Research on Attack Detection System Technology Based on Vehicle Network TSP Platform

Yingying Ji[1, a, *], Huaijin Zhao[2, b], Xing Chen[1, c] and Chenglei Yu[3, d]

[1]The National Computer Network Emergency Response Technical Team/Coordination Center of China Zhejiang Branch, Hang zhou, China

[2]The National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing, China

[3]Hangzhou dianzi university, Hang zhou, China

[a]jiyingying326@163.com, [b]1208631447@qq.com, [c]1242789847@qq.com, [d]10122252@qq.com, email

Keywords: vehicle networking TSP, attack detection, system scheme

Abstract: With the development of vehicle networking communication technology, the security risks of vehicle networking have become increasingly prominent. Information tampering and virus intrusion have been used by hackers in cyber attacks on smart cars. The risk of attacks on the Internet of Vehicles worldwide has intensified, and there have been many cyber attacks against the Internet of Vehicles. In some cases, attackers can control the vehicle's power system, causing the driver's life safety to be threatened. Analysis of the car network attack incidents in recent years, the current major car network attack threat events focused on TSP server attacks. This paper studies the security monitoring of the data from the vehicle end to the TSP platform, collects and analyzes the status and intelligence of the networked car, and proposes a plan to establish a TSP server attack monitoring system for the car network.

1. Introduction

As an important infrastructure, the Internet of Vehicles has become the focus of widespread attention at home and abroad. With the development of the Internet of Vehicles communication technology, the security risks of the Internet of Vehicles have become increasingly prominent. Information tampering and virus intrusion have been used by hackers in cyber attacks on smart cars. In recent years, the risk of attack on the Internet of Vehicles worldwide has intensified. There have been many cyber attacks against the Internet of Vehicles. In some cases, attackers can control the vehicle's power system, causing the driver's life safety to be threatened. In 2015, Chrysler's Jeep model was invaded to reduce the speed of the car, shut down the car engine, suddenly brake or disable the brakes without the user's knowledge. In 2016, the Norwegian security company Promon obtained the Tesla App account username and password in the case of intruding the user's mobile phone. By logging in to the Tesla car networking service platform, the vehicle can be located, tracked, unlocked and started at any time. Resulting in the theft of the vehicle. In 2017, the safety weathervane of the Internet of Vehicles was urgently transferred to the data security and privacy of customers. A database of dealers in the United States was attacked, involving sales data leaks from more than 10 million vehicles in multiple brands. In the same year, Nissan Motor officially announced that its financial company database data information was stolen by hackers, and customers' personal information and loan information were all stolen.

Analysis of the car network attack in recent years, the current major car network attack threats are concentrated in the TSP server attack, so the establishment of the car network TSP server attack monitoring system has a general significance for the domestic car network security risk situation. This paper studies and designs the vehicle network TSP server attack monitoring system program, collects and analyzes the status and intelligence of the networked car, and realizes the safety

DOI: 10.25236/scmc.2019.090

monitoring of the vehicle-to-TSP cloud data, and finds the vulnerabilities contained in the vehicle, and improves the vehicle networking TSP platform. Safety is of great significance.

2. Related research

The attack detection subsystem mainly performs network attack detection for Web services and TSP platforms in the Internet of Vehicles network. It mainly includes server attack detection module, web platform attack detection module, attack result analysis and traceability module.

The deployment mode of the server attack detection module and the web platform attack detection module are both bypassed. That is, the communication data of the target TSP server or the web platform is mirrored or split, and the module is connected to the detection module. Incoming data for analysis and testing will not have any impact on the original server business

2.1 Server Attack Detection Module

The server attack detection module mainly performs attack detection on the TSP platform server in the car network network, and through real-time monitoring and analysis of the network data of the communication, the attack against the TSP server can be found in time, and the suspicious behavior is recorded. And alarms, form an attack behavior log, providing first-hand information for further disposal.

The attack detection mechanism of the server attack detection module mainly includes two parts:

(1) Attack feature pattern matching

Pattern matching analysis compares various network traffic characteristics information collected with known network intrusion and system misuse pattern databases to discover behaviors that violate security policies and mark and record them. Through the built-in rich attack behavior feature database, attack detection using pattern matching method can efficiently detect suspicious network attack behavior. At the same time, by regularly upgrading the database of attack behavior characteristics, the ability to discover new types of attacks can be continuously enhanced.

(2) Statistical analysis of network traffic

Attack detection using network traffic statistics analysis first creates a statistical description of the traffic information object, and collects measurement attributes (such as IP range, traffic size, time characteristics, number of accesses, number of operation failures, and Delay, etc.), to construct the statistical characteristics of the normal operating flow of the system. This feature will be used to compare the behavior of the network and system. Any observations outside the normal deviation are considered to have an intrusion. This method can be used to early warning and discover unknown attack behavior.

(3) malicious code monitoring

Through the analysis of network traffic acquisition, the malicious code automation analysis module is built. Attack behavior was discovered through four processes: sample acquisition, sample detection, comprehensive analysis, and visual display.

In the sample acquisition phase, the module actively crawls the sample file of the car network TSP platform in the public network, receives the server monitoring port traffic analysis and restores the sample file and the propagation log, obtains the required monitoring data, and flows to the sample detection engine. Basic detection, static analysis, dynamic analysis process, obtain file program name, file MD5, operating system, compiler version and other information, and connect third-party analysis engine to detect sample process operation, file operation, system permission operation, network connection, etc; Through the analysis process of sample comprehensive identification analysis, sample threat association mining, homology analysis, etc., comprehensive identification of sample threats and discovery of related attack organizations.

Through the above detection and analysis process, the code epidemic situation, propagation dimension and popular virus situation of the malicious network of the TSP platform server of the country can be visualized, and a real-time attack monitoring module is formed for the important TSP platform. Response, emergency response.

2.2 Web Platform Attack Detection Module

In some car networking networks, there are Web platforms that provide Web services for administrators or users, which facilitates users to conduct Web-based management and operations. However, as a type of service that is extremely vulnerable to attacks on the Internet, the Web platform has great security risks. To ensure the security of the Web service in the TSP platform, the Web platform attack detection module provides a detection form different from the server attack detection, that is, a dedicated Web attack detection.

The web platform attack detection module works at the application layer and can detect attacks specific to the web platform. These attacks are normal web application traffic from the network layer, but the security vulnerabilities of the web services are carefully constructed and can be used on the web. The platform creates a huge hazard.

The web platform attack detection module provides attack detection and protection through the following functions:

(1) Protocol anomaly detection

The web platform attack detection module performs anomaly detection on HTTP requests and rejects requests that do not conform to the HTTP standard. Moreover, it can also allow only some of the options of the HTTP protocol to pass, thereby reducing the scope of the attack.

The RFC has a clear definition of the HTTP packet format. Under normal circumstances, the HTTP packets received by the application should meet the requirements of this specification. In addition, in the specific application, the data type and parameter length of the fields in the HTTP header are clearly defined. This category also creates security problems.

(2) Enhanced input verification

Most of the input-based security issues such as XSS, SQL injection, etc. can be discovered in advance by enhancing the validation from user input. Specific verification rules include:

Use the whitelist input validation at the application input layer to verify that all user input matches the content that the app is to receive. The app only accepts input that matches the desired format

Perform whitelist filtering policies on the client browser (saving round-trip traffic)

Use blacklist and whitelist input validation (in the form of vulnerability "signature" and "experience" behavior) to provide intrusion detection/blocking and surveillance application attacks

Use parameterized statements from start to finish in the application to ensure safe SQL execution

Use escaping techniques in database queries (note the inter-system coding problem, defense based on character encoding bit width bypass: wide byte injection)

Encode the data before sending it to the UI.

(3) Rule-based protection and exception-based protection

Rule-based protection can provide security rules for various web applications. By constantly upgrading the rule base, timely protection against new types of attacks can be achieved.

(4) Condition monitoring

This module can determine if the user is accessing for the first time and redirects the request to the default login page and logs the event. By detecting the user's overall operational behavior, we can more easily identify the attack. The state management mode can also detect anomalous events (such as login failures) and process them when they reach the limit. Effective discovery of violent attacks can be achieved.

2.3 Attack Result Analysis and Traceability Module

The attack behavior recorded by the server attack check module and the web platform attack detection module may be only a tentative attack. To ensure the reliability verification of the attack result, comprehensive analysis of the attack behavior result, environment, and scenario is needed to determine the Whether it is an effective attack. The attack result analysis and traceability module mainly performs comprehensive review and traceability of the attack behavior marked by the server attack detection module and the web platform attack check module.

(1) analysis of attack results

The attack behavior recorded by the server attack check module and the web platform attack detection module is only a log record of a single attack. Whether the attack itself is successful and whether there are vulnerabilities that can be exploited by the attack cannot be determined. Further analysis of the attack results. Through the verification of the specific attack behavior and the query of the access record before and after the attack behavior, the nature of the attack behavior can be determined. For the attack behavior characterized as successful and dangerous, it needs to be further traced and timely implemented on the system. repair.

(2) Attack traceback

For the attack behavior that has been determined to be successful, a further comprehensive analysis of its related IP and related behaviors can achieve its behavioral traceability and source tracing.

Cross-analysis of the access record of the target resource accessed by an attack behavior and the attack record can be used to comb the entire step of the attack and track the complete behavior path of the attacker. Combined with the attack source IP recorded by the system for comprehensive analysis of behavior and IP, the source of the attacker can be traced, and the resulting data can be used for subsequent protection and related departments to enforce the law.

3. Scenario deployment and test simulation

3.1 System software and hardware physical deployment plan

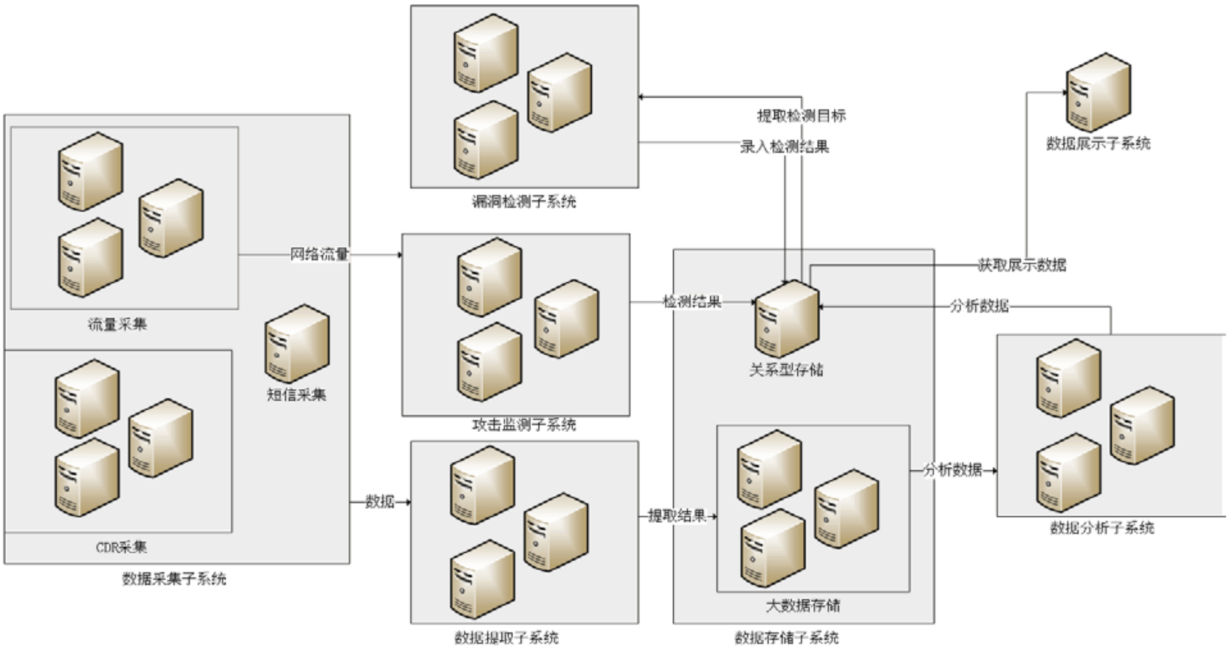
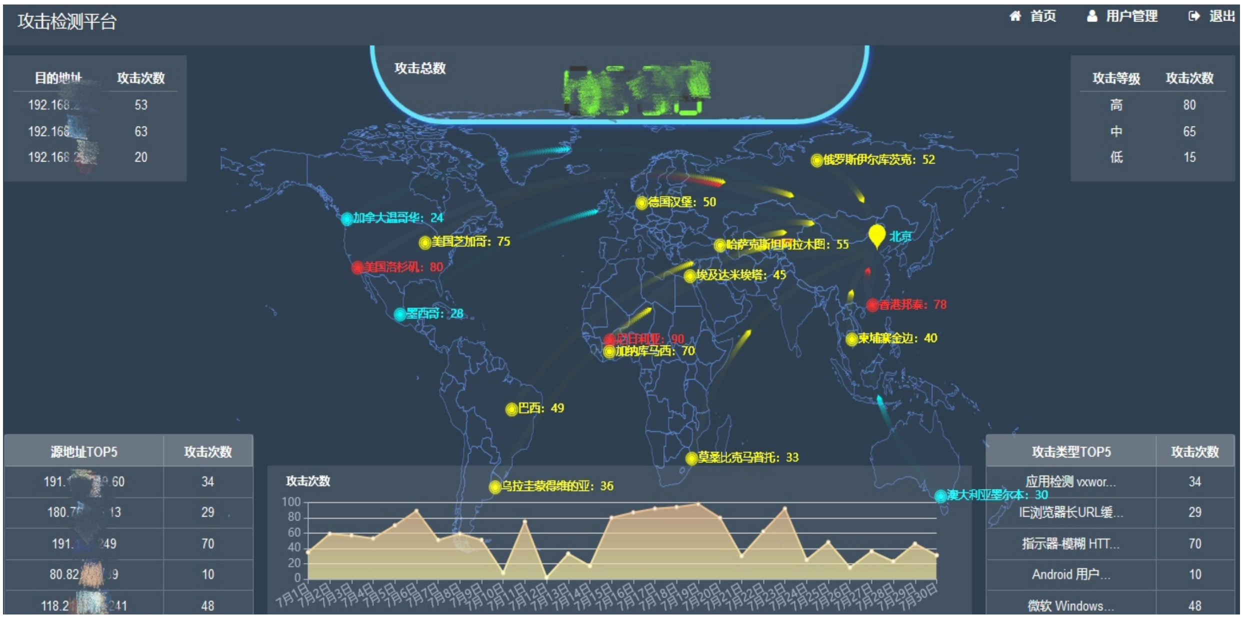


Figure 1. System deployment scenario

3.2 system simulation platform display (analog data)



攻击检测平台

首页 用户管理 退出

攻击总数 [redacted]

目的地址	攻击次数
192.168.[redacted]	53
192.168[redacted]	63
192.168.[redacted]	20

攻击等级	攻击次数
高	80
中	65
低	15

源地址TOP5	攻击次数
191.[redacted]9.60	34
180.7[redacted]13	29
191.[redacted]249	70
80.82[redacted]9	10
118.2[redacted]241	48

攻击类型TOP5	攻击次数
应用检测 vxwor...	34
IE浏览器长URL缓...	29
指示器-模糊 HTT...	70
Android 用户...	10
微软 Windows...	48

Figure 2. Vehicle Network TSP Server Attack Monitoring System Simulation Platform Display (analog data)

According to the system data analysis, the simulated test results can be obtained. The IP address distribution of the foreign attack source is TOP10:

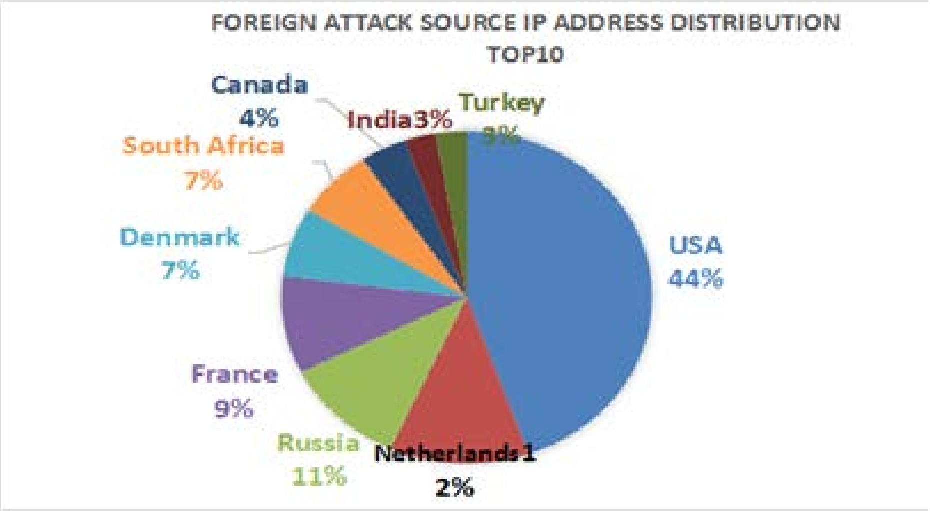
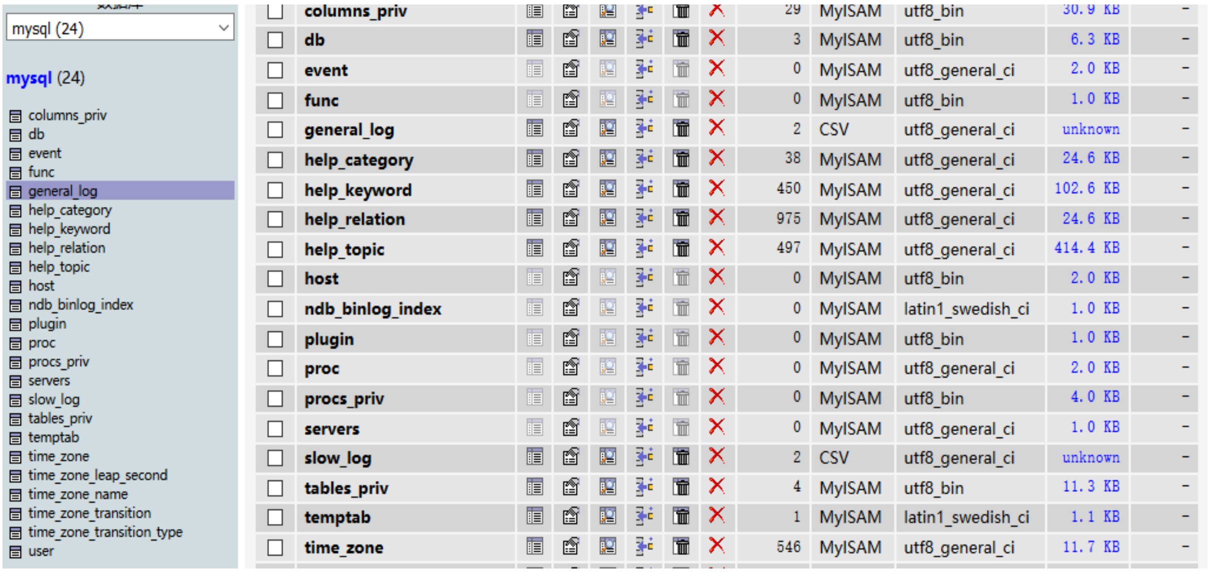


Figure 3. Foreign Attack Source IP Address Distribution

3.3 Vehicle Network Simulation Platform Vulnerability Display



mysql (24)

mysql (24)

- columns_priv
- db
- event
- func
- general_log
- help_category
- help_keyword
- help_relation
- help_topic
- host
- ndb_binlog_index
- plugin
- proc
- procs_priv
- servers
- slow_log
- tables_priv
- temptab
- time_zone
- time_zone_leap_second
- time_zone_name
- time_zone_transition
- time_zone_transition_type
- user

□	**columns_priv**	29	MyISAM	utf8_bin	30.9 KB	-
□	**db**	3	MyISAM	utf8_bin	6.3 KB	-
□	**event**	0	MyISAM	utf8_general_ci	2.0 KB	-
□	**func**	0	MyISAM	utf8_bin	1.0 KB	-
□	**general_log**	2	CSV	utf8_general_ci	unknown	-
□	**help_category**	38	MyISAM	utf8_general_ci	24.6 KB	-
□	**help_keyword**	450	MyISAM	utf8_general_ci	102.6 KB	-
□	**help_relation**	975	MyISAM	utf8_general_ci	24.6 KB	-
□	**help_topic**	497	MyISAM	utf8_general_ci	414.4 KB	-
□	**host**	0	MyISAM	utf8_bin	2.0 KB	-
□	**ndb_binlog_index**	0	MyISAM	latin1_swedish_ci	1.0 KB	-
□	**plugin**	0	MyISAM	utf8_bin	1.0 KB	-
□	**proc**	0	MyISAM	utf8_general_ci	2.0 KB	-
□	**procs_priv**	0	MyISAM	utf8_bin	4.0 KB	-
□	**servers**	0	MyISAM	utf8_general_ci	1.0 KB	-
□	**slow_log**	2	CSV	utf8_general_ci	unknown	-
□	**tables_priv**	4	MyISAM	utf8_bin	11.3 KB	-
□	**temptab**	1	MyISAM	latin1_swedish_ci	1.1 KB	-
□	**time_zone**	546	MyISAM	utf8_general_ci	11.7 KB	-

Figure 4. Vehicle Network TSP Server Attack Monitoring System Simulation Platform Display (Analog Data)

According to the system data analysis, the proportion of the types of vulnerabilities in the simulated test results can be obtained:

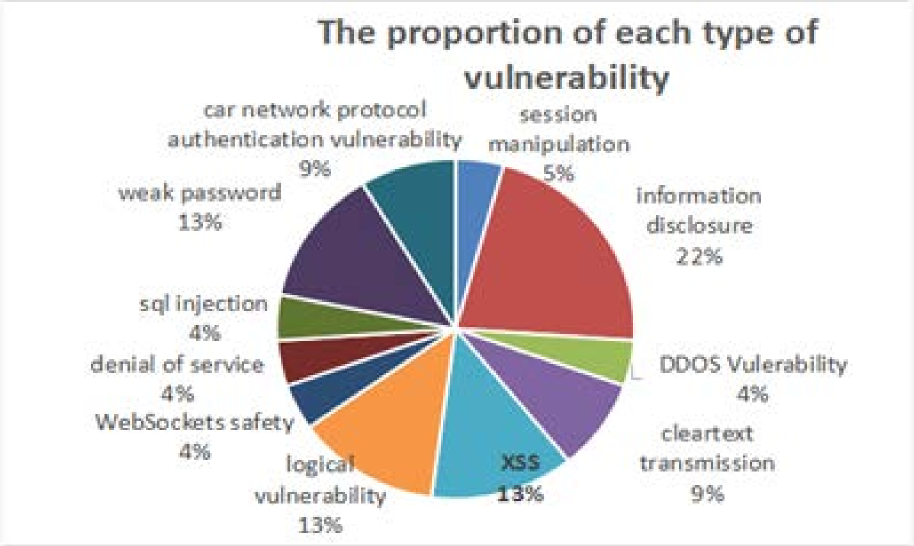


Figure 5. The Proportion of Each Type of Vulnerability

4. Conclusion

This paper studies the security of the vehicle-to-TSP platform data, collects and analyzes the status and intelligence of the networked car, and deploys the design of the TSP server attack monitoring system in detail, and develops the simulation system to derive the test results. The establishment of the TSP server attack monitoring system of the Internet of Vehicles makes up for the gaps that cannot be monitored by the TSP server in the fixed network. It can provide effective data supplement for the big data analysis of the Internet of Vehicles, and has a significant significance for the security risk situation of the domestic vehicle network.

References

[1] Yang Nan, Kang Rongbao. Analysis and Protection of Vehicle Network Security Threats [J]. Communication Technology, 2015, 48 (12): 1421 - 1426.

[2] Ling Zhiwei. Discussion on Information Security Issues in Internet of Vehicles [J]. Electromechanical Technology, 2017 (1): 110 - 112.

[3] Lü Liudi, Zheng Dong, Zhang Yinghui, Yan Ming, Su Yunan. Identity-based Aggregated Signature Authentication in Internet of Vehicles [J]. Computer Engineering and Design, 2018.

[4] Zhang Yuyu. Research on security authentication and privacy protection mechanism based on vehicle cloud [D]. Beijing Jiaotong University, 2018.

[5] WANG Liangmin, LI Tingting, CHEN Long. The Structure and Security of Vehicle Network Based on Vehicle Identity [J]. Journal of Network and Information Security, 2016, 2 (2): 41 - 54.

[6] Huang Yuzhen. Research on network security technology of vehicle network [J]. Electronic World, 2018.

[7] Song Zefeng. Research and implementation of in-vehicle network penetration testing for CAN bus [D]. Chengdu: University of Electronic Science and Technology, 2018.

[8] Wang Shaoqiang, Shao Dan, Wang Yanbai. Analysis and research of network penetration testing technology [J]. Electronic World, 2015, (17): 154 - 155.

[9] Zhao Xi. Research and implementation of penetration testing integrated platform based on Android system [D]. Shanghai: Donghua University, 2016.

[10] Qu Zhuo, Zhou Hanxun, Pei Tianhua. Research on Information Security Penetration Testing Process [J]. Northern Transportation, 2015, (12): 112 - 114.

[11] Liu Yang. Case Analysis and Prevention Strategy of Vulnerability Hazard Based on Penetration Test [J]. Cyberspace Security, 2018, (9): 76 - 78. All manuscripts must be in English, also the table and figure texts, otherwise we cannot publish.