Research on Host Security Protection Technology System Based on Linkage

Feilu Hang[1,*],Linjiang Xie[1], Wei Guo[1], Yao Lv[1] and Wei Ou[1]
[1]Information Center, Yunnan Power Grid Co., Ltd, Kunming, Yunnan, China, 650217

Article Info
Volume 83
Page Number: 5479 - 5487
Publication Issue:
July - August 2020

Article History
***Article Received:** 25 April 2020*
***Revised:** 29 May 2020*
***Accepted:** 20 June 2020*
***Publication:** 28 August 2020*

Abstract

With the rapid development of information technology and network technology in China, information and network security in China is facing great threats, such as hacker invasion, virus infection, network crime, important information leakage, etc., which seriously affect the information security and host security of our country. At present, the traditional defense system can be more effective. However, the most comprehensive protection mechanism can only ensure the security of the system for a period of time, which will quickly find the defects of the system protection mechanism and use it. Therefore, the host will be constantly threatened by the network security. Therefore, our country must strengthen the host security protection technology research, which will better protect the security of our network information. Linkage mode is a way of information sharing between host firewall and host intrusion detection system, which can truly realize integrated active defense. Therefore, based on the linkage mode, this paper studies the host security protection technology system, which will better realize the host security protection. At the same time, this paper develops a host security immune trusted scheme. Finally, the system model is designed.

***Keywords:** Linkage, Host Security Protection Technology, Security Strategy;*

1. Introduction

With the continuous development of communication network technology, China's network construction has entered a period of rapid development. At present, the annual growth rate of network equipment in China is about 15%, and the annual growth rate of network security equipment is more than 70%[1]. With the development of network technology, Internet plays a more and more important role in people's daily life. A large number of network applications, such as e-commerce and online banking, bring great convenience to people's daily life, but at the same time, it also provides a broad platform for the illegal elements to make profits[2]. In recent years, crimes committed through the Internet are increasing day by day, which has a great negative impact on the harmonious development of the whole society[3]. Therefore, network security has gradually become one of the core of the network. However, in the face of increasingly complex network environment, the function and efficiency of network security system has become a very prominent problem. Host security technology has become one of the core concepts of network management in the future[4].

The need for host protection is huge. The core of computer and network operation is data. If there is no data, then there is no security. However, data belongs to the host computer, including personal computers, servers and large disks[5]. At present, viruses and attack threats are attacks aimed at obtaining or destroying data, which is the last line of defense against hosts. Therefore, whether it is a network attack or a peripheral spread attack, we must build a strong defense line on the host, which requires us to study host security protection technology[6].

At present, the network environment is very complex, and there are many security problems. Viruses, Trojans and worms have become familiar to us. Therefore, operating system manufacturers, network equipment manufacturers, system security manufacturers and so on put security protection in a very important position[7]. Linkage mode is a way of information sharing between host firewall and host intrusion detection system, which can truly realize integrated active defense. Through the analysis of the difference between the integrated and the linkage, this paper analyzes the linkage of the host security protection technology[8]. At the same time, this paper develops a host security immune trusted scheme. Finally, the system model is designed[9].

2. Host security risk analysis

2.1. Overview of host security risks

With the rapid development of network, hosts are facing many threats, as shown in Figure 1.

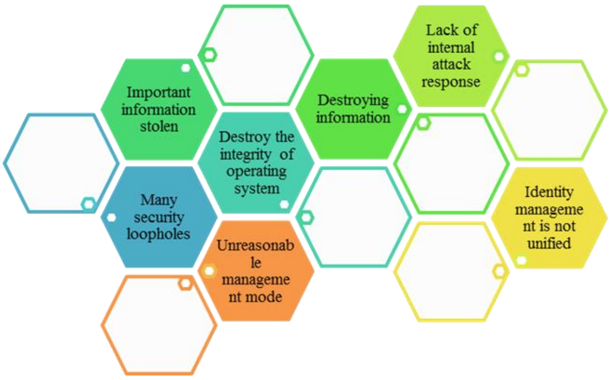
Lack of internal attack response
Important information stolen
Destroying information
Destroy the integrity of operating system
Identity manageme nt is not unified
Many security loopholes
Unreasonab le manageme nt mode

Figure 1. Overview of host security risks.

2.2. Many security loopholes

Because there are many loopholes in the host system, many network criminals will take advantage of these vulnerabilities to launch attacks on the system. At the same time, host system vulnerabilities are not immutable[10]. Through the analysis of vulnerability code examples, we can find that there are new types of vulnerabilities[11]. Although software manufacturers regularly check the system regularly, the intruder usually finds the vulnerability before the vendor checks and uses the vulnerability to do illegal things. Operating system security vulnerabilities have brought a lot of trouble to users. Generally, users will upgrade and improve the host operating system by "patching". Although "patching" to update the operating system is feasible, it also has defects. Generally, system patch has lag, which is the biggest defect of patch type[12]. The lag of system patch is shown in the following aspects. First, the test to patch distribution cycle is long, which can't guarantee the security of the operating system. Second, there is a relationship between patches and vulnerabilities. In general, vulnerabilities are first found and then "patched"[13]. Vulnerabilities are constantly updated, and patches will never be finished. Third, vulnerability tools tend to be automated, and the time for server administrators to "patch" will be shortened[14]. Before the patch is released, network criminals will use the vulnerability to destroy the server. Therefore, "patching" is a way to remedy the vulnerability after it appears.

2.3. Destroy the integrity of the operating system

There are many factors threatening the security of the host, and the biggest threat to the host is to destroy the integrity of the host operating system[15]. Many users do not check during startup, running and service, which will result in virus embedded in the program of executing code or replacing the original program. With the wanton spread of malicious code, the host will be poisoned. After the malicious code is activated, it will obtain the user's current permissions. Through wanton spread, we will destroy the integrity of the host operating system as a whole, which will affect the normal use of users. For example: modify the server information, delete important information, destroy the server, which will cause the server operating system failure.

2.4. Theft of important information

Important information is generally stored in the host computer, which is very important to the computer. Information has the nature of replication and dissemination, which is also the most important tool in the era of big data. The highly developed information will make it easy to copy information. If some important information is disseminated or copied, it will damage the interests of others, which will also have a serious impact on institutions or individuals. If the state's confidential information is leaked, it will pose a threat to national security. Some users use technical loopholes to carry out illegal operations, which will cause important information to be stolen.

2.5. Destroying information

The important information in the host is not only in danger of being copied, but also in the risk of being modified. Malicious modification of computer information will destroy the integrity, authenticity and effectiveness of information. If information loses its validity, authenticity and validity, it will have a great impact on users. Some users' hosts do not use security protection measures. Network criminals take advantage of this vulnerability to modify the important information of hosts.

2.6. Lack of measures to deal with internal attacks

Authorized legitimate users are insiders. However, most of the internal attacks are from inside the information system to the host. Host security measures are generally to protect external host attacks, internal protection measures are less. Therefore, people often ignore the prevention of internal personnel. In terms of attacking hosts, insiders have more advantages than outsiders because they can get access to the important information of hosts and know more about the security and defense measures of hosts. Internal users are familiar with the host situation, so it is very easy for insiders to attack the host by using the defects of host system and the vulnerability of defense measures.

2.7. Identity management is not unified

There are various kinds of security problems in the host, among which the administrator problem is the biggest and most common problem. The authority of the host administrator is very large, but the identity of the host administrator is relatively single. Therefore, the host administrator brings security risks to the host. Because the host is used by many people, many people use the same host account and password when the host operates business. Therefore, it is difficult to distinguish the user identity of the host, and the host can't grant permissions according to the identity of the user. When the host cannot control the access rights, a series of errors may occur in the operation. At the same time, the security of password authentication method is low, network criminals can easily obtain password authentication to launch attacks on hosts.

2.8. Unreasonable host management mode

Each host is managed and maintained by the administrator independently, which is the stand-alone management mode. At present, the management mode of most hosts in our country is single machine management mode, which has security risks and low efficiency. The host administrator maintains the host one by one. If there are many hosts, the host administrator needs to spend a lot of time, and the management efficiency is low and the effect is not good. For some emergencies, the host administrator can't solve it in time, which will have more security problems. Hackers use network viruses to infect multiple hosts, which will lead to the paralysis of the host system.

3. Combination of host firewall and host intrusion detection system

3.1. Integration mode

Generally, host firewall and host intrusion detection coexist in a system in series for protection, which is a strategy to provide access control for host firewall by using host intrusion detection results. By forming a whole, we can achieve the purpose of improving system security. The integration mode has the following advantages.*3.1.1. Realize active defense*

The integration mode is concatenated, which determines the detection and blocking before the attack, rather than just listening. The integration method combines traditional access control with intrusion detection technology, which can share certain information. Through integration, the host realizes the unification of security policy, which will achieve the purpose of active defense.

3.1.2. "Defense load" balancing

Rids often needs to process abnormal data packets, which will consume a lot of system resources. In the integrated mode, the access control module is used to "purify" the abnormal packets, which will help to reduce the workload of the detection engine. However, the integration method does not fundamentally solve the limitations of intrusion detection system, which also brings other problems. Detection engines usually have a high false positive rate. Working in this way will produce a lot of firewall access control rules that block the network. If we do not analyze the results of intrusion detection engine, we will be difficult to use the correct analysis results to formulate security policies, which will eventually affect the normal network services. There is a lack of analysis and synthesis of intrusion detection results in the system, which will produce a large number of firewall rules. Therefore, firewall rules will greatly affect the performance of firewall system. At the same time, we also lack the information feedback of firewall to intrusion detection. Although the active defense is realized by integration, there are still many defects, such as robustness, efficiency and practicability.

3.1.3. Linkage mode

The linkage mode is a way of interaction between host firewall and host intrusion detection system in parallel, which will better realize information sharing. Through parallel connection, the host will truly realize the integrated active defense, which will better protect the security of the host. The main difference between linkage mode and integration mode is that host firewall and host intrusion detection system are separated, and sharing information and interaction are bidirectional. At the same time, the linkage mode can also be divided into direct linkage and indirect linkage.*3.1.4. Direct linkage*

The direct linkage mode is a linkage mode that can interact directly without the second party's transfer, which will make the host firewall interact with the host intrusion detection system better. A unified communication interface is needed between host firewall and host intrusion detection system, which has the advantages of independent system, high reliability and fast response speed. Direct linkage only separates the two functional modules in the integration mode, which lacks the comprehensive reasoning and analysis between multiple subsystems. At the same time, due to the lack of comprehensive analysis, hosts may generate wrong firewall access control rules, which will cause dos and firewall performance degradation.

3.1.5. Indirect linkage

Indirect linkage is relative to direct linkage, which requires information to be transmitted to the other party through the transit of the third party. Due to the intervention of the linkage console, information can be shared and interacted among multiple similar or heterogeneous subsystems. After comprehensive reasoning and analysis, we can’t only improve the accuracy of alarm and reduce false alarm, which can reduce the communication flow between subsystems. Through indirect linkage, we can improve the performance of the system. Through comprehensive analysis, we can get the alarm, which needs to formulate firewall access control rules according to the corresponding security policy. At the same time, the filtering information of firewall can also be fed back to the linkage console, which will better adjust the security policy or control rules. Indirect linkage has the following advantages. First, indirect linkage really realizes the linkage type active defense. Before the host firewall and host intrusion detection, the linkage console is added, which will form an information loop. Through the maximum information sharing, we realize the integration of detection and defense, which will improve the security of the system. Second, through information sharing and global comprehensive analysis, we can greatly reduce the number of false alarms, which will improve the accuracy of detection. Thirdly, as the policy center of the whole system, the linkage console ensures the consistency of security policies. At the same time, indirect linkage is easy to manage and flexible in policy configuration and system monitoring.

4. Trusted scheme of host security immunity

4.1. Host trusted architecture

In order to meet the reliability and practicability of the host system, this paper makes a comprehensive design of the host security and trust. Through the combination of software and hardware, this paper reinforces the host trusted architecture. In this paper, we take the bottom layer as the trusted root of the trusted chip. By ensuring the security big data of the lower layer, we can realize the active defense and security immunity of the host, which will better deal with unknown attacks. Through the host trusted architecture, this paper implements a variety of security functions, such as integrity detection, identity authentication, encrypted communication, key agreement, access control and so on, which will be more in line with the core competence requirements of secure computing environment. The trusted architecture of host security immunity is shown in Figure 2.

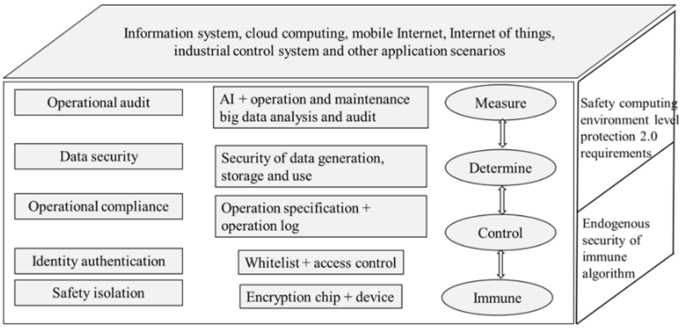
Information system, cloud computing, mobile Internet, Internet of things, industrial control system and other application scenarios
Operational audit
AI + operation and maintenance big data analysis and audit
Measure
Data security
Security of data generation, storage and use
Determine
Operational compliance
Operation specification + operation log
Control
Identity authentication
Whitelist + access control
Safety isolation
Encryption chip + device
Immune
Safety computing environment level protection 2.0 requirements
Endogenous security of immune algorithm

Figure 2. Trusted architecture of host security immunity.

The host security trusted architecture can ensure that the architecture, resource configuration, operation behavior, data storage and policy management can be trusted. Through the dynamic measurement and evaluation of the credibility value of various elements, we can achieve the purpose of active defense. Host security immune trusted architecture includes five levels: security isolation, identity authentication, operation compliance, data security and operation audit. The process of active defense in the architecture can be divided into four collaborative processes: measurement, determination, control and immunity, which will protect the computing resources of the host from the interference and destruction of unknown malicious behaviors. By encrypting chips and devices, we can be a physical trusted core. Through the trusted basic software, we can monitor various behaviors of the system. By combining with the virus antibody in the attack knowledge base, we can measure and judge the threat. By calling the relevant security policies through the control mechanism, we can realize the active security immune protection of computing nodes.

4.2. White list generation based on immune algorithm

By recognizing the immune tolerance process of non self and self, the immune system provides active defense mechanism for the body, which will maintain homeostasis in the body. This method can be used to detect a large number of negative lymphocytes by using the negative selection algorithm. NS has been used in virus protection, human intrusion detection, spam detection and other fields.

In this paper, we use ns algorithm to generate and update the white list, which can realize the dynamic identification of trusted and untrusted behavior. In this way, NS algorithm can achieve the purpose of active defense. First, the detector is randomly generated, which will match each element in the self-set. By collecting unmatched mature detectors, we can discard the matched ones. By performing non autodetection, we can select individuals from the protected data, which will match all elements in the mature detector set. If we can match, we can judge that it is not self. Otherwise, we judge it as self.

In the iterative process, the algorithm is globally convergent while preserving the next generation of the best individuals. The probe is used to collect the data generated during the operation of the host. We can use deep packet analysis to analyze the fields, which will be further compared and filtered through the whitelist. At the same time, the system maintains the white list through security immune algorithm. In essence, the process of data analysis is the process of feature modeling, extraction and matching for the data processed in the bus.

The security detection point set is $A = A_1, A_2, ..., A_n$, the threat detection point set is $D = D_1, D_2, ..., D_m$, and the white list set is $V = V_1, V_2, ..., V_k$. Immune algorithm will determine the white list V by calculating the distance between security monitoring point A and threat monitoring point D.

In the immune algorithm, through the threat detector to detect the threat type, intensity, target, duration and other indicators of operational instructions, we can build a quantitative model, which will better calculate the threat quantitative value. The detector can actively match the detected threat with the antigen. According to the logical relationship and affinity index of immune network, we can calculate and form the white list items. Let A_g be the affinity of threat command set antigen, we can get formula 1.

$$Ag_k = \frac{1}{1+t_k} \tag{1}$$

Among them, t_k is the binding strength of antigen t and antibody k .

Immune recognition is a learning process. The result of learning is to improve the affinity of individual immune cells, expand the population size, and save the optimal individuals with immune memory, which will form a white list with the ability of threat discrimination. When the host system encounters a security threat of the same structure, the host protection system can quickly trigger the security policy for active defense.

5. Research on host security protection technology system based on linkage

5.1. System model

In this paper, the system structure model of the linkage host security protection system is established, as shown in Figure 3.

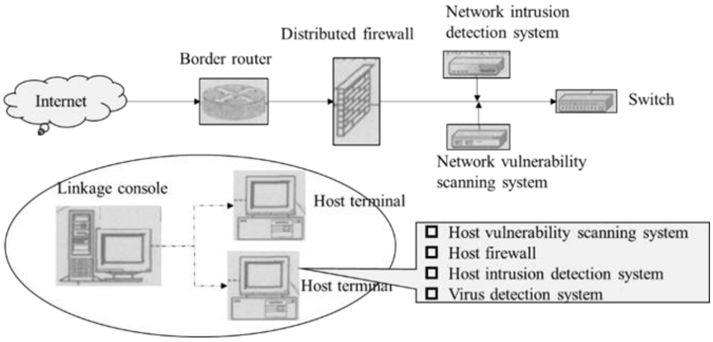
Internet
Border router
Distributed firewall
Network intrusion detection system
Switch
Network vulnerability scanning system
Linkage console
Host terminal
Host terminal
□ Host vulnerability scanning system
□ Host firewall
□ Host intrusion detection system
□ Virus detection system

Figure 3. System structure model of linkage host security protection system.

5.2. Structure of host security protection system

The whole protection system consists of two parts: the linkage console and the terminal host. The terminal host system includes host firewall subsystem, host intrusion detection subsystem based on log analysis, virus detection subsystem and audit centralized subsystem to form a multi-level integrated host protection system. The system structure is shown in Figure 4.

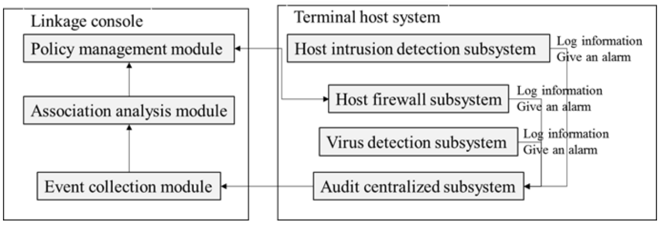

Figure 4. Composition structure of linkage type host safety protection system.

5.3. Workflow of host security protection system

The workflow of host security protection system can be divided into five steps: original information collection, format standardization, real-time analysis, real-time report output and real-time response. First, collect the original information. Collect the log information and alarm information of each subsystem of the host system in real time. Second, format standardization. Audit centralized subsystem is responsible for transforming the alarm information from analysis and extraction into standard event format, and then storing it in event database. Third, real-time analysis. The correlation analysis module conducts comprehensive analysis, inference and Event Association of event information converted into standard format, and saves the relevant processing information and process information in the audit knowledge base. Fourth, policy output (report). The console can output policy report in real time by connecting with the policy executor of host firewall. Fifth, real-time response. According to the policy report sent by the console, the host firewall adjusts its own security policy in time.

5.4. Console module workflow

In this paper, the structure and workflow of the console module are established. The basic structure of the linkage console is shown in Figure 5.

5.5. Linkage stage

When the detection system detects suspicious behavior, the system will generate a meta alarm and send it to the console. According to the attack feature database and audit knowledge base, the console will analyze whether the meta alarm will generate attack behavior by association analysis method, which will better ensure the accuracy and reliability of detection. If an attack is generated, the system will process it according to the system settings. Among them, it is most necessary to divide into two ways.

First, the policy generator automatically generates the policy. The policy management module will form a new access control rule of the host firewall according to the result of association analysis. Meanwhile, through the security transmission module, the system will send to the host firewall subsystem for loading, which will resist the attack from the source.

Second, the security administrator generates the policy manually. Through association analysis, the system can display the analysis results to the security administrator. At this time, the security administrator can manually add the corresponding access control rules according to the analysis results. Then, through the secure transmission module, we can send the policy to the terminal host firewall.

5.6. Encrypted transmission mode

When we manage the host firewall remotely, we must ensure the security of the console itself, which requires us to ensure that the data is not eavesdropping and tampering in the process of transmission. Therefore, we must ensure that only legitimate administrators can manage the host firewall through the console. At the same time, only legitimate host firewall users can obtain the security policy from the console. By using an effective authentication mechanism, we can prevent illegal users from running or accessing the console. By encrypting and decrypting the transmission data between the console and the host firewall, we can ensure the security of the data in the transmission process. Therefore, in order to achieve end-to-end encryption and authentication between hosts, this paper uses the transmission mode of ESP and SA mode. The SA between hosts is transmitted in ESP mode. Therefore, esp provides end-to-end encryption. On the basis of sufficient security of the algorithm, as long as the key is not leaked, the eavesdropper can not obtain the plaintext from the intercepted ciphertext. At the same time, the authentication function between hosts can prevent the attack of fake source address in LAN, which is mainly provided by ESP transmission mode. Finally, the end encryption adopts the transmission mode of ESP, in which there is a sequence number, which has a valid lifetime and message authentication code. Therefore, even if the eavesdropper intercepts the data, it cannot replay the message, so the attack does not work.

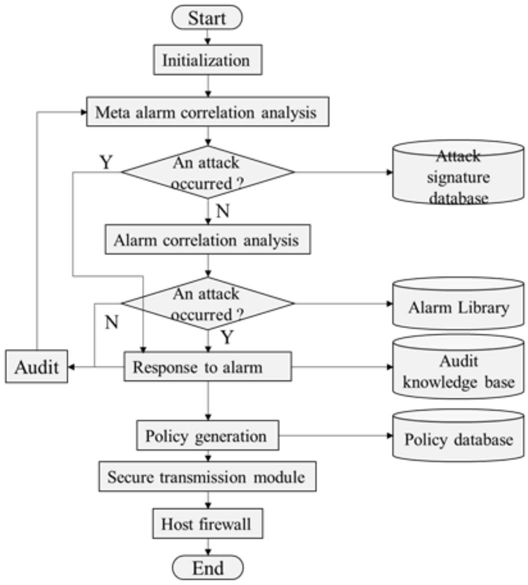

Figure 5. Structure and composition of console module.

6. Conclusion

In this paper, the linkage host security protection technology system is based on the linkage console. Through the linkage of host firewall and host intrusion detection system, we can build a linkage host security protection system. Through the analysis of the model and structure, this paper confirms the host firewall and host intrusion detection system functions of the system model, which will better make up for the parallel and sharing functions of the host firewall and host intrusion detection system, which will improve the security, reliability, robustness and performance of the whole system.

References

[1] Cao Zijian, Zhao Yufeng, Rong Xiaofeng. Design of network intrusion detection and firewall linkage platform [J]. Information network security, 2012, (09): 12-14.

[2] Chen Rui, Chen zemao, Wang Hao. Research on industrial control network threat modeling based on attack graph [J]. Information network security, 2018, 18 (10): 70-77.

[3] Chi Shuiming, Zhou Suhang. Research on DDoS attack defense technology [J]. Information network security, 2012, (05): 27 - 3

[4] Fan Guangyuan, Xin Yang. Analysis and design of firewall Audit Scheme [J]. Information network security, 2012, (03): 81 - 84.

[5] Fang Xin. Research on DDoS attack method in network intrusion detection system based on protocol analysis technology [J]. Information network security, 2012, (04): 36 - 38.

[6] Gao Kunlun. Constructing system network security immune system based on trusted computing technology [J]. Engineering Science and technology, 2017, 49 (2) 28-35.

[7] Guo min, Zeng Yingming, Yao Jinli, et al. Software behavior security analysis based on big data samples [J]. Information network security, 2017, 17 (9): 153-156.

[8] Huang Huajun, Wang Yaojun, Jiang Liqing. Research on network color fishing defense technology [J]. Information network security, 2012, (04): 30 - 35.

[9] Huang Jianhui, Shen Changxiang. Design of TPCM active defense trusted server platform [J]. Journal of Zhengzhou University, 2019, 51 (3): 1-6.

[10] Liang Hong, Liu Jianan, Li Yong. Analysis and prevention of "flame" virus [J]. Information network security, 2012, (08): 157-159.

[11] Shen Changxiang. Building a clean cyberspace with active immune trusted computing network security line [J]. Information security research, 2018, 4 (4): 282-302.

[12] Tian Xiuxia. Teaching reform of information security specialty driven by

innovation practice project [J]. Computer education, 2015 (23): 30-33.

[13] Wang Wei, Shen Xudong. Case based anomaly detection algorithm for migration time series [J]. Information network security, 2019, 19 (3): 11-18.

[14] Xu Fu. Computer terminal immune model based on trusted root [J]. Acta electronica Sinica, 2016,44 (3): 653-657.

[15] Yang Dongxiao, Yan Xiaolang. Some practices in the construction of information specialty [J]. China e-education, 2010 (1): 39-45