Research on Key Technology of Computer Security Monitoring System

Jin hui

Si Chuan University, Chengdu, Sichuan, China

Keywords: Key Technology, Computer Security Monitoring System

Abstract. The development of information technology has brought new challenges to information security. Computer security monitoring system is an effective mechanism to ensure information security. It protects and monitors all kinds of information and user operation in local or remote computer through data acquisition, analysis and processing, rule discrimination, violation prevention and full record. This paper mainly studies the key technologies of document, text and user operation, and analyzes the realization mechanism and application environment of these key technologies by experiment. It is very important to strengthen the system function and improve the efficiency and stability of monitoring.

Introduction

The computer security monitoring system is a computer system which integrates data acquisition, monitoring and control functions. The most typical of which is the data acquisition and monitoring function. The system uses the monitoring and control computer as the main body, and combines the detection device, the actuator and the computer. Monitoring objects, together constitute a whole, in which the computer directly to be monitored by the object of detection, supervision and control process. The security monitoring system of the intranet computer is a kind of management system which can manage all the computers in the network efficiently and safely. It is an important guarantee for information security, and uses the remote control technology to monitor the computer in the network.

According to the source of the computer threat, the author divides it into both internal and external threats. The United States analyzed the components of the computer threat in 2002 and found that the vast majority of threats came from internal threats, part of the hacker from the malicious attacks. Therefore, do a good job of internal key technology to prevent work, is to prevent malicious attacks the key.

The Monitoring Object of Computer Security Monitoring System

In order to deal with the threat, the computer needs to monitor the operation of the system. The scope of the monitoring mainly includes two aspects. The first is to scan the files through the system, and send out the warning files for other malicious attacks such as viruses. Signal, and finally issued by the system administrator to block or delete the file instructions. The second is to monitor the operation of the staff and the monitoring of the content mainly includes the operator whether to use a means of patent, internal data replication and dissemination of its operation of the process of recording, in addition, it can directly block some illegal operation.

The speed of information processing is a significant feature of the network era. As the main form of information dissemination, the security is the main way of monitoring the system to maintain computer security. In particular, in areas where information confidentiality is extremely demanding, such as military, banking, etc., it is necessary to monitor all the details of the operation of the document, whether it is a new document, a file modification, or a file deletion Its record, for the key file copy, modify and delete instructions should be made in advance of the authority, illegal operation should be blocked.

Text monitoring is also a computer monitoring system needs to pay attention to the link, the text is a larger branch of the document, which in addition to the file from the outside, the network is also an important means of its dissemination of external threats for the user's computer path, the monitoring system and the file is roughly similar, in addition, the monitoring system should be text in the text, digital information to understand, military, political and other sensitive information should be promptly removed out to be removed.

For the text, the document is relatively easy to monitor, but for the human operation is weak, limited to the uncertainty of man-made operation, monitoring system, the work of the target is difficult to be reflected in the program, only to monitor the target to hardware system, through the mouse and the key record, the mouse click and keyboard input combination, which analyze the staff in the system on what kind of operation.

Research on Technology and Design of Computer Security Control System

Computer Security Monitoring Object. Computer security monitoring object mainly includes two aspects of information and operation, the monitoring of information is mainly on the system of file and text information monitoring, the operation of the monitoring is mainly on the user generated by the operation of the monitoring, monitoring system Responsibility is to change the file information, text information replication and user manual operation to record and filter, and the time to block the security risks of information.

Network Firewall Technology. The network firewall is software that is located between the computer and the network to which it is connected. All the network traffic flowing into and out of the computer is filtered through the firewall. The firewall scans the network traffic through it, so that it can filter out some malicious attack, so that it is not executed on the target computer. Through the firewall technology can develop a key point to avoid outside the malicious attacks, you can achieve the security monitoring of the computer, and in exceptional circumstances to make alarm prompts, for those relatively large amount of information network communication in addition to the routine Inspection, but also should be made log registration, through the provision of network address translation function, you can ease the IP address of the plight of resource constraints, the firewall has a good network security protection, the intruder must first pass through the firewall security line can contact to the target computer, the firewall can be configured into many different levels of protection, high-level protection may prohibit some services. Firewall can provide users with an ideal service location, although the firewall can protect the computer from hackers malicious attacks, but cannot guarantee the absolute security of the computer, which requires continuous improvement and improvement to prevent more outside interference and attack.

Security Encryption Technology. Encryption technology to the normal operation of e-commerce system provides a strong guarantee, the key as one of the forms, in the transmission agencies play an important role in ensuring the transmission process is safe, because the password algorithm is open, the network the security is completely dependent on the security of the key. Although the method used in different ways, but the key system itself is no difference, there are digital signatures, packet authentication, e-mail encryption and other forms of application, so there is an important branch in cryptography, that is, key management. Key management mainly includes the key generation, allocation, injection, verification and use of the program, its basic duty is to ensure the safety of communication between users.

Image Recognition Technology in Early Warning. The safety monitoring system of the computer usually waits for the safety time to become the fact after being processed by the system. Once the security system is installed, the monitoring range is fixed. As long as the light does not change, the obtained image will be basically the same and the abnormal phenomenon occurs, the image will be a significant change, the use of this principle, through the image recognition can be abnormal before the accident can be issued before the warning signal to remind the user abnormalities and take effective control measures.

Achieve the Intelligent Computer Monitoring System. To achieve the intelligent computer monitoring system can be based on the original monitoring and control system into the artificial intelligence of thinking, to achieve intelligent goals, thereby improving the performance of the original monitoring system to broaden the scope of use; can use artificial intelligence ideas, constitute a new monitoring system, intelligent monitoring and control as a branch of intelligent control, computer intelligent monitoring system is a computer monitoring system and artificial intelligence of the organic combination, is in the ordinary computer monitoring system based on the integration of intelligent application technology.

Open Integrated Network Monitoring and Management System. Network technology in the continuous development of computer network system itself is a powerful and complex integrated network system, the need for a comprehensive network monitoring and management system to ensure that this new monitoring and management system can be composed of multiple monitoring systems, these subsystems can be connected to a bus network, ring network or star network, the network nodes can be corresponding to increase or decrease, can also exist in a separate monitoring system, these sub-monitoring system can be equal, it can be layered, what kind of topology, the designer can be set according to the actual situation, with the new technology, intelligent sensors and controller development and update, the computer security monitoring system will become more intelligent, miniaturization and network.

Computer Host Operating System Security and Physical Security Technology. Host operating system as a direct manager of computer resources, is the basis of computer software system, all the application software is built on the operating system, the operating system security issues are the host computer and network security prerequisites, more not to mention the safety of other applications, the security of the operating system plays a more important role, is the guarantee of the entire computer system security, firewall technology is the network's first line of defense, but also can not completely protect the computer's internal network, but also need to combine some other protective measures can improve the security of the system. In addition to the firewall protection measures, the computer host operating system security and physical security measures is also an effective way to protect the computer system, increased the protection of the internal computer system.

Key Technology of Computer Safety Monitoring

Windows API. The Windows API is an important interface to a computer application that provides programmers with a database of function applications and uses certain functions in the database to control peripherals. RDCW function can provide two monitoring methods to the monitoring system, one is synchronous monitoring, the other is asynchronous monitoring, take asynchronous monitoring, for example, it uses the function is mainly callback function, callback function is focused on the use of the circulatory system, an event in the monitoring is completed, the program will not stop there, when the monitoring needs to continue, the system will enter into the next cycle.

API Hook. API Hook is based on the interception mode of the system, also known as the interface in Windows articulation technology, the working principle is through the application of monitoring and finds the need to mobilize the code, and then transfer the code to the system manager wants to graft Procedures, so as to achieve the blocking of certain documents. When the system administrator needs to open some files, it will advance the function in space, and then call the parameters into the API function, then the DLL will automatically issue instructions to the system, so that the operation into the kernel processing state. Interception system works is relatively simple, only need to enter the code into the DLL and you can achieve the interference of malicious data.

Middle Layer Driver. The computer's driver is the area through which the file needs to be passed. The main function of the driver is to exchange the program that the computer is using to achieve the purpose of buffering. When the system administrator wants to retrieve a file in the program, the transfer code will be driven into the driver, if the driver to join a middle layer file monitoring program, you can achieve some of the abnormal data interception.

Windows API technology is relatively simple, monitoring and implementation of the efficiency is also very good, but there is no ability to expand, in this era of faster updates, the external threats do not have a good ability to adapt; intercept system in the coverage, efficiency and degree of expansion have a good effect, the more obvious shortcomings is to achieve more difficult; Finally, the middle layer of the most obvious advantage lies in the monitoring of its coverage is very wide and because the system is more complex, a certain degree of difficulty, and the implementation of the efficiency compared to the above two ways more general.

The Key Technology Based on Text Copy Monitoring. Text copy of the monitoring is based on the clipboard to design, using the relevant means to grasp the clipboard information changes in the law, so as to achieve the purpose of text monitoring. By installing the monitor on the clipboard and grouping the monitor into a chain mode, when the system administrator replicates the text, the information of the clipboard changes will be redirected to the terminal for information monitoring through the previously set link the addition of the monitored chain will destroy the integrity of the original chain, so when there is no obvious change in the clipboard when there is no need to log off the monitor in order to ensure the integrity of the chain.

Key Technologies Based on Human Operation Monitoring. Keyboard and mouse monitoring is to achieve the main means of monitoring the human operation, which is not talking about the external monitoring, but through the establishment of a related function set up a monitoring chain, the way to monitor the transmission of information, if the information is not there is a security threat, it will be transmitted to the next connection. Which uses a hook function, initially through the function registry to install the Hook, and the callback function into the monitoring program, the event will automatically follow the previously set up a good program to move down, when the data processing is no threat, the process of this stage will be announced, the next event can continue to start. Whether it is the keyboard or mouse are used Windows Hook related technology and it is a very good implementation of the monitoring effect of human operation.

Conclusion

Computer security monitoring system can protect and monitor all kinds of information and user operation in local or remote computer as an effective mechanism to protect information security. Through the in-depth study and analysis of the monitoring techniques such as document, text and user operation, it can better choose the appropriate technology way according to the system requirements, improve the pertinence of the monitoring and ensure the stability and efficiency of the system.

References

[1] Huifang Zhou，Hong Bao,Xinguang Li and Jing Zhang. Application of the Mobile Database to the Embedded oral Translation System[J]: Computer Development & Applications, Vol. 23 (2010) No 12, p.13-14.

[2] Wen Li: The key Technology of Computer Security Monitoring System Research[J]. PC Fan, Vol. 10 (2015) No12, p.23-24

[3] Minghao Hou: Computer Network Security Monitoring and the Key Technology Research[J], Vol. 5 (2016) No 10, p.231-232

[4] Yaling Tang: The Research and Implementation of Computer Network Security Monitoring System[J]. Digital Technology and Application, Vol. 12 (2013) No12, p.170-171