The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 16, No. 5, pp.27-32, Oct. 31, 2016. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2016.16.5.27
JIIBC 2016-5-5

사물인터넷 환경에서의 스마트홈 서비스 침해위협 분석 및 보안 대책 연구

Analysis and Study on Invasion Threat and Security Measures for Smart Home Services in IoT Environment

이명렬*, 박재표**

Myongyeal Lee*, Jaepyo Park**

요 약 IoT(Internet of Things)는 인터넷을 기반으로 모든 사물을 연결하여 사람과 사물, 사물과 사물, 사물과 시스템 간의 정보를 상호 소통하는 지능형 기술 및 서비스 등을 지칭 한다. 이러한 IoT 환경에서의 스마트 홈은 개인주거에 필요한 일상용품/기기에 사물인터넷을 융합하는 것으로 개인의 생활 영역 대부분이 포함되는 융합 사업이라고 할 수 있다. 개인 생활과 가장 밀접한 가정내에서 구현되고 있는 스마트홈 서비스는 다양한 형태로 개발되고 발전하고 있다. 이러한 발전은 긍정적인 효과를 발휘하기도 하지만 보안 문제가 해결되지 않는다면 스마트홈 서비스는 개인 생활의 큰 재앙을 유발할 수 있다. 현재는 스마트홈 서비스 초기 단계이지만 서비스가 발전 할수록 수집하는 개인정보는 증가하게 되며, 이로 인한 빅브라더 등장 우려도 제기되고 있다. 또한 서비스 이상 및 정보의 유출에 따른 다양한 보안 위협이 존재하며 이에 대한 대응책 마련이 요구되고 있다. 이에, 본 논문에서는 IoT 환경에서의 스마트홈 서비스 형태를 알아보고, 스마트홈 서비스가 가지는 보안 위협을 도출하고 대응 방안을 살펴보고자 한다.

Abstract In general, IoT(Internet of things) designate the intelligence technologies and services which interact all necessity information between human and things, things and thing and things and systems with all things connecting through the internet based. The smart home in present of IoT environment fuses the daily supplies/equipment which needs to use for the private life with the internet of things that is the fruit of the converged business through all most private consumption related in vastly. The concept of smart home has been built around early 2000s due to the spread of high speed internet and advanced of smart electronics and internet, furthermore influencing by the enhancement of wireless network and smart devices, it is advanced as a smart home within the internet of things environment. Smart home service inside the house which most closely implemented with personal life is being developed and advanced in various forms. These developments may exert a positive effect, but if it does not resolve the security issues for the smart home service, then it may cause a big plague of privacy and personal life.

Key Words : New convergence service, IoT, Smart Home, Home networking

Ⅰ. 서 론

스마트홈(Smart Home)은 가정 내 기기들을 네트워크로 연동해 모바일 단말이나 PC등을 통해 원격으로 모니터링, 제어 및 동작하는 제품, 서비스, 솔루션 등을 총칭한다. 예를 들어 스마트 홈 서비스가 적용된 가정에서는

*정회원, 숭실대학교 대학원 컴퓨터학과(교신저자)
**정회원, 숭실대학교 정보과학대학원
접수일자 : 2016년 8월 19일, 수정완료 : 2016년 9월 19일
게재확정일자 : 2016년 10월 7일

Received: 19 August, 2016 / Revised: 19 September, 2016 / Accepted: 7 October, 2016
*Corresponding Author: biggale@gmail.com
Dept Computer of Graduate School in Soongsil Univ., Korea

TV, 에어컨, 냉장고 등의 가전제품이나 수도, 전기, 냉난방 등의 에너지 소비 장치, 도어락 등 보안기기 등 가정 내 기기들을 하나의 네트워크로 연결하여 시간과 공간에 구애 받지 않고 모니터링, 제어 및 작동 할 수 있다. 이처럼 스마트 홈 기술 및 서비스가 적용된 홈 네트워크는 스마트폰과 같은 기능형 정보생활 기기가 네트워크를 통해 연결되어 사람과 자연스러운 상호작용으로 인간 중심의 서비스 환경에서 유익한 서비스를 제공함으로써 삶의 질을 향상시키고 보다 스마트한 가정 환경을 누릴 수 있게 끔 돕는다. 스마트홈 서비스 또는 솔루션을 구성하기 위해서는 스마트폰, 태블릿, 스마트 TV 등 각각의 디지털 정보 단말기끼리 동일한 인터페이스를 통해 가정 내 기기들의 정보를 확인 및 조작할 수 있는 환경이 우선적으로 구현되어야 한다. 따라서 모바일 단말을 비롯한 디지털 정보 기기, 유무선 통신망들의 적절한 배치 및 활용과 조작 편의성이 높은 어플리케이션이 필요하다. 이를 구현하기 위해 스마트 홈은 생활 전자기기의 접속을 위한 유무선 홈네트워크, 기존 가전제품에 스마트 기능을 추가한 스마트 가전, 컨트롤러와 센서를 통해 스마트홈 사용자와 직접 연관된 기능을 구현하는 센서 및 디바이스, 센서 및 디바이스를 제어하고 관리 가능한 유무선 제어 관리 단말기 등으로 구성된다. 그림1은 스마트홈 서비스의 일반적인 구성이다. 위와 같이 다양한 요소 기술의 구현을 통해 구축되는 스마트홈 환경은 다양한 보안위험을 가지고 있으며, 이에 대한 해결 방안을 요구하고 있다.

그림 1. 스마트홈 서비스의 구성
Fig. 1. Smart Home Service

II. 국내 스마트홈 시장 동향

국내 스마트홈 시장은 2000년대 중후반 부동산 경기 호황에 힘입어 홈오토에이션 중심의 홈네트워크 시장이 건설사들의 적극적인 관심과 참여로 활성화 가능성이 기대되었으나 표준화, 유지보수, 킬러 어플리케이션의 부재 등으로 인해 주류시장 진입에 실패함으로써 이른바 캐즘 현상 (Chasm)이 나타났다. 이에 시장 성장의 부진으로 대기업은 스마트 홈 산업에 투자를 축소하였고, 사정이 좋았던 홈오토메이션 관련 중소 업체들도 이후 부동산 경기침체로 신규 주택공급이 감소함에 따라 출혈경쟁으로 경쟁력이 갈수록 약화되고 있다. 그마나 글로벌 경쟁력을 갖춘 가전사들이 스마트폰에 이어 스마트 TV에서도 세계시장을 확대해 나가고, 백색가전 분야에서도 스마트 융합가전 제품들을 출시하고 있으며, 통신사업자들도 IP-TV 셋탑박스, 스마트 홈 폰을 속속 출시하면서 스마트홈 분야가 다시 서비스 시장으로서의 가능성을 검증해볼 기회가 엿보이고 있다. 이렇게 시작된 국내 스마트홈 시장은 스마트TV, 스마트가전, 홈 네트워크를 중심으로 연평균 35.5%의 초고속 성장이 예상되며, 가전, 건설, 의료 등 전통 산업의 부가가치를 더해주어 세계시장 경쟁력 상승 및 시장점유확대 기회를 제공한다. 또한 가전시장은 네트워크화된 스마트 가전 중심으로 진화, 2007년 전체 가전시장의 10.4%의 비중을 차지하던 스마트 가전은 2013년 37.8%로 빠른 속도로 진화 혹은 대체되고 있다.[1]

시장조사기관 ABI리서치는 '글로벌 스마트 홈 네트워크 시스템' 시장은 M2M 기술을 기반으로 2017년에는 현재 보다 60% 가량 성장할 것으로 전망하고 있고 한국 전자 통신 연구소(ETRI)는 국내 스마트 홈 관련 시장이 2012년 약 1조500억원에서 2015년 7조원 규모까지 7배 가량 성장할 것으로 전망하고 있다. 그 외에도 국내 스마트 홈의 성장이 기대되고 있는데, 주요 요인은 먼저 인구 구조의 변화에 있다. 우리나라는 이미 인구 구조상 고령화 사회이며, 세계 최단기로 고령/초고령 사회로 진입이 예상되고 있다. 2000년 7.2%로 고령화 사회에 진입하였으며 2010년 12월 (통계청) 11.3%로 노인인구가 542만명이 되었다. 앞으로 2018년에는 15%가 넘을 것이며, 2026년에 20.8%로 초고령 사회로 진입할 것으로 예상된다.[4-6] 스마트 홈은 고령 친화적 산업으로서, 고령 및 장애우의 삶의 질 개선에 반드시 필요한 산업으로 발전될 것이다. 다른 요인으로는 스마트화의 급진전으로 스마트 홈 서비스 확산이 가시화되고 있다는 것이다. 스마트폰 및 패드에 이어 스마트TV의 활성화와 스마트융합가전에 이르기까지 그동안 그려왔던 스마트 홈의 모습들이 가시화되고 있는 것이다. 이를 잘 연결하고 조합하여 효과적인 서비스를 만들어 나가는 것이 중요할 것이다.[3]

표 1. 스마트홈 추진전략
Table 1. Smart Home Strategy

사업자 종류	현상황	전망
통신 사업자	유무선망 가치 제고를 위한 서비스 개발 - 스마트홈 디바이스 간 콘텐츠 공유 및 제어 - N-Screen 서비스 디바이스간 협업 - 스마트기기를 활용한 홈시큐리티 서비스	통신사간 경쟁 치열 - 자사 서비스 기반 이용 가입자 확대 목적
보안 사업자	스마트 디바이스 기반 홈 시큐리티 서비스 경쟁 - ICT 기술을 활용한 실시간 알림 및 양방향 서비스 - 사용자별 유사 서비스 일부 차별화	B2C 시장에서 통신사 협력 - B2C 시장의 마케팅 노하우와 서비스 인프라에 필수적인 통신사와 협력 추구
제조사	가전 기기의 스마트화를 통한 스마트홈 추구 - 가전 기기간 통신 규격 마련, 스마트 디바이스 활용, 스마트 기기 및 저장매체의 콘텐츠 관리 및 공유 - '홈싱크'와 같은 홈허브 기기 개발	통신사와 서비스 주도 경쟁 - 스마트폰 보급으로 인해 앱 형태로 서비스 제공

Ⅲ. 스마트홈 정보보호 위협 및 대응 방안

1. 스마트홈 정보보안 위협

스마트홈 서비스는 생활의 편리함, 생활 수준 향상 등 긍정적인 효과가 발생하지만, 보안 문제가 해결되지 않으면 스마트홈은 재앙이 될 수 도 있다. 아직은 스마트홈이 초기 단계지만 서비스가 고도화 될수록 스마트홈이 수집하는 개인정보는 더 늘어날 수밖에 없기 때문에 사생활 정보 데이터로 인하 '빅브라더' 등장 우려가 제기된다. 정해진 시간에 자동으로 개인맞춤형 서비스를 제공하려면 사용자 이용 정보를 저장/분석한 되 패턴화하는 과정이 필수이기 때문이다. 서비스가 발전하고 편리해질수록 보안 위협에는 취약해지는 셈이다. 개인정보와 관련하여 센서, CCTV 등 현재 스마트홈 관련 단말기는 기껏해야 비밀번호 정도의 낮은 보안 수준만 적용된 것이 대부분이어서 해킹 공격에 취약하다, 스마트홈의 보안은 스마트폰, 스마트 TV 등으로 대표되는 '스마트' 단말 보안과 사용자 인증, 다양한 형태로 제공되는 서비스로 나누어 볼 수 있으며, 스마트 홈에서 발생할 수 있는 위협 및 위험은 표2와 같이 다양하다.[2]

표 2. 스마트홈 정보보안 위협
Table 2. Smart Home Security Threats

구분	내용
도청 및 정보 유출	- 센서의 정보를 불법적인 접근을 통해 알아내는 공격 - 센서 및 게이트웨이 간의 통신에서 스니핑을 통해 데이터 유출 - CCTV 전송 내역 스니핑을 통해 유출
개인정보 침해	- 스마트홈 기기에 저장되어 있는 정보를 읽어 사용자의 성향, 성격 등의 사용자의 개인 신상정보 분석 - CCTV 정보 유출로 인한 개인 사생활 침해
데이터 위/변조	- 센서 및 게이트웨이 통신 간 제어 데이터를 무단으로 위변조 전송하는 공격 - 댁내 가스밸브, 도어락 등 자동 제어기기에 불법적인 행위를 유발하는 공격
위장 공격	- 사용자의 신원 식별을 위한 인증정보가 저장되어 있는 기기에 무단 접근 후 해당 정보를 복제 후 해당 시스템에서 사용자인 것처럼 위장하여 공격
서비스 거부 공격	- 센서와 게이트웨이 등의 통신을 방해하기 위하여 게이트웨이에 무의미한 정보를 지속적으로 전송하여 정당한 통신을 방해하는 공격
물리적 공격	- 스마트기기의 정보를 알아내기 위하여 내장된 메모리를 전력 분석 기법 등 물리적인 공격기법을 통해 알아내는 공격
퍼징 (Fuzzing) 공격	- 스마트홈 기기 및 시스템이 가지고 있는 유효 범위에 대한 공격으로 시스템의 물리적인 범위를 축소 또는 확대시켜 오류를 일으키는 공격 - 스마트홈 기기 및 시스템에 전송되지 말아야할 데이터를 전송시켜 오류를 발생시키는 공격

2. 스마트홈 위협 시나리오

스마트홈 서비스 제공 환경에서 발생할 수 있는 보안 위협에 대한 시나리오를 표 3과 같이 정의할 수 있다.

표 3. 스마트홈 위협 시나리오
Table 3. Smart Home Security Threats Scenario

시나리오	상세 내용
가정용 CCTV 유출을 통한 개인정보침해	- 댁내 CCTV와 게이트웨이 통신 구간에 스니핑을 통하여 CCTV 전송화면이 유출될 수 있으며, 이를 통해 심각한 개인 사생활 정보 침해 문제가 발생함
콘트롤러 해킹을 통한 불법적인 현관문 개폐	- 현관문을 제어하는 콘트롤러 불법 침투를 통해 임의적으로 현관문을 열고 닫을 수 있는 제어권을 획득할 수 있음. 이로 인하여 다양한 범죄에 사용될 수 있음.
콘트롤러 해킹을 통한 댁내 가스밸브 원격 개방	- 현관문을 제어하는 콘트롤러 불법 침투를 통해 임의적으로 현관문을 열고 닫을 수 있는 제어권을 획득할 수 있음. 이로 인하여 다양한 범죄에 사용될 수 있음.
서비스 거부 공격을 통한 댁내 스마트홈 기기 오동작	- 스마트홈 게이트웨이 또는 컨트롤러에 다량의 패킷전송을 통해 댁내 스마트홈 기기의 오동작을 일으킬 수 있음.
패킷 재사용 공격을 통한 비인가자 센서 제어	- 스마트홈 게이트웨이 또는 컨트롤러에서 발생하는 무선 전송 패킷을 도청 및 발생시켜 스마트홈 기기의 제어가 가능할 수 있음.

1) 가정용 CCTV 유출을 통한 개인정보침해

실제 스마트홈 사용자는 다음과 같이 PC 및 스마트폰을 통해 자신의 집 CCTV로 거실을 모니터링 하고 있다. 스마트홈 CCTV의 구성은 IP카메라로 구성되어 있으며, 데이터 통신은 대중적으로 많이 사용되는 WIFI로 구성되어 있다. 이때 WIFI의 무선 AP의 보안관리(인증, 암호화)가 미흡할 경우 CCTV를 통한 개인정보 침해발생이 가능하다.

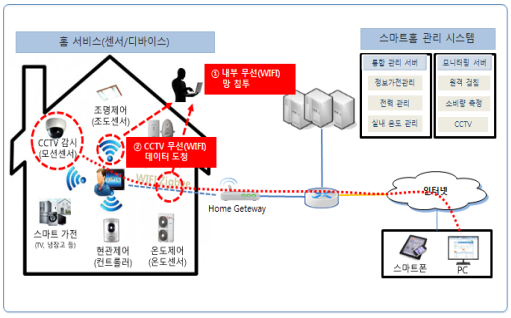

그림 1. 위협 시나리오#1
Fig. 1. Threats Scenario#1

① 공격자는 도청 대상의 CCTV가 설치되어 있는 가정의 주변에서 WIFI 해킹을 통해 댁내 WIFI망에 접근한다.

② 접근된 내부 WIFI 망에서 모니터링 모드를 통한 CCTV 통신 RAW를 확보하여 재조립을 통한 동영상 도청을 수행한다. 이를 통해 공격자는 집안 내부 상황 모니터링 및 개인 사생활 침해 공격을 수행할 수 있다.

2) 콘트롤러 해킹을 통한 불법적인 현관문 개폐

내/외부에 스마트홈 관리 서버를 두고 현관제어를 수행하는 스마트홈 서비스 사용 시 현관문 제어의 경우 스마트홈 관리 시스템의 웹 서비스를 통해 제공되며, LOGIN을 통한 인증을 수행한다. 이때 웹 서버의 인증 시스템에 취약점이 존재할 경우 이를 통한 타 가정의 현관문 제어가 가능하다.

① 공격자는 웹 인증우회 취약점을 통해 현관문 제어 페이지에 접근할 수 있는 권한을 획득한다.

② 현관문 제어 페이지에서 공격자는 현관문을 OPEN 하는 명령을 입력한다.

③~④ 현관문이 열리고, 공격자는 이를 통해 집안 내부로 무단 침입하여, 금품탈취 등의 여러 가지 범죄 행위를 한다.

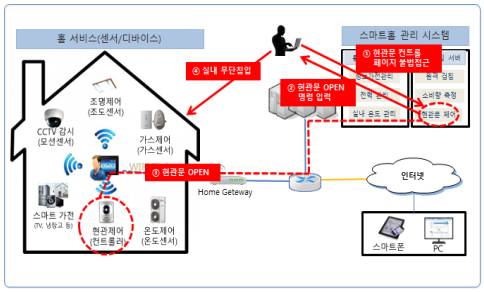

그림 2. 위협 시나리오#2
Fig. 2. Threats Scenario#2

3) 콘트롤러 해킹을 통한 댁내 가스밸브 원격 개방

내/외부에 스마트홈 관리 서버를 두고 가스벨브 제어를 수행하는 스마트홈 서비스 사용 시 가스벨브 제어는 스마트홈 관리 시스템의 웹 서비스를 통해 제공되며, LOGIN을 통한 인증을 수행한다. 이때 웹 서버의 인증(LOGIN) 기능 및 비밀번호가 취약할 경우 이를 통한 타 가정의 가스밸브 제어가 가능하다.

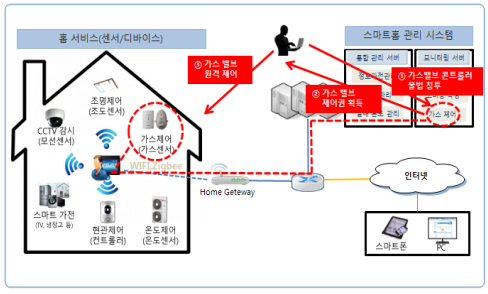

그림 3. 위협 시나리오#3
Fig. 3. Threats Scenario#3

① 공격자는 비밀번호 크랙을 통해 스마트홈 관리 시스템의 가스제어 컨트롤러 페이지에 접근한다.

② 공격자는 침투한 컨트롤러에서 가스밸브를 열고 닫을 수 있는 제어권을 획득한다.

③ 공격자는 원격으로 가스 밸브를 제어 할 수 있다.

4) 서비스 거부 공격을 통한 댁내 스마트홈 기기 오동작

내/외부에 스마트홈 관리 서버를 두고 댁내 센서의 통신은 무선(Bluetooth, WIFI, Zigbee 등)으로 이루어진 스

마트홈 서비스가 구성되어 있다. 이때 서비스거부공격에 대한 설계가 이루어지지 않을 경우, 서비스 거부공격으로 인한 기기의 오작동이 유발될 수 있다.

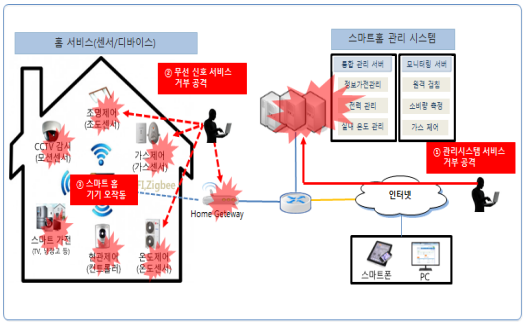

그림 4. 위협 시나리오#4
Fig. 4. Threats Scenario#4

① 공격자는 스마트홈 관리시스템에 대한 서비스 거부공격을 통해 스마트홈 서비스가 제대로 이루어지지 않도록 할 수 있다.
② 공격자는 각 센서에 대한 무선신호 Jamming 등을 통해 방해 전파 등을 발생시켜 정상적인 센서 통신이 이루어질 수 없도록 할 수 있다.
③ '①~②'과정을 통해 스마트홈 서비스의 오동작을 유발할 수 있다.

5) 패킷 재사용 공격을 통한 비인가자 센서 제어

각 센서 통신이 무선신호(WIFI, Bluetooth, Zigbee 등)으로 이루어져 있다. 각 센서는 무선으로 전송되는 데이터에 대한 무결성 검증이 이루어지지 않아 해당 위협이 발생한다.

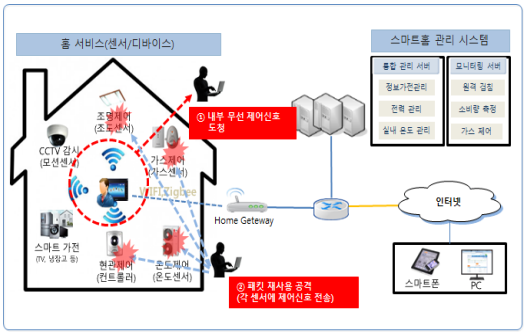

그림 5. 위협 시나리오#5
Fig. 5. Threats Scenario#5

① 공격자는 무선으로 이루어진 센서 통신 데이터를 외부에서 도청하여 각 센서의 제어 신호를 확보한다.
② 확보한 센서 제어 신호를 패킷생성 툴 등을 활용하여 재생산 및 전송하여, 각 센서의 제어를 수행한다.

표 4. 보안 위협 및 대응방안
Table 4. Security Threats and Countermeasures

위협	공격	대응방안		관련 기술
물리적 위협	스마트기기의 하드웨어 해킹을 통한 정보 유출	인증	센서 및 사용자에 대한 인증 제공	기기인증, 사용자 인증
	센서 및 게이트웨이간 통신 도청	암호화	통신 데이터에 대한 암호화 제공	AES, DES, IDEA
	CCTV 전송 데이터 도청 및 복원	암호화	CCTV 통신 구간 암호화	무선통신 암호화
개인정보 침해	스마트홈 기기에 저장된 개인 성향, 성격 등의 정보 노출	암호화	사용자 정보에 데이터 암호화 제공	공개기 기반 암호화
	CCTV 정보 유출 (무단 접근 등)	인증	CCTV 접근 사용자에 대한 인증 제공	IP 접근통제 ID 기반 접근통제
		암호화	CCTV 통신 구간 암호화	AES, DES, IDEA
데이터 위/변조	센서 및 게이트웨이 통신 제어 데이터 변조	무결성	각 센서 및 게이트웨이 장비 통신 시 무결성 제공	AES, MD5
위장공격	위조된 사용자 식별 정보를 통한 인증	무결성	사용자 식별 시 위조 확인 및 무결성 검증 절차 제공	기기인증 사용자 인증
서비스 거부	센서와 게이트웨이 통신방해 유/무선 데이터 전송	인증	센서 및 게이트웨이 통신 시 인증된 기기 및 사용자만이 사용할 수 있는 인증 제공	기기인증 사용자 인증
물리적 위협	스마트기기의 하드웨어 해킹을 통한 정보 유출	암호화	데이터 암호화를 통한 메모리 추출에 의한 데이터 노출 방지	공개기 기반의 암호화
기능제거		기능 제거	하드웨어에 존재하는 JTAG, UART 등의 인터페이스 제거	JTAG, UART, 펌웨어 해킹

Ⅳ. 결 론

IoT 기반 스마트홈은 센서, 네트워크 구간, 스마트 단말 등 3개 부문에 대한 보호대책을 수립하여야 한다. 센서 부문에서는 기기인증, 사용자 인증을 통해 센서 불법 접근 및 위장공격에 대응 할 수 있으며, 데이터 암호화 및 통신구간 암호화를 통하여 네트워크 구간의 도청 및 정보유출에 대응할 수 있다. 스마트 단말 부문은 암호화 및 불필요한 접근 기능 제거 등을 통하여 정보 유출에 대응할 수 있다. 위 표 4는 스마트홈 환경의 보안 위협 별 대응방안 및 관련 기술을 정의하고 있다.

사물인터넷은 인터넷에 연결된 사물에 대한 정보의 통합 및 가공을 통해 스마트홈 환경을 구성하고 다양한 서비스를 제공한다. 이를 위해 다양한 요소기술의 통합 및 연계가 필요하며, 이로 인해 다양한 정보보안 문제가 발생할 가능성을 가지고 있다. 이에 본 논문에서는 IoT 기반 스마트홈의 보안 위협을 분석하고 이에 대한 보안 대책을 제시한다. 이러한 보안 대책을 통해 스마트홈 서비스의 안정적 보급과 활성화에 기여할 수 있을 것이다.

References

[1] Kim Young Kwan, "Smart Home (Home IOT) ecosystems six components", *Digieco*, 2014.11

[2] Kim Howon, "IoT technology and security", *Information Security Journal*, vol.22, no.1, 2012

[3] Park Su Hong, "Mobile IPTV technology and national and international standardization trends", HN Focus Vol20, 2010

[4] Park Jongyoul, Moon Jinyoung, Paik EuiHyun "Module based Security system for a Convergence IPTV Service", Korea Institute of Information Technology, 2010

[5] Kim Moongu, Park Jonghyeon, "Smart TV national and international trends and development directions", TTA Journal, No.131, 2010

[6] Wi Yukyeong, Kwak Jin, "Analysis of Smart TV Trends and Security Vulnerabilities to Use in the Smartwork", Korea Multimedia Society, 2012

[7] Kee-Hyun Choi, Kyung-Soo Jang, Ho-JinShin, "Smart Home Environment for the Protection of Multimedia Digital Contents," The Journal of The Institute of Internet, Broadcasting and Communication (JIIBC), VOL. 11 No. 2, pp. 189-196, 2011.

[8] Minzheong Song, "A Study on Business Types of IoT-based Smarthome: Based on the Theory of PlatformTypology," The Journal of The Institute of Internet, Broadcasting and Communication(JIIBC), VOL. 16 No. 2, pp. 27-40, 2016.

[9] Nak-Hyun Kim, Keun-Wang Lee, Mun-Seog Jun, "A Design of Protocol for Protection of Privacy Using Temporary ID in u-health Environment based on ZigBee," Journal of the Korea Academia-Industrial cooperation Society(JKAIS), Vol. 29, No. 2, pp. 447-480, 2012.

저자 소개

이 명 렬(정회원)

- 2011년 2월 : 숭실대학교 정보과학대학원 정보보안학과 (공학석사)
- 2012년 3월 ~ 현재 : 숭실대학교대학원 컴퓨터학과 박사과정

<주관심 분야 : 정보보호 정책 및 전략, IoT, 디지털포렌식>

박 재 표(정회원)

- 1998년 8월 : 숭실대학교 대학원 컴퓨터학과 (공학석사)
- 2004년 8월 : 숭실대학교 대학원 컴퓨터학과 (공학박사)
- 2010년 3월 ~ 현재 : 숭실대학교 정보과학대학원 교수

<주관심 분야 : 네트워크 보안, 디지털포렌식, 금융IT>