Cloud Storage System which Prevents Information Leakage from Client

Kuniyasu Suzaki*, Toshiki Yagi*, Kazukuni Kobara*, Nobuko Inoue‡, Tomoyuki Kawade‡
{k.suzaki , yagi-toshiki , k-kobara}@aist.go.jp, {ninoue , kawade}@sciencepark.co.jp
* National Institute of Advanced Industrial Science and Technology(AIST), ‡SciencePark Corporation

Abstract
Even if a file on a cloud storage system is encrypted or transferred by secure communication, it becomes plain text on a client machine when a legitimate application opens it. It is not adequate for sensitive contents, because a user may expose the contents by mistake. When a malware has already infected to the client machine, it may steal the contents.

In order to prevent information leakage from a client, we propose special access control for a cloud storage system, which is called NonCopy. NonCopy denies some types of data flows on a process which uses a file on the cloud storage. The file can be opened by a legitimate application, but cannot be copied to other storage, transferred to other via network, printed, and screen-captured&pasted. NonCopy is implemented on Windows and prevents information leakage from client.

1. Introduction

According as cloud storage services turn out popular, information leakage becomes big concerns. Information leakage from servers is dealt with encryption, but the contents must be plain text on legitimate application on a client. The contents may be exposed mistakenly by a user (i.e., inadvertent copying or printing). If the user has evil intent, he can steal it by screen-capture&paste.

Some applications (e.g., MS Office) have a function to encrypt a saved file and allow to distribute it safely in the internet. However, most of these applications also do not limit copying the contents. In addition to encryption, PDF file can add options to prevent printing and screen-capturing&pasting, but normal file cannot set such security functions.

In order to solve the problem, we propose special access control for a cloud storage system. The access control prohibits some channels of data flow on a process which use a file on the cloud storage. The access control system is implemented on Windows and called NonCopy.

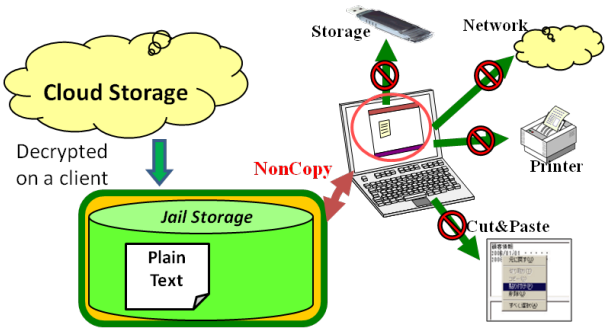

Figure 1. Access Control on Cloud Storage System

2. Outline of Access Control

The access control needs to detect a process which uses a file on cloud storage, and prohibit some channels of data flows on the process. The channels are (1) copying the file to other storage, (2) transferring the contents to other machines through network, (3) printing the contents, and (4) screen-capturing&pasting of the contents. The figure 1 shows the image of the access control.

The access control mechanisms are implemented in kernel space and user space, because some channels of data follow are not easy to prohibit in kernel space only. For example windows manager deals screen-capturing&pasting as a user space capability.

3. NonCopy

The access control "NonCopy" is consisted of 1 service in user space and 3 drivers in kernel space. Figure 2 shows the Structure of NonCopy on Windows. NonCopy service communicates to a driver and maintains process information. The 3 drivers are NonCopy process module, which gets process information, and 2 filter managers (for file and network) for access control.

3.1 Process detection

NonCopy needs to classify active processes into normal process and access-controlled process (NonCopy process). The existence of NonCopy

process is managed by NonCopy Process Module (NPM).

The NPM is informed a PID from a filter manger when a process accesses to a file on the cloud storage managed by NonCopy. The access is detected by the filter manager mentioned in Section 3.2. The PID is registered in NonCopy process list in NPM, and also informed to NonCopy service in user space. The process list is maintained in both kernel and user space.

In order to know termination of NonCopy process, the NPM monitors Process Manager of Windows. The NPM can know process termination using PsSetCreateProcessNotifyRoutine, which is a monitoring function offered by Windows.

3.2 Prevent copying to other storage

NonCopy allows any process to open and save a file in the cloud storage managed, but denies NonCopy process to save a file to other storage.

This mechanism is implemented as a filter manager which is inserted between I/O manager and file system. When an access is issued to the cloud storage, the access is hooked. The PID of the access is send to NPM using IRP (IO Request Packet), and registered as NonCopy process. When a write access issued to other storage, the access is also hooked and checked whether the access is issued from NonCopy process or not. If the access issued from a NonCopy process, it is denied by the filter manager. Read access to other storage is not denied, but the read data cannot go back to the storage, when the process becomes NonCopy Process.

3.3 Prevent network connection

The access control to network is also implemented as a filter manager and inserted between I/O manager and device driver. The access control works the same way of filter manger for file. In some implementation, whole access to network is prohibited during NonCopy process exists.

3.4 Prevent printing

Printing is consisted of complicated tasks because they are substituted to other processes. Even if access control is implemented as filter manger, it cannot detect which access is issued from NonCopy process. Furthermore, network printer is common recently and simple filter manager cannot achieve proper access control.

In order to solve this problem, access control for printing is implemented by replacing entry point of shared library of printing, which is called StartDoc on Windows.

3.5 Prevent screen-capturing & pasting

Screen-capturing&pasting is managed by windows manager as a user space function. A captured contents are stored at data storage called clipboard. Therefore access control for screen-capturing&pasting is implemented in user space.

Fortunately Windows offers Global Hook to inform change of clipboard. NonCopy uses SetWindowsHookEx function of Global Hook to know owner change of clipboard. When an owner is changed, the global hook sends WM_ACTIVATE message. NonCopy discards the data on clipboard when owner is changed from Noncopy process to other. The PID information is given from NonCopy service.

4. Current & Future work

NonCopy is applied on our cloud storage system LBCAS: Loopback Content Addressable Storage. Most of them are client system and will be applied and tested on existing cloud storage.

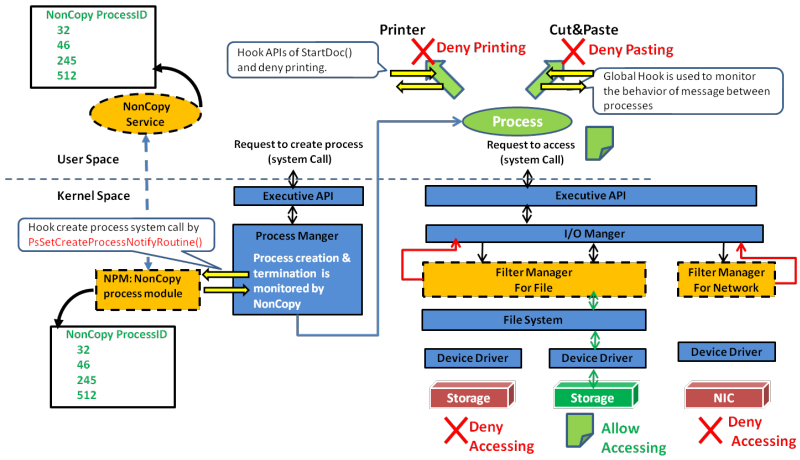

Figure 2. Structure of NonCopy on Windows OS. NonCopy is consisted of 1 service in user space and 3 drivers in kernel space. The components of NonCopy are showed as dotted-lined yellow objects.