Research on cyber security risk of telematics box in intelligent connected vehicle

Chao Ma*, Hao* Zhao* and *Tong* Wang

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

Abstract. With the rapid development of the automotive industry and the wide application of 5G network technology, there are more and more Telematics Box (T-Box) equipped with intelligent operating systems in vehicles and they are becoming more and more complex. Because it is connected to the on-board CAN bus internally and interconnects with mobile phone /PC through the cloud platform externally, the security of T-Box must be fully guaranteed, to make the automotive more secure. T-Box can realize remote control function, so the T-Box information security problem has been paid more and more attention. In this paper, the T-Box were tested from multiple dimensions by using various methods, and the results were statistically analyzed, and the corresponding protection strategies were proposed for the corresponding security risks.

Keywords: Intelligent connected vehicles, T-Box, Cyber security, Risk analysis.

1 Introduction

With the rapid development of Internet, artificial intelligence, cloud computing, big data and other technologies, the Internet of Things (IoT) technology, which takes the Internet of Everything as its target, is developing rapidly, and the Internet of Vehicles (IoV) is the typical application of IoT technology in the traditional automotive industry. Typical IoV system is divided into three modules, namely, on-board intelligent terminal, network transmission and cloud platform. The main goal is to realize the communication between vehicles and people, vehicles and vehicles, vehicles and subgrade equipment, and vehicles and cloud platform [1]. On-board sensing equipment is used to perceive the conditions inside and outside the vehicle, collect real-time road traffic conditions and other information, and transmit it to the cloud platform for analysis and calculation through wireless network, so as to provide real-time and accurate road navigation, emergency rescue and other comprehensive services for the networked vehicle [2]. While the Internet of Vehicles technology brings intelligent experience to users, it also faces risks in information security. T-Box is known as the bridge of communication with the cloud. As a system for information exchange between the inside of the automotive and the outside

* Corresponding author: zhaohao@catarc.info

world, the main function of T-Box is to realize the communication between the automotive and the cloud platform of Internet of Vehicles, which is the core part of Internet of Vehicles. T-Box is an embedded system integrating OBD, MCU/CPU, FLASH, SENSOR, GPS, 3G/4G, Wi-Fi/ Bluetooth and other modules. Internally, it is connected with the on-board CAN bus, and externally, it is connected with mobile phone /PC through the cloud platform. T-Box can mainly achieve remote control, remote query, security services and other functions [3]. Such as: Remote control doors; Air conditioning; Remote vehicle positioning and vehicle condition information query. As an integral part of intelligent connected vehicles, T-Box has been more and more welcomed by vehicle manufacturers and consumers [4].

T-Box is directly connected to the bus inside the car, through the T-Box can get the automotive data from the bus to the user, the user can also send instructions to the bus inside the automotive through the T-Box, to realize the control of the car. With the more and more extensive application of networked automotive technology, T-Box also brings more information security risks to automotive [5]. For example, in 2018, the BBC reported that research by a Chinese Internet security lab showed that hackers could hack into the T-Box by inserting a USB flash drive, using Bluetooth, and the car's own 3G/4G data connection to gain partial control of the automotive while it was moving. This undoubtedly poses a huge threat to the safe driving of vehicles, so it is urgent to strengthen the information security protection of T-Box [6]. On the one hand, T-Box can communicate with the bus inside the automotive to realize the transfer of instructions and information. On the other hand, its built-in modem can interact with the IoV service platform through data network, voice, SMS, etc., which is the link of information interaction between inside and outside the vehicle. T-Box mainly faces several security threats: one is firmware reverse analysis, attackers through reverse analysis of T-Box firmware to obtain encryption algorithm and key, decrypt communication protocol, for eavesdropping or forgery instructions. The second is information theft. Attackers read internal data through the T-Box reserved debugging interface for attack analysis, or obtain user communication data by capturing data packets of communication ports.

2 T-Box cyber security test and analysis

T-Box is the link between inside and outside the vehicle, so it is very important to ensure the safety of T-Box communication. This project conducted an in-depth study on the current security status of T-Boxes for intelligent on-board terminals of intelligent connected vehicles, conducted multi-dimensional security testing and analysis on five T-Boxes(B-026J/B-029C/B-010C/B-020C/B-019C), and finally summarized statistics and analysis on the information security test results of each type of T-Boxes.

2.1 Test method and process

In this paper, signal deceiving, brute force cracking and other testing methods were adopted and related safety guidelines were referred to. By means of IDA, Kali Linux, Wireshark, GDB, CANOE and other tools, 5 T-Boxes were tested for attack, and the repair and improvement suggestions were put forward for the defective T-Box system.

2.1.1 Hardware security testing

Blow PCB chip, reverse extract chip data EMMC/SOC/MCU and storage unit, and analyze the extracted data. Connect the Wi-Fi hotspot, scan the T-Box with the scanning tool and

carry out network/data attack through the USB interface. During the T-Box work, key data signals were monitored and analyzed, while MCU and SoC communication attacks and MCU and CAN communication attacks were carried out[7].

2.1.2 Data security testing

Through the use of SSH and other tools, detect whether there is a configuration file in the file system and whether the onboard memory/controller internal data is encrypted. Scan and test T-Box static files, message data, code data and storage data, and check personal privacy information and location information in the file system through the T-Box hot spot connection.

2.1.3 Application of security testing

By connecting the T-Box hot spot, login SSH service to obtain the system permissions, use the command to view the system kernel update version, check whether the patch is installed in time. Install malicious software into the system, check whether there is a monitoring mechanism in the system to record the running process of malicious software and check whether the malware can run normally, determine whether there is a protective mechanism in the system and whether the protective mechanism is effective. By testing the attack, you can check whether the Linux application is installed with protection, whether the firewall is configured with security policy, whether the system is enabled with anti-stack overflow attack, and whether there are kernel vulnerabilities[8].

2.1.4 System safety test

Connect the T-Box hot spot, log in the SSH service, traverse the file system, get the upgrade package, download the upgrade package to the local, check whether the upgrade package can be opened normally, unpack the upgrade package, and mount the upgrade image to modify the configuration file locally to replace the upgrade package. In this process, the man-in-the-middle attack tool is used to hijack the upgrade and steal the upgrade data.

2.1.5 Network communication security test

To reconstruct the cellular data network by using the pseudo base station and shielding room, to connect the T-Box network to the pseudo base station network, monitor the T-Box communication packet, and analyze it to find the sensitive data. Log in SSH and use the packet capture tool to analyze the network card data. Connect the T-Box hot spot, scan with the port scan tool and analyze the scan results[9].

2.2 Test result

2.2.1 Security vulnerabilities amount statistics

According to the statistical analysis of the test results, B-026J and B-029C T-Boxes have the largest number of vulnerabilities, up to 4, followed by B-010C T-Box, up to 2. B-020C and B-019C T-Boxes have good security performance, only one security vulnerability was found. This is shown in Table 2.1.

Table 1. T-Box vulnerabilities amount.

T-Box	B-026J	B-029C	B-010C	B-020C	B-019C
Amount	4	4	2	1	1

2.2.2 Security vulnerabilities type statistics.

As shown in Table 2.2 and 2.3, the number of communication port vulnerabilities and system upgrade vulnerabilities in the five T-Boxes is large. Among them, the communication port vulnerability appeared the most times, reaching 4 times, accounting for as high as 33%. The type of replay attack vulnerability has the least number of occurrences, which is 1, accounting for 8%. Although this type of vulnerability appears less frequently, security problems can not be ignored, because this type of security vulnerability will bring a very serious threat to the security of intelligent vehicles.

Table 2. T-Box vulnerabilities types.

Types	Communication port vulnerability	System Update Vulnerability	Information disclosure vulnerability	Hardware vulnerability	Replay attack vulnerability
Amount	4	3	2	2	1

Table 3. T-Box vulnerabilities types proportion.

Types	Communication port vulnerability	System Update Vulnerability	Information disclosure vulnerability	Hardware vulnerability	Replay attack vulnerability
Proportion	33%	25%	17%	17%	8%

2.2.3 Security vulnerabilities hazard level statistics.

According to the scope of influence, the way of use, the consequences of the attack and so on, the hazard can be divided into low risk, medium risk, high risk and serious four grades. The test results showed that among the four categories, high-risk vulnerabilities were the most common, accounting for 42% of the total number of high-risk vulnerabilities, 33% of the total number of medium-risk vulnerabilities, and 8% of the total number of serious vulnerabilities. This is shown in Table 2.4. We should promptly strengthen the repair and protection of high - and medium-risk loopholes.

Table 4. T-Box vulnerabilities hazard proportion.

Types	Low level	Medium level	High level	Critical level
Proportion	17%	33%	42%	8%

2.3 Vulnerabilities distribution

2.3.1 Published vulnerabilities

Known vulnerability refers to the open vulnerability existing in the application or component used in the system. Since these vulnerabilities are all public vulnerabilities, most of them have open vulnerability exploitation procedures. Although in the embedded system in the car, these vulnerabilities are very harsh conditions to use, but the existence of open vulnerabilities is still a potential security hidden trouble, its security problem has been

paid more and more attention. By analyzing the component vulnerabilities of the tested models, it is found that there are 66 components with vulnerabilities, with a total of 1022 public vulnerabilities, as shown in Figure 2.1.

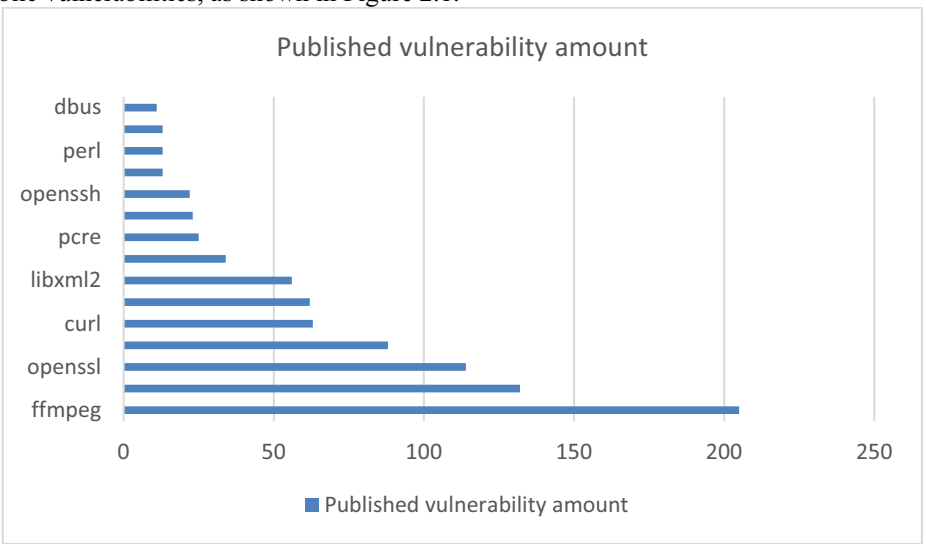

Fig. 1. Published vulnerability amount.

Among these component vulnerabilities, ffmpeg and tcpdump are the most vulnerable components, accounting for 20% and 12% of all component vulnerabilities respectively. These leaky components are common in the Linux system's native applications. This is shown in Table 2.5.

Table 5. Published vulnerability proportion.

Name	ffmpeg	tcpdump	openssl	glibc	curl	freetype
Proportion	21%	12.5%	9%	8%	6%	5%

2.3.2 Unreleased vulnerabilities

Compared with the known vulnerability, the unknown vulnerability is to scan the binary files existing in the system through the binary static vulnerability scanning tool to find the possible vulnerability in the program code. After analysis, most of these unknown vulnerabilities are located in the calls of functions such as read, fscanf, fread, scanf, accept, connect, etc., and the security problem is Unchecked Return Value. This kind of vulnerability may lead to buffer overflow, null pointer de-reference and other serious security problems. For other function calls, also need to pay attention to the return value check, to ensure that the function is safe to use. This is shown in Figure 2.6.

Table 6. Unreleased vulnerability proportion.

Name	fscanf	read	fread	accept	scanf	connect
Amount	311	276	79	66	60	58

3 T-Box Security Policy

T-Boxes are widely used in two broad categories: security-related applications and other applications. Safety-related applications are primarily used to assist driving and may prevent an accident from worsening in life-threatening situations. This type of security is mandatory because any operation of these applications must be secured even if they are being hacked. Other applications include traffic optimization, GPS service, infotainment and so on[10]. The purpose of such applications is to facilitate life. Such applications will generate a large amount of personal privacy data related to users in the process of using them, so security issues must also be paid attention. Based on the above test results and analysis, this paper provides protection strategies from four aspects.

3.1 Hardware protection

Hardware protection is the lowest level of protection measures for cars. The protection of intelligent networked vehicles must start from Hardware protection[11]. Now the relevant enterprises develop Hardware Security Module (HSM) to embed encryption algorithm, access control and integrity check into the automotive control system to strengthen the Security of ECU, to enhance safety levels.

For example: Hide the debug interface in PCB board; The PCB screen printing, chip type and other information is cleared, by hiding these chip information to increase the difficulty of sensitive chips and components to be identified; At the same time, remove the firmware download interface from the cloud, and use a chip with read-write protection and storage capability, which can be set to make the device unreadable[12].

3.2 Data and communication protection

Communication is the most important function of contemporary intelligence made cars, in order to improve the whole security of intelligent made cars, must strengthen the protection of vehicle network communication, such as configuring security strategy in the T-Box, limited network access address, communication port, communication protocols, strengthen the network access control: sensitive information to avoid using log printout way; Avoid hard coding to store sensitive information such as user name, password and key[13]. The private information is transmitted in the form of soft coding and encryption; Sensitive data is encrypted by complex encryption method to avoid plaintext storage. HTTPS and other encryption protocols are used for data transmission in remote communication. Secure stores the public and private keys used to decrypt data.

3.3 Operation system protection

In order to strengthen the data privacy security of users and connected vehicles, it is necessary to strengthen the overall protection of the system and close common dangerous ports, such as 21, 22, 23, 5555, etc. Set firewall filtering rules; Update the application of port in time; Pay attention to kernel bugs and update system kernel timely; Increase the complexity of the system's highest user name and password [14].

3.4 Application protection

In the process of system development, when using third-party components, it is necessary to pay attention to their security status and update them to the latest version in time. In the

process of system development, it is recommended to comply with MISRA 2012 and CERT-C programming specifications; Add a anti-debug mechanism to identify if the application is being debugged or to disable the debugger to prevent attackers from using the debugger to observe the application as it runs; Increase code confusion and convert code into a form that is equivalent but difficult to read and understand[15].

4 Conclusion

As on-board systems become more sophisticated and complex, T-Boxes will become more ubiquitous and more intelligent. This paper first introduces the development of T-Box and the information security problems in the development process, and for the security threats T-Box faces in the Internet of vehicles environment. Take advantage of, threats, brute force signal test method in view of the existing five smart T-Box from the multi-dimensional information security test and the corresponding test results of statistics and analysis, according to the test and analysis results, from the hardware, communications, system and application of four aspects, proposed the corresponding protective measures. In this paper, through the test analysis of a number of T-Boxes, aimed at the rapid development of intelligent networked vehicles in the environment to design a more safe and intelligent T-Box to propose ideas[16].

This work was financially supported by China Automotive Technology Research Center Co., Ltd., Guideline Project-20223405 fund.

References

1. Miller C, Valasek C. Remote exploitation of an unaltered passenger vehicle[J]. Black Hat USA, 2015.
2. M. Wazid, A. K. Das, S. Shetty, and M. Jo, “A tutorial and future research for building a blockchain-based secure communication scheme for Internet of intelligent things,” IEEE Access, vol.8,pp. 88700–88716, 2020.
3. J. Petit and S. E. Shladover, “Potential cyberattacks on automated vehicles,” IEEE Trans. Intell. Transp. Syst., vol. 16, no. 2, pp. 546–556, Apr. 2015.
4. P. Kapoor, A. V ora, and K.-D. Kang, “Detecting and mitigating spoofing attack against an automotive radar,” in Proc. IEEE 88th V eh. Technol. Conf. (VTC-Fall), Aug. 2018, pp. 1–6.
5. Cassias I, Kun A L. Vehicle Telematics: A Literature Review[J]. 2007.
6. I. Rouf et al., “Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study,” in Proc. USENIX Secur. 19th USENIX Conf. Secur., 2010, pp. 1–16.
7. K. Koscher et al., “Experimental security analysis of a modern automotive,” in Proc. IEEE Symp. Secur . Privacy, May 2010, pp. 447–462.
8. Yu He. Research on Information Security of Networked Vehicles and Abnormaldetection Technology of CAN Bus [D]. China National Knowledge Infrastructure,2016:1-68.
9. Wu Chenxu. Research on Key Technology of Vehicle Internal Network Security for Internet of Vehicles [D]. CNKI,2018:1-75.
10. YANG Zhe. Research on Safety Mechanism and Key Technologies for Internet of Vehicles [D]. China National Knowledge Infrastructure,2019:1-80.

11. Vehicle network security white paper [EB/OL]. China Academy of Information and Communications Technology,2017:1-43.]
12. Yang Chunying. Research and implementation of identity authentication technology for Internet of Vehicles [D]. China National Knowledge Infrastructure,2017:1-68.
13. Sun Yanan. Research and Implementation of Safety Reinforcement Technology for Vehicle-mounted Communication Terminal [D]. China National Knowledge Infrastructure,2018:1-73.
14. YU He. Research on Information Security of Networked Vehicle and Abnormal Detection Technology of CAN Bus [D]. China National Knowledge Infrastructure, 2018:1-30.
15. PENG Min. Design and Application of automotive Signal Warning System Based on Wireless Sensor Network [D]. China National Knowledge Infrastructure, 2018:1-40.
16. Li Zhitao. Research and Analysis of Vehicle-mounted Ethernet [D]. China National Knowledge Infrastructure, 2018:1-25.