Journal of KIIT. Vol. 15, No. 12, pp. 17-27, Dec. 31, 2017. pISSN 1598-8619, eISSN 2093-7571 17
http://dx.doi.org/10.14801/jkiit.2017.15.12.17

# 사물인터넷(IoT) 보안 모델링에 대한 연구

전 용 희*

# A Study on the Security Modeling of Internet of Things(IoT)

Yong-Hee Jeon*

본 연구는 2014년 대구가톨릭대학교 연구년 중 수행한 것임.

## 요 약

사물인터넷(IoT)은 다양한 물리적 구성요소와 통신/네트워크 기술, 서비스 API 기술 그리고 사용자 인터페이스 기술과 같은 여러 가지 형태의 기술 요소들을 포함하기 때문에 사이버 보안이 본질적으로 취약하다. 본 논문에서는 IoT 환경에서 보안 취약점과 위협을 분석하고, 그에 대응하기 위한 보안 요구사항을 도출하기 위하여 보안 모델링을 수행하고 그 결과를 제시하고자 한다. 보안 모델링의 목적은 개발 시스템에 대한 보안 위협요소와 공격 가능성을 미리 분석하여 적절한 보안 통제를 위한 요구사항과 대응 기술을 도출하는데 있다. 따라서 사물인터넷 보안 위협요소를 STRIDE 모델링을 통하여 분석하고, 각 위협에 대한 공격 예제 분석을 통하여 공격 트리를 구축한다. 마지막으로 분석된 위협과 공격 예제를 기반으로, 그에 대응하기 위한 보안 요구사항과 기술을 분석하고 제안하며, 대표적 IoT 응용들에 대한 보안 요구사항을 제시한다.

## Abstract

The cyber security of Internet of Things(IoT) is inherently vulnerable since it includes diverse physical components and several types of technology elements such as communication/network technologies, service API technology, and user interface technology. This paper analyzes the security vulnerabilities and threats in IoT environments, and performs the security modeling and presents the results. The aim of security modeling is to derive the requirements and corresponding technology for security control of the system being developed by analyzing threat elements and attack possibility in advance. Accordingly this paper analyzes threat of each component for the IoT by STRIDE modeling and constructs attack trees by analyzing attack examples for every threats. Finally it proposes the security requirements and technology to respond against them, based on the analyzed threats and attack examples, and presents the security requirements for the typical applications for the IoT.

Keywords
IoT, vulnerability, threat, security modeling, security requirements

* 대구가톨릭대학교 IT공학부 교수
- ORCID: http://orcid.org/0000-0002-4880-2788

· Received: Nov. 01, 2017, Revised: Dec. 11, 2017, Accepted: Dec. 14, 2017
· Corresponding Author: Yong-Hee Jeon
The School of IT Engineering, College of Engineering, Daegu Catholic University, 13-13, Hayang-Ro, Hayang-eup, Gyeongsan-si,
Tel.: +82-53-850-2745, Email: yhjeon@cu.ac.kr

## Ⅰ. 서 론

정보 사회의 전역 하부구조로써, 기존과 새로이 생겨나는 통신 기술을 기반으로 하는 사물인터넷(IoT, Internet-of-Things)이 전개되고 있다. 그 결과로 우리는 소위 말하는 초-연결 사회(Hyper-connected Ssociety)로 진입하고 있다. ITU-T Y.2060은 다음과 같이 IoT를 정의하고 있다[1]. “이미 있거나 새로운 서로 동작이 가능한 정보 통신 기술을 기반으로 하는 (물리적 및 가상) 사물을 서로 연결하여 진보된 서비스를 가능하게 하는 정보 사회를 위한 전역 하부구조”. 이외에, 식별, 데이터 포획, 처리 및 통신 기능을 이용하여, IoT는 보안과 프라이버시 요구사항의 이행을 보증하는 한편, 모든 종류의 응용들에 대한 서비스를 제공하기 위하여 사물들을 완전하게 사용한다고 언급하고 있다. 여기서 IoT는 물리적 세계의 객체(실제 사물) 혹은 정보 세계의 객체(가상 사물)를 가리키며, 식별이 가능하고 통신망으로 통합 될 수 있다. 위의 정의에서 보여주는 것처럼, IoT는 지능적 센싱과 액츄에이션(Actuation) 기술을 가지고, 진보된 M2M(Machine-to-machine) 통신, 자동화된 네트워킹, 데이터 마이닝과 의사 결정, 보안과 프라이버시 보호, 그리고 클라우드 컴퓨팅과 같은 다양한 진보된 기술들을 통합하는 하나의 기술로 여겨질 수 있다.

[2]에서 제시하고 있는 IoT 응용 분야를 보면 소매(Retail), 주변 보조 생활, 헬스 케어, 스마트 에너지, 스마트 운송, 생산적 비즈니스 환경, 스마트 하우스, 스마트 시티, 그리고 물류 등과 같이 광범위하다. 이와 같이 IoT는 스마트 그리드 국가 전력망, 의료 및 건강 분야, 교육 및 교통 영역과 같은 여러 가지 형태의 응용들에 적용될 것이기 때문에, 이런 서비스들의 활성화를 위하여 다양하고 복잡한 보안 문제들이 해결되어야 한다. 위와 같은 IoT 서비스의 보안 시스템을 구축하기 위하여 IoT 환경에서 보안 위협들을 분석하고 위협 모델(Threat Model)을 확립하는 것은 필요한 과정이다. 확립된 보안 모델을 통하여, 공격 가능성을 분석하고, 그리고 보안 요구사항과 보안 공격에 대한 대응책이 제공되어야 한다. 그러나 국내에서는 아직 보안 모델링에 대하여 별로 연구가 진행된 바 없고, 참고 문헌도 없는 실정이다.

위와 같은 중요성과 필요성에 비추어, 본 논문에서는 IoT 환경에서의 보안 모델링을 수행하고자 한다[3]. 보안 모델은 주요한 보안 관점과 시스템 행위들의 관계를 정확히 기술한다. 식별된 상위-수준의 보안 목표로부터 유도되는 보안 요구사항들이 시스템 개발 과정의 초기 단계에서 제시되어야 한다. 핵심 보안 요구사항의 성공적인 구현을 위한 필요한 수준을 이해하기 위하여, 보안 모델을 확립할 필요가 있다.

본 논문에서는 보안 모델링의 부분으로 공격 트리 모델과 위협 모델링을 사용한다. 본 논문에서의 보안 모델링과정은 IoT 환경에서 대표적인 시스템 구성 식별, 취약점 및 위협 식별, 공격 트리 구축 및 분석을 통하여 공격 경로를 도출하고, 보안 위협 평가로 공격 가능성을 분석한다. 그리고 대응할 수 있는 보안 통제(Security Control) 및 완화(Mitigation) 메커니즘으로써 필요한 요구사항 및 대응 기술을 제시한다.

본 논문에서는 먼저, IoT 보안 특성과 공격면(Attack Surface)에 대한 분석을 통하여 IoT 보안의 취약점을 조사한다. 그리고 보안 모델링 절차에 대하여 제시한다. 그 다음에 보안 모델링을 위한 위협 식별, 공격 트리 구축 및 분석, 요구사항 및 대응 기술을 제시하고자 한다. 마지막으로 결론을 맺는다.

## Ⅱ. 관련 연구

### 2.1 IoT 보안 특성

IoT에서 사이버 보안은 IoT 장치들을 위한 가장 중요한 특성중의 하나임은 분명하다. IoT 장치들을 위한 보안의 필요성에 대한 많은 관심은 있지만, IoT 환경에서 보안을 어떻게 실행할지에 대한 논의는 상대적으로 적다고 할 수 있다. 다양한 형태의 IoT 장치들을 통하여 여러 가지의 보안 공격들이 발생할 수 있고, 악성코드가 주입될 수 있다. 그리하여 장치 소프트웨어 변경과 대규모 대역폭을 소비하는 분산 서비스거부(DDoS: Distributed Denial of Service) 공격이 유발될 수 있다.

IoT는 센서/장치, 게이트웨이와 같은 다양한 물리적 구성요소와, 통신/네트워크 기술 그리고 서비스 API 기술 및 사용자 인터페이스 기술과 같은 다양한 기술 요소들을 포함하고 있기 때문에, 보안 취약성이 증가된다. 각 IoT 구성요소에 특정한 보안 취약성 이외에, 여러 가지의 보안 취약성이 구성요소들의 연결 지점에도 또한 존재한다. 각 구성요소에 없는 취약성이, 연결로 인하여 새로운 보안 취약성이 유입될 수 있다. 또한 많은 상호작용을 위하여 사용되고 유포되는 연결 장치들의 수가 데이터 프라이버시, 데이터 보호, 안전, 거브넌스(Governance) 및 신뢰에 대한 중요한 문제를 만든다[4].

IoT 환경에서, 인간 통신이 기계에 의하여 중재되기 때문에, 가장(Impersonation), 신분 절도 및 해킹의 가능성을 가진 근본적인 보안 문제가 존재한다[5]. 또한 기존의 IT 시스템에 존재하는 웜과 바이러스, DoS와 DDoS, 패치 되지 않은 시스템, 방화벽과 앤티-바이러스 소프트웨어의 잘못 사용, 권한이 없는 서비스 접근, 프로토콜 보안 취약성, 권한이 없는 사용자 접근, 재연(Replay) 공격, 비합법적 I/O 접근, 부적합한 시스템 로그 기록, 구성 오류 및 실수, 기밀성/무결성 공격, 안전하지 않은 패스워드, 비보호 패스워드, 프라이버시 침해 같은 취약성이 IoT 환경에서도 여전히 가능하다[6].

## 2.2 IoT 공격 면(Attack Surface)

IoT 공격 면은 지역 혹은 전체 인터넷이든, 어떤 네트워크 안의 IoT 장치, 관련 소프트웨어와 하부구조에서 모든 잠재적 보안 취약성의 전체 영역으로 정의될 수 있다. Symantec은 IoT 공격면을 물리적 접속, 클라우드 폴링, 직접 연결, 클라우드 인프라 공격, 멀웨어 등으로 나눈다[4]. 한편 OWASP에 의하면, IoT 공격 면은 다음과 같이 주어진다[7]: 생태계 접근 제어, 장치 메모리, 장치 물리 인터페이스, 장치 웹 인터페이스, 장치 펌웨어, 장치 네크워크 서비스, 관리 인터페이스, 지역 데이터 저장, 클라우드 웹 인터페이스, 생태계 통신, 벤더 백-엔드 API, 제 3자 백-엔드 API, 갱신 메커니즘, 모바일 웹, 그리고 네트워크 트래픽. 표 1은 OWASP 공격 면 별로 잠재적 공격 경로를 보여준다.

표 1. OWASP 공격 면에 대한 잠정적 공격 경로
Table 1. Potential attack path to the OWASP attack surface

| Attack Surface | Potential Attack Path |
|---|---|
| Ecosystem Access Control | trust exploitation attack, access control system attack |
| Device Memory | password attack, credentials-based attack, encryption key attack |
| Device Physical Interfaces | firmware extraction, attack by using CLI, privilege escalation, storage media integrity attack |
| Device Web Interface | SQL injection, cross-site scripting, cross-site request forgery, user information disclosure |
| Device Firmware | sensitive information and URL disclosure, encryption key attack, firmware information disclosure |
| Device Network Services | information disclosure, attack by using CLI, injection, denial of service, service information disclosure, buffer overflow |
| Administrative Interface | SQL injection, cross-site scripting, cross-site request forgery, user information disclosure, IoT Botnet attack, spoofing attack |
| Local Data Storage | data confidentiality and integrity attacks |
| Cloud Web Interface | SQL Injection, cross-site scripting, cross-site request forgery, user information disclosure, pass word attack, spoofing attack |
| Third-party Backend APIs | personal information disclosure, device and location information leak |
| Update Mechanism | update mechanism attack |
| Mobile Application | user information disclosure, password attack, storage data attack, spoofing attack |
| Vendor Backend APIs | trust exploitation attack, spoofing attack, injection attacks |
| Ecosystem Communication | IoT healthcare security attack, ecosystem commands attack |
| Network Traffic | routing attack, DoS attack, Sybil attack |

여기서 IoT 생태계는 스마트폰, IoT 장치에게 네트워크상으로 명령을 보내거나 혹은 정보를 요청하기 위하여 원격으로 동작하는 태블릿과 같은 개체들로 구성된다. 장치는 명령을 수행하거나 네트워크상으로 정보를 보내 원격에서 분석하고 디스플레이한다.

### 2.3 IoT 보안 모델

IoT 보안 모델에 대한 기존의 연구에서는, 여러 가지 독자적인 방법이 사용되고 있다. [8]에서는 IoT 보안의 연구 과제를 분명하게하기 위하여 IoT 보안에서 액터의 역할과 그들 사이의 관계를 분석하였다. 그리고 IoT 보안의 전체론적 관점을 기반으로 한 보안 쟁점에 대한 접근을 제시하고 있다. 여기서 액터는 IoT의 4가지 구성요소 즉, 사람, 지능적 객체, 기술적 생태계 그리고 프로세스를 나타낸다. [9]에서는 IoT에서 보안과 프라이버시 문제에 대한 개요, 분석 및 분류체계를 보여준다. 그리고 IoT를 위한 보안 모델을 제시하고 있는데, IoT에서 보안, 신뢰와 프라이버시를 위한 모델링 메커니즘으로 큐브 구조를 제시하고 있다.

[10]에서는 보안 분석을 지원하기 위하여 IoT 모델링의 여러 가지 과제를 다루고 있다. 제시된 개념적 모델은 IoT 시스템의 보안 분석에 사회-기술적 개념들을 반영하는 구조-지향 접근을 기반으로 한다. 제안된 개념 모델의 사용 예로, 작은 규모의 스마트 홈 예제에 대한 보안 분석을 수행하였다.

위와 같이 몇몇의 기존연구에서는 IoT 보안 모델을 제한된 조건과 환경에서 나름대로 제시하고 있지만, IoT 시스템 설계 단계에서 일반적으로 적용하기 위한 보안 모델링으로는 부족해 보이기 때문에, 본 논문에서는 III장에서의 절차를 사용하고자 한다.

## III. 보안 모델링 절차

시스템의 보안 정책 모델을 개발하기 위하여, 해당 시스템의 보안 모델링이 사용된다. 이 모델은 시스템의 일반적 보호 철학을 제시하고, 또한 보호 메커니즘들을 포함한다. IoT 환경에서 정보의 불법 노출, 수정, 분실 및 손상을 보호하기 위하여, 중요 정보는 보호되어야 한다. 따라서 IoT 보안 정책 모델이 구축, 평가되고 사용되어야 한다. 보안 모델에서 중요한 보안 관점과 시스템 행위들의 관계가 정확하게 기술되어야 한다. 보안 모델은 시스템 개발 과정의 초기 단계에서 반드시 제시되어야 하는 핵심 보안 요구사항의 성공적 구현을 위한 필요 수준을 알기위하여 필요하다. 그러므로 보안 목표로 부터의 보안 요구사항의 유도와 식별이 초기 설계 과정의 문제가 되어야 한다. [11]의 IoT 안전을 위한 전략 원칙에서도 설계 단계에서 보안을 반영할 것을 기술하고 있다.

시스템 보안 모델링을 위하여 Bruce Schneier는 1999년에 공격 트리를 소개하였다[12]. 공격 트리는 사이버 보안 분석에 의한 시스템 침입의 기초를 식별 하는 것을 도와준다. 그림 1은 본 논문에서 사용된 IoT 보안 모델링 절차를 보여준다[3][13].

보안 모델링을 위한 구현 절차는 다음과 같다:

1) 준비: 시스템 문서화, 보안 평가 기준 및 스케줄 배치.

2) 시스템 식별: 시스템 구성요소와 기능, 구성요소 사이의 상호작용, 다른 시스템과의 상호작용, 사용자와 시스템 관리, 네트워크의 상호작용, 시스템 보안 메커니즘.

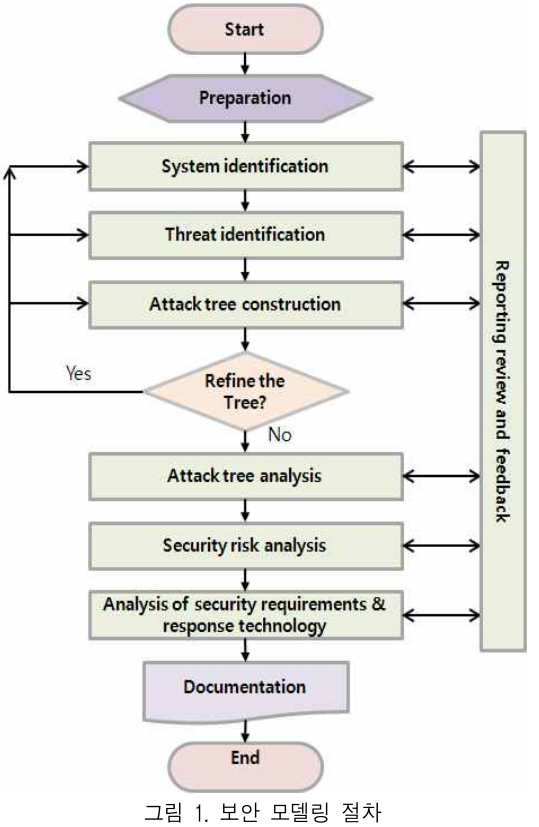


그림 1. 보안 모델링 절차
Fig. 1. Security modeling procedure

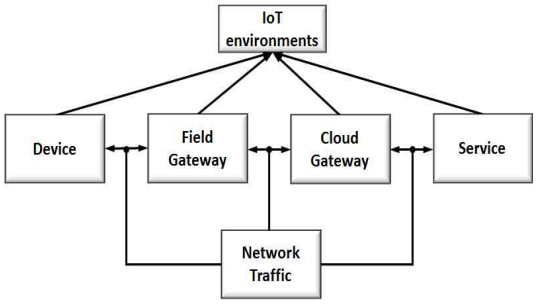


그림 2. IoT 환경에서의 구성요소
Fig. 2. Components in IoT environments

그림 2는 본 논문에서 사용하는 IoT 환경의 구성요소를 보여준다. 구성요소는 장치, 필드 게이트웨이, 클라우드 게이트웨이와 서비스로 나누고, 각 구성요소 사이의 네트워크 트래픽으로 되어있다.

3) 위협 식별: 취약점과 위협 식별, 시스템 취약점과 취약점 접근 지점 식별, 위협 근원지와 위협 형태 목록화

4) 공격 트리 구축: 공격 트리에서 루트 노드는 공격 목표를 식별하고 나타내며, 하부 공격 목표는 중간(Non-leaf) 노드로 구분된다. 루트 노드와 중간 노드는 (AND, OR)에 의하여 연결된다. 가장 세분된 공격 목표는 낙엽(leaf) 노드이다.

그림 3은 공격 트리의 예를 보여준다.

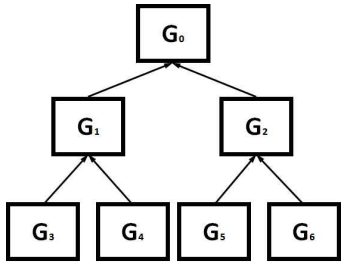


그림 3. 공격 트리 예제
Fig. 3. An example of attack tree

그림 3에서의 공격 트리는 루트 노드 $G_0$, 중간 노드 $G_1$과 $G_2$, 그리고 낙엽 노드 $G_3$, $G_4$, $G_5$, $G_6$으로 구성되어 있다. $G_0$에 대한 가능한 공격 예제는 IoT 시스템 붕괴, 그리고 $G_1$은 IoT 장치 메모리, 그리고 $G_2$는 IoT 장치 물리 인터페이스가 될 수 있다. 낙엽 노드 $G_3$, $G_4$, $G_5$, $G_6$는 각각 패스워드 공격, 암호키 해킹, 펌웨어 노출, 권한 상승 형태의 공격일 수 있다.

5) 트리 정제: 이 단계에서는 트리의 추가적인 정제 필요성에 대하여 결정하고, 모든 잠재적 위협이 트리에서 식별되고 정의되었는지 조사한다.

6) 공격 트리 분석: 이 단계에서는 모든 가능한 공격 시나리오를 생성하여 보안 위험 수준을 결정한다.

7) 보안 위협 평가: 이 단계에서는 시스템 위험 수준(SRL: System Risk Level)을 요구 위험 수준(DRL: Desired Risk Level)과 비교한다. 만약 SRL> DRL이면, 공격 시나리오에 대한 모든 가능한 보안 통제 방법의 목록을 생성한다. 보안 통제는 관리, 운영 및 기술적 통제로 분류된다.

8) 대응책 혹은 요구사항의 선택: 이 단계에서는 공격 시나리오의 SRL을 감소하기 위하여 보안 통제의 효율성을 결정한다. 본 논문에서는 대표적인 IoT 응용 사례 몇 가지에 대하여 실제로 적용할 수 있는 보안 통제 방법이 아닌 요구사항으로 대체하여 제시하고자 한다.

9) 보고서 검토 및 피드백: 이 단계는 다른 단계에서의 분석 과정을 조사하기 위하여 진행 중인 대응 활동을 말한다. 각 단계 완료 시에 분석 결과 보고서를 생성하고, 보고서는 검토자에게 전달하여 분석 결과를 검증한다. 그 다음 분석 결과를 각 완료된 단계의 다음 단계 시작 전 반영한다.

10) 문서화: 마지막으로 모든 과정들을 문서화한다.

## IV. 위협 식별과 공격 모델링

### 4.1 위협 식별

본 절에서는 IoT 환경의 보안 위협을 장치, 필드 게이트웨이, 클라우드 게이트웨이와 서비스로 나누고, IoT 위협을 식별하기 위하여 마이크로소프트에서 제안한 STRIDE 모델을 사용한다[14]. 위협 식별에 관련되는 두 개의 매우 가까운 용어가 있다. 그것은 공격 면과 신뢰 경계이다. 공격 면이 하나의 신뢰 경계이며 그리고 공격자가 공격을 개시할 수 있는 방향이다[15]. 예를 들어, 방화벽은 외부 공격자에 대하여 공격 면을 감소시키기 때문에 유용한

신뢰 경계가 될 수 있다. 그러므로 이 용어들은 서로 바꾸어 사용된다. 따라서 본 논문에서 IoT 환경은 4개의 주요한 공격 면(즉, 신뢰 경계)을 가지며, 그것은 장치, 필드 게이트웨이, 클라우드 게이트웨이와 서비스이다. IoT 장치들로는 스마트 thermostats, 스마트 전구, 스마트 연기 감지기, 스마트 에너지 관리 장치, 스마트 허브, 보안 경고, 감시 IP 카메라, 각종 오락 시스템, 광대역 라우터, 네트워크 부착 저장(NAS: Network Attached Storage) 등이 있다[4]. 또한 IoT 네트워킹 서비스로는 Z-Wave, 지그비, 전력선, 블루투스, 그리고 다른 RF(Radio Frequency) 프로토콜 등이 있다.

위협 모델링은 보안 모델링 방법의 한 수단이다. 그것은 시스템 보안을 해석하기 위하여 취약점 분석을 위한 방법을 제공하고 또한 IoT 환경에서 여러 공격 면을 식별하도록 한다. 위협 모델링의 목적은 IoT 시스템의 정상적 운영동안 발생할 수 있는 가능한 문제점들을 더 빨리 식별하기 위함이다. 그러므로 시스템 개발과 설계의 초기 단계에서 수행되어야 한다. 위협 모델링의 두 가지 핵심 관점은 주요한 보안 설계와 고려해야 할 가능한 공격 면을 정의하는 것이다. 본 절에서는 Microsoft사가 개발한 STRIDE 기반 위협 모델링을 수행한다. STRIDE는 6가지 형태의 보안 속성을 나타내며, 다음을 포함한다: 스푸핑(Spoofing), 손상(Tampering), 부인(Repudiation), 정보 공개(Information Disclosure), 서비스 거부(DoS: Denial of Service), 권한 상승(Elevation of Privilege).

IoT 시스템 환경의 식별을 통하여, 각 구성요소가 자세히 기술되고 구성 요소 사이의 데이터 흐름을 보여주는 다이어그램을 그리고, 그렇게 함으로써 각 신뢰 경계와 네트워크 연결 안에서의 보안 문제가 검토될 수 있다. 표 2는 STRIDE 분류에 의한 주요 IoT 보안 위협 요소를 보여준다.

## 4.2 공격 트리 구축

이 절에서는 4.1에서 논의된 위협 모델링을 기반으로 공격 트리를 구축한다. 그림 4~7은 대표적 IoT 환경에서의 주요 IoT 구성요소에 대한 공격 서브 트리를 보여준다.

표 2. STRIDE 분류에 의한 IoT 위협 요소
Table 2. IoT vulnerability elements by STRIDE classifications

| STRIDE | IoT vulnerability elements |
|---|---|
| Spoofing (S) | cross-service attack; worm, virus or malicious code access; ecosystem trust and/or access control system attack, device memory password and/or credential attack |
| Tampering (T) | cross-service attack, transmission data modification, application code modification, user authentication modification, cloud storage data (including S/W) modification, firmware modification and distribution, removal of device storage media, modification of device code execution flow |
| Repudiation (R) | avoiding the accountability of user |
| Information Disclosure (I) | personal authentication data (password) attack, sensitive information disclosure, transmission information interception, network service eavesdropping, update information disclosure, firmware and storage information extraction |
| Denial of Service (D) | device/network service attack, lack of update mechanism, hiding of firmware version and the latest update date |
| Elevation of Privilege (E) | account access through interface |

공격 트리는 분석된 보안 위협 요소를 바탕으로 Schneier가 제안한 공격 트리 모델링을 적용하여 생성한 것이다. 먼저 그림 4는 IoT 장치에 대한 공격 트리를 보여준다.

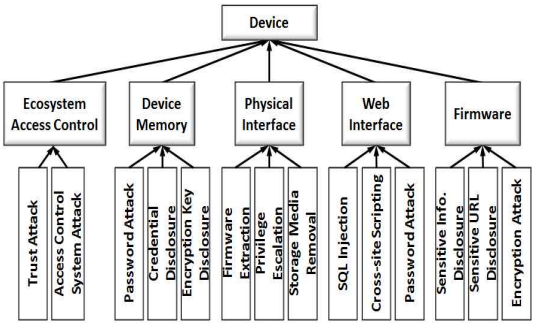


그림 4. IoT 환경에서 장치에 대한 공격 트리
Fig. 4. Attack tree for the device in IoT environments

필드 게이트웨이에 대한 공격 경로는 지역 데이터 저장을 통하여 이루어지며, 주요한 공격 방법은 데이터 절도와 데이터 변경으로 분석된다. 그림 5는 클라우드 게이트웨이에 대한 공격트리를, 그림 6은 서비스에 대한 공격 트리를 나타낸다.

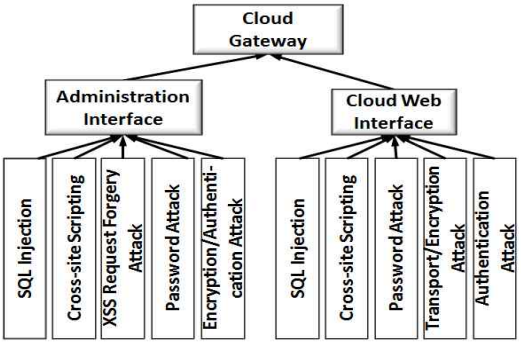


그림 5. 클라우드 게이트웨이에 대한 공격트리
Fig. 5. Attack tree for the cloud gateway

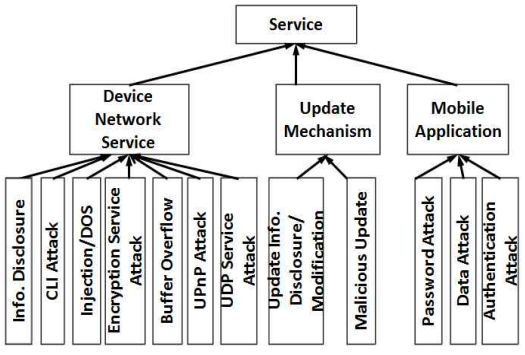


그림 6. 서비스에 대한 공격 트리
Fig. 6. Attack tree for the service

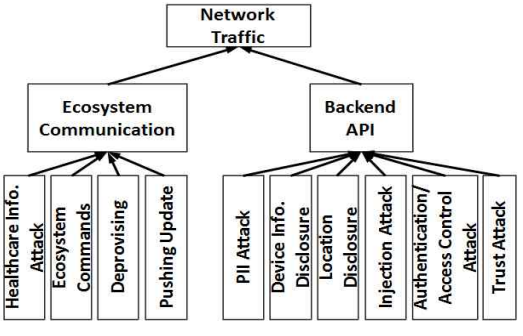


그림 7. 네트워크 트래픽에 대한 공격 트리
Fig. 7. Attack tree for the network traffic

그림 7은 네트워크 트래픽에 대한 공격 트리를 보여준다. IoT 환경에서 네트워크 트래픽은 LAN, LAN에서 인터넷, 가까운 범위 내의 트래픽, 비표준 네트워크 트래픽 등으로 분류된다.

### 4.3 OWASP 취약점 분류 기반 공격 분석

OWASP(The Open Web Application Security Project)에서도 Microsoft사 STRIDE 위협 모델 과정을 권고하고 있다. OWASP가 발표한 2017년 OWASP TOP 10 IoT 보안 취약점은 다음과 같다:

1) 불안전한 웹 인터페이스: 장치관리를 위한 웹 애플리케이션 코드의 결점으로 인하여 공격을 허용할 수 있고, 원격에서 이용될 수 있다.

2) 비효율적 인증/인가: 효율적 메커니즘의 제공으로 사용자 편의성과 보안을 같이 제공해야 한다.

3) 불안전한 네트워크 서비스: IoT 장치가 제공하는 진단, 시험과 디버깅 서비스 등이 잠재적인 보안 허점으로 제공될 수 있고, 공격 코드가 몰래 설치될 가능성이 있다.

4) 전송 암호 부재: 암호화되지 않은 개인 정보가 노출될 수 있다.

5) 프라이버시 문제: 공유 장치 상의 정보가 노출 가능하다.

6) 불안전한 클라우드 인터페이스: IoT 장치의 클라우드 관리 인터페이스가 잠재적 보안 약점이 될 수 있다.

7) 불안전한 모바일 인터페이스: 모바일 인터페이스가 보안 위협이 될 수 있다.

8) 충분하지 않은 보안 구성: 적절한 패스워드와 암호기법 등이 사용되지 않으면, 불법적인 인터페이스 접속을 통한 침해가 가능하다.

9) 불안전한 소프트웨어/펌웨어: 장치의 소프트웨어가 제로데이 취약성, 멀웨어와 다른 공격 기법에 노출될 수 있어, 새로운 위협에 대처하기 위한 정기적 업데이트가 필요하다.

10) 열악한 물리 보안: 장치의 물리적 접속을 통한 접근 제어를 통하여 장치를 보호해야 한다.

표 3은 2017년 OWASP ToP 10의 목록을 적용하여 IoT 환경의 위협을 분류한 결과 아래와 같은 공격 가능성을 보여주고 있다.

표 3. OWASP Top 10 취약점별 공격 가능성 분석
Table 3. Analysis of attack possibility by OWASP Top 10 vulnerabilities

| OWASP order | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| number of threat elements | 18 | 4 | 16 | 10 | 4 | 21 | 9 | 7 | 13 | 6 |
| attack possibility | H | L | H | M | L | H | M | M | H | M |

(Legend: H: High, M: Medium, L: Low)

표 4. IoT 환경에서 일반적 보안 요구사항
Table 4. General security requirements in IoT environments

| Threats | Security Requirements |
|---|---|
| Spoofing | Enforcement of strong password policy for the Thing, account lockout mechanism, authentication, password recovery function, security analysis of application code |
| Tampering | Protection of application code for XSS, CSRF, SQL injection; security event notification, update capability of application/software, secure update, update validation, physical access policy |
| Repudiation | authentication, audit & usage logs |
| Information Disclosure | secure storage of credentials, use of modern encryption techniques, secure data storage, encryption of transport data |
| DoS | port access policy |
| Escalation of Privilege | Enforcement of strong password, Authorization based on the access credentials, two factor authentication |

## V. IoT 보안 요구사항

### 5.1 일반적 보안 요구사항

IoT 환경에서 보안을 위하여 많은 요구사항들이 존재한다. 특히 중요한 보안 요구사항을 보면, 먼저 장치 계정과 와이파이 네트워크를 위한 강한 패스워드 사용이 필요함을 알 수 있다. 디폴트 패스워드도 반드시 변경되어야 한다. 무선 네트워크 설정 시 강한 암호화 기법을 사용해야 하고, 가능한 곳에서는 무선 대신 유선을 사용하도록 한다. 업데이트도 중요하게 보인다. 전송 데이터는 암호를 사용하고, 계정 잠금을 사용하여 전수 공격을 막아야 한다. OWASP IoT 취약점에서 열거된 인터페이스 보안도 중요하다. 표 4는 4장에서 제시된 보안 위협에 대처하기 위한 IoT 환경의 일반적 STRIDE 보안 요구사항을 보여준다.

위의 요구사항들을 만족하기 위해서 기밀성, 무결성, 가용성의 3대 핵심 보안 서비스를 포함하여, 인증 및 권한부여, 계정성(Accountability), 부인 봉쇄, 프라이버시 등의 서비스가 제공되어야 한다[15]. 기밀성은 IoT에서 중요한 보안 특징이며, 중요한 데이터, 보안 신용장과 비밀키는 보호되어야 한다. IoT 사용자에게 신뢰성있는 서비스를 제공하기 위하여 무결성도 의무적 보안 성질이다. 그러나 IoT 응용에 따라서 여러 가지의 무결성 요구사항을 가질 수 있다. 사용자에게 필요한 서비스를 제공하기 위하여 IoT 장치 내의 하드웨어와 소프트웨어 구성 요소들은 악성 코드의 존재나 다른 보안 공격에서도 견고하여야 한다. IoT 환경의 다양하고 광범위한 연결성으로 인하여, 인증 문제가 복잡해진다. 계정성은 다른 보안 기술의 적절한 동작과 부인봉쇄를 막기 위하여 필요하다. 보안 감사는 데이터와 제공 서비스의 취약성을 찾기 위하여 요구된다. 프라이버시는 장치, 통신 및 저장 데이터, 데이터 처리에서 모두 필요하다. 그리고 장치 식별과 위치에 대한 프라이버시도 요구된다.

### 5.2 CV(Connected Vehicle) 응용

CV가 IoT 응용의 초기 응용 사례에 속한다. 모바일 응용과 클라우드에 대한 견고한 연결성을 가진 차량의 통합이 이루어지고 있다. 차량은 다른 IoT 종단점과 통신을 설정할 수 있는 복잡한 IoT 종단점으로 여겨질 수 있다. 이러한 통신은 대표적으로 클라우드를 통하여 일어나게 된다[17]. 표 5는 CV에 대한 대표적인 보안 문제점과 보안 서비스를 보여준다.

표 5. 연결 차량에 대한 주요 보안 문제와 요구사항
Table 5. Main security issues and requirements for the connected vehicles

| | Main Security Issues | Corresponding Security Requirements |
|---|---|---|
| S | exploit an unauthenticated API, exploit mobile application vulnerability, spoof sensors | vehicle platform security, protection of control systems |
| T | modification of MCU, Self-Driving Vehicle code; malware installation | protection of control systems, hardware security control(e.g., MCU), software security |
| R | spoof a CV's sensor | security of roadside equipment and infrastructure, security of messaging and communication protocols |
| I | monitor messaging traffic, vehicle location, regular routes, and duration of stay | security of roadside equipment and infrastructure, security of messaging and communication protocols |
| D | infection of ransomware to restrict/limit use, DoS against traffic infrastructure (jamming), creation of botnets in RSUs | interface security, configuration security |
| E | password attack | both local and remote authentication/authorization |

## 5.3 스마트 그리드(Smart Grid) 응용

스마트 그리드는 IoT의 대표적인 응용 중에서 가장 대규모 IoT 네트워크의 하나로 볼 수 있다. 스마트 그리드는 여러 종류의 유무선 통신 인프라 외에 수많은 스마트 객체, 스마트미터, 센서와 액추에이터 등을 포함할 것이다. 스마트 그리드에서 IoT 기술의 사용으로 발전, 송전, 변전, 배전, 전기사용 및 기타 전력 그리드의 다른 측면에 대한 기술적 지원이 제공될 수 있다[18]. 표 6은 스마트 그리드 응용을 위한 주요 보안 문제점과 해당 보안 서비스를 보여준다[18].

표 6. 스마트 그리드 주요 보안 문제와 요구사항
Table 6. Main security issues and requirements for smart grid

| | Main Security Issues | Corresponding Security Requirements |
|---|---|---|
| S | identity spoofing, unauthorized access | secure device/meter authentication policy, system/application software digital signature, identity management, access control, authentication, accounting |
| T | data tampering, software/firmware compromise, malicious code infection, physical attack | risk profile reduction, input & output validation, session management, data privacy & integrity, access control, confidentiality, accounting & logging |
| R | impersonation of thing | non-repudiation, authentication |
| I | data eavesdropping, privacy issue | secure communications, confidentiality, user privacy |
| D | availability issues, physical attack | QoS policy, availability, access control |
| E | device authorization issue | device/meter authorization policy |

## 5.4 Smart Health 응용

IoT의 중요한 응용 분야의 하나로 스마트 헬스가 있다. 이동 가능한 장치와 센서들의 개발로 원격 환자 진료와 같은 여러 가지 e-헬스가 가능해 졌다. 그러나 이런 IoT의 활용이 중대한 보안과 프라이버스 위험을 동시에 발생시키고 있다. 그러므로 건강 분야에서 IoT 활용을 높이기 위해서도 효과적인 보안 대책이 수립되어야 한다.

표 7은 스마트 헬스 영역에서의 주요한 보안 문제점과 그에 대응하기 위한 보안 요구사항을 보여준다.

헬스케어 클라우드 응용에서 주요한 보안 문제는 정보의 소유권, 신빙성, 인증, 부인봉쇄, 환자 동의 및 권한 부여, 데이터 무결성과 기밀성이다. 정보의 소유권을 확립하는 것은 불법적 접근이나 환자의 의료 정보 오남용을 막기 위해서 필요하다. 신빙성은 근원지의 진실성을 나타내며, 정보의 인증에서 중간자(MITM: Man-in-the-middle) 공격을 방지하기 위하여 개체 인증이 구현되어야 한다.

표 7. 스마트 헬스 주요 보안 문제와 요구사항
Table 7. Main security issues and requirements for smart health

| | Main Security Issues | Corresponding Security Requirements |
|---|---|---|
| S | ownership of information, authenticity and authentication, imposter agent, illegal use of resources | encryption and watermarking techniques, accurate identification of each person, authentication, access control, accounting |
| T | ownership of information, unauthorized alteration of resources, file deletion, corrupted data | data integrity, access control, confidentiality, accounting, data accuracy, fraud control, health record management, data interoperability and information security |
| R | medical insurance fraud | non-repudiation, authentication |
| I | ownership of information, accident disclosure, insider curiosity, data breach by insider, data breach by outsider with physical intrusion | HIPAA minimal disclosure principle, confidentiality, user's privacy, secured data disclosure, advanced encryption algorithms |
| D | unauthorized intrusion of network system | availability, access control |
| E | escalation of healthcare service and/or insurance coverage | authorization |

부인 방지를 위하여 디지털 서명과 암호기법이 적절히 사용되어야 한다. 헬스 케어 시스템에서 불법적 사용에 의한 데이터 손상 방지를 위하여 무결성이 중요하다. 의무 기록에 대한 기밀성은 접근 제어와 암호 기법을 사용하여 제공되어야 한다. 가용성을 위하여 정전, 하드웨어 실패와 시스템 업그레이드로 인한 서비스 중단이 없어야 한다. DoS 공격에 대한 대책도 포함되어야 한다[19].

## VI. 결 론

본 논문에서는 IoT 환경에서 사이버 보안 위협을 식별하고 보안 요구사항을 도출하기 위하여 보안 모델링을 수행하였다.

먼저 IoT 환경에서의 정보보안 요구사항을 도출하기 위해 STRIDE 위협 모델링을 통하여 대표적 IoT 시스템의 각 컴포넌트에 대한 6가지 위협 요소와 대응되는 공격 예제들을 도출하였다. 그리고 Schneier가 제안한 방법을 이용하여 IoT 환경의 각 컴포넌트에 대한 공격 서브트리를 구축하고 공격 경로와 공격 가능성을 분석하였다. 그 결과 2017년 기준 OWASP 취약점 분류 중 불안전한 웹 인터페이스, 불안전한 네트워크 서비스, 불안전한 클라우드 인터페이스, 불안전한 소프트웨어/펌웨어 등에 대한 공격 가능성이 높은 것으로 분석되었다. 마지막으로 IoT 일반적 보안 요구사항을 STRIDE 위협별로 제시하였다. 또한 IoT 응용의 대표적 사례로 Connected Vehicle, 스마트 그리드와 스마트 헬스의 보안 문제점과 보안 요구사항에 대하여 분석하고 제시하였다.

본 논문에서 제시된 보안 모델링과정을 통하여 새로운 IoT 환경 전개에 걸림돌이 되는 지능화된 정보 유출 및 보안 위협에 선제적인 기술을 개발함으로써, 안전한 국가 기간망의 네트워크 구축을 위한 기초가 될 것으로 판단한다.

## References

[1] ITU-T Y.2060, "Overview of the Internet of Things, Series Y: Global Information Infrastructure, Internet Protocols Aspects and Next-Generation Networks", June 2012.

[2] IoT Forum, http://iotforum.org/, [Accessed: June 20, 2017]

[3] P.A. Khand, "Attack tree based Cyber security Analysis of Nuclear Digital Instrumentation and Control Systems", The Nucleus, Vol. 46, No. 4, pp. 415-428, Dec. 2009.

[4] Mario Ballano Barcena and Candid Wueest, "Insecurity in the Internet of Things", Symantec, Security Response, version 1.0, March 2015.

[5] EY, "Cybersecurity and the Internet of Things", March 2015.

[6] Hwa-Jung Seo, Dong-Geon Lee, Jong-Suk Choi, and Ho-Won Kim, "IoT Security Technology Trend", Journal of KIEES, Vol. 24, No. 4, pp.

27-35, July 2013.

[7] IoT Attack Surface Areas, https://www.owasp.org/index.php/IoT_Attack_Surface_Areas, [Accessed: Jun. 08, 2017].

[8] Arbia Riahi, Enrico Natalizio, and Yacine Challal, "A systemic and cognitive approach for IoT security", 2014 International Conference on Computing, Networking and Communications (ICNC), Feb. 2014.

[9] Sachin Babar, Parikshit Mahalle, Antonietta Stango, Neeli Prasad, and Ramjee Prasad, "Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)", CNSA 2010, pp. 420-429, 2010.

[10] Orestis Mavropoulos, Haralambos Mouratidis, Andrew Fish, Emmanouil Panaousis, and Christos Kalloniatis, "A conceptual model to support security analysis in the Internet of Things", Computer Science and Information Systems, Vol. 14, No. 2, pp. 557-578, Jun. 2017.

[11] U. S. Department of Homeland Security, "Strategic principles for securing the Internet of Things(IoT)", version 1.0, Nov. 2016.

[12] Bruce. Schneier, "Attack Trees", Dr. Dobb's Journal, Vol. 24, No. 12, pp. 21-29, Dec. 1999.

[13] Jung-Sook Jang, Eun-Joo Kim, and Yong-Hee Jeon, "Information Security Modeling for the Operation of Highly Trusted Networks", The Journal of Korean Institute of Information Technology, Vol. 12, No. 10, pp. 85-96, Oct. 31, 2014.

[14] Russ McRee, "Microsoft Threat Modeling Tool 2014: Identify & Mitigate", ISSA Journal, pp. 39-42, May 2014.

[15] Adam Shostack, "Threat Modeling: Designing for Security", Wiley, 2014.

[16] Mohamed Abomhara and Geir M. Koeien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks", Journal of Cyber Security, Vol. 4, pp. 65-88, May 2015.

[17] CSA(Cloud Security Alliance), "Observations and Recommendations on Connected Vehicle Security", https://cloudsecurityalliance.org/group/ internet-of-things/, [Accessed June 8, 2017].

[18] Chakib Bekara, "Security Issues and Challenges for the IoT-based Smart Grid", International Workshop on Communicating Objects and Machine to Machine for Mission-Critical Applications (COMMCA-2104), Vol. 34, pp. 532- 537, 2014.

[19] Rui Zhang and Ling Liu, "Security Models and Requirements for Healthcare Application Clouds", Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing, pp. 268-275, Jul. 2010.

## 저자소개

전 용 희 (Yong-Hee Jeon)

1978년 2월 : 고려대학교 전기전자전파공학부(공학사)
1989년 8월 : North Carolina State University 컴퓨터공학과 (공학석사)
1992년 10월 ~ 1994년 2월 : 한국전자통신연구원 광대역통신망연구부 선임연구원
1992년 12월 : North Carolina State University 컴퓨터공학과(공학박사)
2001년 3월 ~ 2003년 2월 : 대구가톨릭대학교 공과대학장
2004년 2월 ~ 2005년 2월 : 한국전자통신연구원 정보보호연구단 초빙연구원
1994년 3월 ~ 현재 : 대구가톨릭대학교 IT공학부 교수
관심분야 : 컴퓨터 네트워크, 네트워크 보안, 통신망 성능분석