

Research on the Construction of Network and Information Security

Architecture in Campus

Zhaoyong Zhou^{1,a}, Xiaoli Zhang¹, Yuan Wang², Xijun Wang¹, Chengyu Cui¹, Xilian Deng¹

¹Network & Education Technology Center, Northwest A&F University, Yangling 712100,
Shaanxi, China

²Yangling High-tech Junior High School, Yangling 712100, Shaanxi, China

^ayz@nwsuaf.edu.cn

Abstract: With the continuous development of information construction at college, network security has become more and more important. At present, there still exist a number of problems in information security construction at domestic college, such as the disconnection between information safety goal and business goal, lake of information safety control measures and deficiency of preventive technologies which caused by lack of investment, consciousness and security professionals. Based on the analysis of the campus network security issues and combined with the architectures adopted by some colleges and enterprises, this paper provides the college network and information security architecture from three aspects: management, technology and service, finally, it looks ahead the prospects and challenges of college campus network security in the future.

Keywords: Campus Network, Network Security, Information Security, Architecture

1. INTRODUCTION

With the rapid development of information technology, the campus network is playing a more and more important role in college teaching, research and management, while its security problems are also increasingly prominent. Network and information security have been paid more and more attention, so to build a reasonable network and information security architecture under college campus network environment has become very necessary. There is not an international authorized and recognized standard definition about network security and information security. There is one definition that information security includes physical security, network security, system security, application security and strategic management, business management, personnel management and security laws which associated with management security. No matter how the definition describes, it means the security problems of network and information ^[1]. Due to the different understandings of people for network and

information security architecture, various information security architecture models that involve technology, management and organization have formed, with different connotation and denotation [2-3]. At present, there still exist a number of problems in information security construction at domestic college, such as the disconnection between information safety goal and business goal, lake of information safety control measures and deficiency of preventive technologies which caused by lack of investment, consciousness and security professionals. Based on the analysis of the campus network security issues and combined with the architectures adopted by some colleges and enterprises, this paper provides the college network and information security architecture from three aspects: management, technology and service, finally, it looks ahead the prospects and challenges of college campus network security in the future.

2. NETWORK AND INFORMATION SECURITY PROBLEM

2.1 Threats of network and information security

The threats of network and information security can be divided into two factors: the natural factor and the artificial factor, in accordance with its origin. The natural factor means security threats caused by natural elements, such as hardware fault, software fault, power fault and various kinds of irresistible natural disaster. The artificial factor means security threats caused by human reasons, can be divided into two situations: artificial improper operation and deliberately sabotage. The first situation means security threats caused by users or managers' incorrect operation. The second situation means man-made sabotage that is to destroy, distort, wiretap, counterfeit and access information resources illegally by software, protocol and management vulnerabilities bypass information security policy, it includes network attack, computer virus, Trojan horse and network wiretap.

2.2 Vulnerabilities of network and information security

The vulnerabilities of network and information security divide into software vulnerability, network protocol vulnerability and security management vulnerability. Software vulnerability means security risk caused by abnormal input which is not taken into account at design and compile time or error code. Buffer overflow, special character combination and operating system multitask competition are the most common software vulnerabilities. In addition, the security risk caused by improper software configuration is also belong to software vulnerability, such as system default configuration, frangibility password and system backdoor. Network protocol vulnerability means security risk caused by imperfection of network communication protocol, for example, almost all the protocols of TCP/IP protocols which is widely used on Internet has security risk. Security management vulnerability means that in practical application, users neglect the management of network and information system which

makes the system under attack, such as lack of perfect security management organization, strict security management system, reasonable personnel allocation, strict authorization and approval system, regular approval and checking system, professional security education and training.

2.3 Analysis of campus network security problem

(1). There are a huge number of information systems with complex function. To satisfy the requirements for college teaching, scientific research and management, all the colleges have built various information systems, such as scientific research management system, educational administration system and digital library. These systems have different development platforms, different running environments, different versions, and most of the managers are unprofessional part-timers, which make the campus network to be the target of attackers easily. Attackers can upload Trojan by website vulnerabilities that lead to service interrupt and data leakage or data deletion.

(2). The structure of network is complex and difficult to manage. Campus network divides into campus intranet, financial private network, one-card private network, monitoring private network, and so on. Because of different applications, each subnet has different structure. Besides that, in the old campus, the position of network equipment has changed frequently without proper planning and multiple campuses because of the large campus area, all of these lead to the complex structure of campus network and complex management.

(3). There are many network viruses and spread quickly. Because of the weak awareness of safety, users have not installed the virus protection software or upgraded the virus library in time, which lead to the inundation of network virus. It is not only endangers the security of users' computer, but also makes great consumption of network resources, and affects the normal use of network.

3. COLLEGE NETWORK AND INFORMATION SECURITY SYSTEM ARCHITECTURE

The security system architecture of Northwest A&F University should from the point of view of overall security, through three systems: security management, security technology and service support, to form the college campus network and information security system architecture, as shown in Figure 1.

3.1 Security management system architecture

Thirty percent technology, seventy percent management ^[4], especially for network and information security. On the basis of actual situation of university, according to the principle of who supervises, who takes charge; who operates, who takes charge; who uses, who takes

charge, Northwest A&F University takes three levels management method for campus network information security. The information commission is entirely responsible for network information security, and to guide, check and supervise the school security work; network and educational technology center, as the technical support unit, takes charge of the network and information security technology protection; each office and academy defines the leaders and part-time network managers, to take charge of their unit’s information system and network security management and daily operation. Meanwhile, to formulate and execute strictly efficient campus network and information security system (see Table 1).

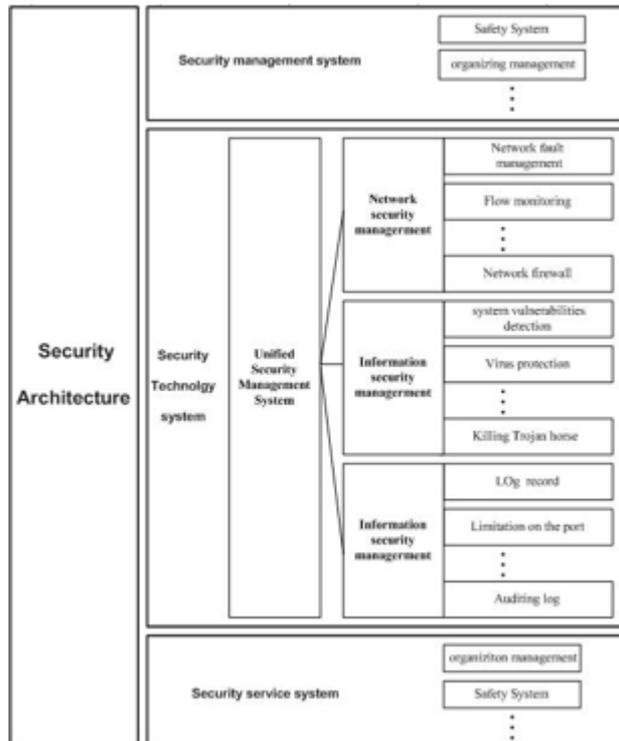


Figure1 Network and information security architecture

Table 1 Security institution of Northwest A&F University

NO.	CN security institution name
1	Network and information security emergency contingency plan
2	Website management method
3	Information system management method
4	Information facilities management method
5	Date security management method
6	CN center room security management method
7	CN users’ network fault treatment standard
8	CN center room server collocation management method

3.2 Security technology system architecture

Security technology system includes three aspects: network security management, information security management and operation and maintenance management. First, a smooth network is the key factor which can ensure the normal running of campus network, it can monitor the export and core node information, so it can restore network quickly when failure occurs. At present, the university build network management platform with Ruijie network to manage all safety equipment. This platform can manage all kinds of interchangers, routers from different brands of campus network (such as Ruijie, Huawei, Huasan and so on), can fully monitor network requirement information, and flow information; second, to set up private network for important information in order to isolate from campus network. The center room of campus network has a certain size of composite security protective measures, and data center server and campus network set access rule through three layers core switches. The center room of campus network should equipped video monitoring, standby power supply equipment, and control measures of water-proof, damp-proof, anti-static and temperature and moisture. Take entrance guard and register system; third, united monitoring and analysis of the whole network security can be realized by united management system platform, managers can grasp the security situation of the whole network. As the source of data and security incident, the managed object means the object can be collected by platform, mainly includes firewall, Ruijie web application firewall (WG-3000) and so on; at last, the operation and maintenance management can guarantee the web operation quality, to avoid personal risk in operation and maintenance, and do not open a remote desktop at firewall, or limit the SSH port management in specific IP range.

3.3 Service support system architecture

Service support system includes daily security inspection, cyclicity security check and cycle security training. Daily security inspection includes regular checking for computer room, security vulnerabilities check for server, network equipment and security equipment, update operation system and patch in time and set password to ensure the update frequentness. Dispose in time when equipment failure occurs to guarantee the network and application system stable operation. Meanwhile, carry out security check regularly, inform safe work condition, and adjust in time.

4. DEVELOPMENT TENDENCY AND CHALLENGE OF CAMPUS NETWORK INFORMATION SECURITY

With the increase of hacker attack capability and coverage, although college campus network is relative independence compared with internet, while because of the connection and interoperability of Internet which makes university campus network be also difficult to keep

alone, so the development of network information security situation is becoming more and more serious for campus network. The current network information security protection work can't just rely on hardware protection such as the traditional antivirus and protective wall, and also need to strengthen its protected object and subject and to enhance the software development aimed at network information security. The government and relevant department should complete related laws and regulations of network security to prevent any network security information crime vulnerability. At present, national education department has required each university to check their own network information security and register the infrastructure of key information and promote the classified protection of information security in education sector. Currently, the computer information security is developing towards high intelligent, that is to say the promotion and popularization of computer intelligent terminal will be quickened, and the service area and operational activity associated with it will be developed and used further. Therefore, we need to deal with this development tendency and challenge positively. We believe with our joint efforts, all kinds of information security problems could be resolved in the future.

5. CONCLUSION

Network information is like a double-edged sword, we take its advantage to improve our life while should pay attention to not be hurt by the blade. Network information security is a constantly changing and increasingly update field, network and information security is relative, on hundred percent of absolute security is not exist. Face with the complex and diverse network security environment, only use one protective measure cannot guarantee the security of network information effectively, we need overall planning, comprehensive consideration, correct strategy and interaction with each other to build a comprehensive, dynamic controllable, safe and reliable network and information security system architecture. Therefore, network and information security needs us to deal with seriously and cautiously, so the security incident can be reduced to a great extent, to protect the network and information security.

REFERENCES

- [1] ZHANG Wei, A study on problems and countermeasures of computer network and information security [J], China CIO News, 2015, 7:58-59 (in Chinese)
- [2] ZHENG Qing-kai, XU Feng, ZHANG You-dong. Information security architecture [M]. Beijing: Electronic Industry Press 2010.
- [3] WU Hai-yan, YU wen-xuan. A review of university information security architecture based on enterprise architecture [J], Journal of Wuhan University (Natural Science Edition), 2012, 58(S1): 102-106 (in Chinese)

- [4] XING Qi-jiang, LIU Hui. The construction and management of network security architecture in the information era [J]. Computer Security, 2006, 10(10): 41-43 (in Chinese)