

## Security Technologies to Support Evolution of Highly Sophisticated Information Society

## Realization of Cybersecurity Requiring Full-Scale Efforts

KAWAMURA Shinichi

## Toshiba's Approaches toward Information Security Technologies Enhancing Social Systems

AKIYAMA Koichiro / SHIMADA Tsuyoshi / SHIBA Masue

The expanding use of cloud-based services and the implementation of various demonstration experiments have been providing concrete directions for smart communities. The technologies essential for information security are shifting with the changes taking place in these contemporary social needs. In order to construct efficient communities, control systems for social infrastructures are inevitably being connected to the Internet. The protection of critical social infrastructures against cyberattacks has therefore become an issue of vital importance.

The Toshiba Group has been engaged in research and development aimed at realizing information security technologies to support safe and secure social systems through totally optimized management from endpoints including mobile terminals and sensors to control systems and cloud-based systems.

## Security Monitoring Technologies for Control Systems

KOJIMA Kenji / TOYAMA Haruhiko

Conventional control systems in the field of social infrastructure systems have been designed with a dedicated operating system and protocol, and connected to the related components via a local network. Security threats from external networks have consequently not been a strong focus of concern. Recently, however, security risks have been increasing and cyberattacks on such control systems have been reported, because versatile operating systems and protocols are being used to reduce costs and systems are being connected to other systems via the Internet to improve operating efficiency. At the same time, with the increase of targeted attacks in the field of information systems, security monitoring technologies have been attracting considerable attention as a new approach to the implementation of security countermeasures.

With the aim of realizing safe and secure social infrastructure systems, Toshiba and Toshiba Solutions Corporation are engaged in the development of security monitoring technologies for control systems.

## PDCA Cycles and Security Exercises to Improve Security of Control Systems for Industrial and Social Infrastructure Systems

KAMBAYASHI Toru / ITOH Satoshi

Accompanying the construction of smart grids as an important component of social infrastructures in recent years, there is a pressing demand to establish and improve cybersecurity to an adequate level for industrial control systems (ICSs) and control systems for social infrastructures connected to such smart grids. Plan-do-check-act (PDCA) cycles using cyberattack simulation tests such as security exercises are essential for this purpose.

Toshiba has been engaged in the establishment and improvement of PDCA cycles and security exercises for ICSs and control systems for social infrastructures. As an association member of the Control System Security Center (CSSC) established through industry-government-academia cooperation, we are now developing and constructing a security exercise system as an important step in PDCA cycles for the security management of ICSs and control systems for social infrastructures.

## Group Key Management Technology for Machine-to-Machine Communication Systems

HANATANI Yoshikazu / KAMBAYASHI Toru / OHBA Yoshihiro

Toshiba has been engaged in the research and development of technologies for machine-to-machine (M2M) communication systems that can organically connect various types of M2M devices including smart meters by means of the Internet Protocol (IP). To construct a large-scale M2M communication system consisting of more than 1,000 M2M devices, a group communication technology to maintain interoperability among multiple vendors' products is essential.

With this as a background, we have been participating since 2012 in the Institute of Electrical and Electronics Engineers (IEEE) 802.21 Task Group d in order to provide an efficient and secure group key management system for large numbers of M2M devices, and are actively promoting the standardization of IEEE 802.21d as a key specification for M2M group communication.

## Implementation of Security Functions in Storage Devices

YAMAKAWA Teruji / ARAMAKI Yasuto / UMESAWA Kentaro

With the growing importance of information security, demand has been increasing for the implementation of appropriate security functions in storage devices such as hard disk drives (HDDs) and solid-state drives (SSDs) according to their applications. In the field of storage products for personal mobile devices, it is necessary to prevent unauthorized leakage of data in the event of loss or theft of a mobile device. In the field of storage products for enterprise use such as data center servers, on the other hand, it is necessary to provide quick and secure data erasing in the event of failure or at the time of disposal of HDDs and SSDs at low cost.

To fulfill these diverse requirements, Toshiba has been developing firmware common to both personal and enterprise storage products using libraries with the necessary security functions, and has also been making efforts to obtain third-party certifications based on a security validation program to certify the design and implementation of these security functions.

## Device Protection and Management Technology Promoting Use of Smart Mobile Devices in Business Environments

IKEDA Tatsuro / MORIJIRI Tomoaki / ABE Shingo

With the widespread diffusion of smart mobile devices including smartphones and tablets in recent years, the use of such devices in business environments has been rapidly increasing.

To provide enterprise-level security for smart mobile devices, Toshiba has developed a secure Android™ platform. Applying this secure platform, Toshiba Solutions Corporation has developed a device protection and management technology for these mobile devices in order to achieve security not only in normal usages, but also in various business environments including the use of tablets as point-of-sales (POS) terminals.

## LISTEE™ Secure Platform Software

KANAI Jun / ISOZAKI Hiroshi

The increase in embedded systems featuring a rich versatile operating system (OS) such as Linux® in recent years has been accompanied by an increased risk of vulnerability. Once security systems including the access control system are defeated through a vulnerability in the OS, information leakages and illegal operations may occur in the embedded system.

As a solution to this issue, Toshiba has developed a secure platform software called LISTEE™ to protect important processing systems and data when security systems are defeated. LISTEE™ can implement security applications separately from a rich versatile OS by means of a fast switching function between the OS and a security application, and also provides a secure update function. This software achieves a balance between enhancement of security and shortening of the development period for embedded systems by improving the security to a level comparable to that attained by hardware.

## Authentication Systems in Era of Cloud Computing and Role of Biometric Authentication Technologies

YAMADA Asahiko / Pakin OSOTKRAPHUN / NISHIMURA Akio

The introduction of loosely coupled systems has been accelerating with the wide dissemination of cloud computing in recent years. In the area of authentication systems, independent services as part of identity as a service (IDaaS) and pure authentication as a service (PaaS) have also been increasing. Although biometric authentication has come into widespread use for user-friendly authentication systems, the introduction of biometric authentication technologies into the Internet environment is hindered by several technical issues associated with information leakage.

To solve these problems, Toshiba Solutions Corporation has developed the Authentication Context for Biometrics (ACBio), a technology that allows biometric authentication to be securely used even in the Internet environment. This technology has been adopted as the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 24761 international standard. We have also launched a related product called ACBioMeister™. PaaS for biometric authentication is expected to be implemented by combining ACBioMeister™ with single sign-on (SSO) technologies.

## Secure Network Architecture Based on Quantum Key Distribution Technology

TANIZAWA Yoshimichi / TAKAHASHI Ririka

Quantum key distribution (QKD), which guarantees communication security based on the principles of quantum physics, is expected to be a vital technology supporting future secure networks.

Toshiba is engaged in the research and development of basic technologies for QKD, as well as network and system technologies using QKD technologies, as elemental technologies to enhance the security of practical network systems. To overcome the technical constraints of current QKD technologies, we have developed a number of technologies including a network in which multiple QKD devices are organized and modern network functionalities are implemented, safer QKD key relaying computer systems, protocols supporting multiple applications, and a routing mechanism for key sharing.

## Reliability Evaluation Technology to Provide Design Guideline for MONOS Type NAND Flash Memories

FUJII Shosuke / YASUDA Naoki

A metal-oxide-nitride-oxide-silicon (MONOS) type memory is under research and development as one of the next-generation NAND flash memory technologies. In order to achieve the practical use of MONOS type memories, high reliability is essential.

Toshiba has developed a novel reliability evaluation technology to provide a guideline for the design of highly reliable MONOS type memories. Using this technology, we have been clarifying the degradation mechanisms unique to MONOS type memories caused by the stress of program/erase cycle operations. As a result, we have demonstrated that interface-state generation, which is the origin of degradation due to cycle operations, has a strong correlation with the amount of charges flowing into the memory cell during erase operations, and that holes injected from the silicon (Si) substrate are the main cause of cycling degradation. We have also confirmed that enhancement of the electron current during erase operations through optimum design of the charge-trapping silicon nitride (SiN) layer is a promising solution to reduce cycling degradation.

## Effective Testing Technology for Sequence Control Programs Based on Coverage Criteria

MARUCHI Kohei / SHIN Hiromasa / YOSHIKAWA Susumu

A variety of social infrastructure systems have recently become ubiquitous in people's daily lives. High reliability of these systems is necessary to assure safety and security. Sequence control programs that can handle each step of control in a predetermined order are often used for the automatic control of these social infrastructure systems. Sufficient testing of such programs is therefore essential to achieve higher system reliability.

Toshiba has developed a new test coverage criterion for sequence control programs in order to confirm the correctness of sequence control programs used in power plants. As part of this study, we have also developed an automatic test generation technology that generates tests to satisfy coverage criteria. We have conducted evaluation experiments using actual power plant programs and confirmed the effectiveness of our newly developed criterion.

## Project Failure Risk Prediction Model for Software Development Projects

MORI Toshiaki / KAKUI Shingo / TAMURA Shurei

With the expanding scale and complexity of software development projects, quantitative project management has become increasingly important. However, conventional approaches based on a statistical model including multiple regression analysis and the Rayleigh model generally have limited applicability to actual software development data containing low-accuracy data, outliers, and missing values.

Toshiba has been constructing a new approach using a project failure risk prediction model based on the naïve Bayes classifier technique in order to manage the probability of nonachievement of objectives in a project. Trial application of this approach to actual software development projects in the social infrastructure field has confirmed that it achieves successful performance without being affected by low-accuracy data and missing values in software development data, and can sequentially renew predictions in accordance with data collected in each project phase.

## Newly Developed EY-5003 Ticket Issuing Machine Achieving Balance between Multifunctionality and Operability

OTOMO Yoko / YAMASHITA Yuki

A ticket issuing machine is a type of service equipment installed at each ticket window of a railway station that issues various types of railway tickets and can also process integrated circuit (IC) card railway tickets. In recent years, demand has been increasing for ticket issuing machines with higher performance and multifunctionality compared with conventional machines, in order to handle larger numbers of passengers and offer diversified services at the ticket window.

To meet these requirements, Toshiba has developed the new EY-5003 multifunctional ticket issuing machine offering significantly improved usability and performance in addition to the conventional functions. The EY-5003 makes it possible to increase the work efficiency of station attendants and satisfy various needs of passengers by issuing a wide assortment of tickets including commuter passes and event tickets.

## Integrated Big Data Platform for Optimal Use of Big Data in Various Fields

KURITA Masayoshi / HATTORI Masakazu / YOSHIMOTO Takehiro

In recent years, attention has been increasingly focused on big data in various fields including social infrastructure systems to identify new sources of value that can be obtained by the rapid analysis of changes in such data.

Toshiba Solutions Corporation has developed the "Integrated Big Data Platform," a fundamental technology to provide solutions realizing the optimal use of big data. This platform makes it possible to handle big data with greater efficiency and ease of use through data gathering, storage, processing, and analysis functions appropriate to the individual characteristics of big data.

Interface Control Technology to Reduce Interface Defects in SiO<sub>2</sub> Formed by Plasma-Enhanced Chemical Vapor Deposition