Cyber Security Technologies for Social Infrastructure Systems

Tadashi Kaji, Dr. Info
Tsutomu Yamada
Toshihiko Nakano, Dr. Eng.
Susumu Serita

*OVERVIEW: Cyber security threats have emerged as a growing concern for all forms of social infrastructure in recent years. Based on its "2×3 Concept," Hitachi has formulated security guidelines to cover each of the design, development, implementation, and operation phases. Technologies being developed by Hitachi to ensure security in all corners of the social infrastructure, right down to the control equipment and other field devices with limited capabilities, include high-speed encryption techniques, the Enocoro*1 low-power stream encryption technique, and device authentication techniques. Also under development in response to the sophisticated cyber threats now being faced are techniques for reducing the workload associated with security operation, including analysing large amounts of log or communications data to detect any viruses lurking in the system.*

INTRODUCTION

INFORMATION technology (IT) is being used to boost the efficiency of social infrastructure throughout the world, with equipment being networked at an accelerating pace. Along with this networking of social infrastructure, the cyber security threats that were once an issue only for corporate information systems have now emerged as a growing concern for all forms of social infrastructure. Since the appearance of the Stuxnet virus in 2010, in particular, persistent and sustained targeted attacks that combine a number of different methods and are directed at a specific organization have caused real damage.

In addition to countering these sophisticated cyber attacks while maintaining operation, social infrastructure systems must also be relied on to be capable of going to a safe state (such as a system shutdown) in the event of their becoming compromised. To achieve this, it is important to build in security functions from the development stage to prevent any deviation from predetermined state transitions due to a threat.

However, the nature of cyber attacks evolves on a daily basis and therefore it is essential for social infrastructure systems with long operating lives to take account of the emergence of threats that were not able to be considered in the initial design. This is making the security measures used during system operation more important. Another factor with social infrastructure systems is that devices installed in the field tend to have very limited system resources (in terms of their processing power or power consumption, for example), and this often complicates the task of implementing security measures.

This article describes Hitachi's approach to ensuring security along with its technologies for providing security measures that encompass all social infrastructure systems, and technologies that support safe and secure operation.

HITACHI'S APPROACH TO SECURITY—2×3 SECURITY GUARANTEE MODEL—

Ensuring the security of social infrastructure systems, particularly the control systems that form part of this infrastructure, requires both the incorporation of security functions at the development phase and the implementation of security measures during the operation phase. The 2×3 security guarantee model[1] provides the basic philosophy for achieving this.

The 2×3 security guarantee model is an approach to maintaining leak-proof security through measures for dealing with and countering threats at two phases of the system life cycle (development and operation) and considered from three different perspectives (functions, environment, and people and organizations) (see Fig. 1).

*1 Enocoro is an extension of development work conducted by the "Research and Development of Technology for Secure Distribution and Storage of Large Amounts of Data" (FY2005 to FY2007) sponsored by the National Institute of Information and Communications Technology. Enocoro is a trademark of Hitachi, Ltd.

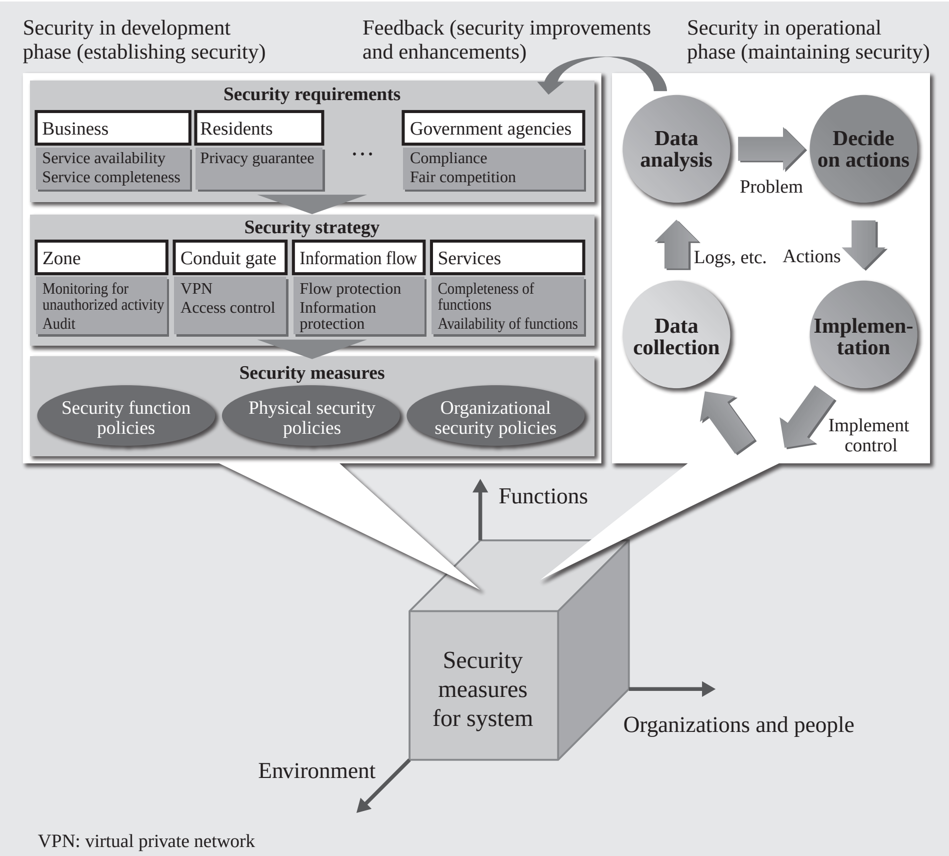


Fig. 1—2×3 Security Guarantee Model.
The model provides leak-proof security through measures for dealing with and countering threats in two phases (development and operation) and considered from three different perspectives (functions, environment, and people and organizations).

Security at Development Phase

The process for building security into systems at the development phase is to identify potential security threats, and then to combine a multi-layered mix of countermeasures ("defense in depth") considered in terms of the three perspectives (functions, environment, and people and organizations) that can be incorporated as part of the systems functions.

Based on security concepts defined in the International Electrotechnical Commission (IEC) standard IEC 62443[2], designing security functions that provide defense in depth requires that the system be divided up into a number of zones, each of which operates under its own security policies, and that the necessary security measures then be considered and implemented separately for each of these zones. By providing safe pipe connections ("conduits") between zones and implementing security measures at their entries and exits ("conduit gates"), this prevents unauthorized users from gaining access to a zone.

In addition to security measures based on this system configuration, Hitachi also believes that, for each service provided by social infrastructure systems, appropriate protections and other security measures are required for the integrity and availability of the functions that make up the service and the information flows between these functions, and therefore has produced security guidelines for their design, development, and implementation. These guidelines specify the implementation of security measures that are appropriate to the importance of the system and its customer requirements, and they comply with major Japanese and international security standards, including the Special Publications (SP) 800 series published by the US National Institute of Standards and Technology (NIST) and the IEC's IEC 62443 series.

Security at Operation Phase

The process at the operation phase is to assess the health of the system and respond rapidly to any problems that arise in order to maintain the security that was built in at the development phase.

As well as incorporating sufficient security functions at the development phase, the security measures in the operation phase are growing in importance for countering sophisticated modern cyber threats. To maintain the security that was built in at the development phase, the operation phase functions assess the security health of the system by collecting and analyzing data from many different points in the system. This allows them to quickly detect and counter any problems that arise. Information is also fed back from the operation to the development phase to enhance and strengthen security.

SECURITY TECHNOLOGIES ABLE TO COVER ALL CORNERS OF SOCIAL INFRASTRUCTURE

Countering sophisticated cyber threats requires security measures that extend to all corners of the social infrastructure.

However, social infrastructure systems are often constrained by very limited system resources in terms of factors such as processing power or power consumption.

To ensure that security measures can cover all corners of social infrastructure systems, Hitachi is developing encryption, authentication, and other techniques suitable for use on these resource-constrained devices.

Enocoro Low-power Stream Encryption

Enocoro is a low-power stream encryption technique developed in 2007. It was adopted in the ISO/IEC 29192 international standard for lightweight cryptography (encryption for small devices) in 2012[3].

One element in Enocoro encryption processing is the substitution box (S-box) that requires only half as many gates to implement as the advanced encryption standard (AES), and shortens the critical path to allow the use of low-power consumption logic cells (see Fig. 2).

As a result, Enocoro can execute data encryption with only about one-tenth the power consumption of AES, the de facto standard.

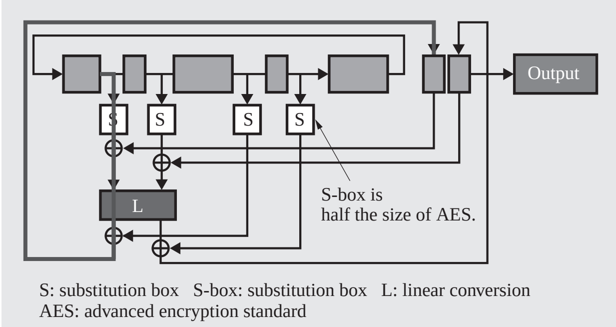


Fig. 2—Basic Configuration of Enocoro.
The S-box requires only half as many gates as AES and has a shorter critical path to allow use of low-power logic cells.

Lightweight Encryption Implementation

In addition to developing the lightweight algorithm described above, another important factor in implementing encrypted communications on devices with limited resources is technology that can provide a lightweight and fast implementation.

Hitachi has developed lightweight encryption technology that achieves high speed and low processing load by generating the random number string required for encryption in advance and limiting the scope of encryption to the minimum required (see Fig. 3).

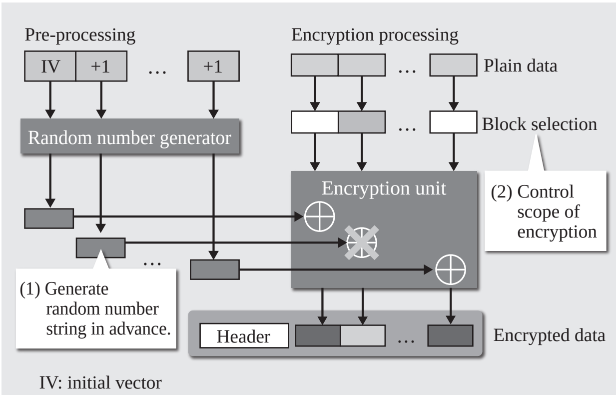


Fig. 3—Overview of Lightweight Encryption Implementation.
This technique achieves high speed and low processing load by generating the random number string required for encryption in advance and limiting the scope of encryption to the minimum required.

This technology is able to deliver approximately 20 times the speed of a standard implementation using AES. Specifically, because it can encrypt 1,500 bytes of data in approximately 40 μs, Hitachi's technology allows encrypted communications to be adopted in situations where it would have been considered impractical in the past due to the processing overhead being too high.

SECURITY TECHNIQUES FOR REDUCING LOAD ON SYSTEM OPERATION

The requirements for the system operation phase are to assess the state of system security and counter any problems that arise.

However, recent cyber attacks have adopted various techniques for covering up their activities and these make it very difficult to identify threats hiding inside the system.

Hitachi is working on the development of techniques that use concepts from applied mathematics to detect problems by analyzing large quantities of logs and communication data. Specific examples include ways of detecting computer viruses hiding inside the system, and evaluating the state of system security.

Analysis of Logs to Detect Unauthorized Communications

Computer viruses have certain characteristics that are different to conventional programs. For example, a virus might periodically connect to its command and control (C&C) server to transmit collected information or receive attack instructions.

In addition to analyzing the characteristics of such computer viruses, Hitachi is also developing techniques that use these characteristics as a basis for automatically identifying log entries that are suggestive of virus activity from the large quantities of log data output by the system. One example is a method Hitachi has developed that exploits this characteristic of periodically communicating with a C&C server, and that works by performing a frequency analysis of the log to find cases of automated access among the large volume of log entries (see Fig. 4).

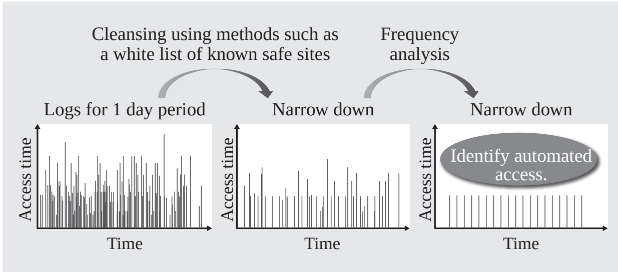


Fig. 4—Analysis of Logs to Detect Unauthorized Communications.
Given that a characteristic of computer viruses is that they periodically connect to a command and control (C&C) server, this technique performs a frequency analysis of log data to find cases of automated access among a large volume of log entries.

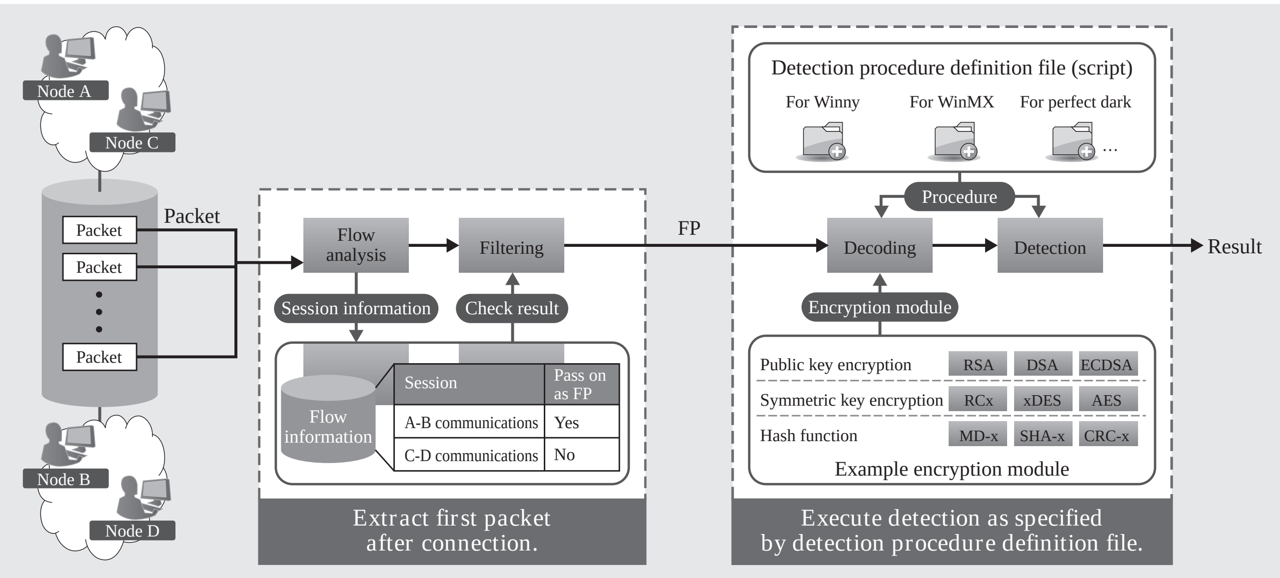
Use of Packet Analysis to Detect Unauthorized Communications

Along with log analysis, Hitachi is also developing techniques for detecting unauthorized communications that use deep packet inspection (DPI) to check the content of data packets.

An issue with DPI is that, because it often requires complex arithmetic processing, analyzing large quantities of data imposes a heavy processing load. Hitachi's technique overcomes this problem and is able to detect unauthorized communications on broadband networks in realtime by selectively narrowing down which of the packets passing over the network to analyze, and by performing its analysis in accordance with a detection procedure definition file.

Hitachi has applied the technique to the detection of communication by peer-to-peer (P2P) file sharing software[*2] and demonstrated that it can detect such traffic on a 10 Gbit/s network with a high level of accuracy (99.78%)[(4)] (see Fig. 5).

*2 This work was conducted as part of the "Research and Development on Detection and Prevention of Information Leakages through Computer Networks" research sponsored by the Ministry of Internal Affairs and Communications.



FP: fast packet RSA: Rivest Shamir Adleman DSA: digital signature algorithm ECDSA: elliptic curve digital signature algorithm
DES: data encryption standard MD: message digest SHA: secure hash algorithm CRC: cyclic redundancy check

Fig. 5—Use of Packet Analysis to Detect P2P Communications.
Peer-to-peer (P2P) communications can be detected with a high level of accuracy by selectively narrowing down which packets to check, and then decoding the selected packets and analyzing their content.

Evaluation of State of System Security*3

The larger systems get, the more they experience all sorts of different events on a daily basis. This makes it increasingly difficult for system operators to correctly assess and respond to the security implications of each event.

Hitachi is developing technology for evaluating the state of security in large systems such as those used in social infrastructure by considering the events that occur in the system in terms of how they impact the security performance as envisaged at the design stage(5).

Specifically, the technology estimates and displays the state of security based on the level of impact of events that occur in the system. A security incident such as an information leak, for example, would be interpreted as a case in which the designed security performance (keeping particular information private) was unable to be maintained.

Evaluating the state of security not only provides operators with early notification of warning signs, it also identifies which of the many such signs have the potential to lead to serious consequences.

*3 This technology incorporates results from the "Research and Development of Security Technology for Encouraging Migration to Cloud to Improve Disaster Readiness" research sponsored by the Ministry of Internal Affairs and Communications.

CONCLUSIONS

This article has described Hitachi's approach to ensuring security along with its technologies for providing security measures that encompass all social infrastructure systems, and technologies that support safe and secure operation.

In the future Hitachi intends to contribute to providing safe social infrastructure that everyone can use with confidence by continuing to research and develop security technologies for countering the ever-evolving threats.

REFERENCES

(1) H. Endo, "HITACHI Security Concept for Industrial Control Systems," 33rd Annual Conference of the Canadian Nuclear Society (CNS2012) (Jan. 2012).

(2) "IEC 62443-2-1: Industrial Communication Networks - Network and System Security - Part 2-1: Establishing an Industrial Automation and Control System Security Program" (Nov. 2010).

(3) "IEC-News Release: IEC and ISO Adopt Lower Power Encryption Standard Enocoro Stream Cipher" (Nov. 2012), http://www.iec.ch/newslog/2012/nr1912.htm

(4) Hitachi News Release, "Development of Software for Detecting P2P File Sharing Traffic on 10-Gbit/s Broadband" (Jul. 2010), http://www.hitachi.co.jp/New/cnews/month/2010/07/0701.html in Japanese.

(5) S. Kai et al., "Development of Qualification of Security Status Suitable for Cloud Computing System," MetriSec '12 Proceedings of the 4th International Workshop on Security Measurements and Metrics, pp. 17–24 (Sep. 2012).

ABOUT THE AUTHORS

Tadashi Kaji, Dr. Info.

Joined Hitachi, Ltd. in 1996, and now works at the Enterprise Systems Research Department, Yokohama Research Laboratory. He is currently engaged in the research and development of information security technology. Dr. Kaji is a member of the IEEE Computer Society.

Tsutomu Yamada

Joined Hitachi, Ltd. in 1994, and now works at the Department of Energy Management Systems Research, Hitachi Research Laboratory. He is currently engaged in the research and development of embedded computer and network architectures, and control system security. Mr. Yamada is a member of the IEEE, International Society of Automation (ISA), The Institute of Electronics, Information and Communication Engineers (IEICE), and The Society of Instrument and Control Engineers (SICE).

Toshihiko Nakano, Dr. Eng.

Joined Hitachi, Ltd. in 1980, and now works at the Control System Security Center, Infrastructure Systems Company. He is currently engaged in the development of security for social infrastructure systems. Dr. Nakano is a member of The Institute of Electrical Engineers of Japan (IEEJ).

Susumu Serita

Joined Hitachi, Ltd. in 2007, and now works at the Service Innovation Research Department, Yokohama Research Laboratory. He is currently engaged in the research and development of security technologies for the use of big data.