으로도 알려지지 않았으며 기업의 내부적인 요소로 포함된다. 금융 정보로는 공개되는 총 매출액 같은 경우는 포함하지 않고 과세 내부 자료, 재무 재표 등 대외비로 취급되는 금융 관련 정보를 포함했다. 기업 정보로는 사업자 번호와 이용하는 고객의 정보 또한 포함된다. 고객의 정보는 개인 정보와 비슷한 정의를 가지지만 기업 내부에 포함되어있는 정보로서 고객에게 정보제공동의를 받은 정보를 뜻한다. 기밀 정보는 기업 대외비 문서, 진료 차트, 설계 도면 등 기업 내부에서의 취급이 기밀로 되어있는 정보를 뜻한다. 마지막으로 사업 정보는 회의록, 내부에서 추진 전에 있는 사업 등에 대한 정보를 뜻한다. 기업 정보는 다른 정보와 다르게 기업에서 악용할 수 있기에 사전에 조사와 기업 내부의 감사를 거쳐야 할 것이다.

비밀 정보	유형	항목
기업 정보	사원 정보	호봉, 연봉, 상여금 등
	금융 정보	과세 자료, 재무 재표 등
	기업 정보	사업자 번호, 고객 정보 등
	기밀 정보	기업 대외비 문서, 진료 차트, 설계 도면 등
	사업 정보	회의록, 내부 추진 사업

표 7. 기업 정보 분류 및 정의 제시

3. 개인 정보

개인정보에 대한 정의 및 분류는 그림 2와 같다. 개인정보는 현재에도 정보보호에 관련하여 큰 이슈가 되고 있고 정의에 관한 논란 및 혼란이 야기되었던 부분이 있었다. 그림 2의 개인정보 정의는 표 4의 국가별 개인정보를 중심으로 모호한 부분이 없게 개정하였다. 특히 통신 및 위치 정보의 항목에 있는 쿠키(Cookies) 및 로그파일(Log file)같은 경우에는 사용자의 성향 또한 드러나기에 중요한 개인정보라 할

비밀 정보	유형 구분	정의	항목
개인 정보	인적 사항	정보주체의 가족 구성원을 포함한 사람에 관련된 정보	이름, 주민등록번호, 여권번호, 운전면허번호, 주소, 연락처, 생년월일, 출생지, 국적, 성별 등
	신체 정보	정보주체의 신체와 관련된 생체 정보	키, 몸무게, 지문, 홍채, DNA, 신장, 가슴둘레 및 추후 사용되는 보안 기술의 생체 정보 등
	의료 정보	신체 정보와 관련하여 의료적 처치 및 검증되어진 정보	병력기록, 의료기록, 신체장애, 혈액형, IQ(EQ 등 포함), 신체테스트 정보 등
	성향 정보	정보주체의 성향이 드러나는 기록 및 정보	좋아하는 스포츠, 도서 및 비디오 대여기록, 물품구매내역, 사상, 종교 등
	조직 정보	정보 주체가 속해있는 조직 및 인터넷 클럽 등의 정보	정당 및 노조 가입 여부, 클럽 회원 등
	재산 정보	정보 주체의 금융, 신용, 소득, 거래에 관한 기록 및 정보	소득, 이자, 수수료, 상여금, 소유 주택 및 토지, 신용평가정보, 대출 등
	교육 정보	교육 및 훈련, 자격증에 관한 기록 및 정보	출석 사항, 학력, 성적, 이수 프로그램, 자격증, 생활기록부, 동아리 활동 등
	법적 정보	정보 주체에게 법적으로 판결되었거나 신청된 기록 및 정보	전과 및 범죄 기록, 재판 기록, 교통 위반 기록, 파산 및 담보 기록, 이혼 기록 등
	근로 정보	정보 주체가 속했거나 과거 속해있던 근무에 관련된 기록 및 정보	직장, 근무처, 경력, 상벌 기록, 직무 평가 기록, 휴가 및 병가 기록 등
	병역 정보	정보 주체의 병역에 관련된 기록 및 정보	병역 여부, 군번, 계급, 근무부대, 병역에 대한 기록(주특기 등) 등
	통신 및 위치 정보	정보 주체의 통신 접속, 내역 및 위치에 대한 기록 및 정보	전화통화내역, 웹사이트 접속 내역, 이메일 또는 전화메시지, 기타 GPS 에 의한 위치정보, 쿠키(Cookiess), 로그파일 등

표 8. 개인 정보 분류 및 정의 제시

수 있다. 개인정보는 본 논문에서 나눈 국가·공공 정보, 기업 정보의 근간이 되는 정보기에 추후 기술의 발전에 따라 정의와 분류가 반복되어야한다.

4. 기대 효과

본 장에서는 정보통신망법 제49조의 “비밀”에 속하는 정보로서 국가·공공 정보, 기업 정보, 개인 정보에 대한 분류 및 정의를 제시하였다. 제시한 바와 같이 “비밀”에 대하여 개정하면 3장에서 분석한 판례마다의 해석 및 견해 차이가 일어나지 않을 것이다. 또한 분류 및 정의가 명확해졌기에 기술의 발전에 빠르게 개정이 가능할 것이다.

Ⅴ. 결론

본 논문에서는 정보통신망법 제49조 비밀에 대한 정의와 항목에 대하여 알아보았지만 비밀의 범위에 기업 정보가 포함되는지에 대한 해석 및 견해차이가 판례 2005도7309와 판례 2017도4240에서 발생하였다. 따라서 “비밀”은 개인 정보만이 아니라 국가·공공 정보, 기업 정보도 포함하도록 분류 및 정의하여 제시하였다. 이에 따른 기대 효과로 판례마다 해석 및 견해의 상충이 발생하지 않을 것이고 기술의 발전에 맞춰 빠르게 개정이 가능할 것이다. 추가적으로 향후의 연구 방향으로는 동 법과 관련된 개별 법률 등이 기술 발전에 맞춰 개정 및 체계 정비를 해야 하며, 정보통신망법 제49조와 관련된 법적 연구가 미비한 수준이기에 더 많은 연구가 필요하다. 또한 법적인 연구 뿐 아니라 정책 및 기술에 관련된 연구 또한 진행이 필요할 것이다.

[참고문헌]

[1] 법제처. 정보통신망 이용 촉진 및 정보보호 등의 관한 법률

[2] 한다빈. (2016). 사이버공격에 대한 정보통신망법 제48조의 문제점과 개선방안 연구. 단국대학교 대학원 IT법학협동과정.

[3] 방송통신위원회, 한국인터넷진흥원. (2011). 정보통신서비스 제공자를 위한 개인정보보호 가이드.

[4] 대한민국법원 종합법률정보. 대법원 2017. 6. 19. 선고 2017도4240 판결 등.

[5] 대한민국법원 종합법률정보. 대법원 2006. 3. 24. 선고 2005도7309 판결 등.

[6] 신동민. (2013). 정보보호 행정법제에 관한 연구 -정보보호의 법적 의의와 정책집행체계를 중심으로-. 광운대학교 대학원 법학과.

[7] 정대경. (2012). 국내외 개인정보보호정책 비교 분석 -개인정보보호 법률과 전담조직을 중심으로-. 정보통신산업진흥원.

내부 정보 유출 경로별 통합 시나리오 점검 방법 연구*

권현우*, 이익준**, 염흥열**

*순천향대학교 융합서비스보안학과,**순천향대학교 정보보호학과

A Study on Integrated Attack Scenario Identification Method by Internal Information Leakage Route

Hyun-Woo Kwon*, Ig-Joon Lee**, Heung-Youl Youm**

*Department of Convergence Service Security, SoonChunHyang University.

**Department of Information Security Engineering, SoonChunHyang University.

요 약

최근 발생하는 정보유출 사례를 살펴보면, 내부자에 의한 개인정보, 기술유출이 지속적으로 발생하고 있음을 알 수 있다. 이러한 내부자에 의한 정보유출에 대비해 기업에서는 다양한 보안 솔루션을 구축하여 운영하고 있지만 각각의 솔루션들은 별도로 운영되기 때문에 통합적인 운영이 힘들었다. 이에 본 논문에서는 유출 경로 및 현황 로그를 시나리오 기반으로 상호 연계 분석하고 A금융사의 적용 사례를 통해 유출 경로별 통합 시나리오를 제안한다. 해당 위협들을 지속적으로 탐지하기 위해 보안 현황정보들을 기반으로 탐지 룰을 작성하고, 룰을 통해 탐지되는 정보는 위험정후로 정의하여 보안담당자에게 실시간으로 알릴 수 있도록 한다.

I. 서론

최근 ICT 산업의 발달로 기업은 업무 시스템의 효율성을 높이기 위해 전자문서의 활용을 더욱 확대하고 있다. 전자문서 사용으로 인해 시간과 공간의 제약을 탈피하고 많은 혜택을 얻게 되었지만 이러한 전자문서의 용이성 때문에 정보의 유출, 도난 등의 역기능 또한 증가하게 되었다. 국가정보원 산업기밀보호센터의 조사에 따르면 2003년부터 2014년도까지 기술유출 438건을 적발하였으며, 기술유출로 인한 연평균 예상 피해액은 50조원으로 추정했다. 전·현직직원 등에 의한 내부유출이 80% 이상을 차지했다[1]. 2014년에는 내부직원에 의해 카드 3사에서 1억 400만건의 고객 정보가 유출되는 사례도 있었다.[2] 내부자의 의한 보안위협이 증가함에 따라 기업은 문서보안(DRM, Digital Right Management), 데이터 유출 방지(DLP, Data Leakage Protection), 모바일 장치 통제시스템(MDM, Mobile Device Management), 네트워크 접근제어(NAC, Network Access Control)와 같은 보안솔루션을 도입하여 로그를 분석, 모니터링을 하고 있지만 보안 담당자마다 로그가 다르게 분석되고, 수집되는 로그의 양이 많아 위협을 식별하는데 어려움이 있다.[3] 효율적인 운영을 위해서 일관된 보안정책을 수립하고 업무에 유기적으로 통합할 수 있는 체계가 필요한 실정이다.

따라서 본 논문에서는 유출 경로 및 현황 로그를 시나리오 기반으로 상호 연계 분석하여 통합 시나리오를 제안한다.

* 본 연구는 과학기술정보통신 및 한국인터넷진흥원의 “고용계약형 정보보호 석사과정 지원사업”의 연구결과로 수행되었음

II. 관련연구

2.1 보안 통제 솔루션

2.1.1 DRM 솔루션

DRM은 디지털 저작권을 보호하는 기술로 문서 파일이나 동영상 파일 등 허가된 사용자 이외에는 접근할 수 없도록 제한한다. 기업에서는 전자문서에 DRM암호화 기술을 적용시켜 정보가 유출, 도난 되어도 정보를 사용할 수 없게 만들 수 있다.[4]

2.1.2 DLP 솔루션

DLP는 기업 구성원, 프로세스, 기술의 결합을 통해 개인정보, 기업의 중요 기밀정보 등이 유출되는 것을 방지하는 솔루션으로 인터넷, 저장매체, 프린터 등을 통제하여 모니터링하고 정보의 유출을 차단할 수 있다.[4]

2.1.3 MDM 솔루션

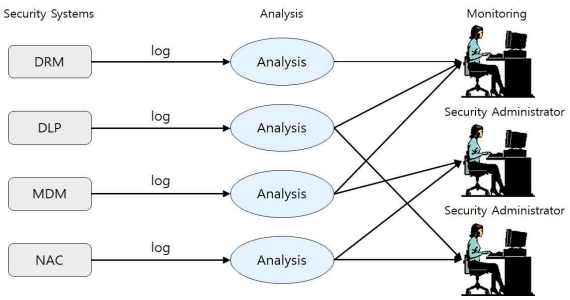
MDM은 스마트폰이나 태블릿, 개인용 노트북과 같은 모바일 기기를 관리, 감시하는 솔루션으로 스마트폰의 촬영으로 중요 기밀정보가 유출될 수 있기 때문에 기업에서 많이 도입하고 있는 추세이다.[4]

2.1.4 NAC 솔루션

NAC는 각종 공격으로부터 효과적으로 네트워크를 보호하는 솔루션으로 허가되지 않은 PC나 노트북, 모바일 단말기 등이 회사 네트워크에 접속되는 것을 차단할 수 있다.[4]

2.2 기존 모니터링 시스템 현황 및 문제점

기존의 보안솔루션 시스템들은 모니터링을 통해 사후추적이 가능하지만 한계가 있었다. 각각의 솔루션들은 별도로 운영되어 통합적인 운영이 되지 않았고, 보안 담당자마다 수집되는 로그가 다르게 분석될 수 있어 체계적인 모니터링이 힘들었다.[3]

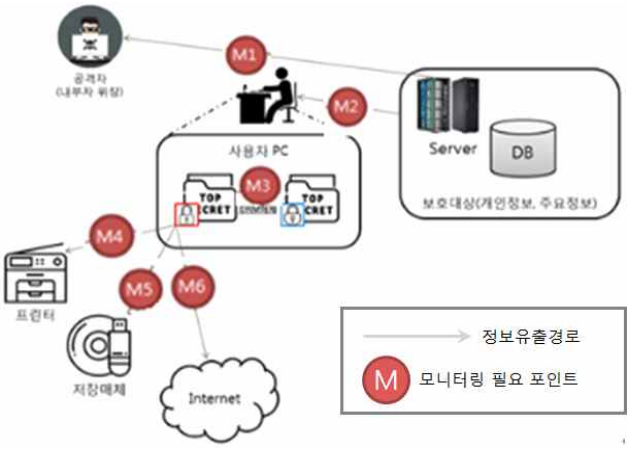


〔그림 1〕 기존 보안 솔루션 로그 모니터링 현황

위 [그림 1]은 기존 보안 솔루션 로그 데이터를 수집 및 종합하여 통계자료로 활용하는 모습이다. 다수의 회사 내 정보보호 관련 부서에서 주기적으로 현황파악을 위해 이용되고 있으나, 해당 현황자료만을 통해 전반적인 위험수준을 판단하기가 힘들어 활용가치가 낮다.

III. 유출 경로별 통합 시나리오 제안

[그림 2]는 정보가 유출될 수 있는 경로마다 모니터링이 필요한 포인트를 도식화하여 나타내었다.



〔그림 2〕 경로별 정보 유출 시나리오 도식화

3.1 A금융사의 보안 환경 분석 및 현황 로그 수집

A금융사의 보안 솔루션에서 저장된 로그를 대상으로 반출 승인 및 암호화 해제 로그, DB 접근 로그, 서버 접근 로그, 웹 키퍼 로그, 개인정보 반출 승인 로그, 망 연계 접근 차단 스트림 로그, 개인정보 보유 로그, 악성코드 감염/치료 이력, NAC IP 할당 현황 등을 수집 대상으로 정하고, A금융사의 보안 활동 현황 정보로 NAC IP할당 현황, 개인정보 보유현황, USB 사용신청, 파일 반출신청, 악성코드 감염내역 등 현황 정보를 [표 1]과 같이 정리하였다.

〔표 1〕 보안 활동 현황자료

구분	내용
NAC IP 할당 현황	1231(내부), 237(외주) (2018년 1월 9일 기준)
개인정보 보유현황	개인정보 미 암호화 100건 이상 보유자 42명 (2017년 12월 기준)
USB 사용신청	29건 (2017년 12월 기준)
파일 반출 신청	2095건 (2017년 12월 기준)

악성코드 감염내역	34건 (2017년 12월 기준)
외부메일 쓰기 예외	마케팅부 (마케팅팀 전체 외부 메일 쓰기 차단 예외)

3.2 시나리오 구성

앞에서 수집된 현황 자료들을 위협경로 관점에서 시나리오로 구성한다. 위협경로와 유출 방법 가능성에 대해 시나리오를 구성하고, 시나리오 선정 기준에 따라 위험등급을 구분 한다. 위협 경로 관점은 누가, 어떤 경로로 어떤 방법을 이용하여 정보를 유출할 경우 그 가능성을 위험유형과 등급으로 분류할 수 있다.[5] 이러한 항목을 조합하여 유출 경로별 시나리오 Pool을 구성한다. 본 논문에서는 파악된 위험과 관리되는 위험 측면에서 연구한다.

〔표 2〕 시나리오 구성

No	경로		시나리오
1	사용자 PC->서버	M2	일반 사용자 PC에서 관리자 계정을 통해 서버로 직접 접근
2	사용자 PC->DB	M2	일반 사용자 PC에서 DBA 계정을 통해 DB로 직접 접근
3	사용자 PC->서버	M1	접근권한이 없는 임직원 IP(혹은 계정)로 서버 접근시도
4	사용자 PC->DB	M1	접근권한이 없는 임직원 IP(혹은 계정)로 DB 접근시도
5	사용자 PC	M3	DRM 해제 신청 시 문서내용과 제목이 불일치
6	사용자 PC	M3	도면, 소스코드, 대외비문서 등 비밀문서의 DRM 해제 요청/승인
7	사용자 PC	M3	승인권자의 IP 이외의 PC에서 DRM 해제 승인

3.3 시나리오 점검 및 결과

[표 2]에서 도출된 시나리오들을 연계하여 아래 [표 3], [표 4]와 같이 통합 시나리오를 만들었다.

〔표 3〕 통합 시나리오 점검

1	No	경로		시나리오
기본 시나리오	1	사용자 PC-> 서버	M2	일반 사용자 PC에서 관리자 계정을 통해 서버로 직접 접근
	2	사용자 PC-> DB	M2	일반 사용자 PC에서 DBA 계정을 통해 DB로 직접 접근
	3	사용자 PC-> 서버	M1	접근권한이 없는 임직원 IP(혹은 계정)로 서버 접근시도
	4	사용자 PC-> DB	M1	접근권한이 없는 임직원 IP(혹은 계정)로 DB 접근시도
점검 세부 시나리오	내용			
	경로	외주직원이 내부 사용자 PC 계정관리 취약점 (AD 미사용)을 이용		
	방법	외주직원 PC에서 내부직원 명의의 계정을 도용하여 문서보안 (DRM) 암호화 해제 또는 이동식 저장매체 사용 승인을 받음		
	영향	내부 중요정보 또는 개인정보가 유출될 가능성이 있음		
	위험 유형	파악된 위험	등급	보통

점검 시 확인 사항으로 첫째, IP 관리시스템(자산관리) 적용 여부, 둘째, 외주직원 PC정보(IP)외 내부직원 PC정보(IP) 목록을 확인한다. 점검 결과 다음과 같은 문제점이 있었다.

- NAC에 미 등록된 IP로 서버접근 및 접근시도 이력이 존재하여 추가 확인이 필요하다.
- 서버에 저장되는 중요/개인정보의 경우 문서보안 암호화가 적용되어 있지 않아 개발 PC로 다운로드가 가능하다. 개발 종류 후 단말기 반출 시 포맷 후 담당자의 확인을 받고 반출하는 프로세스가 있는지 추가 확인이 필요하다.

〔표 4〕 통합 시나리오 점검 2

2	No	경로		시나리오
기본 시나리오	5	사용자 PC	M3	DRM 해제 신청 시 문서내용과 제목이 불일치
	6	사용자 PC	M3	도면, 소스코드, 대외비문서 등 비밀문서의 DRM 해제 요청 /승인
	7	사용자 PC	M3	승인권자의 IP 이외의 PC에서 DRM 해제 승인
점검 세부 시나리오	내용			
	경로	서버 접근 권한이 없는 외주직원 PC(노트북, 데스크탑_HDD 등)		
	방법	임의로 내부 사용자의 계정을 대여 혹은 도용하여 서버에 접근 후 내부 중요정보 및 개인정보를 다운로드하여 단말기에 저장한 뒤 포맷을 하지 않은 상태로 반출		
	영향	내부 중요정보 또는 개인정보가 유출될 가능성이 있음		
	위험 유형	관리되는 위험	등급	낮음

점검 시 확인 사항으로 첫째, IP 관리시스템(자산관리) 적용 여부, 둘째, 외주직원 PC정보

(IP)외 내부직원 PC(IP) 목록, 셋째, 문서보안(DRM) 및 이동식 저장매체 외주인력 허용 정책 여부를 확인한다. 점검 결과 다음과 같은 문제점이 있었다.

- 외주직원의 저장매체 사용 신청건수는 3건이나 만료일 설정과 근기문서 첨부 등 절차상 양호하며, 저장매체 신청 로그 중 외주직원의 IP로 신청된 정보는 없었다.
- 외주직원의 문서보안 암호화 해제 이력이 35건 존재하였으나 검토결과 개인정보가 없는 문서를 해제하는 등 위험도가 낮았다.

3.4 대책

각각의 보안 솔루션 시스템들에서 운영 및 관리되는 보안 현황정보들을 수집하여, 위협경로 및 직무별 보안정책 연관 분석을 통해 위협 시나리오를 도출할 수 있다. 보안현황자료 연관분석의 예는 아래의 [표 5]와 같다.

〔표 5〕 A사 보안 현황자료 연관분석

구분	내용
NAC IP할당 현황 + 운영서버 접근이력	NAC에 할당되지 않은 운영서버 접근 이력 1건
USB 사용신청 + 직무별 보안정책	USB 사용 신청 29건 중 고위험군(외주직원) 이동매체 사용신청 3건
파일 반출 신청 + 보안문서 암호화해제 + 직무별 보안정책	파일 반출 신청 2095건 중 고위험군(외주직원) 문서 암호화해제 신청 35건
악성코드 감염내역 + 운영서버 접근이력	악성코드 감염내역 34건 중 서버침투 관련 악성코드 및 운영서버 접근이력은 없음

해당 위협들을 지속적으로 탐지하기 위해, 보안 현황정보들을 기반으로 탐지 룰을 작성하여야 한다. 탐지되지 말아야 할 이벤트들은 블랙리스트 룰로, 특정 현황정보와 결합되거나 평소와는 다르게 비정상적으로 많이 탐지되는 이벤트는 화이트리스트 룰로 설정을 한다. 룰을 통해 탐지되는 정보는 위험징후로 정의하고, 보안담당자에게 실시간으로 알릴 수 있도록 한다. 또한, 악성코드 감염 경로 등 정보유출 경로로 악용될 위험도가 높으나 파악하기 어려운 잠재위험과 파악되지 않은 위험에 대해 추가 확인이 필요한 경우, PC내 파일들의 행위에 기반한 로그를 수집하고 분석할 수 있는 기법 등 고도화된 분석을 권고한다.[6]

IV. 결론 및 향후 연구 방향

내부자에 의한 보안위협이 지속적으로 발생하면서 기업은 다양한 보안 솔루션을 운영하여 정보 유출을 최소화 시키려하지만 이러한 솔루션들은 개별로 운영 및 관리되어 통합적인 분석이 어려웠다.

본 논문에서는 직무별 컴플라이언스 정책을 적용하고 있는 A금융사의 유출 경로별 통합 시나리오를 적용시켰다. 직무별 고위험군 종사자들을 대상으로 점검 결과 파악된 위험과 관리되는 위험 측면에서 보완해야할 문제점들이 있었고, 향후 위험도가 높은 잠재위험과 파악되지 않은 위험에 대비한 연구가 필요할 것이다.

[참고문헌]

[1] 국가정보원, “기술 유출 통계”, http://www.nis.go.kr/AF/1_5_1_1.do, 2015.

[2] 정정욱, “롯데카드·NH농협카드·KB국민카드, 고객정보 1억400만건 유출, 사상 최대”, http://www.sportsworldi.com/content/html/2014/01/08/20140108024369.html, 2014.

[3] J. Wu, J. Zhou, J. Ma, S. Mei and J. Ren, "An Active Data Leakage Prevention Model for Insider Threat", Intelligence Information Processing and Trusted Computing, 2011.

[4] 채현탁, "PC보안솔루션 로그분석을 통한 보안정책 제안“, 석사학위 논문, 고려대학교 정보보호대학원, 2015.

[5] 양현진, “IT서비스 위험분석 방법을 사용한 전자화 인증평가에 관한 연구”, 석사학위 논문, 숭실대학교 정보과학대학원, 2011.

[6] 정귀영, “통합 보안 로그분석을 통한 효과적 사용자 이상징후 탐지 방안 연구”, 석사학위 논문, 연세대학교 정보대학원, 2016.

블록체인 기술 적용과 개인정보 삭제 및 제3자 제공의 법적 문제에 관한 연구

최용혁

고려대학교 정보보호대학원

A Study on Legal Issues between the Application of Blockchain Technology and Deletion and the Third Party Supply of Personal Information

Yong-Hyuk Choi

Graduate School of Information Security, Korea University.

요 약

암호화폐라는 새로운 패러다임을 몰고 온 블록체인 기술은 데이터의 무결성을 보장하는 분산원장 기술로서 4차 산업혁명시대의 대표적인 미래 기술로 주목받고 있으며, 시대적 흐름을 놓치지 않는 기업이라면 블록체인 기술을 이용하는 새로운 비즈니스 모델 발굴에 힘을 쏟고 있다. 그러나 블록체인이 가지고 있는 고유한 특성인 비가역성과 블록체인 참여자간 블록의 공유는 국내 개인정보 보호법제와의 충돌을 피할 수 없는 상황이다. 본 연구에서는 블록체인의 고유한 이 두 가지 특징을 기반으로 충돌 발생 가능한 개인정보의 삭제와 제3자 제공을 중심으로 국내 개인정보 보호법제와 관련한 문제점을 살펴보고 블록체인 기술 활용을 위한 개인정보 보호법제 개선방향 및 현행법규 준수를 위해 적용 가능한 블록체인의 기술적 대안을 제시하고자 한다.

I. 서론

비트코인의 광풍을 등에 업고 대중의 입에 오르내리기 시작한 블록체인 기술은 4차 산업혁명을 주도할 미래 선도 혁신 기술로 주목받고 있다. 특히 최근 금융권에서는 블록체인 기술을 미래 금융의 핵심 인프라로 활용하기 위한 논의와 연구가 다양하게 전개되고 있으며, 이러한 움직임은 머지않아 다양한 산업으로 확장되어 사회 기반구조에 큰 영향을 끼칠 것으로 전망된다.

기업들이 블록체인 기술을 이용하는 새로운 비즈니스 모델 발굴에 힘을 쏟고 있음에도 불구하고 아직까지 국내 블록체인 기술 활용은 걸음마 수준에 머물러 있으며, 블록체인 기술에 대한 높은 관심에도 불구하고 실제 산업에 어떤 영향을 줄지 확언하기 어려운 상황이다.

기존 IT인프라를 블록체인시스템으로 전환하기 위한 연구가 활발하게 진행 중임에도 불구하고 블록체인 기술 활용의 속도가 빠르지 않은 이유는 무엇일까? 기술적인 측면으로 보면 블록체인 기술은 아직 발전 초기 단계로 다양한 환경에서 안정적인 거래를 담보하기 위해서는 지속적인 발전이 필요하며, 비즈니스 측면으로 보면 비즈니스 모델 발굴 및 검증과정에서 발생하는 경제적 이익 상충 관계를 블록체인 참여로 유도하는 합의를 이끌어내는 것이 쉽지 않기 때문이다. 블록체인의 상용화가 어려운 최대 걸림돌은 비즈니스 측면의 문제라는 주장도 있지만[1] 법·제도 측면에서 기존 법률과의 상충 여부에 대한 구체적인 해석이나 판례가 없어 진입 위험이 해소되지 않거나 누구나 인정할 수밖에 없는 기존 법률과의 상충 문제에 대한 대안이 없다면 블록체인의 상용화는 허울뿐인 연구만으로 만족해야 한다.

본 연구에서는 블록체인의 고유한 특징을 확인하고, 이 특징이 블록체인의 상용화에 걸림돌이 되는 법·제도 중에서도 국내 개인정보 보호

법제와 어떤 점에서 상충되는지 살펴보고자 한다. 또한 블록체인 기술의 활용을 위한 국내 개인정보 보호법제 개선 방향을 고민해 보고 이 문제점을 해결하기 위한 기술적 대안을 제시하고자 한다.

II. 블록체인 기술과 개인정보 보호법제

2.1 국내 블록체인 기술 활용 현황

국내 블록체인 기술 활용은 금융기관을 중심으로 활발하게 전개 중이다. 블록체인을 이용하여 저비용으로 해외송금 및 자산관리에 활용하는 플랫폼을 운영하는 미국 핀테크 업체 R3 CEV와 컨소시엄을 형성하고 있는 골드만삭스, 바클레이즈, JP모건, UBS 등 42개 글로별 대형 은행과 연합하기 위해 하나금융그룹과 신한은행이 R3 컨소시엄에 참여하고 있는데 이 은행들은 R3와 협업을 통해 블록체인 시스템을 표준화하고 이를 통해 글로벌 금융시장에 더 빠르고 효율적인 시스템을 도입할 계획을 가지고 있다.

국내 은행들은 송금분야에서 블록체인 기술을 활용하기 위한 경쟁에 뛰어들고 있다[2]. KEB하나은행은 글로벌 MTO(Money Trasfer Operator)와의 업무제휴를 통해 중개은행을 거치지 않는 중국 해외송금 서비스와 모바일 앱으로 간편하게 해외송금이 가능한 원큐트랜스퍼(1QTransfer)를 출시해 15개 국가를 대상으로 해외송금을 지원 중이다. 신한은행은 글로벌 S뱅크를 활용한 머니그램 특급송금 서비스를 출시하고 실시간으로 해외 송금 서비스를 준비중이다. 우리은행은 위비 퀵 글로벌송금을 통해 우리은행 해외지점으로 외화 송금시 중개은행을 거치지 않고 현지로 바로 송금이 가능하다. 국민은행은 모바일 서비스 KB스타뱅킹과 리브메이트에 해외송금 기능을 추가하였다.

교보생명은 업계 최초로 블록체인 기술을 이용하여 의무기록 사본 발급 연계를 통해 보험금 지급 절차를 간소화한 스마트 보험금 청구 서비스와 고객이 가입한 모든 보험 가입정보를 수집하여 보장분석 시 활용하도록 하는 스마트 스크래핑 서비스를 시범운영하고 있다.

금융투자업계는 금융투자협회가 주축이 되어 세계 최초로 블록체인을 이용한 공동인증서인 체인아이디를 출시하고 12개 증권사를 대상으로 시범운영 중이며 2018년 하반기 중 상용화를 목표로 하고 있다. 증권사 고객이 체인아이디를 발급받게 되면 체인아이디를 서비스하는 증권사에서는 별도의 등록 과정 없이 인증서를 사용할 수 있다.

2.2 블록체인 기술과 개인정보보호 규제의 관계

2.2.1 블록체인의 탈중앙화 속성

블록체인의 개념에 대한 다양한 견해가 존재하는데 거의 모든 개념에서 공통적으로 다루고 있는 내용은 블록체인은 분산 데이터베이스이며, 탈중앙화를 기본 사상으로 하는 분산형 디지털 장부라는 것이다. 국내 정보보호 관련 법률이 대부분 중앙집중형 IT환경을 전제로 구체적인 요건을 정하고 있는 것을 감안할 때 블록체인의 탈중앙화라는 속성은 여러 쟁점을 양산하는 주요 요인이 된다. 또한 블록체인 기술을 이용하는 비즈니스 모델중 상당수가 개인정보의 처리 과정이 수반되는 것을 고려하면, 블록체인의 탈중앙화라는 속성과 국내 개인정보 보호법제의 주요 법적 의무사항 간 상충되는 문제점을 검토하고 그 문제점을 해결하기 위한 대안을 찾는 작업은 피할 수 없는 과제이다. 그렇다면 블록체인 기술을 활용함에 있어서 개인정보보호 규제에 대한 검토는 어느 정도나 이루어졌을까?

2.2.2 개인정보보호 규제 검토 현황

앞서 살펴 본 국내 블록체인 기술 활용 분야의 특징은 은행들의 사례에서와 같이 이미 확보하고 있는 자사 고객만을 대상으로 하는 프라이빗(Private) 블록체인 서비스이거나 교보생명의 사례와 같이 새로운 비즈니스를 개발하기 위한 규제 샌드박스 환경을 최대한 이용하였다는 것이다. 즉, 아직까지 국내 대다수의 블록체인 기술 활용 분야는 상용화 단계까지 이르지 못했거나 개인정보 보호법제와 상충하는 블록체인의 고유한 특징을 주의 깊게 보지 않고 있는 상황이다.

이에 반해 금융투자업계의 공동인증서 서비스는 컨소시엄(Consortium) 블록체인 서비스 형태로 앞서 소개했던 블록체인의 고유한 특징으로 인해 발생하는 국내 개인정보 보호법제와의 충돌을 고민하면서 대안을 찾아본 흔적들이 있다. 그 중, 스마트계약 기술을 활용한 대안은 Ⅳ장에서 설명하기로 한다.

III. 블록체인 기술 적용의 한계

3.1 블록체인 기술의 주요 특징

첫 번째 블록체인 기술의 특징은 데이터의 비가역성(Irreversibility)이다. 블록체인의 데이터 기록 방식은 거래정보를 담고 있는 블록이 체인형태로 연결되어 현재 블록에서는 이전 블록의 해시값과 자신의 해시값을 함께 기록하고 순차적으로 배열되도록 하고 있다. 즉 블록들은 이전 블록 해시값을 기준으로 순차적으로 연결되기 때문에 특정 블록의 데이터를 변경할 경우 블록 간 연결이 끊어지게 되고 이 블록 간 연결 유지 여부를 통해 데이터의 조작 여부를 검증할 수 있게 된다. 이렇게 블록연결을 통해 순차적으로 데이터를 기록하는 특징을 블록체인의 비가역성이라고 한다.

두 번째 블록체인의 특징은 데이터의 공유방식이다. 블록체인은 블록체인 플랫폼을 구성하는 각각의 참여자간 플랫폼이 정한 특정한 합의구조에 따라 거래 데이터를 검증하고 검증된 데이터를 모든 참여자가 분산 저장하는 데이터 공유 방식을 취하며 이렇게 모든 참여자에게 공유되는 데이터 블록은 복사본이 아닌 원본(The Original Copy)으로서 가치를 가지게 된다. 즉 블록체인에 참여하는 모든 참여자는 선택의 여지없이 모두 원본 데이터를 공유하는 특징을 갖는다.

3.2 국내 개인정보 보호법제와의 충돌

3.2.1 개인정보의 삭제에 관한 문제점

국내 주요 개인정보 보호법제들은 모두 보유기간이 경과하거나 처리 목적이 달성된 개인정보는 파기하도록 정하고 있다[3]. 개인정보 보호법에서는 목적 달성이 된 개인정보는 데이터가 복원되지 않도록 초기화 또는 덮어쓰기를 수행하여 파기하도록 하고 있으며, 신용정보의 이용 및 보호에 관한 법률에서는 신용정보제공·이용자는 금융거래 등 상거래관계가 종료된 날부터 최장 5년 이내(해당 기간 이전에 정보 수집·제공 등의 목적이 달성된 경우에는 그 목적이 달성된 날부터 3개월 이내)에 해당 신용정보주체의 개인신용정보를 관리대상에서 삭제하도록 하고 있다. 또한 정보통신망 이용촉진 및 정보보호 등에 관한 법률에서는 개인정보의 수집·이용 목적을 달성하였거나 개인정보의 보유 및 이용기간이 끝난 경우, 그리고 정보통신서비스를 1년 동안 이용하지 않은 이용자의 경우에는 해당 이용자의 개인정보를 파기하도록 하고 있다. 그러나 블록체인에서 개인정보를 이용하는 경우에는 블록체인의 고유한 특징인 비가역성(Irreversibility)으로 인해 데이터의 삭제나 변조가 불가능하다.

3.2.2 개인정보의 제3자 제공에 관한 문제점

파기와 유사하게 국내 모든 개인정보 보호법제들은 수집한 개인정보를 제3자에게 제공하기 전에 정보주체의 동의를 받아야 한다.[4] 제3자 제공에 대한 동의 방식은 엄격한 사전 동의를 요구하는 Opt-in 방식으로 정보주체로부터 사전 동의를 받지 못한 경우에는 절대로 제3자에게 개인정보를 제공할 수 없다. 그러나 앞서 살펴본 블록체인의 데이터 공유방식은 블록체인 참여자가 블록체인에 참여를 결정하고 블록체인망에 참여노드를 연결하는 순간부터 다른 기존 참여자의 블록정보를 원본 데이터로 공유하게 되므로 사실상 블록체인망에 신규 참여를 결정하고 참여노드로 연결하기 전에 모든 정보주체로부터 제3자 제공에 대한 동의를 받아야 하는데 거래고객이 많으면 많을수록 사전 동의는 불가능하게 된다.

IV. 한계 극복을 위한 개선 방안

4.1 개인정보 보호법제 개선 방향

4.1.1 개인정보의 삭제

정보주체인 개인 자신과 관련된 개인정보의

삭제와 처리의 제한을 주된 내용으로 하는 '잊혀질 권리'는 개인정보자기결정권의 하나로 간주된다[5]. 개인정보자기결정권은 '특히 컴퓨터를 통한 개인정보의 데이터베이스화'가 진행되면서 개인정보의 처리와 이용이 시공에 구애됨이 없이 간편하고 신속하게 이루어질 수 있게 되었고, 정보처리의 자동화와 정보파일의 결합을 통하여 여러 기관간의 정보교환이 쉬워짐에 따라 한 기관이 보유하고 있는 개인정보를 모든 기관이 동시에 활용하는 것이 가능하게 되었으며, 개인의 인적 사항이나 생활상의 각종 정보가 정보주체의 의사와는 전혀 무관하게 타인의 수중에서 무한대로 집적되고 이용 또는 공개될 수 있는 새로운 정보환경에 처하게 되었다[6].

이러한 환경의 변화는 개인정보자기결정권의 범주가 워낙 방대해지고 있다는 표현이기도 하다. 물론 끊임없이 다양해지고 범위가 확대되는 개인정보자기결정권의 영역을 정보주체가 잘 행사할 수 있도록 법적인 보장을 하는 것이 바람직한 일이라 하겠다. 그러나 법적인 보장이 잘 이루어지면 정보주체는 개인정보자기결정권의 권한 행사를 권리로 받아들일 수 있을까? 아니면 의무로 받아들이게 될까? 개인정보결정권의 권한 행사 영역이 넓어질수록 오히려 정보주체는 개인정보처리자의 개인정보처리 목적을 제대로 인지하지 못하고 어느 순간 개인정보자기결정권 행사를 위한 요청과 동의를 기계적으로 반복하는 자신을 보게 될지도 모른다.

블록체인의 비가역성이라는 고유한 특징은 데이터의 위변조를 불가능하도록 하기 위한 기술적 장치이며, 이 특징을 통해 블록체인에 저장되는 데이터는 무결성과 함께 안전한 저장이라는 신뢰를 블록체인 참여자에게 제공한다. 데이터 신뢰성의 확보를 희망하는 정보주체에게 개인정보의 삭제에 대한 개인정보자기결정권에 일부 제한을 주는 것을 헌법상 기본권을 침해하는 것으로 보는 것은 법의 지나친 해석일 수 있음을 고려해 보아야 한다.

4.1.2 개인정보의 제3자 제공

4차 산업혁명 시대의 중요한 특징 중 하나가 빅데이터 환경이다. 정보주체의 온라인상에서의 관심사와 행동, 모바일 기기를 통한 위치정보, 그리고 사물인터넷 기기의 각종 센서 등을 통해 실시간으로 방대한 양의 데이터가 축적되고 있으며 기술의 빠른 발전은 기하급수적으로 데이터의 축적을 늘려가고 있다. 이런 환경에서 정보주체가 인지하지 못하는 정보의 생성과 수집 내역을 정보주체에게 일일이 통지하고 동의를 받는다면 그 양이 워낙 방대하므로 정보주체의 인식 범위를 벗어나게 될 수 있으며, 이 경우 정보주체로서는 자신의 개인정보 처리에 대한 인식을 못한 것과 다를 바가 없게 된다.

개인정보자기결정권의 선택권을 제한한다는 것 때문에 현행법은 '포괄적 동의'를 금지하고 있다. 그러나 동의 대상이 너무 많아져서 동의권이 퇴색될 수 있는 문제는 어떻게 보아야 할 것인가? 현행 개인정보 보호법은 정보주체가 상대방과의 계약 체결 및 이행을 위해 불가피하게 필요한 경우에는 개인정보의 수집·이용을 동의 대상이 아닌 것으로 보고 있다[7]. 제3자 제공의 경우도 정보주체가 상대방과의 계약 체결 및 이행을 위해 불가피한 경우에는 동의 대상이 아닌 것으로 개선하는 것도 고려해 볼 수 있다.

현대의 정보화 및 빅데이터 환경에서 엄격한 사전 동의를 요구하는 Opt-in 방식의 규제는 현실적으로 불가능하고 규제의 효용성에도 문제가 있다는 의문을 제기한 사례가 있으며[8] 이에 대한 대안으로 개인정보의 수집보다 이용에 초점을 맞추도록 함으로써 그 활용에 따른 혜택과 개인정보 침해 위험 사이의 균형점을 도출해야 하는 대안도 제시되고 있다.

4.2 스마트계약 기술 활용 제안

개인정보의 삭제에 대한 법적 문제는 블록체인의 스마트계약(Smart Contract) 기술을 이용한 대안을 제시해 본다.

스마트계약은 블록체인의 모든 참여자의 장부의 상태를 변경하는 방식으로 블록체인 상에 자동화된 방식으로 실행되는 프로그래밍 코드를 의미한다. 즉 스마트계약은 기록된 계약을 보관하고, 이행하고, 집행하는 컴퓨터 프로그램

이다. 스마트계약은 컴퓨터 과학자 닉 자보에 의해 1994년에 최초로 소개되었으며 인터넷에서 낯선 사람들과 전자상거래 프로토콜을 설계하는 것과 이와 관련한 '고도로 진화된' 관행을 도입하려는 목표를 추구했다[9].

본 기술 활용 제안의 전제 조건은 다음과 같다.

1. 블록체인의 블록을 생성하고 저장하는 영역(Blockchain Storage)의 접근은 스마트계약을 통해서만 가능하다.
2. 스마트계약을 통해 자동 실행된 결과 값은 별도의 저장소(SCORE Storage)에 최신정보를 기록하고, 블록체인의 저장공간(Blockchain Storage)에 이력정보를 기록한다.
3. 스마트계약 실행결과를 기록하는 저장소(SCORE Storage)의 접근은 스마트계약을 통해서만 가능하다.
4. Fig. 1.과 같은 구성이 가능한 블록체인 플랫폼에서만 적용 가능한 기술이다.



Fig 1. Blockchain Diagram

블록체인 저장소와 스마트계약, 그리고 스마트계약 저장소의 구성은 Fig. 2.와 같다. 스마트계약에서 사전에 약속된 작업이 수행되면 수행내역은 블록체인 저장소에 저장되고, 최종 수행결과 값은 스마트계약 저장소에 기록된다.

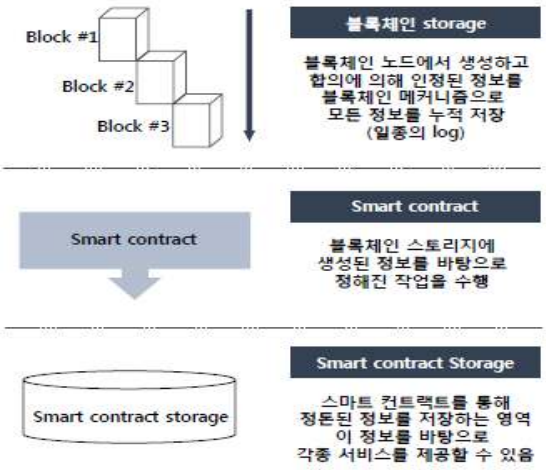


Fig. 2. Relationship of Storages and Smart Contract

개인정보의 삭제절차는 다음과 같다.

1. 특정 정보주체의 개인정보의 삭제요청을 받으면 스마트계약은 블록체인저장소에 삭제요청블록을 생성한다.
2. 이 블록에 의해 스마트계약이 자동으로 실행되어 블록체인저장소에는 삭제이력블록을 생성하고 스마트계약 저장소에서는 해당 개인정보를 완전 삭제 처리한다.

이렇게 되면 결과적으로 최종 결과 값을 저장하는 스마트계약저장소에는 삭제 요청된 정보주체의 개인정보는 모두 삭제되고 스마트계약에 의해 삭제 처리된 작업 내용은 블록체인저장소에 기록된다. 실제로는 블록체인저장소에 정보주체의 개인정보가 남아 있으므로 완전 삭제가 아니라고 볼 수 있지만 이 저장소의 접근은 스마트계약에 의해서만 가능하고 스마트계약의 접근은 스마트계약저장소에 있는 정보를 기준으로 이력조회를 할 수 있기 때문에 블록체인저장소에 남아 있는 개인정보는 쓸모없는 정보가 된다.

만약 블록체인저장소에 있는 정보까지 완전 삭제를 요구한다면 개별 정보의 삭제는 불가능하지만 특정 시점을 기준으로 그 이전의 블록들은 블록체인 체크아웃 기능을 통해 삭제하고자 하는 블록까지 해쉬 처리하여 하나의 블록으로 묶고 다음 블록을 새로운 제너시스 블록으로 지정한 후 새로 묶어서 생성한 블록을 완전 삭제하는 방식으로 삭제할 수도 있다.

V. 결론 및 발전 방향

5.1 결론

본 연구에서는 먼저 블록체인 기술의 두 가지 특징인 비가역성과 정보의 분산 공유를 살펴보고 이 특징들이 국내 개인정보 보호법제의 내용 중 개인정보의 삭제와 제3자 제공에 대한 사전 동의에 있어서 이해 상충되고 있음을 분석하였다. 이러한 내재적인 문제점이 국내 블록체인 기술의 상용화 서비스가 아직 많지 않은 이유와 연관성이 있음을 추론해 보았다. 또한 블록체인 기술과 개인정보 보호법제의 충돌을

피하기 위해 개인정보의 삭제와 제3자 제공에 대한 사전 동의 규정에 대한 개선방향을 제시하였다. 정보의 삭제가 불가능한 블록체인의 비가역성을 파괴하지 않으면서도 법적인 삭제의 의무를 할 수 있는 기술적 대안을 제시한 것도 신선한 접근이 될 수 있을 것이다.

본 연구를 통해 블록체인 기술의 장점을 최대한 활용할 수 있는 여러 다양한 비즈니스가 발굴되고 4차 산업혁명 시대에 맞는 국내 개인정보 보호법제의 개선방향이 꾸준히 논의되는 계기가 되기를 바란다.

5.2 연구의 한계 및 발전 방향

본 연구는 개인정보 보호법제의 개선방향만을 다루고 있다. 또한 스마트계약 기술을 응용한 개인정보의 삭제 방안도 여러 제약조건을 만족하는 기술구조에서만 가능하다는 것을 전제하고 있다. 따라서 법제에 대한 개선은 실제 관련 분야의 전문가들을 통한 보다 더 심도 있는 논의가 이어져서 본 연구에서 다루지 못한 여러 타 법에 관한 충돌 문제도 해결방안을 마련해 갈 수 있는 계기가 되기를 희망한다. 또한 스마트계약 기술을 이용한 블록체인 서비스의 다양한 시도도 꾸준히 이어져서 국내 블록체인 기술 환경이 4차 산업혁명 시대에 세계를 선도하는 장이 되기를 기대한다.

[참고문헌]

[1] Jung-kyoon Kim, Bo-kyung Kim and Yu-jin Lee, The Effects and Implications of Blockchain on Industry and International Trade, IIT TRADE FOCUS-2018-14, pp. 29, April, 2018.

[2] Jae-sung Kim and Seong-chul Lim, “A Study on Possibility of International Trade by using of Block Chain” The International Commerce & Law Review No.75, pp. 140, Aug, 2017.

[3] http://www.law.go.kr, Personal Information Protection Act Article 21, Credit Information Use and Protection Act Article 29, Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. Article 20-2

[4] http://www.law.go.kr, Personal Information Protection Act Article 17, Credit Information Use and Protection Act Article 32, Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. Article 24-2

[5] Chris Conley, The Right to Delete, 2010 AAAI(the Association for the Advancement of Artificial Intelligence) Spring Symposium Series, Palo Alto, California: AAAI Publications, pp. 54 (http://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1158/1482), 2010.

[6] Min-Yeong Lee, “So Called ‘Right to be Forgotten’ and Personal Data Protection.” A Collection of Law Treatises 20.1, pp.70, 2013.

[7] http://www.law.go.kr, Personal Information Protection Act Article 15

[8] Hun-Yeong Kwon, Sang-Pil Yoon and Seung-Jae Jeon, "Conceptual Review of PIR and its Legal Framework in the Age of Fourth Industrial Revolution," The Justice, pp. 34-35, Feb. 2017.

[9] Don Tapscott, Alex Tapscott, “The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World.” pp. 72, 83, 101, 127, May 2016.

공공의 이익을 위한 의료 빅데이터의 활용관련 법률 분석 및 의료법 개정(안)제시

한종찬, 박지환, 서정택

순천향대학교 정보보호학과

Analyze Laws Related to Utilization of Medical Big Data for the Public Interest and to Revise Medical Law

Jong-Chan Han, Ji-Hwan Park, Jung-Taek Seo

Department of Information Security Engineering, Soonchunhyang University.

요 약

의료 빅데이터란 건강데이터, 진료데이터 등과 같은 다양한 의료 관련 데이터를 수집, 저장, 분석해 유용한 정보를 제공하는 기술이다. 현재 건강상태를 진단 할 수도 있고, 과거 이력을 토대로 미래 건강상태를 예측하고 예방 방향을 제시한다. 하지만 학술, 연구, 통계 및 공공의 이익을 목적으로 의료 빅데이터를 수집, 저장, 활용하는데 있어 강력하게 규제하는 국내 법률 때문에 한계점이 존재한다. 그 한계점은 개인정보보호법과 의료법에서 존재하는데, 좁은 이용 및 제공 대상, 개인정보 비식별화 의무, 짧은 보관 기간 등이다. 본 논문에서는 공공의 이익을 위한 의료 빅데이터 활용를 저해하는 국내 법률(개인정보보호법, 의료법)과 해외 법률을 비교·분석하고 이를 해결하기 위해 특별법인 의료법 법률 개정(안)을 제시 한다.

I. 서론

인공지능, 사물인터넷, 빅데이터, 모바일 등 과학기술의 발달에 따라 4차 산업혁명 시대가 열리고 있다. 첨단 정보통신기술이 경제·사회 전반에 융합되는 4차 산업혁명 시대에 빅데이터는 경제·사회 발전의 큰 지표가 된다[1].

빅데이터란 기존에 없던 새로운 개념이 아니라 다양한 형식의 데이터가 축적되어 관계형 데이터베이스와 같은 기존의 데이터베이스로는 데이터의 저장·관리·분석의 허용 범위를 초과하는 대량의 데이터를 의미한다. 빅데이터는 여러 분야에서 활용되고 있는데, 그 중 의료분야에서의 빅데이터 활용이 주목받고 있다[2].

의료 빅데이터란(Medical Big Data)란 건강정보, 진료정보 등과 같은 다양한 의료 관련 데이터를 수집, 저장, 분석해 유용한 정보를 제공하는 기술이다. 의료정보의 종류로는 상병, 수술·처치 및 의약품 처방·조제 데이터, 생산·수입·사용 등 의약품 유통 정보, 의약품 인·허가 정보, 부작용 등 의약품 안전정보, 마약류 등 집중관리 의약품 융합 데이터, 의료기관의 인력·시설장비 정보, 의료기기정보, 의료처치용 치료재료 정보 등의 의료자원 데이터와 환자의 생체 데이터가 있다[3].

현재 의료정보를 통해 다양한 통계 자료, 의료서비스, 인공지능(Artificial Intelligence)과 결합한 헬스케어 제품 연구·개발이 진행되고 있다. 이처럼 의료 빅데이터의 활용과 발전 가능성은 무궁무진하다. 하지만 의료 빅데이터를 이용·제공함에 있어서 법률상 한계가 존재한다. 국내의 엄격한 규제를 하고 있는 개인정보보호법제와 의료법제가 의료 빅데이터 활용을 저해하고 있다.

본 논문에서는 의료 빅데이터의 필요성과 공공의 이익을 위한 의료 빅데이터 수집, 저장, 활용을 규제하는 국내 법률과 해외 법률을 비

교·분석하고 이를 해결하기 위한 관련 법률 개정(안)을 제시한다.

II. 국내 의료 빅데이터 제공 현황

국내에서 의료 빅데이터를 수집 혹은 제공 받는 방법으로는 환자에게 직접 동의를 얻고 수집·이용·제공하는 방법과 건강보험심사평가원(이하 심평원)에서 제공하는 '보건의료 빅데이터개방시스템'(opendata.hira.or.kr)을 이용하는 방법이 있다.

첫 번째 방법은 가장 확실하고 법률상 문제가 생기지 않는 방법이지만 의료기관 종사자가 아닌 경우에는 환자에서 접근하기 어렵고 다양하고 많은 데이터 수집이 불가능하다.

두 번째 보건의료 빅데이터개방시스템을 이용하는 방법은 건강보험심사평가원의 다량의 데이터를 받아 효과적으로 활용 할 수 있다. 보건의료 빅데이터개방시스템은 건강보험심사평가원이 보유한 공공데이터를 개방하는 시스템이며, 공공데이터(데이터셋, Open API), 의료 빅데이터 분석(빅데이터센서), 의료통계분석(질병, 의약품, 의료기관) 등을 제공한다[3].

하지만 국내 보건의료 빅데이터개방시스템 서비스는 한계가 존재한다. 제공하는 데이터는 건강검진 결과이거나 보험 청구용 데이터로 제공되어 특정 질환을 연구하기 위한 상세한 의료정보가 없다는 점이다[4]. 상세한 의료정보가 없다면, 예를 들어 질병을 진단하는 장비를 제작할 때, 진단 정확도가 낮아질 수 있다. 또한 공공데이터는 영리 목적의 이용을 포함한 누구나 이용 할 수 있지만 빅데이터센터분석 서비스는 아래 [표 1]에 해당하지 않는 자는 이용 할 수 없다는 제한점이 존재한다[3].

[표 1] 보건의료 빅데이터개방시스템 제공 대상 [3]

연구 자료	산업체 자료
- 국가, 지방자치단체 및 정부 산하기관 - 연구 중심 병원 및 학술 연구 수행기관 등	- 의약품 품목 허가를 받은 자 - 제약 의료기기 산업 - 컨설팅 회사 및 예비 창업자 등

III. 국내 의료 빅데이터 활용관련 법률 현황 및 문제점

국내 의료 빅데이터를 활용하기 위해서 정보의 수집은 필수적이며 이를 위해 필요한 법률로는 개인정보보호법과 의료법을 예로 들 수 있다. 의료법은 특별법이고 개인정보보호법은 일반법으로 의료법에 특별한 규정이 없는 경우에는 개인정보보호법을 따른다. 데이터의 수집 및 제공과 관련된 부분은 의료법에서 따로 규정하고 있지 않아 개인정보보호법에 의해 규제되는데 개인정보보호법의 강한 규제 때문에 정보를 대량으로 수집해야하는 빅데이터 활용에 문제가 발생한다. 3장에서는 국내 개인정보보호법과 의료법의 현황 및 문제점을 다룬다.

3.1 개인정보보호법의 의료 빅데이터 활용 관련 법률 현황 및 문제점

국내 개인정보보호법은 수집, 이용, 제공, 보관기간 등 규제가 심해 의료 빅데이터 활용에 가장 걸림돌이 되는 법이다. [표 2]는 개인정보보호법 제2조 1항으로 다음과 같다.

[표 2] 개인정보보호법 제2조 1항

> "개인정보"란 살아있는 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.

해당 법률에서 개인정보는 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있으면 개인정보가 되는 것인데 이는 개인을 알아볼 수 없도록 만든 정보들도 모두 개인정보가 될 수 있다는 뜻으로 해석될 수 있다[5]. 해당 법률은 [표 3]과 충돌하여 모순이 되는 법률이다.

[표 3] 개인정보보호법 제18조 2항 4호

> 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우

개인정보처리자는 해당 호의 경우 정보주체

또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제 3자에게 제공할 수 있다. 하지만 해당 호는 “특정 개인을 알아볼 수 없는 형태로 제공할 경우” 즉, 비식별처리를 한 정보 이므로 개인정보보호법 제2조(정의) 1항과 모순이 된다. 예를 들어 환자의 생체데이터를 이용하여 헬스케어 제품을 개발하려고 할 때 개인정보보호법 제18조 2항 4호에 의거하여 생체데이터를 제외한 이름, 성별, 나이 등을 비식별화 처리를 거친 데이터라도 사는 곳, 전화번호 등 어느 하나의 데이터가 결합 된다면 개인정보보호법 제 2조(정의) 1항에 의거하여 개인정보로 성립 한다. 또한 비식별정보는 18조 2항 4호의 목적을 제외하고 불특정 다수에게 공개하는 것은 식별 위험성이 있다고 판단하여 규제하고 있다[7]. 보건의료정보의 경우 다른 정보와는 달리 개인별 맞춤 건강예측이나 보건의료서비스 등을 제공하기 위해서는 개인식별화가 전제되어야 한다. 하지만 비식별정보로 인해서 의료정보를 수집하더라도 활용 또한 쉽지 않은 상황이다[5]. 또한 파기에 대한 문제점도 있다. [표 3]은 개인정보보호법 제21조 1항으로 다음 같다.

[표 4] 개인정보보호법 제21조 1항

개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.

국민건강보험공단에서는 국민의 자신 및 진료내역 등과 관련해 약 2조건의 정보를 보유한 만큼, 이를 바탕으로 의료 빅데이터 활용 사업을 추진해 나가겠다고 밝혔다[6]. 또한, 의료 빅데이터와 지역사회 의료자원을 연계해 건강수명 향상을 위한 전국민 맞춤형 건강관리를 하겠다고 설명했다[6]. 이처럼 국민들에게 맞춤형 건강관리를 하기 위해서는 데이터가 많을수록 효과적이고 지속적으로 필요하게 되는데 보유기간의 경과, 목적 달성 등 지체 없이 파기해야하는 개인정보보호법에 부합하지 않다.

3.2 의료법의 의료 빅데이터 활용 관련 법률 현황 및 문제점

국내 의료법은 정보의 수집이나 이용, 제공에 대한 내용을 규제하고 있지 않으며 제21조의 29항에는 진료기록전송지원시스템의 구축·운영에 관하여 이 법에서 규정된 것을 제외하고는 「개인정보 보호법」에 따른다. 라고 명시되어 있다. 하지만 의료 빅데이터의 활용을 위해서는 개인식별이 필요한 정보의 수집이 불가피하고 정보의 제공이 자유롭게 이루어질 필요가 있으므로 개인정보보호법으로 정보의 수집이나 이용, 제공 등을 규제하는 것은 문제가 된다. 또한 의료법 조항에서도 문제가 되는 부분이 존재한다. [표 5]는 의료법 제21조 2항과 3항으로 다음과 같다.

[표 5] 의료법 제 21조 2항, 3항

법령	내용
의료법 제 21조 2항	의료인, 의료기관의 장 및 의료기관 종사자는 환자가 아닌 다른 사람에게 환자에 관한 기록을 열람하게 하거나 그 사본을 내주는 등 내용을 확인할 수 있게 하여서는 아니 된다.
의료법 제 21조 3항	제2항에도 불구하고 의료인, 의료기관의 장 및 의료기관 종사자는 다음 각 호의 어느 하나에 해당하면 그 기록을 열람하게 하거나 그 사본을 교부하는 등 그 내용을 확인할 수 있게 하여야 한다. 다만, 의사·치과의사 또는 한의사가 환자의 진료를 위하여 불가피하다고 인정한 경우에는 그러하지 아니하다.

의료법 제21조 2항을 보면 환자가 아닌 경우 환자에 관한 기록을 확인할 수 없지만 3항의 어느 하나에 해당할 경우 내용을 확인할 수 있도록 명시되어있다. 하지만 3항의 각 호에서도 공공의 이익을 위한 의료 빅데이터의 열람을 허용하도록 하는 내용은 정의되어 있지 않다. 이처럼 의료법에서도 의료 빅데이터의 활용을

위한 법률이 정의되어있지 않다.

Ⅳ. 국외 의료 빅데이터 활용 관련 법률 현황

국외에서는 의료 빅데이터를 활용하기 위해 효과적인 법률을 지속적으로 재정하고 있다.

2015년 국내 빅데이터 시장 현황을 봤을 때 국내기술 수준은 선진국 대비 62.6%로 수준 격차가 3.3년이 난다고 밝혔다[8]. 이와 같이 현재 국내기술 수준이 국외에 비해 격차가 벌어져 있으며 빅데이터 시장을 국내에서 활발하게 활용하지 못하고 있다는 사실이다. 4장에서는 미국, 영국의 관련 법률을 알아본다.

4.1 미국의 의료 빅데이터 활용 관련 법률 현황

미국은 개인정보보호에 관하여 개별 산업 영역 별로 개인정보보호를 규정하고 있는데 의료정보는 연방법 차원의 HIPPA(Health Insurance Portability and Accountability Act)의 Privacy rule에서 주로 규정하고 있다[9]. HIPP의 적용 대상으로는 의료보험회사, 의료인, 결제기관 등에 대하여 적용되며, 위 적용 대상자에 대해 의료정보의 활용이나 공개에 관련된 업무를 제공하는자 역시 적용된다[10]. HIPPA의 정보보호 규정은 “전자, 서류, 구두 등 형태를 불문하고 의료인 등이 보유하거나 전송하는 개인식별이 가능한 의료정보 일체”를 보호대상으로 규정하며 이를 PHI(Protected Health Information)라고 정의한다[10]. HIPPA 정보보호 규정을 보면 의료인 등은 정보주체의 승인이 없는 경우에 예외적으로 치료, 보험혜택 제공, 법에 의해 요구되는 경우 등에는 PHI를 이용하거나 공개할 수 있다[10]. 또한 16개 종류의 식별인자를 제거한 상태인 “제한된 정보군”이라는 개념을 정의하여 연구, 의료 시스템 운영, 공공 의료 목적 등에 이용될 수 있도록 허용하였다[10]. HIPPA는 비식별정보를 별도로 정의하며 비식별정보의 이용 및 공개에 관하여 규제를 하지 않는다[10].

4.2 영국의 의료 빅데이터 활용 관련 법률 현황

영국에서 환자의 관련 정보는 원칙적으로 제3자에게 공개될 수 없으나, 환자가 자신의 정보가 어떻게 사용되는지 알고 정보공개에 동의를 한 경우나 공공의 이익을 위해 필요할 경우, 법률상의 의무가 있을 경우에 개인정보의 공개가 가능하다[11]. 또한 개인정보의 처리는 생존하는 개인을 식별할 수 있는 정보의 처리에만 적용되며, 비식별 처리된 정보는 대상에서 제외된다[11]. 영국은 의료 정보에 대해서 연구 목적에 대해서는 보유기간에 제한이 없으며, 환자의 동의가 없어도 환자의 식별 가능 정보를 이용하여 역학적 연구를 하는 것이 가능하도록 정하고 있다[11]. 또한 의료, 복지 서비스의 증진, 혹은 국민 건강 증진의 이유를 위해서는 제 3자에게 제공할 수 있다. [표 6]은 국내 관련 법률과 국외 관련 법률을 비교·분석한 표이다.

[표 6] 의료 빅데이터 관련 국내·외 법률 비교

분류	대한민국	미국	영국
의료 정보 이용·제공	통계작성 및 학술연구 등의 목적을 위하여 개인을 알아볼 수 없는 정보로 제공 가능	연구, 의료 시스템 운영, 공공 의료 목적 등을 위하여 이용가능	환자의 식별 가능 정보를 이용하여 역학적 연구가 가능하며 의료, 복지서비스의 증진, 국민 건강 증진의 이유를 위해서 제 3자에게 제공 가능
비식별 정보의 이용·제공	통계작성 및 학술연구 등의 목적 외에는 식별 위험성이 있다고 판단하여 규제	규제하지 않음	규제하지 않음

[표 6]과 같이 국내법률에 비해 국외법률에서 규제를 완화하여 공공의 이익을 위한 의료 빅데이터의 활용을 적극 지원하고 있다. 추가로, 영국의 경우 의료 정보의 보유기간은 연구 목적일 경우에 제한을 두지 않는다.

V. 의료 빅데이터 활용을 위한 의료법 개정(안)제시

제 3장과 4장에서는 국내 법률 현황과 해외 법률 현황에 대해 알아보았다. 국내 법률에서는 이용 및 제공 대상, 비식별화 의무, 짧은 보관기간과 같은 요인으로 인해 의료 빅데이터 활용을 저해하고 있다.

의료정보는 식별 가능한 데이터가 가치가 높다는 특징이 있으나, 이를 개인정보보호법에 적용하면 다른 개인정보보호 사례들과 충돌 할 가능성이 높다. 예를 들면 개인정보보호법 제18조 2항 4호에서 비식별화 과정을 삭제한다면, 식별화 된 데이터가 필요 없는 연구 및 통계작성에 사용되어 개인프라이버시보호가 저해 될 수 있다. 또한, 개인정보보호법에서 보관기간을 늘린다면 다른 목적에서 불필요한 정보가 유출되는 사고가 발생 할 수 있다. 그러므로 일반법 개인정보보호법을 수정하기보다는 특별법 의료법을 수정하는 방향으로 흘러가야한다. 의료법은 특별법으로 특별한 규정이 있는 경우 개인정보보호법보다 우선적으로 적용되기 때문이다. 기존 법률에서 생기는 문제점은 아래 [표 7]과 같다.

[표 7] 기존 법률의 문제점 및 해결방안

기존 법률	문제점	해결 방안
개인정보보호법 제18조(개인정보의 목적 외 이용·제공제한) 2항 4호	비식별화된 의료정보는 가치를 잃을 수 있고, 제공 대상이 한정적이다.	이용 및 제공대상을 확대하고, 이용 및 제공 할 경우 비식별화를 원칙으로 하되 필요한 경우에는 식별화된 데이터도 가능하도록 한다.
개인정보보호법 제21조(개인정보의 파기) 1항	의료 빅데이터 이용을 위한 데이터를 장기간 보존하지 못한다.	연구·학술·통계 및 공공의 이익을 위한 데이터의 보존 기간을 연장한다.
의료법 시행령 제 15조(진료기록부 등의 보존)		

[표 7]의 문제점에 대한 구체적인 개정(안)은 [표 8], [표 9]와 같다.

[표 8] 의료법 의료정보 관련 개정(안)

> 제 N조(의료정보 이용 및 제공)
> ① 의료기관은 환자의 데이터를 동의 받지 않더라도 연구·학술·통계 목적 또는 공공의 이익을 위해 필요한 경우 수집·이용·제공 할 수 있다.
> ② 의료기관은 제 3자에게 데이터를 제공 할 경우 비식별화 된 형태로 제공하여야 한다. 다만, 연구, 학술, 통계목적 또는 공공의 이익을 위해 필요한 개인 식별 가능한 정보의 경우 기술적, 관리적, 물리적 보호조치를 취한다.

[표 6]은 본 논문에서 새로 제시하는 개정안이다. 1항은 기존 법률에서 동의 없이 이용 및 제공 할 수 있는 대상을 '연구 및 통계작성'에서 공공의 이익을 위함으로 확대시켰다. 현행 법률에서는 연구 및 통계 작성의 목표를 충족하려면 관련기관에서 진행되어야 한다. 이를 공공의 이익으로 범위를 확장시켜 관련 기관이 아닌 개인, 소규모 단체까지 이용 할 수 있다. 2항은 기존 법률과 동일하게 비식별화를 기본으로 하되, 전송·보관 과정에서 기술적, 관리적, 물리적 보호조치를 취하면 식별화 된 데이터도 이용·제공 할 수 있다.

[표 9] 의료법 시행령 제 15조(진료기록부 등의 보존) 개정(안)

> ① 의료인이나 의료기관 개설자는 법 제22조 제2항에 따른 진료기록부등을 다음 각 호에 정하는 기간 동안 보존하여야 한다. 다만, 계속적인 진료를 위하여 필요한 경우에는 1회에 한정하여 다음 각 호에 정하는 기간의 범위에서 그 기간을 연장하여 보존할 수 있다.
> **② 연구·학술·통계 및 공공의 이익을 위하여 필요한 경우에는 목적 달성까지 무기한 연장한다.**

기존의 의료법 시행령 제 15조(진료기록부 등의 보존)에서 2항을 추가한다. 기존 법률에 따르면 진료기록부 등은 각 호에 해당하는 기간만큼 저장 할 수 있고, 계속적인 진료를 위함에 따라서만 연장이 가능하다. 즉, 2년에서 10년까지의 데이터만 수집이 가능하다. 데이터의 양이 많을수록 효과적인 빅데이터에 적용하기에는

한계가 있는 법률이다.

추가한 2항은 보관기간을 목적 달성까지 무기한 연장 할 수 있다. 이로서 개인정보보호법 제21조(개인정보의 파기), 의료법 시행령 제 15조(진료기록부 등의 보존) 기존 법률의 한계를 보완 할 수 있다.

VI. 결론

본 논문에서는 공공의 이익을 위한 의료 빅데이터의 필요성 및 국내·외에 관련 법률을 비교·분석하였다. 또한 국내 개인정보보호법의 정보의 수집, 저장, 활용에 대한 강한 규제로 의료 빅데이터 활용이 저해되는 문제점을 제시하였고 의료 빅데이터의 활용을 위해 데이터의 수집, 저장, 활용은 활발하게 이루어져야하므로 의료법에 의료정보의 수집, 저장, 활용에 대한 규제를 완화하도록 하는 개정(안)을 제시하였다. 개인정보보호법보다 우선인 의료법에 개정(안)을 제시함으로써 공공의 이익을 위한 의료 빅데이터에 필요한 의료 정보의 자유로운 이용 및 활용이 가능하도록 하였다. 하지만 개인식별 가능한 정보의 경우 강력한 규제가 필요하므로 개인식별정보의 활용에 대한 제한은 여전히 존재한다. 본 논문을 통해 의료 정보의 다양한 활용으로 국내의 의료 빅데이터 시장이 활성화 되어 연구, 학술등 공공의 이익을 위한 활동이 활발해질 것을 기대하며 향후 연구방향으로는 식별화 된 데이터의 유출 및 해킹을 막기 위한 기술적, 제도적인 연구와 더불어 더 많은 국외 법률을 비교 분석하여 개인식별정보에 대한 활용도를 높일 수 있는 추가적인 연구가 필요할 것이다.

[참고문헌]

[1] 한국정보통신기술협회, IT용어사전 '4차 산업혁명' (word.tta.or.kr)

[2] 조한범, 의료분야 빅데이터 활용을 위한 규제 현황 고찰 및 개선방향 연구, 동국대학교대학원 의료기기산업학과, (2018)

[3] 건강보험심사평가원, 보건의료빅데이터개방시스템(opendata.hira.or.kr)

[4] 남두현, ""보험 청구용"인 헬스케어 빅데이터, 연구 활용 한계", 2017.08.02.

[5] 정명진, 헬스케어 산업발전을 위한 의료빅데이터 활성화 정책, 한국경영학회 통합학술발표논문집(2017)

[6] "국민건강보험공단, 평생건강, 국민행복 등 2025 뉴 비전 준비", 국민일보, 2016.03.29

[7] 노명선, "개인정보 비식별 조치, 세계 각국은 어떻게 하고 있나요", 보안뉴스, 2017.09.20.

[8] 안하늘 기자, "프라이버시 시대는 끝났다"... 빅데이터 시대 이끌 비식별화, 아시아경제, 2016.07.31.

[9] 정현학, 장보은, "보건의료 빅데이터 관련 각국의 법체계", 한국보건산업진흥원, 2015.12.21.

[10] 이영주, "미국 의료정보보호법(HIPPA)의 주요 내용", 법무법인(유)원 뉴스레터 10월호

[11] 장성재, "보건의료 빅데이터 관리시스템 최신 동향", BRIC VIEW 2017-T07, 2017.03.21.

[12] 손영주, 공공보건의료 빅데이터의 민간활용 및 개인정보보호 관련 법제에 대한 연구, 고려대학교 법무대학원 (2016)

[13] 법제처, 의료법 (www.law.go.kr)

[14] 법제처, 개인정보보호법 (www.law.go.kr)

2018 한국정보보호학회 하계학술대회

C4 관리정책교육 4

장 항 배 (중앙대학교)

- **국내외 정보보호제품 도입정책 동향 분석 및 수준 비교 연구**
  손효현, 김광준, 오형근, 이만희
- **UAV 편대를 위한 그룹 리더 기반의 효율적인 보안 그룹 관리 기법**
  김승민, 최문원, 이우엽, 계동욱, 조인휘
- **FAIR에 기반한 기업 정보유출사고시 발생하는 법적배상비용의 통계적 검정을 통한 산출**
  최상원, 유영인, 이경호

국내외 정보보호제품 도입정책 동향 분석 및 수준 비교 연구

손효현*, 김광준*, 오형근**, 이만희*

*한남대학교 컴퓨터공학과, **국가보안기술연구소

Comparative Study of the Policy Trends for Introducing Domestic/International IT Products

Hyo-Hyun Son*, Kwang-Jun Kim*, Hyung-Geun Oh**, Man-Hee Lee*

*Department of Computer Engineering, Hannam University.
**National Security Research Institute

요 약

사이버공격이 전 세계적으로 확산됨에 따라 중앙 행정기관 및 국가 기관에서 다양한 정보보호 제품을 설치·운영하고 있다. 이러한 정보보호제품의 보안기능을 검증하고, 국가정보보호 수준을 제고하기 위해 각국의 정부는 표준화된 공통평가기준을 통하여 도입하고자 하는 제품의 안전성을 평가하고 있으며 더 나아가 국가의 보안요구 사항에 맞는 보안성 검증 제도를 개발·운영하고 있다. 그에 따라 본 논문은 국내 보안적합성 검증과 선진국의 보안성 검증 제도의 동향을 파악하고 그 변화를 분석하였다. 본 연구는 한국의 보안적합성 검증 제도와 미국의 보안성 검증 제도인 CSfC 프로그램간의 비교 분석을 진행한 후, 국내 정책에 대해 보다 효율적인 개선방안을 제안한다. 본 연구는 궁극적으로 선진국의 정보보호제품 도입 관련 정책의 변화를 분석함으로써 세계 흐름에 맞는 국내 보안적합성 검증 제도 정책의 갱신 방안을 제시하여 국가정보통신망의 보안수준 제고에 기여할 것으로 기대한다.

I. 서론

정보통신기술의 비약적인 발전과 네트워크 인프라 확충을 통하여 전 세계를 인터넷망 하나로 엮는 정보사회가 형성되었다. 그러나 정보통신기술 발전과 맞물려 인터넷을 통한 개인정보 및 기밀자료 유출, 해킹 등과 같은 사이버공격이 전 세계적으로 확산되고 있다[1]. 이러한 문제점을 해결하기 위해 각 기관은 다양한 정보보호제품을 도입하여 구축, 운영하고 있다. 따라서 보안요구사항에 적합한 제품을 도입하기 위해 공인된 제품 안전성 평가 및 인증이 요구되고 있다.

그에 따라 각국은 공통평가기준(CC, Common Criteria)을 통하여 도입하고자 하는 제품의 안전성을 평가하고 있으며[2], 추가적으로 각국의 환경에 맞는 평가 및 인가기준을 통해 제품의 신뢰성을 확보하고 국가 정보보호 수준을 제고하고 있다[3]. 국내의 경우 IT보안인증사무국을 중심으로 IT제품을 평가·인증하고 있으며, 추가적으로 중앙행정기관 및 광역시·도 교육청, 주요 정보통신기반시설 관리기관에 도입되는 정보보호제품 및 네트워크 장비 등은 국가정보원을 중심으로 보안적합성 검증 및 보안기능 시험결과서 발급제도를 통하여 국가·공공기관에 도입되는 정보보호시스템의 안전성을 검증하고 있다[4].

본 논문은 2장에서 국내 IT제품 도입정책을 소개하며, 3장에서는 미국의 IT제품 도입정책에 대해 소개한다. 4장에서는 국내·외 정보보호제품 도입정책에 대해 비교 분석하고 5장에서는 더 나은 정책 개선방안을 제안하며 결론을 맺는다.

II. 국내 IT제품 도입정책

정보보호제품의 보안기능을 검증하고 국가 정보보호 수준을 제고하기 위해 정부는 정보보호제품의 객관적이고 공정한 평가 시스템을 필요로 한다. 따라서 국가·공공기관 대상으로 안전성과 신뢰성이 검증된 정보보호제품 공급 및 이용 촉진을 위해 국가정보원과 과학기술정보통신부에서 법에 근거한 정보보호시스템 평가·인증 제도 및 보안적합성 검증 제도를 시행하고 있다.

2.1 CC 평가·인증

정보보호시스템 평가·인증제도는「국가정보화 기본법」제38조 및「국가정보화 기본법 시행령」제35조에 의거하여 상용 IT제품에 보안기능이 포함되어 있을 경우 제품의 보안성을 평가하고 그 결과를 보증하는 제도이다. 국제표준으로 제정하고 국제상호인정협정 (CCRA, Common Criteria Recognition Arrangement) 회원국이 사용하는 공통평가기준 (CC, Common Criteria) 및 공통평가방법론(CEM, Common Evaluation Methodology)을 국내 CC 인증의 평가기준 및 평가방법론에 공통으로 사용하고 있다[5]. 현재 CCRA에서 승인한 최신 버전은 CC V3.1 R5 및 CEM V3.1 R5이며, 국내용 CC인증은 CC V3.1 R2 및 CEM V3.1 R2를 적용하고 있다[6].

CC평가·인증 제도는 정보보호제품에 구현된 보안기능이 평가 신청한 평가보증등급 수준에 부합하는지 검증함으로써, 도입기관이 보안요구사항을 충족하는 정보보호제품을 선택할 때 도움을 주는 것에 제도운영 목적을 가지고 있다. 따라서 국가·공공기관에 정보보호시스템을 납품하기 위해 해당 제품은 국가용 보안요구사항을 모두 만족하고, 구현되어있는 모든 보안기능에 대한 취약점 여부를 검증 받을 경우 주관기관인 IT보안인증사무국으로부터 국내용 CC인증서를 발급 받을 수 있다.

2.2 보안적합성 검증 제도

보안적합성 검증 제도는 국가·공공기관에

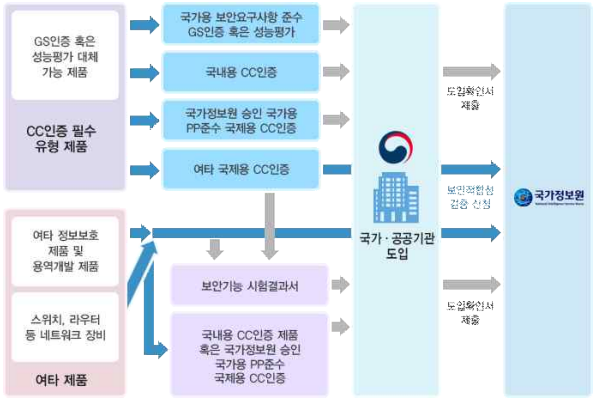


Fig. 1. 정보보호시스템 국가·공공기관 도입절차[4]

도입되는 정보보호시스템의 안전성을 검증하기 위해「전자정부법」제56조 및「공공기록물 관리에 관한 법률 시행령」제5조에 의거하여 국가정보통신망의 보안수준을 제고하고 발생 가능한 사이버 위협에 대응하기 위한 검증 제도이다[4]. 중앙행정기관 및 광역시·도 교육청, 주요 정보통신 기반시설 관리기관에 정보보호제품 및 네트워크 장비 등 정보통신시스템 도입 시 주관기관인 국가정보원에 보안적합성 검증을 신청해야 하며, 도입 기관은 검증결과 발견된 취약점을 제거한 후 운영하여야 한다.

보안적합성 검증을 포함한 전반적인 국내 IT 제품 도입절차는 Fig.1과 같다. 국가정보원은 도입기관으로부터 보안적합성 검증 신청을 받은 후, 국가보안기술연구소에 보안적합성 검증에 대한 시험을 의뢰한다. 국가보안기술연구소는 의뢰받은 정보보호시스템에 대하여 자체 검증을 완료한 후 그 결과를 국가정보원에 제출한다. 국가정보원은 제출받은 검증 결과를 도입기관에 통보하고, 결과를 통보받은 도입기관은 발견된 취약점을 보완한 후 정보보호시스템을 운용한다[4].

보안적합성 검증은 자체기준에 따른 시험을 통해 취약점을 사전에 발견하고 보완함으로써 제품에 대한 보안수준을 제고하는데 그 목적을 가진다. 이때, 국가정보원에서 승인한 국가용 보안요구 사항을 만족하거나, 국내용 CC인증을 받은 제품은 보안적합성 검증 절차를 생략가능하다. 하지만 국제용 CC인증을 받은 제품은 국내 공공기관에서 요구하는 보안 요구사항과 다

른 요구사항으로 CC인증을 받았을 수 있고, CC평가・인증을 받지 않은 제품을 사용하고자 할 경우 안전성을 보장할 수 없으므로 국내 보안규격에 맞추어 보안적합성 검증을 이수해야 한다[7].

국가정보원은 보안적합성 검증을 받은 동일한 제품을 다른 국가・공공기관에 도입하고자 할 경우, 보안적합성 검증 신청 중복에 따른 비효율성을 제거하기 위해 2017년부터 '보안기능 시험결과서' 제도를 추가 운영하고 있다. 보안기능 시험결과서는 보안적합성 검증제도의 일부로써 시험기관이 국가정보원의 검증기준에 따라 정보보호제품의 보안기능 만족 및 구현 여부 등에 대하여 시험결과를 작성한 문서이다[8]. 이 문서는 신청기관(업체) 보관용 및 도입기관 제출용으로 구별하여 발행된다. IT제품 개발업체는 보안기능 시험결과서를 사전에 발부받을 경우 기존의 보안적합성 검증 대비 시간 효율적으로 제품을 국가・공공기관에 도입 가능하다.

III. 미국 IT제품 도입정책

미국 연방정부 및 연방기관, 국가 주요기반시설을 운영하는 기관은 미국 국가안보시스템(NSS, National Security System) 도입에 있어 국가안보시스템위원회(CNSS, Committee on National Security Systems)의 정책에 따라, 국가안보국(NSA, National Security Agency)이 인정한 정보보호제품 도입을 의무화 하고 있다.

3.1 CCEVS 평가・인증

CCEVS(Common Criteria Evaluation and Validation Scheme)는 미국 국내용 CC인증 스킴으로써 정보보호제품의 기밀성, 무결성 등 보안기능의 안전성 및 신뢰성을 검증하는 프로그램이다[9]. CCEVS 평가・인증제도는 상용제품(COTS, Commercial-Off-The-Shelf)을 국가안보시스템에 도입하는 과정에서 사용되는 1차 인증 절차이다. CCEVS 평가・인증제도를 통하여 제품을 도입하기 전 보안성을 검증함으로써 상용제품의 시스템 및 네트워크에 대한 안전성과 신뢰성을 높이는 것에 목적을 가진다.

CCEVS 평가・인증제도의 주관기관은 국가정보보증협회(NIAP, National Information Assurance Partnership)로 국립표준기술연구소(NIST, National Institute of Standards and Technology)와 NSA가 공동 설립한 미국 CC인증기관이다. 인증기관은 NIAP에서 개발·승인한 보안규격인 PP(Protection Profile)를 기반으로 제품의 평가・인증을 수행한다[10].

3.2 CNSSP

미국 연방정부 및 연방기관은 안전성 및 보안성에 대해 검증 받은 상용정보보호시스템 및 정부정보보호시스템(GOTS, Government-Off-The-Shelf)을 국가안보시스템에 도입하도록 정책적으로 의무화 하고 있다. CNSSP #11은 CNSS의 주체로 상용정보보호시스템 및 정부정보보호시스템의 정보 보증 획득을 위한 평가 프로세스를 제시하며 상용제품을 국가안보시스템에 도입할 때 적용한다[11]. 해당 정책은 정보 보증 획득 및 정보 보증 인증을 받은 정보보호시스템을 관리하기 위한 국가 정책이다. 이때, CNSSP #11의 적용범위는 국가 핵심 인프라를 운영하는 연방정부 및 연방기관, 국가 주요기반시설로 한정한다.

정보 보증 획득 및 정보 보증 인증을 받은 정보보호시스템의 보안 관련 기능이 보증된 내용에 따라 수행이 되는지 확인해야하며, 보안평가가 반복 가능해야하고 테스트 가능한 결과를 산출 할 수 있도록 보장해야하는 목적을 가진다. 이에 따라 도입 절차에 따른 보안요구사항을 준수하기 위하여 정책 및 관련 프로세스의 숙지가 필요함을 강조한다.

3.3 CSfC 프로그램

CSfC(Commercial Solutions for Classified Program) 프로그램은 국가안보시스템에 기밀정보를 취급하는 제품을 도입할 경우 요구되는 보안규격의 적합 여부를 검증하는 제도이다[12]. 이 프로그램은 NSA가 주관하여 상용제품을 국가안보시스템에 도입하는 과정에서 CC인증 다음으로 진행하는 2차 인증 절차이다. 개발업체

는 기밀정보를 취급하는 국가안보시스템에 사용될 상용제품을 만들 때, CSfC 검증을 받기 위해 PP 보안규격에 따라 CC인증을 사전에 받아야한다[13].

CSfC 프로그램의 보안규격으로는 CP(Capability Package)가 사용되며 NSA주체로 개발·승인되었다. CP는 시스템 군별로 Mobile Access, Campus WLAN, Multi-Site Connectivity, Data at Rest와 같이 4개의 기능 패키지 세트를 구성하여 대상 제품군의 추가 보안 요구사항 및 환경설정 요구사항을 명시하였다.

CSfC 프로그램을 통해 검증된 제품은 NSA와 합의각서(MOA)를 체결 후 CSfC 구성 요소 목록에 포함된다. CSfC 구성 요소 목록은 공급업체가 정부에 제품을 제공할 때 국가안보시스템의 정보를 보호하기 위해 시스템 군별로 분류된 제품의 기능을 선택하여 사용하도록 제공함에 목적을 가진다.

IV. 정보보호제품 도입정책 비교 분석

본 절에서는 국내의 보안적합성 검증 제도와 미국의 CSfC 프로그램 제도를 비교하여 국내 정책에 대한 개선방안을 제안한다.

Table.1은 두 제도에 대한 비교 분석 결과이다. 비교 항목으로는 주관기관, 신청기관, 적용대상, 평가기준, 보안규격으로 분류하였다. 비교결과 미국의 CSfC의 적용대상은 NSS에 도입되는 기밀취급용 정보통신 시스템으로 한정한다. 반면 국내의 보안적합성 검증 제도는 중앙행정기관에 도입하는 모든 정보보호제품 및 네트워크장비에 대하여 적합성 검증을 수행한다. IT 강대국을 지향하고 있는 대한민국의 특성상 거의 모든 업무가 IT를 활용하고 있는 특징과 사이버공격이 빈번한 점을 비추어볼 때, CSfC대비 모든 시스템에 대한 보안성을 검증하는 보안적합성 검증 제도는 우리나라의 상황에 더 적절한 것으로 판단된다.

추가적으로 미국의 CSfC 제도는 검증된 제품 및 검증항목을 홈페이지에 공개함으로써 제품

Table. 1. 보안성 검증 제도비교

	보안적합성 검증	CSfC
주관기관	국가정보원	NSA (국가안보국)
신청기관	중앙행정기관, 광역시·도 교육청, 주요정보통신 기반시설 관리기관	NSS 운영 도입기관
적용대상	정보보호제품, 네트워크장비	국가기밀취급용 정보통신시스템
보안규격	PP	CP, PP
평가기준	자체 평가 기준	CC인증 및 보안규격 만족 여부

을 도입하고자 하는 국가·공공기관에는 제품 선택의 정보를, 제품을 개발하는 업체에는 평가기준의 정보를 제공해준다. 따라서 우리나라의 보안기능 시험결과서 및 검증된 제품을 공개한다면 보다 나은 검증제도로 발전할 수 있을 것으로 판단된다.

또한, 보안규격 항목에서 보안적합성 검증 제도는 PP만을 보안규격으로 가지고 있으나, 미국은 CSfC 프로그램의 솔루션으로 활용되는 CP를 별도로 개발하여 보안규격으로 사용한다. CP의 구성요소는 PP의 보안요구사항에 충족되는 항목으로 이루어져 있다. 이러한 보안규격을 사용함으로써 더욱 체계적이고 독자적인 검증이 가능하다. 따라서 우리나라도 국내 보안요구사항에 적합한 독자적인 보안규격을 개발하고 표준화하는 것이 바람직한 것으로 판단된다.

마지막으로 평가기준 항목에서 미국 제도는 보안규격 기준인 CP와 PP를 공개 및 표준화하여 사용함으로써 공정성 및 보안성 향상을 꾀하고 있다. 보안적합성 검증 제도에서 사용 중인 자체 검증기준도 표준화하여 사용한다면 보다 나은 보안성을 얻을 수 있을 것으로 판단된

다.

V. 결론

전 세계적으로 정보보호제품에 대한 안전성 및 보안성 평가에 대한 중요성이 강조되고 있는 실정이다. 그에 따라 표준화된 공통평가기준에 국한되지 않고 각 국마다 환경에 맞는 추가적인 보안성 검증 제도를 개발하고 있다.

본 논문은 한국과 미국의 정보보호제품 도입 정책의 동향을 분석하고, 국내의 보안적합성 검증 제도와 미국의 보안성 검증 제도인 CSfC 프로그램을 비교하였다. 그 결과, 국내의 보안적합성 검증 제도의 적용대상은 미국의 CSfC와 달리 기밀정보 취급과 비기밀정보 취급 정보보호제품으로 분류하지 않고, 중앙행정기관에 도입되는 모든 제품을 검증하므로 전반적으로 모든 주요 행정기관의 보안성이 상대적으로 더욱 우수함을 확인하였다.

마지막으로 보안기능 시험결과서의 검증된 제품 공개와, 국내 보안요구사항에 적합한 독자적이고 체계적인 보안규격을 표준화하고 투명하게 공개하는 것을 제안한다. 이 과정에 도입기관 및 개발업체, 관련 연구자들의 다양한 의견을 수렴한다면 더 명확하고 완전한 보안 규격으로 발전할 것으로 기대된다. 보안 규격이 표준화되면 보안적합성 검증에 필요한 기준을 명확히 할 수 있어, 소요 비용 및 시간을 절약할 수 있을 뿐 아니라, 보다 완전한 보안 규격을 통해 안전성 및 신뢰성을 확보하여 장기적으로는 국가정보통신망의 보안수준을 제고할 수 있을 것으로 기대한다.

향후 선진국의 정보보호제품 도입 관련 정책의 변화를 지속적으로 분석함으로써 국내 보안적합성 검증 제도 정책을 갱신하고, 필요시 검증 방안의 개선 방안을 도출하기 위한 체계적인 연구가 필요하다. 또한, 보안적합성 검증에 소요되는 시간 및 인력의 효율성을 증명하기 위해 각국의 보안성 검증에 소요되는 비용 및 시간을 비교·분석할 예정이다.

[참고문헌]

[1] KISA 임진수, “사이버 위협 인텔리전스가 선정한 7대 사이버 공격 전망”, Dec, 2016.

[2] 백남균, 손민우, 김재성, “국외 인증서발행국 CC 기반 정보보호제품 평가 동향”, Dec, 2009.

[3] 이대섭, 홍원순, “국내 평가·인증 정책의 현황 및 향후 추진방향”, Dec, 2007.

[4] 국가정보원, “보안적합성 개요 및 체계”, “http://www.nis.go.kr/AF/1_7_2_1.do”.

[5] 한국정보보호진흥원, “정보보호시스템 평가·인증 가이드”, Dec, 2004.

[6] IT보안인증사무국, “정보보호제품 평가·인증(CC 평가·인증)은 어떤 제도입니까?”, “http://www.itscc.kr/bbs/list.do?board_class=4#faq.27”.

[7] 한성일, 지연희, 이강수, “보안 적합성 평가 방법론의 개선방안”, Jun, 2016.

[8] 국가정보원, “‘보안기능 시험결과서’발급 제도 시행 공지”, “http://www.nis.go.kr/AF/1_7_2_3/view.do?seq=66”, Mar, 2018.

[9] National Information Assurance Partnership, “What is NIAP/CCEVS?”, “https://www.niap-ccevs.org/Ref/What_is_NIAP.CCEVS.cfm”.

[10] National Information Assurance Partnership, “Approved Protection Profiles”, “https://www.niap-ccevs.org/Profile/PP.cfm”.

[11] Committee on National Security System, “CNSSP Policy No.11 - National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products”, Jun, 2013.

[12] National Security Agency, “Commercial Solutions for Classified Handbook”, Nov, 2017.

[13] National Security Agency, “CSfC Frequently Asked Questions”, Nov, 2017.

UAV 편대를 위한 그룹 리더 기반의 효율적인 보안 그룹 관리 기법

김승민*, 최문원**, 이우엽**, 계동욱*, 조인휘*

*한양대학교 컴퓨터소프트웨어학과

**한양대학교 전자컴퓨터통신공학과

An Efficient Secure Group Management Scheme using Group Leader for UAV Squadron

Seungmin Kim*, Moon-Won Choi**, Wooyeob Lee**, Donguk Gye*, Inwhee Joe*

*Dept. of Computer Software, Hanyang University, Seoul Korea
**Dept. of Computer Science and Engineering, Hanyang University, Seoul Korea

요 약

본 논문은 UAV(Unmanned Aerial Vehicle) 편대를 위한 그룹 리더 기반의 효율적인 보안 그룹 관리 기법을 제안한다. UAV 편대 비행을 위한 그룹키를 생성하는 기법을 제안함으로써 UAV 편대의 보안을 유지하면서 동시에 UAV 자원을 효율적으로 사용할 수 있다. 먼저 UAV 편대의 각 리더는 멤버들의 공개키를 소유한다. 그룹의 가입/해제 절차에서 리더들 간의 통신을 통해 멤버들의 공개키를 전송한다. 최종 그룹의 리더는 수집한 공개키를 이용하여 세션키를 생성한다. 이후 전송 대상의 세션키 정보를 제외하고 각각의 그룹 매칭키를 생성한다 이 그룹 매칭키는 전송 대상에게 전송이 된 후 수신한 대상은 자신의 세션키를 포함하여 그룹키를 생성한다. 결과적으로 그룹의 리더를 사용하지 않는 방법과 비교하여, 그룹키가 생성되는 과정에서 연산량 및 전송 비용을 감소시킨다.

Abstract

This paper proposes an efficient secure group management scheme using group leader for UAV squadron. By proposing a scheme for generating a group key for UAV squadron, the UAV resources can be efficiently used and maintain the security of UAV squadrons. First, the members' public keys are transmitted through communication between the leaders in the group join/leave procedure. The leader of the last group generates the session key using the collected public keys. Then, each group matching key for members is generated excluding the session key information of the transmission object. After the group matching key is transmitted to the members, the members generate a group key including its own session key. Compared to the existing scheme, it reduces the computation & transmission cost in the process of generating group key.

Keywords: UAV, Squadron, Group key management, Diffie-Hellman key exchange, Elliptic-curve cryptography, Elliptic-curve Diffie-Hellman

I. 서론

UAV(Unmanned Aerial Vehicle)은 조종사가 탑승하지 않고, 원격 조종 또는 자동/반자동으로 비행하는 항공기이다. 드론(Drone)으로 불리기도 한다[1]. UAV는 군사 목적으로 연구되고

사용되었으나 최근 들어 민간 분야로 확대 되었다. 감시용, 연구개발용, 촬영용, 물류용, 통신용등 다양하게 연구, 개발 및 활용이 이루어지고 있다. 이에 따라 구글, 페이스북, 아마존 등 글로벌 IT 기업들이 UAV 산업에 뛰어들고 있다. 아마존은 2016년 12월 14일에 전 세계에서 처음으로 UAV를 이용한 물류 배송에 성공했다[2]. UAV의 단일 개체의 활용에서 더 나아가 UAV 편대를 이용하면 여러 이점들이 있다. 정찰의 임무에서 같은 시간에 더 많은 정보를 수집 할 수 있다. 물류 배송에서도 편대의 멤버들에게 물류의 무게가 분산되기 때문에 더 무거운 물류를 운송 할 수 있다. 또한 물류의 형태가 바람의 저항을 많이 받거나 단일 UAV로 운송하기 힘든 형태라면 UAV 편대를 이용하여 운송이 가능하다. 하지만 UAV 편대를 관리하기 위해서는 추가적인 기법들이 필요하다. 보안이 취약한 UAV 편대는 보안 취약 구간/지역에서 다수의 UAV가 공격 타겟이 되는 상황이 발생할 수 있다. 또한 UAV 편대의 유연한 변형과 빈번한 멤버교체에서 발생하는 자원 소모를 감소시키기 위한 가입/해제 절차가 필요하다.

본 논문에서는 UAV 편대를 위한 그룹 리더 기반의 효율적인 보안 그룹 관리 기법을 제안한다. 그룹의 가입 및 해제 절차가 그룹 리더에 의해서 중앙 집중형으로 수행되기 때문에 그룹 노드들의 직접 교환으로 갱신하는 분산형보다 키 교환 비용 및 그룹키 갱신 횟수가 감소한다. 이는 UAV 편대의 효율적인 비행과 보안 그룹 관리를 가능하게 한다.

II. 보안 그룹 관리 기법

2.1 Diffie-Hellman Key Exchange with ECC

그룹 관리는 효율적인 가입/해제 방법과 그룹 형성 후의 안정성의 두 가지 관점에서 접근할 필요가 있다. 일반적으로 그룹 내에서의 보안은 그룹키를 이용한 암호화를 통해 이루어진다. 그룹키와 같은 보안 장치가 없다면 누구나 정보를 가로채거나 잘못된 정보를 전송 할 수 있다. UAV 통신은 무선을 기반으로하기 때문에 스니핑과 같은 무선 환경에서 비롯되는 다양한 공격에 취약하다[3].

본 논문에서는 UAV 편대의 리더를 통한 효율적인 보안 그룹 관리 기법을 제안한다. 먼저 보안의 측면에서 공개키 교환을 위한 Diffie-Hellman 키 교환을 적용한다[4]. 두 번째로 그룹키를 생성하기 위해 Elliptic-Curve Cryptography (ECC)를 사용한다[5]. Diffie-Hellman 키 교환은 암호키를 교환하는 방법으로, 암호화 되지 않은 네트워크를 통해 공통의 비밀키를 공유하는 방법이다[6].

2.2 Proposed Scheme

이 장에서는 UAV 편대의 보안 그룹 관리 기법을 제안한다. UAV 편대의 가입/해제 절차에서 단순하게 단일 개체 단위의 가입/해제의 반복 형태로 진행되면 전송 자원의 낭비와 키 갱신에 대한 자원 낭비가 발생한다. 이러한 문제는 자원이 제한된 UAV 환경에 치명적이다. 그럼에도 불구하고 UAV 편대는 그룹 관리가 필요하며 보안 그룹 관리에는 그룹키가 필요하다. 따라서 UAV 환경에서 보안을 유지하면서 동시에 자원을 효율적으로 사용하는 그룹 관리 기법이 필요하다.

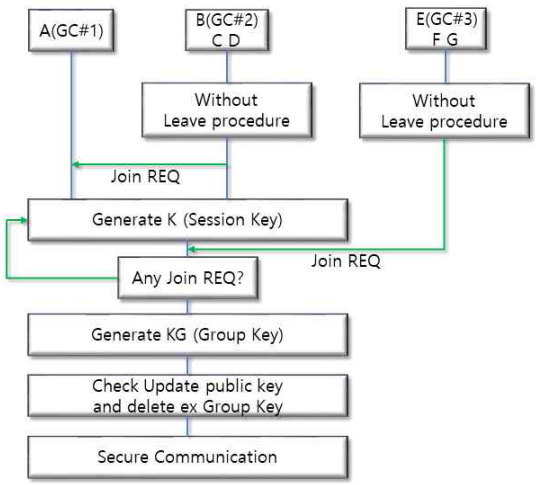


Fig. 1. Join Procedure of UAV Squadrons

Fig. 1은 둘 이상의 멤버를 가진 그룹들이 가입을 요청하는 절차를 보여준다. 자세한 절차는 다음과 같다.

1. 각 그룹의 리더(A, B, E)는 각 그룹 멤버의 공개키 전송 비용을 줄이기 위하여 리더 간 공개키 교환 절차를 진행한다.
2. 그룹1의 리더 A에게 가입 요청을 보낸 리더 B와 E는 각 멤버와 자신의 공개키를 A에게 전송한다.
3. 가입 요청을 받은 리더 A는 가입 요청을 보낸 리더 B와 E에게 자신의 공개키를 전송하고, B와 E는 수신한 공개키를 그룹의 멤버에게 브로드캐스팅한다. 공개키 교환 절차가 완료된 후, 세션키 K_S가 생성된다. 세션키는 K_G 생성 이전에 수신된 가입 요청에 대해서만 생성되며, 이 때 생성되는 세션키의 수는 멤버의 수에 비례한다.
4. 그룹 매칭키를 생성하는 단계에서도 멤버 수에 따라 각 대상의 세션키가 제외된 그룹 매칭키가 생성된다. 그 후 각 멤버에 해당하는 그룹 매칭키를 전송한다. 이러한 방식으로 그룹 멤버의 매칭키가 각각 생성되어 모든 멤버에게 전송된다.
5. 그룹의 각 멤버는 수신한 그룹 매칭키에 자신의 세션키 K_S를 포함하여 그룹키를 생성한다. 보안을 위해 매칭키 수신 응답 메시지를 통해 모든 그룹 매칭키가 올바르게 전송되었는지 확인 후 이전의 그룹키를 삭제한다.

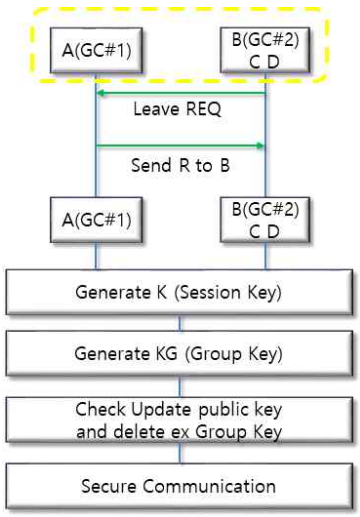


Fig. 2. Leave Procedure of UAV Squadrons

Fig. 2는 4개의 UAV로 구성된 UAV 편대가 해제되는 절차를 보여준다. 초기에 A, B, C, D로 이루어진 그룹이 A와 B, C, D로 나누어지는 절차는 다음과 같다. 해제될 그룹의 리더는 B이며 멤버는 C, D이다. B가 A에게 해제 요청을 보내고 A는 B에게 C, D의 공개키를 전송한다. 이후 가입 절차와 동일하게 각각 의 그룹키를 갱신한다.

가입 절차와 다른 점은 현재 그룹의 리더가 분리될 그룹 멤버들의 공개키를 해당 그룹의 리더가 될 멤버에게 전송한다. 그 후 2개로 분리된 편대는 각 그룹키를 갱신한다.

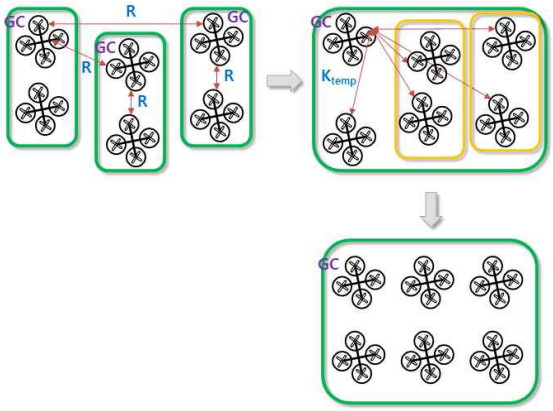


Fig. 3. Join Scenario of UAV Squadrons

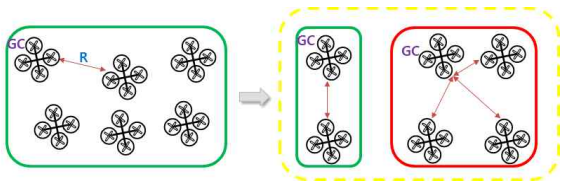


Fig. 4. Leave Scenario of UAV Squadrons

Fig. 3과 Fig. 4에서 UAV 그룹의 리더를 GC(Group Controller)로 표현하였다. Fig. 3은 각각 다른 그룹의 UAV들이 결합되는 시나리오를 보여준다. Fig. 4는 UAV 편대에서 일부 그룹이 분리되는 시나리오를 보여준다.

일반적인 가입/해제 절차의 데이터 전송 비용은 아래와 같은 수식으로 나타낼 수 있다.

그룹이 새로 추가 될 때 그룹 단위가 아닌, UAV가 하나씩 추가되는 경우, 데이터 전송 횟수는 식(1)과 동일하다. 그러나 기존 그룹이 존

재하는 경우, 제안된 절차를 적용한 가입/해제의 데이터 전송 비용은 식(2), (3)과 같이 표현된다.

Table 1. Notation used in the Equation

Name	Explanation
$N_{messages}$	Total number of data Transmissions
n_g	Number of UAV Groups
n_{base}	Number of UAV in base groups
n_{new}	Number of UAV in new groups
n_{leave}	Number of UAV in leave groups

$$N_{messages} = \sum_{i=1}^{n_g-1}\left(\sum_{j=n_{base}+n_{new}(j-1)}^{n_{new}*i+n_{base}-1} j + 2n_{new} + \sum_{k=1}^{n_{new}-2} k \right) \quad (1)$$

식(2)는 여러 그룹의 가입 요청을 고려하여 일반화를 한 수식이다. 해제 절차를 고려한 기존 그룹과 해제 그룹의 데이터 전송 횟수는 식(3)과 같이 표현된다.

$$N_{messages} = n_{base} - 1 + 3 * \sum_{i=1}^{n_g-1}\left(n_{newi}\right) \quad (2)$$

$$N_{messages} = (n_{base} - \sum_{i=1}^{n_g-1} n_{leavei}) - 1 + 3 * \sum_{i=1}^{n_g-1}\left(n_{leavei} - 1\right) \quad (3)$$

III. 성능평가

이 장에서는 제안된 모델의 성능을 평가한다. UAV 환경에서 전송 빈도, 연산 복잡도와 같이 배터리를 소모하는 요소는 비행 성능에 직접적인 영향을 준다. 이러한 점을 고려하여 평가는 두 가지 관점에서 진행 되었다.

먼저 UAV 편대의 그룹이 증가하는 환경에서 자원 관리 성능의 관점에서 기존 기법과 제안된 기법의 전송 시간을 비교하여 평가된다.

두 번째는 그룹 생성 시제안된 기법의 그룹키 업데이트에 소요되는 시간과 빈도를 비교하여 자원 관리 성능을 평가한다. 평가는 다음과 같은 전제 조건하에 수행되었다[7]. 가입 절차에서 기존 그룹의 UAV의 수 n_{base}는 4로 설정하고, 해제 절차에서는 33으로, 가입/해제 요청을 보내는 그룹의 UAV의 수 n_{new}는 3으로 설정했다.

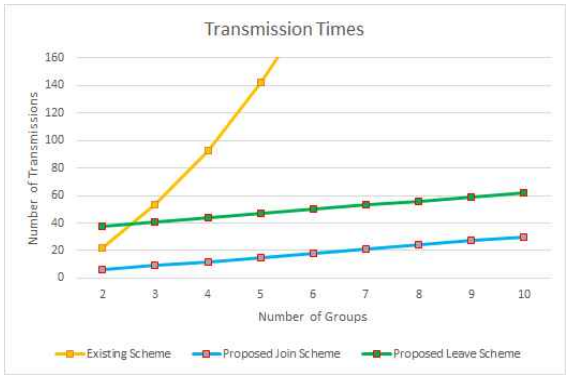


Fig. 5. Evaluation of Transmission Times

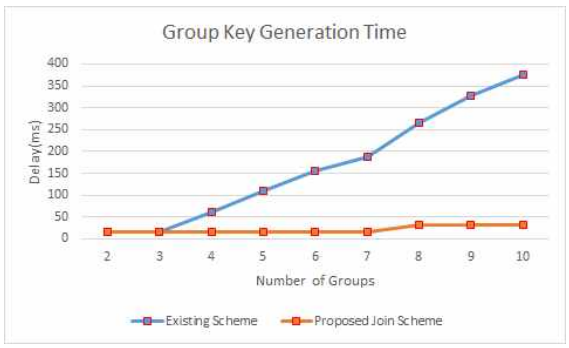


Fig. 6. Evaluation of Group Key Generation Time

Fig. 5는 그룹의 가입/해제 절차를 진행할 때의 송신 횟수를 보여준다. 그룹의 리더를 사용하지 않으면 가입 절차는 단일 개체 단위로 진행되며, 이미 그룹에 속해 있는 개체의 경우 기존 그룹에서 탈퇴 후 가입하는 과정을 거쳐야 한다. 따라서 기존 기법과 개선된 기법은 전송 횟수 측면에서 큰 차이가 있다.

Fig. 6는 그룹키 생성에 소요되는 시간을 비교한 그래프이다. 제안한 기법의 경우, 그룹의 리더는 전체 그룹에서 자신을 제외한 수 만큼의 매칭키를 생성한다. 기존 기법은 UAV 한 대가 가입 될 때 마다 키를 갱신해야 한다. 따라서 그룹이 4개일 때 추가되는 상황부터 차이가 발생하는 것을 확인 할 수 있다.

IV. 결론

최근 몇 년 동안 UAV에 대한 연구 및 개발, 이에 따른 활용 방안들이 큰 이슈가 되고 있다. 또한 인텔의 퍼포먼스와, 평창 올림픽등 UAV 단일 개체의 활용을 넘어선 UAV 편대의 활용을 볼 수 있으며, 앞으로 더 많은 UAV 편대의 활용이 기대된다. 하지만 UAV 편대를 관리하기 위해서는 여러 가지 기법들이 필요하다. 본 논문에서는 UAV(Unmanned Aerial Vehicle) 편대를 위한 그룹 리더 기반의 효율적인 보안 그룹 관리 기법을 제안하였다. 제안한 기법은 연산량과 전송 비용 그리고 보안의 관점을 고려하였다. 제안된 기법에서는 그룹의 리더를 지정하여, 지정된 그룹의 리더들은 멤버들의 공개키를 소유하고 있다. 편대의 변형을 위한 가입/해제 절차 후 갱신된 그룹키를 사용하므로 보안이 적용된 통신을 가능하게 한다. 또한 리더들 간의 통신으로 공개키를 교환하여, 그룹의 모든 UAV와 통신하여 그룹을 형성하는 기법보다 연산량 및 전송 비용의 효율을 높였다. 추후에는 Key table을 이용하여 연산량과 전송 비용을 더 감소시켜 UAV 자원을 더 효율적으로 사용할 수 있도록 방안을 도출할 계획이다.

[참고문헌]

[1] https://en.wikipedia.org/wiki/Unmanned_aerial_vehicle

[2] http://news.joins.com/article/21004086, 2016

[3] Dongxu Cheng, Jiangwei Liu, Zhengyu Guan, Tao Shang, “A One-Round Certificateless Authenticated Group Key Agreement Protocol for Mobile Ad Hoc Networks”, IEICETRANSACTIONS on Information and Systems, vol. E99-D, No.11, pp. 2716--2722, 2016

[4] Lein Harn, Changlu Lin, “Efficient group Diffie–Hellman key agreement protocols”, Computers & Electrical Engineering vol. 40.6, Issue 6, pp. 1972--1980. Elsevier, 2014

[5] https://en.wikipedia.org/wiki/Elliptic_curve_cryptography

[6] Shikha Sharma, C. Rama Krishna, “An Efficient Distributed Group Key Management Using Hierarchical Approach with Elliptic Curve Cryptography“, 2015 IEEE International Conference on Computational Intelligence & Communication Technology, pp. 687--693. IEEE Conferences, 2015

[7] https://www.codeproject.com/articles/22452/a-simple-c-implementation-of-elliptic-curve-crypto

FAIR에 기반한 기업 정보유출사고시 발생하는 법적배상비용의 통계적 검정을 통한 산출

최상원*, 유영인**, 이경호**

*한국외국어대학교 아랍어통번역학과, **고려대학교 정보보호대학원

Estimation for legal compensation costs based on FAIR under information leakage accident of company by statistical test

Sang-Won Choi*, Young-In You**, Kyung-Ho Lee**

*Department of arabic interpretation and translation, Hankuk University of Foreign Studies,
**Institute of Cyber Security & Privacy (ICSP), Korea University

요 약

각 개인의 개인정보에 대한 관심사는 높아지고 있으며 기업의 개인정보유출사고 발생 시 기업을 상대로 한 고객들의 피해보상 소송 또한 증가하고 있다. 기업의 실무자는 이에 대비해 예상 피해금액을 산출해야한다. 이때 신뢰할 수 있는 수치를 통한 산출은 기업의 자본 유동성과 발전 전략 수립에 매우 중요하다. 이에 본고는 개인정보유출사고 발생 시 기업피해금액의 한 축인 법적배상비용 산출방식을 FAIR 및 통계적 검정에 기반해 제시하고자 한다. 구체적으로, 과거 개인정보유출사고의 실제 배상 판결액과 이에 대한 평균값 및 소송인원 비율 등을 기반으로 Shapiro-wilk, t-검정을 수행하여 실효적인 법적 배상금액을 산출하는 방법을 제안하였다. 이를 통해 국내 개인정보유출사고에 대한 일반적인 소송청구비율과 배상액을 도출하여 제시하였다. 본고에서 제안되는 내용들은 정보유출사고가 발생 가능한 의료, 금융 등 여러 분야의 사후대책 수립과 해당 계획에 신뢰성을 확보하는데 기여할 것으로 기대한다.

Keywords:FAIR, Statistical test, Secondary Loss Magnitude, Legal compensation costs

I. 서론

정보화 시대 각 개인의 정보는 회사의 사내 홈페이지에서 부터 쇼핑몰, 통신사에 이르기까지 여러 서버에 저장되어있다. 개인은 기업이 제공하는 서비스를 받기 위해 개인정보를 제공하며 기업은 이를 활용하여 마케팅, 고객관리 등에 적극 이용하고 있다. 이와 같이 정보 제공에 따른 순기능이 있는 한편, 개인정보 유출로 인한 피해 또한 발생하고 있다. e-나라지표(2018)에 의하면 2000년 개인정보 침해신고 상담건수는 2,035건 이었으나 2017년 상담건수는 이보다 약 50배 증가한 105,122건으로 증가했음을 알 수 있다. 또한 2012년 KT 1,200만명, 2014년 국토교통부 2,000만명, 2016년 인터파크 1,120만명의 개인정보가 유출된 사건들이 발생해 기업의 이미지하락, 법적보상비용, 사고대처비용 등의 경제적 손실이라는 결과를 견인했다. 이에 따라 정보유출사고에 대한 예방 및 사후 대책이 필요한 상황이다.[1]

이에 본 논문은 개인정보 유출사건이 발생하는 경우 FAIR모델에 기반해 기업의 손실금액을 추산하고자 한다. FAIR모델의 요소인 Secondary Loss Magnitude(SLM, 간접 손실)의 한 영역을 차지하는 법적보상비용 산출은 정보 유출인원 수 대비 몇 퍼센트의 인원이 피해보상을 청구할 것인지 예측하는데 어려움이 있기에, 과거의 자료들을 통계적으로 분석해 유의미한 수치를 찾아 예측하는 것이 중요하다. 따라서 본고는 정규성 검정 및 t-검정을 통하여 향후 어떠한 방식으로 SLM을 산출할 지 제안하는 것을 목적으로 둔다. 이와 같은 방법은 앞으로의 SLM 산출결과에 또 하나의 근거로써 작용할 수 있을 것이다.

2장에서는 개인정보에 대한 정의와 개인정보

본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2018-2015-0-00403)

유출 피해에 대한 선행연구를 살펴본다. 3장에서는 FAIR 방법론과 본고에서 제안하는 방법을 설명하고자 한다. 4장에서는 실제 기업의 개인정보 유출사건을 본고에서 제시하는 방법으로 분석해 해당 기업의 예상 피해금액을 산출해보고자 한다. 5장에서는 본 논문이 가지는 의의, 6장에서는 결론 및 향후 연구, 7장에서는 본 논문의 한계점을 서술한다.

Ⅱ.선행연구

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제 2조에 따르면, "개인정보란 생존하는 개인에 관한 정보로서 성명, 주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호문자·음성·음향 및 영상 등의 정보를 말한다[2].

Gordon & Loeb(2006)은 기업의 정보유출 사건이 발생 시 초래되는 피해발생 비용을 직간접비용, 명시적,잠재 적 비용으로 나누어 손실금액 산출에 정형화 된 틀을 제시하였다[3].

임규건 외(2018)은 개인, 기업, 국가를 기준으로 4가지 모델(실거래 평균값 기반, 개인인식가치 기반, 보상금액 기반타 국가 기반산출방식)을 통해 개인정보 유출로 인한 사회적 피해를 산출하였다. 해당 연구에서는 각 모델에 따라 피해 산출 금액이 서로 달라질 수 있음을 보여주었다[4].

유진호 외(2009) Gordon & Loeb(2006)의 손실비용 산출모형과 과거 사례를 기반으로, 정보유출사고발생 시 예상되는 피해비용을 산출하기 위한 파라미터를 제시하였다. 해당 연구에서는 '1인당 손해배상금 산출을 위한 파라미터가 주소정보 10만원, ID정보 20만원, 금융정보 30만원으로 제시되었다[5].

김정규 외(2017)는 FAIR 방법론을 통해 기업의 개인정보 유출사고에 따른 기업의 손해규모를 산출한 바 있다. 해당 연구는 FAIR 위험 산출 과정에 대해 전반적으로 가이드한 것이 특징이다[6].

본고는 위와 같이 FAIR 방법론을 통해 기업의 개인정보 유출사고 발생 시 손해규모를 산출하지만, 3장에서 설명할 FAIR의 모든 요소를 고려하기 보다는 SLM에 초점을 맞추어 법적배상비용 산출에 있어 본고에서 제안하는 통계적 검정으로 보다 정밀한 결과를 도출하려한다.

Ⅲ.연구방법

해당 연구는 FAIR 방법론을 기반으로 하고 있으며 SLM(간접 손실)의 한 요소인 법적보상비용 산출 부분에 대한 구체화된 제안이다.

3.1 FAIR 방법론 설명

FAIR 방법론은 위험발생의 원인이 되는 요인들을 세분화해 분석하며 이를 정성, 정량적으로 분석할 수 있도록 해주는 방법론이다. 이는 ISO/IEC 27000-series 표준문서에 제시된 위험분석 방법을 보완하는 방식으로 피해규모 산정에 사용된다[7].

FAIR 방법론을 통한 분석 순서는 다음과 같다.

1단계: 조직의 중요자산, 자산에 손실을 줄 수 있는 위협원 식별 및 시나리오 구성.

2단계: TCAP(Threat Capability, 위협능력), RS(Resistance Strength, 자산 방어력)을 통한 VUL(Vulnerability, 취약성) 산출, 이후 TEF(Threat Event Frequency, 위협빈도)와 VUL을 통한 SLEF(Secondary Loss Event Frequency, 간접손실빈도)/(P)LEF(Primary Loss Event Frequency, 직접손실빈도) 산출.

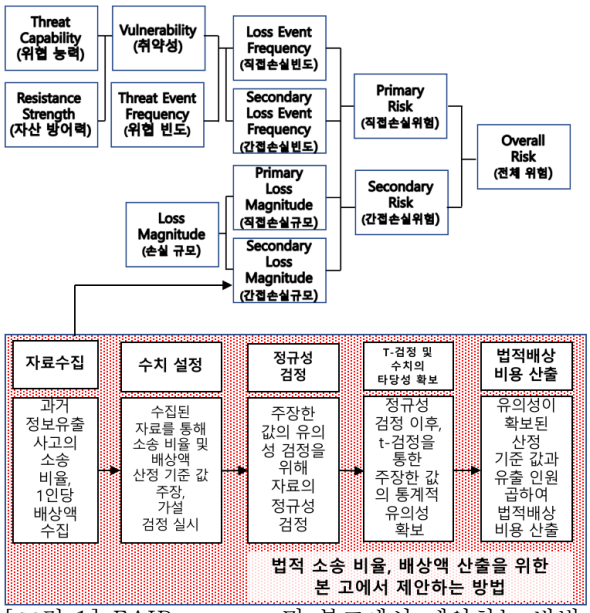
3단계: PLM(Primary Loss Magnitude, 직접피해액), SLM(Secondary Loss Magnitude, 간접피해액) 산출.

4단계: PLM과 (P)LEF를 통한 PR(Primary Risk, 직접손실위험) 산출, SLEF와 SLM을 통한 SR(Secondary Risk, 간접손실위험) 산출.

5단계: PR과 SR을 통한 OR(Overall Risk, 전체위험) 산출.

FAIR 분석 단계는 위와 같이 총 5단계로 이루어져있으며 각각의 요소는 수준에 따라 5개의 Rank(Very Low, Low, Moderate, High, Very High)로 이루어져있다. 각 요소의 Rank는 하위요소간의 Rank 조합으로 결정된다. 예를 들어, [그림 2]와 같이 PR산출의 경우 이를 구성하는 PLM과 (P)LEF를 기반으로 Table을 구성해 산출한다.

이에 대한 전반적인 과정은 [그림 1], Rank 산출 방식은 [그림 2]와 같다. 해당 그림은 본 고에서 제안하는 과정을 포함하고 있다. 제안된 과정은 3.2절에서 구체화된다.



[그림 1] FAIR process 및 본고에서 제안하는 방법.

P L M	VH	M	H	VH	VH	VH
	H	L	M	H	VH	VH
	M	VL	L	M	H	VH
	L	VL	VL	L	M	H
	VL	VL	VL	VL	L	M
PR		VL	L	M	H	VH
		(P)LEF				

[그림 2] FAIR요소 산출 Table.

3.2 본고에서 제안하는 방법

어떠한 수치에 대해 예측을 하기 위해서는 가설검정을 통해 유의미한 자료를 찾아 이를 기반으로 예측을 진행하여야 한다. 일반적으로 표본이 소표본(30개 미만)일 경우 t-검정을 통해 우리가 사용하려고 하는 수치(귀무가설 하 모평균)가 통계적으로 유의미 한지 알아본다. 본 논문에서는 피해인원 대비 소송청구인원 및 청구 금액을 과거의 사례를 통해 통계적으로 유의미한 값으로 산출해 법적배상비용을 산출하려한다. 가설검정의 순서는 다음과 같다.

(본 논문은 유의수준 95%에서 검정을 진행한다.)

1단계: 유의수준, 귀무가설 및 대립가설 설정

2단계: 검정통계량 설정

3단계: 기각역 설정

4단계: 검정통계량 계산

5단계: 통계적 의사결정

귀무가설 하 모평균은 과거 수치에 기반해 주장하며, 실제 수집된 자료의 평균을 통해 설정된 모평균 값이 통계적 유의성을 갖는지 알기 위해 t-검정을 실시한다. t-검정의 검정통계량은 다음의 식으로 계산된다.

$$T=\frac{\overline{X}-\mu_0}{s/\sqrt{n}} \quad (1)$$

($\overline{X}$ = 표본평균, μ_0 = 귀무가설 하 모평균, n = 표본의 수, s = 표본표준편차)

또한 표본평균, 표본표준편차는 다음과 같이 계산된다.

$$\overline{X}=\frac{\sum_i^n(i\text{번째표본의소송비율},1\text{인당배상액})}{\text{표본의갯수}} \quad (2)$$

$$s=\sqrt{\frac{\sum_i^n(i\text{번째표본의소송비율},1\text{인당배상액}-\overline{X})}{\text{표본의갯수}-1}} \quad (3)$$

유의수준이 95%이므로 계산된 검정통계량의 유의확률(p-value)이 0.05보다 크면 귀무가설을 기각하고 0.05보다 작으면 대립가설을 채택한다.

본 논문에서는 제시된 수치의 크고 작음을 검정하는 것이 아닌 옳고 그름을 검정하기에 양측검정을 실시한다. 이때 유의해야 할 점은 t-검정이 자료가 정규분포를 따른다는 전제하에 실행될 수 있으므로, 자료의 정규성 검정이 선행되어야 한다는 것이다.

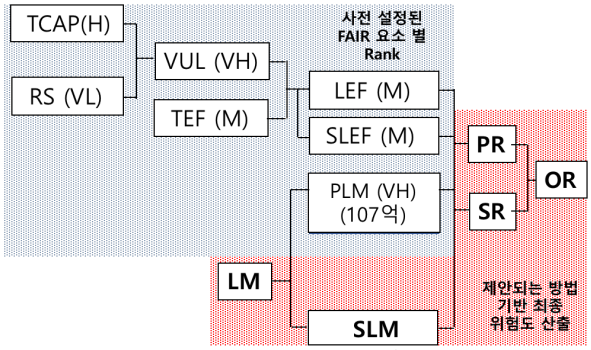
정규성 검정은 R프로그램의 Shapiro-wilk test로 진행된다. 유의수준은 95%, 귀무가설은 '소송청구비율이 정규분포를 따른다.' 로 설정되며 유의확률(p-value)이 0.05보다 크면 귀무가설을 기각하지 않고 0.05보다 작으면 대립가설을 채택하는 방식으로 검정이 시행된다.

이후 다음과 같이 법적배상비용을 산출한다.

$$\text{법적배상비용} = \text{소송비율} \times \text{유출인원} \times 1\text{인당배상금액} \quad (4)$$

Ⅳ. FAIR 방법론을 통한 기업의 손실 규모 산출

본고에서 FAIR 방법론으로 분석할 사례는 2011년 7월 21일 중국해커의 공격으로 3500만 회원들의 정보가 유출된 SK 커뮤니케이션즈(이하'SK컴즈')의 사례이다. 사고가 발생된 직후 분석을 실시한다고 가정하므로 소송비율, 1인당 실제 배상액은 2011년 7월 21일 이전 자료를 바탕으로 한다. 또한 각 table의 구성은 FAIR – ISO/IEC 27005 Cookbook을 참고하였으며 아래 Fig.2에 적힌 Rank는 김정규 외(2017)의 논문과 같이해 그 이후의 단계인 SLM계산부터 실시한다. 아래 [그림 3]은 FAIR process 및 김정규 외(2017)의 논문에서 평가한 요소의 Rank와 향후 산출할 요소이다.



[그림 3] FAIR process 내부 향후 산출 및 사전 설정 요소 구분

4.1 SLM 산출

SLM 산출시 법적배상비용을 통계적 검정으로 산출해본다. 2011년 이전 소송이 발생한 정보유출 사고의 목록은 아래 [표 1]과 같다.

[표 1] 2011년 이전 정보유출 사고 목록

년도	회사명	피해 인원 (명)	소송청구인원 (명)	소송청구비율	1인당 실제 배상액
2005 [8]	엔씨 소프트	54만	1.06만	1.97%	0원
2006 [9]	국민 은행	3.2만	0.1만	3.17%	20만원
2008 [10]	GS 칼텍스	1151 만	1.15만	0.1%	0원
2008 [11]	옥션	1081 만	14.6만	1.35%	0원
2008 [12]	엘지 텔레콤	780만	0.0278만	0.003%	5만원
2008 [13]	하나로 텔레콤	600만	2.3만	0.38%	10만원

수치의 검정에 앞서 언급한 것처럼 t-검정을 사용한다. 이를 위해서는 우선적으로 Shapiro-Wilk test로 자료의 정규성 검정을 해야 한다. 소송청구비율에 대한 검정결과는 유의확률이 0.3613으로 유의수준(0.05)보다 크므로 정규성을 띈다고 할 수 있다. 1인당 청구액에 대한 정규성 검정결과 또한 유의확률이 0.1492로 유의수준보다 크므로 정규성을 띈다고 볼 수 있다.

다음으로 수치 계산에 사용될 자료의 평균값이 통계적으로 유의미 한 지에 대한 t-검정을 실시한다. 소송청구비율의 평균값은 1.17%(소수점 셋째자리 반올림)이다. 가설은 다음과 같이 설정한다.

H0: 소송청구비율은 1,17%이다
H1: 소송청구비율은 1.17%이 아니다

t-검정 결과 유의확률은 0.3437이다. 유의 확률이 유의수준보다 높아 귀무가설을 기각하지 않으므로 소송청구비율은 1.17%로 설정할 수 있다.

1인당 실제보상액은 피고 승소의 경우 0원이 되므로 실제 판결액과 평균값의 차이가 비교적 크게 존재한다. 이에 평균값 58000원이 아닌 중간 값인 10만원을 1인당 실제 보상액으로 설정해 가설검정을 진행한다.

H0: 1인당 실제배상액은 10만원이다.
H1: 1인당 실제배상액은 10만원이 아니다.

t-검정 결과 유의확률은 0.2586이다. 유의확률이 유의수준보다 높아 귀무가설을 기각하지 않으므로 1인당 실제배상액은 10만원으로 설정할 수 있다.

이를 바탕으로 법적배상비용을 계산하면 3500만 명의 1.17%인 ₩95,000 이 소송을 진행한다고 가정 할 수 있다. 또한 각 개인에게 10만원을 배상해야함을 가정하면 법적배상비용은 ₩9995 로 산출됨을 알 수 있다. 김정규 외(2017)의 논문에서는 단순 가정으로 소송 참여 비율을 2%로 설정해 손해배상비용을 ₩1400 원으로 추산하였

으며 본 고의 추 산 값과 약 2.5배 차이가 난다. SLM의 타 요소는 개인정보보호 협회의 2013년 보고서에 따라 홍보비용 약 36억, 매출감소로 인한 손해 691 으로 산출되었음을 알 수 있다. 이에 따라 최종 적으로 SLM은 약 692 으로 산출할 수 있으며 SLM 급은 [표 2]와 같이 VH로 설정할 수 있다.

[표 2] SLM 등급 측정 Table

등급	최솟값(만원)	최댓값(만원)
Very High(VH)	1,000,000	-
High(H)	100,000	999,999
Moderate(M)	10,000	99,999
Low(L)	1,000	9,999
Very Low(VL)	0	999

4.2 PR, SR, OR 산출 및 최종 손해금액 산출

PR은 (P)LEF와 PLM으로 산출한다. (P)LEF가 M이고 PLM이 VH이므로 PR은 VH로 측정된다. SR은 SLEF와 SLM으로 산출하며 SLEF가 M, SLM이 VH이므로 VH이다.

OR은 PR과 SR의 결과로 산출하며 각각의 요소가 VH이므로 OR 또한 [표 3]과 같이 VH로 산출된다.

[표 3] PR 등급 측정 Table

P L M	VH	M	H	VH	VH	VH
	H	L	M	H	VH	VH
	M	VL	L	M	H	VH
	L	VL	VL	L	M	H
	VL	VL	VL	VL	L	M
PR		VL	L	M	H	VH
		(P)LEF				

최종손해금액은 PLM(107억), SLM(692억)에 각각 (P)LEF(M), SLEF(M) 구간을 곱 해 산출한다. (P)LEF, SLEF가 최 소,최 대 구간을 설정하므로 최종손해금액도 최 소,최 대 범 위를 설정한다. 결과 값은 아래 [표 4]와 같다.

[표 4] 최종 손실 금액 산출 구간

Risk type	Frequency	Min Loss	Max Loss
Primary	0.3~0.7	32.1억	74.9억
Secondary	0.3~0.7	207.6억	484.4억
Total		239.7억	559.3억

지금까지 FAIR방법론을 통해,특히 SLM의 법정배상비용을 구체화하며 기업의 정보유출사고 시 발생할 수 있는 손해금액을 측정해보았다. 각 기업의 실무자들은 이와 같은 방법으로 정보 유출 사고발생 시 손해금액을 측정하고 향후 대책을 수립할 수 있다.

Ⅴ. 본고의 의의

본고에서 제시한 방식은 다음과 같은 의의를 가진다 첫 째, 본고의 방식은 정보유출사고가 발생할 수 있는 여러 분야(의료, 금융,통 신,상거래 , 공문서)에서 사용될 수 있다. 어느 영역에서든 과거의 자료를 통해 사후 대책 수립 시 유의미한 수치는 필 요하기 때문이다.

둘째, 정보보안 실무자가 사후 대책을 수립할 경우 이전의 방식보다 신뢰 성 있는 수치를 산출할 수 있을 것이다. 주관에 의한 자료보다 통계적으로 검정된 자료는 자료에 신뢰 성을 주기 때문이다.

셋째, 한국의 기업 사례에만 국한되지 않고 타 국가의 기업 사례에도 적용될 수 있다. 개인정보법과 이에 대한 법의식이 다른 국가에서는 본고에서 산출된 수치가 다를 수 있다. 이 경우에도 유의미한 값을 찾기 위해선 본고에서 제시된 방식을 사용할 수 있다.

Ⅵ. 결론 및 향후 연구

본고는 FAIR방법론에 기반하여 실제 기업의 사례를 통해 SLM의 법적배상비용 산출 방식을 구체화하였다. 구체화에 과정에서 유의미한 값을 산출하기 위해 통계적 검정을 실시하였다. 여타 FAIR요소와 달 리, 법적배상비용은 실제소송인원이 유출인원 대비 몇 퍼센트의 비율을 차지할지 예측하기 어려움이 있기에 본고에서 제시한 바와 같이 통계적으로 유의미한 값을 찾아 예측하는 것이 중요하다.

본 논문에서 제시한 방식은 여러 분야의 정보유출사고 발생 시 사후대책 수립에 적용될 수 있을 것이다. 그러나 각 분야별로 개인이 느끼 는 개인정보의 유출의 심각성은 다를 수 있다. 예를 들면 카드 회사, 은행 같은 금융 분야의 정보유출

사고에 대해서는 심각성을 느끼고 적극적으로 대처할 수 있으나 타 분야에서는 소극적인 대처를 표할 수 있기 때문이다. 따라서 소송비율 추산에 대해 사회심리학적 접근도 필요하다. 이와 더불어 외국사례분석의 경우 해당 국가의 법을 참고할 필요가 있다.

Ⅶ. 한계점

그러나 위와 같은 장점 이외에도 본 논문은 다음과 같은 한계점을 가진다. 첫째, 표본의 부족으로 통계의 검정력이 약하다는 점이다. 앞서 언급한 것처럼 본 논문에 사용된 표본은 SK컴즈 사건이 발생하기 이전의 사례, 특히 법적 분쟁이 발생한 사례만을 적용하였기에 6개의 사례만을 통계적으로 분석할 수 있었다. 그러나 시민들의 개인정보 중요성에 대한 의식이 갈수록 높아지고 더욱 더 많은 인원의 개인정보가 인터넷에 저장되는 만큼, 개인정보 유출에 대한 법적 책임을 묻는 사례가 많아질 것이다. 이에 향후 더 많은 사례를 분석해 이를 보완하고자 한다.

둘째, 실제 최종 판결의 법적배상비용(0원)과 본고에서 산출한 법적배상 비용(595 원)의 차이가 있다. 일반적으로 사고가 발생한 후 본 논문과 같이 예상피해금액을 산출하고 대비하는 것은 중요하다. 그러나 산출된 금액만큼 기업의 자본 유동성이 감소할 수 있으며 이는 최종 판결까지의 기간 동안 기업의 향후 발전 대책수립에 악영향을 줄 수 있을 것이다. 향후 실제 배상 판결이 난 기업의 사례와 배상판결이 나지 않은 기업의 사례를 법적요건을 고려해 분석하며, 해당 결과를 본고와 결합해 법적으로도 타당성 있는 수치를 산출하는 연구를 진행할 예정이다.

[참고문헌]

[1] 통계청, “개인정보 침해사고 상담건수”, “http://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=1366”, 2018년 월 .

[2] 한국정보보호진흥원, " 정보통신망 이용촉진 및 정 보보호 등에 관한 법률," 정보통신정보보호 법령 집, pp. 2-3, 2006년 9월

[3] L.A. Gordon and M.P. Loeb, Managing Resources: A Cost-Benefit Analysis, McGraw-Hill Companies, Inc., 2005년 월.

[4] 임규건, 류미나, 이정미, “개인정보유출 피해비용 산출 모델에 관한 연구,” 정보보호학회논문지, 한국정보보호학회, 2018년 2월.

[5] 유진호,지상 호, 임종인, “개인정보 유노출 사고로 인한 기업의 손실비용 추정,” 정보보호학회논문지, 한국정보보호학회, 2009년 월.

[6] 김정규, 이경호 “FAIR를 통한 개인정보 유출에 따른 기업의 손해금액 산출에 대한 연구,” 정보보호학회논문지, 한국정보보호학 ,회 2017년 2월.

[7] ISO/IEC JTC, International Organization for Standardization, ISO/IEC, 2013

[8] 서울중앙지법,선“ 고 2006가합22338,38197 판결,” 2007년 월 .

[9] 서울중앙지법,선“ 고 2006가합33062,53332 판결,” 2007년 월 .

[10] 서울중앙지법,선“ 고 2008가합111003 판결,” 2010년 월.

[11] 전성무, (2015년 월 12일), “'옥션 개인정보 유출' 피해자들 집단소송 패 소 확정 ”, *new1*,<http://news1.kr/articles/?2092164>, (2018년 월 일)

[12] 김효정, (2009년 11월 9일), “LG텔레콤 개인정보누출, 1심에서 패소 ”, *ZDNET KOREA*,<http://www.zdnet.co.kr/news/news_view.asp?artice_id=20091106203553>,(2008년 월 일)

[13] 이명진, (2011년 월 30일), “개인정보 무단유출 하나로 텔레콤, 2348명에게 배상하라”,*조선일보*,<http://news.chosun.com/site/data/html_dir/2011/07/30/2011073000086.html?Dep0=twitter&d=2011073000086>, (2008년 월 일).

2018 한국정보보호학회 하계학술대회

C5 컴퓨터보안 2

서 승 현 (한양대학교)

- Towards the Advance Persistent Threat' Detection Events
  Sami Ullah, 오희국
- **윈도우 감사 로그를 활용한 침해사고 모니터링 방안 연구**
  김승민, 최문원, 윤인재
- **조건문을 통한 점프테이블 크기 유추에 따른 인다이렉트 점프 주소 계산 방법**
  김문회, 하동수, 오희국
- **전자파 오류 주입을 통한 인증 우회 공격 – Case Study : 지문 인식 시스템**
  이종혁, 조영진, 한동국

Towards the Advance Persistent Threat' Detection Events*

Sami Ullah† , and Heekuck Oh‡

Department of Computer Science and Engineering, Hanyang University.

Abstract

Advance Persistent Threats (APT) are well-known to be undetectable, persistent and stealthy in their nature. In conventional Intrusion Detection Systems (IDS), detection method are based on signatures, patterns or behavioral models of previously known malwares; which makes IDS unfit for APT problem, as APTs are specifically designed to dodge and bypass these detection systems. In this research work, we model the APT nature by kill-chain model and introduce novel anomaly events; captured during APT kill-chain process. Using these events with the crafted whitelisting technique, we can detect APT during its operational duration. Our approach is different from the conventional techniques; which makes it an interesting field of study.

I. Introduction

In the last decade, organizational and industrial cyber systems were being targeted by complex, sophisticated, persistent and stealthy attacks; known as advance persistent threats (APT). These attacks are specifically embattled for an organizational cyber systems, with an aim of being undetected, persistent and being stealthy. APT attackers are known to be highly skilled, well-funded and practice a variety of complex intrusion techniques using undisclosed vulnerabilities and attack methods; which makes the detection difficult for conventional intrusion detection systems at network or host level. Conventional Intrusion detection systems focus only on the signatures or the behaviors of previously known malwares and systematically neglect the unpredictable nature of APTs; which involves the human factor in its execution phase and thus making conventional IDS unfit for such intrusion detections.

Although APTs are target specific and engineered enough to be unique in their nature but they follow an identical kill-chain or attack strategy to achieve their goals [reference]. The kill-chain model categories it into reconnaissance, weaponization, delivery, exploitation, installation, C2 and action attack phases. There is a dire need to introduce new strategy in intrusion detection systems to make the APT detection more accurate and reliable.

In this research, we have tried to mitigate the limitations of current intrusion detection techniques by integrating host and network level intrusion detection systems and adopting whitelisting technique to filter Benjamin activities in the kill-chain model by introducing novel security breach events. Our major contributions are: 1) novel anomaly

* This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2018-2014-1-00636) supervised by the IITP(Institute for Information & communications Technology Promotion)

* This research was also supported in part by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(No. NRF-2015R1D1A1A09058200)

† Author: sami.ullah2316@gmail.com

‡ Corresponding authors: hkoh@hanyang.ac.kr

detection events specifically related to APT behavior. 2) A strategic detection model to detect suspicious activities (in an APT life cycle); with a whitelisting approach.

The rest of the paper is organized into following sections. 2) Related work 3) APT life-cycle 4) Novel anomaly events 5) Proposed detection model 6) Conclusion

II. Related Work

To comprehend with the APT, various types of techniques in different domains have been researched but most of them end up relying on the same intrusion detection systems, which have failed previously. [3] Deduces a new kill-chain model from the well-known Lockheed Martin kill-chain and Mandiant Attack lifecycle and defines combined sub-states based on activity layer (network layer or host layer etc.). Then he applies this kill-chain to track the activity of an APT but the problem is using the security events generated by conventional SIEMs. A mathematical model using machine learning to depict malicious activities has been presented in [3] but their model parameters are memory usage, files in system folder etc. which are not the features of an APT. Paper [3] researched long lived nature of attack campaigns and presented a model to track the flow in different stages of an APT; while relying on the logs of current intrusion detection systems for each stage. [4] Proposed an APT detection model by using multiple known intrusion detection techniques and then correlating their results to pin-point an APT attack. But there is no practical thoughts about which reliable and efficient methods to use for detection.

The research work in [1] has analyzed 22 unique APT technical reports and defined the malicious events or techniques used in each phase of attack. Authors has introduced a more realistic and practical nature of an APT, which seemed to be missed by other researchers. In the light of [1], the previous papers were treating APT like a malware of botnet [reference]; which is not true.

III. APT life-cycle

To understand an APT, we must consider a hacker's deliberate strategy to breach into an organizational cyber space. Martin kill-Chain [reference] attempts to classify an APT attack into seven phases to presents a general theoretical framework of an APT activity and many APT detection models follow it to generate an APT alert.

Mandiant [reference] proposed another framework for an APT activity lifecycle, which is based on the analysis of known APT campaigns and more realistic for IDS. It compromises of eight phases: (1) initial reconnaissance, (2) initial compromise, (3) establish foothold, (4) escalate privileges, (5) internal reconnaissance, (6) move laterally, (7) maintain presence and (8) complete mission. In this framework, phases from 4-7 are expected to be a repeated activity; to maintain persistence in the targeted organization. Both of these models show the diverse scope of an APT attack.

Our research scope is intrusion detection systems, so we focus only those phases which are critical to activities within the organizational cyber space. With our understanding of an APT, we classify it into following five stages based on unique characteristics with novel detection events.

3.1 Reconnaissance:

The first thing to compromise an organization is collecting information about the cyber infrastructure of that organization;

which is called reconnaissance (recon). Recon may be attempted externally: outside the network, or internally: inside the network but it follows the same pattern. Hackers attempt port scanning to know the running services and their version information for custom payload generation, and ping scan to know the running hosts.

3.2 Delivery

In this stage, attacker tries to deliver the dropper or payload through phishing, water-hole attacks, doc/pdf exploits, an infected autonomous USB (bad USB or rubber ducky etc.), a rogue Wi-Fi or any other possible way unknown to us. In each method of delivery, the overall purpose is to deliver the executable and execute it as well before the host application (exploit case) is closed.

3.3 Execution & Persistence

After the delivery phase, execution phase varies depending upon the delivery. If the delivery is C2, it will try to make it persistent by adding it to startup jobs, or registry, or infecting the specific ELF/PE files (to be less noisy). If delivery is a dropper, it will download C2 or recon tool for further control. If the delivery is a recon tool, it may try communicating with the local workstations. It may be acting as server for local network by opening some listening ports. In the execution phase, APT try their best to be silent by using Benjamin calls or applications.

3.4 Lateral Movement

Lateral movement may be for persistence or further recon. APTs achieve it by collecting the network passwords, local credentials using obfuscated hashing tools, Remote Desktop Protocol (RDP), Windows Management Instructions (WMI) etc. They try their best to hide them in the legitimate calls, be less noisy and as stealthy as it could be. Another way to network movement is by exploiting vulnerabilities in the network like windows-SMB vulnerability.

3.5 Data Theft

The overall objective of an APT is espionage or data theft. Data movement may be detectable by Intrusion detections system at the network level but an APT objective would be to hide is in legitimate traffic and avoid file analysis using encryption techniques. Another approach adopted by an APT was uploading the files in mp3 format, which is legitimate for an intrusion detection system.

In all these stages, an attacker always come up with a new strategy or technique unknown to intrusion detection; which makes it undetected. It's is just a cat and mouse game b/w hacker and security researcher if we follow the traditional black-listing approach based on signature or anomaly based detection. so there is need of new strategies in intrusion detection systems.

IV. Novel Critical Events

This section summarizes the unique events which are efficient when adopted with whitelisting approach. Table 1 illustrates the events, which have been categorized w.r.t. each APT stage.

V. Proposed Detection Model

Our proposed solution is using host and network IDS together and filter the processes generating events listed in Table 1. APT takes place in several months and its slow moving; to track it we build kill-chain from the detected events. Each event is also given weight in the kill-chain and then based on

APT phase	Events
Recon	• External port scanning and ping scan detectable by NIDS • Internal port scanning and ping scan • Look for process general local network traffic • Processes using nmap, cmd, netstat etc.
Delivery	• Installation of browser extensions • A downloaded application trying to communicate with internet.
Execution & Persistence	• The one thing each APT will do try to connect with internet, so filter the process accessing internet other than legitimate process like browsers. • Processes launching cmd, PowerShell etc. • Processes trying to change start registry values or startup folder • Illegitimate processes accessing mic or camera • Process accessing LSASS process; a common method to extract passwords.
Lateral Movement	• Filter the process with listening ports • Filter the process communicating with local network • Filter the process for which destination is gateway-ip for incoming packet. As process may be acting as Man-in-the-middle. • Filter RDP process
Data Theft	• Applications accessing files in data drives • Network traffic at abnormal times, as uploading is usually observed at low traffic timings. • Processes using FTP, or filter processes other than legitimate one. • Usually files are encrypted, so we can filter the applications using encryption system calls.

Table 1: APT phases and corresponding critical events

the weighted average of a kill-chain, we decide about the intrusion. We are working on testing the model and include it into our future work.

VI. Conclusion

In this paper, we have analyzed APT nature and proposed another dimension (whitelisting instead of blacklisting) for this research field to get a more practical solution. Conventional IDS fails due to the nature of APT; which is stealthy and slow moving. We have suggested new events, which are generated by APT during its kill-chain. And by following the whitelisting approach along with these novel events, detection can be more promising and accurate. The model and its implementation is in progress and not presented in this paper.

References

[1] Ussath, Martin, et al. "Advanced persistent threats: Behind the scenes." Information Science and Systems (CISS), 2016 Annual Conference on. IEEE, 2016.

[2] Bryant, Blake D., and Hossein Saiedian. "A novel kill-chain framework for remote security log analysis with SIEM software." computers & security 67 (2017): 198-210.

[3] Brogi, Guillaume, and Valérie Viet Triem Tong. "Terminaptor: Highlighting advanced persistent threats through information flow tracking." New Technologies, Mobility and Security (NTMS), 2016 8th IFIP International Conference on. IEEE, 2016.

[4] Ghafir, Ibrahim, and Vaclav Prenosil. "Proposed approach for targeted attacks detection." Advanced Computer and Communication Engineering Technology. Springer, Cham, 2016. 73-80.

[5] Chandran, Saranya, P. Hrudya, and Prabaharan Poornachandran. "An efficient classification model for detecting advanced persistent threat." Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on. IEEE, 2015.

윈도우 감사 로그를 활용한 침해사고 모니터링 방안 연구

윤인재*

*고려대학교 컴퓨터정보통신대학원

A study on monitoring method of infringement using Windows audit log

In-Jae Yun*

*Graduate School of Computer & Information Technology, Korea University.

요 약

네트워크 환경 및 인터넷 활용폭이 다양해지면서 고도화되고 진보적인 보안위협이 발생되고 있으며 발생량도 점차 증가하고 있다. 이에 따라, 네트워크 침입탐지 시스템, 악성행위 탐지 시스템, 웹 방화벽, 안티바이러스 등도 점차 진보 된 악성행위를 탐지하는 데 있어 불충분해짐에 따라 많은 회사 및 보안담당자들은 직관적인 정보를 제공하는 End-Point 로그 수집 및 모니터링으로 변화를 시도하고 있다. 이에 따라, 본 논문에서는 Anti-Virus 및 침입탐지 시스템(IDS), APT, 윈도우 감사로그를 상호 비교하여 보안분석 시스템보다 윈도우 감사로그가 보안위협 및 침해사고를 모니터링하는 면에서 더욱 직관적이고 빠른 대응이 가능하다는 것을 증명한다.

I. 서론

최근의 사이버 침해사고 사례를 보면 드라이브 바이 다운로드, 자바 애플릿 등의 웹을 통한 침해사고, 악성 이메일을 통한 침해사고, 파일서버 등의 서비스를 이용한 침해사고, 저장장치 및 기기를 통한 침해사고 등 다양한 방법을 통해 악성코드 감염 등의 침해사고가 발생하고 있다. 그러나, 악성행위들이 대부분 암호화 및 난독화가 되어가고 있어 기존의 보안위협을 탐지하는 시스템으로는 고도화되고 진보적으로 변화하는 악성 행위를 탐지하지 못하는 이슈가 발생되고 있으며 증가되고 있다.

보안위협을 탐지하는 시스템으로는 침입탐지 시스템, 가상머신을 보유한 악성행위 탐지 시스템, Anti-Virus 등 다양하나 대부분의 시스템별로 위협탐지의 특성이 있어 보안조직에서는 SIEM(Security Information and Event Management)을 통한 보안 시스템 탐지로그를 수집 및 상호 연계 분석을 진행하고 있다. 다양한 보안위협 탐지/차단 시스템들은 현재 알려진 악성파일 및 공격시도에 대한 내용을 탐지 및 차단하며 악성파일은 가상 머신에서 분석된 후 알람을 침해사고가 발생된 이후에 보안담당자에게 가는 형태이며 또한 신규 취약점을 통한 Zoro-Day Attack 등은 탐지하지 못하는 이슈가 계속적으로 발생되고 있다.[1]

이에 따라, 윈도우 감사로그를 통한 악성코드 실행 및 감염, 침해사고를 탐지하고 모니터링 하는 방안이 기존의 여러 보안위협 탐지/차단 시스템을 활용하는 것보다 정확성이 높고 대응이 빠르나든 것을 보인다.

II. 연구 배경

윈도우 계열 악성코드에 의한 침해사고는 많은 회사 및 기관에서는 다양한 보안 시스템을 활용하여 탐지 및 분석한다. 그러나, 보안 시스템별로 탐지구간(네트워크/End-Point), 탐지 특성(시그니처 기반, 가상머신 분석) 등이 있으며

시스템을 구축하는데 많은 비용이 소요되고 각 보안 시스템에서 발생하는 정탐 및 오탐 알람을 일일이 분석 및 대응하기에 시간적으로도 어려운 상황이다.

보통 악성파일 탐지는 두 가지 방법이 있다. 의심스러운 실행 파일에서 악성 콘텐츠를 검색해서 탐지하는 정적 분석과 악성 파일의 동작 중에 발생되는 내용을 통한 동적 행위 탐지로 구분할 수 있다. 상용 Anti-Virus 솔루션들은 대부분 악성 콘텐츠 중심의 정적 분석을 주로 하여 새롭게 난독화 기술이 적용 된 악성 파일은 신규 정보 업데이트 전까지 탐지하지 못한다. 또한, 가상 머신을 통한 분석 솔루션은 의심 파일이 가상머신에 들어간 후 결과 값이 나오기까지 많은 시간이 걸리며 트래픽이 많으면 많을수록 분석해야 하는 건수도 증가하여 알람을 주는 시간과 대응 시간이 길어진다는 단점이 있다[1].

이에 따라, 각 보안분석 시스템, 윈도우 감사로그를 활용하여 상호 비교하였으며 윈도우 감사로그가 SIME을 통해 모니터링 및 분석하기에 정확도가 높고 빠른 대응이 가능하다는 것을 보인다[2].

III. 연구 내용

보안위협 케이스에 대해 시나리오를 정의 한 후 각 Anti-Virus, 침입탐지 시스템, APT(지능형 지속 공격, Advanced Persistent Threat) 탐지 시스템, 윈도우 감사로그 별로 발생 되는 로그의 유/무 및 가상 머신을 통해 분석 후 알람을 주는 시간, 윈도우 감사로그를 상호 비교 한다[3].

윈도우는 독자적인 프로토콜을 채택하고 있으며, 이벤트 뷰어를 통해 로그 검색 및 다운로드가 가능하고 SIEM 을 통하여 로그 연계분석 후 모니터링 하는 방법을 연구한다.[4].

3.1 로그 수집

악성 바이너리 파일 실행 시에 발생되고 저장되는 감사 로그를 포함하여 수집하며 수집되는 감사로그는 [표 1]과 같다.

[표 1] 로그 수집 정보 및 내용

구분	수집 정보	수집 내용
감사 로그	Application	API를 사용하는 응용프로그램의 중요한 이벤트 및 활동 내역을 기록
	Security	시스템 로그온, 파일 접근, 인증, 계정 생성, 권한 사용 등의 내역 기록
	System	시스템 운영과 유지에 관련된 대부분의 정보 등의 내역 기록
	Windows-PowerShell	파워쉘 사용에 따른 내역

3.2 악성파일 탐지 현황

[표 2]에서 보는 것과 같이 침입탐지 시스템은 네트워크 구간에서 탐지 시그니처(문자열)이 존재할 경우 탐지하지만 네트워크 트래픽이 암호화 되었을 경우는 전혀 탐지하지 못하는 것으로 확인되며, Anti-Virus는 End-Point 구간에 설치되므로 기존에 알려진 악성코드에 대해서 탐지는 하지만 신규 악성코드 및 네트워크 구간 트래픽은 별도로 정보 업데이트 전까지 탐지/검사하지 못한다. APT 탐지 시스템 경우에도 네트워크 암호화 트래픽은 별도로 분석하지 못하며 복호화가 가능한 트래픽 및 암호화 되지 않은 트래픽에서는 가상 머신을 통해 행위 분석 결과 확인 할 수 있다.

그러나, 윈도우 감사로그에서는 다양한 행위에 대해 로그 저장하므로 네트워크 트래픽에 대한 내용은 없어도 실제적으로 윈도우 OS 단에서 실행되는 파일 정보, 명령어 정보, 계정 정보 등에 대한 다양한 로그를 확인가능하고 다른 보안분석 시스템들 보다 직관적이므로 빠른 대응이 가능하다.

[표 2] 시스템별 탐지 내역

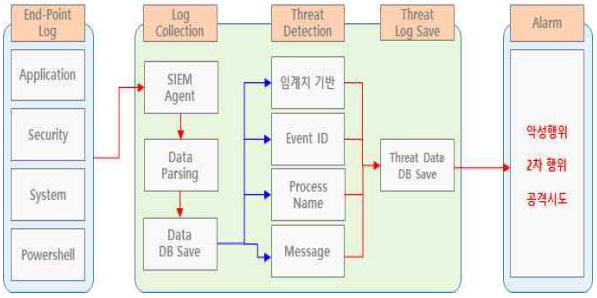
구분	네트워크 구간	End-Point 구간
침입탐지 시스템	△	X
Anti-Virus	X	○
APT	△	X
윈도우 감사로그	X	○

3.3 감사로그 수집 및 저장

윈도우 감사로그는 악의적인 행위 시에만 로

그를 남기는 것이 아닌, 정상적인 행위에서도 로그를 남기므로 많은 데이터가 생성되고 저장된다. 그러므로 해당 데이터를 저장이 필요하며 해당 연구에서는 SIEM에 데이터를 저장 및 가공한다.

[그림 1]과 같이 직관적인 감사로그를 통해 데이터 가공이 가능하며 보안위협과 관련된 정보는 SIEM 메모리상에 상주시켜 위협과 관련된 데이터가 들어왔을 경우 실시간 알람을 받는 형태로 구성한다.

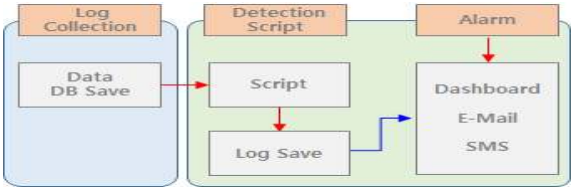


[그림 1] Log 수집 및 위협 탐지 과정

3.4 보안위협 데이터(Log) 검출

저장된 데이터를 활용하여 어떤 정보를 어떻게 이용할 것인지 사전에 정의된 시나리오가 있다면 해당 시나리오에 맞춰 Log Parsing을 진행해야 하며 시나리오를 기반으로 다양하게 위협을 탐지 및 알람을 설정할 수 있다.

보안위협을 탐지하기 위해선 위협이라고 판단되는 정보를 [그림 3] 과 같이 스크립트로 작성하여 SIEM에 등록해야 하며, 메모리에 상주시켜야 한다. [그림 2]는 보안위협 탐지 스크립트가 동작하는 과정을 설명한 내용이며, [그림 3]은 보안 위협에 대한 시나리오 내용 스크립트이며 메모리에 상주 시켜 실시간으로 모니터링 및 분석이 가능한 것을 보여준다.



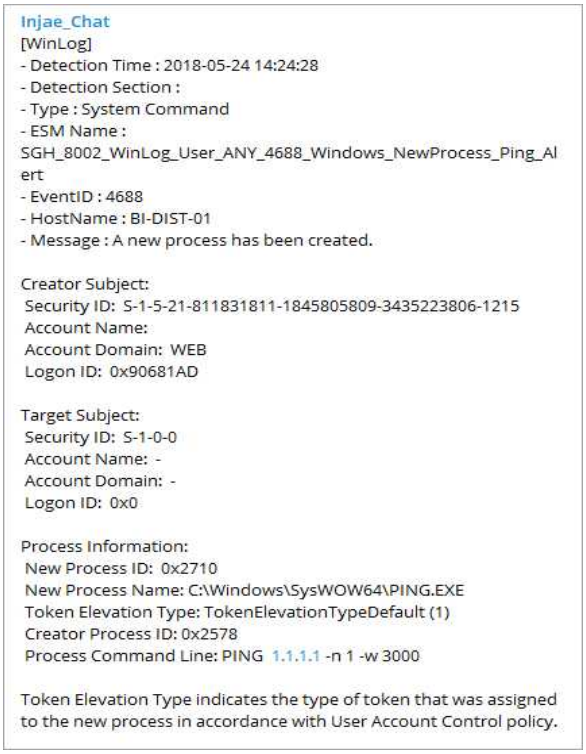
[그림 2] 시나리오 기반 보안위협 탐지 과정

```
eval esm =
case(
event_id == 4688 and lower(message) == "*winrs.exe*",
"SGH_8001_WinLog_User_ANY_4688_Windows_NewProcess_WinRs_Alert",

event_id == 4688 and lower(message) == "*ping.exe*",
"SGH_8002_WinLog_User_ANY_4688_Windows_NewProcess_Ping_Alert",

event_id == 4688 and lower(message) == "*quser*",
"SGH_8003_WinLog_User_ANY_4688_Windows_NewProcess_Quser_Alert",

event_id == 4688 and lower(message) == "*psexec*" and (message != "*hcyoo_dc*"),
"SGH_8004_WinLog_User_ANY_4688_Windows_NewProcess_Psexec_Alert",

event_id == 4688 and lower(message) == "*psexesvc.exe*",
"SGH_8005_WinLog_User_ANY_4688_Windows_NewProcess_Psexesvc_Alert",

event_id == 4688 and lower(message) == "*net.exe*" and lower(message) == "* use *",
"SGH_8006_WinLog_User_ANY_4688_Windows_NewProcess_Net_Use_Alert",

| search isnotnull(esm)

| lookup kafka_win_log esm output type, device, hazard, severity
| fields _time, hazard, esm, device, type, event_id, host, message, tags

| eval key = concat(host, "=", esm)

| serial
[
evtctxadd topic="kafka_win_log" key=key timeout=5m maxrows=0 isnotnull(key)
| eval evt_count = evtctxget("kafka_win_log",key, "counter")
]

| search evt_count == 1

| import esml_server_winlog
```

[그림 3] 시나리오 기반 탐지 스크립트

3.5 보안위협 실시간 알람 (텔레그램 메신저)

[그림 4]와 같이 SIEM의 보안위협 로그를 텔레그램 API를 통해 메신저 연동 가능하며 데스크탑 PC, 핸드폰 등에서 자유롭고 빠르게 탐지된 보안위협 로그를 모니터링 가능하다.



[그림 4] SIEM과 텔레그램 메신저 연동

IV. 연구 결과

보안분석 시스템과 윈도우 감사로그를 비교한 결과, 보안분석 시스템이 알람을 주는 경우는 대부분 사전에 정의된(알려진) 공격들이 대부분 이였으며, 암호화 된 네트워크 구성에서는 탐지 및 알람을 주지 못하는 경우가 많았다. 그에 반해, 윈도우 감사로그는 OS 상에서 이루어지는 행위들에 대해서 로그로 모두 저장하므로 분석시간 면이나 암호화된 네트워크 환경에서 모두 효율성이 높다는 결론을 보였다.

[표 3]과 같이, 20일 평균 저장되는 로그를 바탕으로 효율성을 비교 검증 결과, 윈도우 감사로그가 저장되는 수치는 많은 반변 로그에서 볼 수 있는 내용이 직관적이므로 분석시간이 매우 짧으며 대응이 효율적이라는 것을 볼 수 있다.

[표 3] 탐지로그 및 분석 건수 (시간)

Log Type	Input Data	Analysis Case	Responsetime (1건/min)
IDS	90,465	248	41h 20m (10min)
Anti-Virus	14,224	5	10h (120min)
APT	184	9	9h (60min)
윈도우 감사로그	1,227,091	107	5h 21m (3min)

저장 데이터 대비 분석 케이스는 IDS가 제일 많았으며 Anti-Virus가 가장 적었다. 1건당 분석시간 소요 기준으로는 윈도우 감사로그가 3분으로 가장 짧았고 Anti-Virus 120분으로 가장 길었다. 연구결과, 윈도우 감사로그가 저장되는 로그가 제일 많았지만 분석 케이스 및 분석에 걸리는 시간은 저장로그 수치 대비 가장 효율적으로 확인되었다.

V. 결론

본 연구논문에서는 대량의 윈도우 감사로그를 바탕으로 악의적인 보안위협에 대한 로그를 실시간 탐지 및 대응 할 수 있는 방안에 대해 제시하였다. 더 좋은 방법은 윈도우 감사로그만 보는 것보다 이기종 보안분석 시스템을 함께 로그 분석하는 것이 효율성면에서 더욱 좋을 수 있으므로 여러 가지 시나리오에 대해 파악하고 만드는 것이 중요하다.

또한, 침해사고 피해를 입고 대응 하는 것보다는 보안 위협을 사전에 탐지하고 분석가가 빠른 대응을 할 수 있도록 우선순위가 높은 로그를 경고하는 보안 로그 분석 프레임 워크를 사전에 만들고 제공해야 한다[5].

향후 본 논문에서 연구한 내용과 더불어 이기종 보안 시스템 및 서버로그, 웹 로그 등을 활용하여 보안위협 및 침해사고 모니터링 및 분석하는데 있어 성능 및 효율성 등을 추가 분석하는 연구를 진행 할 예정이다.

[참고문헌]

[1] Konstantin Berlin, David Slater, Joshua Saxe, “Malicious Behavior Detection using Windows Audit Logs”,AISec '15,1,2015.10

[2] 바이러스토탈 (Virustotal) (https://www.virustotal.com)

[3] 지능형 지속 공격(APT) (https://ko.wikipedia.org/wiki/지능형_지속_공격)

[4] 김완집, 염흥열,“이기종 로그에 대한 통합관리와 IT 컴플라이언스 준수”, 한국정보보호학회,제 20권 5호,3,2010.10

[5] Zhou Li, Alina Oprea,“Operational security log analytics for enterprise breach detection”, IEEE Cybersecurity Development Conference,8,2016

조건문을 통한 점프테이블 크기 유추에 따른 인다이렉트 점프 주소 계산 방법*

김문회† , 하동수, 오희국‡

한양대학교 컴퓨터공학과

*A Method of Calculating Indirect Jump Address by Analogy with the Size of Jump Table based on Conditional Branch Statement**

Wenhui Jin† , Dongsoo Ha, Heekuck Oh‡

Department of computer science and engineering, Hanyang University.

Abstract

Indirect jump target address is difficult to calculate and many researches tried to solve this problem to increase the accuracy of disassembly. Most of existing researches focus on the identification of the switch-case code when disassembly the stripped binary code. And the method they used to disassembly the jump table is incorrect when facing some unusual cases. While when we analyzing the binary files we found that there have some unusual code can not be disassembly well. When disassembler facing these unusual code it will give up to calculate the index of jump table and just linear disassembly the rest code. In this paper we purpose a heuristic method that calculate the size of jump table by analyzing the compare instruction patterns. We collecting all possible patterns by analyzing existing binary code to improve the accuracy of disassembly and this may also be helpful to those who are developing disassembler did not consider these unusual patterns.

I. Introduction

Disassembly as a basic technical used in several security researches such as binary instrumentation, binary-level vulnerability search, CFI integrity, etc.

Disassembly technique also contains static and dynamic. In this paper we issues the static disassembly technique for stripped binary.

Even though there have so many researches about static disassembly, it is well - known that static disassembly is an unsolved problem[1]. One of the challenges is that the address of indirect control flow target address is difficult to calculate because its calculation rely on values in other registers or in memory, especially the switch-case and exception handler code.

Each branches of the switch-case uses values in a register or memory to calculate the index in to a jump table and reads the jump address from the jump table and jump

* 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ITCT연구센터육성지원사업의 연구결과로 수행되었음(IITP-2018-2014-1-00636)
이 논문은 2015년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2015R1D1A1A09058200)

† 주저자 : jinwenhui@hanyang.ac.kr

‡ 교신저자 : hkoh@hanyang.ac.kr

there. The way they calculate the index is different and difficult to predict. So many disassembly tools give up to calculate the indirect jump target and linearly disassembly each branch part when they can not identify the length of some jump table.

In this paper we focus on how to calculate the index of the jump table. As our experiment we found that the this is possible to collect. we purpose a heuristic method to solve the problem by collecting all the switch-case jump table index calculation pattern by analyzing 1000 library files in android. And we implement the disassembler by the purposed method.

We discuss the related work in Section 2, our results in Section 3, conclusion in Section 4.

II. Related work

There also have many research try to improve the accuracy of indirect jump. BinCFI[1] purpose a method that they identified the properties of jump table: (1) jump table targets are intra-procedural. (2) target address is computed using simple operation such as addition and multiplication. (3) except index other quantities involved in the computation are constants. (4) they set the index length 50. Based on these characteristics they first identifies the function boundaries and the instructions that perform indirect jump, at least they enumerate possible values for the index variable and compute the jump target for each value, check if it falls within the current region.

UROBOROS[2] also using the similar way that BinCFI used but Ramblr's[3] is different. Both UROBOROS[2] and Ramblr[3] focus on the identification of the jump table because they adopt the symbolization way to disassembly. In regard to the jump target, Ramblr[3] recover the entries of jump table and all possible jump targets through the value-set analysis method and then check the available target address.

In our solution, we also using the similar way with BinCFI that combines the linear and recursive algorithms. But the difference is that we would like to identify each branch case addresses and calculate the index of the jump table accurately such that we can locate the branch address accurately. So we do not try to calculate all possible target address but through collecting the calculation pattern by disassembled library binary files in android. In the end, calculate the accurate jump target address.

III. Our result

There have 3 basic pattern when calculate the length of jump table index. As Figure 1 shows, when analyzing the libc.so file which locate in android libraries, there has one pattern that first compare an immediate value with the input value stored at register R1. Then calculate the jump table index value and assign to the PC register such that program next will jump to corresponding address to execution.

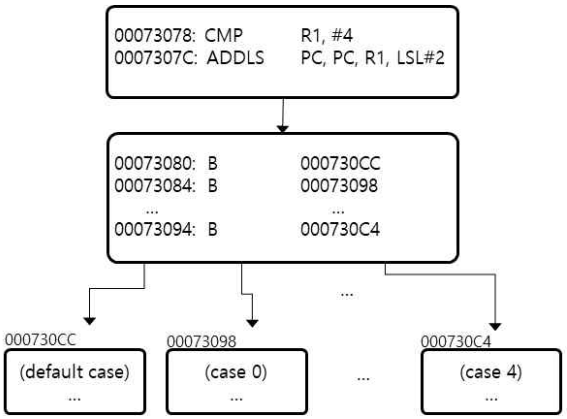


Figure 1 ADDLS

**ADDLS PC, PC, R1, LSL#2*

*if R1 <= 4, then PC = (PC+4) + R1*4*

There also have another pattern that program used much as figure 2. This pattern

also first compare an immediate value with the input value stored at register R1. Then if the input value is larger than the immediate value then jump to the default case address, otherwise using the TBB instruction to calculate the jump table index value.

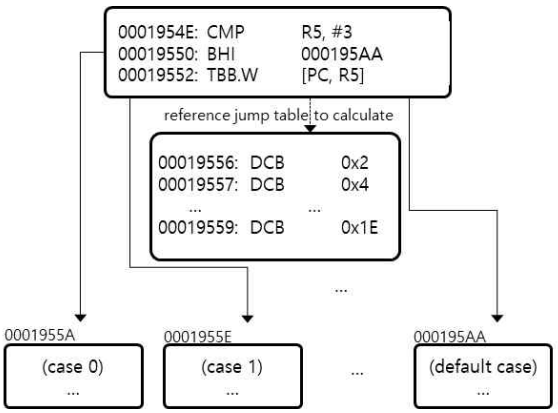


Figure 2 TBB

TBB.W[PC, R1]

*PC = (PC+4) + 2 * jumptable[R1].*

In this pattern program reference the jump table and assign corresponding address to the PC register. Similarly, TBH instruction also using the same way like Figure 3, But the difference between TBB and TBH instruction is that TBB instruction calculate the address with a byte and the TBH instruction with a word.

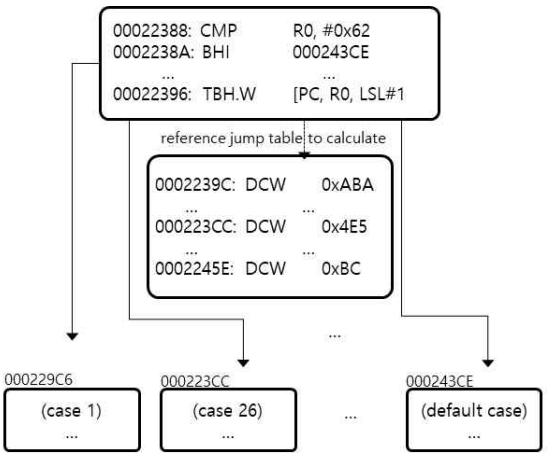


Figure 3 TBH

TBH.W[PC, R1, LSL#1]

PC = (PC+4) + 2 jumptable[R1].*

With this way we plan collecting all the possible patterns of jump table index calculation.

IV. Conclusion

As mentioned above, most papers they considering how to identify the switch-case code but did not considering the different way about the calculation of jump table such that with some cases most disassembler can not disassembly that part successfully. For this reason we want to collecting the patterns to improve the accuracy of disassembly.

Moreover, it is helpful that existing disassembler can update their code based on this research. For people who would like to develop disassembler it is also helpful for them.

V. Future work

In this paper, we just shows the most common patterns that program calculate the jump table index of switch-case. There also have some unusual patterns that we are analysing now, in which situation these pattern appear and how the compiler generate these patterns is also a problem we are interested.

Futhermore, we just testing the library files in android with arm64 architecture and we will continues test more samples.

[참고문헌]

[1] Zhang, Mingwei, and R. Sekar. "Control Flow Integrity for COTS Binaries." USENIX Security Symposium. 2013.

[2] Wang, Shuai, Pei Wang, and Dinghao Wu. "Reassembleable Disassembling." USENIX Security Symposium. 2015.Wang, Ruoyu, et al.

[3] Wang, Ruoyu, et al. "Ramblr: Making Reassembly Great Again." Proceedings of the 24th Annual Symposium on Network and Distributed System Security (NDSS'17). 2017.

전자파 오류 주입을 통한 인증 우회 공격
- Case Study : 지문 인식 시스템

이종혁*, 조영진**, 한동국*,***

*국민대학교 금융정보보안학과, **한국정보통신기술협회, ***국민대학교 정보보안암호수학과

Authentication Bypass Attacks By Electromagnetic Fault Injection

JongHyeok Lee*, Young-Jin Cho**, Dong-Guk Han*,**

*Dept. of Financial Information Security, Kookmin University,

**Telecommunications Technology Association,

***Dept. of Information Security, Cryptology, and Mathematics, Kookmin University

요 약

오류 주입 공격은 공격 대상 디바이스에서 특정 연산이 수행될 때, 순간적인 물리적 오류를 주입하여 오동작을 유도하고 그 결과를 이용하여 비밀 정보를 분석하는 강력한 공격 방법이다. 과거에는 암호 알고리즘에 대한 오류 주입 공격이 주된 관심사였지만, 최근에는 인증 과정에 오류를 주입하여 이를 우회하는 방법에 대한 연구가 활발하게 이루어지고 있다. 본 논문에서는 인증 과정에서 사용 가능한 4가지 if-else 조건문 기반 인증 알고리즘들을 대상으로 전자파 오류 주입 공격을 소개한다. 아두이노 보드에 상용 지문 인식 키트를 연결하여 4가지 if-else 조건문 기반 인증 알고리즘들을 구현하여 실험 환경을 구성하였다. 실험 결과 4가지 방식 모두 100%의 성공률로 전자파 오류 주입을 통한 지문 인증 과정의 우회가 가능함을 보인다.

I. 서론

1996년, P. Kocher는 수학적으로 안전성이 증명된 암호 알고리즘이 실제 디바이스에서 동작할 때 발생되어지는 다양한 물리적 정보들을 이용하여 비밀 정보를 분석하는 것이 가능함을 보였다[11]. 부채널 분석(Side Channel Attack, SCA)은 실제 디바이스에서 발생하는 부가적인 정보(동작 시간, 소비 전력, 전자파 등)를 통해 비밀 정보를 분석하는 공격 방법이다.

부채널 분석은 크게 두 가지 방식으로 분류된다[3]. 첫 번째 분류 방식은 공격 대상에 대한 물리적인 조작 정도에 따라 침투 공격(Invasive Attack), 준침투 공격(Semi-invasive Attack), 비침투 공격(Non-invasive Attack)으로 구분하는 방식이다. 물리적인 조작이란 일반적으로 칩 표면으로부터 패키지를 제거하는 디캡슐레이션(Decapsulation)을 의미한다. 두 번째 분류 방식은 공격 대상에 외부로부터 인위적인 변경을 가하는 여부에 따라 능동적 공격(Active Attack)과 수동적 공격(Passive Attack)으로 구분하는 방식이다[4]. 수동적 공격 방법에는 공격 대상에서 발생하는 부가적인 정보에 대한 측정만으로 비밀 정보를 분석하는 시간 분석(Timing Attack)과 전력 분석(Power Analysis) 등이 있다[4, 11, 12]. 능동적 공격 방법은 공격 대상에 직접적인 물리적 조작을 가하여 비밀 정보를 분석하는 오류 주입 공격(Fault Injection Attack)이 대표적이다. 오류 주입 공격은 실제 디바이스에서 특정 알고리즘이 동작할 때, 외부에서 인위적인 오류를 주입하여 오동작을 유도하며 그 결과를 이용하여 비밀 정보를 분석하는 매우 강력한 공격 방법이다[10]. 클락 글리치 공격(Clock Glitch Attack), 레이저 오류 주입 공격(Laser Fault Injection Attack), 전자파 오류 주입 공격(Electromagnetic Fault Injection Attack)이 대표적인 공격 방법이다[8,

9, 10].

기존의 오류 주입 공격들은 대부분 암호 알고리즘에 오류를 주입하여 비밀 키를 분석하는 방법에 대한 연구들이다. 그러나 최근에는 인증 과정에 오류를 주입하여 이를 우회하는 방법에 대한 연구나 부팅 시스템에 오류를 주입하여 시큐어 부트(Secure Boot)를 우회하는 연구가 활발하게 수행되고 있다[3].

본 논문에서는 인증 과정에서 사용 가능한 4가지 if-else 조건문 기반 인증 알고리즘들을 대상으로 전자파 오류 주입 공격을 소개한다. 아두이노 보드에 상용 지문 인식 키트를 연결하여 4가지 if-else 조건문 기반 인증 알고리즘들을 구현하여 실험 환경을 구성하였다. 실험 결과 4가지 방식 모두 100%의 성공률로 전자파 오류 주입을 통한 지문 인증 과정의 우회가 가능함을 보인다.

II. 전자파 오류 주입 공격 (Electromagnetic Fault Injection Attack)

전자파 오류 주입 공격은 다른 종류의 오류 주입 공격들과 유사하면서도 조금 다른 특징들을 갖는다. 클락 글리치 공격과는 로직 타이밍 위반을 유도할 수 있다는 점에서 유사하고, 레이저 오류 주입과는 트랜지스터의 오동작을 유도할 수 있다는 점에서 유사하다. 하지만 최근에 대부분의 칩 제조사들이 클락 글리치 공격이나 레이저 오류 주입 공격을 방지하기 위해 비정상 클락 감지 센서, 칩 디캡슐레이션 방지 쉴드, 레이저 감지 센서 등 칩 설계 과정에서부터 다양한 대응 기법들을 적용하고 있어 오류 주입 공격을 수행하는 것이 쉽지 않다. 그러나 전자파 오류 주입 공격은 칩 디캡슐레이션 과정이 필요하지 않기 때문에 위와 같은 대응기법에 영향을 받지 않고 공격이 가능하다.

그림 1은 전자파 오류 주입 공격의 원리에 대한 설명이다. 전자파 오류 주입 공격은 전자파 프로브 팁에 순간적인 전류를 흘려 전자기 유도 현상을 발생시킨다. 프로브 팁은 페라이트(Ferrite)에 코일을 감은 형태로 코일에 순간적

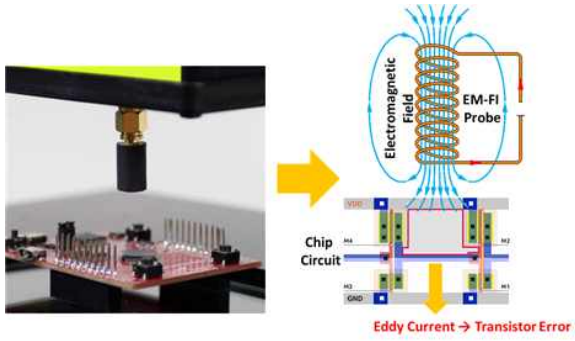


Fig. 1. Principle of an electromagnetic fault injection attack

으로 전류가 흐르면 코일 주변에 전자기장이 발생하고, 자속(Magnetic Flux)에 의해 칩 회로에 와전류(Eddy Current)가 생성되어 트랜지스터에 영향을 끼치게 된다. 이로 인해 칩의 오작동이 발생한다[6, 17, 20].

III. 실험 환경

본 실험에서는 Adafruit 社에서 판매하는 지문 인식 센서[1]와 아두이노 우노 보드[2]를 사용한다. 지문 인식 코드는 제조사에서 제공하는 오픈 소스를 사용한다[7]. 실험의 현실성을 위해 트리거 정보를 제외한 코드의 수정은 최소화하였다.

그림 2는 실험 환경 구성도이다. Riscure 社의 Spider[16], EM-FI Transient Probe[14], EM Probe Stateion[13]을 사용하였으며 소프트웨어로는 부채널 분석 통합 소프트웨어인 Inspector와 데이터 분석 웹 어플리케이션인 FI-GraphIt[15]을 사용하였다. 표 1과 같이 지름과 극성에 따른 4가지 프로브 팁이 존재하며 본 실험에서는 RB 프로브 팁을 사용한다.

Abbreviation	Diameter	Polarity
RS	1.5 mm	Positive
BS	1.5 mm	Negative
RB	4 mm	Positive
BB	4 mm	Negative

Table 1. Type of probe tip

프로그래밍 언어에서 if-else 조건문은 입력값에 대해 조건이 참인지 거짓인지에 따라 다

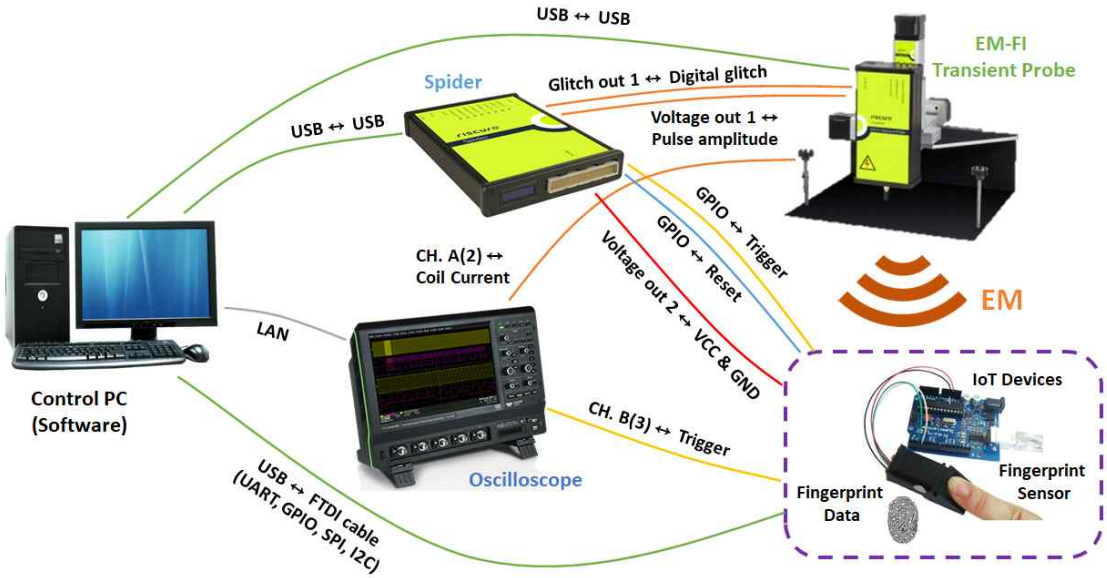


Fig. 2. Experimental configuration diagram

른 코드를 실행시키는 분기문의 한 종류이다. 판단 조건에 따라 동일한 결과를 도출하는 다양한 구현 방식이 존재한다.

if-else V1	if-else V2

if(p == FOUND)
  return SUCCESS;
else
  return FAILURE;
	if(p != NOFOUND)
	  return SUCCESS;
	else
	  return FAILURE;

if-else V3	**if-else V4**

if(p == NOFOUND)
  return FAILURE;
else
  return SUCCESS;
	if(p != FOUND)
	  return FAILURE;
	else
	  return SUCCESS;

Table 2. Four if-else condition codes

표 2는 본 실험의 대상이 되는 4가지 방식의 if-else 조건문이다. 본 실험에 사용된 지문 인식 키트의 경우, p는 스캔된 지문을 데이터베이스에 저장된 지문들과 비교한 결과를 저장하고 있는 변수이다. 'FOUND'는 스캔된 지문과 일치하다고 판단되는 지문이 데이터베이스에 저장되어 있음을 의미하고 'NOFOUND'는 그렇지 않음을 의미한다. 따라서 p 값이 'FOUND'인 경우 인증에 성공한다.

IV. 실험 결과

본 절에서는 아두이노 코드 상에서 전자파 오류 주입 공격으로 인해 발생 가능한 결과들을 설명하고 실제 공격을 수행했을 때 결과를 비교한다.

4.1 예상 가능한 실험 결과

아두이노 코드 상에서 오류 주입 공격으로 인해 발생 가능한 결과는 크게 두 가지이다. 첫 번째는 'jump 명령어 무시'이고 두 번째는 'p 값에 대한 변조'이다. 최종적으로 두 가지 결과 모두 'return SUCCESS' 코드를 실행시킨다.

1) jump 명령어 무시: if-else 조건문은 주어진 판단 조건(p == FOUND 등)에 따라 if 문 아래의 코드를 수행할지 else 문 아래의 코드를 수행할지 결정한다. 판단 조건에 거짓이 되는 입력 값이 주어진 경우, else 문 아래의 코드를 수행하기 위해 jump 명령어가 존재한다. 만약 공격자가 jump 명령어가 수행될 시점에 오류를 주입하여 jump 명령어가 수행이 되지 않게 한다면, 판단 조건에 거짓이 되는 입력 값이 주어졌음에도 if 문 아래의 코드를 수행할 수 있다. 이것이 첫 번째 예상 가능한 결과이다. 이와 같은 결과는 if문 아래의 코드가 'return SUCCESS'인 표 2의 if-else V1과 if-else V2에서 발생 가능하다.

2) p 값에 대한 변조: 본 실험에서 사용된 지문 인식 센서 제조사에서 제공하는 코드는 다음과 같은 과정을 통해 p 값을 생성한다. 우선 'finger.getImage()' 함수를 통해 지문 이미지를 스캔하고 'finger.image2Tz()' 함수로 스캔한 이미지를 데이터베이스에 저장되어 있는 지문 데이터 형태로 바꾼다. 마지막으로 'finger.fingerFastSearch()' 함수로 데이터베이스에 저장된 지문 데이터 중 현재 스캔한 지문과 유사도가 높은 데이터가 존재하는지 찾는다. 그 결과 존재하면 0x00(FOUND)을 p에 할당하고 그렇지 않으면 0x09(NOFOUND)를 할당한다.

본 실험에서는 데이터베이스에 저장되어 있지 않은 지문으로 우회가 가능함을 보여야 되기 때문에 p에 0x09가 저장되어 있음을 가정한다. 일반적으로 전자파 오류 주입을 통해 변수 값을 공격자가 원하는 특정 값으로 변경시키는 것은 어렵다고 알려져 있다. 하지만 0x00이나 0xFF와 같은 특별한 값의 경우는 가능하다. 따라서 본 실험은 두 가지 경우의 변조가 가능하다. p 값을 0x00으로 변조하는 경우와 p 값을 랜덤한 값으로 변조하는 경우이다. p 값을 0x00으로 변조하는 경우 표 2의 4가지 방식 모두 다 공격이 가능하지만 랜덤한 값으로 변조한 경우 if-else V2와 if-else V3에서 우회가 가능하다.

4.1 실제 실험 결과

그림 3은 아두이노 우노 보드의 마이크로컨트롤러를 가로축으로 86등분, 세로축으로 14등분 하여 오류 주입 공격으로 인증 우회가 가능한 영역을 표시하였다. 각 포인트마다 오류 주입을 5회 수행하였다. 초록색 점은 인증 우회에 실패한 지점이고 빨간색 점은 인증 우회에 성공한 지점이다. 그리고 노란색 점은 인증 과정이 중간에 종료되는 등의 비정상적인 동작이 수행된 지점을 의미한다. p 값에 대한 특정한 혹은 랜덤한 값으로의 변조로 인해 우회가 가능한 if-else V2와 if-else V3는 광범위한 영역에서 우회가 가능하였다. p 값을 특정한 값(0x00)으로 변조했을 경우만 인증 우회가 가능한 if-else V4의 경우도 여러 영역에서 인증 우회가 가능하였다.

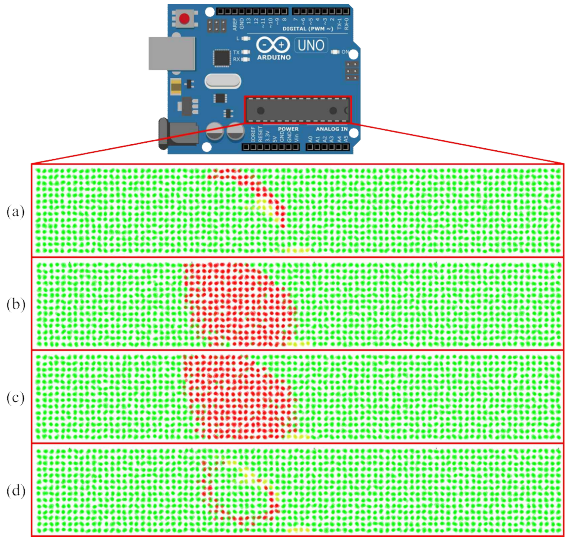


Fig. 3. Electromagnetic fault injection area of vulnerability for (a) if-else V1 (b) if-else V2 (c) if-else V3 (d) if-else V4

각 구현 방식마다의 인증 우회 성공 포인트 한 곳을 선택하여 펄스 세기와 트리거로부터의 지연 시간에 변화를 주어 실험을 진행하였다. 펄스 세기는 50%부터 80%까지 10단위씩 변화를 주었고 트리거로부터의 지연 시간은 0ns부터 300ns까지 10단위씩 변화시켰다. 실험 결과는 그림 4부터 그림 7까지이다. 각 그림의 상단은 전자파 펄스 세기 별 수행 횟수이며 하단은 트리거로부터의 지연 시간 별 수행 횟수이다. 그림 3과 마찬가지로 실험 결과를 색깔로 구분하였다. if-else V2와 if-else V3는 그림 3의 결과와 마찬가지로 유사한 결과를 보였고 지연 시간이 80ns부터 280ns까지 전반적으로 우회가

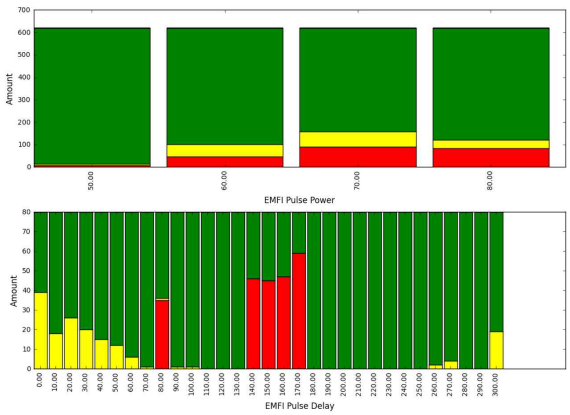


Fig. 4. Histogram of pulse power and pulse delay in if-else V1

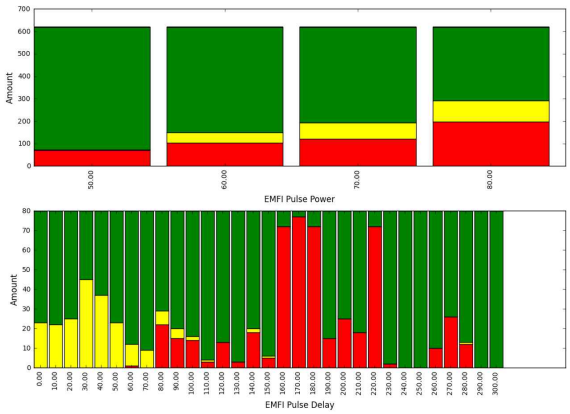


Fig. 5. Histogram of pulse power and pulse delay in if-else V2

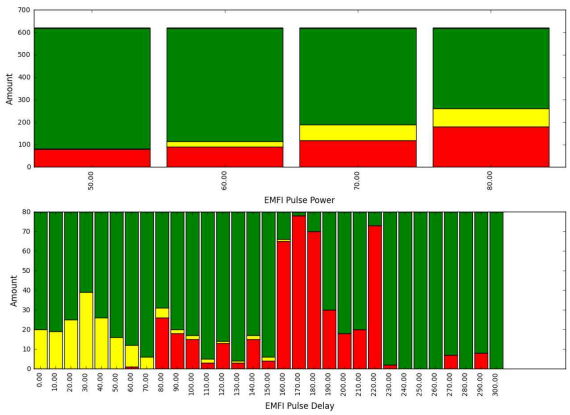


Fig. 6. Histogram of pulse power and pulse delay in if-else V3

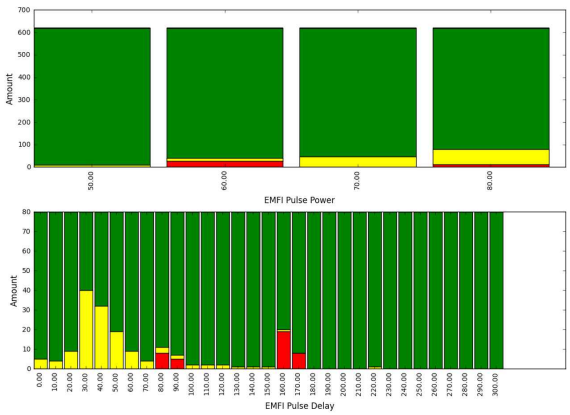


Fig. 7. Histogram of pulse power and pulse delay in if-else V4

가능하였다. 반면에 if-else V4의 경우, 60%의 펄스 세기와 80~90ns와 160~170ns인 조건에서 우회가 가능하였다.

if-else V4에서 최고의 성공률을 찾기 위해 최적의 파라미터를 찾는 실험을 추가적으로 진행하였다. 그 결과, 그림 3(d)의 (37, 5) 포인트에서 펄스 세기는 67%, 트리거로부터의 지연 시간을 163ns로 설정한 경우 1000회 전자파 오류 주입을 수행한 결과 100%의 성공률로 인증 우회가 가능하였다. 나머지 3가지 경우 모두 최적의 파라미터에서 100%의 성공률로 인증 우회에 성공하였다.

V. 결론

본 논문은 인증 정보 생성 과정이 아닌 생성된 인증 정보를 비교하는 부분에 대해 전자파 오류 주입을 통한 인증 우회 공격에 대한 연구이다. 상용 지문 인식 키드를 아두이노 우노 보드와 연결하여 프로토타입의 실험 환경을 구성하였다. 그리고 생성된 인증 정보를 비교하는데 주로 사용되는 if-else 문을 판단 조건에 따라 4가지 방식으로 구분 짓고 각각의 방식마다 인증 우회 실험을 진행하였다. 그 중 가장 안전하다고 여겨지는 if-else V4의 경우에도 최적의 파라미터에서 100%의 성공률로 전자파 오류 주입을 통한 인증 우회가 가능함을 보였다.

최근 생체 인증이 주목을 받으면서 도어락이나 스마트폰 등의 상용 장비에서 지문 등의 생체 정보를 활용한 사용자 인증 기술이 널리 사용되고 있다. 따라서 상용 장비를 대상으로 한 인증 우회 실험이 필요하다.

[사사] 이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2017-0-00380, 차세대 인증 기술 개발)

[참고문헌]

[1] Fingerprint sensor, https://www.adafruit.com/product/751

[2] Arduino Uno, https://store.arduino.cc/usa/arduino-uno-re

v3

[3] A. Vasselle, H. Thiebeauld, Q. Maouhoub, A. Morisset, and S. Ermeneux, “Laser-induced Fault Injection on Smartphone Bypassing the Secure Boot”, Fault Diagnosis and Tolerance in Cryptography (FDTC), 2017 Workshop on, IEEE, pp.41-48, 2017.

[4] E. Brier, C. Clavier, and F. Olivier, “Correlation Power Analysis with a Leakage Model,” International Workshop on Cryptographic Hardware and Embedded Systems, LNCS 3156, pp.16-29, 2004.

[5] F. Koeune, and F. X. Standaert, “A Tutorial on Physical Security and Side-Channel Attacks,” Foundations of Security Analysis and Design III, LNCS 3655, pp.78-108, 2005.

[6] G. Thessalonikefs, “ElectroMagnetc Fault Injection Characterization,” MS thesis, University of Amsterdam, 2014.

[7] Adafruit fingerprint sensor library, https://github.com/adafruit/Adafruit-Fingerprint-Sensor-Library

[8] J. Balasch, B. Gierlichs, and I. Verbauwhede, “An In-depth and Blackbox Characterization of the Effects of Clock Glitches on 8-bit MCUs,” Fault Diagnosis and Tolerance in Cryptography (FDTC), 2011 Workshop on, IEEE, pp.105-114, 2011.

[9] J. J. Quisquater, and D. Samyde, “Eddy Current for Magnetic Analysis with Active Sensor,” Proceedings of Esmart, 2002, pp.185-194, 2002.

[10] M. Joye, and M. Tunstall, “Fault Analysis in Cryptography,” Springer, ISBN 978-3-642-29656-7, 2012.

[11] P. C. Kocher, “Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and other systems,” Annual International Cryptology Conference, LNCS 1109, pp.104-113, 1996.

[12] P. C. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis,” Annual International Cryptology Conference, LNCS 1666, pp.388-397, 1999.

[13] EM Probe Station, https://www.riscure.com/uploads/2017/07/datasheet_emprobestation.pdf

[14] EM-FI Transient Probe, https://www.riscure.com/product/em-fi-transient-probe/

[15] Inspector, https://www.riscure.com/uploads/2017/08/inspector_brochure.pdf

[16] Spider, https://www.riscure.com/uploads/2017/07/spider_datasheet_1.pdf

[17] S. Carlier, “Electro Magnetic Fault Injection,” MS thesis, University of Amsterdam, 2012.

[18] S. Mangard, E. Oswarld, and T. Popp, “Power Analysis Attacks: Revealing the Secret of Smart Card,” Springer, ISBN 987-1-4419-4039-1, 2007.

[19] S. P. Skorobogatov, and R. J. Anderson, “Optical Fault Induction Attacks,” International Workshop on Cryptographic Hardware and Embedded Systems, LNCS 2523, pp.2-12, 2002.

[20] T. Hummel, “Exploring Effects of Electromagnetic Fault Injection on a 32-bit High Speed Embedded Device Microprocessor,” MS thesis, University of Twente, 2014.

2018 한국정보보호학회 하계학술대회

C6 여성과학자

심 미 나 (성결대학교)

- **블록체인 기반 개인정보 처리 추적 관리 시스템 모델 제안**
  김미연, 염흥열
- **ECG를 이용한 인증 시스템에 대한 원격 공격 가능성 분석**
  이선우, 이동훈
- **C++의 동적 디스패치에 적용된 제어 흐름 무결성 검증기법 분석**
  장혜린, 박문찬, 진홍주, 이동훈
- **Invited talk : 지금 시대가 필요로 하는 정보보호 인재상**
  윤혜정 실장(인터파크)

블록체인 기반 개인정보 처리 추적 관리 시스템 모델 제안*

김미연* 염흥열**

*순천향대학교 융합서비스 보안학과 **순천향대학교 정보보호학과

A Proposal for the PII Processing Tracking System based on Blockchain

Mee Yeon Kim, Heung Youl Youm

*Department of convergence service security, **Department of information security engineering, Soonchunhyang University.

요 약

기존의 개인정보 처리 환경은 서류를 기반으로 하며, 간접적으로 처리내역을 알리고 있다. 때문에 정보주체는 초기 동의 후 개인정보에 대한 통제성을 전혀 갖지 못하며, 인가되지 않은 개인정보의 이전이 빈번하게 일어나고 있다. 개인정보 처리내역의 불투명성과, 정보주체가 개인정보를 추적·통제할 수 없는 기존환경의 문제점은 정보 주체의 불편을 초래할 수 있으며, 개인정보에 대한 권리를 떨어뜨린다. 이에 개인정보 이전 및 사용에 대한 기록을 블록체인에 남겨 개인정보 이용(처리)의 투명성, 추적성, 통제성을 보장하는 개인정보 사용 추적 관리 시스템 모델을 본 논문에서 제시하고자 한다. 개인정보 처리를 제한하며, 처리내역을 추적할 수 있는 블록체인 기반의 시스템의 모델을 상위레벨 수준에서 제안하고자 한다.

I. 서론

기존의 개인정보 처리 환경은 서류를 기반으로 하며, 간접적으로 처리내역을 알리고 있다. 때문에 정보주체는 초기 동의 후 정보주체에 의한 개인정보 처리에 대한 통제성을 전혀 갖지 못하며, 인가되지 않은 개인정보의 이전이 빈번하게 일어나고 있다. 개인정보 처리내역의 불투명성과, 정보주체가 개인정보를 추적·통제할 수 없는 기존환경의 문제점은 정보주체의 불편을 초래할 수 있으며, 개인정보에 대한 정보주체의 권리를 떨어뜨린다.

이에 개인정보 이전 및 사용에 대한 기록을 블록체인에 남겨 개인정보 사용의 투명성, 추적성, 통제성을 보장하는 개인정보 사용 추적 관리 시스템을 본 논문에서 제시하고자 한다.

* 본 연구는 과학기술정보통신부 및 한국인터넷진흥원의 "고용계약형 정보보호 석사과정 지원사업"의 연구결과로 수행되었음

블록체인은 대표적인 암호화폐인 비트코인에서 처음으로 사용된 분산원장기술(distributed ledger technology)이다. 블록체인에서는 거래된 내역을 블록 단위로 저장하고, 각 블록이 해시체인으로 서로 연결되어 정보 추가 외에 정보 변경이 힘든 특성을 가진다. 또한, 투명하게 데이터를 분산 저장하는 탈중앙화된 특성이 있다. 이러한 특성으로 블록체인은 새로운 기술 패러다임을 불러왔으며, 다양한 분야에서 활용될 것을 예측하고 있다.

국외에서는 블록체인을 도입하여 정보자원에 대한 접근통제를 실시하고자 하는 연구가 다수 진행되었다. [1]에서는 IoT 기기에 스마트 컨트랙트 기반의 접근통제를 실험적 단계 수준으로 구현하였다. [2],[3]은 블록체인 기반 접근통제 시스템을 연구하여 개인정보권을 향상시키고자 한 논문으로 [2]는 네트워크 프로토콜의 정의를 개발하였고, [3]은 이더리움을 통해 실험적 단계 수준으로 구현한 것이 특징적이다. 그러나 국내

에서는 관련 연구를 찾아보기 힘든 실정이다. 따라서 본 논문에서는 개인정보 처리를 제한하며, 처리내역을 추적할 수 있는 블록체인 기반의 시스템의 모델을 상위레벨 수준에서 제안하고자 한다.

본 고 2장에서는 제안하는 시스템의 모델을 정립하기 위해 시스템 환경 및 시스템 요소에 대하여 서술하였다. 3장에서는 본 시스템에 기반하여 시나리오 예시를 제시하였다. 마지막으로 결론에서 향후 연구에 대한 방향성을 제시하며 마무리 짓는다.

II. 블록체인 기반 개인정보 사용 추적 관리 시스템 모델 정립

2.1 기존 환경의 문제

기존의 개인정보 처리 환경은 서류 기반 약관으로 동의를 얻으며 이후 개인정보 처리자에 의해 처리(이용, 제공, 저장, 출력, 가공 등)되며 파기하기에 이른다. 그러나 수집된 개인정보의 처리 현황은 개인정보 처리자의 통보에 의해 간접적으로 알 수 있을 뿐이고, 초기 동의 후 정보주체는 개인정보에 대한 통제성을 전혀 갖지 못한다. 또한 개인정보가 제3자에게 제공되거나 위탁하는 경우, 고지 혹은 동의로 알림을 받지만 직접적으로 추적할 수 없고 인가되지 않은 개인정보의 이전이 빈번하게 일어날 수 있다. 개인정보의 파기 또한 개인정보 처리 방침으로 공개되고 있으나 파기가 제대로 일어나고 있는지 추적·통제가 불가능하여 사용자의 불편을 초래하는 문제를 안고 있다.

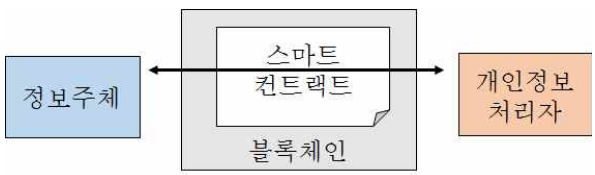
이러한 문제를 해결하기 위하여 본 논문은 스마트 컨트랙트 (smart contract) 기반의 개인정보 사용추적 관리 시스템을 제안한다. 본 시스템을 통해 스마트 컨트랙트에 기록된 약관을 기반으로 개인정보를 통제하며, 트랜잭션으로 개인정보 호출 내역이 남아 개인정보 처리 내역을 투명하게 확인할 수 있으며, 필요 시 추적이 가능할 수 있도록 모델을 제시하고자 한다. 이를 통해 정보 주체의 개인정보 통제권을 향상시키는 취지를 가진다.[3]

2.2 개인정보 사용추적 관리 시스템 모델

본 논문에서 수립하고자 하는 블록체인 기반 개인정보 사용 추적 관리 시스템 모델은 정보주체, 개인정보 처리자, 개인정보 수탁자로 구성된다.

- 정보주체: 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말하며[4], 자신의 개인정보를 개인정보 처리자 또는 수탁자에게 제공하는 자이다. 주로 서비스를 제공받기 위해 자신의 개인정보를 제공한다.
- 개인정보 처리자: 정보주체로부터 개인정보를 수집하여, 개인정보를 처리(수집, 이용, 제공, 저장, 출력, 가공, 폐기 등)하는 자로, 주로 서비스 제공자 역할을 수행한다.
- 개인정보 수탁자: 개인정보 처리자로부터 개인정보 처리 업무를 위탁받아 처리하는 자이다.[5] 개인정보 처리자를 통해 정보주체와 연결된다.

위 시스템에서는 스마트 컨트랙트를 통해 개인정보의 처리에 대한 제한 규정을 두어, 정보주체의 요구에 맞게 개인정보의 전송을 제한할 수 있다. 개인정보가 요청되었을 때, 규정에 의해 전송이 제한되지 않을 시에만 개인정보를 받을 수 있고, 전송 내역은 블록체인에 기록된다. 때문에 개인정보에 대한 통제성을 가질 수 있다. 또한 전송내역을 원장에 기록하여 모든 개인정보의 전송 내역을 확인할 수 있기 때문에 데이터 사용 내역에 대한 추적성과 투명성을 가질 수 있다. 일례로 개인정보 처리자가 개인정보를 개인정보 수탁자에게 전송할 때, 전송이 개인정보 사용 제한 규정을 위배하지 않아야 전송될 수 있고, 전송 내역이 로그로 기록된다.[6]



[그림 1] 정보주체와 개인정보 처리자 간의 스마트 컨트랙트 체결

정보주체의 개인정보는 off-chain 저장소(외부저장소)에 별도로 보관한다. 스마트 컨트랙트는 정보접근 권한만을 부여하며, 권한이 있는 경우에만 개인정보에 접근 가능하다. 정보주체

는 처리자와 정책 기반 개인정보 사용 계약을 생성하여 개인정보의 처리와 재배포를 제한하는 스마트 컨트랙트을 생성하여 블록체인에 등록한다. 개인정보 처리자는 개인정보를 이용할 시, 쿼리를 정보주체에게 전송하는 거래를 생성한다. 거래는 정보주체와 체결한 스마트 컨트랙트에 따라 권한이 적절한지를(계약을 체결한 처리자가 맞는지, 정책에 합당한지 등) 확인하여, 적절한 경우에만 결과값으로 개인정보를 반환한다. 그리고 일련의 거래가 블록체인에 기록된다. 위 모델에 따르면 기존에 있던 개인정보의 수집은 계약체결로, 처리는 거래로, 폐기는 계약의 폐기로 전환될 수 있다.

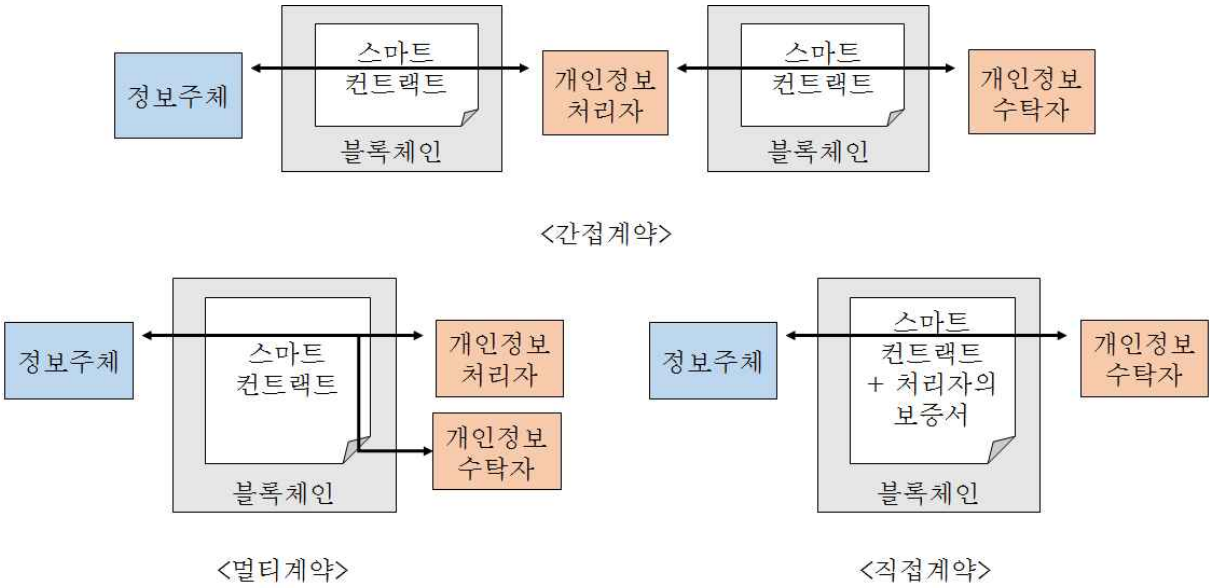
개인정보 처리자에서 수탁자로의 개인정보 이전은 개인정보 처리자와 수탁자 간의 계약 체결로 스마트 컨트랙트화 할 수 있다. 개인정보의 접근 권한을 위임하는 것으로, 이는 처리자를 통한 간접계약, 정보주체와 처리자, 수탁자사이 3자간의 멀티계약, 처리자의 보증을 포함한 정보주체와 수탁자의 직접계약 등 다양한 형태로 이루어질 수 있다. 첫째로 처리자를 통한 간접계약은 수탁자가 처리자와의 계약을 통해 개인정보를 이전받는 형식으로, 데이터는 정보주체에서 처리자로, 처리자에서 위탁자로 두 단계에 걸쳐 데이터가 전송된다. 두 번째로 정보주체와 처리자, 수탁자 모두의 키를 사용하여 멀티계약을 체결하는 방식으로, 기존의 multisig 방식과 유사하다. 마지막으로 개인정보 처리자는 수탁자에게 보증서를 부여하여, 정보주체와 위탁자 간의 직접계약에 보증서를 첨부하는 형태이며, 이는 개인정보 처리자의 통제권이 다소 상실하는 방법으로 볼 수 있다.

이렇게 개인정보 사용 계약을 통해 정책에 따라 개인정보가 처리되고 있는지를 확인할 수 있다. 또한 접근 요청 트랜잭션을 통해 개인정보 처리 내역이 기록되어 이를 감사할 수 있으며, 계약 정책이 잘 준수되고 있는지 추적할 수 있다.

2.3 시스템 요구사항

시스템에서는 개인정보는 약관에 따라 이용되어야 하며, 사용자는 개인정보 이용에 대한 통제권을 가져야 한다. 이러한 요구사항을 반영하기 위하여 개인정보에 대한 접근권한 통제 기능이 필요하다. 이 기능은 스마트 컨트랙트를 통해 구현된다. 즉 개인정보를 접근 가능한 자원으로 취급하는 일종의 접근통제시스템을 스마트 컨트랙트에 기반하여 구현하는 것이다.

또한 사용자는 개인정보의 처리 내역을 투명하게 확인할 수 있어야 하며, 개인정보 처리 내역을 추적할 수 있어야 한다. 이러한 요구사항을 반영하기 위해서는 개인정보에 대한 접근



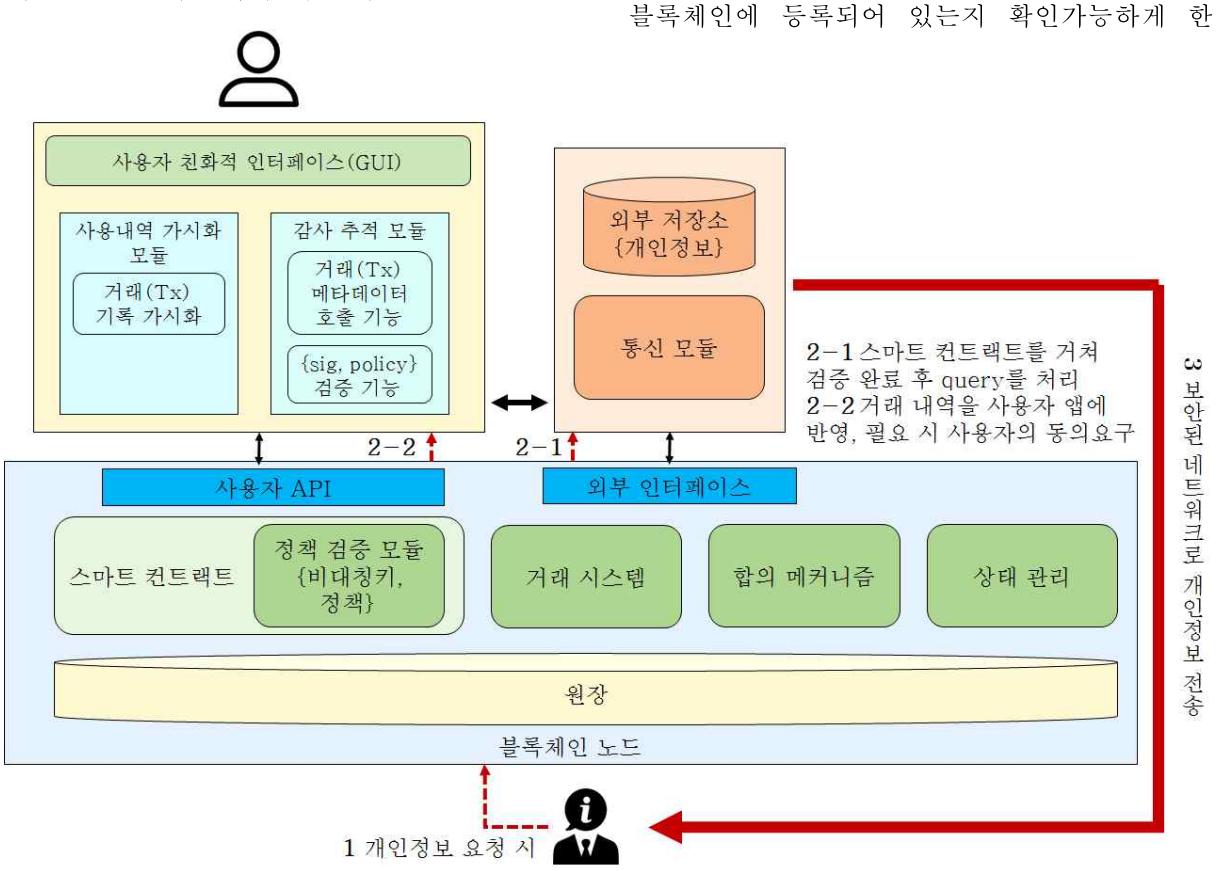
[그림 2] 정보주체와 개인정보 처리자, 개인정보 수탁자 간의 스마트 컨트랙트 체결 예시

기록, 즉 트랜잭션 기록을 확인하는 기능이 필요하며, 트랜잭션이 블록체인에 등재되었는지, 비대칭키쌍과 컨트랙트 상의 정책 등을 통해 트랜잭션이 유효한지 검증하는 기능이 필요하다.[2] 이는 사용자 디바이스에서 실행되는 별도의 경량 노드(lightweight node) 형태의 시스템을 만들어 구현될 수 있다.

정보주체, 개인정보 처리자, 수탁자가 사용할 블록체인 기반 개인정보 사용 추적 관리 시스템은 다음과 같이 나타낼 수 있다. 다음 그림은 블록체인에서 일반적으로 요구되는 모듈 및 기능은 일부 생략하였다.

여기서 개인정보는 접근 가능한 자원으로 외부저장소에 저장된다. 이에 대해 접근을 요청하는 자는 개인정보 처리자 및 수탁자가 포함이 되며, 접근을 부여하는 자는 정보주체 및 시스템이 된다. 블록체인은 일종의 접근통제서버처럼 작용된다. 블록체인 내의 스마트 컨트랙트 기능을 활용하여 정책 기반의 개인정보 접근통제를 구현한다. 이때 검증자(Authenticator)로 비대칭키와 정책을 사용하며 이 둘을 기반으로 개인정보 요청 쿼리에 대한 응답을 판단할 수 있다. (그러나 이에 한정되지 않는다.) 개인정보 요청에 대한 내역은 블록체인의 트랜잭션으로 저장되며, 원장데이터를 이룬다. 스마트 컨트랙트를 거쳐 검증이 완료되고, 권한이 적절한 경우에는 외부 저장소로부터 개인정보를 검색하여 별도의 보안된 네트워크로 요청자에게 개인정보를 전송한다.

사용자, 즉 정보주체의 디바이스에서 구현되는 시스템은 다음과 같이 볼 수 있다. 사용자의 디바이스는 대부분 모바일에서 사용될 점을 감안하여 경량 노드 형식으로 구현됨이 바람직하다. 사용내역 가시화 모듈은 블록체인 상에 기록된 사용자의 거래 기록을 받아와, 사용자가 쉽게 확인할 수 있는 형태로 나타내어 개인정보 사용 내역을 목록화한다. 감사추적 모듈은 필요시 원장으로부터 거래에 대한 메타데이터를 받아와 사용자가 쉽게 확인할 수 있는 형태로 나타내는 방식으로 나타내어, 해당 거래가 블록체인에 등록되어 있는지 확인가능하게 한



[그림 3] 블록체인 기반 개인정보 사용추적 관리 시스템 모델[8]

다. 또한 필요시, 검증자에 대한 재검증(re-verification)을 실시하는 기능을 추가하여 해당 거래의 유효성을 보장할 수 있다.

III. 대표 시나리오

본 논문에서 제시한 모델에 대한 이해를 돕고자 활용 시나리오 예시로, 정보주체와 앱스토어, 게임회사 간의 개인정보 활용 사례를 제시하였다. 정보주체를 '가'라는 개인으로, 개인정보 처리자로는 '나 앱스토어', 개인정보 수탁자를 '다 게임회사'라 하자. '가'는 최초에 '나 앱스토어'의 서비스를 이용하기 위하여 다음과 같은 예시의 스마트 컨트랙트 계약을 맺는다.

[표 1] 정보주체 가와 나 앱스토어 간의 스마트 컨트랙트 내용 예시

정보주체	가
개인정보 처리자	나 앱스토어
개인정보 수집항목	이름, 핸드폰번호, IMEI, 핸드폰기종, 결제수단관련정보 등
정책 예시 1	결제 시, 결제수단관련정보 및 이름 등을 얻을 수 있다.
정책 예시 2	특징적인 목적을 명시하지 않고 일반 목적을 위하여 개인정보 전 항목을 요구할 경우, 정보주체는 이를 거절할 수 있다.

이에 더해 정보주체 '가'는 '나 앱스토어'에 등록된 '다 게임회사'의 게임 애플리케이션 사용을 위하여, '나 앱스토어'를 통해 '다 게임회사'와 직접계약의 형식으로 개인정보 위탁 계약을 맺는다. 즉 '나 앱스토어'는 '다 게임회사'에 대한 보증서를 발급하고, 그를 '가'와 '다 게임회사' 간의 스마트 컨트랙트에 삽입하여 다음과 같은 스마트 컨트랙트를 체결한다.

[표 2] 정보주체 가와 다 게임회사 간의 스마트 컨트랙트 내용 예시

정보주체	가
개인정보 처리자(수탁자)	다 게임회사
보증서 발급자	나 앱스토어
개인정보 수집항목	이름, 핸드폰번호, 게임 id, IMEI, 핸드폰 기종, 결제수단관련정보 등
정책 예시 1	인앱 결제(예, 게임아이템 구매) 시, 결제수단관련정보, 게임 id, 핸드폰기종 등을 얻을 수 있다.
정책 예시 2	정보주체 동의 시, 다 게임회사는 IMEI, 이름, 핸드폰번호 등을 얻을 수 있다.

다음과 같은 상황을 가정해보자. '가'는 자신의 모바일 기기에서 게임 앱을 삭제하였다가, 이를 다시 복구하고 싶으나 본인의 게임id를 몰라 '다 게임회사'에 도움을 요청한 상황이다. 이때 게임회사는 트랜잭션을 생성하여 정보주체의 동의와 함께, 게임id와 IMEI를 외부저장소에 요구하는 쿼리를 정보주체에게 전송하고 정보주체는 이에 동의한다. 그러면 '다 게임회사'는 개인정보를 전송받아 '가'의 요구사항을 처리할 수 있고, '다 게임회사'가 그와 같은 목적으로 게임id, IMEI, 정보주체의 동의를 요구하였으며, 이에 정보주체가 동의하였다는 내역이 트랜잭션으로 남게 된다.

두 번째 상황으로는 정보주체 '가'가 게임아이템을 구매하는 상황이다. '다 게임회사'는 마케팅 전략을 위해 게임아이템을 구매한 개인의 성별, 나이, 핸드폰 기종 등을 수집하고자 하였다. 그래서 '가'가 게임아이템을 구매하자 가의 게임id, 핸드폰기종, 결제수단관련정보 외에 성별, 나이 등을 요청하였으나 이는 스마트 컨트랙트에 기록된 정책에 적절치 않으므로 요청이 거절된다. 또한 '다 게임회사'가 어떤 목적으로 어떤 항목을 요청했고, 이가 거절되어 해당 개인정보가 전송되지 않았다는 트랜잭션이 기록된다.

IV. 결론

본 논문에서는 블록체인과 스마트 컨트랙트에 기반하여 개인정보로의 접근통제 및 처리내역을 추적할 수 있는 시스템의 모델을 제안하였으며, 시스템을 활용하는 사례 시나리오를 작성하였다. 본 논문은 국내에서는 연구되지 않



[그림 4] 첫 번째 활용 시나리오 예시[1]

는, 블록체인을 활용한 접근통제 시스템에 대한 모델을 정립하였다는 점과, 그를 개인정보에 도입하여 정보주체의 프라이버시권을 향상하고자 하였다는데 의의를 가질 수 있다. 그러나 이는 실제 시스템의 구현과 활용 사례의 수집을 통해 보다 면밀한 검증이 필요하며 앞으로 이 분야에 대하여 다음과 같은 연구가 추가적으로 필요할 것이다.

첫째로, 본 시스템 상에서 활용가능한 스마트 컨트랙트의 구현에 대한 연구와 이에 대한 개인정보보호법 관점에서의 검토가 필요하다. 두번째로 스마트 컨트랙트 및 블록체인 구현 시 있을 수 있는 보안 위협에 대한 연구와 이에 대응하는 통제에 대한 연구가 필요하다. 마지막으로 시스템 구현 시, 시스템 안전성 검토와 실제적 도입 방안을 연구하여, 위 분야의 연구에 대한 실용화를 추진하여야 한다.

[참고문헌]

[1] Yuanyu Zhang, Shoji Kasahara, Yulong Shen, Xiaohong Jiang and Jianxiong Wan, "Smart Contract-Based Access Control for the Internet of Things", arXiv, February, 2018.

[2] Guy Zyskind, Oz Nathan, Alex 'Sandy' Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data", Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015, July, 2015.

[3] Ricardo Neisse, Gary Steri and Igor Nai-Fovino, "A Blockchain-based Approach for Data Accountability and Provenance Tracking", arXiv, June, 2017.

[4] 개인정보 보호법 제2조(정의) 제3호(개인정보)

[5] 개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한) 제2호 (수탁자)

[6] Heung Youl Youm, Mee Yeon Kim, Keundug Park, "Proposal for a new work item, Security framework for the PII data usage tracking system based on the distributed ledger technology", ITU-T SG17, ITU-T SG17 C276, March, 2018.

[7] Vitalik Buterin, "차세대 스마트 컨트랙트와 탈중앙화된 어플리케이션 플랫폼", Ethereum Korea 2015.03.

[8] ISO TC 307 SG 3, "ISO TC307 SG3 Draft Report v2" 2017.08.17

ECG를 이용한 인증 시스템에 대한 원격 공격 가능성 분석[1)]

이선우* 이동훈*

*고려대학교 정보보호대학원

Analysis of Remote Attack Potential for Authentication Systems using ECG

Sunwoo Lee* Dong-Hoon Lee*

*Graduate School of Information Security, Korea University

요 약

현재 다양한 IoT(Internet of Things) 디바이스들이 등장하고, 서로가 무선 네트워크를 통해 연결되고 있다. 이에 안전한 서비스를 제공하기 위한 인증 시스템은 필수적이며, 그 중 특히 생체 정보를 기반으로 한 인증 시스템이 각광 받고 있다. 그러나 공격자가 인가되지 않은 방법으로 측정한 생체 정보를 이용하여 인증 시스템을 공격할 수 있다는 가능성이 존재한다. 특히 ECG(Electrocardiagram)를 이용한 인증 시스템의 경우, 사용자의 몸에 물리적으로 접촉하여 측정된 정보만이 정당하다는 가정 하에 인증이 이루어지고 있다. 그러나 ECG는 의료적인 목적으로 원격 측정 방법이 연구 및 개발되어왔으므로, ECG 기반 인증 시스템은 원격으로 측정한 정보를 이용한 공격에 취약할 가능성이 높다. 따라서 본 논문에서는 ECG 기반 인증 시스템에 대한 원격 공격 가능성을 분석한다.

I. 서론

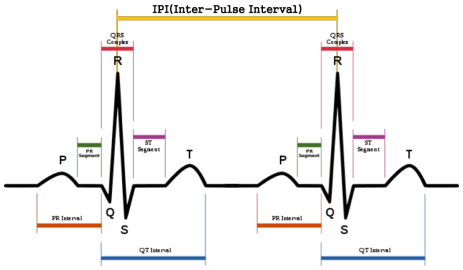
다수의 IoT(Internet of Things) 디바이스들이 등장함에 따라, 다양한 서비스를 제공하기 위해 이들은 무선 네트워크를 통해 연결되고 있다. 이에 인증 시스템은 안전한 서비스를 제공하기 위해 필수적이며, 최근 생체 정보를 이용한 인증 시스템이 각광받고 있다.

생체 정보는 랜덤하며 사람마다 고유하므로 인증 시스템에 이용될 수 있다. 또한 생체정보는 인증이 필요할 때마다 측정이 가능하므로, 인증을 위한 추가적인 정보가 필요 없다는 장점이 있다. 이러한 장점 때문에 실제 많은 곳에서 생체 정보를 기반으로 한 인증시스템이 상용되고 있다[1]. 그러나 인증 시스템의 내부 프로토콜을 해킹하는 것이 아닌, 생체 정보를 인가되지 않은 방법으로 측정함으로써 인증 시스템을 악의적으로 통과할 수 있다. 예를 들어 걸음걸이를 이용한 사용자 인증 시스템의 경우, 공격자가 사용자의 걸음걸이를 따라하여 생성한 걸음걸이 신호를 이용하여 인증 시스템을 악의적으로 우회할 수 있다[2]. 또한 최근 사용자의 걸음걸이를 촬영한 영상으로부터 걸음걸이 신호를 추출할 수 있다는 연구도 발표되었다[3]. 이렇게 생체 정보를 원격으로 측정하는 경우 사용자에 아무런 영향을 끼치지 않으므로 더욱더 위험성이 크다. 특히 생체 정보 중 하나인 ECG(Electrocardiagram)를 이용한 인증 시스템의 경우, 의료적인 목적으로 많은 원격 측정 방법이 연구 및 개발되었으므로[4-7], 원격 공격에 취약할 가능성이 높다. 따라서 본 논문에서는 ECG를 이용한 인증 시스템에 대한 원격 공격 가능성을 분석하고 관련 연구에 대해 살펴본다. 본 연구 결과는 추후 ECG 기반 인증 시스템의 안전성을 향상시키기 위한 기반 연구로 활용될 것으로 기대된다.

1) 이 논문은 삼성전자의 지원을 받아 수행된 연구임

II. 배경지식

ECG(Electrocardiogram)는 심 장의 전기적 활동으로 인해 발생하는 신호로, [그림 1]과 같이 PQRST로 구분된다. 특히 [그림 1]의 R점과 R점 사이의 시간 간격을 IPI(Inter-Pulse Interval)라고 하며, 이는 심 장 박 동수를 뜻 한다. [그림 2]는 ECG 기반 기기 및 사용자 인증 시스템에 대한 개요를 나타낸다.



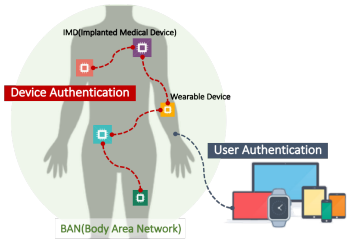
[그림 1] ECG 파형

2.1 기기 인증

IPI는 같 은 시간 및 같 은 사람을 기준으로 측정하면 동일하나같 은 사람일 경우라도 매 시간마다 측정한 IPI는 값 이 다르다. 따라서 이러한 랜덤성으로 인해, IPI는 기기 인증을 위한 값으로 사용될 수 있다 [8]. [그림 2] 같 이 사용자의 몸에 부착된 여러 기기들이 인증을 하고자하면, 동시에 사용자의 IPI를 측정하게 된다. 이때 IPI값은 같 은 시간, 같은 사용자를 기반으로 측정되었으며 모두 동일하며, 이를 통해 기기 인증이 이루어지게 된다.

2.2 사용자 인증

ECG의 파형 은 사람마다 다르다. 즉, ECG의 P, Q, R, S, T점의 시간 간 격 및 높이는 사람마다 유일한 특성을 가지고 있다. 따라서 ECG는 사용자 인증 시스템에 사용될 수 있으며, 실제 이를 상용화한 제품으로 Nymi band가 있다 [9]. 기기가 센 서를 통해 사용자의 ECG를 측정하면, 기기 내 저 장된 ECG의 파형과 이를 비교함으로써 사용자 인증이 이루어진다.



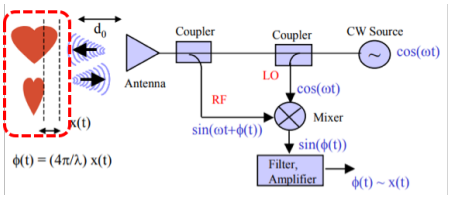
[그림 2] ECG를 이용한 인증 시스템 개요

III. 원격 측정 방법

2절에서 서술한 기기 및 사용자 인증 시스템은 모두 직 접적으로 사용자의 몸에 접촉하여 측정한 생체 정보만이 정당하다는 가정 하에 이루어지고 있다. 그러나 IPI의 경우, 의료적인 목적 및 편리성을 위해 원격으로 측정하는 방법이 연구 및 개발되어왔으며, 이는 기기 인증 시스템에 대한 공격이 가능하다는 것을 의미한다.

Doppler Radar

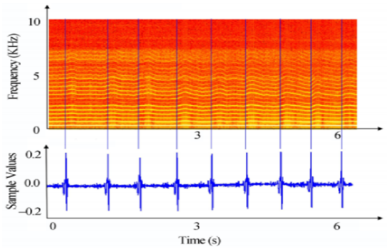
[4]는 [그림 3]과 같 이 사람의 심 장 박동으로 인한 가슴 부위의 위치 변화 를 레 이더를 통해 탐지함으로써 IPI를 측정하는 방법을 제시하였다.



[그림 3] 레이더를 이용한 IPI 측정 방법 [4]

Person's Voice

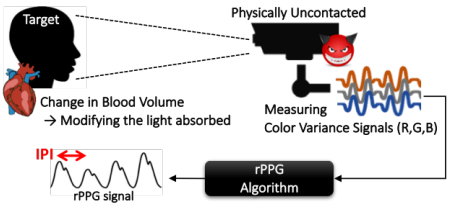
[5]는 사람의 목소리를 통해 IPI를 측정하는 방법을 제시하였다. 본 방법은 [그림 4]과 같이 사람이 모 음을 발음할 때심 장 박 동으로 인하여 목소리의 주파 수가 증가하는 것을 이용하였다.



[그림 4] 사람의 목소리 주파수 변화를 통한 IPI 측정 방법 [5]

rPPG(remote photo-plethysmography)

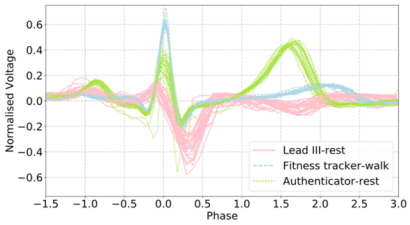
사람의 피부색 은 심 장 박 동으로 인한 혈관의 부피 변화로 주 기적으로 변한다 . PPG(photo-plethysmography)는 이러한 피부색 변화 를 통해 IPI를 측정하는 방법으로, 광학 센 서를 접촉하여 측정하는 방법(cPPG; contact PPG) [6]과, 접촉하지 않고 측정하는 방법(rPPG; remote PPG) [7]의 두 가지 종류 가 있다. rPPG는 [그림 5]과 같 이 카메 라를 통해 촬영한 영상으로부터 사람의 피부 색 변화 신호를 추출함으로써 IPI를 측정할 수 있다.



[그림 5] 카메라를 이용한 IPI 측정 방법 (rPPG)

3.1 ECG 예측 방법

IPI를 원격에서 측정할 수 있음에 반해, ECG를 원격으로 측정하는 방법에 대해선 현재 연구된 바가 없다. 그러나, 특정 기기의 ECG 기반 사용자 인증 시스템을 다양한 환 경 하에서 측정한 여러 사람들의 ECG를 통해 공격할 수 있다는 연구가 발표되었다 [10]. [그림 6]과 같이 ECG의 파형 은 사용자의 상태(휴식, 걷기뛰기) 또는 측정기기에 따라 조금씩 다르기 때문에, 공격 대상의 ECG를 얻 었다고 하더라도 이것을 바로 이용하여 공격 대상의 인증시스템을 통과할 수 없다. 따라서 해당 논문은 다양한 환 경 하에서 측정된 여러 ECG 의 맵핑함수를 정의하여, 이를 통해 ECG기반 사용자 인증시스템을 공격할 수 있다는 것을 보여주었다. 그러나 이러한 연구 또한 공격 대상에 물리적으로 접촉함으로써 측정된 ECG를 얻 는다는 가정 하에 이루어지고 있다.



[그림 6] 다양한 환 경 하에서 측정된 ECG 의 차이 [10]

IV. 공격 가능성 분석

3절과 같 이 공격자는 사용자와 물리적으로 접촉하지 않고도 IPI를 측정할 수 있다. 따라서 공격자는 기기 인증 시스템을 통과하여 공격할 수 있다. 예를 들어, 공격자는 공격 대상의 신체 내부에 이식된 IMD(Implanted Medical Device) ([그림 2])에 악의적인 메 시지를 전송함으로써 공격 대상의 생명을 위협할 수 있다.

PPG와 ECG는 모두 사용자의 심 장 박동으로 인해 발생한 전기적 신호를 측정한 것이다. 따라서 이들 신호는 유기적으로 관계가 있다. 실제로 PPG 파형의 모 양을 토대로 환 자의 심 장 이상을 판단할 수 있다 [11]. 따라서 현재 ECG 자체를 원격으로 측정할 수 있는 방법은 현재 연구된 바가 없지만, 영상 신호로부터 추출한 PPG 신호로부터 ECG 의 특징 점들을 추출가능할 것이며, 이를 이용해 원격으로 ECG 기반 사용자 인증 시스템을 통과할 수 있을 것이다.

V. 결론

본 논문에서는 ECG 기반 기기 및 사용자 인증시스템에 대한 원격 공격 가능성을 분석하였

다. 공격자는 생체 정보를 원격으로 측정하는 경우 사용자에 아무런 영향을 끼치지 않고 생체 정보를 원격으로 측정할 수 있다. 이렇게 측정한 생체 정보를 이용하여 인증 시스템을 공격할 경우, 기기 간의 통신을 도청하거나 사용자의 프라이버시를 침 해할 수 있다심 지어 IMD의 경우, 공격자는 사용자의 목숨까지 위협할 수 있다. 따라서 원격 공격의 가능성을 분석하는 것은 필요하며, 추후 ECG 기반 인증 시스템의 안전성을 향상시키기 위한 기반 연구로 활용될 것으로 기대된다.

[참고문헌]

[1] https://www.nist.gov/speech-testimony/current-and-future-applications-biometric-technologies [accessed 22 May 2018]

[2] Kumar, Rajesh, Vir V. Phoha, and Anshumali Jain. "Treadmill attack on gait-based authentication systems." Biometrics Theory, Applications and Systems (BTAS), 2015 IEEE 7th International Conference on. IEEE, 2015.

[3] 이두형, 최원석, and 이동훈. "걸음걸이 비디오를 활용한 웨어러블 기기 사용자 걸음걸이 가속도 신호 추정." 정보보호학회논문지 27.6 (2017): 1405-1417.

[4] O. Boric-Lubecke, V. M. Lubecke, I. Mostafanezhad, B.-K. Park, W. Massagram, B. Jokanovic, "Doppler radar architectures and signal processing for heart rate extraction", Mikrotalasna Revija, vol. 15, no. 2, pp. 12-17, 2009.

[5] A. Mesleh, D. Skopin, S. Baglikov, A. Quteishat, " Heart rate extraction from vowel speech signals", J. Comput. Sci. Technol., vol. 27, no. 6, pp. 1243-1251, 2012.

[6] Shelley, Kirk H. " Photoplethysmography: beyond the calculation of arterial oxygen saturation and heart rate." Anesthesia &Analgesia 105.6 (2007): S31-S36.

[7] G. de Haan, V. Jeanne, " Robust pulse rate from chrominance-based rPPG", IEEE Trans. Biomed. Eng., vol. 60, no. 10, pp. 2878-2886, Oct. 2013.

[8] Choi, Wonsuk, et al." Less Communication: Energy-Efficient Key Exchange for Securing Implantable Medical Devices." Security and Communication Networks 2018 (2018).

[9] https://nymi.com [accessed 22 May 2018]

[10] Lovisotto, Giulio. "When your fitness tracker betrays you: quantifying the predictability of biometric features across contexts." (2018).

[11] Murthy, V. S., et al. "Analysis of photoplethysmographic signals of cardiovascular patients." Engineering in Medicine and Biology Society, 2001. Proceedings of the 23rd Annual International Conference of the IEEE. Vol. 3. IEEE, 2001.

C++의 동적 디스패치에 적용된 제어 흐름 무결성 검증기법 분석*

장혜린*, 박문찬*, 진홍주*, 이동훈*
*고려대학교 정보보호학과

Analysis of Control Flow Integrity Technique Applied to Dynamic Dispatch of C++*

Hye Rean Jang*, Moon Chan Park*, Hong Joo Jin*, Dong Hoon Lee*
*Graduate School of information security, Korea University.

요 약

C++은 메모리나 타입에 대한 안전성을 보장하지 않기 때문에, 공격자는 이를 이용해 객체의 가상함수 테이블이나 가상함수 포인터를 조작함으로써 프로그램의 제어 흐름을 탈취할 수 있다. 가상함수 테이블이나 가상함수 포인터가 웹 브라우저 또는 C++ 프로그램에 대한 주요 공격 수단으로 이용되면서, 동적 디스패치를 보호하는 방법에 관한 연구가 활발히 이루어지고 있다. 본 논문에서는 제어 흐름 무결성 기법을 통해 동적 디스패치를 보호하는 방법에 대하여 분석한다. 제어 흐름 무결성 기법은 동적 디스패치 과정에서 유효한 함수 집합 또는 단일 함수를 미리 지정함으로써 유효하지 않은 함수의 실행을 막는다. 따라서 이러한 제어 흐름 무결성 기법을 어떤 방식으로 동적 디스패치 보호에 적용했는지 분석하고, 각 기술의 한계점에 대하여 비교한다.

I. 서론

오늘날 C++은 웹 브라우저, 임베디드 시스템 통신 및 금융 어플리케이션 등 많은 프로그램 개발에 사용된다. 이처럼 C++이 많이 사용되는 이유는 프로그래머들에게 코드 작성에 대한 자유와 유연성을 주기 때문이다. C++은 메모리를 자체적으로 관리하는 다른 객체 지향 언어들과는 달리 메모리 관리에 대한 권한을 프로그래머에게 위임한다. 따라서 C++은 프로그래머에게 효율적인 코드 작성과 메모리에 대한 명확하고 정교한 제어를 제공한다.

그러나 이러한 이점으로 인해 공격자에게도 좋은 공격대상이 된다. C++은 내장된 데이터에 대한 접근 또는 덮어쓰기 보호 기능을 제공하지 않으며, 버퍼의 경계를 자동으로 검사하지 않는다. 따라서 메모리에 관련된 다양한 공격의 대상이 되고, 이러한 공격은 제어 흐름에 대한 공격으로 이어져 프로그램에 심각한 영향을 끼친다.

객체 지향 언어인 C++에서 동적 디스패치는 핵심적인 부분으로 가상함수 테이블과 가상함수 포인터로 구현된다. 최근 메모리상의 취약점을 이용한 공격은 대부분 가상함수 테이블과 가상함수 포인터를 대상으로 이루어지기 때문에 동적 디스패치를 보호하는 연구가 활발히 이루어지고 있다[2][3][4][6][7][8]. 본 논문에서는 동적 디스패치에 적용된 제어 흐름 무결성 기법(Control Flow Integrity, CFI)[1]에 대해 분석하여, 각각의 한계점을 기술하고자 한다.

II. 배경 지식

2.1. 제어 흐름 무결성 검증기법

CFI 의 목표는 프로그램의 제어 흐름의 이동을 제한하여 프로그램이 올바르게 실행되도록

* 이 성과는 2018년도 과학기술정보통신부의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2017R1A2B3009643).

하는 것이다[1]. CFI는 크게 두 단계로 이루어진다. 첫 번째 단계는 분석 단계로 올바른 제어 흐름 이동의 기준을 정하기 위하여 정적분석을 통해 제어 흐름 그래프(Control Flow Graph, CFG)를 생성한다. 두 번째 단계는 검증 단계로 프로그램 실행 중에 제어 흐름의 변화가 제어 흐름 그래프와 일치하는지 검사하는 단계이다.

공격자들의 주 공격대상은 간접호출문이며, C++에서는 특히 가상함수에 대한 공격이 가장 많이 발생한다[5]. 따라서 가상함수에 대해 완벽한 방어가 보장된다면, 프로그램에 대한 공격은 더 어려워진다[2].

2.2. 동적 디스패치

C++의 동적 디스패치는 상속 관계에 있는 객체에서 함수를 호출하였을 때, 어떤 클래스의 함수를 부를지 선택하는 프로세스이다. 동적 디스패치는 가상함수 테이블을 이용해 구현된다. 가상함수 테이블은 해당 클래스에서 호출할 수 있는 가상함수들의 주소가 저장된 테이블로 컴파일 타임에 읽기 전용 공간에 생성된다[2]. 객체는 생성자에 의하여 객체의 타입에 맞는 가상함수 테이블 포인터를 할당받음으로써 가상함수 테이블과 연결된다. 객체를 통해 함수가

```
# include <iostream>

class A
{
...
public:
        virtual void Func1() { ...; }
        virtual void Func2() { ...; }

};

class B: public A
{
...
public:
        virtual void Func1() { ...; }
};

int main(void)
{
        A * aaa = new A();
        B * bbb = new B();
}
```

Fig. 1. 다형성을 나타내는 C++ 코드

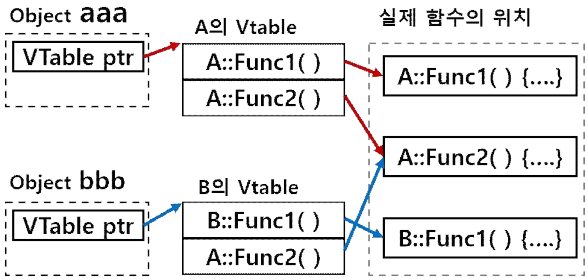


Fig. 2. 동적 디스패치 과정

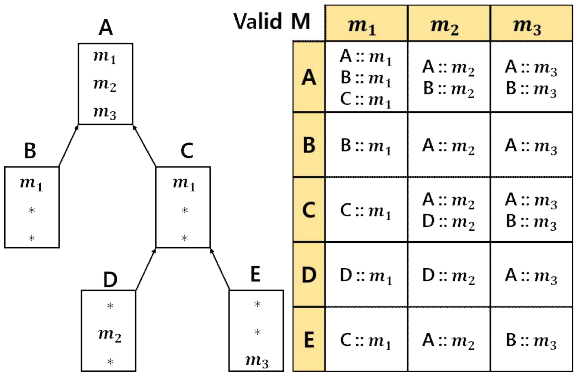
실행되었을 때 객체에 연결된 테이블을 통해 유효한 함수를 실행시킬 수 있다.

Fig. 1.은 상속 관계를 나타내는 C++ 코드이다. 이 코드상에는 상속 관계에 있는 두 개의 클래스가 존재하며, Fig. 2.와 같은 구조로 메모리가 구성된다. 예로 들면, 객체 aaa는 생성될 때 클래스 A의 가상함수 테이블 포인터(VTable ptr)를 할당받는다. 객체 aaa를 통해 함수가 호출되었을 때에는 aaa의 가상함수 테이블 포인터를 통해 A 클래스의 가상함수 테이블을 참조하여 호출된 함수의 주소를 가져와 해당 주소에 있는 함수를 실행시킨다.

이와 같은 과정을 통해 동적 디스패치가 진행되며, 객체는 자신의 타입에 따라 가상함수 포인터를 할당받기 때문에, 객체의 타입에 대한 무결성을 보장하기 위해서는 가상함수 포인터에 대한 무결성을 보장해야 한다.

2.3. 가상함수 테이블 하이제킹 공격

가상함수 테이블 하이제킹(hijacking)은 공격자가 가상함수 포인터를 수정하거나 새로운 가상함수 테이블을 만들어 악의적인 가상함수를 실행시키는 공격이다. 가상함수 테이블 하이제킹 공격의 대표적인 예로는 use-after-free 취약점을 이용한 공격이 있다. 공격자는 먼저 할당이 해제된 객체를 참조하고 있는 허상 포인터(dangling pointer)를 찾고, 다른 공간에 위조된 가상함수 테이블은 만든다. 다음으로 허상 포인터가 참조하는 공간에 위조된 가상함수 테이블을 참조하는 포인터를 저장한다. 마지막으로 이 허상 포인터를 통해 가상함수가 실행되면 공격자는 위조된 가상함수 테이블을 통해 프로그램에 대한 제어권을 획득하게 된다.



Valid M	m_1	m_2	m_3
A	A::m_1 B::m_1 C::m_1	A::m_2 B::m_2	A::m_3 B::m_3
B	B::m_1	A::m_2	A::m_3
C	C::m_1	A::m_2 D::m_2	A::m_3 B::m_3
D	D::m_1	D::m_2	A::m_3
E	C::m_1	A::m_2	B::m_3

Fig. 3. 상속 관계에 따른 유효한 호출 테이블

이 외에도 버퍼 또는 힙 오버플로우, Type Confusion 취약점을 이용한 가상함수 테이블 하이제킹 공격이 가능하다[9][10][11].

III. C++의 동적 디스패치에 적용된 제어 흐름 무결성 검증기법에 관한 연구

3.1. Safe Dispatch

Safe Dispatch[2]는 C++의 동적 디스패치에 대해 처음으로 제시된 보호 기법으로 구현 과정은 다음과 같다.

1) 정적으로 상속 관계를 분석하여 유효한 호출 테이블을 작성한다.
2) 이전 과정에서 생성된 테이블을 기반으로 검사 코드를 삽입한다.

첫 번째 단계에서 생성하는 유효한 호출 테이블은 객체의 클래스 단위로 구분된다. 즉 한 객체에서 가상함수를 호출했을 때 해당 클래스의 가상함수이거나, 하위 클래스에 있는 함수이면 그 호출은 유효한 호출로 판단한다.

Fig. 3.는 간단한 상속 관계를 통해 만든 유효한 호출 테이블의 예이다. Fig. 3.에서 클래스 B와 C는 A를 상속받고 클래스 D와 E는 C를 상속받는다. 각 노드는 각 클래스의 함수 정보를 나타낸다. 자식 클래스에서 *는 부모 클래스의 함수를 그대로 상속받았음을 의미하며 m_i은 부모 클래스의 함수를 재정의한 것을 나타낸다. 즉, B는 A를 상속받아 m_1을 재정의했고, m_2와 m_3은 재정의 없이 그대로 상속받았음을 의미한다. 만약 A 클래스의 함수 포인터를 통해 m_2 함수를 호출한 경우 유효한 함수는 A

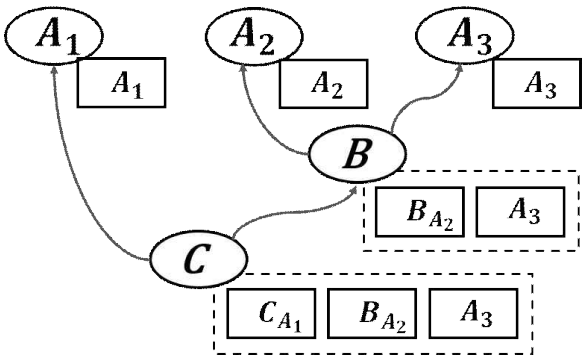


Fig. 4. 클래스 상속 관계의 예

클래스를 상속받은 모든 클래스의 가상함수 테이블에 속한 m_2가 된다. 따라서 호출 가능한 함수는 A의 m_2와 D의 m_2가 된다. (이때 B, C, E에 있는 m_2는 재정의하지 않았으므로 A의 m_2와 같다) C에서 m_2를 호출한 경우에는 C에 속한 A의 m_2와 하위 클래스인 D의 m_2가 유효한 호출로 정의된다. 이렇게 정의된 테이블을 기반으로 검사 코드를 삽입하여 함수 호출마다 제어 흐름의 무결성을 검증한다.

Safe Dispatch는 객체의 타입을 기반으로 한 분석이다. 따라서 가상함수 테이블 하이제킹 공격의 경우, 공격에 사용되는 위조된 함수는 상속 관계 분석 테이블에 속하지 않기 때문에 공격을 탐지하고 막을 수 있다.

3.2. Shrink Wrap

Shrink Wrap[3]은 Safe dispatch와 같이 각 호출 사이트에서 유효한 가상함수들의 집합을 만들어 검증하는 과정으로 이루어진다. Fig. 4.은 간단한 상속 관계의 예를 보여준다. 클래스 B는 A_2와 A_3를 상속받는데, A_2에서 상속받은 함수를 재정의한다. 따라서 B의 가상함수 테이블은 A_2에서 상속받아 재정의한 B_{A_2}와 A_3로 이루어져 있다. Fig. 4.과 같이 한 클래스가 다중상속 받게 되면, 해당 클래스는 상속받은 클래스에 대한 가상함수 테이블을 갖게 된다. 이에 Safe dispatch의 규칙을 적용한다면, Fig. 5.와 같이 호출 위치에서 유효한 함수들의 집합이 커지기 때문에 검증이 불분명해진다. 유효한 함수들의 집합이 커지게 되면 공격자가 공격할 수 있는 범위 또한 넓어지기 때문에 유효한 함수들

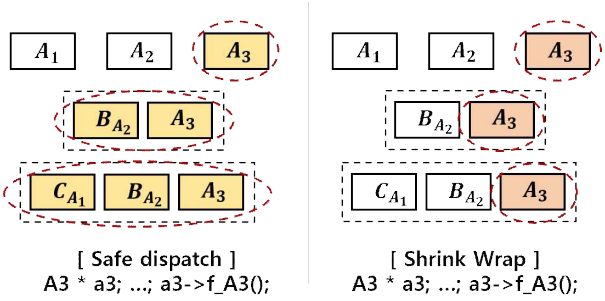


Fig. 4. Safe dispatch와 ShrinkWrap의 예

의 집합을 최대한 작게 만들어야 한다. 따라서 Shrink Wrap에서는 두 클래스에서 상속받은 가상함수 테이블을 분리하여 집합을 생성한다. Fig. 5.를 보면 Shrink Wrap을 적용했을 때 유효한 가상함수 테이블에 대한 집합의 크기가 작아진 것을 확인할 수 있다.

Shrink Wrap은 위와 같은 방법을 통하여 각 호출 사이트에서 유효한 가상함수들의 집합을 생성해 제어 흐름에 대한 무결성을 검증한다.

3.3. CFIXX : Object Type Integrity

CFIXX는 동적 분석을 통해 객체 타입의 무결성(Object Type Integrity, OTI)을 보장함으로써 동적 디스패치를 보호한다[4]. C++에서 상속 관계에 있는 객체가 생성될 때, 객체의 타입에 맞는 가상함수 포인터가 할당된다. 따라서 OTI을 보장한다는 것은 객체의 가상함수 포인터에 대한 무결성을 보장한다는 의미가 된다.

따라서 CFIXX는 객체의 가상함수 포인터에 대한 무결성을 보장하기 위해 생성자에 의해 할당되는 가상함수 포인터를 메타 데이터 테이블에 기록하고, 가상함수가 호출되었을 때는 객체의 가상함수 포인터가 아닌 메타 데이터 테이블에 저장된 가상함수 포인터를 참조할 수 있도록 하는 것을 기본 메커니즘으로 한다. CFIXX는 이전 기법들처럼 유효한 집합을 만들어 검증하는 것과 달리, 동적 분석을 통해 저장된 유효한 포인터를 통해 가상함수가 실행되도록 하는 기법이다.

이 기법에서 고려해야 할 사항은 메타 데이터 테이블의 무결성이다. 메타 데이터 테이블은 실행 시간 중에 생성되기 때문에 읽기 전용 공간에 할당할 수 없다. 따라서 공격자가 메타 데이터 테이블 영역에 있는 데이터를 조작하기 위한 접근이 있을 때 이를 막을 수 없다. CFIXX 기법은 이 문제를 MPX(Memory Protection Extensions)라는 하드웨어를 사용하여 해결하였다. MPX는 입력이 가능한 메모리 영역의 범위를 지정해 메모리에 데이터를 입력할 때마다 접근한 영역이 정해진 범위 내에 있는지 검사하여 메모리를 보호한다. 따라서 이 기법에서는 MPX를 이용하여 메타 데이터에 대한 검증되지 않은 입력을 막아 공격자의 악의적인 수정을 보호할 수 있다.

IV. 분석

앞서 소개한 연구들은 가상함수 포인터를 조작해 기존의 가상 테이블과 관련이 없는 조작된 가상함수 테이블을 참조하여 악의적인 함수를 호출하는 공격에 대하여 효과적으로 방어할 수 있다. 조작된 가상함수 테이블은 객체의 타입과 무관하므로 이 테이블에 속한 함수의 호출은 각 연구에서 제시한 규정과 어긋나기 때문이다[2][3][4].

그러나 가상함수 포인터를 조작해 하위 클래스의 가상함수 테이블을 참조하도록 하는 공격의 경우는 앞의 결과와 다르다. CFIXX는 객체의 검증된 가상함수 포인터를 메타 데이터 공간에 저장하여 보호한다. 따라서 가상함수 포인터를 조작하는 것 자체가 불가능하므로 이 공격을 방어할 수 있다. Safe dispatch는 하위 클래스에 속한 함수를 모두 유효한 호출로 판단하기 때문에 이 공격을 막을 수 없다. ShrinkWrap은 이와 같은 유형의 공격 대부분을 방어한다. 하지만 해당 포인터의 타입과 같은 타입의 클래스에 속한 함수를 호출하거나, 이 함수를 상속받아 재정의한 함수를 호출하는 경우에는 이 기법의 규정상 유효한 함수로 판단하기 때문에 이 공격을 막을 수 없다.

이와 같은 결과는 정적분석을 통해 획득한 정보만을 이용한 CFI의 한계이다. 프로그램이 실행되어 가상함수를 호출했을 때 실제로 유효한 목적지는 단 한 곳뿐이다. 하지만 정적분석을 통한 정보만으로는 이를 정확히 판단할 수 없으므로 유효하다고 판단되는 집합을 생성한

다. 이로 인해 실제로는 유효하지 않지만 유효하다고 판단하는 긍정오류(False positive)가 발생하게 된다. 이 공격을 통해서 CFIXX는 가장 강력한 보호 기법으로 보일 수 있다. 하지만, CFIXX를 구현하기 위해서는 별도의 하드웨어를 사용해야 하는 점을 고려해야 한다.

V.결론

본 논문에서는 C++의 동적 디스패치에 적용된 CFI 연구를 비교 분석하였다. 제안된 기법들은 객체의 타입에 기반 된 분석을 통해 유효한 집합을 구하거나, 검증된 초기 포인터를 보호되는 공간에 저장해 무결성을 보장한다.

본 논문에서 다룬 연구 중 CFIXX는 가장 fine grained 기법이다. 하지만 다른 두 기법 비교하였을 때 하드웨어를 사용해 구현해야 하는 추가적인 비용이 발생한다. 따라서 각 기법은 비용과 보안 성능 간의 트레이드 오프(trade off)가 있다.

추후 연구에서는 본 논문에서 소개한 기법들의 한계를 보완하는 정적분석에 기반을 둔 제어흐름 무결성 검증기법에 관해 연구할 예정이다.

[참고문헌]

[1] M. Abadi, M. Budiu, U. Erlingsson, and J. Ligatti, “Control-Flow Integrity,” In Proc. of ACM CCS, pp 340-353, 2005.

[2] D. Jang, Z. Tatlock, and S. Lerner, “SAFEDISPATCH: Securing C++ virtual calls from memory corruption attacks,” In Symposium on Network and Distributed System Security(NDSS), 2014.

[3] I. Haller, E. Gkta, E. Athanasopoulos, G. Portokalidis, and H. Bos, “ShrinkWrap: VTable Protection without Loose Ends.” In Annual Computer Security Applications Conference, 2015.

[4] N. Burow, D. McKee, S. Carr, and M. Payer, “CFIXX: Object Type Integrity for C++ Virtual Dispatch, “ In Symposium on Network and Distributed System Security (NDSS), 2018.

[5] C. Tice, T. Roeder, P. Collingbourne, S. Checkoway, U. Erlingsson, L. Lozano, and G. Pike, “Enforcing Forward-edge Control-flow Integrity in GCC and LLVM,” In Proc. of Usenix Security 2014.

[6] C. Zhang, C. song, K.Z. Chen, Z. Chen, D. Song, “VTint:Protecting Virtual Function Tables’ Integrity,” In Symposium on Network and Distributed System Security, 2015.

[7] C. Tice, T. Roeder, P. Collingbourne, S. Checkoway, “Enforcing Forward-Edge Control-Flow Integrity in GCC&LLVM,” n Proc. of Usenix Security, 2014.

[8] A. Prakash, X. Hu, H. Yin, “vfGuard: Strict Protection for Virtual Funtion Call in COTS C++ Binaries,” In Symposium on Network and Distributed System Security (NDSS), 2015.

[9] D. Bounov, R.G. Kıcı, S. Lerner, “Protecting C++ Dynamic Dispatch Through VTable Interleaving,” In Symposium on Network and Distributed System Security (NDSS), 2016.

[10] Advanced Exploitation of Mozilla Firefox Use-After-Free Vulnerability, “http://www.vupen.com/blog/20140520.Advanced_ Exploitation_Firefox_UaF_Pwn2Own_2014.php” Pwn2Own, 2014.

[11] Adobe Flash Player AS3 Convolution Filter Use-After-Free Remote Code Execution Vulnerability, “http://www.zerodayinitiative.com/advisories/ZDI-15-134/” ,Pwn2Own, 2015.

2018 한국정보보호학회 하계학술대회

C7 기 타

이 옥 연 (국민대학교)

- **열차 무인운전시스템 랜섬웨어 공격 파급효과 분석 및 대응방안 제시**
  이영비, 이동주, 윤우석, 서정택
- **사이버 위협 시나리오 분석 및 예측의 자동화 방법**
  조성영, 정현숙, 신영섭, 이동재, 임창완, 오행록
- **이동 경로 정보를 활용한 주소 인증**
  박호성, 남승수, 최대선
- **부인방지 기능을 제공하는 이동형 전기자동차 충전기용 보안 에이전트 설계**
  장찬국, 이재훈, 이옥연

열차 무인운전시스템 랜섬웨어 공격 파급효과 분석 및 대응방안 제시

이영비, 이동주, 윤우석, 서정택

순천향대학교 정보보호학과

Analysis of a Ripple Effect of Ransomware on Automated Driving Metro And Countermeasure Suggestion

Young Bi Lee, Dong Ju Lee, Woo Seok Yun, Jung Taek Seo

Department of Information Security Engineering, Soonchunhyang University.

요 약

최근 부산도시철도 4호선, 신분당선, 대구도시철도 3호선 등 국내에서 열차 무인운전시스템을 도입하는 추세이다. 열차 무인운전시스템을 도입하면 비용 절감, 수익 증대, 정시운행성이 높아짐에 따라 열차 운행의 효율성을 높일 수 있다. 그러나 열차 무인운전시스템의 경우 열차와 관제실 간에 실시간으로 위치정보를 주고받으며 안전거리를 자체적으로 계산하는 등 실시간으로 중요한 정보를 주고받는 환경이다. 열차 무인운전시스템에서는 최신 통신 및 컴퓨팅 기술 등이 사용되고 있으며, 이들 시스템 및 통신 환경은 다양한 보안위협으로 인하여 해킹 공격이 발생 가능하다. 이에 본 논문에서는 최근 무차별적으로 발생하고 있는 랜섬웨어 공격이 열차 무인운전시스템을 대상으로 발생하였을 때 어떤 영향을 미칠 수 있으며, 그로인한 파급효과를 분석하여 제시한다.

I. 서론

최근 전 세계적으로 열차 무인운전시스템이 도입되고 있는 추세이다. 표 1과 같이 국내·외 노선들이 열차 무인운전시스템을 적용하여 운영하고 있다.

국가	도시	노선
대한민국	서울·경기	신분당선 (DX Line)*
프랑스	파리	Line 1, 14
싱가포르	싱가포르	North-East Line, Circle Line
독일	뉘른베르크	Line U2, U3
UAE	두바이	Metro (Green, Red)
스페인	바르셀로나	L9, L10, L11
중국	홍콩	Diseneyland Resort Line
브라질	상파울로	Line 4(Yellow)

표 1. 국내·외 운행 중인 무인열차

무인운전(Driverless)은 기관사가 없이 열차를 운행할 수 있다는 장점이 있으나, 비상상황이 발생할 시 단순 장애에도 서비스 일부 중단 혹은 열차 운영이 중단될 수 있다. 따라서 열차 상태 모니터링, 열차 제어에 대한 대응방안이 체계적으로 정립되어야 한다[1]. 국내에서 운영하고 있는 신분당선은 CBTC(Communication Based Train Control) 방식의 철도제어시스템을 적용하고 모든 열차가 완전자동 운행시스템에 의해 무인운전으로 운영되고 있다[2]. 또한 TCMS(Train Control Monitoring System) Console을 도입하여 운행상태와 고장정보 표시 및 주요 장치들에 대한 원격제어가 가능하지만 무선 통신을 사용함으로써 해킹의 위협이 존재하여 보안에 취약하다[3]. 2016년 11월 미국 샌프란시스코 도시철도시스템이 '맘바' 랜섬웨어에 감염되어 티켓 발매가 중단된 사건 등이 있었기에 철도제어시스템에서의 사이버 안전성이 문제로 제기되었다. 본 논문에서는 열차 무인운전시스템과 랜섬웨어에 대해 설명하고, 랜섬웨

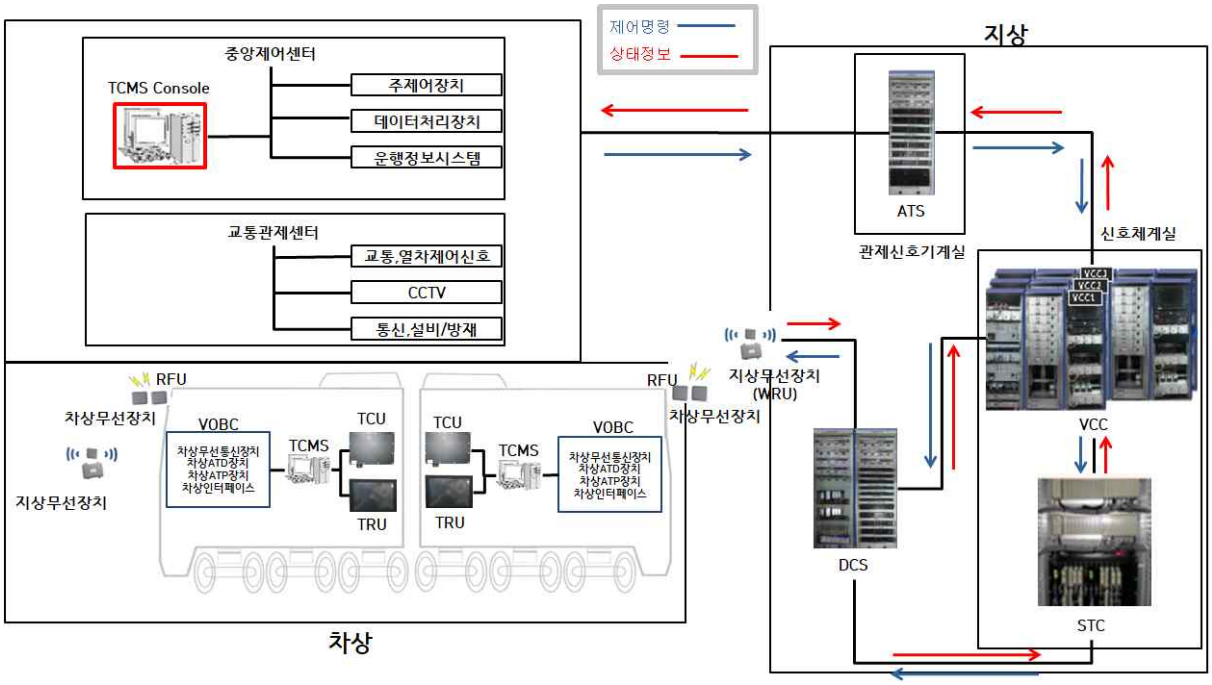


그림 1. 열차 무인운전 CBTC 시스템 구조도

어 공격이 열차 무인운전시스템을 대상으로 발생하였을 때, 그로인한 파급효과를 분석하여 대응방안을 제시한다.

II. 열차 무인운전시스템

현재 운행되는 신분당선에서는 CBTC시스템이 사용하여서 강남~정자 구간까지 정상적으로 운행을 하고 있다. 신분당선은 이동폐색 방식을 사용하고 있으며 기관사가 탑승하지 않고 무인으로 운행되고 있다. 열차 간의 무선 통신을 통해 속도, 운행 위치 등을 원격 제어하고, 열차의 출입문 정보 및 개폐와 속도 가·감속을 제어하는 무인운전 방식을 사용되고 있다. 해당 방식을 사용함으로써 안정성과 정확성을 기존의 유인 방식보다 높일 수 있으며 다른 철도 노선에서도 많은 관심을 보이고 있다[4].

2.1 CBTC 통신기반 열차 제어장치

CBTC는 무인운전시스템에서 핵심적인 장치로서 양방향 무선통신을 이용하여 열차를 제어하는 장치이다. 해당 장치를 이용하여 지상 신호제어 설비가 작동되고 그림 1과 같이 지상의 중앙제어 센터에 설치된 컴퓨터와 통신을 하게 된다[5]. 이때 각 열차의 위치, 속도 등을 연속적으로 확인하여 선행열차 위치와 속도 제한 및 지점까지의 거리를 열차에 무선으로 데이터를 전송하고 각각의 열차가 최적의 속도로 운행 할 수 있도록 하는 제어기능을 수행한다. CBTC 장치 용어는 표 2와 같다.

VCC	Vehicle Control Center. 열차운행 중 지상설비 및 제어구간 내에 있는 운행 중인 모든 열차와 실시간 양방향 통신을 하며 열차 간 최소 안전거리가 지켜지도록 제어한다.
STC	Station Controller. 역에 설치되는 연동장치로 선로 변의 ATP[1]/ATO[2] 기능을 수행하기 위해 VCC와 연계하여 작동한다. STC는 신호기, 선로전환기, 열차출입문 및 승강장 스크린도어를 제어한다.
ATS	Automatic Train Supervision. 실시간 열차위치, 상태 그리고 현장설비 상태를 관제사에게 알린다.

1) ATO : Automatic Train Operation.
2) ATP : Automatic Train Protection.

VOBC	Vehicle On-board Controller. 차상 기동 명령, 열차 진로 설정하고, 차상의 각종 제어 정보를 TCMS에 전송하한 뒤 무선 송수신 장치를 통해 WBC(Waveguide Base Station)와 송·수신한다.

표 2. CBTC 장치 용어

2.2 TCMS Console

TCMS Console은 열차 내부에 있는 TCMS에서 열차 데이터를 무선 통신을 통해 데이터를 교통관제 센터에 전송하고 기관사 대신에 관제사가 열차를 원격으로 조종할 수 있게 해주는 장치이다. 해당 장치를 이용하여 열차의 속도, 제동, 출입문 장치, 냉난방 장치 등 열차가 기동에 필요한 모든 제어기능을 수행 가능하다. 이외에도 고장코드를 수집하여 경영정보시스템(Management Information System)에 전달하고 유지보수 활동에도 도움을 주는 역할을 한다.

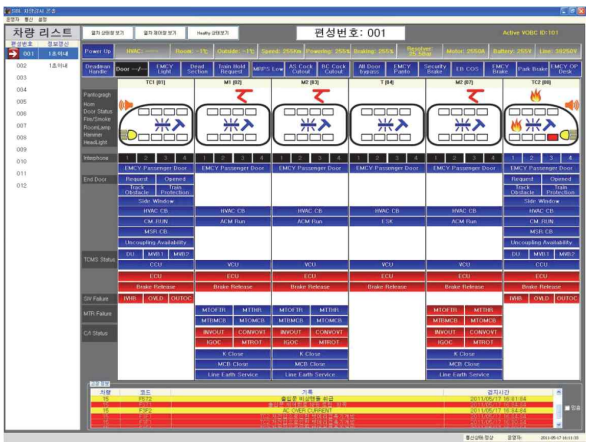


그림 2. TCMS Console

TCMS Console은 위에 그림 2와 같이 구성되어 있으며, 관리자의 편의를 위해 Windows OS 기반의 GUI(Graphical User Interface)로 동작된다.

2.3 지상[3]-차상[4] 서버 간 데이터 흐름

차상 내부의 TCMS는 열차의 운행 정보, 시간 정보, 열차 고장 정보 등을 수집하여 TRU(Train Recording Unit)에게 데이터를 전송한다. 데이터를 받은 TRU는 18GHz 무선 RF(Radio Frequency)를 통해 지상 서버로 전송된다. 차상과 지상이 무선으로 송·수신을 함에 있어 차상과 지상은 표 3와 같이 TCP 프로토콜을 이용하여 통신을 수행한다. 무선 통신 장치를 이용함으로 802.11a 무선 프로토콜 18GHz 대역폭을 사용한다. 무선 송·수신은 TCP 프로토콜을 이용하여 차상에 있는 TRU와 지상서버 간의 논리적 포트 번호인 4960 포트 번호를 이용하여 차량 통합 영상 및 데이터를 전송한다.

항목	설명
TCP 계층 프로토콜	TRU 전송 장치와 지상서버간의 연결
4960 포트	논리적 Well-Known 포트
응용 프로그램 전용 프로토콜	TruSvrPkt 패킷 전용 프로토콜

표 3. 프로토콜 및 포트

전용프로토콜 'TruSvrPkt'은 그림 3과 같이 TCP/IP 통신 패킷을 통해 차량용 통합 영상 및 데이터 전송 장치(TRU)와 지상 서버 간에 통신한다[6].

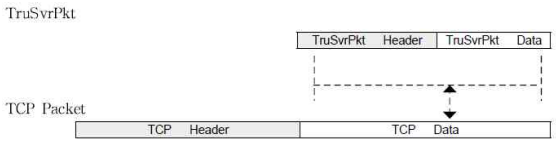


그림 3. 프로토콜 패킷 구조

2.4 지상-차상 서버 간 전송 데이터

열차 무인운전시스템 중에 지상(관제 시스템 서버)와 차상(운행되는 열차)에서 서로 주고받는 데이터는 밑의 표 4와 같다[7].

지상 → 차상 전송 데이터	차상 → 지상 전송 데이터
선행 열차위치정보·제한속도·운전방향·행선지·목표 거리	운전방향·속도 시간·현재위치
열차번호·운전시간·역정차시간·출입문 정보	열차번호·행선지 출입문 정보
경계속도·선로제한 정보	정위치 정차 정보
지정운전모드·이동권한	이동권한
Setup, Key-up, Down 정보	차량고정 정보, 차량상태 정보
출입문 제어 정보	속도 "Zero" 정보
임시 속도제한 정보	편성정보
Reset 정보, 분기기, 연동장치정보	지상제어의 응답

표 4. 열차 무선 통신 간 이동 데이터

3) 지상: 역 내부 데이터통신시스템.

4) 차상: 열차 혹은 차내 데이터통신시스템.

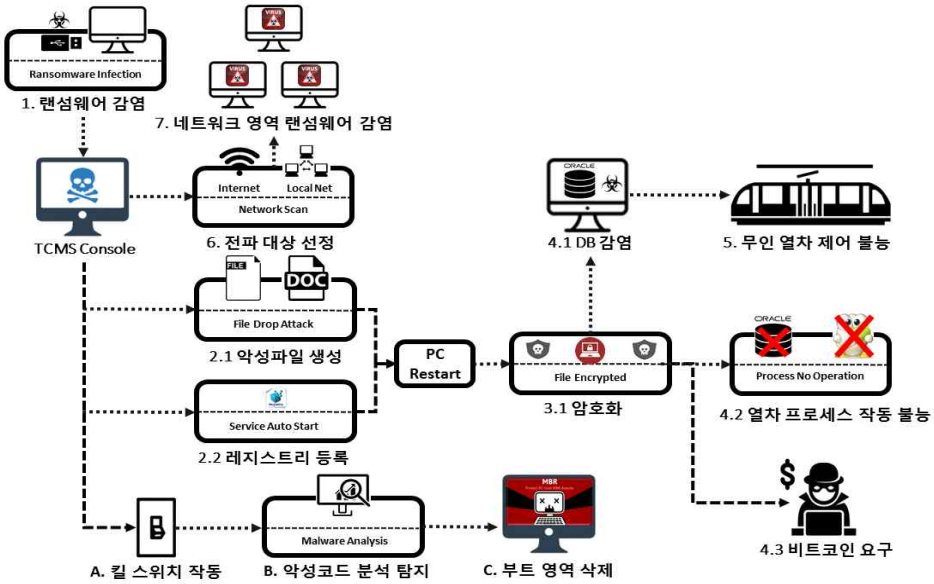


그림 4. 열차 무인운전시스템 랜섬웨어 감염 시나리오 제시

III. 랜섬웨어

랜섬웨어는 멀웨어의 일종으로 인터넷에 연결된 기기에서 의도치 않게 감염된다[8]. 몸값(ransom)과 제품(ware)의 합성어로 컴퓨터에 있는 정보를 암호화하여 사용자에게 돈을 요구한다. 공개된 암호화를 사용하기 때문에 제작이 수월하고 키를 찾기 힘들기 때문에 복원이 어려워서 해커들은 변형되고 정밀화된 랜섬웨어를 제작한다. 이에 랜섬웨어에 의한 피해가 증가하고, 최근 사이버공격 주 대상이 된 제어시스템까지의 영향을 미칠 것이다.

IV. 랜섬웨어 감염 파급효과 분석

4.1 랜섬웨어 감염 시나리오 제시

TCMS Console은 그림 2와 같이 구 버전의 Windows OS를 사용하고 있어 기존에 알려진 다양한 공격 방식의 취약점에 노출되어있다. 본 논문은 제어시스템 내부에서 구 버전의 Windows OS를 서버 관리 PC로 사용하는 것을 타겟으로 시나리오를 제시한다. 해당 시나리오는 여러 방면으로 악성코드가 유입되어, 기존에 알려진 취약점을 이용하여 네트워크 드라이버 및 공유폴더를 통해 네트워크 내의 PC들을 감염시키고 주요 프로세스를 작동 불능 시키며 랜섬웨어로 인해 파일 및 DB(Data Base) 데이터를 암호화 한다. 시나리오에 대한 과정은 그림 4, 표 5와 같다.

Step 1	랜섬웨어 유입
	공격자가 USB(Universal Serial Bus)를 통해서 TCMS Console에 랜섬웨어 악성코드가 유입된다. 악성코드는 네트워크를 스캔하여 연결된 네트워크 상의 PC에 네트워크 드라이버 및 공유폴더 취약점을 이용하여 파일을 전파 및 실행을 유도한다.
Step 2	랜섬웨어 실행
	TCMS Console 관리자는 유입된 랜섬웨어 악성코드를 실행한다.
Step 3	랜섬웨어의 파일 및 프로그램 암호화
	네트워크에 전파된 악성코드는 취약점을 통해 실행되어 랜섬웨어를 통한 파일 암호화 및 주요 프로세스에 대한 접근 및 제어 불가와 DB 파일을 암호화 한다.
Step 4	열차 제어 정보 암호화
	최종적으로 TCMS Console에서 관리하는 주요 열차 제어 정보에 대한 암호화로 열차에 대한 관리가 불가능해진다.

Step 5	주요 프로그램 암호화
	TCMS Console 내 DB 프로그램, Console 프로그램 등 주요 프로그램 암호화로 인해 열차 접근 제어가 불가능해진다.
Step 6	악성코드의 네트워크 정보 습득
	악성코드는 네트워크를 스캔하여 연결된 네트워크상의 PC 정보를 수집한다.
Step 7	네트워크 내 악성코드 유포
	수집된 정보를 통해 악성코드는 네트워크 드라이브 및 공유폴더 취약점을 이용하여 파일을 전파 및 실행을 유도한다.
역공학 시도 시 자가 파괴	
악성코드 및 암호화된 파일을 역공학 기법을 통하여 복구 시도 시 부트 영역을 파괴한다.	

표 5. 랜섬웨어 감염 시나리오

위와 같은 시나리오를 통해 열차 무인운전시스템은 중앙 관제실의 관제사와 데이터 송·수신이 불가능하게 되므로 각종 사고에 노출된다. 표 6은 랜섬웨어 공격에 대한 다양한 감염 방식이다.

Case 1. USB를 통한 내부망 감염
그림 4는 USB를 통해 랜섬웨어가 감염된 것이다. USB 사용 시 사전에 악성코드 검사를 하지 않으면 악성코드 유입 가능성이 존재한다.
Case 2. 외부 네트워크로부터 감염
기본적으로 제어시스템의 경우 외부 네트워크 연결을 차단하는 독립망으로 사용이 되지만 휴대폰 테더링, 외부 네트워크 랜카드 설치 등 편의를 위해 외부 네트워크를 내부 제어시스템에서 사용 시 망혼용 공격을 당할 가능성이 있다.
Case 3. 유지보수 중 개발사로부터의 감염
최근 북한이 제어 시스템을 공격할 때 가장 많이 사용하는 방법이다. 제어시스템의 경우 독립망을 사용하고 보안이 잘되어 있어서 공격이 사실상 불가능하다. 그렇기에 제어시스템에 납품을 하는 개발사 단계에서 장비 또는 프로그램에 감염을 시킴으로써 제어시스템을 공격하는 방법이다.
Case 4. 내부자 위협
내부자가 외부에서 사주를 받거나 개인적인 원한에 의해 제어시스템을 공격하는 위협이다. 내부자는 시스템에 접근이 가능하기 때문에 작은 실수에 의해서도 제어시스템이 공격을 받을 수 있어 항상 보안에 신경 써야 한다.

표 6. 랜섬웨어 감염 경로

4.2 랜섬웨어 감염 파급효과

열차 무인운전시스템이 랜섬웨어에 감염되었을 경우 파급효과는 그림 5와 같다.

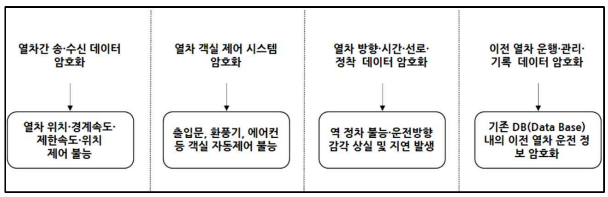


그림 5. 열차 무인운전시스템 랜섬웨어 파급효과

● 열차 간 송·수신 데이터 감염 시

TCMS Console에 수신되는 각종 위치 계산 정보, 제한 속도, 경계 속도 등에 대한 알고리즘 프로그램 파일이 암호화되어 프로세스가 제 기능을 하지 못할 시 무인 열차에 대한 제어권 및 무인 열차 명령 송·수신 기능이 상실되므로 무인 열차의 제어 불능에 따른 충돌 및 급정지를 초래한다.

● 열차 위치·제한·경계속도 데이터 감염 시

선로에 대한 제한 정보, 위치, 다음 역에 정차해야하는 시간 및 운행하고 있는 열차 정보가 없기에 지상과 차상 간 데이터 송·수신 오류로 인해 무인 열차 간의 지연 발생 및 열차간의 사고를 유발 할 수 있어 운행이 정지되므로 무인 열차 승객의 불편 유발 및 경제적 손실을 초래한다.

● 열차 객실 제어 시스템 데이터 감염 시

TCMS는 열차 내의 CCTV, 출입문 제어, 광고 LED 등을 STC를 통해 제어한다. 열차가 정거장에 도착할 시 관제사가 TCMS Console을 통하여 문을 개폐하게 되는데 제어 프로그램 파일이 암호화될 시 출입문 개폐 제어가 불가능 해질 수도 있다. 하지만 역의 스크린 도어 등은 수동으로도 개폐할 수 있게 설계되어있기 때문에 운행 정지 등의 큰 파급은 없을 것이다.

● 이전 열차 운행·관리·기록 데이터 감염 시

DB 내의 무인 열차 제어에 사용되는 프로그램 및 데이터가 암호화 될 시 열차의 원격 제어 기능이 상실되므로 기관사의 수동 조작, 이용객 불편, 경제적 수입 피해 등을 발생시킨다.

Ⅴ. 열차 무인운전시스템 랜섬웨어 대응방안

위에서 분석한 바와 같이 무인운전시스템에서의 랜섬웨어 파급효과는 매우 크다. 그렇기에 랜섬웨어에 대해 항상 경각심을 가지고 대응방안을 염두에 두어야한다. 대응 방안은 표 7과 같다.

Decoy 파일 감염 시 랜섬웨어 대응
랜섬웨어의 특징은 폴더 내의 최상위의 파일부터 감염시킨다는 특성이 있다. 이 특성을 이용하여 최상위에 Decoy 파일을 둔 뒤 파일이 변조 및 암호화 되면 즉각적으로 대응한다.
USB 혼용 사용 금지
외부망에서 사용하는 USB를 내부망에 있는 PC에 연결하여 사용하지 않으며 파일을 USB로 옮기기 전 악성코드 검사를 실행한다. 또한, 주요 시스템과 PC들의 USB Port를 물리적으로 봉쇄한다.
휴대폰 테더링 사용 금지
휴대폰 테더링은 편의를 위해 이용자들이 많이 사용하는 기능이지만 보안을 위해서는 내부망에서 사용하지 않아야 한다.
설치단계에서의 점검
개발사로부터의 감염을 막기 위해서는 시스템 설치 단계에서 점검을 통하여 도입해온 시스템이 악성코드에 감염되어있는 지 확인해야한다.
데이터 백업 및 복구 계획 수립
모든 중요한 정보에 대하여 데이터 백업과 복구 계획을 수립하여 정기적인 백업을 수행하도록 한다. 정기적인 백업이 수행되면 시스템과 데이터의 손실이 최소화되고 복구 프로세스를 신속하게 작동할 수 있다.
열차 무인운전시스템 보안 점검
열차 무인운전시스템을 정기적 기간마다 점검하고 취약점 분석 및 조치를 수행해야 한다.

표 7. 열차 무인운전시스템 랜섬웨어 대응방안

Ⅵ. 결론

본 논문에서는 열차 무인운전시스템과 랜섬웨어에 대해서 설명을 하고, 열차 무인운전시스템이 랜섬웨어에 감염되었을 때의 파급효과 및 대응방안에 대해 제시하였다. 열차 무인운전시스템의 경우에는 앞서 제시한 랜섬웨어 감염시나리오에 대해서 제시된 대응방안 방법을 활용한다면 짧은 시간 안에 열차 무인운전시스템이 정상화가 가능할 것이다. 향후에는 열차 무인 시스템에 대한 랜섬웨어 및 악성코드 탐지 방법과 예방 방법에 대한 연구가 진행되어야 한다.

본 연구는 2018년도 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 과제입니다. (No. 20162220200010)

[참고문헌]

[1] 박종문, 오세화, 이재호.(2014).도시철도 무인운전 적용을 위한 무인운전 특화기능에 대한 연구. 한국철도학회 추계학술대회 논문집

[2] 이영수. (2013). 신분당선 원격차량 제어 및 표시를 위한 TCMS 콘솔. 한국철도학회 철도저널 16권 2호, pp 41~44

[3] 백종현. (2018). 무선통신기반 열차제어시스템 보안 취약성에 관한 연구. 한국통신학회 학술대회논문집, , 568-568.

[4] 송재윤, 류승균, 오세화, 김경수, 이수호. (2012). RF-CBTC 무인운전 시스템 기능구현에 관한 연구. 한국철도학회 학술발표대회논문집, 1443-1452.

[5] 오세화(Sea-Hwa Oh), 김철환(Zhe-Huan Jin), 이기서(Key-Seo Lee). (2014). FHSS 방식을 채용한 RF-CBTC 열차제어시스템 정보 전송의 안정화에 관한 연구. 한국전자통신학회 논문지, 9(4): 455-467

[6] 송재수, 류희문, 이주용, 권용훈, 전환식, 강성원, 이승보. (2009). 철도용 통합 영상 및 데이터 전송장치 개발. 중소기업기술정보진흥원

[7] 최종관, 허상영, 송광렬.(2012). KR S-07050 통신기반열차제어장치(CBTC). 한국철도시설공단

[8] 박재승. (2017). 랜섬웨어(Ransomware)공격에 대한 기업의 방어체계 연구. 동국대학교 국제정보보호대학원 정보보호학과

사이버 위협 시나리오 분석 및 예측의 자동화 방법

조성영, 정현숙, 신영섭, 이동재, 임창완, 오행록

국방과학연구소

An automated method for cyber threat scenario analysis and threat prediction

Sungyoung Cho, Hyunsook Jeong, Youngsup Shin,
Dongdae Lee, Changwan Lim, Haengrok Oh

Agency for Defense Development

요 약

사이버 위협을 탐지하고 대응하기 위해 다양한 보안 센서로부터 생성되는 위협 경보를 효과적으로 분석하고 대응하기 위해 ESM과 SIEM과 같은 솔루션들을 도입하고 운영하고 있으나, APT 공격과 같이 특정 공격 목표를 달성하기 위해 장시간 여러 공격 단계를 수행하는 정교하고 체계적인 사이버 위협에 효과적으로 대응하는 것에 한계가 있다. 본 논문은 위협 경보를 상관분석하여 가장 설득력 있는 사이버 위협 시나리오를 자동으로 분석하고, 그 결과를 바탕으로 다음 위협을 예측하는 시스템을 제안한다. 시스템의 구조와 각 기능에 대한 설계 수준에서 제안하며, 그 과정에서 사이버 위협 시나리오를 분석하고 예측하기 위한 관련 알고리즘에 대한 관련 연구를 분석하였다.

I. 서론

조직을 대상으로 하는 다양한 유형의 사이버 위협에 효과적으로 대응하기 위한 여러 노력들이 지속되고 있다. 그러나 침해사고가 발생한 후 상당한 시간이 지나서야 침해사고의 발생 사실을 인지하는 것이 현실이다.

그 원인 중 하나는 침해사고를 탐지하는 다양한 보안 센서(sensors)(예. 네트워크 보안 솔루션, 엔드포인트 보안 솔루션, 시스템, 애플리케이션 등)에서 발생하는 위협 경보(alert)[1]의 수는 매우 많으나, 위협 경보를 수집하여 분석하고 대응하는 보안 관제 및 분석 자원은 한정되어 있기 때문이다.

한정된 보안 관제 및 분석 자원을 극복하기 위해, 다양한 보안 센서로부터 발생하는 위협 경보를 종합하고 분석하는 것을 도와주는 다양한 솔루션들이 시장에 출시되고 있다. 통합보안관리 솔루션(ESM, Enterprise Security Management)은 보호 대상 네트워크에 설치된 다양한 보안센서를 통합하여 관리해 준다는 이점을 내세웠으나, 다양한 보안 센서로부터 생성되는 위협 경보를 한 장비에서 통합적으로 볼 수 있다는 것 이상의 기능을 가지지 못하였다. 보안 정보 및 이벤트 관리 솔루션(SIEM, Security Information and Event Management)은 다양한 보안 센서에서 생성되는 위협 경보를 통합적으로 수집하는 점에서는 ESM과 비슷하지만, 위협 경보를 빅데이터 기반으로 상관분석하여 위협을 식별할 수 있다는 점에서 차이가 있다. SIEM은 민간 기업에서부터 정부 기관, 군 등 다양한 분야에서 도입하여 운영하고 있다.

그러나 SIEM은 여전한 한계가 있다. APT 공격으로 대표되는 최근의 사이버 위협은 전문적인 공격 집단이 장시간 동안 여러 공격 단계를 통하여 특정 대상에 대한 목표를 달성하기 위한 지속적인 공격을 수행하고 있으나, SIEM은 위협을 식별할 수 있는 수준은 단편적인 수준이며, 전체 사이버 위협의 흐름(context) 관점에 대해 분석하고 있지 못하다. 여전히 많은 침해사고 분석은 침해사고 사후에 전문 분석가가 수작업으로 침해사고와 관련한 다양한 흔적을 수집하여 분석하고, 그 결과에 전문가의 의견을 반영하여 침해사고의 흐름이 포함된 분석 보고서가 도출된다.

이 논문에서는 자동으로 사이버 위협 시나리오를 분석하고, 그 결과를 바탕으로 다음 위협을 예측하는 시스템을 제안하고자 한다. 현재 연구 수준은 시스템 및 각 구성요소를 식별한 수준이며, 각 구성요소에서 실제로 동작하는 알고리즘에 대해서는 연구를 진행하고 있다.

이 논문의 구성은 다음과 같다. 2장에서는 사이버 위협 시나리오를 분석하기 위한 방법과 관련하여, 학계에서 많이 연구하고 있는 경보 상관분석(alert correlation)에 대해서 관련 연구를 분석한다. 3장에서는 관련 연구를 활용하고, 연구들에 내재하는 한계를 극복하기 위해 우리가 제안하고자 하는 사이버 위협 시나리오 및 예측 시스템의 구조를 소개하고, 특히 위협 관계정보를 분석할 수 있는 알고리즘에 대한 이슈를 논의한다. 4장에서 논문을 마무리하고 향후 연구 방향을 소개한다.

1) 일반적으로 위협 이벤트, 로그, 위협 경보 등의 다양한 표현을 사용하나, 본 논문에서는 위협 경보로 용어를 통일하였다.

II. 관련 연구: 경보 상관분석

2.1 개요

경보 상관분석은 보호 대상 네트워크 및 시스템에 설치된 다양한 보안 센서로부터 생성된 다양한 보안 경보를 상관분석하는 것을 말한다. 사이버 위협으로 인하여 생성되는 경보의 수는 매우 많으며, 각각의 경보는 각 보안 센서의 관점에 따라 저수준(low level)의 정보를 포함하고 있다. 또한 보안 센서의 설정 오류 등으로 인해 경보에는 오탐(false positive) 또는 미탐(false negative)이 포함되어 있다[1]. 이는 보안 관제요원 또는 분석가가 위협 상황을 분석하는 데 어려움을 겪는다.

따라서 경보 상관분석 분야에서는 보안 분석가 또는 의사결정자가 보안 상황에 대해 보다 높은 수준(high level)에서 종합적으로 위협 상황을 인식하고 대응할 수 있도록 돕기 위한 다양한 경보 상관분석 기술이 연구되고 있다. 대부분의 경보 상관분석 연구 분야에서 분류하는 기준에 따르면 다음과 같다.

2.2 유사성 기반

유사성(similarity) 기반의 경보 상관분석은 각 경보가 가지는 속성(attribute 또는 feature) 값의 유사성을 기반으로, 유사한 속성을 갖는 경보들을 서로 클러스터링(clustering), 또는 취합(aggregation)한다. 이는 단일한 공격 기법에 대해 다양한 보안 센서가 탐지하여 생성한 경보들에 대해, 중복된 경보를 제거하고 결합(fusion)함으로써, 단일 위협에 대한 고수준에서의 상황인식을 도울 수 있다.

[2, 3, 4, 5, 6, 7]의 연구들은 유사성 기반의 경보 상관분석을 다루고 있다. 이들은 2000년 초반에 주로 연구되었으며, APT 공격과 같은 최근 공격의 성향이 나타나기 전이었다.

2.3 사전 조건-결과 기반

공격자가 여러 공격을 순차적으로 수행하게 될 경우, 이전 단계에서 수행한 공격은 다음 단계의 공격을 위한 준비 과정으로 간주할 수 있다. 이 때 경보를 유발한 공격의 사전 조건(prerequisites 또는 pre-condition)과 결과(consequence 또는 post-condition) 간의 관계를 이용하여, 이전 공격 단계로 인해 발생한 결과와, 다음 공격 단계를 위한 사전 조건이 일치할 경우 두 공격 단계가 연결될 수 있다는 것이 사전 조건-결과 기반 경보 상관분석 기술이다.

사전 조건은 공격이 성공적으로 수행되기 위한 조건을 말하며, 결과는 공격이 성공적으로 수행된 후 발생될 수 있는 모든 결과를 말한다. 이러한 접근 방법은 공격자가 수행하는 전체 공격 시나리오에 대한 정의를 요구하지 않으며, 이전에 발견하지 못했던 공격 시나리오를 발견할 수 있다. 그러나 모든 발생 가능한 공격에 대한 수많은 사전조건과 결과를 구축하

표 1. 경보 상관분석 기술 관련 연구 비교

경보 상관분석 기술 유형	내용	장점	단점
유사도 기반	▪ 유사도에 기반, 서로 유사한 경보를 결합 ▪ 유사도가 임계치를 넘으면 경보가 서로 관련있는 것으로 판단	▪ 여러 센서들로부터 생성된 많은 양의 중복된 경보 감소	▪ 알려진 공격에 대한 경보에 적합 ▪ 경보의 인과성(causality)과 통계적 관계를 밝혀낼 수 없음 ▪ 복잡한 공격을 발견하는 데 제약
사전조건-결과 기반	▪ 공격에 대한 사전조건과 결과에 대한 지식 정의 ▪ 사전 조건: 공격이 성공적으로 수행되기 위한 조건 ▪ 결과: 공격이 수행된 후 발생될 수 있는 모든 결과	▪ 다단계 공격 탐지 (공격에 대한 고수준 뷰를 볼 수 있음) ▪ 공격자의 목적을 판단할 수 있는 유용한 그래프 생성 가능	▪ 설계 복잡성과 사용자 행동으로 인해 실제 네트워크 운영 관점에서 실용적이지 않음 ▪ 모든 공격 행동에 대한 사전조건 및 결과 정보 가 포함된 완전한 공격 데이터베이스를 구축하는 것은 비용이 많이 듦
공격 시나리오 기반	▪ 많은 침해사고는 최종 공격을 성공적으로 달성하기 위해 필요한 다양한 공격 단계 존재 ▪ 사전에 정의된 침해사고 단계를 정의한 것과 비교, 공격 시나리오 구축 ▪ 새로운 경보가 생성되었을 때, 현재 구축된 공격 시나리오와 비교하여 이미 존재하는 시나리오에 추가하거나, 새로운 공격 시나리오를 생성	▪ 잘 정리된 공격을 정확히 탐지 ▪ 여러 센서들로부터 생성된 많은 양의 중복된 경보 감소	▪ 많은 양의 오탐 생성 가능성 ▪ 사용자가 수동으로 공격 시나리오를 특정할 수 있어야 함 ▪ 알려진 공격의 탐지에 한함 (이상 탐지에는 적용 불가) ▪ 다단계 공격 경보는 무시됨

는 것은 전문가의 지식을 기반으로 하며 많은 시간과 비용이 요구된다.

[8, 9, 10, 11, 12, 13, 14]의 연구들은 사전 조건-결과 기반의 경보 상관분석을 다루고 있다.

2.4 공격 시나리오 기반

일반적으로 복잡한 공격은 다단계로 구성되어 있으며(multi-stage attack 또는 multi-step attack), 이전 단계의 공격은 다음 단계의 공격을 위한 준비 과정으로 간주된다. 이러한 전제 조건은 사전 조건-기반 경보 상관분석과 맥락을 같이 한다. 그러나 공격 시나리오 기반의 경보 상관분석은 전체 공격 시나리오를 기반으로 이루어진다.

시나리오는 특정 공격 주체(threat actor)에 의해 발생하는 일련의 공격 패턴(attack pattern)의 조합(캠페인, campaign)으로 간주될 수 있다. 보다 구체적으로, 특정 목적을 달성하기 위한, 논리적으로 연결된 공격 단계들의 연속 과정이 하나의 시나리오에 포함된다.

시나리오 기반 경보 상관분석은, 상관분석을 위해 사용되는 시나리오가 완벽할 경우, 향상된 성능을 보장할 수 있다는 장점이 있다. 그러나 모든 공격에 대한 시나리오를 정의하는 것이 쉽지 않으며, 공격자는 방어 관점에서 알 수 없는 형태로 공격을 수행하므로, 알려지지 않은 형태의 공격을 완벽하게 탐지하지 못할 경우, 해당 접근 방법은 유용하지 않다.

[6, 15, 16, 17, 18, 19, 20]의 연구들은 공격 시나리오 기반의 경보 상관분석을 다루고 있다.

2.5 논의

경보 상관분석에 대한 관련 연구를 분석한 결과는 표 1과 같다. 그러나 앞서 살펴 본 대부분의 연구는 사이버 위협에 대한 사전 지식(prior knowledge)을 요구한다. 사이버 위협의 진화 속도는 점점 빨라지지만, 이를 반영하는 사전 지식을 전문가가 구축하는 것은 현실적으로 불가능하다. 따라서 전문가의 지식 없이도 다양한 보안 센서로부터 생성되는 경보 데이터를 이용한 상관분석 방법이 요구된다.

III. 시스템 구조

3.1 개요

본 논문에서 제안하고자 하는 시스템은, 앞서 2장에서 논의하였던 바와 같이 다양한 보안 센서로부터 생성된 위협 경보를 이용하여 가장 설득력 있는(plausible) 사이버 위협 시나리오를 분석하고, 분석된 위협 시나리오를 기반으로 다음 단계에 올 수 있는 가장 설득력 있는 사이버 위협을 예측하고자 한다. 그림 1은 간단한 시스템 구조를 나타낸다.

3.2 룰셋 기반 위협경보 상관분석 기능

다양한 보안 센서에서 생성되는 위협 경보는 각 보안 센서 관점에서 포함할 수 있는 저수준 정보를 포함하고 있으며, 한 공격 단계(single attack phase)에서 공격자가 수행하는 공격에 의해 발생되는 보안 경보의 수는 매우 많다. 또한 보안 센서의 설정이 완벽하지 않아 오탐(false positive) 또는 미탐(false negative)이 발생할 수 있다.

룰셋 기반 위협경보 상관분석 기능에서는 위협 경보를 이용하여 위협을 분석하기 위한 룰셋(rule set) 기반으로 기존의 SIEM 솔루션과 같이 상관분석을 수행하여 보다 높은 수준의 하이퍼 위협 경보(hyper alert)를 생성한다. 하이퍼 위협 경보는 크게 오프라인 상관분석 기능과 온라인 상관분석 기능에서 활용된다.

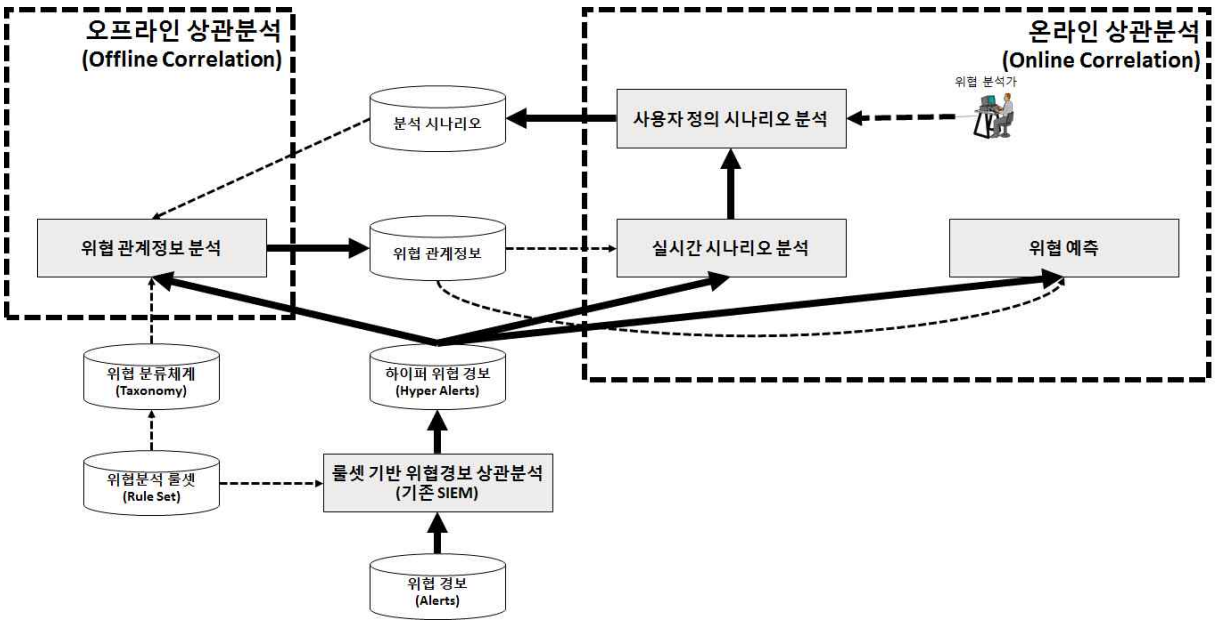


그림 1. 사이버 위협 시나리오 및 예측 시스템 구조

	a1	a2	a3	a4	a5
a1	C(a1,a1)	C(a1,a2)	C(a1,a3)	C(a1,a4)	C(a1,a5)
a2	C(a2,a1)	C(a2,a2)	C(a2,a3)	C(a2,a4)	C(a2,a5)
a3	C(a3,a1)	C(a3,a2)	C(a3,a3)	C(a3,a4)	C(a3,a5)
a4	C(a4,a1)	C(a4,a2)	C(a4,a3)	C(a4,a4)	C(a4,a5)
a5	C(a5,a1)	C(a5,a2)	C(a5,a3)	C(a5,a4)	C(a5,a5)

그림 2. 경보 상관분석 매트릭스(ACM)[22]

3.3 위협 관계정보 분석 기능

위협 관계정보 분석 기능은 위협 분류체계[21]와 같은 사전 지식을 이용하여 위협 관계정보를 분석하는 기능과, 하이퍼 위협 경보를 이용하여 위협 관계정보를 분석하는 기능을 포함한다. 여기서 위협 관계정보는 위협 유형(type) 간의 시간적 관계(temporal relationship)와 인과관계(causal relationship)를 나타낸다.

사전 지식을 이용하여 위협 관계정보를 분석하는 기능은 전문가의 지식 또는 경험치에 의하여 위협 관계정보에 대해 사전에 구축하는 것을 말한다. 이는 시스템이 초기에 구축될 경우 위협 경보 데이터가 충분히 누적되지 않을 경우 사전 지식 기반 위협 관계정보를 이용하여 위협 시나리오를 분석하고 다음 위협을 예측하기 위한 것이다.

하이퍼 위협 경보를 이용하여 위협 관계정보를 분석하는 기능은 위협 경보를 기반으로 하여 룰셋 기반 위협경보 상관분석 기능에서 생성된 하이퍼 위협 경보 데이터를 분석하여 위협 관계정보를 모델링하는 것을 말한다. 가령, 특정 하이퍼 위협 경보 a_i와 b_j가 있을 때, 위협 유형 A와 B는 다음과 같이 나타낼 수 있다.

$$A = \{a_1, a_2, ..., a_i, ..., a_m\},\ 1 \leq i \leq m$$

$$B = \{b_1, b_2, ..., b_j, ..., b_n\},\ 1 \leq j \leq n$$

이 때 위협 유형 A와 B 간 인과관계(시간적 관계는 이미 형성되어 있을 때)는 $A \rightarrow B$과 같이 표현될 수 있으며, A와 B의 인과관계 정도를 나타내는 상관 정도(correlativity)는 $Cor(A,B)$와 같이 표현될 수 있다. 전체 위협 유형 간 상관 정도는 그림 2[22]의 경보 상관분석 매트릭스(ACM, alert correlation matrix)와 같은 테이블에 저장할 수 있다. 여기서 세로축은 이전 위협 유형, 가로축은 이후 위협 유형을 나타내며, 매트릭스의 대각선을 기준으로 대칭되는 두 값은 같지 않다. 즉 $a_1 \rightarrow a_2$에 대한 상관 정도인 $Cor(a_1, a_2)$와 $a_2 \rightarrow a_1$에 대한 상관 정도인 $Cor(a_2, a_1)$은 같지 않다. 위협 유형 간의 상관 정도를 구하기 위한 많은 연구들이 진행되어 왔다. 우리는 이 중에서 베이지안 네트워크(Bayesian network)를 기반으로 한 위협 관계정보 분석에 초점을 두고 있다[22., 23, 24, 25, 26, 27].

마지막으로, 위협 관계정보 분석 기능에서는 온라인 상관분석 기능을 통해 도출된 위협 시나리오를 입력값으로 받아 위협 관계정보를 갱신한다. 위협 관계정보 분석 기능은 실시간으로 수집되는 위협 경보와 무관하게 주기적으로 동작하며(오프라인 분석), 수집되는 위협 경보의 양에 따라 주기가 조정될 수 있다.

3.3.1 베이지안 네트워크

베이지안 네트워크(Bayesian network)는 랜덤 변수의 집합과 비순환 그래프(DAG, directed ascyclic graph)를 통해 그 집합을 조건부 독립으로 표현하는 확률의 그래픽 모델을 말한다. 베이지안 네트워크를 구성하는 DAG의 노드는 위협 유형이며, 노드를 연결하는 엣지는 위협 유형 간의 상관 정도이다.

구체적으로, 위협 유형 A가 발생한 후에 위협 유형 B가 발생한 경우, A와 B 간의 상관 정도는 베이즈 이론(Bayes' Theorem)과 조건부 독립(conditional probability)을 이용하여 계산한다. 이 때 두 위협 간의 인과관계는 다음의 조건을 만족해야 한다고 관련 연구들에서 제안하고 있다[25, 27].

위협 유형 A에 대한 하이퍼 위협 경보 a_i와 위협 유형 B에 대한 하이퍼 위협 경보 b_j에 대해,

- 두 하이퍼 위협 경보는 정해진 시간 윈도(time window) 내에서, a_i 다음에 b_j가 와야 한다.
- a_i와 b_j에 대해, IP 주소와 포트 번호의 관계에 대하여 표 2의 동등 제약조건(ECs, equality constraints) 중 하나 이상을 만족해야 한다.

표 2. 두 위협 유형 간 제약 조건[25, 27]

EC1	동일한 출발지 IP 주소 (a.srcIP = b.srcIP)
EC2	동일한 목적지 IP 주소 (a.dstIP = b.dstIP)
EC3	동일한 출발지 포트 (a.srcPort = b.srcPort)
EC4	동일한 목적지 포트 (a.dstPort= b.dstPort)
EC5	IP 체인 관계 (a.dstIP = b.srcIP)
EC6	역 IP 체인 관계 (a.srcIP = b.dstIP)

실제로는 두 위협 유형 간에 관련성이 존재하는 동등 제약조건의 집합이 선택된다. 다시 말하면 아래의 식을 만족하는 동등 제약조건이 선택된다.

$$P(B, \{ec\}|A) > P(A)$$

두 위협 유형 A와 B에 대한 하이퍼 위협 경보가 가지는 속성으로부터 특징(feature)를 추출하고, 가중치 합을 통해 $Cor(A,B)$을 계산한다. 이를 전체 위협 유형 간의 쌍(pair)에 대해 계산하여, 그림 2와 같은 경보 상관분석 매트릭스를 계산한다. 속성으로부터 추출할 수 있는 특징과, 특징으로부터 가중치 합을 계산하기 위해 필요한 가중치에 대해서는 현재 연구를 진행하고 있다.

3.4 실시간 시나리오 분석 기능

실시간 시나리오 분석 기능은 룰셋 기반 위협경보 상관분석 기능에 의해 실시간으로 생성된 하이퍼 위

협 경보에 대해, 위협 관계정보 분석 기능에서 생성한 위협 관계정보 모델을 이용하여 위협 시나리오를 분석한다. 실시간 시나리오 분석 기능은 실시간으로 수집되는 위협 경보를 기반으로 생성되는 하이퍼 위협 경보 인스턴스에 대한 분석이므로 실시간으로 동작한다(온라인 분석). 해당 기능은 우리의 이전 연구 결과[29]를 기반으로 한다.

구체적으로 설명하면, 특정 하이퍼 위협 경보 a_i가 생성되었을 때, 해당 위협 유형 A와 관련된 위협 유형을 가지는 하이퍼 위협 경보 인스턴스 중 a_i의 특징과 비교하였을 때 임계치보다 높은 특징을 가지는 하이퍼 위협 경보 인스턴스를 선택한다. 이러한 과정을 해당되는 하이퍼 위협 경보 인스턴스가 더 이상 나오지 않을 때까지 반복한다.

3.5 사용자 정의 시나리오 분석

실시간 시나리오 분석 기능에서 도출된 위협 시나리오 목록은 정확하지 않을 수 있다. 이러한 경우 사용자 정의 시나리오 분석 기능에서 위협 분석가의 개입을 통해 필터링할 수 있다. 또는 위협 분석가는 분석 결과가 가장 설득력 있는(plausible) 위협 시나리오라고 판단할 경우, 침해사고 분석 보고서를 생성하기 위해 시나리오에 제목, 설명 등과 같은 메타 정보를 작성하여 저장하게 된다.

3.6 위협 예측 기능

위협 관계정보 분석 기능에서 생성한 위협 관계정보 모델을 이용하여, 룰셋 기반 위협경보 상관분석 기능에 의해 실시간으로 생성된 하이퍼 위협 경보에 대해 다음 단계에서 올 수 있는 가장 설득력 있는 위협 유형과 관련 속성을 예측한다.

구체적으로 설명하면, 특정 하이퍼 위협 경보 a_i가 생성되었을 때, 해당 위협 유형 A와 관련된 위협 유형 중 가장 높은 상관 정도를 가지는 위협 유형을 선택한다. 만약 해당 위협 유형이 C라면 C와 관련된 이전 하이퍼 위협 경보 $\{c_1, c_2, \ldots, c_p\}$들이 가지는 속성에 대한 통계 분석을 수행하여 속성들에 대한 확률 분포를 나타내어 예측된 다음 위협이 가질 수 있는 속성 정보를 분석가에게 전달한다. 이는 다가올 수 있는 다음 위협에 대한 사전적인 대응을 수행할 수 있도록 돕는다.

IV. 결론 및 향후 연구

본 논문에서는 전문가의 지식에 전적으로 의존하지 않고 자동으로 사이버 위협 시나리오를 분석하고, 그 결과를 바탕으로 다음 위협을 예측하는 시스템을 제안하였다. 한다. 이를 위하여 시나리오 분석 및 위협 예측을 위한 경보 상관분석 분야에 대한 관련 연구를 분석하였다. 관련 연구들은 대부분 전문가의 지식이 전적으로 요구되며, 실시간으로 수집되는 위협 경보에 대한 온라인 분석보다는 데이터베이스에 저장된 주어진 데이터에 대한 오프라인 분석에 초점을 두고 있다는 점에서 한계를 보인다.

본 논문에서 제안한 연구 수준은 시스템 및 각 구성요소를 식별한 수준이다. 향후 각 구성요소, 구체적으로는 위협 관계정보 분석 기능에서 실제로 위협 관계정보를 생성하고 업데이트하기 위한 알고리즘, 위협 관계정보를 이용하여 실시간으로 수집되는 위협 경보(특히 기존의 SIEM 솔루션 기능과 매핑되는 룰셋 기반 위협경보 분석 기능에서 출력되는 하이퍼 위협 경보)에 대해서 위협 시나리오를 분석하고 다음 위협 단계를 예측하기 위해 필요한 알고리즘에 대한 연구를 진행하고 있다.

또한 알고리즘을 연구하고 검증하기 위한 데이터셋을 개발하기 위해, 현재 군에서 운용하고 있는 네트워크 환경을 모의한 테스트베드를 구축하고, MITRE ATT&CK을 반영한 모의침투 시나리오를 설계하고 수행하여 각 보안 센서에서 위협 경보를 생성하고자 한다. 이는 2장에서 논의했던 연구들이 알고리즘을 평가하기 위해 사용했던 DARPA 2000 데이터셋의 한계(매우 오래 전에 공개되어 현재의 사이버 위협 동향을 반영하지 못함)를 극복하고자 한다. 또한 데이터셋을 통하여 알고리즘을 평가하는 지표를 결정하여 우리가 개발하고자 하는 시스템이 얼마나 잘 분석하는지를 평가할 필요가 있다.

[참고문헌]

[1] Fredrik Valeur, Giovanni Vigna, Christopher Kruegel and Richard A. Kemmerer, “A comprehensive approach to intrusion detection alert correlation”, IEEE Transactions on dependable and secure computing, vol.1, no.3, pp.146-169, 2004, IEEE.

[2] Alfonso Valdes and Keith Skinner, “Probabilistic alert correlation”, International Workshop on Recent Advances in Intrusion Detection, pp.54-68, 2001, Springer.

[3] Frédéric Cuppens, “Managing Alerts in a Multi-Intrusion Detection Environment”, Proceedings of the 17th Annual Computer Security Applications Conference, pp.22, 2001, IEEE Computer Society.

[4] Herve Debar and Andreas Wespi, “Aggregation and correlation of intrusion-detection alerts”, International Workshop on Recent Advances in Intrusion Detection, pp.85-103, 2001, Springer.

[5] Stuart Staniford, James A. Hoagland and Joseph M. McAlerney, “Practical automated detection of stealthy portscans”, Journal of Computer Security, vol.10, no.1-2, pp.105-136, 2002, IOS Press.

[6] Benjamin Morin, Ludovic Me, Debar Herve and Mireille Ducasse, “M2D2: A formal data model for IDS alert correlation”, International Workshop on Recent Advances in Intrusion Detection, pp.115-137, 2002, Springer.

[7] Benjamin Morin and Herve Debar, “Correlation

of intrusion symptoms: an application of chronicles", International Workshop on Recent Advances in Intrusion Detection, pp.94-112, 2003, Springer.
[8] Peng Ning, Douglas Reeves and Yun Cui, "Correlating alerts using prerequisites of intrusions", 2001, North Carolina State University at Raleigh.
[9] Peng Ning, Yun Cui and Douglas S. Reeves, "Analyzing intensive intrusion alerts via correlation", International Workshop on Recent Advances in Intrusion Detection, pp.74-94, 2002, Springer.
[10] Peng Ning, Yun Cui and Douglas S. Reeves, "Constructing attack scenarios through correlation of intrusion alerts", Proceedings of the 9th ACM Conference on Computer and Communications Security, pp.245-254, 2002, ACM.
[11] Peng Ning, Dingbang Xu, Christopher G. Healey and Robert St. Amant, "Building Attack Scenarios through Integration of Complementary Alert Correlation Method", NDSS, vol.4, pp.97-111, 2004.
[12] Frédéric Cuppens and Alexandre Miege, "Alert correlation in a cooperative intrusion detection framework", Security and privacy, 2002. proceedings. 2002 IEEE symposium on, pp.202-215, 2002, IEEE.
[13] Steven Cheung, Ulf Lindqvist and Martin W. Fong, "Modeling multistep cyber attacks for scenario recognition", DARPA information survivability conference and exposition, 2003. Proceedings, vol.1, pp.284-292, 2003, IEEE.
[14] Faeiz Alserhani, Monis Akhlaq, Irfan U. Awan, Andrea J. Cullen and Pravin Mirchandani, "MARS: multi-stage attack recognition system", Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on, pp.753-759, 2010, IEEE.
[15] Frédéric Cuppens and Rodolphe Ortalo, "Lambda: A language to model a database for detection of attacks", International Workshop on Recent Advances in Intrusion Detection, pp.197-216, 2000, Springer.
[16] Oliver Dain and Robert K. Cunningham, "Fusing a heterogeneous alert stream into scenarios", Proceedings of the 2001 ACM workshop on Data Mining for Security Applications, vol.13, 2001.
[17] Steven T. Eckmann, Giovanni Vigna and Richard A. Kemmerer, "STATL: An attack language for state-based intrusion detection", Journal of computer security, vol.10, no.1-2, pp.71-103, 2002, ISO Press.
[18] Jonathon Abbott, Jim Bell, Andrew Clark, Olivier De Vel and George Mohay, "Automated recognition of event scenarios for digital forensics", pp.293-230, 2006, ACM.
[19] Peyman Kabiri and Ali AGhorbani, "A Rule-based Temporal Alert Correlation System", IJ Network Security, vol.5, no.1, pp.66-72, 2007.
[20] Dongho Kang and Jungchan Na, "A rule based event correlation approach for physical and logical security convergence", IJCSNS, vol.12, no.1, pp.28, 2012.
[21] Sungyoung Cho, Insung Han, Hyunsook Jeong, Jinsoo Kim, Sungmo Koo, Haengrok Oh and Moosung Park, "Cyber Kill Chian based Threat Taxonomy and its Application on Cyber Common Operational Picture", Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA 2018), 2018 International Conference on. pp. 1-8, IEEE, 2018.
[22] Bin Zhu and Ali A. Ghorbani, "Alert correlation for extracting attack strategies", IJ Network Security, vol.3, no.3, pp.244-258, 2006.
[23] Hanli Ren, Natalia Stakhanova, and Ali A. Ghorbani, "An online adaptive approach to alert correlation", International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, pp.153-172, 2010, Springer.
[24] Mirco Marchetti, Michele Colajanni and Fabio Manganiello, "Identification of correlated network intrusion alerts", Cyberspace Safety and Security (CSS), 2011 Third International Workshop on, pp.15-20, 2011, IEEE.
[25] Fatemeh Kavousi and Behzad Akbari, "Automatic learning of attack behavior patterns using Bayesian networks", Telecommunications (IST), 2012 Sixth International Symposium on, pp.999-1004, 2012, IEEE.
[26] Reza Anbarestani, Behzad Akbari, and Fariba Fathi, "An iterative alert correlation method for extracting network intrusion scenarios", Electrical Engineering (ICEE), 2012 20th Iranian Conference on, pp. 684-689, 2012, IEEE.
[27] Chih-Hung Wang and Ye-Chen Chiou, "Alert correlation system with automatic extraction of attack strategies by using dynamic feature weights", International Journal of Computer and Communication Engineering, vol.5, no.1, pp.1, 2016, IACSIT Press.
[28] Ali Ahmadian Ramaki and Abbas Rasoolzadegan, "Causal knowledge analysis for detecting and modeling multi-step attacks", Security and Communication Networks, vol.9, no.18, pp.6042-6065, 2016, Wiley Online Library.
[29] 조성영, 정현숙, 안재홍, 박무성, "사이버 킬체인 기반 다단계 사이버 위협 분석 기법", 2015 한국군사과학기술학회 종합학술대회 논문집, pp.1003-1004, 2015.

이동 경로 정보를 활용한 주소 인증1)

박호성*, 남승수**, 최대선*†

*공주대학교 의료정보학과, **공주대학교 융합과학과

Address Authentication using Location History

Hosung Park*, Seungsoo Nam**, Daeseon Choi*+

*Dept. of Medical Information, Kongju National University,
**Dept. of Convergence Science, Kongju National University

요 약

본 논문은 이동 경로 정보를 활용한 주소 인증 방안 즉, 사용자가 실제로 등록된 주소에 살고 있는지 검증하는 방안을 제안한다. 주소 인증을 위한 기존 연구는 클러스터링 알고리즘을 사용하여 관심 지역을 추출하는 방법을 사용한다. 관심 지역 중 하나에 주소가 포함된다면 해당 주소를 인증하는 것이다. 그러나 주소와 관계없는 불필요한 관심 지역들은 비적합 주소 즉, 다른 유저의 주소나 허위 주소를 인증하는 인증 오류 문제를 야기할 수 있다. 제안 방안은 다른 관심 지역과 구분되는 주소의 위치 정보 조건들을 통해 불필요한 관심 지역들을 제거함으로써 인증 오류 확률을 줄이고자 한다. 다시 말해 긴 지속시간, 높은 데이터 비중, 일관성이라는 세 가지 조건을 모두 만족하는 관심 지역만을 주소 인증에 활용한다. 실험 결과는 제안방안이 기존 연구들에 비해 높은 주소 인증 성공 확률을 가짐을 보여준다.

I. 서론

스마트폰, 웨어러블 디바이스, 사물인터넷 디바이스 등과 같은 스마트 디바이스들의 빠른 성장과 더불어 사용자의 이동 경로 정보의 획득이 용이해지면서, 수많은 위치 기반 서비스들이 개발되어 왔다. 본 논문은 다양한 위치 기반 서비스들 중 하나로써, 사용자의 이동 경로 정보를 활용한 주소 인증을 목표로 한다. 주소 인증은 사용자가 등록된 주소에 실제로 살고 있는지 검증하는 일련의 과정을 뜻한다. 따라서 주소 인증은 관계부처의 실거주자 조사, 주소에 관계된 자격 확인(지역 취업, 입학, 분양, 부동산 거래 등), 비대면 본인확인 등 다양한 분야에서 활용이 가능하다.

이동 경로 정보를 통한 주소 인증 자체는 아직 연구된 바가 없지만, 최근 사용자 인증을 위해 이동 경로 정보를 활용하는 방안들이 제안되었다 [1, 2]. 이들은 이동 경로 정보로부터 사용자의 이동 패턴을 추출, 모델링함으로써 사용자를 식별한다. 패턴 모델링에는 머신 러닝 및 신경망을 사용했다. 그러나 이 방안들을 주소 인증에 그대로 적용할 수는 없다. 이동 패턴 모델은 주소에 대한 어떤 단서도 제공하지 않기 때문이다. 머신 러닝의 학습 과정과 그 결과물인 모델은 일반적으로 블랙박스이며, 따라서 해당 모델로부터 주소 인증을 위한 특징을 직접 추출할 수 없다.

다른 관련 연구인 관심 지역(location of

1) 이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원(No.2016-0-00173, 핀테크 서비스 금융사기 방지를 위한 비대면 본인확인) 및 한국연구재단의 지원(No.2016R1A4A1011761, 핀테크 서비스를 위한 금융 보안 핵실 기술 개발)을 받아 수행된 연구임

* 주저자, hspark@kongju.ac.kr

† 교신저자, sunchoi@kongju.ac.kr

interest or point of interest) 추출은 [3-7] 인증 관련 분야는 아니지만 주소 인증에 활용 가능한 요소를 갖는다. 이들은 클러스터링 알고리즘을 이용하여 이동 경로 정보로부터 관심 지역 즉, 사용자가 빈번히 가는 혹은 오랜 시간 머무는 장소를 특정 한다. 따라서 사용자의 주소가 관심 지역에 속한다면 주소가 인증됐다고 추정이 가능하다. 관심 지역 추출을 위한 클러스터링은 크게 밀도 기반 클러스터링과 시간 기반 클러스터링으로 구분할 수 있다. 밀도 기반 클러스터링은 [3-5] 전체 이동 경로 정보에서 다른 지역에 비해 많은 비중을 차지하는 지역을 찾아낸다. 반면 시간 기반 클러스터링은 [6, 7] 사용자가 일정 범위 안에 일정 시간 이상 머문다면 해당 지역을 관심 지역으로 선별한다. 클러스터링 알고리즘의 특성으로 인해, 시간 기반 클러스터링은 사용자가 한 번에 오래 머문 장소를 잘 찾아내지만 해당 장소가 어느 정도의 비중을 가지는지는 알지 못한다. 또한, 밀도 기반 클러스터는 그와 반대의 특성을 갖는다. 관심 지역 추출을 통한 주소 인증 방법의 가장 큰 문제점은 잘못된 인증의 위험 즉, 다른 유저의 주소나 허위 주소를 사용자의 주소로 인증할 수 있는 위험이 크다는 것이다. 이는 일반적으로 클러스터링 알고리즘이 주소와 관련된 지역뿐만 아니라 다른 많은 관심 지역을 추출하기 때문이다. 다시 말해, 적합하지 않은 주소가 이런 관심 지역들 중 하나에 속한다면 사용자의 주소로 오인할 수 있는 위험이 있는 것이다.

본 논문은 이동 경로 정보를 활용한 사용자의 주소 인증 방안을 제안한다. 제안 방안의 목표는 앞서 언급한 관심 지역 추출을 통한 주소 인증에 비해 인증 오류 확률을 줄이는 것에 있다. 이를 위해, 우리는 일반적인 관심 지역과 구분하기 위한 주소의 위치정보 조건들을 활용한다. 주소의 위치정보 조건들은 다음과 같다.

- 긴 지속 시간 : 주소의 위치 정보는 한 장소에서 오래 지속 된다.
- 높은 데이터 비중 : 주소 지역은 전체 위치 정보에서 매우 높은 비중을 차지한다.
- 일관성 : 앞의 두 조건이 높은 확률로 매일 반복된다.

적은 수의 관심 지역만이 위의 세 가지 조건을 모두 만족할 수 있다. 다시 말해 제안 방안은 주소 지역이 아니라고 생각되는 관심 지역들을 모두 제거함으로써 주소 추정 지역을 최소화하려 한다. 이는 인증 오류 확률 감소에 기여할 수 있다. 제안 방안은 세 가지 조건을 만족하는 주소 추정 지역을 찾기 위해 시간 기반 클러스터링과 밀도 기반 클러스터링을 모두 사용한다.

II. 제안 방안

우리는 여러 관심 지역들 중, 사용자의 주소가 포함되는 하나의 클러스터를 주소 클러스터라고 정의한다. 주소 인증을 위한 이상적인 형태는 일련의 과정을 통해 주소 클러스터 단 하나만을 추출하는 것이다. 그러나 지나치게 엄격한 조건은 오히려 주소 클러스터 역시 제거하는 위험을 초래할 수 있다. 따라서 제안 방안의 설계 원칙은 다음과 같다.

- 주소의 세 가지 조건을 사용하여 주소 추정 클러스터의 수를 최소화한다.

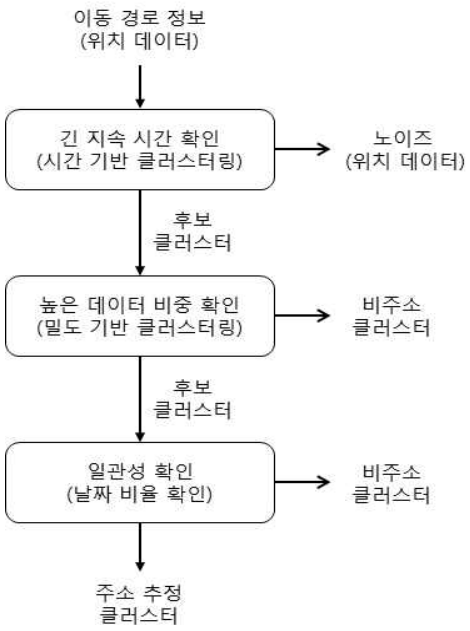


그림 1. 주소 추정 클러스터 추출 과정

그림 1은 주소 추정 클러스터를 추출하는 3단계의 과정을 보여준다. 이동 경로 정보는 연속된 위치 정보들로 구성되어 있으며, 하나의

위치 정보는 타임스탬프, 위도, 경도로 이루어진다. 첫 번째 조건인 긴 지속 시간을 만족하기 위해 제안 방안은 시간 기반 클러스터링을 활용한다. 시간 기반 클러스터링은 시간 흐름에 따라 같은 장소의 위치 정보들로 클러스터를 구성하다가 다른 장소로 이동하는 경우 새 클러스터를 생성한다. 이 때, 지속 시간이 적은 클러스터는 제거한다. 다시 말해 첫 위치를 기준으로 일정 범위 d 안에 일정 시간 t 이상 머문다면 해당 위치 정보들로 클러스터를 생성한다. 일정 범위 d를 벗어나면 새로운 위치를 기준점으로 사용한다. 임계값 변수인 d와 t는 주소 인증 성능에 직접적인 영향을 미치며, 이는 실험을 통해 적절한 값을 찾는다. 생성된 클러스터들은 후보 클러스터가 되어 다음 과정의 입력 데이터로 사용된다.

시간 기반 클러스터링 이후, 남아있는 후보 클러스터들은 서로 겹쳐져 있을 확률이 매우 높다. 시간 기반 클러스터링 알고리즘은 기존의 위치에서 벗어나면 항상 새로운 클러스터를 생성하기 때문에, 같은 장소를 재방문하더라도 새로운 클러스터를 생성하는 것이다. 높은 데이터 비중 조건을 확인하기 위해 우리는 같은 장소의 클러스터를 병합할 필요가 있다. 밀도 기반 클러스터링이 이 문제의 답이 될 수 있으며, 우리는 널리 알려진 밀도 기반 클러스터링 알고리즘인 DBSCAN을 [8] 사용한다. DBSCAN은 시간의 흐름에 관계없이 각 위치점의 이웃점들의 밀도를 기반으로 클러스터를 생성한다. 구체적으로는 각 위치점을 기준으로 일정 범위 r 안에 밀도 n 이상의 이웃점이 존재한다면 해당 위치점은 핵심점이 된다. 하나의 클러스터는 한 장소의 모든 핵심점들과 그 이웃점들로 구성된다. 따라서 시간 기반 클러스터링 이후 남아있는 위치 정보들을 기반으로 DBSCAN을 사용하면 자연스럽게 겹쳐져 있는 클러스터들을 병합하는 결과가 된다. 두 번째 조건인 높은 데이터 비중을 확인하기 위해 각 클러스터들의 밀도를 확인하고 일정 기준 d를 넘지 못하는 클러스터들은 제거된다. 이 때 밀도 기준인 n과 d는 현재 위치 정보 개수를 전체 위치 정보 개수로 나눈 비율을 사용한다. 제거되지 않고 남아 있는 클러스터들은 후보 클러스터로서 다음 과정의 입력 데이터로 사용된다.

마지막 조건인 일관성은 다른 두 조건과 다른 의미를 갖는다. 사람들은 일반적으로 출장, 여행과 같은 특별한 날을 제외하고 매일 주소에 해당하는 위치에 머무른다. 따라서 제안방안은 각 후보 클러스터에서 사용자가 머무른 날짜의 비율을 일관성 기준으로 사용한다. 다시 말해 날짜 비율이 일관성 비율 임계값 c를 넘지 않는다면 해당 클러스터는 제거된다. 각 클러스터의 날짜 비율은 해당 클러스터 위치 정보들의 날짜 개수를 전체 실험 날짜로 나눠서 계산한다. 현재 남아 있는 위치 정보들은 시간 기반 클러스터링과 밀도 기반 클러스터링 과정을 거쳤다는 것을 상기하면, 일관성 확인 과정은 앞의 두 조건이 매일 반복되는지 확인한다는 것을 의미한다. 일관성 확인 과정은 출장, 여행, 허위 주소 인증을 위한 짧은 기간은 거주와 같은 해위로 인해 클러스터가 발생하는 것을 막을 수 있다. 남아 있는 클러스터들은 최종적으로 주소 추정 클러스터가 된다.

만약 등록된 주소가 주소 추정 클러스터에 포함된다면 해당 주소는 인증이 완료된다. 주소 추정 클러스터를 추출하는 일련의 과정은 실제 주소 클러스터를 제거하는 위험을 주의 깊게 피하면서 기존의 관심 지역 추출을 통한 주소 인증 방법들에 비해 최종 클러스터 개수를 줄일 수 있다. 또한 줄어든 클러스터 개수는 주소 인증 오류를 감소시키려는 우리의 목표에 기여할 수 있다. 앞서 언급했듯이, 클러스터의 개수가 늘어날수록 비적합 주소를 인증하는 오류 확률이 증가하기 때문이다.

III. 성능 평가

3.1 실험 환경

주소를 포함하는 이동 경로 정보는 아직 공개된 데이터가 없기 때문에 우리는 직접 데이터 세트를 구성했다. 서울에 사는 27명의 실험자로부터 27개의 이동 경로 정보와 주소를 수집했다. 스마트폰 어플리케이션을 통해 1분 간격으로 24시간 위치 정보를 수집했으며 평균

수집 기간은 63일이다. 한 사용자의 주소 인증 실험 시, 해당 사용자의 주소를 적합 주소로 다른 26명의 주소를 비적합 주소로 사용했다.

표 1. 임계값 변수 값 범위

구분	변수	역할	값 범위
시간기반 클러스터링	s	거리기준	50m-500m
	t	시간기준	1h-6h
밀도기반 클러스터링	r	거리기준	20m
	n	지역밀도기준	0.05%
	d	클러스터밀도기준	4%-40%
일관성	c	날짜비율기준	20%-80%

표 1은 주소 추정 클러스터 추출 과정에서 사용하는 임계값 변수들의 범위를 보여준다. 예를 들어, s가 100m이고 t가 3시간일 경우 시간 기반 클러스터링 알고리즘은 사용자가 기준 위치에서 100m 이내 범위에서 3시간 이상 머물 경우 클러스터를 생성한다. d가 10%인 경우 두 번째 단계에서 밀도가 10% 미만인 클러스터를 제거하며, c가 50%인 경우 세 번째 단계에서 날짜 비율이 50% 미만 즉, 30일 미만인 클러스터를 제거한다. 밀도 기반 클러스터링의 임계값 변수인 r과 n은 각각 20m와 0.05%로 고정했는데, 이는 제안 방안에서 밀도 기반 클러스터링이 클러스터들의 병합에만 사용되기 때문이다. 앞서 설명했듯이 병합된 클러스터의 높은 데이터 비중 확인은 변수 d를 통해 수행한다.

3.2 실험 결과

제안 방안의 성능을 두 가지 기존 연구인 시간 기반 클러스터링(TBC), 밀도 기반 클러스터링(DBSCAN)과의 비교를 통해 보인다.

표 2. 주소 인증 결과

구분	FAR	FRR	AER	클러스터수
TBC	0.0188	0.0370	0.0279	24.21
DBSCAN	0.0296	0.0	0.0148	13.82
제안방안	0.0108	0.0	0.0053	6.81

표 2는 FAR (false accept rate), FRR (false reject rate), AER (average error rate) 세 가지 지표와 27명 실험자의 평균 최종 클러스터 개수를 통해 각 방안의 성능을 보여준다. FAR은 비적합 주소를 적합 주소로 잘못 인증하는 경우의 비율, FRR은 적합 주소를 비적합 주소로 잘못 인증하는 경우의 비율, AER은 FAR과 FRR의 평균 오류율을 의미한다. 우리의 목표는 주소 인증 오류의 비율을 줄이는 것이기에 오류율에 관련된 인자들을 선택했다.

TBC는 s가 250m, t가 4시간인 경우 최대 성능을 보였다. DBSCAN의 경우 r이 200m, n이 0.7%일 때 최대 성능을 보였다. 제안 방안은 s, t, d, c가 각각 200m, 3시간, 24%, 65%인 경우 최대 성능을 보였다. 최대 성능은 AER을 기준으로 선택했다.

모든 지표에서 제안 방안은 기존 연구들에 비해 높은 성능을 보여준다. 이는 주소 추정 클러스터라고 할 수 있는 최종 클러스터의 개수가 기존 연구들에 비해 반 이상 적기 때문이다. 따라서 비적합 주소 즉 다른 사용자들의 주소를 적합 주소로 잘못 인증하는 위험이 줄어들고 FAR 수치를 줄이는 결과를 이끌었다. DBSCAN의 경우 TBC에 비해 클러스터의 개수가 적음에도 불구하고 FAR 수치가 더 높게 나오는 것을 볼 수 있는데, 이는 밀도 기반 클러스터링 결과물인 각 클러스터의 크기 때문이라고 할 수 있다. 항상 클러스터의 크기가 일정한 시간 기반 클러스터링에 비해 밀도 기반 클러스터링은 하나의 클러스터 크기가 경우에 따라 매우 커질 수 있다. 클러스터의 수가 많을 때와 같은 이유로 각 클러스터의 크기가 커질수록 인증 오류의 위험 즉, FAR 수치가 커질 수 있다.

우리의 실험은 한계점을 가지고 있다. 제안 방안은 작은 범위에 많은 실험자가 있을 경우 다른 방안에 비해 더 좋은 성능을 보일 수 있을 것이라 예상한다. 하지만 현재의 데이터 세트는 서울이라는 넓은 지역에 상대적으로 적은 실험자로 구성되어 있다. 따라서 모든 인증 오류율이 4%미만이다. 현재 우리는 한 대학 근처라는 상대적으로 좁은 지역에서 참가자들을 모집하여 데이터를 구성하고 있으며, 새로운 데이터 세트를 포함하여 실험을 확장할 수 있을 것

이라 기대한다.

IV. 결론

본 논문에서는 사용자의 이동 경로 정보를 활용한 주소 인증 방안을 제안했다. 관심 지역 추출을 활용한 기존의 주소 인증 방안에 비해 인증 오류율을 줄이기 위해, 제안 방안은 다른 관심 지역과 구분되는 주소의 위치 정보 조건들을 활용했다. 다시 말해 긴 지속 시간, 높은 데이터 비중, 일관성 이렇게 세 가지 조건을 모두 만족하는 관심 지역만을 주소 추정 클러스터로서 추출했다. 불필요한 관심 지역을 제거함으로써 제안 방안은 비적합 주소를 적합 주소로 잘못 인증하는 오류를 줄일 수 있었다. 실험 결과는 제안 방안이 기존 연구인 시간 기반 클러스터링과 밀도 기반 클러스터링을 활용한 주소 인증 방안들에 비해 주소 인증 오류율을 줄임을 보였다.

[참고문헌]

[1] Upal Mahbub and Rama Chellappa, PATH: Person Authentication Using Trace Histories. IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 2016.

[2] Yang Ye, Yu Zheng, Yukun Chen, Jianhua Feng, and Xing Xie, Mining Individual Life Pattern Based on Location History, International Conference on Mobile Data Management (MDM), Taipei, Taiwan, 2009

[3] Changqing Zhou, Dan Frankowski, Pamela Ludford, Shashi Shekhar, and Loren Terveen, Discovering Personally Meaningful Places: an Interactive Clustering Approach, ACM Trans. Information Systems, vol. 25, no. 3, pp. 12-es, 2007.

[4] Yu Zheng, Lizhu Zhang, Xing Xie, and Wei-Ying Ma, Mining Interesting Locations and Travel Sequences from GPS Trajectories, International conference on World wide web, Madrid, Spain, 2009.

[5] Aditi Gupta, Markus Miettinen, N. Asokan, and Marcin Nagy, Intuitive Security Policy Configuration in Mobile Devices Using Context Profiling, ASE/IEEE International Conference on Social Computing (SocialCom), Amsterdam, Netherlands, 2013.

[6] Jong Hee Kang, William Welbourne, Benjamin Stewart, and Gaetano Borriello, Extracting Places from Traces of Locations, ACM SIGMOBILE Mobile Computing and Communications Review, vol. 9, no. pp. 58-68, 2005.

[7] Quan Yuan, Gao Cong, Zongyang Ma, Aixin Sun, and Nadia Magnenat-Thalmann, Time-aware Point-of-interest Recommendation, International ACM conference on Research and development in information retrieval (SIGIR), Dublin, Ireland, 2013.

[8] Martin Ester, Hans-Peter Kriegel, Jiirg Sander, and Xiaowei Xu, A density-based algorithm for discovering clusters in large spatial databases with noise, International Conference on Knowledge Discovery and Data Mining (KDD), Portland, Oregon, USA, 1996.

부인방지 기능을 제공하는 이동형 전기자동차 충전기용 보안 에이전트 설계

장찬국, 이재훈, 이옥연*

*국민대학교 금융정보보안학과

Designed Security Agent for Portable EV Charger that Provides Non-Repudiation Function

Chan-Guk Jang, Jae-Hoon Lee, Okyeon Yi*

*Dept, of Financial Information Security, Kookmin University.

요 약

스마트그리드 핵심 도메인 중 하나인 전기자동차 충전 인프라의 빠른 구축을 위해서는 인프라의 보안요구사항을 만족하는 보안 설계가 요구된다. 하지만 전기자동차 충전 인프라에 대한 연구는 아직 많이 부족하며, 특히 보안 설계에 대한 연구는 부족한 상황이다. 따라서 본 논문에서는 사전 연구 및 관련 연구에서 도출된 요구사항을 만족하는 보안 에이전트를 설계하여 이동형 전기자동차 충전 인프라에 적용할 수 있도록 한다.

I. 서론

스마트그리드 핵심 도메인 중 하나인 전기자동차의 충전은 기존 아날로그 방식의 주유를 하는 자동차와는 달리, 모든 충전 정보 및 제어 명령이 유·무선 통신을 통해 충전 사업자와 전력 제공자에게 전달되는 시스템을 가진다. 이처럼 여러 ICT 기술을 이용하는 전기자동차 충전 인프라는 여러 연구를 통하여 보안요구사항들을 도출하고 보안 서비스를 제공하여 데이터 노출 및 위·변조 등의 보안 위협은 방지하고 있지만, 데이터 부인방지 기능은 제공하지 않고 있다. 이에 본 논문에서는 전기자동차 충전 방식 중 이동형 전기자동차 충전 방식에서의 부인방지 기능을 제공하는 보안 에이전트에 대해 제안하고 설명하고자 한다. 본 논문의 구성은 총 4장으로 구성된다. 1장은 서론으로 간략한 연구 내용 및 구성을 서술하고 2장에서는 관련 연구에 관해 서술한다. 3장에서는 본 논문의 주된 내용인 부인방지 기능을 제공하는 이동형 전기자동차 충전기용 보안 에이전트를 설명하고 마지막 4장에서는 본 논문의 결론을 맺고 논문을 마친다.

II. 관련 연구

이동형 전기자동차 충전기용 보안 에이전트에서 부인방지 기능에 대한 이야기를 하기에 앞서, 이와 관련된 연구에 대해 정리한다.

먼저 스마트그리드 관련 국내 법규에 관해 설명한 후 이동형 전기자동차 충전 인프라의 보안 설계에 관한 기존 연구에 대해 설명하고자 한다.

2.1 관련 법규

대한민국은 스마트그리드에 관련된 법규로 '지능형전력망의 구축 및 이용촉진에 관한 법률'과 '지능형 전력망 정보의 보호조치에 관한 지침'[1]이 존재한다. 서론에서도 언급하였지만, 전

기자동차 충전 인프라는 스마트그리드의 핵심 도메인 중 하나이므로 본 법규를 만족하여야 한다. '지능형 전력망 정보의 보호조치에 관한 지침' 중 제 7조, 제 8조, 제 10조, 제11조, 제 12조, 제 13조는 정보보호 및 암호에 관련된 조항이다, 제 7조는 무선통신망 보안에 관한 내용이며 3항에서는 지능형전력망 사업자가 무선통신망을 운용할 경우 무선통신 내용을 암호화하여야 한다고 명시되어 있다. 제 8조에서는 지능형전력망의 시스템을 보호하기 위하여 지능형 전력망 통신망에 정보보호시스템을 설치·운용하여야 하고, 정보보호시스템 평가·인증 지침 및 공통평가기준에 의해 인증받은 제품이나 국가정보원장이 그와 동등한 효력이 있다고 인정한 제품이어야 한다고 명시되어 있다. 제 10조에서는 지능형전력망 시스템에서 사용되는 암호모듈은 국가사이버안전센터 IT보안인증사무국의 검증필 암호모듈을 사용하고, 암호알고리즘 보안 강도가 128 비트 이상이어야 한다고 명시되어 있다. 제 11조에서는 지능형전력망 시스템에서 사용되는 암호키의 생성 및 발급, 암호키의 주기적 갱신, 암호키 파기 등을 포함하는 암호키 관리 정책을 수립·시행하여야 한다고 명시되어 있다. 제 12조에서는 지능형전력망 시스템은 중간자공격, 스니핑 공격을 차단하기 위해 상호인증을 수행해야 하는 것을 명시하고 있다. 또한 지능형전력망 기기가 다른 기기 또는 지능형전력망 시스템과의 통신 시 상호인증한 상대방에 대해서만 통신을 허용하여야 한다고 명시되어 있다. 마지막 제 13조에서는 지능형전력망 기기에서 과금과 관련된 통신에 대해서는 부인방지 기능이 제공되어야 한다고 되어있다.

2.2 전기자동차 충전 인프라 보안 연구

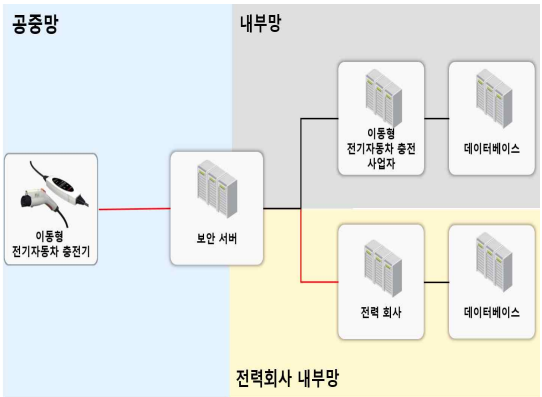
전기자동차 충전 인프라에서의 보안 연구는 크게 두 가지 연구 형태로 나뉜다.

첫 번째 연구는 전기자동차 충전 인프라의 보안요구사항에 관한 연구이다. [2]에서는 전기자동차 충전 인프라의 안전한 구축을 위해 전기자동차 충전 인프라에 대한 논리적 아키텍처를 제시하고 각 인터페이스를 식별하여 해당 인터페이스에서 발생 가능한 보안위협을 식별하였다. 또한, 이러한 보안 위협에 대응하기 위한 보안요구사항을 분석 및 제시하였다. [3]에서는 보안위협모델링을 시행하여 보안 위협을 식별하고 보안 요구사항을 보다 체계적으로 분석하였으며, 여러 위협모델링을 이용하여 발생 가능한 위협을 정확히 식별하고 그에 따른 보안요구사항을 도출하였다.

두 번째 연구 방향은 실제 전기자동차 충전 인프라의 보안 설계에 관한 연구이다. 본 연구는 이전 보안요구사항에 관한 연구를 바탕으로 실제 전기자동차 충전 인프라에 보안 서비스를 적용하는 연구로 [4]에서는 [2]에서 도출하였던 보안요구사항을 실제 LTE 이동통신을 이용하는 이동형 전기자동차 충전 인프라에 적용하고 이동형 전기자동차 충전 인프라의 특징에 맞는 암호화 방법을 제시하였다. 또한, 실제 보안 서비스가 제공되어야 하는 LTE 모뎀에서의 성능 분석 또한 진행되었다.

2.3 기존 이동형 전기자동차 충전기용 보안 에이전트

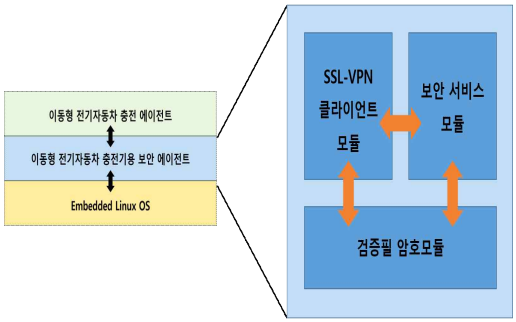
[5]에서는 보안 서비스를 적용한 이동형 전기자동차 충전 인프라를 제안하였고, 해당 보안 서비스를 제공하기 위해 이동형 전기자동차 충전기용 보안 에이전트와 서버용 보안 에이전트 총 두 가지의 보안 에이전트를 제안하였다.



[그림 1] 기존 보안 서비스를 제공하는 이동형 전기자동차 충전 인프라 구성도

그중 이동형 전기자동차 충전기용 보안 에이전트는 이동형 전기자동차 충전기 내 이동통신 모뎀 내에서 작동하며 보안 서버 내의 보안 에

이전트와 통신하여 이동형 전기자동차 충전기가 송·수신하는 모든 데이터에 대해 기밀성과 무결성을 제공하고, 상호 인증 및 키 일치 기능을 수행한다.

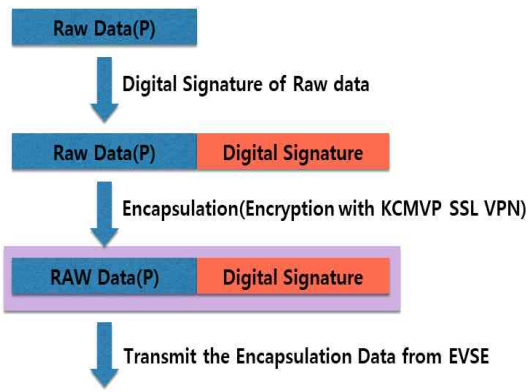


[그림 2] 기존 이동형 전기자동차 충전기용 보안 에이전트 구성도

하지만, 해당 보안 에이전트는 2.1절에서 언급한 부인방지 기능을 제공하지 못한다. 따라서 본 논문에서는 기존 이동형 전기자동차 충전 인프라용 보안 에이전트에 부인방지 기능을 추가하고자 한다.

III. 본문

3.1 부인방지 기능을 제공하는 이동형 전기자동차 충전기용 보안 에이전트



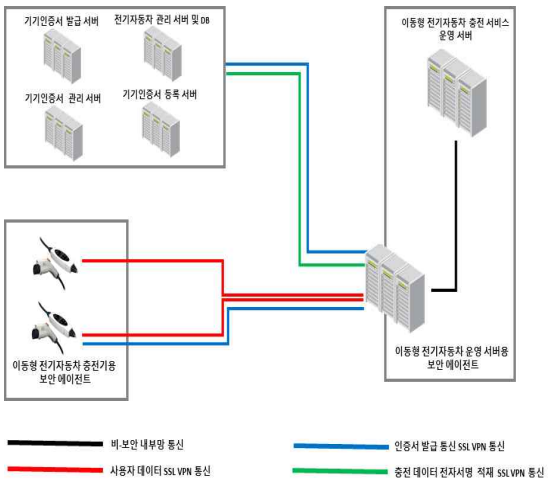
[그림 3] 부인방지 기능을 적용한 이동형 전기자동차 충전기 데이터 흐름

새롭게 이동형 전기자동차 충전기용 보안 에이전트에서 제공하는 부인방지 기능은 2.1절에서 언급하였듯이 지능형전력망 기기에서 과금과 관련된 통신에 대해서는 반드시 제공해야 하는 기능이다. 그리고 해당 부인방지 기능은 반드시 검증필 암호모듈을 사용하여 제공하여야 한다. [5]에서 제안한 기존 이동형 전기자동차 충전기용 보안 에이전트는 SSL-VPN 클라이언트 모듈, 검증필 암호모듈, 보안 서비스 모듈로 구성되고 이동형 충전기에서 발생한 데이터는 해당 보안 에이전트를 거쳐 이동통신을 통해 외부 운영 서버로 전송된다. 데이터가 이동형 전기자동차 충전기용 보안 에이전트에 입력되면 보안 서비스 모듈은 검증필 암호모듈에서 제공하는 ECDSA p-256을 이용해 전자서명을 생성한다. 그 후 전자서명이 부착된 데이터는 SSL-VPN 클라이언트 모듈을 통해 서버용 보안 에이전트로 전송된다. 안전한 통신을 위해 제공되는 전자서명을 생성하는 기능과 암호화 기능이 전체 통신 및 서비스에 영향을 주게 된다면 이는 보안 서비스의 가용성을 해치는 기능이기 때문에 서비스 제공을 고려해야 한다. [5]에서 진행한 실험 중 임베디드 리눅스 장비인 LTE 이동통신 모뎀에서 검증필 암호모듈 KMULiB v2.0을 이용한 ECDSA p-256 전자서명 생성 시간을 살펴보면 전자서명 생성 시 걸리는 시간은 약 0.8초 소요된다. 실험을 진행한 이동형 전기자동차 충전 인프라에서 데이터가 전송되는 주기는 1분당 1회 전송된다. 따라서 원본 데이터에 대한 전자서명 생성 후 암호화 과정을 처리하는 데까지 걸리는 시간은 1초 미만이 소요된다. 이를 통해 전자서명 생성을 통해 부인방지 기능을 제공하는 것은 전체 서비스에 큰 영향을 미치지 않는다는 것을 확인할 수 있다.

3.2 제안하는 이동형 전기자동차 충전 인프라

이동형 전기자동차 충전기용 보안 에이전트에서 전자서명을 생성하기 위해서는 모든 이동형 전기자동차 충전기에 개인키가 있어야 하고 개인키와 쌍을 이루는 기기 인증서(공개키)가 포함되어 있어야 한다. 해당 기기 인증서는 이동형 전기자동차 충전기용 보안 에이전트와 서버용 보안 에이전트와의 상호 인증 시에도 사용된다. 그리고 추후 전자서명을 검증할 개체인

한국전력공사 또한 해당 이동형 전기자동차 충전기의 기기 인증서를 갖고 있어 해당 기기의 공개키를 알고 있어야 한다. 따라서 본 부인방지 기능과 상호 인증 시 사용되는 기기 인증서는 한국전력공사에서 제공하는 PKI 시스템에서 발급받아 사용되어야 한다.



[그림 4] 제안하는 이동형 전기자동차 충전 인프라 구성도

제안하는 이동형 전기자동차 충전 인프라의 모든 공중망 통신은 검증필 암호모듈을 사용한 SSL VPN 통신을 제안한다. 검증필 암호모듈을 사용한 SSL VPN은 [1]에서 요구하는 법적 요구사항을 모두 만족할 뿐만 아니라, [2], [3]에서 분석한 보안 요구사항들도 만족할 수 있다. 또한 국가 및 공공기관에서 정보보안 제품을 사용할 경우 CC 인증을 받은 제품을 사용해야 하므로 제안하는 이동형 전기자동차 충전 인프라에서 사용하는 SSL VPN은 CC 인증을 받아야 한다.[6],[7]

IV. 결론

스마트그리드 핵심 도메인 중 하나인 전기자동차 충전 인프라에 대한 보안은 국내·외에서 다양하게 연구되고 있다. 이에 본 논문에서는 국내 이동형 전기자동차 충전 인프라에서의 법적 요구사항을 만족하고, 나아가 실제 서비스되고 있는 이동형 전기자동차 충전 인프라에 적용해 보았다. 여러 모듈로 구성된 제안하는 보안 에이전트는 각각의 기능을 수행하며 보안 서비스를 제공하면서도 기존 충전 서비스에는 영향을 끼치지 않아야 한다. 현재 대한민국에서는 여러 혜택들을 통해 전기자동차 보급에 힘쓰고 있다. 전기자동차 보급의 가장 핵심적인 요소는 인프라 구축이며 인프라 구축에서도 가장 중요한 점은 보안 설계이다. 본 논문에서 제안한 보안 에이전트 및 인프라 구성도를 시작으로, 많은 연구 및 실증을 통해 하루 빨리 전기자동차 충전 인프라에 보안이 적용되는 계기가 되었으면 한다.

향후 연구 계획은 본 논문에서 언급하지 않은 현재 연구되고 있는 스마트그리드와의 융합과 특히 스마트그리드의 핵심요소가 될 스마트그리드용 PKI 시스템에 대해 연구할 계획이다.

[참고문헌]

[1] “지능형전력망 정보의 보호조치에 관한 지침”[시행 2012.6.20.][지식경제부고시 제2012-129호, 2012.6.20., 제정]

[2] 강성구, 서정택, “전기자동차 충전 인프라에서의 보안 위협 및 보안 요구사항 분석”, 정보보호학회논문지, 22(5), pp. 1027-1037, 2012년 10월

[3] 차예슬, 김승주, “위협모델링을 이용한 전기차 충전 인프라의 보안요구사항에 대한 연구”, 정보보호학회논문지, 27(6), pp. 1441-1455, 2017년 12월

[4] 장찬국, 이재훈, 이옥연, “Encryption scheme In Portable Electric Vehicle Charging Infrastructure”, Computer Applications and Information Processing Technology(CAIPT) 2017 4th Internation Conference on, 2017년 08월

[5] 장찬국, “이동형 전기자동차 충전 인프라 내의 보안 설계 및 구현”, 국민대학교 일반대학원 금융정보보안학과 석사학위 논문, 2017

[6] “국가정보화기본법”[시행 2017.7.26. 법률 제14839호, 2017.7.26., 타법개정] 제 38조

[7] “국가정보화기본법 시행령”[시행 2018.1.25.
대통령령 제28597호, 2018.1.23., 일부개정]
제 35조