**캡스톤 디자인 II**

**종합설계 프로젝트**

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

|  |  |
| --- | --- |
| **Version** | 1.0 |
| **Date** | 2017.09.11 |

|  |  |
| --- | --- |
| **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** | 전체 |
| **수정작업자** | 남혜인 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 수정날짜 | 대표수정자 | Revision | 추가/수정 항목 | 내 용 |
| 2017-9-11 | 남혜인 | 1.0 | 최초 작성 | 전체항목 작성 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**본 양식은 컴퓨터공학부 캡스톤 디자인 II 과목의 프로젝트 수행 계획서 작성을 위한 기본 양식입니다. 문서의 필수 항목을 제시하는 것이니 폰트, 문단 구조 등의 디자인 부분은 자유롭게 설정하기 바랍니다. 양식 내에 붉은 색으로 기술한 부분은 지우고 작성하기 바랍니다.**

**목 차**

[1 개요 (1학기 내용을 간략하게 요약 1/2페이지 이내, 2학기 진행내용 1/2페이지) 4](#_Toc483417162)

[1.1 프로젝트 개요 4](#_Toc483417163)

[1.2 추진 배경 및 필요성 5](#_Toc483417164)

[1.2.1 IoT 기기 사용 증가에 따른 보안 위협 증가 5](#_Toc483417165)

[1.2.2 IoT 기기의 소스코드 공개여부 8](#_Toc483417166)

[**2** **개발 목표 및 내용** 5](#_Toc492373539)

[2.1 목표 5](#_Toc492373540)

[2.2 코드 리뷰 결과 5](#_Toc492373541)

[**3** **프로젝트 팀 구성 및 역할 분담** 6](#_Toc492373542)

[**4** **참고 문헌** 6](#_Toc492373543)

# **개요 (1학기 내용을 간략하게 요약 1/2페이지 이내, 2학기 진행내용 1/2페이지)**

## 프로젝트 개요

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.

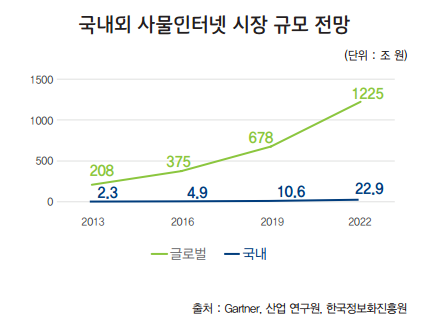
이 프로젝트의 보완할 사항으로 모듈 코드 리팩토링과 웹페이지 UI코드 리팩토링을 할 예정이며,이 프로젝트를 사용할 때의 서비스 튜토리얼을 추가하여 사용자가 보다 쉽게 이를 이용할 수 있도록 하며, 로그인 암호화 기능을 추가할 예정이다.

## 추진 배경 및 필요성

### IoT 기기 사용 증가에 따른 보안 위협 증가

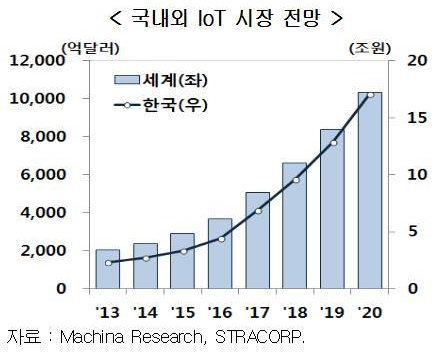
빠른 ICT(Information Communication Technology, 정보통신기술)의 발전으로 인해, 전 세계는 인터넷을 통해 서로 소통하는 환경에서 살고 있다. 아날로그 및 전자 기계 장치의 사용에서 디지털 기술로 넘어오는 제 3차 산업 혁명을 넘어서 현시대는 초연결성, 초지능성에 의한 생산성 향상을 기대하는 제4차 산업 혁명을 맞이하고 있다. 제 4차 산업 혁명은 ICT의 융합으로 이룬 혁명 시대를 의미하며 로봇 공학, 인공 지능, 나노 기술, 생명 공학, 사물인터넷, 자율 차량 등을 포함한 여러 분야에서 새로운 기술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

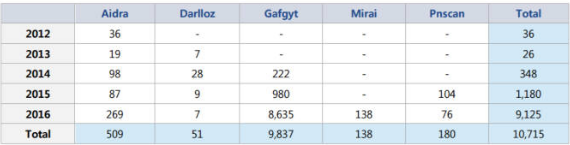


[그림 3] 보안뉴스 기사의 설문조사

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

**본 프로젝트의 수행 목표를 서술하는데, 이 항목 안에 추가 변경되는 기능/비기능 요구사항을 나열한다.(1페이지 이내)**

본 프로젝트의 목표는 사용자의 IoT 기기의 펌웨어에 대해 소스코드가 존재하지 않는 환경에서 바이너리 코드를 분석 비교하여 취약점을 가진 오픈소스 코드가 사용되었는지 확인하고 진단 결과를 보여주는 웹 서비스를 개발하는 것이다. 웹 서비스의 사용자는 ‘Power User’을 대상으로 한다. 여기서 ‘Power User’는 IoT 기기의 펌웨어를 이용하는 보안기관이나 IoT 소프트웨어의 개발자, 또는 IT분야에 대한 지식이 충분한 자를 의미한다. 개발 목표는 크게 다음 3가지이다.

첫째, 대부분의 사용자는 본인이 사용하는 전자 제품, 센서 등이 IoT 기기에 대해 보안 위험성에 대한 인식이 부족하다. “당신의 기기는 안전한가요?”라는 문구를 토대로 사용자들에게 스스로 기기의 보안 취약점을 자각할 수 있도록 도와주는 서비스를 개발한다.

둘째, 많은 IoT 기기 개발자들은 개발에 오픈소스 코드를 많이 이용하고 있다. 하지만 사용한 오픈소스에 대한 보안성을 확실하게 보장할 수 없고, 실제로 취약점이 계속해서 알려진 상황이다. 본 서비스는 개발자들이 개발 단계에서 이 서비스를 이용하여 안전성이 높은 개발을 할 수 있도록 오픈소스의 취약 정도를 쉽게 보여준다.

셋째, IoT 기기의 시스템 위에 모듈이 올려지는 방화벽과 같은 형태의 보안이 아닌, 웹 사이트에서 보안을 점검하는 형태의 보안 서비스를 개발한다. 웹 형태로 서비스를 제안하는 이유는 다음과 같다. 첫째, 사용자가 쉽게 서비스를 사용할 수 있으므로 접근성이 훌륭하기 때문이다. 둘째, 프로젝트의 확장이 용이하다는 웹의 특징 때문이다. 사용자로부터 취약한 펌웨어를 게시판에 업로드하게 함으로써 하나의 커뮤니티를 형성하는데, 이를 통해 다양한 환경의 펌웨어를 점검하는 모듈로 확장시킬 수 있다.

### 2.2.1 추가보완할 사항

기능 요구사항

-사용자는 웹사이트 접속 시 사이트 이용방법을 알 수 있어야 한다. 이를 위해 서비스 튜토리얼을 제공한다.

비기능 요구사항

* 보안 Security
* 사용자 편리성 Usability
* 신뢰성 및 효율성 Reliability & Efficiency
* 양도 가능성 Transferability
* 유지보수 편리성 Maintainability
* 호환성 Compatibility

-

## 코드 리뷰 결과

**코드 리뷰 후, 프로젝트에 대한 팀원들의 생각을 정리하고, 지적된 주요 항목들을 그룹핑하여 요약 정리한다. (1페이지 이내)**

1. CSS 모듈화하는 작업
2. 중간중간 중복되는 코드 정리
3. cpp파일의 토큰화하는 함수에서 배열을 사용하여 if문을 줄일 것
4. DB 쿼리문 사용 시, ‘\*’ 대신 명시적으로 사용할 것
5. DB쿼리문 정리하기
6. cpp파일의 DB 쿼리문 중,  ‘select \* from board where 1 order by ~’ 이 부분에서 where 다음에 오는 ‘1’은 삭제하기
7. DB Connection Pool 사용 고려하기

# **프로젝트 팀 구성 및 역할 분담**

**프로젝트에 참여하는 멤버의 역할을 구체적으로 명시한다.**

| 이름 | 역할 |
| --- | --- |
| 강지형 | - |
| 남혜인 |  |
| 박민경 | - |
| 차진워 | Cpp소스 수정 담당 |

# **참고 문헌**

**참고한 문서, 서적, 기사, 기술 문서, 웹페이지를 나열한다.**

* **Github repository 사이트 및 1학기 문서가 업로드 된 사이트 참조를 반드시 포함한다.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 번호 | 종류 | 제목 | 출처 | 발행년도 | 저자 | 기타 |
| 1 | 깃허브 | https://github.com/jimmyda/SOSfinder |  | 2017.9 |  |  |
| 2 | 깃허브 | 1학기 링크 |  | 2017.3 |  |  |

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