Analyze the Application Value of Data Encryption Technology in Computer Network Security

Jiali Geng[1,*]
[1]College of Information Engineering, Anhui Vocational College of Finance and Trade, Hefei, Anhui, China, 230601

Article Info
Volume 83
Page Number: 5254 - 5259
Publication Issue:
July - August 2020

Article History
Article Received: *25 April 2020*
Revised: *29 May 2020*
Accepted: *20 June 2020*
Publication: *28 August 2020*

Abstract

With the continuous development of network technology, industry informatization has gradually advanced and made great progress. However, computer network security has become the focus of increasing attention. To solve this problem, we must adopt reasonable measures to protect computer network communications. Analysis of data encryption technology is an important guarantee for network security, an important means to effectively maintain network security and protect user information. Relying on the analysis of data encryption technology, this paper expounds and analyzes the application of data encryption technology in computer network security from the perspective of technical methods, aiming to improve the reliability of data communication.

Keywords: *Data Encryption, Computer Network, Communication Security, Application Value;*

1. Introduction

With the development of technology in the information age, computer network technology continues to develop in depth, a large amount of information is transmitted through computer networks, which brings great convenience to people's lives and work, and thus entered the DT (data age)[1, 2]. However, the transmission of data also brings security risks[3]. How to improve the reliability of data information in computer network communication and transmission to prevent economic losses to users due to information leakage has also become an important part of people's work and life. Content and key research directions[4].

Common data encryption technology can be used to protect people's privacy and information security, which has also become a more common computer network security communication protection application technology, especially for the protection of private information, personal accounts, and fund security[5, 6]. As computers penetrate into various fields of society, people are paying more and more attention to the issue of network information security. Relying on the analysis of data encryption technology, this paper expounds and analyzes the application of data encryption technology in computer network security from the perspective of technical methods, aiming to improve the reliability of data communication.

2. Computer network communication security overview and influencing factors

2.1. Overview of computer network communication security

2.1.1. Connotation of network communication

Network communication refers to the network communication protocol, that is, it can formulate standard and normative requirements for transmission codes, information transmission rates, transmission control procedures, and error control.

2.1.2. Threat analysis of network communication security

Information security is the main goal of network communication. In order to continuously improve the level of information security, it is necessary to realize the safe transmission and storage of information. The network is a necessary prerequisite for calling instructions, so the safety of network communication is very critical. Currently, network communication threats are concentrated in two aspects: man-made and non-man-made. The degree of man-made threat is the most obvious, usually including the following aspects: monitoring and stealing line information, analyzing and intercepting data information, stealing user identities, and tampering with information at will.

2.1.3. Connotation of data encryption technology

For data encryption technology, in the actual application process, it can ensure the security of network communication. Encryption technology refers to converting information into meaningless ciphertext after special processing. In terms of receiving, after receiving the ciphertext, a certain technology is used to realize the conversion to plaintext. The method of mutual conversion and calculation between ciphertext and plaintext according to specific rules is usually called a key.

The data encryption technology is a method of encrypting information. Generally speaking, it is divided into two forms of plaintext and ciphertext for encryption, and decryption is different according to the encryption method. Therefore, data encryption usually has symmetric encryption. There are two kinds of key and asymmetric key. The former is also called private key encryption. The sender and receiver hold the same key and can encrypt and decrypt the plaintext; the latter is also called public key encryption, but the sender and receiver have the same key. Encryption and decryption keys are not the same, as shown in Figure 1.

2.1.4. The important role of data encryption

With the rapid development of network technology, network technology is widely used in many fields. Especially with the popularization and development of network technology, man-made and non-man-made security threats also arise. Take a commercial company as an example. Because it has a lot of business secrets and business-related information will be transmitted through network technology, hackers will use illegal means to intercept the information to achieve illegal purposes, causing the commercial company to suffer immeasurable losses.

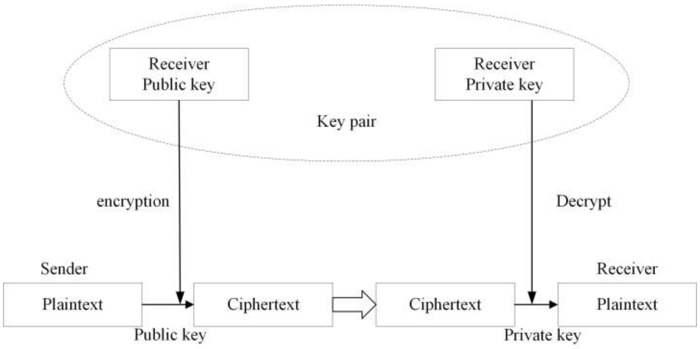

Figure 1. Asymmetric encryption process.

2.2. Influencing factors

2.2.1. Computer virus

There are many types of computer viruses, such as exe and other files with suffixes, which are key factors that threaten the security of network communication. For example, SQL injection, query and attack websites and servers through SQL statements, hackers use computer viruses to attack client computers, and use Trojan horses to implant them. Destroy the basic protection functions of the computer. At the same time, the corresponding operating code is implanted in the computer so that it can copy the code during the operation of the computer, thereby stealing important user information. The typical panda burning incense is a well-known computer virus. Computer viruses are highly contagious, concealed, and destructive. They cause serious damage to the user's computer and even paralyze the computer system. Biological viruses have the ability to reproduce themselves, can infect and regenerate between different computers, have strong replication and transmission capabilities, and are a potential factor affecting computer communication security.

2.2.2. Network and system vulnerabilities

Computer network communications and systems are artificially designed, and there must be vulnerabilities and defects that have not been considered. This has become the main direction of attack and one of the hidden dangers of computer network security. Network vulnerabilities are mainly manifested in computer hardware and software design, and are a manifestation of imperfect operational security strategies. Network hackers bypass the firewall and damage client computers without authorization. Although computers can repair their own vulnerabilities, there are still security policy vulnerabilities during network transmission, which can be easily exploited by hackers and criminals.

2.2.3. Hacking

Hackers are illegal persons with superb computer skills. They can attack computer networks through various viruses and attack strategies to steal important information and data. Hacker intrusion is highly targeted. Once the intrusion target is determined, the computer's security key will be stolen through Trojan horse implantation. After obtaining the security key, the hacker can destroy or obtain the user's personal information to achieve its ulterior purpose.

3. Data encryption technology

3.1. Link encryption technology

Link encryption is also called online encryption, which can realize the purpose of encrypting network communication links. Encryption is completed before the data information is transmitted, and another key is used and encrypted in the next link, and then the transmission is carried out. During the entire process of data transmission, all nodes and links that pass through will be decrypted, and then re-encrypted, so the data information in the communication link is always ciphertext. After the encrypted link, both the sending point and the receiving point of the information are effectively covered, ensuring the concealment of the length and frequency of the information, so as to prevent illegal users from analyzing and using the content of the communication. Through the application of link encryption technology, the security of network transmission of data and information is continuously improved. Affected by link encryption, it is clearly pointed out that the encryption devices at both ends of the link will complete encryption through a certain link mode after synchronization, which increases the burden on network performance.

3.2. Node encryption technology

Compared with the link encryption technology, the node encryption technology has similarities. Specifically, it refers to the node's decryption and re-encryption of data, requiring the communication link as the main carrier to effectively ensure the security of data information. However, unlike link encryption technology, in node encryption, data is not allowed to be presented in plaintext when passing through the node. In the node, a security module is installed and connected to the node machine, which is a kind of cryptographic device. Through the application of this security module, data decryption and encryption are realized. It is precisely because the purpose of node encryption is to ensure that the intermediate node obtains the data information processing method, the header and routing information must be transmitted in plain text. In this case, node encryption is relatively weak in preventing communication services from being attacked.

3.3. End-to-end encryption technology

In end-to-end encryption, when data information is transmitted from the starting point to the receiving point, it is always presented in cipher text. Generally speaking, end-to-end encryption technology is also called off-line encryption and packet encryption. It encrypts data information before transmission and does not decrypt it during transmission. After the data is received, as the recipient, it will follow the key requirements Decrypt the data and present it in plaintext. This shows that data security and confidentiality are always protected during transmission, as shown in Figures 2 and 3. Compared with other encryption technologies, the end-to-end encryption technology is not affected by the damage of the node and it is difficult to transmit data information. Most importantly, the design and use of end-to-end encryption technology is relatively stable and simple, and the actual cost is relatively low. In addition, this encryption technology does not require high synchronization of the equipment, and will not increase the network performance burden. But its most obvious flaw is that it is difficult to conceal the information sending point and receiving point.

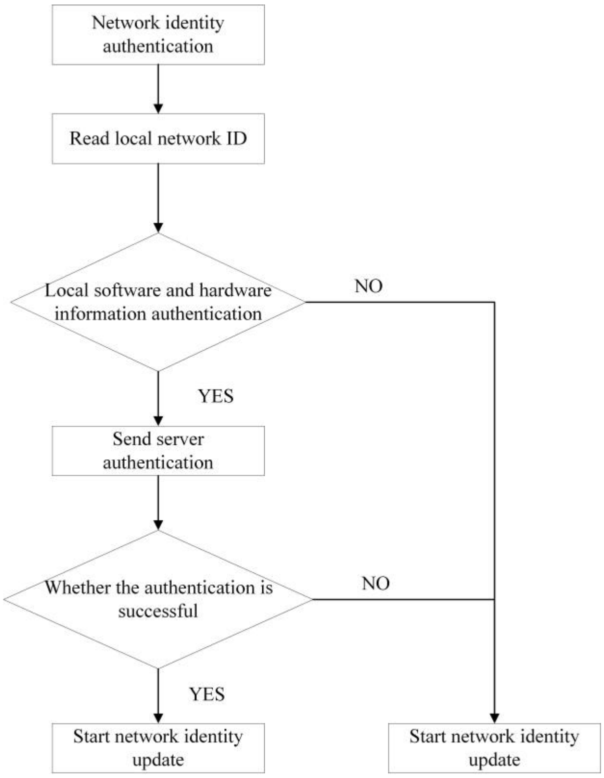
Network identity authentication
Read local network ID
Local software and hardware information authentication
NO
YES
Send server authentication
Whether the authentication is successful
NO
YES
Start network identity update
Start network identity update

Figure 2. Device-side network security.

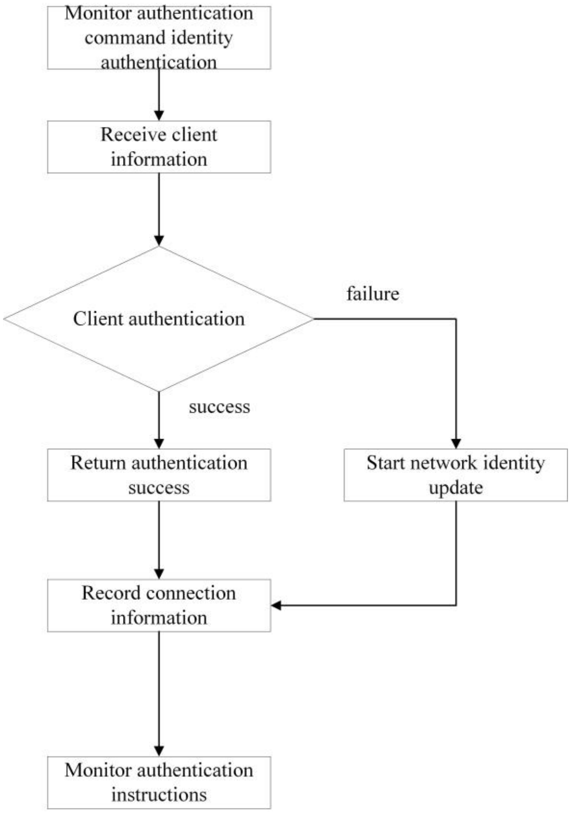
Monitor authentication command identity authentication
Receive client information
Client authentication
failure
success
Return authentication success
Start network identity update
Record connection information
Monitor authentication instructions

Figure 3. Server network security.

The following evaluations are made on the effect of data encryption:

$$A = \left[x_{ij} \right]_{n \times m} = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1m} \\ x_{21} & x_{22} & \cdots & x_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ x_{n1} & x_{n2} & \cdots & x_{nm} \end{bmatrix} \quad (1)$$

4. Methods of data encryption technology

4.1. Symmetric encryption method

In the actual application of data encryption technology, symmetric encryption is a commonly used encryption method, which can complete data encryption and decryption tasks with the same key, so it is more efficient and simple in operation. At this stage, symmetric encryption methods are widely used. Taking the US government as an example, standardized symmetric encryption methods are used in DES encryption. Choosing to use this single key method, due to the openness of the computer network environment, must emphasize the important role of information transmission and storage. Using symmetric encryption methods and ensuring the security of network communication information, key security is always the focus. If the key is difficult to ensure security, it will directly affect the performance of symmetric encryption. Therefore, in practical applications, the standardization of key transmission and storage should be ensured.

4.2. Asymmetric encryption method

The use of asymmetric encryption methods requires the effective use of the public key and the private key in order to avoid being unable to open the encrypted file. The so-called public key can be used publicly, but the private key can only be handed over to the holder for safekeeping, with absolute confidentiality. Comparing the symmetric and asymmetric encryption methods, we can find that the most obvious advantage of the asymmetric encryption method is that it does not need to use the network to transmit the private key, as long as the recipient enters the private key kept by the individual after receiving the data information OK.

In this way, it is possible to circumvent the security problems in the key transfer process. But it should be noted that asymmetric encryption requires a lot of time, and the encryption speed and decryption speed are far behind the symmetric encryption method.

5. Application of data encryption technology in network communication security

With regard to the above-mentioned data encryption methods and technologies, it is possible to expand the scope of its application in network communication security.

Software: Computer network communications often cause the network to be completely paralyzed due to the software being implanted with viruses, and even threaten the security of the system, and data and information security cannot be guaranteed. Therefore, encrypting computer software can effectively detect possible infections in the software. The specific manifestations are as follows: ①The computer software is attacked by a virus, and data encryption can help it prevent the virus and crack the key in time. Avoid the penetration of viruses and protect the software from viruses; ②Unauthorized illegal users can only use the correct key to run the software after cracking the software retrieval data information, and if the key is wrong, not only can’t retrieve the information, but after entering it The software will delete the user data or issue an alarm to actively protect the data.

Database aspect: Nowadays, the daily application of database is becoming more and more extensive, and the security protection of database management system is also receiving high attention. Moreover, the security and confidentiality of database platform will directly affect the security of computer network communication. Therefore, data encryption is required for network databases, and the user can set access permissions to obtain encryption.

At present, the application of data encryption technology in the field of network communication security mainly includes the following aspects.

5.1. E-commerce data processing applications

E-commerce is an online business activity built on a network business platform based on the rapid development of computer technology, information technology and network communication technology. E-commerce integrates many new communication technologies into one, realizing information communication and trade between users and merchants. Users log on to the e-commerce platform through their own identity verification, and conduct trade and communication with merchants. The foundation of e-commerce is a good network communication environment and secure network transmission. Once information leakage and network attacks occur in e-commerce activities, it will cause irreparable losses to businesses and users. Therefore, e-commerce should choose a variety of data encryption technologies to protect users' information security and privacy and reduce the risk of information leakage during network transmission. For example, online platforms such as JD.com, Taobao and Xianyu are typical e-commerce platforms. In order to effectively meet the shopping needs of users, synchronous data encryption technology is adopted to encrypt user information and financial information to ensure the safety and security of user network transmission. Privacy and security.

5.2. LAN data management application

As an internal information network, the local area network is widely used in the internal management of enterprises to realize internal information communication. In order to prevent the LAN from being attacked by external hackers, it is necessary to conduct security management analysis on its data transmission, and adopt the form of symmetric encryption to improve the level of network security transmission management. The survey results show that the number of computer local area networks is increasing day by day, becoming an important part of the internal network construction of enterprises and institutions and playing an important role in the development of enterprises. Data encryption technology can establish a data transmission key without changing the local area network transmission mode, and realize the security of internal information and the security management of information communication. The security requirements of data management in the local area network are relatively low, but the enterprise has higher requirements for internal information security, so it is necessary to adopt a symmetric encryption method with simple operation and small network resource occupation.

5.3. Computer software data processing

Software encryption technology realizes data encryption through software processing, and the encryption principle is consistent with traditional encryption technology. Computer software data processing is to reduce the leakage of user information from software applications, and to ensure the safety of user information by improving the security level of the software. Computer software data processing stores and manages user information and privacy in accordance with relevant requirements to ensure the safety of relevant information. For example, on the premise of data encryption technology, set a password for computer software to log in. Once the user's password is inconsistent, the computer will lock the account or send an alarm message to the bound mailbox and mobile phone to improve the safety of the software. When hackers or viruses invade the computer, the computer software can set up corresponding security walls through data encryption technology to improve the level of data security management. In the process of computer software processing, data encryption technology can be used to provide security protection space for computers, such as online banking security plug-ins and USB shield security controls, to ensure user information and privacy security, and meet the needs of network communication security.

6. Conclusion

This article explains the main methods of data encryption (end-to-end encryption, link encryption, node encryption) and data encryption technology methods (asymmetric encryption, symmetric encryption), and analyzes the calculation process of different methods , At the same time, in view of the implementation of data encryption technology in the network, enumerate the application of data encryption technology, including e-commerce data processing, local area network data processing, and computer software data processing, etc., aiming at the application of data encryption technology in network communication security Provide scientific and reasonable reference.

Acknowledgments

Research on Key Technologies of routing optimization in nested mobile networks Project number: KJ2018A0910.

References

[1] Hamed H, Al-Shaer E. Taxonomy of conflicts in network security policies [J]. IEEE Communications Magazine, 2016, 44(3): 134-141.

[2] Kraemer S, Carayon P. Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists [J]. Applied Ergonomics, 2017, 38(2): 143-154.

[3] Lee, C. P.,Uluagac, A. S., Fairbanks, K. D., Copeland, J. A. The design of netseclab: A small competition-based network security lab [J]. IEEE Transactions on Education, 2018, 54(1): 149-155.

[4] Zhang J. Application of artificial intelligence technology in computer network security[J]. International Journal of Network Security, 2018, 20(3): 1-10.

[5] Stojanov Z, Dobrilovic D, Zoric T. Exploring students' experiences in using a physical laboratory for computer networks and data security [J]. Computer Applications in Engineering Education, 2017, 25(2): 290-303.

[6] Peterson D G. A new era in data network security: Protocol-sensitive encryption [J]. International Journal of Network Management, 2018, 5(4): 214-218.