IoT 보안 이슈 및 국내외 보안기술 개발동향

박 세 환
한국과학기술정보연구원
ReSEAT프로그램
전문연구위원

Ⅰ. 서 론

사물인터넷(IoTs : Internet of Things) 기술 기반의 웨어러블 기기 및 스포츠 용품, 헬스 케어 플랫폼[1] 등 다양한 서비스들이 출시되고 있다. 이를 통해 RFID/USN 기반의 초 연결사회를 구현할 수 있는 기반을 제공하고 있다[1-3].

이 연구에서는 공공 및 사설 네트워크의 특화된 보안강화 전략이 필요한 IoT 프라이버시 보호방안과 IoT 보안위협 요인 및 사례 중심의 IoT 보안 이슈, 국내외 IoT보안 대응 기술개발 및 기업동향에 대해 설명한다.

Ⅱ. IoT 보안 이슈

1. 프라이버시 보호방안

공공 및 사설 네트워크/RFID 기반의 센서네트워크/3G~4G-LTE(A) 등 다양한 네트워크, 단순 신호처리 기능을 가진 저전력/저비용의 센서, 상용OS가 탑재된 시스템 및 단말 등에 따라 특화된 보안전략이 필요하다. IoT 네트워크 보안은 보호할 대상, 범위, 특성, 보안담당 주체 및 보호방법 등에 대해 기존의 사이버 환경과 다른 새로운 시각으로 접근할 필요가 있다. 특히 IoT 네트워크 구축환경에는 기기의 연결방식, 네트워킹, 객체의 속성 등 다양한 환경조건들이 존재한다. 따라서 각 액세스 포인트마다 더욱 주의가 필요하다. IoT 보안위협에 대응하기 위해서는 센서 및 기기, 통신 및 네트워크, 플랫폼, 응용서비스로 구분하여

1) IoT 시스템에서 헬스 케어 플랫폼은 Integrator platform과 Two-sided platform으로 분류할 수 있다. 그러나 이들 분류기준이 많아 어떤 IoT 기기가 어떤 플랫폼에 적용될 수 있는지가 분명하지 않은 점이 있다.

다음과 같이 각각의 보안시스템을 구축할 필요가 있다[4].

- 통신 및 네트워크 : 불완전하게 정의된 표준의 난립으로 인해 과도한 SSL(Secure Sockets Layer : 네트워크 데이터 암호화 프로토콜[2])에 의존하게 됨으로써 보안에 취약한 편이다. 이를 해결할 수 있는 보안시스템을 구축전략이 필요하다.
- IoT 기기 : 가격에 따라 CPU나 메모리 등의 성능이 다양하여 소프트웨어 업데이트 및 관리가 쉽지 않다. 따라서 기존의 보안기술을 적용하기에 어려움이 있어 보안에 취약한 편이다. 이를 해결할 수 있는 보안시스템을 구축전략이 필요하다.

따라서 가장 효과적으로 프라이버시를 보호하기 위해서는 정보의 「센싱-가공-처리-저장-활용」의 supply chain 단계별로 특화된 프라이버시 보호기능을 제공할 필요가 있다. 또한 IoT 보안을 위한 침해대응 체계를 다음과 같이 전면 개선할 필요가 있다.

- IoT 관련 새로운 보안취약점이나 악성코드발생 시 이에 대한 신속한 탐지와 분석을 통해 대응체계를 마련할 필요가 있다.
- 관련 업체 간 경쟁보다는 정보공유를 통한 협력체계를 구성하는 것도 매우 중요하다.

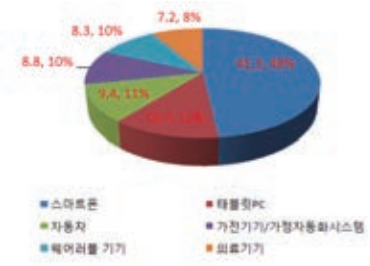
2. IoT 보안위협 요인 및 사례

(1) IoT 보안위협 요인

IoT 네트워크에 연결 가능한 디지털기기의 70%가 수집된 정보를 클라우드 컴퓨팅 시스템이나 로컬 네트워크에 암호화되지 않은 상태로 전송하고 있는 것으로 나타났다. 아울러 IoT 기기의 60%는 보안에 취약한 웹 인터페이스(web interface)를 적용하고 있는 것으로 나타났다. 소프트웨어를 업데이트 할 때에도 60%가 암호화를 사용하지 않는 등 암호화나 사용자 접근 권한 등에 있어 취약점을 갖고 있는 것으로 나타났다. IoT 네트워크 보안 관련 설문조사 결과, 응답자의 2/3가 보안에 대해 다음과 같이 우려하고 있다고 응답하고 있다[5].

〈표 1〉 IoT 기기의 보안 리스크 점유율

구분	보안리스크 점유율[%]
스마트폰	41.3
태블릿PC	10.7
자동차	9.4
가전기기/홈 가정자동화시스템	8.8
웨어러블 기기	8.3
의료기기	7.2



* 자료 : SANS Institute 자료종합/재구성.

- 응답자 중 가장 많은 70%가 민감한 개인정보의 노출에 대해 '매우 우려' 혹은 '다소 우려'라고 응답하였다.
- 응답자의 17.2%는 IoT가 보안에 취약하여 거의 재앙 수준이 될 것으로 우려하고 있다.
- 응답자의 48.8%는 기존의 다른 어플리케이션 및 시스템과 같은 정도의 보안문제를 우려하고 있다.
- IoT 보안 리스크가 큰 기기로 스마트폰 41.3%, 태블릿PC 10.7%, 자동차 9.4%, 가전기기/가정자동화시스템 8.8%, 웨어러블 디바이스 8.3%, 의료기기 7.2% 순으로 나타났다. (〈표 1〉 참조)

(2) 보안위협 사례

IoT 네트워크를 통한 개인정보의 유통(공유)은 다음과 같은 프라이버시 침해문제를 발생시킬 수 있다[3][4][6].

2) SSL 프로토콜은 Web Sphere Application Server를 사용하는 클라이언트와 서버 간 보안 연결을 위해 확실성, 데이터 서명 및 데이터 암호화를 포함한 전송 레이어 보안을 제공한다. SSL의 기본기술은 공용키 암호화로서 엔티티가 공용 키를 사용하여 데이터를 암호화할 때 해당 개인용 키가 있는 엔티티만이 이 데이터를 암호 해독할 수 있도록 한다.

– 헬스 캐어의 경우 개인의 의료진료 기록이 해커에 의해 외부에 유출되는 상황이 발생할 수 있다. 이에 보다 보안이 강화된 의료정보화 전략이 필요하다.
– 지능형 교통시스템(ITS : Intelligent Transportation System[3])의 교통신호등 제어권한을 해킹하여 통제기능을 잃고 교통사고를 유발하거나 교통이 마비되는 상황이 발생할 수 있다. 이에 보다 보안이 강화된 ITS(Intelligent Traffic System) 전략이 필요하다.
– 지능형 전력망 구축을 위한 스마트 그리드(smart grid) 망이 해킹을 당하여 통신과 전력계통이 완전히 다운되는 상황이 발생할 수 있다. 이에 보다 보안이 강화된 그리드 전략이 필요하다.

〈표 2〉 IoT 네트워크의 보안위협 사례

구분	위협사례
프라이버시	– IP카메라 주소를 해킹하여 실시간 영상링크 유포 – 스마트TV에 탑재된 카메라를 해킹하여 사생활 영상 유출 – 구글 글래스의 은행계좌 비밀번호등 금융정보 해킹
스마트 홈	– 홈 네트워크의 라우터를 해킹, 악성 이메일 등 사이버공격 – 로봇청소기에 탑재된 카메라로 실시간 모니터링 가능 – 가정의 온도조절기 제어권 해킹 – 스파이 마이크로 칩을 통한 악성 코드 및 스팸 유포 – PC 게임 화면을 통해 인쇄문서 해킹 – 호텔의 방 온도, TV 온오프, 블라인드 등 원격제어 가능
네트워크	– 차량의 CAN에 접근하여 악의적인 엔진조작 – 가정용 DSL 라우터를 통해 홈 네트워크 해킹 – 컴퓨터 공유기 해킹
제어시스템	– 보호되지 않은 산업용 제어시스템 해킹 – 셋톱박스를 대상으로 한 DDoS 공격
의료	– 800m 밖에서 인슐린펌프를 조작, 치명적인 복용량을 주입
교통	– 교통관리시스템에 위조 데이터를 전송, 주요 인프라 통제
방송	– 중간자공격(Man in the middle)을 이용한 티비싱
사이버 범죄	– IoT기기를 해킹한 온라인 납치 및 살인 등 사이버범죄

* 자료 : 언론매체 보도자료 종합/재구성.

IoT 네트워크는 해커가 인터넷에 연결된 디바이스들을 아주 쉽게 찾아낼 수 있기 때문에 해킹위협이 더욱 가중되고 있다. 2013년 10월 쇼단(shodan) 검색엔진[4]의 등장은 가장 심각한 IoT 네트워크의 보안위협 사례로 꼽히고 있다. 사물인터넷 망을 통한 다양한 분야의 보안위협 사례를 요약하면 〈표 2〉와 같다.

Ⅲ. IoT 보안 기술동향

1. 해외 IoT보안 대응 기술동향

(1) 개요

미국 및 유럽 등에서는 IoT 산업 활성화와 이용자 보호를 함께 고려하는 제도를 시행하거나 준비하고 있다. 이를 위해 시장의 자율규제를 통해 각 서비스 분야별로 보안지침(원칙)을 적용하도록 유도하고 있다. 특히 인간의 건강과 생명에 직결되는 헬스 캐어 분야에서는 보다 강력한 보안지침을 마련하고 이를 의무화하고 있다. 미국정부는 공공 및 민간 전문가 의견수렴을 통해 사이버보안 강화정책을 지속적으로 추진하면서 IoT 보안을 강화시키고 있다. 특히 미국 연방거래위원회에서는 IoT 서비스를 제공하는 단말 및 사업자들이 ⅰ)개인정보보호를 고려한 제품 및 서비스, ⅱ)수집된 개인정보의 강력한 비 식별화, ⅲ)IoT 단말 및 서비스의 투명성 확보 등 3대원칙을 준수할 것을 강력히 권고하고 있다. EC는 IoT 보안기술 개발과 아울러 인증 및 표준화에 초점을 맞추어 IoT 보안 권고사항 및 가이드라인 형태의 보안지침을 마련하였다. 아울러 지속적인 공공 및 민간 의견수렴을 통해 필요한 제도적 기반을 준비하고 있다. 중국정부는 IoT 핵심 원천기술 확보의 일환으로 IoT 보안강화를 통해 IoT 기술을 미래 핵심 산업으로 육성시키고 있다[4][7].

3) 지능형 교통시스템(ITS)은 기존의 교통체계에 정보, 통신, 제어, 전자 등의 지능형 기술을 접목시킨 차세대 교통시스템을 말한다. 교통수단 및 교통시설에 전자 · 제어 및 통신 등 첨단기술을 접목하여 교통정보 및 서비스를 제공하고 이를 활용함으로써 교통체계의 운영 및 관리를 과학화 · 자동화하고, 교통의 효율성과 안정성을 향상시키는 교통체계이다.

4) 쇼단(shodan)은 IoT 네트워크를 효율적으로 운용하기 위한 도구로 개발되었으며, 특히 기업의 IoT 시스템을 잠글 때 유용하게 이용할 수 있는 도구이다. 그러나 점차 이를 악용하여 해커와 테러리스트의 표적이 되고 있다. 쇼단 검색엔진을 이용하면 백 도어(back door)가 노출된 라우터, 안전하지 못한 웹캠, 기본 값 비밀번호를 사용하는 제어시스템 등을 손쉽게 찾을 수 있다.

(2) 주요국의 기술동향[4][7]

■ 미국 동향

– 주요 기반시설을 사이버공격으로부터 보호하기 위해 대통령 행정명령을 발동하고, 국립표준기술연구소의 주도 하에 사이버보안 프레임워크를 수립하여 운용하고 있다.(2013.2)

– 식품의약청(FDA)에서는 의료장비에 대한 보안지침을 마련하고, 이를 준수하지 않은 제품은 미국 내에서 판매 및 유통을 금지하고 있다.(2013)

– 연방거래위원회(FTC)는 학계 및 민간 사업자와 소비자보호단체가 참여하는 워크숍을 통해 IoT 규제를 강화하고 있다[5].(2013.11)

■ 유럽 동향

– 유럽 사물인터넷 연구단에서는 IoT 보안 관련 연구과제를 포함한 전반적인 기술연구를 수행하고 있다.

– 유럽 데이터보호 감독기구 작업반 29(Working Party 29)에서는 IoT 데이터보호와 관련된 권고안(Opinion 8/2014 on the on Recent Developments on the Internet of Things)을 발표한바 있다.(2014.9)

■ 중국 동향

– 중국 공업정보화부는 '사물인터넷 12차 5개년계획'을 통해 IoT 보안 강화와 함께 원천기술의 혁신, 산업생태계 육성, 기술응용수준 제고 등을 추진하고 있다.(2011.12)

– IoT 산업발전 10대 전문 행동계획을 수립하고 핵심 보안기술 개발 및 보안 테스트 평가 플랫폼 구축을 추진하는 등 보안역량을 강화시켜가고 있다.

2. 국내외 IoT 보안 기업동향

IoT 네트워킹 및 제어/접속 플랫폼 구축 분야는 매우 빠르게 확산되고 있으나, IoT 보안시장은 아직 초기 시장진입 단계로서 아직은 선두주자가 없는 상황이다. 이에 국내외 관련 기업들은 시장선점을 위한 경쟁을 본격화하고 있다. 특히 국내 기업의 물리적 복제방지(PUF)[6] 방식의 전자지문 보안 칩 기술력은 IoT 네트워크의 제어 및 접속 플랫폼의 보안을 강화하는 데 크게 기여한 것으로 평가받고 있다[8]. 국내외 IoT 보안기술개발 현황을 〈표 3〉에 나타낸다.

〈표 3〉 국내외 IoT 보안기술개발 현황

	기업명	기술개발동향
국내	KTB솔루션	– 소형/저전력/경량으로 휴대가 용이 – IoT 기기용 웨어러블 방화벽 개발
	시큐아이	– IoT 보안 하드웨어/소프트웨어 모듈 보안게이트웨이개발 – IoT 보안센서 등으로 구성된 IoT 보안플랫폼 개발
	아이씨티케이	– 물리적 복제방지(PUF)[6] 방식의 전자지문 보안 칩 개발
	SGA	– 시큐어OS 기반 웨어러블 및 의료기기용 보안솔루션개발
	펜타시큐리티	– DB암호화 솔루션을 IoT용 데이터암호화 솔루션으로 확장
	마크애니	– IoT 지원 가능한 전자서명 기술 개발
국외	Symantec	– IoT기기 임베디드OS 모니터링 기술 개발 – 침입탐지/차단/접근통제 기능 등 CSP 개발
	Trend Micro	– Broadcom과 공동으로 홈 게이트웨이 보안솔루션 개발
	Infineon Technology	– 스마트홈 등의 기밀데이터 인증 및 암호화솔루션 개발

* 자료 : IoT보안기술관련 자료종합/재구성.

Ⅳ. 결 론

IoT 기술은 사용자의 위치측정 기술과 결합되면서 생활공간 자체를 스마트하게 변화시킬 수 있는 첨단 서비스를 제공하고 있다. 실내외 위치기반 서비스는 모바일 서비스의 새로운 가능성을 제시하면서 지금까지 활성화되지 못했던 사용자 맞춤형 서비스로 부상하게 될 것으로 예상된다. 아울러 IoT 네트워크를 통한 지능통신

5) IoT 활용 단말 및 서비스의 정의, IoT 구현기술의 유형 확인, 소비자 데이터 프라이버시 보호, 데이터 전송 네트워크 보안 등 IoT 보안 관련 다양한 규제이슈에 대해 논의

6) 인간의 지문과 같은 전자지문의 일종으로 IoT 칩 제작 시 발생하는 공정편차를 이용하여 무작위 난수를 발생시키고 구현하는 원천기술이다. 국내 기업에 의해 칩 제작 단계에서 자연적으로 전자지문이 생기도록 구현하는 데 성공한바 있다. 인간의 지문 복제가 힘든 것처럼 물리적으로 복제가 불가능하여 키 안정성을 높이는 차세대 보안기술이다.

(Intellectual communication)이 인간의 삶의 질 향상에 필요한 정보의 가치를 높이고 불확실성을 줄이는 필수 인프라가 될 것으로 기대된다. 사물인터넷 산업을 활성화시키기 위해서는 ⅰ)IoT 시스템/플렛폼/네트워크의 사용자 인증 및 인가, ⅱ)접근제어, ⅲ) 키 및 식별자 관리, ⅳ)신뢰도 및 평판 관리, ⅴ)프라이버시 보호 등과 같은 핵심기술을 조기에 개발하여 미래 인터넷 거버넌스에 대응할 필요가 있다. 아울러 IoT 환경에서의 빅 데이터 처리 및 분석기법 등에 대한 연구와 접목되어야 한다. 사물인터넷 기술이 스마트 홈 산업의 새로운 성장 동력으로 주목받고 있다. 이에 글로벌 경쟁력을 향상시키기 위해 IoT 기술 관련 전후방 핵심 지재권을 확보가 절실하다. IoT 네트워크를 통한 정보통신 페러다임의 변화는 영화에서나 이루어지던 일들이 현실세계에서도 가능하게 하는 티핑 포인트(tipping point)를 제시하고 있다. 더 나아가 ICT 인프라와 접목되어 기후변화, 재난/재해, 여성/어린이/노약자 보호, 에너지 절감 등 다양한 전 지구적인 문제점들을 해결할 수 있을 것이다. 이를 안전하고 편리하게 이용할 수 있는 산 · 학 · 연 · 관 · 민의 공동노력이 필요하다.

이 논문은 미래창조과학부의 과학기술진흥기금과 복권기금 출연사업인 한국과학기술정보연구원이 수행하는 ReSEAT프로그램의 지원으로 수행되었습니다.

참 고 문 헌

[1] 박세환, “사물인터넷 핵심기술 및 시장성 분석”, 주간기술동향 1630호, 정보통신산업진흥원, 2014. 1.

[2] 민경식, “사물 인터넷(Internet of Things)”, NET Term, 한국인터넷진흥원, 2014. 6.

[3] "The Internet of Things Is Poised to Change Everything“, IDC, 2015. 10.

[4] “IoT 현황 및 주요 이슈”, 정보통신기술진흥센터, 2016. 12.

[5] IoT 보안 관련 설문조사 결과(SANS Institute 자료종합).

[6] 김광석, “지능형 교통시스템의 국내외 동향 및 정책적 시사점”, 과학기술정책, 제24권 제3 · 4호, 과학기술정책연구원, 2015. 12.

[7] “IoT 보안 위협 동향”, 이슈분석, 한국과학기술기획평가원, 2015. 12.

[8] http://www.etnews.com/20141010000645

박 세 환

- 조선대학교 전자공학과(공학박사)
- 전 한영대학교 교수
- 현 한국과학기술정보연구원 ReSEAT프로그램 전문연구위원

〈관심분야〉
Broadband ISDN, ICT Convergence Industry Analysis, Knowledge service etc.