Research on Automatic Intrusion Detection System of Vehicle Terminal

Yanyan Han[1,a,*], Changyuan Wang[1], Kexun He[1] and Xiyu Fang[1]

[1]CATARC Automotive Test Center (Tianjin) Co., Ltd, Tianjin, China
a. hanyanyan@catarc.ac.cn
**corresponding author: Yanyan Han*

Keywords: Vehicle terminal, information security threats, intrusion detection.

Abstract: With the rapid development of intelligent, networked and electric vehicles, more and more vehicle terminals including Tbox and vehicle entertainment system are used. At the same time, as the connection interface between the vehicle and the outside world and the upgrading carrier of the vehicle hardware and software, the vehicle terminal also brings huge information security risks to the vehicle. However, there is still a lack of research on the information security protection technology of vehicle terminals. A large number of vehicle terminals operate on the market with low security. This paper starts with the information security detection method of vehicle terminal, and studies an automatic intrusion detection system by simulating remote data intrusion, which can effectively verify the security protection performance of vehicle terminal.

1. Introduction

With the rapid development of intelligent, networked and electric vehicles, more and more vehicle terminals including Tbox and vehicle entertainment system are used. Vehicle terminal not only undertakes more and more functions of body control, electronic and electrical system control, but also provides rich information and entertainment services for vehicle users. At the same time, as the connection interface between the vehicle and the outside world and the vehicle hardware and software upgrading carrier, the vehicle terminal will connect the originally closed vehicle individual to the Internet. However, no matter electric vehicle, heavy-duty diesel vehicle or emerging intelligent Internet vehicle, the vehicle terminals on which they are equipped are lack of protection of safety protection products, which leads to a significant increase in the risk of vehicle information security[1].

In recent years, jeep, Tesla and other events that lead to the vehicle being controlled due to the hacker attack on the vehicle terminal are increasing, which has attracted extensive attention of the industry and the public[2,3]. At first, hackers used computers to access the vehicle diagnosis interface to operate the vehicle, but now they have been able to operate the vehicle through the vehicle wireless network or Bluetooth and other short-distance communication means. Through the information collection and instruction distribution of automobile bus and electronic and electrical system, the black car can be accelerated, decelerated, braked, flameout, or even brake failure, which may lead to great loss or even life safety threat.

Illegal operation of vehicles through cloud computers has been seen in more and more newspapers. If it happens in a specific scene, the consequences are unimaginable. At the national level, countries have begun to attach strategic importance to automobile information security. UN / WP29 autopilot working group focuses on information security and software upgrading, and the information security requirements of vehicle terminal are its important contents. However, at present, there is still a lack of research on the information protection technology and products of vehicle terminals. A large number of vehicle terminals operate on the market with low security. At the same time, there are no clear standards and regulations for the information security test and evaluation methods of the vehicle terminal. At present, there is no unified test method to test whether the information security performance of the vehicle terminal is up to the standard.

In this context, this paper aims to study an information security detection method of vehicle terminal. In view of the characteristics that attackers usually attack vehicles from far or near by using network means and vehicle terminal as the entrance, an automatic intrusion detection system is developed. By simulating remote data intrusion, it can detect whether the vehicle terminal can resist network attack, which can effectively verify the safety protection performance of the vehicle terminal.

2. Design and Implementation of Automatic Intrusion Detection System

2.1. Overview of Needs

First of all, the host deploying the automatic intrusion detection system should be in the same network environment with the vehicle terminal under test, and send specific security event packets to the vehicle terminal under test through the network. The tested vehicle terminal equipment shall be able to identify or record these safety events without damage to function or performance. Therefore, the two main difficulties of the automatic intrusion detection system are the design of the security event data set and the realization of the communication and detection of the vehicle terminal in the same communication network.

2.2. Overall Architecture Design

The system architecture is designed based on C/S mode. Client is an automatic intrusion detection system running on the detection host. During the detection, the detection personnel need to input information, conduct safety detection, conduct data analysis and other operations on the vehicle terminal equipment. Server is the system version control tool, running on the remote server, which is used for version management, remote software upgrade and remote security event library upgrade of automatic intrusion detection system.

The system execution process is shown in the figure below:

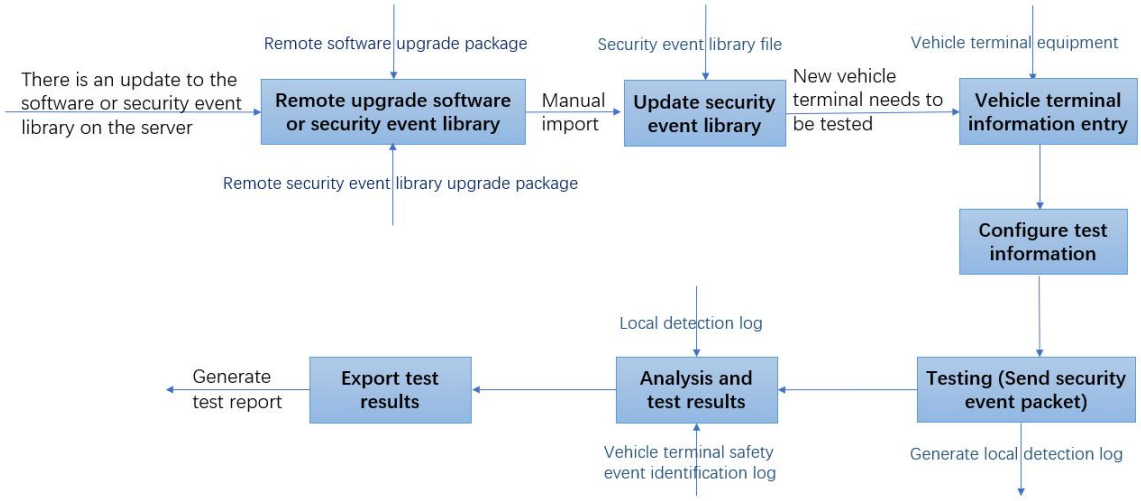

Figure 1: The system execution process.

The specific implementation steps of the system are as follows:

1) Check whether the remote server has a new version of software or the security event library needs to be upgraded. If it needs to be upgraded, download the corresponding data package to the local area first, decompress and replace the corresponding file or content;

2) Judge whether it is necessary to manually update the security event library. For example, in the case of no communication with the server, the tester needs to manually import the latest security event library file;

3) When a new vehicle terminal equipment needs to be tested, first confirm whether the information of the terminal to be tested is complete and meets the testing requirements, and then start to input the information after the information is confirmed to be correct;

4) After the completion of information entry, configure the relevant parameters (such as IP address, port and other parameters) of vehicle terminal equipment detection;

5) At the beginning of the detection, the corresponding data package in the security event database is sent to the vehicle terminal, the detection tool software records the process of sending the security event, and generates the local detection log file; the detected vehicle terminal records the identified security event;

6) Analyze the detection results according to the local detection log file recorded by the detection tool software and the safety event identification log recorded by the vehicle terminal.

7) When exporting test results, you need to input test basis, description, number and other information, and generate test reports according to the fixed report template format.

2.3. Security Event Library

In order to ensure the comprehensive and effective intrusion detection of the vehicle terminal and the in-depth excavation of the vehicle terminal vulnerabilities, a reliable and repeatable attack security event database should be established. Based on the general information system security detection method, the system is constructed according to the characteristics of the vehicle terminal system to ensure the coverage of comprehensive and up-to-date vulnerabilities and test methods. Security events are not immutable, but are constantly discovered and published. When new security events or old security events are not applicable, the security event database needs to be updated. The security event database will be updated regularly with the vulnerabilities included in the international CVE and cnvd vulnerability databases.

According to GB/T 37027-2018 [6], GB/T 20275-2013 [7] and other Chinese national standards, combined with the particularity of communication modules and other components in the vehicle terminal, the event types in the security event database mainly include the following categories: denial of service, port scanning, strong attack and weak password, and overflow.

In the application process, the data security is considered, especially the executed security event command. In order to prevent the command from being changed by malicious strings, the data in this field is encrypted. The encryption algorithm is AES symmetric encryption algorithm.

The encryption and decryption process of the security event command is shown in the figure below.

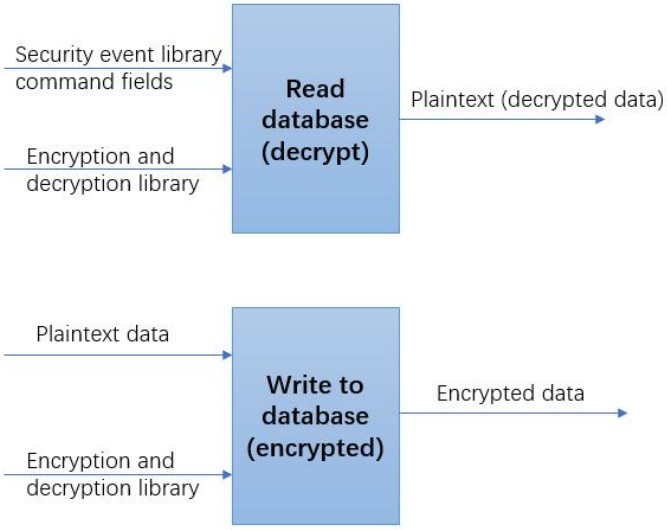

Figure 2: The encryption and decryption process of the security event command.

2.4. Vehicle Terminal Detection Process

The inspection process of vehicle terminal is shown in the figure below

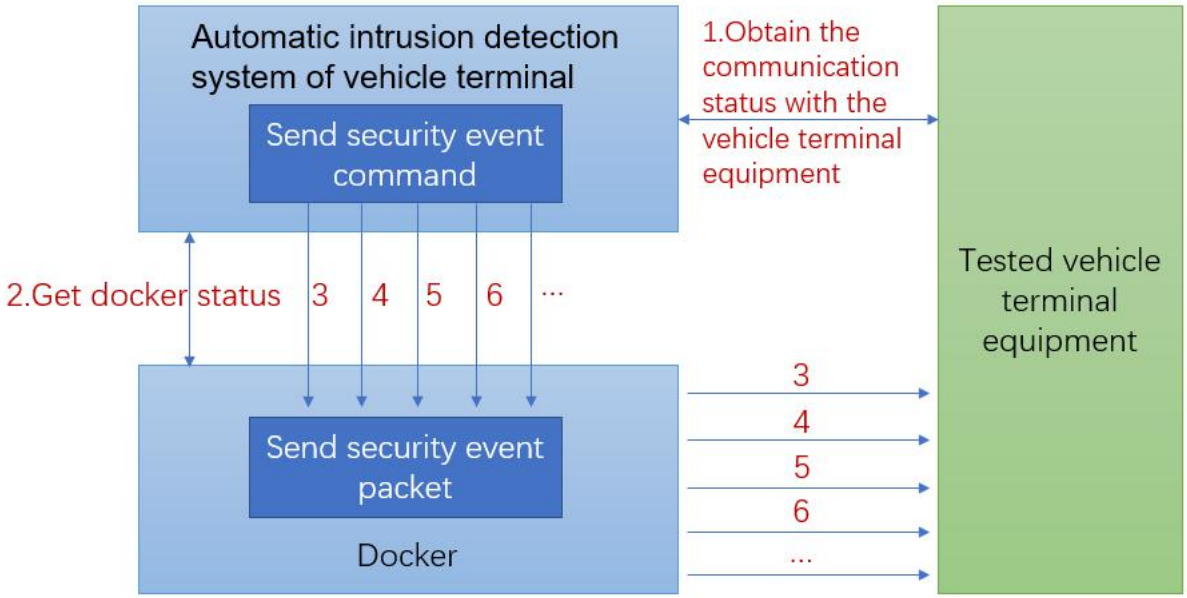

Figure 3: Vehicle terminal detection process.

The detailed detection flow of vehicle terminal is as follows:

1) Obtain the network communication status with the vehicle terminal;

2) Get the running status of the system in the docker container;

3) The software executes the security event command and calls the system in the docker container to send the security event data package. Because the security event command already contains the terminal device IP and other related information, the security event data package will be sent to the designated terminal device to be detected;

4) When the execution of the current security event is completed, the software executes the end command and calls the system in the docker container to close and send the security event packet;

5) Other security events in turn.

3. Summary

The wide application of vehicle terminal brings huge information security threat to the vehicle, and there is no unified detection method to detect whether the information security performance of vehicle terminal is up to standard. In this paper, an information security detection method of vehicle terminal is studied. On the basis of establishing a comprehensive, reliable and renewable security event database, the communication and detection of vehicle terminal are realized in the same communication network. Through this way of simulating the attacker's remote data intrusion, an automatic intrusion detection system for the vehicle terminal is finally realized, which can effectively verify the safety protection performance of the vehicle terminal and ensure the vehicle safety.

References

[1] Yingluo Luo, Qiang Fang. Vehicle on-board terminal information security threats and countermeasures, Telecommunication network technology, 2016, 000(006):35-39.

[2] Information on https://www.freebuf.com/news/72981.html.

[3] Information on https://keenlab.tencent.com/zh/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars/.

[4] Information on http://cve.mitre.org/.

[5] Information on https://www.cnvd.org.cn/.

[6] GB/T 37027-2018 Information security technology-Specifications of definition and description for network attack, China Standards Press.

[7] GB/T 20275-2013 Information security technology-Technical requirements and testing and evaluation approaches for network-based intrusion detection system, China Standards Press.