Network Forensic Technologies Utilizing Communication Information

Takemi Nisase† *and Mitsutaka Itoh*

Abstract

Forensic analysis is becoming increasingly important as the means for enterprises to avoid information security risks. In this paper, we overview computer and network forensics focusing on network forensic technologies that preserve all communication information and analyze it to investigate an incident.

1. What is Forensics?

Forensics is the application of science to questions that are of interest to the legal system. For information security, there are two types of forensics: computer forensics and network forensics.

Forensics is applied after an incident occurs. It involves analyzing information and collecting evidence to determine what happened. Forensic results are used to provide evidence in legal trials and to prevent similar incidents from happening again.

The position of forensics in the cycle of security management is shown in **Fig. 1**. Forensics can be divided into two processes: 1) the legal process for a lawsuit related to an incident and 2) the technical process that clarifies the vulnerabilities of the system based on the cause of the incident and applies security measures. The results are used to support lawsuits and improve daily operations. Furthermore, forensics is used to review overall policy and guidelines.

† NTT Information Sharing Platform Laboratories
Musashino-shi, 180-8585 Japan
E-mail: nisase.takemi@lab.ntt.co.jp

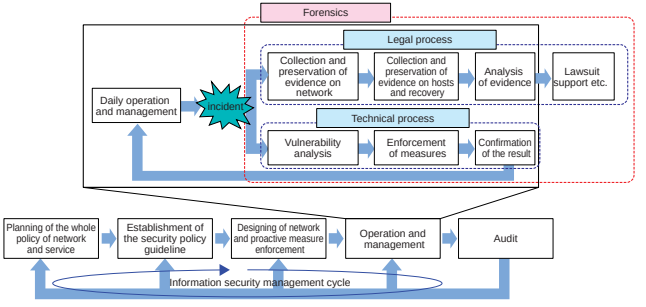

Fig. 1. Position of forensics in the security management cycle.

2. Need for forensics

In Japan, security measures are becoming important as a result of the increase in damage and impact of incidents caused by attacks and the increase in enterprise legal responsibility and dependence on IT technologies. The introduction of defensive technology such as firewalls, patches, and anti-virus software is becoming commonplace in enterprise networks. However, these proactive technologies cannot easily handle attacks on newly discovered vulnerabilities. On the other hand, the period from the discovery of a vulnerability to the first attack based on it has shortened year by year, and "zero-day" attacks are predicted. Furthermore, Warhol worms*1 that can spread around the whole world within 15 minutes and even flash worms that can start a DDoS (distributed denial of service) attack in even less time are predicted. Under these circumstances, anti-virus software vendors are taking early precautions and measures using new attack detecting technologies, but these cannot be guaranteed to absolutely safe. Therefore, forensic technology that provides assured countermeasures and minimizes the various types of damage caused by incidents is needed.

*1 Warhol worm is a term coined by Nicholas Weaver based on the famous words of Andy Warhol: "In the future, everybody will have 15 minutes of fame." http://www.cs.berkeley.edu/~nweaver/warhol.html

3. Computer forensics and network forensics

Network forensics analyzes information about network devices while computer forensics analyzes information residing on hosts (**Fig. 2**). Computer forensics is explained as follows in an article on the Japanese National Police Agency's Web site on high-tech crime and cyber terrorism. [1] "Computer forensics secures evidence in the digital world by applying computer science technology and aims to solve legal problems. It covers techniques for analyzing data inside a damaged computer (including falsified and deleted logs and data) that is difficult to detect by existing methods by using advanced tools and tracing unlawful access." Accordingly, advanced technology that uses specialized tools for analyzing an attacked host is needed.

Network forensics surveys communication logs and other information about network devices, such as routers, switches, and intrusion detection systems (IDSs*2). Then, it clarifies the attack time, the intruder's IP (Internet protocol) address, the attack path, and other information about the intruder.

In the past, IDSs were used to collect the network information, but recently network forensic devices have begun to be introduced. These let us analyze an

*2 Intrusion detection system: a system for detecting incidents in accordance with the rules that describe the characteristics of attacks.

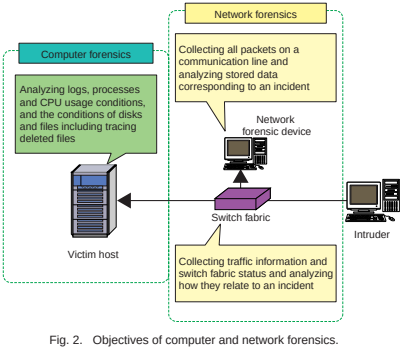

Fig. 2. Objectives of computer and network forensics.

incident after it has occurred because they have large memories and preserve copies of all the packets. One reason network forensic devices have become possible is the fall in price of hard disks with capacities of several hundred gigabytes. For example, a 300-GB hard disk can preserve all the information for a week in the case of 2% average bandwidth usage of a 100-Mbit/s WAN (wide area network) circuit.

4. Relationship between the kind of incident and forensics

According to JPCERT/CC*3, an incident is "an artificial phenomenon concerning computer security including intentional and also incidental things, such as illegal use of resources, denial of services, destruction of data, unexpected disclosure of information, and various actions related to them."

Every piece of information on the host and also on the network related to solving incidents of various kinds must be collected and analyzed. **Table 1** shows the main incident types and the information needed to analyze them. An example of network traces for ordinary intrusions is shown in **Fig. 3**.

*3 JPCERT/CC (Japan Computer Emergency Response Team Coordination Center) http://www.jpcert.or.jp/english/

5. Characteristics and problems of network forensics

(1) Recognizing an attack

Intruders often scan hosts to search for ones having vulnerabilities before making an actual intrusion. Such a trial attack may also be carried out when a new vulnerability is discovered. Thus, when an incident occurs it is important to analyze such precursory indications, even if this information is not related to an actual intrusion.

(2) Collecting evidence of intrusion when there were attempts at concealment, deletion, or falsification

When an intruder succeeds in entering the target host, he/she may conceal evidence on the host to delay discovery. In computer forensics, concealed evidence can usually be found by professional tools, but this requires advanced technology and discovery is not assured. On the other hand, network forensic devices collect and store communication information, so it is difficult for an intruder to hide it. Furthermore, the risks of falsification and deletion are lower because the intruder cannot directly access the stored information.

However, there are some problems with network forensics.

Table 1. Types of incidents and information that should be collected.

Incident type	Incidents	Information (required)
Illegal use of resources	Illegal use of processing power and storage	Host: access log, status of process, CPU usage, and status of files and storage
	Illegal use of network bandwidth	Network: circuit status, numbers of sent and received packets, IP address, protocol used, and status of switch fabric port
	Illegal relay of mail service and proxy service	Host: application log and status of process Network: IP address, protocol used, and data contents
DoS (denial of service)	Destabilization or stoppage of service by consuming server resources	Host: process status, CPU usage, and unusual packet log Network: circuit status, numbers of unusual packets, IP address, and contents of unusual packet
	Destabilization or stoppage of communication by consuming network bandwidth resources	Network: numbers of sent and received packets, IP address, protocol used, and data contents
Data destruction and falsification	Falsification of Web pages, data files, and program files	Host: access log, status of files and storage, and contents of configuration files Network: IP address, protocol used, data contents, and status of switch fabric port
Information leakage	Leakage of secret/confidential contents and interception of communication	Host: access log and status of files and storage Network: IP address, protocol used, data contents, and status of switch fabric port

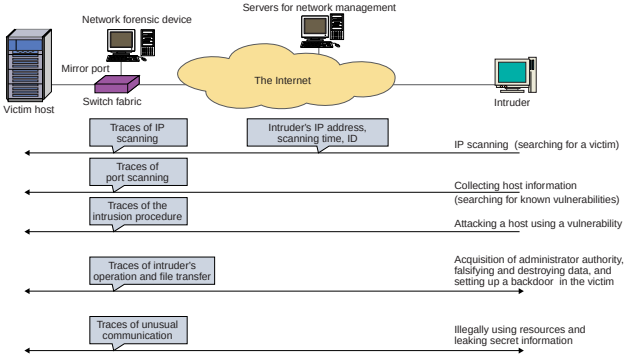

Fig. 3. Traces left on a network by ordinary intrusion methods.

(1) The data retention period decreases as the bandwidth increases

At present, the access bandwidth of the Internet is increasing rapidly. Therefore, the disk capacity needed to preserve all the collected information is also increasing rapidly. Conversely, the increase in communication bandwidth shortens the period of grace from problem detection to countermeasures. For example, a network forensic device with a memory capacity of 1 TB can preserve data corresponding to about 1.5 months in the case of 10% usage of a 10-Mbit/s WAN circuit. However, it can preserve only 4.6 days of data for 10% usage of a 100-Mbit/s WAN circuit. An effective way to solve these problems is to use technology that enables the extension and exchange of memory storage during operation and that automatically backs up preserved information to external memory storage.

(2) Security appliances may be attacked

The functions of security appliances are improving to deal with sophisticated and complicated attacks and in response to demands for advanced operability. However, these advanced functions may make security appliances more vulnerable. For example, the attack against major IDS products was able to crash many IDSs in February 2004. An operator may not recognize an incident correctly after the security appliance stops working and may assume that it is acting normally. Therefore, operators could overlook important signs and the introduction of security appliances could have the opposite effect to that intended.

To solve such a problem, beside the operator always applying the latest patch to the appliance, we need guidelines including ones about the operation flow for handling the case when the appliance itself is involved.

(3) Encryption technology is spreading

Virtual private network (VPN) services using encryption technology such as IPsec and SSL are becoming popular as inexpensive enterprise network access technology. The network forensic device that collects information about an encrypted communication can grasp the source and destination IP addresses and the time of communication, but it cannot detect attack patterns or perform a detailed analysis of the commands used by an intruder, because it cannot analyze the contents of packets. Therefore, analysis requires an operator who can combine information from network forensic devices and information about the victim host.

(4) Enterprise networks may be hit by inside attacks.

Careless operation on company premises and intentional inside attacks sometimes cause incidents in addition to the attacks from the outside. IDS and

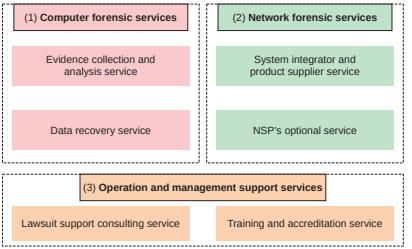

Fig. 4. Classification of MSSP's forensic services in the U.S.A.

forensic devices need to be established inside a company premises network as well as at the boundary between the company premises network and the outside to collect network information about internal incidents. For a large-scale enterprise network, the number of devices is huge and the surveillance and operating costs are high. Considering these problems, some operation systems that manage many IDSs distributed on an enterprise network have been announced.

In response to problems (1) and (3) above, we are researching a forensic architecture that coordinates the information of IDSs arranged on the network and the incident information collected by a host that assures log integrity using secure/trusted OS (operating system) technology. For problem (1), by selectively preserving the most relevant information about an incident, it is possible to reduce the disk capacity of the data storage device. For problem (3), detailed analysis is possible by analyzing the relationship between encrypted information on a network and host information.

6. Trend in the U.S.A.

Let us look the trend of forensic services in the U.S.A., where managed security services are widespread and laws have been strengthened.

A managed security service provider (MSSP) may classify forensics into services for computer forensics, network forensics, and operation support such as training forensic engineers and providing lawsuit support (**Fig. 4**).

(1) Computer forensic services

(a) Evidence collection and analysis service

This service finds the data needed for a lawsuit quickly out of the huge amount of data in a damaged computer system and preserves it as evidence. The main MSSP offers an overall service in concert with other MSSPs.

(b) Data recovery service

This service restores data that will become evidence of a crime or dishonest act. There are two types. A client either brings the storage media to the MSSP or allows the MSSP access to the client system via a network to recover data.

(2) Network forensic services

(a) System integrator and product supplier service

When a security incident occurs, the MSSP uses various security devices and logs, analyzes the correlation between events to reconstruct the process from occurrence to conclusion, and clarifies the cause and criminal evidence. For MSSPs, their appliances are core technologies and they also offer appliance management service.

(b) NSP's optional service

This service offers a menu of intrusion detection and firewall management services as an integral part of the security service provided by network service providers (NSPs). The NSP will remotely monitor customer premises equipment (CPE) and monitor connection points between a network and the CPEs.

(3) Operation and management support services

(a) Lawsuit support consulting service

This service provides consultation for strategy

planning and data collection and also provides experts to testify in court. An accounting firm offers this service as an integral part of the consulting service related to judicial affairs.

(b) Training and accreditation service

This service provides training courses for computer forensic investigators and accreditation for such courses.

7. Trend in Japan

The forensic service market has not been established yet in Japan. However, forensic services are likely to be introduced soon considering enterprise risk control, the need for prompt responses to large-scale information leakages, and new stricter laws affecting enterprises.

Reference

[1] http://www.cyberpolice.go.jp/column/explanation03.html (in Japanese)

Takemi Nisase

Senior Research Engineer, Secure Communication Project, NTT Information Sharing Platform Laboratories.

He received the B.E. and M.E. degrees in electronic engineering from Tohoku University, Sendai, Miyagi in 1985 and 1987, respectively. In 1987, he joined NTT Laboratories. He has engaged in research on ATM voice communication (VTOA), VoIP (Voice over IP), and secure IP communication (IP-VPN). He is currently engaged in research on Internet security technology.

Mitsutaka Itoh

Leader of Trusted Communication Group, Senior Research Engineer, Secure Communication Project, NTT Information Sharing Platform Laboratories.

He received the B.S. and M.S. degrees in mathematics from Waseda University, Tokyo in 1982 and 1984, respectively. In 1984, he joined NTT Laboratories and was engaged in R&D of programming languages, an Ada compiler, object-oriented design, cell phone systems, online-shopping services, ITS systems, IP-VPN service systems, and the resonant communication network. His current interest is network security and trusted communications environments. He is a member of the Institute of Electronics, Information and Communication Engineers of Japan.