IoT 디바이스 펌웨어 취약점 분석

팀원 : 2013104053 김동준

2013104129 한선우

2016110312 송미희

2014104110 신기성

# 개요

여러 소프트웨어 취약점 분석 방법론을 통해 IoT 디바이스 펌웨어의 취약점을 분석한다.

# 서론

## 연구 배경

한국스마트홈산업협회에 따르면 2017년 국내 스마트 홈 시장 규모가 10조원을 돌파한 것으로 나타났다.[1] 이렇듯 스마트 홈을 포함한 IoT 디바이스는 빠른 속도로 늘어나고 있고, 여러 분야에 널리 보급되고 있다. IoT 디바이스는 항상 인터넷에 연결되고 다양한 기기들과 융합되어 있기에 다양한 형태의 보안 문제들을 야기할 수 있다. 이러한 환경에서 ICT 보안 문제들이 선행 연구들에서 논의되었고 그에 대한 기술적∙제도적∙정책적 대응책들이 제언되었다. 하지만 이런 선행연구들은 전반적인 소프트웨어 보안에 관한 연구들이기 때문에 IoT 디바이스가 가진 보안 취약점을 해결하는 데 한계가 있다. 또한, IoT 디바이스는 보급 초기 단계이기 때문에 보안 취약점을 더 가지고 있을 것이라고 예상했다. 그렇기 때문에 IoT 디바이스를 집중적으로 분석해보기로 했다.

## 연구 목표

기존의 소프트웨어 취약점 분석 방법론은 주로 IoT 디바이스가 아닌 개인 PC나 서버 상의 소프트웨어를 대상으로 적용되고 있다. 따라서 이 연구의 목표는 소프트웨어 취약점 분석 방법론을 IoT 디바이스에 적용해보고, 만약 발견된 취약점이 있다면 그것을 분류해서 다른 IoT 디바이스 보안 연구에 밑바탕이 되는 분석 자료를 만드는 것이다.

# 기존 연구

## 기존 연구 1

소프트웨어 테스트 자동화를 위한 오픈소스 취약점 분석 도구들이 많이 소개되어 있으며, 이러한 도구들은 프로세스화 되었을 때 큰 효과를 볼 수 있기 때문에, 오픈 소스 취약점 도구에 대한 도입 시 조직적이고 장기적인 측면에서 고려해야 하며, 활용 가능한 주요 오픈소스 분석 도구에 대한 조사 결과, 큰 틀은 다음과 같다.[2]

소스코드에 대한 코딩 표준/스타일, 복잡도 및 잔존 결함을 발견하기 위하여 사용하는 정적분석 도구, 프로그램을 실행하여 코드 내에 존재하는 메모리 누수, 쓰레드 결함 등을 분석하기 위하여 사용하는 동적분석 도구가 있으며, 단위 테스트, 통합 테스트 등 테스트 단계별 자동화 도구를 활용한 기능 테스트 도구가 있다. 마지막으로 가상 사용자를 인위적으로 생성하여 시스템의 처리량, 응답시간을 테스트하기 위한 성능 테스트 도구 서버 자원에 대한 사용 현황을 파악할 수 있는 시스템 모니터링 도구가 있다.

## 기존 연구 2

## 오픈 소스코드를 기반으로 무작위로 생성한 데이터와 같이 유효하지 않거나 예상치 않은 데이터를 입력하여, 고의적으로 프로그램의 충돌이나 메모리 누수와 같은 예상치 못한 동작을 일으켜 잠재적인 보안 취약점을 탐지하는 퍼징 테스트 기법이 현재 많이 사용되는 분석 도구이며, 기호 값을 사용하여 테스트를 수행하고 기호를 활용한 기호 실행 엔진은 입력 값에 상수 값 대신에 기호 값을 할당하여 진행함으로써 분기를 만나면 모든 분기에 대하여 제한을 설정하게 하는 방법이다. 이러한 기호실행 또한 많이 사용되는 방법 분석 도구 중 하나이다.[3]

## 기존 연구의 문제점

오픈소스 소프트웨어를 대상으로 취약점 탐지를 수행, 분석하였을 때 특정 오픈소스에 대한 주요 오픈소스 분석 도구를 적용시 한계점이 나타났으며, 기존 연구는 소프트웨어 중심의 취약점 분석 연구이므로 IOT디바이스 중심의 오픈소스 취약점 분석 적용 시 취약점 분석 도구에 대해 한계점이 존재하며, 취약점 패턴에 대한 적절한 분석 도구의 활용이 필요할 것이라 생각된다.

# 프로젝트

## 기존 연구와의 차이점 및 해결방안 기존 연구는 소프트웨어 중심으로 연구가 이루어졌다. 그러나 변화하는 시장에 맞춰 IoT 제품들이 많이 나오고 있는 반면에 디바이스 펌웨어 취약점에 대한 논의는 충분히 이루어지지 않았다고 판단되었다. IoT디바이스는 PC, 서버, 스마트폰 등과는 다르게 특수한 목적을 가지고 설계되는 경우가 훨씬 많으므로, 공격자가 해당 기기의 목적을 파악한다면 정보탈취, 기기 오작동을 통한 고의손실을 일으키기가 쉬우므로 취약점 문제가 더욱 대두될 수 있다. 그래서 우리는 IoT 디바이스에 초점을 맞춰 취약점을 분석해보기로 했다. 대상을 IoT 디바이스라는 구체적인 범위를 한정지었다는 점에서 기존 연구와의 차이점이 존재한다. 취약점 분석 방법으로는 이전 연구와 마찬가지로 크게 아래 4가지 주제를 가지고 분석할 예정이다. 퍼징을 통한 취약점 분석 기호실행을 통한 취약점 분석 패킷 분석을 통한 프로토콜 안정성 검증 소스코드 취약점 분석 이 외에도 여건이 된다면 IoT 보안을 서비스/네트워크/펌웨어/소프트웨어/암호화저장의 분야로 나눈 후 각 분야별 취약점 분석을 해 볼 것이다.

## 프로젝트 내용 퍼징은 테스팅을 위한 입력을 무작위로 발생시키고 그 취약점을 분석하는 방법이다. 우리는 해당 방법을 통해 디바이스 내 광범위한 취약점 분석을 실시한다. 기호실행 방식은 퍼징의 커버리지 한계를 극복한 방법이다. 시스템 분기에서 발생할 수 있는 취약점에 대해 테스팅 파일을 작성하여 취약점 분석을 실시한다. 패킷 분석은 디바이스간 통신에 사용되는 프로토콜에서 이동하는 패킷들의 내용이 외부유출이 가능한지에 대해 취약점 분석을 실시한다. 또한 소스코드가 공개된 부분에 대하여 취약점 소스코드 샘플을 수집하여 이전 코드와 해시값이 달라지는 경우 해당 부분에 문제가 생기는지 확인을 하는 방식으로 취약점 분석을 할 예정이다. 위와 같은 분석들을 통해 코드상 취약점을 중점적으로 분석 할 예정이며 더 많은 방법론적 연구를 통해 각 3.A.의 마지막 단락에 쓰여진 부분을 분석 해 볼 예정이다.

# 진행 일정

|  |  |  |
| --- | --- | --- |
| 진행 주차 | 담당 | 내용 |
| ~3 | 전원 | 오픈소스 취약점 사례 분석 및 분류 |
| 4~5 | 전원 | 취약점 분석 방법론에 대한 조사 및 연구 |
| 6 | 전원 | 분석 디바이스와 프로그램 선정 |
| 7~10 | 김동준 | 기호 실행 방법을 통한 취약점 분석 |
| 7~10 | 한선우 | 발생되는 패킷에 대한 보안 취약점 분석 |
| 7~10 | 송미희 | 퍼징을 통한 소프트웨어 취약점 분석 |
| 7~10 | 신기성 | 하드코딩, 데이터 성분 분석 등 소스 코드 내 취약점 분석 |
| 11~13 | 전원 | 분석 결과 취합 및 상관관계 연구 |
| 14 | 전원 | 취약점 관리방안 연구 |
| 15 | 전원 | 발표 및 최종 보고서 작성 |

# 결론

비교적 보안에 취약할 것으로 예상되는 IoT 디바이스에 대한 보안 취약점을 분석해볼 것이다. 기존 소프트웨어에 적용되던 보안 취약점 방법론 및 도구들을 활용해 IoT 디바이스의 펌웨어를 분석해 봄으로써 IoT 디바이스 보안에 대한 이해도를 높일 수 있다. 또한, 본 연구의 결과를 토대로 새롭게 발전하는 IoT 분야에서 보안과 관련된 부족한 후속 연구가 이루어져 IoT 보안에 대한 수준이 향상되기를 기대한다.

# 참고 문헌

1. 권건호, “지난해 국내 스마트홈 시장규모 10조 돌파…2019년엔 21조로 성장”, 『전자신문』, 2016년 2월 8일.
2. 김병국, "오픈 소스의 소프트웨어 보안 문제 및 시큐어 코딩 적용방안." 『*정보과학회 컴퓨팅의 실제 논문지*』 23.8 (2017): 487-91.
3. 오상환, 김태은, and 김환국. "SW 보안 취약점 자동 탐색 및 대응 기술 분석." 『*한국산학기술학회 논문지*』 18.11 (2017): 94-103.