The Application of Data Encryption Technology Based on Network Security Maintenance in Computer Network Security

Na Zhang
Shandong Vocational College of Light Industry, Zibo 255000, China
*Corresponding author: ziyu2008_x@163.com

Abstract: The rapid development of computer technology and the extensive coverage of computer network have promoted the rise of Chinese computer industry in the 21st century. But while computer technology benefits mankind, it also carries great potential risks. For example, the loss or damage of key data, the disclosure or abuse of personal privacy, has undoubtedly brought serious losses to human society. Therefore, it is necessary to develop and make good use of data encryption technology, and to increase the defense line for computer network security, so as to maintain computer network security and reduce the possibility of information being tampered with or stolen. Based on the current situation of computer network security and the necessity of strengthening computer network security, this paper analyzes the factors affecting computer network security, points out the classification and value of data encryption technology, thus provides a scientific theoretical basis for the application of data encryption technology in computer network security.

Keywords: Network security maintenance, data encryption technology, computer network security, applied research.

Introduction

With the increasing maturity of mobile communication technology, the dependence of electronic computers on the network is more and more prominent, and the gradual expansion of computer use has caused users to pay close attention to the computer network security issues, but also prompted users to pay more attention to the enterprise network information security management capabilities. On the basis of data encryption technology, users can use cryptography knowledge to adopt effective data encryption methods to ensure the relative security of the computer operating environment on the premise of rapidly distinguishing information, so as to realize the continuous optimization of the computer network system. By analyzing the present situation of computer network
security, this paper points out the necessity of strengthening computer network security, in order to make the data encryption technology to achieve the maximum value of its own full play in the process of maintaining computer network security.

**Current situation of computer network security and the necessity of strengthening computer network security**

At present, computer network security has aroused widespread concern in the community. In the process of using networked computers, users often face the risk of key data and classified materials being stolen. Computer network system is vulnerable to damage in the shared environment, which undoubtedly poses a great threat to users’ life security and property security. And repairing computer network vulnerability has become the focus of network security technology research.

Data transmission and resource sharing, distributed processing, information centralization and load balancing are the basis of computer network to maintain normal operation. When these functions appear vulnerability, the operation of the computer network will inevitably encounter a variety of problems. In addition, various software and hardware are also important components of the computer network fabric. When the data information in these aspects is tampered with or destroyed, it will also pose a threat to the computer network security.

Active attack and passive attack are two main methods used by computer hackers to attack computer network systems. Among them, the hacker by affecting the computer system operation or changing the system resources to achieve the purpose of the attack is an active attack; however, under the premise of not affecting the system resources, computer hackers attempting to obtain the information of the communication system is passive attack. In addition, a variety of viruses also pose a threat to computer network security. Computer viruses are not only various, but also extremely complex in structure. Some mutated viruses can even infect the core files of a computer. Because computer viruses are essentially malicious code embedded in computer programs, they can corrupt computer data.

The security of computer network is the premise to promote the rapid development of computer network. Secure computer network can provide users with reliable information guarantee, and promote the routine operation of computer network system, as well as the efficient play of the convenient role in computer network, so as to promote the better and faster development of economy and society [1].

**Analysis of factors affecting computer network security**

In order to ensure the safe operation of the computer system, it is necessary to analyze the factors that affect the computer network security. At present, the main factors affecting computer network security are:

First, network viruses. A network virus that lurks in a user’s computer not only spreads very quickly, but can also wreak havoc on the computer. The
network virus, which is made by people but not generated by themselves, has strong replication power, repair power and destructive power, and will have a profound impact on users’ computers. Common network viruses are Trojans and Worms [2]. These two viruses have different forms of action from other network viruses, and their attack methods will be adjusted accordingly for differentiated users. For example, when a worm enters a computer, it will usually delete the original files in the computer system, destroy the computer data, and make the computer completely paralyzed and unable to continue normal use.

Second, run the program. The computer running program having problem is the network security important factor influencing computer operating system. Paying attention to and ensuring the security of the computer running program, regular maintenance and upgrading of the program not only promote the computer to realize the power source of gradual optimization, but also ensure the basis of computer network security.

Third, hacking. Hackers are the main culprits affecting computer network security. In the actual computer use and network operation, hackers will take advantage of the system vulnerabilities and deficiencies, and strongly attack and destruct data information. In order to maintain computer network security, computer technicians must spend a lot of time and energy to prevent hacker attacks for a long time. Usually, hackers will sneak into the user’s computer in a certain attack way and obtain the key data information of the system by means of accurate analysis and calculation. Then, based on the research and judgment of the calculation results, they will take a definite attack behavior.

Data security encryption technology

With the help of encryption algorithm and secret key, the plaintext is converted into ciphertext at the sending end, and then transmitted to the receiving end. And then through decryption algorithm and secret key, the ciphertext restoring to plaintext technology at the receiving end is data security encryption technology. As a reliable means to protect information in the current computer system, data security encryption technology can encrypt information and secretly carry out information transmission, which can make the information security obtain basic guarantee.

Encryption and hiding are two main means of data security technology. Among them, the useful information is encrypted, and information is transmitted in the form of the statement. With password recovery technology, encrypted information always appears as the code through the transmission of noise at the receiving end to initial information. The information content of the attacker cannot have attack behavior, so as to ensure the security of information transmission. However, the information encryption technology is easy to arouse the attacker’s interest in decoding the information while hiding the information content. In order to avoid the emergence of this situation, new information security technology was born, it will transmit the useful information and other information, not easy to
cause the attacker’s attention, so it can achieve the protection of information and communication process.
In general, the increasingly prominent computer network information security problems enhance the user’s attention to information security technology. In order to enable users to fully enjoy the convenience of the computer network, it will improve the security of the computer network system to ensure the process of information transmission from attack, and increase the research and development of the information security technology application [3].

**Classification of data encryption technology**

As the most basic network security technology, data encryption technology mainly includes five main types of technology: node encryption technology, link encryption technology, end-to-end encryption technology, symmetric encryption technology and asymmetric encryption technology.

1. **Node encryption technology.** This kind of data encryption technology mainly relies on the communication link to ensure the security of data information. This technology needs to encrypt all transmitted data, and the transparent state of users in the process of data encryption makes the intermediate nodes of the network to use different keys to encrypt the information on the basis of decryption, so as to ensure that the transmitted information at the network nodes can be presented in ciphertext form. This makes node encryption, which is similar to link encryption, more secure in protecting network data. On the basis of decryption, different keys are used to encrypt the information, which is the significant difference between node encryption and link encryption.

2. **Link encryption technology.** The encryption of a communication link between two network nodes can effectively protect the data transmitted over the network. All information before transmission is encrypted. The received information is decrypted at the node, and then the corresponding link key is used to encrypt the information, and then the data information is transmitted. Due to the application of link encryption technology, data information needs to be transmitted through multiple communication links, which undoubtedly greatly improves the security of information transmission process.

3. **End-to-end encryption technology.** This data encryption technique allows data to appear entirely in ciphertext during transmission from the sender to the receiver. Compared with node encryption and link encryption, end-to-end encryption is more reliable and easier to implement, design and maintain. In the application of end-to-end encryption technology, the transmission mode of messages passing through network nodes must be determined with the help of the destination address. Therefore, end-to-end encryption technology cannot encrypt the destination address of information. In other words, end-to-end encryption cannot obscure the source and destination of a transmitted message. Therefore, this encryption technology can’t effectively prevent attackers from entering the data
transmission process.

(4) Symmetric encryption technology. The technique of encrypting and decrypting data with the same key is symmetric encryption, also known as "key encryption". Encryption algorithm and key management are important factors that affect the security of symmetric encryption. Because data encryption and decryption need to use the same key, this makes the key security transmission is particularly critical. As the most widely used data encryption method in computer network security, symmetric encryption technology mainly includes AES, IDEA and DES three common encryption algorithms. Among them, the commonly used DES algorithm in daily work and life is often used to encrypt binary data. In general, symmetric encryption technology has a wide range of applications, good application effect, and has a significant advantage in terms of encryption speed [4].

(5) Asymmetric encryption technology. In contrast to symmetric encryption, asymmetric encryption requires a combination of public and private keys for encrypting and decrypting data. If the data is encrypted using a public key, the data must be decrypted using the corresponding private key. If data is encrypted using a private key, the data must be decrypted using the corresponding public key [5]. Asymmetric encryption is more secure than symmetric encryption because two different keys are needed for data encryption and decryption. Since both parties of symmetric encryption technology use the same key, the disclosure of the key by either party may cause the data information in the transmission process to be cracked. Asymmetric encryption technology uses two keys to encrypt and decrypt data. The public key is known to the public, while the private key needs to be kept by itself, which makes the process of data encryption and decryption time-consuming. Therefore, symmetric encryption technology is more efficient in the case of large amount of data.

**Value of data encryption technology**

The continuous innovation of data encryption technology plays more and more value, effectively improve the security of network data transmission. In general, the value of data encryption technology is mainly reflected in the following two aspects:

First, the promotion of security level. The construction of computer network security system has not been concerned about and paid attention to in the security level of the problem. Data encryption technology greatly improves the security of data transmission, so that the core data information about the funds flow can be protected by the corresponding security level of the computer system. Therefore, the application of data encryption technology, not only can strictly monitor the transmission process of network data information, but also can enhance users’ trust in computer network security. Second, network security can be assessed. Data encryption technology can show the security level of network data in the process of information transmission and is an important indicator to evaluate network security. The security of data transmission is the basis of constructing computer network
security system. In order to ensure the timely and accurate data transmission, network security agencies must constantly update the data encryption technology, improve the level of data encryption technology through the use of various types of data encryption technology, so that the security and accuracy of data information transmission is fully guaranteed. The use of data encryption technology improves and optimize the quality of data transmission, and it has become the most important network security indicators.

**Application of data encryption technology in computer network security**

*Improvement of data encryption*

With the help of the corresponding cryptographic algorithm, transforming the plaintext data information into ciphertext data information plays the auxiliary role of the key and protects the transmission of data information, which is the fundamental point of data encryption. Node encryption, link encryption and end-to-end encryption are very common data encryption types. For example, when users conduct transactions in online banks, once data information leakage occurs, the encryption system will quickly take appropriate measures to ensure the safe transmission of computer network data.

*Application of packet encryption*

As the most common data encryption method, compression packet encryption mainly includes ZIP and RAR. On the basis of setting the password to decrypt and using the encrypted password to accurately obtain the relevant computer data information, this compression packet encryption method has been widely used in the network mail transportation. In addition, the application of compression packet encryption can also achieve effective compression of mail, release the disk space occupied by files, and improve the overall operation efficiency of the computer.

*Application of node encryption technology*

The gradual improvement and development of computer network promote the effective application of node encryption technology. It is the basic premise of encryption to ensure smooth synchronous or asynchronous lines for data transmission between nodes. In addition, the smooth implementation of data information transmission encryption work also requires that the network intermediate nodes must have the corresponding data information processing capacity. At the same time, node equipment must always maintain a completely synchronous state, and only in this way can prevent network hackers tampering and stealing data information.

*Application of link encryption technology*
The application of link encryption technology can encrypt the links of computer network nodes, ensure the security and reliability of network data information transmission, encrypt the data information before transmission, and choose different types of keys. After the network node decrypts the data information, then it encrypts the data information. Its characteristics lie in the complex encryption and decryption links, which can effectively and comprehensively ensure the security of network data transmission.

Application of end-to-end encryption technology

In the application of end-to-end encryption technology, in the transmission process of the encrypted data from the sending end to the receiving end, there is no need to go through the decryption procedures of each link, so the network data can be well protected. At the same time, the application of end-to-end encryption technology has become extremely popular because of its advantages such as low cost, convenient operation, continuous innovation and optimization in the use process, and the ability to fully meet the actual needs of users.

Conclusion

The application of data security encryption technology can ensure the information security of the computer network, promote the normal operation of the computer system, so as to better meet the work and life needs of computer users. Therefore, we must strengthen the research and development of data encryption technology, promote the continuous innovation of data encryption technology, and provide scientific theoretical basis for the maintenance and safety of computer network security.

References

encryption in cloud databases. Wireless Personal Communications, 4.