IOP Conf. Series: Earth and Environmental Science **69** (2017) 012163 doi:10.1088/1755-1315/69/1/012163

Research and realization implementation of monitor technology on illegal external link of classified computer

Hong Zhang

University of Chinese Academy of Sciences
Chongqing Institute of Green and Intelligent Technology, Chinese Academy of Sciences, 610051 China

Abstract: In recent years, with the continuous development and application of network technology, network security has gradually entered people's field of vision. The host computer network external network of violations is an important reason for the threat of network security. At present, most of the work units have a certain degree of attention to network security, has taken a lot of means and methods to prevent network security problems such as the physical isolation of the internal network, install the firewall at the exit. However, these measures and methods to improve network security are often not comply with the safety rules of human behavior damage. For example, the host to wireless Internet access and dual-network card to access the Internet, inadvertently formed a two-way network of external networks and computer connections [1]. As a result, it is possible to cause some important documents and confidentiality leak even in the the circumstances of user unaware completely. Secrecy Computer Violation Out-of-band monitoring technology can largely prevent the violation by monitoring the behavior of the offending connection. In this paper, we mainly research and discuss the technology of secret computer monitoring.

1. Introduction

In the rapid development of computer technology background, network security has become a hot topic. The host computer network external network of violations is an important reason for the threat of network security. At present, most of the units to improve network security measures and methods are often damaged by people who not comply with the safety rules of human behavior. As a result, it is possible in the the circumstances of user unaware completely, resulting in some important documents and confidential leaks, causing some units can not be estimated losses. Computer out-of-line monitoring technology can monitor the computer's internal network to see whether access the host to the Internet when the access to the Internet, timely access to prevent and control to prevent the leakage of some important file data to improve security.

2. The significance and current situation of the study of illegal outreach situation

The security of computer LAN, namely intranet security, it is a very important topic in the discussion of network security. Common firewall, out-of-band monitoring technology and security gateway and encryption and decryption technology are all aimed at LAN security. Most of the common projects and products on network security, including confidential computer which will be out-of-line monitoring technology violations, by monitoring the behavior of illegal connections to prevent violations of the situation [2].

In recent years, with the continuous development and application of network technology, the network has penetrated into all aspects of our life and work, including a number of international

agencies and military units which have been using computers for daily work and business work. In the rapid development of computer technology background, network security has become a hot topic. In the development of computer network technology, but it also has brought a certain degree of threat and some problems, planted a hidden danger. Most of the organizations and companies in order to prevent leakage of confidential documents within the company, the protection of information security, often using backup data, physically isolating the internal network and set up a firewall and other methods. Related research shows that more than 85% of the sources of network security risks are within the company. This can be obtained in the discussion of the issue of network security, it is not only need to strengthen the security of external networks, but also pay attention to internal staff leaks to strengthen the company's internal network security construction.

Table 1 Different Reasons Analysis for Network Threats

Number	Network threat event	Ratio
1	Internal security threats	85%
2	Internal unauthorized storage	16%
3	Theft of patent information	14%
4	Internal staff financial fraud	12%
5	Data loss or network disruption	11%

At present, China's security checks are mainly means of surgical examination or manual inspection which is the main tool to assist the method. This inspection method depends to a large extent on the professional level of inspectors. In addition, some units and enterprises began to study other professional confidentiality inspection technology, but most of the research results are only applicable to part of the inspection, and can not be widely used, does not have practical significance. Because of its special nature of confidentiality security secrecy technology, it was often linked together with some countries important secrets and benefits, and it may even threaten the country's security. Most of the foreign secret computer security confidential inspection of the core technology is confidential and it is not open to the public [3], so it's an urgent need for an effective and feasible technology to prevent such illegal outbound Internet behavior.

In the design of illegal outreach monitoring program, we need to consider a variety of health technologies and network scanning technology, including a series of network protocols they all will have an impact on the offending monitoring program. Illegal outreach by connecting the external Internet directly to the intranet, it is very easy to open a system from the inside to the outside of a channel, thus bypassing a series of protective measures, it break the physical isolation which is often existed in the secret system. The common ways of illegal outreach activities are: increase the host device in the dense network; disable the local network card for illegal outbound operation or deliberately unplug the network within the network; the use of multi-network card network, thus breaking the physical isolation of the original secret system; secret media directly connected to the external Internet; dial-up network using the way; secretly single or secret network host through CMDA or WLAN and other wireless Internet access [4].

3. Related technology of confidential computer violations monitoring

At present, most of the local area network is the use of TCP / IP protocol network, each host of the network dynamic live static allocates to the private independent IP address. Each of the different hosts have a different IP address that is different from the other host. LAN dial-up violation of the host an is different from the other place which is that has dial-up connection assigned IP address that is no longer a private IP address, but public. If you can get the relevant information about the IP address of the LAN host, you can get the relevant information about the outbound operation of the LAN host. The main methods are as follows.

3.1 Network Blocking Based on 802.1X Protocol

In orders to be able to completely prevent the port of the intervention control, in 2001, IEEE promulgated the 802.1X standard. When the Ethernet port is controlled and accessed, the network

devices such as the switch have passed the 802.1x MAC authentication mode. The extended authentication protocol agent runs on the switch connected to the user to achieve communication with the switch. EAP over LAN runs on the user's computer. The switch divides the physical port of the Ethernet into two ports, uncontrolled logical port and controlled logical port. When the EAP over LAN authentication process is performed on the switch, the controlled logical port is divided into unauthorized and authorized states when the computer is not controlled by the logical port. When the controlled port is authorized, the user is allowed too. When the logical port is in an unauthorized state, the user is not allowed to access it. RADIUS will perform authentication steps and actions on the logical port. The authentication and operation will be performed on the basis of EAP over LAN. When the switch receives the request operation, it will send the authentication data onto the authentication server. The server completes the authentication. As a result, the computer can connect the network through the control of the logical port, use the network resources [5].

3.2 Client-based monitoring

Client-based monitoring mode requires each host has a client within a host, in order to achieve regular monitoring of the client machine to master the actual situation of its network connection, once found the illegal out of the situation, send data to the server host immediately. Thus, preventing the customer to actively carry out illegal outreach operation and it also ensures the security of confidential information. This kind of client-based detection mode can be implemented in a variety of ways, such as monitoring the client machine effective network card, you can get no registration card corresponding to the information, found in the illegal operation, you can block the card, cut off the illegal network operation, and the information of the card to record; it can also be on the LAN host computer packet detection and analysis, once found illegal outreach situation, to block the illegal operation of the card, so that the card can not be used, report and record the information timely to prevent the leakage of classified information.

3.3 Based on SNMP service

SNMP-based monitoring mode on each host is to be installed SNMP in the LAN you can achieve the internal network hosts / hosted which has occurred in violation of the behavior of the monitoring through the SNMP protocol. The main workflow are: select a host of the LAN as a monitoring host, installed in the SNMP protocol based on the development of monitoring software, regularly asked the other host IP address information, the other host computer IP information, once found LAN does not belong to the internal network address of the IP, that is, to change the host to determine the illegal dial-up operation, to make a certain deal. The detection mode based on the SNMP service, all hosts of the LAN is required to install the SNMP protocol, it is difficult in the actual operation and the popularity.

4. Confidential computer offending monitoring system

4.1 system design

The most important function and purpose of the secret system is to monitor whether there is any irregular operation in secret network, thus preventing the leakage of important information and ensuring the security of the information. The client of the system installed in the corresponding secret computer, once the secret host for illegal outbound Internet operation, the computer will send the corresponding data onto the early warning management center, such as MAC address and IP address and other information, at the same time Block, disable its U.S.B interface, thus preventing the leakage of important information. In secret host, the system client cannot be uninstalled, and the early warning center cannot be detected by the firewall, the customer cannot find the system. When the alarm center receives the relevant alarm information, it will immediately send a text message to the corresponding mobile phone, the administrator can receive the information immediately after the relevant processing. The design of the offending computer monitoring system is divided into three modules, mainly for the client module, the network monitoring server module and the external network warning module, the

specific structure is as follows.

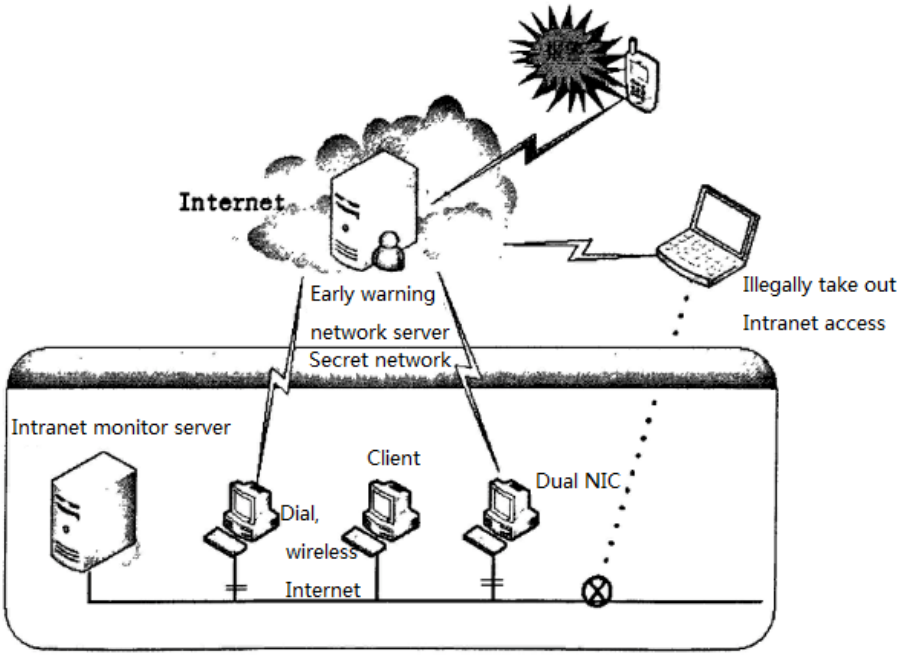

Figure 1 classified computer monitoring system outside the chain structure

The system test mainly tested from two aspects of the performance and function of the secret computer which offending monitoring system.

Through the control of the relevant instructions it can be sent to the client, start the monitor, upgrade the corresponding client version, for illegal access equipment it can also be blocked in time.

Through the illegal outbound security policy management which can set the client's related security policy. It is an configure on the network equipment where the computer is located, through the security policy management, it can also set to monitor the computer after the illegal outbound operation of the blocking method.

The monitoring and management center is able to perform a journal audit function on the monitored host outbound behavior. By querying the client behavior diary, you can learn about the time of the outbound behavior and the information about the computer and IP address. The diary audits function module is shown in Figure2.

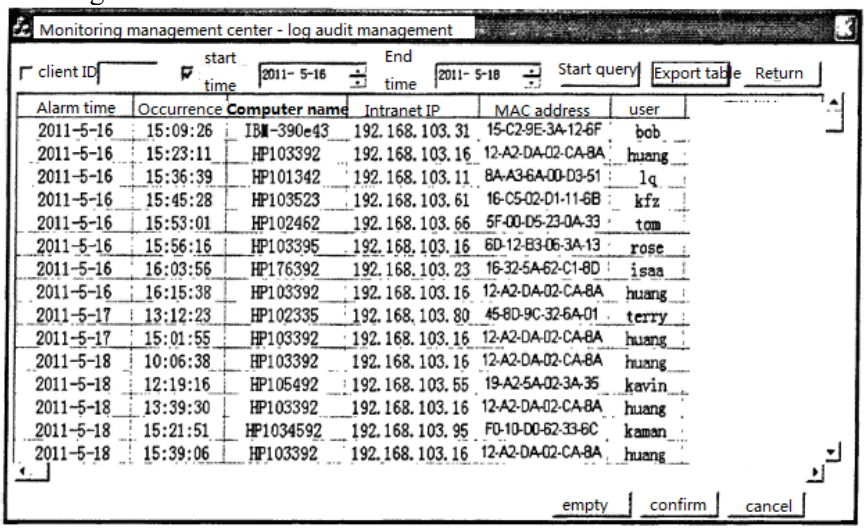

Figure 2 diary audit module

SMS alarm station can select the different alarm content which is sent to the appropriate administrator's phone after receiving the information, as shown in Figure 3. In addition, the SMS alarm module can be customized according to the actual needs of the contents of the SMS alarm to improve the efficiency of the alarm to facilitate the operation of management personnel.

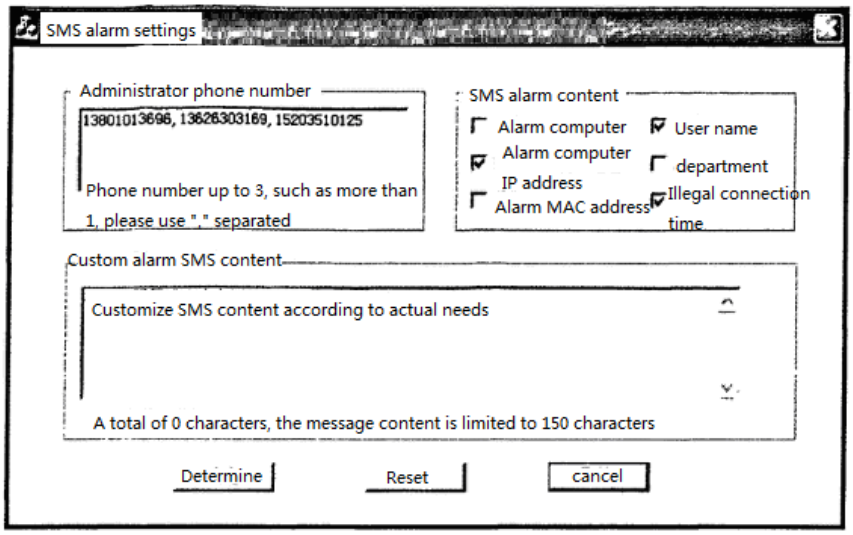

Figure 3 SMS alert Settings

After the completion of the client, It has tested the client and antivirus software compatibility and firewall penetration. Detection results found that the client system with the current mainstream antivirus software such as Jinshan dominates, 360 antivirus rising and other anti-virus software are compatible, through 360 security guards, windows and Skynet and other firewalls, there is no penetration warning. There is a need for 5s ; if the monitoring system is stopped, it takes 30s to restart ; unauthorized U.S.B device access cannot be used ; when part of the hardware or IP is changed, it takes 10min to send the information on the monitoring in the management server. Through the above test we can find that secret computer outreach monitoring system design interface which is simple, it can give better relative maintenance and management, and its' performance can meet the practical requirements to ensure that with other anti-virus software monitoring, it also can penetrate the firewall to complete the relevant alarm work successfully. In addition, the SMS alarm system has a very good practicality, to facilitate the management of the corresponding management operations.

5. Summary

With the continuous development and progress of network computer technology in recent years, the network security also has higher requirements. Most of the units have tried to improve network security measures and methods, but they are often damaged by people who do not comply with the safety rules of human behavior, causing the leakage of important information. Computer out-of-control monitoring technology can monitor the computer's internal LAN to see the host within the LAN access Internet operation, the host if there is illegal outreach operations such as dial-up Internet access and wireless networks, in a timely manner it will prevent such illegal outreach actions, and ensure the safety of classified information to a large extent.

References:

[1] Zhang Guoqing, Zheng Guixing, Yu Bo. LAN Security Risk Analysis and Prevention [J]. Information Security and Communications Security, 2010, (6): 68-70.
[2] Lin Tao, Zhang Jian-biao. Study on Monitoring and Blocking System of Illegal External Connections in Intranet [J].Journal of Network Security Technology and Application, 2006, (8): 48-50
[3] Dai Zhen-hu, Dong Wen-sheng, LI Gang. Analysis of several out-of-band monitoring schemes for

intranet security [J]. Metallurgical Automation, 2008 (1): 439-441.
[4] Zhao Yongsheng, Gu Lize. Study and analysis of host-based non-machine out-link monitoring technology based on routing table [C]. New Development in Communication Theory and Technology, 2009.
[5] Lei Qi-lin, Yang Huihua. Design and Implementation of an Internal Network Outside Monitoring System [J].Guangxi Academy of Sciences, 2008,24 (4), 23 (1): 342-344.