Webpage Tamper-resistant Strategy Based on File System Filter Driver and Event-triggered

Zhenqi Wang
Information & Network Management Center
North China Electric Power University
Baoding, China
w-zhenqi@ncepubd.edu.cn

Weiping Wang
Information & Network Management Center
North China Electric Power University
Baoding, China
wangweiping525@126.com

***Abstract*—In order to develop a more practical, higher security and less time-consuming webpage tamper-resistant system, we proposed a webpage tamper-resistant strategy on the basis of original tamper-resistant strategies and technologies in the paper. This strategy adopted the file system filter driver and event-triggered technology. It also controlled users' writing operations through the file filter driver of the bottom of the system, which can efficiently and actively prevent attackers' illegal tampering. At the same time, it had also set up a monitoring module. The monitoring module and the tamper-resistant module formed a self-protection mechanism of the ring. Therefore, the strategy can greatly improve the security of system.**

Keywords-webpage tamper-resistant; file system filter driver; event-triggered

I. INTRODUCTION

With the continuous development of the Internet, the number of websites increased dramatically. At the same time, network security issues have become increasingly prominent. The phenomenon that webpage illegally tampered is more severe. Attackers have different objectives on using system loopholes and all kinds of tools on the webpage tamper, which caused damages but can't be simply measured. Damages rang from the personal and corporate image to huge business losses, and even affected social stability [1].In conclusion, the problem of webpage illegally tampering can't be ignored. At present, many companies have developed webpage tamper-resistant products, but mostly based on the time polling detection technology, event-triggered technology and core embedded technology. These products didn't get extensive application. Because these three technologies have more or less defects. Therefore, the phenomenon that webpage is illegally tampered often occurs.

Therefore, it is very necessary for us to develop a more practical, security and save-time webpage tamper-resistant system. Nowadays, the file system filter driver technology is widely used in the real-time access control of the files, auditing and virus monitoring etc [2], which provides the necessary technical support for developing a webpage tamper-resistant system based on file system filter driver technology.

II. FILE SYSTEM FILTER DRIVERS

A. File System Driver

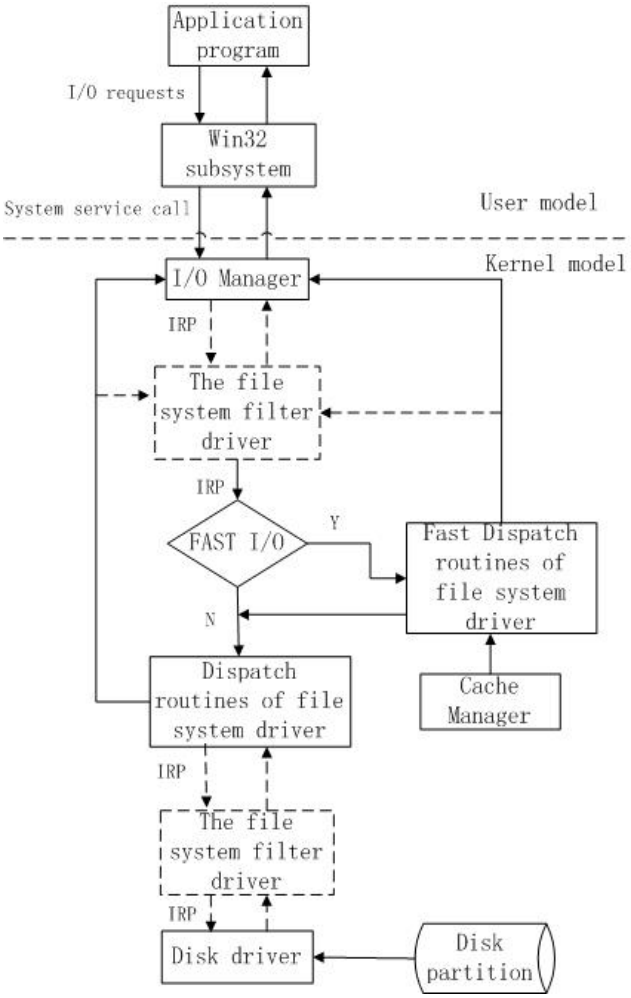

Figure 1. The workflow chart of file system response to I/O request

The file system driver is integral part of the storage management subsystem. It provides non-volatile medium (disk, tape etc.) information storage, and forwards for users. The workflow of the file system driver in response to user

Published by Atlantis Press, Paris, France.

I/O request is shown in Figure 1 [3-5]. The operations of all files are completed by the win32 subsystem called the appropriate service request. The I/O manager receives I/O request from the upper layer, according to the application layer requires sends I/O request packet (IRP package) to the file system driver. The file system driver receives IRP package. Firstly determines whether it is a Fast I/O request. If it is, the file system driver sends it to the Fast Dispatch routine while obtains data from the Cache manager, and then sends the data to the I/O manager. If not, the Dispatch routines handle IRP packets and data is obtained by disk drivers from the disk partition, and then data is also sent to the I/O manager. Finally, data is returned to the application program by Win32 subsystem processing.

The file system filter driver is an optional driver, which provides value-added functions for the file system. It can lie between I/O manager and the file system drivers, or the file system driver and disk drive. If there is a file system filter driver, the control flow of file operations will be changed, as shown in Figure 1 dashed box. IRP package first will be processed by the file system filter driver and then sent to the file system driver. Similarly, the request data also needs to be processed by the file system filter driver and then be returned to application program. Therefore, the file operations can be controlled by using custom routines on the file system filter driver.

B. The Workflow of the File System Filter Driver

The file system filter driver for the file system is attached in the file system [6]. Its goal is to capture all the Windows system operating files behaviors. For example the files are to create, open, read/write, rename, and the directories are to create, open, enumeration, rename, and delete etc [7]. Windows NT I/O Manager constructs IRP according to the users' files request, and then sends IRP to a file system drive. The file system driver converts the file system operations into corresponding to the operations of the storage device driver. And the storage device driver is invoked by the I/O Manager. After the filter driver is attached to the file system, the IRP workflow as shown in Figure 2 [8]. Before I/O Manager sends operation requests to the target device object, it will first check whether the target object has attached to the other drive device object. If there is, and the filter drives in the top of device object stack, I/O Manager will send request to filter driver. Thus, filter driver will intercept IRP before it reaches to file system. After processing, filter driver records the next layer stack location in the IRP, and returns IRP to the I/O manager. I/O manager in turn submits IRP to the next driver for processing, until the bottom driver has dealt with IRP, and returns IRP to the I/O manager. Finally I/O manager releases resources of IRP application.

Thus, the file system filter driver can increase new functions and monitor program to read input /output operation of each file system on the basis of not modifying the system driver and application program. And it has the function to modify the file system. Therefore, file system filter driver technology is usually used for data storage encryption, decryption, virus detection, access control and other fields.

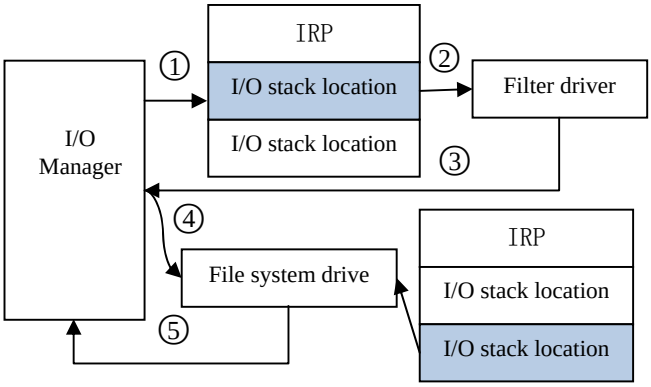

Figure 2. Attached with a filter driver after IRP workflow chart

File system filter driver likes other programs, has a primary function, that is, DriverEntry [9], in the following format:

NTSTATUS DriverEntry(IN PDRIVER_OBJECT DriverObject, IN PUNICODE_STRING RegistryPath)

{

… … … …

return status;

}

DriverObject is a driver object. It is assigned when the system loads the driver. RegistryPath is dedicated to recording drive related parameters registry path. DriverObject driver object has a set of function pointers (Dispatch Functions), before sends IRP to the target device, writes this set of functions. In the Dispatch Functions in accordance with functional requirements deals with these IRP, allows the IRP failed out or successful return, or modifies it, even constructs IRP and sends to the lower driver.

III. THE TRADITIONAL WEBPAGE TAMPER-RESISTANT STRATEGY

At present, the webpage tamper-resistant strategy mainly has three kinds as following [10-12].

A. The Polling Detection Strategy

The strategy establishes a document detection procedure, in the polling way at a certain time to read protected webpage file, and then compares with the pre-save backup webpage file. By comparing the results to determine whether the file has been tampered with. If it has been tampered with, and then restored. The strategy has been basically eliminated, because it consumes excessive server resources and can't prevent continuous tampering.

B. The Event-triggered Strategy

The strategy takes advantage of users' access to the server as a triggering event. Once the event is triggered, the

tamper-resistant program verifies the files' integrity, and determines whether a document had been illegally tampered. If it has been tampered, immediately restored. Obviously, the strategy belongs to the "passive defense", it also unable to resist the continuous tampering and to cope with hackers hijack webpage file write permissions or hackers trying to end the security process etc.

C. The Core Embedded Strategy

This strategy is mainly based on "digital watermarking" technique. When website is deployed, it extracts digital watermark (digital fingerprint) of all the webpage files, then when users need to access the webpage files in the website, extracts digital watermark (digital fingerprint) of the webpage will be accessed, compares the watermark of current extraction with the previous backup. If it finds they are different, this indicates that the file had been tampered, immediately prevents the file from continuing to flow out, and calls the recovery program to restore the tampered webpage. The strategy can effectively prevent tampered webpage outflow, but because when digital watermarking technology extracts large files watermarking, its speed is particularly slow.

According to researched the three kinds of webpage tamper-resistant strategies above, we find that they have their own advantages and disadvantages, but could not be better applied in the webpage tamper-resistant system. Therefore, under the premise of these tamper-resistant strategies deeply researched, this paper proposed a webpage tamper-resistant system design strategy using the underlying operating system file system filter driver technology combined with event-triggered technology.

IV. SYSTEM DESIGN STRATEGY

A. System Design Idea

In this paper, the webpage tamper-resistant strategy mainly consider from the following several aspects:

1) Initiative. According to analyzed several existing tamper-resistant strategies, we find that they have a common shortcoming: passive tamper-resistant strategies. That is, after the webpage had been tampered, these strategies could find and restore it. It is obvious that the process of restoring webpage may impact the system performance. Therefore, it is very necessary that the webpage protection is changed from passive to initiative. That is to say, when hacker tampers webpage, it can be found, and promptly be interrupted the tampering operation. Hacker attacks and tampers webpage mainly through a variety of means writing illegal information to server storage device. Therefore, we can make use of file system filter driver technology and event-triggered technology to effectively control write operations (add, modify, delete etc), to ensure the legitimacy of the write operations. Thus, it can effectively prevent the webpage from illegally tampering.

2) Security. The webpage tamper-resistant system not only needs to ensure that the webpage is legal, but also needs to ensure its security. Sometimes attackers find unable to directly tamper webpage, they might first attack the tamper-resistant system itself, which could make the system top protecting the webpage. Therefore, in order to protect its security mechanism, the strategy sets up a monitoring module. It and the tamper-resistant module formed a self-protection mechanism of the ring, as shown in figure 3.

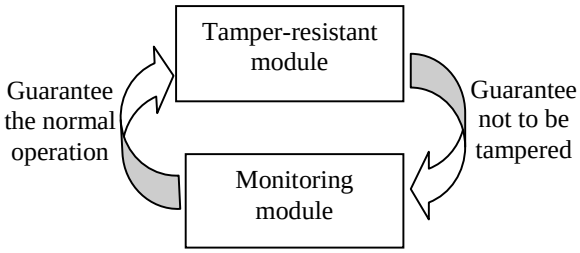

Figure 3. The tamper-resistant system itself protection mechanism

3) High efficiency. Guaranteeing that webpage is not tampered, at the same time we also can't ignore the response speed of user's request. Namely, do not put the cart before the horse, losing the true value of the webpage. The strategy mainly verifies writing operations and directly responds read operations. Therefore, it does not affect the webpage response speed, even if the verification of write operations time-consuming is relatively short.

B. Deployment of the System

According to the system idea above, this paper presents the webpage tamper-resistant system deployment diagram as shown in Figure 4.

Figure 4 shows that the structure of website operation process is mainly divided into three districts.

1) Internet District. In the district, there are normal users and hackers. For a website, it doesn't trust district. Therefore, we set up a firewall to block the application layer attacks as much as possible.

2) DMZ Isolation District. The Web server was deployed in the district. It is open to the external network. So, it must deploy IIS and Apache etc that used to web publishing service system. At the same time, it deployed webpage tamper-resistant system that used to prevent malicious webpage files in the web directory. Its work process is as follows:

a) The release directory IRP (I/O Request Packet) can be intercepted by using the file system filter driver technology in the bottom of the system.

b) Analyzing IRP, then putting all the write request files write on a temporary directory.

Published by Atlantis Press, Paris, France.

c) The feature code of temporary files is extracted by using the MD5 function.

d) The feature codes and their corresponding file basic information are packed and sent to the release server that stored signature library, then compared with the original feature values. If consistent, namely, the write request is legal and then sends verification legitimate message to the Web server. Otherwise, the request is illegal and sends verification illegitimate message.

e) If the Web server receives validation feedback message that is legitimate, then writes the temporary file to the specified web directory, releases and deletes temporary files. On the contrary, the tamper-resistant module writes the access records to the security log and transfers the file to the virus isolation directory, which as evidences of the pursuit of hackers. At the same time, the module sends log information to the management server and alerts to administrators.

3) Intranet District. The release server and the management server were deployed in the district. The release server automatically releases webpage and takes advantage of the hash function (MD5 algorithm) to calculate the hash value of the new release webpage. In order to use verification integrity of the file, the values are stored in the signature library. Meanwhile, the release server sends a message to the Web server. The message contains a storage path of the webpage files storage in the release server. After the Web server receives the message, downloads and verifies the file, and then copies the file to release directory. The Management server is mainly used to manage the release server. In addition, it receives and manages the tamper log, alarm information from the Web server.

V. SUMMARY

In this paper, we proposed a webpage tamper-resistant strategy based on the file system filter driver technology and event-triggered technology, and introduced its deployment. The strategy not only can effectively, rapidly and actively prevent webpage tamper-resistant, but also can protect itself. It has greatly improved than the previous several webpage tamper-resistant strategies, but it also has many inadequacies. In the future, with the increasing development of webpage tamper-resistant technologies, the strategy requires continuous improvement.

References

[1] FAN Jian-hua, and SONG Yun-bo, "Web Page Tamper-resistant Mechanism Based on File-filtering Driver and Event-triggering," in Journal of Chongqing Institute of Technology(Natural Science), vol. 23, No. 12, December 2009, pp.65-70.

[2] Shen Wei, Wang Lei, and Chen Jia-jie, "Design and Implementation of Encryption System Based on File System Filtering Drive," in Computer Engineering, vol.35, No.20, October 2009, pp.157-162.

[3] Fu De-sheng, and Pan Yi, "Multi-Rules Encryption System based on file system filter driver," in Net info Security, vol.7, 2009, pp:44-46.

[4] Gu Zhu,Zhou Liangchen, and Lv Guonian, "The Access Control Technology of Spatial Data Files Based On File System Filter Driver," in Communication Technology,2008.ICCT 2008.11th IEEE International Conference on,Nov. 2008, pp.734–737.

[5] Cao Cheng-long,Fu De-sheng,and Cao Feng-yan, "Solution of removable storage control based on file system filter driver," in Journal of Computer Applications, vol.31,No.6, June 2011, pp.1498-1501.

[6] Zhao Zhongmeng, "A Data Backup Method Based on File System Filter Driver," in Software Engineering(WCSE), 2010 Second World Congress on, vol. 2, Dec.2010, pp:283-286.

[7] Tan Wen,Yang Xiao,and Shao Jianlei, Painting by fishing: Windows kernel security programming, Beijing: Publishing House of Electronics Industry, 2009, pp.163-212.

[8] Li Min,Fang Yong,Liu Ling-chao, and Xiong Fan, "Filter Driver on FSD and its Applications," in Information and Electronic Engineering, vol.3, No.4, Dec. 2005, pp.290-292.

[9] Wang Yong, He Qian, and He Shengtao, "Research on webpage anti-tamper system based on file filter driver," in Journal of Guilin University of Electronic Technology, vol.30, No.5, Oct. 2010, pp.432-435.

[10] Fei Yang, "The webpage tamper-proofing technology," in Computer Security, No.9, 2008, pp.76-77.

[11] Wang haitao, and Du hongwei, "The Analysis of Web Content Security Technology," in Informatization Research, Vol.36, No.12, Dec. 2010, pp.1-3.

[12] Yue-guo Luo, and Hai-jun Tan, "The Design and Implementation of A Real-time Webpage Tamper-Proof Technology," in Mechatronic Science, Electric Engineering and Computer (MEC),2011 International Conference on, Aug. 2011, pp.1743-1745.

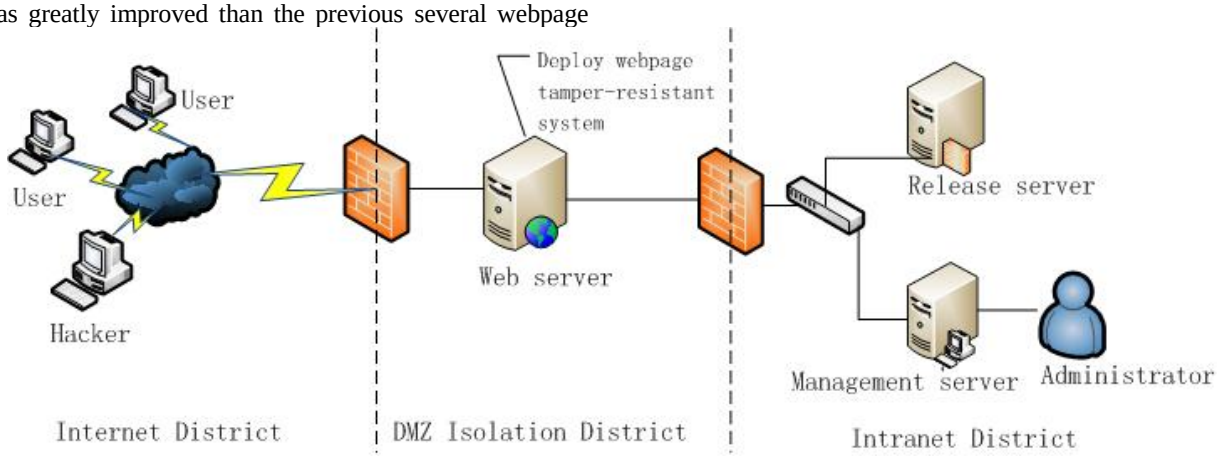

Figure 4. The webpage tamper-resistant system deployment diagram