Application of Computer Information Encryption Technology in Network Security

Aikebaier Jiang.aimait

College of Information Science and Engineering, Xinjiang University Urumchi, Xinjiang, 830046

Keywords: Encryption technology; network security; data information

Abstract: With the continuous development and innovation of science and technology, the computer information encryption technology has also developed effectively. With the development of socialization, network undertakes increasingly larger workload of data information management, and the computer information encryption technology appears to be particularly important. This paper simply introduces the computer information encryption technology mainly from the perspective of the factors influencing network security, discusses the application of different information encryption technologies, and provides reference for researches on the computer information encryption technology in China through effective analysis from different angles.

1. Introduction

With the development of communication technology and computer network technology, the computer technology and network technology have been increasingly more widely applied, but also has brought some challenges to network security guarantee. Therefore, it is necessary to strengthen researches on the computer information encryption technology, and improve the computer network information security coefficient, so as to convoy services for users.

2. Analysis on the factors influencing network security

First of all, many factors lead to network security issues. For example, a hacker uses monitoring, surveillance or the like to have access to the computer system user name, password and IP packet of a target user, and enters the computer system in the name of the user, so as to steal network data of the trusted host server, tamper with and steal the IP address, or the like. Secondly, the computer system writing and actual operation by maintenance personnel would inevitably lead to system loopholes and defects. Most hackers have high computer technologies, and find loopholes or defects that may be present in the system through professional technology and knowledge, so as to intrude into the computer system, illegally have access to network data of target users, and damage the network security. Moreover, computer network virus is also one of the factors that affect the network security. Characterized by rapid spread, easy infection, wide distribution, etc., a computer virus affects the computer system security, or even seriously leads to paralysis of the entire computer system, and is usually spread with a computer program as a carrier. Once a user shares or activates a file or a data packet carried with a computer virus, the system will be infected with the virus, whilst accelerating the virus infection and spread, and affecting the network security in a chain-type spreading manner.

3. Overview of computer information encryption technology

Information encryption technology is one of the important technologies guaranteeing the network security, and is mainly based on the cryptographic science and technology and cryptography, so as to implement encryption processing of data information in the network system, and convert data in the computer to encrypted information using function displacement and replacement, encryption keys, etc. After acquiring encrypted data information, the recipient restores data information using decryption functions or decryption keys, so as to ensure the network data

information security. In accordance with the encryption algorithm, encryption technology can be divided into symmetric encryption technology and asymmetric encryption technology, where the symmetric encryption technology means that during data information transmission, the sender encrypts the data information and the recipient decrypts the data information using the same set of secret keys. In the implementation process, the sender and the recipient will preset and properly manage secret keys of information, thereby ensuring the confidentiality, integrity and security of data transmission. The asymmetric encryption technology has different secret keys, so that data information, when being sent, is encrypted using encryption algorithm, while the data information recipient will encrypt the data using another set of encryption algorithm, i.e., information is encrypted and decrypted using different secret keys. With this method, it is not necessary to exchange secret keys of data information between both sides in the transmission, thereby improving the security and privacy of data information. Encrypted storage technology very easily leads to information leak in the process of implementation of data information storage. For this situation, security guarantee will be implemented using encrypted access control and ciphertext storage, where access control will control users' permissions to use the Internet using a relevant program to prevent illegal users' from unauthorized access to stored information. Ciphertext storage means to encrypt stored information using additional password encryption, algorithm conversion encryption and module encryption. Finally, information confirmation encryption technology: one of the main functions of the computer network is information sharing. In the process of data information sharing, people with ulterior motives will have opportunities for stealing information, will tamper with and counterfeit information. With the information confirmation encryption technology, the scope of information sharing can be defined, so as to exclude people with ulterior motives.

4. Application of computer encryption technology in network security

Transmission encryption technology mainly involves two technologies: line encryption technology and end-to-end encryption, both of which are able to provide security guarantee for data information, where line encryption means to implement encryption of the data information transmission lines using encryption keys, and does not need information security on both sides in the data transmission during the technology implementation. End-to-end encryption means that the data sender implements encryption of information, so as to convert information into information data packet in the form of TCP/IP, which cannot be identified and read by others. The recipient acquires the data information, and then decrypts and recombines the information, thus converting unidentifiable and unreadable information into identifiable and readable data information. Storage encryption technology also involves two technologies: access control technology and ciphertext storage technology, where the first technology guarantees the data information security mainly through the encryption module, additional password encryption and encryption algorithm conversion, and the second technology restricts and reviews users' qualification and permissions, so as to prevent people with ulterior motives from unauthorized access to stored data information.

In the process of implementing network security guarantee, secret key technology is very widely used, and can effectively improve the validity, convenience and security of data information. First of all, the secret key plays a role in encryption using the carriers such as, semiconductor memory, disk, magnetic card and magnetic tape, and involves the generation, distribution, storage, change and destruction of the secret key. Functions of the network confirmation encryption technology mainly include limiting the data information sharing scope. The information confirmation scheme mainly includes the following parts: first of all, it is necessary to guarantee that the recipient quickly identifies the received information; secondly, it is necessary to exclude users except the sender to avoid the phenomenon of tampering with information; and finally, a dispute, if arising, can be treated by a third person in accordance with the relevant standards. Moreover, the information confirmation system mainly involves three aspects as follows: firstly, confirm the information security, confirm the user identity and confirm data signature, where the digital signature mainly refers to the mathematical relationship conversion between open secret keys and private secret keys, the digital signer shall confirm the identity of the information sender, the process first needs to

encrypt information data, and then selects a secret key as the secret key of information data encryption for decryption. Moreover, the data information sender can encrypt data information, and then pass the encrypted data information on to the recipient. After acquiring the data information, the recipient encrypts the secret key using the secret key provided by the sender, thus safely obtaining data information.

Firstly, in the application process of the symmetric encryption technology, it is first necessary to acquire the ciphertext using the encryption algorithm, and then send the ciphertext to the data information recipient. When the data information reaches the recipient, the recipient decrypts the data information using the ciphertext, so as to implement effective browsing and processing. In the process of implementation, the technology has the advantages of difficult decoding, simpleness, convenience and the like, but fails to confirm the identity of both sides in the data transmission in the process of implementing the data transmission. Secondly, the asymmetric encryption technology is mainly used in the aspects of identity authentication and data signature, decrypted and encrypted keys will be implemented in different ways, i.e., requesting the secret keys to appear in pairs, so as to implement effective encryption. Firstly, the open secret key may be any one of the two secret keys, and the other one is the decryption key. Therefore, the open secret key can be released, but for special encryption information, information can only be acquired using special decryption keys. In the process of identity authentication, the information recipient will provide the open secret key to the sender, and then the sender encrypts it. When data information is transmitted to the recipient, the recipient decrypts the information using ciphertext, and the secret key for decryption is the secret key stored by him. The technology can be used to effectively improve the network security.

5. Conclusion

In conclusion, in the new era, with the constant innovation and development of science and technology, computer network technology has been widely used, and importance has been attached to network security issues. In order to effectively guarantee computer information security, it is necessary to effectively improve encryption technologies, achieve the purpose of security guarantee through different information encryption technologies, not only ensure data information security, but also can promote flexible use of data information by users, deeply probe into new encryption technologies, and provide effective guarantee for the security of users' computer databases.

References

[1] Zhao Ling. On Application Value of Data Encryption Technology in Computer Network Security [J]. *Digital User*, 2017 (12).

[2] Jin Chao. Analysis on Application Value of Data Encryption Technology in Computer Network Security [J]. *Network Security Technology & Application*, 2017 (5): 48-49.

[3] Huang Ying. On Application Value of Data Encryption Technology in Computer Network Security [J]. *Network Security Technology & Application*, 2017 (8): 56.

[4] Xu Peng. Analysis on Application of Data Encryption Technology in Computer Network Security [J]. *Network Security Technology & Application*, 2017 (7): 53.