Cloud and Service-Oriented Computing (2022)
Clausius Scientific Press, Canada

DOI: 10.23977/csoc.2022.020106
ISSN 2516-399X Vol. 2 Num. 1

Research on Cross-Border Flow of Vehicle Data

Yujia Li[1,*], Yueyou Wang[1], Jue Wang[1], Hanbing Wu[1], Xianzhao Xia[1]

[1]China Automotive Technology and Research Center Co., Ltd., Tianjin, China
**Corresponding author*

Keywords: Cross-border data flow, Intelligent and connected vehicle, Data security, Data security testing

Abstract: As vehicles are increasingly intelligent and connected, the amount and frequency of vehicle data flowing across borders is growing. The issues of cross-border flow of vehicle data has attracted regulatory attention from many countries and gained widespread industry interest. This paper three main situations for the cross-border flow of vehicle data and the critical issues they bring about. Based on the results of tests carried out on the vehicle, captured packet analysis can verify the presence of data outbound from the vehicle.

1. Introduction

With the development of Internet of Things (IoT) technology, communication technology and artificial intelligence technology, the global automotive industry has started the transformation towards intelligent and connected cars. Data has emerged as an important factor driving the development of intelligent and connected vehicles. Intelligent and connected technologies have a significant impact in fostering the development of the global supply chain in the automotive industry, in particular by enabling data to flow quickly and efficiently between countries [1]. The free flow of data across borders plays a vital role of many aspects of the globalization of the automotive industry, and some countries have introduced regulations on the flow of data as well [1]. The cross-border flow of automotive data is characterized by a large volume of data and complex and diverse channels. These characteristics and country-specific legal regulations put pressure on vehicle data processors in terms of cross-border data security protection. In this paper, section 2 outlines the regulatory features of different countries with regard to data crossing borders. In the third section, the various situations of cross-border flow of vehicle data as well as the issues they can cause. Section 4 presents the verification tests for the cross-data flow, which are carried out in the vehicle. Conclusion and outlook are proposed in Section 5.

2. Regulations for cross-border data flow

Many countries, particularly Europe and the United States and China, have their own regulatory features for cross-border data flows, and the laws and regulations addressing data border crossing in other countries have a significant impact on data cross-border compliance in the automotive industry. Countries are more concerned with regulating the outbound movement of data than the inbound movement of data [2].

With regard to the regulation of cross-border data flows, the EU and the US have developed their

legislation and systems earlier and are now more mature. The EU places greater emphasis on the protection of the rights of data subjects and in principle prohibits the transfer of personal information outside the EU, which can only take place if specified conditions are fulfilled. The US, on the other hand, focuses on the benefits of the free flow of data and regulates it only in a few cases, such as when highly sensitive information is involved [3].

Data outbound is a major aspect of China's system of rules for cross-border data flows, and China has always attached great importance to the movement of important data out of the country [2]. According to “the Management of Automobile Data Security (Draft Provisions)”, which is the first regulation on data security in the automotive industry in China, various categories of vehicle data, including geographic information on important and sensitive areas, data on the flow of people and vehicles, etc., belong to important data.

3. Issues of cross-border data flow

The data ecology of vehicles, especially those equipped with intelligent and connected technologies, is more than complicated. The data interactions of vehicles cover multiple participants, including drivers, connected network operators, vehicle manufacturers, etc., and involve a variety of data outbound situations, exposing the cross-border flow of vehicle data to data process compliance and data security issues.

3.1. Cross-border vehicle data situations

Cross-border data transmission in the intelligent and connected vehicles area is on the rise, and three main situations where vehicle data crosses borders are described below.

3.1.1. Vehicle data back across borders

One possible situation of the cross-border data flow is where a vehicle manufacturer collects vehicle data back to its own cloud and then provides it abroad, including personal user information and important sensitive data within the country. While some vehicle companies collect personal privacy and surrounding geographic data within the normal scope of compliance, there are instances where those data are not held within the country in which the vehicle is operating, but rather on servers outside the country. This is commonly found in joint venture vehicle manufacturers, which may transfer data to their group headquarters located outside the country, in order to enable the vehicle model development and technology optimization.

3.1.2. Component data back across borders

Another situation of cross-border data flow is the transmission of data back from vehicle component suppliers. Some component suppliers, such as engine and battery management systems, currently install the function modules which are internet-enabled on their products. Thus these related products are able to collect data without passing through the in-vehicle network terminal like telematic-box (T-BOX) of the connected vehicles, but transmit it directly to the cloud servers of these component suppliers. The data collected includes core sensitive data such as national geographical locations. A global solutions company for engines claims that it can access product status data directly from its engines, and a supplier of battery management systems for intelligent vehicles also indicates that it can obtain real-time vehicle battery status data to enable advanced warning of faults such as thermal runaway of the battery.

3.1.3. Third-party data sharing across borders

The third-party data sharing is a possible way of transferring data across borders. The improvement of vehicle models and the optimization of vehicle functions demand the support of vehicle data. Therefore, vehicle manufacturers often share vehicle data such as the operational status of vehicle components, faults, and usage situations with the cooperating component suppliers. It is not guaranteed that the data processing by these suppliers will take place within the country. Some joint venture automotive enterprises may provide these data with foreign suppliers of parts and components products as well. Furthermore, some vehicle manufacturers will provide data such as vehicle running status data, user driving behaviors and usage of in-vehicle infotainment services to third-party data service companies for the purposes of facilitating vehicle maintenance and diagnosis, optimizing intelligent driving algorithms, or monitoring battery status, etc.

3.2. Cross-border vehicle data issues

First of all, there are presently circumstances in the vehicle industry where vehicle data crosses borders without proper data security and cyber-security assessments. On the one hand, the security assessments of vehicle data across borders can mitigate the security risk of data being transmitted to insecure recipients or recipients without adequate data security protection ability. On the other hand, security assessment of data outbound is also a legal necessity, since many countries have issued laws, regulations and assessment rules around cross-border data security assessment and risk management [4]. Thus, data outbound activities without security assessment may violate local security regulations and thus pose non-compliance issues of vehicle data processors.

In addition, the scope of critical data in vehicle field that allowed to transmit abroad, as well as the implementation guidelines for cross-border data security assessments are not yet sufficient clear. In this situation, the management process of data across borders, both internally and externally, places a burden on automotive companies, especially those that have to take into account cross-border data security regulations in different countries, such as joint ventures, or multinational companies with branches in several countries.

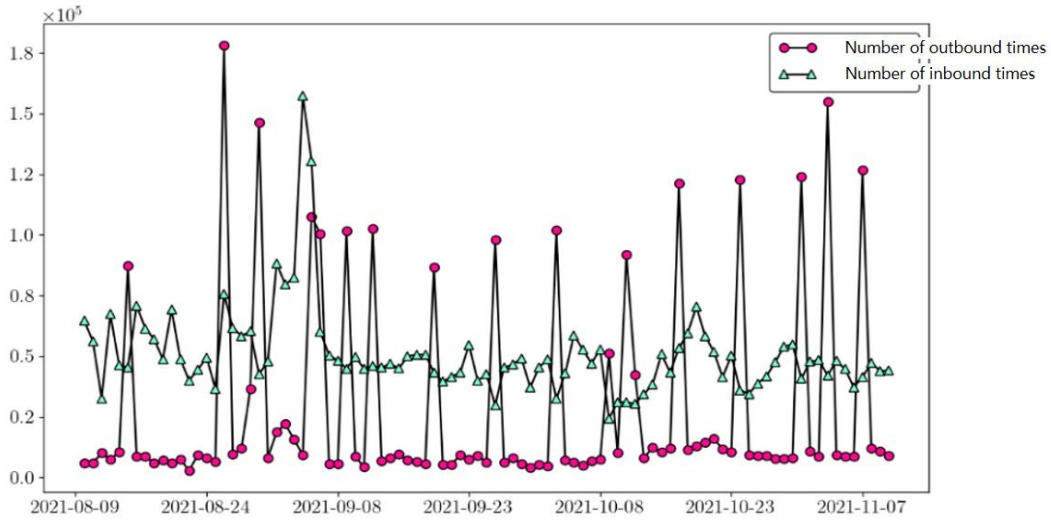

Figure 1: Vehicle data cross-border connectivity counted by day [5]

The high volume and frequency of vehicle cross-border data present challenges for the security management of vehicle transborder data. Cross-border flow data involves personal information such as personal identification or driving license numbers, driving license file numbers, license plate

numbers, mobile phone numbers, addresses, latitude and longitude, and geographic location information. According to CNCERT's [5] study of data cross border for 15 categories of mainstream vehicles sold and operated in China from August 2021 to November 2021, there were 7,327,700 inbound and outbound vehicle data connections. The cross-border traffic flow of vehicle data counted by CNCERT study is illustrated in Figure 1. The maximum number of data transfer abroad in a single day reaching 178,159 (26 August) [5].

4. Test verification

The verification testing for the cross-border data flow of vehicles can be carried out on vehicle models to to confirm if the vehicle under test has an outbound data transmission.

4.1. Methods

The main test method used is to capture and analyse the packets transmitted outwards from the vehicle.

During the verification test, firstly, the WIFI hotspot on the test computer or test phone is turned on. Following this, the vehicle under test is connected to the WIFI hotspot shared by the test computer or test phone via the WIFI settings option of the in-vehicle infotainment (IVI). The communication traffic of the vehicle data is captured from hotspot NICs via flow monitoring software. The captured packets are subsequently analyzed to detect whether the vehicle is sending data to an outbound IP address.

There is an alternative method of accessing data transmitted to the outside of the vehicle, including via cellular mobile networks and wifi, which requires access to the T-BOX system and the highest debugging access to the corresponding interface. During the test, a connection is established between the test PC used and the T-BOX of the vehicle under test, either wirelessly or by wired (using a network cable through the OBD port), in order to access the T-BOX system. Then the flow monitoring software is installed in the system through command instructions or using the flow monitoring software that is already included in the T-BOX system of the vehicle under test. The data transmission functions of the T-BOX are reproduced through IVI or other controllable components. All functions of transmitting data to the outside of vehicles are activated and the flow monitoring software is used to obtain the transmitted data flow packets. The content of the data packets is examined and analyzed to verify whether the IP address of the data recipient is outside the country and whether there is a cross-border flow of data in the vehicle under test.

4.2. Results Analyse

The data packet capture tool used in this paper is Wireshark, which enables the data flow monitoring as well. Wireshark is a widely-used network protocol analyse tool. It captures live network data passing through the NIC on its devices by means of the packet capture library [6]. It does not modify the content of the captured data packet, but only reflects the packet information currently in transit.

As the Wireshark interface shown in Figure 2, the packet capture tool acquires the data sender’s Ip address, receiver’s IP address, communication protocol, length and information of the transmitted outgoing vehicle data. (For data protection reasons, the IP addresses of the data destination and the information are not fully presented here.)

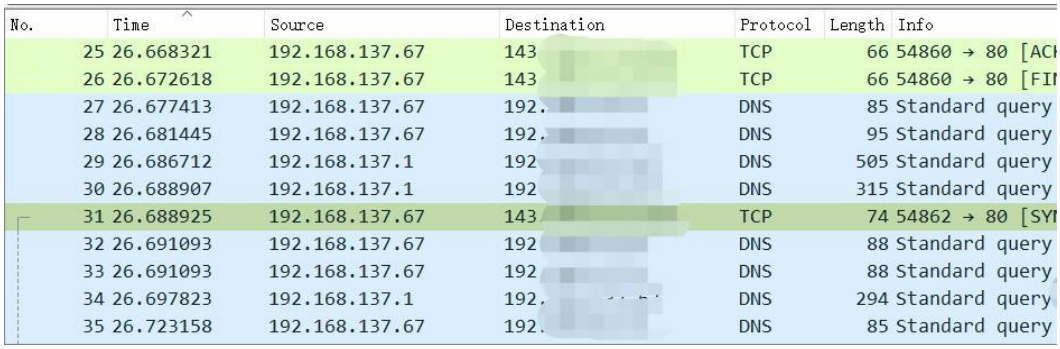

Figure 2: Data packet captured by Wireshark

By running a script that is able to simply run on windows system, the IP address obtained by the packet capture can be automatically retrieved with the specific transmission location of the IP address. Table 1 shows the part of the data outbound test results for one vehicle model, which is being tested for its data flow in China.

Table 1: Data outbound test results of the vehicle under test

IP address of data receiving server	Number of messages	Data flow	Country name	State name
18.xx.xxx.xx	170	22k	America	None
23.xx.xxx.xxx	10	740	Hong Kong	Kowloon City
104.xxx.xxx.xx	10	740	Japan	Tokyo
18.xx.xxx.xx	68	8k	America	None
52.xx.xxx.xx	67	7k	America	None

5. Conclusions

This paper compares the regulatory focuses of the EU, the US and China in relation to cross-border data flows. And the three major situations of cross-border vehicle data are studied, respectively, the vehicle data is transmitted out of the country by the vehicle manufacturer through its own cloud platform, the second way is through components with networking functions, and the third is the vehicle data flows across the border through sharing to third-party data service companies. However, cross-border vehicle data faces a lack of security assessment, unclear assessment guidelines, and difficulties in protecting large quantities of data in diverse scenarios. By capturing and analyzing the data packets in the verification test of the vehicle model, it is found that data is sent from the vehicle and transmitted to an out-of-state server.

Acknowledgements

I have received a lot of support and help from the company and my colleagues regarding the research content of this paper. I would like to thank the company for its support in terms of industry research and testing platforms, my leaders and my colleagues for their assistance in conducting the verification tests.

References

[1] Mitchell, A.D., Mishra, N. Regulating cross-border data flows in a data-driven world: how WTO law can contribute. Journal of International Economic Law, 2019, 22(3): 389-416.
[2] Sun, W. Research on Data Outbound Rules in China, 2020.
[3] Hang, Y. Research on the Supervision Path of Cross-Border Transfer of Personal Information in China ——From the Perspective of Relevant Mechanisms in EU and the US, 2020.

[4] Li, J., Dong, W., Zhang, C., et al. Development of a risk index for cross-border data movement. Data Science and Management, 2022.
[5] Critical Infrastructure Security Emergency Response Center, Vehicle Data Outbound Situation Analysis Report (Issue 2), 2021, [online] Available: https://www.secrss.com/articles/34164.
[6] Wireshark, Packet capture library (libpcap), 2020, [online] Available: https://wiki.wireshark.org/libpcap.md.