# 스마트 홈 및 가전 디바이스 해킹

20195178, 서영재

요 약

최근 첨단 기술, 편리함, AI(인공지능)활용 등으로 IoT를 표현할 수 있으며, 많은 매체를 통해 접할 수 있다. IoT 시장이 성장하고 우리의 일상에 IoT 기반의 제품이 보급될수록 누릴 수 있는 편리함을 늘어간다. 하지만, 그 이면에 존재하는 IoT 보안위협에 대해 경각심을 가지고 이에 대한 대응책을 세워야 한다. 본 논문에서는 스마트 홈 및 가전에 대한 취약점에 대하여 설명하며 이에 대한 대응방안을 강구하고, 높은 수준의 보안대책을 세워야 한다.

## Ⅰ. 서 론

IoT(Internet Of Things) 시장이 성장함에 따라 다양한 분야에서 편리성을 제공하고 삶의 질을 향상하며 새로운 시장 가치를 제공하고 있다. 하지만, 이러한 발전의 이면에는 이를 대상으로 하는 침해사고가 지속적으로 발생하고 있다. 최근 아파트 단지에 설치된 월패드가 단체로 해킹되면서 사생활 노출 문제가 이슈로 떠올랐다. 스마트 홈과 같은 주택과 통신의 융합이 확대되면서 일상적으로 사용하던 전자제품조차 대부분 통신 기능을 갖추고 있다. 스마트 홈이 발전할수록 사용자의 안전에 보다 직접적인 위협을 끼치는 상황이 벌어질 수 있다. 이에 본 논문에서는 스마트 홈 및 가전에 대한 취약점, 공격 시나리오, 공격 방법, 대응방안에 관해 설명한다. 이를 통해 IoT 보안위협의 심각성을 인지하고 경각심을 가져 높은 수준의 보안 대책을 세우고 IoT 디바이스에 대한 보안 인식을 제고해야 한다.

## Ⅱ. 본 론

### 2.1. IoT

IoT(Internet Of Things)는 인터넷에 연결되어 IoT 애플리케이션이나 네트워크에 연결된 장치 혹은 산업 장비 등의 다른 사물들과 데이터를 공유할 수 있는 수많은 '사물' 을 말한다. 인터넷에 연결된 장치는 내장 센서를 사용하여 데이터를 수집하고, 때에 따라 그에 맞게 반응한다. IoT 연결 디바이스와 기계는 업무 및 생활 방식을 개선하는 데 유용하다. IoT는 난방과 조명을 자동으로 조절하는 스마트 홈 기기부터 산업 장비를 모니터링하여 문제를 찾은 후 고장 예방을 위해 자동으로 해결하는 스마트 팩토리에 이르기까지 다양한 분야에 응용되고 있다.

### 2.2. 필요성 및 목적

스마트 홈은 가정 내 스마트 디바이스들을 유·무선 네트워크로 연동하여 자동화, 원격 제어, 에너지 관리 등을 통해 이용자의 편의성을 제공하며 삶의 질 향상과 비용 절약 측면에서 새로운 가치를 제공하고 있다. 또한, 스마트 디

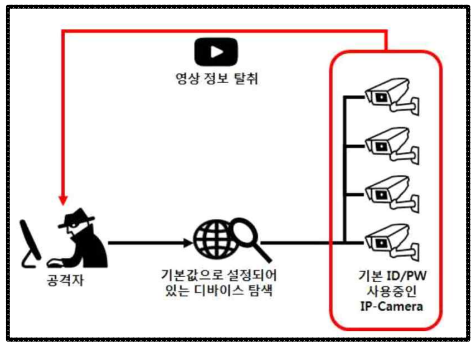
바이스 보급들의 증가와 무선 통신 기술, 센서 기술 등의 발전으로 인해 스마트 홈 구축비용이 감소하고, 가정 내의 에너지 관리에 대한 관심이 높아짐에 따라, 사물인터넷 기반의 스마트 홈 관련 사업이 활발하게 진행되고 있다. 하지만, 이러한 발전의 이면에는 스마트 디바이스를 대상으로 하는 침해사고가 지속해서 발생하고 있다. 특히 스마트 홈에서 수집되는 데이터는 사람과 사물 간의 데이터 교환을 기반으로 사생활에 대한 정보가 포함되고 있어 유출 시 프라이버시 침해 위험성이 높고 파급력이 크다. 이에 제조사, 서비스 제공자 등을 중심으로 정보보호를 위한 데이터 신뢰성, 무결성, 가용성 강화를 위해 노력하고 있지만, 무엇보다 스마트 홈 환경에서 가장 효율적인 정보 보안 방법은 스마트 홈을 활용하고 있는 이용자들에 대한 보안 인식 제고이며, 이를 통해 침해사고를 사전 예방할 수 있도록 해야 한다.

### 2.3. 스마트 홈 · 가전 보안위협 및 대응방안

#### 2.3.1. 정보 유출

대부분의 사물인터넷 디바이스 이용자의 경우 관리자 혹은 접속 가능한 계정의 패스워드를 디바이스 출고 당시 기본 패스워드 그대로 사용하거나, 안전하지 않은 패스워드를 사용하고 있다. 공격자는 자동화된 공격 도구를 통해 패스워드가 기본적으로 설정되어있는 취약한 디바이스에 접속하여 전력 사용량, 영상정보 등을 탈취할 수 있다. 전력 사용량은 시간대별 이용자의 생활 형태를 파악하는 데이터로, 영상정보는 이용자의 사생활이 외부에 노출될 수가 있어 심각한 사생활 침해를 유발할 수 있다.

전 세계 약 7만 3천여 대의 IP 카메라가 해킹되어 '인세캠' 이라는 사이트를 통해 생중계되었다. 한국에서는 약 6000여 개의 IP 카메라가 해킹되었으며 '인세캠' 이라는 사이트 운영자가 '보안 설정의 중요성' 을 알리기 위해 해킹한 것으로 밝혀졌다. 공격자는 공장 출고 당시 설정된 아이디와 비밀번호를 바꾸지 않은 IP 카메라를 해킹 대상으로 하였다. 이를 통해 공개된 장소는 가정집과 공연장, 사무실, 공장, 슈퍼마켓, 미용실, 헬스클럽, 수영장, 카페, 피부 관리실 등 다양하며 사이트에는 IP 카메라가 설치된 위도와 경도가 나와 있고 구글 지도를 이용해 해당 위치를 추적할 수 있어, 이를 악용할 경우 개인 프라이버시가 침해되고 더 나아가 금전적, 물리적 피해까지 발생할 수 있다.




〈그림 1〉
취약한 패스워드를 사용할 경우의 보안위협
공격 시나리오

이와 같은 보안위협을 방지하기 위하여 최초 패스워드는 충분한 보안성을 지닌 패스워드로 변경하여 사용하여야 한다. 또한, 같은 패스워드를 장기간 사용할 경우 보안이 취약해질 수 있으므로 주기적으로 변경하여야 한다.

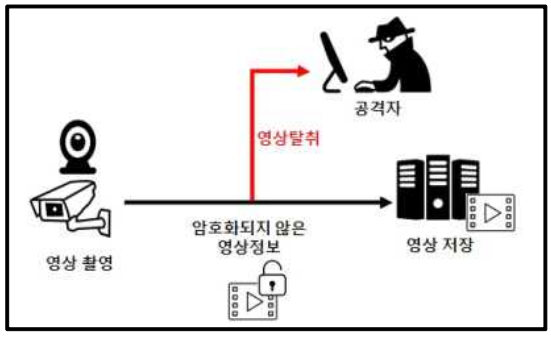
| 예측이 어려운 비밀번호 | |
|---|---|
| 1 | 영문자(대 · 소문자), 숫자, 특수 문자들을 혼합한 구성 |
| 2 | 특수 문자 활용 시, 비밀번호 시작 혹은 끝 부분이 아닌 위치에 삽입하여 설정 |
| 3 | 영문자(대 · 소문자)를 구분할 수 있을 경우, 대 · 소문자를 혼합하여 설정 |

〈표 1〉 안전한 패스워드를 설정할 수 있는 방법

또한, 사물인터넷 디바이스 통신에 암호화를 이용하지 않거나, 취약한 암호방식을 사용할 경우, 공격자는 암호 알고리즘의 취약점을 이용하여 디바이스에 접근하여 사용자의 특정 정보를 탈취할 수 있다.

트렌드넷의 웹 기반 모니터링 카메라 단말기인 시큐어뷰어가 촬영한 동영상이 온라인상에 노출되는 사건이 발생하였다. 이는 트렌드넷이 2010년 4월 펌웨어 업데이트 버전을 상용화할 때 고객의 로그인 계정 정보를 암호화하지 않고 인터넷상에서 동영상을 전송 및 저장하여 발생한 문제로 파악되었다. 또한 트렌드넷 전용 모바일 앱에서도 고객이 로그인 시 계정 정보가 지속해서 단말기에 저장되어 보안에 취약한 구조인 것으로 확인되었다.

이처럼 공격자는 보안 취약점을 통해 IP주소로 접속하여 별도의 인증 절차 없이 영상을 다운로드 받는 등 침해사고를 발생시킬 수 있다.

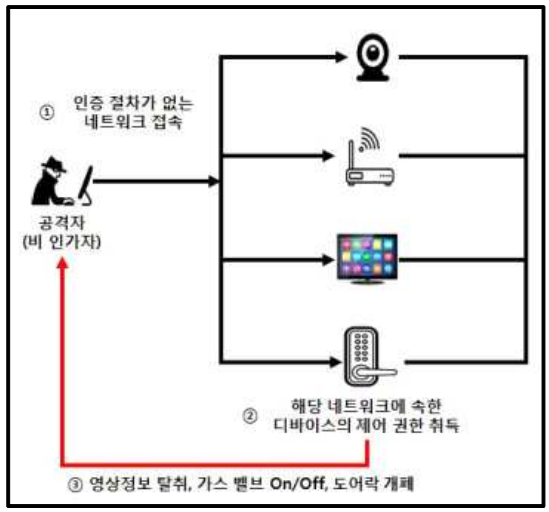



<그림 2>
암호화 절차가 없는 경우의 보안위협 공격 시나리오

이와 같은 보안위협을 방지하기 위하여 사물인터넷 디바이스 간 송/수신하는 데이터의 암호화가 필요하며, 사물인터넷 디바이스에서는 HTTPS 기반 보안 설정이 가능한 제품 이용을 권고한다. 만약 공유기를 이용할 경우 무선 암호화는 보안 강도에 따라 WEP, WPA, WPA2 등으로 분류되는데, 보안 강도가 낮을수록 보안상 문제가 발생할 소지가 크기 때문에, 데이터 암호화 WPA2로 변경하여 보안을 강화하도록 한다.

### 2.3.2. 비 인가자 접속 가능

사물인터넷 디바이스는 실생활과 밀접한 관련을 가진다. 베이비 모니터, 도어락 등 비 인가자가 제어 권한을 탈취하게 될 경우, 홈 컨트롤러에 접속하여 가스밸브를 On/Off 시키거나, 전기료 과다 청구 유발, 도어락 개폐, IP 카메라의 관리자 페이지에 접속 및 영상 정보 탈취 등이 가능하다.



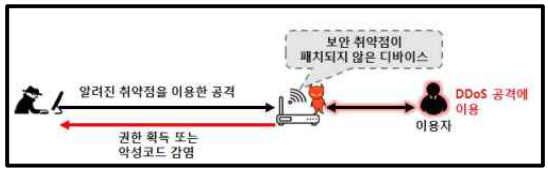

<그림 3>
접근제어가 없는 경우의 보안 위협 공격 시나리오

사물인터넷 디바이스는 인가된 이용자만이 이용 및 관리하여야 하며, 보안위협을 방지하기 위하여 인가된 이용자인지 확인하고, 비 인가자의 보안 위협에 대응할 수 있도록 ID, 패스워드, RFID 태그, MAC 주소 등 다양한 인증 수단을 이용하여야 한다.

### 2.3.3. DDoS 공격 악용

일반적으로 사물인터넷 디바이스에 취약점이 발견되면, 이를 해결한 보안 업데이트가 이루어져야 한다. 하지만 보안 업데이트가 이루어졌음에도 불구하고 이용자들이 해당 업데이트를 적용하지 않는다면, 알려진 취약점이 무방비상태로 노출되게 된다. 이로 인하여 해당 디바이스에 악성코드가 감염되면 DDoS 공격에 활용되어 이용자 모르게 타인을 공격하게 된다.

2016년 10월 주요 도메인 네임 시스템(DNS) 제공업체인 DYN(딘)을 대상으로 한 [1]분산 서비스 거부 공격이(DDoS) 발생하였다. DNS는 웹 라우팅 시스템으로 kisa.or.kr과 같은 웹사이트 이름을 203.255.210.86과 같이 컴퓨터가 읽을 수 있는 숫자로 된 인터넷 프로토콜 주소로 변환해주는 역할을 한다. DNS가 없으면 웹 브라우저는 사용자가 보고자 하는 웹사이트를 찾을 수 없는데, 이러한 서비스를 제공해주는 DYN의 서버에 DDoS 공격이 발생하여 한동안 수백만 명의 인터넷 사용자들이 불편을 겪었다. 공격자는 많은 사물인터넷 디바이스들이 알려진 취약점과 출고 당시 기본 패스워드를 사용하고 있는 점을 이용하여 악성코드를 감염시켜 DDoS 공격에 이용하였다.




<그림 3>
보안 취약점을 가진 디바이스에 대한 보안위협 공격 시나리오

1) 분산 서비스 거부 공격(DDoS) : 수십~수백만 대의 PC(디바이스)를 특정 서버(웹사이트)에 동시에 접속시킴으로써 단시간 내에 과부하를 일으켜 서버를 마비시키는 공격

이와 같은 보안위협을 방지하기 위하여 펌웨어를 최신 버전으로 유지해야 한다. 제조사에서 알려진 취약점을 해결한 버전을 배포하였는지 제조사의 보안 공지 내용을 정기적으로 확인하여 보안 업데이트를 적용해야 한다.

## Ⅲ. 결 론

IoT(Internet Of Things) 시장의 발전함에 따라 같이 따라오는 이면으로 발생하는 보안 취약점에 대해 알고 이에 대한 심각성 및 경각성을 가져 보안 인식을 높인다. 스마트 홈 및 가전에서 발생 가능한 보안위협에 대해 침해사고를 예방할 수 있도록 이용자의 관점에서 보안위협과 대응방안을 알고 이를 연구해야 한다. 스마트 홈 및 가전에서 사용하는 기기 간 통신 기능이 확대되면서 영국, 미국 등 선진국에서 강도 높은 보안 정책이 나오고 있다. 이에 국내에서도 강도 높은 보안대책을 구축해야 한다.

## 참 고 문 헌

[1] ESTsecurity, “보안 위협에 노출된 우리의 일상, IoT 취약점을 아시나요?” , 2018

[2] sas, “Internet of Things(IoT)의 정의 및 중요성”

[3] 미래창조과학부, 한국인터넷진흥원 , “사물인터넷 소형 스마트 홈가전 보안 가이드” , 2016

[4] 전기신문, 안상민 기자, ‘스마트홈, 보안대책 없으면 ‘누군가 당신 집을 엿볼 수 있다, 2021

[5] 정보통신신문, 김한기 기자, ’ [기획]스마트홈 구멍 '숭숭'… 해킹 위협받는 기기들’ , 2018