E-COMMERCE ONLINE PAYMENT SECURITY ISSUES DISCUSSION AND ANALYSIS

Preeti Dhankar*

Abstract:

Nowadays electronic commerce services have risen to become more ... The handling of the payment may involve many ways, such as online banking. Computer network technology is developing fairly rapidly. With the Internet, Hacker and Virus overflows, such as the growing threat of cybercrime, network security management tasks will become increasingly difficult and complex, good grasp of network security issues on protection of network information security. Development of electronic commerce exist in today's security threats and the corresponding technical solutions. Therefore, the article on e-commerce payment security issues of network analysis.

Paper Keywords: Electronic commerce, e-commerce technology , network security , security issues.

* Pursuing Ph.D.

Introduction:

The developed and developing countries, through the Internet to conduct e-commerce transactions have become the trend. With the development of internet and network infrastructure, continuous improvement, our e-commerce Although shape, but the development of electronic commerce security issues have become urgent issues. E-commerce is built on an open network environment, the maintenance of trade secrets is important to promote the use of comprehensive e-commerce security. E-commerce process, buyers and sellers through networking, because internet is an open network, the establishment of trade relations between the two sides of security and trust is more difficult, this article on the e-commerce Internet payment security issues Discussion and Analysis.

The concept and characteristics of an e-commerce

1) The concept of e-commerce: e-commerce (electronic commerce) is a telecommunications network through the production, marketing, sales, distribution and other activities, not only refers to the Internet-based transactions, but also refers to the use of electronic information technology to solve problems, reduce costs, add value and create business opportunities for commercial activities.

2) e-commerce features:

1) The first thing that makes e-commerce so great is Ubiquity; it is available everywhere at anytime. Online the stores never close.

2) E-commerce redefines the traditional distribution model, to reduce intermediate links, allowing producers and consumers to deal directly as possible, and thus to a certain extent changed the socio-economic operation mode.

3) Universal Standards are standards shared by the world. This is a revolutionary thing for not just e-commerce but the world. It gives us all the ability to connect at the same "level" and it provides network externalities that will benefit everyone.

4) E-commerce provides a wealth of information resources for the socio-economic factors provide a more re-combination of the possible, which will affect the social and economic layout and structure.

5) Global Reach is a great feature of e-commerce. It takes the marketplace to market space. You can go "shopping" all around the world in one place.

E-commerce security technology system

1) **Physical security.**

(A) According to national standards, information security level and financial situation, development of appropriate physical security requirements, and by the construction and management to achieve the relevant standards.

(B)Besides application security and network security, the place (usually a data center) that hosts your ecommerce applications should be physically secured and with proper secure operation procedures.

(C)The key system resources (including hosting, application server, security, GAP and other equipment), communications circuitry, as well as the physical medium (soft / hard disk, CD-ROM, IC card, PC card, etc.), should be encrypted, electromagnetic shielding, etc. protection measures, should be placed physically safe place.

(D)The computers that host Web Servers and Database servers must be located in a physically secure facility, usually a secured data center.

2) **Network security**. Network Security refers to the security of operating systems and servers. Hackers can gain portions of control over your operating systems or servers by exploring flaws in operating system and server software. In order to ensure the smooth progress of e-commerce transactions require stable and reliable e-commerce platform should be able to provide services without interruption. Any disruption in the system (such as hardware, software errors, network failures, virus, etc.) may result in e-commerce systems do not work, leaving trade data in determining the effectiveness of time and location can not be guaranteed, often cause great economic losses.

3)**Data transmission and application development OR Business Security.** Mainly refers to business transactions appear in the media in the network security issues, including the prevention of business information theft, tampering, counterfeiting, trade act was to deny, namely, e-commerce to achieve confidentiality, integrity, authenticity, non-repudiation. All sensitive information being transmitted should be encrypted. Businesses can opt to refuse clients who can't accept this level of encryption. Confidential and sensitive information should also never be sent through e-mail. If it must be, then it should also be encrypted. All aspects of business security, but also through various network security technologies and standards for secure transactions implemented encryption and decryption technology ensures the confidentiality of transaction information, but also solve the issue of user's password has been stolen; digital signature is to achieve the full text of the original report of identification, authentication and review it together to put an end to the transaction system, forgery and repudiation acts. To ensure the safety of the major e-commerce technologies: online payment protocol (Secure Sockets Layer SSL protocol and Secure Electronic Transaction, SET protocol), file encryption, digital signature technology, electronic commerce Certification Center (CA).

4) **System administration security.** Primarily to protect the host computer's operating system and database systems. For the protection of system security, the overall idea is: through security reinforced to address the management of security vulnerabilities; and then use security technology and equipment to enhance its security capabilities. System administrators should keep watch for suspicious activity within the business by inspecting log files and researching repeated logon failures. They can also audit their e-business system and look for any holes in the security measures

Safety management process supervision:

To enhance the whole process of safety management

1) Network planning stage, it is necessary to strengthen the construction and management of information security planning. Information security-building need to invest certain amount of manpower, material and financial resources. According to the situation to determine a realistic network security goals and milestones, implemented in phases to reduce investment risks.

2) Project construction phase, construction management unit to a summary of security requirements and safety performance function tests, included in the various stages of construction work of an important part to enhance the development (implementation) personnel, version control management, to strengthen the right development environment, user routing settings, the key to the code inspection.

3) In the operation and maintenance phase, we should note the following:

- The establishment of an effective safety management organizational structure, clear responsibilities, streamline processes, the implementation of efficient management.
- In accordance with classification management principles, strict management and the internal user accounts and passwords, access within the system must pass rigorous identification, to prevent illegal occupation, fraudulent use of legitimate user account and password.
- Develop a sound safety management system, strengthen information network operating systems, databases, network devices, applications, operation and maintenance process safety management.
- To establish pre-emergency police system and establish a network security to maintain logs, records and security-related information and events, it occurs to facilitate tracking and tracing, but also regularly check the logs in order to promptly identify potential security threats.

The establishment of a dynamic closed-loop management process

Network is in constant development and adjustment, it may find new security vulnerabilities, so need to create dynamic, closed-loop management process. To control the overall security policy and guidance, through the security assessment and testing tools (such as vulnerability scanning, intrusion detection, etc.) to keep abreast of the network security problems and security risks, which established the safety of construction planning and strengthening programs, integrated application of various kinds of security products (such as firewalls, authentication and other means), the system adjusted to the relative safety of the state. And to note the following two points:

1) For an enterprise, the security policy is to pay for information security at the core of developing clear and effective security policy is very important. Security organizations according to this strategy is to develop detailed procedures, regulations, standards and security-building plan, program, to ensure that these series of policy norms in the implementation of an enterprise-wide, thereby protecting the investment business and information resource security.

2) To develop a sound, practical information in line with corporate security policy, one must first secure the enterprise information network to assess the situation, namely, the security of information assets, technology and management assessment of the status quo, so that enterprises face security threats and their own a comprehensive understanding of the problem, so as to formulate specific security policies to guide the construction of information security and management.

Conclusion:

This paper analyzes the current e-business Internet payment security, the main technical condition, safety technology, network technology can be said that the more cutting-edge technology, are very advanced technology tools; if used properly, with appropriate safety management measures, the basic guarantee e-commerce online payment security; but it is not 100% perfectly safe, but relatively safe. With the advances in network security technology and credit mechanisms for the improvement of the network will be more secure payment.

References:

- Ke newborn. Internet payment and settlement [M]. Beijing: Electronic Industry Press, 2004.
- Yi Yanbo. E-business regulations [M]. Beijing: Beijing Jiaotong University Press, 2007.
- Guo-Bin, FAN Yue-Jiao. E-commerce security and management [M]. Beijing: Electronic Industry Press, 2006. Reposted elsewhere in the Research Papers Download
- http://www.hi138.com
- http://ecommerce.insightin.com/internet_security/physical_security.html
- http://ecommerce.insightin.com/internet_security/network_security.html
- http://en.wikipedia.org/wiki/Electronic_business