The Security of E-commerce Data Transmission

Guofang Zhao

Department of Computer Technology,

Hebei College of Industry and Technology

Hebei Shijiazhuang, 050091, China

E-mail: zhaoguofang2002@163.com

zhanyou Yan

School of Civil Engineering,

ShiJiaZhuang TieDao University

Hebei Shijiazhuang, 050043, China

E-mail: yanzhanyou@163.com

Abstract—**The amount of data transmission in Electronic commerce (E-commerce) is growing, and the security requirements are also increasing. During the data transmission , the data transmission module is divided into four parts, They are respectively: the Internal network, isolation module, firewall and the untrust domain or external network. At the isolation module, the exchange isolation unit, data transmission unit, file transfer unit, and other units and engines, are set. The security is enhanced in e-commerce in many ways, the large flow of data transfer between different trust domains.**

Keywords-isolation; firewall; transmission security;untrust domains

I. INTRODUCTION

Contemporary information technology and computer network technology has been tremendous development, information technology has become the key to the development of human society and economic factors. E-commerce is the product of the combination of network and economic in recent years. With the expansion of the scope and application of the use of demand, the Internal enterprise business is extended more and more to non-trusted domains, such as the Internet, which would cause a great threat to the security in the enterprise internal network. Due to the internal network data security and confidentiality requirements have the high requirements, how to protect in Maximum extent to the internal network security is a primary problem of the enterprise paying attention to. This article describes a safe and effective method of data transfer between different trust domains.

II. INTRODUCED PRINCIPLE

The framework of the principle of the secure transmission of data between different trust domains is divided into four parts. The first part is the internal network, including various types of servers and clients; Part 2 is isolated parts, including protocol analysis engine, content security engine, design engine and various virus killing engines, as well as file transfer module, data transmission module. Data from Internal network will firstly go through the processing unit in the Internal network, and then go through the isolation exchange unit, and finally go through the external network processing unit to the part 3. After the isolation and handling of this three-layer unit, the data link layer connection will be cut down in circuit, and the exchange will be done in above the network layer. This allows the inner network data to be very effective protection [1]. After into Part 3 and the external network switch, and take another one the firewall ,the data can enter Part 4. The part 4 is untrust domain. The data obtained layers of processing, it can be more safely to the next step transmission. In contrast, data from untrusted domain must go through layers of processed to reach into the internal network. The part 2 is a purely isolated portion plays, it is an important role for the secure transmission of data, in which the data transmission module further plays a decisive role.

III.   DATA TRANSFER MODULE

The data transmission module need by the proxy stub of the Internal network processing unit and the proxy engine of the External network processing unit to work together[2]. The proxy stub is a CGI application, which response the Web requests of the administrator and handle forwarding; The agent engine provides the service of the guard process, which accept request of handling the Proxy stub through the transmission channel. Data processing mainly in the following process:

A.   Exchange the data between the processing unit within the network and the external network.

The data exchange between the processing unit within the network and outside the network processing unit is done through the isolated transmission hardware and software of the independent design and the custom transport protocols[3]. Isolated transmission channel is shown in Figure 1.
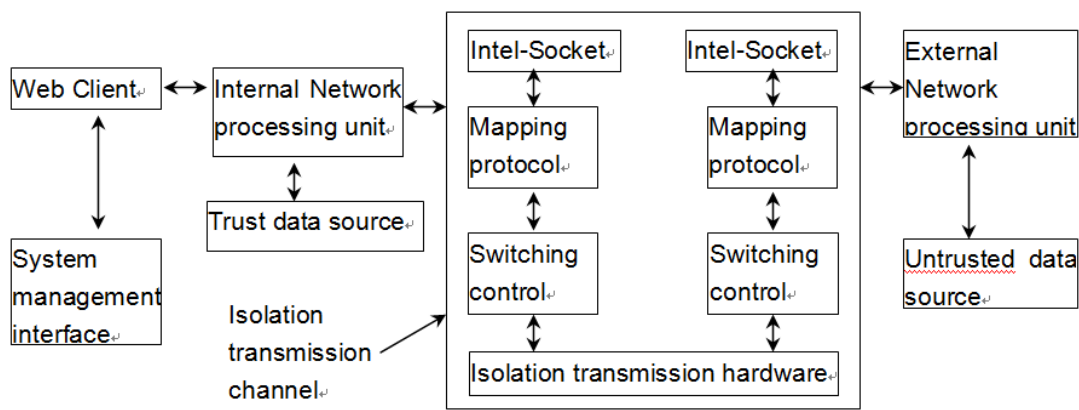

Figure 1.   transmission module with isolation channel

The box in Figure 1 is isolated from the transmission channel, is composed mainly by the high-speed switch and the isolation storage device. Internal network processing unit transmits the user's identification information, data transmission planning, etc. to the external network processing unit. The external network processing unit sends the data operation resultsinformation to the within the network processing unit.Because different data content, the format of the application-layer data within the Internal network processing unit sends and external network processing unit has slightly different.

B.   Read data information

Administrator change the content specified through configuration ODBC.INI file, and achieve the application access to different data sources. The key is connected to the data source.

C.   Data type conversion

Different data systems have different data type definitions, which need to find out the correspondence relation between them. First, to obtain the data type information in the source and target systems, connect the data source, including the various natures of data type; Then based on this information, the correspondence between them needs to determined, corresponding transformation rules needs to develop. In the conversion process, the nature of the various types of data of the data type would be paid attention to.

D.   To achieve the module security

The most critical problem in the modules to achieve is how to safely insert the data from the untrusted domain to the isolate trust domain network. The security is the basis of the module functions. It can be done several aspects to guarantee. The first is the security within the network. Using

the physical isolation system, the internal network and external network are physically isolated. The cutting of the data link layer connection is the most effective safety measures. The second is the security of the isolation channel. In the isolated transmission channel architecture, the only way of the inside and outside the network for data exchange is swap the file through the isolation store device. At this time, outside network intrusion will scan firstly through the scan engine in the external network processing unit. Once found to be unsafe factors, it can not enter into the swap file. So that, the outside the network processing unit like be hidden for the external network. No services available for invasion tempted port. And the external host system using a dedicated security technology, the kernel-level intrusion detection and the compulsory access control can protect the safety of the network processing unit very good.

IV. CONCLUSION

With the combination of the network and economic deepening, the amount of data transfer in the e-commerce is growing. The secure transmission is one of the important goals. This paper presents such a transmission method between different trust domains is on the basis of safety measures, increases the improvement of the isolation channel module, that made the greater improve in the security of e-commerce data transmission. In practical applications, the effect is obvious, get a good evaluation.

REFERENCES

[1] Zhang Zhihong. "Other transactions coexist in the real time of transaction system data organization and access method," computer engineering and Applications, vol.21, pp.23 -25, 2002.

[2] The Constitution, Wan-Cheng Wang. "Design and Implementation of the transmission network," Control Engineering, vol. 9, pp.52-53, 2002.

[3] Yin Yong. "Internal and external network collaboration system Any lnfo," Design and implementation of data communication, vol. 2, pp.34-35, 2003.

[4] Kong Fang, Xu Ting. The design research of data migration tools," Computer application and software, vol. 22, pp.133-135, 2005.

[5] Chen Li, "the B2C electronic commerce secure transmission mechanism of information flow in the study," Journal of Information Engineering University, vol. 3, pp.35-38, 2005.