Research on Information Security Test Evaluation Method Based on Intelligent Connected Vehicle

Yanan Zhang, Shengqiang Han(✉), Stevenyin Zhong, Peiji Shi, and Xuebin Shao

Automotive Data Center, China Automotive Technology and Research Center Co., Ltd., Tianjin 300393, China
{zhangyanan,hanshengqiang}@catarc.ac.cn
http://www.catarc.ac.cn/ac2016/index.html

Abstract. In order to effectively evaluate the information security level for an intelligent and connected vehicle, a novel Intelligent Connected Vehicle (ICV) Information Security Attack and Defense (ICV-ISAD) test evaluation method is proposed in this paper. ICV-ISAD test method is based on long-term large number of real vehicle test experiments. It mainly consists of security threat and risk analysis, test strategy design, test tool call, test point mapping, test procedure execution, and remediation measures mapping. Using ICV-ISAD test method, we conducted test experiments to In-vehicle Network, Telematics Box, Engine Control Unit, In-Vehicle Infotainment, Mobile Application, Radio and Telematics Service Provider for different types of vehicle. The results show that some vulnerabilities exist in ICV's system, such as gateway filtering vulnerability, high-risk port opening, Cross Site Scripting (XSS), Structured Query Language (SQL) injection, weak password, and cleartext network traffic (HTTP). Besides, ICV-ISAD test method could map some remediation measures or recommendations for these vulnerabilities. It denotes that ICV-ISAD test method can effectively test and evaluate the information security of ICV.

Keywords: Intelligent connected vehicle · Information security · Test evaluation · Vulnerability · Remediation measure

1 Introduction

Intelligent Connected Vehicle (ICV) is a new generation of vehicle which is equipped with advanced in-vehicle sensors, controllers, actuators and other devices, and integrates modern communication and network technology to realize intelligent information exchange and sharing between vehicles and X (people, cars, roads, backgrounds, etc.) [1]. The Chinese government said it is paying great attention to the development of intelligent connected vehicles and considers the sector a vital way to ease the burden on transportation, energy consumption and

J. Li et al. (Eds.): SPNCE 2019, LNICST 284, pp. 178–197, 2019.
https://doi.org/10.1007/978-3-030-21373-2_15

environmental pollution [2]. By 2020, the market scale of the country's intelligent connected vehicles sector is expected to exceed 100 billion yuan [3]. However, these rapid changes to enhance the intelligent and connected functions of vehicles are having a serious effect on their security. Specifically, the Internet penetrates into the modern vehicles [4]. Increased connectivity often results in a heightened risk of a cybersecurity attack [5–7], such as Denial-of-Service (DoS) attack, man-in-the-middle attack and Structured Query Language (SQL) injection. In 2015, preeminent hackers Charlie Miller and Chris Valasek dominated headlines with their landmark hack of a Jeep Cherokee [8]. In 2016, team of hackers take remote control of Tesla Model S from 12 miles away [9]. In 2017, Keen Lab discovered new security vulnerabilities on Tesla motors and realized full attack chain to implement arbitrary CAN BUS and ECUs remote controls on Tesla motors with latest firmware [10]. In 2018, researchers hacked BMW cars and discovered 14 vulnerabilities [11].

Cars are getting more and more connected, which means more electronics plus access to the internet. Which, in turn, means more opportunities to hack cars remotely. For the security, generally speaking, the measures of protection against malicious attacks are little known to automotive manufacturers and suppliers. Modern cars need to be developed with security in mind, and that is something that has to be done by security professionals, whereas the Original Equipment Manufacturers (OEMs) lack the ability to comprehensively evaluate the security levels of their cars. Automotive information security can be guaranteed in many ways, such as security standards, regulations and test evaluation methods or public announcement system. As one of the most direct and effective means, the test evaluation method could provide a security process framework and guidance to help OEMs identify and assess security threats and design security into cyber-physical vehicle systems throughout the entire development lifecycle process. However, due to the lack of relevant standards, there are relatively few test evaluation methods for automotive information security in the industry, while most of these methods focus on testing the safety of cars [12,13].

In this paper, a novel Intelligent Connected Vehicle Attack and Defense (ICV-ISAD) test evaluation method is proposed to address the test evaluation issue of automotive security. The article is structured as follows: in the following Sect. 2 it studies the problem and object statement under investigation from the two aspects of ICV's classic system architecture and the main attack surfaces it faces. In Sect. 3 we introduce the test methodology of ICV-ISAD test method from three stages. In Sect. 4 there are some experimental results and analyses for ICV-ISAD test method. After the overall outlook for above, the last section concludes this article with a summary.

2 Problem and Object Statement Under Investigation

While automobile manufacturers have improved the intelligent and connected functions of their automobiles a lot during the past decades, adequate protection measures for vehicle security are not available yet [14]. Moreover, vehicle security related incidents can also affect the safety of automotive systems [15]. All of this interplay between intelligent and security clearly motivates automotive security as a research topic with increasing relevance and importance. Also, it motivates us to explore a test method to evaluate automotive security.

For this section, it serves as a research basis of security test evaluation method analyzing the current state-of-the-art ICV's classic system architecture and the main attack surfaces it faces, respectively.

2.1 Classic System Architecture

The object under investigation is an ICV system consisting of actuators, sensors, and all kinds of embedded ECUs (Electronic Control Units) that are connected with each other through different busses, such as CAN bus, FlexRay, Ethernet and MOST. To investigate the security of ICV more clearly, we develop an ICV's classic system architecture that consists of multiple functional modules, such as Gateway, Telematics Box, In-Vehicle Infotainment, Body Electronic Module, Chassis Controller and Powertrain Controller. It is illustrated in Fig. 1. Specifically, the Classic System Architecture can be clearly seen that the OBD and USB interface can provide direct contact physical attacks, while the Wi-Fi and Bluetooth may be used to attack the ICV's system remotely. Besides, Gateway plays a vital role in the system, which has close ties with many units of the car.

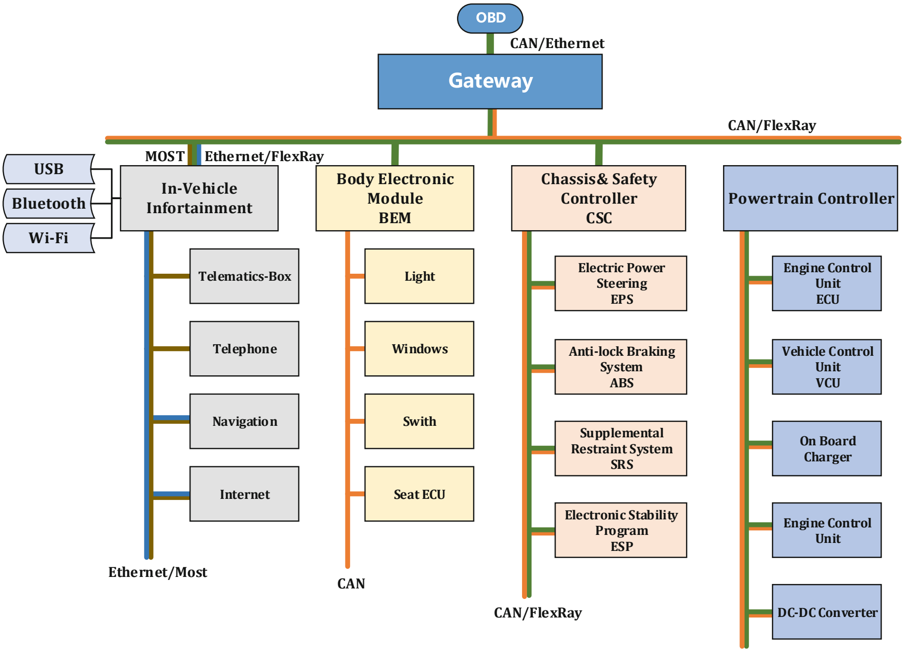


Fig. 1. Intelligent connected vehicle classic system architecture

Furthermore, successful exploitation of the CAN vulnerability on an automobile with this classic system architecture may allow an attacker with physical access and extensive knowledge of CAN to reverse engineer network traffic to perform a Denial of Service (DoS) attack disrupting the availability of arbitrary functions of the car [19]. In the following section, we will do some research on security test evaluation method based on this ICV's classic system architecture.

2.2 Attack Surfaces

The intelligent connected vehicle has a complex system with many embedded Units. With many intelligent technologies being introduced into vehicle, the threats of malicious attack of automotive security are gradually increasing and the problems of information security are increasingly highlighted. It is not difficult to imagine that automobile manufacturers cannot come up with a strong security system for protecting vehicle networks unless they are very well aware of the attack surfaces that an automobile is facing and have a clear understanding of the existing vulnerabilities. Before helping them solve this puzzle, we first need to analyze the main threat surfaces ICV faces at present. Based on the ICV's classic system architecture being presented in Fig. 1, in this section, there is an introduction of the attack surfaces threating ICV's security. An illustration of these attack surfaces is shown in Fig. 2. The details of these seven attack surfaces are as follows.

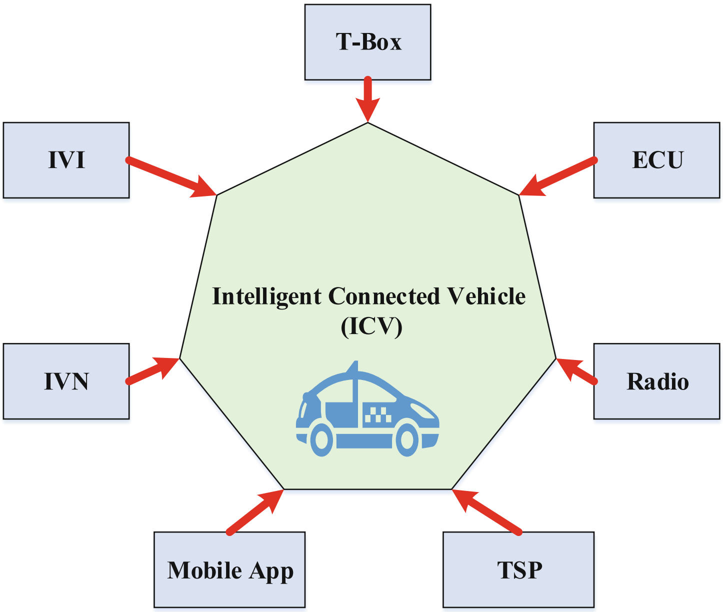


Fig. 2. Attack surfaces that ICV faces

Telematics Box (T-Box). Telematics Box is an electronic unit that integrates all kinds of chips, such as 3G/4G chip, wireless module, communication module, microcontroller (MCU), System on a Chip (SoC). It can be used to the interactive communication between the vehicle and the cloud-platform and connect with the cellular communication networks. In addition, some T-Boxs have the function of tracking with various satellite constellations (GPS, Galileo, GLONASS). As an important communication unit, T-Box's security is critical for that of ICV. Therefore, hackers take it for granted that T-Box is one of the main breakthroughs used to compromise vehicles.

In-Vehicle Infotainment (IVI). In-Vehicle Infotainment is the centerpiece of the car's sound and information system, which provides some direct user experience (UX) for car owners, such as music, applications, navigation. The IVI systems hack is possible and is a real concern [16]. The system is responsible for controlling some of the most vital functions of the car's system. Specifically, IVI systems frequently utilize Bluetooth technology and/or smartphones to help drivers control the system with voice commands, touchscreen input, or physical controls, which exposes outside and provides a direct way to attack the vehicle.

Electronic Control Unit (ECU). During our research on attack surfaces for ICV, electronic control unit consists of all kinds of critical electronic units except T-Box and IVI, such as Central Computer (CEM), Engine Control Unit, Brake Control Module (BCM) and Remote Monitory System (RMS). All of these modules directly control the movement and behavior of the vehicle, and they can do harm to the vehicle once been attacked.

In-Vehicle Network (IVN). In-Vehicle Network is a general term for the internal network architecture of the car and mainly composed of various electronic modules and different types of buses, for example CAN bus, FlexRay, Ethernet, MOST and so on. All of the buses connects to ECU, T-Box and other critical components. IVN is the nerve center of the entire vehicle system and controls the normal operation of the car system. It is the last defensive line to protect the vehicle from being attacked.

Mobile Application (Mobile App). In this work, Mobile App is an automotive program or software application designed to run on a mobile device such as a phone/tablet, which can be used to control vehicle remotely. Besides, the source codes/files of app contain a great deal of privacy information and they can be reversed, recompiled or tempered. So its security plays a vital role in the field of automotive security.

Radio. In term of ICV information security, Radio refers to the technology of using radio waves to carry information in vehicle, such as sound and images, by systematically modulating properties of electromagnetic energy waves transmitted through space, such as their amplitude, frequency, stage, or pulse width. There are Wi-Fi, Bluetooth, Tire Pressure Monitoring System (TPMS), Remote Keyless Entry System (RKMS) and so on. For the security risks of radio, some hackers set up a radio listening station to find and decode hidden radio signals—just like the hackers who triggered the emergency siren system in Dallas, Texas, probably did [17].

Telematics Service Provider (TSP). In research about Telematics Service Provider's security, it mainly serves as the cloud platform and some servers that are used to provide the services to the vehicles on the road, which plays a role in the connected car value chain centered on secure vehicle to cloud data management. Due to its close connection with the Internet, it has attracted the attention of many attackers and has become one of the most commonly used attack surface or path.

These attack surfaces related to vehicles exacerbate the problem of causing much information disclosure or compromising an entire in-vehicle network due to the lack of protective measures in the automotive pipeline (network) and other counterparts. Considering the interests of OEMs and users, they are the main objects used to study common car vulnerabilities and possible attack paths.

3 Test Methodology

Based on the ICV's classic system architecture and seven attack surfaces it faces, in this section, a novel Intelligent Connected Vehicle (ICV) Information Security Attack and Defense (ICV-ISAD) test evaluation method is proposed and the

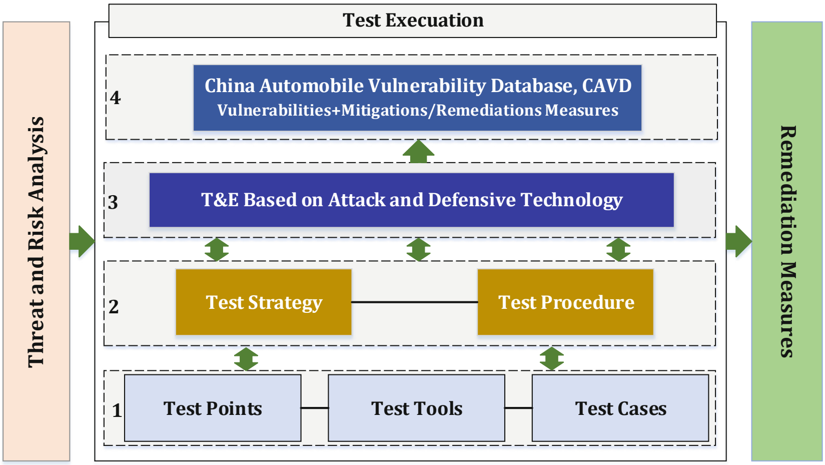

Threat and Risk Analysis
Test Execuation
4
China Automobile Vulnerability Database, CAVD
Vulnerabilities+Mitigations/Remediations Measures
3
T&E Based on Attack and Defensive Technology
2
Test Strategy
Test Procedure
1
Test Points
Test Tools
Test Cases
Remediation Measures

Fig. 3. ICV-ISAD test method architecture

design thoughts of test methodology are presented comprehensively. ICV-ISAD test method shows how to evaluate the information security of the car through testing method that aims to discover security vulnerabilities and threats as well as maps corresponding remediation measures. It is derived from the long-term large number of real automotive test experiments and is constantly optimized in the experiments. In this method, the implementation of the security evaluation realized from three stages, which are Threat and Risk Analysis, Test Execution as well as Remediation Measures.

3.1 Threat and Risk Analysis

Since the dependencies between the vehicle security and the design system architecture described in Sect. 2, there exists a lot of threats and risks for ICV's system or network. In the first stage of ICV-ISAD test method, some threats and risks to the vehicle are considered, respectively. The threat analysis is a process to determine anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy the security of ICV. Table 1 shows an example of threats analysis. Risk analysis is designed to consider the potential for loss, damage or destruction of the vehicle security as a result of a threat exploiting a vulnerability. For an example of risks analysis, see Table 2.

Table 1. Threats analysis

No.	Threat (Vulnerability)	Effect (Attack surface)
1	Compromise of update procedures	IVI
2	Denial of service attacks	IVN, IVI, Mobile App
3	Unprivileged users access to vehicle systems	IVI, IVN
4	Hosted 3rd party software	IVI
5	Network design introduces vulnerabilities	IVN, T-Box, IVI, ECU
6	Physical manipulation of systems can enable an attack	IVI, T-Box
7	Spoofing of messages	IVN, IVI, Radio
8	Man in the middle attack	IVI, T-Box, Radio
9	OBD Diagnostic access	IVN, IVI
10	Unauthorized deletion/manipulation of system event logs	IVI, T-Box
...	...	...

3.2 Testing Execution

In the second stage of ICV-ISAD test method, we will start the testing execution based on the threat and risk analysis. As we can see from the Fig. 3, the stage describes four layers, labeled 1 to 4. Layer 1 is the lowest layer in this stage.

Table 2. Risks analysis

No.	Risk	Effect (Attack surface)
1	Stealing personally identifiable information	IVI, T-Box, TSP
2	Manipulating a vehicle's operation	IVN, IVI, Mobile App
3	Unauthorized vehicle system entry	IVN, IVI, T-Box
4	Compromise of over the air software update procedures	IVI
5	GPS spoofing	Radio
6	Disrupting TPMS signal	Radio
7	The installation package was tampered with	Mobile App
8	Transfer data is hijacked	Mobile App
9	Loss of information in the cloud	TSP
10	Information breach by unintended sharing of data	TSP
...	...	...

Layer 1: Test Baseline Layer. The Test Baseline Layer is the main component in the test execution stage. 335 test points, 733 test cases and 69 test tools are collected in this layer, which are the important part of ICV-ISAD test method. Test points serve as the idea and technical points for the specific implementation of the security test, which are derived from a large number of practical automotive experiments, taking into account the feasibility and applicability. It describes the research ideas and technical points that plays a vital role in the comprehensive security test of automotive components. Some examples of test points are shown in Table 3. Test cases are usually a single step, or occasionally a sequence of steps, to test the correct security behavior or functionality in the design of vehicle, features of objects corresponding to each test points, one part of which is shown in Table 4. Test tools are partly shown in Table 5, which offer the execution of security test and implement quick security analysis to vehicle system function, software binary code and communication traffic packet across multiple automotive units, etc. Many test tools incorporate automatic test capabilities to traversing and discover threats, vulnerabilities and other security problems from the tested objects.

Table 3. Test points

Attack surface	1	2	3	...
IVN	Security access service	Subnet	Gateway	...
T-Box	Key usage	Hash function	SPI bus	...
IVI	Backdoor	Weak token	Port security	...
ECU	CAN bus isolation	Verification level	Secure storage	...
Mobile APP	Decompile	Process injection	Data security	...
Radio	Sniffing	Replay attack	Interference	...
TSP	CSRF vulnerability	Webshell getting	SQL injection	...

Table 4. Test cases

Surface	Test points	Test cases
IVN	Security access	1 Connect the PC to the car through the OBD port
		2 Send 022701 via Vehicle Spy
		3 To test whether the ECU feeds back the seed or not
		4 Observe, analysis and record the results
...	...	...
T-Box	Key usage	1 Confirm whether the encryption key is multi-purpose
		1 Confirm whether the authentication key is multi-purpose
		1 Confirm whether the random number generation key is multi-purpose
		1 Confirm if the digital signature key is multi-purpose
...	...	...
IVI	Backdoor	1 To analyze whether the program has backdoor through the reverse engineering. Such as the hidden browser
	Port security	1 Use nmap to find all open ports
		2 Test whether the opened ports are secure or not
...	...	...

Layer 2: Strategy and Procedure Layer. In Strategy and Procedure (S&P) Layer, we elaborate the thoughts of test strategy and the flow chart of test procedure. The S&P Layer plays a role of bridge between the Test Library Layer and Test and Evaluation (T&E) Layer using for test planning and management. The test strategy is to build a practical test idea and test route based on the test points around a specific test object, such as IVN, ECU, IVI, T-Box, Mobile App, Radio and TSP. Table 6 takes Test Strategy of IVN's Security for an example. The test procedure is a test logic based on test points and test strategies, given in the form of a flow chart. It covers major security test policies such as functional security test, static code analysis, reversing engineering and penetration testing. Test procedure is shown in Fig. 4.

Layer 3: Test and Evaluation Layer. To address the evaluation problem of the security for ICV, the Test and Evaluation (T&E) Layer is deployed in third layer of Test Execution. It focus on evaluating the security defensive capability of vehicle based on the attack and defense technology. Test and Evaluation (T&E) is the process by which a system or components are compared against test points and test strategies according to test procedure. Figure 3 highlights the relationship among the Test Baseline Layer, S&P and T&E Layer. The results are evaluated to assess ICV's security of architecture design.

Table 5. Test tools

No.	Tool name	Function description
1	Burpsuite	Using to analyze network packets
2	jeb2	Decompile apk application
3	Defensics	Fuzz testing by communication protocol
4	IDA-PRO	Decompile and dynamically debug binary file
5	Appscan	To discover vulnerabilities, hosts and services
6	Nmap	Test security of the ports and running services opened
7	Protecode	Analyze, detect and check the known vulnerabilities of binary codes
...	...	...

Table 6. Test strategy for IVN's security

Step	Description
1	Analysis of vehicle network structure and bus type
2	Investigate the open bus service of the OBD interface
3	Call the corresponding test tools for different open services
4	Message reading and analysis
5	Diagnostic service test
6	Denial of service test
7	Brute force cracking test
8	Fuzz testing
9	Summary and analysis

The Test and Evaluation (T&E) involves evaluating an automobile's security from the component level to whole vehicle system as well as its integrated system. Components mainly refer to the units related to seven attack surfaces, such as IVI, T-Box and ECUs. Through black-box, gray-box and white-box testing, it analyzes the security of automotive systems (Fig. 1) to discover unknown vulnerabilities, threats and risks that the car faced based on the seven major attack surfaces (Fig. 2). In the overall execution process of Test and Evaluation Layer, it complies with test strategy and test procedure showed in the S&P Layer. Different test objects and different steps of the test will selectively call the corresponding test points, test tools and test cases in the Test Library Layer.

During the process of security test, Test Baseline Layer and T&E Layer work together under the connection of S&P Layer. For instance, in the security test evaluation of IVI, one of test points is the port security. And all of test process follows to the test procedure and is guided by the test strategies designed in T&E Layer. Specifically, the nmap in the test tools will be called firstly.

Then its test cases corresponding to the port security in the test cases library is going to been matched. Finally the security test of port security will be implemented as follow steps:

1 Use nmap to find all open ports.
2 Test whether the opened ports are secure or not.

Layer 4: Information Security Database. The fourth layer is the information security database, China Automotive Vulnerability Database (CAVD) [18], which is built and operated by Automotive Data Center of China Automotive Technology and Research Center Co., Ltd. It is responsible for collecting the state of the art automotive information security data, such as vulnerabilities, mitigation measures and treatments. These data are mainly derived from the test experiments based on the attack and defense technology and are processed through verification, review, assessment and classification.

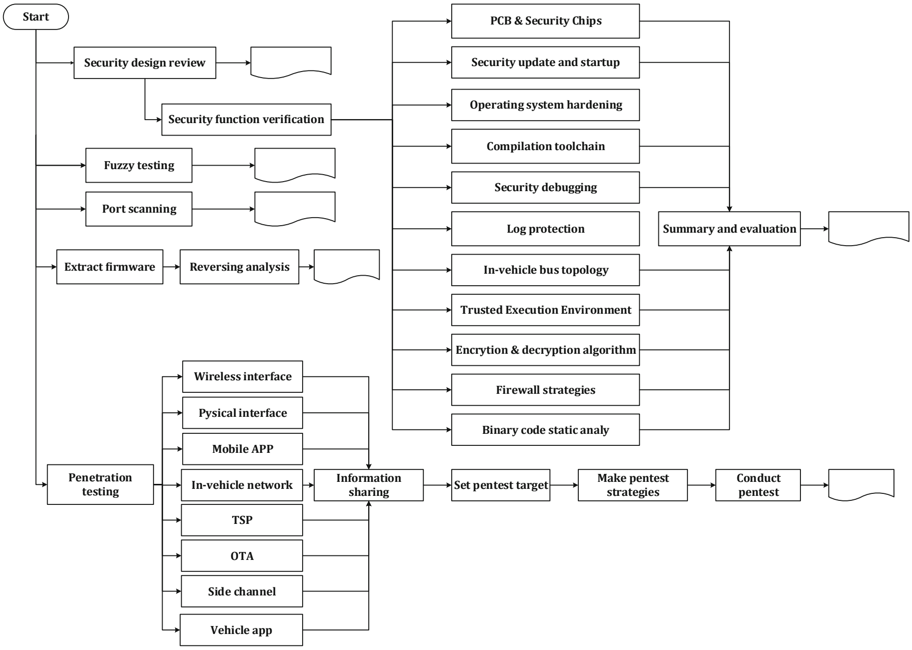


Fig. 4. Test procedure

In addition, as the number of the vehicle's type and testing increases, the data of CAVD would be iterated and updated. Specifically, the vulnerabilities and threats found in the test are matched with that of the CAVD. For the existed vulnerabilities and threats in the library, the corresponding remediation measures or mitigations will be mapped and output from the CAVD. Otherwise for the unknown vulnerabilities and threats, some new protection schemes will be created and stored in the CAVD so as to map the corresponding vulnerabilities or threats next time.

3.3 Remediation Measures

The two stages for test evaluation method of ICV-ISAD have already been mentioned during the presentation of Sects. 3.1 and 3.2. Remediation measures are the output of ICV-ISAD test method. The output function is mainly implemented by the CAVD in the test execution stage. During the period of ICV-ISAD third stage, the basic remediation measures are identified in today's ICV systems that provide some patch recommendations for vulnerabilities to launch attacks based on these test achievements in the first two stages. While this is done with a focus on the vulnerabilities aspects, it also addresses potential threat implications (like those summarized in Table 1), which can arise from successful exploits of vulnerabilities. The ICV's vulnerabilities and threats found in the test are mapped with the CAVD to find the corresponding protection schemes.

4 Test Experimental Results

In our experiments, some different types of cars numbered 1 to 10 were selected to assess the performance of the proposed test evaluation method of ICV-ISAD. The vehicles participating in the experiment have intelligent and connected functions,

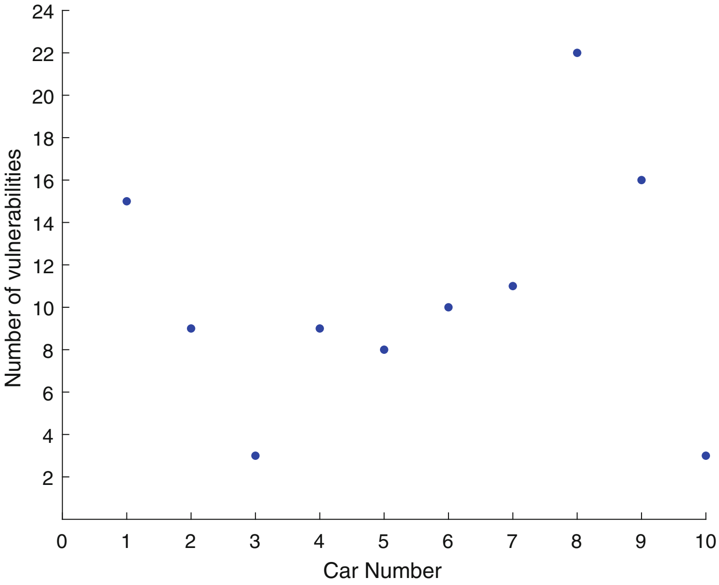


Fig. 5. The number of vulnerability for different car

which generally conform to the system framework shown in Fig. 1 and are faced with seven attack surfaces given in Fig. 2. The test experiment are aimed to evaluate the security of the whole vehicle and their components, such as IVI, T-Box, Mobile App, Radio and TSP, based on the black-box, gray-box and white-box testing.

4.1 Results and Analyses

During the experiments of ICV-ISAD test method, 106 automotive system security vulnerabilities are discovered. As can be seen from Fig. 5, the 10 cars used to the test all have security vulnerabilities, and the average number of security vulnerabilities per car is 10.6. In particular, the number of vulnerability in No. 1, No. 8, and No. 9 cars ranks in the top three.

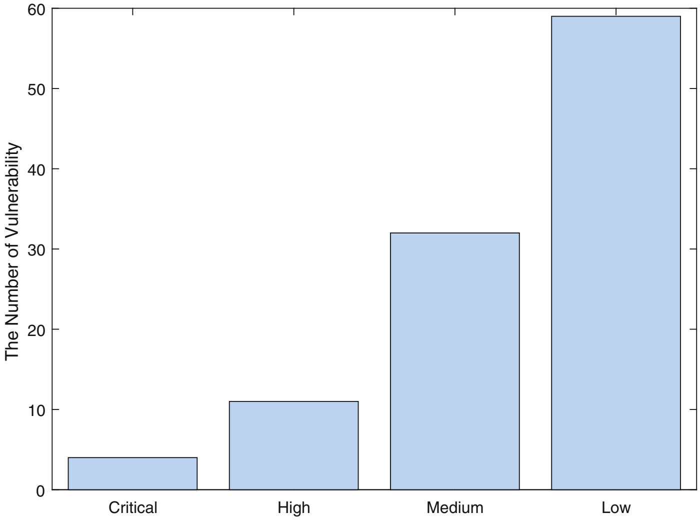


Fig. 6. The number of vulnerability in different severity level

For further analysis, the severity of these vulnerabilities are assessed according to the rule in [19]. The results are shown in Fig. 6, where the bar chart informs us of the fact that there exists 4 critical, 11 high, 32 medium and 59 low vulnerabilities in these cars. The number of vulnerabilities with critical and high levels account for 14.2% of the entire vulnerability, which have a high probability of being successfully exploited to compromise the vehicle remotely. Besides, the proportion of vulnerabilities with medium level is 30.2% in the entire vulnerability. However, once hackers have physical access to the vehicle, these medium vulnerabilities provide great possibilities of destroying the vehicle. Moreover, it can be clearly seen from Fig. 7 that the car's vulnerability covers a large area. They are distributed to various components of the car to varying surface. Three units were found serious vulnerabilities, evolving two in T-Box, one each in Mobile APP and TSP. T-Box, IVI, APP, radios and TSP were discovered vulnerabilities with high level in varying degrees. All of these results indicate that these 10 vehicles have different levels of security risks.

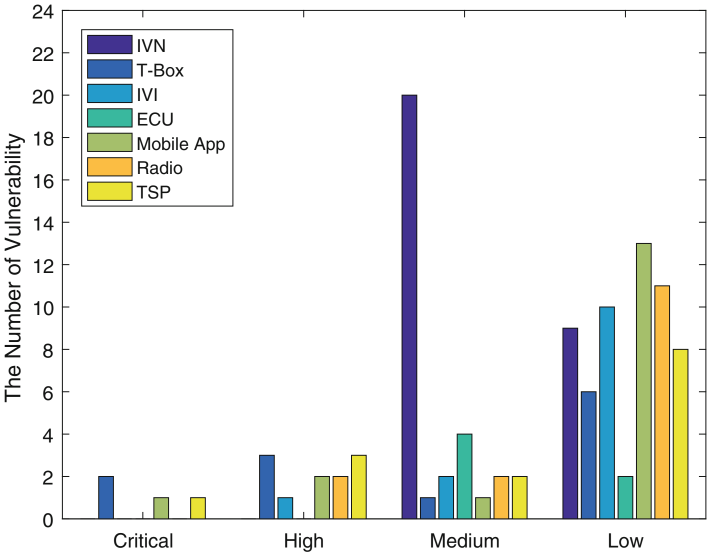


Fig. 7. Vulnerability severity for different vehicle units

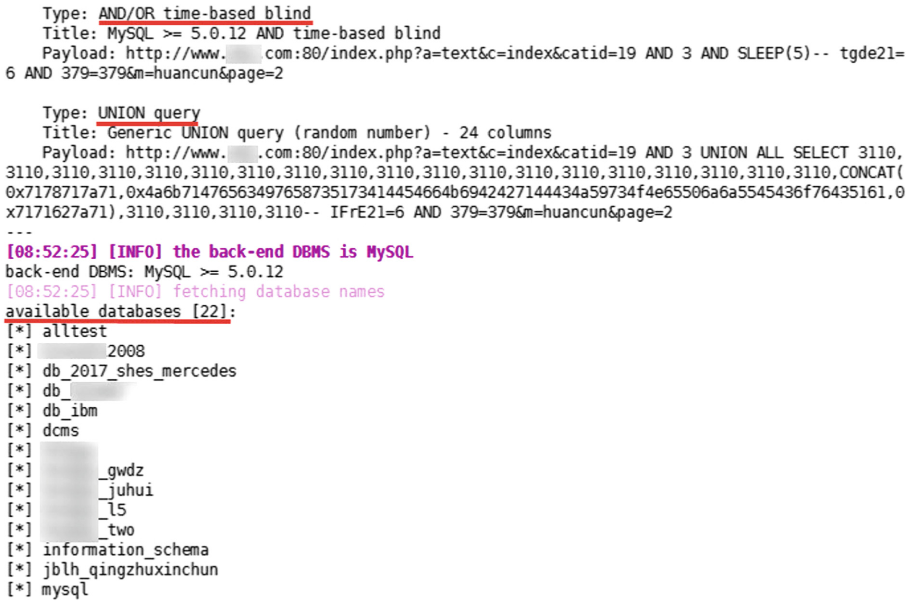
4.2 Typical Vulnerabilities and Threats

In order to better illustrate the efficiency of the ICV-ISAD test method in automotive information security testing and evaluation experiments, we highlight several typical security issues found in the experiments as a result of ICV-ISAD test method, mainly introducing threats and vulnerabilities. Taking into account the privacy protection issues associated with the experimental results, we covered some sensitive information with mosaics.

Radio Vulnerability (Threat). In this paper, the research objectives of radio includes Wi-Fi, Bluetooth, GPS, Wireless Key Fob and Tire Pressure Monitoring System (TPMS).

To evaluate the security of key fobs by using ICV-ISAD test method, GQRX of test tools was called to detect the key frequency band of 315 MHz and 433 MHz at first. Then GNURADIO and USRP of test tools were called to capture and recorded the signal from the wireless key fob. Finally, the effect of the recorded signal was verified by a replay attack to test the security of wireless key fob. The results show that the replay attack is invalid for key fobs encrypted with rolling code, or else the replay attack can open the door and trunk. Specifically, the key fobs of No. 1 and No. 5 car have security risk for having no rolling codes, which can be replay attacked. During the evaluation of GPS security, we tried to cheat and temper the car localization by spoofing GPS signals using radio tools. The results show that it can be performed of GPS spoofing and tempered of the true automotive location if the car locate its position by GPS only, whereas it is difficult to do that in the condition of locating with Wi-Fi, 4G and GPS. In particular, the GPS of No. 1 and No. 3 car have the security risk of spoofing attack for positioning with GPS only.

SQL Injection. Based on the ICV-ISAD test method, when evaluating the TSP security of No. 4 car, we discovered a serious SQL injection vulnerability in one of the TSP's URLs. Specifically, when we stitched the delay string $AND\ SLEEP(5)$ after the one of the TSP's URL, we found that the web page opened after the delay of 5 s, which indicated that its database have executed the spliced URL and it has time-based blind SQL injection. To further verify



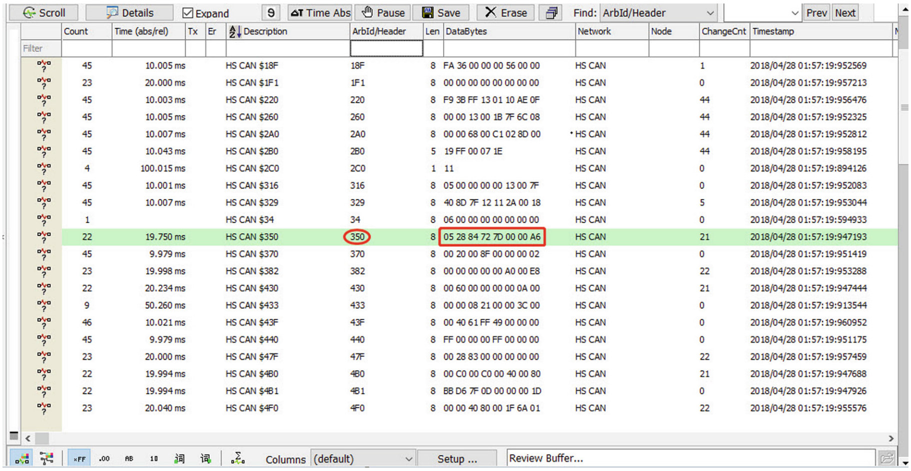
```
    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: http://www.[redacted].com:80/index.php?a=text&c=index&catid=19 AND 3 AND SLEEP(5)-- tgde21=
6 AND 379=379&m=huancun&page=2

    Type: UNION query
    Title: Generic UNION query (random number) - 24 columns
    Payload: http://www.[redacted].com:80/index.php?a=text&c=index&catid=19 AND 3 UNION ALL SELECT 3110,
3110,3110,3110,3110,3110,3110,3110,3110,3110,3110,3110,3110,3110,3110,3110,3110,3110,3110,CONCAT(
0x7178717a71,0x4a6b71476563497658735173414454664b6942427144434a59734f4e65506a6a5545436f76435161,0
x7171627a71),3110,3110,3110,3110-- IFrE21=6 AND 379=379&m=huancun&page=2
---
[08:52:25] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[08:52:25] [INFO] fetching database names
available databases [22]:
[*] alltest
[*] [redacted]2008
[*] db_2017_shes_mercedes
[*] db_[redacted]
[*] db_ibm
[*] dcms
[*] [redacted]
[*] [redacted]_gwdz
[*] [redacted]_juhui
[*] [redacted]_l5
[*] [redacted]_two
[*] information_schema
[*] jblh_qingzhuxinchun
[*] mysql
```

Fig. 8. SQL injection

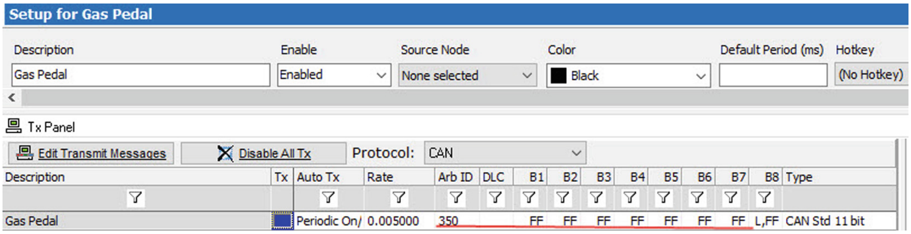
the vulnerability, we detected the address using *sqlmap.py* and found time-based blind SQL injection and union query SQL injection. Besides, a large amount of database information is exposed. As shown in Fig. 8.

Gateway Filtering Vulnerability (Threat). When using the ICV-ISAD test method to evaluate engine-related ECU security, we tested the effects of different ID signals on the vehicle by sending random data. The test results show that the signal corresponding to $ID = 350$ would cause a sudden increase in car speed, as shown in Fig. 9. For further verification, the eight-byte bit data sent by ID of 350 was accurately analyzed. The result shows that the vehicle speed was constantly increasing when all eight bytes were FF, as shown in Fig. 10. The CAN protocol threat can be exploited to compromise the vehicle speed system once hackers have physical access to the vehicle.



Count	Time (abs/rel)	Tx	Er	Description	ArbId/Header	Len	DataBytes	Network	Node	ChangeCnt	Timestamp
45	10.005 ms			HS CAN $18F	18F	8	FA 36 00 00 00 56 00 00	HS CAN		1	2018/04/28 01:57:19:952569
23	20.000 ms			HS CAN $1F1	1F1	8	00 00 00 00 00 00 00 00	HS CAN		0	2018/04/28 01:57:19:957213
45	10.003 ms			HS CAN $220	220	8	F9 3B FF 13 01 10 AE 0F	HS CAN		44	2018/04/28 01:57:19:956476
45	10.005 ms			HS CAN $260	260	8	00 00 13 00 1B 7F 6C 08	HS CAN		44	2018/04/28 01:57:19:952325
45	10.007 ms			HS CAN $2A0	2A0	8	00 00 68 00 C1 02 8D 00	HS CAN		44	2018/04/28 01:57:19:952812
45	10.043 ms			HS CAN $2B0	2B0	5	19 FF 00 07 1E	HS CAN		44	2018/04/28 01:57:19:958195
4	100.015 ms			HS CAN $2C0	2C0	1	11	HS CAN		0	2018/04/28 01:57:19:894126
45	10.001 ms			HS CAN $316	316	8	05 00 00 00 00 13 00 7F	HS CAN		0	2018/04/28 01:57:19:952083
45	10.007 ms			HS CAN $329	329	8	40 8D 7F 12 11 2A 00 18	HS CAN		5	2018/04/28 01:57:19:953044
1				HS CAN $34	34	8	06 00 00 00 00 00 00 00	HS CAN		0	2018/04/28 01:57:19:594933
22	19.750 ms			HS CAN $350	350	8	05 28 84 72 7D 00 00 A6	HS CAN		21	2018/04/28 01:57:19:947193
45	9.979 ms			HS CAN $370	370	8	00 20 00 8F 00 00 00 02	HS CAN		0	2018/04/28 01:57:19:951419
23	19.998 ms			HS CAN $382	382	8	00 00 00 00 00 A0 00 E8	HS CAN		22	2018/04/28 01:57:19:953288
22	20.234 ms			HS CAN $430	430	8	00 60 00 00 00 00 0A 00	HS CAN		21	2018/04/28 01:57:19:947444
9	50.260 ms			HS CAN $433	433	8	00 00 08 21 00 00 3C 00	HS CAN		0	2018/04/28 01:57:19:913544
46	10.021 ms			HS CAN $43F	43F	8	00 40 61 FF 49 00 00 00	HS CAN		0	2018/04/28 01:57:19:960952
45	9.979 ms			HS CAN $440	440	8	FF 00 00 00 FF 00 00 00	HS CAN		0	2018/04/28 01:57:19:951175
23	20.000 ms			HS CAN $47F	47F	8	00 28 83 00 00 00 00 00	HS CAN		22	2018/04/28 01:57:19:957459
22	19.994 ms			HS CAN $4B0	4B0	8	00 C0 00 C0 00 40 00 80	HS CAN		21	2018/04/28 01:57:19:947688
22	19.994 ms			HS CAN $4B1	4B1	8	BB D6 7F 0D 00 00 00 1D	HS CAN		0	2018/04/28 01:57:19:947926
23	20.040 ms			HS CAN $4F0	4F0	8	00 00 40 80 00 1F 6A 01	HS CAN		22	2018/04/28 01:57:19:955576

Fig. 9. Speed control ID


Setup for Gas Pedal

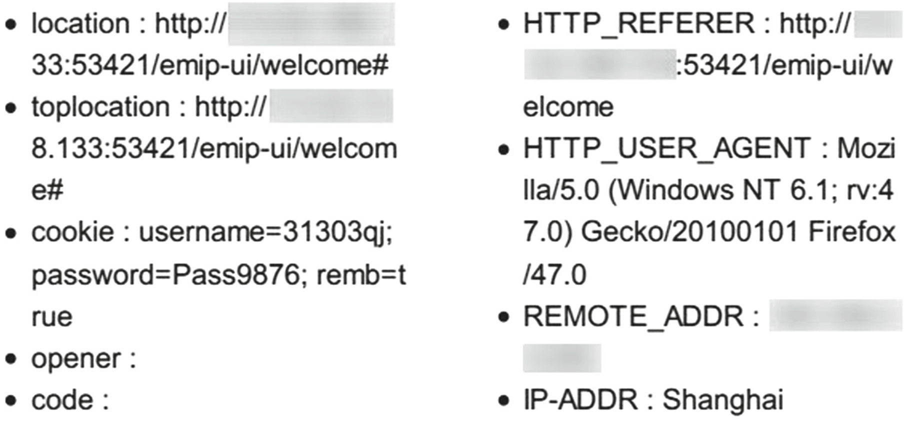
Description	Enable	Source Node	Color	Default Period (ms)	Hotkey
Gas Pedal	Enabled	None selected	■ Black		(No Hotkey)

Protocol: CAN

Description	Tx	Auto Tx	Rate	Arb ID	DLC	B1	B2	B3	B4	B5	B6	B7	B8	Type
Gas Pedal	■	Periodic On/	0.005000	350		FF	FF	FF	FF	FF	FF	FF	L,FF	CAN Std 11 bit

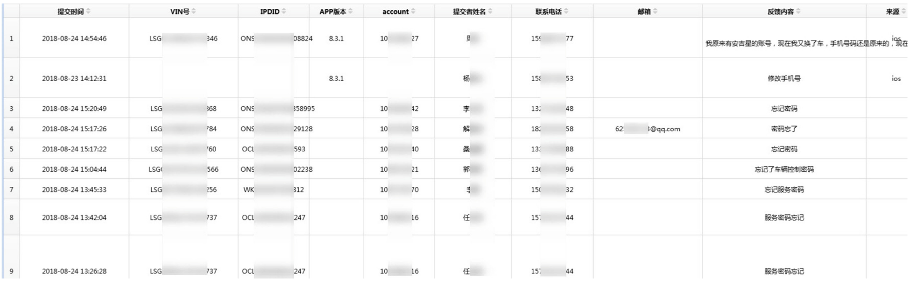
Fig. 10. Speed control by accurate ID message

XSS Vulnerability. Under the test to No. 7 car by ICV-ISAD test method, the feedback communication packets of Mobile APP can be intercepted successfully by Burpsuite. Then we insert the constructed malicious JavaScript into the APP's function of feedback and send it to the server. Through opening the XSS background receiver, we can receive the cookie (username, password) value returned after the malicious code is executed, as shown in Fig. 11. Even more striking, more user personal sensitive information exposed from the server database by further sending the JavaScript with the function of screenshot and reading the website source code again, as shown in Fig. 12.



- location : http://[redacted]33:53421/emip-ui/welcome#
- toplocation : http://[redacted]8.133:53421/emip-ui/welcome#
- cookie : username=31303qj; password=Pass9876; remb=true
- opener :
- code :
- HTTP_REFERER : http://[redacted]:53421/emip-ui/welcome
- HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 6.1; rv:47.0) Gecko/20100101 Firefox/47.0
- REMOTE_ADDR : [redacted]
- IP-ADDR : Shanghai

Fig. 11. The cookie value returned



	提交时间	VIN号	IPDID	APP版本	account	提交者姓名	联系电话	邮箱	反馈内容	来源
1	2018-08-24 14:54:46	LSG[redacted]346	ONS[redacted]08824	8.3.1	10[redacted]27	周[redacted]	159[redacted]77		我原来有安吉星的账号，现在我又换了车，手机号码还是原来的，现在	ios
2	2018-08-23 14:12:31			8.3.1		杨[redacted]	158[redacted]53		修改手机号	ios
3	2018-08-24 15:20:49	LSG[redacted]368	ONS[redacted]358995		10[redacted]42	李[redacted]	132[redacted]48		忘记密码	
4	2018-08-24 15:17:26	LSG[redacted]784	ONS[redacted]29128		10[redacted]28	解[redacted]	182[redacted]58	62[redacted]@qq.com	密码忘了	
5	2018-08-24 15:17:22	LSG[redacted]760	OCL[redacted]593		10[redacted]40	桑[redacted]	133[redacted]88		忘记密码	
6	2018-08-24 15:04:44	LSG[redacted]566	ONS[redacted]02238		10[redacted]21	郭[redacted]	136[redacted]96		忘记了车辆控制密码	
7	2018-08-24 13:45:33	LSG[redacted]256	WK[redacted]312		10[redacted]70	李[redacted]	150[redacted]32		忘记服务密码	
8	2018-08-24 13:42:04	LSG[redacted]737	OCL[redacted]247		10[redacted]16	任[redacted]	157[redacted]44		服务密码忘记	
9	2018-08-24 13:26:28	LSG[redacted]737	OCL[redacted]247		10[redacted]16	任[redacted]	157[redacted]44		服务密码忘记	

Fig. 12. The exposure of user personal sensitive information

4.3 Remediation Measures

In previous work, ICV-ISAD test method was used to evaluate the security of 10 ICVs and 106 vulnerabilities were discovered, especially several typical vulnerabilities and threats were analyzed. To further show its efficiency, in this part, we present some remediation measures or recommendations corresponding to the previous typical vulnerabilities/threats. All of these remediation measures could be mapped from the CAVD database of ICV-ISAD test method, as shown in Table 7.

Table 7. Remediation measures or recommendations

Vulnerability/Threat	Remediation measures & Recommendations
XSS vulnerability	1 Set the value of *httponly* to *true* for vital cookie
	2 To convert character content to *html* entity by using the *htmlspecialchars* function
	3 Filter or remove special *html* tags, such as $< script >$, $< iframe >$
SQL injection	1 Precompile and bind the variables of SQL statements with the function of *PreparedStatement*
	2 Front-end *JS* should have the ability to check for illegal characters
	3 Filter the keywords reserved by the database in the SQL statement, such as AND, OR, EXEC
Gateway filtering	1 OBD port shields each BUS and only reserves diagnostics function
	2 Add hardware Firewalls or other Encrypted Routes to enhance BUS filtering capabilities
Radio vulnerability	1 Protect key fob from *replayattack* by using *rollingcode*
	2 Improve the strength of the wireless key fob's signal encryption algorithm
	3 Use 4G, Wi-Fi and GPS *joint positioning*

5 Conclusion

In this paper, we proposed a novel approach to address the security evaluation problem for ICV based on the attack and defense technology. The proposed ICV-ISAD test method not only helps OEMs secure the car through vulnerability discovery, but also provides the specific remediation measures or recommendations that can be implemented in the vehicle with security risks. Specifically, we explored the ICV's classic system architecture which presents the main automotive units, system buses, and mutual communication relationship, as well as we discussed seven attack surfaces that ICV faces by and large. Based on the classic system architecture and the seven attack surfaces, ICV-ISAD test method has been elaborated from the three stages of threat and risk analysis, test execution, and remediation measures. Also, a special focus has been put to the stage of test execution, which includes the main components and core technologies of ICV-ISAD test method. Experimental results of 10 vehicles security tests show that ICV-ISAD test method can effectively discover security vulnerabilities and threats to evaluate vehicle's security. In addition, some remediation measures or recommendations could be mapped from the CAVD of ICV-ISAD test method to mitigate the corresponding vulnerabilities.

Acknowledgments. The work described in this article has been supported by Automotive Data Center of China Automotive Technology and Research Center Co., Ltd. that provides the laboratory, all the cars, test tools and support required to carry out this research successfully.

The work in this article concerning CAVD has been supported by China Automotive Technology and Research Center Co., Ltd. through the project "Development of Automobile Information Security Vulnerability Database and Emergency Response Platform" under Contract No. 18190122.

References

1. Li, Y.: Big wave of the intelligent connected vehicles. China Commun. **13**(2), 27–41 (2016)
2. Kuang, X.: Intelligent connected vehicles: the industrial practices and impacts on automotive value-chains in China. Asia Pac. Bus. Rev. **24**(1), 1–21 (2018)
3. China prepares to issue temporary 5G licenses to operators. https://technode.com/2019/01/11/chinese-grant-temporary-5g-licence/. Accessed 17 Jan 2019
4. Bécsi, T.: Security issues and vulnerabilities in connected car systems. In: 2015 International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS), Denver, pp. 3–5. IEEE (2015)
5. Parkinson, S.: Cyber threats facing autonomous and connected vehicles: future challenges. IEEE Trans. Intell. Transp. Syst. **18**(11), 2898–2915 (2017)
6. Sadek, A.: Special issue on cyber transportation systems and connected vehicle research. J. Intell. Transp. Syst. **20**(1), 1–3 (2016)
7. Luo, Q.: Wireless telematics systems in emerging intelligent and connected vehicles: threats and solutions. IEEE Wirel. Commun. **25**(6), 113–119 (2018)
8. Mccluskey, B.: Connected cars - the security challenge [Connected Cars Cyber Security]. Eng. Technol. **12**(2), 54–57 (2017)
9. Tesla Model S hacked from 12 miles away. https://www.welivesecurity.com/2016/09/21/tesla-model-s-hack/. Accessed 17 Jan 2019
10. New Car Hacking Research: 2017, Remote Attack Tesla Motors Again. https://keenlab.tencent.com/en/2017/07/27/New-Car-Hacking-Research-2017-Remote-Attack-Tesla-Motors-Again/. Accessed 16 Jan 2019
11. Researchers hack BMW cars, discover 14 vulnerabilities. https://www.helpnetsecurity.com/2018/05/23/hack-bmw-cars/. Accessed 17 Jan 2019
12. Arbabzadeh, N.: A data-driven approach for driving safety risk prediction using driver behavior and roadway information data. IEEE Trans. Intell. Transp. Syst. **19**(2), 446–460 (2018)
13. Jesper, C., Christophe, B.: Nonlinear Optimization of Vehicle Safety Structures: Modeling of Structures Subjected to Large Deformations, 1st edn. Butterworth-Heinemann, Waltham (2015)
14. Siegel, J.E.: A survey of the connected vehicle landscape-architectures, enabling technologies, applications, and development areas. IEEE Trans. Intell. Transp. Syst. **19**(8), 2391–2406 (2018)

15. Sandor, P.: Security and safety risk analysis of vision guided autonomous vehicles. In: 1st IEEE International Conference on Industrial Cyber-Physical Systems (ICPS-2018), Saint-Petersburg, pp. 193–198. IEEE (2018)
16. Li, X.: Connected vehicles' security from the perspective of the in-vehicle network. IEEE Network **32**(3), 58–63 (2018)
17. Hijacking FM Radio with a Raspberry Pi & Wire. https://null-byte.wonderhowto.com/how-to/hack-radio-frequencies-hijacking-fm-radio-with-raspberry-pi-wire-0177007/. Accessed 18 Jan 2019
18. China Automotive Vulnerability Database (CAVD). https://cavd.org.cn/. Accessed 21 Jan 2019
19. CAN Bus Standard Vulnerability. https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-209-01. Accessed 18 Jan 2019