IoT 제품 보안 인증 및 보안성 유지 관리방안

이동혁, 박남제
제주대학교

요 약

최근 IoT 시장이 크게 확대되고 있으며, 이에 따라 IoT 보안의 중요성에 대한 인식도 커지고 있다. 그러나 아직까지 IoT 보안에 대한 정책적 대응은 진행중에 있다. IoT 환경은 실생활과 밀접하게 관련되어 있는 바, 보안 사고가 발생하면 큰 피해가 예상되므로 시급한 보안 대책 수립이 필요한 상황이다.

본 고에서는 IoT 제품의 보안성 관리를 위한 고려사항 및 관리방안을 살펴본다.

I. 서 론

최근 IoT(Internet of Things)가 많은 관심을 모으고 있으며, 관련 연구가 활발하게 진행되고 있다. IoT는 실생활을 인터넷과 연결시켜 준다는 측면에서 생활에 많은 편의를 가져다 주며, 시장에서도 IoT 관련 제품의 출시가 점차 증가하는 추세이다.

그러나, 향후 IoT 환경이 안정적으로 정착하기 위해서는 보안에 대한 신뢰가 보장되어야 함은 자명한 사실이다. IoT는 사물과 인터넷이 결합된 형태로 실제 물리적 환경과 밀접하게 연결되어 있어, IoT에 대한 보안의 위협은 현실의 신체적, 물질적 손실로 그대로 다가올 수 있으며, 이는 IoT 환경 도입의 큰 걸림돌로 작용할 것이다. 특히, IoT 환경의 특성상 종래의 IT환경보다 피해규모가 훨씬 더 커질 수 있다. 따라서 IoT 제품은 설계, 개발, 운영 단계에서 여러가지 다양한 보안 요소가 사전에 고려되어야 한다.

본 고에서는 IoT 보안성 관리 방안에 대하여 살펴본다. 2장에서는 IoT 및 IoT보안에 대한 개요를 살펴보고, 3장에서는 OWASP(The Open Web Application Security Project), OTA(Online Trust Alliance), GSMA(GSM Association)를 중심으로 국외 IoT 보안 가이드라인 현황을 살펴본다. 그리고 4장에서는 IoT 제품의 보안 취약 요소를 살펴보고, 5장에서는 IoT 제품 설계 관점에서의 고려사항을 살펴본다. 6장에서는 IoT 제품의 개발 및 운영시의 보안성 관리방안에 대하여 살펴보고, 7장에서 결론을 맺는다.

II. IoT와 보안

IoT는 최근들어 가장 큰 이슈로 부상하고 있다. IoT는 사람과 사람 또는 사람과 사물을 연결하는 기술이며, 현실세계와 인터넷이 연결되어 다양한 서비스를 제공받을 수 있음에 따라 생활에 편리함을 가져다 준다.

따라서 IoT는 미래의 경제성장동력으로 부상하고 있으며, 전 세계적으로 이에 대한 대책을 세우고 있는 상황이다. 미국은 IoT를 국가 R&D 우선과제로 지정하고 차세대 IoT 과학기술 공학분야에 150개의 프로젝트에 대한 연구투자를 지원하고 있다. 또한, EU는 IoT의 활성화를 위해 기본적으로 추진할 실행과제인 'IoT 액션플랜'을 수립한 바 있다[1].

2016년 현재 IoT는 홈케어, 헬스케어, 자동차, 교통, 농업 등 여러 분야에서 적용되고 있다.

표 1. IoT 적용 분야[2]

분야	내용
홈케어	조명 제어, 지능형 주택관리, 스마트홈 서비스 등
헬스케어	건강보조도구, 헬스정보송수신, 핼스케어 앱 등
자동차	무인자동차, 스마트카, 차량원격관리 등
교통	국도 모니터링, 배기가스 실시간 감지, 택시 무선결재 등
농업	실시간 작물 모니터링, 온/습도 관리, 농작물 수확량 관리 등

향후 IoT시장의 확대를 위해서 반드시 고려해야 할 부분이 보안이다. IoT는 현실 세계와 인터넷이 서로 연결되어 기존 사이버 환경에서의 위협이 현실로 고스란히 전이될 수 있기 때문이다. 또한, 기존의 보안 위협요소뿐만 아니라, IoT 환경의 특성에 따른 새로운 보안 취약점이 등장할 수 있으며, 이는 사전에 충분한 보안 취약점이 검토되지 않는다면, IoT로 인해 발생할 수 있는 심각한 보안 사고를 미처 대응하지 못할 수 있다. 따라

서, 안전한 IoT 환경을 위해 보안에 대한 철저한 대비가 필수적이라 볼 수 있다.

한편, 현재 출시된 IoT 제품에 대한 보안성 유지관리 방안에 대한 대책마련도 시급하다. 현재 IoT 제품의 보안 취약성을 통하여 사용자의 개인정보 침해 등 여러 피해가 접수된 사례가 있으며, 이러한 사고의 빠른 대응을 위한 체계가 필요한 상황이다. 따라서 현재 국내에서는 민관 협력단체인 'IoT 보안 얼라이언스'가 구성되어 있으며, IoT 제품 및 서비스의 기본적인 보안성 확보 지원 및 제도적인 대책을 마련하고 있다.

III. IoT 보안 관련 가이드라인

현재 국외 많은 단체들이 IoT의 보안을 검토하고 있는 상황이다. 여기서는 대표적으로 OWASP, OTA, GSMA가 공개하고 있는 IoT 보안 가이드라인을 살펴본다.

1. OWASP Internet of Things Project

OWASP(The Open Web Application Security Project)는 신뢰할 수 있는 응용프로그램의 개발 및 운영 등을 위해 활동하고 있는 국제 웹보안표준기구이다. OWASP Internet of Things Project는 OWASP의 프로젝트 중 하나이며, IoT 에 관련된 보안 문제의 이해 향상 및 검토를 지원하는 것을 목적으로 활동하고 있다.

2014년에 공개된 'Top 10 Vulnerabilities'는 IoT 에서 발생 가능한 10가지의 주요한 포인트를 정리하였으며 보안 취약점, 공격방법 및 해결방법을 기술하고 있다. 세부 내용은 〈표 2〉와 같다.

표 2. Top 10 IoT Vulnerabilities

취약점	난이도	영향도
안전하지 않은 웹 인터페이스	하	상
불충분한 인증 / 허가	중	상
안전하지 않은 네트워크 서비스	중	중
암호화/무결성 확인의 부재	중	상
개인정보보호 우려	중	상
안전하지 않은 클라우드 인터페이스	중	상
안전하지 않은 모바일 인터페이스	중	상
불충분한 보안 설정	중	중
안전하지 않은 소프트웨어/펌웨어	상	상
물리적 보안의 취약	중	상

2. OTA IoT Trust Framework

OTA(Online Trust Alliance)는 온라인의 신뢰성을 강화하는 것을 목적으로 Symmantec, Verisign 등 100개 이상의 조직이 가입하고 있다. 산하 워킹 그룹인 IoT Trustworthy Working Group(ITWG)는 'OTA IoT Trust Framework'를 개발/공개하였다. 이는 1) 홈오토메이션 및 홈네트워크 제품, 2) 건강 및 피트니스 분야용 웨어러블 기술에 초점을 둔 검토를 실시하였으며, 다음과 같은 30개의 필수 및 권장 사항을 규정하고 있다.

1) 장비는 일반적으로 인정된 보안 통신 프로토콜을 지원해야 한다.
2) 모든 인증정보는 salt를 이용한 해쉬와 암호화를 적용해야 한다.
3) IoT를 지원하는 모든 웹사이트는 사용자 세션을 암호화해야 한다.
4) 사이트의 보안 설정, 정기적인 모니터링 및 지속적인 개선이 필요하다.
5) 취약점 보고를 관리하고 신속하게 대응하기 위한 시스템을 구축, 유지하여야 한다.
6) 모든 소프트웨어 및 펌웨어 업데이트는 출처가 있어야 하며 보안/개인정보보호 설정을 변경해서는 안된다.
7) 타사/오픈 소스 소프트웨어 인벤토리를 관리해야 하며 표준화된 개발 라이프사이클 프로세스를 따라야 한다.
8) 최종 사용자 통신(이메일, SMS 등)에는 인증 프로토콜을 적용해야 한다.
9) 인증 확인이 되지 않는 이메일은 거부하는 정책을 구현해야 한다.
10) 이메일을 사용할 경우 이메일 보안 기술을 포함한 전송레벨의 보안을 도입해야 한다.
11) 사용자 엑세스의 경우 일회성 비밀번호를 제공하거나, 다른 보안 인증 자격 증명을 사용해야 한다.
12) 비밀번호 복구기능을 제공하여야 하며, 암호가 없는 경우 다른 확인 방법(이메일, 전화 등)을 이용할 수 있어야 한다.
13) 잘못된 로그인 시도가 반복되면 사용자 계정 및 지원 계정 잠금이 필요하다.
14) 암호 재설정 또는 변경 시 보안 인증의 실시를 해야 한다.
15) 보안 침해를 받은 경우의 대응책 및 사용자 통지 계획을 수립해야 한다.
16) 사용자가 개인정보보호 정책을 쉽게 찾을 수 있도록 해야 한다.
17) 제품 보증 범위 이상의 보안 및 패치 지원의 실시 기간을 개시해야 한다.
18) 정보의 수집은 서비스 제공에 필요한 항목으로 한정한다.
19) 네트워크 연결이 두절된 경우 작동하지 않는 기능 및 잠재적 영향에 대해 공개한다.

20) 데이터 보존 정책 및 개인정보의 보유 기간을 제시한다.
21) 타 장치, 플랫폼, 서비스 간 페어링 연결 시 사용자에게 통보/승인 요청이 필요하다.
22) IoT 제품 및 서비스의 소유권 이전이 가능해야 하며, 그 방법을 공개해야 한다.
23) 제3자와의 개인정보 공유는 사용자의 동의를 얻은 경우에만 가능하다.
24) 사용자가 IoT 기기의 개인정보 설정이 가능하도록 기능과 설명서를 제공한다.
25) 사용자정보를 판매 및 양도하는 경우가 없음을 서약한다.
26) 제품 반품 시 개인정보보호가 가능하도록 기능이 제공되어야 한다.
27) 정책에 대한 거부 시 제품의 기능에 미치는 영향을 명확히 설명해야 한다.
28) 최소 2년치의 개인정보보호 고지의 변경 이력을 공개한다.
29) IoT 기기의 사용 중단, 분실, 재판매시 개인정보 및 민감정보를 삭제하거나 익명화할 수 있는 기능을 제공하여야 한다.
30) 분실 또는 재판매의 경우 기기의 데이터 및 서비스 데이터를 삭제해야 한다.

3. GSMA IoT Security Guidelines

GSMA(GSM Association)는 2016년 2월 새로운 IoT 제품 및 서비스 개발을 위한 GSMA IoT Security Guidelines를 공개하였다. 주요 대상은 다음과 같다.

- IoT 서비스 제공자 : 신규 IoT 서비스를 개발 예정인 기업 및 조직
- IoT 기기 제조자 : IoT 기기를 제공하는 제조자
- IoT 개발자 : IoT 서비스 제공자를 위한 IoT 서비스 개발을 대행하는 개발자
- 네트워크 통신 사업자 : IoT 서비스 제공을 위한 네트워크 통신 서비스를 제공하는 사업자

GSMA IoT Security Guidelines는 IoT 산업계가 IoT의 보안 문제에 대한 공통적인 이해를 확립하는 것을 지원하며, 안전한 IoT 서비스를 개발하기 위한 방법론을 나타내고 있다. 또한, IoT 서비스의 일반적인 보안 위협과 취약점을 줄이는 방법에 대한 권장사항을 제공하고 있다. 또한, 해당 문서의 범위는 IoT 서비스 및 네트워크 요소의 설계 및 구현에 한정하고 있다.

GMSA IoT Security Guidelines는 다음과 같이 네가지 부분으로 구성되어 있다.

- CLP.11(IoT Security Guidelines Overview Document) : IoT 기술 및 서비스의 개발자에게 안전한 제품을 개발하기 위한 설계 가이드를 제공
- CLP.12(IoT Security Guidelines for IoT Service Ecosystem) : 서비스 에코 시스템의 관점에서 IoT 제품 또는 서비스의 모든 구성요소를 평가하기 위한 가이드라인
- CLP.13(IoT Security Guidelines for IoT Endpoint Ecosystem) : IoT Endpoint 기기의 관점에서 IoT 서비스의 구성 요소를 평가하기 위한 가이드라인
- CLP.14(IoT Security Guidelines for Network Operators) : IoT 서비스 제공을 위한 네트워크 통신 서비스를 제공하는 네트워크 사업자를 위한 시스템 및 데이터 프라이버시 보안 가이드라인

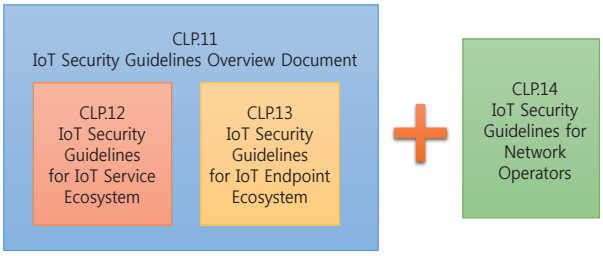

그림 1. GSMA IoT Security Guidelines

IV. IoT 제품의 보안 취약요소

IoT 환경에서는 여러가지 보안 취약점이 존재할 수 있다. 여기서는 알려진 보안 취약점 가운데 IoT 제품의 특성과 연관성이 깊은 보안 취약 요소를 살펴본다.

1. 평문 로컬 API

장치에 내장된 구성요소 및 소프트웨어는 간혹 LAN 로컬 통신을 위한 최신 암호화 표준을 사용하지 못하는 경우가 있다. 만약, 평문으로 통신하게 될 경우 큰 위협 요소가 될 수 있다. 이러한 경우, HTTPS 또는 SSH와 같은 일반적인 암호화 프로토콜을 사용하여 통신할 필요가 있다.

2. 평문 클라우드 API

주요 메이저 서비스 제공 업체는 개인정보보호 및 신뢰성을 보장하기 위해 일반적으로 암호화 방식을 채택하고 있는 상황이다. 그러나, IoT 장치와 연결되는 일부 서비스의 경우, 일반적인 표준을 준수하지 못하는 경우가 있다. 클라우드 API가 평문으로 통신하게 될 경우, 보안 위협요소가 크게 증가한다.

3. 비암호화된 저장

데이터를 평문으로 저장하게 될 경우, 인가되지 않은 자가 해당 데이터에 대한 접근이 가능할 수 있다. 데이터는 인가된 사용자만 접근할 수 있도록 암호화하여 보관하여야 한다.

4. 원격 쉘 접근

IoT제품에 원격 쉘로 접근이 가능한 경우 보안 취약요소가 될 수 있다. 원격 쉘은 개발 단계에서 유용하게 사용될 수 있으나, 제품의 개발이 끝나고 실제 IoT 제품의 출시가 필요한 경우는 해당 IoT 제품의 원격 쉘 접근을 할 수 없도록 조치를 하여야 한다.

5. 백도어 계정

IoT 장치 제조업체는 간혹 기본 계정 또는 서비스 계정을 포함한다. 이 계정은 종종 쉽게 추측 가능한 암호를 사용하는 경우가 있다. 해당 계정은 장치 고유의 암호로 보호될 수는 있으나, 패스워드 생성 알고리즘의 경우 쉽게 유추가 가능하게 될 수도 있다.

6. UART 엑세스

UART(Universal Asynchronous Receiver Transmitter) 인터페이스는 간혹 직렬 케이블 연결을 통해 정상적인 인증 메커니즘을 우회하는 방법으로 IoT 장치에 공격자가 접근하여 장치를 변경할 수 있다. 또한, UART 인터페이스는 일반 사용자의 권한을 초과하는 루트 엑세스의 권한을 부여하는 경향이 있다.

표 3. IoT 제품의 취약요소

취약점	설명
평문 로컬 API	로컬 통신이 암호화되지 않음
평문 클라우드 API	원격 통신이 암호화되지 않음
비암호화된 저장	수집된 데이터를 평문으로 저장
원격 쉘 접근	명령줄 인터페이스에 네트워크로 접근이 가능
백도어 계정	로컬 계정이 쉬운 암호로 추측됨
UART 엑세스	물리적 로컬 공격자가 장치를 변경함

V. IoT 제품 설계시의 고려사항

IoT 제품은 다른 IoT 제품 및 불특정 장비, 시스템에 연결되어도 보안이 유지되어야 하며, 이상이 발생하더라도 상대측에 피해가 없도록 설계되어야 한다. 여기서는 IoT 제품 설계시 고려해야 할 사항에 대하여 살펴본다.

1. 내/외부 및 물리적 보안 위협요소

IoT 제품 및 시스템에서 발생 가능한 위협 요소로, 외부 인터페이스, 내부적 위협, 물리적 접촉에 의한 위협 등이 있다.

외부 인터페이스를 통한 위협요소는 DoS 바이러스 및 스푸핑 등의 공격, 다른 기기에서 정상적이지 않은 데이터를 보낸 경우 등이 있다. 내부적 위협 요소는 장비 및 시스템의 설계 및 사양, 설정 등에서 보안 문제가 존재할 수 있는 부분이며, 구체적으로는 잠재적인 결함, 악성 코드 등을 꼽을 수 있다.

물리적 접촉에 의한 위험은 IoT 제품의 분해, 부품의 무단 교체 등이 해당될 수 있으며, 이러한 위험에 대한 대책이 고려되어야 한다.

2. 비정상 감지시 대응

소프트웨어 및 하드웨어의 결함이나 공격 등에 의한 비정상적인 동작이 발생하면 영향의 파급을 방지하기 위해 먼저 비정상적인 상태를 감지할 수 있도록 할 필요가 있다. 또한, 비정상 상태가 감지된 경우, 다른 IoT 제품에도 영향을 미칠 수 있으며, 이를 방지하기 위해 해당 IoT 장치를 네트워크에서 분리하는 등의 대책이 필요하다.

IoT 제품이 네트워크에서 분리 또는 기능 정지가 발생한 경우, 해당 IoT 장치를 이용하는 다른 IoT 장치에 대한 영향이 최소화되어야 한다.

3. 사용자 안전에 대한 고려

IoT의 특성상 보안 위협 요소가 신체적 안전에 대한 위협요소로도 작용할 수 있다. 예를 들어, IoT 장치 또는 유관 시스템에 공격자가 무단으로 소프트웨어 및 데이터 조작 등을 감행할 경우 오작동이 발생할 수 있으며, 이러한 공격은 보안위협 뿐만 아니라, 실제 사용자의 신체적인 위협, 즉 사고로도 이어질 수 있다. 따라서 이러한 부분이 반드시 고려되어 설계되어야 한다.

4. 기기 상호간 인증 및 권한 확인

IoT 제품에 신뢰할 수 없는 불특정 기기가 연결될 수 있다. 이러한 경우 개인정보가 쉽게 유출되거나 예상하지 않은 동작이 발생할 가능성이 있다. 한편, 동일한 모델의 제품이어도 차후에 출시된 모델과 버전차이로 인하여 연결이 정상적으로 수행되지 않는 경우도 발생한다. 따라서, 연결 시 비정상 여부 판단 및 상대측 기기의 권한 확인, 제공 기능과 정보의 범위를 조절하는 방법 등에 대한 부분도 고려되어야 한다.

5. 설계에 대한 검증/평가 실시

IoT 제품의 보안 설계가 정상적으로 되었는지에 대한 검증 및 평가 절차가 필요하다.

제품 자체는 단독으로는 문제가 없다고 할지라도, 실제 다른 IoT 장치 및 시스템과 연결될 경우 생각지 않은 위협이 발생할 수 있다. 따라서, IoT 특유의 리스크를 고려한 검증/평가 체계가 필요하다.

VI. 개발/운영시 보안성 관리방안

IoT 제품의 보안성 관리 대책은 보안위협과 공격방법을 기반으로 검토되어질 필요가 있다. 그러나, 완벽하게 안전한 관리 대책이란 존재하기 어려우며, 여러 대책을 조합하여 보다 심층적인 측면에서의 대응이 바람직하다.

한편, 보안성 관리 대책의 적용에도 일부 어려운 측면은 존재한다. 예를 들어 자원, 비용, 사고 발생시의 영향도 등 여러 측면을 고려하여 대책을 수립할 필요가 있다.

1. 개발 단계

가. 보안 모듈 및 시큐어 코딩 적용

취약점을 가진 IoT 제품이 시장에 출하되는 것을 방지하기 위해, 개발 단계에서 미리 다음과 같은 부분을 고려해야 한다.

먼저, 새로운 취약점이 발견될 수 있는 소프트웨어 또는 펌웨어의 개발에 보안 모듈이 적용되어 개발되어야 하고, 개발 시에 시큐어 코딩 기법을 활용하여야 한다.

나. 외부 소프트웨어 취약성 고려

외부의 소프트웨어(예를 들어, 오픈 소스 등)을 이용하는 경우, 알려진 취약점이 존재하는지에 대한 확인이 필요하다. 특히, 오픈 소스 소프트웨어는 소스코드가 공개되어 있다는 특징을 가지고 있으므로, 취약점 문제가 공개되기 쉽다는 측면이 있다. 따라서, 외부 소프트웨어의 취약점 관리가 소홀할 경우 공격자의 공격 수단으로 악용될 위험이 크다.

특히, 공개된 샘플 소스코드를 그대로 가져와 개발한 제품의 경우, 취약점이 혼입된 사례도 존재하였다. 따라서, 샘플 코드는 반드시 취약점이 존재하지 않는 것을 확인한 후에 이용할 필요가 있다.

다. 하드웨어 취약요소 고려

하드웨어에서 발생할 수 있는 취약요소가 고려되어 한다. 예를 들어 IoT 제품에 대해 물리적 공격이나, 의도치 않은 하드웨어의 훼손 등 다양한 상황이 발생할 수 있으며, 이를 염두에 두고 설계 및 개발이 되어야 한다.

라. 충분한 테스트 실시

제품 출하 전에 알려진 취약점 검사, 소스코드 검사 등 각종 테스트를 실시하여야 한다. 여기에서 테스트는 여러 가지 측면에서 충분하게 실시되어야 하며, 만약 테스트 시 이상이 발견될 경우는 반드시 출하시에 취약점을 모두 제거한 후 출하하도록 한다.

마. 취약점 업데이트 기능 제공

개발 단계에서 취약점을 완벽히 없애는 것이 현실적으로 쉬운 일은 아니며, 미처 파악하지 못한 취약점이 제품 출시 이후에 발생할 수도 있다. 또한, 제품 출하 시점에서 취약점으로 판단되지 않더라도, 향후 시간이 지나면 해당 부분이 취약점으로 지적될 수도 있다. (예를 들어, 암호화 알고리즘 및 키 길에 대한 부분) 따라서, 제품 출시 후 취약점의 발견에 대비하여 소프트웨어 및 펌웨어의 업데이트 기능을 구현할 필요가 있다.

2. 운영 단계

가. 지속적인 취약점 정보 수집

제품 출시 이후에 신규 취약점이 발생하는 경우를 대비하여, 지속적으로 취약점 정보를 수집하여야 한다. 제품 개발에 이용한 외부의 소프트웨어에 대한 새로운 취약점 등 여러 발생 가능한 취약 요소에 대해 취약점 대책 정보를 수집하고 관리할 필요가 있다.

나. 취약점 발생시 대응방안 수립 통지

신규 취약점이 발생한 경우, 이에 대한 취약점 관련 정보를 신속히 수집하고 대응 메뉴얼을 작성하여야 한다. 여기에는 취약점의 개요, 심각도, 영향범위, 대책방안 등의 정보가 포함되어야 한다. 취약점 대응 매뉴얼이 작성되면, 신속히 관련자에게 전파하여야 한다.

다. 소프트웨어 업데이트 제공

소프트웨어 취약점의 경우 가장 일반적인 대책은 취약점을 해결한 업데이트 소프트웨어를 제공하고, 이용자에게 적용을 권고하는 것이다.

만약, 업데이트 소프트웨어의 제공에 일정 시간이 소요된다고 판단될 경우, 적절한 다른 방안을 고려해볼 필요가 있다.

정보기술에 익숙하지 않은 고연령층이 주 고객층인 제품 등 소프트웨어 업데이트 적용이 쉽지 않은 상황일 경우 원격 조작에 의해 자동으로 업데이트 소프트웨어를 적용하는 방법도 고

려할 필요가 있다. 이러한 경우, 제품 출하시의 시점에서 제품의 자동 업데이트 기능에 대한 내용을 사전에 고지하여야 한다. 또한, 소프트웨어 업데이트를 통하여 제품이 가지는 기능이 변경될 경우, 자동 업데이트는 가급적 피하고 이용자의 동의를 거쳐 업데이트가 적용될 수 있도록 한다.

라. 업데이트 불가시 리콜 실시

소프트웨어 업데이트가 어려운 제품인 경우, 혹은 하드웨어상의 보안 취약점이 발견된 경우에는 즉각적인 리콜 실시가 필요하다. 이러한 경우, 제품을 일단 회수처리 한 후 차후 대책을 진행할 필요가 있다.

표 4. 단계별 관리 방안

단계	관리 방안
개발 단계	– 보안 모듈 및 시큐어 코딩 적용 – 외부 소프트웨어 취약성 고려 – 하드웨어 취약요소 고려 – 충분한 테스트 실시 – 취약점 업데이트 기능 제공
운영 단계	– 지속적인 취약점 정보 수집 – 취약점 발생시 대응방안 – 수립 통지 – 소프트웨어 업데이트 제공 – 업데이트 불가시 리콜 실시

VII. 결 론

안전한 IoT 환경을 위해서는 기술적인 보안 대책 뿐만 아니라, 정책적인 보안 관리 방안 대책도 동시에 고려될 필요가 있다.

따라서 본 고에서는 국외 IoT 보안을 우선적으로 살펴보고, 이후 IoT 제품의 취약 요소를 살펴보았다. 또한, 설계 단계에서 고려해야 할 사항들을 언급해 보았으며, 마지막으로 개발 및 운영 단계에서의 보안성 유지를 위한 관리방안을 살펴보았다.

IoT 환경이 활성화되려면 보안에 대한 고려는 반드시 필요하며, 향후 출시되는 모든 IoT 제품에는 IoT 보안 요소도 함께 적용되어 출시되어야 한다. 이러한 과제가 조속히 해결되어야 안전한 IoT 세상이 도래할 것이다.

참 고 문 헌

[1] 원유재, "IoT(Internet of Things) 정보보호 기술 개발 방향", 한국통신학회, 한국통신학회지 (정보와통신) 32(1), pp.24-27, 2014.12

[2] 김시정, 조도은, "IOT(Internet of Things) 보안 기술 동향", 한국콘텐츠학회지 13(1), pp.31-35, 2015.3

[3] 우성희,"IoT 환경의 의료 정보보호와 표준 기술", 한국정보통신학회논문지 19(11), pp.2683-2688, 2015.11

[4] 일본 총무성, "IoT セキュリティガイドライン", IoT 推進コンソーシアム, 2016

[5] Namje Park, "Implementation of Terminal Middleware Platform for Mobile RFID Computing", International Journal of Ad Hoc and Ubiquitous Computing, Vol. 8, No. 4, pp. 205-219, Nov. 2011.

[6] 일본 IPA 보고서, "IoT開発におけるセキュリティ 設計の手引き", 2016. 5

[7] Namje Park, Jin Kwak, Seungjoo Kim, Dongho Won, and Howon Kim, "WIPI Mobile Platform with Secure Service for Mobile RFID Network Environment", LNCS, Advanced Web and Network Technologies and Applications, Vol. 3842, pp. 741-48, Jan. 2006.

[8] Mark Stanislav, Tod Beardsley, "HACKING IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities", Rapid7, 2015

[9] Namje Park, Marie Kim, "Implementation of load management application system using smart grid privacy policy in energy management service environment", Cluster Computing Vol. 17, No. 3, pp. 653-664, Sep. 2014.

[10] Zhang, Zhi-Kai, et al. "IoT security: ongoing challenges and research opportunities." 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications. IEEE, 2014.

[11] Namje Park and Namhi Kang, "Mutual Authentication Scheme in Secure Internet of Things Technology for Comfortable Lifestyle", Sensors, Vol. 16, No. 1, pp. 1-16, Dec. 2015.

[12] Farooq, M. U., et al. "A critical analysis on the security concerns of internet of things (IoT)." International Journal of Computer Applications 111.7 (2015).

[13] Namje Park, Hongxin Hu, and Qun Jin, "Security and Privacy Mechanisms for Sensor Middleware and Application in Internet of Things (IoT)", International Journal of Distributed Sensor Networks, Vol. 2016, Article 2965438, Oct. 2015.

[14] Zhao, Kai, and Lina Ge. "A survey on the internet of things security." Computational Intelligence and Security (CIS), 2013 9th International Conference on. IEEE, 2013.

[15] Namje Park and Hyo-Chan Bang, "Mobile middleware platform for secure vessel traffic system in IoT service environment", Security and Communication Networks, John Wiley&Sons Ltd, Nov. 2014.

[16] Donghyeok Lee, Namje Park, "Geocasting-based synchronization of Almanac on the maritime cloud for distributed smart surveillance", The Journal of Supercomputing, pp.1-16, 2016.

약 력

이 동 혁

2007년 동국대학교 전자상거래기술전공 공학석사
2015년~현재 제주대학교 컴퓨터교육전공 박사과정
2007년~2008년 한국전자통신연구원 정보보호연구단 연구원
2008년~2015년 KT 플랫폼개발단 과장
관심분야: 클라우드 보안, 스마트그리드 보안, 데이터베이스 보안, 해사클라우드

박 남 제

2008년 성균관대학교 컴퓨터공학과 박사
2003년~2008년 한국전자통신연구원 정보보호연구단 선임연구원
2009년 미국 UCLA대학교 공과대학 Post-Doc,WINMEC 연구센터 Staff Researcher
2010년 미국 아리조나 주립대학교 컴퓨터공학과 연구원
2010년~현재 제주대학교 초등컴퓨터교육전공 교수
관심분야: 융합기술보안, 컴퓨터교육, 스마트그리드, IoT, 해사클라우드 등