Anti-tamper and Cryptographic Solutions for Information Protection

Takayoshi Shiraki
Makoto Sato
Masakazu Noguchi, Dr. Info. Sci.
Soichi Furuya, Dr. Eng.

OVERVIEW: As leaks of information from public infrastructure systems can cause damage at a national scale, it needs to be recognized as a top priority for national security. Based around anti-tamper and cryptographic technologies, Hitachi supplies solutions for preventing leaks that include tools for blocking reverse engineering and functions for full disk encryption and communication encryption. These products are designed and implemented based on know-how that Hitachi has built up through its experience with system development, and on its own risk analyses that assume large-scale attacks.

INTRODUCTION

AT most companies and other organizations, a data leak usually means the loss of personal information or commercial secrets. Such a leakage of information is a major problem that can have serious consequences, including reputational damage to the company or organization and the payment of compensation.

In the case of public infrastructure systems, on the other hand, the damage from information leaks can potentially extend much further than just compensation and reputational damage. In particular, leaks of authentication data or information about the system's configuration or installed software (such as its vulnerabilities) can result in the use of this information to mount cyber-attacks, with consequences such as widespread system shutdowns or the hijacking of system control authorities. In other words, attacks launched against large systems such as those used for homeland security or public infrastructure have the potential to cause damage at a national scale.

Hitachi sees the problem of information leaks as being the top priority for national security. Through the development of systems for national security, Hitachi has also conducted risk analyses that assume large-scale attacks, and has established stringent security against such an eventuality. Hitachi utilizes know-how derived from this experience to supply technology for preventing information leaks that takes account of countermeasures at the level of national security.

This article reviews Hitachi's perspective on the threat of information leaks, and describes two core protection methods, namely anti-tamper and cryptographic technologies, together with Hitachi's solutions for preventing information leaks that utilize these technologies.

INFORMATION LEAK THREATS AND COUNTERMEASURES

Treating data and software as assets that need to be protected, this section describes both the threats to which these assets are exposed and the techniques used to protect them against these threats.

Threats to Information Assets

Fig. 1 shows the threats to data faced by a typical corporation. The figure shows three different environments: the company headquarters, a branch office, and outside the company. This scenario includes the use of fixed personal computers (PCs) for work at headquarters and branch offices, and the use of mobile

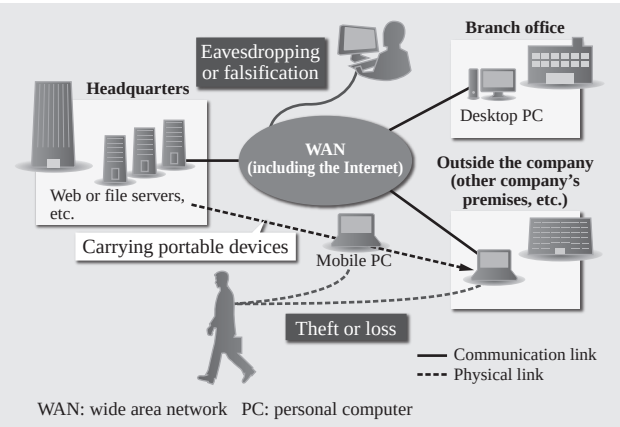

Fig. 1—Threats to Data.
The figure shows the main threats to corporate PCs. These include eavesdropping or falsification via a WAN, and the theft or loss of devices when out of the office.

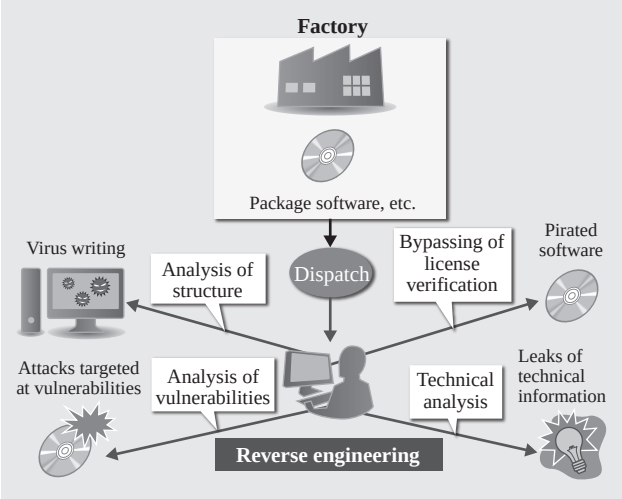

Fig. 2—Threats against Software.
The unauthorized reverse engineering of software can identify how the software works and be used in damaging ways such as the production of pirated versions.

PCs for sales calls and other out-of-the-office work. They also use a wide-area network (WAN) such as the Internet for communications between headquarters, branch offices, and staff on the road. In a situation like this, the main information leak threats are the eavesdropping or falsification of communications data on the WAN, and the theft or loss of PCs or other devices when out of the office. Of particular note in the case of PCs is that, because it is still possible to read the contents of a hard disk simply by removing it and connecting it to another PC, the threat posed by theft or loss cannot be mitigated even if their basic input/output system (BIOS) and operating system (OS) require authentication to access.

Similarly, Fig. 2 shows the threats faced by software. Rather than the vulnerabilities of specific programs that can be resolved by applying a software patch, the critical threat is seen as coming from the sort of malicious reverse engineering shown in this figure. In this context, reverse engineering means the analysis of a program's structure and operation. Reverse engineering can be used to steal technical information or produce pirated versions of software, and attackers can use vulnerability analysis and other techniques on these as the basis for writing viruses. This makes it a starting point for mounting a cyber-attack. Of these, virus writing and vulnerability analysis in particular can be precursors to cyber-attacks, and mounting an attack on special-purpose software typically requires that the software first be reverse engineered. As described above, cyber-attacks on large infrastructural systems can result in damage on a national scale.

Table 1. Threats Faced by Different Types of Information Assets
Of the various information assets that need to be protected, different types of information face different threats.

Type of information	Threat
Software	Reverse engineering
Data on hard disk	Theft or loss
WAN communications data	Eavesdropping or falsification

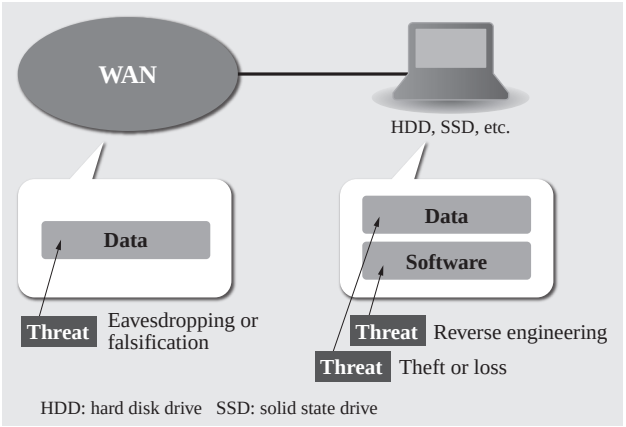

Fig. 3—Types of Information and Threats they Face.
The nature of the threats faced and the countermeasures they require are different depending on the type of information (data or software) and where it is located (WAN or HDD).

Table 1 lists the threats faced by different types of information assets, and Fig. 3 shows the types of information and the threats they face.

The following section describes the countermeasures against these threats.

Use of Anti-tamper and Cryptographic Technologies to Protect Information Assets

Hitachi sees anti-tamper and cryptographic technologies as playing a core role in countering threats to information assets.

Cryptography is an effective way to prevent the loss of information in the form of data. While cryptography can be used for any type of data, it offers limited protection for software. This is because, even if the programs on a computer are encrypted, they must ultimately be decrypted in order to execute. Anti-tamper technology, on the other hand, protects software that cannot be secured by cryptography by making reverse engineering more difficult. Using these two technologies together prevents leaks of both data and software.

Hitachi's Strengths

Hitachi draws on its experience with establishing security for information systems, such as those

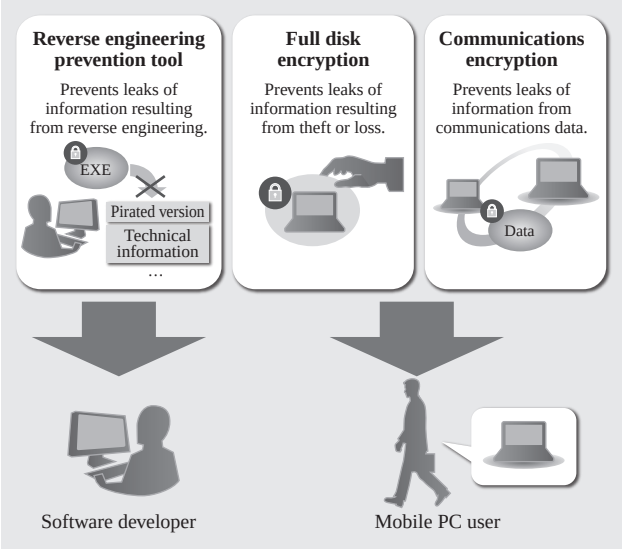

Fig. 4—Solutions for Preventing Information Leaks.
These three key functions protect software, hard disk data, and communications data from leaks.

associated with national security, to supply cryptographic functions that provide a high level of protection. These include techniques for evaluating cryptographic strength (how difficult it is to break the cypher), and Hitachi is able to provide customized cryptographic algorithms for applications that required protection at the level of national security. Because it possesses skills in software implementation and know-how in fields that are essential to anti-tamper techniques, such as central processing units (CPUs) and OSs, Hitachi is also able to supply functions that effectively block reverse engineering.

The following section gives details of a solution that takes advantage of these strengths to prevent information leaks from Windows*1 PCs.

SOLUTIONS FOR PREVENTING INFORMATION LEAKS

This section first gives an overview of solutions for preventing information leaks, then describes the security functions supplied by Hitachi.

Overview

In addition to anti-tamper and cryptographic technologies, countermeasures against the threats described above also need to be implemented in ways that take account of the nature of the threats. Furthermore, PC users do not need to be aware of the countermeasures being used, and comprehensive protection against information leaks is an important feature for guarding against inattention and other forms of human error.

To overcome these challenges, Hitachi supplies following three key security functions for Windows PCs (see Fig. 4).

(1) Reverse engineering prevention tool
(2) Full disk encryption
(3) Communications encryption

These functions provide measures against the three types of threat described in the earlier example (in Table 1). In particular, full disk encryption and communications encryption used together can provide comprehensive protection against leaks of data from PCs. They are effective measures for mobile PCs that are especially at risk from security threats. Comprehensive and enforced use of encryption to secure all information in PCs and elsewhere, with full disk encryption for data on hard disks and communications encryption for communications data, ensures that information leaks do not occur.

Reverse Engineering Prevention Tool

The reverse engineering prevention tool is a software utility for incorporating anti-tamper functions into completed programs in order to make them difficult to reverse engineer.

The following sections describe the methods used for reverse engineering and the anti-tamper functions that counter them, and provide details about how the tool works.

Methods used for reverse engineering

Static code analysis and dynamic code analysis are two ways of reverse engineering software.

Static code analysis analyzes software without executing it. Typically, a disassembler or decompiler is used to convert the executable file (machine language) into a programming language that can be analyzed. Because the person doing the analysis needs to visualize how the program will run, a high level of skill is required.

Dynamic code analysis analyzes software while it is running. This is done using tools such as a debugger (a utility that allows the user to view and manipulate the status of the CPU and memory during program execution) or virtual machine. A virtual machine is a program that emulates the PC hardware and provides the environment for executing the debugger and the software being analyzed. Because it can view the actual operation of the software, dynamic code analysis has the advantage of being comparatively easier to

*1 Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

perform than static code analysis. On the other hand, because the software actually has to execute, there is a potential for unforeseen consequences. For example, some software is designed to detect unauthorized analysis and terminate with an error to prevent the analysis proceeding, or even to corrupt the analysis system. Accordingly, it is subject to a different set of analysis restrictions to static code analysis.

Because the two approaches have their respective strengths and weaknesses, reverse engineering makes use of both, depending on the circumstances.

Overview of anti-tamper functions

The anti-tamper functions in the reverse engineering prevention tool include mechanisms for obstructing both static and dynamic code analysis.

(1) Obstruction of static code analysis

This is done using the executable file encryption function [see Fig. 5 (a)]. Essentially, protection is achieved by encrypting the executable file, and by obfuscating its decryption function and the cryptographic key. This prevents the program from being converted back to assembly language or some other programming language through the use of static code analysis tools such as disassemblers or decompilers.

(2) Obstruction of dynamic code analysis

This incorporates code into the executable file that monitors the CPU, memory, and OS to detect when the program is being analyzed using a debugger and virtual machine [see Fig. 5 (b)][1), 2)]. If such analysis is detected, the code takes some action to prevent it from proceeding, such as halting execution [see Fig. 5 (c)].

To prevent the analysis detection function itself from being reverse engineered, its operation is obfuscated (its operation made more complex so as to be difficult to analyze) to prevent easy analysis. Through these multi-layered measures, resistance to reverse engineering is enhanced.

Implementation of anti-tamper functions

Trying to incorporate these anti-tamper functions during coding makes software development more difficult. They require each programmer to be familiar with the functions, and incorporating the functions in a program adds complexity to the process of writing it. To overcome these problems, what is required is a simple way of protecting software that can incorporate the anti-tamper functions into programs without having to modify their source code. Of particular concern are how to implement decoding of encrypted executable files and analysis detection.

To solve this problem, Hitachi developed a technique for incorporating additional processing without affecting the operation of the executable file, taking account of factors such as the structure of the executable file and the way OS runs software. This allows functions for detecting the decoding and analysis of encrypted software to be added to any executable file. Because decoding is performed

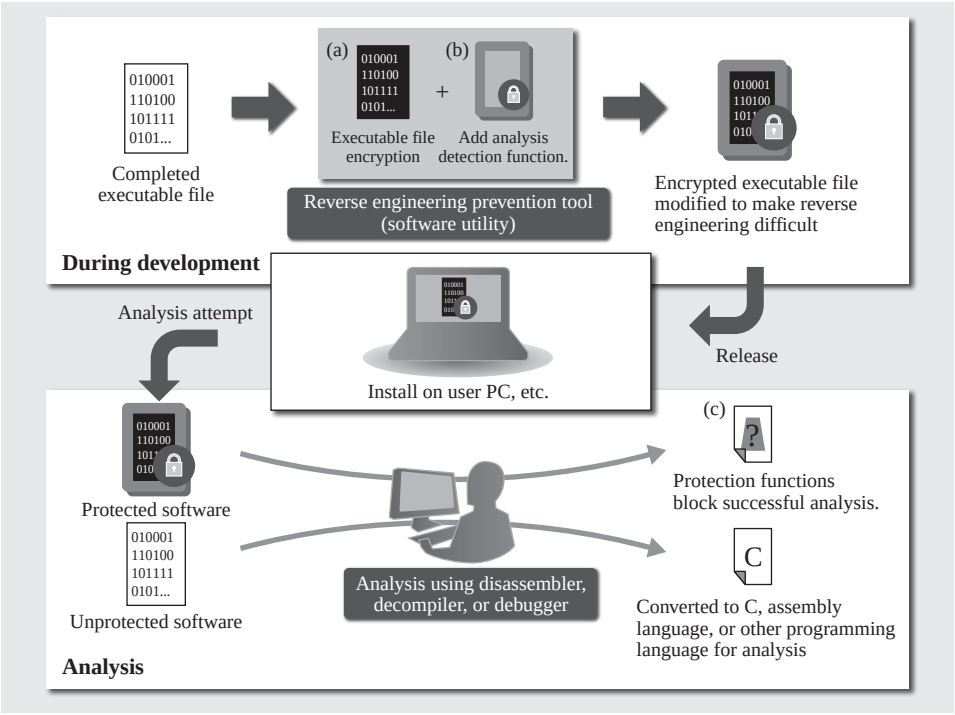

Fig. 5—Reverse Engineering Prevention Tool.
The completed software (executable file) is input to a tool that automatically incorporates anti-tamper functions to make reverse engineering difficult.

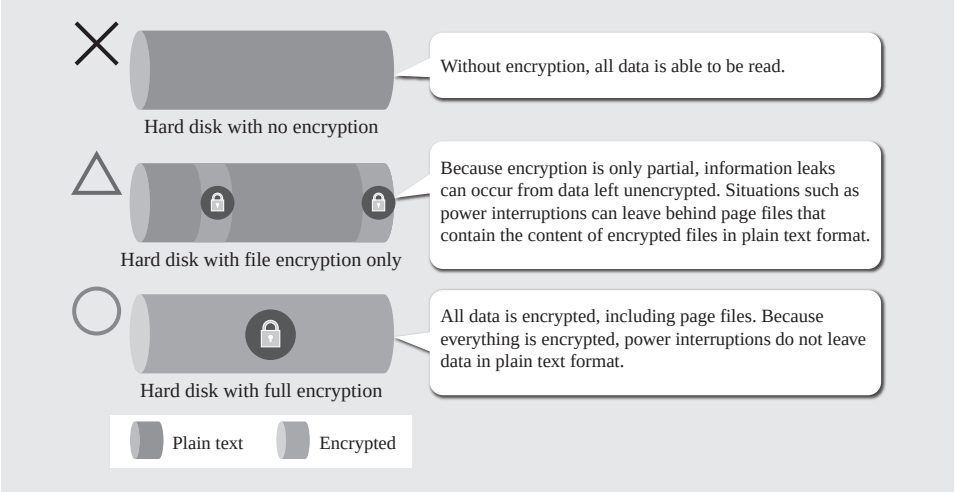

Fig. 6—Full Disk Encryption. Encrypting the entire hard disk prevents data from being left unencrypted. File encryption cannot prevent information leaks from occurring in unanticipated situations.

automatically when the software is run, encrypted programs can be invoked in the same way as the originals, and their operation once running remains unchanged. For example, a program that is invoked by clicking an icon is still invoked this way after the tool has been used to add the anti-tamper functions, and its operation remains the same as before. Also, as the decrypted program is only output to volatile memory (hardware), its code cannot be read off the hard disk.

Using this method, all that is required is to feed the software to be protected as input to the tool and have the tool output the software with the anti-tamper functions added (see top of Fig. 5). The output software is then released and anti-tamper functions protect it from any subsequent unauthorized reverse engineering (see bottom of Fig. 5). This prevents any information from being extracted from the software.

Full Disk Encryption

Use of full disk encryption to enforce encryption prevents information leaks resulting from theft or loss.

Three challenges face this function. The first is automatic encryption of the entire hard disk, including the OS, the second is how to boot an encrypted OS, and the third is preventing a removed hard disk from being decrypted.

To overcome the first challenge, the encryption function is built into the device driver layer (as a filter driver). This means that the encryption function operates as part of the OS, and all write access to the hard disk by application programs or the OS is encrypted automatically (full encryption). Also, because it runs in the same layer as the OS, the encryption function does not affect the behavior of application programs or other user operations. The second challenge is overcome by preboot authentication that performs authentication before the OS boots. Finally, the third challenge is dealt with by using a proprietary boot loader to decrypt the OS as it boots. The following sections describe full encryption and preboot authentication in detail, both of which have important security roles in full disk encryption.

Full encryption

Full encryption enforces the encryption of all data on the hard disk, including files output by the OS (see Fig. 6). One advantage of this function is that it prevents information leaks from occurring through inattention, such as a user forgetting to encrypt data. Another advantage is that even files output by the OS are encrypted.

Although users are not generally aware of files output by the OS, there have been cases when information has been extracted from these files. Paging files are one way this can happen. Paging files are used by the OS to cache data temporarily when memory hardware capacity is insufficient. Such files can be a source of leaks because they can contain data from the volatile memory unencrypted without the user knowing. While a simple file encryption function cannot perform encryptions for these special files, the full disk encryption can, thereby preventing theft of the information they contain.

Preboot authentication

Preboot authentication is a function added along with the full disk encryption function to perform user authentication prior to the OS booting. As decrypting of the hard disk data cannot start until after this authentication is successful, an unauthorized user cannot read its contents even if they remove the hard disk and attach it to another PC. This function provides PCs with a very robust authentication mechanism because it uses its own authentication method, making

it separate to any other authentication such as that performed by the BIOS or OS.

Communications Encryption

Communications encryption prevents leaks of information from communications data by encrypting all communications.

A challenge for this function is to ensure that the communications data from all application programs running on a Windows system is encrypted automatically.

To achieve this, communications encryption is implemented in the device driver layer, the same as the full disk encryption function. This ensures that communications data from all application programs is encrypted automatically, and there is no effect on the behavior of the application programs or user operation.

This function can be provided for the following two types of communications, depending on the application.

Communications via encrypted virtual hub

This method encrypts Ethernet frames and uses Transmission Control Protocol/Internet Protocol (TCP/IP) encapsulation (see Fig. 7). As indicated in Fig. 7, the method can be used for multipoint-to-multipoint communications. Also, authenticating each communications packet prevents the tampering with or spoofing of communications data, and communications can use proprietary cryptographic algorithms to achieve high levels of security, as required. Another feature of this method is that each PC communicates via a server called an "encrypted virtual hub."

Encrypted virtual hubs are servers that emulate a physical hub. They are used to run a single virtual network on top of a WAN (called an "overlay network") so that PCs located both inside and outside the company that connect to the encrypted virtual hubs can communicate as if they are all on the same local area network (LAN). Multipoint-to-multipoint communications works on the same principle. A feature of this communications mechanism is that, since these communication traffic streams are encapsulated as TCP/IP packets (such as port No. 80: Hypertext Transfer Protocol packets), each peer in the network can communicate even over firewalls or Network Address Translation (NATs). For this reason, this way of communication has advantage when a user cannot choose an ideal network environment.

IPsec transport mode communications

Security Architecture for Internet Protocol (IPsec) transport mode communications means IPsec communications in which only the Transmission Control Protocol/User Datagram Protocol (TCP/UDP) payload is encrypted (see Fig. 8). As indicated in Fig. 8, it can be used for point-to-multipoint communications. Like encrypted virtual hub communications, it can use proprietary cryptographic algorithms and perform authentication for each communications packet. Being simpler than encrypted virtual hub communications, high throughput is an advantage. This makes it suitable for use on communication links that can be configured as required, such as between headquarters and branch offices, for example.

CONCLUSIONS

This article has reviewed Hitachi's perspective on the threat of information leaks, and described two core protection methods, namely anti-tamper and cryptographic technologies, together with Hitachi's solutions for preventing information leaks that utilize these technologies.

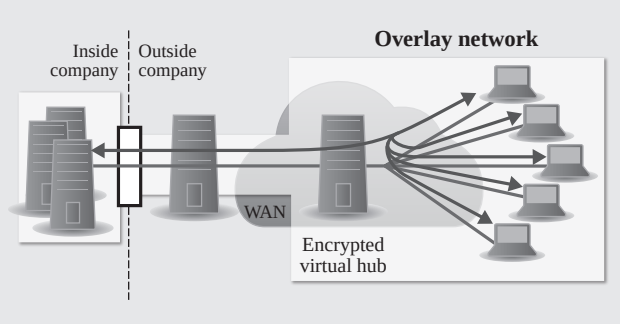

Fig. 7—Encrypted Virtual Hub Communications.
A feature of this method, which encrypts Ethernet frames, is that it makes it difficult to intercept communications in firewalls or other network devices.

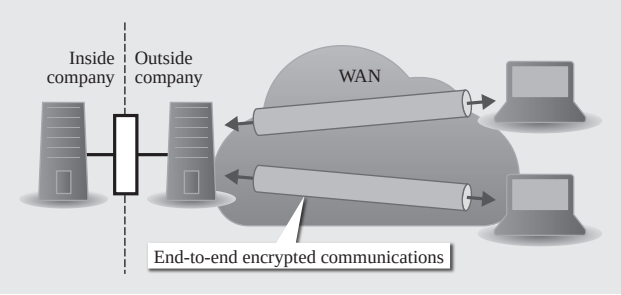

Fig. 8—IPsec Transport Mode Communications.
Security Architecture for Internet Protocol (IPsec) transport mode communications is a comparatively simple communications method that only encrypts the Transmission Control Protocol/User Datagram Protocol (TCP/UDP) payload.

The reverse engineering prevention tool is a high-security technology for preventing information leaks that has been designed and implemented based on detailed risk analyses and experience that Hitachi has built up for itself in system development, as have the full disk encryption and communications encryption functions.

While this article has focused on technology for Windows PCs, the same technology can also be applied to a range of other platforms. In particular, in addition to systems made up of PCs and other general-purpose devices, concern has been growing in recent years about cyber-attacks on systems that include embedded special equipment, including calls highlighting the importance of security measures in fields such as public infrastructure. Hitachi believes that defending systems against attacks like these requires that anti-tamper and other similar functions be provided as standard features in various different types of software. However, before these technologies can be applied to the proliferating number of different platforms, risk analysis and technical investigations are needed to consider their specific requirements.

In the future, Hitachi intends to utilize these technologies for preventing information leaks to make a contribution to greater safety and security in society by supplying advanced custom security solutions in a wide range of fields, including national security and public infrastructure.

REFERENCES

(1) M. Yason, "The Art of Unpacking," Proceedings of Black Hat 2007, https://www.blackhat.com/presentations/bh-usa-07/Yason/Whitepaper/bh-usa-07-yason-WP.pdf

(2) P. Ferrie, "Attacks on Virtual Machine Emulators," http://www.symantec.com/avcenter/reference/Virtual_Machine_Threats.pdf

ABOUT THE AUTHORS

Takayoshi Shiraki

Joined Hitachi, Ltd. in 2007, and now works at the Information and Communication Technology System Department, Defense Systems Company. He is currently engaged in information security business for the defense and crisis management sectors. Mr. Shiraki is a member of the IEEE Computer Society.

Makoto Sato

Joined Hitachi, Ltd. in 1993, and now works at the Information and Communication Technology System Department, Defense Systems Company. He is currently engaged in software development for information security.

Masakazu Noguchi, Dr. Info. Sci.

Joined Hitachi, Ltd. in 1998, and now works at the Information and Communication Technology System Department, Defense Systems Company. He is currently engaged in new business development for the defense and crisis management sectors. Dr. Noguchi is a member of The Mathematical Society of Japan.

Soichi Furuya, Dr. Eng.

Joined Hitachi, Ltd. in 1997, and now works at the Social Infrastructure Systems Research Department, Yokohama Research Laboratory. He is currently engaged in research and development aimed at establishing service engineering and cloud service businesses. Dr. Furuya is a member of The Institute of Electronics, Information and Communication Engineers and the Information Processing Society of Japan.