Computer Life
ISSN: 1819-4818 | Vol. 12, No. 1, 2024

Security Risks in Computer Networks and Application of Data Encryption Techniques

Jode Glen

Université de Montréal, Canada, Lindsay Mitchell, Université de Montréal, Canada

Abstract: With the rapid development of science and technology, people through the computer network for the transmission and exchange of information and data is more and more convenient. This paper analyzes the current situation of computer network security, hidden dangers and the principle of data encryption technology, and discusses the application of data encryption technology in computer network security.

Keywords: data encryption techniques, computer networks, security, algorithms

1. Introduction

With the rapid development of Internet, the resource sharing of computer network is further strengthened, and the information security problem is increasingly prominent. Combined with the development of current technology, the author expounds the current situation of computer network security, the hidden dangers in the network and the application of data encryption technology in the network, analyzes from different angles, and protects computers through data encryption technology.

2. Analysis of the current status of computer network security

Computer network security refers to the use of network management controls and technical measures to ensure that the confidentiality, integrity and availability of data are protected in a network environment [1] . Computer network security includes both physical and logical security. Physical security refers to the system equipment and related facilities are physically protected from damage, loss and so on. Logical security includes the integrity, confidentiality and availability of information.

Although China's research on computer network security started late, our researchers have made great achievements by studying hard, introducing foreign advanced technology, summarizing and innovating research results in time. At present, the more mature security technologies in computer network are: data encryption technology, access control mechanism, identification technology, digital signature technology and so on.

At present, the main task before the researchers is to learn from foreign research experience, in-depth study of data encryption technology,information content monitoring technology, network attack monitoring technology, audit trail technology and evidence collection and other security technologies. In particular, data encryption technology involves the protection of personal privacy, corporate information, and even state secrets and other aspects of information security, and need to focus on research.

3. Potential pitfalls of computer networks

3.1. Pitfalls of computer operating systems

As a supporting software, the computer operating system (OS) has its own memory management, CPU management, peripheral management, etc. Each management involves some modules or programs. If there are problems in these programs, such as memory management problems, and the external network is connected to a defective module, the computer system may crash [1] . Therefore, network intruders use the weak links of the operating system to attack, making the computer system in a paralyzed state, affecting people's normal work and learning.

3.2. Incomplete hazards in the network

The operating system supports the free transfer of files, loading or installation of programs on the network. These functions add various threats to the network. The file transfer function is an important function of the network, such as TCP/IP protocol, FTP, NFS. If there are loopholes in these protocols, network intruders can search the user name according to these loopholes, guess the machine password, and attack the computer firewall.

3.3. Insecurity of database management systems

Database management system (DBMS) is a kind of large-scale software to manipulate and manage databases, which is used to establish, use and maintain databases. It manages and controls the database uniformly to ensure the security and integrity of the database.

Users access the data in the database on the local machine via the network. People from inside or outside the organization may deliberately destroy or tamper with the data. If the data is put on the Web, it may also be damaged by computer hackers or other criminals. Therefore, the insecurity of the database will leak the information that users browse and store on the Internet, resulting in the leakage of users' accounts and passwords, posing a serious threat to users' property and privacy security.

4. Concepts, principles and common methods of data encryption techniques

4.1. The concept of data encryption techniques

Data encryption (DE) technology refers to the process of converting an information (or plain text) into meaningless cipher text through encryption key and encryption function, while the receiver restores the cipher text to plain text through decryption function and decryption key.

4.2. Principles of data encryption techniques

In the actual operation of the computer network, users use the application system to provide services aimed at the smooth transmission of data. Therefore, information security is to ensure the core of the entire computer network. The basic process of data encryption is according to the data encryption algorithm, the original file or data processing (plain text), so that it becomes an unreadable piece of code (cipher text), so that it can only be input into the corresponding key to show the original content, so that you can achieve the protection of data is not stolen by illegal elements, read the purpose.

4.3. Common methods of data encryption techniques

Data encryption is the cornerstone of computer network security technology. In order to prevent information from being accessed by unauthorized persons during storage or transmission, symmetric and asymmetric encryption methods are usually used to protect information.

4.3.1. Symmetrical encryption

Symmetrical encryption, or private key (also known as conventional encryption), is shared by both communication parties with a secret key. It is an encryption method using a single key crypt system. The same key can be used as an encryption method for information encryption and decryption at the same time. Common symmetric encryption algorithms include DES, IDEA, RC4, SKIPJACK, RC5, AES, etc. They have their own advantages, of which DES is The data encryption standard of France is fast and suitable for encrypting large amounts of data. RC2 and RC4 algorithms use variable length keys to encrypt large amounts of data, which is faster than DES algorithm. AES algorithm advanced encryption standard is the next generation encryption algorithm standard with high speed and high security level. At present, one implementation of AES standard is Rijnda el algorithm[2]. Symmetrical encryption also has defects. For example, the key between A and B must be different from that between A and C. Otherwise, the security of messages received by B or C will be threatened [2] .

4.3.2. Asymmetric encryption

Asymmetric encryption is the encryption and decryption is not the same key, usually there are two keys, called "public key" and "private key", they must be used in pairs, otherwise you can not open the encrypted file. For example, a customer of an Internet bank sends encrypted data to the bank's Web site for account operations.

If the decryption key is public, with a private key encrypted information, you can use the public key to decrypt it, for customers to verify that the party holding the private key to publish the data or documents is complete and accurate, the receiver can thus know that this information does come from someone with a private key, which is called a digital signature, the form of the public key is a digital certificate.

Installation programs downloaded from the Internet generally carry the digital signature of the author of the program, which proves that the program is indeed issued by the author (company) and not by the company three-party forgery that has not been tampered with (authentication/verification). If RSA algorithm, invented by RSA Company, is a public key algorithm that supports variable length keys and requires the length of encrypted file blocks.

5. Conclusion

In summary, the application of data addition in computer network security. Encryption technology is the basic technology to ensure the safe transmission and exchange of information under the current situation, which is crucial to the security of computer networks. It is hoped that through the research of this paper, it can attract the attention of experts at home and abroad, and invest more energy, financial and material resources to study data encryption technology, so as to better protect the information security of each network user.

References

[1] Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. IEEE Internet computing, 16(1), 69-73.

[2] Dawoud, W., Takouna, I., & Meinel, C. (2010, March). Infrastructure as a service security: Challenges and solutions. In 2010 the 7th International Conference on Informatics and Systems (INFOS) (pp. 1-8). IEEE.

[3] Rosegrant, M. W., & Cline, S. A. (2003). Global food security: challenges and policies. Science, 302(5652), 1917-1919.

[4] Reddy, G. N., & Reddy, G. J. (2014). A study of cyber security challenges and its emerging trends on latest technologies. arXiv preprint arXiv:1402.1842.

[5] Barnett, J. (2003). Security and climate change. Global environmental change, 13(1), 7-17.

[6] Levy, M. A. (1995). Is the environment a national security issue?. International security, 20(2), 35-62.

[7] Li, X., Wang, X., Chen, X., Lu, Y., Fu, H., & Wu, Y. C. (2024). Unlabeled data selection for active learning in image classification. Scientific Reports, 14(1), 424.

[8] Liang, Y., Wang, X., Wu, Y. C., Fu, H., & Zhou, M. (2023). A Study on Blockchain Sandwich Attack Strategies Based on Mechanism Design Game Theory. Electronics, 12(21), 4417.

[9] Lee, Zhitong, Ying Cheng Wu, and Xukang Wang. "Automated Machine Learning in Waste Classification: A Revolutionary Approach to Efficiency and Accuracy." Proceedings of the 2023 12th International Conference on Computing and Pattern Recognition. 2023.

[10] Guo, H., Ma, Z., Chen, X., Wang, X., Xu, J., & Zheng, Y. (2024). Generating Artistic Portraits from Face Photos with Feature Disentanglement and Reconstruction. Electronics, 13(5), 955.

[11] Wang, X., Wu, Y. C., Ma, Z. (2024). Blockchain in the courtroom: exploring its evidentiary significance and procedural implications in U.S. judicial processes. Frontiers in Blockchain, 7, 1306058.
[12] Lehtinen, R., & Gangemi Sr, G. T. (2006). Computer security basics: computer security. " O'Reilly Media, Inc.".
[13] Landwehr, C. E. (1983). The best available technologies for computer security. Computer, 16(07), 86-100.
[14] Richards, N. M., & Solove, D. J. (2010). Prosser's privacy law: A mixed legacy. Calif. L. Rev., 98, 1887.
[15] Hsiao, D. K., Kerr, D. S., & Madnick, S. E. (2014). Computer security. Academic Press.