

Analysis of Computer Network Security Problems and Countermeasures

FengJiangxi Technical College of Manufacturing, Nanchang,330095

Keywords: Computer network; Network security; Network attack; Counter measures

Abstract. With the continuous advanced of the information, digital and network society, the computer network has gradually become an indispensable aid in people's modern life, and security of computer network is becoming increasingly important. The development of computer network technology not only brings great convenience to people's life today, but it is also difficult to avoid a series of security risks. If the security risks are dealt with in a timely manner, it is bound to lead to the emergence of computer application barriers. Thus it can be seen that it is of great practical significance to study the status quo of computer network security and develop effective strategies.

Introduction

With the development of information technology, the application of computer network is becoming more and more extensive, and the security problems are receiving more and more attention. Whether it is at government sectors, schools and companies, there are sensitive data within the system that need to be protected. And the computer network has the form of connection diversity, terminal distribution inhomogeneity and network interconnection, openness and other characteristics, so that the network vulnerable to hackers, malicious software attacks, so the security and confidentiality of network information is a very important of the subject. Therefore, to ensure the integrity of network information, availability and confidentiality, network security measures must be able to respond to their own vulnerability and a variety of network threats. This paper starts from the security of computer network, and discusses the security of computer network. This paper analyzes the common attack methods such as virus attack, system vulnerability attack, spoofing attack and hacker attack, and discusses the access control strategy, information encryption strategy, virus attack coping strategy, system vulnerability attack strategy, hacker attack coping strategy. And the conventional cryptographic algorithm and public key cryptography algorithm are analyzed.

Types of Computer Network Security Threat

Network threats are potentially exploiting network security flaws that could lead to unauthorized access, information disclosure, resource depletion, resource theft, or destruction. Network security faces threats from many sources and changes over time. There are several types of cyber security threats:

Physical Threat. Including theft, espionage, and identification errors. At present, computer theft has also occurred, especially with the important documents of the machine, making it easy to have illegal acts of theft, resulting in unnecessary losses.

System Loopholes. Including unsafe service, configuration and initialization. System vulnerabilities can easily cause network security threats, to regularly check the system, update the system patch, which can be a good way to prevent vulnerabilities and security threats.

Identity Threat. Including non-comprehensive consideration of algorithm, free password, password crack and password trap. People sometimes need to use the username and password to use the Internet, and at this time, password setting is particularly important and cannot be arbitrarily set. Therefore, there should be a certain degree of difficulty, thus playing a protective role.

Threat to Cable Connection. Including dial-in entry, impostor and eavesdropping. Eavesdropping occurs in cable threats, and in a broadcast network system, each node reads data from the Internet, such as eavesdropping, installing monitors, and so on.

Harmful Programs. Including viruses, trojans, updates or downloads. With the increasing degree of people's dependence on computer systems and the network, computer virus has posed a serious threat to the computer system and the network. Because the various devices in the network

system are interconnected, if a device is attacked by a virus, it may affect the entire network. The virus is destructive, hidden, infectious and communicable, latent and unpredictable.

Current Status of Computer Network Security

In fact, there are various factors that have varying degrees of influence on the computer network, including not only the computer network itself, but also issues with the computer loopholes. Besides, they are also related to the network users to certain degree. On the specific situation of computer network security, existing problems to the network security are mainly in the following aspects:

Poor Safety Supervision. In addition to enhancing the security of computer network, there should also be a powerful supervision system. As is known to all, good supervision can eliminate many hidden dangers and lift network security. At present, there is still a large gap in the security supervision of computer network and there is no scientific and effective regulatory evaluation mechanism, which brings risks to the safe operation of computer network.

Problems with the Network. Most of the current computer network systems have loopholes, and network hackers take advantage of network loopholes to attack the computer system wantonly so as to achieve remote operation, posing threats to computer network personnel. The main reasons for the above problems are:

(1) Extensibility and stability are limited. In the early stage of the design of the network system, due to the lack of comprehensive consideration, resulting in the computer system in the normative and rationality of the existence of different loopholes in the operation of the network system had a direct impact;

(2) Vulnerability in network file server. File server is the computer network hub, the operation of this server on the computer network operation has a greater impact. From a practical point of view, many designers in the design process without the need for network applications to fully consider the lead to unreasonable and imperfect existence, the impact of computer network security;

(3) Vulnerability in the use of the network system. In the provision of switches and firewalls and other equipment, the corresponding lack of standard specifications, for the corresponding level of security and data needs to deploy the network, and then the computer network fast and safe to balance, thus we should have a deep reflection on this.

Protection Strategies of Computer Network Security

Secure Encryption. Encryption technology provides security guarantee for users to carry out e-commerce and also allows users to feel assured about online transactions. With the continuous development and improvement of information technology, asymmetric encryption and symmetric encryption is the mainstream of the development of security encryption technology. The so-called symmetric encryption is mainly password-based encryption technology while decryption and encryption need to use the same password key.

Network Firewall. Network firewall is a technology mainly controlling access to the network. Firewall is used to prevent hackers to get into the network through illegal means so as to obtain resources and data within the network, thus protecting the network interconnection equipment and the internet network environment. The firewall mainly checks various network transmission data through relevant security measures so as to determine whether to allow access to network communications and dynamic monitoring of the network status.

Network Address Translation. Network address translation is to completely retain the IP address, and then provided to the private network for re-use, which allows an address in the Internet. At the same time, it can also be combined with the firewall technology, hidden in other IP addresses, resulting in that external networks cannot access the internal equipment. Network address translation can also break the address restrictions with reasonable arrangements for network address use.

Network Virus Prevention. The network environment has the feature of openness. Viruses attack users' computer in a variety of forms with great destructive power and threat, and they may even bring catastrophic damage to users. Therefore, to prevent viruses is a key link in network security. Network virus prevention technologies mainly include the detection of viruses and prevention of viruses, in which the detection of viruses is to detect the virus poisoning features of a computer so as to judge whether the computer gets virus, such as keyword and self-checks, etc. Prevention of virus is to effectively control the system through the system's memory, judge and detect whether the viruses have invaded into the system so as to prevent the poisoning and damage to the computer.

Security Management. In the network system, there is no absolute reliability and security. Therefore, to develop a sound management system is a key premise to guarantee the network security. Only when users and managers work together and use all the available network security technologies and tools can it be possible to effectively control the network security and prevent invasion of viruses and hackers.

Conclusion

With the development of the Internet, the computer network security is becoming increasingly important. Because of the openness of the computer network, the network is vulnerable to various attacks and destruction. Whether in the local area network or the wide area network, there are natural and man-made and many other factors to form the potential security threats. When we use the network, we should pay particular importance to the network security issues, from their own start, standardize the Internet behavior, not free access to unknown sites, the establishment of network rules and regulations, so that the entire network to a safe and stable environment. In short, network security is a big system engineering. Due to the sharing of the network and the security defects of the communication, the data information transmitted on the Internet is easy to leak and be destroyed, the network is very serious security attack, so the establishment of a more effective network security system is even more urgent.

References

- [1] Wang Z. Design and realization of computer network security perception control system[C]// IEEE, International Conference on Communication Software and Networks. IEEE, 2015:163-166.
- [2] Guo J C, Fan D, Che H Y, et al. An approach to network security evaluation of computer network information system with triangular fuzzy information[J]. Journal of Intelligent & Fuzzy Systems, 2015, 28(5):2029-2035.
- [3] Shao K N. Research on Data Encryption Technology in Computer Network Communication Security[J]. Information Security & Technology, 2016.
- [4] Liu Z, Amp S V. Computer network information security and protection strategy[J]. Electronic Test, 2016.
- [5] Sun Y. Study on computer network security evaluation based on support vector regression machine[J]. Modern Electronics Technique, 2016.
- [6] YihebaguliWusimanjiang. The main hidden danger and management method of computer network security[J]. Electronic Test, 2016.
- [7] Zhao J. Neural networks applicated in computer network security evaluation and reliability analysis[C]// International Conference on Advances in Mechanical Engineering and Industrial Informatics. 2016.
- [8] Liu X. Application of Neural Network Model Combined with Fuzzy Theory in Computer Network Security[C]// International Conference on Electronics, Network and Computer Engineering. 2016.
- [9] Liu Z, Zheng X. Analysis and Discussion on Computer Network Security Issues[C]// International Conference on Machinery, Materials, Environment, Biotechnology and Computer.

2016.

- [10] Wager R, Yarochkin F, Dahlgren Z. Recursive multi-layer examination for computer network security remediation[J]. 2017.
- [11] Zhou X Z, Xin L I. Computer network security technology in molybdenum mining field of applied research[J]. World Nonferrous Metals, 2016.
- [12] Zhu L S. Computer network security precautions in the process of metal metallurgy analysis[J]. World Nonferrous Metals, 2016.