A Forensic Data Analysis of a Bluetooth Device paired with an Android-based Audio Video Navigation System

Keonyong Lee
dept. of Applied Computer Engineering
Dankook University
Yongin-si, South Korea
lky9620@dankook.ac.kr

Hojun Seong
dept. of Computer Science & Engineering
Dankook University
Yongin-si, South Korea
hohojun0930@dankook.ac.kr

Haein Kang
dept. of Software Science
Dankook University
Yongin-si, South Korea
hikang@dankook.ac.kr

Seong-je Cho
Dept. of Software Science
Dankook University
Yongin-si, South Korea
sjcho@dankook.ac.kr

Hyoil Han
School of Information Technology
Illinois State University
Normal, IL, USA
hhan12@ilstu.edu

Kyoungwon Suh
School of Information Technology
Illinois State University
Normal, IL, USA
kwsuh@ilstu.edu

***Abstract*—Recently autonomous vehicles and connected cars are being equipped with various information and communication technology (ICT). The installed ICT on such vehicles and cars makes it possible to record events generated during communication between the built-in ICT module and the driver's mobile phones and driver's activity information. For example, the Audio Video Navigation (AVN) system, an ICT module, interacts with drivers and provides convenient features to drivers. AVN can be connected to a driver's mobile device, and it can be used to store various driver-specific real time information such as driving records, phone call records, SMS, and music playback events. In this paper, we collect and analyze the digital data stored in an AVN installed in a KIA K5 sedan. Most of the analyzed data is related to the activities initiated from the mobile device connected to the AVN via Bluetooth. The result of our research reported in this paper can be useful for the forensic data analysis of vehicles.**

Keywords—Vehicle Forensics, Audio-Video Navigation (AVN), Android, Bluetooth

I. INTRODUCTION

According to the World Health Organization (WHO), traffic accidents across the world result in the death of 135 million people per year and the number is increasing every year. They expect that by the year 2030 traffic accidents will be ranked 5-th for major causes of deaths in the world [1]. Accordingly, there are growing interests in research on identifying the causes of traffic accidents and the responsible party for each accident [2,3].

Recently the growing number of autonomous vehicles and connected cars are equipped with various information and communication technology (ICT) [4]. This trend requires that new hardware modules such as Engine Control Unit (ECU), Transmission Control Unit (TCU), Event Data Record (EDR), Audio-Video Navigation (AVN), and Dashboard Camera (DashCam) be installed as major components in the vehicles that automakers are manufacturing. These new hardware modules installed in the cars record various event information including driver's behavior, and can be used in vehicle forensics [3,5,6].

Audio Video Navigation (AVN) is known as a representative product of IVI (In-Vehicle Infotainment) or ICE (In-Car Entertainment). In general, AVN provides various convenient features to a driver of a vehicle while interacting with the driver. More specifically, most of the AVNs installed in vehicles nowadays first get connected with a driver's mobile device via a Bluetooth connection or USB connection[7,8] and then provides various functionalities such as phone calls, SMS, and audio and video media playback[9]. While providing these functionalities, AVNs record information about events related to each functionality. Such event information recorded by the AVN can be potentially useful for identifying the causes of traffic accidents and the responsible party for each accident.

In this paper, we propose a methodology to use the event information recorded in an AVN, which is connected to a mobile phone via Bluetooth, for vehicle forensics. As a case study, we have chosen a Kia K5 as our vehicle, and the factory installed AVN and analyzed the event information that we could collected from the AVN. Among various AVN data that we could collect from K5 AVN. We analyzed the event data related to the interactions between the AVN and a mobile device connected to the AVN via Bluetooth. More specifically, we compared the event data collected from the AVN with the packets collected from the communication between the AVN and the mobile device.

This paper is organized as follows. Section 2 presents the strategy of collecting data and the findings from the data according to artifacts. Section 3 describes the data analysis of the collected artifacts between the AVN and a mobile device connected via Bluetooth. Finally, conclusions and future work are discussed in Section 4.

II. COLLECTING USER DATA IN ANDROID OS-BASED AVN

This section describes the procedure of collecting data stored in the Android OS-based AVN system. The AVN from a Kia K5 automobile was used in this experiment, and its detailed specification appears in "TABLE I".

TABLE I. KIA K5 AVN'S SPECIFICATION

Manufacturer	LG Electronics
OS	Android 4.2.2 (Jelly bean)
File System	Ext4
Vehicle	Kia K5(2015)
Processor	ARM v7
Chipset	Telechips TCC893x
Kernel version	3.1.10-tcc

To collect data from the Android OS-based AVN, we first started a specific engineering mode, selected the Android setting menu, and activated the Developer Option. Next, we started USB Debugging and obtained an Android Debugging Bridge (ADB) shell through a USB connection.

In the Android system, the root privilege is required to access '/data partition,' which contains the user information. For this, a rooting process is required to access the root privilege. However, acquiring a custom recovery necessary for rooting was not possible. Therefore, we reached the AVN's root shell by exploiting the "Dirty Cow (CVE-2016-5195) [10]" vulnerability.

The Dirty Cow vulnerability is a vulnerability that offers write permission to the Read-Only memory area of the Linux Kernel by using a race condition. The Android system is developed based on the Linux Kernel. Therefore, we can exploit this vulnerability of the Linux Kernel to escalate privileges and acquire the root shell.

After reaching the root shell, we acquired the images of a disk drive in the ADB shell of the AVN. The usage information of a user resides in the low level of /data in the acquired image. "TABLE II" shows the data location of the primary artifacts.

TABLE II. FILE LOCATION OF PRIMARY ARTIFACTS

Artifacts	File Location
Bluetooth Logs (Bluetooth History)	/data/data/com.android.provider.bluetooth
Media Play from USB	/data/data/com.android.providers.media
DMB History	/data/data/com.lge.ivi.dmb
Navigation Logs	/data/data/com.mnsoft.navi

III. ANALASYS OF THE COLLECTED USER DATA

Among the data collected in Section II, we mainly analyzed the data recorded by the Bluetooth communication after the AVN communicated with the mobile device.

The communication information between the AVN and mobile device through the Bluetooth connection is stored in the directory named "/data/data/com.android.provider. bluetooth" of the AVN. The primary artifacts are the MAC address (Media Access Control Address) of the mobile device, device name, phone book, recent phone record, etc.

Since the related information is stored in SQLite format with the extension .db, we analyzed the data by using an open-source forensic tool named "Autopsy [12]," which is used for analyzing "DBbrowser For SQLite [11]" and Android images.

A. MAC Address of Mobile Device connected to Bluetooth

"TABLE III" shows the location and file name that record the Bluetooth MAC address of the mobile device and (2) table names and their corresponding attributes, when an AVN is connected to a mobile device via Bluetooth.

TABLE III. INFOMATION OF THE MOBILE DEVIC CONNECTED TO AVN

Location and File name	Name of DB Table	Attribute
/databases/BTSetup.db	BTDevList	Address
/databases/BTContacts.db	Switch_index	dev# _name
/databases/BTFavorites.db	Switch_index	dev# _name
/databases/BTCallHistory.db	Switch_index	dev# _name

"Fig. 1" shows that the MAC address of a mobile device is recorded in the address attribute of the BTDevList table in the /databases/BTSetup.db file.

Fig. 1. Bleutooth MAC address of connected mobile device in BTDevList

For the KIA K5 automobile used in our study, the number of mobile devices that can be simultaneously connected to the KIA K5 is up to five. Therefore, the number of tuples in the BTDevList is five.

Additionally, the Bluetooth MAC address of the mobile device is recorded in the property 'dev#[index]' of the Switch index table in the files named BTCallHistory.db, BTContacts.db, and BTFavorites.db, which are in the /databases diirectory. (Refer to "Fig. 2".) The Bluetooth MAC address shown in Switch_index has the same value for each index order as the Bluetooth MAC address previously checked in the BTDevList table of the BTSetup.db file.

Fig. 2. Bleutooth MAC address of connected mobile device in Switch index

B. Device Name of Mobile Device connected to Bluetooth

The name of the mobile device connected to the AVN system is recorded in the devname property of the BTDevList table in the /databases/BTSetup.db file (Refer to "Fig. 3".).

The Bluetooth device name such as "[User Name]'s IPhone" or "[User Name]'s Galaxy S##" is assigned to a mobile device. Since such a Bluetooth device name is recorded in the devname property, as shown in "Fig. 3", it can be used to locate the user's name of a mobile device.

Fig. 3. Bleutooth device name of connected mobile device in BTDevList

C. Phonebook of Mobile Device connected with Bluetooth

The phone book of the mobile device that is connected to the AVN is stored, as shown in "Fig. 4". The Dev#[index]Contacts table in the /databases/BTContacts.db file contains the information related to the phone book according to the device index, the user's name, the phone number, and the type of phone numbers.

Fig. 4. PhoneBook of connected mobile device in BTContacts.db

"Fig. 5" shows the format for transmitting the phone book from a mobile device to AVN. This phonebook transmitting format is the vCard (version 2.1) [13] form. When the phonebook of a mobile device is transmitted, it includes the stored name, phone number, and type of phone number for each phone number. is transmitted. The distinct names (version, FN (Formatted name), Tell Type, etc.) of these vCard formats are represented as similar properties (vcard_version, name, fname, num1_type) in the Dev#[index]Contacts table.

```
BEGIN: VCARD
VERSION: 2.1
FN;CHARSET=UTF-8: "Mike"
TEL;CELL: 01000000000
END:VCARD
```

Fig. 5. vCard(v 2.1) Format for transmitting PhoneBook

D. Recent Calls of Mobile Device connected to Bluetooth

"Fig. 6" shows the recent communication information between the AVN and a mobile device via a Bluetooth connection. The recent communication information is stored in the Dev#[index]CallHistory table of the /databases/BTCallHistory.db file in the AVN and includes information such as communication types (Dialed, Received, and Missed), the name recorded in the phonebook, the type of the phone number, the phone number, the duration of communication, etc., which appear according to the index of the mobile device.

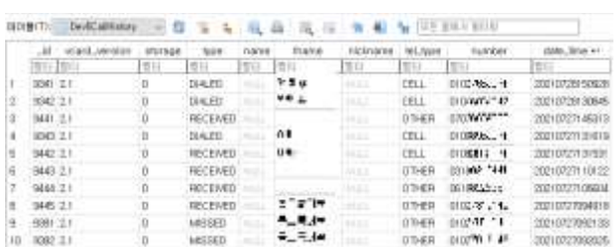

Fig. 6. Recent Call of connected mobile device in BTCallHistory.db

"Fig. 7" shows the format of the vCard (version 2.1) form, which is used in transmitting the recent communication information from a mobile device to the AVN. The information is obtained by analyzing the Bluetooth packet captured in the transmission between the AVN and the mobile device. The transmitted data includes the recorded name and phone number, the type of the phone, the type of communication, the duration of the communication, etc. The vCard form includes the version, FN (Formatted name), Tell type, number, and Datetime, which are similar to the properties such as vcard_version, type, name, tel_type, number, and date_time in the Dev[index]CallHistory table.

```
BEGIN: VCARD
VERSION: 2.1
FN;CHARSET=UTF-8: 김박사
TEL;VOICE:01000000000
DATETIME;
```

Fig. 7. vCard(v 2.1) Format for transmitting Call Log

IV. Conclusion

This paper studies the collection and analysis of the communication data between a KIA K5 and a mobile device via a Bluetooth connection. The findings from the collected data are the artifacts such as Bluetooth records (the connected mobile device's MAC address and name), phone book, recent communication records, etc., which we analyzed.

As shown in "TABLE II" in Section 2, we found various artifacts related to a user's behavior that can be used in forensics and further investigation. We plan to investigate navigation records, DMB records, and media usage. We also plan to build automated tools for AVN data analysis that can be used for AVN forensics.

Acknowledgment

"This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Science and ICT (no. 2021R1A2C2012574), also supported by Research Program funded by the Supreme Prosecutors' Office of the Republic of Korea (SPO), and supported by the MSIT(Ministry of Science and ICT), Korea, under the National Program for Excellence in SW)(2017-0-00091) supervised by the IITP(Institute of Information & Communications Technology Planning&Evaluation) in 2021"

References

[1] WHO(World Health Organization), "Road traffc injuries", (https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries)

[2] M. Cebe, E. Erdin, K. Akkaya, H. Aksu and S. Uluagac, "Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles," in *IEEE Communications Magazine*, vol. 56, no. 10, pp. 50-57

[3] Nhien-An Le-Khac, Daniel Jacobs, John Nijhoff, Karsten Bertens, Kim-Kwang Raymond Choo, Smart vehicle forensics: Challenges and case study, Future Generation Computer Systems, Volume 109, 2020, Pages 500-510

[4] Gonzalo De La Torre, Paul Rad, Kim-Kwang Raymond Choo, Driverless vehicle security: Challenges and future research opportunities, Future Generation Computer Systems, Volume 108, 2020, Pages 1092-1111

[5] H. Mansor, K. Markantonakis, R. N. Akram, K. Mayes and I. Gurulian, "Log Your Car: The Non-invasive Vehicle Forensics," 2016 IEEE Trustcom/BigDataSE/ISPA, pp. 974-982

[6] J. Moos G. Davies, E. Lewis, N. Williams, B. Gichohi, R. Lane, and A. Bellany, "Digital forensics for automobile systems: The challenges and a call to arms," Int. Journal of Forensic Sciences, Jun. 2016.

[7] A. Mourad, S. Muhammad, M. O. Al Kalaa, H. H. Refai, and P. A. Hoeher, "On the performance of WLAN and Bluetooth for in-car infotainment systems," Vehicular Communications, Volume 10, pp.1-12, 2017

[8] R. Nusser and R. M. Pelz, "Bluetooth-based wireless connectivity in an automotive environment," Vehicular Technology Conference Fall 2000. IEEE VTS Fall VTC2000. 52nd Vehicular Technology Conference (Cat. No. 00CH37152), Vol. 4, pp.1935-1942

[9] L. Lu, S. Li and Y. Li, "Design of car Bluetooth hands-free mobile phone system in Linux system," International Conference on Automatic Control and Artificial Intelligence (ACAI 2012), pp.836-839

[10] CVE-2016-5195,https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2016-51

[11] DB Browser For SQLite, https://sqlitebrowser.org/

[12] Autopsy, https://www.autopsy.com/

[13] vCard, "The Electronic Business Card, Version 2.1", A versit Consortium Specification,