디지털산업정보학회 논문지 제11권 제1호-2015년 3월
http://dx.doi.org/10.17662/ksdim.2015.11.1.069

사물인터넷 보안 문제제기와 대안

최 희 식* · 조 양 현**

Security Vulnerability of Internet of Things and Its Solution

Choi Heesik · Cho Yanghyun

〈Abstract〉

Internet of Things(IoT) is electronic devices and household appliances use wireless sensor network in environment of high speed wireless network and LTE mobile service. The combination of the development of Internet and wireless network led to development of new forms of service such as electronic devices and household appliances can connect to the Internet through various sensors and online servers such as a Home Network. Even though Internet of Things is useful, there are problems in Internet of Things. In environment of Internet of Things, information leakage could happens by illegal eavesdropping and spoofing. Also illegal devices of wireless communication interference can cause interfere in Internet of things service, physical damage and denial of service by modulation of data and sensor.

In this thesis, it will analyze security threats and security vulnerability in environment of mobile services and smart household appliances, then it will suggest plan.

To solve security issues, it is important that IT and RFID sensor related companies realize importance of security environment rather than focus on making profit.

It is important to develop the standardized security model that applies to the Internet of Things by security-related packages, standard certification system and strong encrypted authentication

Key Words : IoT, Internet of Things, Security, RFID

Ⅰ. 서론

사물인터넷(IoT, Internet of Things)은 인터넷의 발달과 무선 네트워크의 결합으로 사물이 각종 센서와 홈네트워크와 같은 서버를 통해 인터넷과 연결되어 제공되는 새로운 형태의 서비스로 사물인터넷에서 사물들이 고유한 식별자를 가지고 인터넷에 연결되어 서로 상호작용을 하며 생산자 및 소비자의 역할도 하게 된다[1]. 최근 WiFi 무선 환경과 LTE와 같은 초고속 무선통신의 발달로 센서 네트워크를 이용하여 소형 가전제품 및 생활 가전용품에 센서 네트워크 기

* 삼육대학교 컴퓨터학부 외래교수(제1저자)
** 삼육대학교 컴퓨터학부 교수(교신저자)

술을 활용하고 있다. 이에 사물인터넷은 향후 미래 산업의 패러다임을 바꿀 만한 21세기 유망 동력 산업의 기술로 각광 받고 있다.

최근 이러한 미래 산업에 활력을 불어넣은 사물인터넷과 같은 기술들이 각종 센서, 구동기, 임베디드 장치 및 사용자 단말기와 같은 장치 기술을 크게 발전시키고는 있지만 새로운 형태의 다양한 제품과 이종간의 제품이 연결되어 응용되어 활용되어지기 때문에, 이에 따른 사물인터넷 증가 수에 따른 보안의 위협이 심각한 사회적 이슈로 부상하고 있다.

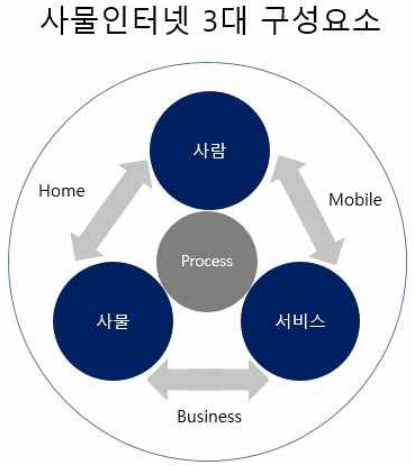
본 논문 구성에서 2장은 기술 및 특징에 대한 관련 연구를 살펴보고 3장에서는 사물 인터넷의 보안 위협 요소에 대하여 살펴보고, 4장에서는 사물 인터넷 보안 위협에 대한 사례를 분석하여 문제제기와 대안을 제시하고, 5장에서 결론으로 마무리 하고자 한다.

Ⅱ. 관련연구

사물인터넷의 3대 구성요소는 인간, 사물, 서비스의 중요한 요소로 이루어진다. 아래 <그림 1>은 사물인터넷이 인간과 사물, 서비스를 포함하는 인간 주변 환경을 상호 보완적으로 연결해 주는 그림을 보여주고 있다. 즉 사물인터넷은 인간이 사물인터넷을 통해서 사물 및 서비스와 소통하며, 사물과 서비스도 사물인터넷 기술을 통하여 서로 소통함을 의미하고 있으며 그 특징적인 요소는 다음과 같다.

① 인간 : 독립적 주체로서의 사람과 그 사람의 사고, 행동 양식 등을 의미한다[2].

② 사물 : 유형의 사물과 무형의 사물로 구성되며, 유형의 사물은 물리적 객체로서의 사물이며, 무형의 사물은 가상 객체로서의 사물을 의미한다. 무형의 사물로는 IT 서비스에서 특정 기능을 수행하는 함수, 객체 등이 될 수 있으며, 아바타도 무형의 사물로 정의할 수 있다[2].



<그림 1> 사물인터넷 구성요소

③ 서비스 : 인간 환경의 3대 요소에서 특정 목적을 위해 구현된 프로세스와 동작 메커니즘 집합을 의미한다[2].

2.1 사물인터넷의 주요 요소 기술

사물인터넷의 3대 주요 요소 기술은 크게 센싱 기술, 유무선 통신/네트워킹 기술, 서비스 인터페이스 기술로 나누며 기술적 역할 특징은 다음과 같다[12].

① 센싱 기술 : 사물 인터넷 서비스의 인터페이스 기술을 담당하는 부분으로 센서를 통해 원격으로 온도, 습도, 열, 가스, 조도, 초음파 등과 같이 주위 환경으로부터 정보를 얻는데 사용된다[2].

② 유무선 통신 및 네트워크 인프라 기술 : 유무선 통신 및 네트워크 장치로는 기존의 WPAN, WiFi, 3G/4G/LTE, Bluetooth, Ethernet, BcN, 위성통신, Microware, 시리얼 통신, PLC 등, 인간과 사물, 서비스를 연결시킬 수 있는 모든 유무선 네트워크를 의미한다[2].

③ 서비스 인터페이스 기술 : 사물인터넷의 특정 기능을 수행하며, 정보를 센싱, 가공, 추출, 처리, 저장, 판단, 상황 인식, 인지, 보안, 사생활 보호, 인증, 객체 정형화, 온톨러지 기반의 시맨틱, 오픈 센서 API, 가상화, 위치 확인, 프로세스 관리, 오픈 플랫폼 기술, 미들웨어 기술, 데이터 마이닝 기술, 웹 서비스 기술, 소셜 네트워크 서비스 등, 자료를 저장, 처리, 변환하는 역할의 서비스를 제공한다[2].

2.2 사물인터넷 최신 기술

최근에는 사물인터넷의 주요 요소 기술을 보완하고 사물인터넷 서비스를 보다 더 편리하게 사용하고 구현할 수 있는 기술들이 개발되고 있다.

① REST(Representational State Transfer) : 인터넷의 정보를 조직하고 사물인터넷을 구성하는 기기들의 상태를 점검하고 전송하며, 클라이언트 서버의 네트워크 환경에서 리소스의 CRUD(Create, Read, Update, Delete) 처리를 지원한다[3].

② MQTT(Message Queuing Telemetry Transport) : 컴퓨터 성능에 따른 제한된 기능을 많이 고려했으며 특히 네트워크 처리 시 속도 차이로 생길 수 있는 연결 과정에 따른 환경도 고려하여 설계된 대용량 메시지 전달 프로토콜이다[3].

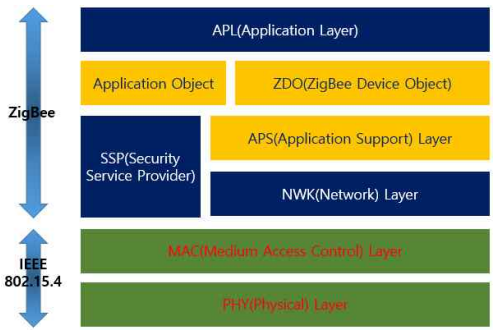
③ XMPP(eXtensible Messaging and Presence Protocol) : IETF에서 제정한 국제 표준 프로토콜로 다수의 클라이언트들에게 인스턴트 메신저를 보낼 수 있으며, Publish/Subscribe 구조를 바탕으로 확장성 있는 XML 기반 실시간 메시지 교환이 가능한 프로토콜이다[3].

④ CoAP(Constrained Environments Application Protocol) : IETF의 CoRE(Constrained RESTful Environments) 워킹 그룹에서 정의한 프로토콜이며, REST(Representational State Transfer) 구조를 가지며 간단한 웹 서비스를 할 수 있도록 만들어진 프로토콜이다. 인터넷에서 센서 노드와 같이 제한된 컴퓨팅 성능을 갖는 디바이스들의 통신을 실현하기 위해 CoAP은 UDP상에서 정의되며, 단순하므로 적은 오버헤드와 멀티캐스트 특성을 가진다[4].

2.3 ZigBee 보안 기술

ZigBee는 최근 사물인터넷에서 무선 표준 기술정보의 하나인 IEEE 802.15. 4를 이용하여 무선을 이용하여 가전제품을 근거리로 조정할 수 있는 기술이다. ZigBee 기술은 적은 전력으로도 무선을 이용할 수 있는 것이 장점이다. ZigBee의 각 장치는 Open Trust Model 방식으로 암호화는 되어 있어 장치 자신에 대한 내부 신뢰성은 보장되지만, 외부와의 통신 과정에서의 보안 위협이 발생할 수 있으므로 별도의 보안에 대한 대책이 없어 현재로서는 단점일 수 있다[5].

<그림 2>는 ZigBee 보안 기술에 적용되고 있는 스택 구조이다.

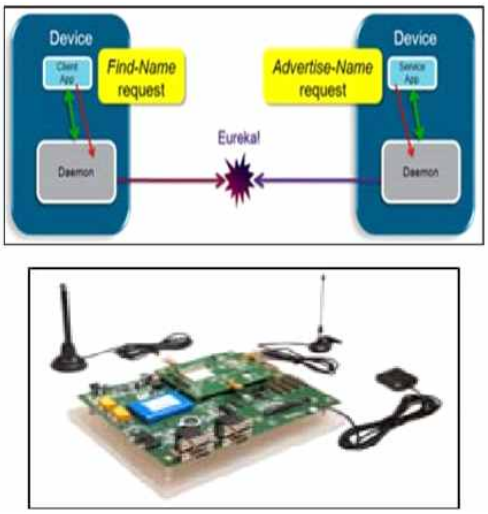


<그림 2> ZigBee 스택구조

2.4 사물인터넷 활용분야

사물인터넷은 매우 다양한 분야에서 활용되고 있

는데 그 활용 영역은 크게 유틸리티(Utilities), 교통 및 물류(Transportation and logistics), 헬스케어(Healthcare), 집, 사무실, 공장 등의 스마트 환경(Smart environment-home, office, plant), 개인 및 소셜(Personal and social), 등 5가지 분야로 나눌 수 있다[10]. 최근 퀄컴사도 AllJoyn이라는 운영체제와 하드웨어 종류에 상관없이 기기를 연결할 수 있는 프레임워크 기술을 개발하고, 주로 가전제품 사를 회원으로 하는 AllSeenAlliance를 <그림 3>과 같이 구성하여 사물인터넷 기술 보급에 나서고 있다[6].



<그림 3> 퀄컴사의 AllJoyn 플랫폼

사물인터넷의 세부적인 활용분야는 <표 1>과 같다.

① 유틸리티 : 사물인터넷을 전력망 및 자동화 기업 등에서 송배전 자동화 시스템에 연결하여 에너지 절감 효과를 기대할 수 있으며, 사물 인터넷의 가장 큰 시장 형성을 기여할 것으로 예측 전망된다.

② 교통 및 물류 분야 : 자동차 운행에 필요한 실시간 교통정보를 제공받고 자동화된 운전까지 가능하게 하는 주행 보조(Assisted Driving), 도로 환경 모니터링, 증강현실 기술을 지도에 구현한 증강 지도(Augmented Map) 등에 사물인터넷이 활용될 것으로 기대된다[7].

③ 헬스케어 분야 : 환자 비상대책 수단으로 의료진의 위치 파악 및 심장질환자의 원격 모니터링을 통한 의료 정보를 인식 및 수집하고 추적함으로써 의료서비스 품질 향상 및 수요가 기대된다[7].

④ 스마트 환경 분야 : 사무실 환경과 산업 현장에 무선 통신 환경을 결합한 사물인터넷 기술을 적용하여 보다 정확한 생산 능력 업무 구현에 적용토록 화하여 박물관/미술관과 헬스클럽 시설에 사물인터넷을 적용한 스마트 환경 구축이 가능할 것으로 보인다[7].

⑤ 개인 및 소셜 : 사물인터넷을 개인과 소셜미디어와 결합한 응용서비스가 가능하리라 기대되는데 스마폰을 이용하여 가정 내 도난 방지용 홈시큐리티 시스템과 도시 정보화 모델, 확장형 게임 룸 등에 사물인터넷이 활용될 것으로 기대된다[7].

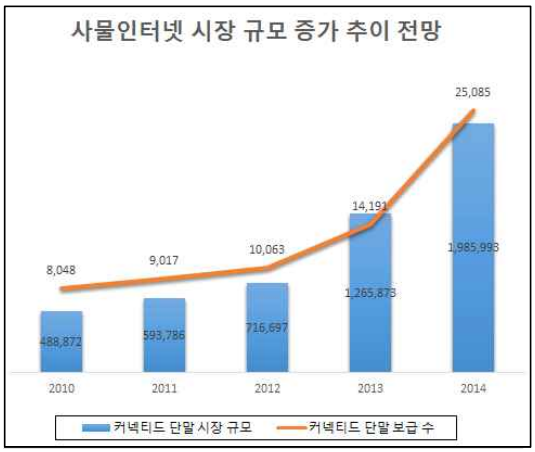
<표 1> 사물인터넷 세부 활용분야[8, 9]

구분	세부 분야
도시	주차, 교통 혼잡, 교통망, 가로등, 쓰레기 관리 등
환경	대기 오염 측정, 산불 예방, 지진 감지 등
수질	수질 관리, 누수 탐지, 홍수 예방
에너지	수력/화력/태양열 발전 설비 모니터링 등
보안	물리적 접근통제
물류	물류/유통망 관리, NFC 결제, 지능형 쇼핑 등
산업	실내공기 관리, 온도 모니터링, 실내측위 등
농경	농작물 온·습도 관리, 기후 변화 감지 등
축산	가축 건강 및 위치관리, 유해가스 측정 등
홈/가전	조명, 가스, 보일러, 세탁기, 에어컨, 커튼, 방범, 원격제어 등
건강	독거노인 건강관리, 운동량 측정, 자외선 측정 등

2.4 사물인터넷 성장 기대

매년 첨단 유망 기술에 대한 전망을 발표하는 가트너는 사물인터넷이 향후 5년~10년 사이에 잠재력을 지닌 주류 기술로 영향력을 발휘 할 것으로 전망하고 있으며 주류 기술로 진입하기까지 걸리는 시간은 10년 이상으로 전망하고 있다.

또한 사물인터넷은 최근 커넥티드 단말의 개체 수 및 유형, 사물의 식별, 감지, 커뮤니케이션 센서 및 기술 등의 비약적 발전과 증대로 영향력 확장이 예상되는 분야로 미래 새로운 차원의 서비스 및 시장 가치를 창출할 기술로 각광받고 있다. 성장적인 측면에서 예측할 때에 글로벌 커넥티드 단말기의 보급 대수는 '11년 약 90억 대에서 '20년 약 250억 대까지 증가할 것으로 전망하고 있으며, 그 시장적 규모 가치 면에서도 '11년 5,937억 달러 <그림 4>에서 '20년 1조 9,860억 달러까지 크게 성장할 것으로 기대하고 있다[10].



<그림 4> 사물인터넷 시장규모 증가 추이

Ⅲ. 사물인터넷 보안 위협 요소

사물인터넷을 실행하는 과정에서 많은 보안 적 위협적인 요소가 존재하고 있다. 현재 사물인터넷이 작동되기까지는 근거리 무선식별장치 및 인터넷 IP를 이용한 홈네트워크 서버에 접속하여 외부 환경으로부터의 데이터 취득을 위해 내장된 센서를 통해 사용자 신원을 식별할 수 있는 인증 과정이 필요하다.

근거리에서는 사물의 신원을 확인할 때는 RFID라는 태그를 각 사물 등에 부착시켜 개인의 정보를 Reader가 읽음으로써 사용자의 정보를 제공받게 되며[11], 광대역 네트워크상에서는 개별 사물에 인터넷 IP주소를 부여받도록 해야 한다.

이에 개별 사물인터넷을 인증하는 과정에서 발생하는 사물인터넷의 위협적인 보안 요소에는 우선 단말기와 센서를 통한 정보 유출, ID 관리 부실에서 발생할 수 있는 도난, 무선 네트워크를 통한 신호교란, DDos 공격, 도청 및 감청에 대한 정보 유출이 예상된다<표 2>. 또한 비인가자로 부터의 해킹은 심각한 보안위협이 될 수가 있다.

3.1 인증관리 소홀

사물인터넷 사용을 위한 서비스를 제공받기 위해서는 보증된 보안 인증 모듈을 거쳐서 사용자 접근을 허용하여 가용성을 보장할 수 있어야 한다. 그러나 최근에는 사물인터넷 사용을 위한 ID와 같은 인증 관리 소홀로 인한 개인정보 누출과 개인식별에 관한 문제가 발생하면서 인증관리 소홀에 따른 사물인터넷 피해가 심각한 상태이다[12].

3.2 플랫폼 붕괴 우려

사물인터넷 일부 기기의 경우 사용자의 인증 시스

템에 불법으로 접근 후, 암호키 해킹에 의한 비 인가 접근자의 플랫폼 붕괴 위험에 대한 노출 우려이다. 공격자는 비 인가된 접근을 시도한 후, 플랫폼을 맘대로 조작함으로써 물리적인 손상 등을 입힐 수 있다[5].

3.3 무선신호 교란(jamming)

사물인터넷을 사용하기 위해서는 대부분 무선 네트워크나 이동 통신망을 통해 서비스가 이루어지는데, 최근 이동통신망, GPS, RFID등 다양한 무선 네트워크를 대상으로 인가받지 않은 불법 무선 통신 교란 장비를 설치하여 정상적인 사물인터넷 사용에 관한 동작을 방해할 수 있다[9].

3.4 이기종 연동과 정보유출

사물인터넷 서비스 환경에서의 이기종 사물 네트워크 간 연동 통신과정에서 정보유출이 발생할 수 있는데 유무선 통신망 서버에 접속하여 사용자의 전력 소비량을 측정하기 위해 스마트미터기를 통한 원격 제어 사용 시 전력 사용내역에 대한 내역이 유출될 수 있다. 유출하는 과정에서는 당연히 개인정보와 같은 정보도 포함될 수 있으며, 데이터 전송 시 암호화 되지 않는 평문 상태의 데이터 전송은 심각한 개인정보 유출 및 사생활 침해에 대한 위험이 발생할 수 있다[5].

3.5 스마트 TV와 데이터 위. 변조

스마트 TV 보급으로 사물인터넷 서비스를 이용한 보안 위협 중 스마트 TV에 악성코드를 감염시켜 내부 카메라의 원격조종을 통해 개인정보를 유출하거나, 사용자 몰래 데이터를 가로채기한 후, 데이터를 위. 변조시킨 후, 정상적으로 네트워크를 통해서 전송받은 데이터로 속이는 위협이다[9].

3.6 서비스 거부(Denial of Service)

사물인터넷 서비스를 사용하기 위해서는 사람 또는 사물에 부착된 단말/센서들이 정상적인 서비스 제공과 사용자의 위치 확인을 위해 단말/센서 간의 게이트웨이를 통해 원격지에서 수시로 연결요청을 시도하게 된다. 공격자는 이를 악용하여 임의로 대량의 연결요청 및 확인 패킷을 지속적으로 전송하고 이를 단말/센서에서 처리하는데 필요한 자원을 소모시킬 수 있다. 또한 이러한 서비스거부 공격은 기기의 전력을 지속적으로 소모하여 서비스가 불가능하도록 유도할 수 있다[9].

<표 2> 사물인터넷 보안 위협 요소

위협 요소	사물인터넷 보안 위협
ID관리	ID 관리 소홀 및 낮은 인증으로 인한 개인정보 및 개인식별 번호 유출 우려
단말기 분실	단말기 분실로 인해 통신기능 상실 및 정보유출에 피해
무선신호 교란	불법 장비를 이용하여 통신을 방해하여 정상적인 서비스를 받지 못하게 함
정보유출	스마트미터기와 같은 원격제어 사용 시 정보내역 및 개인정보 유출 피해 우려
데이터 위. 변조	사용자 몰래 침투하여 데이터를 가로채기하여 데이터를 위. 변조 우려
서비스 거부	원격지에서 수시로 서비스에 대한 요청을 하여 패킷을 증가시켜 접속에 대한 지연을 야기함

VI. 보안 문제점 분석 및 대안 제시

본문에서 살펴본 바와 같이 사물인터넷은 IT기기와 융합된 많은 다양한 서비스와 결합되면서 편리함을 제공하지만 충분히 보안이라는 요소의 취약적인

위협을 초래하고 있다. 즉 사용자들은 새로운 패러다임의 생활환경의 편리함을 제공받고 있겠지만 3절에서 살펴본 바로 사물인터넷 보안에는 정보유출, 데이터 위. 변조, 무선신호 교란 중 여러 가지 취약적이고 위협적인 문제점들이 보이고 있다.

이번 절에서는 사물인터넷의 보안에 대해 문제시되고 있는 핵심적인 문제점을 분석하여 사용자들로 하여금 위험으로부터 예방적인 차원에서 보호받을 수 있는 대안을 제시하고자 한다.

4.1 사례적 상황1

관리용 셋톱박스부터 최근 급증하는 스마트 가전을 노린 유무선 통신의 발달로 센서 및 스마트 단말기의 발전 및 보급은 확산되었지만 여전히 사물인터넷 보안에 대한 위협은 심히 우려가 되고 있다. 이동성 모바일에 대한 편리성으로 요즘은 차량 내부에 까지 각종 이동성 모바일 기기를 차량 내부 시스템에 탑재하여 사용자의 스마트 폰이나 태블릿과 같은 장치를 인터넷에 연결하여 이용하는 사용자는 점차 늘어나고 있다. 당연히 사물인터넷은 이동형 모바일 환경에도 적용 성이 우수하여 사용자들에게는 많은 편리함을 제공하고 있지만, 동시에 연결된 많은 기기와의 결합되는 과정에서는 보안 취약이라는 새로운 위협이 발생하게 된다.

4.2 사례 분석 대안제시-1

차량에 탑재된 WiFi에는 방화벽과 같은 보안 솔루션을 장착하지 않고 이동성 모바일 서비스를 이용하고 있고 또한 핫스팟과 같은 네트워크 서비스를 공유시켰을 경우에는 공격자는 무선 환경의 사물인터넷과 같은 보안성이 약한 기기에 네트워크 침입을 시도하여 차량 시스템에 대한 권한을 갖음으로써 권한 상승과 함께 데이터를 처리하는 공격에 가담할 수도 있다. 결국 공격자는 주요 파일 접근 공격에 성공하게 되며, 차주의 개인정보를 해킹하여 마음만 먹으면 언제든지 개인 식별과 관계된 주민번호, 신용카드, 금융정보와 같은 정보를 탈취하여 사용자에게 피해를 입힐 수 있다.

대부분 사물인터넷 기기에는 보안이 설치되어 있다 하더라도 대부분 낮은 보안 수준의 인증 레벨이 적용되고 있으므로 보안성이 매우 취약하여 공격자가 마음만 먹으면 쉽게 주요 파일 접근과 호스트 기반까지도 공격할 수 있는 매우 보안 수위가 낮은 상태이다. 기본적으로 제공되어야 하는 백신마저 설치되어 있지 않고 또한 데이터와 전송에 필요한 암호화가 적용되지 못하고 있어 데이터 전송에 따라 심각한 보안 위협에 노출되고 있는 실정이다.

안전한 사물인터넷을 사용하기 위해서는 우선 무선 센서를 작동할 때에는 방화벽 솔루션이 안전하게 설치되어 가동되고 있는지를 확인하고 또한 센서 작동 시, 보안 이벤트가 발생하는지를 반드시 확인해야 한다. 또한 스마트 폰과 같은 곳에 개인 식별에 관한 신상 정보가 저장되어 사물인터넷에 관한 인증을 필요로 해야 할 경우에는 보안 인증 모듈이 안전하게 설치되어 있는지도 확인한다. 그런 다음 보안 인증 모듈이 작동되어 데이터 전송 처리 시 암호화되어 사용자에게 보안 인증에 대해 안전하게 사용해도 좋다는 보안인증센터로부터 확인 인증 절차를 거친 후, 사물인터넷을 사용하도록 한다.

4.2 사례적 상황2

두 번째 기술적 분석 사례는 사물인터넷의 최근 급증하는 스마트 생활가전을 노린 위협으로 보안에 다소 무디고 관심이 적은 주부를 대상으로 RFID와 같은 비접촉식 자동 인식 기술을 이용하여 생활가전 냉

장고와 세탁기, 밥솥과 같은 주방기기를 활용한 무선 환경의 사물인터넷에 접근 후, RFID 리더를 통해 정보를 인식하게 된다. 뿐만 아니라 RFID 자체 보안의 취약성이라는 문제를 담고 있기 때문에 공격자들은 RFID 리더에서 입수한 정보를 바탕으로 사용자의 위치 추적을 할 수 있으며, 데이터 인식 계층을 통해서 입수한 주부들의 개인정보 및 이메일을 해킹할 수도 있다. 실제로 최근 미국에서도 스마트 가전 냉장고를 활용한 보안 위협에 대한 피해적 사례가 보고된 바가 있었다.

4.2 사례 분석 대안제시-2

주부들은 편리하게 이용할 수 있는 사물인터넷에 위협적인 요소가 발생할 수 있다는 보안 의식이 없는 것이 큰 문제이다. 사물인터넷은 무선 네트워크, 센서, 자동화 등 다양한 IT와 기기간의 융합으로 편리성을 도모할 수 있는 새로운 산업이니 만큼 주부들은 사물인터넷을 이용할 때는 최소한 정보 이용에 관한 유출 우려와 개인정보 유출 등에 관한 보안의식을 상기해야만 한다. 혹시라도 사물인터넷 사용 시 의심되는 요소가 조금이라도 생기거나 스팸메일을 통해 개인정보 유출 피해가 있었다면 우선적으로 제조사의 소비자 피해 신고센터나 각종 기관 사이버 피해 대응센터를 이용하여 다른 사람들에게도 피해가 더 이상 확산되지 않도록 신고 제도를 생활화하는 것이 분명 필요하다.

또한 하드웨어 제조사는 제품 제조 및 개발 시 무결성 확보에 대한 보안 인증 강화에 대한 제품으로 개발되어야 할 것이며, 안전한 서비스 제공을 위한 보안 표준 가이드라인도 함께 마련되어야 할 것이다. 또한 제품 출고 이후라도 제품 보안 취약에 대한 위협이 발견되었다면 소비자 보호 대책 차원에서라도 또한 범국민의 안전한 제품 사용을 위해서라도 하드웨어 제조사는 보안 위협에 대한 새로운 보안 패치를 개발하여 제품을 구입하는 소비자에게 제공되어야하는 보안 대책 강구가 마련되어야 한다.

특히 스마트 생활가전을 제조하는 하드웨어 제조사는 융합과 응용, 융통성에 대한 기술적 요소에 대한 생활적 편의를 강조하고 있지만 사물인터넷 제품에 보안 강화에는 크게 신경 쓰고 있지 않는 실정이어서 보안 레벨은 극히 낮은 수준에 머무르고 있는 것이 보안 위협의 가장 큰 위험요소이다. 사물인터넷을 좀 더 편리하고 안전하게 사용하기 위해서는 다음과 같은 대안을 제시할 수 있는데 무선신호를 이용하여 해당 사물의 정보를 인식하는 RFID 리더는 보통 센서가 내장된 태그를 자동으로 인식하게 되는데 RFID 보안 리더 하나를 더 추가하여 보안 역할을 담당하도록 한다. 즉 RFID 보안리더는 RFID 리더와 RFID 태그를 관리할 수 있는 수행 역할을 하게 된다. 또한 RFID 보안 리더는 모든 정보를 인식 후 바로 사용하도록 허락하는 것이 아니라, 보안 리더와 사물인터넷 통제국에서 신뢰영역을 인증받기 위해 디지털 서명을 한 번 더 요청하도록 한다. 이 때 신뢰적으로 상호 인증된 디지털 서명 검증을 바탕으로 안전한 사물인터넷을 사용할 수 있도록 통제모드를 해제한다.

Ⅴ. 결론

사물인터넷은 네트워크 서비스와 다양한 IT 관련 기기와의 기술적인 융합의 조합으로 매우 다양한 요소와 특성을 만들어 내므로 한마디로 보안 기술에 대한 표준을 정하기란 쉽지는 않다. 하지만 사물인터넷이 신 성장 동력 산업인 만큼 그 이용 증가도 최근 급속도로 확대되고 있으므로 그 안전에 대한 대책은 매우 시급하리라 본다. 만약 사물인터넷이 새로운 보안 위협적 과제를 해결하지 못하고 또한 기술적, 법제도적인 가이드라인 표준안을 마련하지 못한다면 사물

인터넷은 무서운 재앙을 몰고 다니는 센서, 네트워크, 서버, 무선 모바일 기반의 새로운 악재로 변신될 수도 있다.

본 논문에서는 사물인터넷이 모바일 서비스 환경이나 스마트 가전 환경에서의 누구나가 쉽게 생각할 수 있는 보안의식 결여와 무선 환경이라는 취약적 요소로 인해 발생할 수 있는 보안 취약 환경에 대해서 문제점을 분석하여 그 대책적인 대안을 제시하였다.

우선적으로 이러한 제안된 내용에 대한 문제 요소를 해결하기 위해서는 IT관련 및 RFID 센서를 이용하는 기기 개발 업체에서는 이익 창출보다는 사물인터넷 환경에서 가장 이슈될 수 있는 보안환경에 대한 부분을 중요하게 인식하고, 보안관련 패키지 및 표준 인증체계, 암호화 인증도 함께 탑재될 수 있는 환경을 최우선으로 고려해야 한다. 기술적 대안 제시의 또 다른 방법으로는 RFID 보안 리더 하나를 더 추가하여 보안 역할을 담당하게 하는 신뢰영역 구축 방안이다. 상호 인증된 신뢰영역 구축을 통해 안전한 사물인터넷을 사용할 수 있도록 하는 제안 방법이다.

또한 국내. 외 보안 개발 업체 및 각 산업 표준 연구기관에서도 사물인터넷 보안 위협이라는 문제점을 인식하고 적극적인 보안 솔루션 개발 연구 및 신규 보안 표준화에 대한 전략과 대응 대책에 대한 연구가 꾸준히 진행되어야 할 시기라고 본다.

참고문헌

[1] 김성림, 권준희, “소셜 사물인터넷에서 소셜 관계를 이용한 사물 추천 기법,” 디지털산업정보학회, 디지털산업정보학회 논문지, 제10권, 제3호, 2014, p.49.

[2] 김호원, 김동규, “IoT 기술과 보안,” 정보보호학회, 정보보호학회 논문지, 제22권, 제1호, 2012, p.8-10.

[3] 장원규, 이성협, “국내외 사물인터넷 정책 및 시장동향과 주요 서비스 사례,” 한국전파통신원, 제64호, 2013, p.30.

[4] 김호원, “사물인터넷 서비스에서의 보안 이슈,” 정보과학회, 정보과학회 학술지, 제32권, 제6호, 2014, p.38-39.

[5] 정봉임, 김창수, “사물 인터넷 보안 기술 연구,” 보안공학연구학회, 보안공학연구학회 논문지, 제11권, 제5호, 2014, p.431.

[6] 이형규, 김말희, 방효찬, “사물인터넷(Internet of Things) 기술 동향,” 정보처리학회지, 정보처리학회 학술지, 제23권, 제2호, 2014, p.17.

[7] “사물인터넷이 열어갈 새로운 세상,” 한국콘텐츠진흥원, 제33호, 2013, p.8-9.

[8] 배진석, 조우제, 정윤혁, “Privacy Issues in IoT Communication,” 경영정보학회, 경영정보학회 학술지, 2013, p.761.

[9] 김동희, 윤석웅, 이용필, “IoT 서비스를 위한 보안,” 한국인터넷진흥원, 정보와 통신, 8월, 2013, pp.55-56.

[10] 민경식, “사물 인터넷(IoT)의 시장 정책동향 분석,” 한국인터넷진흥원, 인터넷 & 시큐리티이슈, 9월, 2012, p.13.

[11] 최희식, 박재표, 전문석, “유비쿼터스 RFID 개인정보 침해에 대한 방안 연구,” 디지털산업정보학회, 디지털산업정보학회 논문지, 제6권, 제2호, 2010, p.144.

[12] 서화정, 이동건, 김지현, 최종석, 김호원, “사물인터넷상에서의 보안과 프라이버시 보호 이슈,” 정보처리학회, 정보처리학회 논문지, 제21권, 제2호, 2014, p.56.

[13] 김호원, “사물 인터넷 보안 및 프라이버시 이슈,” 부산대학교, 2014, p.19.

■ 저자소개 ■

최 희 식
Choi Heesik

2008년 3월~현재
강원대학교 IT학부 외래교수
2012년 2월 숭실대학교 컴퓨터학과(공학박사)
2006년 2월 숭실대학교 컴퓨터공학과
(공학석사)

관심분야 : 정보보안, 클라우딩컴퓨터,
유비쿼터스, DRM
E-mail : dali3054@ssu.ac.kr

조 양 현
Cho Yanghyun

1997년 9월~현재
삼육대학교 컴퓨터학부 교수
2012년 2월 광운대학교 전자통신학과
(공학박사)
1985년 2월 광운대학교 전자통신학과
(공학석사)
1982년 2월 광운대학교 전자통신학과(공학사)

관심분야 : 컴퓨터네트워크, 통신망(BcN),
GMPLS
E-mail : yhcho@syu.ac.kr

논문접수일: 2015년 1월 26일
수 정 일: 2015년 2월 8일
게재확정일: 2015년 2월 11일