IoT 장치의 개방형 무선 네트워크를 통한 공격 위험

이건우*

계룡디지텍고등학교

Risk of Attack through an Open Wireless Network of IoT Devices

Geonwoo Lee*

Kyeryong Digitech High School

E-mail : i1384992@naver.com

요 약

IoT(Internet of Things: 사물인터넷)의 보급이 시작되면서 보안 위협 또한 증가하고 있는 추세이다. IoT에 관련된 보안 사고는 재물적 피해는 물론 나아가서는 인간에게 직접적인 위험을 줄 수도 있으므로 이러한 문제들을 방지하기 위해서 IoT 장치의 보안 설비는 매우 중요하다고 할 수 있다. 본 논문은 IoT 장치의 정의와 보안사고 사례, 아키텍쳐, 개방형 무선 네트워크를 사용할 때 발생할 수 있는 보안 문제점에 대해서 서술했다.

ABSTRACT

The number of security incidents is increasing as the Internet of Things(IoT) is distributed widely. The security incidents of IoT can cause financial damages. Moreover, It can become direct threats to humans. In order to prevent these problems, the security installation for IoT devices is important. This paper describes the definition of IoT devices, security incident case, architecture, and the security threats that can occur when a device is connected to network without security installation.

키워드

Wireless, Wi-fi, IoT, Cloud, Security, Reversing

Ⅰ. 서 론

무선 네트워크 서비스의 일종인 Wi-Fi의 대중화를 시작으로 IoT(Internet of Things: 사물인터넷) 장치의 보급이 시작되었다. IoT는 현재 홈, 가전, 의료, 교통 등 다양한 산업분야에서 활용되고 있으며, 본격적으로 시장이 활성화되고 있다. 최근 뛰어난 보안 성능을 갖춘 IoT 장치부터 보안성을 고려하지 않은 IoT 장치까지 많은 장치들이 대거 출시되고 있다. 이에 IoT 장치의 보안 문제가 발생하기 시작하였다. 이에 따른 피해 규모는 2020년 17조 7,000억원, 2030년 26조 7,000억 원까지 증가할 것으로 예측하였다.[1]. 또한 증가하는 IoT 장치의 수와 더불어 IoT 장치의 공격 위험과 이로 인한 개인정보 침해, 생활 안전 우려 역시 증가하고 있는 추세이다.

본 연구에서는 IoT 장치가 개방형 무선 네트워크에서 운용될 때 발생할 수 있는 외부로부터의 공격 노출 위험성과 사례에 대해 알아보았고, 이를 토대로 실제로 일어날 수 있는 공격 기법에 대해 기술하였다.

본 논문의 구성은 다음과 같다. 서론에 이어 2장에서는 관련 연구로 IoT의 정의와 현황 및 보안사고 관련 사례, 아키텍쳐와 보안 위협, 네트워크 보안에 대해서 기술하였고, 3장에서는 개방형 네트워크 사용의 문제점과 클라우드 서버 에뮬레이션

* corresponding author

등 공격에 사용될 수 있는 애플리케이션에 대해 기술하였으며, 마지막으로 4장에서 결론 및 제언으로 맺는다.

II. 관련 연구

2.1. IoT의 정의와 현황

ITU(International Telecommunication Union.)는 IoT를 기기 및 사물에 통신 모듈이 탑재되어, 유무선 네트워크로 연결됨으로써 사람과 사물 간, 사물과 사물 간에 정보 교환 및 상호 소통할 수 있는 지능적 환경으로 해석하고 있다. 또한 다양한 정보통신 기반기술의 발달로 인하여 사물이 소형화되고 스마트화 되어 사물인터넷의 시대가 도래할 것으로 전망하고 있다[2]. 또한 시장조사 전문 업체 가트너 (Gartner) 사는 네트워크에 연결된 장치의 수가 2017년 84억 개에서 2020년 2조 개까지 증가할 것으로 예측하였다[3]. IoT 장치는 기본적으로 네트워크에 연결되어 네트워크상의 다른 IoT 장치, 홈 허브, 사용자의 단말기나 인터넷 상의 서버 등과 통신을 하게 된다. 근래에 들어서는 기존의 가전제품 또한 IoT화 되어 네트워크에 연결되는 사례가 늘어나고 있으며 증가하는 장치의 수에 따라 보안 관련 문제 또한 증가할 것이다[참고문헌 필요].

2.2. IoT 보안사고 관련 사례

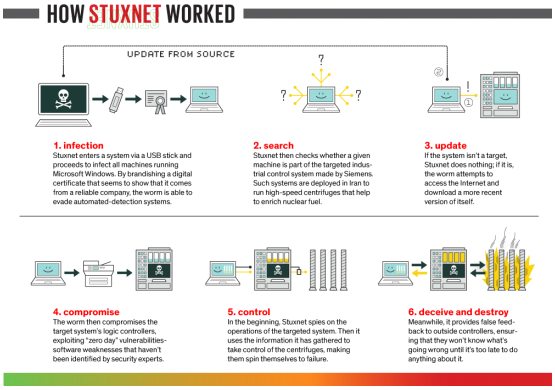

그림 1. Stuxnet의 동작 방법[4]

2010년 이스라엘과 미국이 이란의 핵시설을 마비시키기 위하여 사용하였던 스턱스넷(Stuxnet) 이라는 웜 바이러스에는 지멘스사의 SCADA 시스템을 감염시킨 후 장비를 감시하고, 제어하는 코드가 탑재되어 있었다. 이란의 핵시설은 외부망과 분리되어 있는 환경이었음에도 불구하고 USB 메모리를 바이러스의 매개체로 하여 보안사고가 발생한 것이다. 또한 2014년 국내에서도 SKT 및 LGU+의 네트워크에서 공격이 발생해 각 통신사의 서비스가 일시적 장애를 일으키는 사고가 발생하기도 하였다.

민주주의와 기술센터(Center for Democracy and Technology: CDT)에서는 다음과 같은 시나리오를 발표하기도 하였다. 가정의 전등 센서는 어떤 방이 얼마나 자주 사용되는지를 알 수 있으며, 온도 센서는 누군가가 목욕을 하거나 운동하는 시간, 집을 나서는 시간을 알 수 있다. 또한 마이크를 통해 대화 내용을 쉽게 알아낼 수 있다. 또한 앞으로 수 년 간 법원과 각종 규제 기관들은 IoT 사생활 안전장치를 두고 치열하게 싸우게 될 것이다.[5]

IoT 장치는 특성 상 장치의 펌웨어 취약점으로 인하여 비인가 사용자의 접근이 가능할 수 있다. 또한 센서 네트워크는 특성 상 다양한 보안기술을 개발하거나 응용하기 어렵기 때문에 데이터 도청과 물리적 센서 제거 등의 보안 문제점이 거론된다[6].

2.3. IoT 아키텍처와 보안 위협

인터넷 연결이 가능한 소형 장치는 대부분 TCP/IP 기반의 프로토콜을 사용하고 있다[7]. 따라서 TCP/IP 기반 보안 위협에도 일반적으로 가정에서는 유무선 공유기를 통하여 Wi-Fi 네트워크를 사용하기 때문에 설치의 편의성을 위해 많은 가정용 IoT 장치는 Wi-Fi 네트워크를 이용하도록 설계되어 있다.

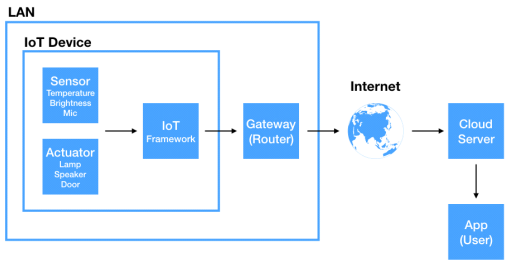

그림 2. IoT 아키텍처

IoT 장치는 그림 2와 같이 센서, IoT 프레임워크, 클라우드 서버, 모바일 애플리케이션 순으로 연결되어 조작된다. 여기서 IoT 장비가 운용 중인 LAN(Local Area Network: 근거리 통신망)에 외부 공격자가 네트워크에 침입한다면 게이트웨이의 설정을 임의로 변경하거나 네트워크 내의 PC를 조작하여 IoT 장치가 비정상적으로 동작하도록 유도하거나, 공격자의 의도대로 조작할 수 있게 된다. 공격자가 LAN에 간섭할 수 있는 가장 쉬운 방법은 물리적으로 가까운 위치에서 무선 LAN에 접속하는 방법이다. 따라서 IoT 장치를 Wi-Fi 네트워크에서 운용 시 보안 설정이 반드시 필요하다.

2.4. IoT와 무선 네트워크 보안

무선 LAN의 보안 방식은 크게 개방형, WEP(Wired Equivalent Privacy), WPA(Wi-Fi

Protected Access), WPA2가 있다. WEP는 무선 LAN 통신을 암호화 하는 가장 기본적인 방식으로 64bit/128bit 암호화 방식과 RC4 알고리즘을 사용한다. 먼저 클라이언트가 AP(Access Point)에 인증 요청을 하면 AP가 랜덤으로 초기화 벡터를 생성하여 전송하고, 클라이언트는 이를 WEP 키로 암호화하여 다시 전송한다. AP는 수신된 응답을 WEP키를 통하여 다시 복호화하고 처음 전송했던 키와 일치하면 연결을 허용하는 방식이다. 단 이 방식은 패킷에서 초기화 벡터를 수집하는 것으로 복호화가 가능하기 때문에 최근에는 사용을 지양하고 WPA를 사용하는 추세이다. WPA(Wi-Fi Protected Access)는 TKIP 알고리즘을 사용하며 단순한 패킷 수집으로는 복호화 할 수 없다. 또한 WPA2의 경우 AES암호화 알고리즘을 사용해 더 강력한 보안을 제공한다.

III. 개방형 무선 LAN을 통한 공격 위험

3.1. 개방형 무선 네트워크 사용의 문제점

최근 IoT 장치의 70%가 암호화되지 않은 네트워크를 통해 데이터를 전송하는 것으로 확인되었다[8]. 이는 역설적으로 70% 이상의 IoT 장치가 MITM(Man In The Middle attack : 중간자 공격), Sniffing, Spoofing 등 TCP/IP를 기반으로 한 공격 기법에 무방비하게 노출되어 있다는 것을 의미한다.

본 연구에서 사용한 IoT 장치인 LED Celling Light는 무선 네트워크를 통하여 장치의 펌웨어에 미리 입력된 IP로 제조사의 클라우드 서버에 연결되며, 이후 사용자의 스마트폰에 설치된 모바일 애플리케이션과 클라우드가 통신하는 구조로 설계되어 있다. 공격자가 AP의 커버리지 안에서 무선 LAN에 접속 한 뒤 IoT 장치가 제조사의 클라우드 서버 대신 임의의 서버로 접속하도록 조작한다면 IoT 장치의 전반적인 권한을 탈취하는 것이 가능하게 된다.

3.2. 클라우드 서버 에뮬레이션

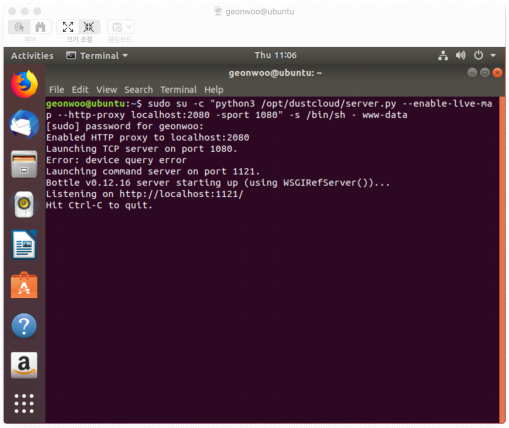

그림 3. Ubuntu 18.04에 설치된 Dustcloud 서버

그림 3의 Dustcloud는 본 연구에서 사용된 스마트 전등의 공식 클라우드 서버 기능 일부를 사용자가 구동할 수 있도록 만들어진 오픈 소스 애플리케이션으로 php를 기반으로 한 웹 UI를 지원하여 컴퓨터에 대한 전문 지식이 없는 사용자도 사용할 수 있도록 개발되어 있다.

또한 이와 같은 애플리케이션의 악의적인 이용으로 인하여 3장 1절에서 언급한 내용과 같이 장치의 부분적, 전반적인 권한을 탈취하는 것이 가능하다.

이후 IoT 장치에 물리적인 접근없이 장치가 임의의 서버로 접속하도록 만들기 위하여, 장치가 서버를 제조사의 클라우드 서버로 인식하도록 하여야 한다. 이는 악성코드로 라우터의 설정을 변경하거나, ARP Spoofing 등을 이용한 DNS Redirection과 같은 방법이 있다. 또한 본 연구에서 사용된 IoT 장비는 제어를 위하여 디바이스 ID와 암호 키가 필요한데, 수정된 펌웨어를 업로드하는 것을 통하여 루트 권한을 하여 얻어내거나[9], 스마트폰의 장치 관리 애플리케이션의 로그에서 추출하여 얻을 수 있다.

3.3. 무선 네트워크를 통한 패킷 캡쳐

IoT 장치들은 대부분 폐쇄적인 시스템 구조로 일반적으로 바이러스에 보다 안전하다고 알려져 있다. 그러나 운영체제 경량화로 인하여 보안 설비가 미비하거나 없는 경우가 많기 때문에 MITM, Sniffing, Spoofing 등 네트워크를 통한 공격에 대해서는 오히려 취약하다.

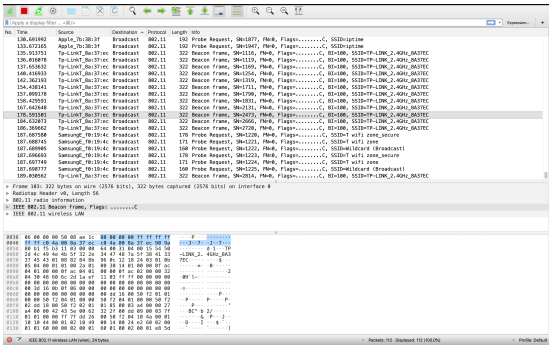

그림 4. Wireshark를 이용한 WLAN 패킷 캡쳐

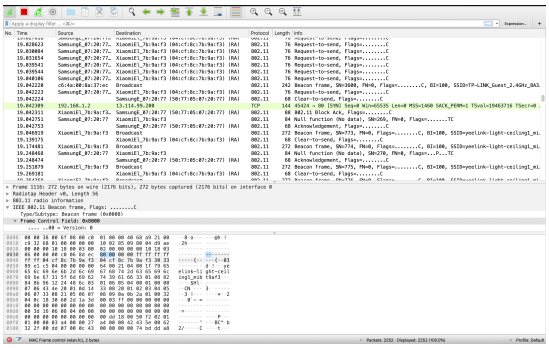

그림 5. 개방형 무선 네트워크 패킷 모니터링

무선 네트워크 접속을 해제한 후 무선 NIC의 동작 모드를 모니터 모드로 변경하면 그림 3과 같이 공중의 무선 네트워크의 패킷, 특히 IoT 장치의 패킷을 수집하는 것을 확인할 수 있다. WPA/WPA2 방식으로 암호화된 네트워크의 경우 비밀번호를 알아야 복호화가 가능하지만, 개방형 네트워크나 WEP 암호화를 사용한 네트워크는 쉽게 복호화가 가능하다. 특히 개방형 무선 네트워크는 그림 4와 같이 별다른 기술 없이도 네트워크에서 오고 가는 패킷을 모두 모니터링 할 수 있다. 또한 다수의 IoT 장치의 개발에서 펌웨어 업데이트를 할 때 별다른 검증 절차를 거치지 않는 경우가 많은데, 만약 개방형 무선 네트워크 또는 WEP 암호화가 적용된 무선 네트워크를 사용한다면 IoT 장치가 OTA 펌웨어 업데이트를 할 때 이를 통하여 펌웨어의 데이터를 캡쳐하여 별도로 저장할 수 있다는 것이다. 이후에 디스어셈블러와 같은 리버스 엔지니어링 툴을 통해 바이너리 데이터를 수정하는 것으로 코드를 삽입하여 루트 권한을 획득할 수 있을 것이다.

3.4. LAN 조작 모드가 활성화 되어있을 경우

일부 사용자들은 서로 다른 제조사의 기기를 통합하여 관리하기 위하여 제조사에서 기본적으로 제공하는 관리 도구 말고도 다른 솔루션을 사용하기도 하고, 스크립트 작성에 이용할 수 있는 라이브러리도 개발되어 있다. 상황에 따라 LAN 조작모드를 활성화시키는 경우도 있는데, 이때 조작용 애플리케이션과 IoT 장치 간에 보안 기능이 동작하지 않는 경우도 있기 때문에 네트워크 보안에 더욱 유의해야 한다.

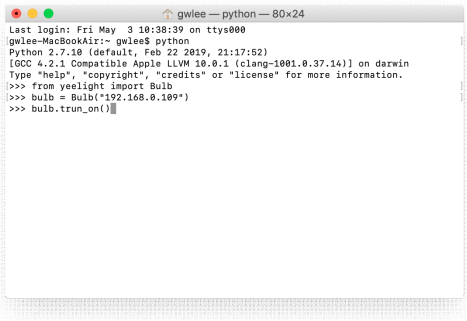

그림 6. LAN을 통한 IoT 제어 스크립트

Ⅳ. 결론 및 제언

IoT의 보급과 함께 일상 생활이 자동화가 되어 각종 기기의 관리 효율성이 높아져, 일상 생활이 편리하여 지고 삶의 질 또한 향상되고 있다. 그러나 IoT의 사용 증가는 IoT 보안 사고로 이어지는 경우가 많다. 특히 가정에서는 유무선 공유기를 별도의 추가 설정 없이 공장 기본 값으로 운용중인 경우가 많은데, 이는 무선 네트워크를 통해 조작되는 IoT 장치의 특성상 외부의 비인가 사용자의 조작을 허용하는 일이 될 수 있기 때문에 보안에 매우 취약하다. 보안 설정이 되어있지 않은 무선 네트워크를 사용하는 것만으로도, 여러 가지 IoT 보안 위협에 노출될 수 있다. 따라서 안전한 IoT 환경 구성을 위해 IoT 장치의 제조사들은 대중의 생활과 직접적으로 연관되어 있으므로 보안 설비에 시간과 비용을 더욱 투자하여 안전한 장비를 생산해야 한다. 그리고 소비자는 각종 보안 위협으로부터 안전하게 설계된 장치를 구입하고, 무선 네트워크에 WPA/WPA2 등 강력한 보안 프로토콜을 적용하거나 IoT 전용 프로토콜을 사용하는 장비를 이용하는 등 IoT 장치의 보안 설비의 중요성을 인지하여야 한다.

References

[1] 황원식, 김승민, e-KIET 산업경제정보, 586th ed. Seoul: 산업연구원, Page 8, 2014

[2] 김민식, 정원준, 사물인터넷(IoT) 관련 가치사슬 및 시장 구성요소 현황, 576th ed. Seoul: 동향, Page 22, 2014

[3] Gartner, Inc. Newsroom Press Releases, “Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016” [Internet] Available :

https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

[4] NJCCIC "Stuxnet" [Internet] Available: https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/stuxnet

[5] Patrick Thibodeau, The ABC of the Internet of Things, Computer world: US, 2014

[6] 한정진, "사물인터넷(IoT) 보안성 검토를 위한 보안아키텍처 설계와 점검항목 구성", Page 31, 2015

[7] Bergmann O, Hillmann K.T, Gerdes S, A CoAP-gateway for smart homes. Computing, Networking and Communications, International Conference, Page 446-450, 2012

[8] Hewlett-Packard Development Company, L.P., "HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack" [Internet] Available : https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676

[9] Daniel Giese, "Reversing IoT: Xiaomi ecosystem" [Internet] Available : "https://recon.cx/2018/brussels/resources/slides/RECON-BRX-2018-Reversing-IoT-Xiaomi-ecosystem.pdf"