ISSN: 2664-9640

Research on Security Risks and Testing Methods for Outbound Data Transfer of Intelligent Connected Vehicles

Jue Wang [a], Junda Li [b] , Xintian Hou [c], Xuebin Shao [d] and Weinan Ju [e]

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

[a] wangjue@catarc.ac.cn, [b]lijunda@catarc.ac.cn, [c] houxintian@catarc.ac.cn,

[d] shaoxuebin@catarc.ac.cn, [e] juweinan@catarc.ac.cn,

Abstract

With the rapid development of automotive intelligence and networking, vehicles are accompanied by a large number of data interaction scenarios. Facing the new characteristics, problems, and risks of outbound data transfer in the development of the intelligent connected vehicle industry. This article studies the outbound data transfer issues generated in typical scenarios of intelligent connected vehicles, mainly focusing on the following aspects: firstly, it studies the characteristics and security risks of outbound data transfer; secondly, it proposes a method for detecting abnormal outbound data transfer and conducts verification. This article is of great significance in guiding the automotive industry to regulate outbound data transfer activities and improve its data security level.

Keywords

Intelligent connected vehicles, Outbound data transfer, Data security risks, Data-security testing.

1. Introduction

With the vigorous development of the digital economy, cross-border data activities are becoming increasingly frequent, and the demand for data processing personnel to outbound data is growing rapidly. With the rapid development of automotive intelligence and networking, there are a large number of data exchange scenarios associated with automobiles. Especially intelligent networked vehicles, there are important data security issues such as cross-border transmission and personal information leakage. Intelligent connected vehicles collect important data such as the surrounding road environment and traffic flow, and also carry a large amount of user information interaction. If these data is leaked, stolen, tampered with, damaged, lost, or illegally used during the outbound process, it will bring data security, network security, social and public security, and even national security risks [1].

In order to prevent potential national security, social security, and personal information security issues caused by outbound data transfer, a regulatory system is gradually being constructed; With the increasing level of intelligent networking in automobiles, the demand for data outbound from multinational enterprises in the automotive industry is increasing, and related security risk events have repeatedly become a hot topic of social concern; At the same time, the automotive industry, as an industry with rich data processing types, large data volumes, long data flow chains, and high data sensitivity, urgently needs to standardize outbound data transfer. In response to the above issues, this article summarizes the safety risks of outbound data transfer in the automotive industry based on the current situation of the industry[2]. At the same time, a outbound data transfer testing method based on abnormal flow of vehicle data is proposed, which can effectively identify abnormal data outbound behavior

ISSN: 2664-9640

generated by vehicles, avoid the occurrence of illegal data outbound behavior, improve the data security level of the automotive industry, and assist in the healthy development of the industry.

2. Characteristics and Main Scenarios of Intelligent Connected Vehicles Data Outbound

2.1. Characteristics of Intelligent Connected Vehicles Data Outbound

2.1.1. Data outbound behavior is common

In order to optimize algorithms, automotive companies may transmit geographic environment information and personal sensitive information collected by sensors such as internal and external cameras as research and development data overseas. Some foreign and joint venture car companies transmit their car VIN codes, employee information, user information, etc. overseas or allow foreign parties to access and view them.

2.1.2. Complex and diverse scenarios for outbound automotive data

Intelligent connected vehicles are gradually extending to services such as transportation, entertainment, and daily life, and with the increase of application scenarios, the types of car data are constantly enriched. For example, more and more mass-produced vehicles are starting to be equipped with new technologies such as autonomous driving, intelligent cockpit, and high-precision maps, attempting to introduce new features such as sentry mode, remote photography, high-precision positioning, and V2X[3].However, the interaction scenarios of automotive data involve vehicle cloud communication, vehicle to device communication, and vehicle to vehicle/road communication, among which the risks and hidden dangers of data export are more prominent. For example, geographic environment information collected by sensors such as satellite navigation signal receivers, cameras, millimeter wave radars, ultrasonic radars, and LiDAR; On board or third-party applications on smart cars constantly collect vehicle driving and personal information; A large amount of data is stored on cloud platforms, and the data can be remotely accessed by overseas R&D personnel through cloud platform servers.

2.1.3. Outbound data involves personal information and important data

Accurate self positioning and surrounding environment perception are the foundation of autonomous driving, so vehicles are generally equipped with satellite navigation signal receivers, cameras, radar and other sensors to collect surrounding road environment and geographic information. Intelligent vehicles involve the processing of a large amount of personal information such as biometrics, communication data, and transaction information. Once aggregated, they can form important data; New energy vehicles involve the processing of charging network data such as geographic location information and vehicle power information.

2.2. Main Scenarios of Intelligent Connected Vehicles Data Outbound

There may be three main ways for intelligent connected vehicles to outbound data. The first method is for automobile companies to directly upload data to foreign servers or transmit it to overseas servers through domestic servers. The second method is to outbound used vehicles or waste parts directly with hardware to foreign countries. The third type is obtained through the back door of car software or hardware or in some way. The main functional scenarios involved include the following three:

2.2.1. Autonomous driving

Intelligent cars are equipped with numerous sensors to assist in autonomous driving, such as satellite navigation signal receivers, cameras, millimeter wave radar, ultrasonic radar, LiDAR, etc. Cars collect a large amount of data through these sensors. And many of these data will be uploaded to the data server of the car manufacturer.

ISSN: 2664-9640

2.2.2. In vehicle or third-party applications

On board or third-party applications on smart cars constantly collect vehicle driving and personal information. For example, collecting audio and video data of drivers and passengers, as well as personal information such as phone numbers, birthdays, and software preferences of third-party application users, and storing them domestically, and then providing them overseas for the development of third-party applications.

2.2.3. Cloud platform

Intelligent connected vehicles will interact with cloud platforms, and domestic enterprises will store car data on the cloud platform, which is accessed remotely by overseas R&D personnel through cloud platform servers.

3. Main Security Risks of Intelligent Connected Vehicles Data Outbound

In recent years, intelligent connected vehicle data security has been carried out on the basis of drawing on data security protection technologies in the fields of mobile phones and the internet. However, overall, automotive companies are relatively weak in data security management systems, security protection technologies, and other aspects, and there are many problems in industrial development.

3.1. Unclear Definition of Important Data

According to the regulatory requirements for intelligent connected vehicles data outbound, automotive companies should conduct a data export security risk assessment before conducting important data outbound[4]. However, at present, the industry has not formed an important data catalog, and the discrimination of important data by automotive data processors and automotive companies in practice is still unclear. There are still doubts about what specific geographic information in sensitive areas includes (only coordinates), what specific data of the car charging network refers to (charging capacity or charging pile location), and whether other geographic information data (curvature, elevation, etc.) are included, which makes it difficult to smoothly carry out important data security assessment work and take corresponding preventive measures.

3.2. Long Industrial Chain and Large Data Sharing Circulation Volume

There are numerous upstream and downstream enterprises in the automotive industry chain, and there is a large flow of data between them, making it difficult to control the export of data. There is a large amount of data application interfaces between the upstream and downstream of the automotive industry chain, and there are overlapping areas between various data processing systems, making the data boundaries fuzzy and the scope of responsibility for data processing difficult to clarify. Vehicle production enterprises usually share information such as vehicle operation status, on-board information service status, and fault conditions with third parties to assist in vehicle maintenance diagnosis, optimize intelligent driving algorithms, monitor battery status, etc. Some joint ventures may also share relevant information with foreign third-party enterprises. In order to ensure the safety of the data sharing process, a unified safety concept should be established upstream and downstream of the industrial chain.

3.3. High Complexity of Intelligent Connected Vehicle Environment

The characteristics of high-speed movement, limited space, and complex environment of automobiles pose higher requirements for safety protection technology. One is that network nodes will switch at high speeds during the process of car movement, which requires high technical requirements to ensure the integrity, security, and link stability of data transmission. Secondly, cars are limited by cost and space, and the high cost of chips makes it difficult to continuously stack the computing power and storage space at the end of the car. Technologies

ISSN: 2664-9640

such as facial recognition/license plate anonymization outside the car require higher computing power at the end of the car, posing higher technical difficulties and costs for enterprises.

4. Intelligent Connected Vehicle Data Outbound Test

4.1. Testing Methods

The automobile data outbound detection method proposed in this article mainly involves building a cellular network scenario for data transmission, data sharing, and data outbound detection environment. After using data capture tools to obtain vehicle external transmission data packets, the target IP address is determined to achieve monitoring of data transmission and outbound situations in Wi-Fi and cellular network scenarios [5].

4.1.1. Wi-Fi traffic monitoring scheme

Open the Wi-Fi hotspot function on the testing laptop, and use the traffic monitoring software "wireshark" on the testing laptop to capture the traffic data of the testing vehicle. Simulate the various pre installed data transmission functions of the test vehicle in sequence, and trigger network interaction scenarios for all personal information processing functions. Capture all external communication data packets of the test vehicle through wireshark software, and monitor the traffic of the vehicle's data transmission through Wi-Fi. Analyze communication message data, analyze whether the destination IP address contains an overseas IP address. For communication messages containing an overseas IP address, check whether the communication message contains personal information and verify whether there is overseas transmission data.The specific operation is shown in Figure 1.

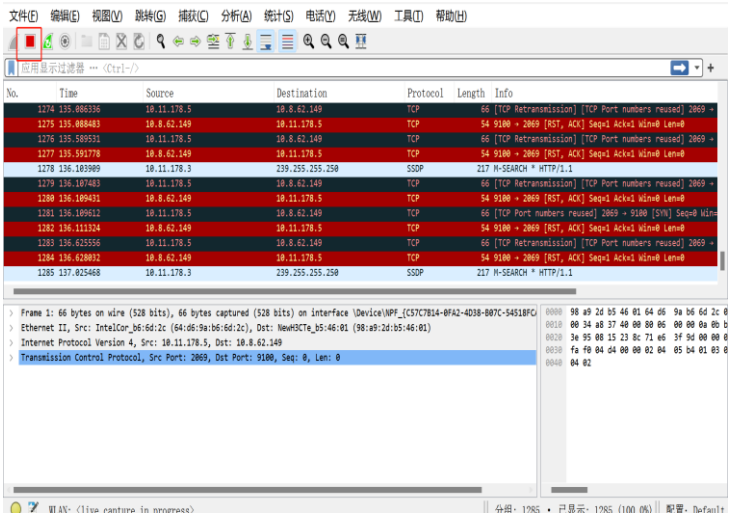

Figure 1: Data monitoring in Wi-Fi scenarios

4.1.2. Traffic monitoring scheme for air port equipment

To build a data private network detection environment, it is first necessary to connect the air port data capture tool to the chip on the ESIM card of the component. Then, the vehicle transmission function is replicated through the vehicle's on-board information interaction system or other controllable components. The air port data monitoring tool is used to capture the external transmission flow, analyze the communication message data, and analyze whether the destination IP address contains an overseas IP address, Verify whether there is overseas transmission data.The main functions of the air port data monitoring tool are shown in Table 1.

ISSN: 2664-9640

Table 1: Main functions of the air port data monitoring tool

Numble	Functions
1	Obtain network data in the Wi-Fi, 4G/5G frequency bands
2	Support decoding of encrypted traffic captured by devices
3	Traffic data between monitoring devices and SIM cards
4	Generate the key required for SIM card encryption and decryption of traffic
5	Forward the generated key to the parsing device for decoding

4.2. Test verification

In order to verify the intelligent connected vehicle data outbound testing method proposed in this article, a test verification was conducted on the export situation of a certain vehicle model data. Simulate and test various pre installed data transmission functions of the vehicle in sequence, and trigger network interaction scenarios for all personal information processing functions. Validate according to the testing method proposed in 4.1, and analyze the experimental results.The test results are shown in Figure 2.

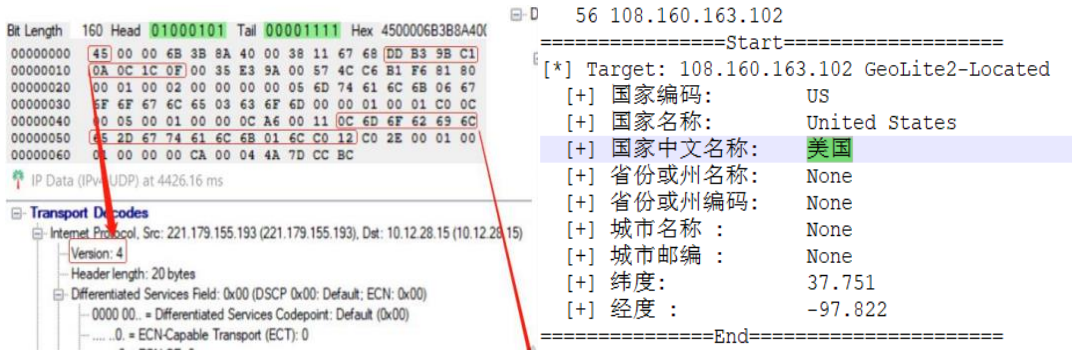

Figure 2: Data outbound test results

The test results show that the recipient of the vehicle data has an overseas IP address and there is an outbound behavior of the vehicle data. Therefore, the testing method proposed in this article can achieve the detection of vehicle outbound data and detect abnormal data outbound behavior generated by vehicles.

5. Conclusion

This article studies and analyzes the main scenarios and security risks of intelligent connected vehicle data outbound behavior. Research has found that the export of automotive data has the characteristics of universality, complex and diverse scenarios, and involving a large amount of important data and personal information. At the same time, there are risks such as difficulty in determining the export of important data, difficulty in controlling the export of industrial chain data, and difficulty in security protection. A vehicle data outbound testing method based on Wi Fi traffic monitoring and air port device traffic monitoring was proposed, and the feasibility of the testing method was verified through vehicle model testing. This article explores the data export compliance path for intelligent connected vehicles, which is of great significance for improving the data security level of the automotive industry.

ISSN: 2664-9640

Acknowledgements

This work was supported by the National Key Research and Development Program of China (No. 2021YFB2501300, 2021YFB2501302).And 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] Mattoo, Aaditya, and J.P.Meltzer: International Data Flows and Privacy: The Conflict and Its Resolution, Journal of International Economic Law (2019)NO. 21.4,p. 769-789.

[2] He Shanshan, Huang Lei, Liu Wenli, et al: How to prevent legal risks in the security of car data outbound, Intelligent Connected Vehicles(2022)NO. 03,p. 48-51.

[3] Pan Yan, Yu Yuzhou, Xu Zhixin: Research on cross-border security of intelligent connected vehicle data based on blockchain technology, China Automotive, (2021)NO. 07,p. 38-43.

[4] Information on:http://www.cac.gov.cn/2021-08/20/c_1631049984897667.htm

[5] Liu Fawang, Xu Xiaoqing, Chen Zhen, et al: Research on Safety Testing and Evaluation Methods for Intelligent Connected Vehicles Equipped with Autonomous Driving Function, Journal of Automotive Engineering (2022), NO. 12,p. 221-227.