Study on Computer Network Technology of Digital Library

Yanming Sui
LinYi University, Linyi, China
suiyanming@lyu.edu.cn

Abstract

With the development of information and communication technology, the concept of libraries has changed dramatically. The traditional libraries are gradually getting digitized. Modern digital library can not be separated from the computer network technology. The potential safety hazard of library computer network constitutes a serious threat to the information security. In this paper, main factors affecting digital library information security are analyzed. Based on the analysis, the author proposes a number of specific computer technologies to eliminate network security risks.

Keywords: Computer Technology; Network Technology; Digital Library

1 Introduction

With the rapid development of information and communication technology, we are now living in a networked society. The information technology is extensively used to record, store and disseminate the information in the digital form. The traditional libraries collect mostly print media, manuscripts etc. In order to meet the demand of information era, the traditional libraries are gradually getting digitized. Great changes have occurred compared with the traditional mode on the operation and management of the digital library. Not only the regular services, such as depository catalogue searching, book reservation and information management of readers and books, but also the new services, such as interlibrary loan, are operating through the computer network. The document information service of digital library has been fully automated by using computer network technology. The Online Pubic Access Catalog in a digital library could allow the reader to access the resource of libraries all over the world through the internet. Network security thus is very crucial to the information security of the digital library. The factors which affect network security of digital library need to be analyzed and some computer technologies which could eliminate network security risks need to be applied during the construction and operation process of the digital library.

2 Digital Library

There are four stages of library development, which are traditional library, automated library, electronics library and digital library. In digital library high speed optical fiber are used for LAN and the access is over WAN and provide a wide range of Internet based services i.e. audio and video conferencing and like other. The majority of the holding of a digital library is in the computer readable form and also acts as a point of access to other on line sources. A digital library is nothing but a large database for the people who are working on hypertext environment. It is an environment, which supports the full life cycle of creation, storage, preservation, dissemination and use of data, information and knowledge. A digital library is not confined to a particular location or so called building, it is virtually distributed all over the world. The user can get his/ her information on his own computer screen by using the Internet. Actually it is a network of multimedia system, which provides fingertip access. Fig.1 is a topological graph of the storage system solution for a large digital library of an university. According to Fig.1, the storage and operation of the digital library are highly depended on the website.

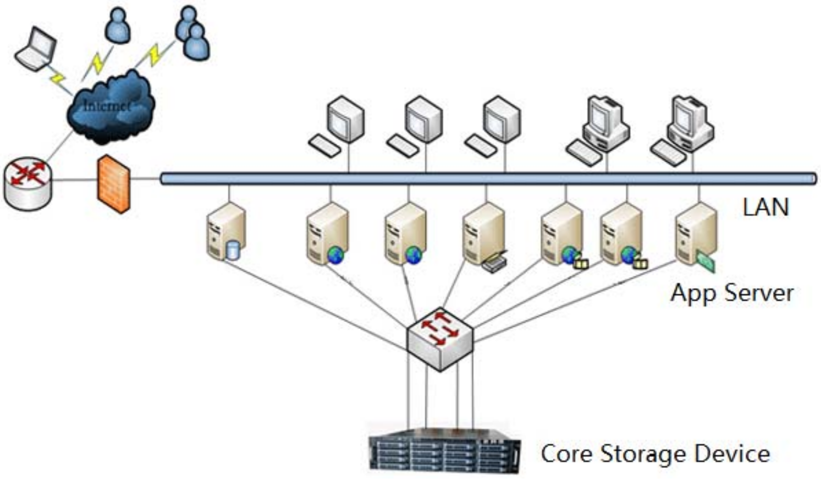

Fig.1

The digital library has many advantages. Traditional libraries are limited by storage space; digital libraries have the potential to store much more information, simply because digital information requires very little physical space to contain it. The user of a digital library need not to go to the library physically; people from all over the world can gain access to the same information, as long as an Internet connection is available. The same resources can be used simultaneously by a number of institutions and patrons. The user is able to use any search term (word, phrase, title, name, subject) to search the entire collection. Digital libraries can provide very user-friendly interfaces, giving click able access to its resources. However, the development of the digital library also faces some challenges. One of the greatest challenges is the network security hidden danger, which could either threat the safety of the digital resource or the personal information of the readers.

3 Main Factors Affecting Network Security of Digital Library

The computer network security of digital library involves computer software and hardware technology, database technology, network technology and library management technology, etc. There are many kinds of factors that affect the computer network security of digital library. The analysis of these factors must be made in order to propose the defense strategy to eliminate network security risks.

Environmental Factor. The computer running has high requirements on the surrounding environment, such as temperature, humidity, power supply stability, etc. The environmental sudden change may affect the data processing. In order to the meet the demand of some good quality network servers, the appropriate power outlet and power UPS (uninterruptible power supply) are needed to ensure power supply stability. Other equipments to guarantee a secure computer system operating environment are also needed.

Human Factors. The human factors that affect the computer network security of digital library include human errors and malicious attack of web hackers.

The most common human factors that cause network security problems are human errors. For example, the improper operation of administrator causes network security vulnerability or data loss. The improper operation of users also would pose a threat to network security, such as user password is too simple, lending the account to others at will because of the lack of safety awareness.

The network security problems caused by web hackers are most severe. The web hackers usually take advantage of network security vulnerability to attack the network of library in order to steal classified information or destroy the integrity and effectiveness of the database. The malicious attack of web hackers can be divided into two categories: active attack and passive attack. The active attack means the web hacker takes various means to destroy the web firewall, attack library database system and make selective destruction of information content. However, the passive attack is more undetectable. It is usually executed without destroying network while classified information is stealing.

Software Factors. The weak software safety also could cause library network security problems. For example, the vulnerability of database system and data transmission technique could cause data loss or data transmission error which may threat the integrity of the network database.

Another software factor that affects network security is the computer virus invasion. Computer virus is a man-made program causing damage effects to computer information or systems when the computer is running. This program is not an independent existence, it concealed among other executable program, not only destructive, but also infectious and latent. The computer virus invasion could interfere with the normal operation of the system and cause the data damage or loss. Extensive network fault is made due to its strong dispersal capacity.

Hardware Factors. Hardware fault may affect library network security as well. Library network system is composed of network servers, disk arrays and other equipment combination. Its security relies on the reliable operation of the overall device. A part of any error, may affect the normal operation of the entire network. In the hardware configuration, you must fully take into account the compatibility between various devices and whether they are configured correctly and so on. If the hardware of the data server breaks down and the data backup is not executed well in daily operation, the massive data losses are inevitable. Although the chance of hardware fault for a single component is tiny, the chance of hardware fault increases a lot in consideration of that a large amount of hardware components are used due to the complexity of the network and data servers seldom shut down.

4 Defense Strategy

In order to cope with all the factors listed above which threat the library network security and keep data information from being stolen and destroyed, the defense strategies are proposed as follows.

Hardware Protection. Hardware protection for network data security mainly refers to the measures by adding hardware components in order to enhance the network security. For example, adding hardware components to CPU, data memory, cache, data input-output channel and peripheral equipment to prevent data damage and keep database integrity. Hardware protection is more reliable than software protection. The combination of hardware and software protection method is needed to ensure the security of some important system and data.

Firewall Technology. A firewall is a network security system that controls the incoming and outgoing network traffic based on applied rule set. Fig.2 is an illustration of where a firewall would be located in the library network. The firewall establishes a barrier between a trusted, secure internal network and another network that is not assumed to be secure and trusted. Firewalls exist both as a software solution and as a hardware appliance. Many hardware-based firewalls also offer other functionality to the internal network they protect, such as acting as a DHCP (Dynamic Host Configuration Protocol) server for the library network.

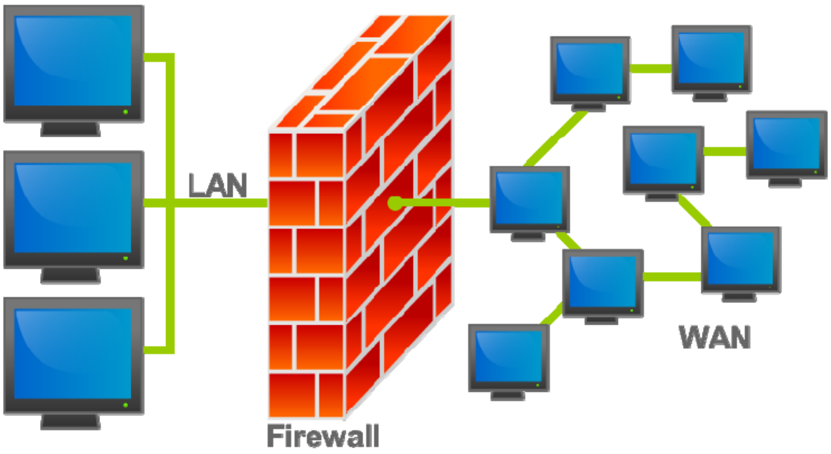

Fig.2

Intrusion Detection Technique. An intrusion detection system (IDS) is a device or software application that monitors library network for malicious activities or policy violations and produces reports to a management station. IDS has becomes a necessary addition to the security infrastructure of nearly every digital library apart from firewall devices.

Network Data Encryption Technique. The data encryption is to protect the data, files, passwords and control information within the network. The network encryption technology includes network transmission encryption and account, password, authority encryption. It could effectively keep from web hackers' illegal visit to the key database and attempt of tampering the data. Fig.3 illustrates how data encryption works. The plain text is transformed to the cipher text by the encryption key and the receiver then transforms the cipher text back to the plain text by the decryption key. The network data encryption technique is one of the most effective method to guard the network security.

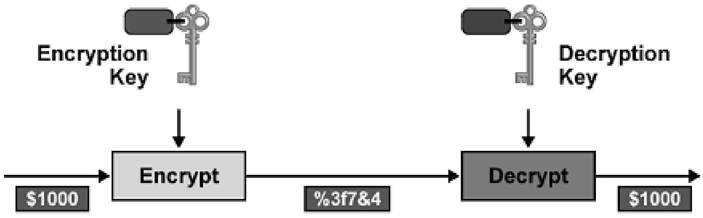

Fig.3

Network Anti-virus Technique. Computer viruses are seriously destructive and threatening for library computer network. Hence, the network anti-virus system is a key link of the network security defense strategy. The network anti-virus technology includes virus prevention in the earlier stage and virus diagnosis and elimination in the later stage. The virus prevention is mainly depend on the anti-virus programs (also known as AV scanners). All AV scanners work with a database that contains information about virus fingerprint or signature. The database needs to be updated frequently so that it contains the most up-to-date virus information.

Data Backup Technique. The ultimate aim of the network security is to protect all kinds of library data resources, including local data and online data. The data backup is the main technique of library network security management system to prevent unexpected accidents. The data backup and recovery technology enables the library network security system to backup or recover data in accordance with different situation. The librarian is supposed to backup the library data at intervals to ensure the data security.

5 Conclusion

The digital resources of the digital library are becoming more and more abundant and the increasingly integration and openness of digital library network is requiring stricter security management. Network technology is developing rapidly.

The network security of digital library will surely face more and more challenges. The new defense strategy and technologies will also be adopted to meet the challenge.

References

[1] Wang H, Library Network Security and Management. Libr Info Serv 4 (2008), p. 29-31

[2] H.B. Chen, Network security threat and Countermeasures, Sci-Tech Information Development and Economy, Vol.12 (2005), p. 219-220

[3] Pomerantz, Jeffrey, & Marchionini, Gary, The Digital Library as Place, Journal of Documentation, Vol.63 (2007), p. 505-533

[4] Information on http://www.researchgate.net

[5] Information on http:// openarchives.org

[6] Information on http://liswiki.org