Research of the Information Security Management Technology of Third Party Logistics Service Platform of Railway Oil Supply Chain

Tingyu Luan[1, a], Li Lei[2, b], Liying Ding[2, c] and Xiaodong Yin[2, c]

[1] MOE Key Laboratory for Urban Transportation Complex Systems Theory and Technology, Beijing Jiaotong University, Beijing 100044, China;

[2] CRM E-Commerce Tech.Co.,Ltd, Beijing 100088, China.

[a]g479920323@qq.com, [b]llei@bjtu.edu.cn, [c]lany@crmec.com.cn

Keywords: Information Safe; Service Platform; Railway Oil Supply Chain; Third Party Logistics.

Abstract. Information exchange security is the basis of railway oil supply chain management, which is of great significance to ensure the reliability of railway transportation and reduce the cost of railway operation. This paper analyzed the safety technical requirements of railway oil supply chain information exchange, and put forward the construction goal, construction principle, construction content and key technology of information exchange security of the information security system of the third party logistics service platform of the railway industry oil supply chain.

1. Introduction

The third party logistics service platform of China railway industry oil supply chain has the functions of fuel oil collection, inventory, and distribution and so on, and achieves data transmission and aggregation between itself and terminal distribution equipment and monitoring equipment. At the same time, it has multiple functions such as comprehensive statistical query. At present, the system provides a complete railway fuel supply chain business implementation and management services for 114 agencies, and 851 users of the two major sectors: the material and the railway[1].

After the platform is put into use, with the expansion of the scale of application, the number of users, service functions, the rapid increase in the application of data, the frequency of business operations, the number will be rapid growth. We must build a sound information security infrastructure, to block security vulnerabilities, to ensure the stability of the system operation, data security, security and reliability of the transaction message. According to the above requirements, this paper puts forward the construction goal, construction principle, construction content and key technology of information exchange security of the information security system of the third party logistics service platform of the railway industry oil supply chain.

2. Information security technology requirements analysis of the platform

Information security needs of the platform mainly from the following two aspects. The first is business security. The internal business is mainly based on the network transmission; the openness of the network determines the vulnerability of its transmission security, so it is necessary to ensure the confidentiality and integrity of data transmission and to confirm the true identity of each operator on the Internet in business operations, and to ensure the authenticity and non-repudiation of the operation. The second is the network security. Open servers on the web, and internal servers connected to them, will inevitably be tempted by malicious attacks and curious people, so it is needed to ensure that the system is highly resistant to attack. The specific requirements include[2]:

(1) Requirements for strong identity authentication, to ensure the authenticity of the identity of visitors.

At present, the railway fuel system through the user name / password to confirm the user's identity. This way is simple and easy, but there are many hidden dangers. First of all, the password is easy to be intercepted when it is sending in clear text transmission on the network. Secondly, once the password is compromised, all security mechanisms will fail.

(2) Requirements for data transmission security.

At present, the transmissions of the data information of railway fuel system in railway internal network and external network are all based on network transmission. The network transmission based on TCP/IP protocol has resulted in the openness of data information, and Information is very easy to be intercepted, the information content is very easy to be cracked. In order to make up the security leak, it is necessary to protect the communication channel for encryption transmission.

(3) Requirements for access control.

Based on identity authentication, give different access privileges to different authorized users, and prohibit the unauthorized user access. Internal and external network users have this requirement.

(4) Requirements for enhancing data audit.

Through the detailed application level logs, we can record the system resources and the application data resource that user access, to meet the initial requirements of non-repudiation of the system. Non-repudiation refers to that the instructions sender can not deny that he has issued the instruction afterwards. To regulate business, to trace the responsibility of the incident, to avoid disputes, this has a great role.

(5) Requirements for single sign on.

While logging in security system, login application system, to reduce the number of user login, increase the ease of use of the system.

(6) Requirements for strengthening the network security of the equipment in the railway internal network.

The internal network builds a secure VLAN, to protect the oil system server deployed in railway internal network from being attacked by viruses, Trojans and worms.

3. Construction goal and construction principle of the information security system of the platform

3.1 Construction goal.

Prevent accidental and malicious attacks, to meet the application infrastructure, application services and information content confidentiality, integrity, availability, controllability requirements. These requirements belong to the categories such as information network, data, information content, information security management.

Protect information assets of enterprises from all kinds of threats Ensure the continuity and availability of business. Reduce the threat of information to enterprises. Ensure the sustainable management of enterprises. Improve the rate of return on investment and competitive advantage of enterprises.

3.2 Construction principle.

In line with relevant state regulations, the principle of overall safety, the principle of unity of the whole network, the principle of standardization and consistency, the principle of moderate protection, the principle of practicality, efficiency and extensibility, the principle of combination of technology and management.

4. Construction content of the information security system of the platform

4.1 Construction of digital certificate server system.

Construct digital certificate server system, to solve the problem of strong identity authentication, to ensure the authenticity of the identity of the person and the device in the login security system and application system. As the underlying infrastructure of the information security platform of the oil distribution system, the root key is stored in the encryption machine, and the personal certificate is stored in the KEY USB.

4.2 Construction of application layer transmission encryption machine.

Construct application layer transmission encryption machine, to ensure that the business data information of the railway oil system is safely transmitted in the application layer when it is

transmitted in the railway intranet network and the extranet network. And give the fine grain control to the user's access authority.

4.3 Construction of the directory server to store user's account information.

Certificate issued by a digital certificate server system and CRL lists are stored in the directory server, and account information maintenance by application layer transmission encryption machine is also unified from the directory server. The user name account information of the oil distribution system is also stored in the directory server.

4.4 Development of single sign on.

Through the development of application layer transmission encryption machine and oil system single sign on, improve the ease of use of the system.

4.5 Construction of UTM firewall.

Construct UTM firewall and partition VLAN, to insulate from the application server of other departments logically. And open anti-virus, anti-spyware, anti-intrusion function module, to protect the application server to avoid the threat from the network.

4.6 Construction of distributed host antivirus server.

Through distributed host anti-virus, to ensure that the host, smart terminal (operating system for XPE) is not affected by viruses, Trojans, worms, malicious code threats. With the UTM firewall and application layer security transmission gateway, set up three layers of solid gas system, and ensure the security of gateway, server, host and intelligent terminal.

5. Research on Key Technologies of information security of the platform

5.1 Network topology of Service platform information security system.

Third party logistics service platform of railway oil supply chain security system includes internet sub-system and extranet sub-system. Network topology is shown in Figure 1.

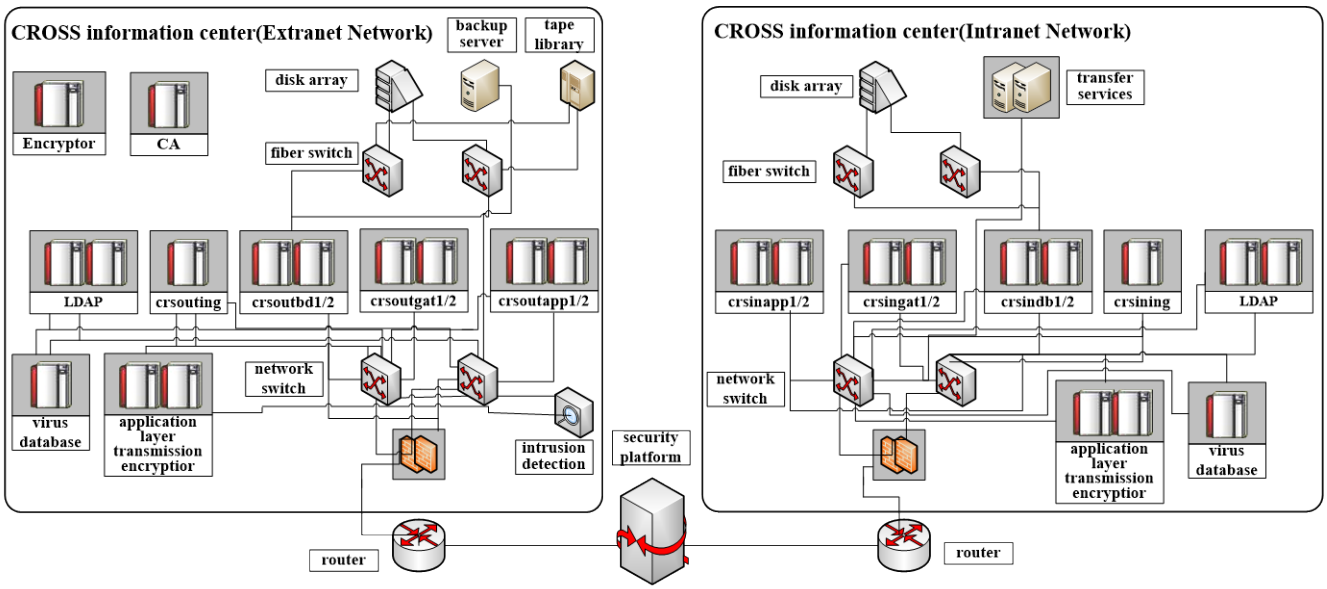

Fig. 1 Security system network topology

5.2 PKI/CA technology of railway oil distribution system.

CA authentication system uses koal CA certificate authentication system, and the certificate follows the X.509 V3standard. Product performance in the form of a hardware server [3].

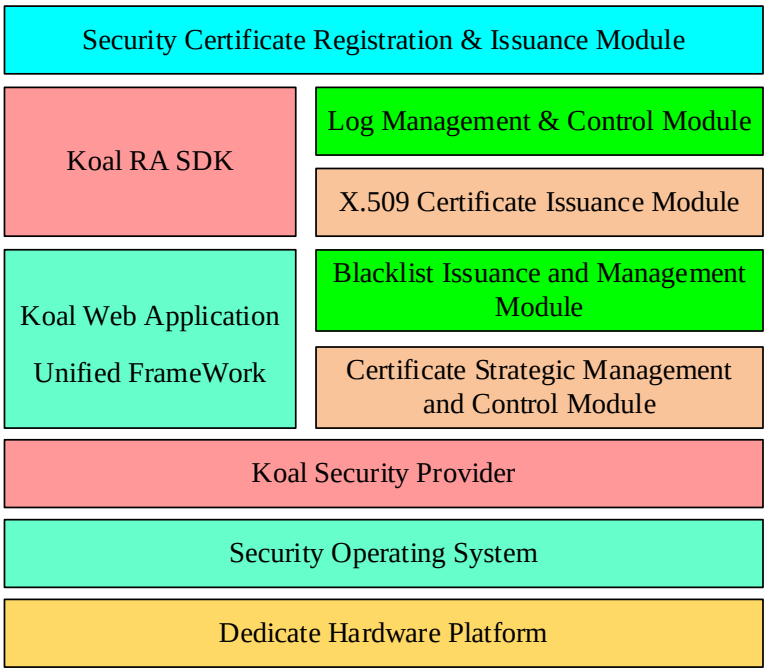

Fig. 2 Framework of CA authentication system

The PKI/CA system is constructed in an independent physical region. This is not physically incorporated into any one network, therefore, to improve the security of the PKI/CA platform [4].

The key of PKI/CA system is produced by the commercial cipher encryption machine which is recognized by the national secret office, and the user certificate and the CRL list are posted to the LDAP server. Deploy the LDAP servers one leader with one-follow in external network and one-follow with one hot stand-by in internal network[5].

The function of PKI/CA system is mainly to complete the registration application, issuance and management of the user certificate.

5.3 Design of application layer transmission encryption machine.

Application layer transport encryption machine SJY26 is an important part of the platform; it is the carrier and guarantee for the safe transmission of all business data. The encryption channel of SJY26 application layer transport encryption machine is developed based on SSL protocol, which is a kind of session layer tunneling technology. It establishes a secure data transmission channel between the client and the server. At the same time, it can also use the public key mechanism to achieve mutual authentication between the browser and the server[6].

Algorithms supported by application layer transmission encryption machine: PKI(X.509), DES, DES, AES, 3AES, RC2, RC4, IDEA, MD5, SHA, RSA, SSL3.0 and so on[7].

6. Conclusion/Summary

This paper analyzed the six requirements of the security technology of information exchange in the railway oil supply chain, and put forward the construction goal, construction principle, construction content and key technology of information exchange security of the information security system of the third party logistics service platform of the railway industry oil supply chain, which included PKI/CA technology of railway oil distribution system and design of application layer transmission encryption machine.

7. Acknowledgment

The paper is sponsored by National Science-technology Support Plan Projects “Research and Application of the Third Party Logistics Service Platform of Railway Oil Supply Chain” (No. 2014BAH23F02).

8. References

[1]. Ma Huijuan, Research on Railway Oil Integrated Supply Model Based on the Third Logistics [D]. Beijing, Beijing Jiaotong University,2013.

[2]. Zhang Haitao, Lan Yun, Ji Shouwen,“Technolgy Report of Information Exchange and safe Technology of Railway Oil Supply Chain”, unpublished.

[3]. Changyuan Luo, Wei Li, Hailin Li, “Measurement Method for Space Networks Authenticated Key Security under Distributed CA”,[J],Journal of Electronic & Information Technology, 2009, 31(10).

[4]. Guo Jinsheng, ”Research of Security Platform Construction Based on CA Digital Certificate”, [J],Modern Electronic Technique,2010, 33(3).

[5]. Zhou Xiaobin, Xu Yong, Zhang Ling, “Research on open identity authentication model for PKI”,[J], Journal of National University of Defense Technology, 2013, 35(1).

[6]. Han Yizhi, Zhao Yi, Tang Xiao-bin, “MD5 Algorithm”, [J],Computer Science,2008, 35(7).

[7]. Hu Shaozhong, Tao Qiuxiang, Yang Guojun, “The Application of Homomorphic Encryption Technology in Cloud Computing Data Transportation”, [J], Bulletin of Science and Technology, 2012, 28(12).