

## Information Security Technologies Supporting Social Infrastructures

Information Security Technologies for Realization of Safe and Secure Social Infrastructures  
KAMITAKE Takashi**Security Threats Surrounding Social Infrastructures and Toshiba Group's Approach to Information Security Technologies**

AKIYAMA Koichiro / ENDO Naoki / OKADA Koji

As cyberattacks on social infrastructures have transformed from a threat to a reality, information security technologies have become increasingly important in recent years to protect society overall as well as individuals and businesses.

Since the early 1980s, the Toshiba Group has been engaged in the research and development of information security technologies, including cryptographic technologies, software protection technologies, and security analysis technologies, to protect a large number of products. These core component technologies are currently embedded in server environments, client environments, and information networks connecting these environments, which form the basis of many social infrastructures, and are being applied to advanced systems such as smart grids.

**Cybersecurity Technologies for Smart Grids**

ITO Satoshi / SHIMADA Tsuyoshi / KANDA Mitsuru

Efforts for the development and standardization of cybersecurity technologies for smart grids are currently being actively promoted in various countries. It is necessary to establish adequate cybersecurity considering smart grids as large-scale cyber-physical systems.

The Toshiba Group has been developing a smart grid security architecture, which divides the whole system into subsystems based on security characteristics to simplify security requirements and defines essential security components. We are also engaged in the research and development of practical applications for Advanced Metering Infrastructure (AMI) security.

**SecureSI™ Secure System Development Methodology for Information Systems of Smart Communities**

ODAHARA Ikuya / KOJIMA Kenji

Smart communities, which represent the next-generation social infrastructure system, have been attracting considerable attention as a solution for the optimization of energy use efficiency. A smart community system, consisting of both information systems and control systems, offers information visualization based on data collected by various sensors and controls equipment so as to optimize the community. It is therefore necessary to protect such systems against new types of security threats resulting from different requirements, such as the priority given to data confidentiality in information systems versus the priority given to availability of services in control systems.

In response to this situation, Toshiba Solutions Corporation has been developing SecureSI™, a secure system development methodology for information systems taking the characteristics of smart community systems into consideration.

**Field Test of High-Speed Quantum Key Distribution Prototype**

James DYNES / Zhiliang YUAN / Andrew J. SHIELDS

Toshiba has developed a high-bit-rate, actively stabilized, and continuously operating quantum key distribution (QKD) system for securing communication networks. This key distribution technology is based on the laws of physics to guarantee security from any attack, and can secure information exchanges in both today's and tomorrow's network infrastructure.

The newly developed QKD system has been robustly field tested on installed fiber in the Tokyo metropolitan area. Other QKD vendors supplied systems to operate over other links in the network. Thanks to an active stabilization technique, the Toshiba QKD system performed stably and continuously with a secure bit rate of 0.3 Mbit/s averaged over a 24-hour period. This high and stable secure bit rate opens the door to the realization of unconditionally secret communications with unparalleled bandwidths.

**Proxy Re-encryption Scheme for Secure Data Sharing in Cloud Services**

YOSHIDA Takuya / MATSUSHITA Tatsuyuki

A proxy re-encryption (PRE) scheme is a type of public-key cryptography that allows a proxy to convert a ciphertext encrypted for a user (delegator) into that for another user (delegatee) without revealing any information to the proxy by using a re-encryption key generated by the delegator. With the wide dissemination of cloud computing in recent years, the PRE scheme is attracting increasing attention as a key security component for the realization of secure data sharing in cloud services.

Toshiba Solutions Corporation and Toshiba Corporation have developed a new PRE scheme with higher security compared with previous schemes. Experiments on a prototype PRE system have confirmed that its performance is sufficient for practical application.

**Security Technology to Protect Device Platforms from Malicious Web Applications**

ISOZAKI Hiroshi / KANAI Jun / KOIKE Ryuiti

In recent software development, the Android™ platform has been increasingly attracting attention as a total ecosystem including an application execution platform and an application distribution platform. While the Android platform has basic security features, there are not enough key security features from the viewpoint of device manufacturers. In particular, it is necessary to implement an access control mechanism that restricts access from Web applications to device-specific functions, in consideration of the architecture where Web applications access device-specific functions provided as browser plug-ins. To solve this issue, Toshiba has developed an access control technology that allows Web applications to control access to device specific functions. This access control mechanism not only makes it possible to easily and effectively introduce existing Web platforms including the Android platform, but also allows application developers to develop Web applications under their existing development environment.

**DFITS™ Technology Supporting Secure Software Development Based on Data Flow Analysis**

HAYASHI Ryotaro / NAKANISHI Fukutomo / HASHIMOTO Mikio

There have recently been many incidents involving unauthorized release of confidential data such as personal information from illegally analyzed software installed in PCs and information terminals. Demand is therefore increasing for technologies to develop secure software with enhanced protection against such threats.

Toshiba has developed DFITS™ (Data Flow Isolation Technology for Security), a technology that supports the development of software more securely and efficiently by automatically performing static analysis of the source code of software and classifying confidential data in the software.

**Built-in Determined Sub-Key Correlation Power Analysis for Efficient Security Evaluation of Tamper-Resistant Cryptographic Modules**

KOMANO Yuichi / SHIMIZU Hideo / KAWAMURA Shinichi

Tamper-resistance techniques are required to protect cryptographic modules against the extraction of secret keys and the conversion of functions.

Toshiba has developed BS-CPA (built-in determined sub-key correlation power analysis), which makes it possible to rapidly evaluate the security of cryptographic modules early in the development process for devices such as integrated circuit (IC) cards and so on. BS-CPA can reduce the impact of process retrogression and decrease device costs through efficient detection of the vulnerability of cryptographic modules.

**Document Management Technologies to Control Distribution of Duplicates and Trace Withdrawal, Disposal, and Reuse**

MIYAZAKI Shingo / MORIJIRI Tomoaki / OGURA Kazuhiro

In an organization, it is necessary for everyone concerned to use the latest versions of business information such as operating manuals, procedures, specifications, and so on, and to strictly control confidential information such as customer information lists, etc. As these documents are updated from time to time, and are copied to various types of media including paper and media for recording digital data, they become widely dispersed throughout the workplace. However, improper usage of such information can lead to business issues, cause violations of laws, and inflict serious damage on the business and society.

In order to strengthen information management and security, Toshiba Solutions Corporation has developed inforester™, an information management system that can control and manage the distribution of various duplicated media by recording their status when they are withdrawn, disposed of, or reused. Furthermore, Toshiba TEC Corporation has developed the ECO-MFP system consisting of multifunctional peripherals with erasable toner and erasing equipment. Through the collaboration of inforester™ and the ECO-MFP system, we are also offering a new document control and management system that facilitates the withdrawal and disposal of paper documents depending on the degree of confidentiality and allows efficient reuse of paper.

**Spin-MOSFET Technologies for Realization of Advanced Memories and Logic ICs**

INOKUCHI Tomoaki / TANAMOTO Tetsufumi / SAITO Yoshiaki

In order to realize memories and logic integrated circuits (ICs) with low power consumption for advanced information and telecommunications equipment, mobile terminals, digital home appliances, and so on, the creation of high-value-added devices through innovative technologies based on new operating principles is required.

Toshiba has developed a spin-transfer-torque-switching metal-oxide-semiconductor field-effect transistor (STS-MOSFET), which is a novel spintronic device integrating memory and transistor functions that offers great potential for future advanced memories and logic ICs. Experiments on a prototype STS-MOSFET confirmed that it achieves clear read and excellent write characteristics with an endurance exceeding  $10^5$  cycles. Large-scale circuit simulations for various field-programmable gate arrays (FPGAs) also demonstrated that the critical path delay is significantly improved by using the STS-MOSFET.

**Analog Circuit Technology for Realization of Millimeter-Wave Near-Field High-Speed Wireless Communication**

HOSOYA Masahiro / WATANABE Osamu

With the ongoing reductions in the cost of storage devices such as hard disk drives and NAND flash memories in recent years, large volumes of data including high-definition videos and pictures are being handled by consumer electronics (CE) products. Expectations are also rising for the easy exchange of large volumes of data between CE products using millimeter-wave (MMW) near-field high-speed wireless communication. The integration of energy-efficient radio frequency and analog circuits on a single chip by means of complementary metal-oxide semiconductor (CMOS) technology is essential to realize a low-cost integrated circuit (IC) offering a high-speed interface with low power consumption.

Toshiba has developed a wide-bandwidth analog baseband (ABB) block with digitally controlled architecture for the realization of MMW near-field high-speed wireless communication.

**Requirement Analysis Method for Reduction of Energy Consumption of Electronic Appliances**

ANDO Takanobu / NAKAZATO Ryu / FUKAYA Tetsuji

Although energy saving is a serious issue for many electronic appliances, it is difficult to strike a balance between energy consumption and functionality or performance, which affect user satisfaction, as well as between energy consumption and development cost. As a solution to this issue, it is necessary to implement sufficient requirement analysis in the upstream processes of electronic appliance development.

Toshiba has developed a requirement analysis method to reduce the energy consumption of electronic appliances without degrading user satisfaction and overrunning development costs. This method provides the optimal plan of requirements through the following processes: (1) creation of requirement candidates; (2) estimation of the effectiveness of energy consumption, the resultant impact on user satisfaction, and the development cost; and (3) selection of requirements.

**High-Speed REGZA™ EPG and REGZA Menu: New GUI Applications of REGZA LCD TVs Powered by REGZA Engine CEVO™**

MURAMATSU Takamichi

With the growing diversity of features of digital liquid crystal display (LCD) TVs in recent years, further functionalities including network applications and the recording of broadcast programs are required in addition to the capability to handle high-definition (HD) images. To meet these requirements, high-performance hardware platforms have become necessary along with software platforms that can take advantage of these hardware platforms.

Toshiba has newly developed the REGZA Engine CEVO as a platform for incorporation into digital LCD TVs in the domestic Japanese market. This platform offers not only HD images but also two newly developed graphical user interface (GUI) applications, the High-Speed REGZA EPG (electronic program guide) and the REGZA Menu, contributing to user-friendly operation.

**SCiB™ Battery Modules for Electric Vehicles**

MIYAMOTO Hidenori / ENOMOTO Takashi / KOSUGI Shinichiro

Electric vehicles (EVs), which release no carbon dioxide into the air and whose batteries can be recharged during driving, are a focus of rising expectations as a means of reducing the burden on the environment. Lithium-ion batteries (LIBs) have recently begun to be installed in EVs due to their high energy density and reduced size and weight.

Toshiba has developed two types of battery modules for EVs applying SCiB™ battery cells, which provide excellent

input/output characteristics, intrinsic safety, superior lifetime, and good performance even in low-temperature environments. SCiB™ battery modules are installed in the i-MiEV M grade EV produced by Mitsubishi Motors Corporation.

These SCiB™ battery modules make it possible to offer the following performance for practical EV applications: (1) sufficient acceleration and driving performance due to the good input/output characteristics, even with a capacity of 10.5 kWh; (2) a mileage of 120 km per single charge (JC08 mode); and (3) excellent fast charging performance, with charging up to 80% of capacity possible in 15 minutes.

**Dual-Stage Actuator for HDD Achieving High-Accuracy Positioning and Wide-Bandwidth Servo Control**

SASAKI Yasutaka / HARA Takeyori

In the latest hard disk drives (HDDs), advanced high-performance technologies for the actuator and servo control are required in order to achieve not only accurate positioning control on data tracks with a pitch of less than 100 nm but also high-speed access onto another data track within a few microseconds.

To realize higher recording density of HDDs, Toshiba has developed a prototype dual-stage actuator (DSA) with piezoelectric elements (Pb [Zr, Ti] O<sub>3</sub>: PZT) attached to the suspension. Experiments on the prototype DSA confirmed that it achieves an improvement of about 30% in positioning accuracy and about 1.7 times wider servo bandwidth compared with conventional single-stage actuators (SSAs).

Nanocontact Magnetoresistance Element for Realization of 2.5 Tbit/in<sup>2</sup>-Class Hard Disk Drives

Technology for and Trends in Standardization of BLUETOOTH® low energy