사물 인터넷의 보안 위협 요인들에 대한 분석

전정훈*

요 약

최근 사물 인터넷(internet of things) 기술은 클라우드 컴퓨팅 서비스(cloud computing service) 및 빅 데이터(big data)와 함께 IT분야에 이슈가 되고 있는 기술 중에 하나로, 다양한 산업분야에서 응용 및 활성화되고 있다. 이러한 동향은 유비쿼터스(ubiquitous) 시대를 실현하는데 중요한 기반 기술의 등장이라 할 수 있다. 그러나 사물 인터넷은 다양한 산업분야에서 실현되고 있는 만큼 보안 문제 또한 다양할 것으로 예상되고 있는 가운데 이에 대한 보안 위협(security threats)들에 대한 대응 방안이 강구되어야 할 것이다. 따라서 본 논문은 사물 인터넷 기술의 적용분야에 대한 사례와 이에 따른 보안 위협들을 분석해 봄으로써, 향후, 사물 인터넷의 보안 대응 방안 마련에 활용될 것으로 기대한다.

Analysis on the Security threat factors of the Internet of Things

Jeon Jeong Hoon*

ABSTRACT

Recently, the Internet of Things is an important technology with a Cloud computing services and a Big data in the IT fields. and The Internet of Things is widely used in various industries. This trend may be referred to as the emergence of significant based technologies for realizing a ubiquitous times. But the security problems of Internet of things are expected to increase with being realized in a variety of industries. and it will be have to provide a corresponding technology to the security threat for this. Therefore, this paper will be analyzed to the security threats of the Internet of Things by the cases. Thereby this is expected to be utilized as a basis for the countermeasure of Internet of Things in a future.

Key words : Internet of Things, Security threats, Ubiquitous, Security threats factors, Information Security of IoT

접수일(2015년11월20일), 수정일(1차: 2015년12월23일), 게재확정일(2015년12월23일)

* 동덕여자대학교/컴퓨터학과

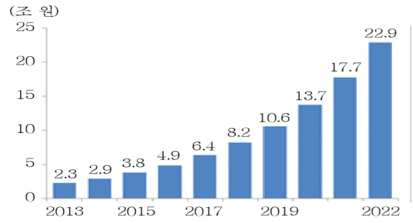
1. 서 론

최근 사물 인터넷 기술은 다양한 산업분야에서 응용 및 개발이 활발히 진행되고 있는 가운데, 스마트 기기의 등장은 사물 인터넷 기술 개발의 촉매제 역할을 하고 있다. 특히 스마트 폰(smart phone)과 테블릿(tablet) PC는 다양한 산업분야의 현장과 일상생활에서 실시간성과 편의성, 정확성 등을 제공해줌으로써, 보다 빠른 속도로 보편화되고 있는 추세이다. 2014년 정보통신산업진흥원의 보고서에 따르면, 2020년까지의 사물인터넷 시장 규모가 약1400조원에 이를 것으로 전망하고 있으며[1], 마이크로소프트(Microsoft)사는 윈도우10 IoT코어라는 플랫폼을 출시하며, 2년 내에 약 10억 개의 기기 보급을 언급한 바 있다[1]. 그러나 한국인터넷진흥원은 사물인터넷의 해킹에 따른 경제적 손실을 약18조원에 이를 것으로 전망하고 있으며, 이러한 손실은 해마다 발생하는 자연재해(2.7조원) 및 사이버공격(3.6조원)으로 인한 피해[2]와 비교해 볼 때, 엄청난 수치임을 알 수 있다. 사물인터넷은 이동성과 실시간성, 호환성, 이식성, 범용성 등을 함께 고려한 보안 기술 및 표준화 작업이 절대적으로 필요한 분야로 전 세계 사물인터넷 관련 글로벌 기업들은 보안 문제에 따른 손실경감 방안도 함께 마련해야 할 것이다. 따라서 본 논문은 사물인터넷의 보안 위협 요인들을 분석함으로써, 향후 사물 인터넷의 대응 기술 개발과 취약성 분석을 위한 연구 자료로 활용될 수 있을 것으로 기대한다. 본고의 논리적 구성을 위해 2장은 사물인터넷의 시장동향과 관련기술들에 대해 알아보고, 3장은 사물인터넷의 위협요인들을 알아본다. 그리고 4장은 위협요인에 따른 대응방안과 마지막 5장에서 결론부분으로써 이글을 마치도록 한다.

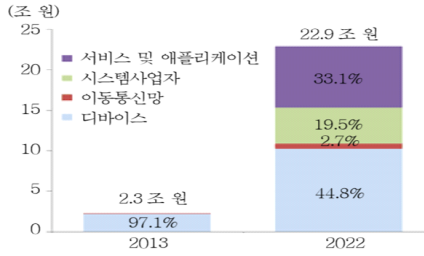
2. 관련 연구

2.1 사물인터넷의 시장동향

사물인터넷은 최근 미국에서 개최한 국제 전자제품 박람회CES(consumer electronics show)를 통해, 가전기업들의 새로운 트랜드(trend) 및 이슈들을 살펴볼 수 있다. 글로벌 기업들의 가전제품들을 소개하는 본 박람회에서는 ICT분야와 가전들을 융합한 제품과 사물인터넷 중심의 초연결사회로 진화한 제품을 새롭게 선보이면서, 전 세계 가전제품의 트랜드가 커넥티드(connected) 중심의 장르로 옮겨가고 있으며, 이종 기기들 간의 융합이 가속화되고 있음을 알 수 있다. 그리고 박람회는 미래 유망분야에 대해 IoT를 통한 스마트 홈(smart home)과 인체 전신으로 확대된 웨어러블(wearable)기기, 신산업영역으로 부상하는 드론(drone)과 로봇(robot), 스마트 카(smart car), 스마트 TV, 3D 프린팅을 6대 이슈로 정리하였다[3].



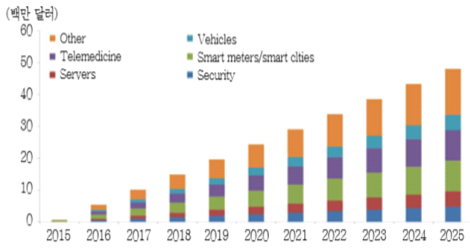
(그림 1) 국내 사물인터넷 시장규모전망



(그림 2) 국내 사물인터넷 시장규모전망

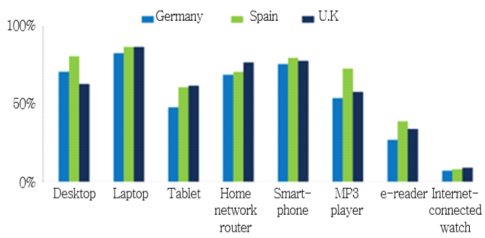
또한 가트너(gartner)의 통계자료에 따르면, 2014년에 비해 2020년 사물인터넷의 부가가치는 약 5배의 성장을 예측하고 있으며[4], 이밖에도 국내·외 사물인터넷 시장 및 정책 동향을 분석한 자료인 [5]는 국내 시장 규모를 그림1,2와 같이 규모면에서 2022년까지 약 6배의 성장과 함께 서비스 및 애플리케이션과 디바이스의 비중이 점차 커질 것으로 전망하였다. 그리고 국외의 경우, 그림 3,4,5의 사용현황과 매출현황을 통해 향후 움직임을 전망해 볼 수 있는데[5], 먼저 그림3을 살펴보면, 미국의 사물인터넷 사용현황으로 2025년까지의 전망치를 나타낸 것으로 스마트 미터

(smart meter)와 스마트 클로스(smart clothes)가 가장 큰 폭으로 성장할 것으로 보고 있으며, 보안과 서버, 자동차 분야는 제한성으로 인해 다소 적은 폭의 성장을 예상하고 있다.

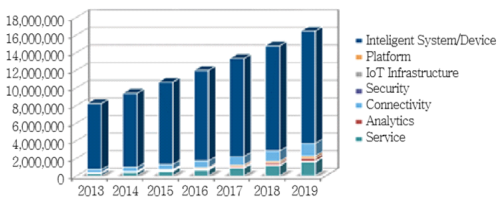


(그림 3) 국외 미국사물인터넷 사용현황 및 전망

그림4는 유럽 국가(독일, 스페인, 영국)들의 사물인터넷 이용현황을 나타낸 것으로 데스크 탑(desk top)과 랩 탑(lap top)에 이어 스마트폰 사용자가 빠르게 증가하고 있어 스마트폰의 활용성이 더욱 높아질 것을 예상하고 있다.



(그림 4) 주요 유럽 국가의 사물인터넷이용 현황

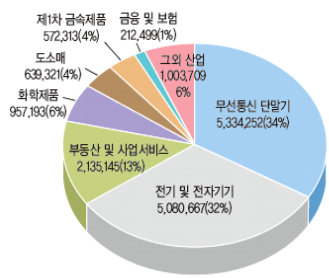


(그림 5) 일본의 사물인터넷 기술요소별 매출액 전망

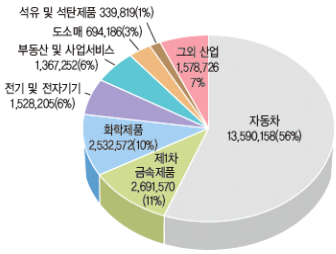
그림5는 일본의 기술요소별 매출액 전망치로 지능적 시스템과 장치의 비중이 점차 증가할 것을 예측하고 있어, 향후 지능형 기능을 탑재한 기기의 비중이 커질 것으로 전망하고 있다. 이와 같은 자료들을 종합해 볼 때, 가전업계의 트렌드(trend) 변화를 통해 사물인터넷 기술이 실생활 깊숙이 확산되고 있으며, 모든 산업분야에 사물인터넷 기술의 적용과 긍정적인 시장 확대가 전망된다.

2.2 사물인터넷의 피해현황

사물인터넷은 소형화와 신속성, 저전력 등 환경요인의 제약으로 무선 전송매체의 비중이 매우 높은 것이 사실이다. 이러한 무선 전송매체의 사용은 기존 무선 네트워크의 취약성을 상속하고 있어, 위험성이 높으며, 향후 해킹에 따른 피해규모는 보다 더욱 커질 것으로 전망된다. 이에 대해 [2]는 해킹 공격에 따른 경제적 손실이 약 18조원에 이를 것으로 보고 있으며, [6]은 스마트폰과 자동차 산업에 따른 피해가 그림6,7과 같이 각각 16조원과 24조원으로 예측하고 있다. 특히 스마트 폰(smart phone)은 다양한 서비스 및 제어가 가능하고, 휴대가 용이하여 편의성과 이동성, 실시간성 등의 다양한 장점을 갖고 있지만, 그림6과 같이 스마트 폰의 무선 전송매체 및 운영체제, 서비스 환경 등에 따른 취약성 총 피해액이 약 16조원에 이르고 있음을 알 수 있다. 이중 무선통신단말기로 인한 피해가 34%이며, 전기 및 전자기기로 인한 피해가 32%로 가장 큰 비중을 차지하고 있으며, 이밖에도 부동산과 사업 서비스, 화학, 도소매, 금속, 금융 및 보험 등 여러 산업 분야에서도 보안 피해가 발생하고 있음을 알 수 있다[6].



(그림 6) 스마트폰 보안피해총액 약16조원[6] 단위 : 백만원



(그림 7) 자동차 보안 피해 총액: 약24조원[6]

또한 최근 보안과 무관하다고 여겨졌던 자동차 분야를 살펴보면, 그림7과 같이 보안 피해액이 약24조원에 이르고 있어, 앞으로 사물인터넷 산업 전반으로 피해가 확산될 것으로 예상된다[6]. 이에 대한 사례로 차량정보수집 단말기(obd2)를 장착한 차량을 휴대폰으로 제동을 제어하거나, 유-커넥티드 카(u-conne cted car)의 오디오를 켜는 등의 보안 취약점들이 발견되었고, 크라이슬러사는 보안문제로 140만대의 자동차에 대해 리콜(recall)조치를 한바 있다[7]. 이러한 사례들은 유-커넥티드 카를 비롯한 모든 사물인터넷 기기에 대한 보안문제의 심각성을 반증해 주며, 향후 해킹 공격의 증가로 피해가 급증할 것임을 예상케 한다.

2.3 사물인터넷의 기술동향

<표 1> IERC의 사물인터넷의 주요 기술 이슈[8]

구분	2012 ~ 2020 주요 이슈
식별 기술	사물의 식별ID, 네트워크 주소 등에 대한 체계 및 융합
서비스 아키텍처링	엑스트라넷을 포함한 글로벌 스케일 서비스 구조
IoT 아키텍쳐	암호화, 인증, 위치인식, 에너지관리
인프라 기술	크로스 도메인간 통합 및 관리 기술
응용 기술	데이터 서비스를 위한 OpenAPI 기술
서비스 기술	IoT-aware process 모델링 및 실행, QoS
통신 기술	Longer range, 상호호환성, 저전력 프로토콜
네트워크 기술	Grid, 클라우드, 애드혹, 하이브리드, 메시 등
SW 및 알고리즘	자가 제어/관리, 마이크로OS, 상황인지, 확장성 등
하드웨어	초저전력 칩/센서, 초박막 디스플레이, 안테나 등
데이터 및 신호처리	센서온톨로지, 자동 컴퓨팅, 인지 컴퓨팅
검색 기술	스케일러블 검색, IoT 브라우저
에너지 기술	printed batteries, Photovoltaic cells, 무선전력
보안 기술	Cognitive security, 자가관리적 보안, Localized Security
Societal 측면 기술	Ambient Computing, 스마트 어시스턴스
소재 기술	카본 나노튜브, 컨덕티브 폴리머, 전도성 잉크 등

<표 2> 사물인터넷 관련 기술[8]

구분	정의
IoT	상호호환가능한 정보와 통신기술을 통해 보다 진보된 서비스 제공이 가능하도록 하는 정보사회를 구축하기 위한 글로벌 인프라[8]
	통신방법과 데이터의 활용을 통해 물리적·가상적 객체를 연결할 수 있는 네트워크 인프라[7]
	표준기반의 상호운용 가능한 통신 프로토콜을 기반으로 자가 설정이 가능한 동적인 글로벌 네트워크 인프라[3]
	네트워크의 네트워크[4]
	표준 기반 프로토콜에 기반하고 고유하게 식별될 수 있는 연결된 객체들의 네트워크[5]
M2M	휴먼과의 상호작용 없이 Subscriber 머신과 서버 또는 Subscriber 머신 상호간의 정보교환[10]
	휴먼의 직접적 간섭 없이도 두 엔터티 이상에서 이루어질수 있는 통신[11]
MTC	휴먼 상호작용이 없어도 가능한 하나 이상의 엔터티가 관여하는 데이터 통신의 한 형태[12]
D2D(LTE기반)	코어네트워크나 기지국의 연결없이 근접거리에서 LTE 무선인터페이스를 이용한 사용자 단말간 직접통신[13]

글로벌 기업들은 사물인터넷 시장 및 표준화의 선점을 목표로 독자적인 기술개발을 통해 다양한 분야를 개척하고 있다. 이에 [8]은 2020년까지의 유망 기술로 아키텍처(architecture)나 상황 인지적 해결, 자가 관리, 자가 제어, 바이오 안테나, 바이오 배터리(bio-battery) 등 자율 프로세싱 기술로 초점이 맞추어질 것으로 예측하고 있으며, 최근 이슈가 되고 있는 사물인터넷의 주요 기술들을 표1과 2와 같이 정리하고 있다. 표1은 인식 보안(cognitive security)과 자가관리적 보안, 지역적 보안 등이 이슈가 되고 있으며, 이는 사물인터넷의 광범위한 분야와 기기들을 보호하기 위한 사물인터넷의 특성을 반영한 것으로 해석해 볼 수 있다. 그리고 표2는 앞서 표1의 기반 기술로서, 인간과 상호작용 없이도 독립적으로 동작하거나 자동 연결 및 교환되는 사물기기들과의 연결 등 사물인터넷 기기들 간의 통신에 필요한 기술들을 정리하고 있다. 이들 기술들을 살펴보면, M2M(machine to machine)은 사물인터넷의 기반 기술로 기기들 간 정보 교환 및 네트워킹을 수행하도록 하며, MTC (machine type communications)는 인간의 상호작용 없이도, 통신을 가능케 한다. 그리고 D2D(device to device)는 사용자 단말기 간의 인터페이스를 통해 직접적인 통신이 가능하도록 하고 있다. 이밖에 관련 프로토콜 기술로는 문서나 이미지, 서비스 등의 정보들에 대해 리소스의 생성, 읽기, 삭제, 업데이트 처리 등 기기들 간의 상태 전송을 지원하는 REST (Representational State Transfer)가 있으며, 대용량의 메시지를 전달하는 프로토콜로 MQTT(Message

Queuing Telemet ry Trans port)가 있다. 그리고 국제 표준(IETF) 프로토콜로서 다수 클라이언트 간에 실시간 메시지 교환이 가능한 프로토콜인 XMPP (eXtensible Me ssaging and Presence Protocol)와 센서(sensor) 노드(node)와 같이 제한된 성능으로 디바이스들의 통신이 가능하도록 만들어진 CoAP(Constrained Environments Application Proto col)프로토콜이 사용되고 있다. 이러한 사물인터넷 관련 기술들은 계속해서 보완 또는 개발되고 있으며, 표준화 작업도 활발히 진행 중에 있다.

3. 사물인터넷의 보안사고와 위협

3.1 사물인터넷의 보안사고 사례

최근 사물인터넷 산업은 글로벌 시장을 빠르게 선점해가고 있으며, 이와 관련한 산업들 또한 동반성장을 꾀하고 있다. 그러나 사물인터넷은 광범위한 산업분야와 효과적인 공격이 가능하기 때문에 이에 따른 위험성은 점차 높아지고 있다. 이에 대해 몇몇 사례들을 살펴보면, Wired지는 사람이 탑승한 상태에서 고속도로 주행 중, 자동차의 시동을 원격에서 끄는 실험을 보도한 바 있다. 그리고 '남 앨라배마 대학(University of South Alabama)의 학생들은 네트워크와 동기화된 심박 조율기(pacemaker)의 임의 조작으로 심박속도를 조절함으로써 환자에게 심각한 위험을 야기할 수 있다'고 밝힌바 있다. 이러한 사건 이후, 미연방수사국(FBI, Federal Bureau of Investigation)과 미국 국토안보부(DHS, Department of Homel and Sec urity)는 사물인터넷에 대한 경고 메시지를 발표하였다. 그리고 미방위고등연구계획국(DARPA, Defense Advance d Research Projects Agency)은 해킹을 방지할 수 있는 비행기 혹은 자율주행 자동차의 물리적 통제시스템의 코드를 개발하는 프로그램을 시작하였고, 미연방수사국(FBI)은 이러한 문제를 해결하기까지 주의해야할 사물인터넷 관련 디바이스(device)들을 예시하기도 하였다[9]. 이와 같은 사례 및 조치들은 사물인터넷의 해킹 공격이 점차 지능화되고, 공격 대상 또한 가전제품을 사용하는 일반인들을 대상으로 하고 있어, 향후 공격 대응이 어려워 질 것으로 예상되며, 앞서 권고사항들을 통해 공격의 심각한 수준에 이르고 있음을 알 수 있다.

3.2 사물인터넷의 위협 요인 분석

3.2.1 가로채기 공격 유형

무선 전송 매체를 사용하는 사물인터넷은 많은 기기들로부터 적은 용량의 데이터를 수집 및 전송하며, 시간적, 공간적 제한은 받지 않기 때문에 다수의 사물들을 연결하는데 사용되고 있다. 그러나 가로채기(intercept) 공격에 취약하여 위협요인이 되고 있다. 이에 대한 대응 기술로 무선 인증과 데이터 암호, 보안 채널(secure channel), 터널링(tunneling) 등이 있지만, 사물인터넷 기기의 수가 증가할 경우, 성능 및 관리상의 문제들이 발생하는 단점이 있다. 따라서 구축환경 및 문제점을 고려한 대응 방안이 마련되어야 한다.

3.2.2 방해 및 위·변조 공격 유형

방해(interrupt) 공격은 유·무선의 경계 없이 시도되고 있으며, 이에 따른 피해도 지속적으로 증가하고 있다. 대표적인 공격 유형으로는 '서비스 거부 공격(denial of service)'이 있으며, 최근 사물인터넷과 관련해 전기 포트 및 전기다리미, 전자 담배, 냉장고 등의 가전제품에 무선 랜을 연결할 수 있는 부품을 삽입해 공격하는 사건들이 빈번히 발생하고 있다. 따라서 이와 같은 사물들을 이용한 공격의 증가에 따라, 경제적, 시간적 손실이 매우 커질 것으로 전망되며, 이에 대한 대응 방안 마련 또한 쉽지 않을 것으로 예상된다. 그리고 위조(fabrication)와 변조(modification) 공격은 유·무선 네트워크상에서 전송 또는 저장 데이터에 대한 위·변조나 사용자를 위장한 공격 등을 포함하며, 복합 형태로 공격이 이뤄진다. 이에 대한 사례로 최근 원격지에서 인가된 사용자를 위장해 자동차의 제어장치를 조작하거나 정상적인 기기를 가장해 공격하는 등 인간의 생명까지 위협하고 있으며, 인증 또는 전송 데이터에 대한 위·변조 공격을 통해 2차적인 공격으로 이어져, 막대한 경제적 손실뿐만 아니라 개인의 생명까지 위협하는 요인이 되고 있다.

3.2.3 바이러스 및 웜 공격 유형

사물인터넷은 궁극적으로 기기들을 관리할 시스템을 필요로 하기 때문에 바이러스 및 웜의 유입 가능성을 배제할 수 없다. 그러나 이와 같은 공격에 대응하기 위해 백신을 사용할 경우, 속도 저하문제와 이를 악용한 공격 가능성을 배제할 수 없다. 따라서 바이러스 및 웜은 사물인터넷 기기나 사물들을 관리할 시스템(스마트 기기 등) 등에 위협요인이 되고 있으며, 인터넷과의 연결이 될 경우, 피해 확산이 매우 빠르게 진행될 것으로 예상된다. 따라서 바이러스 및 웜의 공격 차단을 위해 문제점들이 고려된 대응 방안이 마련되어야 한다.

4. 보안 대응

4.1 정보보호 요소별 대응 분석

4.1.1 기밀성과 무결성

기밀성(confidentiality)은 가로채기 공격에 대한 대표적인 대응 기술로 암호화를 통해 비밀성을 보장한다. 최근 커넥티드(connected) 자동차에 대한 원격 통제가 가능함을 증명한 실험으로 사물인터넷 기기간의 송·수신 데이터에 대한 가로채기 공격의 가능성을 배제할 수 없다. 특히 사물인터넷의 대표적인 공격 대상으로 스마트폰(smart phone)과 스마트 홈을 꼽아 볼 수 있으며, 이들을 연결하는 네트워크의 경우, ZigBee나 WiFi, RFID, Bluetooth 등 무선 전송매체의 사용으로 위험성이 매우 높다. 따라서 각각의 무선 전송매체들은 보안성 제공을 위해 다음과 같은 보안 대응 기술을 적용하고 있다. ZigBee는 SSM(Standard Security Mode)과 HSM(High Security Mode) 2가지 모드를 제공함으로써 보안대응을 하고 있으며, Open Trust Model 방식의 암호화를 제공하고 있다. 그리고 WiFi는 TKIP(Temporal Key Integrity Protocol)과 CCMP(Counter mode with CBC-MAC Protocol 등의 보안 프로토콜을 제공하고 있다[10]. 그러나 무선 전송매체에 대한 보안성과 무결성 제공은 기기들의 종류와 유형, CPU, 메모리의 크기 및 소비전력, 전송 속도 등 여러 환경들을 제약하기 때문에 강제화할 수 있는 상황은 아니다. 이에 대해 최근 미래창조과학부는 민간 자율의 사물인터넷 보안 내재화를 위한 “2015년 사물인터넷 보안 얼라이언스”를 통해 정보보호 요소(기밀성, 무결성, 인증성)를 고려한 사물인터넷 기기 및 정보의 오용을 최소화할 수 있는 방안에 대해 논의된 바 있다[11]. 이밖에도 무선에 대한 대응 방안으로 경량 암호 사용이나 하드웨어 암호 모듈화가 제안되고 있으나[12], 사물인터넷 기기 수와 무선 환경, 데이터 량 등과 같은 환경 변수들로 인해, 향후 기밀성과 무결성 적용 여부가 사물인터넷 기기의 크기와 성능, 시장성에 매우 큰 영향을 미칠 것으로 예상된다.

4.1.2 인증성과 접근 통제성, 가용성

사물인터넷 기기들에 대한 인증 문제는 매우 중요하다. 현재 ‘스마트 홈’ 서비스에 적용 및 사용되고 있는 기기 인증 및 사용자, 관리자에 대한 인증 정보의 유출문제는 사물인터넷 기기들에만 국한 된다고 볼 수 없다. 특히 인증 정보의 유출은 단순히 망 공격뿐만 아니라, 유출된 인증정보를 악용한 제3의 공격 이 가능하며, 개인정보의 유출 및 경유지로 악용될 소지가 있기 때문이다. 따라서 개인정보의 관리 및 취급, 사용에 대한 인식 개선과 교육과 관리 및 취급자에 대한 가이드라인의 마련이 필요하며, 접근자에 대한 식별 기술의 보완 및 개발을 통해 인가되지 않은 사용자 및 기기 등의 통제가 이뤄져야 한다. 그러나 이와 같은 인증 및 접근 통제 기능을 사물에 탑재할 경우, 이에 따른 속도 저하 및 시스템 부하 증가 등의 문제들이 동반함을 고려한 대응방안이 마련되어야 한다. 그리고 관리 시스템의 경우, 기기들을 악용한 공격에 취약하기 때문에 ‘서비스 거부 공격(denial of service)’과 같은 공격에도 노출되게 된다. 따라서 관리시스템의 가용성 보장을 통한 대응이 필요하며, 기기들 간의 보안채널과 같은 연결 유지기능을 통해 불필요한 데이터의 유입이 방지되어야한다.

5. 결 론

최근 사물인터넷은 다양한 산업분야와 일상생활 깊숙이 응용범위가 확대되면서 빠른 속도로 진화하고 있

으며, 관련 기술들은 응용범위의 확장과 함께 새롭게 개발 및 등장하고 있다. 그러나 이러한 상황에서 사물인터넷에 대한 공격기술은 다양한 공격 대상과 유형으로 나타나고 있어, 사물인터넷 기술의 활성화와 보편화, 기술발전 등에 저해요인으로 작용할 것으로 보이며, 향후 보안사고의 규모 및 경제적 손실이 크게 증가할 것으로 예상되고 있다. 따라서 본 논문은 최근 사물인터넷의 보안 기술과 위협요인들에 대해 대표적인 공격유형에 따른 분석과 정보보호 요소별 대응방안의 분석을 통해, 보안 취약성 분석 및 사고예방, 보안 기술 개발, 사물인터넷 기술 개발 등에 유용한 자료로 활용될 수 있을 것으로 기대한다. 그러나 향후, 사물인터넷의 응용 범위의 확장과 다양한 기술 개발이 예상되고 있는 가운데 사물인터넷의 발전에 따른 폭넓은 보안위협요인 및 취약성 분석에 체계적이고, 지속적인 연구를 통해 대응 방안 마련 및 새로운 보안 기술개발이 이뤄져야 할 것이다.

참고문헌

[1] http://www.zdnet.co.kr/news/news_vie w.asp?artice_id=20150501190021, “MS 사물인터넷 용 윈도우10 전격공개,” ZDNet Korea, 2015.5.1

[2] http://www.dongascience.com/news/vie w/7952, “떠오르는 사물인터넷 보안 먼저 해결해야,” 동아사이언스, 2015.8.28

[3] 미래인터넷팀, “미(美) 국제 전자제품 박람회(CES) 2015 동향분석,” 한국인터넷진흥원, Internet & Security Focus, pp.30-44, 2015.1

[4] 전정훈, “사물인터넷 기술동향과 전망에 관한 연구,” 융합보안학회, vol.14, no.7, 2014.12

[5] 이현지, 김광석, “사물인터넷의 국내외 시장 및 정책 동향,” 한국정보통신기술진흥센터, 주간기술동향, 2015.9.16

[6] KIET 산업연구원, “사물인터넷 시대 안전망, 융합보안산업,” E-KIET 산업경제정보, no.586, 2014.4.15.

[7] http://www.zdnet.co.kr/news/news_view.asp?artice_id=20150726142756, “크라이슬러, 자동차 140만대 리콜 해킹위험 때문,” ZDNet, 2015.7.26.

[8] 전정훈, “사물인터넷의 기술 동향과 전망에 관한 연구,” 한국융합보안학회, vol.14, no.7, 2014.12

[9] http://mirian.kisti.re.kr/futuremonitor/ view.jsp?cn=GTB2015090245&service_code=03, “FBI and DHS Warn of Security Risks from the Internet of Things,” 2015.9.21.

[10] 장봉인, 김창수, “사물인터넷 보안 기술 연구,” 보안공학연구논문지, Vol.11, No.5, 2014.10

[11] 미래창조과학부, “사물인터넷 보안 얼라이언스,” 보도자료 2015.6.18.

[12] 박지예, 신새미, 강남희, “사물인터넷 환경에서 경량화 장치 간 상호 인증 및 세션키 합의 기술,” 한국통신학회논문지, Vol.38B, No.09, 2013.3.8.

[저자소개]

전 정 훈 (Jeong-hoon Jeon)

2000년 8월 숭실대학교 일반대학원 컴퓨터학과 공학석사
2008년 2월 숭실대학교 일반대학원 컴퓨터학과 공학박사
2005년 5월~ 현 동덕여자대학교 컴퓨터학과 교수

email : nerdrandy@dongduk.ac.kr