Research on Security Issues and Strategies of E-commerce

Jing Hu

Abstract. Today, e-commerce activities develop rapidly. The paper deeply discusses the problems of network security that the e-commerce is facing, explores and researches the security issues of e-commerce, which is conducive to the healthy development of e-commerce. The paper analyzes the common potential security risks of the present network transaction, and proposes security measures.

Keywords: e-commerce; internet; network security.

Overview of e-commerce

E-commerce is a production of information when the commerce of the modern enterprise has developed to a certain extent and combined with the present advanced computer technology, and is a new commercial transaction method in order to meet the fast-paced life and work of modern people. Specifically speaking, buyers and sellers can transact without facing each other, and communicate and transact with internet, for example, the popular online shopping and WeChat payment all belong to e-commerce. The application scope of e-commerce is wide, and its transaction mode can be divided into the transaction between enterprise and enterprise, enterprise and individual, individual and individual, enterprise and government. With the development of computer technology, the application of e-commerce becomes more and more wide with tremendous developing potential.

Performance of security issues of e-commerce

Stealing transaction information. Stealing transaction information of e-commerce mainly refers to the transaction information of the two parties is stole by the third party, or the document provided by one party to the other party is illegally used by the third party. The threaten is caused by the insufficient
encryption measures or security level in the process of transmitting information. Attackers can invade by installing intercept device on public telephone network, internet, wire tapping and within the electromagnetic radiation range, or by intercepting data on routers and gateways where the data package passes. The attackers can find the law and format of information by several times of stealing and analysis, in order to obtain the content of the information and then gain the confidential Information, which can derive defrauds like winning trap, pitfall of cash on delivery and phishing website.

**Tampering transaction materials.** E-commerce transaction pays much attention on the authenticity and integrity of information. When the transaction information is transmitted in network, attackers can revise the information halfway with various means and technical methods after they understand the commercial information or master the law of the network information data. Then they send the tampered false information to the receiving terminal, and the customer can not distinguish the information in general. Then the information loses authenticity and integrity. This method is not fresh and can be realized on a router or gateway.

**Transacting with identity theft.** During the network transaction of e-commerce, fake server, whose name is similar with the that of seller’s server, is often established and pretends to be seller to establish false orders and transact. Customers are attracted to the platform to consume with favorable conditions through the fake transaction platform which cheats the customers out of payment. Users usually can not judge because of the fictitious network platform. The most method adopted by lawless person is “phishing sites” to carry out information cheat, that is, a similar real shopping website is duplicated or the bank website is simulated. By propagating false consuming information or bank information, the personal interest of consumers is infracted. Therefore, the transaction of e-commerce needs identity recognition of both parties. Only then can not the opportunity be provided to the third party to carry out false transaction.

**Reason of the generation of the security issues of e-commerce**

**Vulnerabilities of operating system** Each operating system has vulnerabilities. Therefore, network invaders can enter the system, obtain many operation authorities of data, and gain what they want through the security vulnerabilities of the system in order to gain profits in e-commerce activities. How the vulnerabilities generate? In fact, we do not patch the system in time, or patch the system with the software of the third party and the lowest level is acquiescently chose in settings. Moreover, we do not enhance the shield for system, such as firewall system and intrusion detection system. Besides, there may be Trojan virus embedded by people with ulterior motives. All of these provide convenient conditions for invaders.

**Hacker’s attack** Hacker is the biggest danger in the security of e-commerce. Their purpose is to steal interests, such as commercial secrets and personal accounts and passwords, and gain economic profits. Hacker is the biggest
hidden trouble among our present security threatens. Their attack methods are too many to prevent.

**Weak consciousness of managers** Good enterprise and personal account all have rigorous managing mechanism which protects our interests from harm. However, in fact, many enterprizes of e-commerce have not established rigorous system and managing system of hardware, and there is nobody responsible for that. Even if some enterprizes of e-commerce have been aware of the importance of security and bought products, such as firewall, IDS, and antivirus software, they do not pay attention to the setting and updating. Some even use pirated software. These have significant effect on our network security and lead to enormous loss. With the development of computer technology and the popular of internet, the speed of computer virus invading internet and destroying resource becomes faster. The environment of e-commerce is seriously threatened. At present, many lawless persons collect information with “viral invasion”, and send the simulate e-mail or pictures and videos to strangers depending on the incompletion of antivirus information of personal computers. If they are opened, the virus will attack the computer by itself and send back the personal information on the computer, which seriously threatens the transaction security of e-commerce.

**Primary strategy to enhance the security of e-commerce**

**Perfecting defense system** Hacker has many attacking methods, so we can not take the initiative to attack and only passively prevent. First, antivirus software can be installed to prevent its scanning of port and delivery of system virus. The antivirus software should be updated in time to prevent hacker’s attack effectively. Second, needless port can be closed, such as 21 port of ftp, 23 port of remote logins. Only can the port 80 be opened in order to not affect internet. Third, share should be cancelled, which should be changed in registry. You can consult a professional or check it on Baidu. Fourth, the safety index of browser should be improved. High safety value should be set. Fifth, you should not login some bad websites. Scanning code or clicking pictures all maybe the common methods that the hacker uses under your client. In short, hackers are everywhere, and we should increase our safety consciousness which is the most important.

**Enhancing the identity authentication of personal information** We know that the core of e-commerce is not electronic but commerce. Electronic is a part of commerce and an actual representing part. Its main purpose is to finish commerce. The consumption subject of commerce is consumer and the subject of personal financial information of consumers is still consumer. At present, the products for the security of e-commerce, no matter software or hardware, all protect the security of electronic products, such as computer antivirus software, firewall, U shield, etc. There is no confirmation to the most important consumption subject. Any computer network system has defect, and even the famous Microsoft system also regularly release patches to make up for vulnerabilities. We should clearly and soberly recognize that simple protection of the electronic system is one-sided. Once lawless persons steal the personal
information of consumers with system vulnerabilities, then the so called most perfect safe information guarantee exists in name only.

It will be different if we enhance the identity authentication of personal information. It will firstly check if the financial system of the authenticated object is accordant with the personal information left on transaction platform or if it is correct during the e-commerce transaction to inspect whether the authenticated object is the real consumption subject. The safety indicator of this type of authentication is high. The main form of expression is physiological information verification, such as fingerprint (or palm print and cheilogramma) verification, iris verification, etc. However, the cost of this type of verification is higher and the information collection is significantly affected by the hardware. If the research on this aspect is enhanced, reducing cost or influence of hardware will begin a new era in the field of identity verification of personal information security of e-commerce information.

**Developing the research method of “cloud” technology** At present, the most advanced computer network technology is “cloud” technology. The most prominent characteristic of “cloud” technology is to analyze the computer network information submitted by users with several servers and feed back to users depending on computer network technology.

If we apply “cloud” technology to the guarantee of network security technology of e-commerce, what will happen? Before the transaction of e-commerce, consumers upload the information of website to a cloud server who check the authenticity of the website and the transaction information will be sent to another cloud server, and the accuracy of information will be checked; meanwhile, the transaction platform will upload the information of the consumer to a cloud server and firstly check the personal consumption ability of the consumer, then the personal information will be uploaded to another cloud server to check the authenticity of the consumption; on the other hand, financial institutions will also upload the personal information of the consumer to a cloud server to check if the information is correct, and then upload the information of the transaction platform to another cloud server to check the safety and stability of the transaction platform. All of these information will be gave back to the parties, and the consumer can decide whether to continue the e-commerce transaction. The process seems to be complex, but as for the great cloud calculation, this information retrieval process can be finished only within several seconds.

**Strengthening the safety awareness of managers** No problem can be solved only by technology. Problems referring to people is the problem of management. Only the manager pay more attention can the safety awareness be improved. The propagation of the large medias is also an important way to increase the safety awareness of managers, followed by comprehensive safety program, enhanced management of network security, developing relevant system, regular check, updating network devices, etc. Only in this way can our e-commerce environment be safe and dependable, and can users be more reassuring to shop online.
Improving the legal supervision of e-commerce security In the era of internet, the law of e-commerce security should be improved, and institutionalizing construction of e-commerce should be enhanced. Meanwhile, the content like the rights and responsibilities of the parties in e-commerce, the legal relationship of electronic contract, electronic authentication and electronic payment security should be clearly stipulated to ensure the good development of e-commerce.

Conclusions

In the era of internet, e-commerce develops rapidly. If the development of e-commerce want to be kept, it is necessary to pay attention to the security issues of e-commerce. Establishing and improving a perfect and harmonious e-commerce environment are not only the requirement of the common consumers but should be considered by the government on the macro-control. Meanwhile, the computer network security technician should strive for it. We have reason to believe that with the advancement of science and technology, we will welcome a new era of e-commerce in the near future.

Acknowledgements

The primary idea of the paper is from the summary and analysis of the papers of Wei Dan, Yu Xiuli, Li Sujuan, Song Pengkun, Li Wenlong and Sun Jinxia. I would like to extend my sincere gratitude to them.

References