Journal of Engineering and Applied Sciences 13 (Special Issue 11): 8695-8699, 2018
ISSN: 1816-949X

Analysis of Vulnerability and Security of AI Bluetooth Speaker Connected with IoT

Seung-Woo Kim and Dea-Woo Park
Department of Convergence Science Technology, Hoseo Graduate School,
Hoseo University, Venture, Asan, Korea

Abstract: Utilizing the cloud, AI (Artificial Intelligence) technology combined with the technologies of the 4th Industrial Revolution. AI speaker in IoT (Internet of Things) environment is equipped with speech recognition technology. AI speaker is a tool of voice and music transmission, personal privacy and contents of business use a cloud, AI technology to have a kind of business mechanism. With the popularization of AI speakers in the IoT environment, privacy and work-relatedness are increasing. If a hacking attack occurs on the AI speaker and Bluetooth, the user will not know whether or not his or her device is hacked. In this study, we study the vulnerability and hacking methods of AI speakers in IoT environment and study the security methods for AI speaker and Bluetooth hacking attacks.

Key words: AI speaker, IoT, security, Bluetooth, vulnerability, transmission, acking

INTRODUCTION

The 4th Industrial Revolution is emerging as a revolutionary issue in the whole world including South Korea and active discussions on new technologies and new industries such as VR (Virtual Reality), IoT, ICT (Information and Communications Technologies) and AI are underway. In particular, the voice recognition speaker has begun to receive attention as a product that provides voice recognition technology to the Bluetooth speaker to provide life services such as music, schedule management, IoT and internet search. Major AI speaker products include Amazon Echo, SKT Nugu, Google Home, KT GigaGenie and KakaoMini (Anonymous, 2017). It will continue to be release. As the AI speaker becomes popular, if a wireless hacking attack occurs, the user can not know whether his or her device has been hacked and hacking damage can occur (Baek, 2010).

Therefore, in this study, we have study related concept of AI speaker in IoT environment and overall vulnerability about Bluetooth. And we study security of AI Bluetooth speaker connected with IoT and the security countermeasure against the hacking.

Literature review

AI speaker product trends: The AI speaker is a loudspeaker type with artificial intelligence algorithms based on the cloud internet and offers various services through wired/wireless internet connection. It can be used only by voice recognition without having to manually manipulate various functions such as entertainment (music, radio, etc.,), schedule management, shopping, voice call/message transmission/reception, IoT device control (smart home) is the biggest feature.

In the IoT era, IoT era has become a key device in the smart home era by remotely controlling other home appliances by commanding the speech recognition speaker. The key features of the AI speaker are shown in Fig. 1 with key components summarized K Model AI speak spec (Yang, 2017) in Table 1.

AI speaker vulnerability: In the voice data collected by the AI speaker not only the voice command but also the surrounding voice and conversation with other persons are stored as voice data with many sounds occurring in the same space.

Therefore, if the voice data is badly used for hacking, the personal information of the user may be seriously infringed. A hacker uses malicious code such as a computer virus to leak not only the password but also the financial information and the personal information without the infected person knowing it. Hacked personal information causes financial damage and is used as personal information such as advertisements.

Table 1: K Model AI speaker spec

Product name	K	Power	12 V/2 A
Speaker	2 inch	Output	Rating 7 W
Microphone	4 channel built-in	AUX	3.5 mm stereo
Size/weight	76.6×76.6×110.2 mm/390 g	USB	2.0 (Charge smartphone)
Processor	Cortex A9 quad 1.4 GHz	Bluetooth	4.2+EDR
OS/memory	Android 5.1.1/1G Ram	Wifi	802.11a/b/g/n/ac

Corresponding Author: Dea-woo Park, Department of Convergence Science Technology, Hoseo Graduate School, Hoseo University, Venture, Asan, Korea

BlueBorne (Anonymous, 2018a) Bluetooth security vulnerability: The security company 'Armis' has discovered eight security vulnerabilities in Bluetooth and bundles them into Blueborne. Blueborne is a compound word of Airborne which means Bluetooth and air and Blueborne is a hacking attack that uses Bluetooth wireless communication to hack.

There are three conditions to attempt a Blueboot attack using this vulnerability. First, a smartphone with Bluetooth enabled and secondly, a hacker within the range of Bluetooth communication (within about 10m). Third, it should be a smartphone that is not updated with Bluetooth security patch (Anonymous, 2018b).

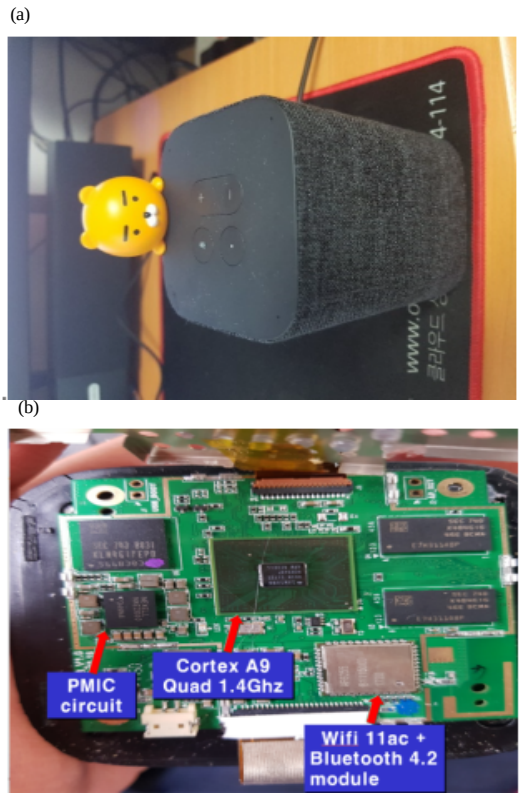

Fig. 1: AI speaker K Model and disassembly

File transfer in Bluetooth: When a file is transmitted from the transmitting apparatus to the receiving apparatus, the transmitting apparatus inputs the pin number together with the pair request. When a pair request is received from the receiving apparatus, a value equal to the pin number input from the transmitting apparatus is input and the pairing is performed, thereby ensuring the transmission reliability between the two apparatuses. After the pairing is done, if the data is transmitted from the transmitting device, due to the characteristics of the Windows operating system, analysis and improvement of security vulnerability when data is transmitted in the Bluetooth environment related research enter the device layer from the application layer and transmit to the receiving device through the RFCOMM driver do. The receiving device receives data from the RFCOMM driver in the device layer and enters the application layer. Thus, the security of the mutual authenticated transmission interval is provided by the pin number but the security at the adaptation layer, the device layer and the device is weak. The overall file transfer in Bluetooth is shown in Fig. 2.

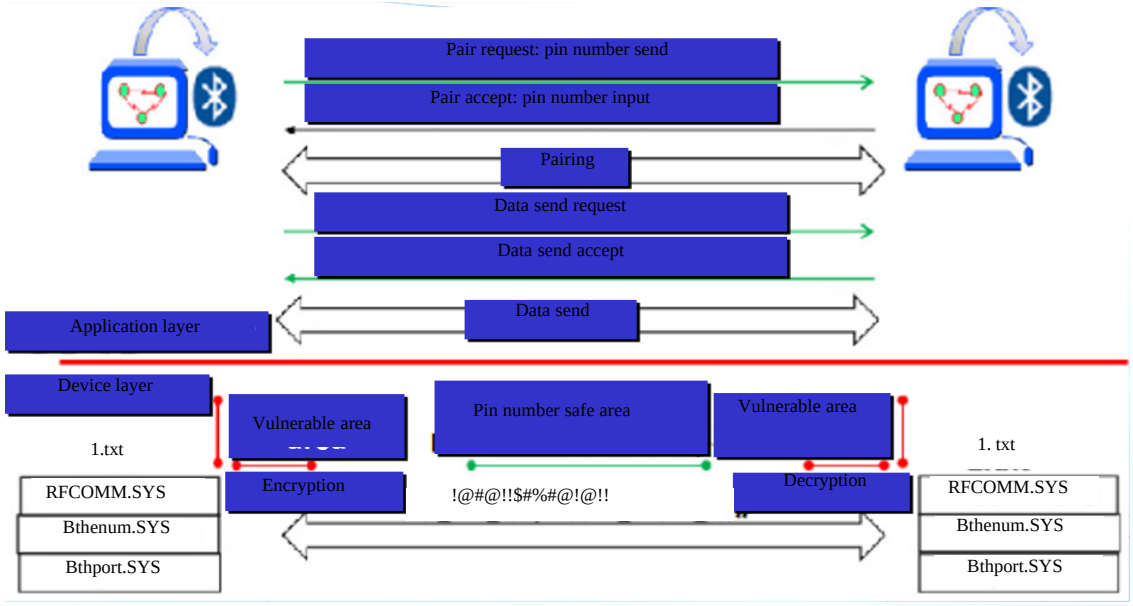

Fig. 2: Bluetooth connection and file transfer

MATERIALS AND METHODS

AI speaker security vulnerability analysis

AI speaker company's voice information management status: It is summarized in Table 2, that all the sound is gathered through the speaker microphone even before the AI speaker call, the voice information should be provided when the information of the police investigation (law enforcement agency) is requested and the personal information can be leaked by the external hacking or internal office personnel.

Experiments and vulnerability analysis: The test environment operating system in KaliLinux was used as an attack tool in Table 3 to identify vulnerable sections between Bluetooth file transfers and a BLE sniffer Bluetooth USB module was connected to Fig. 3 for sniffing.

Bluetooth hacking tools: There are three tools to test: Kali Linux.

Hciconfig: It is a utility for Linux commands that are used to interact with Bluetooth devices. Figure 4 shows the Bluetooth interface name, MAC address and the amount of packet data sent and received.

Hcitool: It can try to connect to the Bluetooth stack and Fig. 5 can scan for Bluetooth devices. It can also use the inq option to get more information about Bluetooth.

Sdptool: Figure 6 is a tool that can display and check the services running on the Bluetooth device based on the information collected using the hciconfig and hcitool tools.

(a) (b)

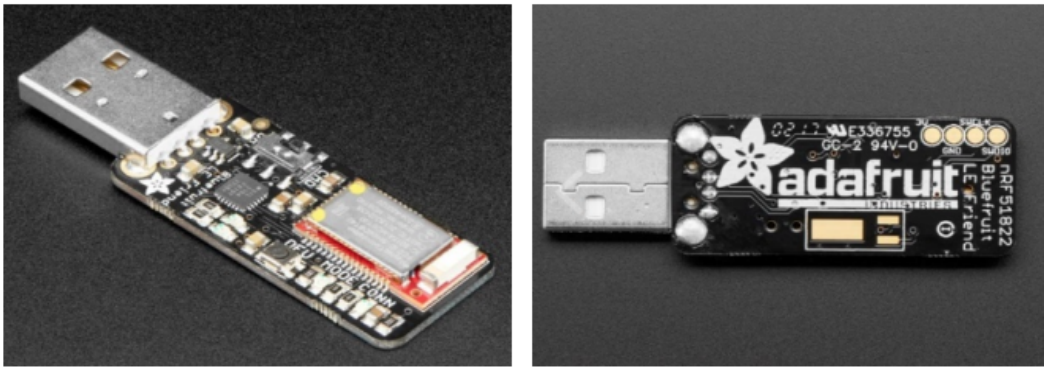

Fig. 3: Bluefruit LE Sniffer-Bluetooth Low Energy (BLE 4.0)-nRF51822 V.3.0 a and b

```
root@kali:~# hciconfig
hci0:   Type: Primary  Bus: USB
        BD Address: E8:2A:EA:55:14:E5  ACL MTU: 8192:128  SCO MTU: 64:128
        UP RUNNING
        RX bytes:13443 acl:48 sco:0 events:244 errors:0
        TX bytes:2073 acl:48 sco:0 commands:98 errors:0
```

Fig. 4: Hciconfig

```
root@kali:~# hcitool scan
Scanning ...
        0C:1C:20:06:11:C5       7104
        00:01:95:18:2A:D5       n/a
root@kali:~# hcitool inq
Inquiring ...
        0C:1C:20:06:11:C5       clock offset: 0x0000    class: 0x2c0414
```

Last 4 digits of the serial number

Fig. 5: Hcitool scan, hcitool inq

Fig. 6: Sdptool

Table 2: AI speaker's voice(user data) storage management status

Division	Naver (Clover)	Kakao (Kakaomini)	Sktelecom (Nugu)	KT (Giga genie)
Listen to the call	○	○	○	○
Keep before call	△	×	×	×
Post-call archiving	○	○	○	○
Provide information	User: × Police: △	User: ○ Police: ○	User: × Police: ○	User: ○ Police: ○

Table 3: Attack tool

Division	Contents
Software	Kali Linux 64 bit Ver. 2018.2
Hardware	Lenovo Thinkpad x240(i5-4300 u, 8G)
	Bluefruit LE Sniffer-nRF51822 V3.0

RESULTS AND DISCUSSION

AI speaker security countermeasure in iot environment Security guide line: Companies are provided to restrict the collection of voice data, to archive and manage it and to be requested by an investigative agency. Nevertheless, companies that introduced AI speakers still do not give users guidance on when, how they are collected and how long they are archived. Governmental guidelines such as information gathered through AI speakers, processing methods and accessibility of employees are required. Excessive regulations should be eased but new discussions on privacy laws created based on past standards are need.

Bluetooth security countermeasures: Install and check 'Blueborne Scanner' on Google Play. If you install the BlueBorne Scanner and scan it and it says 'Your device is vulnerable', you can get a blueborne attack. Even if you are aware of this problem, users will be exposed to security vulnerabilities unless smartphone manufacturers provide Blueborne security patches.

Bluetooth off when not in use: The easiest way is to turn off Bluetooth when not in use. Also, Bluetooth can be used as a target for long-term music in one place. Bluetooth communication distance is 10 m, it can be used in places where there is no person but it can be a target of hacking if it is used for a long time without moving in a public place or a lot of cafes.

CONCLUSION

In this study, we study the technical attacks of AI speakers using Bluetooth, analysis the vulnerabilities of AI speakers and suggest security solutions. The IoT environment is becoming popular but there is a lack of security awareness and the majority of people are exposed to hacking.

In addition, companies that have introduce AI speakers have yet to provide users with guidance on when how and how long voice information was collected. Governmental guidelines for information and processing methods collected through AI speakers, employee access rights and voice information requests from investigative agencies are needed. As the market for AI speakers will gradually increase, we need to be aware of this and prepare countermeasures. In this study, we study improve the security awareness of AI speakers in IoT environment.

REFERENCES

Anonymous, 2017. Problems and improvements of Artificial Intelligence (AI) appliances. Korea Consumer Agency, Korea.

Anonymous, 2018a. The attack vector BlueBorne exposes almost every connected device. Armis, Inc., Palo Alto, California. https:// armis. com/blueborne/

Anonymous, 2018b. [The Heikacao app is an application that helps you set up your cacao mini and cacao AI devices]. Kakaomini, Internet, Korea. https: // kakao. ai/product/kakaomini. (In Korean)

Baek, J.K., 2010. A Study of Security Vulnerability in Bluetooth Environment. Soongsil University, Seoul, South Korea,.

Yang, E.H., 2017. Intrusion Detection and Analysis in Wireless Network Environment. Hanseo University, Seosan, South Korea,.