Design and Implementation of the Monitoring System for Critical Documents

Huang Gaofeng Zhou Xueguang
The Naval University of Engineering, Department of Information Security
Wuhan, China
huanggaofeng@163.com

***Abstract*—How to secure the storage and transmission of computer's information has always been a hot topic. This paper presents a document monitoring and protecting system on Windows platform. The system realizes the real-time monitoring and protection of user's critical documents, as well as giving early warning of removing, tampering and other malicious operations. It prevents the information from changing and insecurely flowing, avoiding the illegal intrusion of hackers and the virus' attacks and undermining. The system has been verified by the experiment, with the characters of real-time, high efficiency, accuracy, ease of use and so on.**

Keywords-monitoring system; document monitoring; real-time monitoring; critical documents

I. INTRODUCTION

The computer has become an indispensable tool in people's lives, and they use it to store much personal information, which include inevitably much personal privacy, a large number of important documents and so on. There are some special files in the system, and we call them Critical Documents. The critical documents, in a general sense, are a type of files of great value or significance for users, or a type of files of core functions for the system. Therefore, how to protect the user's critical document is very important for security problems. Considering this problem, this paper introduces a novel system to monitoring critical file modification and give warnings to protect system security.

At present, there exists some document monitoring software, which can take a certain effect on monitoring the computer's files, folders and other operations. For example, Rising antivirus® software[1] and others take a certain effect on monitoring the computer's operating system files, and also provide the protection and treatment of files, etc; other typical document monitoring software, such as Skye , File Monitor, Anyview and others[2-4], also implement some corresponding functions.

However, there are some shortcomings in that software, as follows:

1) They don't meet the demand exactly. It is difficult to achieve the purpose of demand, for example, the confidential information's leakage for the misuse of sensitive areas, caused by the lack of dynamic monitoring and processing mechanism. Once destroyed, the file will fail to be inspected.

2) They can't meet the Real-time requirement of monitoring. When a file is changed, the system can not detect it immediately. Users need to launch the software, and then the modifications can be obtained by scanning. It is difficult to meet the applications which require the relatively high and real-time monitoring.

3) Operating platform and development environment is not uniform. With different operating systems, the results may be different, causing that some features are not work properly across various platforms.

4) Source code is not open, so it is difficult to be expanded. Since there may be unknown shortcomings or bugs, it will give a huge risk for information security.

In order to overcome the above shortcomings of document monitoring, we design and implement an innovative monitoring system for computer documents. The monitoring system can carry a real-time monitoring for important data or files in computer, and more importantly it has made some breakthrough in real-time monitoring, efficiency and accuracy.

II. THE MODEL OF MONITORING SYSTEM

The file operations of computer are categorized into two categories: One is the operation of the document itself, for example, creating a new document, opening the file, closing the file, reading and writing files, etc; the

other is the operation of the file's content, for example, finding the file in the strings, inserting and deleting and so on.

In Windows operating system, all users' requests for file operations go through the process to handle the file system data, and file system driver is a component of I/O subsystem, which provides users with the services of accessing data on the disk that is the non-volatile storage media. I/O Manager supports the layered driver model, and each IRP (I/O request packet) is handled respectively through every layer of the driver, until the request is fulfilled by a layer driver. Therefore, the drivers made by third party developers have the opportunity to insert into the hierarchy, capture and process the request from the upper operation, and the drivers are called the filter drivers [6].

Therefore, we build up a system monitoring model, as shown in Figure 1. The file monitor engine includes two aspects: Window's file API function monitoring and the monitoring based on the file system drivers [7][9].

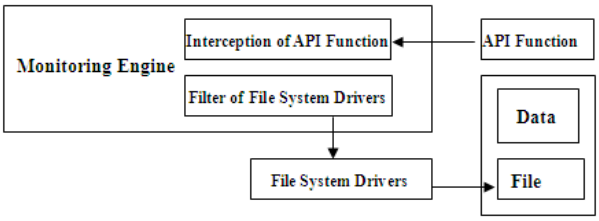

Figure 1. The model of monitoring system

III. The Main Technologies of Document Monitoring System

A. *The intercepting and calling technology of system*

In Windows system, the kernel module NTOSKRNL.EXE exports a system call table (Service Table), all operations such as process management, file operations, and memory management, are completed finally by the interface functions provided by the system call table.

In Windows, there are certain shortcomings when intercepting system calls. The CreateFile kernel function of windows can be used to open the object (not just the files), furthermore, it can be used to load device drivers, can also be used to create and open a Windows system, pipe objects, mail slot object and the physical drive. Therefore, intercepting system calls needs to filter a lot of information what people do not care about, avoiding unnecessary system overhead.

B. *The Mounting Technology of Virtual Device*

To avoid these above shortcomings, there is a monitoring technology of file operations which is only related to the file system of Windows operating system. We call it the mounting technology of virtual device.

The Mounting Technology of Virtual Device writes virtual device driver, and mounts the virtual devices to the disk devices, so as to get all the information of file operations. The code in this way is at the lowest level of the system, and only one device driver can monitor all file operations.

C. *The Combination of Two Technologies*

The combination of the intercepting and calling technology of system and the mounting technology of virtual device can guarantee both the security of system and the transparency of monitor process [10].

The core of monitoring technology of file operations is a kernel driver file called FILEM.SYS. The monitor program loads the driver FILEM.SYS after it starts the monitoring of file operations Once FILEM.SYS is initialized, it registers a device to the system, and implements and monitors the communication of programs through the interface function FilemonFastIoDevice-Control in the kernel. Monitoring program passes the command to the driver by calling basic API functions [9].

For each I/O device to be monitored, we must first obtain a handle of the file system, and get the handle related to I/O device through the function IoGetRelatedDeviceObject from it. After that, the drivers call the function IoCreateDevice to create a new virtual I/O device for the monitoring device, and then the new virtual I/O device is linked to the monitored I/O device. All the operating requests of monitored I/O device will be first sent to the virtual I/O device, and then sent to a real virtual device I/O device by the virtual device. Each operation request contains the file handle, the operating parameters of the content and so on. After an operation, the return value will be sent to the virtual device. By adding appropriate code to the virtual I/O device interface process, you can record all operations. Figure 2 illustrates the processes of intercepting I/O operations as follows.

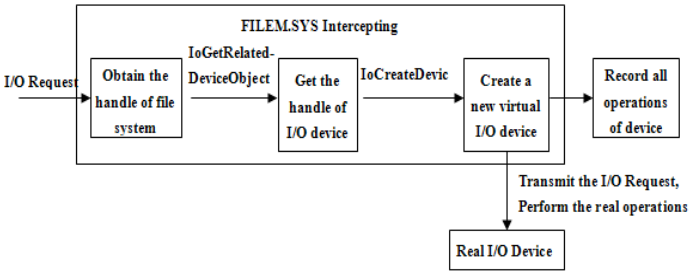

Figure 2. Flow chart of intercepting I/O operations

IV. THE DESIGN OF DOCUMENT MONITORING SYSTEM

The implementation of system is divided into 3 parts, including file content monitoring, folder monitoring and the management of document, as shown in Figure 3.

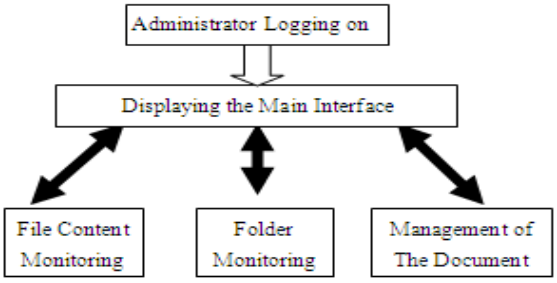

Figure 3. Flow chart of the monitoring system

Any attempt for illegal operations of sensitive or important documents in the computer, will be monitored and controlled by our document monitoring system. Meanwhile, the system records the illegal operations, and warns system manager by showing the recording results. The framework of the document monitoring system is shown in Figure4:

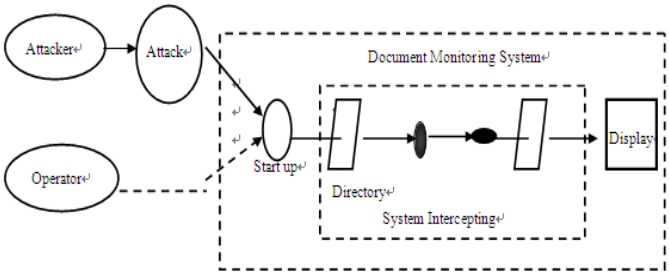

Figure 4. Framework of the document monitoring system

V. *System Performance Testing*

A. *Testing Environment*

The operating system is Windows XP, and.Net Framework 2.0 is required.

B. *Functional Tests*

Firstly, we test the system's main function. It mainly consists of the following tests:

1) The tests of file's content monitoring
2) The tests of folder monitoring
3) The tests of the monitoring and management system.

C. *Testing Results*

1) The Testing Procedure

Open the monitoring system, and select the folder in the disk that you want to monitor, carrying out a series of operations on the contents of the file and on the folder respectively. The testing results are shown in Table 1:

TABLE 1: THE RESULTS OF MONITORING TEST

Testing Project	Testing point	Accord with the strategy or not?
The test of file's content monitoring module	Create a file	Yes
	Rename a file	Yes
	Delete a folder	Yes
	Modify the contents of the document	Yes
The test of folder monitoring module	Create a folder	Yes
	Rename a folder	Yes
	Delete a folder	Yes
	Operations of the files in the folder	Yes
The test of document management module	Open the folders and files needed to monitor	Yes
	Display file's name	Yes
	Display accurately the time of last access to the folders and files	Yes
	Management functions	Yes

2）The Result Analysis

- The file content monitoring module:

When the contents of the file are changed, (deleted, renamed and so on) the system can accurately detect the changes and warn users at real time. Our experiments show that it realizes all of the monitoring functions, and can monitor the operations of illegal users effectively. The result is shown in Figure 5:

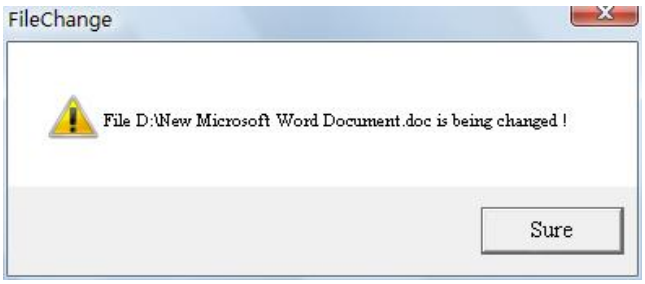

Figure 5. The warning message box of file being changed

- Folder monitoring module:

When a folder is modified, the system can accurately show what operations have been applied to the folder. When the files in the folder are changed, the system can also show what changes have happened to the folder. This experiment shows that the monitoring system realizes the fold monitoring functions, and can monitor the operations of illegal users effectively. The result is shown in Figure 6:

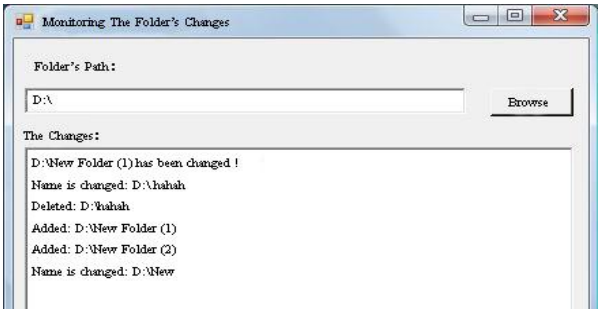

Figure 6. The warning of the illegal operations of folder monitored

- Document Management Module:

The monitoring system can accurately shows the attributes of the files, which plays a very important role in system management.

C. Performance Test

Only a little resource is needed to realize the monitoring functionality. A testing program is developed to perform concurrency operations of the file and folder modification. CPU utilization and memory utilization are recorded under different experimental configure conditions, as illustrated in Figure 7. We notice that the amount of both CPU and memory increase with the increase of the number of concurrent monitoring documents, but the increase is not very obvious. It shows that the impact on system performance is limited, and monitoring system runs smoothly in the entire testing process.

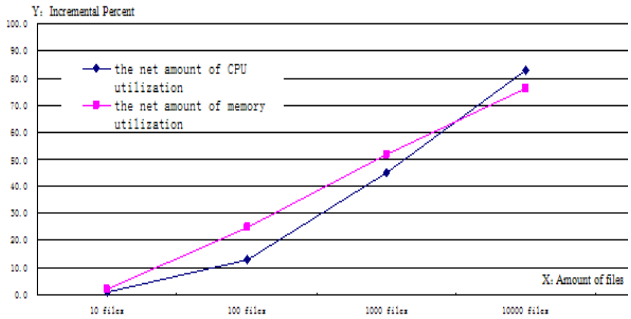

Figure 7. The impact of monitoring on the computer resources

VI. *Conclusions*

The monitoring system has many advantages, such as real-time, high efficiency, accuracy, ease of use. It dominates other monitoring systems in the following aspects:

(1) Monitoring objects are clear. The system can monitor the illegal document's operations such as deleting and tampering from either local or network.

(2) The system can set different levels of monitoring according to the level of the document's importance, thus saving more resources and improving the efficiency.

We no only use the above monitoring system to protect our critical documents, but also use some other methods to strengthen the security mechanisms of our computer system at the same time such as the encryption of communication and the authentication, etc. In a word, we must try my best to improve the defense capability of the system itself in order to reduce the false negative rates and false positive rates of the monitoring system for critical documents as much as possible.

REFERENCES

[1] Rising, http://pc.rising.com.cn/risd.html

[2] Skye, http://www.skye.cn

[3] Anyview, http: //www.ismyway.com

[4] File Monitor, http://www.sysinternals.com

[5] Qing Sihan, Liu Wenqing, Wen Hong. Operating System Security [M]. Peiking: Tsinghua University Press, August 2004.

[6] Dai Shijian.The Technology of Data Recovery (2nd Edition) [M]. Peiking: Electronic Industry Press, 2005

[7] Christian Seifert, Ramon Steenson, Ian Welch, etal. Capture-A Behavioral Analysis Tool For Applications and Documents [J]. Digital Investigation, 2007, 4 (1): 23-30

[8] Qu Jin, LI Qingbao, Bai Yan, etc. Application of File System Filter Driver In Network Secure terminal [J]. Computer Applications, Mar 2007, 27 (3): 624-626

[9] Zhao Bin, Liu Changqi, etc. The Monitoring Technology of File Operations of Windows Operating System [J] Computer Engineering and Applications, Nov 2004 (11): 131-133, 168

[10] Hu Hongyin, Yao Feng, HE Chengwan. Solution of Windows Files Security Protection Based on File System Filter Driver [J]. Computer Applications, Jan 2009, 29 (1): 168-171