전기에너지와 사물인터넷 보안기술

김 진 철 팀장 / 한전KDN㈜ 전력IT연구원
kjckdn71@gmail.com

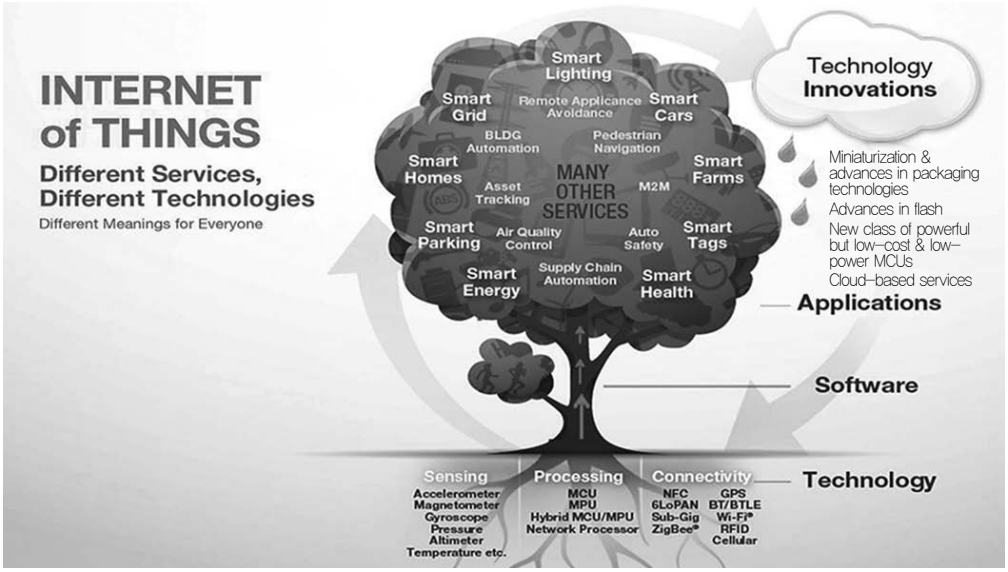
1. 사물인터넷의 개요

최근 인간과 사물, 사물과 사물 간을 네트워크에 연결하여 새로운 부가 서비스와 비즈니스 기회를 창출하는 사물인터넷에 대한 관심이 높아지면서 이를 전력산업에 적용하기 위한 기술개발이나 실증시험이 활발하게 이루어지고 있다. 사물인터넷의 사이버 보안은 일반 IT 사이버 보안과 다르게 사이버 세상뿐만 아니라 우리의 실생활 공간에서 존재하는 사물과 관련된 것이므로 일상생활에서 직접적으로 광범위한 피해를 경험할 수 있다는 점에서 그 중요성이 매우 크다고 할 수 있다.

사물인터넷에 대한 정의는 표준화 단체와 관련 기관 간에 다소 차이가 있지만, 국제표준화기관인 ITU(International Telecommunication Union)에서는 사물인터넷을 '언제 어디서나 어느 것과도 연결될 수 있는 새로운 통신 환경으로 인간과 인간, 인간과 사물, 사물과 사물을 연결하는 '객체의 제약'을 해결하는 것이 핵심이다'라고 정의하고 있다. 국내의 한국인터넷진흥원에서는 사물인터넷 기술을 초연결사회의 기반 기술로서 사물 간 인터넷 혹은 개체 간 인터넷으로 고유 식별이 가능한 사물이 만들어낸 정보를 인터넷을 통해 공유하는 환경이라고 정의하고 있다.

[그림 1]과 같이 사물인터넷은 센싱 기술, 프로세싱 기술, 네트워크 기술을 기반으로 이를 구현하는 소프트웨어 기술을 통하여 스마트그리드, 스마트 에너지, 스마트 조명, 스마트카, 스마트 농업, 스마트 태크, 스마트 헬스케어, 스마트 파킹, 스마트홈과 같은 다양한 분야에 적용되고, 기술적인 혁신을 통하여 새로운 제품과 서비스를 출현시킬 것이다.

ITU-T는 2011년부터 본격적인 사물인터넷 기술에 대한 표준화를 추진 중에 있으며, 네트워크 및 통신 분야에서의 기능 모델, 유즈 케이스, 서비스 구조, 에코시스템, 식별자 등 관련 표준을 개발하였다. 2015년 6월 ITU-T SG20(IoT and its applications including smart cities and communities)이 신설되어, 사물인터넷 관련 표준화

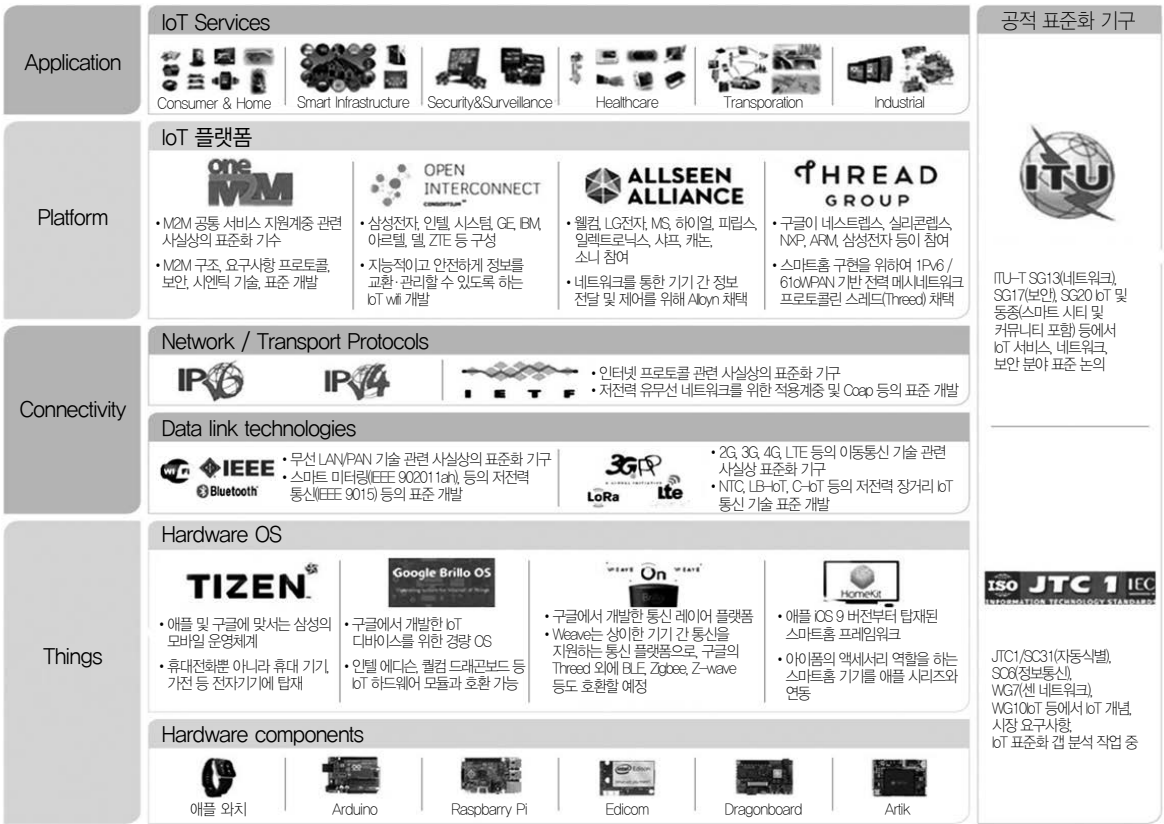


[그림 1] 사물인터넷 기술과 융합 서비스
(출처 : Internet of Things : Future of Technology and Innovation, Patterns7, 2015)

를 주도적으로 진행하고 있다. ISO/IEC JTC 1은 2014년 11월에 JTC1/WG10이 신설되어 사물인터넷의 개념, 시장의 요구사항 분석 및 사물인터넷 표준화 갭 분석 등 JTC 1의 표준화 영역에서 사물인터넷을 체계적으로 표준화하기 위한 작업이 진행되고 있다.

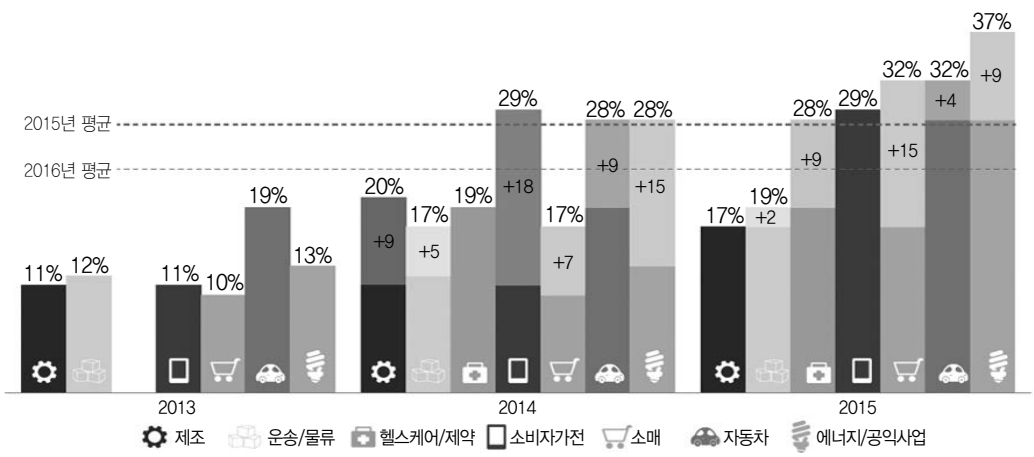
먼저 사실상의(de-facto) 표준화기구인 IETF(Internet Engineering Task Force), oneM2M(one Machine to Machine), IEEE(Institute of Electrical and Electronics Engineers) 등에서도 사물인터넷 관련 표준화 활동을 활발하게 진행하고 있다. IETF에서는 ACE, DTLS 등과 같은 저전력 소규모 네트워크 적용 표준 개발을 진행하고 있으며, CoRE(Constrained RESTful Environments) 워킹그룹에서 사물인터넷에 적합한 CoAP(Constrained Application Protocol) 표준을 개발하였다. oneM2M에서는 2015년 1월에 M2M 구조 및 요구사항, 프로토콜 및 보안, 유지관리 및 시멘틱(Semantic) 등에 대한 표준을 제정하여 발표하였다. IEEE에서는 2014년 6월 사물인터넷 참조 모델 및 참조 구조 작업 그룹인 IEEE P2413을 통하여 본격적인 사물인터넷 기술 표준화에 착수하였다.

사물인터넷과 관련된 주요 협의체(연합체)로는 OCF (Open Interconnect Consortium), AllSeen Alliance 등이 있다. OCF는 기존 삼성, 인텔, GE, IBM 등이 주축이 된 Open Interconnect에서 2016년 3월 새로운 멤버로 기존 AllSeen Alliance의 주축 멤버인 퀄컴, 마이크로소프트, Electrolux 3개 글로벌 기업을 새로 추가하며 200개를 넘는 회원사를 보유하고 있으며, 매우 빠르게 성장세가 증가하고 있다. OCF는 사물인터넷 오픈 플랫폼 표준 규격을 개발함과 동시에 독특하게 오픈소스를 개발하여 외부에 확산하는 역할을 동시에 수행하고 있다. 규격서 개발 이후 각 업체가 자사 제품에 무상 특허 정책의 오픈소스를 탑재함으로써 사물인터넷 시장의 확산을 추진 중이다. 그밖에도 Open Automotive Alliance, TIZEN, Continua Health Alliance, Thread Group 등이 사물인터넷 관련 표준을 개발하고 있다.



[그림 2] 사물인터넷 국외 표준화 동향

(출처 : 사물인터넷 기술 표준화 동향과 표준특허 확보를 위한 제언, 지식재산정책 제26호, 2016)



[그림 3] 주요국 산업별 사물인터넷 도입 추이

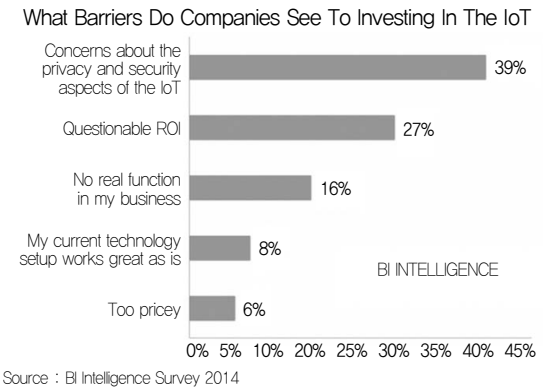
(출처 : 사물인터넷 발전과 보안의 패러다임 변화, KISTEP InI 제14호, 2016, 원출처 : 보다폰, 2015)

사물인터넷 활용에 따른 전 세계 시장 규모는 시장 기관에 따라 2020년까지 1.9조 달러에서 19조 달러에 달할 것으로 전망되었다. 또한, 2015년 6월에 Mckinsey에서 발표한 자료에 의하면, 연간 최소 3.9조 달러에서 최대 11.1조 달러의 경제적 파급효과가 발생할 것으로 전망하였다.

하지만, 이러한 낙관적인 시장 전망과는 달리 전 세계 사물인터넷 도입은 아직 미미한 수준으로 나타났다.

글로벌 통신회사 Vodafone이 전 세계 16개국, 7개 산업에 종사하는 650명이 임직원을 대상으로 온라인 설문조사 결과에 따르면, 2015년 조사 대상 기업의 27%가 사물인터넷을 도입한 것으로 나타났다. 이는 2013년 12%, 2014년 22%에서 점진적으로 증가한 것으로 나타나지만 여전히 사물인터넷 도입은 초기 수준임을 보여준다. [그림 3]과 같이 산업별로는 에너지·공공 분야가 제일 높게 나타났고, 제조 분야는 가장 낮은 도입율을 보이고 있으며, 헬스케어/제약 분야의 도입율은 매우 높은 성장세를 보이고 있다.

사물인터넷의 낙관적인 시장 전망과 달리 아직 도입이 많이 되지 않는 장벽에는 어떤 것들이 있는지 BI Intelligence에서 2014년에 조사한 결과에 따르면, [그림 4]와



[그림 4] 사물인터넷 주요 장벽 (출처 : BI Intelligence, 2014)

같이 보안 관련 응답이 39%로 가장 높은 것으로 나타났고, ROI, 사물인터넷 도입에 따른 실질적인 개선 여부에 대한 불안함, 높은 가격 등으로 아직은 기업들이 망설이고 있는 것으로 나타났다. 즉, 기업들의 사물인터넷 투자에 가장 높은 장벽으로 인식하고 있는 부분은 사이버 보안이었다.

미래창조과학부는 사물인터넷의 보안 중요성에 대한 관심이 높아짐에 따라 2014년에 사물인터넷 정보보호 로드맵을 발표하고, 사물인터넷에 대한 센서/디바이스, 네트워크, 플랫폼/서버스별 보안 위협(Risk)과 보안 요구사항(Requirement)을 아래 [표 1]과 같이 정리하였다.

구 분	보안 위협	보안 요구사항
센서 / 디바이스	• 저사양 디바이스 해킹 • 디바이스 관리 취약점 증가	• 저사양 디바이스 보안기술 : 백신, 암호화, 인증 등 • 디바이스 보안 관리기술 : 보안 패치, 감시체계 등
네트워크	• 무선 네트워크 취약 • 네트워크 트래픽 공격량 급증	• 통합 네트워킹에 요구되는 단말 상호간 인증·보안 • 통합 해킹 공격 탐지·대응 • 대규모 기기·네트워크에 대한 보안 상태 감시체계
플랫폼 / 서비스	• 공개 플랫폼의 취약 • 사용자 정보 유출/추적	• 기기간 인증, 키 관리, 접근 제어 • 개인정보 수집 제어 • IoT 환경에 특화된 보안 플랫폼

[표 1] 사물인터넷 보안 위협 및 보안 요구사항

발생일	설 명
2014.1	미국 보안업체 Proofpoint는 스마트 TV와 냉장고, 홈네트워크 라우터를 해킹하여 '좀비가전'을 만든 뒤 악성 이메일을 75만 건 발송한 사이버공격 사례를 공개
2014.3	보안컨설팅 업체인 Team Cymru는 해커들이 D-Link, Tenda, Micronet, TP-Link 등이 제조한 30만여 개의 공유기를 해킹했다고 경고
2014.6	유로폴(Europol)은 올해 또는 수년 안에 자동차, 의료기기, 웨어러블 기기 등 IoT 기기를 해킹한 온라인 납치와 살인 등 사이버범죄 발생을 우려하며, 정부에 대책 방안을 요구
2014.8	블랙햇을 통해 KNX 프로토콜 기반의 취약성으로 인해 아이패드2만으로 중국의 한 호텔의 방 온도, TV 온오프, 블라인드, 문 밖 표시등에 이르기까지 원격 제어 시연
2014.9	ISEC 2014 콘퍼런스에서 로봇청소기 원격 조종을 위해 필요한 앱의 인증 방식 취약점과 로봇청소기에 연결되는 AP의 보안 설정상의 취약점 등을 악용해 로봇청소기에 탑재된 카메라로 실시간 모니터링 시연
2015.8	블랙햇에서 주행 중인 지프 체로키 차량의 전화선을 이용한 원격 조작으로 액셀레이터, 브레이크 기능을 무력화하는 실증을 선보였으며, 이 영향으로 피아트·클라이슬러·오토 모빌스(FCA)는 140만 대의 차량을 리콜 실시
2016.8	블랙햇을 통해 차량의 임의 조작, IoT 스마트 조명 시스템 조작 등의 시연을 선보임 – 차량 정보를 취득하는 'OBD2' 커넥터를 통해 액셀레이터와 브레이크 기능을 비활성화하거나, 임의 조작과 스마트 IoT 조명 시스템을 드론으로 원격 해킹하여 빌딩 부근 정전 시연
2016.9	텐센트 산하 '킨 보안 연구소' 연구진이 테슬라의 전기자동차를 해킹해 달리는 차량을 원격으로 급브레이크를 걸고, 사이드미러, 트렁크, 좌석, 방향 지시등을 원격 제어 기능을 시연
2016.10	16.2.12.~6.15일까지 불특정 다수의 공유기를 해킹해 스마트폰을 허위 포털 사이트로 접속하도록 유도하여 악성 앱을 유포한 후 스마트폰 1만 3,501대로부터 포털 계정을 부정 생성

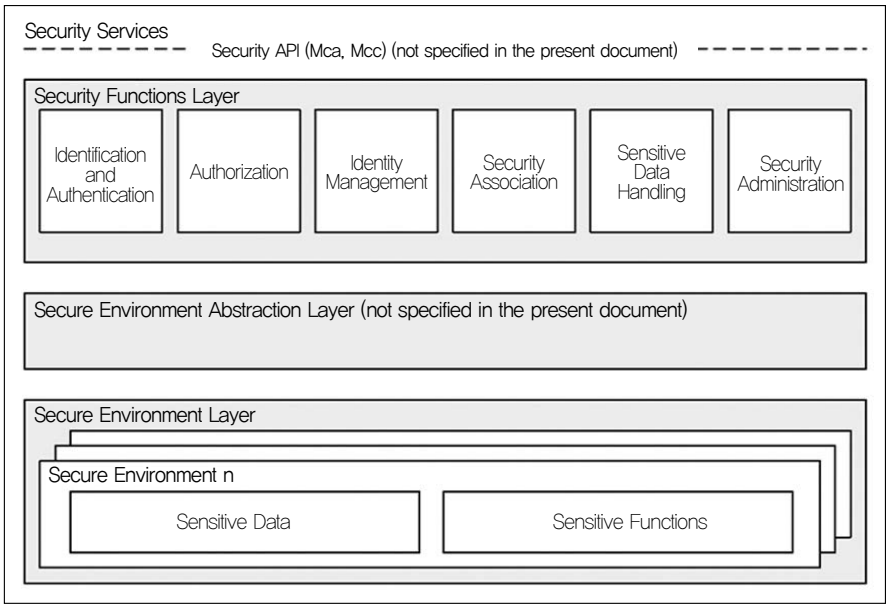
[표 2] 사물인터넷 관련 보안 위협 사례

사물인터넷 사이버 보안 위협은 사이버 세상뿐만 아니라 우리의 실생활 공간에서 존재하는 사물과 관련된 것이므로 위의 [표 2]와 같이 일상생활 속에서 직접적으로 광범위하게 피해를 경험할 수 있다. 사물인터넷 보안에 대한 피해사고와 가능성은 사물인터넷이 발전하고 보급됨에 따라 더욱 빈번하게 일어날 수 있다.

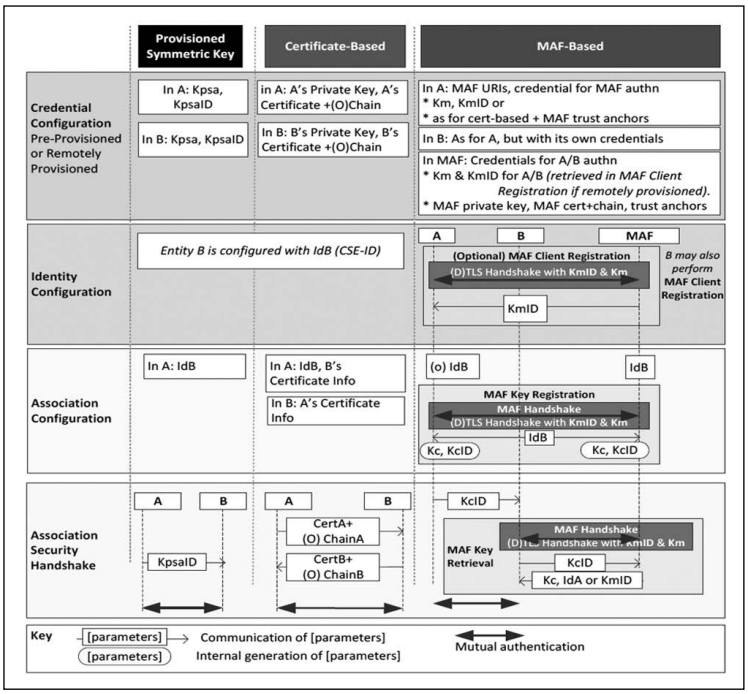
2. 국내외 사물인터넷 보안기술 동향

사실상의(de-facto) 표준화기구인 oneM2M에서는 사물인터넷 플랫폼과 관련된 보안기술이 표준화가 진행되고 있다. OneM2M의 보안 아키텍처는 우측의 [그림 5]와 같다. OneM2M에서는 Security Function Layer, Security Environment Abstraction Layer, Secure Environment Layer로 나누고, 특별히 Security Function Layer에 필요한 기능으로 식별 및 인증, 인가, 식별 관리, 보안 연계, 민감 데이터 처리, 보안 관제 등으로 정의하였다.

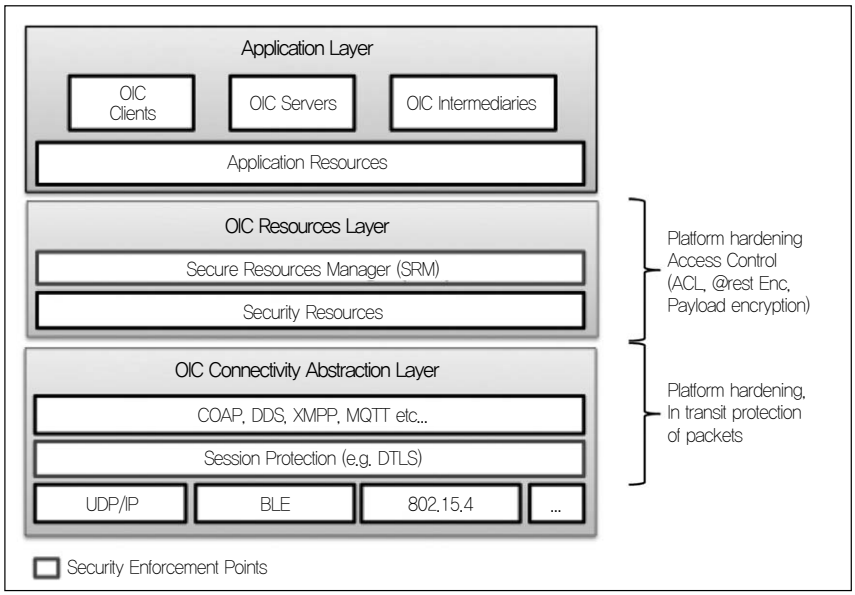
사물인터넷에서는 다수의 센서/디바이스들이 광범위한 현장에 설치되고, 유무선 네트워크를 통하여 네트워크에 접속하기 때문에 이를 위한 식별/인증 및 인가 기술이 기반이 되는 경량화된 보안 연계 설정(Security Association Establishment) 기술을 매우 중요하게 보고 있다. [그림 6]에서는 OneM2M의 보안 연계 설정 방법을 배분된 대칭키를 이용한 방식, 인증서 기반 방식, MAF(M2M Authentication Function) 기반 방식 등 3가지 보안 연계 설정 방식을 비교, 설명하고 있다. 센서/디바이스의 프로세싱 능



[그림 5] OneM2M의 보안 아키텍처
[출처 : OneM2M, TS-0003-V2.4.1(Security Solutions), 2016]



[그림 6] OneM2M의 보안 연계 설정 프레임워크
[출처 : OneM2M, TS-0003-V2.4.1(Security Solutions), 2016]



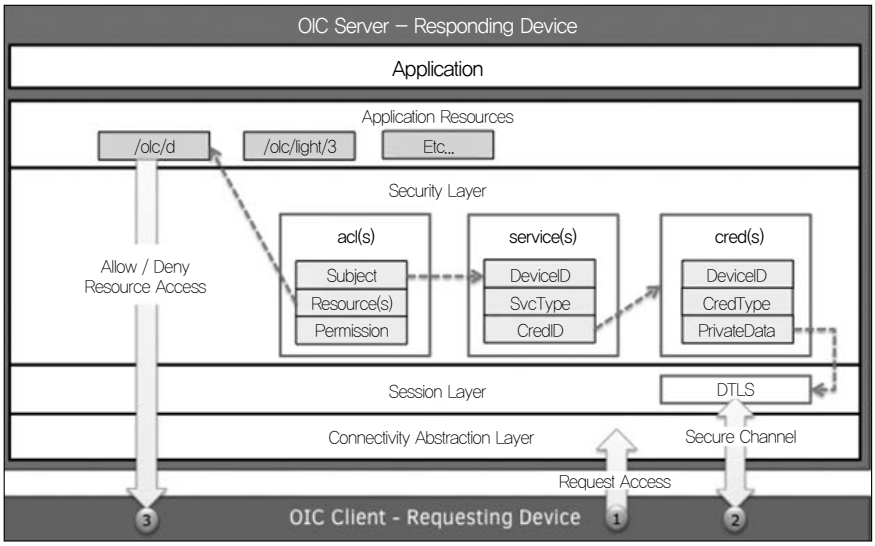
[그림 7] OCF의 보안 아키텍처
(출처 : OCF, OIC Security Specification V1.1.0, 2016)

력, 네트워크 프로토콜 및 환경 등 사물인터넷 기술을 적용하는 어플리케이션 특성과 수준에 적합한 보안 연계 설정 방법을 채택할 수 있다.

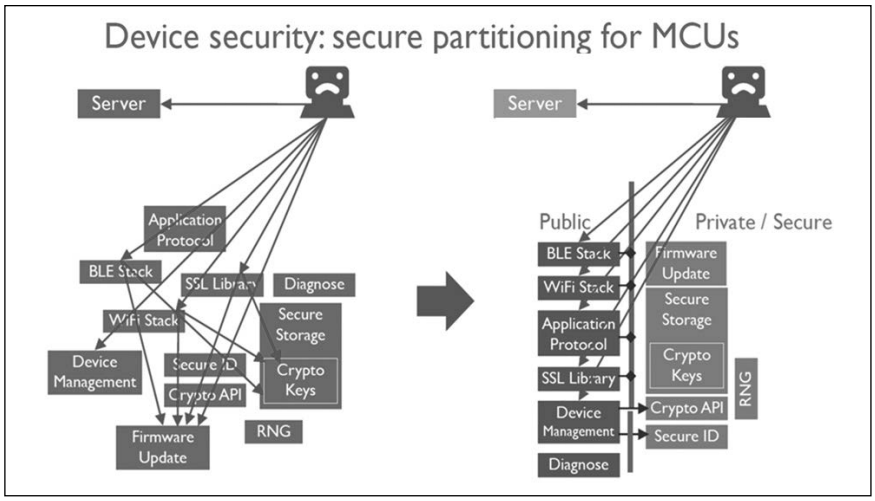
OCF에서는 보안 규격인 OIC Security Specification V1.1.0을 2016년에 발표하였다. OCF에서는 보안 아키텍처를 위의 [그림 7]과 같이 OIC Resource Layer에 SRM (Secure Resource Manager)를 두고 JWE(JSON Web Encryption)과 JWS(JSON Web Signature)와 같은 매커니즘을 통하여 전송계층과 독립적으로 페이로드를 보호할 수 있도록 했다. 또한, OIC Connectivity Abstraction Layer에는 기존 TLS 방식보다 경량화된 DTLS(Session Protection)을 사용하여 경량화된 방식으로 전송계층에서 보안기술을 적용하고 있다.

OCF에서는 연결 설정 프레임워크는 [그림 8]과 같고, 먼저 OIC 클라이언트가 OIC 서버에게 연결 요청을 하고, DTLS를 통하여 OIC 서버와 OIC 클라이언트가 연결되면, ACL(Access Control List)에 있는 클라이언트가 맞는지 확인하고, 어떤 서비스가 인가되는지 확인하고, 인증 정보를 확인하여 OIC 서버의 리소스에 접근하려는 OIC 클라이언트의 요청을 허가할 것인지, 부인할 것인지를 결정하여 OIC 클라이언트에게 통보한다.

국외 기업들의 사물인터넷 보안기술 동향을 살펴보면, SYMANTEC은 디바이스/게이트웨이에 필요한 보안기술, 네트워크에 필요한 보안기술, 서비스에 필요한 보안기술을 정의하고, 사물인터넷의 End-to-End 보안기술을 개발하고 있다. INTEL은 자사 IoT 플랫폼의 가장 큰 특징을 Secure, Scalable, Interoperable한 플랫폼으로 목표를 잡고 있다. INTEL은 보안이 사물인터넷의 핵심적인 기술이라고 인식하고, End-to-End 보안이 가능한 보안기술을 자사 제품에 적용하도록 개발하고 있다. ATMEL은 암호 알고리즘과 보안 프로토콜을 자사 반도



[그림 8] OCF의 보안 연계 설정 프레임워크 (출처 : OCF, OIC Security Specification V1.1.0, 2016)



[그림 9] ARM의 디바이스 보안 (출처 : ARM, 2016)

체 칩에 내장시켜서 사물인터넷 센서/디바이스를 위한 보안기술을 제공하고 있다. ARM은 [그림 9]와 같이 일반적인 부분과 F/W 업그레이드, 암호 알고리즘, 암호키, 암호 API, ID 등과 같은 보안 및 개인정보가 포함되고(부분이 분리된), 보안기술이 적용된 자사 솔루션을 개발하였다.

3. 전기에너지 사물인터넷 보안기술 동향

전기에너지 분야에서는 표준화된 OneM2M, OCF 등의 사물인터넷 플랫폼을 적용한 사례는 아직 없지만, 연구과제를 통하여 AMI와 배전 분야 등에 일부 적용하여 현장 실증을 하고, 점진적으로 시범사업과 본사업을 추

진할 예정에 있다. 하지만, 전력IT 사업과 스마트그리드 실증사업 등을 통하여 기기 간 자율적인 유무선 네트워크를 통하여 정보를 교환하는 시스템은 이미 현장에 구축되어 활용되고 있고, 최근에 기반시설에 대한 보안 중요성이 높아짐에 따라 보안기술을 적용하는 방안 수립과 연구개발이 추진되고 있다.

가. AMI 시스템 보안

AMI 시스템은 스마트그리드의 근간을 이루며, 또한 동시에 악의적인 행위의 공격 대상이자 연계 시스템으로의 침입경로가 되며, 이는 스마트그리드의 치명적인 약점이 될 수 있으며, 이로 인한 스마트그리드의 보안 취약성 증가의 요인이 된다.

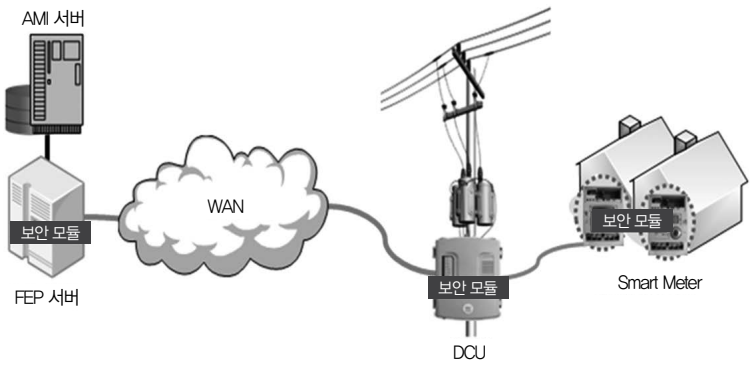
WAN 구간과 연계되는 AMI 네트워크는 기존 인터넷망이 가지고 있는 보안 취약성으로 인해 외부 공격에 쉽게 노출될 수 있다. 기존 네트워크에서 사용되는 범용적인 통신장비 및 서버시스템을 사용하는 경우로, 이들 시스템이 가지고 있는 보안 취약성이 AMI 보안 취약성으로 연결된다. AMI 보안 취약성을 통하여 스마트그리드 네트워크에 침투하여 전력시스템의 제어권을 획득한 후, 전력공급의 차단 등 전력 통제권의 상실 등으로 직결될 수 있다는 것이다.

2009년 미국에서 수행된 스마트그리드 모의해킹(CNN 2009. 3)에서 내부로의 손쉬운 침투가 가능함이 확인되었으며, 침투한 해커는 대규모의 스마트 미터 조작이 가능할 수 있었는데, 이는 전기 수요 증감을 통한 전력망 불안정을 유도해 대도시를 대상으로 하는 정전사태 유발까지 이루어질 수 있다는 것이다. 실제로 미국 전력망에서 중국 및 러시아 출신으로 추정되는 사이버 스파이가 설치한 악성코드가 발견(CNN 2009. 4)된 사례가 있으며 이는 악성 코드를 이용한 전기공급 차단이 가능하며 나아가 사이버 무기화로서의 가능성을 말해주는 것이다. AMI 보안 취약성에 대한 보안 요구사항을 정리하면 다음과 같다.

AMI 보안은 대상 기기 간 상호인증, 암호화 저장 및 암호화 통신을 기반으로 한다. AMI 보안의 적용 대상 기기는 아래 그림과 같이 수용가 측에 설치된 스마트미터, 변대주에 설치된 DCU, 검침센터에 설치된 FEP 서버를 그 대상으로 하며, 각각의 대상에 대하여 보안 모듈을 적용하여 상호간 인증, 암호화 저장 및 암호화 통신을 수행한다.

항 목	설 명
기밀성	• AMI 시스템의 전송 데이터 및 저장 데이터의 기밀성 보장 • 비허가된 기기와 사용자에게 정보가 공개되지 않도록 함 • 블록 암호와 같은 암호 알고리즘에 비밀 키를 적용하여 제공
무결성	• AMI 시스템의 전송 데이터 및 저장 데이터의 무결성 보장 • 데이터의 생성·전송·저장 중에 비허가된 방법으로 변경되지 않았음을 보장 • 메시지 인증코드나 디지털 서명과 같은 암호 알고리즘에 비밀 키를 적용하여 제공
개체인증	• AMI 시스템의 통신 시, 통신 주체 간의 상호인증 보장 • 상호인증은 정보 생성 기기와 사용자 검증 • 디지털 서명, 메시지 인증코드 기법과 같은 암호 알고리즘을 통해 제공
가용성	• AMI 시스템의 통신 및 서비스에 대한 가용성 보장 • 가용성은 AMI 시스템 정보 및 데이터에 대하여 인가된 사용자의 접근 적시성 상시 보장

[표 3] AMI 보안 취약성에 대한 보안 요구사항



[그림 10] AMI 시스템 보안기술 적용 대상 기기

AMI 시스템에 대한 보안 취약성 극복을 위하여 기기 인증, 암호화 저장 및 암호화 통신 등을 적용하였지만, 이것 외에도 악의적인 사용자 행위에 대해서 그 이상의 보안사항이 요구될 것이며, 이에 대한 보안성 강화와 물리적 보안등 추가적인 보안 시스템 도입과 개선을 필요로 한다.

나. 배전지능화시스템 보안

배전지능화시스템은 배전선로를 감시하여 전력공급 신뢰도를 향상시키기 위한 시스템으로 전력산업의 중추적인 분야이며, 물리적으로 타 시스템과 분리된 통신 네트워크에 의해 운영되었다. 이런 이유로 보안 침해 위험이 오픈 시스템에 비하여 상대적으로 적은 것이 사실이었지만, 최근 스마트그리드를 배경으로 한 분산전원 등 타 시스템과의 연계 및 통신 프로토콜인 DNP3의 구조적 문제에 따라 보안 취약성이 점차 증가하고 있는 추세이다. 따라서, 안정적인 전력 공급을 위한 배전지능화시스템의 보안 강화를 위하여 보안 시스템의 필요성이 대두되고 있다. 특히 배전지능화망은 SCADA와 더불어 주요 기반시설로 지정되어 있어 그 필요성은 더욱 커지고 있다.

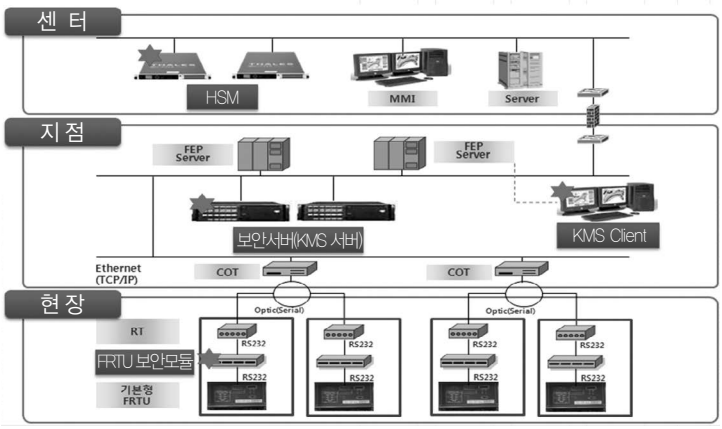
DAS 주장치와 현장의 단말장치 간의 메시지 통신은 DNP3을 사용한다. 하지만 DNP 자체에 보안 기능은 없어 다양한 방법의 악의적인 공격으로 시스템 교란이 가능하다. 이러한 단점은 FEP과 FRTU에서 송수신되는 메시지를 암호화하고, 인증을 하여 메시지의 침해를 방지할 수 있다.

공격 유형	내 용
방 해(Interruption)	• 물리적으로 제어시스템의 일부가 파괴되어 통신을 할 수 없게 되는 등 가용성에 대한 공격
가로채기(Interception)	• 비인가자들의 불법적인 접근에 의하여 발생되는 기밀성에 대한 공격
불법 수정(Modification)	• 불법 변경에 의한 메시지 위변조 및 수정 등 무결성에 대한 공격
위 조(Fabrication)	• 네트워크 상에 위조된 메시지를 삽입하거나 파일에 레코드를 추가하는 등 인증에 대한 공격

[표 4] 배전지능화시스템 보안 취약성

설비명	주요 기능
FRTU 보안 모듈	• 메시지 암·복호화 및 인증 • 키 관리
보안 서버	• 프로토콜(DNP) 처리 • 메시지 암·복호화 및 인증 관리
HSM	• 메시지 암·복호화 및 인증 • 키 생성 및 저장

[표 5] 배전지능화시스템 보안 취약성에 대한 보안 요구사항



[그림 11] 배전지능화시스템 보안기술 적용 대상 기기

현재 시스템의 수정 없이 보안 시스템을 구성하는 방안으로 그림과 같이 보안 서버와 보안 모듈을 별도의 장치로 구성하여 DAS 보안 시스템을 적용할 수 있다. 보안 서버는 FEP과 FRTU에서 사용하는 DNP Standard Protocol 메시지가 송수신될 경우 Secure DNP3.0 Protocol을 이용하여 메시지에 대한 보안 및 메시지가 발생한 장비 응 인증하여 악의적으로 발생하는 위협을 방지할 수 있다. 기존 DNP3.0에 보안 기능을 적용한 IEC 61850-5 기술 표준을 적용하여 운영이 가능하다.

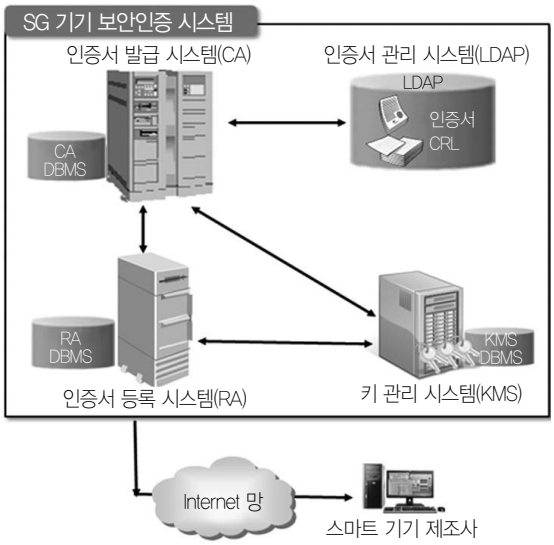
전력망 내의 제어기기는 고도화되고, 자동화되어 지능형으로 발전하는 만큼 보안에 대한 이슈와 새로운 공격 기법에 의한 침해 사례가 다변화되고, 지능화되고 있다. 정보통신망에서의 보안 공격에 대한 해결책은 명확하게 제시되지 못하고 있는 것이 지금까지의 현실이지만, 다양한 시도를 통해 전력망 자동화 장치의 보안 환경 구축에 현실적인 솔루션의 해답을 제시할 수 있다. 또 전력망 디바이스 인증, End-to-End 보안 환경 구축, 제어 디바이스의 보안 적용 등을 통해 그 피해를 방지할 수 있다.

다. 기기 보안인증 시스템

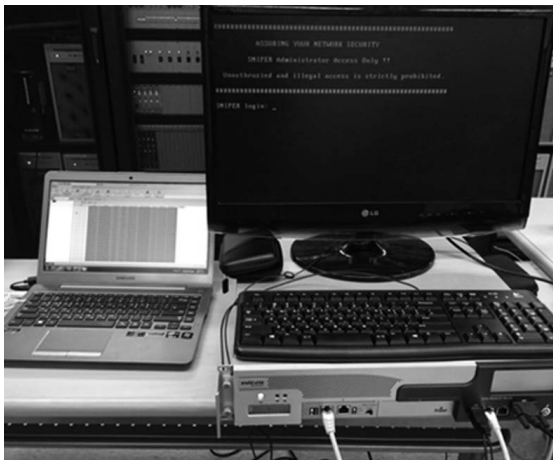
전력 분야 현장 기기들은 넓은 공간에 산재되어 있어 공격자가 쉽게 접근하여 기기 및 네트워크에 대한 장애 유발 및 통신상의 주요 메시지에 대한 위변조 공격이 가능하다. 따라서, 통신 객체 간 암호화 및 적법한 인증 절차가 적용되지 않는다면 기기 정보 유출은 물론 전체 전력 제어망에 치명적인 피해를 야기할 수 있다.

기기 보안인증 시스템은 전력 분야에서 운영되는 기기에 대한 인증서 발급, 등록, 관리 및 검증 서비스를 제공함으로써 지능형 전력망에 대한 사이버 테러를 방지하고 신뢰성 있는 통신 환경을 제공하는 보안 인프라 시스템이다. 우측의 상단 [그림 12]는 PKI 기반 기기 보안인증 시스템의 기본 구성을 보여준다.

PKI 기반 기기 보안인증 시스템은 인증서 발급시스템(CA), 인증서 관리 시스템(LDAP), 인증서 등록 시스(RA), 키 관리 시스템(KMS)으로 구성된다. 인증서 발급 시스템은 X.509 국제 표준 기반으로 기기 인증서를 발급하고, 인증서 등록 시스템은 스마트 기기 제조사로부터 전송된 인증서 발급 요청을 키 관리 시스템으로 전달하며 발급된 인증서에 대한 다운로드 서비스를 제공한다. 키 관리 시스템은 기기 인증 서 발급에 필요한 키 쌍(개인키, 공개 키)을 생성하고 안전하게 관리하며, 인증서 관리 시스템은 발급된 인증서를 저장하고 관리하는 역할을 수행한다.



[그림 12] 기기 보안인증 시스템의 기본 구성



[그림 13] 이상징후감시시스템

라. 이상징후감시시스템

지난 2010년 등장한 스턱스넷(Stuxnet)은 대표적인 제어시스템 대상의 공격 사례로 다수의 보안 취약점을 이용하였다고 알려져 있다. 산업시설을 감시하고 파괴하는 최초의 악성 소프트웨어로 산업기반시설 전반에 걸쳐 큰 혼란을 야기했다. 최근에는 제어시스템을 대상으로 한 사이버공격이 점차 고도화·지능화됨에 따라 제어시스템 환경에 적합한 화이트리스트(Whitelist) 기반 네트워크 비정상 트래픽 감지 기법이 많이 연구되고 있다.

이상징후감시시스템은 제어시스템 내부로 유입되는 네트워크 트래픽을 모니터링하고 감시하여 분석 및 통계를 수행하고, 화이트리스트 기반 이상징후 감시를 이용하여 공격 시그니처 등 외부로부터 업데이트 없이 운용이 가능한 시스템으로 제어시스템 환경/자산 변화에 신속한 대처가 가능하다. 이상 징후감시시스템은 일부 급전소/급전분소에 설치되어 시범 운영 중이며, 향후 SCADA 보안관제 솔루션의 이상징후감시센서로 활용될 수 있다.

4. 결 언

사물인터넷 보안 위협은 사이버 보안뿐만 아니라 실생활과 밀접한 사물로 확대 가능하므로 피해 속도 및 규모적인 측면을 고려할 때 사회적 비용은 기하급수적으로 증가할 수밖에 없다. 센서·디바이스, 이기종/유무선 통합 네트워크, 다양한 서비스/플랫폼에 따라 다양한 보안 위협과 이에 대응하는 새로운 보안 요구사항 및 보안 체계 정립이 필요하다. 전기에너지 분야에도 4차 산업혁명 영향으로 전력계통 전 계통에 사물인터넷 기반 새로운 시스템이 도입될 것으로 예상되며, 이를 위해서 사물인터넷 보안 플랫폼 기반의 사물인터넷 환경에 적합한 경량화된 인증·인가·연계·접근제어 등의 보안기술 개발이 필요할 것으로 생각된다.