**캡스톤 디자인 II**

**종합설계 프로젝트**

|  |  |
| --- | --- |
| 프로젝트 명 | *SOSfinder* |
| 팀 명 | *SOFA* |
| 문서 제목 | 수행계획서 |

|  |  |
| --- | --- |
| **Version** | 0.3 |
| **Date** | 2017.10.10 |

|  |  |
| --- | --- |
| **팀원** | 차진원 (조장) |
| 강지형 |
| 남혜인 |
| 박민경 |

|  |
| --- |
| **CONFIDENTIALITY/SECURITY WARNING**  이 문서에 포함되어 있는 정보는 국민대학교 전자정보통신대학 컴퓨터공학부 및 컴퓨터공학부 개설 교과목 캡스톤 디자인II 수강 학생 중 프로젝트 “SOSfinder”를 수행하는 팀 “SOFA”의 팀원들의 자산입니다. 국민대학교 컴퓨터공학부 및 팀 “SOFA”의 팀원들의 서면 허락없이 사용되거나, 재가공 될 수 없습니다. |

**문서 정보 / 수정 내역**

|  |  |
| --- | --- |
| **Filename** | 수행계획서-SOSfinder.doc |
| **원안작성자** | 남혜인 |
| **수정작업자** | 남혜인, 박민경 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 수정날짜 | 대표수정자 | Revision | 추가/수정 항목 | 내 용 |
| 2017-9-11 | 남혜인 | 0.1 | 최초 작성 | 전체 문서 항목 작성 |
| 2017-10-7 | 남혜인 | 0.2 | 수정 | 목표, 요구사항, 코드리뷰결과 수정 |
| 2017-10-10 | 박민경 | 0.3 | 전체 수정 | 전체 문서 항목 수정 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**목 차**

[1 개요 4](#_Toc495413311)

[1.1 프로젝트 개요 4](#_Toc495413312)

[1.2 추진 배경 및 필요성 5](#_Toc495413313)

[1.2.1 IoT 기기 사용 증가에 따른 보안 위협 증가 5](#_Toc495413314)

[1.2.2 IoT 기기의 소스코드 공개여부 8](#_Toc495413315)

[2 개발 목표 및 내용 9](#_Toc495413316)

[2.1 목표 9](#_Toc495413317)

[2.1.1 시스템 기능 요구사항 10](#_Toc495413318)

[2.1.2 시스템 비기능(품질) 요구사항 11](#_Toc495413319)

[2.2 코드 리뷰 결과 12](#_Toc495413320)

[3 프로젝트 팀 구성 및 역할 분담 14](#_Toc495413321)

[4 참고 문헌 15](#_Toc495413322)

# 개요

## 프로젝트 개요

최근 IoT(Internet of Things, 사물인터넷) 기기의 확산이 진행되면서, IoT 기기를 대상으로 하는 악성 공격들이 이루어지고 있다. 하지만 IoT 기기는 취약 부분에 대한 점검과 보수보다는 기능적인 추가를 더욱 우선시하여 발전하고 있는 추세이다. 앞으로 점점 더 많은 기기가 공격의 대상이 될 수 있으며 각각의 IoT 기기가 취약점을 가지는지에 대한 파악이 중요하다.

본 프로젝트에서는 최근 취약점이 알려진 오픈소스의 특정 소스코드 모듈을 다양한 플랫폼을 대상으로 컴파일하여 바이너리 코드 레벨의 시그니처 집합을 생성함으로써, ‘사용자의 IoT(Internet of Things, 사물인터넷) 기기의 취약점 포함 여부를 파악할 수 있는 서비스’를 구현한다. 여기서 사용자는 ‘Power User’로서, IoT 기기의 펌웨어를 이용하는 보안기관이나 IoT 소프트웨어의 개발자를 의미한다. 본 프로젝트에서 제공하는 기능은 아래와 같다.

첫째, IoT 기기 내부의 오픈소스 취약점 점검 기술이다. 사용자에게 자신의 IoT 기기에 있는 소프트웨어를 업로드하게 하여 해당 기기가 가진 취약점을 점검한다.

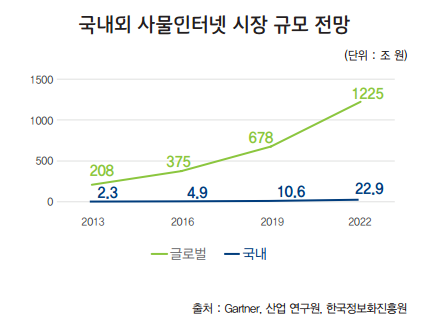
둘째, 취약점 정보 업로드 기술이다. 서비스를 제공하지 않는 소프트웨어 또는 최근에 발표된 취약점을 가진 소프트웨어를 사용자로부터 업로드 할 수 있게 하여, 사용자의 참여로 취약점 데이터베이스의 시그니처를 확장한다.

## 추진 배경 및 필요성

### IoT 기기 사용 증가에 따른 보안 위협 증가

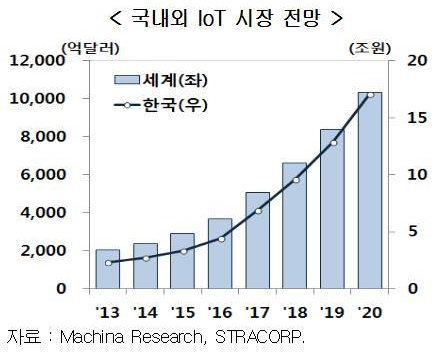
빠른 ICT(Information Communication Technology, 정보통신기술)의 발전으로 인해, 전 세계는 인터넷을 통해 서로 소통하는 환경에서 살고 있다. 아날로그 및 전자 기계 장치의 사용에서 디지털 기술로 넘어오는 제 3차 산업 혁명을 넘어서 현시대는 초연결성, 초지능성에 의한 생산성 향상을 기대하는 제4차 산업 혁명을 맞이하고 있다. 제 4차 산업 혁명은 ICT의 융합으로 이룬 혁명 시대를 의미하며 로봇 공학, 인공 지능, 나노 기술, 생명 공학, 사물인터넷, 자율 차량 등을 포함한 여러 분야에서 새로운 기술 혁신을 기대하고 있다. 본 프로젝트는 IoT(Internet of Things, 사물인터넷)를 통한 세계의 발전에 초점을 맞추고 있다.

IoT는 다양한 사물이 각기 부착된 통신장치와 센서를 통해 네트워크에 연결되고 정보를 공유할 수 있는 기술이다. 또한 가트너(Gartner)가 선정하는 10대 전략기술에 2012년부터 매년 내면 선정되어 ICT시장의 산업을 이끄는 핵심 부가가치 산업으로 급부상하고 있다. 이러한 기술을 활용하여 실생활영역에 적용되면서 다양한 경제적 가치와 더불어 효율성 및 편의성이 한층 높아질 것으로 기대되고 있다. 국내외 사물인터넷 시장은 많이 증가할 것으로 보인다.



[그림 1] 국내외 사물인터넷 시장 규모 전망

또한 현대경제연구원이 발표한 ‘사물인터넷(IoT) 관련 유망산업 동향 및 시사점’ 보고서에 따르면 세계 IoT 시장은 2015년 약 3천억 달러에서 2020년 1조 달러로 연평균 28.8% 성장할 것이고, 국내 IoT 시장은 연평균 38.5% 성장할 것이라는 전망이 나왔다. 같은 기간 국내 IoT 시장 규모도 3조3천억원에서 17조1천억원으로 연평균 38.5% 성장할 것으로 예상됐다.



[그림 2] 국내외 IoT 시장 전망, 한국경제연구원

하지만 빠른 속도로 발전하는 IoT 기기에 대한 보안 위협 사례가 발표되면서, IoT 기기의 보안 문제는 아주 중요한 문제가 되었다. IoT의 확산에 따라 해킹이 더욱 쉬워지게 되었고, 네트워크 인프라가 점점 더 넓어짐에 따라 해킹할 수 있는 환경이 넓어지게 되었다. 2015년에 진행한 한 기사의 설문조사에 의하면 그 해의 가장 큰 보안 위협은 ‘IoT(사물인터넷) 기기의 보안위협’ 이라고 응답한 사람이 가장 많다고 한다.[[1]](#footnote-1)

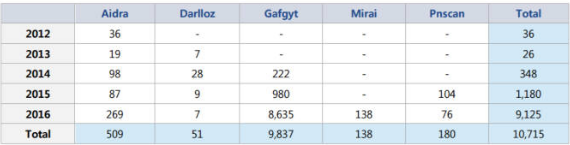


[그림 3] 보안뉴스 기사의 설문조사

Akamai 위협 연구팀은 최근 인터넷에 연결된 수백만 대의 사물인터넷(IoT) 기기가 웹 기반 자격 증명 스터핑 공격의 소스로 사용되는 사례를 보고했다. 이러한 문제점은 이전에도 보고된 바 있으나, 수정되지 않고 IoT 기기에 적용되었다. 이 기기들은 Dyn이라 불리는 DNS 호스트에 DDoS 공격을 가하여 큰 문제를 발생시켰다.

사물인터넷 기기의 보안 위협은 리눅스 운영체제와 밀접한 연관이 있다. IoT 기기에 탑재되는 운영체제는 주로 임베디드 리눅스이며 리눅스는 오픈소스 소프트웨어이다. 따라서 IoT 업체들은 개발에 용이한 리눅스 운영체제와 오픈소스 소프트웨어를 많이 사용한다. IoT에서 제공하는 여러 어플리케이션 레벨의 소프트웨어들 역시 오픈소스를 활용한 소프트웨어인 경우가 다수이다. 오픈소스 소프트웨어는 다양한 개발자들의 참여로 코드 품질이 매우 높지만 생산 속도가 빠르고 많은 오픈소스를 생산하는 만큼 많은 취약점을 보유 및 패치한다. 만약 특정 IoT 기기가 보안에 취약한 오픈소스 소프트웨어를 포함한다면 IoT 기기 역시 취약점을 가지고 있기 때문에 보안위협에 영향을 끼칠 것이다. 그 밖에도 IoT 서비스는 기술 자체 혹은 구현 방법의 문제점으로 인해 다양한 취약점이 존재할 수 있다. 안랩(AhnLab)에 따르면 2008년 리눅스 악성코드가 처음 보고된 후 2016년 10월 기준으로 1만개를 넘어섰다고 한다. 이것은 특정 기기만 감염시키는 악성코드와 지속해서 변형이 나오지 않는 것을 제외한 수치이다.

[2] 보안뉴스 [설문조사] 올해 가장 큰 보안위협은 ‘사물인터넷’



[그림 4] 안랩이 공개한 주요 리눅스 악성코드 발견 현황

이처럼 IoT 기기를 노리는 악성코드는 급증하지만 대응은 쉽지 않은 것이 현실이다. IoT 기기는 상당수 보안을 고려하지 않고 설계되었다. 안전한 IoT 사용을 위해서, 기기 제조사가 보안을 강화한 펌웨어를 업데이트하고, 사용자는 지정되어 있는 초기 비밀번호를 바꿔야 한다. 보편적 사용자는 사용하는 기기가 위험에 유출되어 있는지에 대한 인식이 부족하고 기기가 보유한 취약성에 대해 바로 알 수 없다. 따라서 본 프로젝트는 IoT 기기에 들어있는 취약한 소프트웨어를 진단해주는 웹 서비스를 설계하고자 한다.[[2]](#footnote-2)

### IoT 기기의 소스코드 공개여부

최근에 IoT 보안이 주목을 받으면서 이와 관련한 프로젝트들이 활성화 되었다. 하지만 관련 프로젝트들은 소스코드를 기반으로 검사하여 취약한 IoT 기기를 찾는 형태이다. 바이너리 코드 기반으로 검사를 하는 경우는, 주석에 달려있는 정보를 가지고 오픈소스의 존재 유무를 따져 라이선스 문제에 대한 대책으로 나와있는 상황이다. 이러한 경우 소스코드에 대한 지식이 있는 개발자만이 주로 사용하여, 프로그램 또는 제품에 라이선스로 인한 문제를 피해갈 수 있게 한다.

그러나 중요한 것은 소비자들이 주로 사용하는 IoT 기기의 소스코드 공개는 대부분 이루어지지 않는다. 또 오픈소스 라이선스의 문제로 인한 소스코드의 공개에도 부분적 공개나, 사용 출처를 표시하는 것으로 그치는 경우도 많다. 만약 제품의 전체 소스코드가 공개되어도 컴퓨터의 프로그래밍 언어를 공부하지 않은 일반 사용자의 경우에는 소스코드가 일반적인 문자에 지나지 않은 의미를 가진다. 이처럼 소스코드는 제한적으로 공개되기도 하지만 공개가 되어도 일반 사용자는 소스코드를 이용한 검사를 함에 어려움이 있다.

따라서 일반적인 사용자에게는 ‘실행 파일만 가지고 자신이 소유하고 있는 IoT 기기가 취약한지 한눈에 알려주는 서비스’가 필요하다.

# 개발 목표 및 내용

## 목표

1학기 캡스톤 디자인 수업을 통해 서비스의 개발을 완료하였다. 본 프로젝트는 사용자의 IoT 기기의 펌웨어에 대해 소스코드가 존재하지 않는 환경에서 바이너리 코드를 분석 비교하여, 취약점을 가진 오픈소스 코드가 사용되었는지 확인하고 진단 결과를 보여주는 웹 서비스이다.

따라서 이번 2학기 캡스톤 디자인 수업의 목표는 1학기에 진행한 기존 프로젝트를 구조적으로 보완하는 것과 코드 클린화를 진행하는 것이다. 이를 위해 첫째로, 사용자의 IoT 기기에 대한 정확한 분석을 위해 분석 모듈의 알고리즘을 수정한다. 기존의 사용했던 방식이 아닌, 슬라이딩 윈도우 방식을 기준을 두고 진행하여 정확하고 빠른 알고리즘을 목표로 한다.

둘째로, 서비스를 제공하는 웹 사이트의 데이터베이스 환경을 수정한다. DB Pool 기능을 적용하여, 다수의 사용자가 서비스를 사용할 때 효율적인 데이터베이스의 사용을 목표로 한다.

### 시스템 기능 요구사항

|  |  |  |
| --- | --- | --- |
| **프로그램 유형** | **IoT보안 웹 서비스** | **진행상황** |
| **요구사항** | Database 연결을 효율적으로 관리하기 위해 Database Connection Pool을 적용한다. |  |

|  |  |  |
| --- | --- | --- |
| **프로그램 유형** | **취약점 점검 알고리즘 모듈** | **진행상황** |
| **요구사항** | 1. 코드 리팩토링을 진행한다.  - 중복코드줄이기  - 토큰함수의 조건문 줄이기  2. 정확도 향상을 위해 알고리즘을 수정한다.  - Exacting Window를 기준으로 하여 비교 횟수를 최소화 한 ‘슬라이딩 윈도우 방식’을 적용하기  3. 모듈의 효율성 향상을 위해 Database 구조를 수정한다.  - 기존의 한 가지 테이블로 구성된 것을 취약점 테이블과 플랫폼 테이블로 구분하기 |  |

### 시스템 비기능(품질) 요구사항

|  |  |  |
| --- | --- | --- |
| **요구사항** | **내용** | **진행상황** |
| **정확성** | IoT 기기의 취약점 점검 모듈의 알고리즘을 수정함으로써, 정확하고 빠른 점검을 제공하며 서비스의 정확성을 높인다. |  |
| **효율성** | 웹 서비스의 Database 환경을 수정함으로써, 효율적인 DB 연결로 효율성을 높인다. |  |

# 프로젝트 팀 구성 및 역할 분담

| 이름 | 역할 |
| --- | --- |
| 강지형 | 서버 구성 및 웹 서비스의 Database 수정 |
| 남혜인 | 서버 구성 및 웹 서비스의 Database 수정 |
| 박민경 | 취약점 점검 모듈의 알고리즘 및 Database 수정 |
| 차진원 | 취약점 점검 모듈의 알고리즘 및 Database 수정 |

# 참고 문헌

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 번호 | 종류 | 제목 | 출처 | 발행년도 | 저자 |
| 1 | 깃허브 | https://github.com/jimmyda/SOSfinder |  | 2017.9 |  |
| 2 | 깃허브 | https://github.com/chunksong/SOSfinder |  | 2017.3 |  |
| 3 | 기사 | <http://www.yonhapnews.co.kr/bulletin/2016/07/12/0200000000AKR20160712109300002.HTML> | 연합뉴스 | 2016.7 | 박의래기자 |
| 4 | 기사 | <http://www.boannews.com/media/view.asp?idx=45510> | 보안뉴스 | 2015.3 | 김태형기자 |
| 5 | 논문 | Winnowing: Local Algorithms for Document Fingerprinting | SIGMOD | 2003.12 | Saul Schleimer,  Daniel S. Wilkerson,  Alex Aiken |

1. [1] 연합뉴스 "한국 사물인터넷시장, 2020년 17조…연평균 38% 성장 전망" [↑](#footnote-ref-1)
2. [↑](#footnote-ref-2)