스마트 홈 환경에서 보안 위협 대응에 관한 연구[1]

백인주*, 이경호*
*고려대학교 정보보호학과
e-mail : kellogg3@korea.ac.kr

A study on Security Threat Response in Smart Home Environment

In-Ju Paek*, Kyung-Ho Lee*
* Institute of Cyber Security and Privacy, Korea University

요 약

ICT 기술의 발전에 따라 다양한 서비스들이 등장하고 있다. 특히 스마트 홈은 가전제품들을 인터넷에 접목시켜 집안 내에서뿐만 아니라 외부에서도 원격으로 제어가 가능하다. 이러한 편리성 때문에 여러 방면으로 이용성이 급증하고 있다. 하지만 아직까지 보안 기술에 있어 취약점이 많기 때문에 사생활이 노출될 가능성이 있다. 본 논문에서는 스마트 홈 환경에서 국내외 위협사례를 살펴보고, 발생 가능한 위협시나리오를 통해 위협요소를 분석한다. 또 대응방안을 제시하여 기기 개발 시 보안 관점에서의 체계를 개선을 하기 위한 방안을 논하고자 한다.

1. 서론

4 차 산업혁명의 시대가 오면서 스마트 홈이 등장했다. 집안 내부의 가전제품에 네트워크를 연결하여 집안과 외부를 소통할 수 있게 해준다. 스마트 홈 시장 규모는 나날이 확장되고 있다[1]. 시장조사기관 Statista 에 따르면 세계 스마트 홈 시장규모는 2017 년 275 억달러에서 2022 년 534 억달러로 증가할 전망이다[2,6]. 스마트 홈 이용은 생활에 편리성을 가져다 주기 때문에 유용하지만 개발에 앞서 보안설계에 다방면으로 미흡하여 보안에 취약하다. 개인정보 유출은 개인의 금전적, 신체적, 정신적으로 심각한 위험에 이어질 수 있다[3].

본고에서는 스마트 홈 환경에서의 국내/외 발생했던 해킹사례 분석 및 발생가능 위협시나리오를 통해 스마트 홈의 보안방향을 연구 하고 계속 발생하는 문제점을 보완하기 위한 대책 방안을 모색하고자 한다.

2. 본론

2.1 스마트 홈 보안 연구 범위

스마트 홈이란 ICT 기반으로 주거환경에 접목되는 현상을 나타내는 것으로[1,8], 한국 정보통신기술협회에서는 지능형 정보 생활 기기와 네트워크가 연결되어 인간중심의 서비스 환경에서 기기와 사람과 상호작용을 하며 실감 생활 서비스를 제공하는 기술로 정의했으며 한국 스마트 홈 협회에서는 주거환경에 IT 를 융합하여 국민의 편익과 복지를 증진시키는 사람중심 의 생활 환경이라고 정의하였다[3,4].

스마트 홈 위협요소들은 광범위하고 다양하기 때문에 이를 분석하기 위해 스마트 홈의 구성요소를 나눠, 요소별로 위험을 나눌 필요성이 있다. 스마트 홈 의 구성요소는 크게 5 개로 나뉘며 표 1 과 같이 스마트 기기, 네트워크, 플랫폼, 디스플레이, 컨텐츠, IoT 표준화가 있다[3].

<표 1> 스마트 홈의 구성요소

구성 요소	하위 요소	예시
스마트 기기	생활 가전류, 신성장 제품류	백색 가전류, 웨어러블디바이스 등
네트워크	유/무선 인터넷	GiGA, LTE
플랫폼	홈허브, 운용 OS	셋탑, 홈 키트, 안드로이드, iOS
디스플레이	컨트롤 디바이스	핸드폰, 태블릿 PC 등
컨텐츠	생활 가전, 신제품	생활가전 원격제어, 에너지/헬스케어 등
IoT 표준화	B2B 사업 영역	스마트 기기

2.2 스마트 홈 구성요소의 해킹 사례

사물 인터넷의 미흡한 보안의 문제로 경제적인

[1] *) 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학 ICT 연구센터육성 지원사업의 연구결과로 수행되었음
(IITP-2018-2015-0-00403)

피해가 확산되고 있다. 산업 연구원에 따르면 2015 년 13.4 조원의 규모에서 2030 년에는 26.7 조원에 이르는 전망이다[5]. 이러한 피해를 막기 위해서는 현재까지 어떤 피해가 있었으며 어떻게 대응을 했는지에 대한 분석 연구가 필요하다. 또 발생 가능한 시나리오로부터 위협을 설계함으로부터 위험을 예방하고자 한다. 다음은 스마트 홈 구성 요소별로 국내/외에서 발생된 스마트 홈 해킹 사례를 매핑하고, 각 사례별로 공격 유형 및 위협 요소를 분석하였다.

2.2.1 스마트홈 기기의 공격 시나리오

스마트 기기 자체에서는 기기가 오작동되면서 인프라 자체가 마비될 수 있다. 또한 기기가 분실되거나 기기자체의 위변조가 일어나게 될 경우 개인정보가 변조되고 유출이 될 가능성이 있다[4]. 스마트워치의 공격 시나리오를 살펴보면 사용자의 신체적 정보, 운동량, 위치, 음악듣기, 카메라기능 등이 있으며 블루투스로 휴대전화와 연동하여 전화 및 메시지기능이 있다. 이 기능들을 살펴보면 스마트워치가 몰래카메라로 이용되어 피촬영자가 촬영을 인지하지 못하여 개인정보가 노출이 되는 경우가 있다. 이 경우는 기기 자체의 위험성이 존재하는 것이다. 또한 스마트 냉장고안에서 발생할 수 있는 위협 시나리오이다. 공격자는 스마트 냉장고 기능 중 기기내부촬영 기능이 존재한다. 촬영된 데이터로 식량 정보를 분석하고 신체적 정보 및 생활패턴을 알 수 있는 자료가 수집된다. 또 다른 기능 중 구매 기능은 기기와 연동된 마트에 배송 요청한 물품 데이터들이 관리되지 않을 경우, 생활패턴 및 신체적, 종교적 정보 등 다양한 개인정보가 노출되기 쉽다.

2.2.2 스마트홈 네트워크의 공격 시나리오

네트워크 상에서는 사물인터넷 내의 네트워크 통신 프로토콜에서 문제가 발생되어 정보가 변조되거나 유출될 수 있다. 또한 미라이 봇넷과 같은 대단위 사물봇에 의해 서비스거부공격이 일어날 수 있다. 2012 년, 보안업체 레블룬사는 스마트 TV 해킹을 시연하였다. 위협 시나리오는 스마트 TV 에 악성소프트웨어 설치 후 최고 접근권한을 얻어 조작, 파일 검색 및 개인정보를 획득할 수 있었다. 해킹 공격 방법은 희생자의 TV 에 인터넷이 연결되어있을 경우 원격으로 조정할 수 있는 제로 데이 버그 였고, 리눅스 OS 및 펌웨어의 취약점을 이용하였다. 내부의 방화벽의 미흡한 보안과 백신프로그램 미설치 등으로 인한 TV 가 대상이다. 또한 미국에서는 공개된 네트워크에 디폴트된 암호 혹은 취약한 암호설정으로 인해 노출된 스마트홈 장치가 많다는 문제점이 있었다. 전세계의 피싱 및 스팸메일이 스마트 가전 해킹을 통해 발송되었다. 해킹툴인 씽봇이 스마트홈의 네트워크에 침입해 가전제품에 설치되었다. 발송된 IP 를 파악해 공격을 차단하는 방법이 쉽게 IP 에서 보내는 이메일 건수를 10 개 이하로 제한하는 수법을 이용하였다. 공격자들은 가정용 라우터와 기기자체의 허술한 보안조치를 이용한 사례이다. 2016 년, 중국의 시옹마이테크놀로지사는 CCTV 와 DVR 장비를 해킹 후 미라이 봇넷이 Dyn DNS 서버 공격을 하여 1200 여 개의 주요사이트를 마비시켰다.

2.2.3 디스플레이 및 컨텐츠 내 해킹 사례 및 위협 시나리오

기기 자체에서의 인증 및 기기와 기기가 연동할 때, 사용자와 기기가 인증할 때 스마트홈 기기들은 경량 암호를 사용한다. 이때 발생할 수 있는 취약점들을 사례를 통해 분석하고자 한다. 또한 불법적으로 암호키를 가로채어 플랫폼 전체에 위협을 줄 수 있다. 마지막으로 클라우드 시스템의 보안 취약점을 이용해 프라이버시 침해에 대한 위협이 존재한다. 또한 사용자가 악성 애플리케이션을 설치 할 경우, 인지하지 못하고 실시간 음성 데이터 등이 공격자에게 전송될 위험이 존재한다. 실제 2013 년, 러시아에서 발생된 관련 위협사례를 살펴보면, 중국산 수입다리미와 주 전자해킹에 활용되는 스파이 마이크로칩을 탑재하였다. 이는 200m 근방의 보안설정이 안된 네트워크 접속 및 해당 네트워크에 연결된 컴퓨터로 바이러스 전송, 도청이 가능하고 수집된 데이터를 해외서버로 전송이 가능하다. 또한 웹캠 제조사 트렌드넷의 동영상 유출사건을 살펴보면, 웹 기반 모니터링 카메라 단말기인 시큐어뷰어가 해킹되었던 사례이다. IP 주소를 알면 수집된 정보를 다운 받아 이용할 수 있는 미흡한 보안 설계로 인해 일어났다. 또한 모바일 앱에서도 사용자 로그인 계정 정보가 지속적으로 단말기 내부에 저장되었던 점에서 보안이 뚫린 사례이다.

2.3 스마트 홈 환경에서 공격 유형

앞서 말한 스마트홈의 구성 요소 별로 발생된 해킹 위협사례와 공격 시나리오를 통해 공격 유형을 분석했다. 공격유형은 프로토콜 공격, 도청 공격, 암호 알고리즘 및 키 관리 공격, 스푸핑과 위장, 운영체제 및 애플리케이션 무결성 공격, 서비스 방해와 거부, 물리적 보안, 접근 통제 공격이 있다[7].

2.4 스마트 홈 보안 대응 방안

위협이 발생되는 원인은 스마트 홈 플랫폼관점, 개발자관점, 사용자에 관점에서 살펴보았다. 스마트 홈 플랫폼 구조에서 발생되는 위협 원인은 현저하게 늘어나고 있는 피해건수와 경제적 피해금액을 견주어 봤을 때 스마트 홈에서 발생하는 원인들을 분석할 필요성이 있다. 스마트 홈 환경에서는 사용자의 거의 모든 개인정보가 오가고 있고 미흡한 보안기술로 인해 정보획득이 용이하기 때문에 정보탈취의 타깃이 된다. 스마트 홈은 또한 다양한 디바이스가 연결되면서 보안고려사항이 많고, 다양한 공격시나리오가 존재하기 때문에 다방면에서 보안기능을 탑재 하는 데에 어려움이 있다. 개발자의 관점에서는 빠르게 개발

하여 시장을 점유하기 위해 보안기능을 탑재하지 않고 판매를 하는 경우도 있고 기기의 단가를 낮추기 위해 보안패치를 하지 않고 출시한다. 또한 악의적인 판매자인경우 기기에 높은 권한을 부여하고 판매 후 사용자의 정보를 탈취한다. 사용자의 문제는 사용자가 보안 인식의 문제와 개인적부주의로 나눌 수 있다. 개인이 부주의하게 기기를 분실하는 경우도 있지만 가장 중요한 보안 사고 원인 중 하나는 사용자의 인식이다. 보안이 약한 비밀번호 설정, 업데이트를 하지 않고, 고려하지 않은 권한 허용 등이 큰 보안사고로 이어질 수 있다. 개발자 관점에서, 스마트 홈 개인정보 보호를 위해 계층을 나눠 적절한 보안 기술 적용해야 한다. 앞서 구분한 디바이스, 네트워크, 플랫폼/서비스계층에서 각 필요한 대응을 한다. 디바이스 계층에서는 경량, 저전력 암호를 사용하고, IoT 보안 운영체제 이용한다. 또한 서비스의 취약점 보안패치 및 업데이트를 지속적으로 이행하여야 한다. 네트워크 보안계층에서는 안전한 IoT 게이트웨이 구축하고 보안 프로토콜 준수 및 안전한 변수를 설정한다. 또한 침입탐지 대응, 원격 보안관리 및 철저한 관제 시스템 도입을 한다. 마지막으로 서비스 보안계층에서는 스마트인증 기술, IoT 프라이버시 보호기술, IoT 보안솔루션 제공이 필요하다. 또한 사용자들에게 초기 보안 설정 방안을 제공할 필요성이 있다.

3. 결론

고령화 시대에 접어들면서 스마트 홈의 필요성은 늘어나고 있지만 스마트 기기의 미흡한 보안 문제로 인해, 개인 정보 보호의 문제의 해결은 큰 숙제로 다가왔다. 이 논문은 스마트 홈의 기기 구성요소를 세 부분으로 나누어 각 부분별 개인정보 침해 해킹 사례와 발생 가능한 시나리오 접근을 통해 취약점을 분석하였다. 따라서 스마트 홈 환경에서 개인정보보호를 위한 기술적, 법률적으로 대응하기 위한 연구방향을 제시하여 가이드라인을 구축하는데 도움을 줄 것이다. 이후 연구에도 더 많은 가능성을 열어두고 다방면의 관점에서 보안에 관한 연구가 진행되어야 한다.

참고문헌

[1] 이학준, “사물인터넷 기반의 스마트 홈”, 한국통신학회지 (정보와통신) 제 32 권 제 4 호, 2015.03, 44-49
[2] 스태티스타, “스마트 홈 시장 규모 추정치”
[3] KISDI, “IoT 환경에서의 개인정보 이슈”
[4] 김정녀 (2017), “초연결 환경에서 보안위협 대응을 위한 사물인터넷(IoT) 보안 기술 연구”, 한국전자통신연구원, 2017.
[5] Gartner (2014), ‘Market Trends: TSP, Must Invest in the Rapidly Evolving IoT Ecosystem Now”, 2014. 3. 27.
[6] 한국 정보화 진흥원 (2013), “창조적 가치연결, 초연결사회의 도래”, IT & Future Strategy 제 10 호
[7] 남서울대 산학협력단 (2015), “사물인터넷 시대의 개인정보 침해요인 분석 및 실제사례조사 최종보고서”
[8] KISA, “홈 가전 IoT 보안 가이드”