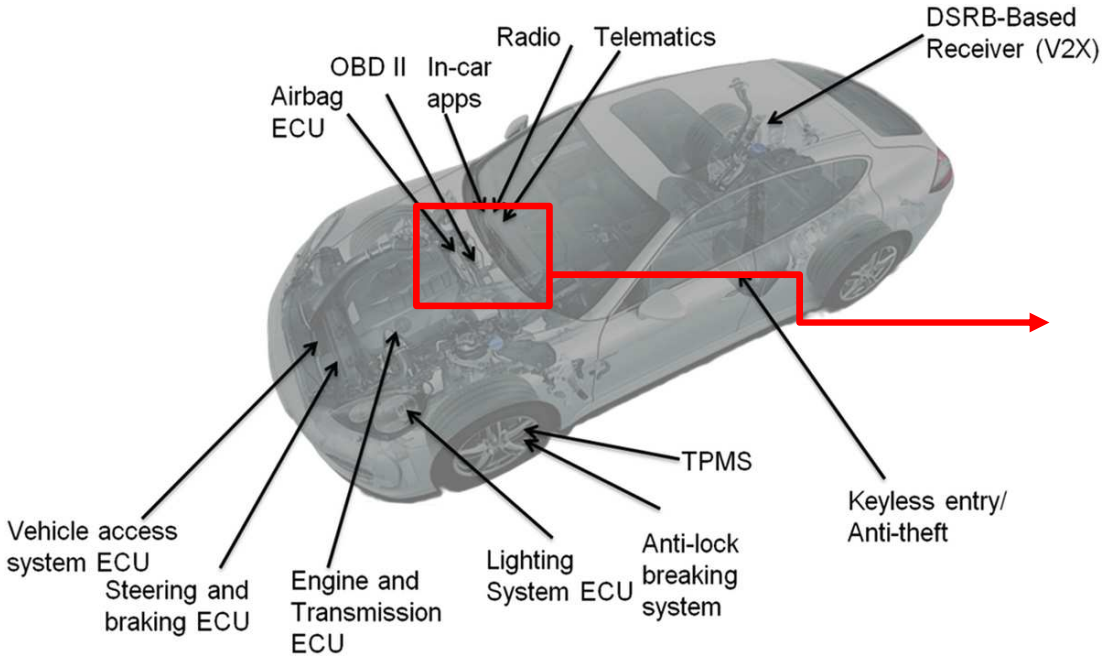
A Forensic Data Analysis of a Bluetooth Device paired with an Android-based Audio Video Navigation System

Keonyong Lee, Hojun Seong*, Haein Kang**,
Seongje cho,* Hyoil Han***, Kyungwon Suh***
Dept. of Applied Computer Engineering, Dankook University
*Dept. of Computer Science & Engineering, Dankook University**
*Dept. of Software Science, Dankook University***
*School of Information Technology, Illinois State University****

Presenter
Haein Kang

Introduction

- The number of traffic accidents in the death is increasing every year, Accordingly, there are growing interests in research on Car Forensics.
- Recently, Car trend(connected car, Self-driving) requires that new hardware.
  - Engine Control Unit(ECU), Transmission Control Unit(TCU), Audio-Video Navigation(AVN) record various event information including driver's behavior
- Specially, AVN provides various convenient features to a driver.
  - Usually, driver pairs own mobile device to AVN via Bluetooth to using convenient features(Call, Play music, SMS etc…)



Collecting User Data in Android OS-Based AVN

- Target : KIA K5(Android 4.2.2, Jelly Bean)
- To collect from Android OS-based AVN, we obtained an ADB(Android Debugging Bridge) shell through USB connection
- To access userdata(/data) in android OS, we should obtain root privilege shell
  - No way for rooting Android OS based AVN System(Custom Recovery, Tool etc..)
  - Because Android developed on the Linux Kernel, We can exploit the vulnerability of the Linux Kernel to escalate privileges (CVE-2016-5195, Dirty-CoW)
- Finally, We acquired various artifacts(Bluetooth log, Media, DMB, Navigation) from userdata(/data) section

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

Analysis of the collected user data

- We mainly analyzed the data recorded by Bluetooth pairing between AVN and user mobile device
- The userdata stored in the directory name “/data/data/com.android.provider.bluetooth” of the AVN system image
- We obtained various artifacts about Mobile Device Connected to Bluetooth
  - Mac Address, Device Name, Phone Book, Recent Call History
- Because artifacts stored .db file format, we used “DB browser for SQLite” tool

Artifacts	Location and File name	Table	Attribute
Mac Address of Mobile Device Connected to Bluetooth	/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
Device Name of Mobile Device connected to Bluetooth	/databases/BTSetup.db	BTDevList	devname
Phonebook of Mobile Device connected with Bluetooth	/databases/BTContacts.db	Dev#contacts	-
Recent Call of Mobile Device connected with Bluetooth	/databases/BTCallHistory.db	Dev#CallHistory	-

Analysis of the collected user data(Example)

- MAC Address, Mobile Device Name of Mobile Device Connected to Bluetooth

Table BTDevList | 5 entries | Page 1 of 1 | Export to CSV

_id	devname	address	status	a2dp_st...	avrcp_s...	priority
62	iPhone ([redacted])	6C:AB:31:[redacted]	0	0	0	0
63	iPhone ([redacted])	3C:2E:FF:[redacted]	0	0	0	0
65	[redacted]	34:A8:EB:[redacted]	0	0	0	0
66	갤럭시 노트 10	74:9E:F5:[redacted]	0	0	0	0
68	[redacted]의 Galaxy S21	78:46:D4:[redacted]	2	2	0	1

- Recent Call of Mobile Device Connected to Bluetooth

테이블(T): Dev5CallHistory | 모든 열에서 필터링

	_id	vcard_version	storage	type	name	fname	nickname	tel_type	number	date_time
	필터	필터	필터	필터	필터	필터	필터	필터	필터	필터
1	9341	2.1	0	DIALED	NULL	[redacted]	NULL	CELL	0102[redacted]	20210728150928
2	9342	2.1	0	DIALED	NULL	[redacted]	NULL	CELL	0104[redacted]	20210728130845
3	9441	2.1	0	RECEIVED	NULL		NULL	OTHER	070[redacted]	20210727145313
4	9343	2.1	0	DIALED	NULL	[redacted]	NULL	CELL	0108[redacted]	20210727131619
5	9442	2.1	0	RECEIVED	NULL	[redacted]	NULL	CELL	0108[redacted]	20210727131531
6	9443	2.1	0	RECEIVED	NULL		NULL	OTHER	0318[redacted]	20210727110122
7	9444	2.1	0	RECEIVED	NULL		NULL	OTHER	0618[redacted]	20210727105604
8	9445	2.1	0	RECEIVED	NULL	[redacted]	NULL	OTHER	0102[redacted]	20210727094918
9	9391	2.1	0	MISSED	NULL	[redacted]	NULL	OTHER	0102[redacted]	20210727092133
10	9392	2.1	0	MISSED	NULL	[redacted]	NULL	OTHER	0102[redacted]	20210727092025

Conclusion

- We studies the collect and analysis of the communication data between KIA K5 and mobile device via Bluetooth connection
- Except Bluetooth connection history artifacts, other various artifacts exists
- We plan to investigate Navigation record, DMB records, and media usage
  - Also, plan to build automated tools for AVN data analysis

Thank You !

"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"