편집위원 : 이임영 (순천향대학교)

사물인터넷 보안 표준화 동향

김영갑, 황인태
세종대학교

요 약

최근 다양한 산업 분야에서 사물인터넷(Internet of Things; IoT)에 관련된 연구가 활발히 진행되고 있다. 기존 네트워크 환경에서와 같이 IoT 또한 다양한 보안 공격으로부터 노출 되어 있으며, 여러 가지 보안 이슈가 존재한다. IoT 환경에서는 디바이스, 플랫폼, 통신프로토콜의 이종성 문제로 인하여 공통의 보안 서비스 제공이 힘들게 되고 이를 해결하기 위하여 상호운용성 제공이 가능한 표준이 필요하게 된다. 본고에서는 다양한 보안 이슈들로부터 안전한 IoT 환경 구축을 위하여, IoT 보안 관련 국내외 표준화 기관를 분석하고, 각 기관에서 제시하고 있는 IoT 보안 관련 표준 및 표준화 동향을 분석하고자 한다.

Ⅰ. 서 론

사물인터넷(Internet of Things; IoT)은 인간과 사물, 그리고 서비스를 상호 연결해주는 기술로, 인간, 사물, 서비스가 주요 구성요소로 서로 상호작용을 하게 된다. IoT는 구성요소가 단순히 상호작용 하는 것뿐만 아니라, 정보를 환경으로부터 얻고 이 정보를 원하는 사용자에게 맞추어 의미 있는 정보를 만들어 주기도 한다. 또한 보안, 인증 등 다양한 기능이 IoT의 서비스 인터페이스 기술을 통하여 제공된다[1]. 최근 IoT에 관련된 연구가 의료분야, 자동차, 주택 분야 등 여러 산업 분야에서 활발히 진행 되고 있으며, IoT 관련 상품들도 등장하였다. 이와 같이 IoT에 대한 관심이 고조 되고 있는 가운데, 기존의 네트워크 환경에서 가능했던 DoS (Denial of Service), 트래픽 분석, 도청, 변조, 중간자 공격 외 다수의 공격 또한 IoT 환경에서도 시도 할 수 있다[2].

IoT가 여러 분야에서 관련 연구 및 개발이 활발해 지는 만큼 IoT 환경에서의 보안은 날로 중요성이 부각되고 있다. 보안 문제 해결을 위한 관심과 노력이 증가하고 있고, 이에 따라 표준화에서도 단순히 기술적인 내용 만이 아닌 보안 관련 내용이 제정 및 논의 되고 있다[3]. 하지만, IoT에 대한 관심의 증가에 따라IoT 관련 표준화 동향 분석에 대한 연구가 많이 진행되는 반면 IoT 보안 관련 표준 분석에 대한 연구는 거의 없다. 이에 본고에서는 안전한 IoT 환경을 만들기 위한 여러 표준화 기구의 IoT 보안 표준화에 대한 내용을 분석하고자 한다.

본고의 구성은 다음과 같다. 제2장에서는 표준화와 표준화 기관에 대해 기본적인 배경지식을 기술하고, 제3장에서 IoT 표준과 관련한 표준화 기구에 대해 설명한다. 제4장에서는 3장에서 언급한 표준화 기관에서 제정한 IoT 보안 관련 표준을 분석하고 종합한다. 마지막으로, 제5장에서는 본고의 내용들을 정리하며 결론 짓는다.

Ⅱ. 표준 및 표준화 기관 분류

1. 표준 및 표준화 개념

일반적으로 표준이란 “합의에 의해 작성되고 공인된 가관에 의해 승인된 것으로서 주어진 범위 내에서 최적 수준의 성취를 목적으로 공통적이고 반복적인 사용을 위한 규칙, 지침 또는 특성을 제공하는 문서”로 정의하고 있다[4]. 보다 세부적으로, 정보통신 분야에서의 표준이란, “통신망으로 연결되어 있는 각종 정보시스템이 다양한 형태의 정보통신 서비스를 제공하거나 이용하는 데 있어 필요한 통신 주체간에 합의된 규약(protocol)과 이러한 규약의 집합”을 의미한다[5]. 이러한 정보통신 표준은 효율적인 정보의 생산과 이용을 가능하게 한다. 정리하자면, 사전에 약속된 내용이 표준(standard)이며, 약속을 하는 절차 또는 활동이 표준화(sandardization)이다

과거에 표준화는 시스템 간의 상호호환성(interoperability) 보장, 서비스 간 연동, 소비자 편익 제고 등 기술적인 측면에서 그 역할이 중요시되었으나, 근래에는 표준화가 초기시장 장악을 통한 국제 시장 선점이라는 전략적 수단으로 강조되고 있다. 아울러 표준화는 특허기술의 반영을 통해 기업의 이익을 극대화 · 다양화하는 수단으로 활용되고 있기 때문에 국가 및 기업

에게 있어 중요한 활동이다.

IoT 기술의 발전에 따라 여러 기업에서 다양한 장비와 서비스가 개발되고 있으며, 이들 간에 상호운용성 문제가 크게 부각되어 장비와 서비스의 보급과 이용의 제약으로 이어졌다. 이에 각 표준화 기관들이 이러한 문제들을 해결하기 위한 표준을 제시하고 있으며, 이를 따르는 개발자들은 서로 다른 제품들과 서비스들 간의 상호호환성을 통한 기술의 조화 및 효과적인 이용을 기대하고 있다.

2. 표준 및 표준화 기관 분류

표준의 종류는 표준화의 참여범위, 표준화의 진행정도, 표준의 구현정도, 표준의 적용방법, 표준제정기구에 따라 분류할 수 있으나 [5], 본고에서는 가장 일반적으로 사용하는 표준화의 참여 범위에 따라 표준 및 표준화 기관을 분류하고자 한다. 표준은 표준화의 참여범위에 따라서 국제표준, 지역표준, 국가표준, 단체표준, 사내표준으로 나뉜다. 이에 따라 표준화 기관도 국제표준화 기관, 지역표준화 기관, 국가표준화 기관, 단체표준화 기관, 사내표준화 기관으로 분류할 수 있다. 국제표준화 기관은 전 세계 대부분의 국가가 참여하여 표준을 도출하는 기구이며, 지역표준화 기관은 어느 특정 지역의 소속된 국가들이 표준을 제정하는 기구이다. 국가표준화 기관은 국가 내의 이해당사자들 (특정 기관 및 조직)하에 표준을 제정하는 기구이고, 단체표준화 기관은 국가 내의 표준화 단체와 같은 기구를 의미 한다. 마지막으로 사내표준화 기관은 제품 및 서비스를 제공하는 입장에서 표준을 제정하는 기업이나 기업 얼라이언스(alliance)를 말한다. 이와 더불어 표준은 표준제정기구에 따라 공식표준(de jure standards)과 사실상표준(de facto standards)으로 구분된다. 공식표준은 통상적으로 공식 표준화 기관에서 제정한 표준을 말하며, 사실상표준은 포럼이나 컨소시엄 등 비공식 표준화 기구에서 만들어져 공식표준과 같은 효력을 가지고 있다. 앞서 언급한 데로, 본고에서는 표준화의 참여범위에 따른 표준 및 표준화 기관에 기반하여 IoT 보안 표준 및 표준화 기관에 대하여 분석하고자 한다.

Ⅲ. 사물인터넷 표준화 기관

1. 국제표준화 기관

가. ITU-T

ITU-T(International Telecommunication Union-Telecommunication) [6]은 국제 전기 통신 연합 부문의 하나로 통신 분야의 표준을 제정하는 대표기관으로, 2005년부터 IoT 표준을 제정하는 최초의 기관이다. ITU-T의 TSAG (Telecommunication Standardization Advisory Group) 하부에 IoT 표준 개발을 조율하는 JCA-IoT (Joint Coordination Activity on Internet of Things)를 설치하고 IoT 표준 개발을 목적으로 Io-GSI를 구성하였다. ITU-T FG M2M (Focus Group on the M2M Service layer)에서 M2M 서비스 계층에 대한 요구 사항 및 구조에 대한 표준을 개발 중이며 M2M 상호운용 표준 개발을 하는 SG(study group)11, 차세대 네트워크를 관련 개발하는 SG13, 멀티미디어 서비스 표준을 개발하는 SG16이 FG M2M을 지원하고 있으며, 보안 관련 표준을 개발하는 SG17도 IoT 표준 개발을 지원하고 있다.

나. ISO/IEC JTC1

ISO/IEC JTC1 [7]은 ISO(International Organization for Standardization)와 IEC(Independent Electrotechnical Commission)의 합동 기술위원회(joint technical committees 1)로 1987년에 설립된 표준화 기구이다. JTC1 내에서는 SWG(special working group)5가 IoT 관련 표준 개발 독려 및 관련 업무 조율 등 코디네이션 역할을 수행하고 있으며, 센서 네트워크(sensor network)를 다루는 WG(working group)7, 빅 데이터를 다루는 WG9, IoT를 다루는 WG10, 보안 기술을 다루는 SC(sectional committee)27이 IoT 표준 개발에 참여하고 있다.

2. 지역 표준화 기관

가. ETSI

ETSI(European Telecommunications Standards Institute) [8]는 회원사의 요구에 부응하는 기술표준 개발과 유럽시장 단일화에 따른 정보통신 관련 분야에 요구되는 표준을 개발하고, 세계 정보통신 표준의 제안 및 촉진에 기여함과 동시에 세계 표준의 사전 구축을 목표로 1988년에 설립되었다. ETSI의 M2M (Machine to Machine) 표준 스펙은 OneM2M의 기초가 된다.

3. 단체 표준화 기관

가. IEEE-SA

IEEE(Institute of Electrical and Electronics Engineers) Standard Association(IEEE-SA) [9]은 IEEE내 IoT 기술들을 비롯한 다양한 분야에 대한 표준 및 실험인증과 관련된 프로젝

트를 진행하고 있다. 2014년에 IEEE IoT Community [10]를 만들어 IoT 구조 작업을 시작했으며, 프로젝트 그룹인 P2413 [11]을 통하여 관련 표준개발에 박차를 가하고 있다. IEEE에서 개발하고 있는 IoT 관련 표준은 무선랜, 지능형 차량, 유비쿼터스 네트워크, 스마트 그리드, 의료 기기 등 다양한 분야에서 사용되어질 수 있는 기술들을 지원하고 있다[12].

나. 한국정보통신기술협회(TTA) 및 사물인터넷 포럼

국내에서는 한국정보통신기술협회(TTA) [5]를 중심으로 사물인터넷 기술의 표준화가 진행 되고 있다. TTA는 OneM2M 대표 표준 기관으로 표준 개발 및 확산에 노력하고 있다. 국내에서는 TTA외에 사내표준화 기관으로 사물인터넷포럼 [13]이 있다. 사물인터넷포럼은 SKT, KT, ETRI, KISDI, KETI 등의 기관들이 참여하고 있으며 IoT 기반 IT 서비스 확산과 기술 개발 촉진을 목표로 하고 있다. 하지만, 아직 특별한 활동을 보이지 않고 있다.

4. 사내표준화 기관

가. IETF

IETF(Internet Engineering Task Force) [14]는 오픈 국제 커뮤니티로 인터넷 관련 표준을 제정 하며, IETF의 작업은 워킹 그룹(working group)에 의해 진행 된다. IoT 관련 표준으로 6LoWPAN (IPv6 over Low power Wireless Personal Area Network-Overview)과 IoT 통신에 많이 쓰이는 CoAP(Constrained Application Protocol)을 개발하였다. CoAP은 CORE WG에서 개발하였으며 ETSI, OneM2M 등에서도 관련 표준을 개발하고 있다.

나. OneM2M

OneM2M [15]은 M2M/IoT 표준화 기관으로 ETSI, 미국의 TIA(Telecommunications Industry Association), ATIS(Alliance for Telecommunications Industry Solutions), 일본의 ARIB (Association of Radio Industries and Business), TTC (Telecommunications Technology Committee), 중국의 CCSA (China Communications Standards Association), 한국의 TTA에 의해 설립되었다.

OneM2M은 오직 IoT 한 분야에 특화되어 표준을 개발하는 단체이며, 회원사나 다른 여러 업체에서 oneM2M 표준 기술을 적용하여 개발된 솔루션 및 서비스도 시연하고 홍보를 진행하고 있다. 대표적인 WG으로는 IoT 서비스의 요구사항 관련 표준을 제정하는 WG1, 네트워크 아키텍쳐와 그 구성 엔티티에 관한 표준을 제정하는 WG2, HPPT, CoAP, MQTT 등의 IoT에 활용되는 프로토콜 관련 표준을 제정하는WG3, 보안 관련 표준을 제정하는 WG4가 있다.

다. OGC

OGC (Open Geospatial Consortium) [16]는 정부기관, 기업 및 비영리기관들로 구성된 국제표준화기구로서 공간정보를 기반으로 하는 다양한 형태의 표준을 개발하고 있으며, 개발된 표준의 상당수는 관련 산업분야에서 활발히 사용되고 있다. IoT 관련 하여 SensorThings API 표준문서를 발간하여, 현재 IoT 통신프로토콜로 사용되고 있는 CoAP, 6LoWPAN 등을 보완한다.

라. AllSeen과 OIF

AllSeen Alliance [17]는 오픈소스 IoT플랫폼AllJoyn을 제공한 퀄컴인코퍼레이티드와 LG, 파나소닉, AT&T 등의 회사로 이루어져 있으며 개발한 표준이 AllJoyn을 통해 확산하는 것을 추진하고 있으며 최근에는 oneM2M과 연계하여 표준을 제정하였다.

OIF(Open Interconnect Foundation) [18]은 인텔, 브로드컴, 델, 삼성전자 등의 회사가 각 사의 제품 간에 무선통신 정보 공유가 가능하도록 통신 방법을 개발하고 실생활에서 사용하는 전자기기 통신용 오픈소스를 공개를 추진할 목적으로 설립되었다. AllSeen Alliance에 대항하는 Alliance이며 AllJoyn과 마찬가지로 최근에 OneM2M을 통해 표준을 제정하였다.

Ⅳ. 사물인터넷 보안 표준 분석

제3장에서 IoT 관련 표준화 기관을 살펴보았고, 본 장에서는 IoT 보안 관련 표준 문서들에 대해 분석하고자 한다. 앞서 살펴보았듯이, IoT와 관련하여 많은 표준화 기관들이 표준을 제정하고 있지만, 본고에서는 표준화 활동이 활발한ITU-T, ISO/IEC JTC1, IETF, ETSI, OneM2M 등 5개 표준화 기관을 대상으로 IoT 보안 관련 표준들을 살펴 보고자 한다.

1. 국제 표준

가. ITU-T

ITU-T에서 제정한 IoT 보안 관련 표준은 〈표 1〉에서와같이 F, X, Y Series에서 나타난다.

F Series는 "NON-TELEPHONE TELECOMMUNICATION SERVICES"에 관한 내용을 담고 있으며, 이 중F.748 [19]에 IoT어플리케이션 보안 요구사항과 개인정보 보호 등의 내용을

담고 있다.

X Series는 "DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY"에 관한 표준으로,이 중 X.650 ~ X.579는 "OSI NETWORKING AND SYSTEM ASPECTS - Naming, Addressing and Registration" 을 X.1310 ~ 1339는 "SECURE APPLICATIONS AND SERVICES - Ubiquitous sensor network security"을 포함하고 있다. X.675 [20]와 X.1314 [21]에 IoT 관련 프레임워크(framework)의 인증과 권한 부여, 그리고 통신 주체들의 보안에 관한 내용을 담고 있다.

Y.4700 ~ 4799는 "INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES - Management, control and performance"에 관한 표준으로, Y.2060 [22], Y.2063 [23], Y.2066 [24], Y.2067 [25], Y. 2068 [26], Y.2075 [27], Y.4111/Y.2076 [28], Y.4112/Y.2077 [29], Y.4552/Y.2078 [30], Y.4553 [31], Y.4702 [32]에 IoT 보안 관련 내용을 담고 있다. IoT의 전반적 보안요구사항부터 IoT플랫폼, 게이트웨어, 어플리케이션 등이 갖추어야 할 보안 요구사항 (보안 및 프라이버시, 인증, 권한부여, 접근제어, 보안 운영 등) 등의 내용을 포함하고 있다.

나. ISO/IEC JTC1

ISO/IEC에서는 ISO/IEC 30128에 IoT 보안 관련 내용을 포함하고 있으며, 일반적인 센서 네트워킹에서 네트워크 어플리케이션 인터페이스에 관련한 보안 고려사항이 기술되어 있다. JTC1 WG10, SC32에서 관련 표준 작업을 진행되는 것으로 파악되지만, 국제 표준이 되기까지 다소 시간이 걸릴 것으로 예상된다.

2. 지역표준

앞서 언급하였듯이, ETSI의 IoT 관련 표준 문서는 OneM2M 표준의 기초가 되기 때문에 보다 자세한 내용분석은OneM2M 표준문서를 통해 살펴 보겠다.

3. 사내표준

가. IETF

IETF에서는 IoT 무선 통신 프로토콜인 6LoWPAN [33]과 CoAP [34]에 관련하여 이들 프로토콜의 문제점, 통신 상에서의 인증 및 암호화 등에 관련한 보안 요구사항에 초점을 맞추어 표준을 제정하였고, 이를 활용하는 다양한 방법에 관한 방향을 제시하는 내용도 포함하고 있다. 관련 표준 문서는 〈표 2〉에서 요약한 봐와 같이RFC 4919 [33], RFC 6606 [34], RFC 7228 [35], RFC 7252 [36], RFC 7388 [37], RFC 7554 [38], RFC 7641 [39], RFC 7650 [40]이다.

나. OneM2M

OneM2M은 지역 표준화 기구인 ETSI를 필두로 많은 국가 및 단체 표준화 기구들이 파트너 멤버로 참여하고 있다. IoT 기능을 수행하는 아키텍쳐 모델, 그 기능과 거기에 필요한 접근 권한 부여 보안 절차, 서비스 제공자(service provider; SP)와 IoT 디바이스와의 통신, 통신을 위한 인증, IoT 전반적인 보안 요구사항, OMA DM (Open Mobile Alliance Device Management)와 LWM2M(Light-Weight Machine To Machine)과 같은 IoT 기기 관리 기술, CoAP, HTTP, MQTT, WebSocket를 이용한 통신을 위한 인증, 암호화, 권한 부여, 상호운용성 테스트에서 행해야 할 보안 절차에 관한 표준들이 제정되어 있다. 〈표 3 및 4〉는 ETSI 및 OneM2M에서 제정한 IoT 보안 관련 표준의 내용을 요약한 것이다.

다. IoT 보안 표준 분석

〈표 5〉은 앞서 설명한 여러 표준화 문서를 2장에서 분류한 표준화 기구에 따라 정리한 것이다. 공식표준화 기관이며 국제표준기관인 ITU-T에서는 IoT 무선 네트워크와 차세대 네트워크에서의 접근권한, 인증, 인가를 비롯한 보안과 보안된 스마트 어플리케이션에서의 데이터, 개인정보 보호에 관해서 표준들이 제정되어 있다. ISO/IEC JTC1에서는 센서 네트워크를 이용한 어플리케이션에서의 인터페이스 보안에 관한 표준을 제정하고 있지만, 국제 표준에 등록되기까지 많은 시간이 소요되는 특성상 국제표준으로 등록된 문서는 그리 많지 않은 것을 확인할 수 있다.

사실상 표준화 기관이며 사내 표준화 기구에 속하는 IETF에서는 제한된 자원의 디바이스들의 통신으로써의 6LoWPAN과 CoAP에 관하여 보안 관련 표준들이 존재하였으며, ETSI를 필두로 하는 OneM2M은 전반적인 IoT 보안 요구사항, 네트워크 아키텍쳐에 관한 보안, IoT 환경에서의 통신 프로토콜인 MQTT, HTTP, CoAP, WebSocket Binding의 보안, OMA DM, LWM2M과 같은 기기 관리 기술, 그리고 상호운용 테스트에서의 보안에 대한 표준 등을 제정 하였다. 최근에는 AllJoyn, OIC와 각각 협력하여 해당 기업 얼라이언스와의 아키텍쳐에 관하여 표준을 제정하였고, 핵심 내용으로는 접근제어에 관련한 보안 내용이 있다.

표 1. ITU-T의 IoT 보안 관련 표준

Standard	Title	Security-Related Contents
F.748.0	Common requirements for Internet of things (IoT) applications	7 Characteristics of IoT applications 7.14 Security 7.15 Privacy 8 Common requirements for IoT applications 8.7 Security 8.8 Privacy protection
X.675	OID(Object Identifier)-based resolution framework for heterogeneous identifiers and locators	7.8 Support of authentication and authorization
X.1314	Security requirements and framework of ubiquitous networking	6 High-level security framework for ubiquitous networking 7 Security threats and requirements 7.1 Service and transport security domain 7.2 End-user security domain 7.3 UN application security domain 7.4 Other network security domains 7.5 End-to-end connectivity security domain 7.6 Interface security domain Appendix 1.1 3GPP M2M security framework 1.2 oneM2M security framework
Y.2060	Overview of the Internet of things	8.6 Security capabilities
Y.2063	Framework of the web of things	10. Security considerations
Y.2066	Common requirements of the Internet of things	8.8 Security and privacy protection requirements 8.8.1 Communication security 8.8.2 Data management security 8.8.3 Service provision 8.8.4 Integration of security policies and techniques 8.8.5 Mutual authentication and authorization 8.8.6 Security audit
Y.2067	Common requirements and capabilities of a gateway for Internet of things applications	7.7 Security functions support 8.5 Security management related requirements Security and privacy Self-management and remote maintenance 9. Common capabilities of a gateway for IoT applications
Y.2068	Functional framework and capabilities of the Internet of things	8.7 Security and privacy protection capabilities 10 Security considerations
Y.2075	Capability framework for e-health monitoring services	8. Capability framework 8.7 Secure capabilities of EHM(E-Health Monitoring) components
Y.4111/ Y.2076	Semantics based requirements and framework of the Internet of things	8.2.6 Semantics based requirements for the security capabilities 9.7 Security capabilities
Y.4112/ Y.2077	Requirements of the plug and play capability of the Internet of things	6.2.2 PnP security capability 7.2 PnP security capability related requirements 7.2.1 PnP authorization 7.2.2 PnP access control 7.2.3 Firewall protection 7.2.4 Device and application data security
Y.4552/ Y.2078	Application support models of the Internet of things	7.2.5 Configurable security and privacy protection capabilities 10. Security consideration
Y.4553	Requirements of smartphone as sink node for IoT applications and services	6.2.6 Security 8.8 Security and privacy
Y.4702	Common requirements and capabilities of device management in the Internet of things	8.4 Security management capability

표 2. IETF의 IoT 보안 관련 표준

Standard	Title	Security-Related Contents
RFC4919	IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals	4 Problems 4.6 Security
RFC6606	Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing	5 6LoWPAN Routing Requirements 5.4 Support of Security 6 Security Considerations
RFC7228	Terminology for Constrained-Node Networks	5 6LoWPAN Routing Requirements 5.4 Support of Security 6 Security Considerations
RFC7252	The Constrained Application Protocol	9 Securing CoAP 9.1 DTLS-Secured 11 Security Considerations
RFC7388	Definition of Managed Objects for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)	7 Security Considerations
RFC7554	Using IEEE 802.15.4e Time-Slotted Channel Hopping(TSCH) in the Internet of Things (IoT):Problem Statement	4 Security Considerations
RFC 7641	Observing Resources in the Constrained Application Protocol (CoAP)	7 Security Considerations
RFC 7650	A Constrained Application Protocol (CoAP) Usage for REsource LOcation And Discovery (RELOAD)	10 Security Considerations

표 3. ETSI 및 OneM2M의 IoT 보안 관련 표준 (1/2)

Standard	Title	Security-Related Contents
ETSI TS 118 101 V1.1.0 TS-0001-V2.10.0 [41]	Functional Architecture	6 oneM2M Architecture Aspects 6.2 Common Services Functions 6.2.10 Security 6.3 Security Aspects 6.5 Inter-M2M SP Communication 6.5.3 DNS Provisioning for Inter-M2M SP Communication 6.5.3.1 Inter-M2M SP Communication Access Control Policies 9 Resource Management 9.6.2 Resource Type accessControlPolicy 10.2 Resource Type-Specific Procedures 10.2.21 〈accessControlPolicy〉 Resource Procedures 11 Trust Enabling Architecture 11.3 M2M Operational Security Procedures 11.3.2 Authentication and Security Association of CSE and AE 11.3.4 M2M Authorization Procedure
ETSI TS 118 102 V1.0.0 TS-0002-V2.7.1 [42]	Requirements	6 Functional Requirements 6.4 Security Requirements
ETSI TS 118 103 V1.1.0 TS-0003-V2.4.1 [43]	Security Solutions	5 Security Architecture 5.2.2 Secure Environment Abstraction Layer 6 Security Services and Interfaces 6.1 Security Services and Interactions 6.1.2.2 Operation phase 6.1.2.2.2 Authorization to access M2M resources 6.2 Security Service Layer 6.2.1 Access Management 6.2.1.1 Authentication 6.2.2 Authorization Architecture 6.2.3 Security Administration 6.2.4 Identity Protection 6.2.5 Sensitive Data Handling

표 4. ETSI 및 OneM2M의 IoT 보안 관련 표준 (2/2)

Standard	Title	Security-Related Contents
ETSI TS 118 103 V1.1.0 TS-0003-V2.4.1 [43]	Security Solutions	6.2.5 Sensitive Data Handling 6.2.6 Trust Enabler security functions 6.3 Secure Environment Abstraction Layer Components 6.3.1 Secure Environment 6.3.3 Secure Environment Abstraction 7 Authorization 7.1 Access Control Mechanism 8 Security Framework 8.1 General Introduction to the Symmetric Key Security Frame work 8.2 General Introductions to the Certificate-Based Security Framework 9 Security Framework Procedures and Parameters 9.1 Security Association Establishment Framework Procedures and Partners 9.2 Remote Security Provisioning Framework Procedures and Parameters 10 Protocol and Algorithm Details 10.1 Certificate-Based Security Framework Details 10.2 TLS and DTLS Details 10.3 Key Export and Key Derivation Details
TS-0004-V2.7.1 [44]	Service Layer Core Protocol Specification	7 oneM2M procedures 7.5 Primitive-specific procedures and definitions 7.5.1.2 Notification procedures 7.5.1.2.10 Notification for End-to-End Security Certificate-based Key Establishment 7.6 Security Procedures 7.6.2Procedure for applying End-to-End Security of Primitives
TS-0005-V2.0.0 [45]	Management Enablement(OMA)	5 OMA DM 1.3 and OMA DM 2.0 5.5 DM Server Interactions 5.5.4 Access Control Management 6 OMA Lightweight M2M 1.0 6.5 LWM2M Server Interactions 6.5.4 Access Control Management
TS-0007-V2.0.0 [46]	Service Components	6 M2M Services 6.3 Authorization A.2.3 Authentication and Authorization of Requests A.2.3.2 Common M2M Service Capability Parameters for Request Authentication and Authorization
ETSI TS 118 108 V1.1.0 TS-0008-V1.3.2 [47]	CoAP Protocol Binding	6 CoAP Message Mapping 7 Security Consideration
ETSI TS 118 109 TS-0009-V2.6.1 [48]	HTTP Protocol Binding	6 HTTP Message Mapping 7 Security Consideration
ETSI TS 118 110 V1.1.0 TS-0010-V2.3.1 [49]	MQTT Protocol Binding	6 Protocol Binding 7 Security 7.1 Introduction 7.2 Authorization 7.3 Authentication 7.4 Authorization by the MQTT Server 7.5 General Consideration
ETSI TS 118 113 V1.0.0 TS-013-V1.0.0 [50]	Interoperability Testing	5 Testing conventions 5.4 Pre-conditions 5.4.2 Security
TS-014-V2.0.0 [51]	LWM2M Interworking	6.Architecture Aspects 6.6 LWM2M Object Security 6.6.2 LWM2M Interworking Access Control Policy 6.6.3 IPE and Object Security provisioning
TS-020-V2.0.0 [52]	WebSocket Protocol Binding TS	7 Security Aspects
TS-021-V2.0.0 [53]	OneM2M and AllJoyn Interworking	6 Architecture Aspects 6.6 AllJoyn access control mapping
TS-024-V2.0.0 [54]	OIC Interworking	6 Architecture Aspects 6.7 OIC Provisioning and Security 6.7.2 OIC Interworking Access Control Policy

표 5. IoT 보안 관련 표준 요약

Classification		Organization	Contents for IoT Security
By Participation Range	By Authority		
International	De jure	ITU-T	Security Requirements of various IoT Frameworks with Authentication, Authorization, Access Control and Privacy protection Security Management for IoT Data, Privacy protection for Secure IoT application
		ISO/IEC JTC1	Security for Sensor network application interface
Regional	De facto	ETSI	Same as OneM2M
National & Association, and Company		IETF	Authentication, Encryption/Decryption, Authorization and Access Control for 6LoWPAN and CoAP used for resource-constrained devices Security for TSCH, RELOAD
		OneM2M	Security for Functional architecture of IoT with Access Control, Authentication and Authorization Overall Security requirements of IoT IoT Security Architecture with Authentication, Authorization, Access control, TLS and DTLS etc. Authentication, Encryption/Decryption Authorization and Access Control for HTTP, MQTT, CoAP, WebSocket Binding Security for Device Management Technology (i.e., OMA DM, LWM2M) Access Control for Interoperability testing Access Control for AllJoyn and OIC Architecture

표 6. IoT 보안 관련 표준 분류

	Data Confidentiality	Data Integrity	Availability	Non-Repudiation	Authentication	Authorization (Access Control)
ITU-T	F.748.0, X.1314, Y2060, Y.2067, Y.2075, Y4553 Y.4702	F.748.0, X.1314, Y.2060, Y.2066, Y.2086, Y.2075, Y.4112/Y.2077, Y.4552/Y.2078, Y.4702	X.1314	X.1314	F.748.0, X.675, X.1314, Y.2060, Y.2066, Y.2067, Y.2086, Y.2075, Y.4111/Y.2076, Y.4112/Y.2077, Y.4552/Y.2078, Y4553, Y.4702	X.675, X.1314, Y.2060, Y.2063, Y.2066, Y.2067 Y.2086, Y.2075, Y.4111/Y.2076, Y.4112/Y.2077, Y.4552/Y.2078, Y.4702
IETF	RFC 4919, RFC 6606 RFC 7252, RFC 7388, RFC 7554, RFC 7641	RFC 6606			RFC 6606 RFC 7554 RFC 7650	RFC 7252 RFC 7641 RFC 7650
OneM2M	TS-0001, TS-0002 TS-0003, TS-0004 TS-0021	TS-0001, TS-0002, TS-0003, TS-0004, TS-0007	TS-0002, TS-0003	TS-0002, TS-0003	TS-0001, TS-0002, TS-0003, TS-0004, TS-0007, TS-0008, TS-0009, TS-0010, TS-0020, TS-0021,	TS-0001, TS-0002, TS-0003, TS-0004, TS-0005, TS-0007, TS-0008, TS-0009, TS-0010, TS-0013, TS-0014, TS-0021, TS-0024

앞서 언급한 IoT보안 관련 표준들을 X.800 [53]에 정의된 보안 서비스를 기준으로 분석하면 〈표 6〉과 같다. 많은 표준 문서들이 IoT 어플리케이션, 플랫폼 및 통신 상에서의 데이터의 기밀성 및 무결성, 인증, 접근제어 등의 보안 요구사항에 초점이 맞추어져 있다. 반대로 가용성이나 부인방지에 관한 표준화가 부족하며 이에 대한 보다 적극적인 표준화가 필요하다는 것을 의미한다. 이러한 표준을 통하여 디바이스, 플랫폼 및 통신 프로토콜의 다양성에서 오는 이종성을 해결할 수 있을 것으로 기대된다. 하지만, 이와는 별도로, IoT의 자원제약성 및 동적 환경에 적합한 유연하고 확장성이 좋고, 경량화된IoT 보안 기술 개발 및 표준화 등이 보다 시급할 것으로 판단된다.

V. 결 론

최근 다양한 분야에서 IoT에 관련된 연구가 활발하게 진행되고 있다. IoT에서도 보안 이슈는 빼놓을 수 없는 요소이며, 높아진 IoT 보안 요구에 따라 보안 관련 표준이 활발히 개발되고 있는 상황이다. 본고에서는 보안 위협들로부터 대응하기 위한 ITU-T, IETF, OneM2M, ISO/IEC JTC1 등의 여러 표준화 제정 기구의 IoT 보안 관련 표준들을 분석하였다. 국내에서도 IoT 보안에 관한 표준 제정에 힘쓰고는 있지만 국외에 비해 많이 부족한 편이다. 차후 국내에서도 더 많은 IoT 관련 기업 및 기관이 협력하여 IoT 보안 관련 표준 제정을 추진이 필요할 것으로 보인다. 또한, 표준들은 일반적인 IoT 보안 요구사항 및 이를 구현하기 위한 간단한 절차 등을 소개하고 있지만 이를 구현하기 위한 구체적 방법 및 도구를 제시하고 있지 않다. 따라서 IoT 환경에서의 안전한 통신 환경을 구축하기 위한 구체적 방법 및 도구에 대한 연구가 진행되어야 할 것이다.

Acknowledgement

이 논문은 2015년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.B0184-15-1001,글로벌 IoT 연합을 위한 시맨틱 IoT 클라우드 기술 및 공통 테스트베드 한·EU 개발). 또한 본고는 논문 [54][55]의 확장 버전임.

참 고 문 헌

[1] H. Kim, D. Kim, "IoT Technologies and security", Review of KIISC, Vol. 22, No.1, pp. 7-13, 2012.

[2] M. Hossain, M. Fotouhi, R. Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things", IEEE World Congress on Services, New York, USA, pp. 21-28, 2015.

[3] V. Gazis, "A Survey of Standards for Machine to Machine (M2M) and the Internet of Things (IoT)" IEEE Communications Surveys & Tutorials, 2016.

[4] 국가기술표준원, "표준의 정의", http://standard.go.kr

[5] 한국정보통신기술협회(TTA), "표준화의 개요", http://www.tta.or.kr

[6] ITU-T, http://www.itu.int

[7] ISO/IEC JTC 1, http://www.iso.org/iso/jtc1_home.html

[8] ETSI, http://www.etsi.org

[9] IEEE-SA, https://standards.ieee.org

[10] IEEE Internet of Things, http://iot.ieee.org

[11] IEEE P2143, http://grouper.ieee.org/groups/2413

[12] 송재승, "IEEE의 사물인터넷 기술표준 및 글로벌 협력", TTA저널, pp.36-40, 2016

[13] 사물인터넷포럼, http://iotforum.kr

[14] IETF, https://www.ietf.org

[15] OneM2M, http://www.onem2m.org

[16] OGC, http://www.opengeospatial.org

[17] Allseen Alliance, https://allseenalliance.org

[18] OIF, https://openconnectivity.org

[19] ITU-T, "Common requirements for Internet of things (IoT) applications", F.748.0, ed. 1.0, ITU-T, 2014.

[20] ITU-T, "OID-based resolution framework for heterogeneous identifiers and locators", X.675, ed. 1.0, ITU-T, 2015.

[21] ITU-T, "Security requirements and framework of ubiquitous networking", X.1314, ed. 1.0, ITU-T, 2014.

[22] ITU-T, "Overview of the Internet of things", Y.2060, ed. 1.0, ITU-T, 2012.

[23] ITU-T, "Framework of the web of things", Y.2063, ed. 1.0, ITU-T, 2012.

[24] ITU-T, "Common requirements of the Internet of things", Y.2066, ed. 1.0, ITU-T, 2014.

[25] ITU-T, "Common requirements and capabilities of a gateway for Internet of things applications", Y.2067, ed. 1.0, ITU-T, 2014.

[26] ITU-T, "Functional framework and capabilities of the Internet of things", Y.2068, ed. 1.0, ITU-T, 2015.

[27] ITU-T, "Capability framework for e-health monitoring services", Y.2075, ed. 1.0, ITU-T, 2015.

[28] ITU-T, "Semantics based requirements and framework of the Internet of things", Y.4111/Y.2076, ed. 1.0, ITU-T, 2016.

[29] ITU-T, "Requirements of the plug and play capability of the Internet of things", Y.4112/Y.2077, ed. 1.0, ITU-T, 2016.

[30] ITU-T, "Application support models of the Internet of Things", Y.4552/Y.2078, ed. 1.0, ITU-T, 2016.

[31] ITU-T, "Requirements of smartphone as sink node for IoT applications and services", Y.4553, ed. 1.0, ITU-T, 2016.

[32] ITU-T, "Common requirements and capabilities of device management in the Internet of things", Y.4702, ed. 1.0, ITU-T, 2016.

[33] N. Kushalnagar, G. Montenegro, C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) : Overview, Assumption, Problem Statement, and Goals" RFC 4919, IETF, 2007.

[34] E. Kim, D. Kaspar, C. Gomez, C. Bormann "Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing" RFC 6606, IETF, 2012

[35] C. Bormann, M. Ersue, A. Keranen, "Terminology for Constrained-Node Networks" RFC 7228, IETF, 2014

[36] Z. Shelby, K. Hartke, "The Constrained Application Protocol (CoAP)" RFC7252, IETF, 2014

[37] J. Schoenwaelder, A. Sehgal, T. Tsou, C. Zhou, "Definition of Managed Objects for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN)" RFC7388, IETF, 2014

[38] T. Watteyne, M. Palattella, L. Grieco, "Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the Internet of Things (IoT): Problem Statement", RFC7554, IETF, 2015.

[39] K. Hartke, "Observing Resources in the Constrained Application Protocol (CoAP)", RFC7641, IETF, 2015.

[40] J. Jimenez, J. Lopez-Vega, J. Maenpaa, G. Camarillo, "A Constrained Application protocol (CoAP) Usage for Resource Location And Discovery (RELOAD)", RFC7650, IETF, 2015.

[41] OneM2M, "Functional Architecture", TS-0001 ed. 2.10.0, OneM2M, 2016.

[42] OneM2M, "Requirements", TS-0002 ed. 2.7.1, OneM2M, 2016.

[43] OneM2M, "Security Solutions", TS-0003 ed. 2.4.1, OneM2M, 2016.

[44] OneM2M, "Service Layer Core Protocol Specification", TS-0004 ed. 2.7.1, OneM2M, 2016.

[45] OneM2M, "Management Enablement (OMA)", TS-0005 ed. 2.0.0, OneM2M, 2016

[46] OneM2M, "Service Components", TS-0007 ed. 2.0.0, OneM2M, 2016.

[47] OneM2M, "CoAP Protocol Binding", TS-0008 ed. 1.3.2, OneM2M, 2016.

[48] OneM2M, "HTTP Protocol Binding", TS-0009 ed. 2.6.1, OneM2M, 2016.

[49] OneM2M, "MQTT protocol Binding", TS-0010 ed. 2.4.1, OneM2M, 2016.

[50] OneM2M Partners Type 1, "Interoperability Testing", TS-0013 ed. 1.0.0, OneM2M, 2016

[51] OneM2M Partners Type 1, "LWM2M Interworking", TS-0014 ed. 2.0.0, OneM2M, 2016.

[52] OneM2M, "WebSocket Protocol Binding", TS-0020 ed. 2.0.0, OneM2M, 2016.

[53] R. Shirey,"Internet Security Glossary, Version 2", RFC 4949, IETF, 2007.

[54] 나윤종, 김영갑, "사물인터넷 보안 표준화 동향 분석", 2016년 정보처리학회 춘계학술발표대회 논문집, 제23권, 제1호, pp.307-310, 2016.

[55] I. Hwang, Y.-G. Kim, "Analysis of Security Standardization for the Internet of Things", In Proc. of 2017 International Conference on Platform Technology and Service, Busan, Korea, IEEE Press, Feb. 13 - 15, 2017

약 력

김 영 갑

2003년 고려대학교 이학석사
2006년 고려대학교 이학박사
2006년~2008년 고려대학교 정보보호대학원 연구교수
2008년~2010년 국가평생교육진흥원 선임전문원
2010년~2013년 고려대학교 연구교수
2013년~2015년 대구가톨릭대학교 IT공학부 조교수
2015년~현재 세종대학교 정보보호학과 조교수
관심분야: 보안공학, IoT 보안, 빅 데이터 보안, 위험분석

황 인 태

2015년 한국외국어대학교 공학사
2016년~현재 세종대학교 정보보호학과 석사과정
관심분야: 보안공학, IoT 보안, 스마트 헬스케어 보안, 시스템 보안