Featured Articles II

Security Research and Development

Research and Development of Advanced Security Technology

Tadashi Kaji, Ph.D.

OVERVIEW: The damage done by cyber-attacks in recent years is spreading to all areas of society due to the targeting of IoT systems used in social infrastructure as well as IT systems. In response to these circumstances, Hitachi has been promoting the continuing research and development of cybersecurity as part of its mission of building and operating safe and secure social infrastructure. This article describes the research and development being undertaken to implement Hitachi's system security concept. The aim of this research is to achieve quick responses to cyber-attacks in cooperation with system stakeholders through the design and development of robust IoT systems that people can use for a long time to come with peace of mind.

INTRODUCTION

CYBER-ATTACKS on information technology (IT) systems are becoming more sophisticated. With corporate activity having become more dependent on IT, the potential for damage due to an attack on IT systems is a direct business risk.

Security countermeasures are also becoming essential for control systems, an area that was previously outside the scope of cyber-attacks, due the emergence of Internet of Things (IoT) systems that use IT for interconnecting devices. This makes it important for research into cybersecurity to take on new issues.

This article presents an overview of new research and development being undertaken in response to these circumstances, including an explanation of the security concept being promoted by Hitachi.

HITACHI'S SYSTEM SECURITY CONCEPT

Security countermeasures are essential for the IT and IoT systems used in social infrastructure, not just to protect information, but also in terms of the ability of social infrastructure to continue providing services despite being exposed to a variety of threats. Meanwhile, the increasing number of devices connected to networks means that targets that were not previously at risk of attack are now increasingly likely to suffer damage. Another new development is that IT and IoT systems are using interoperation to implement various functions.

Accordingly, Hitachi believes that action needs to be taken in response to the following three trends to ensure the information security of IT and IoT systems.

(1) Growing diversity of threats
(2) Importance of incident response
(3) Greater interdependence

To deal with these trends, Hitachi has been promoting its Hitachi system security concept since 2013[1] (see Fig. 1).

The implementation of security functions for components and security operation management

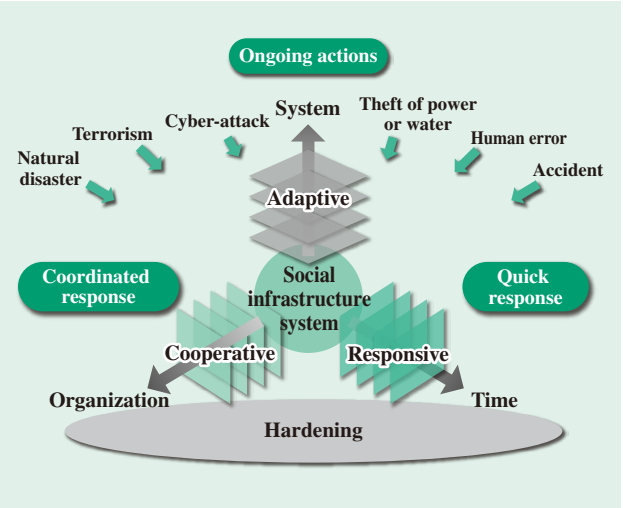


Fig. 1—Hitachi System Security Concept.
Along with the traditional idea of hardening, the Hitachi system security concept also highlights improvements to security in terms of it being adaptive, responsive, and cooperative.

for systems are both important for improving the information security of IT systems. The Hitachi system security concept identifies where improvements are needed to deal with the above three trends in terms of both functions and management.

FEATURES OF THE HITACHI SYSTEM SECURITY CONCEPT

This section gives an overview of the sort of security the Hitachi system security concept is seeking to achieve.

Building Robust Systems

A cyber-attack is an action that compromises the confidentiality, integrity, and availability of the assets in a system that are to be protected. To counter such an action, it is necessary to make the system more secure.

The first requirement for preventing cyber-attacks on an IT system is to identify and authenticate users and only permit access once identity is verified. Common methods used on past systems have included user name and password authentication whereby the user's identity is confirmed by having them enter a password that only they know, or having the user present a smartcard containing information identifying them that is protected by a personal identification number (PIN) so that only they can access it.

Unfortunately, there have been numerous instances on current IT systems of damage caused by "social engineering" methods that deceive users into revealing their passwords or phishing sites that covertly harvest passwords. Given the existence of various other methods, including being able to guess passwords easily or copy passwords that have been written down in a notebook, for example, or malicious use of sites for resetting passwords, any system that is based on existing systems cannot necessarily be described as secure.

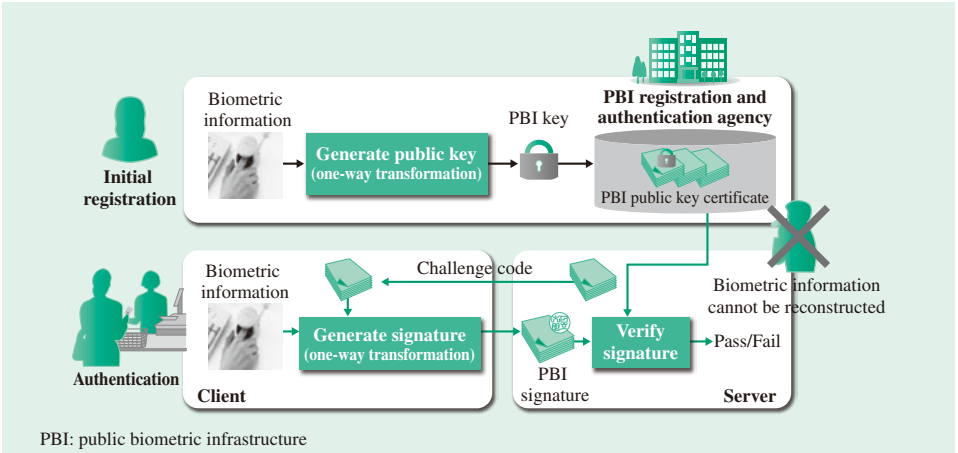
In response, Hitachi has developed a public biometric infrastructure (PBI) (see Fig. 2) for more secure personal identification that combines biometric information that cannot be stolen by an attacker with what is currently the most secure form of public key infrastructure (PKI).

Even more than IT systems, IoT systems with interconnecting devices have strong requirements for lower costs and are often implemented on low-cost hardware, even at the expense of processing performance. Accordingly, it has been difficult to include security functions for encryption that provide secrecy of communication paths and the exchange of authentication between communicating parties on current IoT systems. Hitachi has responded by developing resource-saving encryption techniques that target the hardware used by IoT systems and that are able to operate using minimal resources compared to past techniques.

Guarantee with respect to Long-term Availability

Unlike personal computers (PCs) or smartphones, the devices used in IoT systems sometimes need to remain in use for a decade or more in order to keep system costs down. By contrast, the methods used by cyber-attacks are evolving in ingenuity on a daily basis, such that there is a need for ongoing security countermeasures such as installing software patches when a new system vulnerability is identified.

Unfortunately, whether software is commercial or open source, software maintenance is only available for a limited time. As the support periods for IT systems are typically about five years, in order to provide a long-term guarantee, it is important that they



PBI: public biometric infrastructure

Fig. 2—How PBI Works. PBI provides a means of personal identification that prevents an attacker from impersonating a user by using a PBI key generated by a one-way transformation of biometric information.

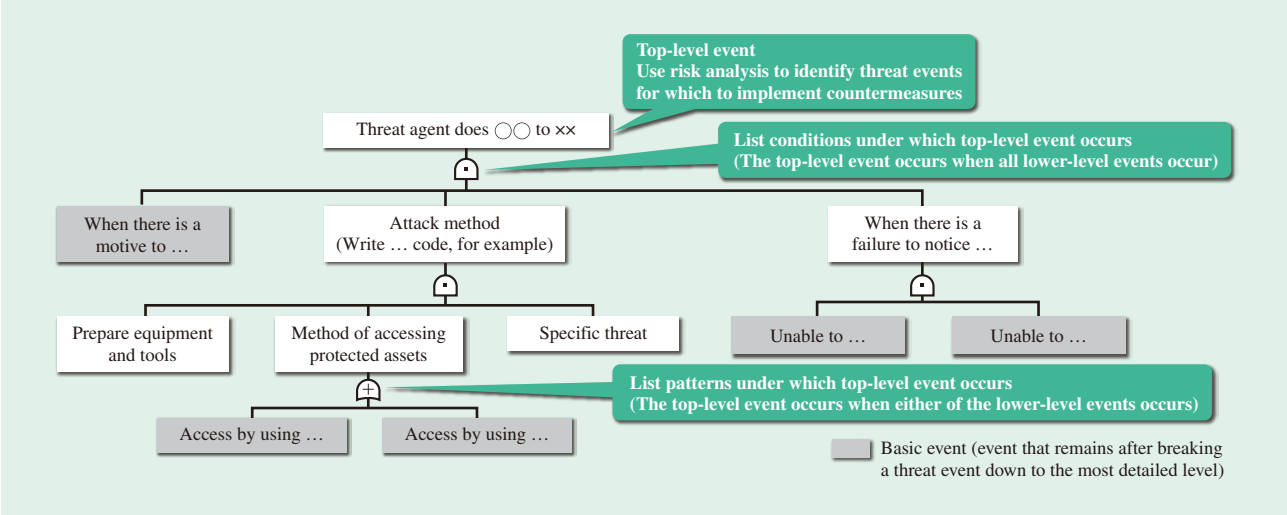


Fig. 3—Determine Threat Countermeasure Objectives Using Fault Tree Analysis.
Fault tree analysis is used to investigate how to counter the basic events that lead to threat events by considering the factors involved in terms of motivations, methods, and the conditions under which the threat events can occur.

are designed to allow for ongoing countermeasures as well as eliminating vulnerabilities. To achieve this, Hitachi has developed security design techniques intended specifically for IoT systems.

Devices used in IoT systems have sensors and actuators, which means they can interact with the physical realm as well as cyberspace. The focus of past IT systems has been on protecting information in cyberspace, with security design based on preventing information from being stolen or tampered with by third parties. This leaves room for doubt as to whether the techniques used on IT systems are suitable, in their current form, for the security design of IoT systems and devices. In the case of IoT devices that have potential implications for human life if subject to a cyber-attack, such as vehicles with a network connection, it is necessary to treat the device's control functions as an important aspect that needs to be protected along with information.

Hitachi has developed security design techniques specifically for IoT systems that build on those for IT systems and are characterized by identifying threats and considering countermeasures on the basis that the scope of protection also covers device functions. These techniques are based on standard security design procedures and are made up of four phases, namely, defining the scope to be considered, identifying security issues, formulating countermeasure objectives, and selecting security requirements. A feature of this process is that the things that the selected security requirements are intended to prevent can be logically explained by identifying the security issues and formulating the countermeasure objectives in an analytical and comprehensive manner.

Specifically, the particular task of identifying threat events among the security issues is performed with respect to the assets to be protected (including functions) in a comprehensive manner from the perspectives of *where*, *who*, *when*, *why*, and *what*. It can also produce logically explainable countermeasure objectives by conducting a detailed analysis of the attacker's motivations and methods and the conditions under which an attack can be launched for all of the identified threat events using the fault tree analysis method, and studying ways of countering the end events of the tree (see Fig. 3).

Achieving Quick Responses

IT systems have been exposed to a variety of cyber-attacks over the past half-century. As a result, IT vendors have built up expertise in security design and strengthened capabilities for responding quickly when an attack happens (incident response).

To avoid detection during an intrusion, targeted and other recent cyber-attacks have featured increased use of advanced and highly-engineered malware that only runs on systems with the targeted operating system (OS) or application installed. It has also been claimed that half of such malware is undetectable by existing anti-virus techniques based on pattern-matching.

Accordingly, to enable a response to be mounted against such malware at an early stage, Hitachi has been researching techniques for the automatic and rapid evaluation of malware behavior by executing

this highly-engineered malware under a wide range of different conditions and recording how it behaves. This helps achieve faster incident response by implementing exit point defenses, for example, based on behaviors identified by this technique, such as the transmission of information by the malware to a site controlled by the attacker, in which case connections to that site can be blocked (see Fig. 4).

Sharing Information to Improve Security

While convenience is improved through interoperation between IT and IoT systems, there are concerns about it increasing the overall harm to the system due to the damage resulting from an attack or incident on one subsystem leading to damage to other subsystems. To prevent this, it has become necessary to respond in a coordinated manner utilizing the *orient* and *decide* steps of incident response described above.

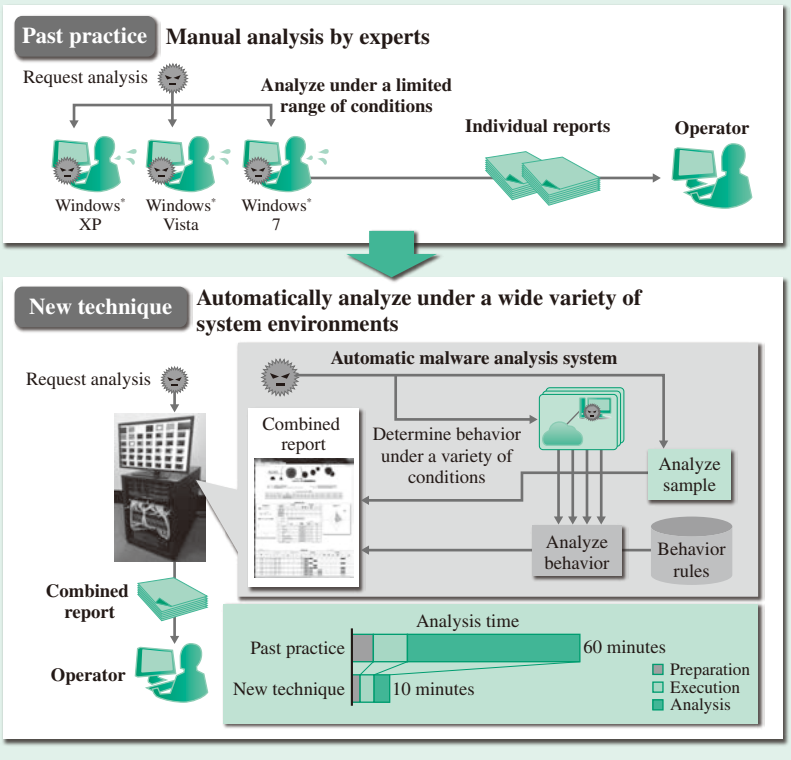
Hitachi has proposed its symbiotic autonomous decentralization concept for encouraging new growth by supplying value created by linking different systems and other mechanisms to all of the stakeholders in the associated systems[(2)].

In the case of symbiotic autonomous decentralized systems, obtaining an accurate understanding of what is happening across various different organizations or operators (subsystems) requires the sharing of information between organizations such as information sharing and analysis centers (ISACs) or incident response teams. In order to respond quickly, it is also important to be able to process incident response information automatically. The Cyber Threat Intelligence (CTI) Technical Committee (TC) of the Organization for the Advancement of Structured Information Standards (OASIS) is currently formulating the Structured Threat Information Expression (STIX*), Trusted Automated Exchange of Indicator Information (TAXII*), and Cyber Observable Expression (CybOX*) standards specifying key information formats for IT systems, and work has just started on adapting these standards for use on IoT systems.

STANDARDIZATION ACTIVITIES

Moves to formulate a variety of standards for IoT system security are accelerating. For industry, work is proceeding on the IEC 62443 security

* STIX, TAXII, CybOX and the CybOX logo are trademarks of The MITRE Corporation.



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

Fig. 4—Malware Automatic Analysis Technique.
This technique automatically analyzes malware under a wide variety of system environments to determine the behavior of malware that varies depending on the environment.

standard for control systems, primarily through the International Electrotechnical Commission (IEC). For areas that deal primarily with networks and IT, standards bodies such as the IEEE, oneM2M, the International Organization for Standardization (ISO), and International Telecommunication Union Telecommunication Standardization Sector (ITU-T) are working together to formulate security standards.

Hitachi's involvement to date in security standardization for IT and IoT systems has included contributing to the establishment of security concepts and to implementing security functions that take account of the characteristics of IoT systems.

In the former case, Hitachi is contributing to the IEC to improve security by guaranteeing long-term availability, achieving a quick response, and information sharing as well as building systems that are resilient, in step with trends in IoT and IT systems. Hitachi is also working with the Control System Security Center, a Japanese technology research organization, to conduct research and development using standards, with work proceeding on raising awareness and a program of security exercises.

In the latter case, Hitachi has proposed a lightweight (able to run on minimal resources) encryption algorithm to ISO and IEC with the aim of enabling security functions to be implemented on IoT devices that need to deliver realtime performance despite limited central processing unit (CPU) and memory capacity. As a lightweight encrypted communications protocol is also required for IoT devices to verify each other's identity and to gain access to secure communication links, Hitachi has proposed a standard technique to the ITU-T and is participating in the formulation of standard techniques at oneM2M.

CONCLUSIONS

Because IT and IoT systems will serve as platforms for the social infrastructure of the future, it is critical that they utilize the latest technology to provide for all eventualities, including cyber-terrorism. This article has provided an update on the latest research on security for IT and IoT systems in the context of the Hitachi system security concept.

Current techniques for building resilient systems provide the basis for maintaining the cybersecurity of IT and IoT systems with low cost and long life. It is also important to identify threats during system development and maintain the most effective countermeasures over a long period of time, to mount a quick response during system operation, and to strengthen defenses against increasingly sophisticated cyber-attacks by sharing security information between stakeholders. Hitachi intends to continue contributing to the creation of safe and secure social infrastructure by working on the research and development of the latest technologies based on these considerations.

REFERENCES

(1) M. Mimura et al., "Hitachi's Concept for Social Infrastructure Security," Hitachi Review **63**, pp. 222–229 (Jul. 2014).
(2) N. Irie et al., "Information and Control Systems –Open Innovation Achieved through Symbiotic Autonomous Decentralization–," Hitachi Review **65**, pp. 13–19 (Jun. 2016).

ABOUT THE AUTHOR

Tadashi Kaji, Ph.D.
Security Research Department, Center for Technology Innovation – Systems Engineering, Research & Development Group, Hitachi, Ltd. He is currently engaged in the research and development of cyber security technology. Dr. Kaji is a member of the IEEE Computer Society.