Research on Applications of Data Encryption Technology in Security of Computer Network Communication

Na Li[1, a]

[1] Jiangxi Technical College of Manufacturing, Nanchang, 330095, China

[a]email

Keywords: Data encryption, Computer network, Communication security

Abstract. In recent years, computer network communication system has been widely spread in many industry fields, which has brought great convenience to people's daily life and work. At the same time, it also raises a series of information security problems. This paper points out the common threats faced by network security in the current period and explores some data encryption technologies applied in the security of network communication, including the technologies of link encryption, node encryption and end to end encryption to provide some references for the relative researchers.

Introduction

Data encryption technology is the necessary management method to ensure the security of network communication. It mainly refers to the network information processing in a special way, and converts the information into the cipher text which is not easy to understand. These cipher text can be converted to plaintext only by the specific technology and software only after the receiver receives it effectively. The cipher and plaintext method for converting the cipher under certain rules is the key. Whether it is personal, government office, or business, each stage of the network exists in people's work and life, along with people's entertainment and office, information and business, the network has become an increasingly important part of people's work and life. However, some human and non-human factors, such as hackers and loopholes, have always threatened the information security and some trade secrets of the network. Some hackers use illegal means to intercept important secrets of some commercial companies on the internet. Hackers will be some Trojans and viruses, embedded company’s office system, leading to some of the company's office system paralyzed, seriously affecting the normal operation of the office system, the company caused great economic losses. In addition, there are some hackers use illegal means to steal network users online banking account and password, others will be the bank account in the deposits removed, impersonate others to their relatives and friends ask for property, causing serious damage and loss of credibility to others. Therefore, the use of data encryption technology to protect network security is of great significance. How to effectively avoid the security problems in the communication process, is the focus of attention in the computer network communication security technology. From the point of view of current communication security measures, data encryption technology plays an important role.

Threats to Security of Computer Network Communication

Information Theft. In the data transmission process, the gateway node and the router node are very dangerous. Hackers can intercept data from the computer network at this point. If the network data information is not encrypted, then the information leakage will happen. The operating system of many enterprises is the use of foreign research and development, although there is no problem in actual use, but these products really have left the back door or what other defects, the general enterprise is difficult to judge from a professional point of view, the above reasons can lead to the enterprise's financial information stolen. On the other hand, especially for large enterprises, the network accounting information system has many nodes, that is, there are many user terminals, at the same time, a large amount of information used by the application system is concentrated in the server. If the staff is careless, the user name and password leaked to others, or leave the machine, forget to

withdraw from the system, etc., will make the financial information into the risk of theft. According to historical data, to steal financial information in the case above by insiders or collusion of crime, stealing their financial information to obtain illegal economic interests, many of which a huge amount of money involved. For information theft network crime, its technical characteristics mainly show that such crimes are implemented through specialized processing of computer means and network transmission program. On the one hand, criminals steal information need to master the special and difficult for the network user identification code and computer virus, the virus implanted "or program by specific means, on the other hand, transmission of information crime people use specialized instructions to control the infection of network users and the receiving process, such as virus with the operation of computer operation, network will automatically be infected user related information is sent to the specified mailbox crime.

Information Tampering. Computer network information data in the network transmission hypothesis does not take encrypted transmission mode, so when the intruder information can be intercepted data tampering, the subsequent data receiver cannot obtain the corresponding real network information. In general, closely related data and the future development of the enterprise, the enterprise is secret information, shall not be leaked, but most of the software system mainly focus on the accounting information system and improve the financial system to comply with design. Specifically, the data distortion risk is manifested in the following aspects of tampering with data. Tampering with data refers to the process of tampering with the data transmitted to the destination after the intruder has understood the data format and rules through certain techniques. Generally, data integrity can be destroyed in three ways. The offender changes the order of the data stream or changes the content of the information, such as the delivery address of an order commodity, or the deletion of part of a data or parts of a data stream. Falsifying data mainly for false website and store, email, subscribe to the user order, forged a large number of users. Email, limited enterprise resources, the legitimate users can not normally access cyber source, which has a strict time requirements of the service cannot even get fake response users, send a lot of emails, information can be stolen merchandise information and user credit enterprises. If the authorized database system manager initiates attacks on the database system from within, the entire system's data is in a transparent, undefended state. At the same time, most of the database systems use backup mechanism to copy the data to other media regularly to make remote backup storage. If the database system managers intentionally steal data backup media, it will cause data tampering in the database system.

Information Destruction. If the unauthorized computer user can impersonate the computer to authorize the user to enter the system, the overall security of the computer structure system will be threatened and the consequences will be unimaginable. The network provider in addition to care about the network information security, but also consider how to cope with unexpected natural disasters, military strikes to destroy the network hardware, and how to restore the network communication in the network is abnormal, maintain the continuity of network communication. In essence, the network security including the security network system hardware, software and network transmission of information, which is not caused by accidental or malicious destruction of the attacks, network security not only the technical aspects of the problem, also have governance problems, two aspects complement each other, indispensable. Information security is the organization should clear the need to protect the information resources, to ensure the confidentiality of information, integrity and availability, and maintain good coordination. Information security is very important to both the government and the enterprises. In order to prevent the occurrence of information security incidents or incidents, the firewall and intrusion monitoring systems are taken into consideration in the technical aspects. Artificial network intrusion and attack behavior make network security face new challenge. Information maintained during storage or transmission is not modified, not destroyed or lost. The network has a sudden development in just ten years. The network has the characteristics of opening information and sharing information, which makes the circulation of information at a high speed and greatly facilitates the production and life. However, due to the characteristics of network opening and information sharing, network security is faced with huge risks, which provides opportunities for some people who maliciously destroy personal or company network information.

Data Encryption Technology Applied in Network Communication Security

Link Encryption Technology. Link encryption is mainly on the communication lines of information encryption, encrypted in transmission, each node in the link to the data encryption, and then move on to the next node then encrypted, then transmission. Therefore, the data transmission process, the data is always in the process of transmission and encryption, encryption can effectively conceal and send the link point data transmission, the length and frequency of information hiding, to prevent the process of information transmission made illegal user attacks, to provide security for data transmission. However, link pricing requires synchronization of cryptographic devices at both ends of the link, which will have an impact on network performance and slow data transmission. The link between two network nodes, the link encryption can effectively guarantee the security of computer network information data. In the link encryption process, the information transmission will be encrypted many times. A network message usually passes through multiple communication links. Because of the different types of single communication message is decrypted after data will be encrypted, so the information content in the data link road will produce, in encrypted mode will be reached if things go on like this link encryption, message transmission source coverage and transmission news coverage. In order to ensure the security of the information in the transmission process, the information data is encrypted on the network communication link, which is also called online encryption. In the process of data transmission, use a different key information transmission time information encryption and decryption, encrypts the data before transmission, in the process of transmission in network nodes after decryption, using different encryption keys again. Link encryption, through repeated encryption and decryption, seeks to transfer data to absolute security.

Node Encryption Technology. The node encrypts all data to decrypt and re encrypt it at the node, so as to protect the data security in the communication process. Unlike link encryption, encryption of data node after node is not in plaintext form, with a security module node, and the node connection module, data decryption and encryption process in security module, which can effectively avoid the safety problem of data decryption process. Due to the need to develop data encryption processing way node encryption, data transmission and arrival process or in the form of plaintext transmission, so the data has not arrived at the node or node into the receiver through this stage vulnerable. There is a big difference between node encryption mode and link encryption mode, node encryption technology cannot allow the relevant messages in plaintext form in network nodes, the node will receive the message encryption decryption depth, then based on applied on different stage operation again secret key encryption, is based on the operation mechanism of node security this module in the process of operation. The technical requirements of the header and the road information should be existed in the form of plaintext encryption security data network node, it will give the intermediate node to provide reliable and scientific information processing approach, so the node encryption technology to curb cyber attackers of communication services is relatively weak link analysis. Node encryption technology defects, encryption equipment level to achieve a high degree of synchronization in the actual operation in the link node need both ends of reasonable protection, and reasonable coordination to complete the final encryption operation, overseas information data loss and special conditions of information data loss phenomenon has occurred.

End to End Encryption Technology. End to end encryption, data transmission from the point to the receiving point, are presented in the form of text, encrypt the data before transmission, transmission process does not decrypt or encrypt again, until the data is transmitted to the corresponding receiver, receiver using the secret key to decrypt the data, to recover the plaintext state. Compared with the other two modes of transmission, end-to-end encryption has some advantages. First of all, it will not be transmitted because of the damage of a node. Secondly, the design and use of end-to-end encryption is relatively simple, and the transmission cost is low. Again, end-to-end encryption does not require much synchronization of the device. Its disadvantage is that it can not conceal the defects of the transmission point and the receiving point. End to end encryption technology has the characteristics of low cost, simple technology and convenient maintenance. End to end encryption technology in the practical application process, other users can normally use the

computer network and will not be adversely affected, but the end-to-end encryption work is the most important need to do security work. End to end encryption systems are cheaper and are more reliable, easier to design, implement, and maintain than link encryption and node encryption. End to end encryption also avoids synchronization problems inherent in other cryptographic systems because each packet is encrypted independently. Therefore, a transmission error that occurs in a packet does not affect subsequent packet packets. From the user's intuitive sense of security requirements, end-to-end encryption is more natural. A single user might choose this encryption method so as not to affect other users on the network. This method only requires the source and destination nodes to be kept secret. Therefore, in the study of improvement and innovation, these two aspects need to be further deepened.

Conclusion

Nowadays, network applications are becoming more and more widespread. Network t is an important tool to transmit information. It is very significant to do well the work of network communication. Therefore, we should not only be good at using data encryption technology to effectively prevent the virus, but also to strengthen network security management to make the network more secure and reliable.

References

[1] Shao Kangning, Research on Data Encryption Technology in Computer Network Communication Security [J]. Cyberspace Security, 2016(2): 29-32.

[2] Wang Xiucui, The Application of the Data Encryption Technology in the Network Communication Security [J]. Software Guide, 2011, 10(3): 149-150.

[3] Yu Guangxu, Computer Network Security in the Use of Data Encryption Technology [J]. Computer Knowledge and Technology, 2013, 9(6): 1338-1339+1348.

[4] Zhang Tao, Application and Research of Transmission Encryption Technology of Wireless Network Data [J]. Wireless Internet Technology, 2015(19): 16-17.