Application of Data Encryption Technology in Computer Network Security

Wei CHU
School of Computer Engineering, Bengbu University, Bengbu, Anhui 233000, China
Email: 1656601536@qq.com

Abstract: With the development of information technology, the problem of computer network security is becoming more and more prominent. Illegal invasion, information disclosure, virus impact and network vulnerability are all factors that affect computer network security. In order to effectively guarantee the integrity and confidentiality of data and information, people must pay attention to computer network security.

1. Introduction
With the continuous expansion of the field of network applications, it is becoming more and more important to ensure the confidentiality and security of information, which has attracted the attention of relevant departments. In this paper, the data encryption technology in computer network is briefly introduced, so that people have a certain understanding of the data encryption technology and network security.

2. Analysis of Factors Affecting Computer Network Security

2.1. Illegal invasion
The computer usually faces the threat of illegal invasion when carrying out network activities, which affects the confidentiality and integrity of data. As far as its main means are concerned, network hackers illegally obtain IP packets, data messages, passwords or user names from the computer network by means of monitoring, and then use these data to enter the computer network to illegally steal, tamper with or delete data information from the IP address on the computer as a computer user.

2.2. The network server information was leaked
The computer operating system, which must be compiled by professionals, still has defects. For network hackers, they themselves have very professional computer theory and advanced computer network operation skills. Therefore, they often use these defects in computer systems to carry out network attacks on computers, thus illegally obtaining some network information and seriously threatening the security of computer networks.

2.3. Computer virus influence
Computer viruses are various, widely distributed, highly contagious and covert, affecting other host devices in the computer network system to a certain extent, and even worse, threatening to paralyse the entire computer network system. Most computer viruses are stored in computer programs. If the virus cannot be cleaned or scanned in time, once the file containing the virus is opened, the virus will...
be activated or shared immediately, causing it to spread or infect other devices quickly, resulting in the effect of chain propagation, making important data vulnerable to lose and posing a serious threat to the security of the computer network.

2.4. Network defects
In general, when the computer operating system is running, it mostly supports multi-process or multi-user application at the same time, and the host of the computer network system also allows multiple users to be connected at the same time. When the system sends or receives data, all processes or users running at the same time may have to transmit data. Once there is a network defect in the computer, it is easy to be attacked by hackers, so the security of data and information is difficult to be effectively guaranteed. Therefore, relevant personnel must pay full attention to it.

3. Analysis of Computer Network Security

3.1. Security problems in computer network system
At present, most computer systems adopt windows series. There are some defects in such systems, which are easy to be attacked by hackers or viruses while people are surfing the Internet. If the computer system is attacked, it will be difficult for the computer to guarantee its normal operation, and the information of the corresponding computer users will be easily cracked by hackers and logged in indiscriminately, making the data information in the computer face the threat of all leakage, which will bring great security risks to the computer network system[1]. Therefore, it is extremely important to strengthen the application of encryption technology in computing system. After the software is attacked, it will also cause the information to be eavesdropped or damaged to a certain extent in the course of data information transmission. All of these may bring hidden dangers to the security of computer network system, which requires researchers to attach great importance to and formulate corresponding countermeasures for improvement.

3.2. Potential security risks in network operation
The stability of computer network security in use is hardly guaranteed. When data is transmitted in the network, it is easy to be attacked at multiple levels, causing data information to be damaged or lost. If the situation is serious, it may also paralyze the network system and seriously interfere with people's normal life. In the network transmission of data information, if you want to transmit correctly, you must rely on the signing of the communication protocol. However, the actual situation is that there are still many loopholes in the communication protocol signed in the network transmission, which will bring convenience to the spread of viruses or hacker attacks. Intruders usually use various illegal means to obtain customer information, which makes it difficult to ensure network security. Therefore, the security risks of data information in network transmission must be highly valued by relevant departments[2]. Although the current network security technology we have is difficult to completely prevent computer viruses or hackers from invading, we can still adopt certain data encryption methods to enhance the level of network security and keep user data confidential.

3.3. Potential security risks in the database management system
At present, the network database management system we use also has certain security risks, because the security of the computer system currently used will pose a certain threat to the database management, and such security risks must be paid full attention to and maintained in time. As far as the database management system is concerned, the data information stored in it is very rich. If it is stolen by network hackers, it may cause great security risks. In particular, the data of some important departments will have a great impact on economic development once they are leaked.
4. Analysis of Computer Encryption Technology

4.1. Overview of data encryption
As the core system of computer system security protection, data encryption needs to transform plaintext data information into ciphertext information with a key according to a pre-determined key algorithm. Data security is the main reason for key generation. There are many types of ciphertext, including node encryption, link encryption and end-to-end encryption. Especially in e-commerce or banking system, the application of data encryption is extremely important. For example, in the banking system, the data encryption technology is mainly manifested in the link management between network devices, which can facilitate the connection of devices and further ensure the interaction and contact between multiple network devices. When the switch and firewall are set up, encryption and continuous monitoring can be carried out on the way of data transmission to the system equipment, which can protect the data to be transmitted to a certain extent and make it more difficult for illegal users to steal the data[3]. For some important data, data can be protected by multiple encryption methods, which can improve the security performance of computer network and make it have more practical application value.

4.2. Introduction to data encryption technology
Computer network security includes network equipment security and network information security, and data encryption technology is an important measure to ensure data security. It mainly needs to encrypt the data information to be transmitted in the computer network to a certain extent according to the relevant knowledge of cryptography and the science and technology related to cryptography, so that the data information can be transmitted safely. In this process, technologies such as encryption key and function replacement are fully utilized to convert data information in the computer network into encrypted data, and then the receiver of the data information uses decryption key or decryption function to restore the encrypted data information into the original data message, which is conducive to improving the concealment and security of data transmission in the computer network system to a certain extent. Data encryption technology can be divided into symmetric encryption technology and asymmetric encryption technology. As far as asymmetric encryption technology is concerned, it needs to be applied to a variety of different keys, and the sender of the data message encrypts the original data message with an encryption algorithm. The receiver will use another set of secret decryption keys to decrypt the encrypted data message sent by the sender and then restore it to the original data message for use by the user[4]. In general, asymmetric encryption technology needs to use public key and private key. When decrypting data information, it is necessary to use a previously agreed private key protocol. In this way, the confidentiality and security of data information transmission and key management can be guaranteed in the process of computer users transmitting information. Symmetric encryption technology refers to a security measure in which the encryption key of a data message is the same as the decryption key when data information is transmitted in a computer network. This method can usually save data transmission time to a certain extent, but requires higher key management for both sides of data information sharing; otherwise it is difficult to ensure the security and integrity of data transmission.

5. Application of Data Encryption Technology in Computer Network Security

5.1. Application of Link Data Encryption Technology
In daily use, link data encryption technology mostly provides services for multi-section computer network systems, because it can scientifically divide the route of network data transmission and encrypt data information of different sections or transmission paths, as shown in fig. 4-1. As far as the data transmission of different road sections is concerned, different encryption algorithms are usually required, and the data information received by both sides of the data information transmission is presented in ciphertext form. In this way, once a network hacker obtains such information through
illegal means, it is also difficult to crack the data information, and its data information security ability is better. In addition, the application of link data encryption technology can also fill in the data information to be transmitted in time so that the length of data information in different sections or transmission paths can be changed, which is conducive to the difference of data information and affects the ability of network hackers to interfere with and judge data information.

5.2. Application of end-to-end data encryption technology
Generally speaking, the end-to-end data encryption technology can effectively simplify the encryption process of link data encryption technology, thus facilitating the use of data information by both sides of information transmission, as shown in Figure 4-2. End-to-end data encryption usually requires specialized ciphertext for data transfer. When it is used in computer network system, the requirement for data encryption or decryption is low. Only ciphertext needs to be transmitted, which is beneficial to fully guarantee the system information security of computer network. At the same time, when the end-to-end data encryption technology is used, its operation and maintenance investment is relatively small, and this encryption technology has an independent transmission path in the data transmission process, even if a data packet transmission error occurs in the transmission process, it will not interfere with the transmission of other data packets, thus improving the integrity and security of data transmission to a certain extent. In addition, once the end-to-end data encryption technology is applied in computer network collaboration, the IP address of the information receiver will be converted or revoked at any time, making it difficult for other network users to crack the data information, which to some extent can effectively reduce the probability of network hackers illegally stealing or tampering with the data and further improve the security of the data information in the computer network system.

5.3. Application of data signature authentication technology
As an important means of protecting data information, authentication technology can use the means of identifying and determining user identity information to prevent other illegal users from obtaining user information, thus effectively ensuring the data information security of computer networks. Digital signature authentication technology usually includes password authentication and data authentication. The password authentication method is generally relatively simple and convenient, and its use charge is low, so it has a wide application range. However, on the other hand, the requirement for password setting is high, and it needs to be changed in time so as to ensure the security of data information. The data authentication method needs to encrypt the data and continuously check the calculation method of
the key so as to improve the security and confidentiality of the data information in the computer network system to a certain extent.

5.4. Application of node data encryption technology

The node data encryption technology usually requires professionals to encrypt the route of data transmission to ensure the security of data information transmission in computer networks. Before transmitting the data information, it is necessary to encrypt the data information to a certain extent by using the node data encryption technology. In this way, it can be ensured that the data information is presented in the form of ciphertext on the way of transmission, thus avoiding the data information being recognized by network hackers on the way of transmission. This can effectively improve the confidentiality and security of data information, but the node data encryption technology still has many defects in the way of data transmission, which must be fully paid attention to by relevant personnel, which is beneficial to the security of computer networks. For example, in the technology of node data encryption, data information is usually required to be transmitted to both sides and encrypted in plain text. If the data information is disturbed by sudden changes in the external environment during transmission, it will be difficult to ensure the security of data information transmission.

5.5. Application of cryptographic key data technology

The cryptographic key data technology is almost the same as the asymmetric data encryption technology when encrypting data information in a computer network and has two forms of public key and private key. However, unlike asymmetric keys, public keys have higher security performance and need to encrypt data information before data transmission, so that data information can be effectively prevented from being eavesdropped during transmission. When people are using the private key, the data information requires the data transmission parties to use the same key to encrypt and decrypt the data information in advance[5]. At the same time, the private key is used to manage the data information during transmission so that the private key and the public key complement each other, which can effectively improve the security of the computer network system and ensure the confidentiality of data transmission.

6. Conclusion

With the development of information technology, computer network security technology has attracted more and more attention, because people's production and life are closely related to the practical use of the network. People are surfing the Internet every day. Network security is very important to people. If data information is stolen, it will bring great losses to people. Therefore, it is very important for computer network system to properly use encryption technology, which can protect network data and is extremely necessary for the sustainable development of computer industry.

References

[1] Shang W. Development and Trend Analysis of Computer Network Security in China[J].Electronic Technology and Software Engineering,2016,(1):196-197.
[2] Kang L Z. Current Situation and Development Trend of Network Security Technology[J].Network Security Technology and Application,2015,(4):176-179.
[3] Xin Y. Research and Implementation of Bus IC Card Asymmetric Key Management System[D]. Beijing Jiaotong University,2016.
[4] Xin L. Research on Technical Architecture of Big Data Security and Privacy Protection[J].Research on Information Security,2016,2(3):244-250.
[5] Pan Y. Research on Data Encryption Scheme Algorithms Supporting Homomorphic Arithmetic Operations[J].Journal of Communications,2015,36(1):167-178.