스마트 시티를 위한 홈 IoT 보안 구축에 관한 연구

윤혜민*, 전상훈**
*극동대학교 해킹보안학과
201763036@kdu.ac.kr, jjumperz@kdu.ac.kr

A Study on developing security of Home IoT for Smart Cities.

Heamin Yun*, Sanghoon Jeon**
*Dept. of Hacking Security. Far East University

요 약

최근 사물인터넷 기술은 IT 기술의 발전함에 따라, 농업, 의료, 자동차, 가전기기 및 스마트 홈 등에 이르기까지, 다양한 분야에 적용되고 있다. IoT 기술의 발전과 함께 IoT 보안에 대한 인식과 중요성이 증가하고 있으며, 보안 위협에 대응하기 위해 분야별 보안기술 가이드라인 및 표준기술이 발표되고 있다. 그러나 보안 위협 및 취약점 등에 대한 보안사고가 증가하고 있으며 이는 IoT 제품을 사용자들에게 피해로 다가오고 있다.

따라서, 본 논문에서는 홈 IoT 기반 환경에서의 보안 위협의 사례를 분석하고, 이에 대한 홈 IoT 운영 및 대응방법을 제시하여, 하고자 한다.

1. 서론

최근 IoT 서비스를 이용한 다양한 제품 및 서비스가 발전됨에 따라, 스마트 홈 기기가 일상생활에 새로운 인공지능 및 로봇 기술 등이 접목된 새로운 형태의 IoT 기기들의 도움이 증가하고 있다. 연결된 IoT 기기 간의 생성된 데이터를 통해 실시간 의사결정에 도움을 줄 수 있을 뿐만 아니라 일반 소비자의 경우 스마트 냉장고, 스마트 TV와 같은 가전제품부터 시작해 가스 밸브와 난방 시스템 등 생활에 직결된 서비스까지 IoT 기기를 사용되고 있다.

홈 IoT 기술 특성상 제한된 전력량과 메모리, 계산능력 등의 하드웨어 사양을 가지며, 항상 유선, 무선으로 연결되고, 이기종 네트워크, 디바이스 플랫폼으로 구성되어 있으며, 사토리 봇넷을 이용한 개인 CCTV 해킹, DDoS 공격 등의 공격을 이용해 사물인터넷 기기 자체에 손상을 입히는 것 등의 다양한 보안 위협 및 취약점이 급증하고 있는 것이 현실이다.

사물인터넷 기반 서비스는 공개된 인터넷을 기반으로 구축됨에 따라, 기존의 물리적인 공격이 아닌 인터넷을 통한 공격을 할 수 있게 되어, 과거보다 공격과 침입이 간편해지고 은밀한 공격이 가능하여, IoT 보안 취약점 개수는 매년 증가하고 있다. 국내 IoT 보안 관련 신고 건수는 5년간 1600건에 이르며, 2020년 하반기에 6억 3,900만 건의 취약점 개수가 2021년 상반기에는 약 15억 개 이상으로 증가해, 앞으로 더 많은 보안 취약점이 발견될 것으로 예상한다[1]. 그리고 현행 주택법의 '지능형 홈 네트워크 설비 설치 및 기술기준'에는 홈 네트워킹 보안 관련 지침이 없는 상태이다[2].

따라서, 본 논문에서는 안전한 스마트 시티를 위한 홈 IoT 시스템의 취약점 및 보안사고 등을 분석하고 안전한 구축 및 운영 방법을 제시하고자 한다.

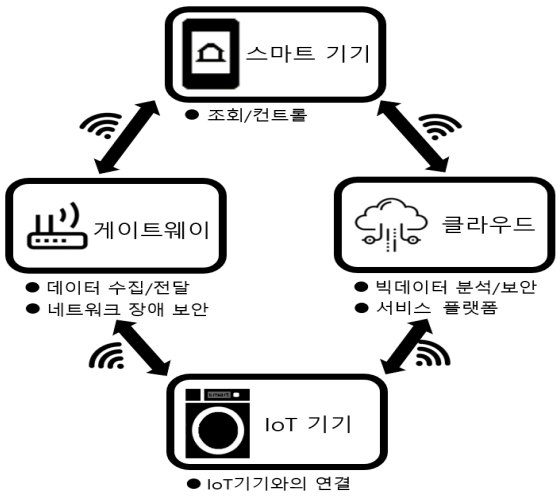
2. 본론

2.1 일반적인 홈 IoT 기기의 시스템 구성

일반적으로 홈 IoT 기기는 스마트기기와 IoT 기기를 연결하기 위한 네트워크와 IoT 기기의 데이터를 수집하기 위한 게이트웨이, IoT 기기의 데이터를 분석하는 서비스 플랫폼인 클라우드로 구성되어있다. 홈 IoT는 5G, LTE 등과 같은 IP 기반 통신방법과 IP를 사용하지 않고 통신 프로토콜을 이용한 블루투스, NFC 등의 통신방법으로 IoT 기기와 스마트기기를 연결하고 있다. 그리고 IoT 기기 자체의 저장용량과 제어시스템의 부족함을 해결하기 위해 게이트웨이, 클라우드를 이용하고 있다[3].

그림1과 같이, 게이트웨이 시스템은 센서로 수집한 데이터를 중앙 홈 게이트웨이 한 곳에 수신하고, 수신한 데이터를 스마트 홈 플랫폼에 전송해 외부에서도 사용자가 IoT 기기의 정보를 받아 제어할 수 있게 한다.

클라우드 시스템은 스마트기기와의 대규모 데이터를 처리하는 부분에서 안정적인 서비스를 제공하며 지능형 서비스를 제공하기 위해 빅 데이터 분석을 진행하기도 한다.



[그림 1] 홈 IoT 기기의 시스템 구성도

2.2 홈 IoT 기기의 취약점 및 침해사고 사례

현재 지속적으로 스마트 홈 환경에서 IoT 취약점을 통한 다양한 침해사고가 발생했으며, 2014년에는 네트워크상에 연결된 스마트 홈의 IoT를 해킹하여 이메일 시스템이나 메시지 송신 기능 등을 통해, 악성 프로그램 및 스팸 내용이 포함된 이메일에 의한 침해사고가 발생했다.

2017년에는 미라이 봇넷을 이용해 인터넷에 있는 텔넷 포트를 스캔 후, 기본값으로 로그인 시도를 한 후 CCTV와 공유기를 대량으로 모은 후, DDoS 공격을 시도해 주요 사이트를 마비시켰고, 2019년 국내에서는 IP 카메라 1800대를 해킹하고 1만 655차례 접속해 사생활을 훔쳐보는 침해사고도 보고되고 있다. 2021년에는 월 패드라는 IoT 허브를 이용해 한 가정을 해킹하면 연결되어 있는 네트워크를 통해 아파트 단지를 해킹에 대한 가능성이 발표하기도 하였다.

IoT 보안 가이드라인에서는 IoT 환경에서의 IoT 계층별 보안 위협은 센서/디바이스 계층, 네트워크 계층, 플랫폼/서비스 계층과 같이, 3가지 계층으로 분류해서 대응방안을 마련해야 한다고 정의하고 있지만, 센서/디바이스 계층에서는 저사양의 디바이스에 대한 해킹으로 적절한 보안기술 적용이 어렵다는 단점을 갖고 있다[4].

[표 1] 국내외 스마트 홈 IoT 침해사고 사례

연도	내용
2013	美 라스베이거스에서 스마트 TV에 탑재된 카메라를 해킹해 사생활 영상 유출 시연[5]
2014	스마트 홈 IoT의 네트워크를 해킹 후 메일 기능을 이용해 악성 프로그램이나 스팸 메일 전송
2015	SECUINSIDE에서 mugmung은 Hack RF를 이용한 RF 신호 재전송을 통해 스마트 홈 장비에 대한 공격발표[6]
2016	Joseph Hall은 ShmonCon에서 Z-Wave 프로토콜을 사용하는 스마트 홈 제품의 제어권 획득에 관한 내용 발표[6]
2017	미라이 봇넷을 이용한 DDoS 공격
2019	IP 카메라 1800대를 해킹 후 1만 655차례 접속해 사생활을 훔쳐보는 사건 발생
2021	월패드를 이용한 아파트 단지 해킹 가능성 발표

IoT 기기는 급속도로 증가하고 있으며, 이에 따른 보안패치 적용, 관리, 모니터링의 어려움이 커지며 관리 취약점이 증가하고 있다. 또한, 스마트 홈 기기들이 경량 암호를 사용하는 점을 이용해 불법적으로 암호를 가로채는 위험이 있으며, 이때 불법 애플리케이션을 설치할 경우, 사용자가 인지하지 못한 채, 실시간 음성 등이 공격자에게 전송될 수 있는 취약점이 보고되고 있다.

네트워크 계층에서는 앞서 말한 미라이 봇넷과 같은 악성코드 및 DDoS에 감염되면 대규모 트래픽의 공격을 받게 되는 취약점이 존재하며, 프로토콜에 문제가 발생하여 정보가 변조되거나 유출될 수 있는 약점이 보고되고 있다[7],[8].

플랫폼/서비스 계층에서는 오픈 API와 같은 오픈 플랫폼의 취약점을 악용하여, 디바이스 및 서비스 간의 데이터 위변조 및 탈취, 오작동을 유발하는 등의 취약점이 노출되고, 디바이스로부터 수집된 정보를 가지고 조합하여 새로운 정보를 만들게 되면 개인정보 유출 및 침해사고에 대한 우려가 커지고 있다[7],[8].

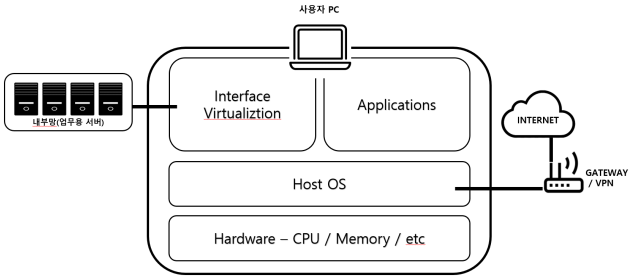
3. 안전한 홈 IoT 구축을 위한 제안방안

3.1 네트워크 분리

현재 홈 가전 IoT 제품들은 하나의 허브인 월패드에 묶여 관리되고 있으며, 월패드는 아파트 단지, 공동주택에 하나로 묶인 네트워크로 관리되고 있다. 이는 한 가정이 해킹을 당했을 시 다른 여러 가구까지 피해를 보게 되는 큰 문제로 이어질 수 있다. 이에 대한 보안 위협에 대응하고 비용문제를 해결하기 위해, 두 가지의 네트워크 분리 방법을 제안한다.

첫 번째 방법은 그림 2와 같이, 클라이언트 기반 가상화(Client Based Computing) 네트워크 분리로서, 클라이언트

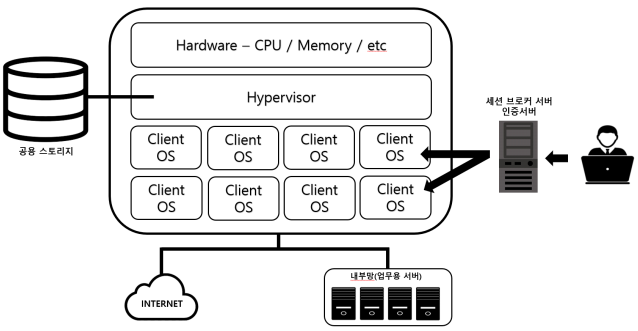
기반 가상화 네트워크 분리란 가상화 기반에서 동작하며, VPN을 통해 내부 네트워크로 접속하도록 함으로써 네트워크 분리를 실현하는 방법이 있다.



[그림 2] 클라이언트 기반 가상화 네트워크 분리

현재 사용되는 OS에 가상의 공간을 생성하고, 가상공간 내에서 실행된 애플리케이션만 인터넷에 접속되도록 함으로써, 시스템 자원을 크게 소비하지 않기 때문에 기존의 허브에 적용 가능하다. 최소한의 비용으로 네트워크 분리를 구축할 수 있어, 가상 머신 영역에서는 VPN 터널링을 통해 외부 네트워크 접속이 이뤄지기 때문에, VPN을 이용한 암호화된 데이터 통신이 가능한 장점을 갖고 있다[9].

두 번째 방법은 서버 기반(Server Based Computing) 네트워크 분리가 있다. 서버 기반 네트워크 분리란 외부 물리 서버에 가상화 기술을 적용해 VMware 같은 가상머신을 생성하고, 해당 가상머신을 통해 외부네트워크 혹은 내부네트워크 접근이 가능하도록 환경을 구축한 다음, 사용자에게 해당 가상화 서버에 대한 접속계정만 할당해주는 방식으로, 그림 3과 같이, 외부 물리 서버의 자원을 이용해 가상화를 하고 있어, 사용자가 원하는 점에 따라, 다양한 사양의 OS 환경을 구축할 수 있다는 장점이 있다[9].



[그림 3] 서버 기반 네트워크 분리

그러나, 사용자 수만큼 생성된 계정에 따라 비용이 올라가며 VDI 솔루션에 대한 라이선스 그리고 가상화 서버에 올라가는 OS 라이선스 비용까지 전부 포함하기 때문에 클라이언트 기반의 가상화 네트워크 분리보다 비용이 많이 들지만, 더 안전하다.

3.2 FIDO(Fast IDentity Online) 인증체계

네트워크 분리는 한 가정이 해킹당할 시 다른 여러 가정까지 위험해지는 문제를 해결해줄 뿐, 허브가 해킹당하는 근본적인 대응방안이 되지 못하고 있다. 이를 해결하기 위해 FIDO 인증을 대응방안으로 제안한다.

FIDO 인증은, PKI 인증과 같이 공개키 암호 시스템에 바탕이 되어 강력한 인증 서비스를 제공하면서도 사용자별 인증서 발급이 필요하지 않고, 생체 인증 등과 결합해 안전하고 편리한 인증 서비스 제공이 가능하다[10].

네트워크 통신 시, 일어나는 보안 위협에 대응하기 위해서는 아이디, 비밀번호 등을 이용한 보안 인증체계를 필요로하고 있다. 따라서 그 중, 지문, 홍채와 같은 생체 정보를 입력해 좀 더 강력하면서도 PKI 인증체계보다 간편한 보안체계를 구축할 수 있다. 그리고 FIDO 인증체계를 도입하게 되면 사용자별 인증서를 발급하는 번거로운 방법 대신, 사용자가 인증 시, 사용하는 인증 장치의 생산자별로 인증서를 발급하는 것을 이용해, 더욱 안전한 데이터 송수신을 가능하게 할 수 있다. FIDO 인증에서 사용되는 공개키는 인증 장치에서 생성되어 서버별로 다르게 등록되며, 시스템 규모와 관계없이 중앙에서 관리가 가능해진다. 이는, 새로운 보안 위협이 나왔을 시, 이에 대한 보안 패치를 원활히 추가할 수 있기 때문에, FIDO 인증체계를 대응방안으로 제안한다.

3.3 클라우드 보안 탐지모델

네트워크 분리와 FIDO 인증을 도입했음에도 보안 위협이 오는 경우를 대비해 클라우드 보안 탐지모델을 사용해 대응하는 것을 제안한다.

클라우드 탐지모델을 도입하게 되면 보안 위협을 인지하게 되는 문제를 손쉽게 탐지할 수 있게 되며, 자동화를 통한 보안 위협에 대해 바로 격리를 함으로써, 보안 위협에 더 강력하게 대응할 수 있는 장점을 갖고 있다[11].

4. 결론

본 논문에서는 기존의 홈 IoT 기기 구성과 홈 IoT 기기의 취약점 및 침해사고사례에 대해 파악하고 그에 대한 안전한 스마트 홈 시티 구축을 위한 방안으로 네트워크 분리, FIDO 인증방법을 접목한 방법을 제안하여, 보안 위협에 대응하고자 한다.

스마트 홈 IoT 취약점을 이용한 사이버 공격의 피해는 기존의 기업에서 사용되는 IoT와는 달리, 실제 거주자의 프라이버시 침해, 경제적 손실, 안전과 생명을 위협하기 때문에,

이러한 잠재적인 위험을 예방하기 위해, 향후에는 제안한 방법을 바탕으로 홈 IoT의 취약점을 개선하여, 안전한 스마트 홈 IoT 구축하여, 안전성을 증명하도록 하겠다.

참고문헌

[1] Karspersky Lap IoT Cyberattacks Escalate in 2021, According to Kaspersky, https://www.pymnts.com/news/security-and-risk/2021/kaspersky-detects-iot-cyberattacks-double-last-year, September, 2021

[2] 지능형 홈네트워크 설비 설치 및 기술기준, 과학기술정보통신부

[3] 이영헌, 조정훈, 박종혁, 스마트 홈 IoT 보안기술 연구 동향 및 고찰, 한국정보처리학회, 제 26권 1호, pp. 174-177, 5월 2019년

[4] ICT 융합 제품/서비스의 보안 내제화를 위한 IoT 공통 보안 가이드, 한국인터넷진흥원 2016년

[5] 홈 가전 IoT 보안 가이드라인, 한국인터넷진흥원 7월 2017년

[6] 박중오, 클라우드 서비스 기반 스마트 홈 환경에서 안전한 데이터 통신을 위한 메시지 통신 프로토콜 설계, 중소기업융합학회, 제 11권 7호, pp 21-30, 7월 2021년

[7] 원종혁, 홍정완, 유연우, “IoT 계층별 보안 위협 분석 및 대응기술 개선방안 연구”, 중소기업융합학회, 제 8권 6호, pp. 149-157, 5월 2018년

[8] 백인주, 이경호, 스마트 홈 환경에서의 보안 위협 대응에 관한 연구, 한국정보처리학회, pp. 282-284, 10월 2018년

[9] 이용희, 유승재, 가상화를 이용한 논리적, 물리적 망 분리 구축, 한국융합보안학회, 제 14권 2호, pp. 25-33, 3월 2014년.

[10] 박승철, PKI 인증과 FIDO 인증에 대한 비교 분석, 한국정보통신학회, 제 21권 7호, pp. 1211-1419, 7월 2017년

[11] 김창석, 김종민, 망 분리 환경에서의 IT 보안 위협 및 대응방법 분석, 한국정보통신학회, pp. 638-640, 5월 2021년