스마트 홈 IoT 보안 기술 연구 동향 및 고찰

이영헌, 조정훈, 박종혁
서울과학기술대학교 컴퓨터공학과
e-mail : {movestos, jojeong3766, jhpark1}@seoultech.ac.kr

Research Trends and Considerations of Security Technology of Smart Home IoT

Young Hun Lee, Jo Jeong Hoon, Jong Hyuk Park
Department of Computer Science and Engineering, Seoul National University Of Science and Technology

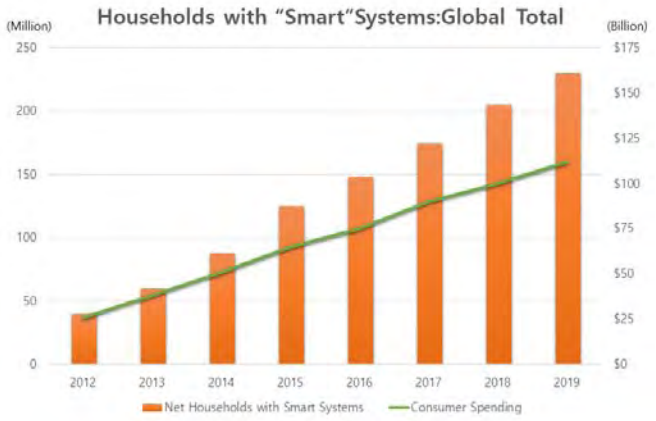
요 약

최근 ICT(Information Communications Technologies)의 발전과 센서 제조 공정의 발전을 통해 저용량, 경량 디바이스를 이용한 스마트 홈 시장이 성장하고 있다. 특히 스마트 홈 IoT의 환경은 모든 사물을 인터넷으로 연결하고 상호 통신을 통해 다양하고 많은 양의 정보를 수집하여 일상생활을 편리하게 해주는 IoT(Internet of Things)가 계속 증가하고 있다. 하지만, 이러한 증가량과 함께, 스마트 홈 환경에서 대한 기술표준화가 이루어지지 않았으며 원활한 서비스 제공 뿐만 아니라 보안 문제가 발생하고 있다. 특히, 이기종 네트워크, 디바이스를 사용하는 스마트 홈 IoT의 경우 다양한 인증 방법이 존재하며, 이에 따른 취약점이 발생하게 된다. 보안 취약점을 이용한 공격으로 개인정보 유출이나 경제적 손실 등 피해를 발생시키고 있으며, 추후 인명피해까지 발생할 수 있다.

따라서, 본 논문에서는 스마트홈 환경의 IoT 보안 방안에 대해 알아보고, 관련 보안사고의 사례 및 인증 기술을 살펴봄으로써 미래 스마트 홈 IoT 보안 기술의 발전과 적합한 보안 대책과 보안 취약점에 대한 보안 체계를 마련하는 것에 도움이 될 것이다.

1. 서론

현재 통신 기술의 발전과 스마트 디바이스, 센서 제조 기술의 발달로 다양한 스마트 디바이스 종류가 기하급수적으로 증가하고 있다. 이러한 스마트 디바이스를 통한 서비스의 영역이 확장되어, 전 세계 스마트 홈 시장이 급격하게 성장하고 있다. 시장 조사 기관 Strategy Analytic에 따르면 480억 달러로 조사되었고 연간 평균 19%씩 성장하여 2019년에는 1,150억 달러의 시장 규모를 이를 것으로 예상하고 있다[1].



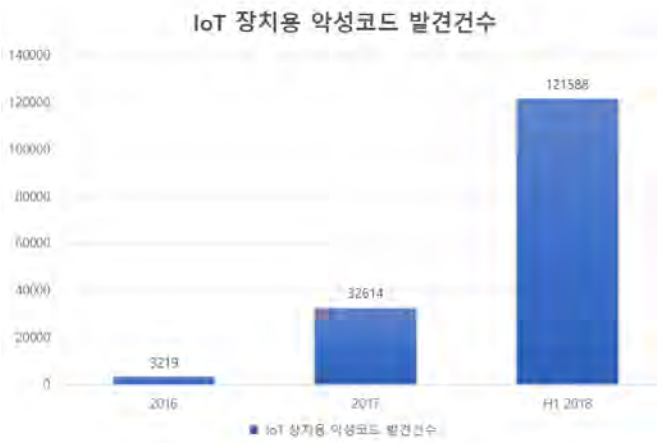
(그림 1) 스마트홈 시장 전망치

또한, 국내 스마트 홈 시장의 경우 2025년까지 연 평균 9.5%에 이르는 고성장이 예상되며 2025년 시장 규모는 31조원에 이를 것으로 예측했다[2]. 지속적인 스마트 홈 시장의 성장과 함께 IoT(Internet of Things), 센서, 음성인식 기술 등이 융합되어, 거주자에게 편리한 서비스를 제공하는 디바이스 환경이 구축되고 있다[3].

스마트 홈을 구성하기 위해 사용되는 IoT는 사물들이 인터넷을 통하여 사물과 사람, 사물간 데이터 통신 및 교환을 통해 상호 작용하는 기술 및 서비스를 의미한다. 스마트 홈의 IoT 환경에서는 거주자에게 지능형 서비스 제공을 위해 다양하고 많은 양의 디바이스 데이터를 수집하며, 언제 어디서나 지속적으로 서비스가 제공되어야 하는 특징을 가진다[4][5]. 하지만 스마트 홈 IoT 기술 특성상 다양한 보안 위협에 노출될 수 있는 단점이 존재한다. 특히, 제한된 전력량과 계산능력, 메모리 등의 하드웨어 사양을 가지며 항상 유/무선으로 연결되고 이기종 네트워크, 디바이스 플랫폼으로 구성되어 다양한 보안 위협 취약점 존재 가능성이 있다. 이러한 보안 위협은 스마트 홈 플랫폼 운영에 오류를 일으키거나 거주자에게 잘못된 서비스를 제공하게 되어 스마트 홈 플랫폼이 자체적으로 기능을 상실할 수 있다.

스마트 홈 내부 IoT기기가 증가되면서 외부의 사이버 공

격에 노출될 가능성이 높아지고 공격방법이 다양화되고 있다. IoT에 대한 취약점 공격에 대한 증가추세는 미국 카스퍼스키랩에서 발표한 IoT보고서 (그림 2)에서 보여준다[6]. 2016년 3,219건에 불가하던 취약점의 개수는 2017년 32,614건으로 크게 증가했고, 2018년 상반기 121,588건 까지 증가하여 앞으로 더 많은 보안 취약점이 발견될 것으로 예측된다.



(그림 2) IoT 장치용 악성코드 발견건수

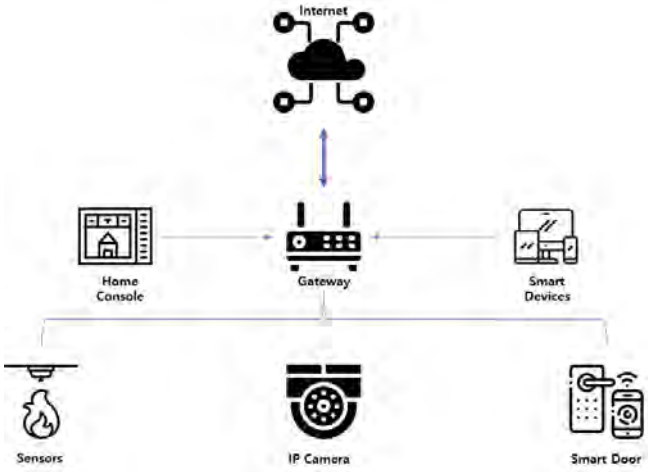
현재 스마트 홈 IoT 환경은 서비스를 위해 다양한 이기종 홈 디바이스 제어와 네트워크 환경을 가지고 있으며 발생할 수 있는 보안 취약점을 해결하기 위해 많은 연구와 다양한 인증 표준화가 진행되고 있다. 하지만 현재까지 제안되어져 오고 있는 다양한 통신과 보안 프로토콜들은 취약점과 여러 공격들에 의해 개인정보를 침해 문제들이 발견되고 있다[7][8]. 본 논문에서는 스마트 홈 관련 보안 기술 동향 및 보안 요구사항을 알아본다.

2. 스마트 홈 IoT 네트워크 환경 및 시스템 구성

스마트 홈 IoT 네트워크 구성은 사물과 인간, 사물과 사물 등 서비스를 하기 위해 분산되어 있는 환경 요소들을 서로 연결시킬 수 있는 유무선 네트워킹으로 되어 있으며, 무선 네트워크를 중심으로 발전하고 있다.

다양한 IoT간 연결이 요구되므로 여러 네트워크 기술이 사용되고 있다. 인터넷 연결 기반인 WIFI, 3G/4G/LTE 등을 통해 데이터를 주고받는 IP 기반 프로토콜 기능이 사용되며, IP를 사용하지 않는 Bluetooth, ZigBee 등의 통신 프로토콜을 사용하는 IoT의 경우는 주변 노드와 연결하여 데이터를 통신할 수 있다.

스마트 홈 시스템은 사용자가 장소와 시간에 구애 받지 않고 스마트 홈 네트워크 내의 IoT 기기들의 정보 조회와 제어할 수 있는 기능을 제공 한다. 이를 위해, 홈 IoT 제어를 위해 다양한 네트워크 기술과 하드웨어를 이용한 시스템이 구성되고 있으며 대표적으로 게이트웨이, 클라우드, Hybrid로 구성된 시스템으로 구분할 수 있다. 게이트웨이 방식은 홈 네트워크에 연결된 가전, 센서, IoT 등 스마트 기기에 대한 데이터를 중앙 홈 게이트웨이 한곳에 수신하고 이를 스마트 홈 플랫폼에 전송하여 사용자가 외부에서도 스마트 홈의 IoT 제어 및 서비스를 제공 수 있도록 한다. 기존 홈 네트워크에서 각각 다르게 구성된 인터페이스와 제약조건을 가지고 있을 경우, 독립적인 모니터링 또는 제어만 가능할 수 있는 단점이 있다. IoT 홈 클라우드 시스템은 각각의 클라우드에 맞는 인터페이스를 구성하고 이를 스마트홈 플랫폼을 통해 단일화 하여 서비스를 구성하여 다양한 종류의 홈 IoT 및 센서, 모듈이 협업하여 사용자에게 서비스를 제공할 수 있는 구성이 가능하다. 앞서 기술한 게이트웨이와 클라우드 하이브리드 스마트 홈 시스템을 결합한 하이브리드 시스템은 모니터링과 제어는 게이트웨이를 활용하고, 세분화된 제어가 필요할 경우 IoT 클라우드를 이용할 수 있도록 구성하고 있다.



(그림 3) 스마트홈 IoT 시스템 구조

3. 스마트홈 IoT 보안사고 사례 및 공격 종류

현재 지속적으로 스마트 홈 환경에서 IoT의 취약점을 통한 다양한 보안 사고가 발생하고 그 양은 증가하고 있다. 다양한 종단간 IoT 기기들의 하드웨어적 취약점, 이기종 네트워크 연결 구성으로 인한 취약점, 보안되지 않은 게이트웨이 및 클라우드를 통한 공격 방법들을 통해 다양한 보안 사고를 발생 시킬 수 있다. 이러한 취약점들은 스마트 홈 환경으로 해킹 프로그램, 악성코드 등이 유입 될 수 있으며, 도청과 변조 하여 이를 외부의 공격자에게 전송하는 것이 가능하다. 실제로 IoT와 관련된 디바이스, 센서 등 디바이스 내부에 스파이 마이크로 칩이 발견되기도 하였으며, 확인되지 않은 수량은 훨씬 더 많을 것이다. 또한, 사용자가 자주 사용하는 IoT를 이용하여 스마트 홈 네트워크상에 존재하는 디바이스들이 악성코드에 의해 감염되어 DDOS(Distributed Denial of Service) 공격이나 개인정보유출 등에 악용 될 가능성 또한 존재한다[9][10]. 또한, 미국 보안업체인 Proofpoint사에 2013년 말에서 2014년 초까지 전 세계 스마트 홈 네트워크 환경의 IoT와 라우터 등에 의해 약 75만 건의 스팸, 악성코드, 피싱 등이

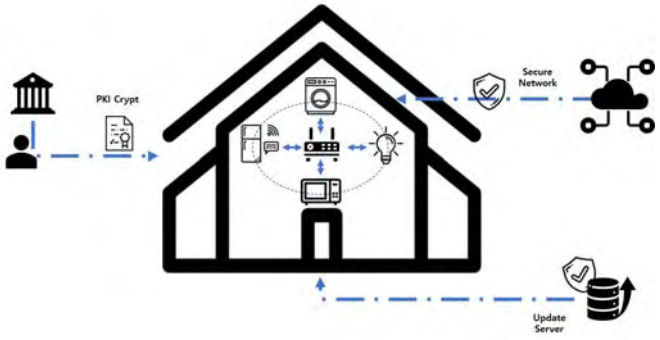
발생 하였다. 이는 스마트 홈 외부 공격자들이 네트워크상에 연결된 스마트 홈의 IoT 등을 해킹하여 메일이나 메시지 송신 기능 등을 통해 악성 프로그램이나 스팸 내용을 포함된 메일이 보내지기도 하였다. 이렇듯 현재 스마트 홈 네트워크 환경이 발전함에 따라, 취약점을 통해 다양한 사이버 공격이 발생하고 있다[11].

<표 1> 국내외 스마트홈 IoT 보안관련 이슈

연도	국가	내용	연구기관
2013	독일	Smart TV 해킹 프로젝트	Amsterdam Univ.
2014	터키	냉장고 해킹을 통한 스팸메일 75만 건 발송 사례 발견	ProofPoint
2014	한국	냉장고 내부 셋톱박스 해킹에 의한 게임사 DDoS 공격 사례 발견	KISA
2014	한국	공유기의 취약점을 통해 통신사 DNS를 DDoS 공격	미래창조과학부
2014	중국	유아용 CCTV 자체 소프트웨어 결함으로 약 700여개의 CCTV에서 촬영 중인 실시간 영상링크 유포	정보통신기술진흥센터
2016	미국	Telnet, SSH 포트가 오픈되어 있는 IoT 디바이스에 Brute Force를 통해 접근	-
2017	독일	인터넷에 노출된 프린터를 대상으로 IPP(Internet Printing Protocol) 포트와 LDP(Line Printer Daemon) 등을 통해 경고문 출력	Ruhr-Universität Bochum
2017	중국	수백개의 벤더사에서 1200개 이상 브랜드로 판매되고 있는 중국 무선 웹캠 버그 공개	-

4. 스마트 홈 IoT 보안 기술 요구사항

스마트 홈 환경에서 관리되어야 할 보안 요소는 크게 4가지로 구분할 수 있다. 공격자들은 스마트 홈 데이터조작 및 무결성 훼손, IoT 통신환경 네트워크 공격 등을 통해 공격을 시도할 가능성이 있다. 그러한 위협에 모두 대응해야만 안전한 스마트 홈 구현이 가능하다. 다음은 스마트 홈 IoT 인증기술에 대한 요구사항이다.



(그림 4) 스마트홈 IoT 보안 시스템

● 통신데이터 암호화를 통한 안전한 네트워크 환경 구축

스마트 홈의 경우 사용자가 언제 어디서나 거주환경에서와 같이 디바이스를 통해 조작할 수 있는 환경을 제공하는데 이에 필수적인 기술은 VPN(Virtual Private Network)이다. 공동으로 네트워크를 이용하면서 인증, 암호화, 터널링과 같은 기술을 활용하여 가상 사설 보안 네트워크를 구축하고 인터넷만을 통해 전용선으로 연결한 것과 같이 통신할 수 있다. 더 나아가 SSL-VPN을 활용하여 다양한 디바이스에서 웹 환경으로 자유롭고 안전하게 스마트 홈을 제어 할 수 있다.

● PKI(Public-Key Infrastructure)인증체계

PKI는 권한을 가진 사람, 디바이스 및 어플리케이션에 신뢰할 수 있는 ID를 부여하고 인증, 암호화 및 서명을 통해 안전한 데이터 송수신을 가능하게 한다. PKI는 시스템 규모에 상관없이 다양한 트러스트 모델을 관리할 수 있고 중앙 집중화가 가능하다. 이는 보안과 규모, 새로운 보안 프레임을 원활하게 추가할 수 있으므로 비용을 줄임과 동시에 전문기술에 대한 종속성을 최소화 할 수 있다. 또한 스마트 홈 IoT의 ID는 수명주기를 거치면서 관리하여 스마트 홈 운영 환경에 보이지 않는 수백 개의 ID를 포함한 복잡한 환경에서도 잠재적인 취약성을 방지할 수 있을 것으로 생각된다.

● H/W 기반의 보안 모듈 제공

소프트웨어 보안은 비용적으로 효과적이고 구현 및 유지 보수를 할 수 있다는 장점이 있지만 디바이스 운영체제의 보안 수준만큼만 보안의 강도를 가진다. 운영체제에

보안 결함이 있는 경우 암호화 코드가 제공하는 보안이 쉽게 위협받을 수 있다. 신뢰점(root of trust)를 구축하기 위해서는 하드웨어 기반 기법을 토대로 한 신뢰할 수 있는 소프트웨어로 시작되어야 한다. 따라서 보안 마이크로 컨트롤러(MCU)를 사용하고 이의 내부적인 변경이 불가능한 메모리로부터 소프트웨어를 실행해야 한다.

5. 결론

본 논문에서는 스마트홈 IoT 구성과 발전현황을 파악하고 스마트홈 IoT의 보안사고 사례를 통해 무선 및 IoT 취약점을 통한 다양한 상황에 따른 대응기술에 대해 서술하였다.

빠르게 성장하고 있는 스마트홈 시장과 ICT를 이용한 자동화로 효율성과 편의성이 증대되고 있다. 사람과 가장 밀접하다고 볼 수 있는 거주지에서 사용 중인 IoT는 다양한 정보 수집 및 제어 기능을 수행하고 의존도는 높아지고 있지만 이에 따른 취약점 또한 드러나고 있다.

스마트 홈 IoT의 취약점을 이용한 사이버 공격의 피해는 산업 현장이나 외부에서 사용되는 IoT와는 다르다. 실제 생활에 밀접한 데이터를 수집하고 이기종 네트워크와 디바이스를 통한 공격은 거주자의 프라이버시 침해, 경제적 손실, 더 나아가 안전과 생명을 위협한다.

그러므로, 스마트 홈 환경의 이기종간 통신, 제한된 IoT의 컴퓨팅 능력과 에너지 효율성을 고려한 디바이스 보안 방안을 제안해야 하며, 다양한 공격패턴 학습을 활용한 인공지능 보안 및 무결성 유지를 위한 블록체인 등 최신 기술을 적용하여 보안체계를 설계하여야 한다.

Acknowledgement

- This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2018-0-00644, Linux Malware Dynamic Detection & Protection Solution on Embedded Device).

참고문헌

[1] Robles 외 3명. "A review on security in smart home development." International Journal of Advanced Science and Technology, vol.15, 2010.

[2] 한국스마트홈산업협회, “국내 스마트홈 산업 동향 조사”,2015

[3] Komninos 외 3명, "Survey in smart grid and smart home security: Issues, challenges and countermeasures." IEEE Communications Surveys & Tutorials vol.16, no.4, pp.1933-1954, 2014.

[4] Yick, Jennifer 외 2명, "Wireless sensor network survey: computer networks“, ELSEVIER, vol.52, pp.2292-2330, 2008.

[5] ZHANG 외 5명, “IoT security: ongoing challenges and research opportunities”, In: Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on. IEEE, pp.230-234, 2014.

[6] Kaspersky Lab, “New trends in the world of IoT threats“, https://www.kaspersky.com/about/press-releases/2018_new-iot-malware-grew-three-fold-in-h1-2018, Access by Mar, 2018.

[7] P. de Leusse외 3명, "Self managed security cell, a security model for the internet of things and services", In Advances in Future Internet, 2009 First International Conference on, pp. 47-52, 2009.

[8] D. Hong외 13명, "Hight: a new block cipher suitable for low-resource device", In Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems(CHES 06), pp.46-59, 2006.

[9] FADELL, “Handling security services visitor at a smart-home”, U.S. Patent Application No 14/587,835, 2015.

[10] Jose 외 2명, "Smart home automation security." SmartCR, vol.5, no4, pp269-285, 2015.

[11] Zhu 외 2명, "A new authentication scheme with anonymity for wireless environments." IEEE Transactions on Consumer Electronics, vol.50, no.1 , 231-235, 2004.