HILL PUBLISHING

Advance in Information Technology and Computer Science, 2024, 1(1), 5-7
https://www.hillpublisher.com/Journals/aitcs/
ISSN Online:
ISSN Print:

Computer Network Information Security and Encryption Technology

Shengzhi Zhu, Xiaoman Qiu, Yuanchao Qi

Wuhan Donghu University, Wuhan 430212, Hubei, China.

How to cite this paper: Shengzhi Zhu, Xiaoman Qiu, Yuanchao Qi. (2024) Computer Network Information Security and Encryption Technology. *Advance in Information Technology and Computer Science*, 1(1), 5-7.
DOI: 10.26855/aitcs.2024.12.002

Received: October 14, 2024
Accepted: November 4, 2024
Published: November 26, 2024

***Corresponding author:** Shengzhi Zhu, Wuhan Donghu University, Wuhan 430212, Hubei, China.

Abstract

Computers have become common equipment in all fields of society and are of great significance to promoting social development. Because the network is open and complex, it will also be threatened by many factors during the operation of computer networks, such as hacker attacks, network viruses, system vulnerabilities, etc. In order to effectively protect the information security of users, computer network security protection should be strictly carried out to meet the diversified and personalized use needs of users. With the improvement of technical level, network threats also show diversified characteristics. It is necessary to continuously optimize data encryption methods and carry out technological innovation to adapt to the characteristics of current network threats and enhance system protection capabilities.

Keywords

Computer; network information security; encryption technology

Introduction

In the era of Internet communication, computer technology uses electronic computers as carriers to collect, transmit and process information. It is a new way of information processing. As a result, the importance of computer information data encryption technology has gradually become prominent. As an important tool for protecting information data security, encryption technology is also facing many challenges in infrastructure, database storage, network security, etc. in the context of the new era. With the goal of ensuring computer information data security, improving the protection and usability of encryption technology has become a focus of research in the computer field.

1. Working principle of computer data encryption technology

The working principle of data encryption technology: based on the application of encryption algorithms, ciphertext is created. The staff needs to use a fixed key to unlock the complete ciphertext content. In fact, it is to use the encryption function and key to re-sort the network information and generate the encrypted ciphertext. In the process of receiving information, the information receiver needs to use the encryption function and key specified in advance to decrypt the ciphertext to ensure the security of computer network information in the transmission and application links. The commonly used computer encryption algorithms mainly include the encryption information permutation table algorithm, the encryption information cyclic shift method, the encryption information XOR operation algorithm, etc.

2. Factors affecting computer network security

2.1 Software attack

Hacker attacks and network viruses are the most common security risks in computer networks. They can invade computer network systems, causing risks such as system paralysis and information leakage. In order to deal with the

security issues of computer network systems, virus detection and killing software must be used to improve the level of network security protection. However, virus detection and killing software often detects and kills specific viruses, and there is a certain lag in application. If some criminals use network viruses, Trojan viruses, etc. to attack computer network systems and steal accounts and information, it will cause serious network security risks.

2.2 Computer system problems

The first is the computer operating system, which is an important prerequisite for ensuring the operation of computers and software. It has strong scalability and rich functions, which brings hidden dangers to computer network security. Even old computer companies like Microsoft have encountered network security problems. The other is computer system software. Since some computer system software has many loopholes in the early development process, this provides hackers with opportunities to invade directly. By implanting Trojan viruses in computers, they launch attacks on computers and achieve comprehensive control over computer equipment, taking the opportunity to view confidential files and steal user passwords.

2.3 Inadequate security maintenance

During the operation of the computer system, it is necessary to continuously monitor the operating status of the server, improve security awareness, promptly detect abnormal conditions in the system operation, and locate and troubleshoot faults. If the security maintenance of the computer information system is neglected, it will increase the operating risk of the information system and provide some security loopholes with opportunities for invasion; in addition, the network firewall is an important barrier to protect the computer system from attacks by viruses, hackers, etc. If the network firewall is not configured properly, the software is not updated in time, and the virus is not detected and killed in place, it will provide some network viruses with opportunities to invade, causing security risks to the computer information system.

3. Key points of data encryption technology application in computer network security

3.1 Symmetric and asymmetric encryption

Symmetric encryption and asymmetric encryption are two common types of computer information data encryption technology. Symmetric encryption technology is one of the simpler and more frequently used encryption technologies in current information data encryption technology. This encryption technology is an encryption technology that realizes encryption and decoding functions at the same time based on single- key encryption. This encryption technology is used in data transmission processes with large amounts of data due to its simple operation and fast encryption speed. Asymmetric encryption and symmetric encryption are essentially different in terms of the number of keys. Symmetric encryption only requires one key, while asymmetric encryption requires two keys, namely the public key (publickey) and the private key (privatekey). In the actual information data encryption process, users must hold the public key and the private key.

3.2 Key data encryption

When using key data encryption technology, the most important thing is to do a good job of key management, ensure that the master key meets the requirements of data transmission, and use key encryption to achieve comprehensive data protection. In this process, management is mainly implemented through session keys and initial keys. In key management, the security level and life cycle of the master key should also be clarified. The master key is generated based on a pseudo-random number generator. The data encryption effect will be affected by the key distribution effect and negotiation effect.

3.3 Identity authentication and data signature information authentication

When operating a computer network system, identity authentication technology can be used to quickly identify and authenticate, clarify the operator's relevant permissions, and achieve the purpose of protecting data security. If the operator's permissions do not meet the pre-set requirements, the protection program can be automatically executed to avoid illegal operations and information leakage, respond to access policies in a timely manner, and improve the operating environment of the computer network system. In practical work, identity authentication technology can be

applied to asymmetric encryption and symmetric encryption algorithms to play a reliable security protection role. In recent years, digital signature authentication technology has also been commonly used in data encryption work, and the network security level will be comprehensively improved with the authentication of user information. In the encryption and decryption of data, public and private keys can also be used. This is the basic feature of digital signature authentication technology, which can prevent user information from being deviated.

4. Practical application of data encryption technology in computer systems

4.1 Use of encryption technology in computer software

When encryption technology is used during computer operation, antivirus software is usually encrypted to prevent computer data files from being invaded by viruses. Staff can apply data encryption technology on the software inspection system to check for problems in data files. If the content of files stored in the computer has been invaded by viruses, encryption measures need to be used to deal with it. It should be noted that staff need to encrypt computer software during the application of data encryption technology to improve the confidentiality of data transmission.

4.2 Virtual network security application

Virtual networks, with their user account virtualization and other features, add a certain degree of difficulty to the security encryption of computer information data. At present, virtual network applications mainly rely on virtual network router devices to achieve wireless network services or provide corresponding network services to multiple users. In order to effectively reduce the computer information data security threats brought by virtual network security, we should use the advantages of encryption technology to enhance the Internet's ability to analyze and defend against potential threats, so as to ensure the security and stability of various types of data in the computer. From a technical point of view, the encryption of computer information data in virtual networks can appropriately use the RSA encryption algorithm, which uses two encryption methods, public key and private key, on the basis of asymmetric encryption algorithms, making encryption technology irreversible in encryption algorithms.

5. Conclusion

Ensuring the security of computer networks can provide reliable protection for people's normal production and life, and avoid huge losses when using computer networks. Data encryption technology mainly includes symmetric encryption technology, asymmetric encryption technology and digital signature authentication technology. In practical applications, the technical points of end-to-end data encryption, key data encryption, node data encryption, identity authentication and data signature information authentication, and database encryption should be clarified to give full play to the role of data encryption technology and reduce the risks of computer network operation.

References

[1] Du Mingming. Discussion on computer network information security and encryption technology[J]. Digital Communication World, 2022(07):76-78.

[2] Lin Wei, Zhang Yuxi, Zhang Chi. Application of data encryption technology in computer network information security[J]. Wireless Internet Technology, 2022, 19(13): 27-29.

[3] Wang Shuman. Analysis of data encryption technology in computer network information security[J]. Electronic Test, 2022, 36(07): 86-88.

[4] Zou Jiabin. Research on data encryption technology in computer network information security[J]. China High-tech, 2022(02):42-43.

[5] Wang Qin. Discussion on computer network information security and encryption technology[J]. Science and Technology Innovation and Application, 2021, 11(33): 90-92+96.

[6] Chen Yumei. Application of data encryption technology in computer network information security[J]. Digital Technology and Application, 2021, 39(03): 174-176.

[7] Wen Zhu. Analysis of application countermeasures of data encryption technology in computer network security[J]. Electronic Technology and Software Engineering, 2020(17):259-260.

[8] Zhang Fangkun, Wang Hongyan. On the impact of encryption technology on computer network security[J]. China New Technologies and New Products, 2020(15):139-140.