

CONFERENCE PROCEEDINGS MITA 2019

The **15th** International Conference
on Multimedia Information Technology
and Applications (**MITA2019**)

June **27** - July **1**, 2019

VNUHCM-UEL, Ho Chi Minh City, Vietnam

Organized by

Korea Multimedia Society (KMMS), Korea

Vietnam National University-Ho Chi Minh City

University of Economics and Law (UEL), Vietnam

www.icmita.org



Poster Session B

When & Where: June 28, 15:30 ~ 16:30, A Hall Lobby, A1 Building

Chair: Prof. Mikio Hasegawa (Tokyo University of Science, Japan)

- PB-1. Directionality Change Study according to Array Change of Ultrasonic Transducer for Completely in the Canal Hearing Aids** 246
Jin Wan Seok*, Sungdae Na**, Qun Wei*** and Myoung Nam Kim*
*Kyungpook National University, Korea
**Kyungpook National Chilgok University Hospital, Korea
***Keimyung University, Korea
- PB-2. Deep Learning Based Pedestrian Detection Embedded System For Traffic Light Control** 248
Pu-Lum Son* and Joon-Jae Lee*
*Keimyung University, Korea
- PB-3. A Decentralized Copyright Management System Centered on Copyright Holders** 252
Hye-Bin Kim*, ByeongGyu Jeong* and Sang Uk Shin*
*Pukyong National University, Korea
- PB-4. Analysis of Fish Behavior Responses in Chemical Stress Using Permutation Entropy and Fractal Dimension Algorithms** 256
Quach Kha Quang*
*Dong Thap University, Vietnam
- PB-5. Analysis of the Core Technique for Copyright Infringement Sites Tracking and Automatic Evidence Collecting** 259
Seul-Ki Choi* and Jin Kwak*
*Ajou University, Korea
- PB-6. Home IoT Devices and Network Domination with AI Speaker Vulnerabilities** 263
Ju-Seong Ko* and Jin Kwak*
*Ajou University, Korea
- PB-7. PCB Conformal Coating Inspection System** 267
Hyeong-Jo Yoon*, Ndayishimiye Fabrice* and Joon-Jae Lee*
*Keimyung University, Korea
- PB-8. Design of a parking management system with user convenience** 271
Jeong-Min Oh*, So-Jeong Park*, Tae-Seong Yun*, Jeong-Gook Koh* and Tae-Wook Kim**
*Tongmyong University, Korea
**Autonics, Korea

Home IoT Devices and Network Domination with AI Speaker Vulnerabilities

Ju-Seong Ko

ISAA Lab., Dept. of Computer Engineering
Ajou University
Suwon, Republic of Korea
jsko.isaa@gmail.com

Jin Kwak

Dept. of Cyber Security
Ajou University
Suwon, Republic of Korea
security@ajou.ac.kr

Abstract—The number of AI Speakers is expected to continue to grow significantly. AI Speakers have combined various environments and new technologies for the convenience of users, and are being used in several fields. However, vulnerabilities and threats to AI Speakers continue to be reported, and problems arise over their control through vulnerabilities. In this paper, we analyze which vulnerabilities AI Speaker has, how an attacker takes control of AI Speaker by exploit the vulnerability and what threat can be caused in Home IoT network. And we propose requirements for detection system according to characteristics of AI Speakers.

Keywords—Home IoT; AI Speaker; malicious code;

I. INTRODUCTION

Recently, Home IoT services based on IoT devices have been providing various conveniences of life. As user's demand increases and information technology progresses, the services offered by Home IoT are becoming more diverse and life-altering. However, security issues arise as the IoT devices process the private information of users for providing services. Home IoT devices are continuously targeted by various malicious codes from attackers.

A previous attack path of Home IoT network was IoT hub that connects Home IoT network(internal network) and Internet(external network)[1,2]. However, with AI Speakers added to Home IoT, a new attack path through them was created. The vulnerability of the AI Speaker itself enables an attack on the Wi-Fi connection used by Home IoT. In addition to Wi-Fi connection, AI Speakers also use Bluetooth to provide services, which can cause new vulnerabilities in Home IoT.

The number of AI Speakers are expected to increase significantly. According to an analysis, the number of AI Speakers is expected for 142-million devices to be used in 2022 as shown in Fig. 1[3].

With the number of AI speakers considered vulnerable growing significantly, a large number of Home IoT networks are expected to be targeted by the attackers. If breach occurs to the Home IoT network, users can lose control of IoT devices or users' private information may be leaked. So, it is the most important thing to prevent threats before occurring.

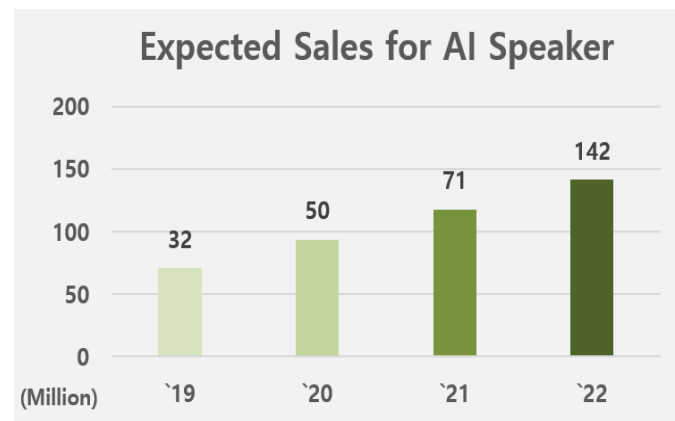


Fig. 1. Prospect of AI Speaker Sales

Therefore, this paper shows how Home IoT network can be dominated by an attacker with AI Speaker vulnerabilities, and proposes a countermeasure based on white-list based detection system.

II. RELATED WORKS

A. IoT devices Breach Incidents

In most of IoT devices breach incidents, the cause was vulnerabilities of the outermost(nearest to Internet) devices in Home IoT network. We show three breach incidents from them.

In 2013, a technology reporter of BBC News reported that Foscam's baby monitoring camera made a strange noise. It was because a hacker took control of the camera. The hacker used just "admin" to log in, and no password[4].

In 2014, Proofpoint analyzed that Home IoT devices were abused for other cyberattacks. Attackers had hacked the devices connected to Internet and sent 750,000 e-mails using Home IoT devices' mailing function. This incident points that vulnerable Home IoT devices can be used to cyberattack[5].

In 2016, Around the world, 73,000 personal CCTVs had been hacked and broadcasted on Internet site. In this incident, the cause is that the users did not change the initial ID and password of the CCTV connected to Internet. Using initial IDs

and passwords, Attackers accessed the CCTVs and collect private information[6].

B. Home IoT Network and Security

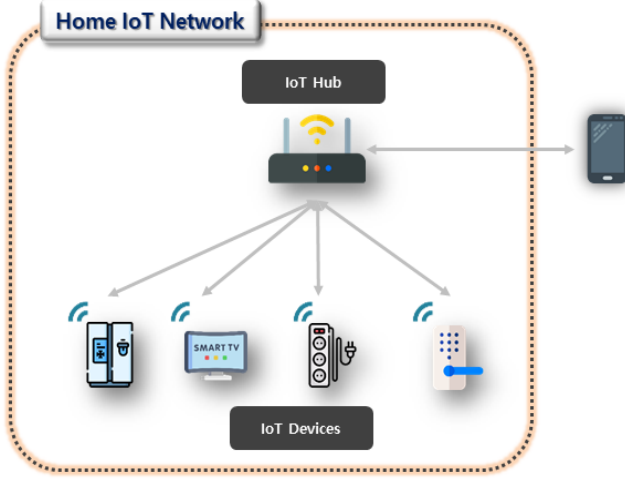


Fig. 2. General Home IoT Network Structure

Fig. 2 shows general Home IoT structure composed of IoT devices and a outermost hub. There are several advantages of using the hub for IoT network, some of which are following[7].

- Data collection and management are fully controlled by the hub device and kept within the Home network.
- A hub splits the Home network to separate traffic, minimized attack surface and protect Home IoT operations.
- A hub may assist with device authentication before authorizing it onto the IoT network.

To access a Home IoT network from external network, it must go through the hub. Therefore, many studies of Home IoT network security are focusing to threats about the hub and a wireless network from the hub[1,2]. But, it could be vulnerable if an attack begins in the network.

C. Vulnerabilities of AI Speaker

There are many concerns about security of AI speaker. The AI speaker supports both Bluetooth and Wi-Fi, but the vulnerabilities from them are continuously reported. Blueborne is one of Bluetooth vulnerabilities. Blueborne allows attackers to leverage Bluetooth connections to penetrate and take full-control over AI speaker. If not connected to Bluetooth, but as long as Bluetooth is on, this attack vector allows attackers to access AI speaker[8]. And on Wi-Fi, there is a KRACK(Key Reinstallation AttaCK) from WPA2 vulnerability. This attack abuses cryptographic protocols to reinstall an already-in-use key. This resets the

key's associated parameters and causes the AP to reinstall the key[9].

Security issues for AI speaker is summarized on below Table 1.

TABLE I. SECURITY ISSUE FOR AI SPEAKER

No.	Security issues	Vulnerability from
1	Blueborne	Bluetooth
2	KRACK	WPA2

D. Abnormal Behavior Detection based on Whitelist

Whitelist-based security policy may be more effective in defending against cyberattacks than blacklist-based one in order to detect abnormal behavior in the restricted internal network. The advantage of a whitelist-based policy is that it allows behaviors from pre-authorized IP addresses, ports, etc. Other behaviors are considered as malicious behavior and not allowed. But even if it's not malicious, behaviors that are not allowed are blocked, which can reduce availability[10].

III. ANALYSIS OF NEW ATTACK PATH

In this chapter, we analyzes new attack path through AI speaker and explains why it is difficult to detect them.

A. New Attack Path from AI Speaker

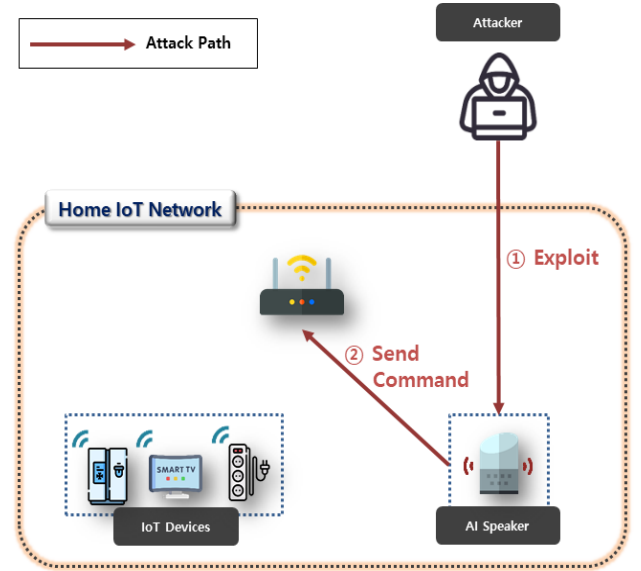


Fig. 3. New Attack Path from AI Speaker

Previous security studies of Home IoT is focused on IoT hub. However, with the addition of AI speaker, a new attack path has been created. The new attack path from AI speaker is composed of exploiting vulnerabilities and sending command to Home IoT network in Fig. 3.

① Exploit vulnerabilities

Attackers exploit the AI speaker with security issues in Table 1, to take control over AI speaker. The key point is that attacker does not go through the IoT hub and access to AI speaker directly.

② Send commands to Home IoT network

And then, attackers send command through IoT hub. the command can be a propagation of malicious code to other IoT devices or data leakage to attackers. The key point is that the packet sent by AI speaker is encrypted, so we cannot detect the attack easily. The encrypted packet is shown in Fig. 4.

B. A Difficulty to Detect Attacks through New Path

	192.168.137.170	TLSv1.2
192.168.137.170		TLSv1.2
	192.168.137.170	TLSv1.2
	192.168.137.170	TLSv1.2
192.168.137.170		TLSv1.2
192.168.137.170		TLSv1.2
192.168.137.170		TLSv1.2

Fig. 5. Encrypted Packets of AI Speaker

Fig. 4 shows some of the packets by AI Speaker (192.168.137.170), which indicates that AI Speaker sends and receives encrypted packets. A packet encryption ensures the confidentiality of communications, but which makes it more difficult to detect abnormal behavior in Fig. 3. The hub only knows the sending and receiving addresses and does not know whether the packet contains malicious contents.

IV. ATTACKS BEGINNING AT AI SPEAKER

Fig. 5 shows attack path and result through an AI Speaker in Home IoT network. Taking control of AI Speaker is equal to dominate the entire network of Home IoT for an attacker. Therefore in Fig. 5, the attacker can send some malicious commands to the hub as a trusted node in the network. The malicious commands are following: malicious code propagation in Home IoT network and data leakage to attacker.

A. Malicious Code Propagation in Home IoT Network

“(A) Propagation” in Fig. 5 is to propagate some malicious codes to other Home IoT devices. If the malicious codes are executed on Home IoT devices, the devices are taken control by the attacker through C&C server. Finally, the devices are dominated and operate malicious activities intended by the attacker.

B. Data Leakage to Attacker

“(B) Data Leakage” in Fig. 5 is to make data to be leaked to an attacker. The AI Speaker and other devices collect and process and the users’ private information. Also, the devices

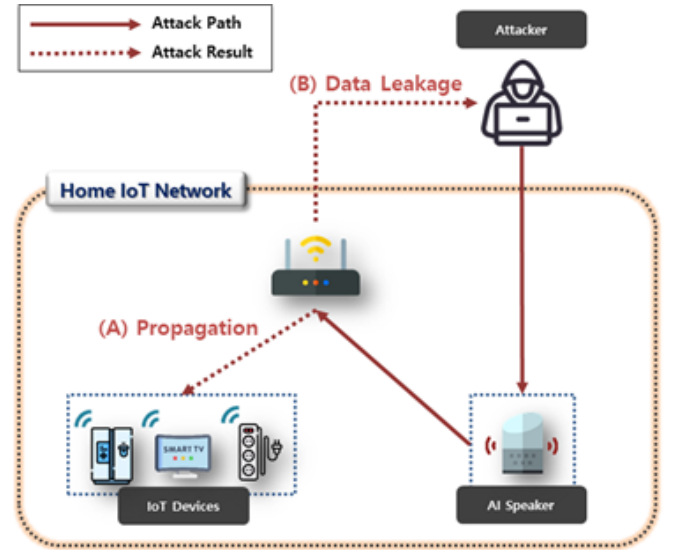


Fig. 4. Attacks Beginning at AI Speaker

may store some configuration information set by user. Normally, the devices process/ information and remove them immediately. But the attacker can modify the process/remove cycle to send information to the attacker. Finally, the attacker can collect users’ private information and configuration information created in IoT Home network.

Occurring damages from attack results in Fig. 5 are summarized on below Table 2.

TABLE II. ATTACK RESULTS AND OCCURRING DAMAGES

Attack Results	Occurring Damages
Propagation	Domination of the entire network and devices’ activities intended by an attacker
Data Leakage	Leakage of private information and configuration information

V. REQUIREMENTS FOR DETECTION SYSTEM

As Home IoT devices deal with users’ sensitive information, protecting threats is important. However in III-B, we pointed that AI Speakers communicate encrypted packets with a receiver. It makes it difficult for Home IoT hub to detect security attacks. As shown in Fig. 5, we can only see the IP address of the sender and receiver, so we have to consist of the detection system with limited information.

A detection system based on whitelist can degrade the availability of the entire network. However in Home IoT network, the devices’ behavior and receiver are fixed, so we can apply the detection system based on whitelist. In this chapter, we propose the requirements to detect security attacks based on whitelist.

A. Whitelist based on Behaviors

In Home IoT network, the IoT devices perform activities to provide a convenience for the users. Therefore, the devices do not open ports not specified in the device’s manual or communicate with other devices through those ports. Not only

the ports, but the activities that the devices perform do not violate the manual. So, we can extract the whitelist of behaviors from device's manual.

B. Whitelist based on IP Addresses

As mentioned it, we can see the IP address of the sender and receiver. In Home IoT network, the IoT devices' communication are targeted: if the device is general IoT device, it communicates with user's controller through IoT hub, or if the device is AI Speaker, it communicates with the other IoT devices and the service provider's server.

If AI Speaker sends malicious command to another IoT device and the device performs the command, the IoT device's activity will be detected by whitelist based on behaviors.

Therefore, we can compose of a whitelist for Home IoT devices' communication targets and detect based on the whitelist.

TABLE III. REQUIREMENTS TO DETECT BASED ON WHITELIST

Based on	Requirements to Detect based on Whitelist
Behaviors	Check the devices' behaviors from the devices' manual
IP Addresses	Check the communicating IP addresses from the devices' characteristic

VI. CONCLUSION

We analyzed a Home IoT network's a new attack path with AI Speaker's vulnerability. With the addition of AI Speaker to the Home IoT network, new vulnerabilities and threats can occur. In a world where the number of AI Speakers is increasing greatly and the generalization of IoT, it is expected to come as a big threat. As the possibility of a threat, we proposed requirements for whitelist-based countermeasure. we need to build an automated internal threat detection system based on these requirements for private networks.

As we analyzed the attack path through AI Speaker, a threat from internal network is difficult to detect and prevent it. In addition to AI Speakers, however, a variety of IoT devices

can be added, and in such cases more threatening channels can be created.

Therefore, in future work, we should develop a threat detection system that can occur in Home IoT network through AI speakers, and eventually build a threat prediction and prevention system that can occur from additional Home IoT devices.

Acknowledgment

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2017R1E1A1A01075110).

References

- [1] Sang-Sik Bang, "A Study on Security Threats and Information Protection in Smart Home IoT Service Environment", Masters dissertation, Konkuk University, Aug 2018.
- [2] Ho-Seok Ryu, "A Study on the Security Architecture for Secure Smart Home System in IoT", Masters dissertation, Ajou University, Dec 2015.
- [3] Maeng Soo Kang, "Smart Speaker Market Treends and Prospects", KDB Industry Technology Research Center, Nov 2018.
- [4] Dave Lee, "Hacker 'shouts abuse' via Foscam baby monitoring camera", Technology report of BBC News, <https://www.bbc.com/news/technology-23693460>, Aug 2013.
- [5] Proofpoint, "Proofpoint uncovers Internet of Things(IoT) cyberattack", <https://www.proofpoint.com/us/proofpoint-uncovers-internet-things-iot-cyberattack>, Jan 2014.
- [6] KISA, "Internet of Things Small Smart Home Appliance Security Guide [for users]", Guide and Manual, <https://www.krcert.or.kr/>, Dec 2016.
- [7] IoT Security Foundation, "IoT Security Architecture and Policy for the Home – a Hub Based Approach", <https://www.iotsecurityfoundation.org>, Nov 2018.
- [8] Ben Seri, Alon Livne, "Exploiting BlueBorne in Linux-based IoT devices", <https://armis.com/blueborne/>, Sep 2017.
- [9] Mathy Vanhoef, Frank Piessens, "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2", the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1313-1328, Nov 2017.
- [10] Jong-Sun Kim, "A study on the implementation of intrusion detection system based on whitelist for substation automation system", Ph.D dissertation, Korea University, Jun 2015.