Practical Methodology for In-Vehicle CAN Security Evaluation

Hyun-Bae Park[1], Yongeun Kim[1], Jaeseok Jeon[1], Hee Seok Moon[1], and Samuel Woo[2*]
[1]Korea Automotive Technology Institute, Cheonan, Korea
{hbpark, kimye, jsjeon, hsmoon}@katech.re.kr
[2]Electronics and Telecommunications Research Institute, Daejeon, Korea
samuelwoo@etri.re.kr

Abstract

Modern vehicles are equipped with a variety of Electrical and Electronic (E/E) systems for the convenience of a driver. However, with the increasing use of Electronic Control Units (ECU) to mount vehicular E/E systems, the cyber threats are also increasing. Vehicular security is a very important function which is directly connected to lives of drivers and passengers. Hence, modern vehicles should be provided with an information security function. In case that autonomous vehicles are commercialized in the future, an evaluation methodology will be needed to check if vehicles are normally provided with an information security function. In this paper, we propose a security evaluation methodology and tool that can analyze the security level of In-vehicle network without the information provided by the vehicle manufacturer. The proposed evaluation methodology is designed based on four types of attacks that can be performed on In-vehicle Controller Area Network (CAN). In addition, we design and develop the evaluation tool that can measure changes in vehicle conditions using various sensors. Finally, we conduct experiments using actual vehicles to evaluate the effectiveness and accuracy of the proposed method. The proposed methodology and tool enable us to analyze security level of In-vehicle network very easily and fast.

Keywords: in-vehicle CAN security, security evaluation, automotive security, in-vehicle CAN penetration test

1 Introduction

The modern vehicles are loaded with various kinds of electronic control units (ECUs). ECUs are used to establish a lot of security and convenience functions. Communication protocols like Controller Area Network (CAN), local interconnect network (LIN) and Flexray are being used for efficient communication among ECUs[8]. However, communication protocols for In-vehicle network have no information security function[18]. Along with the accelerated electronization of vehicles, various kinds of security threats which occurred in the existing Information and Communications Technologies (ICT) environment are also occurring in a vehicular environment. Particularly, hacking researches on forced control of a vehicle using vulnerabilities of In-vehicle network are being published continually. For these reasons, there is a growing interest in vehicular security[21]. Recently, a working group in WP.29 is researching on the development of vehicular security guidelines and evaluation standards [17]. However, without full understanding of a manufacturing process of a vehicle, it is very difficult to define security evaluation standards. In addition, it is also difficult to define essential information to be acquired from vehicle makers for the evaluation of security.

Journal of Internet Services and Information Security (JISIS), volume: 9, number: 2 (May 2019), pp. 42-56

*Corresponding author: Hyper-connected Communication research Laboratory Information Security Research Division Network Security Research Section, ETRI, 34129 218 Gajeongno Yuseong-gu, Daejeon, 34129, South Korea, Tel: +82-10-5654-5911

In this paper, we propose a methodology for the security level evaluation which can be done even without specific information given by vehicle makers. We design the methodology based on the four types of cyber attacks that occur most frequently in the In-vehicle environment. We also design and develop the evaluation tool for automatically checking a change of vehicular state while conducting the four type of attacks. The three sensors used to make the evaluation tool are image sensor(can detect a change of a dashboard automatically), sound sensor(can detect a sound from a vehicle so identify a point of time when abnormal symptoms happen), and vibration sensor (can detect micro-movement or vibration occurred from a vehicle). We conduct experiments using actual vehicles to evaluate the effectiveness and accuracy of the proposed methodology and tool. Through experiments, we confirmed that the security of In-vehicle networks can be evaluated using the proposed methodology. The main contributions of this paper are as follows.

- We defines items of Penetration test which should be conducted when evaluating security of In-vehicle CAN. The four kinds of items are as follows: First, Denial of Service attack. Second, data frame replay attack. Third, Fuzzing attack. And fourth, impersonation attack.
- We propose a security assessment methods that can be performed without the information provided by the vehicle manufacturer.
- We have design and develop the evaluation tool that can measure changes in vehicle conditions using various sensors. We fabricate a semi-automated evaluation tool using the three type of sensors (sound, video, and vibration).
- We conduct experiments using actual vehicles to evaluate the effectiveness and accuracy of the proposed methodology and tool.

The composition of this paper is as follows. Firstly, we describe basic the background knowledge of In-vehicle network. Then, the related works are explored. In Section 4, we introduce the security evaluation methodology and environments. Section 5 discusses the results of the use case. Finally, we reach the conclusion in Section 6.

2 Background

2.1 Automotive E/E Architecture

The newest vehicles are loaded with various kinds of ECUs. More than one ECU assemble and compose subsystems. Representative subsystems include Powertarin, Chassis, Body, Infortainment and so forth(The safety system comes under the Chassis system) [6]. Table 1 shows communication protocols used by each subsystem.

Kind	**Communication Protocol**
Powertrain	High Speed CAN, FlexRay, CAN-FD
Chassis	High Speed CAN, FlexRay, CAN-FE
Body	Low Speed CAN, LIN
Infortainment	MOST, Ethernet

Table 1: In-vehicle network communication protocols

Subsystems use communication protocols like CAN, LIN, FlexRay, Media Oriented Systems Transport (MOST), Ethernet to establish a communication environment among ECUs. In general, core subsystems of a vehicle construct a sub network environment using CAN [14]. In-vehicle Network is organized as shown from Figure 1.

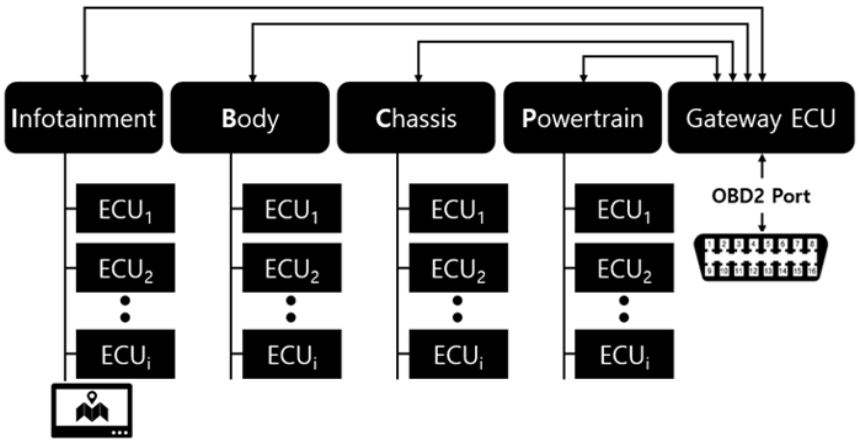

Figure 1: In-vehicle network environment

2.2 In-vehicle Network and Controller Area Network

2.2.1 In-vehicle Network Protocol

Introduction of CAN Bus system allowed car makers to dramatically reduce the complexity of a communication line. Hence, CAN was designated as ISO standard in 1993 and has been used most frequently for construction of In-vehicle network for the past 20 years. However, recently, rapid development of automobile-IT convergence is calling for a communication protocol faster than CAN .

The FlexRay protocol was developed to solve limitations of CAN. FlexRay offers a data transmission rate faster than CAN [15]. Furthermore, it can transmit a larger amount of data using a data frame. However, application of FlexRay to a subsystem which uses CAN may be time-consuming and expensive. Flexray has not been used in many fields because of such a drawback. CAN FD was developed to solve a weak point of Flexray [7]. CAN FD has strengths of both CAN and Flexray. CAN FD provides a data transmission rate faster than CAN. Besides, using a single data frame, it can transmit data 8 times more than CAN [19].

High speed communication protocols like CAN-FD and Flexray were developed to solve shortcomings of CAN, But CAN is still used in the automobile industry. There is a possibility that vehicular communication protocol will be changed to Ethernet but the majority of cars available now use CAN. In this Chapter, we examine a security threats that may be generated by the security vulnerability of CAN.

2.2.2 Controller Area Network (CAN)

CAN is a sender ID-based broadcast protocol. As the communication protocol guaranteeing high reliability, CAN has been most frequently used for construction of In-vehicle network for the past 20 years. CAN has representative advantages as follows [4].

- Efficient error detection and recovery mechanism

- Efficient media access control by carrier sense multiple access with collision detection (CSMA/CD).
- Minimization of data transmission delay time using priority

A CAN data frame consists of 7 main fields as shown from Figure 2. Functions of each area are as follows. Start of Frame (SOF) is composed of one bit. SOF informs every receiver of start of transmission. Arbitration(ECU ID) field plays a role in preventing a collision of a data frame. Control field plays a role in displaying the properties of a data frame. Data field is used for data transmission. It can transmit 8byte data to the maximum. Cyclic Redundancy Code is used to identify if data frame was transmitted to a receiver normally. The receiver activates ACK bit if he received a data frame normally. End of Frame means transmission of a data frame was completed.

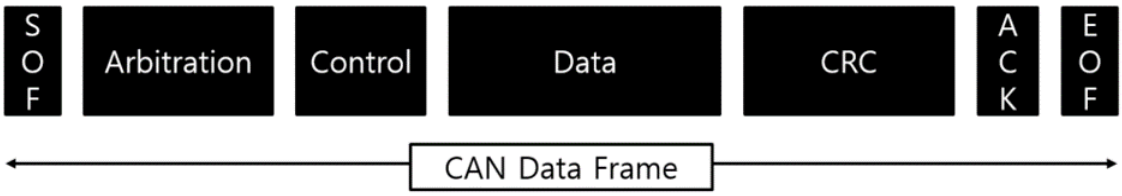

Figure 2: CAN data frame format

2.2.3 Vulnerabilities of CAN

CAN was developed in 1980s. At the time of its development, automobiles had a very closed network environment. As a result, CAN has no information security function (e.g. access control, confidentiality and authentication) since it was designed considering the closed vehicular environment only. That is, if accessing to a CAN communication line is possible for vehicles using CAN, cyber attack may be performed. K. Koscher et al. analyzed vulnerabilities of In-vehicle CAN using a real vehicle [9]. They pointed out that these kinds of security vulnerabilities above lead to threats to security as follows:

Data frame sniffing: All ECUs connected to In-vehicle CAN can participate in communication. An attacker can eavesdrop on all data frames sent to the In-vehicle CAN. CAN data frames are not encrypted. An attacker can analyze the meaning of the CAN data frame.

Impersonation attack and Replay attack: Since the CAN data frame does not have an authentication field, an attacker can use a valid ECU ID to perform an impersonation attack. Also, a replay attack can be performed using data frames acquired in advance.

DoS attack: CAN executes an arbitration process to prioritize transmission. An attacker can send a number of high priority data frames to prevent other ECUs from communicating.

3 Related Work

A range of ICT technologies were applied to vehicles without any proper consideration of security so vehicles came to be a target for cyber attack. There have been numerous vehicular hacking researches using a real vehicle published since 2010. In 2010, K. Koscher et al. conducted a hacking experiment using a real vehicle and pointed out problems of In-vehicle network. They proved vehicles can be controlled forcibly using vulnerabilities of CAN in their experiment. Various vehicular hacking studies were conducted based on their research findings [9]. Stephen Checkoway et al. presented their research findings about hacking into telematics ECU mounted to a vehicle. They analyzed vulnerabilities of the Aqlink

protocol used for Telematics ECU and performed an attack to control the vehicle. Aqlink is the communication protocol used for Ford Sync service and GM OnStar service. They hacked into the vehicle using three vulnerabilities(vulnerabilities of Buffer Overflow, initialized random number and authentication) of the Aqlink protocol [3].

Charlie Miller and Chris Valasek published their research findings about hacking into Toyota Prius and Ford Escape. In their hacking, they conducted forced control of acceleration, brake, steering functions and also dashboard status of a vehicle. They published an in-depth technical document about how to analyze vulnerabilities of ECU and In-vehicle CAN [16][13][12]. Samuel Woo et al. hacked into a smart-phone application to control a vehicle forcibly. They hacked into the smart phone application for vehicles used by drivers and carried out an attack for remote control of the vehicle [20].

A lot of studies on vehicular security were conducted in addition to vehicular hacking. In particular, researches on regulations and guidelines on vehicular security are being done actively in the United States, Japan and European nations. In regard to vehicular security, representative security projects are as follows.

- **SEVECOM (Secure Vehicle Communication)** : The project to develop security technologies for Vehicle to Vehicle communication (V2V) and Vehicle to Infrastructure communication (V2I). Research on authentication technologies was conducted to prevent a cyber attack [11].
- **EVITA(E-Safety Vehicle intrusion protected Applications)** : The project funded by FP7(Seventh Framework Programme) of EU(European Union). Security technologies were developed to protect In-vehicle network [1].
- **PRECIOSA(Privacy Enabled Capability in Cooperative Systems and Safety Application)** : The research on Privacy protection for C-ITS(V2V / V2I) [10].
- **OVERSEE(Open Vehicular Secure Platform)** : The research on open platform for vehicle communication [5].
- **PRESERVE(Preparing Secure Vehicle-to-X Communication Systems)** : The project to integrate and market security technologies researched/developed for V2X communication [2].

After a range of vehicular security projects, there have been researches on security guidelines to be observed in an automobile environment. “Approaches for Vehicle Information Security(Information Security for “Networked” Vehicles)” were published by IPA. The document analyzed threats to security that had occurred in an automobile environment and summarized measures for security to solve(remove) such threats. Measures for security derived from threats summarized above are used when designing the E/E system mounted to a vehicle. Furthermore, it described Effort which should be made by a developer for security in a Life Cycle of automobile development(planning, development, operation, disuse).

“Cyber Security and Resilience of smart cars (CSR)” was presented by ENISA. CSR defined a meaning of a smart car and conducted asset and risk analyses for smart cars. In addition, it described the security scheme to construct a smart car environment secured from these threats. The purpose of CSR is to implement “asset analysis”, “threat analysis” and “definition of protection technology” for smart cars. Definitions by CSR may be used at agencies/enterprises which research/develop/produce smart car-related products including car makers, Tier-1, Tier-2 and Aftermarket suppliers. As shown from above, various vehicular security researches were conducted but no definite evaluation methodology was developed to evaluate security of a vehicle. This paper suggests the evaluation methodology to check security status of In-vehicle CAN. Our proposed methodology for security evaluation allows one to identify security status of a vehicle very easily and fast.

4 Proposed Security Evaluation Methodology and Tool

In this paper, we propose the evaluation methodology to check security vulnerabilities of In-vehicle CAN. Based on vehicle hacking researches, it defines four types of representative cyber attacks which may be done in In-vehicle CAN. Four types of attacks include a Replay attack, Impersonation attack, DoS attack and Fuzzy attack. Our proposed security evaluation methodology includes followings.

- Definition of evaluation methodology: In the definition of the evaluation methodology, we introduce how to conduct four types of attack tests and analyze results.
- Definition of evaluation tool: In the definition of the evaluation tool,We design and develop the evaluation tool that can measure changes in vehicle conditions using various sensors.

Before explaining the proposed method, we define the terms used in this paper. The terms we use are:

Abnormal data frame: It means a data frame maliciously inputted other than data frame from a normal ECU(replay attack and impersonation is done using an abnormal data frame.)

Abnormal traffic: It means a situation where a larger quantity of communication traffic occurs than permitted traffic in a vehicle(DoS attack is done using abnormal traffic.)

Impersonation attack: It means an attack for attacker to falsely transmit information which should be done by certain node.

Replay attack: It means an attack that sniffs and replays certain data frame.

DoS attack: It means an attack that makes resources of certain system scarce and prevents users from using them under the intended purpose.

Defined follow-up measure or action: It means an action for defending against abnormal data frame or traffic if it happens.

Network separation: It means a communication channel separated.

Collection of driving status data: It means collection of a data frame happened when user is adjusting a vehicle including a sharp turn, sudden acceleration and deceleration.

4.1 Definition of Evaluation Environment

In this section, we introduces an environment setting and evaluation tools for measuring the changing conditions of vehicles.

4.1.1 Checks Before Evaluation

- Build an environment for high speed CAN communication in a vehicle and check if normal communication is being done.
- Verify validity of four items in Table 2 to check if In-vehicle network is conducting normal high speed CAN communication.

Test Item	Detailed Item		Criterion (Spec.)
Physical layer check (electrical properties)	Communication voltage level	RECESSIVE	CAN_H (VH) : 2.5 (2.0∼3.0) V CAN_L (VL) : 2.5 (2.0∼3.0) V
		DOMINANT	CAN_H (VH) : 3.5 (2.75∼4.5) V CAN_L (VL) : 1.5 (0.5∼2.25) V

Table 2: High-speed CAN Network Communication Standard (ISO 11898-2)

- Measure CAN-H and CAN-L signals using an oscilloscope to measure a voltage level of communication line. Identify the validity of results measured using Table 3. Conduct a security evaluation test in case a result measured is valid.

Division	Measured Item (Standard Tolerance)	Measured Value	Standard Validity
RECESSIVE	CAN_H (VH) : 2.5 (2.0∼3.0) V CAN_L (VL) : 2.5 (2.0∼3.0) V	2.40 V 2.43 V	Valid Valid
DOMINANT	CAN_H (VH) : 3.5 (2.75∼4.5) V CAN_L (VL) : 1.5 (0.5∼2.25) V	3.66 V 1.26 V	Valid Valid

Table 3: Standard Tolerance

4.1.2 Measuring Equipment

Figure 3 shows a schematic diagram of equipment's for evaluation of vehicle security.

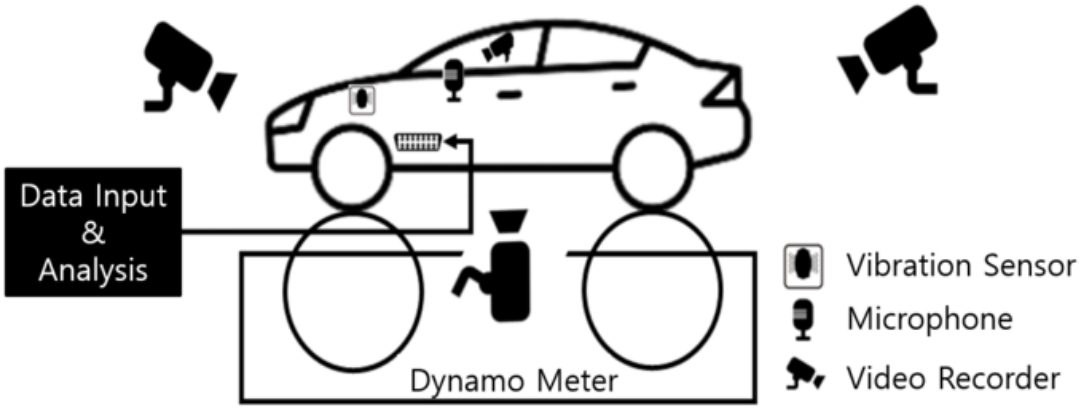

Figure 3: Vehicle Security Evaluation Environment

Video equipment: The image sensor is used to measure the operation of the instrument panel of a vehicle and a control device (e.g. seat, door, etc.). Store data occurred from In-vehicle CAN when a change is detected. Figure 4 shows an image processing technique for identifying a change of an image.

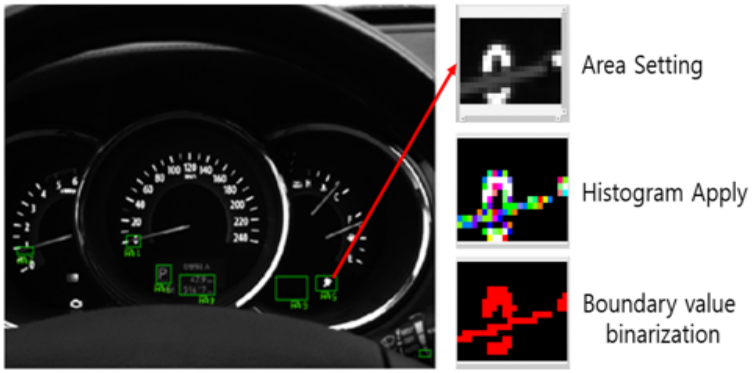

Figure 4: Motion Structure of Video Equipment

Sound equipment: The sound sensor is used to measure the noise generated from the vehicle. Install a microphone near a dashboard and measure a sound wave change. Determine that there are abnormalities in a vehicle in case of a change more than 4 dB. Figure 5 shows the way to detect a sound wave change.

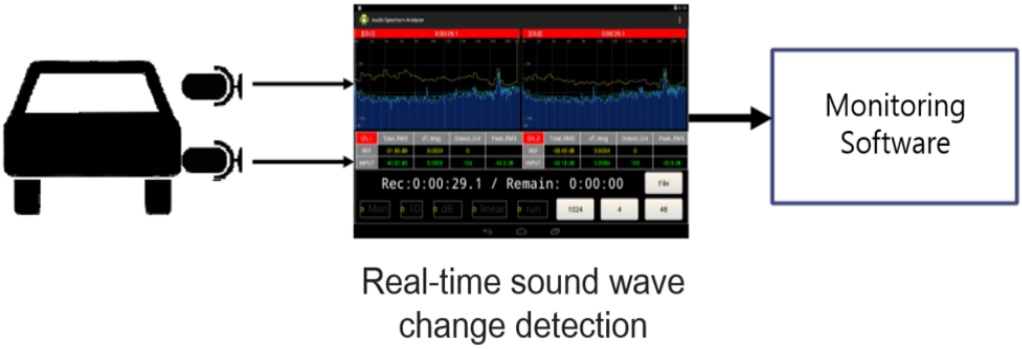

Figure 5: Motion Structure of Sound Equipment

Vibration sensor: Install a vibration sensor to an engine to identify a change of a car engine. Figure 6 shows a vibration sensor.

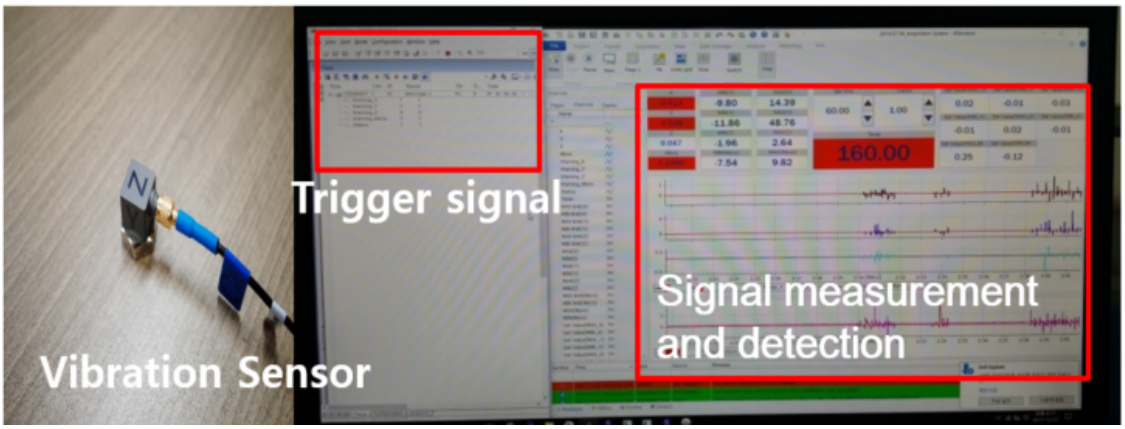

Figure 6: Motion Structure of Vibration Sensor

Attack tool: Connect a device entering an attack message into In-vehicle CAN to an OBDII port of a vehicle.

Monitoring software: Software checking and controlling status of video and sound equipment, vibration sensor and attack tools. Store event data from each measuring equipment.

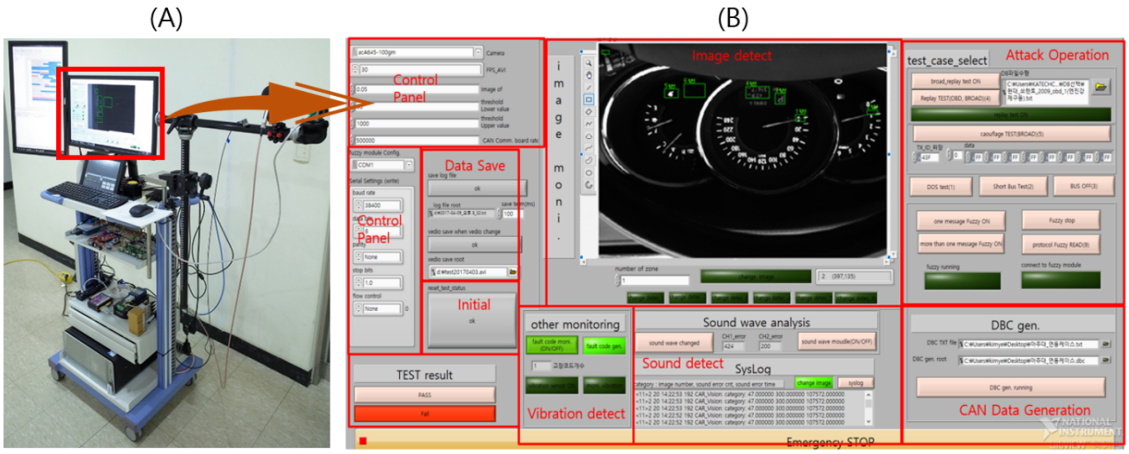

Figure 7: Security Evaluation Management Tools (A) Hardware, (B) Control Software

Video and sound equipment and a vibration sensor above are attached to an evaluation target(vehicle). Figure 7 shows security evaluation management tools(control software and hardware) which process data from each sensor.

4.2 Test Methodology

The security evaluation is conducted at the evaluation environment described above. A change of vehicular status is to be identified during four types of attack tests. Evaluation items consist of replay attack, impersonation attack, DoS attack and fuzzy attack. Main contents and detailed procedures of each item are as follows.

Item		**antiDoS**	
Purpose		Check effects of DoS attack on In-vehicle network	
Order	**Method**	**Procedure & Content**	**Result**
1	Initial state	A vehicle is at initial state.	
2	Input data	Connect a message injection device for test to OBD port of the vehicle.	
3	Perfor -mance	Generate a DoS test (ID with high priority) message and inject it into OBDII port for 10 mins.	
4	Verifica -tion	Test a change of vehicular status using measuring equipments. If there is no change of status, classify it as the vehicle secured from DoS.	Safe /unsafe
Result Confirmation		If there is no change of status, classify it as the vehicle secured from DoS. (test result=”Secure”)	

Table 4: Procedure of DoS Attack Test

DoS attack test: Perform the DoS attack defined from Table 4. Transmit a message rapidly from a message transmission equipment to create status above the bandwidth tolerable in In-vehicle CAN. Transmit a message fast for more than 99% of the bandwidth. Monitor a change of vehicular status using a measuring equipment.

Replay attack test: Perform the replay attack defined from Table 5. Monitor a change of vehicular status using a measuring equipment. For a replay attack message, it is possible to use a data frame acquired from an automotive diagnostic tool. Here, follow the procedure defined from Table 6.

Item		**antiReplay-1**	
Purpose		Check if vehicle can cut off a message replayed	
Order	**Method**	**Procedure & Content**	**Result**
1	Initial state	A vehicle is at initial state.	
2	Input data	Connect a CAN message injection device to OBD port of the vehicle.	
3	Perfor -mance	Conduct logging of a message generated while driving at 60km/h to generate a test message for 5 mins.	
4	Perfor -mance	Inject logged message into OBD port.	
5	Verifica -tion	Test a change of vehicular status using measuring equipments. If there is no change of status, classify it as the vehicle secured from replay attack.	Safe /unsafe
Result Confirmation		If there is no change of status, classify it as the vehicle secured from replay attack. (test result=”Secure”)	

Table 5: Procedure of Driving Data Replay Attack Test

Item		**antiReplay-2**	
Purpose		Check if vehicle can cut off a message replayed	
Order	**Method**	**Procedure & Content**	**Result**
1	Initial state	A vehicle is at initial state.	
2	Input data	Connect a CAN message injection device to OBD port of the vehicle.	
3	Perfor -mance	Collect a message transmitted from an automotive diagnostic tool.	
4	Perfor -mance	Inject logged message into OBD port.	
5	Verifica -tion	Test a change of vehicular status using measuring equipments. If there is no change of status, classify it as the vehicle secured from replay attack.	Safe /unsafe
Result Confirmation		If there is no change of status, classify it as the vehicle secured from replay attack. (test result=”Secure”)	

Table 6: Procedure of Forced Drive Replay Attack Test[using an automotive diagnostic tool]

Fuzzy attack test: Perform the Fuzzy attack defined from Table 7. Use a data frame collected from the vehicle for the Fuzzy attack. In addition, a data frame for attack may be generated by combination of random ID and data. Monitor a change of vehicular status while transmitting the data frame for attack to In-vehicle CAN.

Item		**antiFuzzy**	
Purpose		Check if vehicle can cut off a message replayed or using an abnormal ID	
Order	**Method**	**Procedure & Content**	**Result**
1	Initial state	A vehicle is at initial state.	
2	Input data	Connect a CAN message injection device to OBD port of the vehicle.	
3	Perfor -mance	Conduct logging of a message generated while driving at 60km/h to generate a test message for 5 mins. Create a message composed of random ID and random data to generate a test message.	
4	Perfor -mance	Inject logged message and newly generated message into OBD port.	
5	Verifica -tion	Test a change of vehicular status using measuring equipments. If there is no change of status, classify it as the vehicle secured from fuzzy attack.	Safe /unsafe
Result Confirmation		If there is no change of status, classify it as the vehicle secured from fuzzy attack. (test result=”Secure”)	

Table 7: Procedure of Fuzzy Attack Test

Impersonation attack test: Perform the impersonation attack defined from Table 8. Monitor a change of vehicular status using a measuring equipment. However, an impersonation attack test is not possible without data collected from OBDII port.

Item		**antiImpersonation**	
Purpose		Check if vehicle can cut off a message replayed	
Order	**Method**	**Procedure & Content**	**Result**
1	Initial state	A vehicle is at initial state.	
2	Input data	Connect a CAN message injection device to OBD port of the vehicle.	
3	Perfor -mance	Generate a message for attack using an ID utilized in the vehicle to generate a test message.	
4	Perfor -mance	Inject the attack message generated into OBD port.	
5	Verifica -tion	Test a change of vehicular status using measuring equipments. If there is no change of status, classify it as the vehicle secured from imperson -ation attack.	Safe /unsafe
Result Confirmation		If there is no change of status, classify it as the vehicle secured from imperson -ation attack. (test result=”Secure”)	

Table 8: Procedure of Impersonation Attack Test

5 Practical Use Case and Discussion

Practical Use Case: In order to verify the accuracy and efficiency of our security evaluation method and tool, we conducted an experiment using a real vehicle. The experiment was conducted using four types of vehicles. The experimental environment is shown in Figure 8. We observed the condition of the vehicle while carrying out the four cyber attacks defined in Chapter 4. When observing the condition of the vehicle, we used the automation tool we manufactured. During the attack, when an abnormality in a vehicle occurs, the automation tool floats an alarm and stores status information of In-vehicle CAN. Table 9 shows the results of experiments using four types of vehicles. Fail indicates that cyber attacks can not be prevented, and Pass indicates that cyber attacks can be prevented.

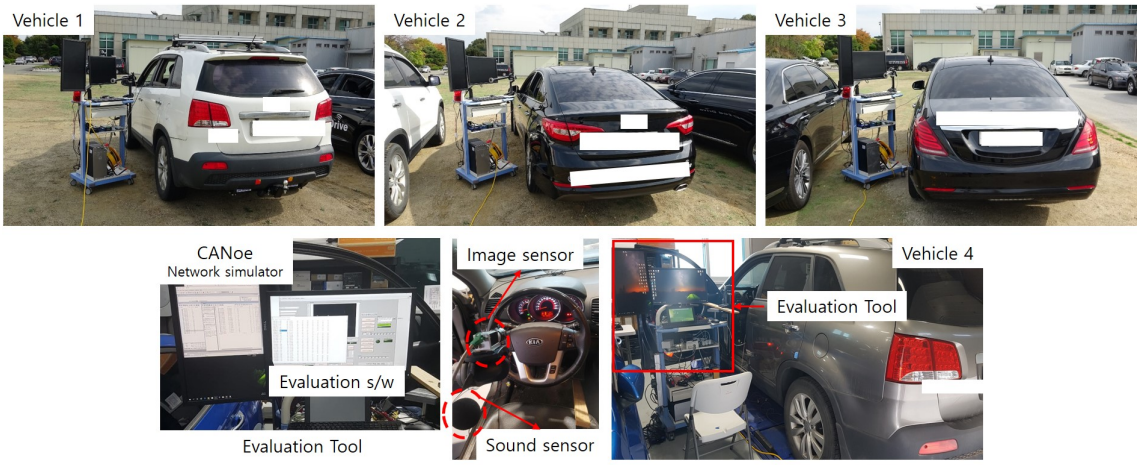

Figure 8: Evaluation Environment and Tools

Table 9: The Results of Security Evaluation based on the our proposed methodology.

No	Model	anti-Impersonation	anti-Replay-1	anti-replay-2	anti-Fuzzy	anti-DoS
Vehicle 1	2009	Fail	Fail	Fail	Fail	Fail
Vehicle 2	2010	Fail	Fail	Fail	Fail	Fail
Vehicle 3	2016	Pass	Pass	Fail	Pass	Pass
Vehicle 4	2014	Fail	Fail	Fail	Fail	Fail

Discussion: We conducted experiments using real vehicles and proved that we can measure the security of vehicles as an evaluation tool we designed and manufactured. While conducting the experiment, it took less than an hour to evaluate a single vehicle that did not provide any information from the vehicle manufacturer. Most of the time spent in the evaluation took to get the data frames used for the attack. The time taken to perform a physical security assessment is around 10 minutes. As shown in Table 9, all vehicles except vehicle 3 are very vulnerable to cyber attacks. For vehicle 3, all attacks were able to prevented except for one type of cyber attack. After reviewing the design of the vehicle 3, it was confirmed that the vehicle 3 is performing the access control using the gateway ECU. Unfortunately, Vehicle 3 is vulnerable to entity authentication and can not prevent replay attacks based on diagnostic tools. In this way, using the evaluation methods and tools we proposed, it is possible to evaluate the safety of a car very easily and quickly.

6 Conclusion

Interest in vehicle security has grown rapidly over the past decade. The newest vehicles cut off inflow of malicious data using the access control system. However, every vehicle on the market is not loaded with such a security device. Now, along with the commercialization of connected car and autonomous car, security became an essential function for vehicles. Although automotive information security technology has been continuously developed, there is no way to analyze the level of automotive security. We proposed the methodology to evaluate the security level of a vehicle without any information given by vehicles makers. In the proposed evaluation method, we defined the penetration test items to be considered in the vehicle. We also designed and developed the evaluation tool for automatic check of a change of vehicular status while conducting the security evaluation. In addition, we conducted experiments using actual vehicles to evaluate the effectiveness and accuracy of the proposed methodology and tool. As a result of experiments, most vehicles did not prevent the penetration test items we defined. Fortunately, vehicles equipped with gateway ECUs can prevent all attacks except replay attacks based on diagnostic tools. Through experiments, we confirmed that we could evaluate the security of in-vehicle network using the proposed evaluation method.

Acknowledgments

This research was supported by the Korea Ministry of Land, Infrastructure and Transport. It was also supported by the Korea Agency for Infrastructure Technology Advancement (Project No.: 18TLRP-B117133-03)

References

[1] E-safety vehicle intrusion protected applications. Fraunhofer Institute SIT, 2008. `https://www.evita-project.org/EVITA_factsheet.pdf` [Online; accessed on May 1, 2019].

[2] N. Bißmeyer, S. Mauthofer, J. Petit, M. Lange, M. Moser, D. Estor, M. Sall, M. Feiri, R. Moalla, M. Lagana, et al. Preparing secure vehicle-to-x communication systems. the PRESERVE project, 2014. `https://www.preserve-project.eu/sites/preserve-project.eu/files/PRESERVE-D5.4-Deployment_Issues_Report_V4_V1.2.pdf` [Online; accessed on May 1, 2019].

[3] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno, et al. Comprehensive experimental analyses of automotive attack surfaces. In *Proc. of the 20th USENIX conference on Security (SEC'11), San Francisco, California, USA*, volume 4, pages 447–462, August 2011.

[4] M. Farsi, K. Ratcliff, and M. Barbosa. An overview of controller area network. *Computing & Control Engineering Journal*, 10(3):113–120, June 1999.

[5] A. Groll, J. Holle, C. Ruland, M. Wolf, T. Wollinger, and F. Zweers. Oversee a secure and open communication and runtime platform for innovative automotive applications. In *Proc. of the 7th Embedded Security in Cars Conference (ESCAR'09), Dresden, Germany*. IMPRINT, November 2009.

[6] H. Gustavsson and J. Axelsson. Evaluating flexibility in embedded automotive product lines using real options. In *Proc. of the 12th International Software Product Line Conference (SPLC'08), Limerick, Ireland*, pages 235–242. IEEE, September 2008.

[7] F. Hartwich et al. Can with flexible data-rate. In *Proc. of the 2012 IEEE Conference on Communications (iCC'12), Ottawa, Canada*, pages 1–9. IEEE, June 2012.

[8] K. H. Johansson, M. Törngren, and L. Nielsen. Vehicle applications of controller area network. In *Handbook of networked and embedded control systems*, pages 741–765. Springer, 2005.

[9] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, et al. Experimental security analysis of a modern automobile. In *Proc. of the 2010 IEEE*

Symposium on Security and Privacy (SP'10), Berkeley/Oakland, California, USA, pages 447–462. IEEE, May 2010.

[10] M. Kost, J.-C. Freytag, F. Kargl, and A. Kung. Privacy verification using ontologies. In *Proc. of the 2011 6th International Conference on Availability, Reliability and Security (ARES'11), Vienna, Austria*, pages 627–632. IEEE, August 2011.

[11] T. Leinmüller, L. Buttyan, J.-P. Hubaux, F. Kargl, R. Kroh, P. Papadimitratos, M. Raya, and E. Schoch. Sevecom-secure vehicle communication, January 2006. `https://people.kth.se/~papadim/publications/fulltext/sevecom-early-1.pdf` [Online; accessed on May 1, 2019].

[12] C. Miller and C. Valasek. A survey of remote automotive attack surfaces, 2014. `http://illmatics.com/remote%20attack%20surfaces.pdf` [Online; accessed on May 1, 2019].

[13] C. Miller and C. Valasek. Remote exploitation of an unaltered passenger vehicle, 2015. `http://illmatics.com/Remote%20Car%20Hacking.pdf` [Online; accessed on May 1, 2019].

[14] T. Nolte, H. Hansson, and L. L. Bello. Automotive communications-past, current and future. In *Proc. of the 2005 IEEE Conference on Emerging Technologies and Factory Automation (ETFA'05), Catania, Italy*, volume 1, pages 985–992. IEEE, April 2005.

[15] R. Shaw and B. Jackman. An introduction to flexray as an industrial network. In *Proc. of the 2008 IEEE International Symposium on Industrial Electronics (ISIE'08), Cambridge, UK*, pages 1849–1854. IEEE, June-July 2008.

[16] C. Valasek and C. Miller. Adventures in automotive networks and control units. Technical report, IOActive, 2014.

[17] A. Vasenev, F. Stahl, H. Hamazaryan, Z. Ma, L. Shan, J. Kemmerich, and C. Loiseaux. Practical security and privacy threat analysis in the automotive domain: Long term support scenario for over-the-air updates. In *Proc. of the 5th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS'19), Crete, Greece*. SCITEPRESS Digital Library, March 2019.

[18] M. Wolf, A. Weimerskirch, and T. Wollinger. State of the art: Embedding security in vehicles. *EURASIP Journal on Embedded Systems*, 2007:074706:1–074706:16, December 2007.

[19] S. Woo, H. J. Jo, I. S. Kim, and D. H. Lee. A practical security architecture for in-vehicle can-fd. *IEEE Transactions on Intelligent Transportation Systems*, 17(8):2248–2261, March 2016.

[20] S. Woo, H. J. Jo, and D. H. Lee. A practical wireless attack on the connected car and security protocol for in-vehicle can. *IEEE Transactions on intelligent transportation systems*, 16(2):993–1006, 2015.

[21] S. Woo, D. Moon, T.-Y. Youn, Y. Lee, and Y. Kim. Can id shuffling technique (cist): Moving target defense strategy for protecting in-vehicle can. *IEEE Access*, 7:15521–15536, January 2019.

Author Biography

Hyun-Bae park received an BS degree in Electronics from Hanbat National University, Daejeon, Korea, in 2008. He is currently a researcher at Korea Automotive Technology Institute(KATECH), His research interests include vehicular positioning, vehicular wire-wireless networks communication technology and vehicular various security issues. (V2X,CAN,Penetration test).

Yongeun Kim received his B.S., M.S., and Ph.D. degrees in electrical engineering from Chonbuk National University, Jeonju, Korea in 2005, 2007, and 2010, respectively. He is currently a Researcher with the Vehicle-IT Convergence R&D Center, Korea Automotive Technology Institute, Cheonan, Korea. His main research interests include electric machinery and its drives, micro controller, and applications of motor drives such as electric vehicles.

Jaeseok Jeon received an M.Eng. degree from Kongju University, Cheonan, Korea, in 2011. He is currently a researcher at Korea Automotive Technology Institute(KATECH), His research interests include electronics control units, controller area network(CAN) security, and In-vehicle Network technology.

Hee Seok Moon received an Ph.D degree from Hanyang University, Seoul, Korea, in 2014. He is currently a researcher at Korea Automotive Technology Institute(KATECH), His research interests include electronics control units, controller area network(CAN) security, and In-vehicle Network technology.

Samuel Woo received the Ph.D. degree in information security from Korea University, Seoul, Korea, in 2016. He joined the Electronics and Telecommunications Research Institute in 2016. Currently, he is working as a senior researcher of the network security research laboratory of the ETRI. His research interests include cryptographic protocols in authentication, security and privacy in vehicular networks, and controller area network (CAN) security.