

IP 카메라 취약점 진단 시스템

(IP Camera Vulnerability Assessment System)

팀 명	SentriX
지도교수	유승재 교수님
팀 원	전 성 배 (팀장) 김 수 연 송 채 연 이 동 하 송 재 혁

2025. 11. 4

중부대학교 미래융합공학부 정보보호학전공

목 차

1. 서론
 - 1.1 연구 배경
 - 1.2 연구 목적 및 주제선정
2. 관련 연구
 - 2.1 IoT 및 스마트홈 보안 위협 동향
 - 2.2 IP 카메라 보안 취약점 연구
 - 2.3 IoT 보안 사고 사례 분석
 - 2.4 기존 보안 진단 연구의 한계
 - 2.5 본 연구의 차별성
3. 본론
 - 3.1 시스템 개요
 - 3.2 전체 구성도
 - 3.3 주요 기능 구성
 - 3.4 프로그램 구현
 - 3.4.1 스캐너 모듈 구현
 - 3.4.2 취약점 진단 흐름
 - 3.4.3 보고서 생성
 - 3.5 개발 환경
4. 결론
 - 4.1 결론
 - 4.2 기대 효과
5. 참고 자료
6. 별첨
 - 6.1 소개자료(폼보드)
 - 6.2 프로젝트 소개
 - 6.3 팀원 소개
 - 6.4 발표자료

1. 서론

1.1 연구 배경

사물인터넷(IoT) 기술의 발전은 TV, 냉장고, 로봇청소기, 도어록, 홈캠 등 다양한 스마트홈 기기의 보급을 가속화하며 가정의 편의성을 크게 높였다. 반면, 이러한 기기의 확산은 개인정보·사생활 영상의 유출, 원격 제어를 통한 물리적 침해, DDoS와 같은 네트워크 공격 등 새로운 보안 위협을 초래하고 있다. 특히 IP 카메라(홈캠)는 불법 촬영·영상 유출 사례가 반복적으로 보도되며 사용자 불안을 증폭시키고 있으며, 스마트 도어록이나 가전제품의 취약점은 곧바로 물리적 피해로 연결될 위험이 있다. 기존 정보보호 가이드라인은 주로 개발단계의 보안 설계(secure-by-design)에 초점을 맞추고 있으나, 출시 이후 운영 중인 기기를 대상으로 한 실시간 취약점 진단과 신속한 대응 체계는 아직 부족하다. 또한 많은 상용 보안 도구는 전문가 중심으로 설계되어 일반 사용자가 설치·운영하기 어렵고, RTSP·ONVIF 같은 임베디드 기기 특유의 프로토콜이나 펌웨어 기반 취약점까지 포괄적으로 점검하지 못하는 한계가 있다. 이처럼 공급 후에도 0-day 취약점이나 기본 계정·약한 비밀번호 등으로 인한 공격이 계속 발생하는 현실을 고려할 때, 사용 편의성과 접근성을 동시에 갖춘 사용자가 직접 실행 가능한 운영 단계의 점검 수단이 요구된다.

1.2 연구 목적 및 주제선정

본 연구는 스마트홈 환경에서 광범위하게 활용되는 IP 카메라를 대상으로, 사용자가 손쉽게 실행할 수 있는 로컬 중심의 취약점 진단 도구를 설계·구현하여 실무에서 즉시 활용 가능한 보안 점검 체계를 제안하는 것을 목적으로 한다. 기존 연구와 도구들은 제조 단계의 보안 설계나 네트워크 인프라 보호에 치중되거나, 클라우드·전문가 중심의 자동화 솔루션에 의존하는 경향이 있다. 그러나 실제 운영 환경에서는 사용자 스스로 주기적으로 또는 필요시 직접 점검을 수행할 필요가 있으며, 기본 계정 방치나 펌웨어 미업데이트 등 단순한 설정 문제도 심각한 공격으로 이어질 수 있다. 따라서 전문가가 아니더라도 즉시 실행 가능한 실용적 진단 도구의 필요성이 크다.

이에 본 연구는 다음과 같은 세부 목적을 갖는다.

첫째, 별도 복잡한 설치 절차 없이 웹 UI 또는 로컬 환경에서 실행하여 로컬 네트워크 내 IP 카메라를 직접 검사할 수 있는 진단 도구를 구현한다. 사용자는 도구에 대상 장비의 IP를 입력하고 스캔을 수행함으로써 보안 점검의 접근성과 통제성을 확보할 수 있다.

둘째, RTSP·ONVIF 등 IP 카메라 고유 프로토콜 분석과 펌웨어·CVE 매칭 기법을 통합한 진단 엔진을 도입하여, 단순 포트 스캔을 넘어 실제 공격 가능성이 높은 취약점을 정밀 검출한다. 이는 임베디드 장치 특유의 취약성(기본 계정, 익명 RTSP 접근, 구버전 펌웨어 등)을 현실적으로 식별하는 데 중점을 둔다.

셋째, 진단 결과는 내부 취약점 정의 및 보안 가이드라인과 연계하여 CVSS 4.0 기반의 정량적 위험도로 산출하고, 사용자가 이해하기 쉬운 형태의 PDF 보고서로 즉시 출력할 수 있도록 하여 결과의 실무적 활용성을 높인다.

또한 서버 운영 및 결과 처리는 OpenStack 기반의 서버 환경에서 수행되어 진단 데이터의 안정적 처리와 보고서 생성을 지원하도록 구성하였다.

주제 선정 이유는 다음과 같다.

스마트홈 환경은 급격히 보급되고 있으며 그 중심에는 홈캠, 도어락, IoT 센서 등 네트워크에 연결된 다양한 스마트 기기가 존재한다. 그러나 이들 기기는 기능성에 비해 보안 설정이 미흡한 경우가 많고, 기본 계정 유지나 펌웨어 미업데이트와 같은 단순한 관리 소홀로도 심각한 보안 사고가 발생할 수 있다. 특히 IP 카메라는 사생활 영상 유출과 직접적으로 연결되는 장비이기 때문에 보안의 중요성이 매우 크지만, 일반 사용자가 손쉽게 점검할 수 있는 보안 도구는 부족한 실정이다.

또한 현재 제공되는 많은 보안 진단 도구는 전문가 중심으로 설계되어 설치가 복잡하거나 사용 과정이 어렵고, 임베디드 장치 특유의 RTSP·ONVIF 프로토콜 기반 취약점을 제대로 분석하지 못한다는 한계가 있다. 이러한 문제를 해결하기 위해 본 프로젝트는 사용자가 직접 보안 점검을 수행할 수 있는 실용적인 도구 개발을 목표로 하였으며, 높은 활용성·보안 실습 가능성·기술적 확장성이라는 측면에서 개발 주제로서 충분한 의의가 있다고 판단하였다.

2. 관련연구

2.1 IoT 및 스마트홈 보안 위협 동향

사물인터넷(IoT)은 스마트홈, 스마트팩토리, 스마트시티 등 다양한 분야에서 활용되며 일상생활 속에 빠르게 확산되고 있다. 특히 홈 네트워크 환경에서는 IP 카메라, 스마트 도어락, 스마트 TV, 음성 스피커 등 다양한 IoT 기기들이 네트워크에 연결되어 운영된다. 그러나 이러한 편의성의 확산과 함께 IoT 기기를 악용한 보안 공격 역시 증가하고 있어 심각한 보안 문제가 지속적으로 제기되고 있다.

IoT 기기는 설계 단계에서 보안보다 기능성과 상호 연결성 위주로 개발되는 경우가 많고, 메모리·CPU·전력 등 하드웨어 자원이 제한적이기 때문에 일반적인 PC나 서버 수준의 보안 체계를 적용하기 어렵다. 한국인터넷진흥원(KISA) 보고서 등에서도 IoT 보안 위협은 디바이스 단계에서 더 빈번하게 발생하며, 네트워크를 통해 대규모 확산 위험을 동반한다고 지적하고 있다. 이러한 보안 위협은 단순한 정보 유출을 넘어 실제 물리적 피해로 이어질 수 있다는 점에서 더 높은 수준의 보안 대응이 요구된다.

대표적인 사례로 Mirai 계열의 대규모 DDoS 공격이 있으며, 해당 공격은 보안 설정이 미흡한 IoT 기기들을 감염시켜 봇넷을 구성한 후 사이버 공격에 악용하였다. 또한, 외부에서 접근 가능한 RTSP/HTTP 포트를 통해 IP 카메라 영상이 무단으로 수집·유통된 사례도 보고되었다. 이러한 사례들은 IoT 기기가 네트워크에 연결된 순간 공격 대상이 될 수 있음을 보여주며, 보안이 고려되지 않은 IoT 환경은 사용자 프라이버시와 안전에 심각한 위협이 될 수 있음을 시사한다.

2.2 IP 카메라 보안 취약점 연구

IP 카메라는 영상 수집·전송이라는 특성상 프라이버시·무단 접근 리스크가 특히 큰 장치로 분류된다. 경량화된 하드웨어와 단순한 펌웨어 구조 때문에 인증·암호화가 취약한 경우가 많고, 출고 상태의 기본 계정 그대로 방치되거나 약한 비밀번호를 사용하는 사례가 반복적으로 보고되고 있다. 실험 기반 연구에서는 Shodan과 같은 검색 엔진을 통해 외부에 노출된 IP 카메라를 손쉽게 식별할 수 있으며, 익명 RTSP 접근이나 기본 계정 탈취를 통해 영상 탈취·서비스 거부(DoS) 등이 현실적으로 가능성이 확인되었다.

또한 IP 카메라의 펌웨어에는 제조사·모델별로 다양한 취약점이 존재하며, 펌웨어 버전 관리 미비로 알려진 CVE가 오랫동안 방치되는 경우가 많다. 이에 따라 펌웨어 기반 취약점이 실제 공격으로 이어지는 사례가 보고되었고, 펌웨어 분석을 통한 취약점 탐지 및 CVE 매칭 기법이 연구의 핵심 방법론으로 자리 잡았다.

학술적·정책적 관점에서도 IP 카메라를 포함한 스마트홈 디바이스의 보안성 확보 필요성이 지속적으로 제기되어 왔다. 제도적 개선과 제품 출시 전 보안 요건 강화가 필요하다는 점은 여러 연구에서 공통으로 권고되고 있으며, 특히 사용자 친화적 고지·동의의 체계와 제조사 수준의 보안 설계(secure-by-design)가 강조되고 있다.

2.3 IoT 보안 사고 사례 분석

실제 사고 사례는 이론적 위험을 현실로 확인해 주며, IP 카메라 및 스마트홈 기기의 취

악성이 얼마나 심각한지 보여준다. 대표적인 사례들은 다음과 같다.

- Mirai 계열 봇넷 및 대규모 DDoS 악용: Mirai 악성코드는 기본 계정·약한 비밀번호를 남겨둔 IoT 기기를 대량으로 감염시켜 봇넷을 구성하고, 이를 통해 대형 DDoS 공격을 수행하였다. 이 사건은 제조사·사용자·서비스 제공자 모두의 보안 책임이 결합되지 않으면 대규모 시스템 피해로 이어질 수 있음을 시사한다.
- 공개 노출 카메라 및 영상 유출: 외부에서 접근 가능한 RTSP/HTTP 포트를 통해 IP 카메라의 영상이 무단으로 수집·유통된 사례가 반복 보고되었다. 연구에서는 Shodan 등을 이용한 노출 탐색과 익명 접근을 통해 실시간 영상이 탈취 가능한 현실을 실증하였다.
- 스마트홈 생태계의 개인정보 위험: 대형 제조사 중심으로 AI스마트홈 생태계가 확장되며 방대한 생활 데이터가 수집·활용되고 있다. 이 과정에서 불충분한 고지·동의, 데이터 유통과정의 불투명성이 문제로 지적되었고, 관련 기사와 보고서는 개인정보 보호법·제도 정비의 시급함을 강조한다.
- 월패드·가정용 기기 해킹 등: 국내에서도 아파트 월패드·홈캠 등 가정 내 장비가 해킹되어 사용자 프라이버시가 침해되거나 서비스가 마비되는 사례가 보고되었고, 이는 제도적·기술적 대응의 필요성을 환기시켰다.

2.4 기존 보안 진단 연구의 한계

선행 연구와 상용 솔루션은 IP 카메라·IoT 취약점 탐지에 유의미한 기여를 해왔지만, 실제 운영 환경(특히 일반 사용자 환경)에서 적용하기에는 몇 가지 반복되는 한계가 있다.

첫째, 다수의 상용 도구와 연구는 전문가 중심으로 설계되어 설치·운용이 복잡하고, 사용자 접근성이 낮다.

둘째, 많은 점검은 단순 포트 스캔이나 네트워크 레벨의 탐지에 치중하여 RTSP·ONVIF 같은 임베디드 장치 고유 프로토콜과 펌웨어 기반 취약점을 충분히 다루지 못한다.

셋째, 펌웨어 분석·CVE 매칭을 수행하더라도 펌웨어 버전 수집의 어려움과 매칭의 자동화 한계로 인해 실무 적용이 번거롭고 누락이 발생하기 쉽다.

넷째, 보고서·결과 표현 측면에서 일관된 위험도 산정과 사용자 친화적 설명을 동시에 제공하는 도구가 적다.

다섯째, 개인정보·프라이버시 측면의 정책·법적 고려를 통합적으로 반영하는 연구는 상대적으로 부족하다.

이러한 한계들은 기술적 탐지 성능뿐 아니라 실제 사용자가 운영환경에서 즉시 활용 가능한 ‘실용성’ 부족으로 귀결된다.

2.5 본 연구의 차별성

본 연구는 위의 한계들을 실무 적용 관점에서 보완하는 데 초점을 맞춘다. 구체적으로는 다음과 같은 차별성을 가진다.

1. 사용자가 별도 소프트웨어 설치·다운로드 없이 웹 UI에서 접근하여 점검을 수행할 수 있도록 설계한다. 이는 사용자가 별도의 파일을 내려받거나 설치하지 않아도 되는 방식을 의미하며, 접근성 및 배포 편의성을 높인다.
2. ONVIF 호출을 통한 장비 식별과 RTSP 스트림 접근성 확인을 기본 워크플로우에 포함하여 임베디드 장치 특유의 검사 항목을 기본으로 채택한다.
3. 펌웨어 버전 수집 → 내부 취약점 사전·CVE 매칭 → CVSS 4.0 기반 위험도 산정의

엔드투엔드 자동화 파이프라인을 구현함으로써 펌웨어 기반 누락을 줄이고 결과의 우선 순위를 명확히 한다.

4. 결과는 비전문가도 이해하기 쉬운 형태의 표준화된 PDF 보고서로 자동 생성하여, 현장 대응(비밀번호 변경, 펌웨어 업데이트 등)에 즉시 활용 가능하도록 설계하였다.

5. 제도적·정책적 권고사항을 보고서 내 권고 섹션에 통합하여 기술·관리적 대응을 함께 제시한다.

3. 본론

3.1 시스템 개요

이 프로젝트는 로컬 네트워크 환경에서 사용자가 직접 IP 카메라의 보안 상태를 점검할 수 있도록 설계된 보안 진단 도구이다. 시스템은 웹 UI 또는 로컬 실행 파일 형태로 제공되며, 사용자는 대상 장비의 IP 주소와 인증 정보를 입력하여 진단을 수행할 수 있다. 진단 과정에서는 ONVIF를 이용한 장비 정보 수집, RTSP 스트림 접근성 확인, 기본 계정 여부 및 약한 인증 탐지, 취약 포트 점검, 펌웨어 버전 분석과 공개 취약점(CVE) 조회 등이 수행된다. 분석된 결과는 내부 취약점 사진과 매핑되어 CVSS 4.0 기준으로 위험도가 산정되며, 표준 형식의 PDF 보고서로 출력된다. 이러한 시스템 구조는 별도의 설치나 고급 보안 지식 없이도 누구나 기초적인 IoT 보안 점검을 수행할 수 있도록 설계되었다.

3.2 전체 구성도

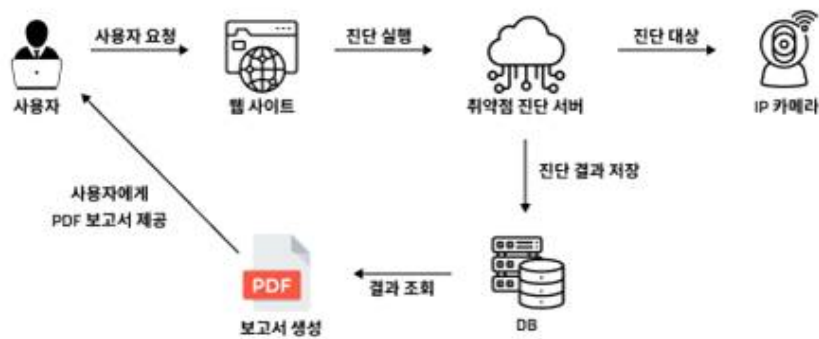


그림 1. 시스템 전체 구성도

사용자는 UI에서 스캔을 시작하고 결과를 화면으로 확인하거나 보고서로 저장할 수 있다. 시스템은 모든 민감 데이터를 로컬에 보관하고 불필요할 시 즉시 삭제하도록 설계 되었다.

3.3 주요 기능 구성

시스템의 주요 기능은 다음과 같다.

1. 장비 식별(ONVIF): ONVIF 호출을 통해 제조사, 모델명, 펌웨어 버전 및 RTSP 스트림 URI를 수집하고 이후 검사에 활용한다.
2. 스트림 접근성 확인(RTSP): 인증 없이 스트림에 접근 가능한지 검사하고 접근 허용 시 썸네일 이미지를 캡처하여 증거로 보관한다.
3. 웹 인증 점검: 관리용 웹 페이지에 대해 널리 알려진 기본 계정·약한 비밀번호로 로그인 시도를 수행하여 인증 취약성을 판별한다.
4. 서비스·포트 점검: Telnet(23), FTP(21) 등 보안상 취약한 레거시 포트의 개방 여부를 검사하고 보안 권고를 제시한다.
5. 펌웨어·CVE 연동: 수집된 펌웨어 버전을 내부 최신 목록과 비교하고, 장비 모델명을

기반으로 공개 취약점(CVE) 데이터베이스를 조회하여 알려진 취약점 존재 여부를 확인한다.

6. 결과 표준화·위험도 산정: 발견 항목을 내부 취약점 사전과 매핑한 뒤 CVSS 4.0 규칙에 따라 점수를 부여하고 우선 순위화한다.

3.4 프로그램 구현

2.4.1 스캐너 모듈 구현

스캐너는 모듈화되어 각 기능을 독립적으로 수행하도록 설계되었다. 주요 모듈은 다음과 같다.

- onvif_scanner: ONVIF 프로토콜을 통해 device 정보와 스트림 URI를 수집한다.
- rtsp_scanner: 확보한 RTSP 주소로 ffmpeg를 호출하여 스트림을 캡처하고 익명 접근 여부를 검증한다.
- web_scanner: HTTP 포트 접근 및 기본 자격 증명 시도를 통해 웹 인증 취약성을 탐지한다.
- port_scanner: 비동기 방식으로 Telnet/FTP 등 위험 포트의 연결 가능성을 검사한다.
- firmware_checker/cve_scanner: 펌웨어 버전 비교와 CVE 데이터 조회를 수행하여 알려진 취약점을 탐지한다.

각 모듈은 표준화된 결과 포맷을 반환하여 중앙 처리 모듈이 취합·정리할 수 있도록 구현되었다.

3.4.2 취약점 진단 흐름

진단은 다음 순서로 진행된다. 먼저 onvif_scanner로 장비 정보를 확보하고, 확보된 스트림 정보는 rtsp_scanner와 web_scanner의 입력으로 사용된다. 이후 port_scanner, firmware_checker, cve_scanner가 병렬로 실행되어 각자의 검사를 수행한다. 모든 개별 검사 결과는 중앙 처리 모듈에서 통합되며, _normalize_and_guidelines 단계에서 내부 취약점 정의 및 보안 가이드라인과 매핑된다. 마지막으로 apply_cvss_policy_bulk를 통해 CVSS 점수가 부여되고 최종 보고서 데이터가 생성된다.

3.4.3 보고서 생성

취합된 결과는 pdf_report.py에 의해 표 형식의 평가표와 상세 진단 내용, 썸네일 등을 포함한 PDF 문서로 생성된다. 보고서에는 각 취약점 항목에 대한 설명·영향·권고사항이 명시되며, CVSS 점수와 심각도 등급이 함께 표기된다.

3.5 개발 환경

개발 언어는 Python을 사용하였으며, 간단한 웹 UI는 FastAPI와 순수 JavaScript/HTML로 구현하였다. RTSP 캡처는 FFmpeg를 이용하였고, 취약점 매핑과 점수 계산은 vulnerability_definitions.py, security_guidelines.py, policy.py, calculator.py를 중심으로 동작하며, PDF 생성은 reportlab 기반으로 처리된다. 개인정보 보호를 위해 캡처된 썸네일과 로그는 로컬에만 저장하고, 필요시 즉시 삭제하는 정

책을 적용하였다.

4. 결론

4.1 결론

본 프로젝트는 IP 카메라 환경을 대상으로 한 실질적인 보안 진단 도구를 구현함으로써 일반 사용자도 운영 단계에서 직접 보안 점검을 수행할 수 있는 방법을 제시하였다. 모듈형 스캐너 구조를 적용하여 ONVIF·RTSP·HTTP 기반의 정보 수집과 인증 취약점 검증, 취약 포트 탐지, 펌웨어 및 공개 취약점 분석을 효율적으로 처리할 수 있도록 하였으며, 진단 결과는 CVSS 4.0 기반으로 정량화하여 취약점의 우선순위를 명확히 제시하였다. 또한 PDF 보고서 자동 생성 기능은 결과 활용도를 높여 실무 환경뿐 아니라 교육·훈련 환경에서도 활용 가능성을 확보하였다.

이 시스템은 사용자가 자신의 홈 네트워크에서 발생할 수 있는 보안 위협을 직접 확인하고 대응할 수 있게 함으로써 IoT 보안 인식을 높이고 예방 중심의 보안 관리 문화를 확산하는 데 기여할 수 있다. 아울러 프로젝트 구조가 확장 가능하게 설계되어 있어, 향후 다른 IoT 기기(스마트 도어락, NAS, 홈 허브 등)로 대상 범위를 넓히는 것이 가능하며, 커뮤니티 기반 오픈소스 보안 프로젝트로 확장할 잠재력도 갖추고 있다.

4.2 기대 효과

본 시스템은 홈 네트워크 환경에서 IP 카메라의 보안 상태를 주기적으로 점검할 수 있는 실용적인 셀프 보안 진단 도구로 활용될 수 있다. 사용자는 장비의 보안 취약점을 직접 확인함으로써 보안 위협을 인지하고, 기본 비밀번호 변경이나 펌웨어 업데이트와 같은 사전 대응을 수행하여 영상 유출 등의 보안 사고를 예방할 수 있다. 또한 OpenStack 기반 서버 환경을 활용하여 진단 결과를 안정적으로 처리하고 보고서를 제공함으로써 실사용 중심의 구조적 완성도를 확보하였다. 시스템은 모듈형 구조로 설계되어 향후 다양한 IoT 기기 보안 점검 기능을 추가하거나 확장할 수 있는 가능성을 갖추고 있으며, 실제 네트워크 환경에서 적용 가능한 보안 도구로 활용될 수 있다.

5. 참고 자료

- (1) 최성규, “IoT 장치의 취약점 분석절차 및 점검항목 도출,” 아주대학교 정보통신대학원 석사학위논문, 2020.
- (2) 이기택, “사물 인터넷 스마트 기기의 취약점 분석 및 보안성 측정 방법에 관한 연구,” 고려대학교 정보보호대학원 박사학위논문, 2021.
- (3) 한국인터넷진흥원(KISA), “홈가전 IoT 보안가이드,” 2017.
- (4) 한국인터넷진흥원(KISA), “IoT 공통보안가이드,” 2016.
- (5) 조이든·박수진·강남희, “사물인터넷의 경량 IP 카메라 취약점을 이용한 해킹 공격 및 대응 방안,” Journal of Digital Contents Society, 2019. (업로드 파일)
- (6) 이동혁·박남제, “IoT 기기의 보안성 확보를 위한 제도적 개선방안,” 제주대학교(보고서/학술자료), 2017. (업로드 파일)
- (7) 이애리·손수민·김현진·김범수, “사물인터넷(IoT) 환경에서 개인정보보호 강화를 위한 제도 개선 방안,” 연세대학교(보고서/학술자료), 2016. (업로드 파일)
- (8) “삼성과 LG ‘AI 스마트홈’ 생태계 급팽창, 개인정보보호법 손질 시급한 과제로,” BusinessPost(보도자료/기사), 2024.07.09. (업로드 파일)
- (9) KISA, “[KISA Insight 2022 Vol.05] 지능형 IoT 사회의 보안이슈 분석,” 2022. (업로드 파일)
- (10) “사물인터넷 기반의 스마트홈” (학술/개요 자료), (업로드 파일, 연도 미상)
- (11) “(해외)사례2” (사례집/보고서), (업로드 파일, 연도 미상)
- (12) “과학기술정보통신” (보도자료/정책자료), (업로드 파일, 연도 미상)
- (13) “KCI_FI002277032.pdf” (학술 자료), (업로드 파일, 연도 미상)
- (14) “사물인터넷(IoT) 관련 사이버범죄 동향 및 형사법적 규제” (법·범죄 관점 논문), 2015. (업로드 파일)

6. 별첨

6.1 소개자료(폼보드)

SENTRIX
⚙️

IP 카메라 취약점 진단 시스템

팀장 - 전성배 | 팀원 - 김수연, 송재혁, 송채연, 이동하

개요

본 시스템은 일반 사용자가 자신의 IP 카메라와 스마트홈 기기의 보안 상태를 직관적으로 확인할 수 있도록 고안된 웹 기반 진단 도구다.
 기기 연결 정보와 설정을 바탕으로 IoT 특화 취약점을 자동으로 검사하고, 발견된 취약점에 대해 이해하기 쉬운 설명과 단계별 권고안을 제시하여 사용자가 스스로 보안 수준을 개선할 수 있도록 돕는다.

구상도

결과보고서

기대효과

일반 사용자가 자신의 IoT 기기 보안 위협을 직접 확인하여 기본 계정 등 취약점을 사전에 발견·조치하게 함으로써 영상 유출 등 심각한 사고를 예방하고, OpenStack 기반의 웹 서비스로 복잡한 보안 기능을 실용적으로 제공하는 모델을 제시하여 관련 연구와 실무에 기여한다.

2025 정보보호학과 졸업작품 전시회 @SENTRIX

6.2 소스 코드

<https://github.com/thdcodussongchaeyeon/Graduation-work>

6.3 팀원 소개

SentriX는 팀장 전성배를 포함하여 김수연, 송채연, 이동하, 송재혁으로 구성되어 있다. 팀장 전성배는 프로젝트 총괄을 맡았으며, 김수연은 서버 제작을 담당하였다. 송채연은 펌웨어 점검을 수정하였고, 이동하는 포트 점검을 맡았다. 송재혁은 스크립트 작성을 담당하였다.

6.4 발표자료