2012 International Conference on Computer Science and Electronics Engineering

Research of the File Access Security based on Hardware Confirming Mechanism

Chen Liandong
Hebei Province Electric Power Company Information Center
Shijiazhuang, China
chenliandong1@126.com

Chen Fei
Control and Computer Engineering School
North China Electric Power University
Beijing, China
chenfei0428@126.com

Ding Tao
Control and Computer Engineering School
North China Electric Power University
Beijing, China
eilwen_dt@163.com

Guo Ming
Hebei Province Electric Power Company Information Center
Shijiazhuang, China

Abstract—**Aiming at how to ensure the file security access in the Information Systems, this paper presents the new idea of hardware confirming mechanism, constructs the hardware confirming model on the basis of it, and designs the relevant file access technical architecture. It intercepts the process which will access the protected files, while detecting the local hardware signal, to implement the security access control for the confidential files and ensure the trusted operations on these files.**

Keywords- file security; hardware confirming; access control

I. INTRODUCTION

With the development of information technology, computer plays a vital role in our daily life. Informatization is becoming the inevitable trend to the enterprise development. Therefore, information security has become increasingly valued by the people. It is important to secure access to important files on computers, which relates the development of the enterprises. How to protect enterprise information security and do not affect the daily work is an important issue which must to be solved.

As Trojans and other hacker techniques flooded, the traditional approach has been difficult to ensure the protection of data confidentiality and integrity. To achieve the security of information system in the file access control, this paper presents the new idea of hardware confirming mechanism, constructs the hardware confirming model on the basis of it, and designs the relevant file access technical architecture. It ensures the legitimacy of file access and trusted operations on files.

II. RELATED RESEARCH

Generally speaking, there are two traditional file protection technologies [1]: one based on access control and the other based on data encryption.

The technology based on access control depends on the authority distribution. It usually uses the simple authority judgment to stop the file access from unauthorized process. Because this protection is in the user mode, any process can access the temporary files in the protection procedure or the plaintext in the cache [2, 3]. Once hackers get enough permission, they can access confidential files unscrupulously. In addition, the file is stored on disk in plain-text, so there are potential safety problems. Therefore, the single access-control is not strong enough.

The technology based on data encryption is dependent on the encryption algorithm and key management. It encrypts the plaintext and stores it on disk in ciphertext so that the important files can be protected to a certain extent. Even if hackers get the chance to access confidential files, they can only receive a pile of useless data since the data cannot be decrypted currently. Although this method is useful, the traditional encryption software requires users to encrypt and decrypt manually, which is hard to operate. And because it relies solely on cryptography mechanism, it cannot ensure the trusted operations on files.

III. FILE ACCESS BASED ON HARDWARE CONFIRMING MECHANISM

A. Hardware Confirming Mechanism

With the prevalence of the hacker technology, traditional way of file protection has been difficult to ensure data confidentiality and integrity, especially file access security. The latest Trojan technology is more and more complicated, and toward the hidden files, hidden processes, hidden communication direction [3, 4]. Because of its close combination with the operating system, the conventional defense software is difficult to distinguish the file access operation is a real user operation or Trojan illegal action.

The study found that, the Trojan programs always hook system service calls in order to insert messages, which simulate the actual operations from keyboard or mouse, into the message queue of current system task, so that they could connect to the hosts with the remote control or get the access to the important files. And there is no hardware signal from the hardware ports on the controlled host, when Trojan simulates the normal user operation [5, 6]. Under this circumstance, the access operation can be judged through the local hardware signal confirming. In the confirmation process, the way of

978-0-7695-4647-6/12 $26.00 © 2012 IEEE
DOI 10.1109/ICCSEE.2012.469

checking hardware port signals can judge whether the operating signal of keyboard or mouse is come from local host operating. If there is no right hardware signal from local host, it can be known that this operation is not the legitimate access action, and it should be refused. The hardware confirmation of local operation ensures the file access is issued from the local host instead of the remote control, and implements security and non-repudiation of file access.

B. Model of Hardware Confirming Mechanism

According to the hardware confirm thought, we set up the hardware confirming model as shown in figure 1. The model increases the hardware signal detection module based on the existing file access control, and implements the local hardware confirmation to the file access operation.

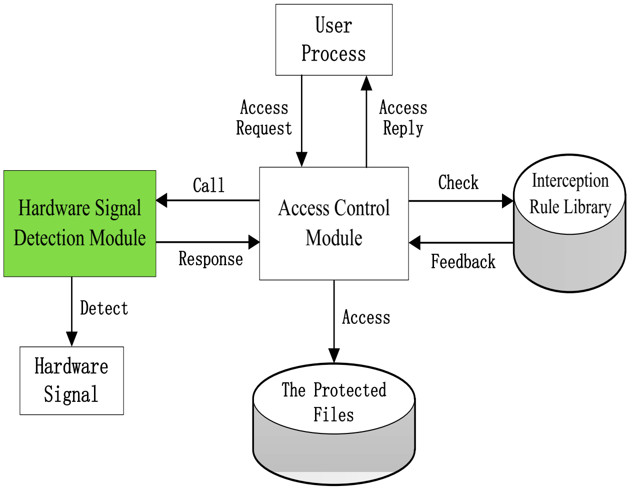

Figure1. Model of Hardware Confirming Mechanism

In this model, the file access operation requires the confirmation of the access control module. The access control module intercepts the access and other operations of user process to the protected files, and inquires the interception rule library deciding whether or not to request hardware signal confirmation. If necessary, it will send check request to the hardware signal detection module. The hardware signal detection module is responsible for monitoring the signal information on the hardware port, and then response the checking results to access control module. If the hardware confirmation is not necessary or the access action has passed the local hardware confirmation, access control module will allow the user process to access the protected files. Otherwise, it will refuse the operation.

There are lots of processes when system at running. But actually, just for some special processes requires hardware confirming rather than all operation. With the help of interception rule library, the process which should be intercepted will be found and recorded. It ensures the security and efficiency of file access.

The host hardware signal detection must to be judged through the operating system low-level drive. It distinguishes the message between hardware signal and software simulation signal, and connects the target process of hardware signal with hardware message. By modifying the kernel hardware drivers or driver collaborative programs, it will detect the status of hardware port at real time and implement the judgment to the hardware signal.

C. The File Access Technical Architecture Based on Hardware Confirming

Modern operating system has two different execution modes: user mode and kernel mode. The program in these two modes runs in different processor level, and has different access authority to the system and hardware resource. The program running in user mode cannot optional calls the data structure and code of kernel mode, and has some limits when access to the system or hardware resource. The process running in user mode needs to communicate with the system kernel, and application requests will be transferred to the kernel space through the system calls. Then, the kernel code executes the kernel space function calls so that implement the kernel function, such as process scheduling, IO management, and so on. The driver is also located in the kernel space. It communicates with hardware, gets the status information of hardware and control the normal running of hardware [7, 8].

Modify the current system architecture on the basis of the established hardware confirming model. It will implement the security control to file access in the kernel layer, and ensure the access behavior is truly sent by the local host. The specific technical architecture is shown as figure 2 below.

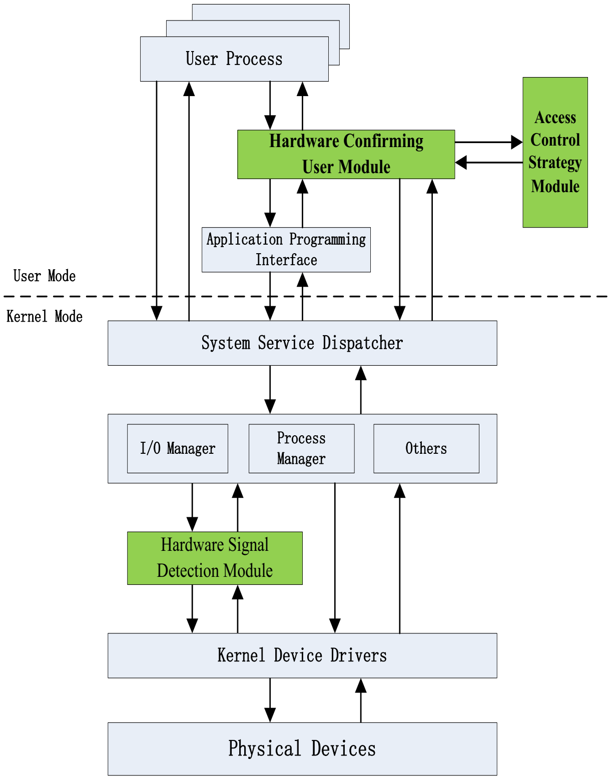
User Process
Hardware Confirming User Module
Access Control Strategy Module
Application Programming Interface
User Mode
Kernel Mode
System Service Dispatcher
I/O Manager
Process Manager
Others
Hardware Signal Detection Module
Kernel Device Drivers
Physical Devices

Figure2. The File Access Technical Architecture Based on Hardware Confirming

- Access control strategy module: According to the information system security level requirements, the module ensures the security of file access through strategy control. It defines the information of process which needs to be monitored and let it as the basis of process monitoring. The module collects access control strategy, establish corresponding interception rule library and ensure dynamic update for the strategy.
- Hardware confirming user module: The module monitor running process in the operating system. When finding uncertain operation which need to hardware confirmation or unauthorized process which will access sensitive files, it calls access control strategy module to check the operation security, and handle the return information. If the process is the identified illegal process, the module will intercept it and stop it from accessing files; and if the operation of the process need to hardware confirming, the module will inform hardware signal detection module through inter-process communication to confirm the access behavior.
- Hardware signal detection module: The module accepts calls coming from hardware confirming user module and detects whether there are any hardware signal belong to this process with a specific time. If there is the corresponding signal, it will inform the hardware confirming module that the file access behavior is safe and call the kernel driver to implement file access. If there is no hardware signal in the set time, it will forbid the access operation of this process.

D. The File Access Procedure Based on Hardware Confirming

The hardware confirming of file access need the cooperation of multi-module, and also need some related deals for the user and kernel space. When hardware confirming module intercepts the file access process, it calls the access control module to check the security for the process. And then, hardware signal detection module in the kernel layer detects the hardware signal of the process which passes the security checking. The detailed execution procedure is shown as figure 3 below.

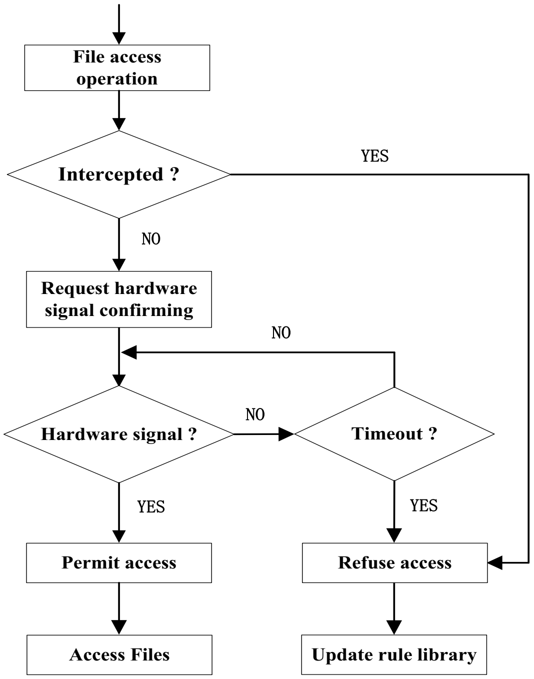

Figure3. The File Access Procedure Based on Hardware Confirming

IV. CONCLUSION

Concerning of the changing technology, hackers and Trojans, the traditional ways can no longer guarantee to protect file access security. This paper based on the existing file access controlling, presents the new idea of hardware confirming mechanism, constructs the hardware confirming model on the basis of it, and designs the relevant file access technical architecture.

The file access control based on hardware confirming mechanism uses the local host hardware signal detection for access control to ensure that the file access operations from the actual operation of the local host behavior. It prevents the damage from Trojans, remote control and other malicious programs. And finally, it achieves the safety protection for files in information system.

REFERENCES

[1] Shen Wei, Wang Lei, Chen Jia-jie, “Design and Implementation of Encryption System Based on File System Filtering Drive,” Computer Engineering, vol.35, No.20, 2009, pp.157-159.

[2] Li Min, “The Study and Implement of WFSFD-based File Encryption/Decryption Technology,” Sichuan University, 2006.

[3] Liu Hong-yue, Fan Jiu-lun, Ma Jian-feng, “Research Advances on Access Control,” MINI-MICRO SYSTEMS, 2004.

[4] Bao Lian-cheng, Zhao Jing-bo, “A survey on access control technology,” Electric Drive Automation, vol.28, No.4, 2006, pp.1-5.

[5] Wu An-he, Tai Ming, Yu Hong-tao, “Windows 2000/XP WDM Device Driver Development,” Electronic Industry Press, 2003.

[6] Mark E.Russinovich, David A.Solomon, Microsoft Windows Internals, Fourth Edition, Washington, 2004.

[7] Tan Wen, Yang Xiao, Shao Jian-lei, “Windows Kernel Security Programming,” Electronic Industry Press, 2009, pp.223-273.

[8] Guo Jing-huan, Meng Xiang-di, Xiong Mu-di, “The application of multi-thread mechanism using in the communication between application and driver,” Microcomputer Information, vol. 21, 2005, pp.129-131.