Research on Computer Network Security and Encryption Technology

Yanmei Huang

Jiangxi University of Engineering, Jiangxi, Xinyu, 338000, China

Keywords: Computer, Network Security, Encryption Technology

Abstract: Data encryption technology plays an active role in data storage, transmission and application security in computer networks. Therefore, optimizing the computer network security system requires targeted research from the application of data encryption technology. Under the premise of studying the influencing factors of computer network data security, this paper discusses the classification of data encryption technology and the application of data encryption technology in the network, hoping to provide reference for relevant personnel.

1. Introduction

With the rapid development and popularization of Internet technologies and mobile terminals, people's daily lives and all walks of life have been greatly affected and changed to adapt to the arrival of the Internet era. In the era of the Internet, data transmission has become more convenient. Especially in the case of cloud computing, artificial intelligence, big data, etc., data transmission and sharing have become more frequent, and the amount of data transmission has expanded dramatically. Moreover, people's daily life and work are increasingly dependent on computers, and the transmission of information and data in learning, work, entertainment, etc., depends on computer networks. As one of the components of computer network technology, network information security, if it has security flaws and loopholes, will inevitably make the computer network vulnerable to damage, which poses a huge threat to users' security [1]. In this context, the security of computer networks is closely related to people's vital interests, and has received extensive attention and attention. It has become an inevitable trend to develop computer network technology to ensure the security of computer networks. Data encryption technology plays a huge role in identity authentication and secure transmission of data and information, which can effectively guarantee people's privacy and the security of transmitted information and data. Therefore, research on data encryption technology for computer network security is strengthened. Therefore, it is very necessary and meaningful to improve the security of computer network. For this reason, this paper studies and discusses the data encryption technology of computer network security.

2. Overview of Data Encryption Technology

Data encryption technology refers to converting a message into a ciphertext that is meaningless and difficult to be read by converting the encryption key and the encryption function. The receiver of the information can restore the ciphertext to the decryption key and the decryption function. The original information, in the process of information transmission to provide security assurance, to prevent information leakage, etc., is the core technology of computer network security, can be called the cornerstone of network security technology [2]. Data encryption is used to encrypt data and information. Only encrypted data and information can be decrypted and retrieved from the specified user or network. In this process, the sender and receiver need to pass some special The information is used for encryption and decryption. This is the key. Different keys have different encryption algorithms. Generally speaking, there are two types of keys used in data encryption technology: one is a private key, and the private key is often called a single key or a symmetric key. The sender encrypts and receives the plaintext. The same key is used to decrypt the ciphertext, so before the data and information are transmitted, the two parties exchange the keys of each other, so

  DOI: 10.25236/eeems.2018.035

that when the information data is transmitted, the encryption is performed by using the own key, and the receiver receives the key. After the information can be decrypted with the other party's key, this method is not only easy to operate, but also has the characteristics of high security strength, high speed and small calculation amount. Although it is the oldest key, it is still widely used. The most important thing in the process of data and information transmission between the two parties is the management of the key. If the key is lost or is known to a third party other than the two parties, the ciphertext may be leaked, resulting in loss of both parties, especially When data and information are transmitted by multiple parties, the key to be kept is increased and complicated. The private key uses symmetric encryption technology, which is also the most commonly used technology in data encryption. The data encryption algorithms usually include IDEA, AES, and DSE. Taking DES as an example, it is an encryption algorithm that groups data into 64-bit data blocks, 8 of which are used as parity tests, and the remaining 56 bits are used as keys [3]. The second is the public key. The public key is usually called the asymmetric key. The difference is different from the private key. The key used in encryption and decryption is different, although the encryption key and the decryption key. There is a certain connection, but only one key can't easily derive another key. Generally, a public key has a common encryption key and multiple decryption keys. Because it uses two different keys, even if one key is leaked or disclosed, another key is kept safely and there is no information leakage, and it can still be used for encryption. The privacy of the public key is good, but anyone who has a public key can send messages and data, so it is difficult to identify the sender, so the sender will use a digital signature to indicate identity. The public key uses an asymmetric encryption technique, and uses an encryption algorithm such as RSA or elliptic curve to calculate the data or information to be transmitted using an encryption algorithm to obtain a value, which is used as a verification signature. Taking the RSA algorithm as an example, the algorithm can effectively resist all current known password attack methods and is the most widely used public key algorithm. Asymmetric encryption technology can be used not only in the encryption of data and information, but also in the field of digital signatures, digital certificates and other information [4].

3. Factors Affecting Data Security in Computer Networks

The data in the computer network is subject to physical damage, human (intentional or unintentional) damage, malicious code such as viruses, and its security is greatly threatened.

First, computer security technology is not fully applied in the network construction process, resulting in physical and logical security holes in the network platform. Second, because the computer network itself has an open feature, it brings more application and service experience to users, and it also means that all kinds of information on the network are exposed to leakage risks. Third, due to the large number of hackers, viruses, Trojans and various malicious codes on the network, information is at risk of being attacked, destroyed, and illegally stolen, resulting in serious threats to business data, user information, and personal privacy. And because the network has international characteristics, it means that the network attack is not only from the users of the local network, but also hackers from other countries on the Internet. Fourth, the operating system, communication protocols, and various application systems in the network cannot be absolutely secure technically, and the existing loopholes are easily exploited by illegal intruders such as hackers. Fifth, the freedom of the network is both an advantage of the network and an important factor in the security threat of the network. Because most networks have no technical constraints on the use of users, users are free to access the Internet, publish and obtain various types of information, which will result in security in the process of obtaining information.

In view of the fragile nature of data, computer networks need to adopt various technical means to ensure its confidentiality, integrity and availability when transmitting data. In computer networks, data encryption technology is one of the key reliable technologies to ensure data security.

4. Principles and Classification of Data Encryption Technology

Data encryption is the process of processing data information originally called "plain text" in a

way that makes it an unrecognizable code (called "ciphertext"). The receiver uses the correct key to restore the ciphertext to The original data, so as to achieve the purpose of the data is not illegally stolen, used, as shown in Figure 1. It can be seen from Fig. 1 that the plaintext can be converted into ciphertext by the encryption key and the encryption algorithm, and the ciphertext is transmitted, and the ciphertext to be transmitted is transmitted to the specified location, and then decrypted by using the decryption algorithm and the key. The initial plaintext content is finally obtained.

Data encryption technology can be divided into symmetric encryption, asymmetric encryption and hybrid encryption according to the key used in the encryption process. Symmetric encryption is to process the plaintext and the encryption key together by the encryption algorithm to make it into ciphertext transmission. The receiver uses the decryption key to reverse decrypt the ciphertext and restore it to plaintext. The encryption and decryption process uses the same key. This method has high efficiency, but the key is transmitted along with the encrypted information. In the transmission process, the security of the key needs to be ensured. Commonly, there are DES, IDEA, and 3DES algorithms. Asymmetric encryption uses two different keys, encrypting the information with a public key, and the recipient of the information decrypts the information using a private key. This cryptosystem is also known as a public key cryptosystem. In the asymmetric encryption mode, the private key is not transmitted with the ciphertext, which avoids the possibility of being stolen and intercepted during the key transmission process. Commonly, RSA, Elgamal, and ECC algorithms are available. Symmetric encryption technology has a fast encryption speed, and asymmetric encryption technology has relatively high security. Later, a hybrid encryption technique combining the two was used: firstly, the ciphertext was generated in plaintext using a symmetric encryption algorithm, then the private key was generated by an asymmetric encryption algorithm, and finally the ciphertext and the private key were mixedly transmitted.

5. Data Encryption Technology in Computer Network Security

From the data in computer networks, data encryption technology can be divided into storage-level encryption, transport-level encryption, and application-level encryption.

File-level storage encryption technology can encrypt files on the local computer and network storage NAS through the data leakage protection DLP mechanism. It automatically encrypts the data written to the storage medium at the operating system layer in combination with cryptography and file analysis technology. . Encrypted File System in Windows EFS provides file encryption based on a public key policy. In addition, professional commercial encryption software using IDEA, RSA, and AES algorithms can also provide efficient file-level encryption.

There are three main methods: operating system layer encryption, DBMS client encryption, and DBMS kernel layer encryption. Operating system layer encryption directly encrypts database files through the operating system. The DBMS client encryption method acts on the outer layer of the database system. The data is encrypted before the data is written into the database. The decryption process is performed before the retrieval. The encryption and decryption process is completed by the database encryption system. DBMS kernel layer encryption is implemented inside the database by modifying the DBMS kernel and encrypting and decrypting before being accessed by the operating system. From the perspective of encryption strength, it is divided into database level, table level, record level, field level and data item level ladder.

This type of encryption is implemented on a storage array, typically by implementing a static data encryption algorithm on the controller of the controller or disk enclosure. Media encryption technology encrypts the entire storage disk or virtual volume through a data encryption module or professional software on a storage device (disk, tape, removable storage media, etc.). The encryption module or encryption software protects the data on the storage medium from being leaked by physical theft by modifying or hiding the storage device type and model parameters. However, except for the storage device, all data is processed, transmitted, and stored in plain text. .

Data transmission encryption technology encrypts the transmitted data stream to prevent eavesdropping, leakage, tampering and destruction on the communication line. There are three main methods: link encryption, node encryption and end-to-end encryption [5].

The data is encrypted by the encryption device at the data link layer of the OSI, decrypted before the next node receives the data, and the information is decrypted and re-encrypted in each node until it reaches the receiver, and the information in the node exists in clear text. of.

Node encryption requires encryption and decryption of data, and every two nodes encrypt data with the same key. Node encryption is similar to link encryption. At the data link layer, the data is encrypted by the node's own security module, and the intermediate node decrypts and encrypts the data. The message is encrypted in the node except for the header and routing information. In node encryption, except that the sending node and the receiving node appear in plaintext, the intermediate node performs key conversion, that is, a cryptographic device connected to the node machine is used at the node, and the ciphertext is decrypted in the device. It is re-encrypted, and the plaintext does not pass through the node machine, which avoids vulnerable links at the link encryption node.

The end-to-end encryption technology acts on the application layer. The data is encrypted by the sender and decrypted by the receiver. All information except the header is transmitted in cipher text. This encryption method is less expensive and more reliable than link encryption and node encryption. End-to-end encryption means that the still data needs to be encrypted and then encrypted while the data is being transported until it finally reaches its destination. End-to-end encryption provides the highest level of data confidentiality if data is encrypted using well-known, trusted algorithms.

Application-level encryption is the integration of encryption technology into a specific application system. It is closely related to the application, and the confidential information is dynamically encrypted and decrypted by monitoring the entire running process of the application. Application-level encryption tightly integrates the access control of the key with the application itself, clarifying the access scope of authorized users and users, preventing unauthorized users from unauthorized access and authorizing users to access unauthorized.

In addition, a new security mechanism is to construct a sandbox, put sensitive information and data in a closed environment, and the processing results are fed back to the client through transparent encryption. Sandbox technology can effectively prevent applications from being attacked by malicious code such as hackers or Trojans.

6. Conclusion

Practice has proved that in computer network systems, data encryption technology is widely used, which has played a very good role in protecting computer network security. In the era of data informatization, the rapid development of e-commerce, government affairs, online transactions and some new industries is inseparable from the application of data encryption technology. However, data encryption is only a technical means of network security protection. There are still many shortcomings in the actual application process. The challenges faced by network security are becoming more and more serious, especially in the aspects of e-mail transmission and online transaction. Large, for the Internet with rapid development, in order to meet the more powerful, reliable and fast protection needs of computer network security, further innovation of encryption technology is an important issue to be solved urgently.

References

[1] Zhu Wenya. Research on Application Value of Data Encryption Technology in Computer Network Security [J]. Manufacturing Automation, 2012(6): 35-36.

[2] Yang Jiancai. Research on Application Information Encryption Technology in Computer Network Security [J]. Computer CD Software and Applications, 2012(3): 18-19.

[3] Wang Jiawei. Research on the Application of Information Encryption Technology in Computer Network Security [J]. Computer CD-ROM Software and Application, 2012(3): 22-23.

[4] Cui Wei. Application Information Encryption Technology in Computer Network Security [J]. Shanxi Electronic Technology, 2012(5): 66-67.

[5] Wu Sujuan. Application Research of Data Encryption Technology in Computer Network Security [J]. Computer Knowledge and Technology, 2014(36):8633-8634.