IOT(Internet of Things) 보안 기술 동향
Technology Trends for IOT Security

김시정(한남대학교), 조도은(목원대학교)

차 례

■ keyword : | IOT 서비스 | IOT 보안 | 사물인터넷 | 보안 위협 |

1. 서론

최근 ICT(Infomation Communications Technologies) 환경의 비약적인 발달로 일상생활 환경에서 사물과 인터넷의 연결을 통한 다양한 서비스가 제공되고 있다. 더불어 유비쿼터스 환경 제공의 가속화로 사물인터넷(IOT)와 사물지능인터넷(M2M)에 대한 관심이 매우 높아지고 있다. 전문가들은 향후 10년간 유망한 IT 분야로 IOT를 꼽고 있다. IOT에 대한 미래 전망이 밝은데 힘입어 우리나라는 2009년에 방송통신위원회에서 "사물통신 기반구축 기본계획안" 을 발표 했고, 현재 미래창조과학부를 중심으로 다양한 서비스 개발, R&D 지원, IOT 인프라 구축을 추진하고 있다[1].

이렇게 IOT 서비스는 IT 기술 발전 로드맵의 핵심이 되고 있다. 그러나 다양한 서비스 개발을 통한 활용 사례를 분석해 보면 해결 되어야할 문제점이 대두 되고 있으며, 서비스 보급 확장에 따른 여러 가지 문제점이 도출되고 있다. 이와 같이 사물 인터넷은 사람과 사물의 보다 편리한 정보 송수신을 제공하여 새로운 서비스 시장의 확대 등의 많은 이점이 있으나 다양한 이기종의 유·무선 통신상에서 발생할 수 있는 보안상의 취약성을 가지고 있다. 특히, 다양한 플랫폼 환경에서 발생할 수 있는 보안 문제들의 해결이 매우 시급하다.

본 논문은 활발히 개발되고 있는 IOT의 서비스의 보안 동향 및 보안의 취약성에 대하여 살펴보고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 IOT의 기술 요소와 서비스의 동향을 살펴보고, 3장에서는 IOT 서비스의 보안 위협에 대하여 서술한다. 그리고 4장에서는 취약성 대응 동향을 기술하고 마지막으로 결론을 맺는다.

2. IOT 서비스 이용 사례

2.1 IOT 서비스

ITU-T world Summit on the information Society의 "ITU Internet Report"에서 사물인터넷의 개념을 "정보통신 기술을 이용하여 사람과 사물간의 언제 어디서나 정보를 송수신할 수 있게 해주는 기술 (2005)" 이라고 정의하고 있다 [2].

또한 미래창조과학부는 "사람과 사물 그리고 사물대 사물 간의 지능통신 서비스를 언제 어디서나 안전하고 편리하게 실시간으로 이용할 수 있는 미래 방송통신 융합 ICT 인프라 (2009)"라고 정의했다.

IOT는 현재 다양한 분야에 서비스 응용이 적용되고 있다. 1차 산업 환경에서부터 미래 산업의 전반에 걸쳐 그 서비스가 확대되고 있다.

최근 IOT는 모바일 플랫폼을 기반으로 스마트화 되어 가고 있다. 또한 좀 더 개방된 표준화를 기반으로한 환경에서는 서비스를 위한 앱 개발 자체보다 앱 개발 인터페이스등의 소프트웨어적인 요소를 기기에 활용하기 위한 노력이 증가하고 있다.

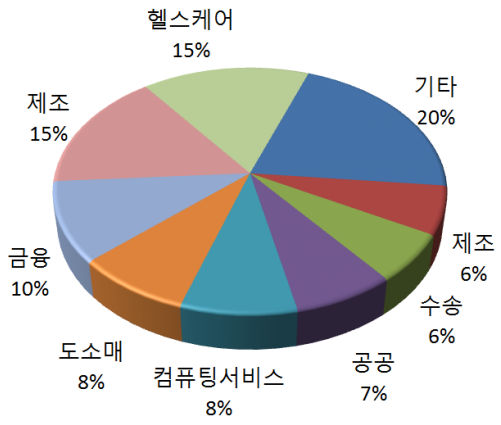
특히 IOT 플랫폼 분야는 초기 관리/서비스 위주의 정리와는 다르게 하드웨어 , 서비스 제공 디바이스, 통신 네트워크, Data Field등의 별도 Zone 플랫폼 산업으로 발전하고 있다.

아래 [표 1]은 사물인터넷의 각 분야에 걸친 응용을 나타낸 것이다[3].

표 1. 사물인터넷 적용 분야

분야	내용	서비스 제품
헬스 케어	전강보조도구, 헬스 정보 송수신, 스마트폰을 이용한 헬스 케어 앱	핏빗플렉스(핏빗), 픽스(코벤티스), S헬스 서비스(삼성전자), 2net(퀄컴), 트윗피(하기스)
홈케어	조명 제어, 지능 주택관리, LBS방법, 외출 보안 시스템, 냉난방환기 자동 조절, 스마트 홈서비스	스마트싱스(Smartthings), 스마트홈, 스마트라이프(SKT)
자동차	텔레매틱스, 무인자동차, 스마트카, 커넥티드 카, 차량원격관리	OnStar(GM), Sync(포드), 블루링크(현대차), 무인자동차(구글), 스마트 오토모티브(SKT)
교통	교통안전, 국도 모니터링, 배기가스 실시간 감지, 택시 무선 결재, 디지털 운행관리	지능형 교통 서비스, 지능형 주차 서비스 SF Park(샌프란시스코시)
농협	실시간 작물 상태 모니터링, 온도/습도 감지 조정, 농작물 수확량 재고관리	스마트팜(SKT), 지능형 파종 서비스, 지능형 젖소관리 서비스(네델란드 사프크드사)

다음 [그림 1]은 2020년까지 향후 산업별 IOT에 대한 부가가치 창출 비중을 나타낸 것이다.



▶▶ 그림 1. 2020 산업별 IOT 부가가치 창출 비중[4]

2.2 보안 기술 요소

Gartner(2013)는 IOT의 구성요소(Elements of the IOT)를 수평적인 기술요소(horizontal technologies) 시장과 수직적인 산업(vertical industrial sector) 시장으로 구분하여 분석 제시 한바 있다[5].

IOT는 다양한 통신 기술의 적용으로 그에 따른 보안 기술 적용이 필요하다. IOT 서비스의 보안 기술은 유·무선 네트워크, 첨단 단말기 및 센서, 사물·사람·장소에 관한 Big 데이터 통신 등의 인터넷 구성 요소에 대한 다양한 해킹 및 정보 유출, 위변조를 방지하기 위한 기술등을 말한다.

IOT 서비스 사례는 다양한 분야에 적용되고 있다. 때문에 서비스 적용 분야에 따라 기능·애플리케이션·인터페이스 등이 매우 다양하므로 이에 따른 다양한 네트워크 환경을 기반으로 하므로 개별적으로 적합한 보안 기술 적용이 요구된다. IOT의 보안 이슈는 다음과 같다 [6].

- 프로토콜 및 네트워크 보안 (Protocol and - Network Security)
- 정보 보호 및 사생활 보호(Data and Privacy)
- 시스템 장애 방지(Fault Tolerance)
- 계정 관리(Identity management)

3. IOT 보안 위협

3.1 보안 위협

IOT 서비스에 관련한 터미널 및 시스템의 경우 데이터를 스스로 확보하고 처리하는 기능을 탑재 하였다면 사이버 공격의 주요 목표가 될 수 있다. 특히 사물인터넷의 터미널은 아직까지 단순한 컴퓨팅 기능과 보안성에 매우 취약한 것이 현실이다. IOT 단말의 보안상의 문제점은 다음과 같다[3].

- 사물인터넷 단말의 취약성이 크다.
- 서비스의 다양성 문제로 보다 수준 높은 보안 솔루션의 도입이 어렵다.
- 데이터 통신상의 외부공격에 대한 확인이 어렵다.
- 네트워크 구조의 복잡성으로 인한 침입 경로가 매우 다양하다.

IOT 서비스는 통신 구조와 서비스 단말기가 매우 다양하다. 간단한 통신 기능을 탑재한 단말기의 경우 개별적 소프트웨어 설치 등을 통한 구동이 어렵기 때문에 보안 모듈의 장착이나 통합적인 제어 시스템에 대한 보안 솔루션 적용이 요구된다. 아직까지 일반 가전제품에 대한 해킹 공격을 확인할 수 있는 방법은 많지 않다. 대규모의 피해 사례는 보고되고 있지 않지만, IOT에 대한 보안 문제는 이미 가시화되고 있다.

다음은 보고된 IOT 서비스와 관련된 보안상의 문제점이다 [6].

- 2013년 9월 미국연방거래위원회는 보안용 웹 카메라 벤더 트랜드 넷(TRENDnet)의 CCTV 제품에 시큐어 뷰어(SecureView)가 보안상의 결함이 있음을 인정
- 독일 IT 보안업체 리큐리티랩스(Recurity Labs)는 2013년해킹 실험을 통해 독일 남부 에틀일겐(Ettlingen) 의 전력 공급을 외부에서 무단으로 차단할 수 있음을 입증함으로써 보안상의 심각성을 가시화
- 2010년 이스라엘과 미국이 이란의 핵 설비를 마비시키기 위해 사용했던 바이러스 스턱스 넷(Stuxnet)의 존재가 알려지면서 주요 기반 시설에 대한 해킹의 문제점 대두
- 2014년 11월 국내에서도 SK 브로드밴드 및 LG유플러스의 네트워크를 목표로한 공격이 발생해 각 통신사의 서비스가 일시적으로 장애를 일으키는 사고 발생

3.2 보안 취약성 분석

사물인터넷은 여러 가지 구성 통신 기술과 다양한 단말기 상의 취약성, 이미 출시된 다양한 서비스에서 그 취약성이 나타나고 있다 [7]. 사물인터넷을 구성하는 각 요소 기술의 보안 기술은 디바이스나 운영체제 기술, 통신 및 네트워크 기술 웹 서비스 및 응용 서비스 등에서 네트워크 보안 요소, 즉 기밀성, 무결성, 인증, 접근제어, 외부의 해킹 방지, 비인가된 접근 차단 등의 보안 기술의 향상으로 보안의 취약성에 대응하고 있다. 다음은 IOT의 보안상의 취약성을 분석한 것이다 [8].

- IOT 단말의 취약성 : 정보 인식의 입력 노드 및 태그의 비정상적인 조작과 데이터 리더의 동작 중 불법적인 도청, 비인가된 사용자의 불법적인 접근이 가능하다.
- 데이터 서버의 취약성 : 서버에서도 불법적인 도청과 디렉토리 서버 공격에 취약하고, 데이터 서버에 대한 불법적인 정보 획득에 취약하다.
- 센서 네트워크의 취약성 : 센서 네트워크 특성상 다양한 보안 기술의 응용 및 개발이 어렵다. 센서의 물리적 위치성 및 접근성에 대한 보안성이 취약하다. 센서로의 불법적인 데이터 도청 및 센서의 물리적인 제거 및 비정상적인 설치 시도 등의 보안상 문제점이 대두된다. 단말 센서로부터 유입되는 데이터의 암호화 적용 모듈이 필요하다.
- 애플리케이션의 취약성 : 서비스 접근시 보안/인증에 대한 보안 모듈이 요구된다. 미들웨어를 통한 데이터 유입시 단말의 운영체제 하드웨어 자원 등에 가상화 기술을 통한 논리적 물리적 격리 및 접근의 관리에 취약하다[9].
- 자원 송수신의 취약성 : IOT 단말을 통해 송·수신되는 자원은 매우 제한적이다. 때문에 외부 공격자의 지속적인 접속 시도 및 서비스 요청에 대한 서비스 거부 공격에 취약하다. 미들웨어 그룹에서 발생하는 트렌젝션에 대한 효율적인 분배와 로그정보에 대한 전송에 보안상의 문제점을 야기 할 수 있다.

다음 [표 2]는 IOT 구성 요소에 대한 보안 위협이다 [4].

표 2. IOT 구성 요소의 보안 위협

구성요소	보안 위협
단말장치	사용자의 분실/도난 사고,파손
센서 네트워크	통신교란, 정보의 도청, 위조/변조,
서비스	정보의 유출, 데이터 위조/변조, 서비스 거부
서버	불법적인 접근, 악성코드,

4. 취약성 대응 동향

4.1 IOT 취약성 대응 분석

이와 같이 사물인터넷의 보안이 IT 전반에 걸쳐 새로운 문제로 대두되면서 사물 인터넷의 취약성에 대응하기 위해 민간 연구기관은 물론 국가 기관도 연구에 노력을 기울이고 있다. 월포트 보고서는 사물인터넷은 사회전반에 걸친 인터넷 혁명이라고 언급한바 있다. 때문에 디지털 혁명이라 부를 만한 변화를 가져올 잠재력이 존재하지만 이와 동시에 보안 위협과 개인정보 침해에 따른 문제점이 심각하다 [5].

이미 미국과 유럽 여러 나라들은 사물인터넷 서비스를 통한 보안 침해를 우려하여 제도적 지원을 검토 중에 있다. 사물인터넷 서비스 시장을 자율적으로 규제하면서, 능동적으로 분야별 보안성 귀제의 적용을 고려하고 있다.

• IOT 구성 장비에 대한 보안[10]

IOT를 구성하고 있는 장비는 유·무선서비스와 스마트 장비의 결합으로 이루어져 있다. 또한 장비의 특성상

경량의 장비로 구성되어 있다. 때문에 저전력 암호화 모듈의 적용이 필요하다. 또한 IOT 플랫폼의 구성 운영체제에 대한 보안 모듈의 운영이 필요하다. 뿐만 아니라 기기의 인증에 대한 위조 및 변조의 방지용 보안 솔루션이 적용된다.

• IOT 서비스를 위한 네트워크 보안

IOT 서비스를 위한 네트워크는 기존의 네트워크와 센서 네트워크가 응용된다. 때문에 게이트웨이에서의 보안 솔루션 적용과 네트워크의 외부로부터의 침입에 대응 하는 솔루션이 적용되어야 한다. 또한 IOT는 원격 제어 서비스 응용이 다양하므로 원격 보안 관리에 대한 보안성 강화도 역시 필요하다.

• IOT 플랫폼과 애플리케이션 보안

IOT는 기존의 스마트 장비에 대한 적용이 대부분을 차지한다. 때문에 서비스에 사용되는 스마트 장비에 대한 철저한 보안 인증이 필요하다. 뿐만 아니라 가정과 개인이 접속하여 사용하는 경우 금융, 헬스 등의 개인정보에 대한 암호화 전송 기술과 정보 열람의 접근 제어에 대한 보안 모듈이 적용되어야 한다[11].

• 모바일 금융 적용 따른 강화된 보안

이미 일반화된 모바일 금융 서비스를 기반으로 하고 있는 IOT 서비스는 강화된 보안 모듈로 사용자 인증 및 데이데 암호화, 단말에 대한 특수성을 고려해야 한다. 더블어 프라이버시에 대한 보안성도 고려해야 하며 개인정보 송수신과 접근, 정보관리 라이프 사이클을 적용하여 보안성 또한 높여야 한다.

4.1 정부의 대응 동향

사물인터넷 서비스 보안을 위한 국내 정부의 대응은 현재 보안 내재화된 사물인터넷 7개 분야[12]로 규정하고 각 산업에 대해 공통적인 사물인터넷 보안 원칙을 수립하였다. 또한 분야별 세부 보안 고려사항을 도출하여 업계가 수용 하도록 유도하고 있다.

2015년부터 추진되는 “보안 내재화 사업”에서는 국민 일상생활과 밀접하고 사용화가 가장 빠르게 이루어지는 분야별로 적용하고 2016년 이후 나머지 산업분야에 대한 보안 원칙 적용이 도입될 예정이다.

또한, 사물인터넷 사용자가 보다 안심하고 서비스에 접근할 수 있도록 보안 인증 제도를 적용하고 민간인증 시스템의 활용도 활성화할 예정이다.

정부의 보안 로드맵에 따르면 저사양 디바이스 보안 기술에 대해서 백신, 암호화, 인증에 대한 개발 및 적용, 그리고 디바이스관리에 따른 기기 운영의 신뢰성 보장, 무결성 검증, 센서/디바이스의 보안 패치 적용 등이 있다.

또한 네트워크 장비의 모니터링을 위한 이중망 연동을 위한 프로토콜 상호 운용성 기반 마련과 이기중 사용에 따른 네트워크 환경을 고려한 보안 기술의 적용을 요구하고 있다.

상호 인증 키관리 및 신뢰키 관리를 위한 안전한 개방형 플랫폼 이용 지침과 디바이스/사용자 서비스 상호간의 인증키에 대한 신뢰할 수 있는 보안 모듈의 필요 등을 포함하고 있다.

5. 결론

통신 서비스의 다양화와 스마트 기기의 보급이 가속화 됨에 따라 다양한 IOT 서비스가 개발되어 일반에 제공되고 있다. 현재 사물인터넷 서비스 기술은 미래 개발 핵심이라고 지목 된다. 유비쿼터스 기술과 통신 기술 그리고 스마트 기기를 통한 서비스 응용은 다방면으로 산업과 생활에 접목되고 있다.

뿐만 아니라 사회 기반 시설의 접목도 이루어져서 많은 기반시설의 관리 및 모니터링에 사물 인터넷 서비스가 제공 된다. 하지만 이로 인한 문제점도 대두되고 있다. IOT 서비스를 위한 통신에서도 기존의 통신 기반 서비스에 존재하는 보안상의 문제점은 물론 IOT 기반의 특성을 동반하는 보안상의 취약성을 나타내고 있다.

이미 여러 서비스 형태에서 보안상의 취약성이 보고 된 바 있다. 무선 단말 장치에 대한 물리적 분실 및 도난, 무선 통신에서의 신호 교란과 외부의 비정상적 접속, 데이터 송수신시 정보 유출, 도청, 위조/변조, 그리고 서비스 거부 공격에 취약하다 이에 대안 보안 대응책이 적용되어야 한다. 특히 IOT 보안의 대응 방안은 그 서비스의 특성에 따라 사례별로 적용되어야 하는 어려움이 있다. 본 논문은 IOT 서비스의 개발 사례를 살펴 보고, 서비스 제공 환경에서 발생할 수 있는 보안상의 문제점을 서술하였다. 또한 IOT 서비스 기술 구조를 통해 보안상의 취약성을 살펴 보고, 이에 대한 대응 방안과 정부의 대응

동향에 대하여 기술 하였다. 앞으로 정부의 IOT 보안 위협에 대한 대응 방안을 기반으로 IOT 서비스의 적용 분야별로 개방적 능동적 보안 모듈적용에 대한 연구 및 개발이 요구 된다.

참고문헌

[1] 김동희, 윤석웅, 이용필, “IOT 서비스를 위한 보안”, 한국인터넷진흥원, 8, 2013

[2] Matk Weisr, “The Computer for 21st Century”, Scientific American, 1991.

[3] https://securityin.wordpress.com/2014/10/27/1-iot-%EA%B5%AC%EC%84%B1-%EC%9A%94%EC%86%8C-%EB%8F%99%ED%96%A5/

[4] Cisco, Gartner, Machine Reserach, K&C Consurting

[5] 산업연구원, “사물인터넷 시대의 안전망, 융합보안산업”, 4, 2014

[6] 심층보고서, “사물인터넷 보안 위협 동향”, Internet & Security Bimonthly, vol 5, 2014.

[7] 손태식, 고종빈, “Cloud Computing에서의 IOT(Internet of Things) 보안 동향”, 정보보호학회지, 제22권 제2호, 2, 2012.

[8] 심승현, 김학범, “사물인터넷 MQTT 기술”, 정보보호학회지, 제24권 제6호 12, 2014.

[9] 김우년, “Homeland Security 에서의 M2M(사물지능통신)” 보안 동향, 정보보호학회지, 제22권 제2호, 2, 2012.

[10] 김호원, “사물인터넷 환경에서의 보안/프라이버시 이슈”, TTA Journal vol. 153, 05/06 2014.

[11] http://www.fnnews.com/news/201410300834296404

[12] 미래창조과학부, “사물인터넷(IOT) 정보보호 로드맵”, 10, 2014.

저자소개

● 김 시 정(Si-Jung Kim)

- 1990년 2월 : 한밭대학교 컴퓨터공학과 (공학사)
- 1995년 8월 : 한남대학교 컴퓨터교육학과 (교육학석사)
- 2002년 2월 : 한남대학교 컴퓨터공학과 (공학박사)
- 2013년 2월 ~ 현재 : 한남대학교 초빙교수

<관심분야> : 정보보안, 멀티미디어, 스마트그리드

- E-Mail: sjkim6183@daum.net

● 조 도 은(Do-Eun Cho)

- 1997년 2월 : 충주대학교 컴퓨터공학과 (공학사)
- 2001년 2월 : 세명대학교 컴퓨터교육학과 (교육학 석사)
- 2007년 2월 : 충북대학교 컴퓨터공학과 (공학박사)
- 2008 ~ 현재 : 목원대학교 공학교육혁신센터 조교수

<관심분야> : 정보보호, 유비쿼터스보안, USN, 스마트그리드

- E-Mai : decho@mokwon.ac.kr