Featured Articles

Trends in Cybersecurity and Latest Countermeasures

Satoshi Takemoto
Makoto Kayashima, Ph.D.
Kunihiko Miyazaki, Ph.D.
Yasuko Fukuzawa, Ph.D.

OVERVIEW: For the IT systems that underpin social infrastructure, advances are taking place in the fields of information systems, industrial control systems, and cyber-physical systems that are based on the high-level integration of these information and control systems. On the other hand, unauthorized access is becoming increasingly sophisticated and extensive, with even industrial control systems that were once considered secure against these threats now being exposed to serious cyber-attacks. Hitachi supplies a comprehensive range of cybersecurity, including information security solutions provided by Hitachi and managed security services, security for industrial control systems that is also intended for cyber-physical systems, incident response by Hitachi Incident Response Team, and malware analysis for preventing targeted attacks and other evolving threats. Hitachi is also working on advanced research and development aimed at ensuring safe and secure social infrastructure.

INTRODUCTION

IN recent years, there have been rapid advances in information technology (IT) systems, particularly in the fields of cloud computing and mobile digital devices, therefore cybersecurity technologies are playing an increasingly important role. While the spread of cloud computing is bringing benefits such as the on-demand availability of extensive resources, there are concerns such as data leaks or unauthorized access by cloud system administrators. In the case of cyber-physical systems that combine information and control systems, while these are opening up the prospect of new social infrastructure developments such as smart grids or smart cities, cyber-attacks on industrial control systems that were once considered secure against these threats are revealed. Reported examples include the Stuxnet malware that infiltrates industrial control systems and causes control devices to behave abnormally, and unauthorized access to automotive embedded systems, medical devices, or other equipment that poses a risk to human life. One way of going about this has been the use of social engineering whereby attacks take advantage of people's psychological vulnerabilities or mistakes to inflict damage.

Meanwhile, supply chains being established for things like parts procurement or the development of IT systems and the products used to build them are increasingly taking advantage of open technologies and commercial off-the-shelf products, and of trends such as globalization. This raises the problem of how to ensure security throughout the supply chain when the development and management related to security is performed by both local and overseas suppliers.

Given these developments, Hitachi is working to supply comprehensive services, products, and technologies related to cybersecurity. Specific examples include information security solutions provided by Hitachi[(1)], which supply products ranging from consulting to security measures and operational services; a managed security service; security for industrial control systems that is also intended for cyber-physical systems; incident response and countermeasures against the vulnerabilities of products and solutions by the Hitachi Incident Response Team (HIRT); and multi-environment dynamic analysis systems for the automatic analysis of environment-dependent malware (please refer to other Hitachi publications for more information about these).

This article describes advanced research and development being undertaken with a view to its use in security services and products supplied by Hitachi, including a security verification technique that uses formal methods, technologies for implementing secure cloud computing environments, and security evaluation techniques for embedded systems.

SECURITY VERIFICATION TECHNIQUE USING FORMAL METHODS

Formal methods are techniques based on mathematical logic that are used to mechanically verify that programs or other specifications do not contain defects or inconsistencies. There is particular interest in formal methods in fields that require high levels of safety and reliability, with their use in development recommended by international standards in industries such as aviation, railways, or automobiles, for example. Hitachi's involvement in the field includes the release of software[(2)] that supports the efficient use of formal methods, and research and development of formal verification techniques for automotive control software[(3)].

A feature of formal methods is their ability to demonstrate comprehensively that no defects are present within a particular scope. This makes the technique valuable for security verification where there is a need to guarantee safety even under conditions where it is not known what sort of people will attempt an attack. A typical example of a security verification technique that uses formal methods would be one used to verify the safety of a cryptographic protocol.

Cryptographic protocols provide a way of establishing secure communication by combining a variety of cryptographic functions (including encryption and electronic signatures). Examples include Transport Layer Security (TLS) and the Security Architecture for the Internet Protocol (IPsec). These play an essential role in maintaining the security of Internet and various other communications.

Verifying that a cryptographic protocol is secure is not easy. While the individual cryptographic functions (components) that make up the protocol must themselves be secure, this on its own is insufficient.

The following shows the procedure for the Needham–Schroeder public-key protocol for sharing keys.

(1) A → B: $\{Na, A\}_{Kb}$
(2) B → A: $\{Na, Nb\}_{Ka}$
(3) A → B: $\{Nb\}_{Kb}$

Here, N*x* is a random number generated by agent X, K*x* is the public key belonging to X, and $\{\cdot\}_{Kx}$ means to encrypt the data enclosed in parentheses using K*x*.

Executing the protocol using this procedure results in the secret exchange of keys Na and Nb between A and B. This protocol had been believed to be secure for nearly 20 years after it was first proposed in 1978. In 1996, however, Gavin Lowe found that a man-in-the-middle attack involving someone intercepting the communications between A and B could discover Na and Nb. This attack could be achieved without breaking the $\{\cdot\}_{Kx}$ encryption function used as a component of the protocol.

Even for a comparatively simple specification like this one, the difficulty of verifying the security of the protocol arises because it operates in parallel between a number of agents and in a non-deterministic way. It is typically difficult to check all possible situations without overlooking or omitting any.

In his research into the above attack, Lowe used a formal method tool (model checker) called failures-divergence refinement (FDR) to confirm the attack and verify the security of the updated protocol. A number of verification methods and tools based on formal methods such as model checking and theorem proving have been developed or proposed, and work is progressing on assessing the security of protocols in actual use such as WiMAX[*1] or European standards for railway communications.

Meanwhile, the interrelationships between verification methods and tools for cryptographic protocols that use these formal methods are not always well understood, and it has not been clear how the results of assessment should be interpreted in practice.

In response, Hitachi has since 2006 been involved in the international standardization of security assessment for cryptographic protocols. As a result of Hitachi's work as project editor of ISO/IEC JTC 1/SC 27/WG 3 in conjunction with partners such as the National Institute of Information and Communications Technology (NICT) and the National Institute of Advanced Industrial Science and Technology (AIST), the ISO/IEC 29128 standard (Verification of Cryptographic Protocols) was published in 2011. This standard specifies the common items required to be described when assessing a protocol (the protocol specification, intruder model, security requirements, and self-assessment). It also defines four protocol assurance levels (PALs) that indicate the degree of verification: PAL1 (informal argument), PAL2 (formal paper-and-pencil proof), PAL3 (tool-aided bounded verification), and PAL4 (tool-aided unbounded verification).

In December 2013, NICT, Hitachi, Ltd., KDDI R&D Laboratories, Inc., and Nippon Telegraph and Telephone Corporation (NTT) established the

*1 WiMAX is a trademark or registered trademark of the WiMAX Forum.

"Cryptographic Protocol Evaluation toward Long-lived Outstanding Security" (CELLOS) consortium for cryptographic protocol evaluation technology[4]. The consortium aims to encourage the wider adoption of secure cryptographic protocols through the international collection and dissemination of reliable information on the security of cryptographic protocols, discussion about information and communication technology (ICT) systems, and the publishing of security information resulting from these activities. This will include participation by universities, research institutions, and interested companies from Japan and other countries so that activities can be undertaken through an international cooperative framework that extends beyond Japan.

TECHNIQUES FOR IMPLEMENTING SECURE CLOUD COMPUTING ENVIRONMENTS

The use of cloud computing provides numerous benefits, including on-demand access to extensive resources. However, because users who store their data in the cloud are not able to check the cloud systems themselves, they need some other way to protect against information leaks due to people (including possibly system administrators) accessing their data without authorization. In response, Hitachi is researching and developing technologies based on encrypted data such as electronic signatures using biometric data and privacy-preserving information processing.

Electronic Signature Technology Using Biometric Data

Conventional authentication enhanced techniques have included the use of hardware tokens such as smartcards and the use of public key infrastructure (PKI). While these help improve security, there are problems in terms of inconvenience and of poor cost-benefit. Another problem with the conventional techniques is that they have used anti-tampering devices such as smartcards or have been based on a centralized model that requires strict management of authentication data. In response, Hitachi has developed a public biometrics infrastructure (PBI)[5] that uses public templates*2. PBI works by converting the biometric templates into a form from which the original data cannot be recovered, thereby making it secure for the data to be published without risk to privacy, but still allowing it to be used for purposes such as authentication or electronic signatures (see Fig. 1).

*2 This technology incorporates results from the "R&D on Cloud Security Technologies for Disaster Preparedness and Emergency Response" project sponsored by the Ministry of Internal Affairs and Communications.

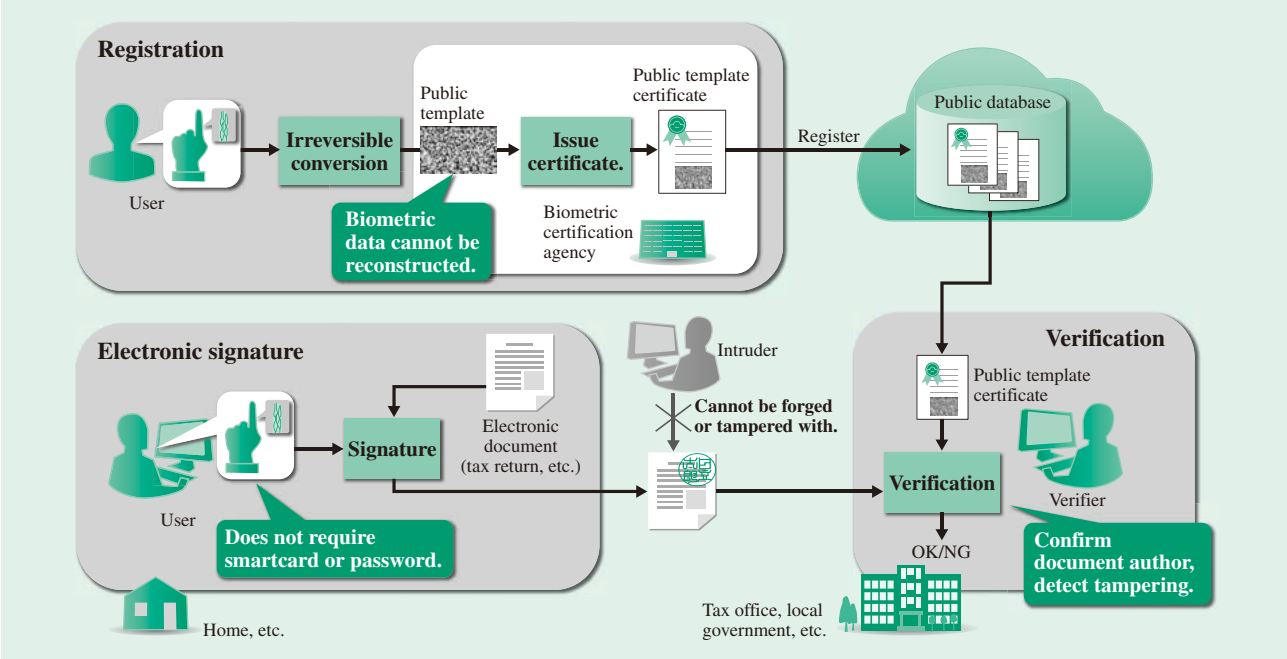

Fig. 1—Biometric Authentication Platform with Public Templates.
The platform facilitates the migration of payment, e-government, and other systems that require strict user authentication to the cloud, and the linking of identities (IDs) across other related systems at low cost.

Using a new electronic signature scheme that tolerates errors in the private key, PBI can verify (authenticate) a signature using error correction and an appropriate threshold setting provided the error in the analog data that is invariably generated each time the biometric data is retrieved is within a given range. Because it is not possible to recover the original biometric data from the public key (public template) used to verify the electronic signature, anyone can perform signature verification (authentication) without risk of the biometric data being leaked or forged. Furthermore, by reducing the security of the newly developed scheme to that of the Waters signature*3 scheme, the security of which has already been proved mathematically, it has been proven that the Hitachi scheme cannot be broken by any form of attack.

Use of this scheme makes it possible to implement systems that require strict user authentication (such as payment or e-government systems) on the cloud, and to link identities (IDs) across other related systems at low cost.

Technologies for Privacy-preserving Information Processing

Data encryption has commonly been used to ensure the confidentiality of the data used by a system. However, because the data needs to be decrypted for use, this provides an opportunity for system administrators, malware, or others to read the data.

To minimize this risk, Hitachi has developed an encryption technique[6] that supports fast searching*4 (see Fig. 2). The technique achieves efficiency based on common-key encryption, and ensures high security that allows comparisons of encrypted data to be performed using homomorphic encryption.

Hitachi has also utilized this technique to develop and commercialize a privacy-preserving analysis technique[7] that can obtain the frequencies with which a number of keywords appear in an encrypted database, and then compare these to find correlation rules.

SECURITY EVALUATION TECHNIQUES FOR AUTOMOTIVE EMBEDDED SYSTEMS

In recent years, networks, devices, operating systems (OSs), and other components that are widely used in IT have also started to find uses in automotive and other embedded systems. Accordingly, the importance of countermeasures against cyber-attacks is also growing in this field. Examples have already been demonstrated in which automotive embedded systems are manipulated remotely via a network. Because attacks on vehicles have the potential to put human life at risk, there is a need to offer automotive security at an early stage.

In Europe, which has led the way in the study of automotive security, the 7th Framework Programme for Research and Technological Development (FP7) has proposed standards for hardware security modules (HSMs) and has also embarked on an investigation into the security evaluation in automotive embedded systems that incorporate HSMs.

*3 A digital signature scheme proposed by Brent Waters in 2005. The scheme has been shown to fulfill the requirements of EUF-CMA (probability of existentially unforgeable under chosen-message attacks), a widely accepted definition of the security of electronic signature schemes, under the Computational Diffie-Hellman (CDH) assumption (a mathematical assumption).

*4 This technology incorporates results from the "R&D on Cloud Security Technologies for Disaster Preparedness and Emergency Response" project sponsored by the Ministry of Internal Affairs and Communications.

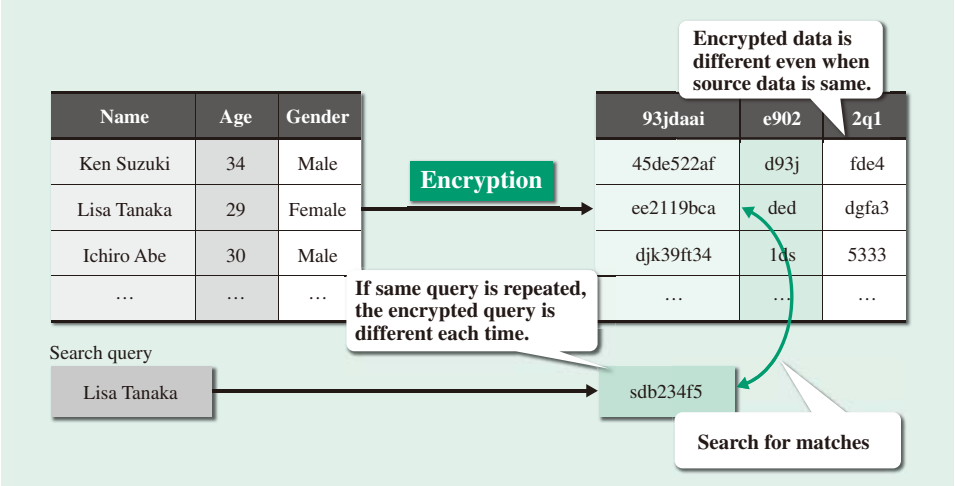

Fig. 2—Features of Searchable Encryption Technique. The technique combines common-key encryption and homomorphic encryption to achieve both high speed and security.

Accordingly, Hitachi has applied security evaluation techniques based on the safety analysis techniques for plants it developed during the 1980s to automotive embedded systems. In Japan, Hitachi is participating in the standardization of security evaluation techniques and has proposed methods for threat analysis and risk assessment.

The following sections describe the threat analysis and risk assessment methods that form the core of these security evaluation techniques for embedded systems for vehicles.

Definition of Target System of Evaluation

Security threats can be described in terms of, "which threat agents exist, and what adverse action they perform on which assets" in the target system of evaluation.

In addition to information, which has conventionally been treated as an asset to be protected, the assets in automotive embedded systems also include embedded system firmware and the functions that control mechanisms such as the engine or brakes. A system model is produced from the nature of the assets and from data flow diagrams that specify data flows in relation to these assets.

The threat agents are those people involved at any point along the lifecycle of a vehicle, which includes its manufacture, its use by the owners who purchased the vehicle new or second-hand, and ultimately its disposal. This is because confidential information held by automotive embedded systems is stored and accessed not only during the normal usage phase but also at other phases such as during manufacturing, delivery, or servicing.

With respect to what adverse actions are performed (the threats), all of the things that can happen for each entry point are studied, and are also considered in terms of types of failure called confidentiality, integrity, or availability that can occur for each type of asset. For example, it is important that the functions of an automotive IT system operate as correctly as expected, and failure of integrity or availability must be prevented. Similarly, it is important that the information exchanged between central servers and vehicle-mounted intelligent transport system (ITS) devices is protected from disclosure and modification, and failure of confidentiality or integrity must also be prevented.

Identification of Threats

For the target of evaluation, the threats are identified from four perspectives (see Table 1).

By applying to these perspectives, the system model, lifecycle, and adverse actions, which are studied in defining the target system of evaluation described in the previous section, it can be exhaustively identified what threat agents exist and what adverse action they perform on which assets at what phases.

Risk Assessment

The risk that threats pose to an IT system has been typically assessed by deriving from the value of the assets and the attack cost, which depends on how the threats are carried out. This is an effective approach when there are numerous examples of attacks, and a consensus can be reached about the cost of the attack method, including factors such as the execution time needed to undertake the attack and the capabilities of the person launching it.

In the case of automotive embedded systems, while a number of example attacks have been identified at the research level, there is not the same wide range of attack method variations that exist for IT systems. As a consequence, we consider that it is difficult to estimate the cost of attack methods. Therefore, Hitachi has developed a threat risk assessment method that is based on the common vulnerability scoring system (CVSS) used to score the severity of IT system vulnerabilities.

This method assigns an asset value to each asset in terms of confidentiality, integrity, and availability and then it calculates a score for risk from the degree of ease in mounting an attack, which is derived from the metric that reflects how close the threat agents need to get to the assets and from the existence of barriers that they break through to access to them. Even in cases such as automotive embedded systems where there is a lack of accumulated know-how about security threats, the method can calculate a risk value analytically from the definitions of the threats and the system of evaluation. It can also incorporate consideration of factors such as risk to life into the risk assessment by treating functions as assets and, for the purpose of

Table 1. Perspectives for Identification of Threats
The system model, lifecycle, and adverse actions, which are studied in defining the target system of evaluation, are applied to these perspectives.

Perspective	Explanation
Where	Identify entry points for attacks.
Who	Identify threat agents.
When	Identify lifecycle phases for attacks.
What	Identify adverse actions.

valuation, raising the estimated asset value in the case of functions for which loss of integrity or availability has serious consequences.

CONCLUSIONS

This article has described developments in the field of cybersecurity for the IT systems used to support social infrastructure, and advanced research and development being undertaken with reference to these.

In the future, Hitachi intends to continue contributing to the provision of safe and secure social infrastructure by supplying new security solutions and developing technologies for use in these solutions.

REFERENCES

(1) Hitachi Secureplaza Security Solution, http://www.hitachi.co.jp/Prod/comp/Secureplaza/index.html in Japanese.
(2) Hitachi News Releases, "Release of Highly Reliable and Efficient Software Development Technology for Social Infrastructure" (Feb. 2013), http://www.hitachi.com/New/cnews/130212a.html
(3) Hitachi News Releases, "Development of Highly Reliable Verification Technology for Automotive Control Software Using Formal Methods" (Apr. 2013), http://www.hitachi.co.jp/New/cnews/month/2013/04/0416a.html in Japanese.
(4) Hitachi News Releases, "Establishment of Cryptographic Protocol Evaluation Toward Long-Lived Outstanding Security (CELLOS) Consortium" (Dec. 2013), http://www.hitachi.com/New/cnews/131219b.html
(5) Hitachi News Releases, "Successful Development of Biometric Digital Signature Technology" (Feb. 2013), http://www.hitachi.com/New/cnews/130218.html
(6) Hitachi News Releases, "Searchable Encryption Technology Supporting the Prevention of Information Leakage on Cloud Systems" (Mar. 2012), http://www.hitachi.co.jp/New/cnews/month/2012/03/0312.html in Japanese.
(7) Hitachi News Releases, "Development of Privacy-preserving Analysis Technology for Analyzing Data in Encrypted Form" (Jan. 2014), http://www.hitachi.co.jp/New/cnews/month/2014/01/0121b.html in Japanese.

ABOUT THE AUTHORS

Satoshi Takemoto
Advanced Cybersecurity Technology Department, Advanced Security Technology Operations, Services Creation Division, Information & Telecommunication Systems Company, Hitachi, Ltd. He is currently engaged in the creation and launch of a new security business.

Makoto Kayashima, Ph.D.
Enterprise Systems Research Department, Yokohama Research Laboratory, Hitachi, Ltd. He is currently engaged in research on information security. Dr. Kayashima is a member of the Information Processing Society of Japan (IPSJ), The Institute of Electronics, Information and Communication Engineers (IEICE), and The Japanese Society for Artificial Intelligence.

Kunihiko Miyazaki, Ph.D.
Enterprise Systems Research Department, Yokohama Research Laboratory, Hitachi, Ltd. He is currently engaged in research on formal methods and information security. Dr. Miyazaki is a member of the IPSJ and the IEICE.

Yasuko Fukuzawa, Ph.D.
Enterprise Systems Research Department, Yokohama Research Laboratory, Hitachi, Ltd. She is currently engaged in research on information security and cryptography. Dr. Fukuzawa is a member of The Institute of Electrical Engineers of Japan (IEEJ), IPSJ, and IEICE.