Falsification Prevention and Protection Technologies and Products

InfoCage — Information Leakage Protection Software

By Masaru KAWAKITA,* Kazuo YANOO,† Masahiro HOSOKAWA,* Hiroshi TERASAKI,* Satoshi AOKI* and Toshimitsu USUBA*

ABSTRACT We have developed InfoCage, which is an information leakage protection software product. InfoCage is a security solution that prevents information leakage from an organization by limiting the confidential data move operations performed by users who are authorized to access secure servers. This paper focuses on the data move control function, which is one of the technical features of the product.

KEYWORDS **Information leakage, Policy management, Bell-LaPadula model, Logging**

1. INTRODUCTION

Recently, a number of companies have been alleged to have leaked customer information. These events have been intensely reported in the media and have been considered to be associated with social problems. People are now more nervous than they have been in the past about the handling of their privacy information, including personal post and e-mail addresses. In such circumstances, legislation has advanced to the stage of placing businesses under obligation to manage personal information in a secure way. If a company is found to have leaked customer private information, they will receive not only direct damage due to the payment of compensations, but also tremendous damage resulting from lost trust such as lost customers and a decline in its stock price. This kind of problem is not limited to customer information. Recently, an increasing number of companies in the manufacturing industry have begun to manufacture their products overseas. These companies are more likely to suffer the risk of leakage of design drawings and other business secrets.

It is believed that about 80% of confidential information leakage cases are caused by crime or inadvertence committed by people inside the organization. Conventional methods of controlling access to confidential data and encrypting information are not adequate to prevent such information leakage. In order to protect organizations from information leakage risks NEC has developed a technology that can prevent confidential-data files on a server from being leaked during operations on these files. For this purpose it has introduced an information leakage protection software product, InfoCage.

2. InfoCage's CONCEPT

InfoCage is a security solution that prevents information leakage from within an organization by limiting confidential data move operations performed by users who are authorized to access secure servers.

InfoCage permits all authorized users to browse and edit confidential information stored on secure servers and to save such information on secure servers. However, it limits operations performed by these authorized users to copy and save information from a secure server to a local disk and to copy and paste information from a secure server to other software, or to perform other operations that could lead to the transportation of confidential information to the outside of the secure server. Since InfoCage allows operation control rules to be specified for individual users and/or organizational units, it is possible, for example, to permit specific users or organizational units to perform print and/or other specific operations, in consideration of the particular duties assigned to such users or organizational units.

A noteworthy feature of InfoCage is its ability to handle information on a secure server and information located elsewhere in a completely different manner. For example, consider information that can be viewed on a browser. If it is on a secure server, InfoCage can inhibit such information from being printed or moved out of the secure server. If the information is from another site, InfoCage allows it to be printed and saved like ordinary data. This means

* System Platform Software Development Division
†Internet Systems Research Laboratories

that InfoCage does not inhibit all save operations on a single terminal, but inhibits save operations if they link to a certain server. In other words, InfoCage allows two types of information to be freely handled on the same terminal. Firstly, the information that must be maintained as confidential and must not be moved out and secondly, the information that is not so confidential. Some competitive products inhibit all print and save operations on a terminal in order to prevent information leakage. These products limit operations on information that is not so confidential. Such products tend to sacrifice business efficiency for high security. Another feature of InfoCage is that it can handle two types of secure servers: Web and file servers. It is possible to assign different security policies to these servers and manage server operation logs on a single management server. In addition, multiple secure servers can be liked to each other to ensure, for example, that confidential downloaded data from a secure Web server can be saved on a secure file server.

3. FUNCTIONS OF InfoCage

The InfoCage system provides three functions: Client Monitoring, Policy Management and Log Management.

The Client Monitoring function controls confidential data moves from the secure server. More specifically, it controls operations for saving or printing confidential data to a client hard disk or removable media, capturing secure server screens (printing screen contents), and moving/copying confidential data text via cut-and-paste actions.

The Policy Management function is used to create, distribute, and update policies that control confidential data moves from secure servers. Policies are established by duly authorized administrators and control operations performed by individual users or groups to print confidential data, capture screens, and paste data. Policies are distributed automatically when a user logs in to the Windows system on a client or when a policy expires.

The Log Management function ensures that logs of operations on client PCs are managed on a management server in a consistent manner. It collects logs of attempts (legal or illegal) made to access confidential files from client PCs and stores them in a relational database on the management server to ensure that the logs can be viewed and searched for on a dedicated viewer.

4. CLIENT MONITORING MODULE

4.1 Overview

The control function available to the InfoCage client is based on the Bell-LaPadula (BLP) model[1]. The BLP model is outlined below.

- Security labels are assigned to subjects, which are processes or other entities that perform operations and also to objects, which are files and other entities on which operations are performed. A magnitude sequence is defined for security labels.
- A subject cannot read an object that has a security label higher than that of the subject. This is referred to as the No Read Up (NRU) rule.
- A subject cannot write to an object that has a security label lower than that of the subject. This is referred to as the No Write Down (NWD) rule.

The BLP model has been applied to a large number of practical systems in an attempt to realize secure operating systems[2]. However, InfoCage is unique in that it can provide BLP-based security functions for existing practical applications (Version 1.0 serves Microsoft Office products).

The InfoCage Client Monitoring module is implemented as middleware. It hooks operations performed on the operating system or GUI system by the process and provides three BLP-based functions for resource access control, prevention of confidential information leakage during inter-process communication and usability improvement (**Fig. 1**). These functions are explained below.

4.2 BLP Access Control Model

4.2.1 InfoCage BLP Model

InfoCage defines only two security levels: Confidential and Ordinary. No other level is provided to classify security labels. This is both simple and understandable to users. These two security levels are necessary and sufficient to prevent any leakage of confidential data from a business system.

Subjects are processes. When a process starts, Confidential or Ordinary mode is specified for the process and continues to be effective while the process is active. In InfoCage version 1.0, only predefined types of applications can run in Confidential mode and other applications will always run in Ordinary mode.

4.2.2 BLP Application to Resource Access

Files on secure servers are treated as Confidential

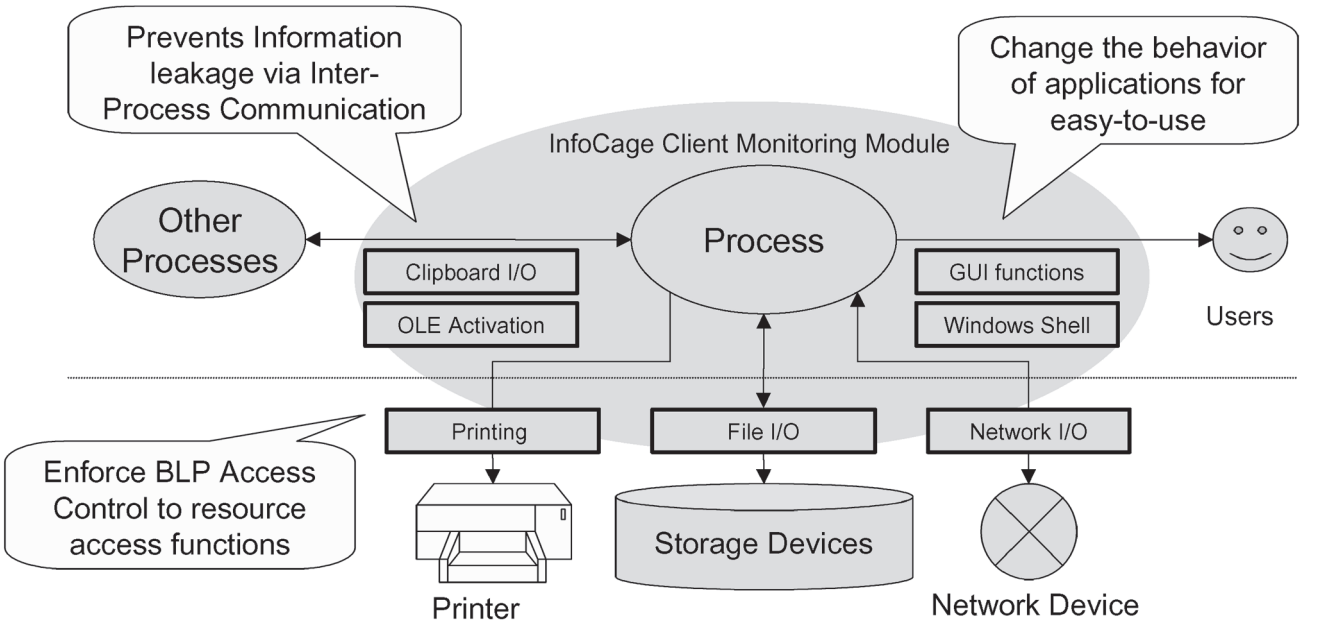

Fig. 1 Client Monitoring Module.

objects, whereas other files are treated as Ordinary objects. Therefore, only processes that run in Confidential mode can read files on a secure server (NRU rule). Processes that run in Confidential mode can only write to files that are located on a secure server (NWD rule). It is not possible that Confidential files demote to Ordinary files and leak out.

Printers and network devices are generally specified as Ordinary objects. Therefore, a process that runs in Confidential mode cannot print on a printer and cannot send files across the network.

The above functions ensure that unauthorized users are inhibited from printing data from a secure server, copying it to removable media and take it out, and attaching it to an e-mail and sending it. Such move operations can be totally prevented.

4.3 Prevention of Insecure Information Flow via IPC

Since processes are defined as subjects, complete security cannot be guaranteed without applying the BLP model to inter-process communication (IPC) as well. However, IPC based on the Component Object Model (COM) is extensively used within the Windows operating system. This raises a problem when the BLP model is applied to the Windows operating system.

InfoCage ver.1.0 does not include a feature used to directly monitor IPC. However, the following features prevent leakage of confidential information being transmitted via IPC.

- Clipboard control: Inhibits copy-and-paste operation for data transmission from a Confidential process to an Ordinary process by monitoring clipboard operation API functions.
- OLE activation: Starts any OLE-activated process in Confidential mode if the OLE object is embedded or linked in a confidential file.

4.4 Enhancement of User Interface

A drawback of conventional secure operating systems is that the operating system cannot be easily handled by users because its concept is considerably different from the concept of ordinary operating systems. InfoCage alleviates problems involved in an environment in which Confidential and Ordinary modes are mixed, by implementing the following functions. The operating system for InfoCage clients is Microsoft Windows 2000 Professional or XP Professional Edition.

4.4.1 Shell Support

InfoCage as implemented ensures seamless switching between Confidential and Ordinary modes for the client. It also enables users to use Confidential-mode applications without having to receive special training or perform a special operation.

When a typical user wants to work on a file, he accesses the desired file in Explorer, which is a standard Windows shell and then double-clicks the file to activate the edit application associated with the file.

This typical workflow does not need to be changed in an environment that includes an InfoCage implementation. If the target file exists on a secure server, a separate Confidential-mode application will be activated when the file is double-clicked in Explorer.

If an edit application is already active at this time, there exists a single-instance application that reuses the edit application to open the file. If editing of a confidential file is specified in Explorer when an Ordinary-mode process is already active, the Ordinary-mode process opens the confidential file and is permitted to move the contents of the confidential file to an ordinary file and to save the ordinary file. This could lead to information leakage. In contrast, InfoCage forces each process to run in either Confidential or Ordinary mode. Therefore, if an attempt is made to edit a file when a process is already active in a mode that is different from the mode intended for the file, the file will be opened in a state with access permission that is changed based on the behavior determined by the specification in **Table I**. Applicable single-instance applications include Microsoft Office products.

4.4.2 User Interface

When a Confidential-mode process attempts to write to an Ordinary file, a warning message needs to be displayed in order to inhibit this attempt. Such an attempt occurs when a malicious user performs such an action intentionally or when an application internally tries to write an Ordinary file in order to read configuration or other information. When a general GUI application is in use, the warning is displayed in a modal message box to ensure that the user is notified that his/her operation has failed. In this case, however, the warning is frequently displayed although the user does not perform improper operation. As the user needs to suspend operation in order to respond to the message usability is harmed. Nevertheless, if a user inadvertently attempts to move Confidential data, but is not warned by a message, he/she loses the opportunity of recognizing his/her improper operation. To overcome this difficulty, the InfoCage implementation uses the balloon method, which is a standard notification feature of the Windows operating system. It is modeless and supports time-out termination. If this method is in use, the user does not need to suspend operation when he/she receives an inappropriate warning, because the warning is modeless. If the user attempts to perform an improper operation, he/she can recognize the reason for the improperness by reading the message in the balloon within a certain length of time. **Table II** shows comparison of Warning Methods compares these two warning methods.

The InfoCage implementation inhibits Confidential-mode processes from operating on printers and e-mail in order to prevent information leakage via these routes. However, users do not always understand the behavior of Confidential-mode processes and are likely to be unaware of whether particular functions are available or not. Considering this, UI components (such as menus) that correspond to unavailable functions are grayed out to ensure that they cannot be selected by users. As a result, when a Confidential-mode process is active, menu items relating to a printer or e-mail are grayed out to ensure that users can understand that these functions are unavailable, before trying to use them.

It is also possible to visually recognize whether a user-activated application is running in Confidential or Ordinary mode. When it is running in Confidential mode, the caption for the process's main window includes a statement about running in Confidential mode.

5. POLICY MANAGEMENT

5.1 Policies

InfoCage allows rules to be specified to permit or inhibit operations for moving confidential files. A set of such rules is referred to as a policy. More specifically, it is possible to specify whether to permit or inhibit confidential data printing, screen capture, and

Table I Responses to single-instance applications.

Mode of already Open application	Mode of the file to be opened	Access permission assigned to the file to be opened
Confidential	Confidential	No change
Confidential	Ordinary	Write-protected
Ordinary	Confidential	Inaccessible
Ordinary	Ordinary	No change

Table II Comparison of warning methods.

Method	Mode	Termination
Message box	Modal	OK button pressing
Balloon	Modeless	Close button pressing or elapse of a certain time after the beginning of the display

data pasting for individual users and groups.

In InfoCage, the following three types of policies can be used. Combinations of these three types ensure various settings.

- Default policy (inhibition only)
- Group policy (permission, inhibition, or non-setting selectable)
- User policy (permission or non-setting selectable)

5.2 Policy Inheritance

Policies are inherited when group/user policies that have not expired and default policies are merged. When merged, user policies, group policies, and default policies are assigned priorities in that order. Merged policies will become policies when they are actually applied to a user. If no effective group/user policy exists for a user, the default policies should be the policies to be applied to the user.

For example, consider that a data user 'a' belonging to group A logs in within the period of validity of a group/user policy (**Fig. 2**-(A)). Since the user policy permits move operation, a user can move confidential files out. Regarding a print operation, the user policy specifies non-setting, whereas the group policy specifies permission. The user can print Confidential data because the group policy definition is inherited by the user policy. Regarding screen capture, the default policy is inherited because non-setting is specified in both the user and group policies. As a result, the user cannot capture screens.

If only the group policy is effective, a policy resulting from the merging of the group and default policies is applied (Fig. 2-(B)). If no effective policy exists, the default policy is applied (Fig. 2-(C)).

6. LOG MANAGEMENT

This section explains the logging requirements and the mechanism used to collect and manage user operation logs.

It is necessary, when information leakage occurs, to enable identification of the person who has leaked information. Logs of operations on client PCs is the key to identifying the information leaker.

InfoCage user operation logs are temporarily stored in a file on the local disk of the client PC and are uploaded to the management server. On the

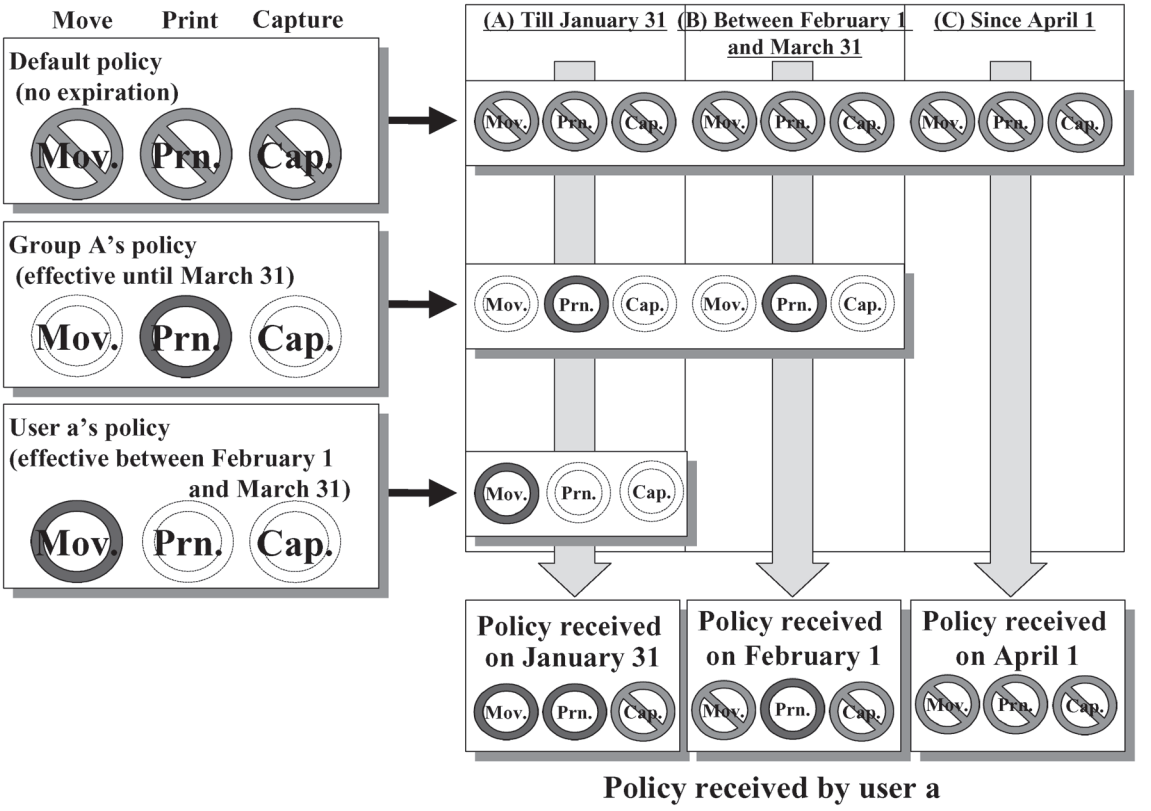

Fig. 2 Policy inheritance.

management server, operation logs collected from individual client PCs are temporarily stored on disk files and then managed on a database in a consistent manner.

The above InfoCage log collection and management mechanism is designed in consideration of the following three categories of logging requirements:

First, logs need to be reliable. Since logs are key information for identifying the information leaker, it is necessary to provide a mechanism that can prevent logs from being falsified by a malicious user. For this purpose, InfoCage calculates hash values when collecting user logs and verifies these values in order to detect falsification attempts. In addition, SSL communication used for log uploading helps to detect falsified logs.

Secondly, it is important to provide a mechanism that can prevent logs from being lost or intentionally deleted. To prevent logs from being lost, InfoCage only permits log deletion from a file when the file is successfully uploaded from the local disk or registered into the database. Therefore, even if the step of uploading or registration to the database ends abnormally, the logs are not lost. To prevent logs from being deleted, InfoCage locks log files to ensure that no agents other than InfoCage can write to log files.

Third, logs need to be maintainable. InfoCage manages the log database in a consistent manner to ensure that it is easy to detect illegal user operations and manage the logs.

In the way explained above, even when information leakage occurs, InfoCage can provide information that helps identify the source of the information leak, including the logs of operations performed by users who have handled the leaked data and the logs of users who had logged in by the time the leakage was discovered.

7. NEC'S INFORMATION LEAKAGE PROTECTION SOLUTIONS

Information leakage protection measures to be used by companies vary depending on the business style of the company. One product alone cannot completely protect the company from damage incurred by information leakage. When installing products, it is important to decide on operation policies, including which servers should contain confidential information and what rules should be used for management. It is also important to manage actual user operations in order to detect signs of risks, such as an attempt being made by a worker to move confidential information out. NEC provides a solution menu to satisfy a wide variety of company needs, from information resource management consulting to operation outsourcing. In addition to InfoCage for information move protection, NEC develops and commercializes various information leakage protection products that include enhanced file encryption and authentication features.

8. FUTURE DEVELOPMENT PLAN

NEC plans the following technical development and product enhancement in order to improve the maneuverability and usability of InfoCage:

· Policy definition expansion

The policy definition will be expanded to ensure that information move permissions can be defined more meticulously. Research and development efforts for GUIs that can be used by administrators more easily for definition are also planned.

· Log analysis function

When the number of clients increases, it is more difficult to understand the safety of overall confidential information handling. The log analysis function will be enhanced using statistical and other techniques to ensure that administrators can more easily understand the current status of information management within the organization.

· Enhanced linkage with business applications

In many cases, business confidential information is contained in business systems and handled and managed in specific document management software. Such business applications often use their own user management and document management features. Before InfoCage's control policies can be applied to individual users and documents contained in business applications, it is necessary that user and document information can be passed between InfoCage and the business application. NEC plans to provide InfoCage with APIs to enable such meticulous control.

9. CONCLUSION

The functions and technical components of the information leakage protection software InfoCage have been discussed. By installing InfoCage, companies can prevent even users who are authorized to access confidential information on a secure server from moving confidential information out of the server. In addition, InfoCage's protection functions are designed not

to influence move-out operation on information that is not confidential. To maintain both security and usability, we have developed an access control technology that works in a way that depends on the security mode and have implemented this technology in the product. We shall continue technical development efforts for product function enhancement in order to ensure that InfoCage can be used more easily and may thus enable a more meticulous policy control.

REFERENCES

[1] D. E. Bell and L. J. LaPadula, "Secure computer systems: Unified Exposition and Multics Interpretation," Technical report MTR-2997, MITRE, 1976.

[2] Sun Microsystems, Trusted Solaris Operating System, http://wwws.sun.com/software/solaris/trustedsolaris

Received December 2, 2004

* * * * * * * * * * * * * * * * *

Masaru KAWAKITA received his M.E. degree in Information Systems Engineering from Osaka University in 2004. He joined NEC Corporation in 2004, and is now Researcher of the System Platform Software Development Division. He is engaged in the research and development of system security solutions.

Kazuo YANOO received his M.E. degree in information engineering from the University of Tokyo in 1994. He joined NEC Corporation in 1994, and is now Assistant Manager of Internet Systems Research Laboratories. He is engaged in the research on information security.

Masahiro HOSOKAWA received his M.E. degree from the Tokyo Institute of Technology in 1988. He joined NEC Corporation in 1988, and is now Manager of the System Platform Software Development Division. He is engaged in the research and development of system security solutions.

Hiroshi TERASAKI received his M.S. degrees in information engineering from Ibaraki University in 1998. He jointed NEC Corporation in 1998, and is now an Assistant Manager of the System Platform Software Development Division. He is engaged in the research on information security.

Satoshi AOKI received his B.Sc. and M.Sc. degrees from Waseda University, Tokyo, Japan, in 2001 and 2003, respectively. He then joined the System Platform Software Development Division, NEC Corporation. He is a member of the IEICE in Japan. His current research interests include cryptography and information security.

Toshimitsu USUBA received his M.E. degree in Electrical and Electronic Engineering from Utsunomiya University in 2004. He joined NEC Corporation in 2004 and is now Developer of the System Platform Software Development Division. He is engaged in the research and development of system security solutions.

* * * * * * * * * * * * * * * * *