국내 IoT 플랫폼 보안에 관한 연구

유진용*, 김영갑*,†
*세종대학교 정보보호학과
e-mail: instrol30@gmail.com , alwaysgabi@sejong.ac.kr

A Study on Security Analysis of Domestic IoT Platforms

Jin-Yong Yu*, Young-Gab Kim*
*Security Engineering Lab., Dept. of Computer and Information Security, Sejong Univ.

요 약

사물인터넷(Internet of Things; IoT)이 차세대 성장동력으로 부상하면서 선진국을 비롯한 많은 단체들이 IoT 육성을 위한 전략을 세우고 있다. 특히 플랫폼(platform)은 IoT의 중요요소기술로 여겨지면서 IoT 플랫폼 보안에 대한 관심은 나날이 높아지고 있다. 현재 국내 IoT 플랫폼('ARTIK', 'Thingplug', 'IoTMakers')들은 oneM2M과 같은 국제표준기술을 기반으로 플랫폼의 다양한 기능을 제공해줌으로서 사용자가 IoT 생태계(ecosystem)에 보다 쉽게 접근할 수 있도록 독려하고 있다. 이렇듯 IoT 플랫폼 기술이 빠른 속도로 성장하고 있는 반면, 국내 IoT 플랫폼들의 보안에 대한 분석이나 연구사례가 거의 없다. 따라서 본 논문에서는 현재 상용화하고 있는 국내 IoT 플랫폼들을 대상으로 보안분석을 수행하고 보안이슈와 보완방안을 시사한다.

1. 서론

사물인터넷(Internet of Things; IoT)이 차세대 성장동력으로 부상하면서 주요 선진국들은 IoT 산업에 대한 적극적 지원을 하고 있으며, 국내에서도 IoT 육성을 위한 전략을 세우고 있다[1]. 일찍이 가트너, 시스코, IDC(International Data Corporation) 등의 기업들은 IoT를 미래의 유망한 기술 중 하나로 선정하였으며[2], IDC는 IoT 시장규모가 2015년부터 2020년까지 연평균15.6%만큼 성장할 것으로 전망했다[3]. 이에 구글 과 아마존, 삼성, 시스코 등의 글로벌 기업들은 IoT 시장을 선점하기 위해 IoT 와 관련된 기술이나 표준, 디바이스 등을 개발하고 있으며, 그 중 IoT 플랫폼은 특히 중요한 기술로 손꼽힌다. 그 이유는 IoT 플랫폼이 가지고 있는 기본적인 기능들을 IoT 디바이스에게 제공해줌으로서 향후, 기하급수적으로 늘어날 것이라고 예측되는 IoT 디바이스들에 직·간접적으로 영향을 미칠 수 있기 때문이다[4]. 이처럼 IoT 플랫폼은 IoT의 핵심기술로 자리 잡고 있으며, 그 중요성이 증대됨에 따라 IoT 플랫폼의 보안에 대한 관심은 나날이 높아지고 있다. 현재 국내의 IoT 플랫폼들은 oneM2M 및 OCF(Open Connectivity Foundation)와 같은 국제표준을 채택함으로서 다양한 디바이스와의 호환성뿐만 아니라 국제표준에서 제공하는 보안기술을 기반으로 IoT 플랫폼의 보안성을 향상시키고 있다. 그러나 저전력, 저사양이라는 IoT가 갖는 제약으로 인하여 기존의 보안방법으로는 급격하게 변화하고 있는 IoT 환경을 보호하기에 역부족한 상황이다[5]. IoT 플랫폼 역시 앞서 서술한 제약성을 지니고 있기 때문에, 이에 적합하고 다양한 보완기술이 적용되어야 할 필요성이 있다. 그러나 현재 국내에서는 IoT 플랫폼에 대한 보안분석 및 연구사례가 거의 없다. 따라서 본 논문에서는 국내 IoT 플랫폼의 보안요소를 분석하고 각 IoT 플랫폼에 대한 보안이슈와 보안방안을 시사하고자 한다. 2장에서는 IoT 플랫폼의 국제표준기술동향과 보안에 관련된 연구들을 소개하고 3장에서는 국내 IoT 플랫폼('ARTIK', 'Thingplug', 'IoTMakers')이 지니고 있는 보안요소를 분석한다. 4장에서는 살펴본 각 IoT 플랫폼의 보안요소를 비교, 분석하여 보안이슈와 그에 따른 보완방안을 시사한다. 5장에서는 결론에 대하여 서술한다.

2. 관련 연구

IoT 플랫폼 기술과 관련된 연구로 최환석 외[6]는 국제 컨소시움(AllSeen Alliance, OCF), 국외 기업(구글, 인텔, 마이크로소프트, 애플 등), 국내 기업(SKT, KT, LG U+)의 각 IoT 플랫폼들이 지니고 있는 기술적 특징 및

† 교신저자

이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2016-0-00498, (창조씨앗2단계)딥러닝 기반 사용자 행동정보 분석을 통한 인증 및 시스템 내 이상행동 탐지 기술 개발)

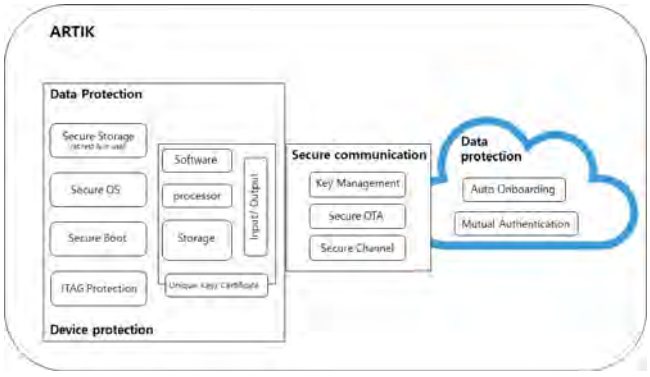
동향을 조사하였다. 김성윤 외[7]는 국제표준인 oneM2M이 IoT 플랫폼에 제공하는 기술요소와 관련된 연구로 oneM2M의 개발에 참여하고 있는 국내·외 기업과 oneM2M 플랫폼에서 제공하는 서비스 기능인 등록 기능, 보안 기능, 네트워크 연동 기능 등을 살펴보았다. Intae Hwang 외[8]는 국제표준기구 및 IoT 보안표준에 대하여 살펴보고 현재 적용되고 있는 IoT 보안의 한계를 시사하고, 안전한 IoT 환경을 구축할 수 있도록 방향을 제시하였다. oneM2M 표준 프로토콜에 관련된 연구로 K. Tang 외[9]는 XMPP(Extensible Messaging and Presence Protocol), CoAP(Contrained Application Protocol), MQTT(MQ Telemetry Transport)를 실시간 커뮤니케이션을 가능하게 하는 필수 프로토콜로서 주목하고, 이를 분석하였다. 전운배 외[10]는 KT의 M2M/IoT 서비스 플랫폼과 관련된 연구로 주요기술을 소개하고 KT가 지향하는 비즈니스 구조에 적합한 기술과 플랫폼을 제시하였다.

3. 국내 IoT 플랫폼 보안분석

현재 국내에서 개발된 IoT 플랫폼에는 삼성의 'ARTIK', SKT의 'ThingPlug', KT의 'IoTMakers'등이 있다. 'Thingplug'와 'IoTMakers'는 국제표준화기구인 oneM2M표준 개발에 참여함으로서, oneM2M의 표준기술을 기반으로 다양한 디바이스와의 호환성을 향상시키고 보다 안전한 통신환경을 조성하고 있다. 'ARTIK'도 또한 국제표준화기구인 OCF의 회원으로 표준개발에 참여함으로서 오픈소스인 'IoTivity' 플랫폼을 기반으로 'ARTIK'의 다양한 IoT 디바이스와 호환성과 보안성을 향상시키고 있다. 이렇듯 국내 IoT 플랫폼들은 국제표준기술을 채택함으로서 기술성과 보안성의 기반을 갖춰가고 있다. 다음은 각 IoT 플랫폼들이 지니고 있는 보안요소에 대한 분석이다.

I. ARTIK

삼성에서 개발한 'ARTIK'은 저전력(low power)을 지향하는 IoT 플랫폼이자 하드웨어, 소프트웨어, 클라우드, 보안, 생태계(ecosystem) 등을 포괄하는 통합플랫폼이다. 'ARTIK'은 디바이스와 애플리케이션, 3rd party cloud에 이르기까지 'ARTIK Cloud'를 통해 데이터의 전송·교환을



(그림 1) ARTIK security architecture

수행한다. 즉 'ARTIK Cloud'를 통해 데이터 통신이 이루어지며, 'ARTIK'은 'ARTIK Cloud'와 통신방법으로 REST(REprsentational State Transfer), Websocket, MQTT(Message Queuing Telemetry Transport), CoAP(Constrained Application Protocol) 프로토콜을 지원한다. 또한 'ARTIK'은 안전한 데이터 통신을 위해 (D)TLS(Datagram Transport Layer Security) 및 산업 표준 암호화 알고리즘을 사용하여 디바이스 및 애플리케이션 간의 통신을 보호하며, 'ARTIK module'은 AES(Advanced Encryption Standard) 및 RSA(Rivest, Sharmir, Adleman) 암호화 및 암호 해독을 위한 암호엔진(crypto engine)을 제공한다. 세션 암호화 키 생성을 위한 방법으로는 ECDH(Elliptic-curve Diffie - Hellman)를 사용하여 IoT가 가지고 있는 제약성인 저전력 환경에서도 높은 수준의 보호기능을 제공한다. 통신보안의 또 하나의 핵심기술인 인증방식으로는 PKI(Public Key Infrastructure)을 채택하고 있다. 'ARTIK'은 통신보안 뿐만 아니라 정당한 사용자만이 자원에 접근할 수 있도록 접근토큰(Access Token)을 이용한 인증방법인 OAuth를 채택하여 적용하고 있다. 내부적으로 'ARTIK'은 최신의 OAuth2를 이용하여 사용자를 인증하고 있으며, 3rd party cloud 등과 같이 외부로부터 접근이 이루어지는 경우 외부에서 지원하는 OAuth 버전에 따라 OAuth1과 OAuth2를 선택하여 인증을 수행한다. 또한 'ARTIK'은 인증의 안전성, 편리성, 환경 등에 따라 접근토큰발급을 위한 다양한 방법을 지원하고 있다. 그 밖에 (그림 1)과 같이 'ARTIK'은 출처가 검증된 소프트웨어만을 하드웨어 플랫폼에서 실행할 수 있으며, 데이터저장소는 삼성에서 제공하는 Secure Element, TrustZone기반의 TEE(Trusted Execution Environment)등의 보안기술을 적용하여 안전한 데이터저장환경을 구축하고 있다.

II. Thingplug

'Thingplug'는 SKT에서 개발한 통신사업체 최초 국제표준 oneM2M 기반의 개방형 플랫폼이다. 통신사업체인만큼 데이터 전달을 위한 통신망의 기능은 중요하다. KT의 'IoTMakers'가 NB(Narrow Band)-IoT 망을 이용하는 것과 달리, 'Thingplug'는 주로 전국적으로 구축이 잘 되어 있는 LoRa(Long Range)망을 이용하여 디바이스와의 통신을 지원하고 있다. LoRa는 통신망 내에서는 데이터의 안전한 통신을 위하여 MAC 프로토콜 처리, AES-128 암호화, ADR(Adaptive Data Rate)등 다양한 보안기능을 제공한다[11]. 'Thingplug'에서 지원하는 자원을 사용하기 위해서 REST API(Application Programming Interface)를 이용하여 접근하게 되는데 통신을 위하여 oneM2M 표준 프로토콜인 HTTP(HyperText Transfer Protocol)와 MQTT를 지원한다. 또한 'Thingplug'는 저사양 장치 및 근거리 통신 프로토콜로 oneM2M 표준에서 지원하고 있는 CoAP을 사용하지 않고, SKT에서 독자적으로 개발한

프로토콜인 GMMP(Global M2M Protocol)을 사용한다. 그 이유는 oneM2M의 사용 사례에 비해 GMMP는 디바이스와 플랫폼 사이의 프로토콜로서 이미 다양한 사용서비스에 활용되었으며, 이를 통해 편리성과 안정성이 입증되었기 때문이다[12]. 또한 보다 안전한 통신을 위하여 TLS를 지원하고 있다. 이 밖에도 'Thingplug'의 보안기능에는 REST API에 정상적인 사용자의 접근인지를 인증하는 uKey라는 개념과 단말에서 접근하기 위해 사용되는 dKey라는 개념이 존재한다. 'Thingplug'에서는 포털에 회원가입을 한 유저 한해서 단말등록을 하여 단말 정보 관련 외부 API 접속 시 uKey를 할당하여 접속할 수 있는 디바이스를 특정한다. dKey는 단말의 논리 정보를 등록하는 remoteCSE가 생성된 경우 response로 dKey가 전달되며 해당값을 이용해 container, contentInstance 등의 자원을 생성한다. 다시 말해서 dKey는 단말의 새로운 자원의 생성 또는 기존 자원의 변경을 위해 사용되는 반면, uKey는 어플리케이션에서 'Thingplug'에 생성된 자원의 정보를 확인 또는 단말 제어를 하고자 할 때 사용하게 된다.

III. IoTMakers

'IoTMakers'는 KT에서 개발한 개방형 IoT 플랫폼으로 사용자들이 쉽게 IoT 생태계에 참여할 수 있도록 다양한 기능을 지원하는 플랫폼이다. 또한 'Thingplug'와 마찬가지로 국제표준인 oneM2M 기술을 적용하였으며 NB-IoT망을 이용하여 통신을 지원한다. 'IoTMakers'는 세계최초로 NB-IoT 기반의 서비스 시연에 성공하였으며 같은 LPWA(Low Power Wide Area)기술을 적용한 LoRa 망과는 다르게 면허 주파수 대역을 사용하여 다른 주파수의 간섭이 거의 없다[13]. 뿐만 아니라, 3GPP(3rd Generation Partnership Project)와 ETSI(European Telecommunication Standards Institute)등과 같은 국제표준기구에서 검증된 보안 솔루션을 사용함으로서 안전한 통신을 제공한다. 'IoTMakers'의 또 다른 특징은 'ARTIK'과 'Thingplug'와는 다르게 플랫폼에서 제공하는 자원을 사용하기 위해서 REST API가 아닌 자체적으로 제공하는 Open API를 통하여 자원에 대한 접근을 시도한다. Open API와의 통신을 지원하는 프로토콜로는 자체적으로 제공하는 표준 I/F(Immunofluorescence) 프로토콜을 사용하거나 oneM2M의 표준 프로토콜인 HTTP와 MQTT를 사용하여 통신한다. 데이터 기밀성을 위한 암호화 방식으로는 AES-128과 AES-256을 지원하며, 각 암호화 알고리즘은 CBC(Cipher Block Chaining)모드와 CTR(Counter)모드를 지원한다. 'IoTMakers'는 통신을 보다 안전하게 지원하기 위해서 TLS 통신방식을 채택하고 있다. 또한 애플리케이션과 디바이스 연동 시, 포털 사이트로부터 인증을 위한 비밀 값(secret)과 디바이스ID(Identifier), 패스워드(password) 등 연동 및 인증을 위한 정보들을 발급 받는다. 사용자 인증의 경우 'ARTIK'과 마찬가지로 접근토큰을 이용한 OAuth 방식으로 정당한 사용자를 인증한다.

4. 국내 IoT 플랫폼 비교분석

IoT 플랫폼의 보안의 중요성이 점차 증대되면서, 국내 IoT 플랫폼들은 국제표준기술을 기반으로 보다 안전한 보안기술을 제공하기 위하여 보안기술 개발에 힘쓰고 있다. 분석한 내용을 표로 정리한 (그림 2) 와 같이 서술한 국내 IoT 플랫폼들은 국제표준기술을 기반으로 개발되었다. 또한 누구든지 IoT 생태계에 참여할 수 있도록 오픈소스(open source)형식을 띄고 있으며 플랫폼 자원에 접근하기 위한 방법으로 API를 지원하고 있다. API와 통신을 위한 프로토콜로는 각 IoT 플랫폼의 국제표준 프로토콜(HTTP, MQTT, CoAP, Websocket)을 사용하거나 자체(SKT, KT)에서 개발·지원하는 프로토콜(GMMP, I/F)을 사용한다. 데이터의 암호화 알고리즘으로는 공통적으로 AES와 RSA를 지원한다. 'Thingplug'에서는 국가표준인(Korean Industrial Standards; KS) ARIA를 추가적으로 지원하며, 'IoTMakers'에서는 ECC(Elliptic Curve Cryptosystem) 암호화방식도 사용한다. 또한 보다 안전한 통신을 위하여 TLS를 이용한 통신방식을 각 IoT 플랫폼에서 공통적으로 적용하고 있다. 데이터의 무결성검증과 인증 및 부인방지를 위한 기술로 'ARTIK'에서는 PKI(Public Key Infrastructure)를 지원하고 있으며, 'IoTMakers'에서도 NB-IoT망 내에서 PKI를 지원하고 있다. 'Thingplug'는 무결성검증과 인증을 위한 기술로 LoRa망 내에서 MAC(Message Authentication Code)을 지원하고 있으며, 부인방지를 위한 기술은 아직 지원하지 않고 있다. 사용자를 인증하는 방법으로는 'ARTIK'과 'IoTMakers'가 공통적으로 OAuth 방식을 채택하고 있으며, 'Thingplug'는 uKey라는 값을 할당받아 사용자인증을

	Main International Standard	Open Source	REST API	Supported Protocols	Cryptography	Secure Communication	Integrity	Non-repudiation	Authentication	Token type
SAMSUNG ARTIK	OCF	Yes	Yes	MQTT CoAP Websocket	AES RSA	SSL/TLS/ DTLS	PKI	PKI	PKI	OAuth
SKT Thingplug	oneM2M	Yes	Yes	HTTP MQTT GMMP	AES RSA ARIA	SSL/TLS/ DTLS	MAC	—	MAC	uKey
KT IoTMakers	oneM2M	Yes	No	HTTP MQTT CoAP	AES RSA ECC	TLS/DTLS	PKI	PKI	PKI	OAuth

(그림 2) Compare platform security factors

수행한다. 이렇듯 국내 IoT 플랫폼은 각 플랫폼이 지닌 보안기술로 안전하게 보호되는 듯 보인다. 그러나 클라우드 기반의 'ARTIK'은 플랫폼의 독립성을 지키기 어려우며 클라우드 기술의 핵심인 가상화로 인한 취약점이 존재한다[14]. 'Thingplug'는 비면허 주파수 대역을 사용하며 Broadcast 전송방식을 가진 LoRa망의 특성에 따른 취약점이 존재한다. 'IoTMakers' 역시 구축이 미흡한 NB-IoT 망과 oneM2M의 자원을 한정적으로 지원[15]하는 것으로 인한 보안 취약점이 존재한다. 따라서 외부로부터 공격이 취약한 클라우드 특성상 'ARTIK'은 인증에 대한 절차나 환경 등을 더욱 강화할 필요가 있으며 서버에 대한 보안 강화 및 데이터 트래픽 제어에 관심을 기울여야 한다[16]. 'Thingplug'는 현재 비면허 주파수 대역 사용과 Broadcast 방식을 이용하여 야기되는 취약점을 LBT(Listen Before Talk)을 지원하여 보완하고 있으나 문제가 해결된 것이 아니므로 보다 안전한 통신망을 이용하는 것이 바람직하다. 뿐만 아니라 'Thingplug'가 자체 개발한 GMMP 프로토콜의 안전성을 상세히 검사하여 최신의 프로토콜과 비교하여 선택하는 것을 권장한다. 'IoTMakers'는 oneM2M의 리소스를 더욱 폭넓게 지원할 수 있도록 인터페이스를 구축해야 하며, 미완성된 NB-IoT 망에서의 통신은 통신의 취약점을 보완할 수 있는 기술을 적용하여 보다 안전한 통신이 이루어질 수 있도록 해야한다. 그러나 결국 서술된 IoT 플랫폼들과 같이 독자적으로 개발된 플랫폼은 타 플랫폼과 연동하는데 있어 한계성을 갖는다. 향후 모든 자원이 공유되는 초연결사회에 따른 플랫폼연동은 불가피한 일이며, 연동과정에서 서로다른 플랫폼의 특성으로 인한 취약점이 발생하는 것 또한 불가피하다. 따라서 서로다른 플랫폼을 연동하기 위해 플랫폼의 특성을 통합시킬 수 있는 보안표준이 요구되며, 보안표준은 플랫폼 특성에 따라 다양한 보안기능을 제공할 수 있어야 한다.

5. 결론

본 논문에서는 급격하게 성장하고 있는 IoT 산업에 따라 IoT 플랫폼보안의 중요성이 증대되고 있는 이유에 대하여 언급하고 국내 IoT 플랫폼의 보안요소를 분석하였다. 각 IoT 플랫폼의 보안기술은 대게 공통적인 방식을 채택하고 있었으나 플랫폼의 기반, 통신환경, 용도 등에 따라 지원하는 보안방법에 다소 차이를 보였다. 그에 따라 플랫폼마다 각기 다른 취약점이 발견되었고, 4장에서는 발견한 취약점을 시사하고 간략한 보안방안을 제시하였다. 현재 IoT 산업은 국가적 차원에서 지원을 받을 만큼 크게 성장하였으며, 취약점은 앞으로 발전하는데 있어 치명적인 악재로 다가올 수 있다. 따라서 본 논문에서 분석한 결과를 토대로 IoT 플랫폼에 필요한 보안기술을 적용하여 보다 안전한 IoT 기술성장이 이뤄지길 기대한다.

참고문헌

[1] IITP "IoT 현황 및 주요 이슈," http://www.kosta.or.kr/mail/2015/download/ICT_Insight_04_IoT.pdf

[2] Se-Ra Oh, Young-Gab Kim "Security Requirements Analysis for the IoT," *IEEE 2017 Platform Technology and Service(PlatCon)*, pp.1-6, February 2017

[3] IDC (International Data Corporation), "Worldwide Semiannual Internet of Things Spending Guide," https://www.idc.com/ getdoc.jsp?containerId=IDC_P29475

[4] Se-Ra Oh, Young-Gab "Interoperable Security Framework for Heterogeneous IoT Platform," KIPS Tr. Comp. and Comm. Sys, Vol.7, No.3 pp.81~90

[5] AhnLab, "IoT 플랫폼에서의 보안 해결책은?," http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=25437

[6] 최환석, 이우섭 "사물인터넷 플랫폼 기술 및 국제 표준화 동향," 방송과 미디어, 20(3), 8-30

[7] 김성윤, 김기영. "oneM2M 사물 인터넷 플랫폼 기술 동향." 정보과학회지, 32.6 (2014.6): 31-36

[8] Intae Hwang, Young-Gab "Analysis of Security Standardization for the Internet of Things," *IEEE 2017 Platform Technology and Service(PlatCon)*, pp.1-6, February 2017

[9] Konglong Tang, Yong Wang, ,Hao Liu ,Yanxiu Sheng, Xi Wang, Zhiqiang Wei "Design and implementation of push notification system based on the MQTT protocol," International Conference on Information Science and Computer Applications (ISCA 2013)

[10] 전운배, 백송훈. "KT의 M2M/IoT 서비스 플랫폼." 한국통신학회지(정보와통신), 30.8 (2013.7): 40-45

[11] 이리나, 이가람, 김호원. "LoRa 기술 분석." 한국통신학회 학술대회논문집, (2017.6): 217-218.

[12] 고가람, 안홍범, 김규백, 이종은, 이상민, 이재한 "Thingplug로 시작하는 IoT 서비스개발," http://thingplug.github.io/img/ThingPlug로_시작하는_IoT_서비스_개발_Sample.pdf

[13] 서 석, 신은정, 조권도 "협대역 사물인터넷 기술동향," Electronic and Telecommunications Trends pp.11-20 31권 5호 (통권 161)

[14] 김지연, 김형종, 박춘식, 김명주. "클라우드 컴퓨팅 환경의 가상화 기술 취약점 분석연구." 정보보호학회지, 19.4 (2009.8): 72-77.

[15]GIGA IoTMakers "oneM2M protocol 연동가이드," file:///C:/Users/instr/Downloads/oneM2M%20protocol%20연동가이드_v1.1.0.pdf

[16]김태형, 김인혁, 민창우, 엄영익. "클라우드 컴퓨팅 보안 기술 동향." 정보과학회지, 30.1 (2012.1): 30-38