Research on Computer Network Security and Encryption Technology

Yanjun Wang[1, a]

[1] Nanyang Medical College, Nanyang, Henan, China, 473000

[a]email,

Keywords: Computer, Network Security, Encryption Technology

Abstract. With the development of global information technology and popularization of Internet, computer network security issues become the focus of attention. Data transmission on the network should ensure its confidentiality, the authenticity, integrity and non-repudiation. The only effective means of solving these problems is the use of modern cryptography. As the core technology of information security, encryption technology has got more and more people's attention. Application of cryptographic techniques as before, no longer confined to the military, political and diplomatic fields, its commercial value and social value began to be widely recognized.

Introduction

With the development of computer network technology, information technology has become a global trend in human development, computer network has been in the field of national defense, finance, telecommunications, securities, commercial and daily life has been a large number of applications, especially in the United States not long ago set up network warfare Command, proposed network-centric warfare ideology, which exudes a sense of the importance of network technology. However, due to the diversity of computer networks have links, uneven distribution of the terminal and network openness, connectivity and other features, resulting in the network vulnerable to hackers, crackers, malicious software and other hacking attacks. Therefore, online security and privacy of information is a critical issue.

The Current Situation of Computer Network Security

Computer network continues to reflect its unique advantages at the same time, due to the complexity of the network system of openness, sharing of resources, system, linking the diversity, the uneven distribution of the terminal, network agnostic and other border Cause [2], the computer network has also brought many problems, the most important issue is security. In highly open computer network environment, unauthorized access, impersonate legitimate users, destroy data integrity, interference system uptime, viruses and malicious attacks, wiretapping, and other safety issues arising cause great damage.

Our network security is also increasingly exposed many problems. Large-scale hacking and computer virus spread on the Internet incidents occur frequently, so that our many government departments, business and educational institutions, are subject to varying degrees of abuse, and some even caused a very bad social impact and major economic losses. Computer network security is to overcome these security issues, make use of computer networks more secure born and developed. Computer network security refers to the data network system hardware, software, and systems are protected from accidental or malicious reasons destruction, alteration, disclosure, system continuous, reliable and normal operation to prevent and control illegal harmful information dissemination, maintain network security, in essence, it is to maintain ethics, regulations and national interests.

The rapid development of computer networks, widely used today, computer network security is a critical issue for the protection of computer network security assets, gain an advantage in the competition to meet the regulatory requirements of so great importance on personal life, business contacts, economic activities, and even political and military aspects also have a lot of leverage.

The Overview of Encryption Technology

Encryption technology is the integrity, authenticity and reliability to ensure that the obtained data of electronic information, and the application of one or some mathematics, physics, electronic data storage and transmission of information in the process of protection and to prevent information leakage or tampering techniques. Information encrypted by the encryption system is to process the raw digital information (plaintext), in accordance with the encryption algorithm transforms the plaintext into digital information was completely different process.

With the computer network security is receiving increasing attention in order to protect the network security encryption technology also appears more important. Usually used in common computer network security encryption includes symmetric encryption and asymmetric encryption techniques.

Symmetric Encryption Technology. It is also called private key encryption technology, computer network security generally used in e-mail encryption, to ensure secure e-mail messaging. Its outstanding feature is that the information on the data encryption and decryption keys are the same, that the decryption key can be calculated from the encryption key, and vice versa. When the communication process to encrypt e-mail, e-mail sender first using an encryption algorithm (typically DES algorithm and IDEA algorithm) to encrypt the plaintext ciphertext, the ciphertext is then sent to the recipient via the network, the recipient receives the message after the ciphertext using the decryption algorithm to retrieve the original plain text, and ultimately makes the e-mail communication is completed. This encryption technology is simple and efficient, it is difficult to decipher, and it is more commonly used; however, there are also symmetric encryption technology can not verify the identity of the message sender and receiver sides simultaneously informed of key problems and other issues.

Asymmetric Encryption Technology. It is also known as public key encryption technology, refers to encrypt and decrypt the information using different keys of an encryption technology, computer network security in general is mainly used in digital signatures and authentication information exchange in the field. In an asymmetric encryption system, the key is decomposed into a pair (ie, public key and private key), which is the key in any one can be used as a public key (encryption key), by way of the non-confidential others open, and the other to be preserved [2] as a private key (decryption key). In the use of asymmetric encryption technology to network communications between the two sides authentication, the sender often use the public key to encrypt the plaintext addressee (usually with the National Bureau of Standards and the United States RSA algorithm proposed DSA algorithm) into ciphertext, and then send to the addressee, after receiving the ciphertext addressee, you must own private key to decrypt the information to obtain the plaintext. Because a private key is protected by a personal care, so after using this technology, the security of the computer network will be greatly enhanced, but also to ensure access to the user's identity information; however, due to the need for strong math program, so asymmetric encryption very slow, sometimes it takes several hours.

The Message Digest and Integrity Identification Techniques. Encryption technology has one message digest is information or text value. Hash it through a one-way encryption function will play a role and produce news. If the sender of a message using its own private key to encrypt the digest embodiment, it can be referred to as a digital signature of the message. If at the time of transmission of the message changes, the recipient after analysis summary comparison of the two, will be able to confirm the information is changed at the time of transmission. To some extent, a summary of information ensures the integrity of information transmission.

For the integrity of the identification technology which is to meet the requirements of confidentiality by identity, passwords, keys and other items of information on the implementation of identification data. Corresponding parameters set in advance, after the input feature, the system automatically its comparative analysis of information so as to realize the encryption and data protection.

Storage Encryption and Transmission Encryption Technology. In order to reduce or even avoid information leakage data generated in the reservoir when the information should be stored encrypted. Ciphertext storage and access control on the two forms of storage encryption technology, the former mainly through conversion of the encryption algorithm, and set an additional password encryption module and other forms of implementation. The latter are more inclined to qualifications and powers, to review and restricted by the user to identify and then make a judgment on its legality.

Line encryption and end-end encryption are two main forms of transport encryption technology, through the data stream of information during transmission encryption, data encryption to achieve the purpose. For line encryption, which means each line by setting a different encryption key encryption to achieve the effect, but the line encryption on the source and destination safely ignored, it became the line encryption drawbacks. For end encryption, which is the information automatically encrypted when the sender sends, and enter the TCP / IP information packet, then unreadable or unrecognized information data to the Internet, when the data information security reach their destinations after , it will automatically be restructuring, decryption, and readable information data is formed.

Key Management Encryption Technology and Confirm Encryption Technology. For ease of use of the information data, in many cases the key information has become one of the data encryption means of expression. Thus, key confidentiality and became the main target of theft. There are media keys; magnetic tape, semiconductor memory, disk and USB flash drives. Key generation, distribution, storage, and other replacement and destruction of all sectors constitute the key management techniques. Confirm network information encryption technology is strictly limited by the scope of information in order to prevent information from being illegal counterfeiting, tampering or counterfeiting. A safe and feasible information program should be allowed to legally confirm the information recipient can verify the message received is authentic; in addition to the message sender cannot be issued their own denial. According to different purposes, specific information to confirm the system can be divided into message confirmation, identification and digital signatures. That is, if one of the key information encrypted data can only be solved with another key. After B with A's public key to unlock the information and data before it can be confirmed sources. This ensures that at the source of the sender of the message has a message to non-repudiation.

The New Development of Encryption Technology and Its Application in Computer Network Security

Encryption technology after years of development, no longer limited to only two kinds of symmetric and asymmetric encryption technology, and gradually more technological development to confidentiality. Here the main focus of new technology application of machinery to computer network security will be described on digital signature technology, information hiding technology and quantum cryptography wind.

Digital Signature Technology. Digital signature technology is the depth development of asymmetric encryption (public / private key encryption technology), to ensure the security of important information technology business transactions, often used in computer network security and e-commerce transactions to ensure corporate LAN security. On the application of e-commerce transactions in the field of digital signature technology commonly used RSA encryption and SSL protocol (now commonly SSL3.0) to improve the security of credit card transactions; secure digital signature can confirm the identity of the sender, because the digital signature You must use the private key and save the others not to copy, once they leave a record of participation in the information and transactions cannot be denied. Under the protection of this technology, the security of e-commerce transactions can be greatly enhanced, can be used for shopping and enter personal credit card information in a secure protected.

Information Hiding Technology. Information hiding is a similar encryption technology (to avoid the illegal theft of information) of the new development, its basic principle is to first use concealment algorithm embedded secret information hidden in the carrier, and then extract the information carrier and the recipient with the original hidden key so concealed information becomes explicit. This technique is commonly used on the intranet, in the company's internal information dissemination, while general information dissemination at all levels within the enterprise, but only to hide that information to get one or two people, and he (they) can use secret key to the hidden information extracted. The advantage of this technique is real-time, to avoid the second encrypted second information transmission and the potential safety problems; and because after the information is difficult to detect the hidden, so you can try to avoid attacks.

Quantum Cryptography. Quantum cryptography is quantum mechanics and cryptography combined with the product, the main application of quantum complementarity principle and quantum no-cloning theorem to manage key and the encrypted information data, which is the latest achievement encryption technology. The basic principles of quantum cryptography is the first information the sender encrypted information and the key exchange with the receiving party in the ciphertext transmission, once the eavesdropper to steal information, the information is encrypted quantum state will change, but this change is not available rehabilitation; and both receive and transmit the information can easily detect whether the information had been stolen [3]. Currently, quantum encryption technology is continually study, its application in computer network security is also not yet clear, but this technology will become the Terminator struggle between "confidential" and "theft".

Conclusion

With the popularity of the Internet, a computer network security has become related to each country, the vital interests of the company and personal things. Encryption technology is the protection of our critical security technology transfer and exchange of information across the network this open space, with the continuous progress of science and technology, encryption technology will gradually accurate and complete technology, which for the establishment of computer network security systems and Perfection is helpful.

References

[1] He Xiangdong, Li Jingyuan. Microcomputer Applications, Vol. 1 (2013) No 53, p.52-53

[2] Duan Hong, Wang Yunhui, Wang Qunyong. Computer Security, Vol. 4 (2013) No 27, p.92-94

[3] Zhu Wenya, Jing Jianfen. Manufacturing Automation, Vol. 6 (2012) No 19, p.35-36

[4] Li Xiaoliang. Digital Technology and Applications, Vol. 29 (2013) No 27, p.21-23

[5] Zhang Gongxu, Sun Jing. Telecom Power Technologies, Vol. 8 (2012) No 27, p.57-60

河南省南阳市文化宫街 35 号，18737756166，王燕军