Creative Education
2012. Vol.3, No.4, 406-412
Published Online August 2012 in SciRes (http://www.SciRP.org/journal/ce)
http://dx.doi.org/10.4236/ce.2012.34064

A New Construction Scheme for Information Security Lab

Li Zhu, Huaqing Mao, Zhiwen Hu
Wenzhou University Oujiang College, Wenzhou, China
Email: 38995791@qq.com, mr.maohuaqing@qq.com, 448766175@qq.com

Received May 31st, 2012; revised June 28th, 2012; accepted July 10th, 2012

At present, it is urgent for us to build fully functional information security laboratory. In this paper, the function and requirements of a new information security lab are analyzed. And a construction scheme for information security laboratory is put forward. The lab not only provides services for teaching and training, but also provides security evaluation, authentication and extension services for local governments, institutions and enterprises. Our teaching and training practice shows that the scheme of such information security laboratory proposed in this paper is effective and reasonable.

Keywords: Information Security Laboratory; Construction Scheme; Extension Services

Introduction

At present, information security has become a comprehensive, cross-discipline area, which integrated the accumulation of knowledge and latest research results on computer, telecommunication, microelectronics, mathematics, physics, and many other areas. (Zhang, Huang, & Liu, 2004) Information security is also a complex system, which involves the construction of information infrastructure, networks and systems, information systems and business application systems development, information security laws and regulations and safety management system etc.

Therefore, information security is a direct project-oriented and application-oriented professional field. Information security education is an engineering culture (Wang, Tan, & Huang, 2006). If engineering practice system is established in colleges and universities, the students could carry experiments and practice in the system, which will have great significance in improving practical ability and the cognition ability of technology (Gu & Huang, 2006). In the situation where a great deal of security talents are required, the universities should play to their strengths to build an appropriate information security laboratory with perfect functions.

Why to Build Information Security Laboratory in Colleges and Universities?

The great development of globalization and informatization has brought rare opportunities for China's information industry development, but it has also presented a serious challenge. The rapid development of Internet has directly affected innovation of science and technology, the development of information industry and the rise of knowledge economy. Information network is gradually becoming the foundation of economic prosperity, social stability and national development; at present, the number of Internet users in China has reached 360 million. The online transaction amount is as high as $30 billion every year. However, the network brings unprecedented hidden danger to our life. According to the estimation of National Computer Network Emergency Treatment Coordination Center, the annual production of dark industry formed by cybercrime has exceeded $238 million, which results in a loss of more than $7.6 billion. A page will become a hacker "dinner table" in every 5 seconds; the rate of being experienced "network link" for small and medium-sized web sites is up to 5 per thousand.

At the same time, with the evolution of network convergence and next generation networks, a large number of new businesses and technologies without security evaluation have been brought to the market. The inherent security risks in the IP network are extending to other networks, which will lead to more security risks. It is visible that information security issues have changed from purely technical issue to global national security issues. Along with the process of information developing, the increased information security risks and threats have become the key problem of the national security and social stability. Faced with the increasingly grim situation of network information security, taking scientific and effective measures is necessary and feasible.

At present, the talents of network technology tend to be saturated. According to research report published by the computer world news has estimated the demand for the national information security talents will reach to more than 300,000. Currently, quantity of information security engineer talents is few; especially the compound talents are lacked. For example, the network managers are not familiar with storage expertise and storage management planning, and it is seriously short of manpower for the professional storage device manufacturers and service providers. There are few training institutions to offer storage classes, even if they open the storage courses with high training cost. It is forecasted that the demand of national network storage talents is more than 600,000 per year. However, it only offers around 10,000 a year presently, which indicates that the demand gap is enormous.

From above analysis, we can see that the demand of network information security talents in China is lacked, and the ability of talents also need to be further enhanced. It is necessary and urgent to build high level information security laboratory with completed function in college and university. The laboratory should meet the needs of different levels of information security laboratory base and talent training base, which will promote practical ability training of the students, broaden students' ideas

and vision, improve the quality of teaching, and finally provide good conditions for cultivating innovative information security talents in universities and colleges.

Current Status & Construction Target

With the development of the network and information technology, information security has become the key information technology of 21st Century. Therefore, the ministry of education has established information security professionals from 2000. Currently, there are more than sixty colleges to start the information security major as well as the higher vocational colleges. Domestic universities such as Wuhan University, Beijing University of Posts and Telecommunications, Shanghai Jiao Tong University have set information security major early and constructed large-scale labs of information security. In addition, each university or college who has opened information security major, combined with their own characteristics, put forward the suitable construction ideas for the laboratory construction; however, there are still some limitations and deficiencies.

Firstly, Many network and information security laboratories are reconstructed from the original network engineering labs, which are lacking special security experimental equipments and unable to complete professional experimental courses.

Secondly, at the beginning of the construction, only the simple experimental teaching process is considered, which leads to the students' little knowledge about the experiments. Besides that, because of the lack of communication between the students and the teachers, students learn passively, and the inspiration of innovative consciousness that the teachers give to the students is not enough. This will affect the students' ability to solve problems independently

Thirdly, the laboratory of Information security serves for a single object without its own hardware advantages, which can't provide the requirements of local extended service and scientific research requirement of the teachers.

Therefore, building a network and information security laboratory combined with scientific research, teaching and service will play an important role in the development of information security technology as well as the training. It also provides security evaluation, authentication and extension services for local governments, institutions and enterprises.

Function Requirements for Information Security Laboratory

On the one hand, we should pay attention to the related forefront research, intensive technologies and hot application in information security field; on the other hand, it is needed to build information security engineering practice environment to cultivate comprehensive information security talents. Engineering application of information security is strong; therefore, we should focus on authenticity of the experimental environment and design comprehensive experiments to cultivate security sense of the students (Aboutab, 2006). The following three aspects of services are supported by the lab:

Firstly, it is research-oriented. It will provide good experimental environment for scientific research and validation including the basic theory, security frame, security mechanisms, security technologies and other aspects.

Secondly, it is teaching-oriented. The lab will help the students to improve their practice activity. In the information security laboratory, the students could carry out security experiments in different levels and different directions.

Thirdly, it will support extension services. It will support socialization training services for information security majors. The two talents cultivation modes including "school education" and "vocational training" need to be combined; the two modes of "teaching in class" and the "online learning" also need to be combined. It also provides multi-level training and certification mechanisms of universal and specific complementary levels; it also supports safety training services and products promotion. Through the combination with well-known security vendors, it provides training and certification of security products to meet the needs of enterprise users; it also supports testing function for network devices and security devices; it supports testing and validation services for large network, and also it provides security test and evaluation on the commercial network.

Requirements for Network and Information Security Laboratory

The construction of information security lab involves many new technologies. As a fully functional network security lab, it is able to simulate real environment as much as possible. At the same time, we should deduce the cost of devices to achieve high-yield with low-input. The lab will provide the students with the same work environment as they work after graduation. Based on the above considerations, the following principles (O'Leary, 2006) should be confirmed:

1) Practical, easy to use and apply.

The security devices used in lab should have strong practicability. We should adopt mainstream security devices and software in the market, combine with the mainstream command line configuration so that the students can experience and learn a variety of network attack and defense techniques in real work environment, which guarantees that what skills they have learned can be fully applied in the work after they graduated. Besides that, the convenience of teaching in the lab needs to be taken into full consideration. It should be easy to use for the teachers and students. The opening management system is adopted for unified management. The system provides different users including students, teachers and administrators access to the lab by the network, which makes it possible that the users can do experiments remotely. This will improve the utilization rate of the lab, and the teachers and students can carry out experiments and communicate in their spare time.

2) The technology should be advanced, function of the lab should be comprehensive and devices should be compatible and scalable.

Firstly, with the rapid development of the network security technologies, the equipments and management systems in the lab should be updated timely to adapt to the development of the technologies. So, the lab should have good compatibility and scalability at the beginning of lab construction. When the new technologies appear, the hardware and software can be upgraded, and the new equipments can be used in the laboratory. The lab will provide devices including firewall, IDS/IPS, VPN, anti-virus, anti-spyware, high security, hacking, encryption and decryption, and other security devices and software etc, which will provide a more comprehensive network security learning platform for us.

Secondly, the network information security technologies are

constructed based on the network protocol. Current IPv4 network is transiting to the next generation network which supports IPv6 protocol. In addition to providing nearly infinite IPv6 addresses, security of IPv6 is also greatly improved. Therefore, we should fully take the compatibility of the IPv6 protocol into account in the future. The laboratory design will consider future employment demand for the students. So the availability and extension should be taken into account.

3) It will provide services for objects with different levels.

The related courses of information security are covered with wide range of content. The students of different levels and different majors need to master different theory and technologies. This requires that the lab not only provides experimental teaching environment for the teachers and students in our college but also provides network security vocational training for the whole community. Besides that, the lab will also provide security evaluation, authentication and extension services for local governments, institutions and enterprises (Yang, Yue, & Liaw, 2004).

A Construction Scheme for Information Security Laboratory

Function Structure

The function structure of the lab is shown as **Figure 1**.

The information security lab is divided into three regions: training room, work area and the equipment area. Each area is separated by toughened glass. The training room is used for training and teaching, which includes platform, LED screen announcement area, blackboard, projection area and hexagonal tables. The training room will meet the need of eight-group students to do experiments at the same time. Each group has six computers. The working area is provided for laboratory administrator and teachers. There are four sets of work tables and chairs for teachers. The equipment area is used for placing experimental equipments, including network cabinets, server cabinets and UPS equipment area etc. The network cabinet area is designed for placing various security equipments and network switching equipments; the server cabinet area is designed for placing required servers; the UPS equipment area is used for placing UPS host and UPS battery.

The functions provided by the lab include training, teaching, security evaluation authentication and extension services for the local governments, institutions and enterprises.

Training & Teaching Platform

The topology of the information security lab is described in **Figure 2**.

Each terminal group connects to the central switch by anti-virus system, intrusion defense system and firewall, and eventually connects to the machine Cabinet Server. Each group corresponds to a cabinet server, which uses virtual machine to simulate various servers (such as: patch Server, WEB server and virus server) that act as target area. The work area of teacher can use a projector, security audit system and log audit system to display students' behavior of attack target area. Each

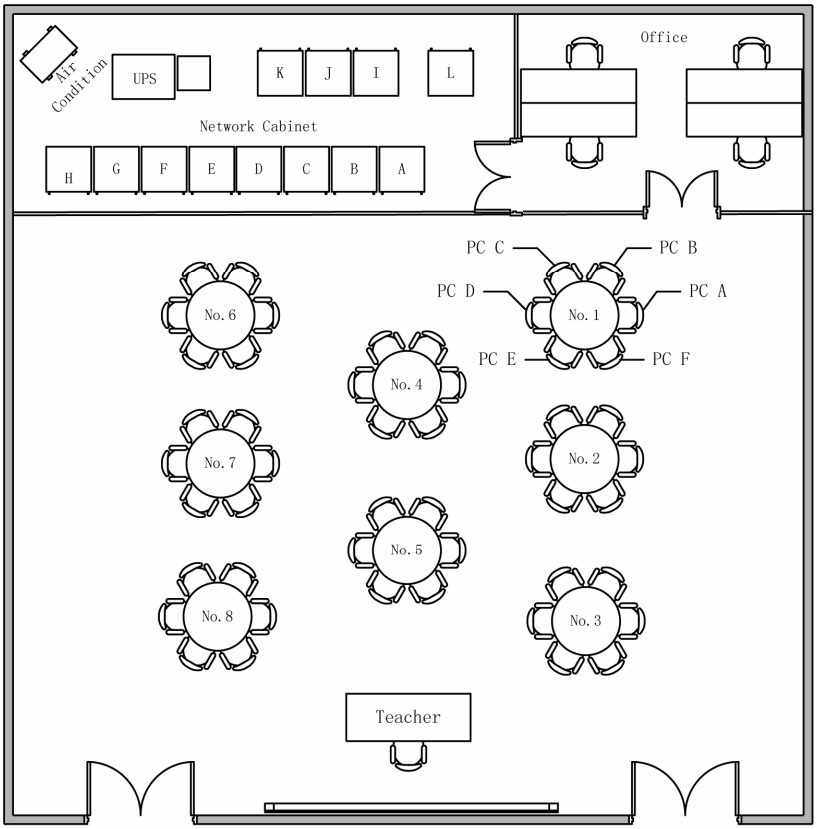

Figure 1.
Structure of the lab.

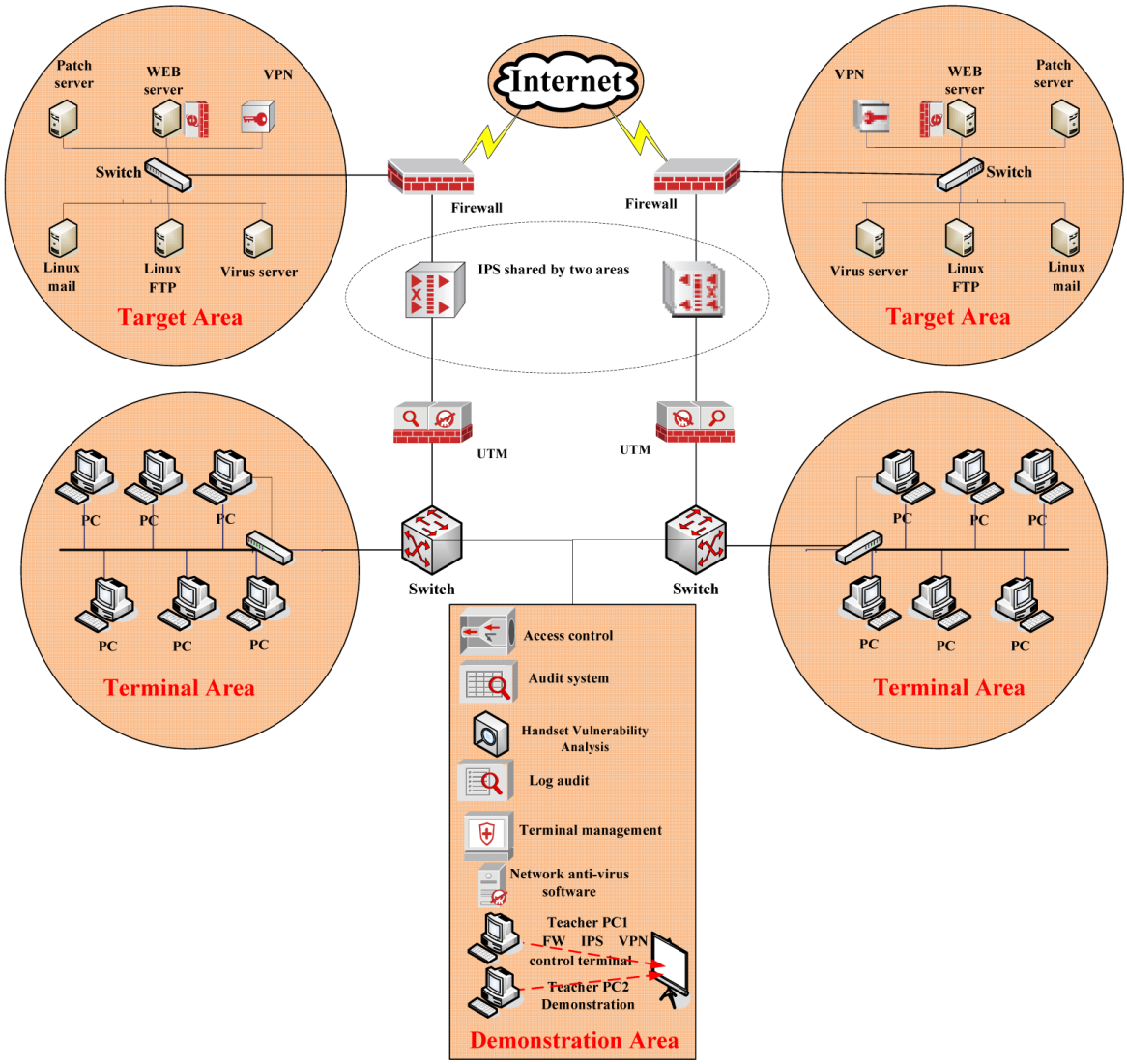

Figure 2.
Topology of the information security lab.

of the two groups students share an intrusion prevention system. The security devices are put in six cabinets as **Figure 3**.

Experimental Modules of Training & Teaching

The content division of information security experiments is shown in **Table 1**.

Security Evaluation, Authentication and Extension Services

The center of information security evaluation as is shown in **Figure 4** has owned advanced information security vulnerability analysis resources, and evaluation equipments; the functions provided by the center include: basic research on vulnerability, product security vulnerability detection, system hidden analysis and testing equipments; in accordance with national laws and regulations, it can provide technical support to countries in information security area. It also provides the community with public services, information technology products and security vulnerabilities analysis of the systems and communications. The information security center is responsible for information network of the party, security risk evaluations of important information system; developing information technology products, security test and evaluation of systems and engineering construction; theoretical study on information security testing and evaluation, technology development, standards development and so on.

It also provides product testing, evaluation and certification services for computer information system of the party and government organs in Wenzhou and Zhejiang areas. It accepts delegates of government departments and industry, and provides testing services of products, engineering and services. The security evaluation services include security evaluation testing, security system counseling, security system building, security program reorganization, host evaluation, business systems testing, network architecture evaluation, data security evaluation, security consolidation, emergency response and security patrol. During the development of technical system

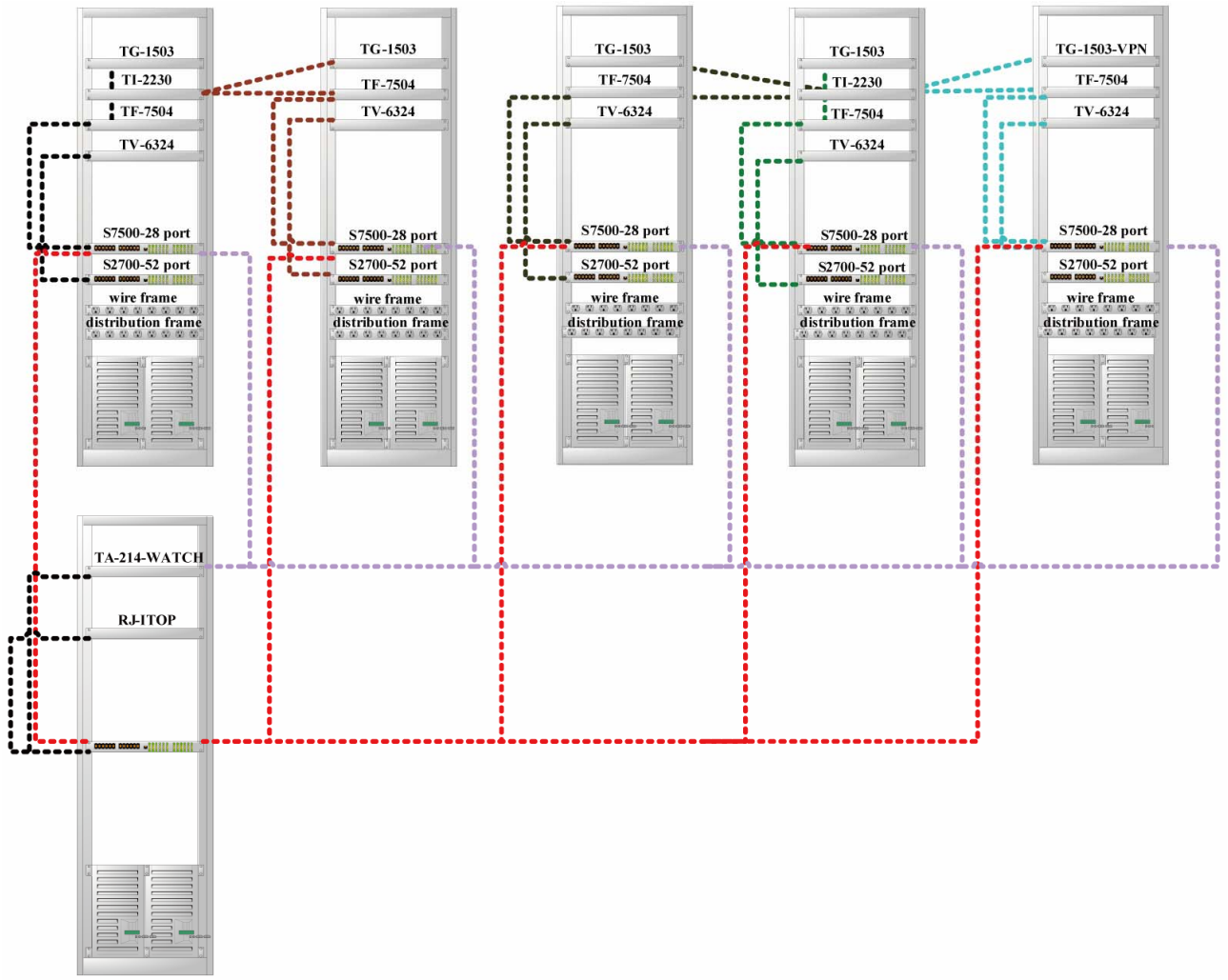

Figure 3.
Cabinets of security devices.

Table 1.
Experiment modules.

The experiment modules	Experiment projects
Security access control technology	Deployment experiment, routing experiment, NAT experiments, firewall and IDS experiment, logging system experiment
Security technology (VPN)	VPN deployment, IPSEC VPN, SSL VPN, Gateway to gateway tunnel configuration, the client to the gateway tunnel experiment
Detection and defense technologies	Trojan detection and defense, overflow detection and defense experimental, denial of service and defense detection, system vulnerabilities category detection and defense, worms detection and defense, HTTP detection and defense
Virus protection technology	Feature code testing, calibration and detection of the virus behavior, virus and malware virus
Vulnerability analysis technology	CGI vulnerability analysis, the buffer overflow analysis, denial of service analysis, backdoor vulnerability analysis, and protocol vulnerability analysis
Security audit technology	Behavior audit analysis, log analysis, database audit analysis, equipment and system audit analysis
Terminal security technology	Software patches and system distributing technology, terminal behavior management technology, illegal inline management technology, illegal connection management, experimental remote management and terminal security access
Attack and defense technology	Scanning technology, sniffer and Anti-sniffer technology, WEB attack and defense technology, the buffer overflow attack and protection, network spoofing attack and defense, DDOS attack and defense and password cracking

construction, the network security, host security, application security, and data security need to be considered. The technology tools include terminal security management system, network anti-virus software, vulnerability scanning system, security audit system, access control system, firewall, antivirus gateway, intrusion prevention systems, and VPN systems. The security management system includes safety management rules, security management institute, personnel security management, system construction management and operation and maintenance management etc.

The information security evaluation service modules are shown as **Table 2**.

Conclusion

Information security education is a kind of engineering culture education. In this paper, the function and practice requirements of an information security lab are analyzed. The scheme of an information security laboratory is proposed. The lab provides not only services for teaching and training, but also security evaluation, authentication and extension services for local governments, institutions and enterprises. Our teaching and training practice shows that the scheme of such information security laboratory proposed in this paper is effective and reasonable.

Acknowledgements

This work was supported by a grant from Zhejiang province college lab research project: Research on construction trinity of network and information security lab (Grant NO. Y201236) and teaching reform project of Wenzhou University in 2012: Construction on innovation practice teaching system of Network

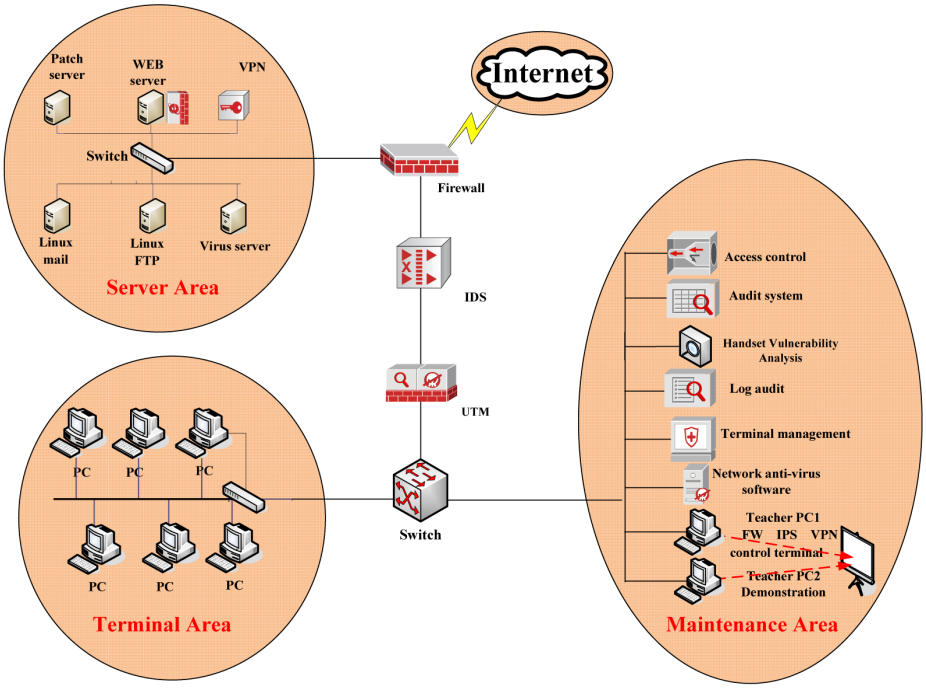

Figure 4.
Topology of information security evaluation center.

Table 2.
Modules of information security evaluation service.

Project name	Service content	Service object
Device performance and attack-defense detection evaluation	Device performance and attack-defense detection technology experiments	Enterprise, security product manufacturer
Security evaluation project	Security evaluation and evaluation, classified protection evaluation service	Government, Enterprise, financial and energy enterprises
Company qualification certification	Company security service engineering aptitude intelligence and company emergency response aptitude intelligence	The enterprises engaged in information security
Personnel qualification certification	CIW, CISP and CISSP	Government and personnel staff of information construction in enterprises and institutions
Security training certification	CIW, CISP and CISSP	Government and personnel staff of information construction in enterprises and institutions

and information security (Grant NO. 12JG68B).

REFERENCES

Aboutabl, M. S. (2006). The CyberDefense laboratory: A framework for information security education. *Proceedings of the 2006 IEEE Workshop on Information Assurance*, Phoenix, 10-12 April 2006. doi:10.1109/IAW.2006.1652077

Gu, N. J., & Huang, L. S. (2006). Exploration on information security professional curriculum. *Journal of Beijing Electronic Science & Technology Institute, 14*, 13.

O'Leary, M. (2006). A laboratory based capstone course in computer security for undergraduates. *SIGCSE'06(ACM)*, Houston, 1-5 March 2006.

Wang, H. H., Tan, Y. S., & Huang, W. Z. (2006). Discussion on information security professional talent training mode. *Journal of Wuhan Institute of Chemical Technology, 28*, 56-59.

Yang, T. A., Yue, K.-B., & Liaw, M. et al. (2004). Design of a distributed computer security lab. *Journal of Computing Sciences in Colleges, 20*, 332-346.

Zhang, H. G., Huang, C. H., & Liu, Y. Z. (2004). Talent training and course system of Information security profession. *High Science Education, 2*, 16-20.