The Design of Framework for Detecting an Insider's Leak of Confidential Information

Eunju Baek
Graduate School of Information Management & Security
Korea Univ., Anam-dong, Seongbuk-gu, Seoul
+82-2-3290-4738
ej0083@korea.ac.kr

Yeog Kim
Graduate School of Information Management & Security
Korea Univ., Anam-dong, Seongbuk-gu, Seoul
+82-2-3290-4276
yeog@cist.korea.ac.kr

Jinwon Sung
Graduate School of Information Management & Security
Korea Univ., Anam-dong, Seongbuk-gu, Seoul
+82-2-3290-4738
jinwonsung@korea.ac.kr

Sangjin Lee
Graduate School of Information Management & Security
Korea Univ., Anam-dong, Seongbuk-gu, Seoul
+82-2-3290-4893
sangjin@korea.ac.kr

ABSTRACT
The confidential information such as the technical know-how or the business information of an enterprise is very important because it may make the enterprise do the business or not. The enterprise, therefore, are in control of its confidential or critical information with the support of a lot of time and fund. In spite of their effort, 87% of the leak of confidential information is due to insiders[1]. The cause of the leak of confidential information is the negligent or weak control of employee's E-mail, instant message, P2P and so on. It also comes that insiders leak some information maliciously for the purpose of economical profit or are industrial spy. The frequency of those is increasing more and more[2]. The insiders are very skilled in the equipments or systems of the organization which they belong to and can delete immediately their traces after their improper activities. Therefore, it needs the acquisition of data in conformity with the leak type of confidential information for finding out the evidence.
We propose a framework to detect and prevent the leak of confidential information according to the leak type with the forensic sight. And the framework has also the function of the first response and the gathering evidence.

Categories and Subject Descriptors
D.2[Software Engineering], D.2.0[General], D.2.10[Design], K.6.5[Security and Protection]

General Terms
Security

Keywords
Insiders, Leak of information, Digital forensics

E-FORENSICS 2008, January 21-23, Adelaide, Australia

DOI 10.4108/e-forensics.2008.2658

1. Introduction

1.1 Motivation

The confidential information of the enterprise decides the competitive power of the enterprise. Therefore, the confidential information which has a free hand a life and death of the enterprise is dealt very importantly. According to the result of the research about leak of confidential information from 2003 to Oct., 2006, at NISC(National Industrial Security Center), 87% of leak of confidential information is due to an insider[1]. The insider is the person who has an authority in specific information[3]. The frequency of leak of confidential information is increasing because of careless use of E-mail, messenger and P2P by employees and leak by industrial spy or improper activities of employees for economic reasons. These leaks of confidential information suffer a great economical loss. According to NIS research from Jan to June, 2007, the damage from leak of confidential information is nearly 40 billion dollars[1]. Although the enterprise prepares the correspondence against leak of confidential information by the insider for the survival by itself, it is not enough to prevent the leak because techniques have become highly wrought. Therefore, we propose a framework which can detect and prevent the leak of confidential information. The proposed framework observes and detects the leak of information according to the leak of information type from target PC. And it extracts the evidence in the investigation required, so it can detect the leak of confidential information from a digital forensic point of view. Base on acquired evidence, the enterprise can audit by itself or produces the evidence to submit to the forensic organization. In this paper, we propose a framework which detects and observes the trial of the leak and provides proper first correspondence procedure.

1.2 Legal Issues

Our proposed framework is debatable about infringement of privacy. The proposed framework carries out the monitoring. In a lot of enterprises, for the security, they take a monitoring their employee's work. But this activity conflicts with employee's constitutional right, this is, privacy. Because in the position of management, an important thing is property rights, while in the position of employee, they want privacy in their work place.

American case, base on Sarbanes-Oxsley Act[4], the management gave the rights that they can monitor their employee's work against improper act through E-mail or messenger. Base on Sarbanes-Oxsley Act, the enterprise contrives a basis which can evade their responsibility from monitoring employees. And British case, through 'Regulation of Investigatory Powers Act 2000', E-mail monitoring is illegal without agreement of both side of communication[5]. In the same manner, in Japan, it permits specific method of acquisition about monitoring as provided by law. On the basis of some countries act, the proposed framework can escape the problem with privacy if there exist agreement of monitoring and the management gives the accurate information to employees.

2. Related Work

2.1 Leak of Information by an Insider

Almost information systems have the threat such as viruses, worms, hacking or improper act by the employees. In case of outsourcing, especially leak of information by an insider increases a possibility that outsourcing people can access the information or internal system. Therefore, it is required method of management about threat from the authorized insider[6]. Therefore, it is required the study about use of computer system information in the internal enterprise and system intrusion from internal. And also it is required the study about profiling of the insider for understand their character and related procedure which is required to the investigator in the investigation of intrusion of insider[7].

2.2 Forensic Network

For the analysis and store of real evidence into detect framework, it is required construction of forensic network. Forensic network is composed of high performance server and target PC. In other words, it is like 'server-client' structure. It means real server can acquire the evidence from target PC remotely. In forensic network, the client system is the target of imaging, while the server stores the imaging files. Therefore, if forensic network structure establishes, during the investigation, the server connects the client remotely and can conduct the acquisition of evidence such as imaging. It is required the system that the enterprise don't stop its business during the investigation. Another good point is that it doesn't need physical access to acquire the evidence to target PC[8].

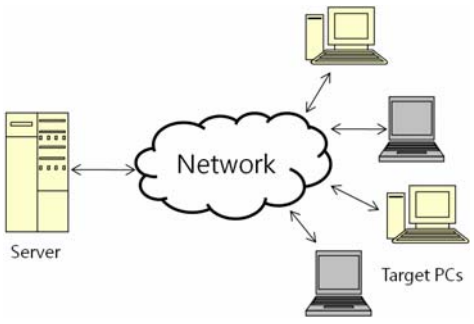

Figure 1. Forensic Network

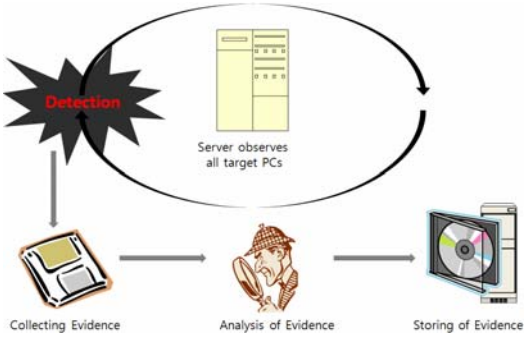

Figure 2. Operation of Framework

2.3 Method of Detection According to Leak Type

In leak of confidential information, the keeping a factor in mind is that the insider maybe can deal with systems or any equipments because they already understand internal system in the enterprise. Then, the most dangerous thing is that if the insider deletes the traces of leak, the management can't be aware who did commit a crime. Therefore, it is required the acquisition according to leak type and the detection of trial of leak is very important.

2.4 Design of Detection Framework

Our proposed detection framework is designed for the prevention of leak of confidential information by improper activities from the insider. Our framework's works are an observation, detection, extraction of evidence and store the evidence. It is shown a state of framework's operation in Figure 2. The server always observes a trial of leak of confidential information. As soon as the leak is detected, the server acquires the evidence from the target PC quickly. The acquired evidence will be analyzed and will be stored in the server.

There are two type of the detect frameworks. First, that is "Simple Server-Client". Owing to simple structure, it is comparatively easy in the implementation. But a weak point is that it is occurred the overload on center server. In Figure 3, it is shown an operation of simple server-client when the trial of leak is detected. The second structure is "Server-Agent-Client". This is being lost the overload of server, while it requires a lot of the cost of maintenance and it is complex in the implementation. It is shown the operation of detection of leak in server-agent-client in Figure 4. It is required proper selection according to range of detection.

Table 1. Compare between Framework

	Server-Client	**Server-Agent-Client**
Scale	Comparatively small	Comparatively large
Operation	Comparatively easy	Complex
Weak point	Overload of server	Expensive cost
Object	Small-scale enterprise	Large-scale enterprise

Figure 3. Operation of Detection in Simple Server-Client

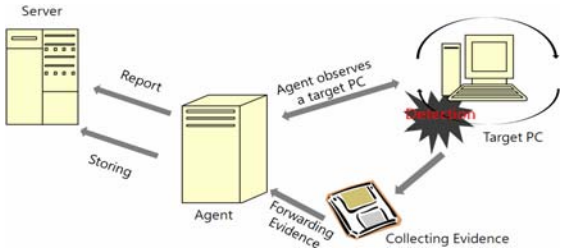

Figure 4. Operation of Detection in Server-Agent-Client

2.4.1 Simple Server Client

Simple Server-Client structure is a form that the client connects the server directly. The center server observes periodically each target client which connects it directly. Above mentioned, because simple server-client structure has simple form, the management is easy, while it is occurred overload of the server. So it is suited to operate in a small-scale enterprise or an enterprise which doesn't need work with many computers.

2.4.2 Server-Agent-Client

There is an agent whose affair is decentralization of the server's work between the center server and clients. The agent manages the PCs such as each department of the enterprise or each floor in the enterprise. And it reports the condition of target PCs to the center server. This operation has a difficulty in management, so it is suited to operate in a large enterprise. Each agent is placed on each department or floor and it manages target PCs.

3. Necessary Information in Detection According to Method of Leak

3.1 Necessary Techniques to Extract Information

3.1.1 Analysis of Windows Registry

Windows registry is the system database that contains the information required to boot and configure the system, systemwide software settings that control the operation of Windows, the security database, and per-user configuration settings [9]. Registry includes a lot of settings which cause an effect in the performance and operation. So it is very useful to gain information about Windows internals.

If the insider tries to leak the confidential information through removable storage media, the unique information of removable storage media remains in an attached system [10]. Therefore, the information can judge the trial of leak after the inspection of specific registry keys.

Nowadays, a study on analysis of Windows registry is progressing with activity. In this paper, it is required some of registry information, so it is better access the specific registry keys directly than using other forensic tools.

3.1.2 Analysis of Messenger

A messenger was developed for communication with other people. The messenger supports not only communication like E-mail but also real-time communication and transmission with the other party. For this convenience, a lot of people use the messenger.

Monitoring network packet is used for detection of the leak of confidential information through the messenger. In case of a large-scale enterprise, this method needs a lot of money and human strength. So after the crime occurs, it can be used the evidence by acquisition of information about IDs/Passwords, saved chat logs and received files, etc.

3.1.3 Analysis of E-mail

Usually people access to their E-mail in two ways: through application or using web-mail. In case of use of web-mail, because it is not easy to recovery of contents, using the forensic tool is better to analyze web-mail information. In case of using E-mail application, it is acquired information such as transmission information, location of automatic save, identification information and address book, etc.

3.1.4 Analysis Policy of the Enterprise

There is a method that detects the leak depend on the enterprise's policy. If it specify the policy restriction of access to the system after closing office, the unnecessary access which occurs after closing office is possible to guess the leak of confidential information. If the person who doesn't have the authority to access tries to access the specific information, it can be a basis of leak.

3.2 Detection Depend on Leak Type

3.2.1 Through the Removable Storage Media

A small size storage media has become public according to development of techniques. It is used for leak of confidential information more and more. The use of removable storage media leaves the traces on Windows registry. So it can be confirm that which kind of removable storage media attaches on target PC. Windows registry is a database stores the system properties information. It is used all Windows OS series [11]. Therefore, through the removable storage media's unique ID, leak of confidential information can be detected after check the Windows registry. It is possible to confirm whether the storage media whose suspect use target PC or not. This information is very important to grasp an unauthentic access of media.

3.2.2 Through Communication Media

The type of the leak via network can be a use of instant message of messenger, E-mail and P2P.

• Detection Use of Messenger

Almost of the enterprise, the observation of E-mail is doing while, the observation of messenger neglects due to the limitation like expense. Therefore, it is vulnerable about leak through messenger yet. When the leak through messenger occurs, the information which will have to acquire is user ID, saved chat logs, downloaded files and cookie files, etc. Messenger information provides the information which can confirm kind of messenger and transmitted files the other party. Also it uses option of "save chat record", through this information, it can be confirmed the fact of unwholesome transmission, conspiracy of crime, the fact of leak of critical data.

•Detection Use of E-mail

Almost of the enterprises use the system for observing employee's E-mail. So it is not easy to leak through this method by the insider. But if the insider uses changing the subject or contents, attached file, there is enough for leak. The information about E-mail provides the information which can confirm the transmission of E-mail to other party. Not web-mail, E-mail application stores transmitted files or E-mails, so if the insider tries to leak confidential information, information related E-mail have to be acquired then it can prepare the evidence for leak.

•Detection Use of P2P

P2P is the form or application which let transmit the data with any person who connects the server or each other. All PCs which use this application for downloading and sharing files are connected each other. Lately, user of P2P is increasing steadily. The leak of confidential information is different from intentional leak. In Japan, recently, one of police man was fired because of sharing critical information via P2P. He installed P2P application on his office's computer. But he didn't know his confidential folder set up share folder. When he was aware this fact, confidential files already spread. In case of P2P, whether it is intentional or not, it can be used for leak of confidential information. So it needs special care. To look into leak of confidential information via P2P is that it is necessary to check Windows registry keys or check default install path. And find the files which store the information about download files, temporary download files or deleted files. Then analyze them.

4. Conclusions and Future Work

For the economic purpose, the crime such as leak of confidential information is increasing lately. Actually, this comes from the inside not the outside. In this paper, the proposed framework for prevention of leak tries to prevent threat from the inside. But two methods of framework provide the legal issue which conflicts with privacy. Therefore, the enterprise wants to use this framework will solve this problem with the part of the employee and management.

Hereafter, we will implement the proposed framework and we will construct the framework suited for the enterprise. It will be practiced through the test that used forensic tool and detect the leak of information from internal enterprise. And we will provide a surrounding has no effect on target PC's OS.

5. ACKNOWLEDGEMENTS

This work was supported by grant NO. M10640010005-06N4001-00500 from the national R&D program of MOST and KOSEF.

6. REFERENCES

[1] National Industrial Security Center. DOI=http://www.nisc.go.kr.

[2] Lee, H. G., Lee, S. M., Nam, T. Y., and Jang, J.S. 2006. Technique trend about prevention of leak of confidential information.

[3] AKS-Labs. Insider threat to corporate information security. Find Protected AKS-Labs. DOI=http://www.findprotected.com/solutions/security-consulting/insider-threat.htm

[4] Sarbanes-Oxley Act. Wikipedia. DOI=http://en.wikipedia.org/wiki/Sarbanes-Oxley_Act

[5] Regulation of Investigatory Powers Act 2000. DOI=http://www.opsi.gov.uk/acts/acts2000/20000023.htm

[6] P. Gaonjur, and C. Bokhoree. 2006. Risk of Insider Threats in Information Technology Outsourcing: Can deceptive techniques be applied?. Security and Management 2006(Las Vegas, Nevada, USA, June 26-29, 2006). CSREA Press 2006. 522. DOI=http://www.informatik.uni-trier.de/~ley/db/conf/csreaSAM/csreaSAM2006.html

[7] Eric D. Shaw. The role of behavioral research and profiling in malicious cyber insider investigations. Elsevier Ltd., Digital Investigation. 3, 1(Mar. 2006), 20-31. DOI=http://dx.doi.org/10.1016/j.diin.2006.01.006

[8] Philip Sealey. Remote forensics. Elsevier Ltd., Digital investigation. 1, 4(Nov. 2004), 261-265. DOI=http://dx.doi.org/10.1016/j.diin.2004.11.002

[9] Mark E. Russinovich, and David A. Solomon. "Microsoft Windows Internals Fourth Edition:Microsoft Windows Server 2003, Windows XP, Windows 2000", Microsoft Press, 2004.

[10] Harlen Carvey. Tracking USB storage : Analysis of windows artifacts generated by USB storage devices. Elsevier Ltd., Digital investigation. 2, 2(June 2005), 94-100. DOI=http://dx.doi.org/10.1016/j.diin.2005.04.006

[11] Registry, Microsoft MSDN. DOI=http://msdn2.microsoft.com/en-us/library/ms724871.aspx