A Visualization System for Analyzing Information Leakage

Yuki Nakayama, Seiji Shibaguchi, Kenichi Okada

Chapter 19

A VISUALIZATION SYSTEM FOR ANALYZING INFORMATION LEAKAGE

Yuki Nakayama, Seiji Shibaguchi and Kenichi Okada

Abstract Information leakage is a growing public concern. This paper describes a visualization system for tracing leaks involving confidential information. In particular, the system enables administrators to determine which hosts have confidential documents and the means by which confidential information is transmitted, received and duplicated. The visualization system is scalable to large organizations and can track various means of information propagation in a seamless manner. Also, it helps prevent information leaks, analyze transmission routes and present forensic evidence.

Keywords: Information leakage, visualization, data tracing

1. Introduction

Information leakage has become a serious problem. A recent survey of more than 800 CIOs reported that organizations lost an average of $4.6 million due to the leakage of intellectual property [7]. It is imperative to protect intellectual property and sensitive information by devising countermeasures against information leakage.

Countermeasures against information leakage can be broadly classified as before-the-fact or after-the-fact measures. Before-the-fact countermeasures aim to prevent leakage (e.g., prohibiting the use of USB drives, printing confidential documents or sending confidential data by email). After-the-fact measures involve incident response and digital forensic investigations [12]. Digital forensics is the use of scientifically derived and proven technical methods and tools for the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence for the purpose of facilitating or furthering the reconstruction of events [13].

Research conducted in Japan [3, 9] indicates that information leakage by insiders is about 1% of the total and that human error, such as employees losing their laptop computers, is the main cause of information leakage. Similar results have been observed in the United States [2], where human error contributes to as much as 35.2% of the information leakage that occurs in the private sector. Consequently, it is important to focus on preventing leakage due to human error.

Our visualization system contributes to both before-the-fact and after-the-fact countermeasures. Specifically, it traces the pathways of confidential information and supports the visualization of the routes. It allows administrators to know which users have confidential documents, enabling them to remove the documents or to prohibit the users from using laptops outside the enterprise. Therefore, leakage due to human error, such as the loss of a laptop, can be prevented. Furthermore, the system contributes to digital forensic investigations by enabling administrators to rapidly analyze the cause of a leakage and presenting forensic evidence using an intuitive interface.

2. Related Work

This section discusses some of the existing tools for combating information leakage and highlights their deficiencies.

Vontu Data Loss Prevention [11] provides proactive countermeasures against information leakage. Also, it implements systematic security controls such as restricting the use of USB drives. However, these controls hinder routine work and lower productivity. Also, they can only prevent information leakage that occurs in a predictable manner. On the other hand, humans can analyze problems from various perspectives and make systematic judgments about the risk of leakage at any given time. Our visualization system assists humans in understanding rapidly changing situations that may involve information leakage.

SKYSEA Client View [10] and InfoCage [4, 5, 8] support after-the-fact countermeasures. These tools monitor the operation of hosts and write the results into text-based log files. They also analyze the log files to ascertain the cause of information leakage. However, they do not attempt to streamline analytic work or simplify evidence for presentation in court. Consequently, administrators must devote considerable amount of time and effort to analyzing large amounts of log data. Eliminating this step is important to simplifying analytic work. Our visualization system facilitates the presentation of evidence related to information leakage in a clear, concise and simple manner.

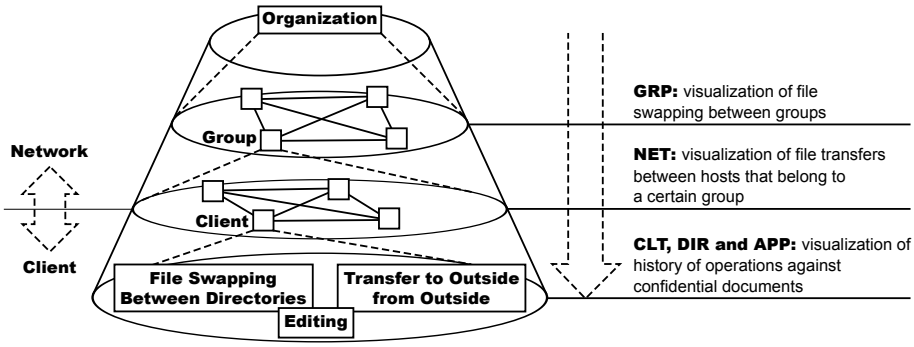


Figure 1. Scalable and seamless visualization.

3. Visualization System

Our visualization system monitors the transmission of confidential information via pathways such as email, removable media and applications. It enables administrators to identify the locations of confidential documents. If necessary, they can then implement security measures such as ordering employees to remove the sensitive documents or prohibiting the removal of specific computers from the enterprise.

The visualization system also contributes to the rapid analysis and clear presentation of forensic evidence in the event of an information leakage. Moreover, damage to the organization is minimized due to the rapid response.

Two key requirements related to visualizing information transmission pathways are:

- **Scalable Visualization:** A visualization system must be flexible with regard to changes in the number of hosts and the number of confidential documents that appear on the watch list.
- **Seamless Visualization:** Information can be propagated by various means – file swapping via email or peer-to-peer networks, transporting data on portable devices such as USB flash drives, moving or copying files to a computer, and editing or duplicating files using applications. A visualization system should achieve broad coverage of these diverse means of data transmission and integrate the means seamlessly.

Our system addresses these requirements using five different visualization methods (Figure 1). The five methods are group-based (GRP), network-based (NET), client-based (CLT), directory-based (DIR) and application-based (APP) methods. GRP and NET observe file swap-

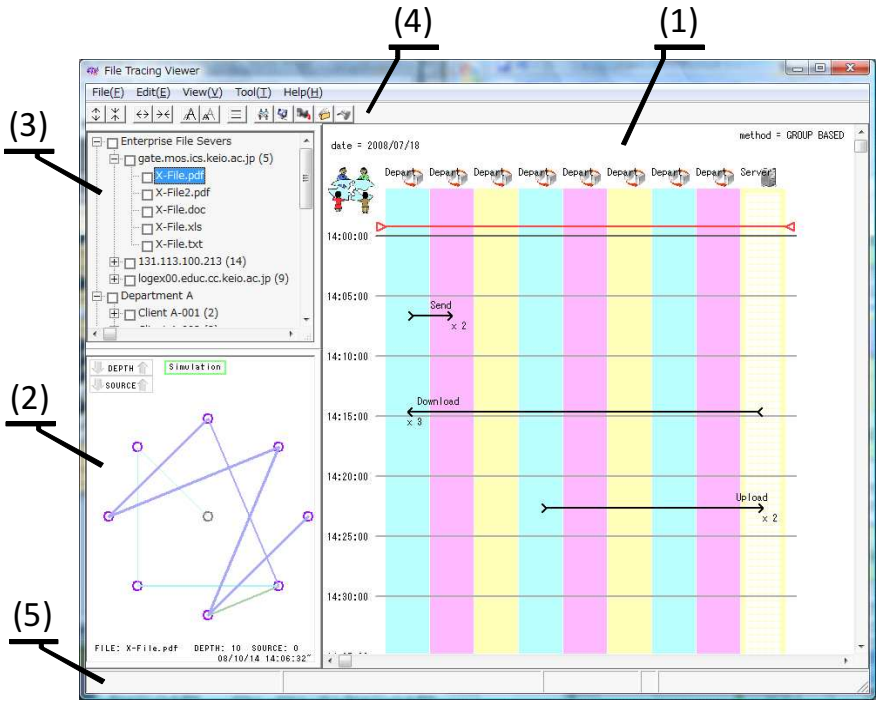


Figure 2. CROWS Up Viewer.

ping through networks. CLT, DIR and APP monitor computer use by employees. GRP visualizes file swapping between groups comprising a given number of hosts. NET displays file transfers between hosts that belong to targeted groups. CLT monitors confidential documents received and dispatched by a particular client. DIR shows the transfer of confidential documents between the directories of a single client. APP monitors applications when a user has confidential documents open.

4. CROWS Up Viewer

We have implemented a prototype called the "CROWS Up Viewer" (CROWS: Catch Reveal by Observing and WitneSsing), which meets the design goals described in Section 3. The system is implemented in C++ and runs under Windows XP/Vista.

Figure 2 shows the CROWS Up Viewer. The main panel (marked (1)) presents the primary interface for each of the five visualization methods. The sub-panel (2) shows the sub-methods that assist with analytic work. The tree view (3) shows the documents possessed by each host. The

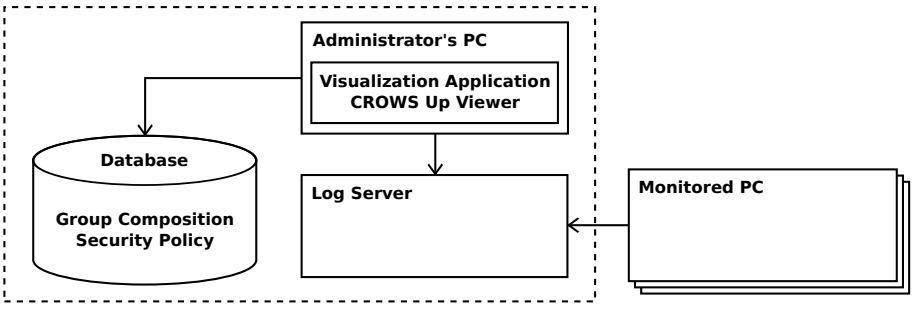


Figure 3. System architecture.

toolbar (4) provides buttons for user interaction and enables users to customize the CROWS Up Viewer interface. The status bar (5) shows details regarding the position of the on-screen cursor.

4.1 System Architecture

Figure 3 shows the visualization system architecture. A monitoring program is required to be installed on client computers in advance. This program is linked to a database, which stores a definition file for each client machine and records data. The monitoring program refers to the definition file for each client and writes results to log files, which are transmitted to a management server. Administrators use the visualization system to view the collected data.

The monitoring program uses API hooking to reveal the internal operations of the computer. This approach has been used in intrusion prevention [1], dynamic malware analysis [14] and unknown virus detection [6].

4.2 Visualization Methods

This section describes each of the five visualization methods used in our system.

GRP The group-based method (GRP) visualizes file swapping between groups comprising a given number of hosts. The top-left corner of Figure 4 shows an example of GRP visualization. The box-shaped areas represent groups and servers, and the arrows between the areas indicate file swapping; the other arrows represent file swapping in unsafe networks. Note that the time axis is set in vertical direction. For example, Figure 4 shows that Group A has sent two files to Group C at 14:07. Although details such as filenames are not visible in the figure,

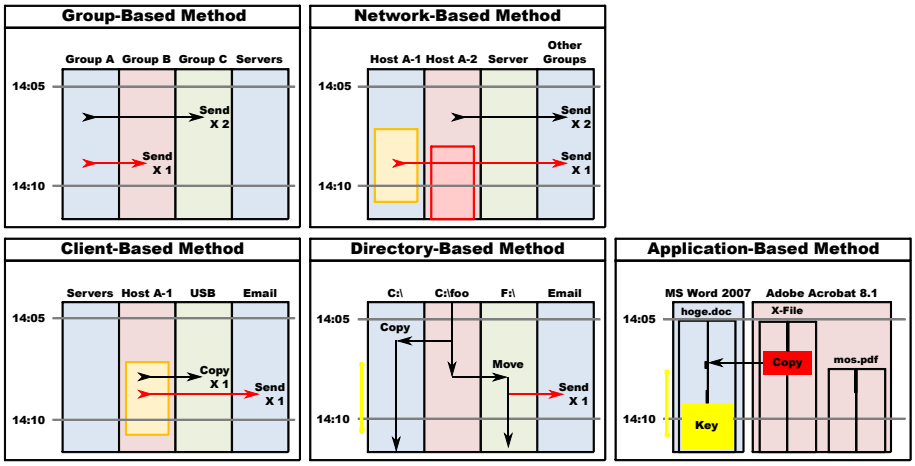


Figure 4. Visualization methods.

they can be made to appear in the toolbar by hovering the cursor or in a dialog box by clicking the mouse.

GRP provides a simulation monitor (SimMon) and a tracing monitor (TrcMon) for supporting analytical work (Figures 5 and 6). Each group is represented as a node in these monitors. The center node indicates the server group while the peripheral nodes denote client computer groups. In SimMon, the lines between the nodes represent file swapping and various colors are used to indicate operations such as file downloads, uploads and transfers (Figure 5). SimMon changes its display continually and enables administrators to run simulations that show file swapping in a dynamic workplace environment.

TrcMon shows the transmission routes of a single confidential document. The weights of the lines connecting the nodes represent the passage of time; thinner lines represent older transmissions and thicker lines represent newer transmissions. Various colors are used to highlight the branches of a document pathway. Figure 6 shows a document that has been transmitted from a server to a Group 1 user and then from Group 1 to Group 3, from Group 3 to Group 5, and eventually from Group 5 to two separate groups. It is possible to interact with TrcMon to change the time when a trace is started or to adjust its depth.

Note that GRP monitors FTP downloads and uploads, the sending of email and whether or not hosts connect to unsafe networks.

NET The network-based method (NET) displays file transfers between hosts that belong to a specified group. In Figure 4, the areas on the left represent clients, servers and other groups. The arrows between

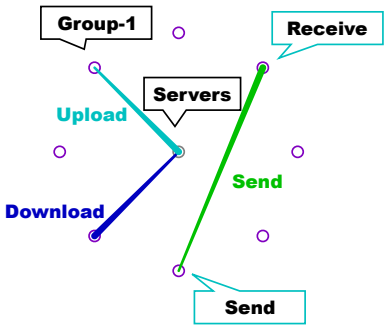


Figure 5. SimMon (GRP).

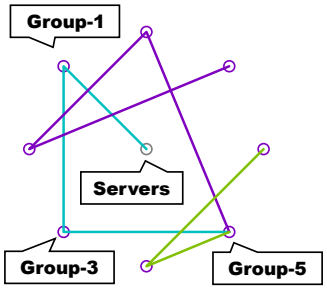


Figure 6. TrcMon (GRP).

these areas represent file swapping. Colored diagonal line areas in NET alert administrators to the status of particular clients. Hosts that are experiencing security problems (e.g., hosts that are not using antivirus software or a firewall) are shown in red. Clients that are connected to unsecured networks are shown in yellow.

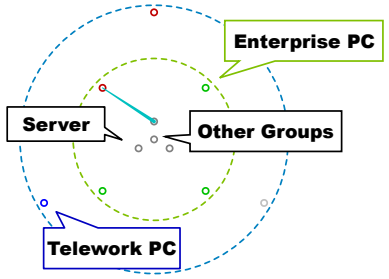


Figure 7. SimMon (NET).

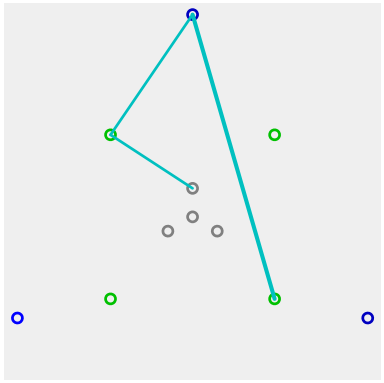


Figure 8. TrcMon (NET).

NET also provides SimMon and TrcMon (Figures 7 and 8). The node in the center represents other groups and the circularly arranged nodes represent servers and enterprise/remote clients. Nodes of various colors represent online enterprise computers (green), online remote computers (blue), offline hosts (grey) and hosts having security problems or hosts connected to unsafe networks (red).

NET monitors the downloading and uploading of files and the sending of email. Also, it monitors hosts that connect to unsafe networks or experience security problems.

CLT The client-based method (CLT) monitors confidential documents received and dispatched by a targeted client. The bottom-left corner of Figure 4 shows an example of CLT. The rectangular areas, starting from the left, represent the file servers in an enterprise, clients, removable media and email. The figure shows an example where Host A-1 has copied a confidential document to a USB flash drive at 14:08.

CLT monitors FTP downloads and uploads to enterprise servers, the sending of email, copying to or from removable media, writing to magnetic media, printing of documents and the number of confidential documents on a host.

DIR The directory-based method (DIR) shows the transfer of confidential documents between the directories of a single client. Figure 4 shows an example of DIR, where a confidential document was copied from `C:\foo\` to `C:\` at 14:06.

DIR monitors the copy, move, remove/recover, open/close, save as, print, upload, send, compress/decompress, convert and split/combine operations with respect to confidential files.

APP The application-based method (APP) monitors all applications when a user has confidential documents open. Figure 4 shows an example of its operation. Each application is drawn as an area on the display in which APP displays the confidential documents opened by the application. The heavy lines represent active windows. In the example, the user has copied text data from `X-File` to `hoge.doc` at 14:07.

APP also provides DspMon (display monitor) as shown in Figure 9. DspMon duplicates a computer screen at a given time and provides an intuitive representation. A framed rectangle denotes an active window and underlined filenames indicate that the files are confidential.

APP monitors the copying/pasting of text and bitmap data; the position/size of application windows; the z-index of windows; keystrokes; the opening/closing of documents; and save/save as and print commands.

4.3 Analytic Workflow

This section describes an example analytic workflow conducted using the CROWS Up Viewer. In the example, we assume that an administrator has learned that a file has been leaked and attempts to analyze the cause of the leakage.

First, the administrator examines the tree view in the upper left portion of the CROWS Up Viewer and selects the file to be traced. At this point, the CROWS Up Viewer removes all the other files from view.

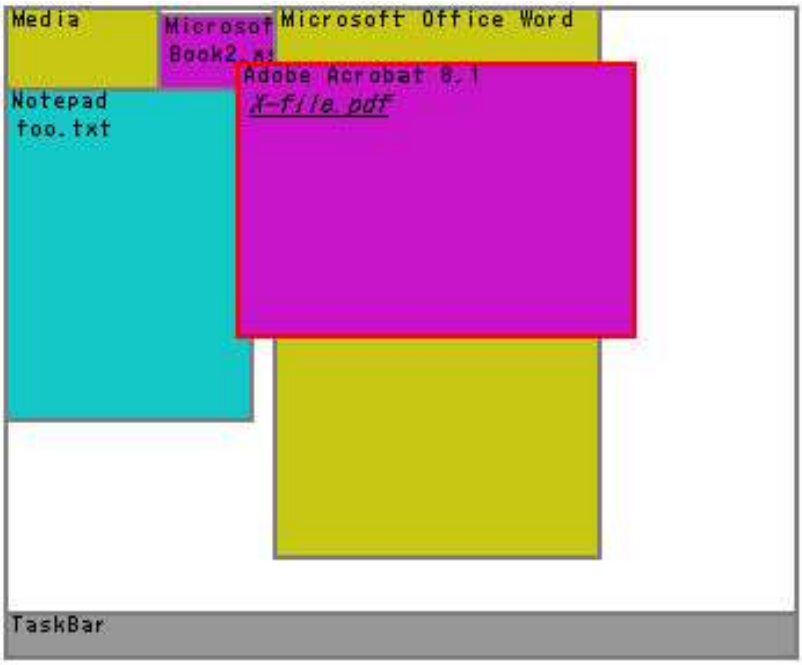


Figure 9. DspMon.

The administrator then employs the five visualization methods in sequence (Figure 10). First, the groups that received the file are analyzed using GRP, after which, the administrator applies NET to the groups to identify the hosts that received the leaked file. It is important to note that the groups that transfer a file via an unsafe network receive a higher priority. Using NET, the administrator first observes the colored diagonal areas that identify clients with security problems (red) and clients connected to unsafe networks (yellow). Thus, the administrator can check if viruses, worms or other malicious software caused the leakage or if the file was stolen by data sniffing.

Next, the administrator uses CLT, DIR and APP to investigate the hosts flagged by NET. CLT provides information about incoming and outgoing transfers of the file; DIR provides information about the use of the file; APP shows the operations that the user performed using various applications.

The CROWS Up Viewer enables the administrator to analyze the situation intuitively even if the events are complex. As a result, the cause of the file leakage can be determined promptly and appropriate mitigation actions can be taken.

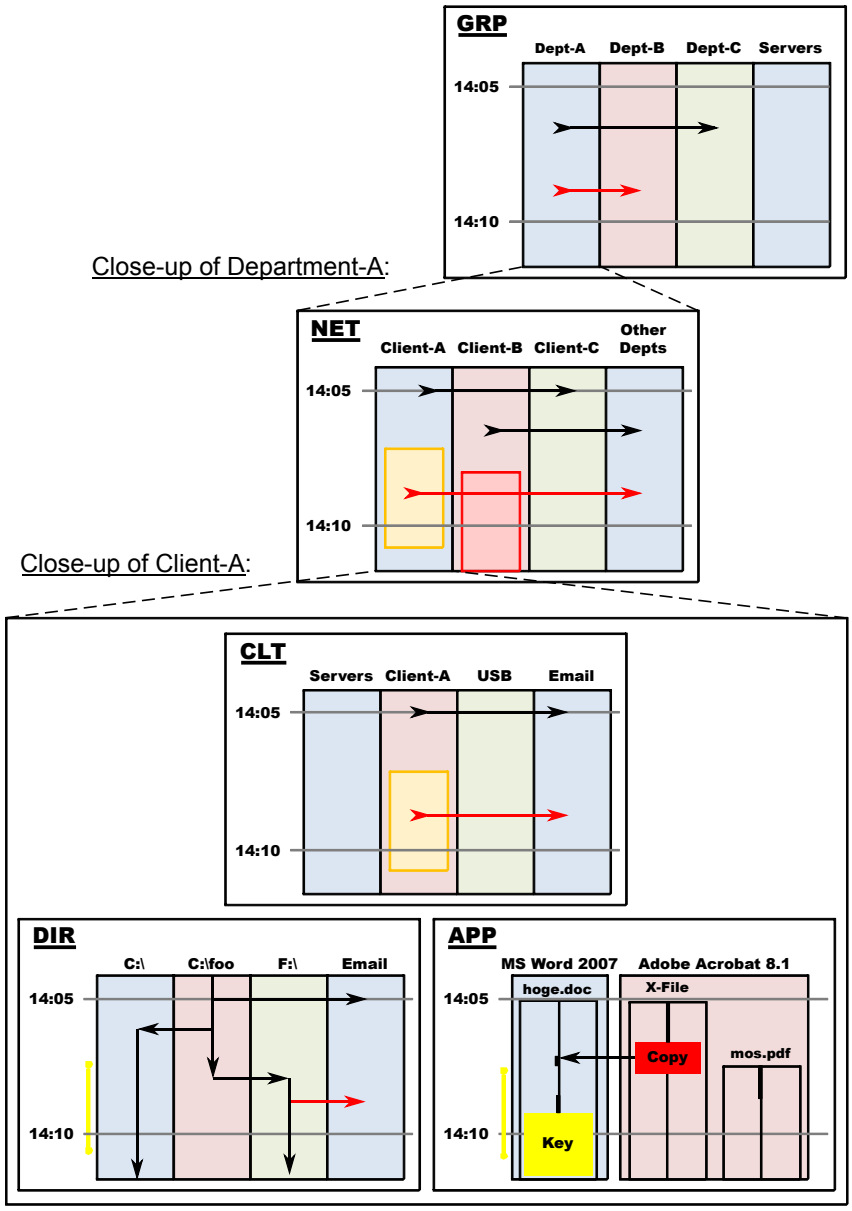


Figure 10. Analytic workflow.

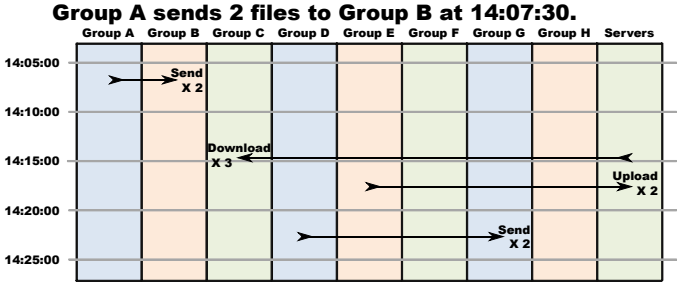
5. Experimental Results

We conducted an experiment to verify the usability of the visualization system. The subjects of the experiment were twenty university students who were pursuing degrees in information engineering. The

File-swappings between groups

Time	Operation	Source	Destination	# Files
14:07:30	Send	Group A	Group B	2
14:15:23	Download	Server	Group C	3
14:18:56	Upload	Group E	Server	2
14:07:30	Send	Group D	Group G	2

Question:
Group A sends 2 files to Group B at 14:07:30.



Question:
Group E uploaded 2 files to a server at 14:18.

Figure 11. Sample evaluation questions.

subjects performed simple analytic tasks using text logs and visualized logs, and answered 26 true/false questions about the tasks – thirteen questions regarding the text logs and thirteen regarding the visualized logs (Figure 11). We evaluated three characteristics of the visualization system: (i) accuracy; (ii) speed; and (iii) ease of understanding based on the percentage of correct answers to the survey questions and the time required to answer the questions.

The subjects were divided into two groups to address the possibility that they might become accustomed to the analytic work, which could affect the comparison between the text log and visualized log results. Subjects in Group 1 analyzed the text logs first, followed by the visualized logs. Subjects in Group 2 answered questions about the visualized logs first, followed by questions about the text logs. Each group comprised ten subjects.

Table 1 shows the results of the experiment. P_{txt} is the percentage of correct answers for the text logs; P_{viz} is the percentage of correct answers for the visualized logs; FS is fractional reduction in the time required $((T_{txt} - T_{viz})/T_{txt})$, where T_{txt} is the time required for analyzing the text logs and T_{viz} is the time required for analyzing the visualized logs.

An F-test and a t-test were conducted between: (i) P_{txt} of Group 1 and P_{txt} of Group 2; (ii) P_{viz} of Group 1 and P_{viz} of Group 2; and

Table 1. Experimental results.

Group 1			Group 2		
P_{txt}	P_{viz}	FS	P_{txt}	P_{viz}	FS
0.92	1.00	+0.43	0.92	1.00	+0.60
0.85	1.00	+0.37	0.77	1.00	+0.25
0.62	1.00	+0.16	0.92	1.00	+0.20
1.00	1.00	+0.45	0.92	0.92	+0.26
0.85	0.92	+0.62	0.92	1.00	+0.34
0.85	1.00	+0.20	1.00	1.00	+0.40
0.85	1.00	+0.17	1.00	1.00	+0.31
0.62	0.92	+0.33	0.85	0.92	+0.39
1.00	1.00	+0.30	1.00	1.00	+0.32
0.92	1.00	+0.19	0.92	1.00	+0.28

(iii) FS of Group 1 and FS of Group 2. No significant differences were observed for a significance level of 5%. Thus, we can conclude that no significant difference exists between Group 1 and Group 2, i.e., the tests can be regarded as having been conducted under the same conditions.

The means and standard deviations (upon combining Groups 1 and 2) are:

$$P_{txt} = 88 \pm 11\% \quad P_{viz} = 98 \pm 3\% \quad FS = +34 \pm 13\%$$

The percentage of correct answers related to the visualized logs were higher than those for the text logs, and no significant difference exists at a level of 1% ($p < .01$). The fractional reduction in the time required indicates that the visualized logs facilitate rapid analysis. Therefore, the visualization system supports accurate and rapid analysis.

After the experiment, we also polled the test subjects about the ease of understanding of the visualized logs versus the text logs. All the subjects felt that the visualized logs were easier to understand than the text logs.

6. Conclusions

Information leakage is a serious problem and it is imperative that organizations employ effective countermeasures to protect confidential information. Our visualization system efficiently traces the flow of confidential information and helps identify potential information leaks, enabling administrators to assess the risk and implement mitigation strategies. The system also supports forensic investigations of information leaks and assists with the collection and presentation of evidence. Experi-

mental results indicate that the visualization system supports human understanding and facilitates the rapid and accurate analysis of information leaks.

References

[1] R. Battistoni, E. Gabrielli and L. Mancini, A host intrusion prevention system for Windows operating systems, *Proceedings of the Ninth European Symposium on Research on Computer Security*, pp. 352–368, 2004.

[2] Identity Theft Resource Center, 2008 data breach totals soar, Press Release, San Diego, California (www.idtheftcenter.org/artman2/publish/m_press/2008_Data_Breach_Totals_Soar.shtml), 2009.

[3] Information-Technology Promotion Agency, Countermeasures Against Information Leakage: Seven Rules for People Working in Business Enterprises, Tokyo, Japan (www.ipa.go.jp/security/english/virus/antivirus/pdf/Leakage_measures_eng.pdf), 2006.

[4] M. Kawakita, K. Yanoo, M. Hosokawa, H. Terasaki, S. Aoki and T. Usuba, InfoCage – Information leakage protection software, *NEC Journal of Advanced Technology*, vol. 2(1), pp. 40–46, 2005.

[5] K. Kida, H. Sakamoto, H. Shimazu and H. Terumi, InfoCage: A development and evaluation of confidential file lifetime monitoring technology by analyzing events from file systems and GUIs, *Proceedings of the Second International Workshop on Security*, pp. 246–261, 2007.

[6] R. Koike, N. Nakaya and Y. Koui, Development of a USB flash memory for detecting computer viruses, *Information Processing Society of Japan Journal*, vol. 48(4), pp. 1595–1605, 2007.

[7] McAfee, Unsecured Economies: Protecting Vital Information, Santa Clara, California, 2009.

[8] NEC Corporation, No. 1 market share for domestic quarantine tools for three consecutive years, Press Release, Tokyo, Japan (www.nec.co.jp/press/ja/0808/2701.html), 2008.

[9] Security Incident Investigation Working Group, Survey Report of Information Security Incidents 2007, Version 1.0, NPO Japan Network Security Association, Tokyo, Japan (www.jnsa.org/result/2007/pol/incident/2007incidentsurvey_e_v1.0.pdf), 2008.

[10] Sky Corporation, SKYSEA Client View, Osaka, Japan (www.skyseaclientview.net).

[11] Symantec Corporation, Data loss prevention: Products and services, Mountain View, California (www.symantec.com/business/theme.jsp?themeid=vontu).

[12] S. Tsujii and E. Hagiwara (Eds.), *Encyclopedia of Digital Forensics*, Nikkagiren Press, Tokyo, Japan, 2008.

[13] S. Willassen and S. Mjolsnes, Digital forensics research, *Telektronikk*, vol. 2005(1), pp. 92–97, 2005.

[14] C. Willems, T. Holz and F. Freiling, Toward automated dynamic malware analysis using CWSandbox, *IEEE Security and Privacy*, vol. 5(2), pp. 32–39, 2007.