Computer Network Security Analysis Modeling

Xue Zhao

Guangdong University of Science & Technology, Dongguan, 523083, China

77188649@qq.com

Keywords: computer; network; security; analysis modeling

Abstract: Computer networks have become more and more important in people's lives. People are increasingly relying on computer networks in their work and life. Some criminals come to nothing and attack computer networks to steal the property of others. It poses a greater threat to the lives and property of the people. Since computers often hold important work and living information, once the information is stolen, the consequences can be imagined. With the increasing complexity of computer technology, the effect rate of its model has been greatly reduced, which has severely hindered the exertion of its role, resulting in frequent computer security accidents. This article mainly analyzes the current computer security environment in China and discusses the maintenance of computer network security.

1. Introduction

The ultimate goal of security research is to establish a security model for security analysis. The establishment of this model is based on the system resources and security factors of the computer network. According to the different needs of security, classify and determine the main threat. In fact, this model already exists, but with the rapid development of the Internet, this makes the resistance of the original model greatly reduced. Therefore, the research on computer network security analysis modeling needs to continue to deepen.

2. Status of computer network development

2.1 Computer network security

Network and information security are hot topics in the field of communications and computers today. Computer network security refers to the security of the Internet formed on the basis of electronic computers and the information security contained in each network system based on the main network. The purpose of network security is to ensure that static and dynamic data are protected from malicious attacks. The data in the computer will not be stolen or tampered with, ensuring the security of the entire computer network. The definition of the International Committee for Standardization of Computer Security is: for the data processing system and the technical and management security protections taken, the protection of computer hardware, software, and data is not subject to destruction, alteration, or disclosure due to accidental or malicious reasons. The definition of the National Computer Security Center of the US Department of Defense is: To discuss computer security, we must first discuss the statement of security requirements. In general, a secure system will use certain specialized security features to control access to information. Only appropriately authorized people, or processes conducted on behalf of these people, can read, write, create, and delete this information. The definition of the Department of Computer Management Supervision of the Ministry of Public Security in China is: Computer security refers to the security of computer assets, that is, computer information system resources and information resources are not threatened or harmed by natural and man-made harmful factors.

For the definition of network security, the definition of computer system security by the International Organization for Standardization (ISO) is: the security protection of the technology and management established and adopted for data processing systems. The protection of computer hardware, software, and data is not caused by accidental and malicious reasons. To destroy, change and leak. From this, the security of the computer network can be understood as: through the adoption of various technologies and management measures, the network system can operate normally, thereby ensuring the availability, integrity, and confidentiality of the network data.

2.2 Computer network security status

At present, computer network communication is widely used. People use computer networks to achieve a high-skilled life mode. Compared with traditional life modes and work, their efficiency and accuracy have been greatly improved. It has increased the communication between individuals. Frequency has expanded the personal circle of communication[1]. At present, the analysis of computer network security is mostly carried out from various aspects such as protection strategy, recovery and detection, and on this basis, a PPRRR network security model is established. This model is used in traditional network security information assessment and analysis. On the basis of the above, for the establishment of different characteristic networks, it can achieve the most effective assessment, analysis and measurement, and ensure the effectiveness of overall information security. This model is an active defense model. Control security and information security are two important components of network security. Control security refers to real-name authentication, authorization, access control, and so on. However, in the internationally standardized organization system, information security refers to the availability, completeness, confidentiality, and reliability of the information. Since its development, the network environment has encountered security threats from all walks of life, whether it is control security or information security. The main ways that computer networks are subject to security threats are as follows.

2.2.1 Computer virus infection

Some financial institutions, banks, etc. are often attacked by hackers. The emergence of computer viruses also poses a great threat to the safe operation of computers. The early days of computer viruses, "panda burn incense," are still people's minds.Figure 1 below shows the computer's internal conditions after being infected by the “Panda Panda” virus.

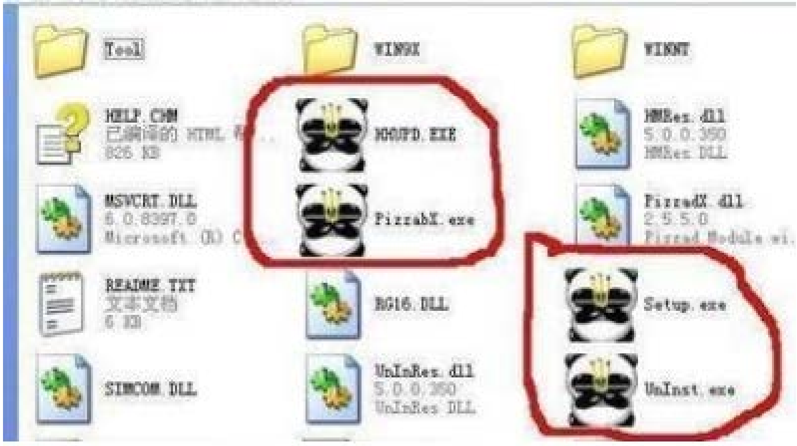

Figure 1 "Panda burns incense"

2.2.2 The network itself lacks a sound defense capability

Today, some networks and applications are still in an unprepared state, and people have limited knowledge of network security knowledge and a greater probability of network danger[2].

2.2.3 Domestic computer technology now lags behind

Although it has now entered the modern society, but in China's information technology research and development, basically rely on some advanced foreign technology and professional equipment, whether it is hardware or software, lack of independent innovation research and development efforts.

3. Computer network security analysis

3.1 Computer network security attributes

The computer network has the same basic security attributes as the social organization system. It includes the security needs of the computer network, the corresponding system devices, the strict network permission settings, and the modeling of the main body connection relationship.

First, the need for security is based on the premise of confidentiality of information in the user's system, and it satisfies as much as possible the user's usability and security needs[3]. Second, the corresponding basic system equipment means that the computer network system is made up of components made of different equipment components, and its internal functions are also different, including hosts, routers, and central servers. Different devices play different roles. Features. Third, the strict network access permission setting means that in the network operating environment, the computer network implements different permission settings for different users, usually including Root, Superuser, and Guest. Fourth, the modelling of the main body connection relationship is a relational model established by the Internet based on the TCI/IP protocol. At present, the basic protocols of the computing network system used throughout the world are developed.

3.2 Problems with the current model

Existing computer Internet models classify the security level, but there are still some problems in the classification of their levels. In particular, the basic network related equipment has not been given adequate attention. This leads to the network security system in the basic field. There are shortcomings, especially as the basic routers and switches of network equipment. They are simple in structure, convenient in network access, have no internal security protection mode, or have simple security protection modules.

Specifically, the existing problems in the current model mainly include the following four aspects. First, TCP/IP is very fragile. The cornerstone of the Internet is the TCP/IP protocol. Unfortunately, the agreement does not consider much about network security. And, because the TCP/IP protocol is publicly available, if people are familiar with TCP/IP, they can use its security flaws to implement network attacks. Second, the network structure is not secure. The Internet is a kind of inter-network technology. It is a huge network connected by numerous LANs. When people use one host to communicate with hosts on another LAN, the data flow between them is usually heavily forwarded by many machines if the attacker uses a host on the user's data flow path. He can hijack the user's data packet. Third, it is easy to be eavesdropped. Because most data streams on the Internet are not encrypted, people can easily eavesdrop on e-mails, passwords, and transmitted files on the Internet by using tools provided free of charge on the Internet. Fourth, users lack security awareness. Although there are many security protection barriers in the network, people generally lack security awareness, which makes these protection measures useless[4]. For example, if people want to avoid extra authentication of the firewall proxy server, a direct PPP connection is made to avoid firewall protection.

3.3 Factors affecting overall computer network security

At present, the factors that affect the overall computer network security include the following: First, network information is prone to leaks, and is used for tampering and illegal transmission. At present, due to technical problems and equipment problems, the computer network is full of loopholes. The key data in the computer is easily eavesdropped or controlled, and even problems such as information alteration and interception occur. Second, there are security loopholes in the computer network itself and loopholes in some development software. It is a core factor affecting computer network security. There are obvious loopholes in the two major components of the computer, which will lead to the emergence of user resources and key information. Leakage will expose users to unprotected malicious attacks and be easily controlled. Third, with the development of modern Internet technologies, hackers' aggression is also intensifying. Hackers search for and search for the Internet for a certain benefit and purpose, to find loopholes in the Internet, and use loopholes to steal user information.

4. Computer network security analysis model

Using security factors hidden in the computer network, and based on the calculation of security attributes, establish a computer network security analysis model. At present, the existing computer network security analysis and modeling are based on the nature of the network as the starting point for analysis, to grasp the potential defects in the computer network, and use the transposition mode to simulate the network attacker offensive route, so that the overall The security of computer networks is analyzed to fundamentally improve the security level of computer networks. The main computer network analysis models include two types:

The first is the topology model. It is a model constructed with the aid of physical models. It is based on the existing computer resources and uses computer or related information transmission equipment to form media points, thus realizing the point and line structural model. This model must rely on the connection point between the computer network equipment and the network connection relationship in order to realize the final computer network analysis and realize the final computer network transformation [5]. In the computer network, the device should be identified by the IP address and the device name, and the security of the computer network should be effectively improved from the basic device. In the topology model, the core point is to achieve the link between the media and hardware devices, in order to complete the link between the device and the media.

The second is the attack model. At present, the factors that affect the security of computer networks are diversified. Among them, hacking attacks are the main factors. Therefore, in order to improve the security of computing networks, hacking routes should be taken as the starting point and access to computing networks should be granted. , attack attributes and other elements are analyzed and strengthened. Starting from the access rights, it comprehensively monitors user information and resource types managed by system administrators to implement network information protection for administrators; monitors the management contents among various levels, controls the underlying access rights, and increases the trust of the firewall. Degree; establish Trojan horses, prevent viruses, strengthen protection against hackers, establish effective protection models, and strengthen weaknesses.

5. Conclusion

Computer network security issues have gradually entered people's field of vision. In general, network security is not only a technical issue but also a security management issue. We must consider security factors in a comprehensive manner and formulate reasonable goals, technical solutions and related supporting laws and regulations. Absolute security of the network system does not exist, computer hardware and software are constantly upgrading, and the requirements for computer network technology are getting higher and higher, and network security technology is bound to advance with the development of network applications. Therefore, modeling security analysis from multiple perspectives can provide a new security model for the future and provide strategies and lessons for improving computer network security.

References

[1] Zhang Tao; Hu Mingzeng; Yun Xiaochun; Zhang Yongzheng. Research on Computer Network Security Analysis Modeling[J];Journal of Communications;2005-12

[2] Zhang Tao; Hu Mingzeng; Yun Xiaochun; Zhang Yongzheng. Research on Computer Network Security Evaluation Model[A];2005 New Development in Communication Theory and Technology——Course of the Tenth National Youth Communication Conference[C];2005

[3] Jing Weiliang. Research on network security assessment technology based on attack graph[D];Harbin Engineering University;2008

[4] Hu Jian. Design and Implementation of Investigation and Analysis Subsystem of IMS Network Vulnerability Assessment System[D];Beijing University of Posts and Telecommunications; 2010

[5] Cheng Liansheng. Discussion on Computer Network Security Technology[J];Science & Technology Innovation Herald;2009-07