IoT 보안 국내외 동향 및 IoT 보안 기술

서혁준
LG CNS 부장

IoT 는 이용자의 개입 없이 서로 통신하며 이용자에게 이로운 서비스를 제공하지만, 보안이 고려되지 않을 경우 큰 위험이 초래될 수 있다. 최근 IoT 기기를 이용한 디도스 공격이나 홈CCTV가 해킹되어 영상이 실시간 노출된 것은 알려진 해킹 사고에 불과하다. 알려지지 않은 다양한 IoT 보안 이슈가 있으며 보안 대책을 적용하지 않는다면 사고는 언제든 발생할 수 있다. 본 고에서는 국내·외에 발표된 IoT 보안 가이드의 내용을 살펴보고, IoT 사고 예방을 위해 적용해야 할 IoT 보안 기술을 살펴보기로 한다.

Ⅰ. 서론

가트너에서 발간한 2013 년 보고서에 의하면, PC, 태블릿, 스마트폰을 제외한 사물인터넷 기기가 2020 년에 260 억 대에 이를 전망이다. UN 은 2020 년 세계 인구가 77 억 명이 될 것으로 예상하고 있으며, 이 경우 세계 인구의 3.4 배에 달하는 IoT 기기가 설치 및 운영되어 생활 주변에 IoT 가 이용자 개입 없이 서로 통신하며 편리한 서비스를 제공하게 될 것임을 예상해 볼 수 있다. 그러나, IoT 기기가 해킹된다면 이는 불편함으로 바뀔 수 있다는 점을 고려해야 한다. IoT 에 보안이 고려되지 않아 발생한 사고 사례를 살펴보면 다음과 같다.

안나센빠이라는 ID 를 사용하는 익명의 개발자는 미라이(Mirai)라는 악성코드를 제작하여 2016 년 9 월 IoT 장비를 대상으로 봇넷을 구성하고, 약 600Gbps 이상에 해당하는 악의적인 공격 트래픽을 발생시켜 대규모 디도스(DDoS) 공격이 가능함을 보여주었다. 카스퍼스키 보고서에 따르면 2016 년 3 분기 중 봇넷을 사용한 디도스 공격 표적에 든 나라가 67 곳이었다고 한다. 이 중 중국 소재 목표가 전체 공격의 62.6%로 1 위를 차지했고, 미국은 18.7%로 2 위, 한국이 8.7%로 3 위에 꼽혔다.

* 본 내용은 서혁준 부장(suh_hyuck_jun@hotmail.com)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP 의 공식적인 입장이 아님을 밝힙니다.

러시아에서 운영중인 인세캠(Insecam)이라는 사이트에는 국내에 설치된 CCTV 수백 대를 포함한 전 세계의 해킹된 CCTV 영상이 실시간으로 중계되고 있다. 국내 CCTV에는 빌딩 로비, 수영장, 개인 사무실, 백화점 매장 등 불특정 장소가 다수 포함되어 있으며, 인세캠 이용자는 별다른 로그인 절차 없이도 해킹된 CCTV 영상을 PC 브라우저를 통해 시청할 수 있다. 국내에서는 러시아 인세캠 사이트가 유해 사이트로 지정되어 있어 접속할 수 없지만 외국에서는 해킹된 국내 CCTV 기기가 전송하는 영상을 시청할 수 있다.

본 고에서는 IoT 보안 기술의 동향을 국내·외에서 발표된 주요 IoT 보안 가이드를 통해 살펴보기로 한다.

Ⅱ. 국내외 IoT 보안 가이드

1. 국외 IoT 보안 가이드

가. GSMA IoT 보안 가이드라인

2016 년 2 월, 세계이동통신사업자협회(GSM Association: GSMA)는 IoT 시장의 안전한 서비스 발전과 확산을 촉진하기 위해 'GSMA IoT 보안 가이드라인(The GSMA IoT Security Guidelines)'을 발표했다. 모바일 업계의 자문을 받아 작성된 이 지침은 IoT 서비스 제공자, IoT 기기 제작자, GSM 망 운영자를 포함한 IoT 생태계의 모든 참여자를 위해 제작되었으며, 잠재적 위협에 대처하는 기술과 방법 그리고 이를 실행하는 방안에 대한 개략적인 설명을 통해 서비스 제공자들이 보안 서비스를 구축하도록 방향을 제시한다.

[표 1] GSMA IoT 보안 가이드 문서의 구성

구성	설명
개요	- 프로세스 보안 - 가이드 활용 방안 - 신체부착형 심박 측정기, 개인 무인비행기, 차량 센서 네트워크 사례
서비스 보안	- 서비스 보안 모델 - 서비스의 중요, 높음, 중간, 낮음 보안 권고 사항
기기 보안	- 기기 보안 모델 - 기기의 중요, 높음, 중간, 낮음 보안 권고 사항
네트워크 보안	- 네트워크 보안 모델 - 망 사업자를 위한 보안 권고 사항

<자료> GSMA, IoT Security Guidelines, GSM Association, CLP.11~14, 2016. 11. 7.

<자료> GSMA, IoT Security Guidelines Overview Document, GSM Association, CLP.11, 2016. 11. 7, p.16.

[그림 1] IoT 모델 예시

개요에서는 위험 분석, 개발 보안 라이프사이클(Secure Development Lifecycle: SDL), 개인정보보호 프로세스를 설명하고 있으며, 서비스・기기・네트워크 보안이 개별 문서에서 다루어진다.

(1) 서비스 보안

서비스는 웹 서버, 웹 애플리케이션 서버, 데이터베이스 서버, 인증, 네트워크, 빌링 티어(Tier)와 같은 구성 요소를 말하며, 구성요소 및 연결 관계를 고려하여 보안 모델을 수립해야 한다.

서버 복제 이슈, 기기 이상 행위 탐지, 비정상 기기 접속 차단, 서버 해킹, 원격 공격 이슈 해결을 위해서는 해당 권고 사항을 충족해야 한다. 예를 들어, 원격 공격의 가능성을 줄이기 위해서는 인터넷 노출 인터페이스, 업데이트, 입력값 검증, 출력값 필터링, 방화벽 규칙 권고사항을 충족해야 하고, 기기 이상 행위를 탐지하기 위해서는 접속 기록, 커뮤니케이션, 네트워크 인증 서비스, 알림에 대한 긍정/부정 오류 평가를 충족해야 한다.

권고사항은 우선순위별(중요, 높음, 중간, 낮음)로 나누어 제시되어 있으며, 이 중 중요와 높

[표 2] 서비스의 중요, 높음 보안 권고 사항

우선 순위	설명	우선 순위	설명
중요 (Critical)	- 신뢰할 수 있는 컴퓨팅 환경(TCB) 구현 - 안전한 초기화 - 인터넷 노출 인터페이스의 안전한 구현 - 안전한 영구 저장소 - 관리 모델 - 접속 기록과 모니터링 - 사고 대응 - 사고 발생 후 복구 - 서비스 폐기 - 보안 등급 분류 - 데이터 유형 분류	높음 (High)	- 명확한 권한 관리 - 암호 아키텍처 - 안전한 커뮤니케이션 - 네트워크 인증 서비스 - 프로비저닝 - 안전한 업데이트 - 데이터 관리 정책 - 서버를 이용한 인증 - 입력값 검증 - 출력값 필터링 - 비밀번호 복잡도 - 애플리케이션 인증 및 권한 관리 - 방화벽 규칙과 시스템 하드닝 - 개인정보보호

<자료> GSMA, IoT Security Guidelines for Service Ecosystems, GSM Association, CLP.12, 2016. 11. 7, pp.19-51.

음에 해당하는 항목은 [표 2]와 같다.

(2) 네트워크 보안

네트워크 보안 영역의 권고 사항은 3GPP(3rd Generation Partnership Project) 사업자를 대상으로 하며, 3GPP 망에서 이용자/기기 등의 식별, 인증, 안전한 커뮤니케이션 채널의 권고 사항이 있다.

(3) 기기 보안

사양에 따라 기기를 구분하면 저사양 기기, 게이트웨이(허브), 고사양 기기가 있으며, 제약을 고려한 적절한 보안 모델을 정의해야 한다. 즉, 네트워크 통신, 접근 가능한 네트워크 서비스, 콘솔 접근, 로컬 버스 커뮤니케이션, 칩 접근 공격에 대한 청사진이 필요하다.

[표 3] 기기 보안 모델

공격 유형	보안 모델
네트워크 통신 공격	- 크레덴셜 및 토큰 보호 - 블루투스 또는 802.15.4 근거리 통신의 스니핑이나 중간자 공격 방어
네트워크 서비스 공격	- 포트스캐닝을 통해 확인된 SSH 등의 서비스에 Common Gateway Interface (CGI) 스크립트 실행 취약점 제거
콘솔 접근 공격	- 기기 인쇄회로기판에 노출된 UART를 통한 로컬 하드웨어 공격을 방어
로컬 버스 커뮤니케이션 공격	- 쓰기 가능한 메모리(SD/MMC, NVRAM, EEPROM)의 내용 변경 방어 - 하드웨어 버스를 지나가는 평문 키의 노출 방어 - 하드웨어 회로에 위·변조 메시지 주입 가능성 제거
칩 접근 공격	- CPU 분해 방어 - 내부 EEPROM, NVRAM에서 비밀값 추출 방어 - 내부 SRAM 메시지 가로채기 방어 - X-Ray 분석 방어

<자료> GSMA, IoT Security Guidelines for Endpoint Ecosystems, GSM Association, CLP.13, 2016. 11. 7, p.15-18.

기기 복제 대응, 안전한 기기 식별자, 보안 하드웨어 칩의 적용, 펌웨어 소프트웨어의 위·변조 대응, 원격 코드 실행 방어, 비인가된 디버깅 방지, 부채널 공격 방어, 안전한 원격 관리 방안 마련, 해킹된 기기 탐지를 위한 권고사항을 알 수 있다. 예를 들어, 원격 코드를 실행하기 어렵게 하려면 메모리 보호, 내부 메모리에 비밀값 저장, 안전한 OTA(Over-the-air), 애플리케이션 실행 시 적절한 실행 권한 부여, 애플리케이션 권한 분리 설계, 언어 보안, 운영체제 보안, 이용자 인터페이스 보안, 제3자 소스코드 감사를 고려해야 한다.

기기의 중요와 높음에 해당하는 보안 권고 항목은 [표 4]와 같다.

[표 4] 기기의 중요, 높음 보안 권고 사항

우선 순위	설명	우선 순위	설명
중요 (Critical)	- 기기의 신뢰 컴퓨팅 환경(TCB) 구현 - 보안 하드웨어(Trust Anchor) 사용 - 변조를 막는 보안 하드웨어를 사용 - 신뢰 컴퓨팅 환경(TCB)용 보안 API - 계층 키 구조(Root of Trust) 규정 - 풀필먼트 이전에 기기 개인화 - 애플리케이션 원상 복구 - 기기를 고유하게 프로비저닝 - 기기 패스워드 관리 - 입증된 난수 발생기(RNG) 사용 - 암호 서명된 애플리케이션 바이너리 - 원격 기기 관리 - 접속 기록과 진단 - 메모리를 보호 - 내장 롬(ROM) 밖의 부팅 - 메모리의 핵심 영역 잠그기 - 안전하지 않은 부트로더 - 완전 순방향 비밀성(PFS) - 기기 통신 보안 - 기기 ID를 인증	높음 (High)	- 비밀을 내부 메모리에서 이용 - 이상 동작 감지 - 변조를 막는 제품 케이싱 이용 - 보안 하드웨어의 기밀성과 무결성 - 무선 애플리케이션 업데이트 - 부적절하게 구현된 상호 인증 - 개인정보보호 관리 - 프라이버시 및 고유의 기기 ID - 적절한 권한으로 프로그램 실행 - 애플리케이션 구조에서 책임 분리 - 언어 보안

<자료> GSMA, IoT Security Guidelines for Endpoint Ecosystems, GSM Association, CLP.13, 2016. 11. 7, p.25-58.

나. OWASP IoT 프로젝트

애플리케이션 보안과 관련된 다양한 활동과 연구 성과를 발표하고 있는 OWASP(Open Web Application Security Project)에서 진행하는 IoT 보안 프로젝트는 프로젝트, 공격 표면 영역, 테스팅 가이드, 주요 취약점으로 구성되어 지속적으로 업데이트되고 있다.

[표 5] OWASP IoT 구성

구성	설명
프로젝트	세부 프로젝트: 펌웨어 분석, ICS/SCADA, IoT 보안 정책
공격 표면 영역	18개 항목으로 구성된 공격 표면 및 이와 관련된 취약점
테스팅 가이드	10대 영역으로 분류된 IoT 보안 고려 사항
주요 취약점	16개 항목으로 구성된 주요 취약점 및 이와 연관된 공격 표면

<자료> OWASP, OWASP Internet of Things (IoT) Project, The OWASP Foundation, 2017.

(1) 공격 표면 영역

[표 6]은 공격 표면을 18개로 정의하였으며 타 보안 가이드와 비교를 위해 계층으로 분류해 보았다.

서비스 공격 표면은 기존의 웹 뿐만 아니라 백엔드 API, 에코시스템 커뮤니케이션이 포함되

어 있고, 기기 공격 표면도 웹과 네트워크 뿐 아니라 기기 메모리(민감 정보), 로컬 데이터 저장소(암호화되지 않은 키, 데이터 무결성 체크 미흡, 고정적인 암・복호화 키 사용), 하드웨어(센서)로 세분화되어 있다.

[표 6] OWASP IoT 공격 표면 영역 정리

계층	OWASP IoT 공격 표면 영역	계층	OWASP IoT 공격 표면 영역
서비스	- 에코시스템 - 제 3 자 백엔드 API - 벤더 백엔드 API - 에코시스템 커뮤니케이션 - 클라우드 웹 인터페이스 - 모바일 앱	기기	- 기기 웹 인터페이스 - 기기 네트워크 서비스 - 인증, 권한 관리 - 기기 메모리 - 로컬 데이터 저장소 - 물리적 인터페이스 - 기기 펌웨어 - 업데이트 매커니즘 - 관리자 인터페이스 - 하드웨어(센서)
네트워크	- 네트워크 트래픽	개인정보	- 개인정보보호

<자료> OWASP, IoT Attack Surface Areas Project, The OWASP Foundation, 2017.

(2) 주요 취약점

기기 분해 후 디버그 포트를 이용한 코드 실행, 펌웨어 업데이트 체크 기능의 부재, 저장소(NVRAM, EEPROM) 데이터 위・변조, 압축된 펌웨어 추출을 취약점으로 정의하고 있다. 직렬 주

[표 7] OWASP IoT 주요 취약점

유형	주요 취약점
인증	- 이용자 계정명 수집 - 취약한 패스워드 - 계정 잠금 해제 - 이중 인증
네트워크 보안	- 암호화되지 않은 네트워크 서비스 - 서비스 거부
암호화 구현	- 잘못 구현된 암호화 - 암호화되지 않은 업데이트 전송
코드 실행	- 기기 내 코드 실행(JTAG 인터페이스, 부채널 공격 이용) - 콘솔 접근(SPI, UART)
펌웨어 업데이트	- 업데이트 체크 기능 부재 - 업데이트 기능 부재 - 펌웨어 버전 노출, 마지막 업데이트 일자 노출
안전한 저장소	- 위변조 가능한 저장소 - 저장장치 미디어 분리 - 저장소에서 펌웨어 추출

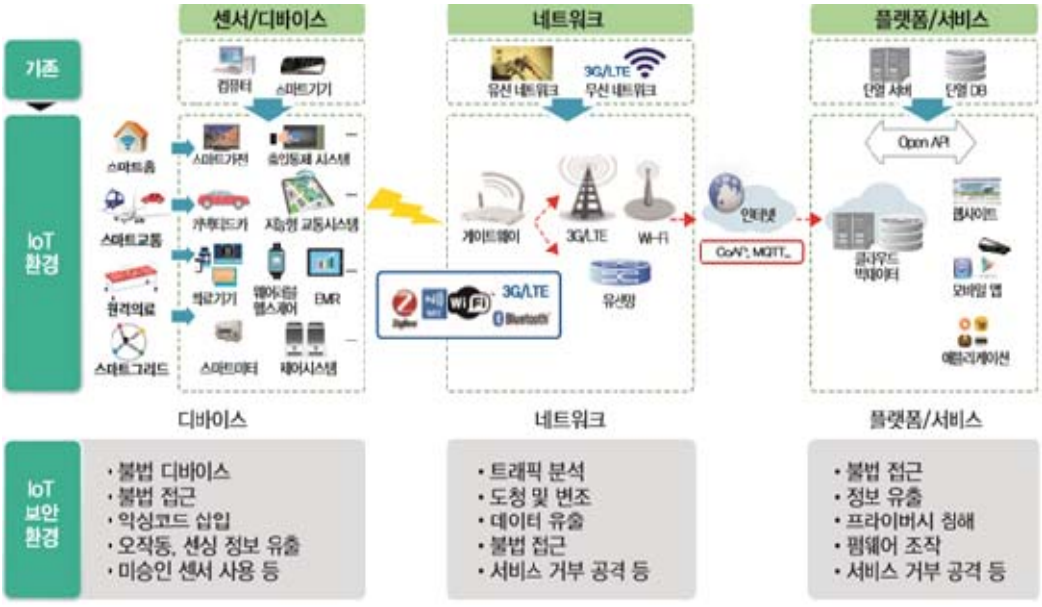
<자료> OWASP, IoT Vulnerabilities Project, The OWASP Foundation, 2017.

변기기 인터페이스 버스(Serial Peripheral Interface Bus) 또는 범용 비동기화 송수신기(UART) 포트에 접근하여 코드를 실행할 수 있거나, 애플리케이션 무결성 검사를 우회하여 업데이트를 할 수 있다든가, EEPROM(Electrically Erasable Programmable Read-Only Memory)에서 중요 값을 획득할 수 있다든가 하는 것 모두가 IoT 보안 취약점에 해당한다.

2. 국내 IoT 보안 가이드

가. IoT 공통 보안 가이드

2016 년 9 월, 한국인터넷진흥원에서는 산・학・연 전문가와 얼라이언스를 구성하여 ICT 융합제품 및 서비스의 보안 내재화를 위한 IoT 공통 보안 가이드를 발표했다. IoT 보안 환경은 [그림 2]와 같이 센서/기기, 네트워크, 플랫폼/서비스 계층으로 구분되는데, 공통 보안 가이드는 산업을 특정하지 않고 공통적인 보안을 서술하며 디바이스 계층의 보안만 다룬다.



<자료> IoT 보안얼라이언스, IoT 공통 보안 가이드, 한국인터넷진흥원, v1.0, 2016. 9, p.9.

[그림 2] IoT 환경에서의 보안 위협

15 개 항목으로 구성된 가이드 내용은 [표 8]과 같다. 각 항목의 해설과 사례, 관련 기술 소개는 분야별 전문적인 내용을 포함하고 있다.

[표 8] IoT 공통 보안 가이드 15개 항목

단계	IoT 공통 보안 원칙	IoT 공통 보안 가이드
설계 개발	1) 정보보호와 프라이버시 강화를 고려한 IoT 제품·서비스 설계	① IoT 장치의 특성을 고려하여 보안 서비스의 경량화 구현 ② IoT 서비스 운영 환경에 적합한 접근권한 관리 및 인증, 종단 간 통신 보안, 데이터 암호화 등의 방안 제공 ③ 소프트웨어 보안기술과 하드웨어 보안 기술의 적용 검토 및 안전성이 검증된 보안 기술 활용 ④ IoT 제품 및 서비스에서 수집하는 민감 정보(개인정보 등) 보호를 위해 암호화, 비식별화, 접근관리 등의 방안 제공 ⑤ IoT 서비스 제공자는 수집하는 민감 정보의 이용목적 및 기간 등을 포함한 운영정책 가시화 및 사용자에 투명성 보장
	2) 안전한 SW 및 HW 개발기술 적용 및 검증	⑥ 소스코드 구현단계부터 내재될 수 있는 보안 취약점을 사전에 예방하기 위해 시큐어 코딩 적용 ⑦ IoT 제품·서비스 개발에 사용된 다양한 S/W에 대해 보안 취약점 점검 수행 및 보안패치 방안 구현 ⑧ 펌웨어/코드 암호화, 실행코드 영역제어, 역공학 방지 기법 등 다양한 하드웨어 보안 기법 적용
배포 설치 구성	3) 안전한 초기 보안설정 방안 제공	⑨ IoT 제품 및 서비스 (재)설치 시 보안 프로토콜들에 기본으로 설정되는 파라미터 값이 가장 안전한 설정이 될 수 있도록 “Secure by Default” 기본 원칙 준수
	4) 안전한 설치를 위한 보안 프로토콜 준수 및 안전한 파라미터 설정	⑩ 안전성을 보장하는 보안 프로토콜 적용 및 보안 서비스 제공 시 안전한 파라미터 설정
운영 관리 폐기	5) IoT 제품·서비스 취약점 패치 및 업데이트 지속 이행	⑪ IoT 제품·서비스의 보안 취약점 발견 시, 이에 대한 분석 수행 및 보안패치 배포 등의 사후조치 방안 마련 ⑫ IoT 제품·서비스에 대한 보안 취약점 및 보호조치 사항은 홈페이지, SNS 등을 통해 사용자에게 공개
	6) 안전 운영·관리를 위한 정보보호 및 프라이버시 관리체계 마련	⑬ 최소한의 개인정보만 수집·활용될 수 있도록 개인정보 보호정책 수립 및 특정 개인을 식별할 수 있는 정보의 생성·유통을 통제할 수 있는 기술적·관리적 보호조치 포함
	7) IoT 침해사고 대응체계 및 책임추적성 확보 방안 마련	⑭ 다양한 유형의 IoT 장치, 유·무선 네트워크, 플랫폼 등 다양한 계층에서 발생 가능한 보안 침해사고에 대비하여 침입탐지 및 모니터링 수행 ⑮ 침해사고 발생 이후 원인분석 및 책임추적성 확보를 위해 로그기록의 주기적 저장·관리

<자료> IoT 보안얼라이언스, IoT 공통 보안 가이드, 한국인터넷진흥원, v1.0, 2016. 9, p.19.

나. 홈·가전 IoT 보안 가이드

2017년 7월, IoT 보안 얼라이언스 제4차 정기회의에서 ‘홈·가전 IoT 보안 가이드’가 발표되었다. 스마트 TV, 스마트 냉장고, 홈 CCTV, 네트워크 카메라, 디지털 도어락, 공유기 등 실생활에 사용되는 가전을 대상으로 보안 구현 방법과 사례를 제시하고 있다.

[표 9] 홈・가전 IoT 보안 가이드의 내용

유형	주요 내용
소프트웨어 보안	시큐어코딩, 알려진 보안 취약점 점검・제거, 최신 제3자(서드파티) 소프트웨어 사용
물리적 보안	외부 인터페이스 접근 보안, 디버그 포트 접근 보안, 부채널 공격 대응, 메모리 공격 대응
플랫폼 보안	설정값 및 실행코드 무결성 검증, 안전한 업데이트, 감사기록
인증	인증・접근 통제, IoT 기기간 상호 인증
암호화	안전한 암호 알고리즘 사용, 안전한 암호키 관리, 안전한 난수 생성 알고리즘 사용
데이터 보호	안전한 통신 채널, 저장・전송 데이터 보호, 개인정보보호

<자료> 홈・가전 IoT 보안 가이드, 한국인터넷진흥원, 2017. 7. 18, 제4차 회의 공개 내용

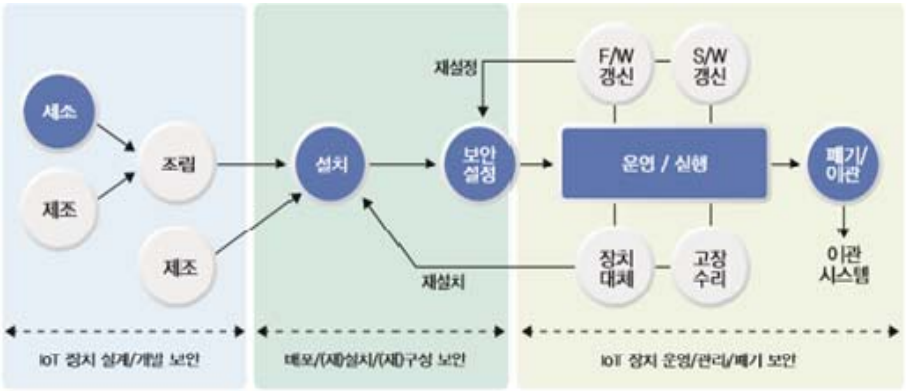
Ⅲ. IoT 보안 기술

국내외 IoT 보안 가이드는 일반적인 보안 요구사항에서 산업별 세부 체크리스트 및 해설서 형태로 구체화되고 있으므로 이를 참고하여 IoT 보안을 준비할 수 있다. 이번 장에서는 적용해야 할 주요 보안 항목을 프로세스, 서비스, 기기 관점으로 살펴보겠다.

1. IoT 보안 프로세스

가. 개발 보안 라이프사이클(SDL)

마이크로소프트사는 보안 수준이 높은 안전한 소프트웨어를 개발하기 위해 자체 수립한 SDL(Secure Development Lifecycle) 방법론을 적용하였으며, SDL이 적용된 소프트웨어는 이전 버



<자료> IoT 보안얼라이언스, IoT 공통 보안 가이드, 한국인터넷진흥원, v1.0, 2016. 9, p.18.

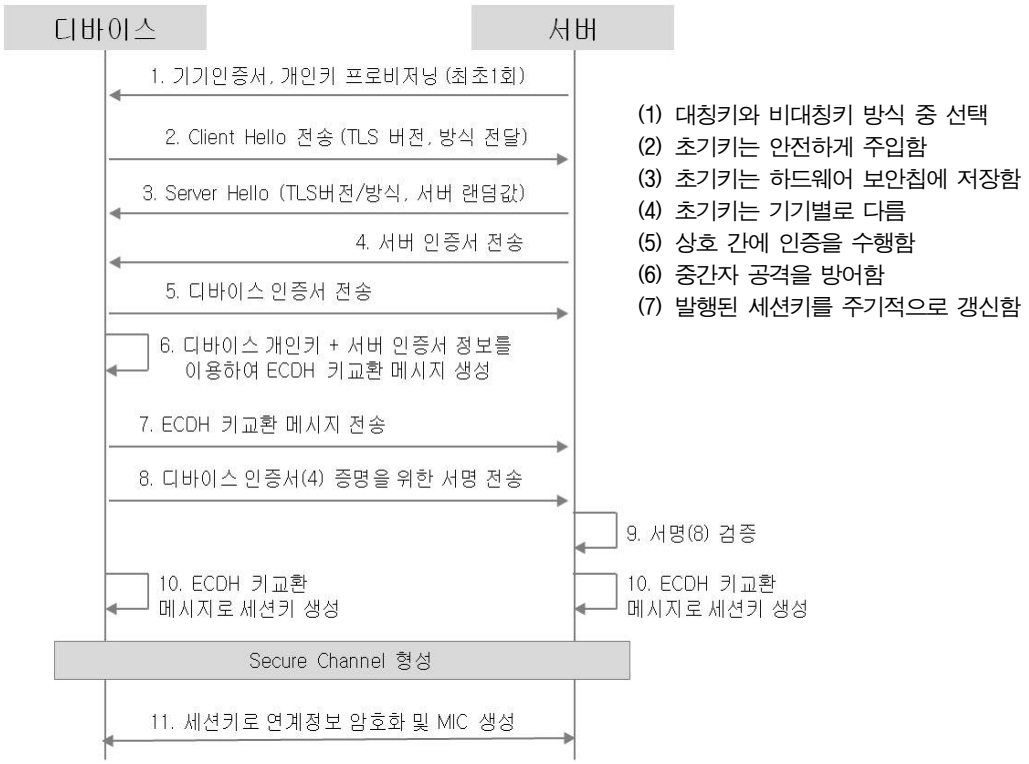
[그림 3] IoT 제품 및 서비스의 전주기 단계별 보안 고려사항

전에 비해 50% 이상 취약점이 감소하였다고 발표했다.

2. IoT 서비스 보안

가. 상호 인증

기기는 서버를 인증하고 서버는 기기를 인증해야 한다. TLS(Transport Layer Security), PSK (Pre-shared key), UICC(Universal IC Card) 등의 기술이 있으며 [그림 4]와 같이 구현해야 한다.

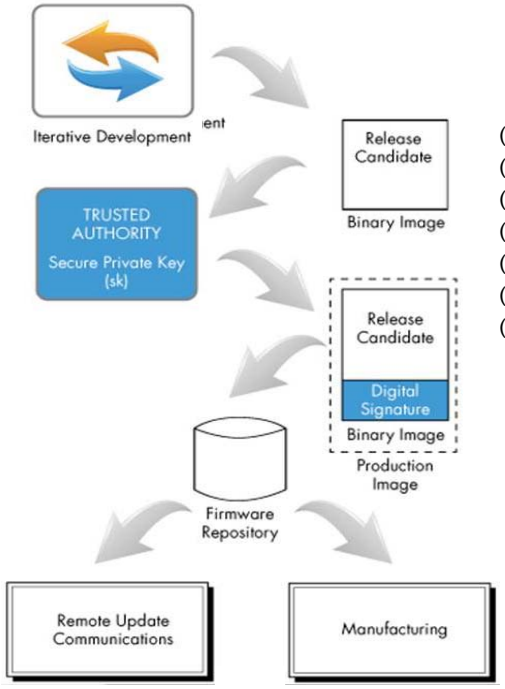


<자료> LG CNS, IoT 보안 상호 인증 업무 흐름도, 2016. 12.

[그림 4] 상호 인증 흐름(예시)

나. 안전한 펌웨어 업데이트

IoT 기기 소프트웨어의 보안 취약점이 발견되면 체계적이고 신뢰할 수 있는 방법으로 보안 패치를 적용할 수 있어야 한다. 애플리케이션 업데이트에는 [그림 5]와 같은 기술이 필요하다.



(1) 원격에서 펌웨어 업데이트 기능 제공
(2) 주기적인 패치 제공
(3) 펌웨어 파일을 서버에 등록 시 암호화 및 서명
(4) 암호화 및 서명 시 안전한 암호 알고리즘 사용
(5) 상호 인증에 성공한 기기만 다운로드 허용
(6) 암호화된 연결을 통해 업데이트할 펌웨어 전송
(7) 가능한 시큐어 부팅과 연결

<자료> Loren K. Shade, “Secure Remote Firmware Updates”, Allegrosoft, May 2011, p.7.

[그림 5] 안전한 원격 펌웨어 업데이트 구현

3. IoT 기기 보안

가. 하드웨어 보안

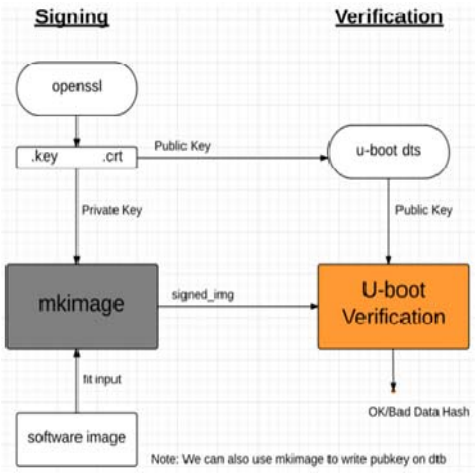
소프트웨어로 생성된 키는 주로 기기의 메모리(NVRAM)에 저장되기 때문에 해킹을 통해 유출될 가능성이 있다. 이 같은 소프트웨어 기반 보안 방식의 구조적인 문제점을 보완하기 위해 등장한 것이 하드웨어 기반 보안 방식이다. SE(Secure Element)에 해당하는 물리적 복제 방지 기능(PUF), 신뢰 플랫폼 모듈(TPM), 보안 MCU, USIM 에서 이러한 하드웨어 보안을 제공한다. 기기에 보안 칩을 장착하여 일차적으로 안전성을 확보하고, 이후 소프트웨어들이 실행되면서 이상이 없는지를 확인하여 키 관리 문제를 근본적으로 해결한다.

나. 부팅 및 실행 전 소프트웨어 위·변조 탐지

기기 부팅 및 실행 전 서명 검사를 통해 해킹이나 악성코드 침투에 의한 소프트웨어 위·변조를 근원적으로 방지해야 한다. 구현 방식은 다양하나 한 예로 서명 생성은 개인키로 하고

서명 검증은 공개키로 할 수 있으며, 키를 이용한 서명을 하기 때문에 개인키가 없는 제 3 자는 바이너리 파일을 위·변조할 수 없다.

IoT 기기를 부팅 시 부트로더와 커널 등이 순차적으로 메모리에 로딩되며, 소프트웨어 무결성 검사에 사용하는 순환중복검사(CRC) 또는 해시(hash) 알고리즘은 의도적인 소프트웨어 변조를 방어할 수 없다. 보안 측면의 소프트웨어 위·변조 방지를 위해서는 서명(signature) 방식이 사용되어야 하며 소프트웨어를 로딩하는 시점에서 서명을 검사한 후 실행하는 시큐어 부팅 기술이 적용되어야 한다.



<자료> JagannadhaSutradharudu Teki, Verified RSA Boot on ARM target, U-boot Mini Summit, Oct. 2013.

[그림 6] U-boot verified RSA boot

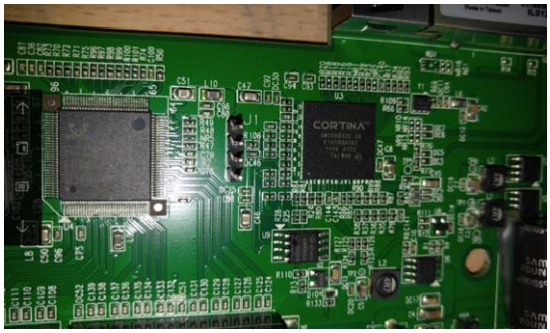
	Security Features					Ease of Management
	Software			Hardware		
	CRC ECC	Hash	Signature	Write Protected Bootloader	TPM	
Normal Boot	O	-	-	-	-	Easy, but no protection
Secure Boot (by digest)		O		Root of Trust (Reference Value)		Bad
Secure Boot (by signature)		O	O	Root of Trust (Signer's public key)		Good + Easy to update OS image without modifying Bootloader
Trusted Boot		O		Root of Trust	Root of Trust (Secure Storage)	Good (for connected device) + Device Authentication + Integrity Protection + Integrity Report

<자료> Steve Johnson, Panasonic, "Trusted Boot Loader", Chair Security WG, April 12, 2006, p.12.

[그림 7] 부트로더의 보안 수준

다. 디버그 포트를 통한 해킹 방지

기기의 디버그 포트를 통해 기기 운영체제의 관리자 로그인에 성공하거나 비밀값을 읽지 못하도록 보안 기술을 적용해야 한다. 기기를 해체 후 인쇄회로기판에 노출된 비동기화 송수신기(Universal asynchronous receiver/transmitter: UART) 포트에 전기적인 무작위공격을 가하더라도



[그림 8] 공유기에 노출된 디버그 포트를 이용한 해킹

반응하지 않도록 응답 차단을 하고, 별도의 하드웨어 장치를 연결하여 비밀키를 송수신한 경우에만 접근이 활성화되도록 해야 한다.

Ⅳ. 결론

IoT 보안을 고려하지 않을 경우 해킹으로 인한 장애, 사생활 감시, 심지어는 안전 문제까지도 발생할 수 있다. 이에 대해 각국은 IoT 제품 및 서비스의 보안 내재화를 위한 IoT 보안 가이드를 발표했으며 정부는 IoT 보안인증제 시행을 2017년 7월 발표하기도 했다.

이제는 이용자 보호, 컴플라이언스 준수를 위해 IoT 보안 준수가 필수 사항이며, 보안을 서비스 기능으로 인식하여 차별화 요소로 가져갈 필요도 있다.

[참고문헌]

[1] 한국인터넷진흥원, “IoT 공통 보안 가이드”, 2016. 10. 6.
[2] 한국인터넷진흥원, “소프트웨어 개발보안 가이드”, 2017. 1.
[3] 한국인터넷진흥원, “홈가전 IoT 보안 가이드(IoT 보안 얼라이언스)”, 2017. 7.
[4] GSMA, “GSMA IoT Security Guidelines - complete document set”, 2016. 2. 9.
[5] JagannadhaSutradharudu Teki, Verified RSA Boot on ARM target, U-boot Mini Summit, Oct. 2013.
[6] Loren K. Shade, “Implementing Secure Remote Firmware Updates”, Allegrosoft, May 2011.
[7] OWASP, “OWASP Internet of Things(IoT) Project”, The OWASP Foundation, 2017.
[8] Steve Johnson, Panasonic, “Trusted Boot Loader”, Chair Security WG, April 12, 2006.
[9] senr.io, JTAG Explained(finally!): Why ‘IoT’, Software Security Engineers, and Manufacturers Should Care, 2016. 9. 28.