Study on the Application of Computer Security Technology in E-commerce

Shiyu Wang1,*

1Department of Basic Application, Shandong Transport Vocational Collge, Shandong, 261100, China

*Corresponding author e-mail: Shuixx80@sdjtzyxy.com

Abstract. With the rapid development of economy, e-commerce has become a part of people's life, which has changed people's way of life. Taobao, Jingdong and other B2B, B2C, C2C trading platforms have changed the traditional way of shopping, which can meet the consumption needs of modern people. Therefore, the 21st century has entered the era of e-commerce. At present, there are many hidden dangers on the Internet, such as stealing information, tampering with information, counterfeiting and so on, which will seriously damage the property security of Internet users. However, e-commerce is inseparable from the Internet, which requires us to continuously strengthen computer security technology (hereinafter referred to as CST). Computer network security has become a key issue of e-commerce, which requires us to constantly improve information security and anti-counterfeiting. Therefore, we have applied a variety of computer security technologies in e-commerce, such as digital signature, firewall, VIP and so on. First of all, this paper analyzes the role of CST in e-commerce. Then, this paper puts forward some problems. Finally, this paper puts forward the CST applied in e-commerce.

Keywords: Computer Security Technology, E-commerce, Application

1. Introduction

E-commerce has become a part of people's life. However, there are many security risks in e-commerce, which will lead to many loopholes on both sides of the transaction [1]. Therefore, we must strengthen CST, which will lead to malicious attacks by criminals. Through CST, we can protect the security of e-commerce transactions, which will protect the information security and property security of all parties to the transaction [2-4]. Therefore, CST has been applied to e-commerce, which also needs continuous improvement of protection technology. With the rapid development of e-commerce, more and more attacks and viruses begin to target the e-commerce plate, which also drives the research and development of computer technology. Through CST, we can protect the network information security, which can protect the confidentiality of the information of both sides of the transaction [5-7].
2. The role of CST in E-commerce

2.1. Characteristics of CST

CST mainly includes operating system security, database security and network security, which can protect the computer hardware and software from being tampered and damaged due to malicious reasons. In the information society, computer technology has been applied to various industries, which has become the basis of most industrial operations. Therefore, CST is directly related to economic development. In the application of Internet, the most important protection of computer is the security of data storage. Some computer viruses, illegal access may cause damage to the database, which is the most important problem [8].

2.2. The role of CST in E-commerce

In the development of e-commerce, both sides of the transaction rely on the Internet to complete the relevant operations, which is highly dependent on the network platform. In the process of transaction, if the illegal elements steal the database and other relevant information, it may cause serious economic losses. Therefore, security vulnerabilities will have a significant impact on the stability of society. Therefore, the purpose of the application of CST in e-commerce should be to establish network barriers, which can reduce the impact of external factors on the business platform. Through CST, we can ensure the security of capital transactions and information, which will improve the user experience in consumption and shopping. Therefore, CST is the foundation of e-commerce, which can improve the service quality of e-commerce [9].

3. Security risks of e-commerce network

3.1. Stealing information

Without encryption, the data information is transmitted in plaintext on the network. The intruder can intercept the transmitted information on the gateway or router through which the data packet passes. Through repeated theft and analysis, we can find the law and format of information, and then get the content of the transmission information. Therefore, this can cause information leakage of online transmission [10].

3.2. Information tampering

E-commerce transactions generally require users to register their personal information first. If the intruder attacks the computer network maliciously, personal information may be leaked. At this time, the intruder will take the opportunity to add, delete or arbitrarily modify the information, which will destroy the integrity of network information [11].

3.3. Forgery of information

The forgery process of e-commerce transaction information is completed in Ming channel. Because some businesses do not strictly encrypt the user information, some lawbreakers take advantage of this vulnerability to forge user information. By changing the e-mail, criminals can send the false e-mail address to users and inform them to pay, which is easy to make users fall into the network fraud [12].
3.4. The destruction of information

Network hackers use advanced technology to invade the computer internal network system, which will obtain important business information. At the same time, hackers can wantonly destroy the information content, which will cause great consequences [13].

4. Practical application of CST in E-commerce

4.1. Data encryption technology

Data encryption technology in CST can play a very good effect in e-commerce. In e-commerce transactions, the main way to encrypt data information is to use private key and public key, which can ensure the security of e-commerce activities. At the same time, data encryption technology can effectively prevent intruders from destroying information, which can ensure the information security and reliability of e-commerce transactions. The schematic diagram of symmetric key encryption / decryption is shown in Figure 1.

![Figure 1. Schematic diagram of symmetric key encryption / decryption](image)

4.2. Firewall technology

Firewall is mainly composed of software and hardware equipment, which is an effective barrier for information security in e-commerce activities. Packet filtering technology firewall is mainly used to check the passing of each packet, and then judge whether the packet passes or not according to its attributes. If the IP set by the firewall is dangerous, then the output data will also be intercepted by the firewall. Address migration firewall technology is mainly combined with the application requirements, which can shield the intranet address to ensure its security. Proxy service firewall technology mainly acts as an intermediary, which can monitor and control the communication information of application layer. Firewall technology is shown in Figure 2.

![Figure 2. Firewall technology](image)
4.3. VPN Technology

VPN technology is an important way of information encryption. Through VPN, we can form a virtual private network that can transmit media, which can be used for bilateral transactions. VPN technology is shown in Figure 3.

![Figure 2. Firewall technology](image)

4.4. Database encryption technology

Database encryption technology is a method of using encryption technology to protect database information, which can protect database security. Through a special algorithm, database encryption technology can change the original database information, which will lead to unauthorized users unable to obtain encrypted information. The database encryption technology is shown in Figure 4.

![Figure 3. VPN technology](image)

![Figure 4. Database encryption technology](image)
4.5. Safety warning

Vulnerability warning can reach the patch probability in a short time, which can resist external threats. Usually, we can start security warning according to the abnormal network traffic, which can improve the security of both sides of the transaction. The security early warning module is shown in Figure 5.

![Security alert](image)

**Figure 5.** Security alert

4.6. Identity authentication technology

Shopping on the e-commerce platform needs to be standardized in the identification technology. Only after identification, users can log in to the network normally. However, the identity of network communication is uncertain, which needs to strengthen the identification technology. Through the identification technology, we can prevent the intruder's malicious attack and destruction, which will ensure the normal and orderly operation of e-commerce transactions. The identity authentication center is a fair third party, which lays a foundation for the establishment of an authoritative framework for the identity authentication process. Identity authentication center builds a mutual trust environment for online transactions, which solves a series of problems such as online identity authentication, public key distribution and information security. Identity authentication is the key to ensure the security of e-commerce. The certificate with public key is digitally signed by the identity authentication center, which makes the certificate unable to be forged. Each user can obtain the public key of the authentication center. By verifying the digital signature of any digital certificate, the authentication center can determine whether the certificate is issued by the authentication center and whether the digital certificate is legal. By analyzing the digital identities of both parties, we can determine the legitimacy of their digital identities, which can avoid malicious tampering of personal information.

5. Conclusion

The healthy development of e-commerce is inseparable from CST, which is the basis of network transactions. Through CST, we can reduce the problems in the development of e-commerce, which can better create a secure trading environment. By improving CST, we can meet the needs of people's convenient transactions, which is also the purpose of social development.
References

[1] Cai Baoyu. Application of computer network security technology in e-commerce [J]. Computer products and circulation, 2020 (05): 18.

[2] Duan Huijun. Discussion on the application of computer technology in e-commerce with tea product sales as an example [J]. Fujian tea, 2020 (06): 80-81.

[3] Han Shufang. Application of computer network security technology in e-commerce [J]. Electronic technology and software engineering, 2020 (15): 231-232.

[4] Huang Jipu. Analysis of the application of computer network security technology in e-commerce [J]. Digital technology and application, 2020 (03): 192-194.

[5] Li Jun. application of computer network security technology in e-commerce [J]. Satellite TV and broadband multimedia, 2020 (08): 20-21.

[6] Li Manyuan. Application of computer network security technology in e-commerce [J]. Modern marketing (next issue), 2020 (07): 98-99.

[7] Liu Zhijie. Application of computer technology in e-commerce [J]. Computer products and circulation, 2020 (05): 20.

[8] Shi Yinghui. Application of computer network security technology in e-commerce [J]. Papermaking equipment and materials, 2020 (02): 230-231.

[9] Wang Gang, Yang Ning, Yu Xiaona. Application of CST in e-commerce transactions [J]. Information and computer (theoretical Edition), 2020 (19): 12-15.

[10] Yun Pengyu. Application of computer network security technology in e-commerce [J]. Computer knowledge and technology, 2020 (18): 224-225.

[11] Zhang Yanting. Application analysis of CST in e-commerce [J]. China new communication, 2020 (22): 134-135.

[12] Zhang Yumin. Application of computer network security technology in e-commerce [J]. Information and computer (theoretical Edition), 2020 (15): 198-200.

[13] Zhang Zhihao. Application of computer network security technology in e-commerce [J]. Journal of science and technology economy, 2020 (20): 17.