Data Exchange Technology Across Networks Based on Trusted Computing

Chao Li¹,*, Xiang Han, Zhao Liu², and Li Zhao¹

¹First Research Institute of the Ministry of Public Security of PRC, Beijing, 100048, China
²People’s Public Security University of China, Beijing, 100038, China

Abstract. The authors analyze the existing technologies in the field of cross-network data exchange and their deficiencies in ensuring the safe transmission of data. We propose a technology to improve the security of data exchange across networks, which is based on trusted computing. We design an audit method of the data exchange to prevent the leakage of sensitive information, investigate the subject of the leak and ensure the integrity of the data transmission. We have proved the credibility of the method and the ability of data security protection in the process of cross network data exchange, by protecting data files and applications.

1 Introduction

At present, with the rapid development of information technology, information technology has been deeply applied to politics, national defense, finance, science and technology, industry and other key areas. In order to ensure the security of the network, physical isolation is adopted in various fields, but the method of physical isolation makes cross network data exchange difficult. At present, the data exchange between networks adopts the methods of mobile media copy, dual network card host, FTP transmission, Gate Ferry and data encryption. With the continuous upgrading of network security problems such as hacker intrusion and virus attack, the above-mentioned cross network data exchange methods have exposed many shortcomings, which can no longer meet the current requirements of people for cross network data exchange.

In view of the current situation, this paper proposes a cross network data security exchange method based on trusted computing. This method uses trusted computing to strengthen the protection of system process and system data resources, which can prevent system process from being tampered, data leakage, hacker intrusion and virus attack.

2 Current situation of cross network data exchange technology

2.1 Copy of removable storage medium

The traditional method is to manually copy the data that needs to be exchanged across the network to a mobile storage medium such as a mobile hard disk for data exchange across the network. Mobile storage such as mobile hard disk has the advantages of large media capacity, portability and flexibility. In cross network data exchange, this method has high
security because of its physical isolation. However, there are several deficiencies in this way: only a part of authorized personnel is qualified to copy data, so it cannot meet the growing data exchange; poor real-time performance, unable to achieve real-time transmission; there are some security risks, which are easy to cause data copy errors and tampering problems, and mobile storage media are easy to be infected by viruses [1]; lack of audit for exchange data, unable to guarantee the integrity of data transmission.

2.2 Dual network card host

The dual network card host is to install two network cards on one host, which connect two different networks respectively, and transmit the data of one network to another network through the dual network card host. The data transmission speed of cross network data exchange mode with dual network card host is fast, which can review data files, easily check viruses, and centrally control data. However, the security of the transmission mode is difficult to be guaranteed, the implementation cost of hardware is high, and the transmission audit function is lacking.

2.3 FTP transmission

File transfer protocol (FTP) is a set of standard protocols for file transfer on the network, which is a common and traditional way of data transfer across the network. FTP allows users to communicate with another host in the form of file operation (such as file addition, deletion, modification, query, transmission, etc.). The cost of implementation of this method is low, it can check whether there is virus in the file, and the operation is relatively simple. However, FTP transmission is not suitable for the transmission of large files, and the security of this method is difficult to guarantee. It has a large transmission delay, prone to transmission errors, transmission interruption and other problems, and lacks the audit function.

2.4 GAP and FGAP

Gap, the full name of security isolation gateway, realizes the ferry of internal and external network data through ferry type data transmission. The gateway is generally composed of internal host, external host and special disconnector system. At the same time point, the gateway only exchanges data with one of the internal or external networks, that is, when the gateway is connected to the external network, the gateway will automatically disconnect with the host of the internal network. This way can ensure that the internal network and the external network do not realize the exchange of information, and realize the physical isolation between the two networks [2]. FGAP is the inheritance and development of GAP, which is used for data transmission from classified network to unclassified network, high-level network to low-level network, to prevent the leakage of key sensitive information of classified network and high-level network. The basic principle of the shutter is based on the unidirectionality of the light. The data to be transmitted is mirrored to the target position by the optical splitter to realize the data transmission [3]. However, simultaneous interpreting of data across networks by using GAP and FGAP may cause a single channel failure problem, and its transmission rate has been determined and cannot be expanded, which cannot meet the requirements of different transmission rates of various applications [4]. And this method does not exchange records, and cannot audit the data exchange behavior.
2.5 Data encryption storage and transmission

Data encryption storage and transmission of cross network data exchange process is generally composed of three main modules: data collection, data exchange and data distribution. The data acquisition module obtains business data from data source, performs format check, security filtering and other operations on business data, and rejects the data that does not meet the requirements. The data exchange module first encrypts the business data file at the software level, and then writes the encrypted data file to the disk data directory. The data exchange module reads the data file from the disk data directory, and exchanges the data file to the end-to-end data unit, and writes the encrypted data file to the disk data directory. The data distribution module reads the encrypted file from the disk, checks the integrity of the data file, refuses to process the incomplete data file, decrypts it, obtains the original data, and finally distributes the decrypted business data to the target data source.

There are some shortcomings in the way of data encryption storage and transmission cross network data exchange: there is no consistency check on the execution code within the operating system; the access of resources is not strictly controlled within the operating system; regular system upgrade can prevent known threats, but the protection ability for unknown threats is weak; the risk of data leakage in the data exchange system.

3 Design of cross network data security exchange technology based on Trusted Computing

3.1 Basic concepts of trusted computing

Trusted computing is a trusted computing platform based on hardware security module, which is widely used in computing and communication systems to improve the overall security of the system. The definition of trusted computing in ISO / IEC15408 standard is: the behavior of a trusted component, operation or process can be predicted under any operating conditions, and it can well resist the damage caused by application software, virus and certain physical interference.

Compared with the traditional concept of security, trusted computing has the meaning of two-way security: maintaining the interests of computer system users and the operation of foreign users. At present, Trusted Computing Platform Alliance (TCPA) and Microsoft's next generation secure computing base are the leading research in trusted computing.

3.2 Design of cross network data exchange scheme

In order to solve the problem of insufficient data protection in the process of cross network data exchange, this paper proposes a scheme of using trusted computing to strengthen the protection of system process and system data resources, to prevent the system process from being tampered and data leakage.

3.2.1 Hardware design

The whole data exchange process is divided into three parts: external network, isolation area and internal network. The internal and external network is the data source and destination of data exchange, and the isolation area is the data exchange system based on trusted computing. The hardware structure is composed of two mainboard hosts, which are
divided into external network exchange unit and internal network exchange unit. The internal exchange unit receives and forwards the data that needs to be exchanged from the internal network, and the external exchange unit receives and forwards the data from the internal exchange unit. The two mainboards are installed with trusted reinforcement hardware, which solves the problem of data anti tampering at the hardware level. After the data from the external network is transmitted to the isolation area, first check the data receiving format in the external network switching unit to achieve security filtering, and then transmit it to the internal network switching unit for integrity verification before data distribution. The data from the internal network also needs to be transmitted to the isolation area. The data format is checked through the internal network exchange unit to realize the security filtering. The data integrity verification and data distribution are carried out in the external network exchange unit. The system hardware structure based on trusted computing is used to realize application trust, configuration trust and access trust. The hardware design is shown in Figure 1.

3.2.2 Software design

The software of cross network data exchange mainly consists of three modules: data collection, data exchange and data distribution. The following describes the data security protection measures of trusted hardware reinforcement from the whole process of data exchange. The flow chart is shown in Figure 2.
The process of data cross network exchange is as follows:
- Data collection: obtain business data from data sources;
- Data check: perform format check, security filter and other operations on business data, and reject the data that does not meet the requirements;
- Data encryption: encrypt business data files;
- Write data in: write the encrypted data file to the disk data directory;
- Trusted detection: when there is a process to read the data file, the trusted reinforcement program will detect the process, judge whether it is a certified process, and carry out consistency verification, judge whether the program has been tampered, only allow the program that passes the trusted authentication and has not been tampered to read the data file, and protect the data security;
- Data reading: the data exchange module reads data files from the disk data directory;

Figure 2. Software design flow chart.
- Data exchange: the data exchange module exchanges the data files to the peer data unit, and the data files of the external network exchange unit to the internal network exchange unit;
- Write data in: write the encrypted data file to the disk data directory;
- Trusted detection: whether it is data exchange module or data distribution module or any behavior that wants to read data files, trusted detection should be carried out. Only program processes that pass trusted authentication and have not been tampered with are allowed to read data files to protect data security;
- Data reading: the data distribution module reads data files from the disk data directory;
- Integrity verification: check the integrity of data files and refuse to process incomplete data files;
- Data decryption: decrypt the data file to obtain the original data;
- Data distribution: distribute the decrypted business data to the target data source.

3.3 Audit of cross network data exchange

The data transmission across the network based on Trusted Computing relies on hardware devices, so it is impossible to know the process information and results of data transmission. In order to prevent all data to be transmitted from missing, and transmission interruption caused by network interruption and other reasons, and ensure the integrity of transmission data, this method has the audit function of cross network exchange data. The main body of audit function is audit log. The contents of audit log include the start and end time of data exchange, ports of sender and receiver, contents of exchange, operation behavior of administrator, etc. By looking up the log information, the sender can verify whether the data to be transmitted has completed the transmission, as well as the cause and location of the transmission interruption, and the receiver can judge whether all the data to be received has been received.

The audit log is used by the administrator of the classified network to judge whether the sensitive information is leaked. By checking the information of the sender and the receiver in the audit record, determine the responsible subject of the leakage and investigate the relevant responsibilities. As electronic evidence, audit log plays a warning role for those who want to disclose secrets and protects important data from being stolen by lawbreakers. The audit log records all operations of the administrator to avoid information leakage caused by internal personnel. The log records shall be stored and transmitted in a unified and standard format, and shall be backed up and archived on a regular basis. Only authorized audit management personnel have the right to view and archive. Auditors can check and archive regularly, extract and view the historical records of the exchange, verify the exchange content, check the illegal transmission behavior, and the viewing behavior will also be recorded to avoid unexpected deletion, modification or coverage. If the log information involves the content of the secret network, it needs to desensitize the log information to maintain the security of the sensitive information.

4 Security analysis of cross network data security exchange technology based on trusted computing

4.1 Realize the protection of data files

Trusted reinforcement protects data files. Any reading behavior of data directory files will be trusted detected. Non certified programs are not allowed to access the data directory. The detailed implementation process is as follows:
- The trusted reinforcement program monitors the data directory `/data/` in real time;
- When the behavior of reading the data directory file is detected, the data reading process is obtained, and the process program is compared with the program in the white list to determine whether it is an authenticated program;
- If it is a non-certified program, the data file read operation is rejected.

![Diagram](image)

**Figure 3.** Data file protection process.

Through the protection of data files, it can effectively prevent attackers from illegally obtaining data content, copying data to U disk, sending files to other servers through the network, tampering with data files, deleting data files and other attacks will fail, and the data will not be disclosed, tampered with or illegally transmitted.

### 4.2 Implementation of application protection

Trusted reinforcement protects applications, including application startup detection and application file tampering detection. The detailed implementation process is as follows:

- Whitelist control mechanism: Based on the whitelist control mechanism, the whole root of the system is scanned first, and the binary files and executable files are recorded with hash values, which are saved in the white list database. The kernel module controls the program execution according to the white list library. When the startup of the executing program is detected, the kernel module first extracts the hash value of the starting program, and then hashes the contents of the whitelist library. If the record exists in the whitelist library, it is allowed to execute, otherwise, it is denied to execute the program.
- Real time monitoring of application directory/APP/.
- When the application file modification behavior is detected, extract the hash value of the content of the file to be modified, and then check the hash value of the content in the white list database. If the record exists in the white list database, the modification is allowed, otherwise, the modification is rejected.
Through the protection of the application program, the behavior of changing program files and tampering with program files will fail, the data exchange program cannot be tampered, and the attacker cannot obtain data, which can effectively prevent the attacker from stealing data by illegally tampering with the application program.

![Application protection process diagram]

**Figure 4.** Application protection process.

5 Conclusion

In view of the problems existing in the current data exchange in the cross network isolation environment, such as mobile media copy, dual network card host, FTP transmission, Gate Ferry, data encryption storage and transmission, this paper proposes a method of cross network data security exchange based on trusted computing, and designs the software and hardware. This method adopts the mode of both internal and external prevention and internal prevention as the main goal to protect the data exchange system. From the hardware level, it realizes the anti-tampering of the system data and controls the data access permissions. Only the data exchange process is allowed to access the business data directory on the disk to prevent other illegal programs from reading the data and causing data leakage. At the same time, in order to ensure the safety of the system's own operation behavior, the data exchange behavior is audited to facilitate traceability.

It is proved that this method can protect business data from any illegal program process, equipment and personnel during the storage and transmission process of cross network data exchange system, avoid data leakage and enhance the security of cross network data transmission. At the same time, it protects the core configuration files from illegal tampering and audits the system operation behavior, which improves the security of the system itself, thereby ensuring the integrity and non-repudiation of data transmission across the network.
This paper is supported by the National Key R&D Program of China Project 2018YFC0809802.

References

1. Yuanming Nie, Huiliang Han, Liping Gu, Computer Security, J, 04, 50-52(2013).
2. Yan Li, Chunling Wang, Information Technology and Informatization, J, 01, 36-37(2005).
3. Chenglin Li, Laser Journal, J, 39(04), 134-138(2018).
4. Yue Yang, Ruobing Wang, Rui Liu, Computer Applications and Software, J, 34(04), 135-141(2017).
5. Fangyong Hou, Jin Zhou, Zhiying Wang, Zhen Liu, Application Research of Computers, J, 12, 1-4+22, (2004).