Research on Potential Security Hazards and Defense Technology Existing in Colleges and Universities’ Campus Network

Lina Qin

ABSTRACT

At present, the constant development of network technology has gradually increased network users and network size. Network has gone deep into people’s daily life, study, work and other fields. In colleges and universities, the teaching trial network in traditional forms has been converted into operational network combined with scientific research and logistics service. The latter undertakes the important task of teaching, research, management and foreign exchange, lastly, not only provides convenience for education, but also plays a vital role on information construction in colleges and universities. Campus network in colleges and universities is the core carrier of transferring digitized information, so its efficient running is an urgent to be solved thing at present. However, campus network in colleges and universities always suffers from a variety of hazards such as natural disaster, loopholes in management, viruses, and so far as to its own defects in architecture. If the hazards cannot be paid close attention and solved as soon as possible, campus network will be running slowly, unsteadily and even fall into a paralytic state. Based on this, the paper lists defense technology against the existed security hazards as a standpoint, carries out the detailed research.

INTRODUCTION

In colleges and universities, campus network is constructed which provides teachers and students with teaching and research, provides administrators with
management and foreign exchange for information. All aspects of development cannot continue without campus network’s good running. Therefore, it is necessary to pay attention to security protection for campus network. The paper introduces potential security hazards existing in colleges and universities’ campus network, and lists defense technology to improve campus network’s security.

**POTENTIAL SECURITY HAZARDS WHICH EXIST IN COLLEGES AND UNIVERSITIES’ CAMPUS NETWORK**

**Potential Physical Security Hazards**

Security hazards caused by natural calamities specifically include earthquake, storm, flood, fire and so on. The security hazards belong to the category of physical security in network, are essential conditions to network system security. According to the related investigation and analysis, First and foremost, in our country, there are lack of measures such as preventing electromagnetic leakage, lighting protection, waterproof and fire prevention in colleges and universities’ computer rooms. Besides, the computer room’s grounding system is not reached a right location and has very poor ability to resist natural disasters, so safety accidents frequently emerge; Last but not least, the phenomenon that equipment damage due to power outages and data leakage caused by damaged or stolen equipment generally occurs. Therefore, it is necessary to set physical security countermeasures to avoid hazards caused by natural disasters[1].

**Management Loopholes Which Exist in Colleges and Universities’ Campus Network**

**CHAOTIC MANAGEMENT ORDER WHICH EXISTS IN COLLEGES AND UNIVERSITIES’ INTERNET PLACES**

In order to meet teachers and students’ requirements of sharing campus network resources, most universities provide them with computer rooms. However, because some colleges and universities lack consistency between monitoring and managing campus network, so computer rooms are in a chaotic state. In addition, as some computer rooms lack secure and effective registration management system, so it is difficult to achieve the goal of unifying users’ identification. Moreover, in order to manage and control computer rooms’ computer, managers install the recovery card into each computer. If the computer is shut, it is bound to return to its own initial condition, so it causes a lot of loopholes in managing campus network, for instance, workers cannot save Internet access log [2]. In short, the potential safety hazard is especially notable.
WEAK SAFETY CONSCIOUSNESS ABOUT THE CAMPUS NETWORK

In colleges and universities, construct the campus network is at an early stage, most of workers have weak security consciousness about campus network. From the perspective of analyzing campus network users, users are basically confined to the primary lever in applying computer, unable to correctly deal with the illegal invasion into network. However, in the process of constructing campus network, the relevant workers only concern to the network’s convenience and high efficiency, neglect improvement to network security, often do not to explore the actually existing low efficiency and security risks, lack the relevant knowledge and technology about keeping information privacy, managing password, fixing bug, preventing to modify data maliciously and damage the system [3].

LACK OF EFFECTIVE MEANS IN MONITORING AND SECURITY MANAGEMENT

In colleges and universities, campus network is mainly to provide teachers and students with services. For example, email system is the more commonly used application software; however, it is a key way to spread malicious remarks such as pornography, reactionary speech through email. Therefore, it is necessary to construct email system strictly. But, in fact the constructed email system is either a free version downloaded from Internet, either a generated version after modification. Only in individual rich colleges and universities, managers invest money to buy email system so as to attach their great importance to campus network, however the bought email system is in low security level because of their neglect of campus network’ hidden safety hazard. By this mean, it not only cannot protect campus network’ security performance, but also cannot effectively monitor and manage all letters which go through the campus network. In other words, it lacks effective means in monitoring and securely managing campus network.

Threats of Network Viruses

By the threat of network viruses, it is easy to reduce campus network performance so as to leak the internal important data in colleges and universities. With the rapid development of network technology, the level of creating viruses is more and more advanced. Besides, fusion of hacker software and network viruses is inclined to produce harmfulness network virus. In this case, it is inevitable to cause the leakage of campus network users’ privacy, cost more network resources and reduce network performance. In a word, it is very important to effectively avoid threats of network viruses. However, at the current stage, most of defense countermeasures against viruses in colleges and universities are limited to a stand-alone computer, it is unable to prevent network viruses from running rampantly [4].
Safety Defects of the Campus Network Architecture Itself

Security of the campus network architecture itself refers to security of application system and security of network operating system. At the present stage, whether it is UNIX or Windows operating system, the related developers usually have the backdoor to them, namely security vulnerabilities of the system itself. Security vulnerabilities are mainly caused by internal viruses, so it is important to use formal technology to remove viruses.

DEFENSE TECHNOLOGY AGAINST THE POTENTIAL SAFETY HAZARDS WHICH EXIST IN COLLEGES AND UNIVERSITIES’ CAMPUS NETWORK

Countermeasures in Physical Security

Countermeasures in physical security can prevent facilities and equipment on campus network from damage caused by natural disasters and illegal behavior. Countermeasures in physical security specifically include security in equipment and security in environment two aspects.

SECURITY IN EQUIPMENT

It is well known that natural factors cause flood, fire and electric leakage. In colleges and universities’ computer rooms, it is necessary to be equipped with fire-fighting facilities and waterproof measures for device interface and power socket. In addition, network lines are constructed technically by lighting-protection, resisting electromagnetic interference and preventing information from being intercepted. Lastly, it is necessary to prevent equipment from being destroyed and stolen artificially.

SECURITY IN ENVIRONMENT

Security in environment specifically refers that the current environment should be in the security protection such as disaster protection, regional protection, etc.
Perfect the Management on Campus Network

STANDARDIZE THE MANAGEMENT AND MONITOR TO INTERNET PLACES IN COLLEGES AND UNIVERSITIES

From the perspective of scientific research and teaching, the internet places should be broaden so as to provide convenient working and learning environment for teachers and students in colleges and universities. However, from the perspective of network security management, it is need to unify monitoring, identification, and the management software of computer room so as to ensure the overall safety of campus network.

At present, the management to internet places in most colleges and universities is often in its own state, namely different management system. It cannot correctly identify the online users, and is difficult to control malicious internet behavior. In addition, recovery cards are commonly applied to each computer room on campus, although it is easy to manage computer rooms, but increases the probability of hidden security trouble. According to the provisions of our country’s relevant departments, in colleges and universities’ internet places, it is need to save online log occurred at least the last three months [5].

STRENGTHEN NETWORK SECURITY CONSCIOUSNESS

In order to clear network security consciousness, in colleges and universities, it should specially create network security mechanism, formulate consistent rules and regulations, reasonably avoid potential safety hazards, and limit users’ illegal behavior on campus network. At the same time, it should try to control the threat of network viruses, strengthen to train campus network users for professional computer knowledge and maintenance staff for technical knowledge so as to effectively enhance their ability to cope with network risk, make network users install network security software consciously so as to achieve the purpose of safe access to the Internet.

PERFECT THE E-MAIL SYSTEM

In order to perfect the e-mail system in colleges and universities’ campus network, it is necessary to provide monitoring and safety management system to the potential safety hazards. At present, some colleges and universities apply cheap or free e-mail system on campus network, its performance and features could not meet the requirements of network security and users to the e-mail system, so it cannot effectively monitor e-mail system and filter malicious information in internet access log. All in all, it is necessary to introduce firewall with high performance to control external threats, normally which is set up between internal network and external network. In colleges and universities, firewall could isolate internal network from
external network, its three interfaces are respectively interface to external network, which connects router to the Internet; interface to internet network, which connects inside core switcher; interface to Demilitarized Zone, which connects external servers such as domain server, FTP server, WWW server and so on [6].

In the process of configuring firewall, colleges and universities’ network workers should strictly check the address, purpose, port and protocol of IP packets, in addition, configure the keyword filtering and sensitive address so as to prohibit illegal and unnecessary access to the campus network from external network.

Configure Systematic and Complete Security Equipment on Campus Network

From the perspective of campus network’s overall technical framework in colleges and universities, campus network belongs to the local area network. In order to avoid large-scale network attack, it is necessary to create unified monitoring equipment and network security management system on campus network and the interface to external network. At present, because of a high-speed campus network, in the process of accurately configuring security equipment, it is necessary to carefully analyze the campus network’s overall performance, concern about the adverse impact on network performance so as to realize the purpose of configuring equipment safely.

CONCLUSIONS

The defense work on campus network security in colleges and universities is a systematic and complete engineering. It is necessary to construct defense system in intelligent form so as to protect key information and data on campus network. At the same time, it is necessary to promote network users’ security consciousness and skill levels so as to create a civilized and healthy network environment in colleges and universities. In this way, it is possible to realize information construction and spread, achieve the steady and rapid development goal.

ACKNOWLEDGEMENTS

First and foremost, I would like to thanks my workmates Ning Han, Hongkai Lin for their help in investigation and requirements analysis. Besides, the campus network in Wuhan Business University as an experimental base plays an important role in this research. Last but not least, the research is funded by a Teaching and Research Project of Wuhan Business University (2015N025).
REFERENCES