Application of Computer Network Security Information Encryption Technology

Dan Wang¹*, Huichuan Liu¹

¹Shandong Labor Vocational and Technical College, China

*Corresponding author e-mail: wangdan@sdlvtc.cn

Abstract. With the continuous development of information technology, computers have been widely used in various fields of society, filled with rich information in the network, network security has been widely concerned. In view of the problem of insufficient network security, we must strengthen the application of security measures, among which information encryption technology is one of the important means to ensure network information security at the present stage. This paper mainly summarizes the information encryption technology, analyzes the factors affecting network security, and puts forward effective protective measures to ensure the security of computer network.

Keywords: Computer Network Security, Information Encryption Technology, Application

1. Introduction

Computer network security includes a lot of content, such as hardware, software, resources and other security. Therefore, to ensure the security of computer network is to ensure the security of computer hardware, software, resources and so on, to avoid its destruction or leakage, and to have a certain impact on the operation of computer network system. In view of this situation, we must take effective preventive measures and techniques to ensure the security of information and ensure the orderly progress of related work.

2. Overview of information encryption technology

Information encryption technology is a technology that uses mathematics and information technology to protect electronic information in the process of transmission and storage to prevent leakage. With the popularization of computer technology and Internet technology, the problem of information security has been paid much attention to. It is necessary to use information encryption technology to improve the security of computer network. Its technical model is divided into data encryption model and two cryptographic systems [1].

The general data encryption model can be described as: when the sender sends out the plaintext information, the encryption key is set by the encryption algorithm to convert the information into ciphertext. The encrypted information is transformed into plaintext by the decryption key set by the decryption algorithm, and the plaintext information is transmitted to the information receiver. In the
process of transferring information into ciphertext, foreign intruders may attack and tamper with ciphertext, which may lead to the disorder of information and the problem of information transmitted to the receiver. The encryption key and the decryption key in the process of information transmission can be the same or different [2-3]. The decryption algorithm and the encryption algorithm are inverse operations each other. In the process, if not in accordance with the pre-arranged key generally can not solve the plaintext. But at present, almost all the applicable cryptographic systems are breakable, that is, ciphertext is not absolutely safe. In order to ensure the security of ciphertext, it is necessary to develop an unbreakable cryptographic system.

At present, the widely used cryptosystem can be divided into two types, one is symmetric key cryptosystem, the other is public key cryptosystem. The computer encryption operation model is shown in figure 1.

![Figure 1. Computer encryption model.](image)

### 2.1. Storage encryption technology

When storing information data, it is very easy to leak data and information, so in computer network, the most concerned is ciphertext storage and access control. Cryptographic storage refers to the use of encryption module, additional password encryption, encryption algorithm conversion and other encryption technology: access control refers to an effective control of user rights, through relevant means to determine the legitimacy of users, and then limit their use rights, to ensure the security of network operation.

### 2.2. Network information recognition and encryption technology

In the Internet, most of the information can be shared in the network. To some extent, it provides a chance for some lawbreakers to share information through information sharing, forgery and counterfeiting. Network information confirmation encryption technology is a technology that defines the scope of network information sharing and avoids illegal tampering and forgery of information. In a security information confirmation scheme, the legitimate receiver can confirm the authenticity of the information they receive; others can not tamper with the network shared information; when the network information data is in dispute, it can be arbitrated by a third party. The receiver can decrypt the information through the common key to avoid some network insecurity.

### 2.3. Network transmission encryption technology

The main function of transmission encryption technology is to achieve the encryption of information data transmission [4]. At present, the application of transmission encryption technology includes end-end encryption and line encryption. End end encryption refers to the automatic encryption by the sender at the automatically encrypt, when transmitting data, can enter the TCP/IP packet through the data, after the data reaches the client, the client decrypts the corresponding information. Line encryption refers to the expansion of line encryption for different encryption keys without considering the security protection of information.

### 2.4. Network key management encryption technology

Key encryption technology is an effective encryption technology to ensure network security management at this stage. Its biggest advantage is to ensure the use of data information. In the application of this encryption technology, we must note the security of key generation, distribution,
preservation and destruction. In the application of this technology, the media used to achieve magnetic card, semiconductor storage, disk and so on. The schematic is as follows:

![Figure 2. Schematic illustration of the principle of key encryption.](image)

3. Factors affecting computer network security

3.1. Computer virus
Computer virus refers to a program that can be inserted into computer programming, damage computer functions, cause data loss, and fail to use the juicer normally. And this program code or instruction can be copied by itself. The characteristics of computer virus mainly include: latent, infectious, hidden, destructive and so on. At present, the sap computer virus has become an important factor affecting the computer network security, and the degree of computer damage is becoming more and more serious, so we must pay more and more attention to it.

3.2. Computer operating system vulnerabilities
At this stage, when designing a computer operating system, there will be some loopholes. With the gradual application of customers, these vulnerabilities will gradually become prominent, and suppliers will find these problems in time, and then according to the actual situation [5]. Check and repair accordingly. But. Some system vulnerabilities and found by hackers will threaten the network security of computers, they will compile some programs, steal some important information or personal privacy in the computer, and even seriously lead to the paralysis of the juicer.

4. The Role of Information encryption technology on the evaluation index of computer network security

4.1. Role of confidentiality
Both symmetric key cryptography and public key cryptography promote confidentiality. If there is no encryption algorithm to encrypt plain text data, Then the information and its content can be easily read by the intruder after obtaining the information in the process of propagation, thus the confidentiality of the information is lost. The encryption process and decryption process of symmetric key cryptography are the same key and algorithm. The intruder can easily encrypt the stolen ciphertext, so that the ciphertext can be deciphered. Compared with public key cryptosystem, symmetric key cryptosystem has less effect on confidentiality.
4.2. Role of endpoint discrimination

For some network fraud caused by unknown customer identity at both ends of the endpoint, we can adopt end-to-end encryption algorithm. The data of end-to-end encryption algorithm is encrypted and decrypted only at the endpoint, that is, only between the sender and the receiver, but not in the transmission process. This enables only the sender and receiver to encrypt and decrypt the information in the transmission, and the intruder in the process of information transmission can not obtain the encrypted information. This greatly improves the identification of sender and receiver at both ends of the endpoint and reduces the possibility of criminals impersonating one of them [6].

5. Protective measures for computer network security

5.1. Strengthening the construction of computer network security management system

In the process of improving computer network security, we should strengthen the construction of security management system, and then supervise the contents and aspects of computer network security to realize the security of computer network operation. In the construction of computer network security management system, we must strengthen the formulation of risk assessment mechanism, set up security management framework, establish security management technology platform, and ensure the overall implementation of security management measures.

5.2. Enhanced access control

In the process of computer network operation, we must strengthen the control of access rights, ensure the security of network resources, there will be no illegal use and access, access rights are the important content to ensure network security. To ensure the reliability and security of computer network operation by setting access rights and specifying user rights.

6. Conclusion

Using encryption technology to encrypt communication messages in computer network transmission can well meet the needs of encrypted communication and ensure that information is not illegally stolen by hackers or third parties. In a word, it is necessary for people to pay attention to network security when they use the network to work and study. In the study of computer network security, we must analyze the factors that affect its security, so that we can improve it pertinently, put forward the corresponding prevention and solution measures their own network security. At the same time, information encryption technology is also a very important preventive measure, which effectively ensures the security and reliability of computer network operation.

References

[1] Li Xiaoli. The application of data encryption technology in computer network security. Digital Technology and Applications, 2011(06)
[2] Liu Qiaojia. Application of Information Encryption Technology in Computer Network Security. Computer Optical Disc Software and Application, 2012(16)
[3] Research on the Application Value of Zhu Wenya Data Encryption Technology in Computer Network Security, Tian Manufacturing Automation, 2012(03)
[4] Pan Fang's research on modern information encryption technology based on information security. Information security and technology, 2011(02).
[5] Application of Tian Ruixia and Wang Feng Data Encryption Technology in Computer Networks. Information Security and Technology, 2014(02)
[6] Wang Jiayu. Research field on the application of information encryption technology in computer network security. Computer CD-ROM Software and Applications, 2012(09)