

Research on Cyber-security Risk of In-Vehicle Network Equipment of Intelligent Networked Vehicles

Jue Wang^a, Yueyou Wang^b, Xintian Hou^c

China Automotive Technology and Research Center Co., Ltd., Tianjin, 300000, China

^awangjue@catarc.ac.cn, ^bwangyueyou@catarc.ac.cn, ^chouxintian@catarc.ac.cn

Abstract

The rapid development of intelligent networked vehicles has also raised cyber-security problems, and vehicle cyber-security has become an important part of national security. In order to improve the cyber-security level of intelligent networked vehicles, this paper conducts cyber-security risk analysis for several in-vehicle network equipment with high installation rates in intelligent networked vehicles. Mainly carry out the following aspects: firstly, conduct research on the attack path, attack method and damage caused by security risks; secondly, carry out test verification, and conduct real vehicle tests on the security risks existing in in-vehicle network equipment. This paper is of great significance for guiding the development of vehicle network equipment protection and improving its cyber-security level.

Keywords

Intelligent networked vehicles; In-vehicle network equipment; Cyber-security risk; Cyber-security testing.

1. INTRODUCTION

Intelligent networked vehicle is an emerging industry in which multiple industries such as automobiles and information and communication technology are integrated and developed. It has become an important breakthrough and strategic commanding point for the technological transformation, transformation and upgrading of the automotive industry. The rapid development of intelligent networked vehicles has also caused many cyber-security problems. Different from traditional active safety and passive safety, once a vehicle cyber-security problem breaks out, it will cause the privacy of drivers and passengers, property safety, and endanger the society. stability and national security [1].

In particular, in-vehicle network equipment such as telematic-box (T-Box), in-vehicle infotainment (IVI), in-vehicle gateways, and electronic control units (ECU), as an important part of automotive hardware security, are widely used in intelligent networked vehicles. However, the large-scale application of in-vehicle network equipment also brings serious cyber-security risks. In order to better deal with the hidden dangers of cyber-security, this paper conducts in-depth analysis and verification of the possible security risks of vehicle network equipment, in order to improve the cyber-security protection and response ability of vehicle network equipment, and reduce the possibility of security incidents.

2. IN-VEHICLE NETWORK EQUIPMENT INTRODUCTION

2.1. Vehicle Information Interaction System

Vehicle Information Interaction System refers to the communication system installed on the vehicle, generally refers to T-box, IVI and the hybrid products of the two. The vehicle

information interaction system is mainly composed of GPS unit, external communication interface, electronic processing unit, microcontroller, mobile communication unit, memory and other devices, which can realize the interaction between in-vehicle terminal information and cloud, roadside, etc. Its main functions are shown in table 1, it is mainly used in typical application scenarios such as vehicle-cloud communication, vehicle-vehicle communication, and vehicle-road communication [2].

Table 1. Main functions of vehicle information interaction system

Main Function	Specific Contents
remote control vehicle	remote control of doors, engine, air conditioning, windows, trunk, whistle and flashing lights, upgrades, etc.
communication network	bluetooth communication, 4G/5G, Wifi, mobile Internet, mobile APP, etc.
infotainment	radio, audio playback, video playback, mobile TV, life information query, etc.
assisted driving	integrated electronic map, navigation service, reversing assistance, driving behavior analysis, itinerary management, one-key navigation, etc.
security service	remote diagnosis, road rescue, automatic vehicle alarm, automatic remote upload of vehicle abnormal information, monitoring anti-theft, etc.

2.2. In-vehicle Gateway

In-vehicle gateway is also called the central gateway. Through the isolation between different networks and the conversion between different communication protocols, in-vehicle gateway can exchange information between functional domains that share communication data [3]. In-vehicle gateway is mainly composed of main control chip, communication interface module (CAN interface, vehicle Ethernet interface, etc.), memory and other devices. It is mainly used in typical application scenarios such as in-vehicle communication, its main functions are shown in table 2.

Table 2. Main functions of in-vehicle gateway

Main Function	Specific Contents
route signal	transfer signals between different domains, convert signals, and realize the mapping of signals between different packets
logical processing	participate in logical judgment, process after receiving one or some corresponding signals, and send the processed signals to the corresponding domain
safe isolation	filter abnormal signals, effectively isolate domains, detect and deal with exceptions in a timely manner, etc.
network management	network status monitoring and statistics, error handling, sleep wake-up, signal priority judgment, etc.

2.3. Electronic Control Units (ECU)

Electronic control unit is a control device on the vehicle that realizes a series of functions such as data analysis, processing and transmission. It can collect the signals of each sensor to perform operations, and convert the results of the operations into control signals to control the

controlled object [4]. Its key components include main control chip, input/output interface (I/O), analog-to-digital converter (A/D), memory, etc. With the development of automobile intelligence and networking, more and more ECUs are deployed in automobiles, such as advanced driver assistance system (ADAS), electronic anti-lock braking system (ABS), etc.

3. CYBER-SECURITY RISK ANALYSIS

3.1. Cyber-security Risk of Vehicle Information Interaction System

The vehicle information interaction system is an important node for network interaction inside and outside the vehicle. Once attacked, it will cause major security risks. The common cyber-security risks of vehicle information interaction system mainly include the following aspects:

One is the risk of sensitive information leakage. At present, almost all vehicles equipped with the information interaction system upload driving data such as speed, fuel volume, fault information, and geographic location to the cloud server, and a small number of vehicles upload data such as reversing images and pictures. Attackers can intercept external communication data (such as geographic environment information, personal information, etc.) through eavesdropping, hijacking and other methods to carry out illegal activities, threatening national security or causing leakage of sensitive personal information.

The second is the risk of open port attacks. On the one hand, vehicle information interaction system has multiple open service ports, if the port protection mechanism is weak, it is easy for attackers to illegally use it to obtain advanced management rights, and then can send illegal control commands to the vehicle to control the vehicle. On the other hand, the vehicle information interaction system has multiple short-range communication ports, and attackers can use these ports to carry out network attacks on the vehicle information interaction system service, and there are security risks such as wifi hijacking, bluetooth vulnerabilities, and malicious USB installation.

The third is the risk of illegal vehicle control. The function of remote vehicle control has become a key function of vehicle information interaction system. Remote vehicle control refers to the function of remotely using a mobile phone to change the state of the vehicle, including but not limited to functions such as opening and closing doors, starting the engine, opening and closing the air conditioner, and opening and closing the windows. An vehicle information interaction system with the function of sending vehicle control commands, attackers can obtain control authority of the cloud platform through man-in-the-middle attacks and send vehicle control commands to the vehicle information interaction system, and the attacker can control the vehicle in real time and in batches. Affect personal and property safety, and even social and public safety.

The fourth is the risk of vehicle APP trojan implantation. At present, there are a large number of APPs in the vehicle information interaction system, which are mainly provided by third-party software suppliers, and the vehicle enterprises have limited control over them. Moreover, the vehicle app is different from the mobile app, in addition to the risk of data leakage, attackers can also use DNS hijacking to implant trojan horses on the vehicle to further gain system control rights.

3.2. Cyber-security Risk of in-vehicle Gateway

As the network communication center, the in-vehicle gateway is usually at the end of the remote attack chain, once breached, the attacker can control the functions of the entire vehicle through the in-vehicle network. Common cyber-security risks of in-vehicle gateway mainly include the following aspects:

One is the risk of malicious instruction spreading. Attackers can issue malicious instructions, illegal control instructions, high-frequency flood attack instructions, etc. by impersonating legitimate users. If the gateway is deceived and forwards illegal attack instructions, it will lead to malicious acceleration, functional failure of the entire vehicle, network paralysis, vehicles cannot run normally, and in severe cases, it will lead to regional traffic paralysis and cause social panic.

The second is the risk of illegal invasion. Attackers can connect to the OBD interface and send various messages such as diagnosis and control to the vehicle gateway. If the gateway forwards the control messages, it will affect various components of the vehicle. In severe cases, it will lead to the restart of the power domain controller, the vehicle gear shift, and the emergency stop of the vehicle, threatening the personal safety of drivers and passengers.

3.3. Cyber-security Risk of Electronic Control Unit

The limitations of ECU computing resources and capabilities make it difficult to design effective security solutions, and it is difficult to directly deploy traditional security mechanisms to ECU. In addition, with the increasing number of ECU functions on the vehicle, the amount of code implemented also increases, and the potential code vulnerability problem becomes more and more prominent. The common cyber-security risks of ECU mainly include the following aspects:

One is hardware security risk. In order to facilitate maintenance and debugging, there are a large number of readable silkscreens and exposed debugging ports on the ECU hardware of current vehicles, which are prone to anti-reverse analysis.

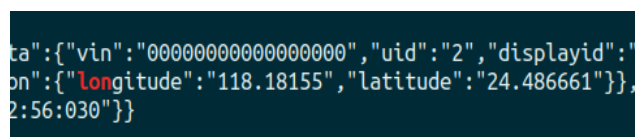
The second is firmware security risk. At present, the firmware flashing mechanism of most ECUs is not protected by network security, which may cause the ECU firmware or its configuration data to be tampered with, affecting the driving safety of the vehicle.

The third is the risk of executing illegal software upgrade tasks. Attackers can tamper with or forge software upgrade packages, build illegal software upgrade tasks, and affect the normal functions of the vehicle.

4. TEST VERIFICATION

In order to verify the common cyber-security risks of in-vehicle network equipment, the penetration test was used to conduct network security tests on in-vehicle network equipment of several models, and the experimental results were analyzed [5].

(1) Carry out a test on the vehicle information interaction system of a certain vehicle model, check the log and export it, and use the regular search method to check whether the system contains sensitive data. The test results show that the vehicle information interaction system of the vehicle model has leakage of positioning coordinate information, and there is a risk of sensitive information leakage.



```
ta":{"vin":"0000000000000000","uid":"2","displayid":"0
on":{"longitude":"118.18155","latitude":"24.486661"}},
2:56:030"}}
```

Figure 1. Positioning coordinate information leakage

Carry out a test on the vehicle information interaction system of a certain vehicle model, and through port scanning, it is found that some ports in the system are open, use the Android system debugging tool adb to connect the port to enter the system, and then obtain the highest

control authority, and find a large amount of sensitive information such as private keys, certificates, and passwords. The test results show that the vehicle information interaction system of this model has the risk of open port attack.

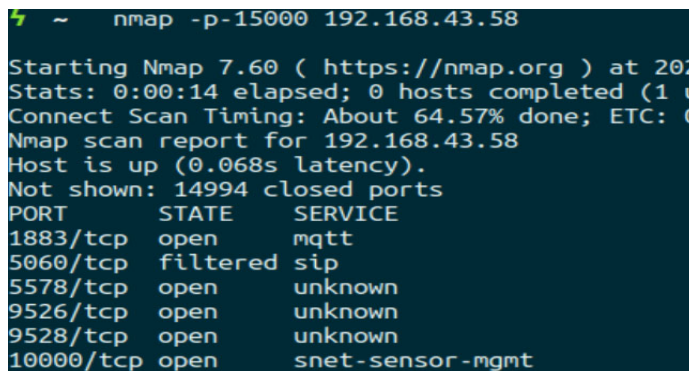


Figure 2. Port scanning result

Carry out a test on the vehicle gateway of a certain vehicle model, by constructing abnormal data frames, and detecting whether the gateway port receives data frames with abnormal periods. The results show that the tester sends periodic data frames that do not conform to the definition of the communication matrix, detects the received data frames at the designated destination port, and can still receive abnormal periodic data frames. The test results show that the vehicle gateway of this model has the risk of spreading malicious instructions.



Figure 3. Abnormal period data frame acceptance

Carry out a test on the ECU of a certain vehicle model, by tampering with the upgrade check bit and data bit of the upgrade package and reprogramming, verify whether the system will verify the modified core firmware. The test results show that after modifying the upgrade check digit, the upgrade software prompts that the programming fails, but the actual programming is successful, and it can also be started normally. Therefore, the ECU of this model has the risk of executing illegal software upgrade tasks.

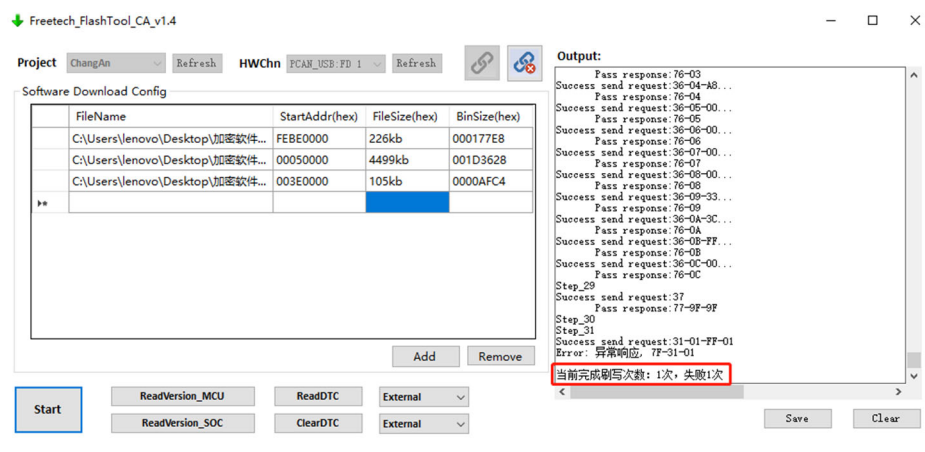


Figure 4. The upgrade software prompts that the programming failed



Figure 5. ECU starts normally

5. 5. CONCLUSION

This paper studies and analyzes the possible cyber-security risks of the in-vehicle network equipment of the intelligent networked vehicle. It is found that the common security risks of the vehicle information interaction system are the risk of sensitive information leakage, the risk of open port attack, the risk of illegal vehicle control and the risk of vehicle APP trojan implantation; The common security risks of in-vehicle gateway are the risk of malicious instruction spreading and the risk of illegal invasion; The common security risks of ECU are hardware security risk, firmware security risk and the risk of executing illegal software upgrade tasks. Through penetration test, the possible safety risks of different models are verified and analyzed. This paper has guiding suggestions for carrying out the protection measures of intelligent networked vehicles, and is of great significance to improve the cyber-security level of in-vehicle network equipment.

ACKNOWLEDGMENTS

This paper is supported by the company and the technical team. Thanks to the company for providing the experimental platform and test vehicle for this paper, the team members for providing technical support and guidance, and the company leaders for their concern.

REFERENCES

[1] Rizvi S , Willet J , Perino D , et al, "A Threat to Vehicular Cyber Security and the Urgency for Correction", Procedia Computer Science, 2017, 114:100-105.

- [2] Anonymous, "Global light vehicle OE connectivity market - forecasts to 2031 - 2016 Q3 Edition: In-vehicle infotainment (IVI)", ProQuest Journal, 2016. PP 38-67.
- [3] Jin S P , Kim D H , Suh I H , "Design and Implementation of Security Function According to Routing Method in Automotive Gateway", International Journal of Automotive Technology, 2021, 22(1):19-25.
- [4] Zhang J , Liao Z , Zhu L , "Research on Design and Implementation of Automotive ECUs Software Remote Update", Applied Mechanics & Materials, 2015, 740:847-851.
- [5] Wu W, "A Survey of Intrusion Detection for In-Vehicle Networks", IEEE Transactions on Intelligent Transportation Systems, 2019, PP(99).