Electronic Commerce in Computer Networks

Kezhu Feng[1,a*] and Shan Gao[2,b]

(Xijing University)

[1]Xijing University, No.1 Xijing Road, Chang'an District, Xi'an City, Shaanxi Province ,China

[2]Xijing University, No.1 Xijing Road, Chang'an District, Xi'an City, Shaanxi Province ,China

[a]8264772131@qq.com, [b]2420150483@qq.com

Keywords: Computer, Network, Electronic Commerce

Abstract. Computer major is a big category, including computer technology, network technology and its application. It is in the field of computer. E-commerce is the specific application of computers, and is a new field related to trade. The application of e-commerce is very wide, computer is its foundation, and the focus is on the development and application of e-commerce. The network system must strictly abide by all kinds of relevant technical principles and follow all kinds of relevant technical standards and norms. In the design, we should note that the network system must conform to the principles, and also should pay attention to the electronic commerce network security hidden dangers, electronic commerce transactions in the application of network security technology.

Introduction

The design of computer network system should follow the principle: (1) Four high: high bandwidth, high reliability, high performance, high security; (2) Three easy: easy to manage, easy to expand, easy to use; (3) Two support: Support the principle of virtual LAN and multimedia application.

For computer network system, good level design provides a good guarantee for network reliability, network performance and network scalability. At present, networks are faced with the ever-increasing need for performance and scalability. In addition, the network must be guaranteed to provide key features such as high availability, manageability, and flexibility. But the basic design principles and the ability to switch between layers 2 and 3 have not changed significantly. The main changes are in a wider range of network devices and technologies that can support more network applications and improve scalability and usability. New features should include QOS, multi-tier services, increased trunk bandwidth, increased gigabit port density, and greater switching capacity.

Computer Network System Design Principles

The network system must strictly abide by all kinds of relevant technical principles and follow all kinds of relevant technical standards and norms. In the design review, we should note that the network system must conform to the following principles.

(1) Advanced and practical. With the rapid development of computer technology, the cycle of equipment update and elimination is becoming shorter and shorter. In order to ensure the system has a long life cycle and protect the investment, in the system hardware and software configuration, comprehensive consideration of practical objectives, investment and international computer technology development trend, planning.

(2) Sustainable development and economy. Computer network technology is a rapidly developing field. The system construction must consider the expansion and change of the system in the future, so the scalability of the system must be maintained. The adoption of mature, stable, high performance-price ratio, strong expansion ability of the product, not only to avoid using too high performance configuration, resulting in the waste of resources and investment tension, but also to

DOI: 10.25236/sser.2019.233

prevent the lack of system processing capacity, expansion capacity is not enough to adapt to the needs of future development.

(3) Openness and scalability. Considering the needs of development, the operating system, network communication protocol and interface used should comply with international standards and the trend of technological development, so as to keep the system with strong interconnection ability, openness and scalability.

(4) Reliability and maintainability. The system must have high reliability and security. In the system design, we must consider these factors to establish a reliable and maintainable network system.

The Electronic Commerce Network Security Hidden Danger1

Stolen Information: because encryption measures are not adopted. The data information is transmitted in clear text over the network. An intruder can intercept messages as they pass through a gateway or router. Through repeated stealing and analysis, the rules and format of the information can be found, and then the content of the transmitted information can be obtained. Cause online transmission of information leaks

Tampering The Information. When an intruder mastered the format and pattern of the information, and they modify data transmitted over a network before sending it to a destination through various technical means and methods. This approach is not new. You can do this on a router or gateway.

Due to mastering the format of data and being able to tamper with the passed information, an attacker can pretend to be a legitimate user to send fake information or take the initiative to obtain information, which is usually difficult for remote users to distinguish.

Malicious Damage: because the attacker can access the network. It is possible to modify the information in the network. Get confidential information online. You can even sneak inside the network. The consequences are very serious.

Network Security Technology Applied In E-commerce Transactions

To improve the security of e-commerce, a variety of network security technologies and protocols can be used. These technologies and protocols have their own scope of use and can provide varying degrees of security for e-commerce transactions.

Firewall Technology. Firewall is the main network security equipment at present. Firewall usually USES the security control means mainly has the packet filter, the status detection, the proxy service because it has assumed the network boundary and the service, to the internal illegal access is difficult to control effectively. The isolation technology of the single network firewall, which is most suitable for the relatively independent network with limited access to the external network and relatively concentrated network services, determines its important role in e-commerce security transactions. At present, firewall products are mainly divided into two categories: proxy service based and state detection based.

Firewall also has its inherent shortcomings.

(1) The firewall cannot prevent the attack by the firewall. For example, unlimited outgoing dialing from within a protected network is allowed. Some users can form a direct connection to the Interne'. Thus bypass the firewall: create a potential backdoor attack channel, so should ensure the uniqueness of the channel between the Intranet and the extranet.

(2) Firewall cannot prevent the transmission of infected software or files. This can only be done by installing real-time anti-virus monitoring software on each host.

Data Encryption Technique. Firewall technology is a passive defense technology. It is difficult to effectively defend the unsafe factors in e-commerce activities. Modern cryptography should help. Encryption technology is the main security measure adopted in e-commerce, which can be used by traders in the stage of information exchange as required. At present, encryption falls into two categories. Namely symmetric encryption/symmetric key encryption/private key encryption and asymmetric encryption/public key encryption. Many institutions now use the abbreviation PKI. The implementation of public key system technology constructs a complete encryption/signature system. More effectively solve these problems. The keys are split into a pair (that is, a public or encryption key and a private or decryption key). Any of these pairs of keys can be exposed to others in an unclassified manner as a public key (encryption key). Public key used to protect against secret? The private key is used to decrypt the encryption information. The private key can only be held by the trader that generated the key pair. Public keys can be widely distributed. But it only corresponds to the trader used to generate the key. Trade party of confidential information by using the scheme, is the basic process of trade exchange party A generated a pair of keys and will be one of those as a public key to other trading parties publicly: get the public key trade party b use the key to the confidential information is encrypted and then sent to the trade party A again save yourself with another pair of private key to decrypt the encrypted information. Party a may only use its private key to decrypt any information encrypted by its public key.

Identity Authentication Technology. Identity authentication is also known as authentication or confirmation. It is a process to verify whether the authenticated object conforms to or is valid by verifying the authenticity and validity of one or more parameters of the authenticated object, which is used to ensure the authenticity of data. Prevent attackers from impersonating tampering, etc. The identification of human physiological characteristic parameter f (such as fingerprint identification and iris identification) is highly secure. However, it is difficult and costly to implement. At present, the parameters used in computer communication are password, identifier key, random number and so on. And the public key cryptosystem (PKI) authentication technology based on certificates is generally used. To realize the identity authentication based on public key cryptography algorithm. A trust and trust verification mechanism must be established. Each entity on the network must have a digital identity that can be verified. This is called a digital certificate. Digital certificate is the identity certificate of each entity in the online information exchange and business transactions. Has uniqueness. The certificate is based on the public key cryptosystem. It associates the user's public key with the user's own attributes, such as name, unit, and so on. This means that an authority trusted by all parties online should be responsible for verifying the identities of various entities and issuing and managing digital certificates, namely certificate authorities. The CA digitally signs all the user attributes, certificate attributes and the user's public key with its own private key to generate the user's digital certificate. In secure communication based on certificates. A certificate is a credential to prove the user's legal identity and provide the user's legal public key. Therefore, the main function of certificate management facility CA, as a network trusted institution, is to manage and maintain the certificates issued by it, and provide various certificate services, including issuing, updating, recycling and archiving of certificates.

Digital Signature Technology. Digital signature also known as electronic signature has important applications in information security including identity authentication, data integrity, non-repudiation and anonymity. Digital signature is a combination of asymmetric encryption and digital digest. Its main way is: a message from the text message sender generates a 1 28 b the hash value of it (or message digest), with its own private key for the hash value is encrypted form the sender's digital signature, and then the digital signature will be as the attachment of a message with message is sent to the receiver of a message messages receiver firstly calculated from the original message received 1 28 bit a hash value (or message digest). The sender's public key is then used to decrypt the digital signature attached to the message. If the two hashes are the same, the receiver can confirm that the digital signature is from the sender. The original message can be authenticated and non-repudiated by digital signature.

Summary

E-commerce security puts forward double requirements for computer network security and business security. It is more complex than most computer networks. In the process of the construction of electronic commerce involves many safety technology issues to formulate safety technology rules and implement safety technology means can not only promote the development of safety technology, but also promote the formation of safe electronic commerce system. Of course, no one security technology will ever provide permanent and absolute security, because the network is changing. The application is changing, so the means of invasion and destruction are also changing, and only the continuous progress of technology is the real security guarantee.

References

[1] Tianshu Xu. Research on Internet finance model under e-commerce platform [J]. China market,2019(07):185-186.

[2] Chaojie Wang, Ran Mang, Ran Li. Application of artificial intelligence in computer network technology in the era of big data [J]. Shandong industrial technology, 2019(06):146.

[3] Yue Yu, Yating Wang. Computer network technology application in the enterprise intelligent management [J/OL]. Electronic technology and software engineering, 2019 (04): 9 [2019-03-13]. HTTP: / / http://kns.cnki.net/kcms/detail/10.1108.TP.20190304.1522.020.html.

[4] Ning Ni, Yan Li, Wenjun Zhou. The computer network security problems and solutions [J/OL]. Electronic technology and software engineering, 2019 (4): 195 [2019-03-13]. http://kns.cnki.net/kcms/detail/10.1108.TP.20190304.1523.280.html.

[5] Na Lian. The application of firewall technology in computer network security [J/OL]. Electronic technology and software engineering, 2019 (4): 197 [2019-03-13]. http://kns.cnki.net/kcms/detail/10.1108.TP.20190304.1523.284.html.

[6] Hongzhi Zeng. Artificial intelligence era of big data in the application of computer network technology [J/OL]. Electronic technology and software engineering, 2019 (4) : 235 [2019-03-13]. http://kns.cnki.net/kcms/detail/10.1108.TP.20190304.1523.350.html.

[7] Yu Zhang. Computer information security and reasonable maintenance in network environment [J]. China management informatization,2019,22(05):158-159.

[8] Hongfei Ma. Application of computer network technology in electronic information engineering [J]. Electronic testing,2019(Z1):157-158.

[9] Lijin Chen. The influence of e-commerce on the current international economic and trade research [J/OL]. Brand research, 2018 (S2): 66 + 75 [2019-03-13]. https://doi.org/10.19373/j.cnki.14-1384/f.2018.s2.042.

[10] Bin Xiang. On the optimization of computer network database security management technology [J]. Shandong industrial technology,2019(05):173.