Research on Security Protection Technology of Digital Library System in the Era of Equal Protection 2.0

Zhijie Li
School of Information Engineering, Guangdong Mechanical & Electrical College, Guangzhou, Guangdong, China
Email: 2006010012@gdmec.edu.cn

Abstract. New Coronavirus pneumonia is eroding the world, and digital libraries are even more important. How to control the network security of digital library system? According to the requirements of equal protection 2.0, this paper analyzes the security requirements of digital library network, and puts forward the security protection technology of digital library system under equal protection 2.0 system from the four perspectives of secure communication network, secure area boundary, secure computing environment and security management center. Based on the security protection technology framework of equal protection 2.0, this paper studies the security evaluation method of digital library, and puts forward the security protection technology solution.

Keywords. Digital library; equal protection 2.0; network security.

1. Research Status of Digital Library System
Digital library is an excellent product in the development of the information age. Compared with the traditional library, it has the advantages of small size, large storage capacity, fast processing speed and multimedia integration, especially during the epidemic period. The development time of digital library is relatively short. In the process of development, it is inevitable to encounter various network security problems. The construction, management, maintenance and other links may be threatened by security. The security of the whole system needs to be improved [1]. Maintaining network security has become an important part of maintaining national security. The blackmail incidents of the government, universities, hospitals, manufacturing industry and other related enterprises are increasing year by year. Therefore, the state issued the basic requirements for classified protection of network security (hereinafter referred to as equal protection 2.0) in May 2019, which puts forward new standard requirements for China's network security related work. The network security evaluation and protection of digital library system need to keep pace with the times, according to their own business needs and the requirements of equal protection 2.0. Based on the security protection technology framework of equal protection 2.0, this paper studies the security evaluation method of digital library, and puts forward the security protection technology solutions.

2. System Security Requirement Analysis
Digital book network system, according to the relevant provisions of equal protection 2.0, is classified as equal protection three-level system, mainly from the security communication network, security area boundary, security computing environment, security management center and other four aspects of equal protection security analysis.
There are some deficiencies in the secure communication network of the digital library system, which need to be further upgraded. The main performance is as follows: using technical means to realize the analysis and detection of network traffic; Need to use data encryption and verification technology to ensure the security of operation and maintenance; Encrypted communication measures are needed to improve the security of communication; Dynamic trusted verification mechanism is needed to ensure the program from virus intrusion, malicious code loading, unauthorized identity access and other security threats [2].

The digital library system needs to be further upgraded in terms of regional border security, which is mainly manifested in the following aspects: it needs to solve the problem of business interruption caused by DDoS through anti DDoS attack protection, server host resource optimization, etc; Network intrusion detection and prevention technology is needed to solve the problem of hackers using system vulnerabilities to carry out malicious attacks; It is necessary to audit the firewall to prevent the redundancy of firewall policy; Through access control measures to solve the problem of unauthorized access to the internal network of external personnel [3].

The digital library system needs to be further upgraded in terms of computing environment security, which is mainly manifested in: Using Intrusion Detection and other technical means to solve the problem of being attacked by downloading malicious files by mistake; Use vulnerability scanning technology and repair to solve the vulnerability problem of system or equipment; Using identity authentication and access control technology to solve the problem of unauthorized access.

The digital library system needs to be further upgraded in the aspect of security management center, mainly in the following aspects: it has the ability of situation awareness, traffic monitoring and centralized security management, and can quickly and timely deal with intrusion and attack problems; Audit and record relevant administrators to prevent misoperation or illegal operation; Real time monitoring the use of system resources to prevent unreasonable calls [4].

3. System Security Protection Technology
According to the relevant requirements of equal protection 2.0, a series of measures such as identity authentication, data security, intrusion detection and defense, and centralized management and control are added to improve the digital library system from the four perspectives of secure communication network, secure area boundary, secure computing environment, and security management center, as follows.

In view of the mature online digital library system and perfect network structure, communication network security focuses on communication transmission and trusted verification. In the process of communication transmission, hypertext transmission security protocol (HTTPS), virtual private network technology (VPN) and image traffic analysis technology are used to build security protection. The communication transmission security of the terminal in the system business level is realized by the HTTPS protocol, and the encrypted transmission is realized. In order to solve the data encryption and verification technology in the remote operation and maintenance, VPN is added in the security control area to facilitate the remote operation and maintenance of the administrator. By setting VPN access strategy and working mode to match the operation and maintenance administrator’s authority, the VPN special equipment with IPSec VPN technology can realize the functions of behavior audit, terminal security check, flexible network access and multi factor authentication. Tap shunter technology can realize the network traffic image collection of digital library system. The control center and traffic detection platform can realize the perception and analysis of the system network situation, and solve the problem of insufficient network traffic analysis ability. Tap shunting can mirror all the data including the wrong data packet, achieve real-time image, no delay, and can load the wrong timestamp [5]. Through the “zero trust” trusted access system, the network level access control of user access is realized in the security control area, which ensures the security of the book application system and prevents unauthorized users from accessing. The trusted access system has the functions of authentication before access, data centric and continuous dynamic authentication.
The security zone boundary involved in equal protection 2.0 includes boundary protection, intrusion prevention, malicious code, access control, security audit, trusted verification, spam prevention, etc. According to the results of demand analysis, the security design is mainly aimed at boundary protection and intrusion prevention. In order to optimize the performance of firewall and restrict the behavior of internal personnel to access the external network, firewall policy audit technology and illegal external connection detection technology are used to achieve border protection. Policy audit technology is mainly implemented from the aspects of redundant security policy, security policy convergence, policy hit frequency, etc. in the illegal external connection detection, the client detection is deployed on the user terminal, Complete the monitoring of users’ online behavior, and based on packet detection technology, through sniffing the network connection, complete the monitoring of illegal extravasation behavior. Once the illegal extravasation behavior of users is detected, the system immediately blocks it in real time. Intrusion prevention system accurately finds all kinds of intrusion attacks and blocks them in real time. It can effectively deal with vulnerability attack, Trojan horse backdoor, worm virus, database attack, brute force cracking and other attacks, and make up for the lack of deep defense effect of transport layer protection products [6]. It adopts anti DDoS and intrusion technology to realize the defense and detection of external attacks, two detection methods based on traffic characteristics and traffic anomaly are used to identify DDoS attacks. Packet filtering and rate limiting are used to fight against DDoS attacks. Auxiliary measures such as reducing exposure, improving network bandwidth and load balancing are used to improve the ability of anti DDoS.

The security computing environment involved in equal protection 2.0 includes security audit, access control, identity authentication, intrusion prevention, trusted verification, data integrity and confidentiality, malicious code prevention, data backup and recovery, residual information protection and personal information protection, etc. According to the results of demand analysis, it mainly focuses on identity authentication, intrusion prevention Data security and malicious code prevention. In the digital library system, the identity authentication technology is combined with a variety of security protection technologies, and the strong authentication factor verification is added in the login process to realize the strong authentication function of user login and improve the system security. In the security design of intrusion prevention, through apt intrusion detection and NFA network traffic probe, the attack behavior is detected and alerted in the exit firewall and security control area to realize the security protection of the library management system, deploy WAF to strengthen the security protection of the application system, and have the security protection functions of anti SMS verification abuse, malicious registration attack and interface protection. The webpage tamper proof system deployed in WAF has the functions of automatically monitoring the folder, automatically publishing the page and protecting the content of the page. The data security platform is constructed in the security control area, and the integrity, availability and security of data are guaranteed through the design of database audit, database desensitization, database leakage prevention and database backup and recovery modules. The vulnerability scanning system is used to test the penetration of the operating system, network equipment, firewall and remote services, and comprehensively evaluate the patches, ports and vulnerabilities in the system, so as to discover and modify the vulnerabilities in time, and improve the system's ability to resist malicious code attacks. The vulnerability scanning system can help to discover the internal asset security risks and improve the system's ability to resist malicious code attacks. Realize the vulnerability assessment of internal network.

The security management center involved in ISO 2.0 includes audit management, security management, system management and centralized control. The log management system is deployed in the security control area to collect the log information and audit information related to all hardware devices in the library management system. According to the strategy, the log information and audit information are classified and stored to achieve ex post evidence collection, facilitate system troubleshooting, and ensure that the security events do not recur. The log audit system has the functions of large-scale deployment, report reporting, log standardization, threat intelligence collection.
and utilization Retrieval technology and interactive analysis. In the aspect of security management of equal protection 2.0, in order to realize the configuration of security policy, parameter setting and check and save of security marks, configuration verification tools are used to check and control the security policy. Configuration verification needs to check the server, account and system configuration. Configuration verification tools are deployed in the security control area to help find the configuration defects in the network and applications, Through the web file scanning and system service optimization of the server system, the security risk of the current server is determined. Through the account security check, the hidden account, clone account, weak password account and other risks leading to account theft are found. Through the system configuration security check, the security and anti attack ability of the system are improved. The system has a large network scale, more equipment and accounts, and more complex management. In order to realize the security management and control of operation and maintenance, the operation of the system administrator also needs to be controlled and audited. In the system management, the centralized management of IT resources is realized through the 4A security management platform, and the comprehensive security management and control of accounts, authentication, authorization and audit are carried out. Centralized management and control is used to control the security devices or components distributed in the network, and to monitor the operation of network links, security devices, network devices and servers, so as to grasp the security situation of the whole system operation, find and deal with system faults in time, and ensure the continuity of application services. The centralized management and control center covers information collection, information analysis, information management and control Security disposal, user presentation and system support are five functional modules to control the operation of the system in real time.

4. Research Summary of Safety Protection Technology
According to the framework of equal protection 2.0, this paper puts forward the upgrading scheme of digital library security protection from four aspects: secure communication network, secure area boundary, secure computing environment and security management center. The security protection upgrade scheme transforms the security communication network from the two aspects of communication transmission security and trusted authentication, strengthens the security area boundary from the two aspects of boundary protection and intrusion prevention, upgrades the security computing environment from the aspects of identity authentication, access control, intrusion prevention, data security, and so on, and improves the security computing environment from the aspects of audit management, system management, data security, etc. The safety management center has been improved in the aspects of safety management and centralized control.

References
[1] Song T 2019 The security and protection of the computing network of digital library Modern Information Technology 21 147-148.
[2] Ma L 2019 Practice and thinking on the construction of e-book resources in public libraries in the era of big data Think Tank Era 36 287.
[3] Cai Y 2020 Transformation and thinking of digital resource construction of University Library in post epidemic era Library Emergency Service 10 11
[4] Zhang J J 2019 Opportunities and challenges in the construction of Digital Library in the era of big data Rural Staff 15 200.
[5] Zhang Q Z 2020 Research on the safe operation scheme in the era of equal protection 2.0 Informatization in China 12 61.
[6] Guo W 2020 Research on the co construction and sharing of digital resources in university libraries under the network environment Inside and outside LAN Tai 33 79.