IoT 디바이스 보안 점검 기준

정용식*, 차재상**
SK텔레콤*, 서울과학기술대학교**

요 약

최근 IoT 기술이 홈케어, 헬스케어, 자동차, 교통, 농업, 제조업 등 다양한 분야에 적용되면서 신성장 동력의 핵심으로 IoT 서비스를 제공하거나 IoT 환경을 자체적으로 구축하여 산업현장에 도입하려는 기업이나 기관이 증가하고 있다. 그러나 IoT 환경은 인터넷을 통해 현실세계와 IoT 디바이스가 직접 연결되는 특성으로 인해서 IoT 보안의 중요성이 더욱 강조되고 있으며 IoT를 이용한 보안 사고 사례 및 취약점이 지속적으로 발표되면서 IoT 보안 위험 또한 계속 증가되고 있다. 이렇게 IoT 환경에는 많은 취약점과 보안 위협이 존재하기에 IoT 제품의 최초 설계/개발 단계부터 배포/설치/구성 단계, 운영/관리/폐기 단계까지 IoT 제품 및 서비스의 각 단계별로 보안 요구사항과 가이드라인을 적용하여 보안을 내재화하고 IoT 제품 및 서비스를 도입하는 사용자 입장에서 IoT 보안에 대해서 관심을 가지고 스스로 확인 할 수 있도록 보안 점검 기준이 필요하다.

본고에서는 IoT 디바이스의 특성과 보안 요구사항에 따른 보안 원칙 및 보안 가이드를 살펴보고 IoT 기술을 산업현장에 적용하고자 하는 기관/기업에 적용 가능한 IoT 디바이스의 보안 점검 기준을 제시한다.

I. 서 론

IoT(Internet of Things, 이하 IoT) 기술은 사람과 사물, 사물과 사물의 연결을 통해 생활 속 모든 것들을 상호 연결시키는 기술로 모든 유관 사업에 영향을 미치면서 ICT 산업 분야의 새로운 성장 동력으로 각광받고 있다. 글로벌 시장조사 기관인 가트너, ABI리서치 등은 2020년에 250억개 이상의 사물들이 상호 연결될 것으로 전망하고 있으며, ICT 업체인 시스코에서는 500억개 이상의 사물들이 상호 연결될 것으로 전망하고 있다[1]. 그러나 이러한 성장과 더불어 다양한 종류의 수많은 사물들이 상호 연결되어 정보를 교류하게 되는 IoT 환경의 특수성을 고려하면 IoT에 대한 보안의 위협은 현실의 신체적, 물질적 손실로 그대로 다가올 수 있으며 따라서 IoT 제품은 여러가지 다양한 보안 요소가 사전에 고려되고 준비되어야 한다[2].

특히, IoT 디바이스는 그 크기와 비용을 가능한 최소로 유지하려는 경량화, 저비용 특성에 따라 최소 성능만을 유지할 수 있도록 설계되어 제작되고 있으며, 따라서 한 번 제작되어 배포/설치 된 후에는 보안 패치 등의 업데이트가 불가능하거나 고비용이 수반되는 경우가 많기에 최초 설계/개발 단계부터 보안을 내재화하고, IoT 디바이스의 배포/설치/구성 단계에도 취약점이 발생하지 않도록 보안 설정을 갖추어 적용하는 것이 중요하다.

그러나 IoT를 도입하여 산업현장에 적용하고자 하는 기업/기관의 입장에서는 설계/개발 단계부터 배포/설치/구성 단계까지는 IoT 기술에 대한 전문성을 보유한 제조사 및 서비스 제공사의 영역이어서 운영/관리 단계 외에는 IoT 기술에 대한 보안성을 검토하기 어렵다. 따라서 IoT 기술을 도입하려는 사용자 입장에서 산업현장에 적용하는 IoT 디바이스에 대해서 IoT 보안 관련 점검하고 확인할 수 있는 보안 점검 기준이 필요하다.

본고에서는 IoT 디바이스의 등급 분류와 함께 국내에 발표된 IoT 보안 원칙, 보안 가이드에 대해서 알아보고 IoT를 도입하는 사용자가 활용할 수 있는 IoT 디바이스의 보안 점검 기준을 제시하고 결론을 맺도록 한다.

Ⅱ. 본 론

1. IoT 디바이스 플랫폼 계층

IoT 서비스를 구성하는 디바이스 플랫폼은 크게 세 개의 계층(layer)으로 분류를 할 수 있다. 먼저 센서나 액츄에이터 등 사물인터넷의 신경계인 디바이스(Things) 계층, 말단 디바이스의 데이터를 수집하여 인터넷으로 전송하는 게이트웨이 계층, 그리고 수집된 대규모 데이터의 분석 및 처리를 담당하는 서비스 계층으로 구성된다. 각 계층의 설명은 다음과 같다[3][4].

가) 디바이스 계층(Device Layer)

디바이스 계층은 다양한 성능과 기능을 가진 센서 등의 IoT 사물(Things), 즉 디바이스들로 구성되어 있으며 각 디바이스는 다른 디바이스 또는 게이트웨이와 지그비, 와이파이, 블루투스, 무선랜 등 다양한 네트워크 프로토콜을 사용하여 통신한다.

나) 게이트웨이 계층(Gateway Layer)

게이트웨이 계층은 디바이스 계층과 서비스 계층을 연결해주는 서비스를 제공한다. IoT 게이트웨이의 성능 및 기능은 용도에 따라서 다양하게 나타날 수 있다. 단순하게는 디바이스에서 센싱된 정보를 수집하여 전달(bypass)하는 저전력의 경량화 게이트웨이부터 센서들을 관리하고 및 다양한 보안 기능을 제공하는 고사양의 게이트웨이까지 다양하다. 또한 게이트웨이의 형태 역시 전용장비, 기존의 장비(예: 무선공유기, CCTV 등)에 통합된 형태, 또는 스마트 폰 등 디바이스에 게이트웨이 기능 모듈이 탑재된 형태 등으로 게이트웨이의 다양한 구성이 가능하다.

다) 서비스 계층(Service Layer)

서비스 계층은 다양한 IoT 애플리케이션이 수행될 수 있도록 필요한 기능을 제공하는 계층으로 주로 정보 처리 및 정보 저장 기능 등을 포함한다.

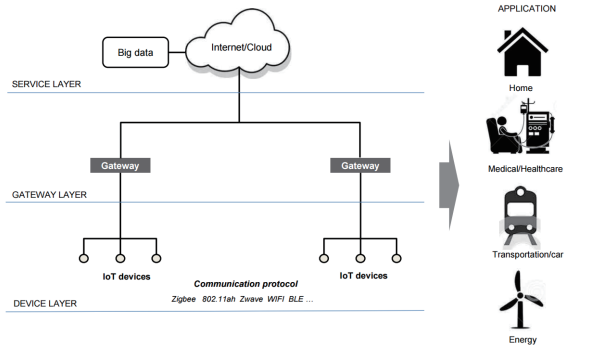


그림 1. IoT 서비스 계층도

2. IoT 디바이스의 기능에 따른 분류

IoT 디바이스는 통신 네트워크에 참여하여 수행하는 기능이나 형태에 따라 데이터 전송, 수집, 센싱 및 엑츄에이팅, 일반 디바이스 등 다음과 같이 네 가지 종류의 디바이스로 분류하고 있다[3][4].

가) 데이터 전송 디바이스(Data-carrying device)

통신 기능이 없는 물리적 사물(Physical thing)에 부착되어 간접적으로 통신 네트워크와 물리적 사물을 연결시켜 데이터를 전송하는 기기로 RFID 태그 등이 해당된다.

나) 데이터 수집 디바이스(Data-capturing device)

물리적 사물과 상호작용 할 수 있는 능력을 가지고 있으며, 읽고 쓰기가 가능한 기기이다. 상호작용은 데이터 전송 디바이스를 통해 간접적으로 일어날 수도 있고, 물리적 사물에 부착된 데이터 전송자(Data carriers)를 통해 직접적으로 일어날 수도 있다. 전자의 경우, 데이터 전송 디바이스의 정보를 읽을 수 있으며, 통신 네트워크를 통해 데이터 전송 디바이스에 지정된 정보를 선택적으로 쓸 수도 있으며 RFID 리더 등이 해당된다.

다) 센싱 및 엑츄에이팅 디바이스(Sensing and Actuating device)

주변 환경과 연관된 정보를 탐지하고 측정하여 디지털 전자신호로 변환하거나, 정보 네트워크로부터의 디지털 전자 신호를 동작(Operations)으로 변환하는 기기이다. 일반적으로 로컬 네트워크 상의 센싱 및 엑츄에이팅 디바이스는 유무선 기술을 이용하여 서로 통신하며, 외부의 통신 네트워크와 연결하기 위해 게이트웨이를 이용한다.

라) 일반 디바이스(General device)

임베디드 프로세싱 및 통신 능력을 갖고 있으며, 유무선 기술을 통해 통신 네트워크와 연결된다. 일반 디바이스는 산업 기계, 가전 제품, 스마트 폰과 같은 다른 IoT 응용 도메인을 위한 기기와 장비를 포함한다.

3. IoT 디바이스의 역량에 따른 등급 분류

IoT 디바이스는 리소스와 프로세싱 능력 등 디바이스의 역량 및 특성에 따라 등급 0부터 등급 3까지 네 가지 등급의 디바이스로 다음과 같이 분류하고 있다[4][5].

가) 등급 0 디바이스

제약이 아주 많은 초소형/초경량/초절전 센서와 같은 디바이스이다. 메모리 및 프로세싱 능력에 제약이 많아서, 안전한 방법으로 직접 인터넷 통신을 하지 못한다. 이러한 디바이스는 통신에 필요한 충분한 리소스를 가지고 있지 않아 게이트웨이 등을 통해서 인터넷 통신에 참여하게 된다. 일반적으로 안전하게 관리되지 못하기 때문에, 사전에 아주 작은 설정 파일을 통해 구성된다. 최소한의 통신 능력만을 가지고 있으며 관리 목적으로 Keep Alive 시그널에 응답하거나 디바이스의 상태정보를 전송할 수 있다.

나) 등급 1 디바이스

리소스 및 프로세싱 능력에 제한을 가지고 있어서, 기존의 통신 프로토콜인 HTTP나 TLS와 같은 프로토콜 스택이 완전하게

적용된 다른 인터넷 기기와 쉽게 통신할 수 없다. CoAP와 같이 IoT 디바이스를 위해 특별히 설계된 제약을 가지고 있는 프로토콜 스택을 사용하기에는 무리가 없다. 대상 디바이스로는 8/16 비트 프로세서를 기반으로 하는 혈당측정기와 같은 의료 헬스 기기, 온도조절기와 같은 스마트홈 기기 등이 있다. 게이트웨이의 도움 없이 다른 디바이스와 통신이 가능하며, 통신 네트워크에서 요구하는 보안 기능 지원이 가능하다. IP 네트워크 통신상의 완전한 피어(peer)로서 통합될 수 있으나, 프로토콜이나 애플리케이션의 사용을 위한 메모리, 코드 스페이스, 전력 소비 등은 가능한 제한할 필요가 있다. 이러한 디바이스에서는 어떤 형태의 애플리케이션을 실행할 수 있는지, 어떤 프로토콜 메커니즘이 적합한지를 이해하는 것이 무엇보다도 중요하다. 메모리 및 다른 리소스 제한으로 인해, 의도적으로 운용에 필요한 몇 가지 선택된 기능만이 지원될 수 있다. 또한, 지원되는 기능은 정적으로 사전에 결정되는 것이 아니라 동적으로 얼마든지 변경될 수 있다.

다) 등급 2 디바이스

기본적으로 기존 통신 프로토콜 스택 지원이 가능하거나 리소스 제약을 거의 받지 않는 디바이스이다. 대상 디바이스로는 32 비트 프로세서를 기반으로 하는 IP 카메라나 스마트 미터기 등을 들 수 있다. 그러나, 이러한 디바이스도 경량화되고 전력 소모가 적고 대역폭이 적은 프로토콜을 사용하는 것이 상당한 이득이 된다. 통신을 위해 보다 적은 리소스를 사용하면 애플리케이션에 보다 많은 리소스를 제공할 수 있기 때문이다. 등급 2 디바이스에서 경량화된 프로토콜 스택을 사용하는 것은 개발 단가를 낮추고, 다른 디바이스와의 상호 운용성을 증가시킬 수 있는 장점이 있다.

등급 1 디바이스와 같이 어떤 형태의 애플리케이션을 실행할 수 있는지, 어떤 프로토콜 메커니즘이 적합한지에 대한 평가가 필요하다.

라) 등급 3 디바이스

등급 2 이상의 능력을 가지고 있는 스마트폰이나 테블릿 같은 디바이스이다. 기존 프로토콜을 사용하는데 변경이나 수정 없이 대부분 기존의 프로토콜을 사용할 수 있다. 리소스 및 프로세싱 능력에 별다른 제약이 존재하지 않으나, 전원 공급에 대한 제약은 여전히 존재한다.

〈표 1〉에 IoT 디바이스의 등급에 따라서 각 디바이스에 일반적으로 적용 가능한 하드웨어의 성능 기준을 표시하였다.

표 1. IoT 디바이스 등급 분류별 성능

구분	디바이스 성능
등급 0	– CPU : 10MHz 이하 – 데이터 : 10KB 이하 – 코드 크기 : 100KB 이하 – 운영체제 : Firmware
등급 1	– CPU : 100MHz 이하 – 데이터 : 50KB 이하 – 코드 크기 : 250KB 이하 – 운영체제 : TinyOS, Contiki, RIOT, NanoQplus
등급 2	– CPU : 500MHz 이하 – 데이터 : 250KB 이하 – 코드 크기 : 1MB 이하 – 운영체제 : embedded Linux
등급 3	– CPU : 1GHz 이하 – 데이터 : 1MB 이하 – 코드 크기 : 5MB 이하 – 운영체제 : Amdroid, iOS, Tizen

4. IoT 디바이스 보안 요구사항

IoT 디바이스의 보안 취약점과 IoT 플랫폼의 개방화를 통한 이기종 단말, 네트워크, 애플리케이션 간의 연동에 따라 새로운 보안 위협이 다양하게 발생하고 있으며, IoT 환경에서 정보 보안의 3대 요소인 기밀성, 무결성, 가용성이 침해될 가능성이 높아지고 있다. 이러한 보안 위험으로부터 사물인터넷 기기를 안전하게 지키기 위한 보안 요구사항을 TTA 표준에서는 다음과 같이 정의하고 있다[5].

가) 기밀성(Confidentiality) 관련 보안 요구사항

[SR-C1] 사물인터넷 기기 간 전송되는 메시지는 불법적인 스니핑(sniffing) 또는 도청 방지를 위해 암호화된 형태로 전송되어야 한다.

[SR-C2] 사물인터넷 기기는 정보유출 방지를 위해 웜, 바이러스와 같은 악성코드 감염이나 외부 해킹 공격을 탐지하고 방어할 수 있는 기능을 제공해야 한다.

[SR-C3] 사물인터넷 기기는 정보유출 방지를 위해 개인정보 및 암호 키와 같은 중요 데이터를 암호화하여 안전하게 처리 및 저장 관리하여야 한다.

[SR-C4] 사물인터넷 기기는 물리적 공격(Physical Attack)으로부터 안전성과 신뢰성을 보장하기 위해 부당 변경 방지(Tamper Resistance) 기능을 제공해야 한다.

[SR-C5] 사물인터넷 기기는 기기 복제 방지를 위해 기기 고유 식별정보가 외부로 유출되거나 변경되지 않도록 안전하게 처리 및 관리해야 한다.

나) 무결성(Integrity) 관련 보안 요구사항

[SR-I1] 사물인터넷 기기는 데이터 위변조 방지를 위해 데이터 무결성 검증 기능을 제공해야 한다.

[SR-I2] 사물인터넷 기기는 펌웨어, 운영체제와 같은 시스템 레벨의 디바이스 플랫폼 무결성 검증 기능을 제공해야 한다.

[SR-I3] 사물인터넷 기기는 부팅 시 소프트웨어에 대한 무결성 검증, 인가된 소프트웨어만이 로드되고 실행되어 기기의 신뢰성을 보장하는 시큐어 부팅(Secure Booting) 기능을 제공해야 한다.

다) 가용성(Availability) 관련 보안 요구사항

[SR-A1] 사물인터넷 기기는 사용자, 시스템, 보안 이벤트에 대한 적절한 로그 기능을 제공해야 한다.

[SR-A2] 사물인터넷 기기는 물리적 제거/파괴 및 비정상적인 설치 시도 방지를 위해 주기적인 Keep Alive 메시지 전송 또는 기기 상태 정보 전송 기능을 제공해야 한다.

[SR-A3] 사물인터넷 기기는 외부 공격자의 지속적인 접속 시도 및 서비스 요청에 대한 서비스 거부 공격과 같은 외부 공격에 대응할 수 있는 기능을 제공해야 한다.

[SR-A4] 사물인터넷 기기는 도난이나 분실, 설치 및 폐기 등에 적절히 대응하기 위한 보안 모니터링 및 보안 관리 기능이 제공되어야 한다.

[SR-A5] 사물인터넷 기기는 안전한 소프트웨어 업데이트 및 보안 패치 기능을 제공해야 한다.

[SR-A6] 사물인터넷 기기는 다양한 형태의 기기에 쉽고 적절한 보안 정책을 안전하게 설정할 수 있는 기능을 제공해야 한다.

[SR-A7] 사물인터넷 기기는 소프트웨어 오류나 악성코드 감염에 의한 오동작 시에도 해당 모듈 분리 및 제거, 접근 권한 제한 등의 기능을 통해 소프트웨어 안전성을 보장해야 한다.

라) 인증/인가(Authentication/Authorization)관련 보안 요구사항

[SR-AU1] 사물인터넷 기기는 비인가된 사용자의 접근을 차단하기 위해 사용자 인증 기능을 제공해야 한다.

[SR-AU2] 사물인터넷 기기는 불법적인 기기의 접근을 차단하기 위해 기기 인증 기능을 제공해야 한다.

[SR-AU3] 사물인터넷 기기는 안전하고 강력한 비밀번호를 설정하고, 주기적인 업데이트 기능을 제공해야 한다.

[SR-AU4] 사물인터넷 기기는 안전하고 자율적인 통신 환경 구축을 위해 기기 간 상호 인증 기능을 제공해야 한다.

[SR-AU5] 사물인터넷 기기는 정보유출 방지 및 프라이버시 보호를 위해 Ownership 제어와 같은 권한 제어 및 설정 기능을 제공해야 한다.

[SR-AU6] 사물인터넷 기기는 불법적인 사용자 및 기기의 접근을 차단하는 접근 제어 기능을 제공해야 한다.

[SR-AU7] 사물인터넷 기기는 기기 복제, 변경, 도용을 방지하기 위한 기기 고유 식별정보 검증 기능을 제공해야 한다.

IoT 디바이스 보안 요구사항은 모든 IoT 디바이스에 공통적으로 제시된다. 그러나 3절에서 살펴본 IoT 디바이스 등급 분류와 같이 리소스와 프로세싱 능력에 차이가 있어서 등급 0부터 등급 3까지의 모든 IoT 디바이스가 보안 요구사항을 완벽하게 충족할 수는 없다. 〈표 2〉는 IoT 디바이스 등급 분류에 따른 보안 요구사항을 보여준다[5].

표 2. IoT 디바이스 등급 분류별 보안 요구사항

구분	보안 요구사항
등급 0	보안 요구사항 2건 적용 [SR-C5]식별정보 관리 [SR-A2]상태정보 전송
등급 1	보안 요구사항 11건 적용 [SR-C1]전송메시지 암호화, [SR-C3]데이터 암호화, [SR-C5]식별정보 관리 [SR-I1]데이터 무결성 [SR-A2]상태정보 전송, [SR-A7]소프트웨어 안전성 [SR-AU1]사용자 인증, [SR-AU2]기기 인증, [SR-AU3]비밀번호 관리, [SR-AU5]권한 제어, [SR-AU6]접근 제어
등급 2	아래 2건 외 보안 요구사항 20건 적용 [SR-C2] 악성코드 대응 [SR-A3] 외부공격 대응
등급 3	보안 요구사항 22건 전체 적용

5. IoT 보안 원칙 및 가이드라인

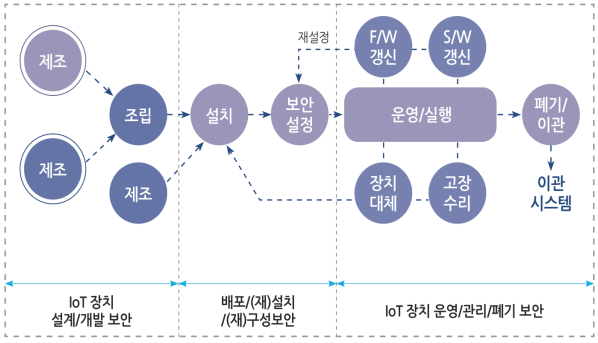
IoT 기술은 다양한 물리 공간의 사물들과 가상 공간의 프로세스 및 데이터들이 인터넷을 통해서 상호 연결되는 초연결사회(Hyper-connected society)가 구축되고, 이를 기반으로 사용자 중심의 지능형 서비스를 제공하기 위해 거대한 정보가 생성, 수집, 공유, 활용되는 광범위한 기술로 IoT 기술의 활성화 및 신규 서비스 창출을 위해 신뢰성을 부여하는 IoT 보안은 반드시 제공해야 하는 핵심요소이다[20].

이에 한국인터넷진흥원에서는 IoT 제조업체, IoT서비스 제공자, 보안업체를 포함하여 업계, 학계, 공공기관 등 약 60여개

기관이 공동으로 참여하는 국내 최초의 민간 자율 IoT 보안 협의체인 "IoT 보안 얼라이언스"를 출범하여 2015년 "IoT 공통 보안원칙"과 "IoT 공통보안가이드"를 발표하여 안전한 IoT 이용환경 조성 기반을 마련하고 있다[6][7].

가) IoT 디바이스 생명주기별 보안 고려사항

IoT 기반의 융합 서비스가 활성화 될수록 서로 다른 기능과 역량을 가진 이기종 IoT 디바이스들이 기하급수로 증가하면서 상호 연동 될 것이기에 기존 시스템 중심으로 설계된 인터넷 보안 기술만으로는 안전과 프라이버시 보호를 수행하기에 무리가 따른다. 따라서 IoT 장치 및 서비스의 '설계-개발' 단계부터 보안과 프라이버시 보호 체계를 고려해야 하고, IoT 장치를 '배포, 설치'하는 단계에서도 사전에 잠재적 보안 위협을 차단할 수 있도록 해야 하며, 실사용이 이루어지는 '설정-운영-실행-폐기' 단계에서는 이 전 단계를 모두 고려하여 전주기적 침해 요소의 분석 및 대응 방안을 마련해야 한다. 〈그림 2〉는 IoT 디바이스의 생명주기별 보안 고려사항을 나타낸다.



※ F/W: Firmware, S/W : Software

그림2. IoT 디바이스 생명주기별 보안 고려사항

나) IoT 공통 보안 원칙

국내 IoT 보안 협의체인 "IoT 보안 얼라이언스"에서는 IoT 장치 및 서비스의 설계부터 운영 및 폐기까지 전체 생명주기에서의 보안 위협과 취약성을 점검하고 보안을 내재화하기 위해서 고려해야 하는 IoT 공통 보안 7대 원칙을 발표하였다.

① 정보보호와 프라이버시 강화를 고려한 IoT 제품 · 서비스 설계
② 안전한 SW 및 HW 개발기술 적용 및 검증
③ 안전한 초기 보안설정 방안 제공
④ 안전한 설치를 위한 보안 프로토콜 준수 및 안전한 파라미터 설정
⑤ IoT제품 · 서비스 취약점 패치 및 업데이트 지속 이행
⑥ 안전 운영 · 관리를 위한 정보보호 및 프라이버시 관리체계 마련
⑦ IoT 침해사고 대응체계 및 책임추적성 확보 방안 마련

다) IoT 공통 보안 가이드

다.1. 설계/개발 단계

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
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

다.2. 배포/(재)설치/(재)구성 단계

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
⑩ 안전성을 보장하는 보안 프로토콜 적용 및 보안 서비스 제공 시 안전한 파라미터 설정

다.3. 운영/관리/폐기 단계

⑪ IoT 제품 · 서비스의 보안 취약점 발견 시, 이에 대한 분석 수행 및 보안패치 배포 등의 사후조치 방안 마련
⑫ IoT 제품 · 서비스에 대한 보안취약점 및 보호조치 사항은 홈페이지, SNS 등을 통해 사용자에게 공개
⑬ 최소한의 개인정보만 수집 · 활용될 수 있도록 개인정보보호정책 수립 및 특정 개인을 식별할 수 있는 정보의 생성 · 유통을 통제할 수 있는 기술적 · 관리적 보호조치 포함
⑭ 다양한 유형의 IoT 장치, 유 · 무선 네트워크, 플랫폼 등에다양한 계층에서 발생 가능한 보안 침해사고에 대비하여 침입탐지 및 모니터링 수행
⑮ 침해사고 발생 이후 원인분석 및 책임추적성 확보를 위해 로그기록의 주기적 저장 · 관리

6. IoT 디바이스 보안점검 기준

IoT 제조사나 서비스 제공자는 설계 단계부터 지금까지 살펴본 보안 요구사항에 따른 보안 가이드를 적용하여 디바이스나

서비스를 개발할 수 있다. 그러나 IoT 기술을 도입하는 기관/기업에서는 제조사나 서비스 제공자가 설계/개발 단계에 보안을 어떻게 적용하였는지 확인이 어렵기에 보안 가이드를 기준으로 IoT 사용자 입장에서 도입하고자 하는 IoT 디바이스에 대한 보안 점검 기준을 다음과 같이 제시한다.

가) 접근권한 관리 및 인증

① 접근 계정 및 권한 확인
- 유지보수 목적으로 제조사 등에서 접속하는 관리자 계정 사용 중지
- 인증된 클라이언트는 타 클라이언트의 데이터에 접근하지 못하도록 권한 관리

② 비밀번호 정책
- 관리자 계정의 모든 디바이스에 공통 비밀번호 사용 금지
- 펌웨어 등 디바이스에 비밀번호 저장 금지
- 특정 횟수 이상 비밀번호 틀리는 경우 계속 시도하지 못하도록 재시도 딜레이 추가

③ 클라이언트 인증
- 인증 없는 정보 요청에는 응답 금지
- 인증 전에는 민감한 정보 평문 전송 금지
- 고유 식별자만을 사용한 디바이스 인증은 금지하고 다른 정보와 함께 인증 수행
- 여러 디바이스와 공통으로 동일한 단말 인증서 사용 금지
- 일정 시간 이후에 인증 세션 종료

나) 종단간 통신 보안 및 데이터 암호화

① 알고리즘 및 적정한 키 길이에 따른 안전성 확인

② 통신구간 암호화는 전구간 TLS 적용 권장

③ salt, iv 사용으로 암호화 안전성 확보

④ 암복호화용 키는 소스코드나 시스템 내부파일 형태로 저장 금지

⑤ 안전한 키관리를 위해서는 하드웨어 기반 보안솔루션 사용 권장

다) 보안 적용 기술 방식 확인

① 적용기술의 안전성 확인
- 적용된 보안 기술 목록 및 안전성 검토 결과 요청
- 암호모듈 검증 또는 CC 인증 여부 확인

② 하드웨어 보안 기법 적용
- 디버깅용 입출력 포트(UART/JTAG 등) 이용 디바이스 내부 shell 연결 및 실행 가능
- IoT 서비스의 특성상 고도의 보안 요구시 시큐어 부트, 펌웨오 코드/암호화, 실행코드 영역 제어 등하드웨어 보안 기법 적용 필요

라) 시큐어 코딩 및 보안 패치

① 시큐어 코딩 적용 여부 확인
- 소스코드 취약점 제거를 위한 시큐어 코딩 적용 여부 확인
- 패치버전의 시큐어 코딩 적용 여부 확인

② 지속적인 보안 취약점 점검 및 패치방안
- 보안 취약점 점검 주기 및 일정 확인
- 안전한 보안 패치 적용 방안

③ 모의해킹을 통한 안전성 검증
- 하드웨어 모듈이나 근거리 통신 프로토콜 공격 등 로컬 해킹에 대한 모의해킹
- 시나리오를 통한 전문 진단인력의 모의해킹
- 모의해킹 취약점에 대한 조치 또는 대응 방안확인

마) 설치 단계 보안 설정

① 초기 설정 값이 가장 안전한 설정이 될 수 있도록 제조사에 단말 초기 설정값 요청

② 사용하지 않는 기능은 기능 비활성화

③ 외부에 오픈된 포트는 최소화

④ 주요 프로토콜의 보안 프로토콜 적용 및 안전한 파라미터 설정

바) 개인정보보호 수집 시 관리 방안 마련

① 개인정보는 수집은 가능한 최소화, 수집 시 가능하면 비식별화

② 개인정보 수집 시 개인정보보호 관리체계 수립 후 기술적, 관리적 보호조치 수행

③ 수집된 개인(민감)정보의 접근관리, 인증, 저장 및 전송 시 암호화 등 보호조치 필요

⑤ IoT 서비스 제공자가 개인정보 수집 시 운영 정책 공개 요구

사) 침해사고 대응 및 책임 추적성 확보 방안

① IoT 서비스는 보안 침해사고에 대비하여 침입탐지 및 모니터링 수행

② 책임추적성 확보를 위해 로그기록 저장 및 관리

③ 다른 시스템에 로그 기록을 남기는 경우 시간 동기화 및 삭제, 위/변조 방지 대책 적용 필요

III. 결 론

본고에서는 IoT 환경에 대한 보안 가이드와 IoT 사용자가 수행 할 수 있는 IoT 디바이스 보안 점검 기준에 대해서 살펴봤

다. 안전한 IoT 환경을 위해서는 제조사, 서비스 제공사, 사용기관/기업 등 관련된 이해 당사자 모두 보안에 관심을 가지고 각자의 역할을 수행해야 한다. 그러나 현재 IoT 환경에서는 제조사와 서비스 제공사 위주의 보안 가이드가 제공되고 있기에 IoT 사용자의 입장에서는 제조사나 서비스 제공자에게 의존하지 않고 자체적으로 보안 관련 사항을 확인하고 점검하기에는 어려움이 많았다. 본고에서 정리한 IoT 디바이스 보안 점검 기준을 기초로 IoT 환경을 도입하는 기관이나 기업에서 IoT 보안에 대해서 제조사 및 서비스 제공사에 적극적으로 요청하고 점검을 수행하면서 안전한 IoT 환경이 구축되길 바란다.

Acknowledgement

본 연구의 일부는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터 육성지원사업의 결과로 수행되었음(IITP-2016-R2718-16-0004)

참 고 문 헌

[1] 한국인터넷진흥원,"IoT 제품 및 서비스 보안성 강화방안 연구", 2015
[2] 이동혁, 박남제,"IoT 제품 보안 인증 및 보안성 유지 관리 방안", 한국통신학회지 33권 12호, 2016
[3] 한국정보통신기술협회, "사물인터넷 정의 및 참조 모델", 2013
[4] 김선태,정종수,송중근,김해용, "IoT 단말 플랫폼동향 및 생태계 구축", 전자통신동향분석 제29권 제4호, 2014
[5] 한국정보통신기술협회, "사물인터넷 기기 등급 분류 및 보안 요구사항", 2016
[6] IoT 보안 얼라이언스, "IoT 공통 보안 가이드", 한국인터넷진흥원, 2016
[7] IoT 보안 얼라이언스, "IoT 공통 보안 원칙 v1.0", 한국인터넷진흥원, 2016
[8] 한국인터넷진흥원, "2017년 7대 사이버 공격 보안 보고서", 2016
[9] 배상태, 김진경, "사물인터넷(IoT) 발전과 보안의 패러다임 변화", 한국과학기술기획평가원 KISTEP InI 14호, 2016
[10] OWASP." IoT Security Guidance" (https://www.owasp.org/index.php/IoT_Security_Guidance)

약 력

정 용 식

1992년 성균관대학교 공학사
2006년 성균관대학교 공학석사
2014년~현재 서울과학기술대학교 정보통신미디어공학 박사과정
관심분야: 융합기술보안, LED-IT 응용기술, IoT, IoT 보안, 개인정보보호기술

차 재 상

2000년 일본 東北(Tohoku)대학교 전자공학과 (공학박사)
2000년~2002년 한국전자통신연구원(ETRI) 무선방송 기술연구소 선임 연구원
2002년~2005년 서경대학교 정보통신학과 전임강사
2005년~현재 서울과학기술대학교 전자 IT미디어 공학과 교수
2008년 미국 Florida University, Visiting Professor
관심분야: LED통신, 조명IT융합신기술, LBS, ITS, UWB, 무선홈네트워크, 무선통신 및 디지털방송 등