Research on Computer Network Security Based on Data Encryption Technology

Yicong Zhang[1,a], Shujun Zhou[2,b]

[1] ZhuHai College of JiLin University, 519041 ZhuHai, China
[2]Department of Computer Science and Technology ZhuHai College of JiLin University , 519041 ZhuHai, China
[a] 8176156@qq.com [b] 18224683@qq.com

Keywords: computer network security, data encryption, Software Encryption, Virtual Private Network

Abstract: The internet is facing many crises and difficulties in the rapid development period. More and more people begin to pay attention to the problem of network security. The most effective strategy is to use data encryption technology to protect the safety of the network. Data encryption technology is divided into symmetric encryption technology and asymmetric encryption technology. Applied in the areas of computer software encryption, internet electronic commerce and virtual private network, the data encryption technology effectively safeguards the computer network security.

1. Introduction

Network security mainly refers to the thing computer hardware and software and the contents of the memory can be saved in a relatively safe network environment, which is not affected by any external program to prevent all resources from viruses. Network security management can effectively achieve the protection of network resources, so that its security level has been continuously improved. One of the reasons for computer network security threats is the vulnerability of computer operating system itself. Network applications are operating on the computer operating system as a carrier. Hackers are using computer operating system vulnerabilities, in the process of network running applications, steal information of user data. It will affect the normal operation of serious computer virus invasion probability increases. The spread of computer virus spread quickly, causing great damage to the computer system, the user's information data cannot be guaranteed. Therefore, the computer operating system to improve and update the design to be reasonable, and ensure its safe operation, better defense network attacks, prevent virus invasion, to provide protection for user information and privacy. There are many security vulnerabilities in web applications and web site, log in web applications and web interface, does not require a user name and password login, but through illegal means to enter into the network login, you can program or web site system, which will form a very big security hidden danger. The destruction of network protocol and the transmission line attack will lead to network security protocol vulnerabilities, vulnerable to virus attacks and intrusion. Validation vulnerability attacks are the use of loopholes in the program, the attack on the network database, thereby stealing user information. Will steal the user information into the login interface, the system cannot determine the authenticity of the identification. It is often judged as legitimate users, leading to illegal users into the system.

2. Concept and Categories of Data Encryption

2.1 Concept

Data encryption technology refers to the application of related techniques in cryptography will be a plaintext encrypted key and encryption function, to replace or shift it, making it hard for others to read. It becomes meaningless for the cipher text information receiver, can use the decryption key and the decryption function of reducing cipher text, thus achieving the hidden information transmission. This is very important for the core technology of computer network data security. Traditional data encryption methods include permutation table algorithm, improved permutation table algorithm, cyclic shift algorithm and cyclic redundancy check algorithm. Computer data encryption technology is to add a certain amount of data to the program, if the input key cannot be consistent with the content of the key set, the data will be converted to no practical meaning of the text. If the input key is the same as the set key, the data can be opened smoothly without any change. The research of data encryption technology is to study the key program of the data, the program is complicated, and the difficulty of the hacker is increased to ensure the absolute security of the network information.

2.2 Categories

The common data encryption technology is divided into symmetric encryption technology and asymmetric encryption technology.

Symmetric encryption technology, also called shared key encryption, refers to the information sender and receiver use the same key for encryption and decryption of data, which requires communication before the safe transmission of cipher text must agree on a public key. Therefore, the security, confidentiality and integrity of the data can be ensured only if the key is not compromised by both parties. Symmetric encryption algorithm is an earlier encryption algorithm, the technology is mature. In the symmetric encryption algorithm, the data sender sends the plaintext and the encryption key together with the special encryption algorithm to make it into a complex encrypted cipher text. If the recipient receives the cipher text, if you want to interpret the original text, you need to use the encryption key and the same algorithm to decrypt the cipher text. In the symmetric encryption algorithm, only one key is used. Both of them using the key need to know the encrypt data in advance. The workflow of the symmetric encryption is shown as follows:

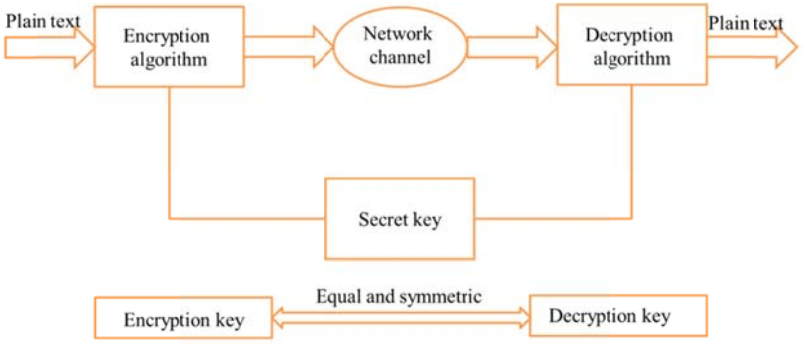

Figure 1 Diagram of symmetric encryption

Asymmetric encryption is also called public key encryption. It means that the sender and receiver use different keys to encrypt and decrypt the data. The keys are divided into public key and private key. The asymmetric encryption technology is based on the key exchange protocol, and the two sides of the communication can communicate with each other directly without changing the key. If the public key is used to encrypt the data, only the private key can be decrypted with the

corresponding private key. If the data is encrypted with the private key, only the public key can be decrypted. Because encryption and decryption uses two different keys, this algorithm is called asymmetric encryption algorithm. Compared with asymmetric encryption and asymmetric encryption, the security of the communication is better: symmetric encryption both use the same key, if one side of the secret key was leaked, then the entire communication will be cracked. The asymmetric encryption uses a pair of keys, one for encryption and decryption. In addition, the secret key is stored by the users. The workflow of the asymmetric encryption is shown as follows:

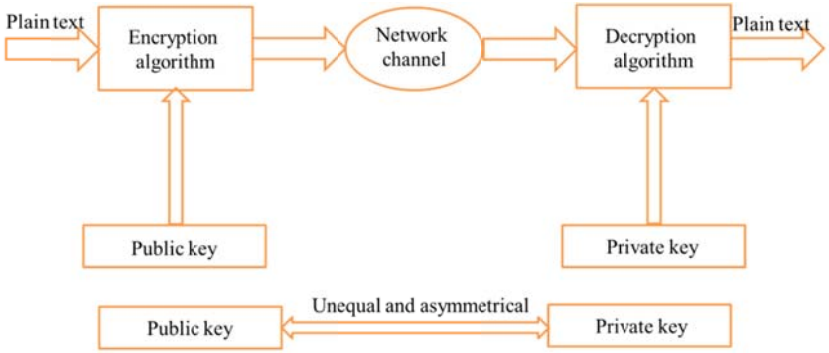

Figure 2 Diagram of asymmetric encryption

3. Applications Areas of Data Encryption Technology

3.1 Computer Software Encryption

The computer in the process of operation, software and procedures are likely to be hackers. The application of encryption technology in encryption software can effectively prevent the vicious attacks. The operator is required in the process of system operation, strict monitoring of the encrypted files and timely processing of being a virus or illegal program files, to avoid the spread of the virus to affect the safe use of the network. Encryption software in the application of data encryption technology, computer software and programs can help the normal operation. As in the process of communication, it can be applied to data encryption algorithm for data encryption: first of all, not only can significantly improve the effectiveness of data protection, effectively prevent the illegal theft of data and break the communication, and also can help the algorithm can effectively prevent data tampering in the unconscious environment; secondly, data encryption algorithm the complex, used in computer communication technology can effectively meet the application requirements, while the decoding difficulty is relatively large, can significantly improve the communication data security. The use of computer software is an integral part of, in the daily use of computers, computer software most commonly invading viruses and hackers, because the software design flaw are most likely to suffer from virus and hacker intrusion. The application of data encryption technology in software can effectively block the invasion of computer virus and hacker. During the execution of encryption, encryption operator must detect encrypted data to avoid files hidden in the virus, if detected virus, integrity and confidentiality must be processed and detection software, data and system, to curb the spread of the virus. Therefore, the application of data encryption technology in software encryption plays an important role in the protection of computer network security and information data.

3.2 Internet Electronic Commerce

With the rapid development of e-commerce, the modern society is more information, people's daily work and life style has changed greatly. Electronic commerce to network as the carrier, the network platform in order to carry out the transaction, so the electronic commerce network is unable

to get rid of various risk factors exist, if not effective use of encryption technology, all kinds of privacy information in the transaction will easily be stolen criminals, resulting in significant loss of both parties, both sides continue to cooperate reputation and influence the possibility of. The network security and transaction information also affects the electronic commerce transaction security, the use of digital certificates, instant electronic payment security protocol encryption and digital signature data, can improve the environment of computer network security, security related information of the transaction security. E-commerce has become the mainstream mode of the current business transactions. The corresponding social information is also developing rapidly. Our work and life has played a very significant impact. Operation and transaction of electronic commerce is based on the network platform, so the stability and security of the network is based on the premise of electronic business operation; in the process of operation and transaction, there is a certain risk. The huge user information in the transaction process, not processing encryption technology, is bound to cause information leakage. The two sides of the transaction will have a certain effect. The advantages of data encryption technology can effectively ensure the safe operation of e-commerce in the network platform. The common encryption algorithm used in the electronic commerce is the ElGamal encryption algorithm. The safety of the ElGamal encryption algorithm lies in intractability of elliptic curve discrete logarithm problem. We randomly select a big prime number p (200 bits decimal number) and a number of g (1<g<p-1). The numbers of p and g are public for every user. The encryption process is shown as follows: firstly, we find out the public secret key E=(y) in the public secret key database; secondly, we randomly select an integer k (1<k<p-1) and C1=gk mod p, C2=ykM mod p; finally, the (C1, C2) is send to the user U as a clear text. The decryption process is to calculate M=C2(C1x)-1 mod p.

3.3 Virtual Private Network

At this stage, many enterprises have set up their own local area network. Due to the establishment of branches in different places, the need to hire a dedicated route to achieve the unity of the local area network in order to form a wide area network. In the virtual private network, the value of data encryption technology is that the data from the sender's virtual private network automatically through the router to encrypt the hardware, and then the data in the form of cipher text to the internet. When the cipher text reaches the specified virtual private network, its router will automatically decrypt it. Virtual private network recipients can read plaintext. The user access virtual private network gateway through a virtual private network client, the client first two factor authentication for user password, use virtual private network client that users have a digital certificate and the certificate at the same time using digital certificate technology, bidirectional authentication to complete the virtual private network gateway server and user identity after the gateway server a symmetric session key, and distributed to the user and the virtual private network gateway server communication, encrypted authentication and session key protection in the process of transferring the security of information using the session key, mainly through non symmetric encryption algorithm to complete. Virtual private network system not only to authenticate the identity of the user, but also on the system transmission data transmission in the process of certification, confirmation message has been sent all the virtual private network system Hash abstract algorithm for all the data transmission encryption to realize digital signature, effectively ensure the integrity the data in the transmission process, to prevent others from tampering.

4. Conclusion

The popularization and application of computer network have brought great convenience to the daily life. At the same time, the issues of computer network security become particularly important. The application of data encryption technology greatly improves the security of computer network.

Data encryption technology is used in various fields of society, effectively eliminating the computer network security threats and protecting the fundamental interests of network users.

References

[1] Zhu Wenya, A study on the application value of data encryption technology for the network security, Manufacturing Automation, 34(3), pp. 35-36, 2012.

[2] Ni Dong, The Research on the Application of Data Encryption Technology in Computer Network Security, Journal of Jining Normal University, (5), pp. 36-40, 2016.

[3] Zhao Kejia, Data Encryption Technology in Computer Network Security Application Inquiry, Information Security and Technology, (12), pp. 81-82+85, 2015.

[4] Lin Hai, The Application Value of Data Encryption Technology in the Network Security, 7(12), pp. 154156, 2016.