ISBN 978-952-5726-10-7
Proceedings of the Third International Symposium on Computer Science and Computational Technology(ISCSCT '10)
Jiaozuo, P. R. China, 14-15, August 2010, pp. 014-016

Realization of Information Security in Electronic Commerce

Li Fu-Guo[1] , Dong Yu-Jie[2]

[1]WanFang College of Science and Technology of HeNan Polytechnic University, Jiaozuo,China
E-mail: lfg@hpu.edu.cn
[2]WanFang College of Science and Technology of Henan Polytechnic University, Jiaozuo,China
E-mail: hpudyj@hpu.edu.cn

***Abstract*—With the wide application of E-commerce, E-commerce security issues become more prominent and urgent. This article discussed information security issues in electronic commerce activities, some solutions are proposed to realize E-commerce security in operation and E-commerce environment.**

Index Terms—**Electronic commerce,Information security, Realization, Network**

I. Introduction

E-commerce is the use of advanced electronic technology to general business activities. E-commerce includes two aspects: First, business activities; second electronic means. Modern electronic commerce is a new business activities based on Internet technology, is the main mode of business operation of 21st century market economy. With the globalization and opening of the internet, without restriction of time and space bring all sorts of e-commerce transactions insecurity. Network information security issues has become an important factor affecting the development of electronic commerce. Therefore, research in an open network environment e-commerce security becomes a very urgent and important field.

II. Measures against E-commerce security issues to be taken

E-commerce security issues relate to various aspects of e-commerce and participate in all aspects of e-commerce transactions, it is a systems engineering and social issues to solve the e-commerce security issues, need participation of whole society. But at the operational level, the following measure should be adopted.

First of all, we should build e-commerce security technology framework systems. In the e-commerce transactions, e-commerce security is mainly network security and transactions security. The network security is the network operating system against network attacks, viruses, so that keep a continuous and stable network operation, commonly used firewall technology protection measures. Transaction security is the data protection of the parties are dealing not be destroyed, as both non-disclosure and transaction identity confirmation, you can use encryption, digital certificates and authentication, SSL (Secure Socket Layer)security protocol, SET(Secure Electronic Transaction) and other technologies to protect.

A. Computer virus prevention technology

Computer viruses are actually a kind of function program running in the computer system, it can destroy and infect against computer system. Virus transmission through the system after a successful attack or breach of license, the attackers usually implant in the system procedures such as Trojan horses or logic bombs, facilitate conditions for the subsequent attack to computer system or network[1]. The current anti-virus software is facing the challenge of the Internet. Currently, hundreds of new viruses were produced in the world every day, and more than 90% of viruses are spread via the Internet. In order to effectively protect the enterprise's information resources, required anti-virus software can support all internet protocols and e-mail systems may be used by e-commerce users, so that it can adapt in time and keep up with the rapidly changing pace of the times. Most anti-virus software mostly focus on stand-alone anti-virus, although some manufacturers introduced a network version of the antivirus products, it only be used in the desktop and file server for protection, the scope of protection is still relatively narrow, so anti-virus vendors should try to enhance protection of the gateway or e-mail server as quickly as possible .Only effectively cut off the entrance of the virus, it will be possible to avoid economic losses of e-business users caused by outbreak of virus.

B. Firewall technology

Firewall as a separator, limiter and analyzer, it mainly used for implementing the access control policy between the two networks, it effectively monitored the network and all activities of the network, it provided necessary access control for the internal network without causing the network bottlenecks, control the data access system of the network through security policy to protect critical resources within the network.

C. Intrusion detection system

With the increasing risk factor of network security, IDS (Intrusion Detection System) as a beneficial complement to firewall, it can help the network system quickly find the coming possible attack, IDS expanded the security management capacities of system administrator (including Security audits, Monitoring, Attack recognition and responsion) and improved the integrity of the information security infrastructure.

Intrusion detection system is a dedicated system which give a real-time monitoring to network activities and behind a firewall, it can work with firewalls and routers and used for checking all communications, records and prohibited network activities of a LAN(Local Area Network) segment, it can be re-configured to prohibit the malicious data traffic come from the outside of the firewall[2]. IDS can quickly analyzed the information on the network or did user audit analysis in the host, manage and monitor network access through the centralized console, so that realized linkage between IDS and network switching equipment. The information of various data streams reported to the safety equipment, IDS can detect network access based on reported information and data streaming content, carry out targeted actions quickly when network security events were discovered, and send these actions response to security incident to firewall or switch, the switch or firewall closed and disconnected accurate port, IDS tried to cut off the connection initiatively and respond immediately when network attacks were discovered.

D. Information encryption method

The purpose of information encryption is to protect the data, files, password and control information within the network and also to protect data transmitted online. Network encryption methods commonly used link encryption, endpoint encryption and node encryption[3]. Link encryption is designed to protect the link information security between network nodes, endpoint encryption's objective is to protect data transmitted from source user to the destination user, the purpose of node encryption is to protect the transmission link between the source node and the destination node. Users can select encryption methods appropriately according to network conditions.

E. Digital certificates and authentication

Digital certificates and certification is a series of data in network communication which marks identity of the communication parties and also a rigorous identity authentication system established through the use of symmetric and asymmetric cryptography. Digital certificates and authentication have following functions :the data not to be stolen by other people except the sender and the receiver and not to be altered during transmission, the sender can confirm the identity of the receiver through digital certificate , the sender can not denied for the information which to be sent.

F. SSL security protocol

SSL is a secure communications protocol. SSL provides a secure connection between two computers, the entire session is encrypted, thereby ensuring the security of transmission. SSL has three characteristics: using symmetric cryptography to encrypt data; using authentication algorithm to proceed the integrity test; using asymmetric cryptography for authentication of the end entity identification.

G. SET technical standards

SET (Secure Electronic Transaction) is a technical standards which pay for the security funds through open network, SET provides real security rule to the applications of electronic transaction based on credit card: ensure secure transmission of the internet and transmission data is not stolen by hackers; orders and personal account isolated, when the order contains the cardholder account sent to businesses, the business can only see the orders but not the cardholder's account; cardholders and merchants authenticated mutually, so that to determine the identity of both communication sides, usually a third party responsible for providing credit guarantee to both sides of the online communications; requires the software follow the same protocol and message format so that software developed by different manufacturers have compatibility and interoperability function and may be run on different hardware and operating system platforms.

III. Environment Measures to Keep E-commerce Information Security

A. Construct a sound e-commerce system

Actively participate in international cooperation and integrate international e-commerce framework, construct e-commerce system suitable for China's national conditions. As a sovereign state, in order to safeguard national interests and economic security, we must pay attention to proprietary technology development which related to e-commerce technology, not all rely on imports. Therefore, we must increase investment, focus on the research and development of e-commerce security technology.

B. Strengthen the laws and regulations

To against the new types of crime related to information technology and information systems, government departments should organized forces quickly and combined with the objective of e-commerce needs so that to strengthen the existing laws and regulations related to electronic commerce, it is a usual practice of human history to fight against crime with the use of law. Chinese government can strengthen the laws such as: "The People's Republic of China Criminal Law", "the National People's Congress Standing Committee decision on Internet security", "Contract Law", "Copyright Law" and other related laws. In these laws, it can properly increase the penalties provisions for cyber crime and increased the terms of copyright protection of network works. Relevant authorities of the government should develop departmental rules and regulations firstly so that to against related issues need to be solved quickly with the development of e-commerce such as electronic payments, tax Administration, security certification, network and information security, intellectual property rights protection, consumer protection and so on, when necessary, administrative rules and regulations can be issued by the State Department, and then rose to the legal procedures.

C. Speed network infrastructure construction

Information infrastructure is the material basis and the carrier for development of electronic commerce. Speed up the network infrastructure construction, promote the process of enterprise information, it is the direct driving force to enhance the research of science technology and application in the related applied fields with which we can obtained the "innovation" and "sustainable development" in the information security field and information field. The development of information infrastructure needs support of variety of disciplines and talents, the joint efforts of government and industry, in particular the Government's strong investment and macro-control.

Ⅳ. Conclusion

Chinese Government should strengthen the research of e-commerce information security, so that to establish a flexible legal framework to regulate e-commerce, so that to make e-commerce open, reasonable and legalization. This will ensure not only the interests of all e-commerce sides but also the smooth progress of e-commerce. Enhance the security of e-commerce, in addition to using advanced science and technology arm, but also its own e-commerce companies to take proactive security measures. Enterprises must carry out its internal security awareness education for all staff so that they can fully understand the importance of enterprise information security, and take appropriate preventive measures to against insecurity factors, this is the only way to ensure the safe operation of e-commerce information.

References

[1] JIN Bo, SONG Ping, “A Probe into the Information Security of Electronic Documents in Electronic Government,” Journal of Shanghai University (Social Science Edition), vol. 16, pp. 128–129, March 2009.

[2] YUAN Jia-bin, GU Kai-kai, YAO Li, “Security Grid Technology Based on Information Security Control Theory,” Journal of Nanjing University of Scinece and Technology (Natural Science Edition), vol. 31, pp. 423–425, April 2007.

[3] WANG Da-kang, DU Hai-shan, “Encrypt & Crack Technology in Information Security,” Journal of Beijing University of Technology, vol. 32, pp. 498, June 2006.