Journal of Web Systems and Applications (2021) 3: 13-16
Clausius Scientific Press, Canada

DOI: 10.23977/jwsa.2021.030103
ISSN 2560-6913

Research on Information Encryption Technology Applied in Computer Network Security

Yi Shen[1], Haoming Yan[2]

1. Department of Computer Science, San Francisco State University, San Francisco, Ca 94132, , USA

2. Aerospace Engineering, University of Arizona, Tucson, Az 85719, USA

Keywords: Computer network security, Information encryption technology, Application, Research

Abstract: in recent years, people pay more and more attention to the security of computer network. According to the practical work experience, this paper briefly analyzes the application of information encryption technology in computer network security. The first part briefly introduces the related concepts of information encryption technology, and the second part is the research on the application of information encryption technology in computer network security, Finally, the application of information encryption technology is analyzed.

1. Introduction

Information encryption technology is a technology to ensure the information security of the network. It is an active preventive measure for information security. By using a certain encryption calculation method, the plaintext can be turned into a secret text that can not be read directly, so as to prevent illegal users from acquiring and interpreting the original data and ensure the security and confidentiality of the data. We call the process of converting plaintext into plaintext encryption, the process of converting covert text into plaintext decryption, and the key is a variable parameter used in the process of encryption and decryption. In the past, people used to encrypt the data stream through traditional software. When only the ciphertext is mastered, it is very difficult to decipher the encryption algorithm of these ciphertexts [1]. In addition, a good encryption algorithm has little impact on the performance of the system, and even brings some convenience to the system, such as PKZIP, which can compress or encrypt data, killing two birds with one stone.

2. Research on the Application of Information Encryption Technology in Computer Network Security

Computer networking is the development trend of modern computers. With the continuous improvement of networking, people put forward higher requirements for network security while transmitting information, data and communication. Therefore, the security and encryption technology of information and data have changed.

The traditional security concept believes that only the outside of the network can not be trusted, and the inside of the network can be completely trusted. This leads to the traditional information and data security, which takes the firewall, intrusion detection and other defense against the external network as the main body, ignoring the important role of information and data encryption in the network.

2.1 Introduction to Information Hiding Technology

By using information authentication and access control technologies, we can effectively prevent illegal users from using or approaching, which is equivalent to adding a layer of “security door” to the information to be protected; Through password technology, the information content to be protected can be converted into other content that illegal users cannot. Information hiding technology uses multimedia as the carrier to hide the information that needs to be protected, so it is not easy for illegal users to detect or notice the existence of hidden information. This can not only effectively prevent illegal users from extracting information, but also avoid many unnecessary attacks. Compared with traditional cryptography, information hiding technology breaks through the limitations of digital works protection and reduces the wanton dissemination and replication caused by media disclosure [2].

2.2 Storage Encryption Technology and Transmission Encryption Technology

2.2.1 Storage Encryption Technology

In order to prevent the leakage of information data in the storage process, it is necessary to encrypt the information storage. Ciphertext storage and access control are two forms of storage encryption technology. The former is mainly realized through the conversion of encryption algorithm, the setting of encryption module and additional password. The latter is more inclined to review and restrict the qualification and authority, and judge whether it is legitimate by identifying users.

2.2.2 Transmission Encryption Technology

Line encryption and end-to-end encryption are two main forms of transmission encryption technology. The purpose of data encryption is achieved by encrypting the information data stream in the transmission process. Line encryption refers to setting different encryption keys for each line to achieve the effect of encryption, but the neglect of the security of source and sink has become the disadvantage of line encryption. End to end encryption is that the information is automatically encrypted when sent by the sender, enters the TCP / IP information packet, and then transmitted to the Internet with unreadable or unrecognizable information data. When these data and information arrive at the destination safely, they are automatically reorganized, decrypted and formed into readable information data.

2.3 Message Digest and Integrity Authentication Technology

2.3.1 Message Digest Technology

In information encryption technology, information digest is the one-to-one information or text value. It is generated by a one-way hash encryption function acting on the message. If the sender of the message encrypts the digest with his own private key, it is called the digital signature of the message. The receiver decrypts the information sent by the message sender through the key. If the

message changes during transmission, the receiver can confirm whether the message is changed during transmission by analyzing and comparing the two abstracts. To some extent, information summarization ensures the integrity of information transmission [3].

2.3.2 Integrity Identification Technology

Integrity authentication technology is to meet the requirements of confidentiality by authenticating password, key, information data and identity. Set the corresponding parameters in advance. After inputting the characteristics, the system automatically compares and analyzes them, so as to realize the encryption of information and the protection of data.

2.4 Key Management Encryption Technology and Confirmation Encryption Technology

For the convenience of using information data, the key is synthesized into one of the performance means of information data encryption in many fields. Therefore, the key has become the main object of confidentiality and theft. The media of key mainly include; Magnetic tape, semiconductor memory, magnetic disk, USB flash disk.

The generation, distribution, preservation, replacement and destruction of key constitute the key management technology.

Network information confirmation encryption technology strictly limits the scope of information to prevent information from being illegally forged, tampered with or counterfeited. A safe and feasible information confirmation scheme should enable its legitimate information receiver to verify whether the received message is authentic; In addition, the sender cannot deny his message. According to different purposes, the specific information confirmation system can be divided into message confirmation, identity confirmation and digital signature. Due to the existence of certain mathematical relationship between public key and private key, digital signature is formed. That is, if the information data encrypted by one of the keys can only be unlocked by the other key. For example, as the sender, a encrypts the information data with its own private key and transmits it to the receiver B. B can determine the source of the message only after unlocking the information data with a's public key. This ensures that the sender of the information can not deny the sent information at the source.

3. Application Analysis of Information Encryption Technology

In e-commerce activities, information encryption technology can protect both dynamic files and static files, such as the encryption of disks and folders in hard disks by PIP software in order to prevent others from stealing information. Information encryption technology is mainly used in how to actively defend “dynamic” problems.

3.1 Key Application Management

Although the private key is not public, if the user mostly uses the same key in the process of exchanging information, it cannot be disclosed for a long time. If a accidentally learns the key of user B, all the information that user B has exchanged with other users will no longer be confidential to user a. At this time, the more times the key is used, the more materials will be eavesdropped. Therefore, emphasizing the use of a key in a conversation or information is an effective way to reduce disclosure. When using the key, it should be replaced in time to reduce exposure.

If D user is a member of a 2000 person organization, if he wants to have a secret conversation with anyone in the organization, the number of keys that the user needs to master will be very large. How to reduce the number of keys it has, the best way to solve this problem is to establish a

distribution center (KDC) with secure and feasible keys provided by (Kerberos) on the Internet. This user only needs to know a key to talk with KDC.

3.2 Email and Online Payment

Forging an e-mail is very easy, because most users will simply think that the sender is the name and e-mail address displayed on the e-mail. In practice, we can judge the true identity of the sender of information through digital signature based on information encryption technology.

Online payment is more and more used in e-commerce, so online payment has become a very important link of modern e-commerce. How to ensure the security of online payment has become one of the tasks of information encryption technology. In actual work and life, various enterprises have adopted different means to achieve secure online payment. At present, digital authentication protocol has been recognized by most enterprises [4].

3.3 Quantum Encryption Technology

Using quantum technology, we can realize the all-optical network of the traditional cryptosystem, and improve the completion of key exchange and information encryption to the optical fiber level[5]. If an attacker attempts to detect and accept the information sent by the information sender, it will have a certain impact and change on the quantum state, and this change is an irreversible damage to illegal users, The sender and receiver of information can easily detect whether the quantum has changed and judge whether it has been attacked.

4. Conclusion

The application of information encryption technology not only ensures network security, but also promotes the sustainable development of e-government and e-commerce. Of course, information encryption technology is only an active defense technology. It is not omnipotent. To some extent, it can only solve the problems, not avoid the risks. There are still great risks in specific applications such as online payment, e-mail, server access and so on. Therefore, only by increasing the investment in the research and development of information encryption technology, can we timely ensure the integrity and correctness of information and provide a stronger backing for network security.

References

[1] Formal analysis of TPM2.0 key management APIs[J]. Qianying Zhang,Shijun Zhao,Yu Qin,Dengguo Feng. Chinese Science Bulletin. 2019(32)

[2] A Message Digest Disposing Algorithm Based on RC4[J]. LIU Yabin, CHEN Jing, DU Ruiying, ZHANG Huanguo School of Computer, Wuhan University, Wuhan 430072, Hubei, China. Wuhan University Journal of Natural Sciences. 2019(03)

[3] Algebra model and security analysis for cryptographic protocols[J]. HUAI Jinpeng & LI Xianxian School of Computer, Beijing University of Aeronautics and Astronautics, Beijing 100083, China Correspondence should be addressed to Huai Jinpeng (email: huaijp@buaa.edu.cn). Science in China(Series F:Information Sciences). 2019(02)

[4] Trusted Next Generation Internetand Its Development[J]. Wu Jianping, Bi Jun (Network Research Center of Tsinghua University, Beijing 100084, China). ZTE Communications. 2018(01)

[5] BrowserGuard: A Behavior-Based Solution to Drive-by-Download Attacks. Fu-Hau Hsu,Chang-Kuo Tso,Yi-Chun Yeh,Wei-Jen Wang,Li-Han Chen. IEEE Journal on Selected Areas in Communications . 2019