IoT 융합보안의 동향 분석 및 보안 강화방안

최용수
성결대학교 파이데이아대학

Ⅰ. 서 론

IoT 라는 단어가 대두되고 단시간에 일반 사용자의 실생활 속에 그리고 산업의 일부 분야에 적용되어 그 가능성을 높이고 있다. 더욱이 4차 산업혁명의 시작과 함께 인공지능, 빅데이터 분석 기술 등과 더불어 미래의 산업혁명을 이끌 선두주자가 되어졌다. 우리가 인지하건 그렇지 않건 우리는 네트워크의 센서가 되기도 하고 그 정보들을 이용하기도 한다.

Industrial IoT에 있어서는 더욱 그러할 것이다. 공상과학영화에서나 보던 장면이 머릿속에 그려지지 않는가. 로봇이 로봇을 만들어 내는 상상속의 공장!

물론 이글에서 센싱, 통신, 제어와 같은 내용에 대해 자세히 설명하지는 않는다. 저자보다 세부 기술에 대해 잘 설명할 수 있는 분들이 아주 많기 때문이다.

본 글에서는 IoT에서의 융합보안에 대해 좀 더 중점을 두고 이야기를 풀어가고자 한다.

Ⅱ. IoT 융합 보안의 필요성 및 시장 분석
Ⅲ. IoT서비스 확산에 따른 각국의 보안 기술 정책 흐름
Ⅳ. IoT에서의 보안 위협
Ⅴ. IoT 보안 솔루션 개발 현황
Ⅵ. IoT 플랫폼, 서비스 보안 개발의 시사

Ⅱ. IoT 융합 보안의 필요성 및 시장 분석

IoT 비즈니스 유형을 보면 보안서비스의 필요성을 알 수 있다. IoT

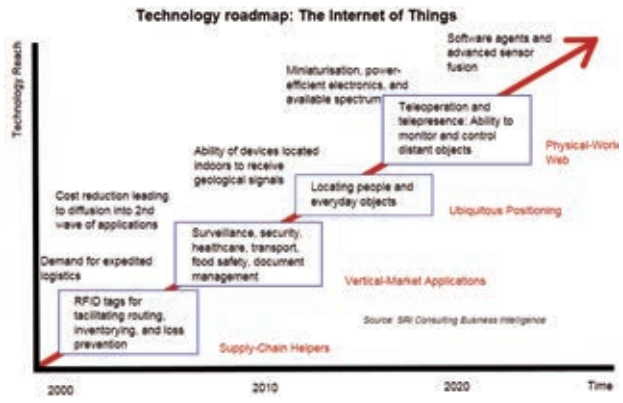
서비스의 유형은 초기에는 기업간(B2B)서비스였으나 한동안 일반 소비자형(B2C)서비스로 변화하였으며 최근에는 기업주도의 플랫폼 시장으로 변모하고 있다. 각각의 분리된 개별시장(Vertical Market)을 형성하고 있는 IoT 비지니스 유형은 개인화서비스(스마트홈, 헬스케어, 미아방지 등), 지불/결제(매장판매관리, NFC 결제 서비스 등), 물류, 유통, 보안/관제, 의료, 자산관리 등에서 많이 활용되고 있음을 알 수 있다.

이러한 마켓의 유형 중에서도 보안관련 비즈니스 모델은 주로 지역, 빌딩 등의 관제에 포커싱 되어있는 것을 알 수 있다. 사실 지역이나 빌딩의 관제라고 하나 실제 가장 많은 부분은 CCTV라고 해도 과언이 아닐 것이며 글로벌 시장을 위해 수립해야할 성장과제이기도 하다.

〈그림 1〉의 IoT 기술 로드맵을 한번 살펴보자. 비록 CCTV기반의 보안시장이 주도적이기는 하나 Mobile과의 연계, 다양한 센서와의 융합 등으로 IoT의 확산으로 이어지고 있음을 유추할 수 있다.

사물인터넷의 주요 분야별 전망을 보더라도 보안과 관련한 주목할 만한 항목이 있다. 바로 자동차(Automotive)분야에서 향후 도난 방지를 위한 보안 및 추적(Security, Tracking)의 전망이 활성화되고 자동차 플랫폼으로의 적용이 크게 늘어날 전망이다.

자동차에 통신의 기능이 부가된 Connected Car가 몇 년 사이 최첨단의 기술로 급부상하고 있다. 바로 자동차 내부 장치 간, 자동차 간, 자동차와 주변 환경과의 통신을 수행하는 기술이다. 미국의 유명한 시장조사기관



〈그림 1〉 IoT 기술 로드맵

인 Gartner에서 "The Top Connected Application in 2020"리스트에 Connected Car를 1위의 자리에 올렸으니 그 가치는 매우 클 것으로 기대가 된다.

그렇다면 연결은 통신을 의미하고 통신에 장애가 생기거나 악의적인 개입이 발생한다면 그로인한 결과는 독자의 상상에 맡기겠다. 실제 몇 년 전 국내의 유명 정보보호 전문기관에서 스마트폰 앱을 통해 차량의 통신에 개입하여 차량의 브레이크 작동을 불능화하고 엔진 스로틀을 최고로 올리도록 하는 해킹을 선보였다. 물론 실제 차량에 이러한 기술을 적용해 시범을 보였으니 그 장면을 보는 사람은 섬뜩함 마저 느낄만하다.

Ⅲ. IoT서비스 확산에 따른 각국의 보안 기술 정책 흐름

2009년 7월 EU(유럽연합)에서는 사물 인터넷의 구체적인 추진계획인 14개의 사물인터넷 액션 플랜(Internet of Things-An Action plan for Europe)을 수립하고 연구개발 및 시범서비스를 추진하고 있다. 특히, 사물인터넷 연구화 혁신 촉진을 위해 'Horizon 2020' 프로그램을 통해 2016년부터 2년 동안 약 1억 4천 유로를 투입하여 IoT연구개발을 투입하는 등 액션플랜을 완성하기 위한 노력을 보이고 있다.

EU의 액션플랜에서는 연구개발, 서비스, 인프라 구축, 개인 정보보안 대책, 법 · 제도 그리고 평가체계마련 등의 행동지침을 제시하였다. 특히, 사생활 및 개인정보 침해에 대한 대응을 필수적으로 요구하였으며 정보보호 조치로 민감 정보 인프라의 보호와 모니터링을 제안하였다.

EU는 5G 이동통신, 미래인터넷(Future Internet), 클라우드, 빅데이터 등의 에코 시스템 구축을 위한 R&D와 중소 · 중견기업이 참여하는 사업 생태계 형성을 지원하고 있으며 EU의 연구개발 지원을 통해 개발된 EU산 플랫폼 및 제품을 EU의 스마트 서비스에 적용하려 노력하고 있다.

EU는 다양한 응용분야에 사물인터넷 기술과 융합 서비스를 접목하여 새로운 산업 및 시장 창출을 도모하고 있다. IERC 주도하에 교통, 스마트홈, 스마트시티, 건강관

리 등의 14개 서비스 도메인 대상의 R&D를 추진하고 있으며 유럽위원회(European Commission)는 사물인터넷이 빠른 속도로 발전하면서 기존의 산업 및 시장 모델에 근본적 변화를 야기시키고 있다고 경고하였다. 예를 들어, 사물 및 사람과 공간 정보를 의사결정에 활용하면서 기업의 편익은 증대되었으나, 사물인터넷 도입에 따른 이익이 특정 사업자의 시장지배력을 강화시켜 시장경쟁체제가 와해될 가능성 증대, 사회적 파급력이 확대됨에 따라 사용자 의사결정권이 침해될 우려가 있는 등 윤리적 측면의 갈등의 유발 가능성 등에 대한 우려를 지적하였다. IoT의 순기능을 사회 구성원이 누리기 위해 개인정보 보호 등의 위협요인에 대한 분석 및 관련 연구에 대한 투자 · 지원이 요구된다는 점을 지적한 것이다.

산업발전에 있어 후발주자이지만 초식공룡과 같은 덩치를 가진 이웃나라 중국의 예를 보자. 중국 공업정보화부는 2011년 12차 5개년(2011~2015) 계획에 사물 인터넷을 추가한 '사물망 12-5 발전규획'을 수록하였다. 12-5발전규획은 8대 추진방향을 가지고 있는데 그 중 보안을 포함하며 정보안전 보장을 정책적으로 명시하였다. 정보안전 보장 추진방향에는 1. 안전기술 R&D강화, 2. 안전보장 시스템 구축 보완, 3. 네트워크 인프라 보호 강화 천명하였다. 단순한 글로벌 시장의 잠식 이후에 대한 대비를 국가가 주도하고 있다고 보여진다.

특히, 일본은 2009년에 수립한 'i-Japan 전략 2015'에서 지진 감지, 원격진료 등 미래 디지털 안전사회 구현을 위한 센서 네트워크 기반의 사물통신(M2M) 기술 및 서비스를 개발하는 계획을 포함하였다. 5대 전략으로는 '액티브하고 쾌적한 생활', '빅데이터의 활용에 의한 사회 · 경제 성장', '리치(rich) 콘텐츠 향유', '견고하고 유연한 ICT 인프라 구축', '세계 최고 수준의 보안 환경 구축'을 들 수 있다.

또 문부과학성에서는 2014년 국제수준의 연구환경을 구출할 목적에서 'IoT 시대의 ICT 시스템 아키텍쳐에 관한 연구개발과제(2015~2020)'를 발주하며 사물인터넷 시대의 새로운 컴퓨팅 기술로서 지능형 분산처리가 가능한 기술을 연구 개발하는 목표를 설정하였다.

위에서 보인 일본의 5대 전략이 너무 추상적이라고 생각되지는 않는가. 하지만 언제인가 세계에서 가장 안전한 도시로 도쿄가 선정되었다는 기사를 본 저자로서는 이와 같은 대전제가 가지는 정책 의지를 깊이 느끼고 얄밉게도 철저한 일본의 정책방향 제시와 실제적인 수행에 다시금 찬사를 보냈다.

대부분의 국가들이 IoT의 미래비전을 제시하는 가운데 스마트글라스와 같은 첨단제품들이 나올 때 마다 제기되었던 프라이버시 보호를 정책적으로 통제한다는 미래지향적인 틀을 제공했다 할만하다. 저자도 민감정보의 범위를 분류하고 취득된 민감정보에 대해 저항요인을 최소화하는 표현 방법의 연구를 제안한바가 있어 공감하는 바가 크다.

현재까지의 사물인터넷 기술은 수직시장 위주로 성장하였으므로 프라이버시나 보안의 위협성에 대한 필요성을 크게 인지하지 못하였다. 개별의 시장들이 폐쇄성을 가지고 있다고 해도 과언이 아닌 것이다. USN이 자신들만의 프로토콜을 사용한 덕분에 시장에서 크게 부흥하지 못함도 비슷한 이유일 것이다. 특히, 국내의 사물인터넷 서비스 시장은 이동 통신사를 중심으로 소규모 센서 네트워크 서비스(예를 들어, 물류추적, 원격 검침 서비스, 공공 서비스)가 주를 이루고 있어 소비자 시장으로는 크게 확산되지 못하였다. 이동통신사 중심의 단순결제, 보안 서비스 외에 텔레매틱스, 헬스케어, 스마트 팜 등 최근 기술이 적용된 서비스도 상용화되기 시작하였다.

국내에서도 사물인터넷 시장의 확대에 따라 보안위협에 대한 노출도 증가하게 될 것이다.

2016년의 통계를 보면 국내 사물인터넷 서비스는 개인화서비스의 비율이 가장 높으며 지불/결제, 사회/문화 분야의 순으로 활성화되고 있다. 2012년에는 Automotive 분야가 상대적으로 보급 비중이 높았고 다음으로 지능형 빌딩, 가정 등의 순위를 기록한 것에 비해 서비스의 변화가 크게 이루어졌다. 향후 국내 사물인터넷 서비스 시장은 헬스케어, 생활 편의 등 '소비자 영역'으로도 크게 확대가 될 것으로 전망되면 자동차 분야와 스마트미터는 더욱더 기술고도화가 이루어질 전망이다.

결국 시스템, 네트워크, 플랫폼에 대한 총체적인 보안위협이 증가한다고 단언할 수 있다.

국내에서의 IoT 정보보호 로드맵의 주요 현안은 다음과 같다.

– 보안이 내재화된 기반 조성
– 글로벌 융합보안 시장을 선도하는 9대 보안 핵심기술 개발
– IoT 보안 산업경쟁력 강화

정부에서 시행하고 있는 IoT 융합보안 실증사업(〈그림 2〉 참조)의 7대 분야(스마트카 서비스 모델, 공급기관 연계형 헬스케어, 스마트 그리드 에너지 관리시스템, 스마트 홈 관리 시스템, 지능형 스마트 공장, 개방형 스마트 시티 플랫폼, 스마트 클린-워터 정수장)에서 IoT제품 또는 서비스의 설계단계부터 유통공급 및 유지보수 전주기에 걸친 보안 내재화 추진을 목표로 하고 있으며 공급자의 3대 보안원칙으로 '안전한 구조설계', 핵심요소의 안전한 개발, 공급망 안전 확보'를 제시하였다.

국내 IoT 정보보호로드맵을 토해 보안과 안전을 고려한 민간주도의 IoT보안인증 도입을 적극 지원하고 IoT 제품 및 서비스를 안전하게 보호하기 위해 디바이스, 네트워크, 서비스 · 플랫폼 등 3계층별 특성을 고려한 9대 보안 핵심기술을 개발하는 '시큐어돔'프로젝트도 추진한다. 이는 IoT 침해사고에 대한 종합적인 대응체계를 단계적으로 마련하겠다는 정책적 의지로 비쳐져 기대를 할 만한 흐름인 것이다.

Ⅳ. IoT에서의 보안 위협

Gartner Research에 따르면 2016년 현재 약 64억개의 사물들이 연결되어져 있다고 예측하였다. 단적인 예로 자동차는 내부 네트워크(CAN 통신)에 수백개의 센서와 여러 컴퓨터가 연결되어 있다. 또 DHL이나 Cisco System는 2015년 기준으로 약 150억개의 연결된 디바이가 있을 것이라 추정하였고 2020년에는 500억개의 디바이스 연결을 예측하였다. 하지만 몇 년전 중국산 다리마와 러시아산 전기 주전자에서 무선 네트워크에 접속해 악성코드와 스팸을 유포하는 기능이 발견되는 등 IoT 제품에서의 보안위협은 실제로 드러나고 있다. 검색엔진

〈그림 2〉 IoT 융합보안 실증 사업 추진 방향

'Shadon'은 네트워크에 연결된 난방 제어시스템, 정수처리장, 자동차, 신호등, 태아 심장 모니터링, 발전소 제어장치와 같은 다양한 디바이스를 쉽게 검색가능하다. 이렇듯 네트워크 기반의 응용 및 서비스들은 편리성은 높였지만 해킹 등을 통한 보안의 위협성도 증대시키고 있음을 의미한다.

실제 발생하였던 보안 침해 사례를 살펴보자. 리눅스웜을 통한 원격 조정 공격으로 Linux.Darlloz는 가정용 라우터, STB(Set-Top Box), 산업 통제 시스템 ed의 디바이스를 감염시켰음이 확인되었다. 또 보안 취약점 악용한 사생활 침해로는 미국 유아 모니터 생산업체 SW취약점 발표 후 수백대의 카메라에서 실시간 영상이 대중에게 유포되기도 하였다. 시스템 오류로 인해 개인 데이터 유출의 경우 가전제품에서 맞춤형 광고를 위해 소비자의 콘텐츠 시청 정보를 수집하였고, 기능의 미사용에도 불구하고 계속적인 정보 수집이 발생한 사례가 있다.

〈그림 3〉 융합보안의 범위(응용분야)

이와같이 폭발적으로 성장하는 IoT 네트워크 기술이 직면하는 도전 중의 하나는 연결된 시스템을 구축하기 위한 명확하고 공통적인 구조를 가지지 않는다는 점이다.

이에 선도적 안티바이러스 보안 솔루션을 제공하는 Symantec의 경우 다음과 같은 사물 인터넷 안전이용 수칙을 발표하기도 하였다.

1. 인터넷 연결 장치와 인터넷 사이를 연결해주는 모뎀 및 라우터를 안전하게 보호, 수시로 방화벽 구성이 제대로 이루어지고 있는지 체크할 것
2. 나의 네트워크에 어떤 디바이스가 연결돼 있는지 체크하고, 개인 컴퓨터 외 셋톱박스, 태블릿 PC, 스마트 폰 등 다양한 기기 역시 보안에 취약할 수 있다는 점을 기억할 것
3. 구매한 기기가 홈 네트워크에 연결된다면, 인터넷으로도 보안 위협 요소가 접근할 수 있으므로 보안에 각별히 주의할 것
4. 모든 기기는 보안 설정에 유의하며, 기기에 원격 접근이 가능한 기기라면 사용하지 않을 때엔 제품을 꺼두거나 제품의 원격 접근 기능을 비활성화 시켜 원격 접근 기능이 실행되지 않도록 하는 것
5. 모든 기기의 비밀번호는 초기 비밀번호나 '123456'이나 'password'처럼 쉽게 유추 가능한 비밀번호가 아닌 문자, 숫자, 기호 등을 조합한 안전한 비밀번호를 사용하는 것
6. 마지막으로 보안 취약점이 발견되는 즉시 제조사의 홈페이지를 접속해 보안 관련 소프트웨어와 패치를 다운 받아, 최신 버전으로 유지할 것

즉, 앞으로 펼쳐질 IoT기반의 응용들은 융합보안의 필요성을 가지므로 위의 수칙은 기존의 정보보안기술과 물리보안에서의 보안 수칙을 망라하는 융합보안 이용 수칙이라고 해도 과언이 아닐 것이다.

그렇다면, 실제 융합보안에서 발생 가능한 피해들을 나열해 보자.

의료정보망 해킹에 의한 원격의료기기 조작이나 개인의료정보 유출, 스마트카 해킹에 의한 교통망 교란, 차량 절도, 스마트 그리드 해킹에 의한 대규모 정전, 전기요금 조작, 금융망 해킹에 의한 주가 및 잔고 조작, 개인 신용정보 유출, 스마트 홈 해킹에 의한 스마트 홈침입, 스마트정보가전 해킹, IT융합부문 해킹에 의한 제품의 신뢰성 저하 및 기업의 생산성 저하의 피해를 초래하게 될 것이다.

그중 스마트 카 해킹은 차량에 탑재된 40~100여 개의 전자제어유닛(ECU)을 연결하는 네트워크인 CAN(Controller Area Network: Bosch에서 차량 네트워크용으로 개발함)을 해킹하는 경우인데 실제 침해 연구가 이루어진 실증 연구를 소개해 보겠다.

해커는 부착이 의무화된 자동차 자가진단장치인 OBD를 통해 CAN을 도청하고 제어 메시지를 보내는 형태로 요인암살, 테러, 무작위적 범죄 행위가 발생할 가능성이 매우 높은 경우이다. 악성 앱을 통해 스마트폰을 감염하여 차량 안에서 앱을 구동하여 CAN통신 내용을 무선 통신망을 통해 외부로 전송하거나 반대로 CAN통신에 참여해 공격메시지(가속, 엔진 폐쇄, RPM조작, 핸들 제어 등)를 차량에 주입하게 함으로써 오작동을 유도하는 것이다.

Ⅴ. IoT 보안 솔루션 개발 현황

단말이나 센서 보안을 위한 기기 인증기술 분야에서는 타 기기와의 통신 시 올바른 기기에서 전송된 데이터인지 식별 및 인증하는 기술, ID/PW 인증, 인증서 인증, SIM(Subscriber Identification Module) 등을 개발하고 있다. 가능하다면 물리적 접근이 불가하도록 통제하는 것은 꼭 필요할 것이다.

실제, Hewlett Packard가 IoT 취약점을 분석한 보고서는 IoT 기기 중 70%가 암호화나 사용자 접근 권한 설정 등에서 취약점을 가지고 있는 것으로 분석하였다.

전자 OEM 기술자 및 대표들의 설문조사에 따르며 대표적 장애로 Trusted Platform Module과 같은 하드웨어 솔루션이 필요하다고 하였고, 제품의 수명주기는 보안 업데이트 능력에 달려 있으므로 이진 해쉬(Hash)와 같은 보안요소의 사용을 통해 안전하게 디자인될 필요가 있다고 하였다. 결국 글로벌 전기전자 제품을 생산하는 OEM들은 판매 전략에서 보안성을 촉진책으로 사용할 것이라

고 답하였다.

임베디드 및 모바일 소프트웨어 기업 Wind River는 2013년 소프트웨어 플랫폼 2.0을 발표하며 통신채널과 데이터, 단말기기의 안전을 위한 게이트웨이 보안 기능을 제공하고자 하였다. RFID/USN, ZigBee, 무선 랜, 모바일 네트워크와 같은 네트워크 영역은 저전력, 고속 통신을 위한 기술요소를 활용해야 하므로 IDP 2.0에서는 다양한 단거리 무선통신 프로토콜에 대한 데이터 전송 및 네이티브 지원을 위해 MQTT(Message Queue for Telemetry Transport) 지원 및 OMA(Open Mobile Alliance)-DM과 같은 안정된 관리 프로토콜을 지원하는 장점을 가진다. 또 Wind River의 RTOS(Real Time OS)인 'VxWorks 7'은 USB, CAN, 블루투스, 파이어와이어 등의 주요 프로토콜을 지원하고 보안 데이터 스토리지, 트러스트 부트, 사용자와 정책에 대한 관리기능 까지 폭넓게 제공한다. 또 Monaco는 Nano-Crpto, DTLS, Update, Cert, EAP, NanoSec, NanoSSH와 같은 임베디드 보안 솔루션을 개발하였다. 결국 리눅스나 펌웨어가 OS로 활용되는 IoT 기기는 시큐어 OS기반 원천기술의 활용으로 보안성을 강화해야 한다. 더구나 IoT는 대부분 임베디드 시스템으로 개발되어야 하는데, 일반 PC와 달리 임베디드 시스템은 24시간 무중단 서비스를 보장받아야 하며, 잦은 패치와 백신의 업데이트가 불가능하다. 국내 기업인 SGA에서 발표한 솔루션은 주요 임베디드 시스템에서 화이트리스트(whitelist) 기반의 악성코드 탐지 및 차단 기능을 제공하고 시스템 중요자원의 불법 삭제 및 변경을 차단한다.

살펴본 바와 같이 IoT 응용은 저전력, 경량화된 단말과 센서에 최적화된 보안 메커니즘 적용이 필수이므로 Cisco는 몇 년 전부터 Open Platform Application 및 분석기술을 포함한 보안 솔루션 확장을 준비하였으며 최근에는 '시큐리티 에브리웨어'라는 구호를 내걸고 기업용과 통신사용으로 전문화한 솔루션을 출시하며 데이터센터, 엔드포인트, 지점, 클라우드에 걸친 네트워크 위협을 가시화하고 통제할 수 있는 방법을 구체화했다. Cisco의 새 보안 솔루션은 센서 수를 늘려 네트워크 전반에 걸친 위협 가시성을 높이고, 통제 지점을 늘려 보안 정책 능력을 강화한다. 분산된 조직 보안 관리를 통합 및 단순화함으로써 위협 탐지 시간과 대응시간을 단축해 공격이 미치는 영향을 낮춘다. 공격 전후 경로를 차단하면서 경로에 따라 방어 기능을 확장한다.

한편, 국내기업인 Secui는 정보유출 및 도감청 방지를 위한 암호 알고리즘 고도화, IoT경량고속 암호기술 개발, 차세대 인증기술 등 원천기술 연구를 수행하며 경량 암호기술을 이용한 IoT보안 플랫폼 사업화를 추진하고 있다. Secui가 제공하는 보안기능들을 보면 하드웨어 기반 보안모듈로 위변조, 정보유출을 차단하기 위해 타워곡선알고리즘(ECC)과 함께 국산 경량고속 암호알고리즘인 LEA를 적용하였다.

IoT에서 적용되어야 하는 융합보안기술의 개발범위를 현재의 예측으로 국한하는 것은 매우 위험하기에 국내외에서 경연대회, 전문조직 구성을 통해 IoT 환경을 위한 시스템구축, 솔루션 출시 등의 보안 사업 다각화를 추진하는 사례들이 늘고 있다. Cisco는 'The Cisco Security Grand Challenge'에 30만 달러를 투자하였으며 Symantec은 IoT 보안 관련 조직을 구성/운영하며 연구보고서를 발표하도록 하여 자사의 솔루션과 서비스를 통해 IoT를 지원할 수 있는 기술을 제공하고자 하였다.

Ⅵ. IoT 플랫폼, 서비스 보안 개발의 시사

IoT 서비스 보안에서는 통신/네트워크 보안 기술(CoAP, MQTT 등), Open API 보안 기술(OAuth 등), 플랫폼 보안, 서비스 보안, 해킹 대응, OS 보안, 접근제어와 인증/인가 기술 등 기존의 보안기술을 활용하여야 하며 프라이버시 보호기술, 디바이스/서비스/데이터 통합 보안 기술 그리고 Security Anchor기술에 대한 지속적인 연구가 필요하다.

사물인터넷 서비스의 창출은 다양한 디바이스, 플랫폼, 데이터 주체, 응용 서비스의 융 · 복합을 통해 생성되므로 매우 복잡하며 인증 · 인가 기법, 접근 제어 · 권한 제어 기법, ID관리 기법, 키 관리 및 분배 기법, 신뢰 제어 기법과 같은 기본 보안 요소들을 갖춰야 한다.

IoT 플랫폼 보안에서 DB관리를 통해 Privacy · Trust

관리 기술을, 프로토콜을 이용하여 인증 · 인가 기술을, 그리고 OS 보안과 네트워크 보안 기술을 통해 안전한 데이터 전송기술을 완성하게 되는 것이다.

정부의 정책변화 및 풍부한 네트워크 인프라로 인해 국내 IoT 시장의 급성장은 명백해 보인다. 하지만 현재까지는 응용의 개발에 대한 고민이 주였으나 이제부터라도 보안적 관점의 기조를 명확히 수립하고 사용자 측면에서의 서비스 활용 방안을 고민해야 할 것이다.

참 고 문 헌

[1] 공만식, 채홍준, 유보현, "기계저널", Vol. 56, No. 2, 2016

[2] 김호원, "사물인터넷 환경에서의 보안/프라이버시 이슈," TTA Journal, Vol.153, 2014

[3] 장봉임, 김창수 "사물인터넷 보안 기술 연구," Journal of Security Engineering, Vol.11, No.5, 2014

[4] 주대영, 김종기 "초연결시대 사물인터넷(IoT)의 창조적 융합 활성화 방안," ISSUE PAPER 산 업 창 조 화 시 리 즈, 2014

[5] 전혜영, "사물인터넷(IoT) 관련 유망산업 동향 및 시사점," 한반도 르네상스 구현을 위한 VIP 리포트, 통권 662호, 2016

[6] 황원식, "산업 패러다임에 따른 미래 제조업의 발전전략," K I E T 산 업 경 제, 3월호, 2016

[7] "윈드리버, 사물 인터넷(IoT) 위한 최신 소프트웨어 플랫폼 IDP2.0 발표", NEWSWIRE, 2013

[8] "윈드리버, IoT 위한 임베디드 OS 'VxWorks7' 출시", DATANET, 2014

[9] "시큐아이, IoT 보안 강화…'암호인증연구소' 설립", ZDNet, 2014

[10] "유화석 한솔인티큐브 대표이사 "사물통신 · 모바일 보안사업 진출", 파이낸셜뉴스, 2014

[11] "사물인터넷 확산으로 인한 보안 위협 '주의'", IT DAILY, 2014.

[12] "Cisco expands security solutions with open platform, analytics", ZDNet, 2014

[13] "Security & The Internet of Things", VDC Research, 2013

[14] "Embedded Software Security Solutions to Ride Rising Tide of Internet of Things", device management forum,

최용수

- 1998년 강원대학교 제어계측공학과 공학사
- 2000년 강원대학교 제어계측공학과 공학석사
- 2006년 강원대학교 제어계측공학과 공학박사
- 2006년~2007년 연세대학교 첨단융합건설연구단 연구교수
- 2007년~2013년 고려대학교 정보보호대학원 연구교수
- 2013년~현재 성결대학교 교양교직부(멀티미디어) 조교수
- 현) 대한전자공학회 컴퓨터소사이어티 협동부회장

〈관심분야〉
Multimedia Hashing, Information Hiding, Watermarking, Steganography, Image Forensics, Forgery Detection 등