# IoT 기기의 해킹 사건과 보안 동향

임한비[O], 이가현[*], 이훈재[**]
[O]동서대학교 정보보안학과,
[*]동서대학교 일반대학원 디지털포렌식학과,
[**]동서대학교 정보보안학과
e-mail: dlagksql4@gmail.com[O], igh1116@naver.com[*], hjlee@gdsu.dongseo.ac.kr[**]

# Hacking and Security Trends in IoT Devices

Ga-Hyeon Lee[O], Hoon-Jae Lee[*], Young-Sil Lee[**]
[O]Dept. of Information security, Dongseo University,
[*]Dept. of Digital Forensic, Dongseo University,
[**]Dept. of Information security, Dongseo University

● 요 약 ●

현재 IoT 기기들은 일상생활에서 필수 가전기기가 되어가고 있다. 가정에서는 스마트홈으로 연결된 냉장고, 세탁기, 인공지능 스피커 등이 이미 많이 사용되고 있으며, 자율주행 차량과 키오스크 등 하루에도 매우 다양한 IoT 기기들을 가깝게 접하고 있다. 스마트 워치(Smart Watch)가 출시된 이후로는 IoT 기기가 매 순간 사용되며 사용자 개인정보와 사생활 등 중요하고 예민한 정보와 기업의 기밀 정보가 자동으로 기기에 저장되고 있다. 이러한 이유로 해커들의 타깃이 되어 새로운 해킹 수법이 발생하고 보안 취약점이 발견되고 있다. 본 논문에서는 IoT 기기에 관련하여 최근에 발생하는 해킹 사건들과 보안 취약점을 분석하고 이에 따른 대책을 알아보고자 한다.

**키워드:** IoT 기기(IoT Devices), 해킹(hacking), 보안(Security)

## I. Introduction

최근 IoT 기기들은 사용자들에게 일상생활의 편리함을 주는 필수 기기가 되었다. 스마트 홈, 인공지능 스피커, 스마트 워치, 자율주행차량, 키오스크 등 주변에 IoT 기기가 일상화되었다. 이 때문에 사용자의 일거수일투족이 기록되고 저장되어 자료화되고 있다. 이에 따라 해커들의 타깃이 되어 사용자의 개인정보와 사생활이 유출되는 사고가 발생하고 있다.

IoT 시장은 2023년까지 16.1%의 연평균 성장률을 보인다. 하지만 빠르게 출시되고 있는 기기들에 비해 IoT 보안정책 및 체계가 구축되어 있지 않아 취약점은 지속해 발견되고 있다[1].

이에 따라 최근에 일어난 IoT 기기의 해킹 사건에 대해 알아보고 보안 취약점을 분석해 대책을 알아보려 한다.

## II. Preliminaries

### 1. Related Case

#### 1.1 월패드(Wall Pad) 해킹 사생활 유출 사건

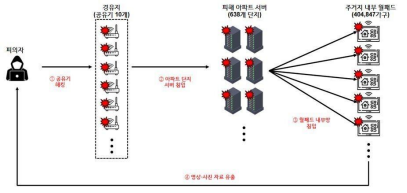

Fig. 1. Case Diagram[2]

위 사건의 범인은 아파트 거실에 설치되어있는 월패드를 타깃으로 선정하여 자동화된 해킹 프로그램을 만들어 범행을 저질렀다. 월패드는 가정의 난방, 조명, 현관문을 제어할 수 있는 IoT 기기로 카메라가 달려있어 사용자의 사생활을 훔쳐 볼 수 있다.

범인은 추적을 피하기 위해 불특정 다수가 많이 사용하는 음식점이나 숙박업소 등 다중 이용시설의 무선공유기를 우선 해킹하여 IP를 우회했다. 우회된 IP로 아파트 단지 내 서버를 해킹해 개인 주거지의 내부 월패드에 침입하였고 월패드를 해킹한 범인은 악성 프로그램을 설치하여 월패드를 통해 집안 불법촬영에 성공하였다. 범인은 8월부터 11월까지 해킹을 시도하였고, 피해 아파트 단지 638곳으로 세대수는 40만4847가구이다[2].

월패드 해킹은 아파트 단지 서버 하나만 해킹하여도 세대주 각각의 월패드를 해킹할 수 있다는 것이 취약점이다. 따라서 대책 방안으로 망 분리가 필요하다. 세대별로 물리적 혹은 논리적인 방법으로 분리해 구성해야 할 필요가 있으며, 또한 네트워크 통신의 데이터를 암호화하고 단말 접속 시 인증 방안을 마련해야 한다[3].

### 1.2 의료기기 해킹 사건

식품의약품안전처가 발표한 자료에 따르면 인슐린을 주입하는 펌프의 설정이 바뀌어 환자에게 인슐린이 과도하게 주입하거나 중단시킬 수 있는 위험이 확인되었다. 또한 이식형 심장박동기 해킹으로 기기의 배터리를 빠르게 고갈시키거나 심장 박동 조정기능을 무단으로 변경할 수 있다는 위험이 발견됐다[4].

의료기기들은 병원의 와이파이로 통신이 되기 때문에 쉽게 해킹될 수 있으며 암호화 되어 있지 않아 더욱 문제가 된다. 사용자의 생명과 직결된 만큼 보안에 더욱 신경을 써야만 한다. 우선 의료기기들의 네트워크 연결을 관리할 관리자가 필요하며, 데이터 암호화와 강한 인증 절차[5]를 통해 접근을 제한 할 수 있도록 하고 소프트웨어의 주기적인 업데이트를 통해 보안을 강화해야 한다.

### 1.3 자율주행 차량 해킹 사건

위 사례는 보안 전문가가 자율주행차량 해킹 시연에 성공한 사례이다. 해킹시연에 성공한 차량은 Jeep Cherokee으로 인포테이먼트 시스템이 탑재된 차량으로 인포테이먼트란 자율주행차량의 주요 서비스 시스템으로 주행과 관련된 정보와 즐길 거리를 동시에 제공하는 시스템이다. 이는 자율주행 차량에서 필수 시스템으로 보안전문가들은 이 시스템을 공략하였다.

고속도로를 주행하는 동안 Jeep의 인포테이먼트 시스템으로 연결되는 휴대전화 네트워크를 통해 자동차에 대한 접근 권한을 획득하였다. 그 외 쉐보레의 U커넥트 엘레매틱스 시스템에서 원격 취약점을 발견했다. 이 또한 모바일 네트워크를 통해 시스템의 접근권한을 얻은 것이다[6].

단순 주행 데이터만 얻은 것이 아니라 와이퍼, 핸들, 깜박이등 자동차의 주요 주행 기능도 해킹이 가능하였기 때문에 인포테인머트 시스템과 주행 기능을 분리해야 하며 해킹 시 운전자를 보호할 수 있는 물리적 방안을 개발할 필요성이 있다.

## III. Conclusions

현재 IoT 기기 해킹은 개인정보 유출과 사생활 유출뿐 만 아니라 사용자의 생사 문제에 직면해 있다. 하지만 현재 출시 되고 있는 IoT은 대부분이 네트워크로 연결되어 있고 사용자의 편리를 위해 기기를 직접 작동하기보다는 컨트롤러를 사용하여 작동 시키고 있다.

따라서, 이러한 연결이 많아질수록 보안 측면에서의 허점은 많아진다. 기계와 컨트롤러의 연결로 작동 된 다면 인증 절차는 더욱 엄격하게 이루어져야 하고, 네트워크로 연결하여 작동하면 데이터를 전달에 하는 과정에서 암호화는 필수이다.

또한 소프트웨어 업데이트로 보안의 취약점을 보호할 수 있기 때문에 주기적인 소프트웨어로 업데이트도 필요하다. 가장 큰 문제점은 IoT 개발 속도에 따라가지 못하는 보안정책 및 체제이다. 국가적 관심을 통해 빠른 보안정책 및 체제를 구축해 나가야 할 것이다.

## REFERENCES

[1] Cho Young-Min “A Study on System Development to Improve IoT Firmware Vulnerability Analysis Efficiency.” Korea Industrial Security Study.April.2022

[2] Wallpad article https://www.hani.co.kr/arti/society/society_general/1072351.html

[3] Jeong Hoon Jeon "A Study on the Response to Smart Home Attacks" The Society of Convergence Knowledge Transactions

[4] Medical Device article https://www.boannews.com/media/view.asp?idx=116851

[5] Lee Young-seok "Certification Method for Safe IoT Environment" Korea Information and Electronics Communication Technology Association. 2015. February

[6] A self-driving car article https://www.ciokorea.com/news/26030