The application of information security technology in electronic commerce

Xinyi Chen[1, a]

[1]School of computer science and technology, Chongqing University of Posts And Telecommunications, Chongqing 400065, China;

[a]anfieldk18@gmail.com

Keywords: Electronic commerce; information security; application.

Abstract. With the rapid spread and development of the Internet all over the world, e-commerce has gradually become the mainstream of trading. E-commerce has a unique way of trading and provides new global business opportunities, hence more and more people are using the Internet for transactions. However, in recent years, e-commerce information security has become the main reason for hindering its rapid development. Through the analysis of the importance of information security in e-commerce, this paper discusses the potential problems, the solutions and the technologies need to be applied. The research content of this paper provides the necessary guidance for the rapid development of e-commerce and the improvement of application level.

1. Introduction

Electronic commerce, also known as e-commerce, has drew the attention of the Internet. Firms and organizations worldwide have emerged on the Internet to provide services, products, and everything you can think of. However, not everyone survived in this game. Those who succeed understand that they do e-commerce for making money by providing a new service through the Internet, by enlarging the range of an existing service, or by providing services at relatively lower cost. Yet those who choose to perform e-commerce are taking a risk. They are making investment in newly appeared technologies and new methods of providing products and services with the hope of earning profit from it. These risks caused by several problems: people may not accept the service, new target customers might not appear as predicted, or the existing customers may not like the new service. All the new threats and weakness caused by performing e-commerce must be taken into consideration by these organizations and the risks created by these threats need to be taken into account.

Without trust, most prudent business operators and clients may decide to forgo the use of the Internet and revert back to traditional methods of doing business [1, 2]. To counter this trend, the issues of information security at the e-commerce and customer sites must be constantly reviewed and appropriate countermeasures devised. These security measures must be implemented so that they do not inhibit or dissuade the intended e-commerce operation [3]. This paper will discuss pertinent information and network security issues to e-commerce and customer privacy and some proper solutions to them. These threats originate from both hackers as well as the e-commerce site itself.

2. E-commerce information security requirements and problems

E-commerce is different from the traditional way of trade, the transactions are carried out through the network, buyers and sellers cannot face to face during the process of the transaction, which requires the network to transmit our various information, including name, address, telephone, bank card password and other private information. This requires that the trading environment for e-commerce to be very safe, otherwise the information may leak or be stolen at any time. In general, due to the openness of the Internet itself and the existing technical problems in the e-commerce platform, the reality of the e-commerce system is facing a lot of security issues, these problems are mainly concentrated in five areas, shown as in Figure 1.

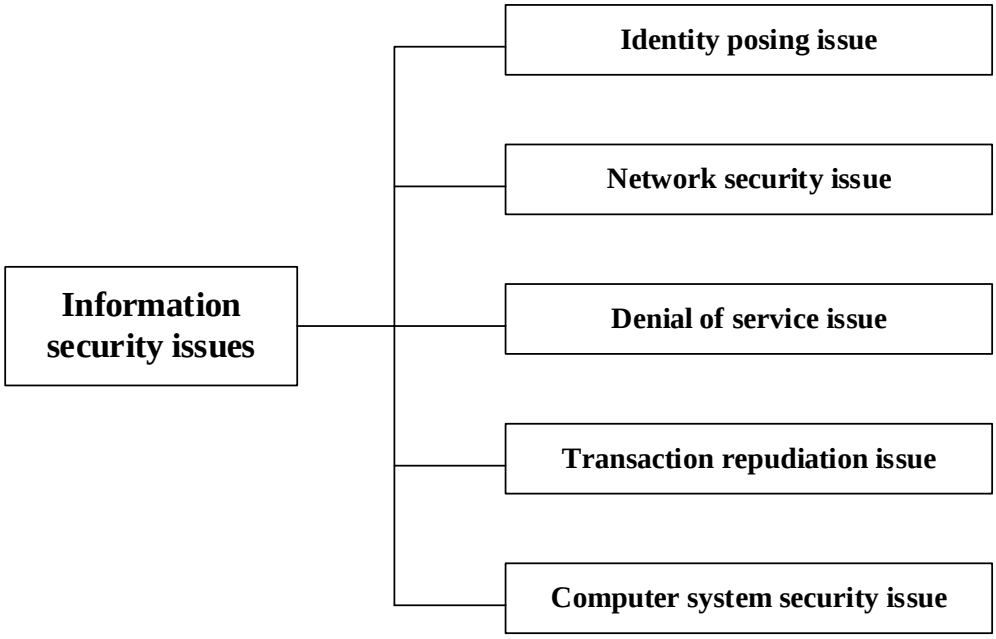

Fig. 1 Information security issues in electronic commerce

Identity posing. As e-commerce is different from the traditional way of trading, it cannot clear the identities of both parties to the transaction, which gives online hackers more chances to use illegal means to steal legitimate users' information and trade them with others in order to get illegal interests. At present, the pervasive phenomena are posing as legitimate users to make transactions, posing to frame others up, posing as the host computer to cheat other legitimate users or legitimate hosts and so on.

Network Information Security Issue. Because of the openness of the Internet, when the data transmission is on the network channel, the illegal users will analyze the physical characteristics of the network and the use of protocols, and damage the information through interception, deleting, tampering, insertion and other means [4]. In general, the interception is the attacker in the transmission channel to intercept confidential or useful information, such as bank accounts, passwords, etc.; deleting is to delete a certain part of the information or all, so that legitimate users cannot get complete information; tampering is through changing the order in which the information flows are transmitted to modify or impair the content of the information; insertion is the insertion of invalid information in the useful information so that the legitimate user obtain an error message or invalid information.

Service Refusal Issue. This type of problem is mainly caused by the attacker by forging a large number of false information, taking up the normal information channel or server resources, so that legitimate users cannot access the necessary network resources, making the services with strict time limit cannot get timely response. For example, as for a virtual shop, an attacker can fake a large number of user information, and send invalid orders to take up network and server resources, so that the site cannot provide timely feedback to the normal user.

Disavowal of both parties to the transaction. This type of issue is mainly caused due to some users maliciously deny their own information to pass the buck. For example, the site publisher denies the information they just sent so that they are not responsible for the users; the buyers deny their orders and do not receive goods; sellers deny the products they sell so that they refuse to take responsibility for the quality problems. The settlement of these problems requires a uniform arbitration standard and a strong arbitration institution.

Computer system security issues. As the users are scattered around the world, not every machine can be guaranteed to run normally and effectively, hence the data loss caused by hardware damage, the data leak caused by virus, and intrusion attacks brought by the Trojan will bring severe computer system security issues.

3. The main security technology in e-commerce

The security of e-commerce depends heavily on the improvement of technology. These technologies include encryption technology, authentication technology, access control technology, information flow control technology, data protection technology, software protection technology, virus detection and removal technology, content classification identification and filtering technology, network hidden scanning technology, system security monitoring alarm and audit technology, and of which the most important is the firewall technology, encryption technology and identity authentication technology.

Firewall technology. Firewall is a popular solution for enterprise network security issues that is, putting the public data and services outside the firewall so that the access to internal resources of the firewall is limited. In general, the firewall is not anti-virus, although there are a lot of firewall products claim that it has this feature. Another weakness of firewall technology is that the update of data between firewalls is a challenge and cannot support real-time service requests if the delay is too large. In addition, the firewall using filtering technology, filtering usually reduces the network performance by more than 50%. If purchasing the high-speed router to improve network performance, it will greatly improve the economic budget. As a network security technology, the firewall has a simple and practical features with high transparency. It can reach to a certain security requirement without modifying the original network applications. However, if the firewall system is compromised, the protected network is in an unprotected state.

There are many advantages of firewall technology, one is that by filtering the unsafe service, it can greatly improve the network security and reduce the risk of the host in the subnet; the second one is to provide access to the system control; third one is to pretend the attacker from attacking useful information; the fourth is that the firewall can also record and statistics through its network communication, to provide statistics on the use of the network, according to statistical data to determine possible attacks and detection; fifth, the firewall provides means to develop and implement network security strategy, which can be centralized management of enterprise intranet.

Data Encryption Technology. Data encryption technology is the most basic network security technology, which is mainly used to ensure the data in the storage and transmission process of confidentiality. The technique uses the mathematical method to reorganize the original information so that the content that is publicly transmitted on the network after encryption is an incomprehensible character for the illegal recipient. As for legitimate recipients, people can use the key through the decryption process to get the original data, so as to achieve the purpose of protecting information. The process of becoming a ciphertext is called encryption, and the process of reverting to the plaintext is called decryption. The variable parameter used for decryption is called the key [5]. The general data encryption model is shown in Figure 2.

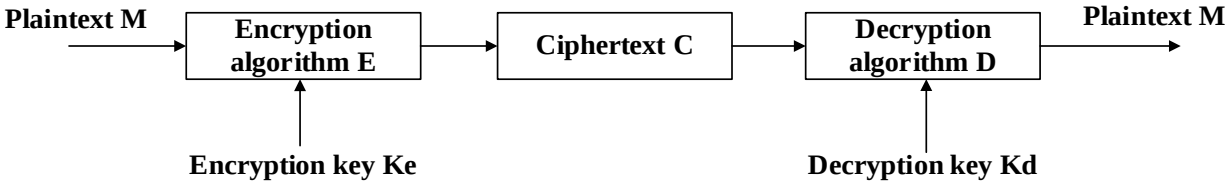

Fig. 2 General data encryption model

General data encryption methods are commonly used in two categories: one is symmetric encryption, one is asymmetric key encryption. (1) In the symmetric key encryption system, the key used for encryption is the same as the key used for decryption. Or although the key is not the same, one can be derived from one of the keys, that is, the sender and the receiver use the same key. The use of symmetric key system does not need to exchange encryption algorithm, only need to exchange encryption key, thus it can simplify the encryption process, enhance the encryption and decryption speed, yet there is issues of key allocation, preservation and management. The widely used symmetric encryption algorithm is the DES algorithm. (2) In the asymmetric key encryption system, the encryption and decryption of the information used by the key is different. And it can not be derived from one key to another. The asymmetric key encryption system solves the problem of key allocation,

preservation and management of the symmetric key encryption system, but the encryption algorithm is complex and the encryption and decryption speed is slow. The earliest representative algorithm for asymmetric key encryption is the RSA algorithm. It can be seen that the two encryption techniques have their own advantages and disadvantages, and they are complementary in the Internet open network environment.

Basic encryption technology. The basic encryption technology is not enough to ensure the security of transactions in e-commerce, information authentication and identity authentication technology are important technical means to ensure the safety of e-commerce indispensable. Authentication technology is an effective way to prevent the transaction information from being tampered with, deleted, repeated and forged. It plays an important role in the security of various information systems in open environment. There are digital signatures, digital timestamps, and digital certificates and so on.

A digital signature is a result of using someone's private key to encrypt a particular message digest hash value, which links people to a specific message, similar to a handwritten signature. In daily life, usually with a document to sign to ensure the true validity of the document to prevent its rejection. In a network environment, electronic digital signatures can be used as simulations.

In a written contract, the date and signature of the document are the key to preventing the file from being forged and tampered with. In electronic transactions, it is also required to secure the time and date of transaction documents, and digital time stamp service will be able to provide electronic file publishing time security.

In the transaction payment process, the participating parties must use the certificate issued by the certification center to prove their identity. The so-called digital certificate, is to use electronic means to confirm the identity of a user and the user access to network resources.

4. Conclusions

The issue of information security in the field of e-commerce has always been a matter of concern. Therefore, how to solve this problem better is the motivation to promote e-commerce better and faster. Through the analysis of the importance of information security in e-commerce, this paper discusses the potential problems, the solutions and the technologies that are applied. Security is the core and soul of e-commerce. However, because the security problem is constantly evolving, so the means to solve security problems will continue to change. At present, e-commerce also has many new technologies, but has not yet been able to form an effective and secure e-commerce security system, which requires increased efforts to research and develop information security and confidentiality technology to establish a secure business environment.

References

[1] Ratnasingham, P. (1998). The importance of trust in electronic commerce.*Internet research*, *8*(4), 313-321.

[2] Suh, B., & Han, I. (2003). The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of electronic commerce*, *7*(3), 135-161.

[3] Turban, E., King, D., Lee, J., & Viehland, D. (2002). Electronic commerce: A managerial perspective 2002. *Prentice Hall: ISBN 0*, *13*(975285), 4.

[4] Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The journal of strategic Information Systems*, *11*(3), 245-270.

[5] Coppersmith, D. (1994). The Data Encryption Standard (DES) and its strength against attacks. *IBM journal of research and development*, *38*(3), 243-250.