Research on Security Management of Computer Network System

Jun-sheng Ma[1, a], Tie Ma [1,b] , Hui Li[1,c] , Xiao-ting Li[1,a] and Jun-qiang Yang[1,b]

[1] Department of Network service, Xi'an Communication Institute, Xi'an 710106, China

[a]51375908@qq.com, [b]813086903@qq.com, [c]583822272@qq.com

Keywords: Computer Network System, Security Management, Security Policies

Abstract: With the rapid development of network science and technology, people are dependent on the network and usage greatly improved, but the network to bring convenience, but it also brings a lot of network security issues, it has become a constraint computer network construction greatest limiting factor. This paper describes the impact of the computer network system security management of specific issues, according to the system requirements of practical application, in terms of the system operating environment, hardware systems, software systems, network systems and system data, such as design of the computer network system security policy and implementation are discussed. Through the computer network security threats faced by the system proposed safety management, regulations are important to ensure the development and implementation of computer network system security. Proposed computer network system security management strategies, we hope to enhance the computer network security have some help.

Theoretical Introduction of Security Management

Network security refers to the various components of the digital network system from accidental or malicious reasons destruction, alteration, and disclosure of, and mechanisms to ensure continuous digital network system normal operation, the ultimate aim is to achieve a digital network information processing and transmission process to maintain reliable confidentiality, integrity, availability and controllability. The development of the entire system is very complex, involving various computer and network technology, so that the various functions needed by campus computer network security management can be achieved, including network monitoring, equipment management, user management and fault management and so on.

Network security features include: confidentiality. Ensure that the information on the digital network is not disclosed to unauthorized users or for its use; integrity. Prevent information from digital libraries unauthorized users from tampering with, namely to ensure that information is not modified in the storage or transmission, is not destroyed and missing features; availability. Ensure digital information and information systems used by authorized users do to prevent computer viruses or other man-made factors causing the network and the system can 't operate properly and denial of service or used as a rival [1].

Network system is secure against all kinds of threats to system security weaknesses in risk factors and systems from several aspects of the system design, equipment configuration, software application, system operating environment, take planning, control and a series of measures to prevent the system any form of damage, and after the destruction of the protection system can quickly resume normal operation. Therefore network authentication must be considered appropriate security means ,which are authentication integrity, non-repudiation of the information, replay attacks and transport security, also be considered to avoid the user's identity forgery, tampering, repudiation, posing, etc. authentication is the first hurdle of network security system, Fig.1 shows logical structure of the safety system.
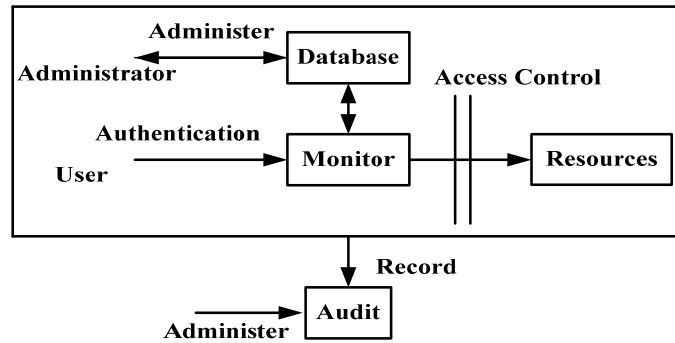
Fig.1. Logical structure of the safety system

The Basic Principles of Network Security System

For the safety in compute and its network system requirements include: Make sure the file and transaction information is not tampered with, information to be protected; personal information confidential; various data material can have timely access and so on [2]. Fig.2 shows the principles of network security system.
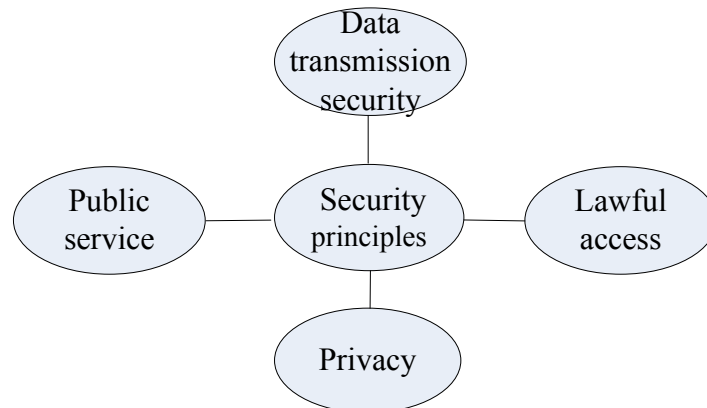

Fig. 2.The principles of network security system

The computer and network systems for use and access public services should be very convenient, and must be able to withstand a long uninterrupted run. The computer for public access and use is to provide readers with various public services, if the defect due to security measures, the inconvenience to the reader, or the reader does not need to provide timely press online search and other services, which will make service image libraries affected. When readers use the 's public computers, some personal information will remain on your computer, such as the local computer will record a web browser to access records, the proxy server will record the readers visited website addresses, leaving the reader when using a public computer systems files will be saved. More information to protect the privacy of legitimate readers should bear the responsibility.

Another new face is a legitimate question access to the computer and network systems. Since many libraries to provide access to Internet services to all readers, they must set up Internet access and filtering bad information and other issues. In addition, many libraries also offer services via the Internet to access the system and resources, the must use restrictions in accordance with the relevant agreements for such access is carefully controlled. Data transmission main purpose is to ensure the security of data transmission is not eavesdropping on the communication line, alteration and destruction, achieve this goal are the main technical data encryption and data integrity authentication techniques [3].

The Establishment of Security System

Computer network system according to the need of practical application, analyze the possibility of a variety of risk, and according to the degree of difficulty system and data recovery, combined with

factors such as investment funds, design a scientific, rational, careful and practicable the computer network security system [4].

Secure network system is the computer network system security key. Operation and service of digital resources information management system needs to rely on a network, but the public and open Ethernet protocol, resulting in a lot of security risks. Hacker attacks on the computer network system, the virus destroyed the vast majority from the network. Therefore, the development and implementation of effective network security policy is to protect the computer network system security is very important part. Information Management System is the most important application system, its security is directly related to normal operations carried out an open. Already high between the campus network and the external Internet, enterprise-class firewall as a barrier to outside hackers is difficult to carry out effective attacks on the 's the computer system, but the 's server if they are directly exposed to the campus network, campus network from malicious internal or mischievous attacks are difficult to prevent.

Libraries should adopt VLAN (Virtual LAN) technology, the server area, office area, a public inquiry machine area, according to the different areas such as electronic reading devices logically divided into different independent LAN segments. In this way, both to ensure the secure server area, but also facilitate the management of network addresses, but also reduce the network load, effectively preventing large LAN network problems caused by the storm. Computer network security management is a systematic project, which requires the decision-making, management, technology layers effort with proceed from the safety aspects of institution building and technical means to enhance information security awareness education and training to enhance self-protection awareness, take comprehensive preventive measures, and continue to improve and perfect the security management measures. To upheld awareness of security, and gradually adopt a comprehensive and feasible security measures to reduce security risks to a minimum.

Security Policies of Computer Network System

Once the network system being hacked, infected with the virus, hundreds of thousands or even millions of bibliographic information collection and distribution of information, the museum self-built database data such as lost or destroyed, the loss will bring disastrous. The computer network technology to achieve network security management system to ensure the safety of the network system, reliable operation, mainly includes the following aspects. Fig.3 shows the security policies of computer network system.
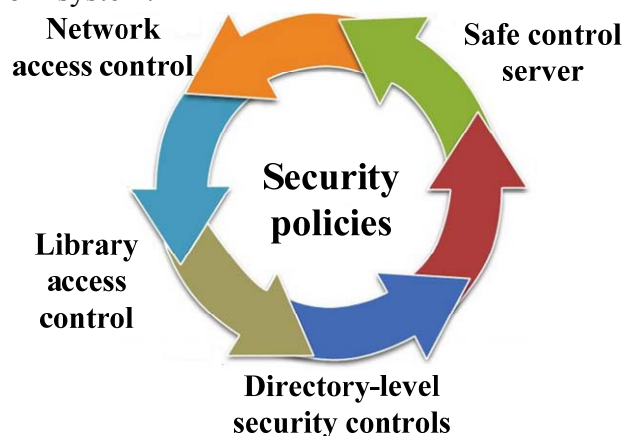

Fig. 3.The security policies of computer network system

Network Access Control can control the legitimate Internet users log on to the network server and access to network resources, control the time and manner permitted network user networks. Network users can access control can be divided into three steps: identification and verify the user name; identification and verify the user password; default user account limit checking. Permissions control network is a protective measure taken against the illegal operation network. Network users and user groups are given certain privileges, specify the network users and user groups which

directories, subdirectories, files, and other network resources can be accessed. With the development of computer and network technology, more and more rampant virus activity, therefore, maintain a good network system security, you need to choose a strong anti-virus, anti-virus capabilities and real-time monitoring capabilities of antivirus software [5].

Computer network system should allow the user access to directories, files, and other network resources. Network users in the directory specified level permissions to all files and subdirectories are valid, the user can further specify access permissions for subdirectories and files in the directory of the. Access to directories and files in general are: the system administrator privileges, read access, write access, create permissions, delete and modify permissions, search permissions, access control permissions. Server is a very important role in terms of management. Security control server includes the server console can set a password to lock to prevent unauthorized users to modify, delete or destroy critical information network system resources; server login time limit can be set, to detect and shut down illegal visitors intervals and so on.

Conclusions

The popularity of computer and network technology for the modern routine management and reader service work to bring convenience, while the computer network security systems have become the most important issue to be solved for each. In this paper, the basic principles of computers and network systems security, computer system security objectives elaborated, pointing out how to make computer security policies, and the implementation process should be continuously improved to meet the fundamental principles of the computer system security to achieve the goal of system security. Through the computer network security threats faced by the system proposed safety management regulations are important to ensure the development and implementation of computer network system security. Reliable network maintenance measures are taken from the system to the application, in order to ensure safe and efficient operation of the network system by a relatively complete of network security defense system.

References

[1] M.DIMOPOULOUM. An Automated University Course Timetabling System Developed in a Distributed Environment. A Case Study European Journal of Operational Research, 2004, 4(153):136-147.

[2] YANG WENXIANG, LYNCH, BEVERLY P. On Knowledge Management and the Role of the in the Process of Knowledge Management [J], Chinese Librarianship, 2006, (21): 10-11.

[3] AbadCL, Boni11aR1. An Analysis on the Schemes for Detecting and Preventing ARP Cache Poisoning Attacks.27Th International Conference on Distributed Computing Systems Workshops, Toronto, Oct, 2007: 60.

[4] Matthew Connolly．Mobilizing Web Presence and Services：A Student- Collaboration to Create Mobile Site and iPhone Application[J]．The Reference Librarian, 201 1(52):27-35.

[5] Daniel Chudnov. A Mobile Strategy Web Developers Will Love[J]．Computers in 1ibraries，2010(5): 24 -26.