석사학위 청구논문

지도교수 김 기 천

스마트 홈 IoT 서비스 환경에서의 보안위협과 정보보호 방안에 관한 연구

2017년 8월

건국대학교 정보통신대학원

정보보안학과

방 상 식

스마트 홈 IoT 서비스 환경에서의 보안위협과 정보보호 방안에 관한 연구

A Study on Security Threats and Information Protection in Smart Home IoT Service Enviroment

이 논문을 공학 석사학위 청구논문으로 제출합니다

2017년 6월

건국대학교 정보통신대학원

정보보안학과

방 상 식

방상식의 공학 석사학위 청구논문을 인준함

심사위원장 (인)

심사위원 (인)

심사위원 (인)

2017년 6월

건국대학교 정보통신대학원

목 차

표 목 차

그 림 목 차

ABSTRACT

A Study on Security Threats and Information Protection in Smart Home IoT Service Enviroment

Bang , Sang sik
Department of Information Security
Graduate School of Information and Telecommunications
Konkuk University

With the development of information and communication technologies, various services are provided through connection of objects and the Internet

In particular, smart home IoT service, which is spreading recently due to the continuous development of Internet of things, provides user convenience to connect smart devices in home with wired / wireless network so that it can be used anytime and anywhere easily and conveniently. However, instead of providing user convenience, the Smart Home IoT service environment is based on the exchange of data between people and objects, so it contains information that is close to privacy such as personal information (name, date of birth, phone number, address, etc.) The risk of personal information infringement is high. In addition, there may be a serious threat such as unauthorized intrusion through smart door lock hacking, hacking of smart home controller, malfunction of other people's smart home

device and overcharge of electricity bill. It is important to respond to information security measures against security threats because such smart home infringement causes financial, physical, and psychological harm. In this paper, we investigate the security breaches occurring in the smart home IoT service environment and divide the security threats of the smart home IoT service into three categories (security threats related to devices, networks, and personal information) and propose countermeasures.

Key words: Internet of Things, smart home, security threat, information protection plan

제1장 서론

제1절 연구배경 및 목적

정보통신기술(ICT: Internet and Communication Technology)의 발달로 사람, 사물, 공간, 데이터 등 모든 것이 연결되는 초 연결사회가 도래하게 되었다. 편리함, 즐거움, 안락함 등 인간의 기본적인 욕구를 만족시킬 수 있는 스마트 홈 IoT 서비스가 보편화 됨에 따라 비로소 우리의 삶이 보다 질적으로 편리하게 변화하게 된 것이다.

스마트 홈 IoT 는 기존의 가정환경에서 모바일 기기나 가전제품 등을 인터넷과 통신으로 연결하여 정보를 수집하고, 교환하는 플랫폼을 의미한다. 정보통신기술 발달 및 IoT 환경을 통해 스마트 홈 IoT 기술, 서비스의 발달과 그 보급에도 가속화가 진행되고 있다. 2016년 국내 스마트 홈 시장이 12조 원을 돌파하는 등, 향후 2019년까지 연평균 20% 이상 성장, 2019년에는 21조원까지 확대될 전망이다. 분야별로는 스마트TV & 홈 엔터테인먼트 분야가 전체 스마트홈 시장의 58%를 차지했으며, 가전, 조명, 냉난방 등을 포함한 스마트 융합가전이 그 뒤를 이었고, 스마트 홈 시큐리티, 홈오토메이션, 스마트 그린홈 순으로 하나의 시장을 형성했다. 가정용 전자제품부터 보안장치, 난방 및 조명 시스템에 이르기까지 다양한 종류의 인터넷 연결 장치들이 개발되면서 스마트 홈 IoT는 보다 구체화 되고 생활에 밀착화 되고 있다. 하지만 스마트 홈 IoT 서비스의 보안은 여전히 미흡하며 사용자들은 디바이스 인증 취약점, 네크워크 공격, 개인정보 노출 등 다양한 보안 위협에 노출되어 있다.[1]

본 논문에서는 향후 스마트 홈 IoT기술에 대한 정보보호와 안정성 확보가 그 어느 때보다도 높게 대두되고 있는바, 이와 관련된 보안 위협 및 요구사항을 파악하고 그에 대한 정보보호 방안을 제시하고자 하는데 그 목적을 두었다.

제2절 연구 범위와 방법

본 논문의 연구는 '스마트 홈 IoT 서비스 환경에서 보안위협과 정보보호 방안에 관한 연구' 주제로서 스마트 홈 IoT 서비스를 사용하는 사용자들의 디바이스 인증 취약점 및 네크워크 공격, 개인정보 노출 등 보안위협과 요구사항 범위를 연구하였고, 이와 아울러 보안 측면에서 디바이스 인증 취약점, 네크워크 공격, 개인정보 노출 등의 보안 위협을 방어하기 위한 정보보호 방안을 고찰하였다.

사물 인터넷과 스마트 홈 IoT 기술과 동향의 분석을 통하여 나타나는 보안 위협 및 유형이 무엇인지를 검토하였고, 이로 인해 스마트 홈 IoT적용분야에 대한 개인정보 침해 사례와 이에 따른 보안 위협들을 분석해 봄으로써, 본 연구가 향후 스마트 홈 IoT 서비스의 정보보호 대응 방안 마련에 활용될 것으로 기대한다.

제2장 관련 연구

제1절 IoT 서비스

1. IoT 서비스 정의

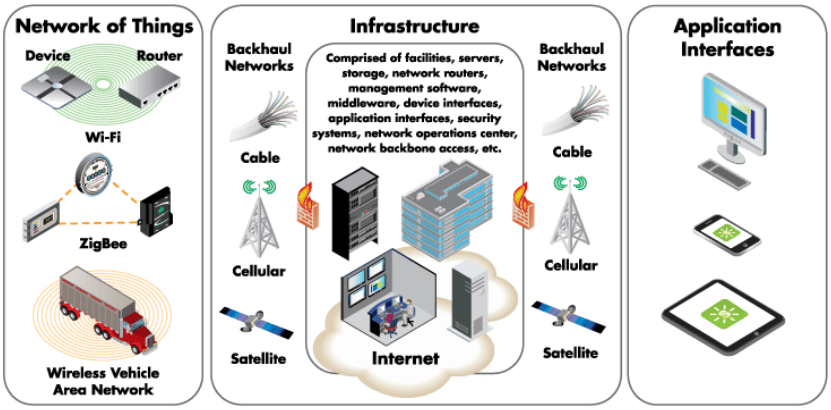
사물인터넷(internet of things), 영어 머리글자를 따서 'IoT'라 약칭하기도 한다. 1999년 매사추세츠공과대학(MIT)의 오토아이디센터(Auto-ID Center) 소장 케빈 애시턴(Kevin Ashton)이 향후 RFID(전자태그)와 기타 센서를 일상생활에 사용하는 사물에 탑재한 사물인터넷이 구축될 것이라고 전망하면서 처음 사용한 것으로 알려져 있다. 이후 시장분석 자료 등에 사용되면서 대중화되었다.

사물인터넷은 기존의 유선통신을 기반으로 한 인터넷이나 모바일 인터넷보다 진화된 단계로, 인터넷에 연결된 기기가 사람의 개입 없이 상호간에 정보를 주고 받아 처리한다. 사물이 인간에 의존하지 않고 통신을 주고받는다는 점에서 유비쿼터스나 M2M(Machine to Machine: 사물지능통신)과 비슷하기도 하지만, 통신장비와 사람과의 통신을 주목적으로 하는 M2M의 개념을 인터넷으로 확장하여 사물은 물론이고 현실과 가상세계의 모든 정보와 상호작용하는 개념으로 진화한 단계라고 할 수 있다.

<그림 2-1> M2M, IoT, IoE의 포괄적 개념

이를 구현하기 위한 IoT 주요 3대 기술 요소로는 유형의 사물과 주위 환경으로부터 정보를 얻는 '센싱 기술', 사물이 인터넷에 연결되도록 지원하는 '유무선 통신 및 네트워크 인프라 기술', 각종 서비스 분야와 형태에 적합하게 정보를 가공하고 처리하는 등, 각종 기술을 융합하는 '서비스 인터페이스 기술'이 있다.

IoT 기술을 활용을 구체적으로 살펴보면 아래[그림 2-2]와 같다. IoT는 인간과 주변 환경과의 상호 연결을 위해 센싱기술과 각종 유무선 네트워크 기술을 사용하며, 연결망을 통해 수집한 정보는 상황 인지 소프트웨어, 오픈 플랫폼 기술, 미들웨어 기술, 웹 서비스 기술, 소셜 네트워크에 의해 가공/처리 되고 이를 통해 유/무형의 사물과 각종 서비스와 연결된다.[2]



자료: http://www.digi.com/lp/internet-of-anything

<그림 2-2> 인간과 주변 환경의 IoT 개념도

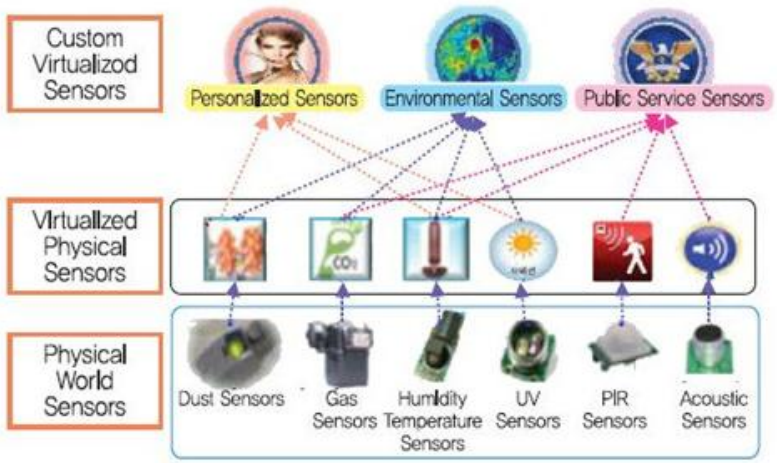
2. IoT 서비스 기술

1) 센싱 기술

센싱이란 사물이나 그 근접한 주위환경에 전자태그를 부착하여 온도, 습도, 열, 가스, 초음파, 원격감지, 전자파흡수율, 레이더, 위치, 영상센서

등을 통한 변화를 감지하여 수집한 정보들을 전달하는 핵심기술이다. 센서는 원격 감지, 레이더, 위치, 모션, 영상 센서 등의 유형 사물과 주위 환경으로부터 정보를 얻을 수 있는 물리적 기기를 말한다. 이러한 물리적 센서에는 표준화 인터페이스 및 정보 처리 능력을 내장한 기능도 포함된다.

가상 센싱 기술은 주로 IoT서비스의 인터페이스 구현에 사용되며, 기존의 독립적이고 개별적인 센서보다 한 차원 높은 다분야 센서기술을 사용함으로써, 보다 고차원적인 정보를 수집할 수 있다.



자료: http://www.industrysolutions.co.kr/news/articleView.html?idxno=4095

<그림 2-3> ETRI의 SVM의 센서 구상도

최근의 센서 기술은 표준화된 인터페이스를 기반으로 한 플랫폼과 정보처리 모듈을 탑재한 스마트 센서로 발전되어 가고 있으며, 수집한 데이터에서 특정 정보를 추출하는 가상 센싱 기능을 이용하여 사물인터넷 서비스 플랫폼에 적용되고 있다. 스마트기기는 가속도계, GPS, 센서, 카메라 등의 다양한 다중 센서들이 내장되어 더 지능적이고 고차원적인 웨어러블 컴퓨팅 서비스를 제공하고 있다. 정보처리 능력을 내장한 스마트 센서는

사람의 오감 기능처럼 센서가 상황을 인지하여 정보를 스스로 센서 노드에서 처리하거나 무선망을 통해 전달시켜주는 운영체제를 가지고 있다. 센서노드의 통신반경은 1m~10m 이며, 여러 개의 센서노드 간 연결되어 있는 네트워크를 센서 네트워크라고 한다.

센서 노드를 구현하기 위해서는 모든 사물들에게 고유한 식별체계와 주소체계를 인식시켜야 한다. 아직까지는 시맨틱URI(Uniform Resource Identificationo)를 기반으로 한 식별 체계가 많이 사용되고 있지만, IP주소에 대한 수요가 점차 증가 되어감에 따라 기존의 32비트의 IPv4 체계로는 폭발적으로 증가하고 있는 사물들에게 고유주소를 모두 할당하기 어려워 128비트의 IPv6 체계로 이동하고 있는 추세이다. 또한, 사물의 운영에는 지속적인 에너지 공급이 필요한데, 태양 에너지나 열에너지 등을 이용하여 전력을 공급할 수 있다. 더불어 TinyOS, MANYTIS 등의 저전력 에너지 운영체제를 사용하여 사물이 발생시키는 에너지 소모를 낮추는 방식도 활용되고 있다.

국내외 동향은 90년대 후반부터 RFID/USN 기술, 센서의 소형화, 저전력 기술 등의 개발과 센서를 활용한 환경 데이터의 수집 및 관리 등에 관한 연구가 진행되어 왔다. 영국의 ARM사, Qualcomm사, Texas Instruments사 등은 사물 인터넷의 센싱 칩셋 개발 제품으로 무선 송수신 칩, 센서, 마이크로 콘드톨러 등을 개발하였다. 미국의 IBM사, E-device사, Telular사, SIMCOM사 등에서는 IoT모듈인 무선 송수신 칩 및 마이크로 콘트롤러 등을 개발하였다. IBM사는 2013년 대용량의 센싱 데이터를 효율적으로 관리할 수 있는 사물인터넷망과 연결된 게이트웨이인 메시지 사이트를 개발하였다.[2]

2) 네트워크 인프라 기술

인간, 사물, 서비스 등의 분산된 사물인터넷 요소들을 서로 연결시켜

주는 유무선 통신 네트워크는 WPAN(Wireless Personal Area Network), WiFi, 3G/4G/LTE, Bluetooth, Ethernet, BcN, Microware, 위성통신, 시리얼 통신, PLC(programmable Logic Controller)등 거의 모든 상용화 네트워크를 이용할 수 있다. 인프라 기술이란 IP를 제공하거나 무선통신 모듈을 탑재하는 방식을 말한다. LTE의 등장으로 인하여 유선 인터넷 수준 이상의 초고속인터넷이 무선 인터넷으로도 가능해졌다. 네트워크 기술은 그 비용과 관리면에서 무선통신이 사물간 통신에 적합하며, RFID, 블루투스, 지그비, NFC, 와이파이, LTE-A 등이 이러한 근/원거리 무선통신에 사용되고 있다. 센서가 수집하는 정보들은 3G, 4G, LTE, BcN, 위성 등의 유무선 네트워크를 통해 교환되거나 WPAN(WiFi-Direct, Bluetooth, RFID/NFC 등)을 통해 독립적으로 전달 가능하다. 대표적으로는 블루투스, RFID, 지그비와 같은 비 IP WPAN 기술과 IP와 연동하기 위한 6LoWPAN과 RoLL 기술이 연구되고 있다. 그러나 사물인터넷이 보편화 됨에 따라, 사용량 증가로 인한 트래픽이 발생하면, 그 처리에 효율적인 소프트웨어 정의 네트워크(SDN)가 대체 인터넷망이 될 것으로 예상하고 있다.

최근 사물 인터넷에서 다양한 대역폭의 활용과 저 전력이 중요한 요인으로 부각되면서 블루투스(Bluetooth)와 지그비(Zigbee) 등과 같은 무선 네트워크 기술을 활용하려는 움직임이 활발히 이루어지고 있으며, 다양한 네트워크 기술을 효과적으로 활용하기 위하여 네트워크의 융합화를 위한 여러 방안들이 고려되고 있다. 예를 들면, 현재 상용화 되고 있는 HetNet(Hete
rogonous Network)은 많은 사람들이 몰리는 곳이나 기지국의 전파가 약한 곳에 펨토셀(Femto cell)과 원격무선장비(Radio Remove Hend)등과 같은 작은 기지국을 추가적으로 설치하여 통신 품질을 강화한 네트워크이다. 이처럼 네트워크의 융합화가 발전되면 다양하고 새로운 개념의 네트워크 인프라가 개발 될 것이라고 기대하고 있다.

국내외 동향에서는 해외의 AT&T, Verizon, Sprint사 등과 국내 SKT, KT, LGU+사 등에서 기본적인 유/무선 네트워킹 및 전문적인 M2M서비스 제품을 개발하고 있다. IBM사는 사물과의 일관된 정보전달 방법을 위하여 HTTP를 대체할 MQTT 프로토콜을 제시하였고, OASIS(Organi
zation for the Advancing open standards for the information society)에 의해 사물인터넷의 표준 프로토콜로 사용되고 있다. Coap(Constrained Environment Application Protocol)는 인터넷에서 센서 노드와 같이 제한된 컴퓨팅 성능을 갖는 디바이스 간의 통신을 실현하기 위해 IETF의 CoRE(Constrained RESTful Envifonments) 워킹 그룹에서 만들고 있는 응용계층 표준 프로토콜이다. 웹 서비스 구현 시, TCP, HTTP와 같은 프로토콜보다는 보다 가벼운 프로토콜이다.

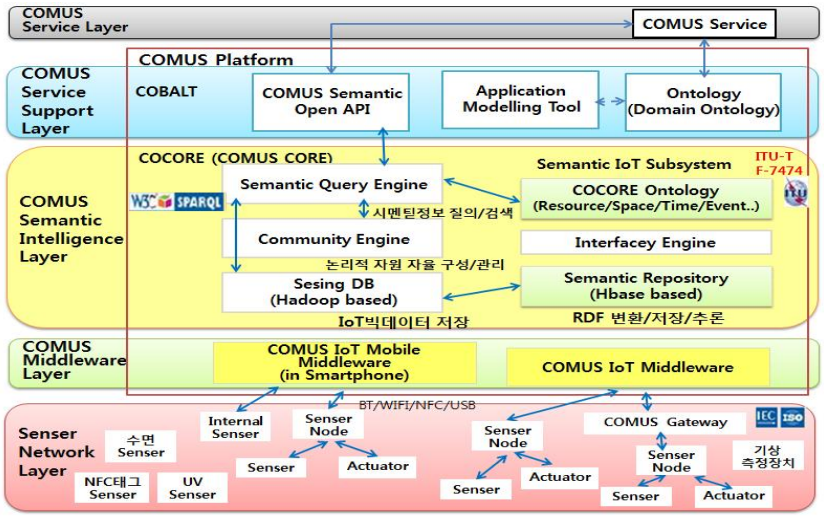
2015년 3월 바르셀로나에서 열린 세계 최대 모바일 전시회 '모바일 월드 콩그레스'(MWC)에서 우리나라의 SKT사는 5G 네트워크와 결합한 사물인터넷, 위치기반, 인텔리전스 등의 다양한 서비스 플랫폼을 공개하였다. KT사는 '5G 시대의 라이프 이노베이션'을 주제로 한 발표에서 공연장이나 도심 등의 무선 트래픽 밀집지역이나, 셀 경계 지역에서도 끊이지 않는 차세대 무선 네트워크 기술과 기존의 무선인터넷(WIFI) 주파수 대역을 엘티이(LTE)에 활용하는 기술, 9개 주파수 대역을 묶어 1Gbps의 속도를 구현하는 '9밴드 시에이(CA)' 등 5G의 기반이 될 신기술 등을 선보였다. [7]

3) 플랫폼 기술

사물인터넷을 통한 특정 기능(저장, 처리, 변환 등)의 서비스를 수행하는 사물 간 연동을 플랫폼에서 처리한다. 말하자면 플랫폼이란 사물 간 인터넷을 할 수 있도록 물리적인 통신 네트워크의 원활한 작동을 돕는 운

영체제이며, 사물 간의 정보를 주고받는 기술 표준이자 각종 애프리케이션의 핵심 기술이라고 할 수 있다.

서비스 플랫폼의 환경은 사물인터넷 서비스를 개발자가 요구하는 기능을 사용하기 쉽게 제공 할 수 있는 편의성을 가지고 있어야 하며, 낮은 비용으로 다양한 서비스를 개발 할 수 있어야 한다. 그러기 위해서는 모든 사물을 등록하고, 사물의 상태를 모니터링 하는 기능 또한 제공되어야 한다. 그림2는 ETRI사에서 개발한 개방형 시맨틱 USN 서비스(COMUS:Common Open Semantic USN Service) 플랫폼이다.



자료: 김재생, 『사물인터넷의 기술 소개 및 정책 방안』

<그림 2-4> ETRI사의 COMUS 플랫폼

COMUS 플랫폼은 USN 인프라와 사용자가 운용하는 다양한 IoT 기기와 센서를 사용하여, 언제 어디서나 원하는 기기 및 센싱 정보를 쉽게 활용할 수 있는 의미정보 기반의 서비스를 제공한다. 시맨틱 데이터의 표현방식을 따라 각 USN 자원의 메타 데이터를 변환하여 시맨틱 데이터로 가공하여, 비로소 정보를 재생산할 수 있다.

핸디소프트사에서 ETRI사와 2010년부터 공동 연구한 개방형 IoT 서비스 플랫폼(COMUS) 기술을 이전 받아 상용화한 IoT 플랫폼이 HANDYPIA이다. 기존의 IoT플랫폼은 센싱 데이터를 있는 그대로 전달해주는 역할만을 담당 했지만, HANDYPIA는 온톨로지 기반을 활용하여 시맨틱 IoT플랫폼으로 센싱 데이터를 표준화 작업 등을 거쳐 의미 있는 정보로 가공할 수 있다는 특장점이 있다. 스마트폰이나 셋톱박스 등 각종 스마트기기에 탑재된 모바일 IoT 미들웨어 기술인 '모리(MoRI: Mobile Resource Intrerchange)'를 통해 각종 내/외장 센서의 플랫폼간 연결을 돕는 기술도 제공된다. 'HANDYPIA'를 통해 개발한 '오미(五味)길' 서비스는 염도 와 온도 측정이 가능한 생활형 센서를 스마트폰 IoT 미들웨어 기술인 '모리(MoRI)'와 연계하여 사용자의 건강과 현재상황을 고려하여 그에 적합한 음식 및 음식점을 추천해주는 서비스이다.[7]

(a) (b) (c)

자료: 김재생, 『사물인터넷의 기술 소개 및 정책 방안』

<그림 2-5> (a)HANDYPIA 서비스, (b)플랫폼, (c) 서비스 오미(五味)길

4) 빅 데이터 처리 및 보안 기술

가트너사는 사물인터넷 기술을 사용하는 사물의 개수가 2020년 무렵에는 260억 개에 이를 것으로 예상하였다. 이렇게 많은 사물이 연결되면, 인터넷을 통한 빅데이터가 수집되고, 이 수집된 빅데이터를 관리하기 위한 효율적인 노력이 병행되어야 한다. 사물인터넷은 센서로부터 수집한 데이터와 센서 자체에서 생성되는 데이터를 대규모 데이터 센터에 지속적이며 체계적으로 저장하고, 사용자의 요청이 있을 때에는 이 데이터를 전달하는 서비스를 수행한다. 이러한 빅데이터의 효율적인 관리를 위해서는 빅데이터 기술과 더불어 클라우드 컴퓨팅 기술의 발전이 동반되어야 한다.

빅데이터란 다양한 종류의 대규모 데이터의 생성, 수집, 분석, 표현을 특징으로 하는 대량의 정형 또는 비정형 데이터 집합으로 정의할 수 있다. 빅데이터 기술의 발전을 통해 사물인터넷 분야에서도 의미 있는 정보를 제공할 수 있으므로 그 중요성이 부각되고 있다. 따라서 빅데이터로부터 의미를 추출하고 그 결과를 분석하는 효율적인 알고리즘의 개발 기술도 필요하다. 그러나 빅데이터를 수집하고 분석하기 위해서는 개인의 사적인 정보까지 수집할 필요가 있어서 사생활 침해화 보안 문제가 발생할 수 있으며, 모든 사물이 해킹의 대상이 될 수도 있다. 그렇기 때문에 유/무선 네트워크, 첨단 기기 및 센서, 사물, 사람, 장소 등의 사물인터넷 구성 요소에 대한 보안기술이 강화되어야 하는 것이다. [7]

3. 스마트 홈 개요

1) 정의

스마트 홈이란 사물인터넷(IoT)을 기반으로 가전, 에너지관리, 네트워크, 보안, 냉난방 및 환기, 홈 엔터네인먼트를 비롯하여 다양한 스마트 기기를 연동 및 제어하는 스마트 홈 솔루션과 각종 서비스를 포함하는 개념을 말한다. 여기서 사물인터넷은 여러 사물이 만든 정보를 공유하는 컴퓨터 통신망을 일컫는데, 이 중 스마트 홈은 가전제품을 비롯한 조명에너지, 보안기기 등은 물론 이고 스마트 카, 스마트 시티, 스마트교육 등이 연동된 모습이라고 할 수 있다. 한마디로, 우리의 주거환경에 정보통신기술을 융합하여 공간과 기기의 제약 없이 폭넓고 다양한 정보와 서비스를 제공함으로써 경제적 편익, 건강과 복지 증진, 안전한 생활이 가능하도록 하여 삶의 질을 한층 더 높게 만들어주는 인간 중심적인 주거생활 공간이 바로 스마트 홈 이다.

2) 스마트 홈 시장 전망

스마트 홈은 국내에서 1990년대 말 초고속인터넷의 보급으로 일반 가정에도 홈 네트워크 사업의 활성화 계기가 마련되었으나 그 기회를 살리지 못하고 정체상태가 되었고, 2000년대 후반에 들어서야 스마트 폰의 대중화와 사용자 수요가 발생함에 따라 초기단계의 스마트 홈이 구축되었으며, 2010년대 중반 사물인터넷의 상용화로 인하여 상황 인지형 스마트 홈이 본격적으로 도입되었다. 스마트 홈의 발전 모델은 IoT기술을 활용하여 거주자의 의도와 상황을 파악하고 그에 따라 적절하고 쾌적한 환경을 스스로 제공하는 주택이라 할 수 있다. 궁극적으로는 개인의 주거에 필요

한 모든 일상용품과 기기들에 사물인터넷을 융합하는 것이기 때문에 개인정보와 관련된 개인의 모든 생활영역에 방대하게 걸쳐있는 융합사업의 결정체라고 해도 과언이 아니다. 그만큼 시장규모도 크고, 성장잠재력도 크다. 글로벌 IT기업이나 전자·통신업체들이 앞다투어 시장선점을 위해 각축을 벌이고 있는 이유이기도 하다.

스마트 홈 산업은 통신, 방송, 가전, 건설, 콘텐츠 등 다양한 분야가 융합된 복합 산업으로 산업간의 파급효과가 큰 가치사슬을 통하여 지속적으로 부가가치를 창출 해 낼 수 있는 성장 산업이다. 센서, 스토리지, Post-PC 처럼 스마트 홈 의 실질적 구성요소가 되는 분야뿐만이 아니라 음성인식, 텔레메틱스, DTV 산업처럼 정보를 수집하는데 필요하거나 수집한 정보를 처리하여 의미가 있는 데이터를 만들어내는데 활용하는 컴퓨터그래픽, 컨텐츠 산업 등 스마트 홈 활성화는 다양한 분야의 시장에 까지 영향을 미치게 되는 것 이다.

스마트 홈 사업의 장기적인 전망은 긍정적이지만, 아직까지는 스마트 홈 서비스 시나리오가 구체화 되지 않고, 비지니스 모델도 불분명한데다, 개인정보 유출의 심각성이 대두되고 그 해결방안의 확립이 제대로 이루어지지 않아 스마트 홈 시장 확대에 걸림돌로 작용하고 있다.

제2절 스마트 홈 IoT 보안 침해사례

1. 다리미와 전기 주전자 침해사례

중국산 다리미와 전기 포트에 해킹에 활용되는 스파이 마이크로칩이 탑재되어 있는 것이 러시아이에서 발견되었다. 이처럼 가전제품에 포함된 스파이 마이크로칩은 보안되지 않은 무선 네트워크에 연결할 수 있다. 일단 네트워크에 연결되면 악성코드와 스팸을 유포 할 수 있고, 도청을 통해 개인정보를 수집하고, 이를 네트워크를 통해 해외의 서버에 전송하는 기능도 포함하고 있었다. 실제로 확인된 수량만 30여개에 달하고, 확인되지 않은 수량은 훨씬 더 많을 것으로 추측된다. 이러한 시도는 다리미와 전기 포트가 주로 쓰이는 호텔에서 각국 정상이나 주요 기업 CEO, 사업가 등을 대상으로 한 해킹으로 추측되고 있다. 다리미 및 전기 포트에 의해 배포된 악성코드를 통하여 대량의 좀비PC들이 만들어졌다면, 이들 좀비 PC들은 통제를 통한 대규모 해킹 공격에 악용될 수 있다.

2. 봇넷 'Thingbots' 취약점을 악용한 침해사례

미국 보안업체 Proofpoint사에 따르면 Thingbots이란 인터넷에 연결되어있는 스마트TV와 냉장고와 같은 가전을 통해 Phishing과 Spam-mail을 전송하는 사이버 공격을 말한다. 대규모 사이버 공격을 시작하는데 사용될 수 있는 "봇넷"을 이용하여 개인용 컴퓨터를 아무도 모르게 좀비화 시킬 수 있는 것처럼, Proofpoint사는 한 연구결과를 통해 "thingbots"으로 홈 라우터, 스마트 가전기기 등 스마트 홈 IoT 기기들에 대하여 악의적인 행동을 하기 위해 침투하여 좀비기기로 변형, 실제로 해킹에 사용할 수 있음을 밝혔다.[15]

위와 같은 방식으로 미라이(Mirai)를 이용한 대규모 DDoS 공격으로 1200여개 미국 주요기관 사이트를 마비시키는 사건이 발생했다. 약 12만대의 IoT기기(IP 카메라, NAS 등)가 공격에 악용됐다. 미라이 악성코드는 공장 출하 시, 설정된 기본 ID/PW를 그대로 방치한 IoT기기를 대상으로 기본 계정을 삽입하여 관리자 권한을 획득 후 감염시키는 방식을 사용했다. 또한 인터넷에 연결된 IP카메라가 전 세계로 생중계 되는 사례가 있었다. IP카메라 관리페이지 접속 시, 접근 가능한 사용자를 확인하지 않거나, 기본 ID/PW를 이용해 로그인이 가능한 점을 악용한 침해 사례였다. 취약한 포트와 기본 ID/PW 설정으로 방취된 점을 악용한 사례라고 볼 수 있다.

3. 유아 모니터 카메라 침해사례

영국 BBC의 보도내용에 따르면 미국 텍사스주의 한 가정의 유아 모니터링 카메라가 음란한 소리를 출력하였는데, 이는 FOSCAM사의 제품 취약점을 이용한 공격으로, 공격자는 해킹을 통해 카메라에서 음란한 소리가 나오도록 지시한 사례이다. 가정에서 아이들의 안전을 보강하기 위하여 모니터링 장비를 사용하는 것은 매우 유용할 수 있지만, 인터넷에 연결되는 장비를 사용하고자 한다면, 이로 인해 발생 할 수 있는 잠재적인 취약성에 대해 주의할 필요가 있는 것이다. 위 사례는 제품의 펌웨어 및 소트프웨어에서 발견된 취약점을 악용한 침해 사례이다.[36]

4. 스마트 가전기기의 침해사례

미국 보안업체인 Proofpoint사에 따르면 2013년 말부터 2014년 초까지 전세계에서 75만건의 피싱, 스팸 등의 악성 이메일이 가정에 설치한 홈네트워킹 라우터, 스마트 TV, 냉장고와 같은 스마트 가전제품들에 의해

발송되었다. 공격자들이 인터넷으로 연결된 가전기기 등을 해킹하여 제품에 탑재된 메일 기능을 악용하여 피싱, 스팸등의 악성 메일을 보냈다. 이러첨 사이버 공격에 스마트 가전기기들이 활용되기 시작했다고 볼 수 있다. 스마트 TV 해킹을 통하여 TV에 탑재된 카메라로 집안 내부를 생중계 할 수 있다. 또한, 마이크로 목소리를 녹음도 가능하다. TV 홈쇼핑 주문번호를 임의로 변경하여 사진, 동영상, 음성, 신용 카드 번호, 계좌번호, 위치정보 등의 정보를 수집/변경하여 악용하여 개인적인 피해가 발생할 수 있다.[20]

5. CCTV를 통한 프라이버시 침해

최근 전 세계의 7만 3000여개의 개인용 CCTV가 해킹되어 생중계되는 사건이 발생했다. 우리나라에서만도 약 6000여개의 CCTV가 해킹되었으며, 이는 미국에 이어 세계 두 번째로 많은 피해자가 발생한 것으로 조사되었다. 결론적으로는 '인세캠' 이라는 사이트의 운영자의 보안의 중요성을 강조하기 위해 해킹한 것으로 밝혀졌지만 일반 식당, 카페뿐만 아니라 개인 가정 집까지도 해킹을 통해 얼마든지 엿볼 수 있음을 확인 한 셈이다. 대부분의 CCTV는 네트워크 연결이 가능하다. 또한 관리자가 스마트폰을 통하여 실시간으로 CCTV 영상을 확인 할 수 있어 스마트폰을 통해 사진, 동영상, 음성 등의 추가적인 개인정보를 수집할 수 있다. 사이트에서는 CCTV가 설치된 위도와 경도도 확인할 수 있어 구글맵을 이용하여 해당 지역 위치 추적도 가능하다. 악용할 경우 개인프라이버시가 심각하게 침해되거나 금전적 피해까지 발생할 수 있음을 시사하는 것이다.

제3절 스마트 홈 IoT 서비스 보안 위협

1. 디바이스 계층의 보안 위협

1) 디바이스의 비인가된 접근

무선 공유기가 대중화된다는 것은 공격자에게는 공격대상이 큰 폭으로 증가한다는 것을 의미한다. 원격으로 감시하고 설정할 수 있는 기기의 경우에는 그 위험이 더 크다. 공격자는 비인가 디바이스를 정상적인 디바이스로 위장하여 무선 네트워크를 통해 악성 코드를 삽입하는 것이 가능하다. 악성 코드가 삽입된 스마트 디바이스는 좀비 디바이스가 되어 분산 서비스 거부 공격을 일으킬 수 있다. 또한, 홈 네트워크에 연결된 로컬 PC 및 스마트 디바이스들을 연쇄적으로 감염시켜 2차, 3차 피해가 발생할 수 있다.

2) 데이터 위·변조

스마트 홈 사용자는 무선 네트워크를 통해 내·외부에서 스마트 홈의 데이터를 송·수신할 수 있다. 공격자는 비 인가된 디바이스 및 센서를 통해 인가된 사용자로 위장하여 데이터를 전송하거나 가로채어 위·변조가 가능하다. 이는 스마트 홈 디바이스와 사용자들에게 위·변조된 데이터를 전달하여 잘못된 인증 및 서비스가 이루어지도록 위장하는 위협 방식이다.

3) 정보유출

스마트 홈이란 무선 네트워크를 통하여 스마트 디바이스가 통신하는 환경을 말한다. 공격자는 무선 네트워크를 통해 스마트 디바이스에 접근

하여 스마트 홈의 정보를 얻을 수 있다. 악의적인 공격자에게 노출될 경우에는 심각한 2차 피해로 이어질 수 있다.

4) 장치의 절도 및 분실

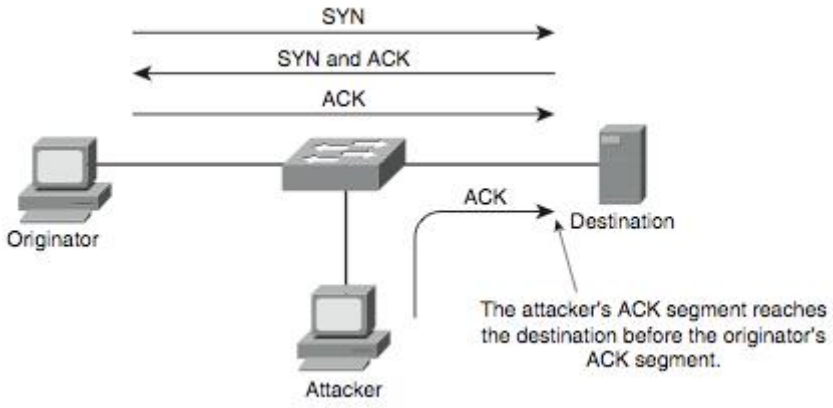
스마트 홈 장치가 분실되면 공격자가 접근해서는 안 되는 정보에 접근 및 수신할 수 있어 기밀성이 손상될 수 있고, 스마트 홈 장치에 저장된 인증 정보를 사용하여 네트워크에 대한 접근 권한을 얻을 수 있으며, 이는 네트워크 침해로 이어질 수 있다.

2. 네트워크 해킹을 통한 보안 위협

1) IP 스푸핑(Spoofing)

스마트 홈 IoT 환경은 가정 내에서 무선 인터넷을 이용하여 가전 기기 등을 제어한다. 그렇기 때문에 무선 인터넷 사용 시 암호화 설정을 하지 않을 경우 중요한 정보를 도청할 위험은 항상 따른다. IP 스푸핑(IP spoofing)은 정보의 기밀성에 대한 위협이다. TCP/IP 구조적인 결함으로 인하여, 허가되지 않은 사용자가 내부망에서 외부망으로 전송되는 패킷으로부터 발신처를 도용하여, 마치 허가된 사용자인 것처럼 위장하여 시스템을 공격하는 방법이다.

출발지 라우팅 정보와 출발지 IP 주소를 이용하여 <그림 2-6>과 같이 상대방 호스트가 자신의 호스트를 신뢰하게 만드는 방법이다



자료: https://laurasecurity.wordpress.com/2008/08/04/ip-spoofing-attack/

<그림 2-6> IP 스푸핑 process

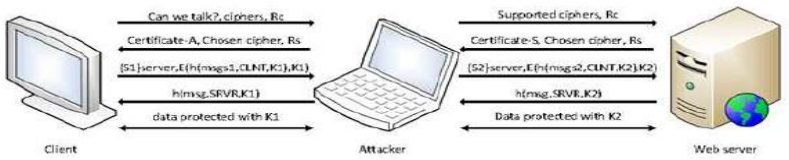
패킷별(Per-Packet) 암호화의 경우, 공격자는 알려진 데이터 패킷의 응답으로부터 데이터 스트림을 재구성할 수 있기 때문에 다음 패킷을 스푸핑 할 수 있다. IP 스푸핑을 이용한 공격은 공격자들이 만들어 놓은 관련 소스가 풍부하여, 일단 신뢰하는 호스트로 접속한 후 흔한 버그로도 공격이 가능하다. 또한, TCP/IP 자체와 호스트 응용계층에서는 막을 수 없다는 문제점도 가지고 있다. TCP/IP 프로토콜은 본래 학술적인 용도로 인터넷이 활성화되기 이전의 설계된 프로토콜이다. 초기 연구 단계에서 송신자와 수신자 사이의 통신에만 중요성을 두고 연구가 진행되었기 때문에 보안은 크게 고려하지 않았다. 패킷에 대한 암호화 및 인증 등도 고려하지 않았기 때문에 오늘 날 네트워크상에서 발생하고 있는 보안의 기본 요소 중 기밀성, 무결성 등도 보장할 수 없는 것이다.

2) MITM(Man-in-the-Middle)

인터넷은 기본적으로 클라이언트/서버 아키텍처를 기반으로 작동한다. 사용자는 중앙서버에 접속하고 해당 연결을 통하여 필요한 정보를 수신한

다. 인터넷을 연결하면 사용자가 요청한 정보와 그 요청에 따라 수신되는 정보는 전체적으로 전송되는 것이 아니라 패킷이라는 작은 패키지로 분할되어 전송된다. 이 패킷들은 명령받은 목적지에 도달하기 까지 여러 기기를 거치며, 목적지까지의 각 단계를 홉(hop)이라고 한다. 패킷은 라우터, 게이트웨이 및 브릿 등과 같은 기기를 거치는데, 중간자는 클라이언트 또는 실제 서버를 포함하여 이러한 기기들 사이의 어떤 지점이든 위치 할 수 있다. 중간자 공격이 위험한 이유는 모든 통신 내용을 도청 할 수 있으며, 나아가서는 그 데이터를 조작 가능하다는데 있다. 이 경우에는 심각한 결과가 야기 될 수 있다.

아래 <그림 2-7>처럼 중간자(Man-in-the-Middle) 공격 해킹이 발생 할 수 있다.



자료: Smart TV Hacking, University of Amsterdam, 2013

<그림 2-7> 중간자 공격

스마트 TV와 웹 서버 통신 시, 공격자가 스마트 TV와 웹 서버간에 위치하여 전송 데이터에 접근하여 비인가 열람 및 데이터의 위·변조가 가능한 공격 방법이다.

3. 개인정보관련 보안 위협

IoT는 가전제품, 전자기기, 헬스케어, 원격검침, 스마트 홈, 스마트 카 등 다양한 분야에서 정보 공유 및 제어가 가능하다. IoT의 글로벌네트

워크화로 인해 생활의 편리성을 가져올 것이라는 기대와 함께 이에 대한 해킹, 정보유출 등의 다양한 침해요인에 대한 우려가 높아지고 있다. 더욱 이 위험한 것은 <표 2-1>에서 보는 바와 같이 보안 취약성으로 인한 다양한 침해위협 및 정보 유출로 인한 개인정보의 침해이다.

침해위협요소	대표사례
프라이버시 격차에 따른 개인정보 주체의 통제·감독권 결여와 정보 불균등에 따른 보안위협	웹 카메라 등 IoT의 비밀번호 설정을 모르는 고령자, 아동 등의 지나친 사생활 침해
동의서를 읽거나 동의에 클릭하여도 실질적 동의로 보기 어려운 상황 발생	사용자들은 사물인터넷 장비의 개인정보 처리 인지가 미흡하여, 동의서를 읽거나 클릭해도 그 내용을 인지하지 못함
수집목적을 벗어난 IoT 수집정보의 유출 위험 증가	복잡한 사물인터넷을 통해 수집된 개인정보가 원래의 목적을 상실하고 제 3의 목적으로 가공되어 제3자에게 제공될 위험
사용자들의 사용 형태나 습관 등의 모니터링 유형화에 따른 침해위험	병원에서 진단형태나 습관 등을 모니터링하여 의사들의 진단에 관여할 위험
병원에서 진단형태나 습관 등을 모니터링하여 의사들의 진단에 관여할 위험	개별 정보의 식별가능성이 떨어지는 정보가 조합과정에서 익명성, 비식별성의 보장이 어려움
IoT 기기간 자동교환에 따른 보안 위험 증가	농협계좌 1억대 무단 인출로 인한 개인정보 유출과 같이 위험요소 식별 및 자체 분석의 어려움

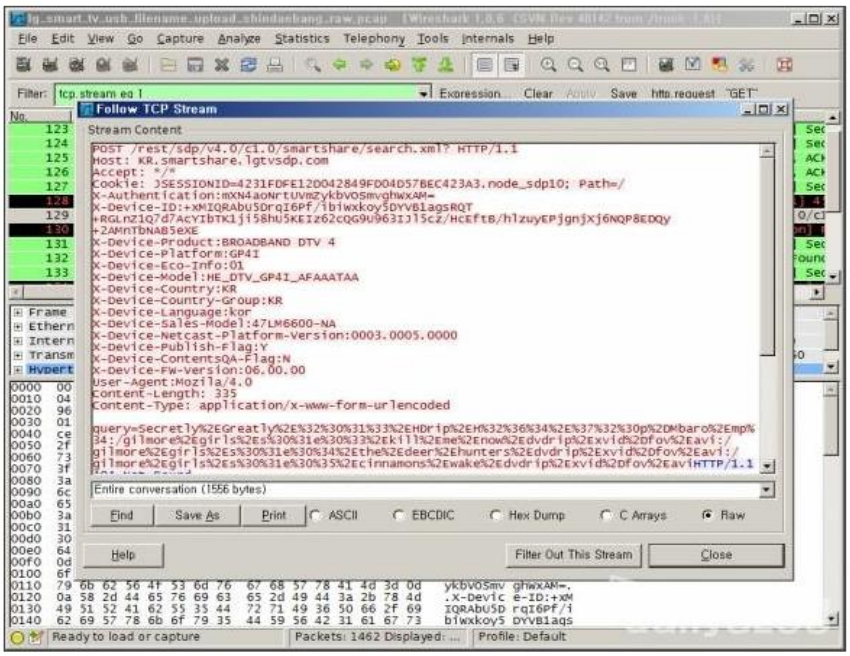
자료: IoT시대에서의 개인정보보호정책과제에 관한 연구

<표 2-1> IoT 환경에서의 개인정보 위협요소

IoT의 확산은 산업적 측면에서 혁신을 의미한다. 그러나 개인정보의 오남용에 따른 피해 증가 가능성을 동시에 내포하고 있다. IoT의 확산은 데이터 수집이 가능한 디바이스의 증가, 엄청난 양의 데이터 축적과 다방

면에 걸친 데이터 활용이라는 측면에서 개인정보보호에 대한 요구가 커질 수 밖에 없다.[31]

또한, IoT는 엄청난 양의 데이터 수집과 활용을 전제로 함에 따라 필연적으로 개인정보 침해 가능성을 증가시킨다. 일례로 L기업의 스마트 TV가 사용자의 시청 채널 및 시간, 미디어 파일 이용 목록 등의 개인정보를 L기업의 서버로 전송하는 사례가 발생했다. 스마트 TV 내장 기능인 사생활 보호 기능 중 '시청 정보 수집' 설정을 비활성화 하더라도 고객의 동의 절차 없이 L기업의 서버로 전송되었고, 시청 정보 외에도 스마트 TV와 연결된 USB 등 외장하드에 있던 동영상 및 사진 파일의 이름도 전송 된 사례이다.[32]



자료: http://www.dailysecu.com/?mod=news&act=articleView&idxno=5721

<그림 2-8> 스마트TV를 대상으로 테스트한 결과

스마트 TV 뿐만 아니라, 스마트 홈 IoT에 사용되는 가전 기기는 부착된 센서를 통해 집안 내 상황에 대한 정보를 비롯하여 행태정보, 민감

정보 등을 수집한다. 집 내부의 사람 움직임, 방안의 온도, 습도, 불빛의 밝기, CCTV, 가스 밸브 등을 감지, 스마트 그리드의 경우 어떤 활동에 전기를 많이 소모하는지 여부, 여행으로 인해 장기 외출을 했는지 등 부재 여부, 집안에서 사용하는 기기 목록 등이 파악 가능하다. 이처럼 스마트 홈 IoT시대에서는 가정에서 사용하는 가전기기를 통하여 실시간 개인정보를 수집함으로써 정보보안 위협을 낳고 있다. 때문에 스마트 홈 IoT을 통해 사용되는 모든 기기는 개인정보 유출, 사생활 침해 등의 보안위협요소를 발생시킬 수 있다는 우려가 제기되고 있다.

제4절 스마트 홈 IoT 서비스 보안 요구사항

1. 디바이스 계층의 보안 요구사항

1) 디바이스 인증 및 식별

스마트 홈 IoT환경에서 가정에서 사용하는 인터넷 무선 공유기를 통하여 비정상적인 디바이스를 정상적인 디바이스로 위장하여 접근하는 것이 가능해졌다. 따라서 가정에서 사용하는 모든 스마트 기기들은 정상적인 디바이스로부터 전달된 메시지임을 검증 받을 수 있어야 한다. 더불어, 비정상적인 디바이스에 대한 접근 및 차단이 이루어져야 한다.

2) 데이터 무결성

스마트 홈 IoT환경에서 사용자는 내·외부에서 무선 네트워크를 통해 스마트 홈의 데이터를 송·수신 할 수 있다. 이때 공격자는 중간 과정에서 데이터를 가로채어 스마트 홈 디바이스의 메시지와 데이터 위·변조가 가능하다. 메시지 및 데이터 위·변조 함으로써 스마트 홈 디바이스의 오작동을 유발하고 사용자에게 혼란을 초래 할 수 있는 것이다. 따라서, 스마트 홈 환경에서 무선 네트워크를 통해 전송되는 모든 데이터와 메시지는 위·변조 되지 않아야 한다.

3) 데이터 기밀성

스마트 홈 IoT환경은 그 내부에 지극히 개인적인 민감한 데이터를 포함하고 있다. 공격자가 무선 네트워크를 통해 스마트 홈 IoT 디바이스

에 접근하면 이러한 데이터 등의 정보가 유출 될 수 있다. 따라서 스마트 홈 IoT 디바이스 통신 환경에서 공격자 및 비정상적인 사용자는 확인 할 수 없도록 데이터는 항상 암호화 하여 전송되어야 한다.

2. 네트워크 환경에서의 보안 요구사항

1) 통신 채널 보호

스마트 홈 IoT 환경에서는 디바이스 간 통신을 하기 위해 채널을 생성한다. 생성된 통신 채널은 실시간으로 감시 및 제어함으로써 보호해야 한다. 통신 데이터에 대한 암호화 알고리즘을 구현 및 적용해야 하며 무선 공유기 및 네트워크 암호도 필수적으로 적용해야 한다.

2) 네트워크 제어 기술

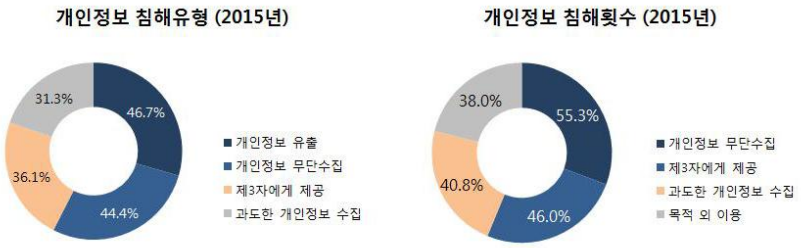
공격자는 스마트 홈 IoT 기기에 감염된 악성코드를 이용하여 트래픽을 급격히 증가시켜 서비스 거부 공격 및 분산 서비스 거부 공격을 유도한다. 악성코드에 감염된 기기에 의한 트래픽 폭증 공격(DDoS)을 방지하기 위해서는 네트워크 모니터링 및 관리 기술이 필요하다. 접근 권한을 분류하여 비정상적인 사용자에 대한 접근 및 통제가 필요한 것이다.

3. 개인정보관련 보안 요구사항

스마트 홈 IoT 환경에서 가전기기를 통하여 불법적인 데이터 수집/분석에 의한 개인정보 침해피해가 늘어나고 있다.

개인정보보호위원회 조사에 따르면 개인정보 침해 피해에 대한 상담

건수는 ‘14년 158,900건으로 ‘05년 18,206건 대비 약 8배 이상 증가한 것으로 나타났다. 침해의 유형은 ‘개인정보 무단 수집’의 빈도가 가장 높았으며, ‘제3자에게 제공’, ‘과도한 개인정보 수집’, 목적 외의 이용’ 등의 순으로 나타났다. [31]



자료: 박경률, “개인정보보호정책 설정 및 협상 규격을 이용한 홈 IoT 환경에서 개인정보보호에 대한 연구”

<그림 2-9> 개인정보 침해유형 통계

위의 통계에서도 확인할 수 있듯이, 스마트 홈 IoT환경에서도 개인정보 침해에 대한 위협은 예외가 될 수 없다. 스마트 홈 IoT은 데이터 수집이 가능한 디바이스를 활용하여 방대한 양의 데이터를 축적하고 다방면에 걸쳐 축적된 데이터를 활용한다는 측면에서 개인정보보호에 대한 요구가 가중되고 있다. 따라서 스마트 홈 IoT신뢰도 제고를 위해서는 기술적·관리적 조치뿐만 아니라 컴플라이언스 이슈도 고려되어야 한다.

제3장 스마트 홈 IoT 정보보호 방안

제1절 정보보호 방안

1. 디바이스 보안 정책 방안

디바이스 입장에서 바라 본 보안상의 문제는 '비인가의 디바이스 접근', '데이터 위·변조', 정보유출, 장치의 절도 및 분실 등이다. 이와 같은 보안 문제는 개인 정보의 유출 및 데이터 위·변조로 인한 사용자 혼란 등이다. 이에 대응하기 위한 보안 검토 사항을 정리해 보며 다음과 같다.

첫째, 디바이스의 원격 잠금 및 원격 파일 삭제 기능 등의 물리적인 보안 대책이 필요하다. 둘째, 외부에서 데이터 접근 시 사용자 인증과 관련한 보안 대책이 필요하다. 셋째, 스마트 홈에서 사용하는 주요 기기의 프로그램 실행 시 다른 프로세스 실행을 감지 및 제거 기능이 필요하다.

이처럼 정보보호 방안에 대응하기 위한 중요한 보안 검토 사항이 있음에도 불구하고, 스마트 홈 IoT 내에서의 디바이스 이용은 필수불가결한 이용 방법 중 하나일 것이다. 현재 많은 기능을 포함하고 있는 디바이스는 개인정보 관리는 물론, e-mail, 통화 내역, 스케줄 관리, 타인과 주고받은 문자 내역, SNS와 같은 사생활, 사진, 동영상 등을 모두 가지고 있다. 하지만 이러한 디바이스는 보안문제와 관련하여 개인정보 보호 및 정보 유출 방지 등 중요한 보안 이슈를 해결하지 못하면 스마트 홈 IoT서비스를 이용할 디바이스로는 선택이 불가능하게 될 것이다.

이처럼 디바이스의 보안을 위협하는 문제를 예방하기 위하여 디바이스 보안에 해당하는 보안 정책을 아래와 같이 제시한다.

① 인증을 거쳐 등록된 디바이스만 가정내의 시스템 접속을 허용한다.

② 무결성 체크를 통하여 무결성이 훼손된 기기는 접근을 통제

및 차단을 한다.

③ 스마트 홈 IoT 서비스 사용 시, 홈·가전 기기와 비정상적인 접속 시 강제 접속을 차단한다.

④ 비밀번호 문자 조합 및 주기적인 변경을 수행한다.

⑤ 스마트 홈 IoT 서비스 사용에 미 등록된 디바이스 접속을 차단한다.

⑥ 모든 송·수신 데이터를 암호화 한다.

2. 디바이스 취약점 대응 방안

취약점을 가진 스마트 홈 IoT 제품이 시장에 공급되는 것을 방지하기 위해서는, 개발 단계에서부터 다음과 같은 부분을 고려해야 한다.

첫째, 새로운 취약점이 발견될 수 있는 소프트웨어 또는 펌웨어의 개발에는 보안 모듈이 선행 적용되어야 하며, 개발 시, 시큐어 코딩 기법을 활용하여 개발되어야 한다.

스마트 홈/가전 제품에 시큐어 코딩을 적용하지 않을 경우 데이터 검증 및 표현, 보안 기능, 시간 및 상태, 에러 처리, 코드오류, 캡슐화, API 오용 등에서 보안 취약점이 발생할 수 있으며 공유기, IP 카메라, 앱 등의 XSS 취약점은 사용자 정보를 모으기 위한 1차 공격으로 이루어지는 경우가 있어 필터링 적용이 필요하다.

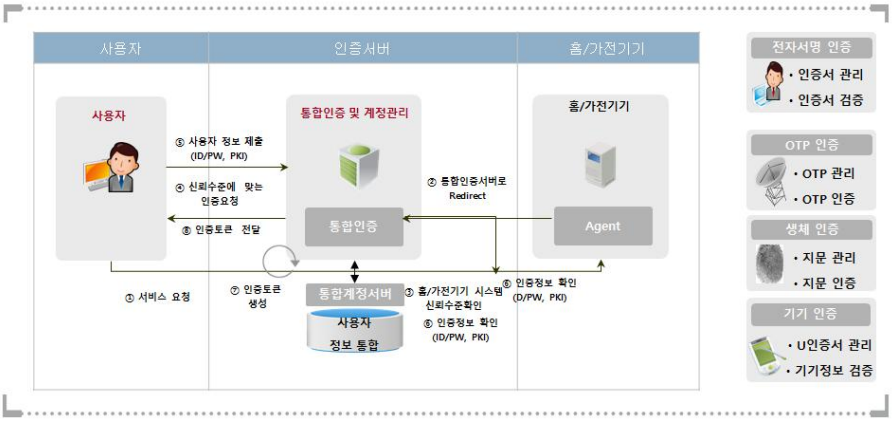
둘째, 스마트 홈에서 사용하는 제품에 대한 관리 및 제어를 위해 인가자를 식별 및 인증할 수 있어야 한다.

보안요소	상세내용
인증(AuthN)	- 인증을 위해서는 패스워드 와 같은 지식기반 인증, 스마트카드/보안토큰과 같은 소유

	기반인증, 지문과 같은 생체 정보 기반 인증, 공개키 인증서를 사용한 객체 인증 가능
인가(AuthZ)	- 해당 자원에 대한 사용 권한을 확인하여 접근 권한을 부여 - RBAC(Role Based Access Control), ABAC(Attibute Based Access Control)과 같은 접근제어 기법 연동 필요
IM(ID Management)	- 사물을 다른 사물과 구별하고 식별하기 위해서 식별자 관리(Identity Management:IM)가 필요

<표 3-1> 인증/인가/IM(ID Management)

위의 <표 3-1>은 기존 통합계정관리(IAM: Identity Access Management)에 포함되어 있는 기술이다. 안정성이 검증된 표준 보안 기술을 활용하여 스마트 홈 IoT 서비스에 확장 적용하여 스마트 홈 시스템 관리를 위한 계정 및 액세스 관리 기능을 제공 할 수 있다. 또한, 기존 ID/PW, 인증서 등의 1-Factor 방식에서 지문을 통한 생체인증이나 OTP인증 등과 결합하여 2-Factor 방식으로 인증을 강화함으로써 개인정보 침해에 더욱 효과적으로 대응할 수 있다.



<그림 3-1> 통합계정관리 구성도

3. 네트워크 정보보호 방안

스마트 홈 IoT 서비스 환경에서의 기기는 그 특성상 유·무선 네트워크로 연결되어 있다. 즉, 다양한 침투 경로를 통한 보안 위협을 지니고 있는 것이다. 때문에 다양한 서비스가 제공될수록 해당 서비스에 존재하는 보안 위협이 공유 될 가능성은 높아진다. 스마트 홈 기반에서 네트워크 간의 보안을 확보하기 위해서는 연결되어 있는 디바이스가 서로 신뢰할 수 있는 디바이스인지 확인할 수 있어야 하며, 디바이스간의 송·수신 데이터가 제3자에 의해 도청되는 것을 방지할 수 있어야 한다. 이를 위한 대응 방안이 바로 SSL(Secure Sockets Layer)프로토콜을 이용한 방식이다. SSL을 사용하면 공용 네트워크 상에서도 안전한 트랜잭션 처리가 가능하다. 하지만 약점도 존재한다. 그 약점은 크게 두 가지로 나누어 볼 수 있다. 첫째는 SSL 서버 인증서의 탈취·복제의 위험이다. 둘째는 SSL 세션 처리를 위한 암/복호화가 속도 및 성능 저하를 가져올 수 있다. 이러한 문제들을 해결하기 위해 네트워크 패킷에서 중요 정보(계정 로그인, 기기 제어 명령 등)가 노출되거나 도청되지 않도록 특정 데이터만을 보호

하는 공개키 기반구조(PKI :Public Key Infrastructure)의 부분 암호화이다.

<그림 3-2> 데이터 암호화 Service Flow

SSL(Secure Sockets Layer)은 대체로 특정 부분 암호화 방식을 적용함에 있어서 <표 3-2>와 같은 기능 및 보안 요구사항을 충족하여야 한다.

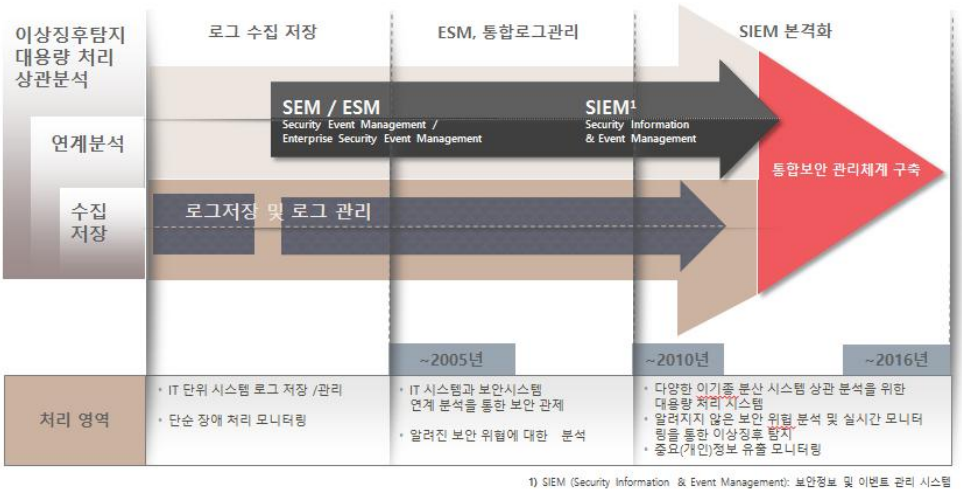
보안요소	상세내용
부인방지	- 전자봉투 방식, 대칭키 암호화 방식 모두 사용 - CRL, OCSP를 통한 인증서 유효성 검증
보안성/안정성	- 국내 및 국제 표준 알고리즘 사용(SEED, AES, 3DES, RSA, KCDSA, SHA-1, SHA-2 등) - 보안 채널 생성 시마다 사용자 세션키를 갱신하여 안전한 세션키 교환 수행

	– 키 관리 프로토콜(ECDH, DH 알고리즘 등)를 적용
기밀성/신뢰성	– 비 대칭키 암/복호화, 대칭키 암/복호화, 의사 난수 생성 – 공개키 및 대칭키 암호화 방식으로 네트워크에 전송된 데이터에 대한 위변조 여부 및 무결성 검증

<표 3-2> 공개키 기반구조 암호화 보안요구 사항

4. 개인정보보호 방안

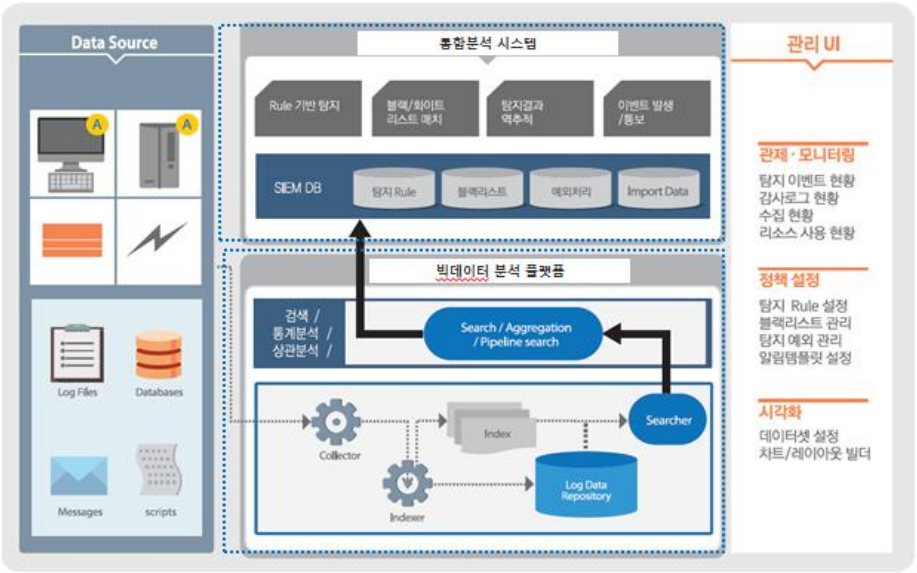
스마트 홈 IoT 환경에서의 보안 위협은 단순 개인정보의 유출뿐만 아니라 가정내에 심각한 피해를 야기하고 있다. 현재 빈번하게 발생하는 개인정보 유출사고의 대부분의 원인은 기술적 조치 부족에서 따른 것이다. 스마트 홈 IoT서비스의 활성화와 개인정보보호라는 두 마리 토끼를 잡기 위해서는 기술적·관리적 수단의 강화를 전제로 하여 개인정보의 활용에 유연하게 대처할 필요가 있다. 그 대응방안으로 추후 사고 재발 방지 및 사전 사고 방지, 선제적 대응을 위한 이상 징후에 대해 빅데이터 기술을 접목하여 일반적인 침해사고 모니터링 뿐 만 아니라 시나리오 기반의 보안 모니터링을 통한 통합보안 관리체계를 구축해야 한다.



<그림 3-3> 통합보안 관리체계 추이

현재 스마트 홈 IoT 환경에서 사용하는 기기의 경우 이상징후 확인 시 각각의 기기별로 접속하여 확인하여야 하므로 이상징후에 대한 조기탐지 및 사전 대응이 어렵고, 개인정보 유출에 취약하다. 이에 비해 통합보안 관리체계(Big Data Platform & SIEM)를 사용하면 일괄적인 모니터링 뿐만 아니라 시나리오 기반의 보안 모니터링을 위한 기반까지 마련할 수 있다.

아래 <그림 3-4>와 같이 차세대 통합보안 관리체계 구성 및 역할은 크게 세가지로 나눌 수 있다. 첫째로 Big Data Platform 으로 노드(Collector, Indexer, Searcher) 및 데이터 디바이스 관리, 수집유형, 디바이스별 정책, 정책 패턴관리 영역 이다. 둘째는 SIEM 영역으로 시나리오 기반 보안 위협 탐지(실기간 이벤트 현황 모니터링), 실시간 이벤트 조회(감사, 탐지), 룰/시나리오 관리영역이다. 마지막으로 사용자 편의성으로 Web Interface 영역으로 구성된다.



<그림 3-4> 통합보안 관리체계 구성도

통합보안 관리체계(Big Data Platform & SIEM)를 통해, 스마트 홈에서 사용하고 있는 각각의 제품들에 대하여 보안을 강화 할 수 있다. 보안 강화를 통한 장점에 대해 열거 해 보자면 다음과 같다.

우선, 각각의 제품에 대한 통합 관리 체계를 강화 할 수 있으며, 개인정보 유출방지를 위한 시나리오 기반 분석을 이 가능하다. 또한 보안사고 발생 시, 체계적 증적 추적 관리 체계를 확보할 수 있으며, 보안 감사(Audit)기능을 추가 강화 할 수 있다. IT Compliance 대응 체계 수립이 가능하기 때문에 다양한 정보유출 방지 및 법적 규제 준수를 위한 보안이 가능하다. 마지막으로 고위험군 모니터링을 통하여 보안 사고를 사전에 예방 할 수 있다.

제2절 정보보호 효율적 모델 제시

본 논문에서 제시한 스마트 홈 IoT 정보보호 방안을 활용함으로써, 스마트 홈 IoT 서비스를 이용하는 사용자는 계정 및 권한 접근을 효율적 통합관리 및 중요개인정보 Life-Cycle 단계별 내부통제 미비점에 대한 보안 기능 강화를 통한 내부통제 체계화 및 보안 역량을 강화할 수 있을 것으로 기대한다. 또한, 점차 강화되고 있는 정보보안 Compliance에 능동적으로 대처하므로 스마트 홈 IoT 서비스를 통한 사용자의 정보유출사고 위험 감소 및 대외 신뢰도가 한층 높아질 것으로 기대한다.

먼저, 디바이스 정보보호 정책 방안을 적용함으로써 다음과 같이 4가지 측면에서 정보보호 기대효과를 확인할 수 있다. 첫째, 일괄정책 및 통합관리를 통한 일관성 있는 관리체계를 사용자들에게 제공할 수 있다. 둘째, 정보유출 방지를 위한 가정 내의 보안기능을 강화 할 수 있다. 셋째, 강화되는 IT보안 법적 규제 및 준수사항을 만족할 수 있다. 마지막으로 가정 내의 디바이스 등록/삭제 등의 기능 자동화를 통한 업무 연속성 및 안전성 확보가 가능하다.

시장 조사 기관 가트너에 따르면 디바이스에 통합계정관리 보안 정책 적용 시 1년에 300% ROI 효과를 볼 수 있으며, 관리 대상 사용자와 시스템이 많을수록 ROI 효과를 볼 수 있는 기간이 짧아진다고 발표한 바 있다.

계정관리 측면		User Self Service 측면		패스워드 관리 측면	
정보보안 정책 미 적용	정보보안 정책 적용	정보보안 정책 미 적용	정보보안 정책 적용	정보보안 정책 미 적용	정보보안 정책 적용
$6.00/user (1year)	$0.80/user (1year)	$7.40/user (이벤트발생)	$1.30/user (이벤트발생)	$19.30/user	$2.60/user

1년에 $5.20/user 절감	1개의 시스템당 $16.10/user 절감	1년에 $16.70/user 절감
사용자의 노동력과 교육 비용이 절감	사용자가 아닌 시스템의 자동 관리로 누락 및 노동력 감소	헬프 데스크 직원 비용 절감

<표 3-3> 정보보안 정책 ROI 효과

다음으로 네트워크 정보보호 방안이다. 기존에 사용하고 있는 방안으로는 SSL(Secure Sockets Layer) 프로토콜 방식이 있다. 기존 SSL 프로토콜 방식이 가지는 문제점은 서버의 성능 저하로 SSL 프로토콜의 연산과정은 많은 계산능력을 필요로 하기 때문에 과부하로 긴 응답시간을 유발 할 수 있다. 하지만 공개키 기반 구조의 부분 암호화를 적용하여 문제점을 보완할 수 있다. 공개키 기반구조는 Resource전체를 암호화 하는 것이 아니라 경량 보안 프로토콜로 사용자 중요정보만 부분 암호화 하기 때문에 서버 성능 개선 뿐만 아니라, 속도도 뛰어나다. 또한, 데이터 송수신 대상이 본인인지의 여부를 인증서를 통해 증명, 상대방 위장을 원천적으로 봉쇄하기 때문에 보안성이 뛰어나다.

마지막으로는 개인정보 보호를 하기 위한 통합보안 관리체계 구축이다. 기존의 전통적인 개인정보보호 방식은 첫째, 정보 수집 시 동의 획득, 둘째, 암호화를 통한 개인정보보호, 세번째는 접근 제어를 통한 정보 유출 방지 또는 시스템 보안 기법(방화벽 등)을 통한 정보 유출 방지였다. 하지만, 2000년 대 이후로는 데이터 수집 및 가공/활용 단계에서 데이터 마이닝 기법을 활용한 개인정보 보호를 강화하고 있다. 개인정보 침해 문제는 Top-Tier 서비스 수준에서 중요하게 취급 될 필요가 있다.

현재 스마트 홈 IoT 환경에서 사용하는 기기의 경우 이상징후 확인 시 각각의 기기별로 접속하여 확인하여야 하므로 이상징후에 대한 조기탐지 및 사전 대응이 어렵고 개인정보 유출에 취약하다. 이에 비해 통합보

안 관리체계(Big Data Platform & SIEM)를 사용하면 일괄적인 모니터링 뿐만 아니라 시나리오 기반의 보안 모니터링을 위한 기반까지 마련할 수 있다. 또한, 각각의 제품에 대한 통합 관리 체계를 강화 할 수 있으며, 개인정보 유출방지를 위한 시나리오 기반 분석이 가능하다. 보안사고 발생 시, 체계적 증적 추적 관리 체계를 확보 할 수 있으며, 보안 감사(Audit) 기능을 추가 강화 할 수 있다.

<그림 3-5> 통합보안 관리체계 기대효과

<그림 3-5>와 같이 스마트 홈 IoT의 개인정보보호의 정보센싱, 가공/처리/활용을 단계별로 보호 및 관리 할 수 있으며, 해킹 패턴 분석, 개인정보 로그 데이터 관리, 개인정보 침해 추적성 등의 기능을 통하여 개인정보에 대한 효과적인 강력한 보안 강화 기능을 기대할 수 있다.

제4장 결론

유비쿼터스 시대로의 진입은 더욱 가속화 되고 있다. 스마트기기의 상용화와 통신기술의 발달로 스마트 홈 IoT는 다양한 영역에서 널리 활용되고 있다. 우리가 가정에서 날마다 사용하는 가전들은 디지털화 되고, 이제는 언제 어디서나 스마트 홈 IoT 서비스를 제공받을 수 있게 되었다. 스마트 홈 IoT는 디지털 시대에서 우리 삶의 질을 실질적으로 향상시킬 수 있는 방안으로 주목 받고 있다. 그러나 스마트 홈 IoT에 대한 보안은 여전히 소극적이며, 개인은 물론 기업에서도 보안에 대한 경각심을 늦추고 있는 것이 현실이다. 산업연구원의 분석에 따르면 국내 IoT 보안사고 피해는 날로 급증하고 있으며, 그 피해액은 2015년 13조 4000억원, 2020년 17조 7000억원, 2030년에는 26조 7000억원에 이를 수 있다는 연구결과가 나왔다.

스마트 홈 IoT서비스를 제공하는 기업은 서비스 개발만큼이나 그 보안유지를 위해 적극적인 투자로 보다 수준 높은 보안대책을 제시하여, 사용자에게 보다 안전한 서비스환경을 제공하여야 한다.

본 논문에서는 스마트 홈 IoT 환경에서 안정적인 서비스 제공을 위해 발생할 수 있는 각종 보안 위협을 디바이스, 네트워크, 개인정보보호 관점으로 분류 하였다. 그리고 각각에 대해 분석하고 그 대응 방안을 제시하였다. 디바이스의 취약점 대응방안으로 보안 모듈 및 시큐어 코딩 기법을 활용하고 디바이스 인증 시, 통합계정관리를 활용하여 계정 권한 및 액세스 관리 기능을 적용해야 한다. 네트워크 취약점의 대응방안으로는 디바이스간 안전한 송/수신 데이터 전달을 위한 공개키 기반구조의 데이터 암호화 적용이 필요하다. 개인정보보호적 관점에서는 비정형 및 로그를 분석하여 개인정보 노출을 탐지/모니터링하는 빅데이터 기술을 접목한

통합보안 관리체계 구축으로 대응 할 필요가 있다.

스마트 홈 IoT는 우리의 실생활, 가정에서 날마다 사용하는 만큼 태생적으로 보안에 취약하고 그 피해는 개인이 고스란이 떠안게 되는 구조이기 때문에 이제 보안은 선택이 아닌 필수적 요건이 되어야 함은 물론, 보안 사고에 대한 문제의 심각성은 더욱 부각 될 것이다.

스마트 홈 IoT는 이제 거스를 수 없는 물결이 되었다. 보안 위협을 사전에 완전히 예방하는 것은 쉽지 않겠지만, 본 논문에서 제시한 보안 요구 사항 및 대응 방안이 안전한 스마트 홈 IoT 서비스 환경 조성 및 활성화에 기여할 수 있을 것으로 기대한다.

그리고 향후 개인이 스마트 홈 서비스를 보다 안전하게 누릴 수 있도록 하기 위해서는 보안 위협에 대한 대책이 선결되어야 하며, 스마트 홈 IoT 서비스를 제공하는 기업부터가 나서서 보안에 대한 인식제고가 이루어져야 한다. 무엇보다 스마트 홈 분야의 정보보호 관리체계 수립 방안을 위한 연구가 지속되어야 할 것이다.

참 고 문 헌

[1]이영란,“IoT 로 주목받는 스마트홈 시장동향 및 업체별 사업전략”, 『 appMagazine』, 2016.05.

[2] 김호원, 김동규 (2012), “IoT 기술과 보안”, 『한국정보보호학회지』, 22(1), 7-13.

[3] 원유재 (2014). “IoT(Internet of Things) 정보보호 기술 개발 방향”, 『한국통신학회지(정보와통신)』, 32(1), 24-27.

[4] 김영관,“스마트홈 생태계 6대 구성요소”, 『DIGIECO』, 2014.11.

[5] 김선구, "IoT기술 현황과 홈 IoT기술 동향 분석을 통한 홈 IoT서비스 모델 제시”,『 전남대학교 전기전자컴퓨터공학과 전자컴퓨터공학』, 2016.8 .

[6] 김동희 외 2, “IoT 서비스를 위한 보안”, 『한국정보보호학회지』, 제30권 제8호, 2013.8 .

[7] 김재생, "사물인터넷의 기술 소개 및 정책 방안”, 『한국콘텐츠학회』, 제13권 제1호, 2015년.

[8] 박세환, 박종규, “사물인터넷의 기술 및 시장 분석을 통한 산업 활성화 방안”, 『한국기술혁신학회 학술대회』, pp.85~91, 2014.10.

[9] 표철식,“사물인터넷 기술 동향”, 『한국전자파 학회지』, 제25권 제4호, 2014년 7월.

[10] 제주대학교, “사물인터넷 기술 및 융합서비스 워크숍”, 『제주대학교』, 2014년 6월.

[11] 김영훈, 양준근, 김학범, “M2M/IoT의 동향과 보안위협”, 『한국정보보호학회지』, 제24권 6호, 2014년 12월.

[12] 박종훈, “심각한 보안 취약점으로 무방비 상태에 있는 사물인터넷”,

『정보통신산업진흥원』, 2013년 5월.

[13] 박종훈, “사이버 공격 위험성에 노출된 비무장 상태의 스마트그리드”, 『정보통신산업진흥원』, 2013년 6월.

[14] 미래창조과학부, 한국인터넷진흥원, “사물인터넷 소형 스마트 홈・가전 보안 가이드[기업용]”, 2016.12.

[15] “사물인터넷시대의 개인정보 침해요인 분석 및 실제사례 조사”, 『남서울대학교 산하협력단』, 2015.12.9.

[16] “IoT 시대, 새로운 보안 위협”, 『Biz & Tech/스페셜 리포트』, 2015.9.1 , http://skccblog.tistory.com/2450.

[17] “전 세계 CCTV 7만 3000대 누구나 본다”, 『 미디어IN호주나라』, 2014.11.10 , http://media.bojunara.com/archives/4320.

[18] “중국산 가전제품, 스마트폰 앱, 절대 사용금지!”, 『NewDaily』, 2014.02, http://www.newdail.co.kr/news/article.html?no=193744.

[19] 이명렬, 박재표, “사물인터넷 환경에서의 스마트홈 서비스 침해위협 분석 및 보안 대책 연구”, 『JIIBC』, 2016년 5월 5일.

[20] 신동헌, “무선 홈 네트워크 환경에서 보안 취약점 분석”, 2008년.

[21] 류호석, 곽진, “스마트홈에서의 보안 위협 및 보안요구사항 분석”, 『한국인터넷정보학회 학술발표대회 논문집』, 113-114.

[22] 전정훈, “사물 인터넷 보안 위협 요인들에 대한 분석”, 『한국융합보안학회』, 제15권 제7호, 2015년 12월.

[23] 한국인터넷진흥원, “IoT 디바이스 보안인증 기반 연구”, 2015년 12월.
전재홍, 박대우, “해커의 유비쿼터스 홈 네트워크 공격에 대한 정보보호 기술”, 2007년.

[24] 유양, “빅데이터 서비스에서 IP SPOOFING 공격에 대한 대응 모델 설

계”, 『경상대학교 대학원』, 2016.2.

[25] 미래창조과학부, “사물인터넷(IoT) 정보보호 로드맵”, 2014.10.31.

[26] 신영진 (2015), “IoT시대에서의 개인정보보호정책과제에 관한 연구”, 『한국행정학회 학술발표논문집』, 692-710.

[27] 나성현, “IoT 환경에서의 개인정보보호 이슈”, 『정보통신정책연구원』, 2015년 8월 13일.

[28] 박경률, “개인정보보호정책 설정 및 협상 규격을 이용한 홈 IoT 환경에서 개인정보보호에 대한 연구”, 『건국대학교』, 2016년.

[29] 호애진 기자, “LG 스마트TV 개인정보 무단수집 논란...직접 테스트 해보니”, 『데일리시큐』, http://dailysecu.com/news_view.php?article_id=5721 , 2013. 11. 21.

[30] 개인정보보호위원회, “2014년 개인정보보호 실태조사 보고서”, 2015. 04.

[31] “Internet of Things(IoT) Cyberattack”, 『Proofpoint』, January 2014,http://www.proofpoint.com/about-us/press-releases/01162014.php.

[32] “Your Fridge is Full of SPAM”, 『Proofpoint』, January 2014, http://www.proofpoint.com/threatinsight/posts/your-fridge-is-full-of-spam-part-ll-details.php.

[33] “Hacker ‘shouts abuse’ via Foscam Baby monitoring camera”, 『BBC』, August 2013, http:www.bbc.com/news/technology-23693460.

[34] Emmanuel , “Who is this man-in-the-middle”, 9.10.2015, https://techtalk.gfi.com/who-is-this-man-in-the-middle/.

국문초록

스마트 홈 IoT 서비스 환경에서의 보안위협과 정보보호 방안에 관한 연구

정보통신의 기술 발달로 사물과 인터넷의 연결을 통한 다양한 서비스가 제공되고 있다. 특히, 사물인터넷의 지속적인 발전으로 최근 보급이 확산되고 있는 스마트 홈 IoT 서비스는 가정내 스마트 디바이스들을 유/무선 네트워크로 연결하여 언제, 어디서나 보다 쉽고 편리하게 사용할 수 있도록 사용자의 편의성을 제공하고 있다. 하지만 사용자 편의성을 제공하는 대신 스마트 홈 IoT 서비스 환경은 사람과 사물간의 데이터 교환을 기반으로 하기 때문에 개인정보(이름, 생년월일, 전화번호, 주소등), 이미지, 동영상 등 사생활에 밀접한 정보를 포함하고 있어서 개인정보 침해 위험성이 높다. 또한 스마트 도어락 해킹을 통한 무단침입, 스마트 홈 컨트롤러를 해킹하여 타인의 스마트 홈 기기 오작동 및 전기 요금 과다 청구 등 파급효과가 큰 위협이 발생 할 수 있다. 이러한 스마트 홈 침해 사고는 금전적, 물리적, 정신적인 피해를 유발하기 때문에 보안위협에 대한 정보보호 방안 대응이 중요하다.

따라서 본 논문에서는 스마트 홈 IoT 서비스 환경에서 발생한 보안침해 사례를 검토하였으며, 스마트 홈 IoT 서비스가 가지는 보안 위협을 크게 3가지(디바이스, 네트워크, 개인정보관련 보안 위협)로 나누어 도출하고 대응 방안을 제시하고자 하였다.

주제어: 사물인터넷(Internet of Things), 스마트 홈, 보안 위협, 정보보호 방안