http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (24): 7930-7937, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.7930.7937

Research on Classified Protection-based Security Construction for University Information Systems

[1]Chunling Wu, [1]Hehua Li and [2]Wei Wei
[1]Chongqing College of Electronic Engineering, Chongqing, China
[2]Xi'an University of Technology, Xi'an, China

Abstract: Information security classified protection is a basic system of China's information security protection. Conducting information security classified protection in colleges and universities is not only a key content in strengthening national information security work, but also an effective measure to improve the information security level of university networks. The paper first summarizes common information subsystems in China's universities and colleges, describes the functions of these subsystems and offers the recommended classified protection levels for these subsystems. Then, this paper divides an university information system into various modules based on security domain according to the security strategy of "all Grade II systems forming one security domain and each Grade III forming one security domain" and gives the access control methods for security domain boundaries. Finally, according to the requirements on Grade II systems by China's national standards concerning classified protection, this paper analyzes the contents and objectives of security construction for Grade II security domains from five aspects, thus offering a reference for universities to conduct classified protection based information security construction.

Key words: Classified protection, security domain, information security, information System

INTRODUCTION

Information security classified protection, hereinafter referred to as classified protection, refers to that a state, via formulating and implementing unified managerial codes and technical standards on classified security protection, organizes citizens, legal persons and other organizations to implement security protections of information systems according to their classifications and supervises and manages the implementation of classified security protection. Classified protection system is a basic system for improving the capacity and level of information security, for safeguarding national security, social stability and public interest and for guaranteeing and promoting the healthy development of informatization during a country's social and economic development as well as informatization. The overall requirements of classified protection are "strong focus, graded responsibility, classified guidance and step-by-step implementation" and are to clarify the security responsibilities of the departments in charge of information security and the organizations and individuals who construct, operate, maintain or use an information system, thus requiring the departments, organizations and individuals to implement classified protection, respectively.

The Education Management Information Center under the Ministry of Education of China set up the Information Security Testing and Evaluation Division in April 2010, which is responsible for technology consulting, testing and evaluation of information security classified protection, thus starting classified protection for university information systems (Education Management Information Center under the Ministry of Education of China, 2013). A university information system, formed by computers and supporting equipment, consists of a variety of subsystems that collect, process, store, transmit and retrieve the university's service information. When a university is conducting information security development based on classified protection, the university should first analyze its information system in relation to national security, social order, public interest, as well as the legitimate rights and interests of citizens, legal persons and other organizations, according to its own characteristics and then determine the infringed objects when its information system is damaged and the severity of infringement of these objects and then decide the classified protection grade of its information system and finally implement relevant security measures in accordance with the national provisions corresponding to the decided classified protection grade,

Corresponding Author: Chunling Wu, Chongqing College of Electronic Engineering, Chongqing, China

thus meeting national requirements on classified protection (GB/T 22240-2008, 2008; GB/T 22239-2008, 2008).

When a university information system or subsystem's service information security and system service abilities is damaged, the severity of the infringement against the infringed objects due to this damage has close ties with the administrative level of the institution to which the information system belongs, the importance of the service, the degree of the infringement and the university's education scale. The damage of the service information security and service abilities of an ISU's information subsystems belonging to the four classes, namely enrollment management, data integration, school management and basic network services, may negatively and seriously impact the working order and functions of the university. This may bring adverse effects to the society on a certain scope, causes serious damage to social order and public interests and incurs serious harm to the affected students and public. Meanwhile the damage of the service information security and service abilities of an ISU's information subsystems falling to the four classes, namely teaching support, scientific research management, public service and information release, may seriously impact the normal order of the university and disturb the university in carrying out its normal functions, infringing the legitimate rights of the university, teachers and students and causing legal issues.

Therefore, classification and enhanced protection of universities information systems in accordance with the requirements of classified security protection is not only a requirement from national information security system but also a practical demand of colleges and universities to enhance their levels of information security. For the sake of facilitating writing: the word "university" is used in this paper to refer to "university and college"; the information system of a university is shorted as ISU.

Overview and classification of subsystems of an isu: Since the information system of a university (ISU) is generally large and complex, for more effectively achieving the objectives of classified security protection, based on service needs an ISU can be divided into subsystems that can be furthered classified and graded. The specific methods and standards for system classification is given in GB/T 22240 - 2008 Information security technology-Classification guide for classified protection of information system (GB/T 22240-2008, 2008), which presents common service subsystems generated from system division and recommended classification level for conducting classified security for them.

Teaching support class: An ISU's subsystems falling into the teaching support class is recommended to be rated as Grade II System. This class of subsystems includes the educational management system (including undergraduate, graduate, online education, adult education and international student education), resource-sharing assistant teaching system, teaching evaluation system and scientific research management system. Specifically, the scientific research management system, if involving confidential or cutting-edge research fields and information, should be rated in accordance with the relevant national standards on classified protection of classified systems (Anonymous, 2013; BMB 17-2006, 2006; BMB 20-2007, 2007).

School management class: The vast majority of information subsystems belonging to the school management class are suggested to be rated as Grade II System. These subsystems include the office and transaction processing system, personnel management system, financial management system, asset management system, teacher management system and student education management system and archive management system. In addition to these seven subsystems, the education educational electronic document and information exchange system providing the function of file transfer between subordinate colleges and universities and supervising educational administrative departments should be rated as Grade III System according the requirements of supervising departments since this exchange system is the document transmission platform that is designated by the Ministry of Education and runs in a unified and nationally networked way.

Data integration class: An ISU's subsystems belonging to data integration class consist of public database system, information portal system and unified authentication management system. Specifically, the public database system is an information subsystem providing functions of data sharing, data analysis and general inquiry; the information portal system is an application subsystem enabling single-point logging and information syndication; the unified authentication management system is a comprehensive service system providing functions of identity management and authentication, as well as access authority control. Since damage of these three subsystems will cause severe impacts and losses to the university, it is recommended that these systems are rated as Grade III system according to the classification standards of classified protection.

Information release class: An ISU's sub-systems falling into information release class include the school information release platform, university portal website, as well as the websites of the university's various departments and research institutions. The school information release platform is a management system for releasing university-related documents, notices and announcements. The university portal website is the university's official portal website for information release, information publication, policy consultancy and social services. These two subsystems could be rated as Grade III System or Grade II System according to actual demands. The rest subsystems can be rated as Grade II System.

Public service class: An ISU's public service system consists of the logistics management subsystem, campus card subsystem, library management subsystem and security monitoring subsystems. Among them, the campus card subsystem provides the unified authentication and management of applications including meal cards, student ID cards, working ID, medical cards, network access cards, attendance cards and access control cards. Thus, this subsystem is relatively important and can be rated as Grade III System in light of practical demands. The remaining subsystems can be set as Grade II System.

Enrollment and employment class: The enrollment management system of an ISU is a subsystem providing various functions including online registration, information publication and admission inquiry for students of all levels, including college students, undergraduate, graduate and doctoral students. It is recommended that the enrollment management system is classified as Grade III System. Furthermore, it is recommended that the autonomous enrollment management system and employment management system are classified as Grade II System.

Basic network service class: An ISU's subsystems falling into basic network service class typically include: Campus network operation and management system, e-mail system and network video service system, as well as forums and community websites. The campus network operation and management system provides the functions of operation monitoring, device management and network maintenance for the entire campus network of the university, is the management and control core of the entire campus network and guarantees the normal operation of all service systems. Since this system plays a major role, it is recommended as Grade III System.

Classified protection-based security domain division and boundary protection: The ultimate goal of security construction for ISUs is to reduce security risks and hazards to an acceptable level under the premise of technical and managerial feasibility. Achieving this goal requires not just determining the brands of firewalls and intrusion detection systems but also overall consideration of how to install these safety devices in the existing network architecture so as to enable and maximize the functions of these devices. If there is not a reliable and practical foundation network of clear structure and expansion flexibility and if security development still adheres to the conventional practice of setting up for each subsystem a self-contained, decentralized and separated security system, even using the most advanced security devices is only to build a castle in the air, which is unable to fundamentally weaken the security threats and pitfalls of information system. Therefore, introducing security domain division to overcome and transform defects stemming from the traditional overall structure of information systems becomes a top priority for colleges and universities to realized classified protection (Hu and Fan, 2010; Sang *et al*., 2010).

Security domains and principles of security domains division: Security domain division is to put different subsystems' equipment components of similar or identical security attributes the same security domain according to each subsystem's service attributes, equipment composition, information properties, users and security objectives, under the unified guidance of security policy (Hu and Fan, 2010; Hong *et al*., 2008). Security domain division is not traditional physical isolation. Physical isolation passively stops the process of informatization due to threats to information security and cuts off network connection, resulting in disenabled information be sharing. Since security domain division is realized under the premise of careful analyses of security requirements of each system and security threats facing each system, it attaches due importance to precaution of security threats and permits normal transmission and exchange of legal data among systems.

It should be noted that security domain division aims at giving full play to the overall effectiveness of security products rather than subverting the original overall structure of an information system. Security domain division should follow the following basic principles:

- Security domain division should be conducted in accordance with the working role undertaken by and

individual security demands of each device in the information system and by giving due consideration of specific deployments of security products
- There should not be too many security domains. Too many security domains will lead to excessively complex security strategy and cause great inconvenience for future management
- Security-domain division should ensure that mutual visits among various security domains do not pass too many routers
- Transformation of existing network structure should consider protection of current investments so as to avoid duplication of investment and construction

Security domain division of university information systems: A university should divide the subsystems of its information system into different security domains before conducting classified protection-based security construction. Security domain division is to define the boundaries of different domains, to implement inter-domain boundary control and to realize enhanced protection of key subsystems. A security domain materializes as the collection of one or more physical network segments or logical network segments. The difficulties in security domain division incurred by an application subsystem crossing multiple physical environments, such as equipment rooms, could be solved by assigning the involved physical network segments or subnets on the campus network level to the same security domain since security domain is a logical area.

As analyzed and summarized in Section 1 herein, there are 20 Grade-II subsystems in an ISU, including:

- Four in the teaching support class
- Seven in the school management class
- One in the information release class
- Three in the public services class
- Two in the enrollment and employment class
- Three in the basic network service class

An ISU has ten Grade-III subsystems, including:

- Classified research management system
- Electronic documents and information exchange system designated by the Ministry of Education of China
- Public database system
- Information portal system
- Unified authentication management system
- University information release platform
- School portal website
- Campus card system
- Unified enrollment management system
- Campus network management system

It should be noted that not all colleges and universities have all of these subsystems and that these subsystems may be named differently. Conducting security domain division as per the strategy of "all Grade II systems forming one security domain and each Grade III system forming one security domain" produces the following structure of security domain division for an ISU, as shown in Fig. 1.

Realization of security domain and boundary protection: Security domain division cannot be divorced from deployment of security products. The realization of security domain and boundary protection can use the following methods (GB/T 25070-2010, 2010):

- **Security segregation via firewalls:** Use dual interface firewalls to achieve boundary isolation, connect each firewall interface to different security domains so as to realize access control. A firewall may also be logically divided into multiple virtual firewalls and each virtual firewall system can be seen as a completely independent physical firewall device, which has independent system resources, administrators, security policy and user authentication database, etc.
- **VLAN segregation via layer 3 switches:** Use layer 3 switches to divide VLANs for security domains and adopt switch access control lists or firewall modules for achieving access control among security domains
- **VLAN segregation via layer 2 switches:** Divide VLANs for security domains at layer 2 switches, connect TRUNK to routers or firewalls and conduct access control at uplink routers or firewalls

Access control rules for security domains: Configuring access control rules in the boundary protection devices of a security domain realize boundary protection. Therefore, access control rules can be realized by configuring switches or firewalls.

The boundary security protection of a Grade II security domain needs to meet the following conditions:

- Be able to permit or deny explicitly access of data stream according the session state information
- The granularity of access control should be at network segment level
- According to the access control rules between the user and the system, the granularity of access control should be individual users

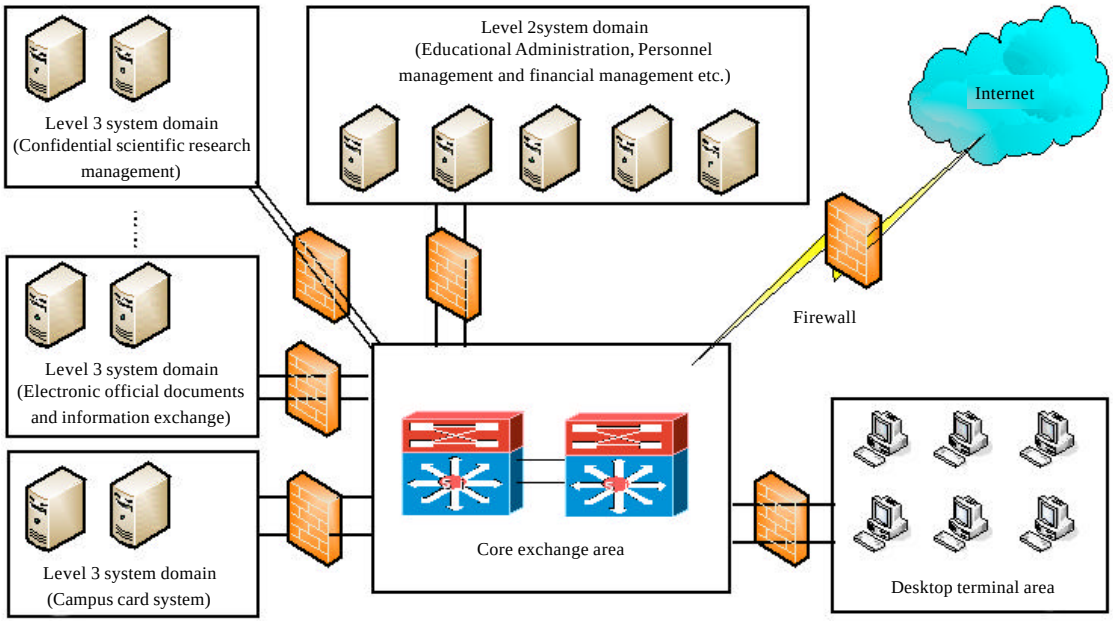

Fig. 1: Logical security domain division of the information system of a university

The boundary security protection of a Grade III security domain needs to meet the following conditions:

- Be able to permit or deny explicitly access of data stream according the session state information
- The granularity of access control should be at port level
- Be able to filter information entering and exiting the security domain and to realize instruction level control for application-layer protocols

Intrusion detection within security domains: According to the security demands of different protected objects in a security domain, AAA, IDS and anti-virus systems are deployed to achieve security within the security domain. The detection scope of intrusion detection systems deployed within Grade II System and Grade III System security domains should include all Grade II System servers and Grade III Systems servers. Intrusion detection should meet the following requirements:

- Customize intrusion detection strategies, for instance, customizing intrusion detection rules according to the source IP addresses, destination IP address and port number as well as service type of intruded data packets
- Customize real-time alarm strategies in case of serious intrusion-detection events
- Be able to monitor at least the following attacks: port scanning, brute force attacks, Trojan backdoor attacks, denial-of-service attacks, buffer overflow attacks, IP fragmentation attacks and network worm attacks
- In case of a detected attack, the intrusion detection system should record the IP address of the attack source, the attack type and the attack destination IP as well as the attack time. In case of a serious intrusion, the system should be able to give out a warning timely

Contents and objectives of classified protection-based security domain construction: When an ISU is divided into subsystems, these subsystems are put into different security domains (ranging from Grade I to III) since they have security demands in varying degrees. Thus, they have different requirements on classified protection-based security construction. This section takes Grade II security domain as an example to introduce the construction contents and objectives for security domains of different grades.

Grade II security domain mainly covers the hosts, servers and networks associated with Grade II systems. The classified protection-based security construction for Grade II security domain is mainly aimed at implementing the various specifications and requirements for Grade II System set forth in GB/T 22239-2008, 2008 Information

security technology -- Baseline for classified protection of information system. Therefore, information security should be constructed comprehensively from five aspects including network security, host security, application security and data security and security management.

Network security: Network security development based on requirements of Grade II classified protection is to achieve the following objectives:

- The network structure is clear, with a redundant space sufficient to meet the demands during service peaks
- According to the working functions and importance of each department and the degrees of importance of classified information, set different network segments for different departments, allocate available IP address range to each segment in accordance with the principle of convenient management and control
- Deploy access control devices on the network boundary and control access among the services hosts of varied network segments and between the service hosts and offices terminals
- Enable and start the security auditing function of network devices so as to track various events of network devices, including operational status, equipment maintenance and configuration changes
- Login passwords set for network equipment are in line with the requirements of classified protection on password security and adopt secure remote login method, such as SSH, for remote control of network devices
- Be able to permit or deny explicitly access of data stream according the session state information; the granularity of access control at network segment level
- Monitor at network boundaries the following attacks: port scanning, brute force attacks, Trojan backdoor attacks, denial-of-service attacks, buffer overflow attacks, IP fragmentation attacks and network worm attacks

Host security: ISUs' hosts are generally of a higher security level since the network information center of each college or university has configured certain host security strategies and established a pertinent safety management system. For instance, the security, operation and maintenance of hosts are under the charge of a dedicated person. Nevertheless, generally there are still some security issues to be solved. Combining the relevant requirements of Grade II classified protection, construction and transformation of host security classified protection from aspects, including host identity authentication, access control, security auditing, intrusion prevention, malicious code prevention and resource control, should be conducted so as to achieve the following objectives:

- Assign different user names for the different users of operating systems and database systems to ensure that each user name is unique
- Implement strict access control policies for limiting users' access and manipulation of hosts
- Implement rigorous security audit strategy so as to ensure that host security incidents are investigable and accountable
- Host operating systems should follow the principle of minimum installation, installing only the required components and applications
- Set host operating systems to guarantee automatically update and installation of latest patches
- Set the number of host logging attempts with incorrect passwords and the locking of hosts due to timed-out operation
- Set the maximum or minimum limit on each user's use of hosts' system resources

Application security: Classified protection construction is to achieve the following Grade II protection objectives of application security:

- Set identity authentication measures for all users logging onto application systems
- Run an audit system that is able to audit the operation of each logged user
- Implement sufficient encryption measures to ensure the confidentiality, integrity and availability of data during network transmission
- Application software is able to conduct automatic recovery, guaranteeing that application systems are able to automatically restore in case of operation errors

Data security: According to classified protection's requirements on data security of Grade II systems, ISU's data security needs to be constructed and transformed from aspects, including data integrity, confidentiality and availability, as well as data backup and recovery, in order to achieve the following objectives:

- Ensure the integrity and confidentiality of important information, e.g., management data and service data, during transmission and storage

- Ensure that there are appropriate measures to conduct information recovery in case of a detected integrity error during data storage
- Ensure system availability by providing hardware redundancy for critical network equipment, communication lines and data processing systems

Security management: Many information security management personnel at colleges and universities hold and practice the erroneous thinking of "stressing security devices while neglecting security management". The information security management agencies and management system construction at many colleges and universities do not meet the national requirements on information security classified protection. Thus, classified protection development strives to achieve the following objectives:

- Under the guidance of the university's overall policy and strategy on information security, the information security management agency can reasonably plan the development of information security strategies, timely release various documents and regulations on information security and periodically revise and correct the problems in all kinds of information security systems and regulations
- Establish the posts of system administrator, network administrator and security administrator and specify the work responsibilities, division of labor and skill requirements of each post in the safety management agency
- Be able to access technical support in safety and technical trainings and knowledge exchanges from security industry experts, professional security firms and security organizations, so as to ensure that the security maintenance of the university's information system is in line with classified security's basic requirements on security management, keeps up to the times and demonstrates a certain degree of progressiveness
- Conduct regular vulnerability scanning. In case of detected system security vulnerabilities, timely remedy is made. Before a system patch is installed, the patch should be first tested in a test environment and only after the back up of important files the patch may be installed
- Establish an institution of system security management, to make provisions for the system security policy, security configuration, log management and day-to-day operational processes
- Maintain systems according to applicable operating manuals; keep detailed operation logs, including important day-to-day operations, operation and maintenance records, as well as parameter settings and modification; prohibit unauthorized operations
- Analyze operation logs and audit data on a regular basis in order to detect abnormal behavior timely
- If a major change is to be made to the information system, an application should be summited to the supervising leader. Only with the examination and approval from the leader, the change may be made. After the implementation of the change, notice relevant personnel

CONCLUSION

Campus networks and university information systems have been the forefront of China's Internet development and playing an increasingly important role as infrastructure for university informatization in teaching, research and management. Universities' implementation of classified protection of information systems could be better reduce security risks and respond to cyber threats, thus protecting the normal operation of information networks.

Since China started late in conducting classified protection of information security, compared to developed countries (Education Management Information Center under the Ministry of Education of China, 2013) and university information systems is not receiving due attention as e-government systems from China's departments in charge of information security and information security construction lacks funds, classified protection construction of university information systems still has a long way to go.

From currently available information: For universities that have not constructed information security systems in a standardized and sound way, their information security protection level reaches Grade I in general and some systems reach Grade II. For universities that have constructed information security systems in a standardized and sound way, their information security protection level is higher and reaches Grade II in general and some systems reach Grade III.

ACKNOWLEDGMENTS

This study is supported by 2013 Chongqing higher education key project of teaching reform (Program No. 132116, Project leader: Hehua Li).

This job is also supported by China Postdoctoral Science Foundation (No. 2013M542370).

REFERENCES

Anonymous, 2013. Classified protection of classified information systems. Baidu, June 5, 2013.

BMB 17-2006, 2006. Technology requirements on graded protection of information systems involving state secrets. British Medical Bulletin, UK.

BMB 20-2007, 2007. Management specification on graded protection of information systems involving state secrets. British Medical Bulletin, UK.

Education Management Information Center under the Ministry of Education of China, 2013. Thematic work on the classified protection of educational information security. China, May 10, 2013.

GB/T 22239-2008, 2008. Information security technology-baseline for classified protection of information system. http://www.cn-standard.net/ebzdetail/742/EB223605.shtml.

GB/T 22240-2008, 2008. Information security technology-classification guide for classified protection of information system. http:// www. codeofchina.com/gb/it/18935.html.

GB/T 25070-2010, 2010. Information security technology-technical requirements of security design for information system classified protection. http://www.cn-standard.net/ebzdetail/501/597841D0.shtml.

Hong, X., A. Peng and J.W. Liu, 2008. Partition and hierarchical protection of E2 government system. J. Chongqing Institute Technol., 22: 99-103.

Hu, Z.R. and H. Fan, 2010. Design implementation and application of technical plans for classified protection-based security construction of information systems. Publishing House of Electronics Industry, China.

Sang, S.Y., G.A. Xu and M. Zhang, 2010. Design and implemention of security level conformance verification platform for information systems. University of Beijing, China.