[사물인터넷] IoT 보안 기술 관련 표준화 동향

개요

IoT(Internet of Things)란 사물인터넷이란 뜻으로 각종 사물에 센서와 통신 기능을 내장하여 인터넷에 연결하는 기술을 의미한다. 여기에서 사물이란 의미는 책상, 벽, 가전제품 등 우리 주변에 흔히 볼 수 있는 모든 사물을 의미하기는 하지만 실제로는 가전제품, 모바일 장비, 웨어러블 디바이스 등 통신기능과 센서를 가지고 있는 다양한 임베디드 시스템을 의미한다. 따라서, IoT 서비스에 보안 기능을 적용하기 위해서는 이러한 작은 임베디드 시스템 또는 디바이스에 성능을 파악하고 이에 적합한 보안 기술을 사용하여야 한다.

초기 IoT 서비스는 센서기반의 서비스가 주를 이루었으며 다양한 센서가 주변의 정보를 수집하여 중앙시스템으로 주기적으로 전송하는 서비스였기 때문에, 해당 IoT 서비스에서는 연산능력이 충분하지 않은 작은 센서나 중간 노드들에 보안 기능을 적용하기 위한 경량화된 암호알고리즘이나 인증기술 적용이 필요했다. 최근에는 ITS(지능형 교통시스템), 스마트 카. 스마트 공장, 스마트 의료기기 등의 융합서비스도 IoT 서비스 범주에 포함하기도 하기 때문에 해당 융합 서비스에 적용 가능한 보안기술 등도 최근 개발되고 있는 추세이다.

IoT 보안 기술과 연관된 표준들의 개발도 최근에 급증하고 있으며, ITU-T 뿐 아니라 ISO/IEC, IETF, ETSI, GSMA, CITS 등 다양한 표준화 기구에서도 IoT 보안 기술 표준화가 추진 중에 있다. 특히, ITU-T 에서는 SG20이라는 IoT 전담 스터디그룹을 지난해 개설하여 활발히 표준 개발이 진행되고 있으며, IoT 보안 분야 표준을 개발 중인 SG17에서도 다양한 IoT 보안 기술 표준화가 개발 중에 있다. 본 표준화 보고서는 지난 2016년 8월 29일부터 9월 10일까지 스위스 제네바에서 개최된 ITU-T SG17 정기회의에서 논의된 IoT 보안 기술과 관련한 표준화 동향을 소개하고자 한다.

IoT 보안 기술의 필요성

최근 IoT 란 단어는 IT를 다루고 있는 사람들에게는 더 이상 낯선 단어는 아니다. 그리고 이미 다양한 IoT 서비스들이 우리 일상생활에 조금씩 스며들고 있으며 조만간 일상 생활에 깊숙히

자리 잡게 될 것이다. 즉, 우리가 아침에 눈을 뜰 때부터 밤에 잠자리에 드는 시간까지 모든 일상생활이 IoT 서비스로 살아갈 날이 멀지 않았다고 할 수 있다. 따라서, 이러한 IoT 서비스가 일상 생활 전체로 확산되기 전에 보안에 대한 고민을 하지 않으면 최근 온라인상에서 발생하는 해킹 사고의 피해보다 몇 백배 피해가 늘어날 수도 있다. 특히, 이용자 개개인의 생명이 위협받을 수도 있기 때문에 IoT 서비스 보안이 더욱 중요한 이유이다.

CES 2016이나 MWC 2016 등을 보면 기존에는 스마트 폰, 가전제품 등 단일 제품에 대한 새로운 기술을 소개하는 것이 주였다면, 최근에는 가정, 직장, 병원, 빌딩 그리고 도로 까지 모든 것이 연결되고 상호 연계하여 서비스를 제공하는 기술들이 주를 이루고 있다. 이를 반증하는 중요한 키 포인트는 바로 자동차이다. 특히, 2016년도 CES나 MWC의 경우 가전이나 스마트 폰 보다 스마트 카 부스가 더욱 핫하고 이슈의 중심에 서 있었다. 따라서, IoT 서비스가 다양한 사물들이 단순히 통신기능이나 센서 기능만을 가지고 운영되는 것이라 아니라, 보안 기능이 탑재되어 우리 일상생활에 편리성뿐 아니라 안전성까지 담보하는 서비스가 제공되어야 할 것 이다. 최근, ITU-T 에서도 이러한 필요성을 인지하고 다양한 IoT 보안 기술 표준을 개발하고 있으며, 특히, IoT 전담 스터디그룹인 SG20을 설립하여 기존 보안 스터디그룹인 SG17과 협력하여 다양한 표준을 개발하고 있다.

IoT 보안 기술 표준화 진행 상황 및 표준화 회의 결정사항

현재 SG17 Question 6에서 추진하고 있는 IoT 보안 기술 관련 표준화는 총 2건이 있으며, 그 중 일본에서 제안한 “IoT 디바이스 보안을 위한 부분 암호화 기법(X.iotsec-1)” 권고안은 2014년 9월 회의에서 신규 표준화 과제로 채택되어 개발 중에 있는 권고안이며, 두 번째 권고안은 한국(순천향대)에서 제안한 “IoT 환경에서의 보안 가이드라인(X.iotsec-2)” 이며, 2015년 4월 신규 표준화 과제로 채택되어 개발 중인 권고안이다. 이외에도 지난 2014년 9월에 신규 표준화 과제로 채택된 “ITS 통신 디바이스를 위한 소프트웨어 업데이트(X.itssec-1)”와 “V2X 통신 시스템을 위한 보안 가이드라인(X.itssec-2)” 등의 권고안이 개발 중에 있다. 특히, X.iotsec-1과 X.itssec-1 권고안 등은 2016년 3월에 Determination 승인 요청을 하였으나, 미국/영국/GSMA 등의 반대로 Determination이 연기되었다가, 2016년 9월 회의를 통해 Determination 승인

요청하기로 합의되어 현재 Determination 단계에 들어가 있다. 별다른 이견이 없을 경우 2017년 3월 회의에서 최종 표준으로 채택될 예정이다.

한국에서 제안하여 개발 중인 “IoT 환경에서의 보안 가이드라인(X.iotsec-2)” 권고안은 2016년 9월 회의를 통해 기고서 내용을 모두 반영하기로 합의하였으며, 2018년 상반기 최종 표준 채택을 목표로 표준을 개발 중에 있다. 또한, 한국(ETRI)에서 X.itssec-2 권고안은 차량간(V2V), 차량과 인프라간(V2I), 차량과 단말기간(V2N) 등에서 필요한 보안 요구사항을 정의하는 권고안으로 2017년 10월 최종 표준 채택을 목표로 표준을 개발하고 있다.

이외에도 ITU-T 내 IoT 전담 스터디그룹인 SG20과 ISO/IEC 등에서도 IoT 보안 관련 표준을 개발 중에 있다. SG20에서는 “IoT 시스템의 안전성 및 프라이버시 보호를 위한 신뢰된 IoT 디바이스 식별(Y.IoT-IoD-PT)“, “IoT 안전성 보장을 위한 보안 기술(Y.IoT-sec-safety)”, “IoT 위조방지를 위한 정보관리디지털구조” 등과 같은 IoT 보안 표준을 개발하고 있다. 또한, ISO/IEC 에서는 IoT 및 ITS 보안에 활용 가능한 경량화된 암호기술에 대한 표준을 개발 하였으며 현재 추가 표준을 개발 중에 있다. 해당 표준은 ISO/IEC 29192(Lightweight cryptography) 시리즈 이며 본 표준에는 블록암호기법, 스트림 암호기법, 비대칭 기술을 이용한 메커니즘 등이 포함되어있으며, 최근 버전에서는 해쉬함수와 MACs 등이 추가되어 개발 중에 있다.

IoT 보안 기술 표준화 관련 시장 전망 및 국내 표준화 활동에의 제언

IoT 보안 기술의 경우 국내 산업계, 정부, 학계에서 많은 관심과 다양한 IoT 서비스에 활용 가능한 보안기술 개발이 활발히 진행되고 있다. 또한, CES2016이나 MWC 2016 등에서 보는것과 같이 IoT 서비스/기술은 전세계적으로 가장 관심을 갖는 분야이며, 해당 분야의 보안기술에 대한 관심 또한 매우 높다. 따라서, IoT 보안 기술 표준화에 대한 시장성은 매우 높다고 할 수 있으며, IoT 보안 기술에 대한 표준화 선점은 향후 국내 산업 경쟁력에도 크게 도움이 될 것으로 판단된다. 따라서, 최근 학계, 산업계를 중심으로 활발히 개발되고 있는 우수한 IoT 보안 기술에 대해 적극적으로 국제 표준화를 추진하여 국내 기술의 우수성을 전세계에 입증하는 계기를 마련해야 할 것이다.

백종현 (KISA 팀장, ITU-T SG17 Q6 라포처, jhbaek@kisa.or.kr)