Computer Network Security Management System in University Information Construction

ZhaoYonggang

Henan Logistics Vocational College,Zhengzhou,Henan,China

Abstract

In the process of using the computer network, the main page is hacked, the virus overflows, the information is stolen and so on, which brings the inestimable loss to the security of the campus network. Therefore, how to improve the security of campus computer network has become a common concern. This paper discusses the importance of network security in Colleges and universities, and points out the factors that threaten the network security in Colleges and universities. Based on the analysis of the security problems existing in the computer network system and the current situation of network security management in Colleges and universities, this paper puts forward some measures to strengthen the computer network security management in Colleges and universities. This paper studies and designs a set of computer intranet terminal security management system which is suitable for the characteristics of colleges and universities, including domain management subsystem, patch management subsystem, access control subsystem and platform monitoring subsystem. This paper makes a comprehensive analysis of the functions of each subsystem, and introduces the corresponding management processes and strategies. This paper describes the relationship between the subsystems and analyzes the interface between the architecture and other application systems.

Keywords*: Computer network, network security, security management, patch management system.*

I. Introduction

In recent years, with the rapid development of information technology, especially the development of the Internet, the computer network has also been popularized, and the computer Intranet in government organs, the military, enterprises and institutions has also a considerable scale [1-2]. In government agencies, with the development of e-government, new and higher requirements are put forward for information security. From the height of economic development, social stability, national security and public interest, we fully understand the importance of network system security [3].

The internal network of E-government in our unit belongs to the secret computer network of government organs. How to build the network and application system well, and ensure the security of information is the first problem to be considered. If information security is not guaranteed, the reliability and availability of the network will be greatly reduced [4-5]. Therefore, the construction of information security system should be considered simultaneously while the network construction is being carried out, including the division of security domain, network anti-virus system, vulnerability scanning system, information security comprehensive audit system, etc. Through these measures, the information security of our internal network has been greatly improved, but there are still some obvious problems in the actual operation, mainly the source of the security problem - the terminal is not effectively managed, which makes the risk of using the terminal to attack still exist [6].

Therefore, on the basis of market research, we chose the product of a company with the highest market share in the computer intranet terminal management, and established a set of computer terminal security management system in our e-government intranet [7-9]. It includes domain management subsystem, patch management subsystem, access

ISSN: 0010-8189

control subsystem and platform monitoring subsystem. Starting from strengthening the management of Intranet computer terminals, we established a unified intranet terminal security management platform to prevent illegal access, illegal external connection and unauthorized use of mobile media. We successfully solved the problems and obstacles in the construction of intranet security system, solved the security management difficulties of a large number of computers, and provided guarantee for the construction and application of e-government Intranet in our unit.

II. Analysis and design requirements

2.1 System design objective and performance index

1. System design objectives

1) Optimize the system management architecture, because most of the risks come from the internal network, showing the characteristics of equipment dispersion, problem concealment and application complexity, for managers, the management is difficult, the management process is complex, and they can not respond to and deal with security incidents in a timely and effective manner. Therefore, on the basis of optimizing and improving the intranet security management architecture, the system design should achieve unified management, comprehensive monitoring, real-time blocking and timely information.

2) Establish and improve the system management mechanism. As the access mode, equipment, users and managers of the government information network vary greatly among different system departments, there is a lack of unified management. It is necessary to establish and apply the system management mechanism, and improve it in the follow-up operation and maintenance.

3) The application performance of the system requires the design of the system to ensure the good application performance of the system and meet the management requirements on the basis of ensuring the feasible architecture and functional innovation.

2. System performance index

1) Reliability and safety requirement analysis

Because the border security management system has a large area of subordinates, it is very important, subordinates to each equipment, and has high real-time requirements, so it must have very high security and reliability. Here is a special highlight, specifically divided into server-side security, client-side security and communication security for special design and development. Special software modules are needed to protect the client, protect and detect the status of the management server, so as to ensure the safe and reliable operation of the system.

2) Performance requirement analysis

Considering the application environment of the system, the consumption of client resources and network resources should be reduced as much as possible. Due to the large management equipment, the management side has higher requirements for management ability, and the server needs to be purchased separately, so the relative resource consumption does not need to be particularly low.

2.2 System design requirement analysis

Based on the above problem description and system application performance index requirements, in order to ensure the safety of the intranet terminal and the normal operation of the e-government system, the unit has established a set of Intranet terminal security management system in the intranet. The overall resource and network security planning of the intranet terminal is carried out, the illegal access of mobile storage devices to the intranet is controlled, the static IP is bound with the MAC address, the intranet terminal adopts the real name registration system and the automatic distribution of patches, which effectively solves the problems of illegal computer access,

mobile storage leakage and illegal external connection in the network. The terminal security management system configures the application strategy of the whole system through web, manages the network and queries the alarm data to prevent the threat of insecurity factors to the internal network. At the same time, standardize the management system, set up a special network operation and maintenance management team, truly achieve the internal network security management [10].

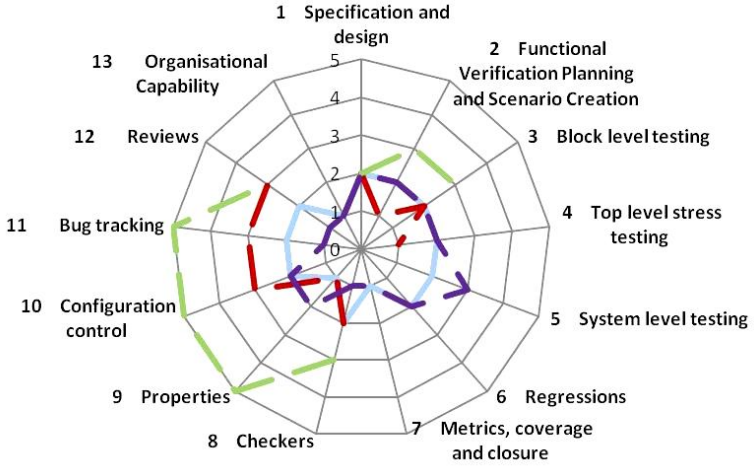


Fig 1: System requirement analysis diagram

III. System overall design

3.1 System architecture design

The system adopts C / S (client / server) mode for information collection and monitoring strategy implementation. The device manager (integrated device scanner) and database are installed and configured at the management end. The client carries out data collection and control management of the client. The network management personnel carry out unified policy control at the management end.

The system adopts B / S structure for maintenance and management, the foreground uses web browsing to manage and register users, and the background uses sol database to count and store user data. The administrator can manage and query all kinds of information by logging in the management page of intranet management server at any client of the network; All network clients need to install client programs to monitor and manage them.

Through the intranet security management server, the network carries out all kinds of strategies and configurations of network clients, network violation monitoring, network access equipment networking status monitoring, intranet mobile storage media security management, and carries out all kinds of behavior and status monitoring of clients. The client program on the network client can report the status information, log information and alarm information of all kinds of network clients, and can deal with abnormal computers such as network disconnection. It can also carry out remote fault diagnosis and maintenance on the client through the system.

3.2 System module design

This system is mainly composed of area manager (integrated area scanner), client program, web central management control platform and management information base module. The logic diagram of system function module is shown in Figure 2.

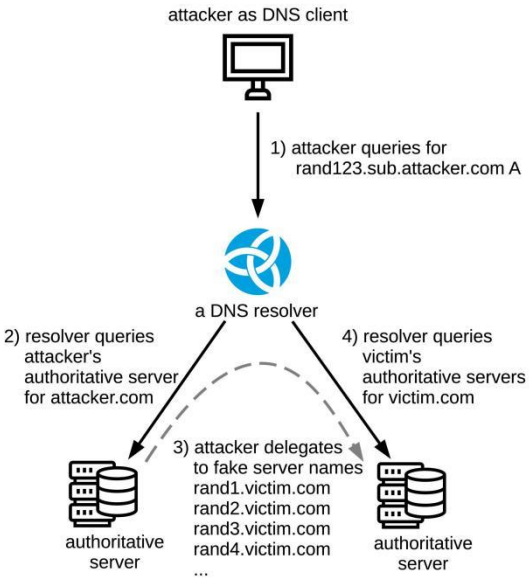


Fig 2: System module flow chart

3.3 Database design

1) Database access design

Network terminal illegal outreach and behavior monitoring system uses the most mainstream B / s system architecture. B / S structure is a real three-tier structure. It takes accessing web database as the center, HTTP as the transmission protocol, and clients access web server and its connected background database through browser. We call it B / S (Browser / server) mode. In the database access, the network terminal illegal outreach and behavior monitoring system uses ADO (ActiveX data objects) access design method in the communication between each module and the database. ADO uses native data source to access database through ODBC. These databases can be relational database, text database, hierarchical database or any database supporting ODBC. The main advantages are easy to use, high speed, occupying less memory and disk space, so it is very suitable for the database access technology as the network terminal illegal outreach and behavior monitoring system.

ADO is a set of special objects to access the database. It provides a complete database access solution for the network terminal illegal outreach and behavior monitoring system. ADO object is executed on the server side, and provides the content containing database information to the management configuration module, regional management module and other modules. The client can also read and write the database according to the specified permissions. ADO contains many objects, among which connection object and Recordset object are mainly used to control database access. To establish a database access, we must first create a connection object, and then use the Recordset object based on this connection object to complete the database slave operation.

In the system workflow, metadata extraction and identification of resource information data should be done well, and classification should be made according to the classification standard defined by the system. Using B / S structure, the administrator completes the management and operation of the network terminal illegal external connection and behavior monitoring system in the browser. Different administrators need certain operation authority to the system database. For the system security, the administrator enters the system after the user login verification, completes the setting of the management configuration module, and updates the database related data operation.

2) Database security design

The network terminal illegal outreach and behavior monitoring system adopts Microsoft SQL SERVER2000 as its own database service system. SQL SERVER 2000 has passed C2 security certification of American government-this is the highest certification level that the industry can have, so it is quite safe to use SOL SERVER. The security and ease of use of SQL SERVER are the reasons why we choose to use it as our database system. Based on the consideration of database security, we have added the following security mechanisms to the design of illegal outreach and behavior monitoring system of network terminals.

(1) provide the latest Microsoft service package and database upgrade files. Ensure the security of the system platform. The most effective way to improve the security of database service is to upgrade to SQL Server 2000 Service Pack 3A (SP3A), and install all the security updates released by Microsoft. The security and stability of database system platform is the foundation of database security. We will provide all Microsoft service packages and upgrade files of database security we use.

(2) User password security. Because SQL Server can't change the sa user name, and can't delete this super user, we must protect this account with the strongest protection and use a very strong password. The network terminal illegal outreach and behavior monitoring system does not need to use sa account in the database application, and as long as there are users with corresponding rights to the network terminal illegal outreach and behavior monitoring system database, the normal use and maintenance of the system can be completed.

(3) The central management configuration platform (Web management platform) sets the security of database operation. The Web management platform uses ASP technology to exchange data with SQL SERVER. Here, by limiting the login IP range of users, administrators can limit their system user rights according to the use of different operators. From the perspective of practical application and security, the illegal outreach of network terminals and the normal operation of behavior monitoring system are guaranteed.

(4) Perfect log system and data optimization tools. We can log in to the central management configuration platform to query the management and operation logs of the system set by the management personnel, or query the specific changes of the database made by the operator or database administrator through the log system of the database. With the increase of usage time, there may be more useless data redundancy. We can use the data reorganization tool in the central management configuration platform to tune the database.

IV. System function design and Implementation

4.1 Access control

WinPcap (Windows packet capture) is a free and public network access system under Windows platform. Its main function is to send and receive original data packets independent of host protocol (such as TCP / IP). The purpose of developing WinPcap is to provide the ability to access the bottom layer of the network for Win32 applications. It provides the following functions:

(1) Capture the original data packets, including the data packets sent / received by each host on the shared network and the data packets exchanged with each other;

(2) Before the packets are sent to the application, some special packets are filtered according to the user-defined rules;

(3) Sending the original data packet on the network;

(4) Collect the statistical information in the process of network communication.

The security access module of the system obtains the ability of sending original data packets and monitoring network data packets through WinPcap driver. The module sends ARP request to the whole LAN, detects all online hosts, and obtains all legitimate hosts through the server. Then distinguish all the illegal hosts and construct pseudo ARP packets to cheat, so as to make the illegal hosts and legitimate hosts unable to communicate.

4.2 Lllegal outreach

Under normal circumstances, the host is connected to the LAN through Ethernet. The network card is bound with internal IP address, subnet mask and gateway. TCP / IP protocol will generate a routing table according to these information. The routing table points the default route to the gateway. Any network data transmission will use the routing table to select the optimal path for transmission. When the host dials, in addition to the original Ethernet card connected to the LAN, the host will also have a WAN connection generated by dialing. The IP address, subnet mask and gateway assigned by ISP will be bound on the E1 of the network. The system will add some routing tables, and the first default gateway will be updated to a new IP address. According to the different routing information, we can distinguish whether the host is dialing or not.

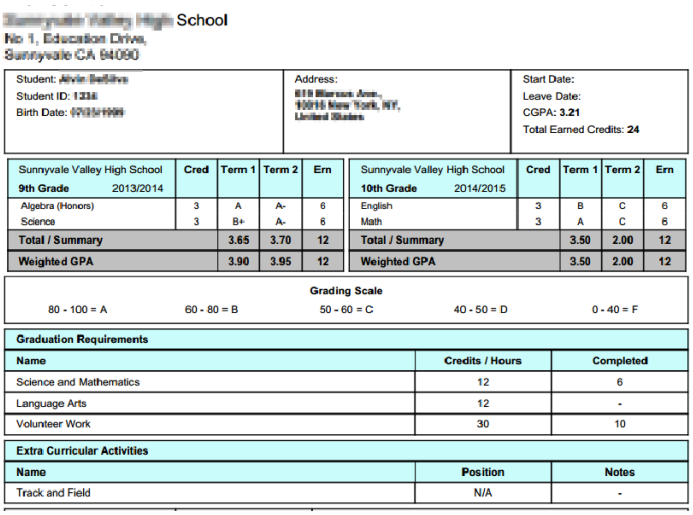
Assume that host A is an internal network host. When it receives ICMP message from external network host B when it has no dial-up connection, its route finds that this message is not the IP of this network. Therefore, it first sends an ARP message to default gateway C to obtain the gateway physical address, and then constructs an ICMP response message with B as the destination IP address and default gateway physical address as the destination physical address. However, after A dials the Internet, the default gateway of A has changed. When A obtains the default physical address through ARP, there will be no ARP response message, so there will be no ICMP response message. According to this difference in network traffic, dial-up hosts in the network can be found.

4.3 Patch upgrade management

The system realizes the function of patch automatic analysis and distribution. It only needs to set appropriate policies to realize the automatic scanning and installation of system patches, which greatly facilitates the users to install network patches.

The server waits for the policy task of the web management and control platform, and the task information is transmitted in XML format; After receiving the task information, the server first parses the XML string and jumps the task information recorded in the XML string to the corresponding task processing flow for processing; If the received task type is "automatic analysis and distribution task", the server first establishes sub tasks according to each target host in the task and processes them separately. The server sends the instruction of patch scanning to the target host and waits for the target host to feedback the result of patch scanning.

The server receives the XML string of the analysis result of the target host, parses the XML string, analyzes which patches have been installed and which patches have not been installed, and writes it to the database. According to the patch installation information of the target host and the distribution strategy and installation strategy formulated during the task formulation, the server generates the distribution task for the target host. The server waits for the patch installation result of the client, and records the installation status, installation time and other information fed back by the client into the database table of the subtask. At this point, the whole task is finished. During task execution, if individual clients are not online, subtasks cannot be executed. The server adopts the following policies to solve this situation. If the client is not online, the sub tasks of this client will be suspended. The server periodically checks whether the suspended subtasks are qualified for execution. If the execution conditions are met, the suspended sub tasks will be reactivated and executed again.The achievement of one student in MVC academic affairs system is shown in Figure 3.



[redacted] School
No 1, Education Drive,
Sunnyvale CA 94090

Student: [redacted] Student ID: [redacted] Birth Date: [redacted]	Address: [redacted]	Start Date: Leave Date: CGPA: **3.21** Total Earned Credits: **24**

Sunnyvale Valley High School **9th Grade** 2013/2014	Cred	Term 1	Term 2	Ern
Algebra (Honors)	3	A	A-	6
Science	3	B+	A-	6
Total / Summary		**3.65**	**3.70**	**12**
Weighted GPA		**3.90**	**3.95**	**12**

Sunnyvale Valley High School **10th Grade** 2014/2015	Cred	Term 1	Term 2	Ern
English	3	B	C	6
Math	3	A	C	6
Total / Summary		**3.50**	**2.00**	**12**
Weighted GPA		**3.50**	**2.00**	**12**

Grading Scale

80 - 100 = A | 60 - 80 = B | 50 - 60 = C | 40 - 50 = D | 0 - 40 = F

Graduation Requirements

Name	Credits / Hours	Completed
Science and Mathematics	12	6
Language Arts	12	-
Volunteer Work	30	10

Extra Curricular Activities

Name	Position	Notes
Track and Field	N/A	-

Fig 3: The achievement of one student in MVC academic affairs system

4.4 Mobile storage media management

Taking data as the center, the user is the user of data, the host is the storage of data, and the mobile storage medium is the Migrator of data. All of them are given unique identification within the scope of the system, and they carry out mutual authentication. Only after the authentication and authorization is successful, can the legitimate user access the data on the legitimate mobile storage medium on the legitimate machine, and form a detailed log for audit. The system sets up a USB label making tool. By making labels on the mobile storage media, the data in the mobile storage media can be protected and encrypted, and the comprehensive management of the mobile storage media, such as the use scope authorization and access control, can be realized. The mobile storage media usage management system can divide the whole mobile storage media into two parts: exchange area and secret area. The protected area can only be accessed by password authentication.

By writing two kinds of labels with different control rights and functions to the mobile storage media, the hierarchical authority control is realized, and the terminal authorization within the specified scope is realized. The control of the mobile storage media is realized through the cooperation of policy and label. Note that formatting removable storage media does not remove labels.

Common label: after writing the common label, the read and write functions of the removable storage media are restricted according to the policy settings in the management area. If the mobile storage medium authentication is used outside the management area, the read and write functions of the mobile storage medium authentication are not limited. Encryption label: after the encryption label is written, the ordinary removable storage medium (U disk, mobile hard disk, etc.) is divided into two controllable areas: exchange area and secret area. Secret network can only generate secret area. Both the exchange area and the secret area need to input independent passwords when they are started. When the data is stored in the two areas, they are stored in the form of encryption. The specific applications of the two areas are as follows:

In secret network or office network with high requirements, only one secret area can be generated. The secret area can only be accessed by entering the correct password after passing the authentication label on the host with corresponding security policy. Meanwhile, the host with security policy can control the use of the mobile storage media without label authentication according to the policy. In the common office network, it can generate two areas: exchange area and secret area. The use method of the confidential area can be the same as the above classified network or the office network with high requirements. The use of the switch area can be restricted by policy in the internal network according to the user's needs. When the switch area is used on the external network,

the password must also be entered before it can be used. The secret area is not visible on the external network.

V. Conclusion

Due to the short time and high requirements, the system is not fully considered from design to implementation, because the security management of Intranet terminal is a very complex system engineering, involving all aspects, and the implementation process is also quite complex, through the continuous improvement of the dynamic process from planning to design, from design to implementation, from implementation to modification. During this period, the company's technical personnel, implementation development engineers and our professional and technical personnel who participated in the system development have all made arduous efforts, so that the system can be successfully installed and put into operation. The operation effect of the system has basically reached the established goal, but there are still some defects and areas that need to be improved.

References

[1] Lin, Y., Wang, Y., & Kung, L. A. (2015). “Influences of cross-functional collaboration and knowledge creation on technology commercialization: evidence from high-tech industries”. Industrial Marketing Management, 49, 128-138.

[2] Liu, D., & Guo, X. (2017). “Exploring gender differences in acceptance of mobile computing devices among college students”. Information Systems and e-Business Management, 11(1), 1-27.

[3] Peteet, B. J., Brown, C. M., Lige, Q. M., & Lanaway, D. A. (2015). “Impostorism is associated with greater psychological distress and lower self-esteem for african american students”. Current Psychology, 34(1), 154-163.

[4] Pinto, J. C., Loureiro, N., & Taveira, M. D. C. (2015). “Psychological intervention in portuguese college students: effects of two career self-management seminars”. Journal of College Student Development, 56(5), 518-524.

[5] Shiau, W. L., & Chau, P. Y. K. (2016). “Understanding behavioral intention to use a cloud computing classroom: a multiple model comparison approach”. Information & Management, 53(3), 355-365.

[6] Tzu-Fei Chen RN MSN Doctoral Student Lecturer, & Kuei-Ru Chou PhD RN Professor. (2015). “Construct validity and reliability of the chinese version of the disaster preparedness evaluation tool in Taiwan”. Journal of Clinical Nursing, 24(7-8), 1132–1143.

[7] Wang, C. C., Chen, C. F., & Chen, C. T. (2015). “Exploring the different aspects of internet leisure use by college students”. Information Development, 31(1), 5-12.

[8] Wang, X. (2016). “Course-taking patterns of community college students beginning in stem: using data mining techniques to reveal viable stem transfer pathways”. Research in Higher Education, 57(5), 544-569.

[9] Zhang, Q., Goodman, M., & Xie, S. (2015). “Integrating library instruction into the course management system for a first-year engineering class: an evidence-based study measuring the effectiveness of blended learning on students' information literacy levels”. College & Research Libraries, 76(7), 934-958.

[10] Zhou, Y. X., Ou, C. Q., Zhao, Z. T., Wan, C. S., Guo, C., & Li, L., et al. (2015). “The impact of self-concept and college involvement on the first-year success of medical students in china”. Advances in Health Sciences Education, 20(1), 163-179.