TOSHIBA REVIEW

2007. VOL.62 NO.7

Special Reports

Information Security Technologies

Evolving Information Security Technologies
OCHIAI Masao

Toshiba Group's Efforts in Information Security Technology Field
YAMADA Asahiko/SHIMBO Atsushi/KITAORI Shoji
Information security technologies are an increasingly critical element of information technology for the protection of information. As information security technologies become more widespread, an important issue is how securely they are designed and implemented. In line with these trends, the Toshiba Group is working on the development of secure implementation methodologies for system integration, the application of information security technologies to various products including digital contents protection, and next-generation fundamental technologies. Our aim in these development activities is to contribute to the improvement of people's lives.

SecureSI$_{TM}$ Innovative System Integrator and Its Application to Retail Solutions
NISHI Mayumi/YAMADA Tatsuya/ODAHARA Ikuya
Toshiba Solutions Corporation has developed SecureSI$_{TM}$, an innovative system integrator that materializes our security design methodology to the procedures level in order to ease the rapidly growing demand for security engineers. We are promoting the extensive application of SecureSI$_{TM}$ to our solutions development in parallel with the reinforcement of security engineers' capabilities. For example, we have applied SecureSI$_{TM}$ to the development of a "point service system for customers," one of our retail solutions, and have successfully drawn up and systematically deployed security measures for the system taking customers' proposals into consideration. The security threat analysis was carried out by a systems development engineer who was not greatly experienced in security engineering but was significantly assisted by SecureSI$_{TM}$.

Content Protection Technology Applied to HD DVD
KATO Taku/ISOZAKI Hiroshi/ISHIHARA Atsushi
HD DVD, the "next-generation DVD," offers new experiences to users including high-definition video contents and interactive contents. However, the importance of content protection technology has increased. For this reason, a new content protection technology called the advanced access content system (AACS) has been developed.
AACS has been adopted for HD DVD players and recorders and is expected to be widely used in many types of devices and media. This technology contains a number of security protection elements to assist content providers. It can be applied not only to contents stored on media but also to networking technologies.

MQbic$_{TM}$ Content Protection Technology Adopted for MOOCS Service
NOGUCHI Masanori/MATSUKAWA Shinichi/KAIYA Kazuhiro
Accompanying the widespread dissemination of digital content delivery, there is a strong need for digital rights management (DRM) technology to protect copyrights while maintaining the users' convenience. Toshiba Solutions Corporation and Toshiba collaborated to develop MQbic$_{TM}$, a DRM technology that utilizes the secure digital (SD) memory card and achieves the ideal balance between users' convenience and copyright protection.
MQbic$_{TM}$ is employed as the DRM technology for the MOOCS electronic music distribution service operated by NIFTY Corporation.

Efforts for Standardization of MPEG-21 Rights Expression Language (REL) Profiles
ITO Satoshi/KAMBAYASHI Toru/AISU Hideyuki
MPEG-21 Part5:Rights Expression Language (REL) which defines the rights expression language for digital rights management (DRM), is expected to be one of the key technologies for flexible DRM and DRM interoperability. Recently, the efforts have been made for the development of MPEG-21 REL profiles that will be used for specific applications.
The MPEG-21 REL MAM (Mobile And optical Media) Profile was developed for the future applications to devices that have physical limitations on their capabilities and resources such as mobile devices and optical disc devices.

Secret Sharing Scheme and Its Applications
HOSAKA Norikazu/TADA Minako/KATO Takehisa
With the enactment of the Financial Products Exchange Law and the Personal Information Protection Law, enterprises are required to strictly manage confidential information and personal information. On the other hand, operational efficiency tends to slow down when information has to be strictly managed. Secret sharing schemes are therefore attracting attention as a technology that can solve this problem.
Toshiba Solutions Corporation has developed a new secret sharing algorithm that is faster than previous algorithms. It is applicable to a broad range of systems, and has already been applied to a document management system and a content delivery system of Toshiba Solutions Corporation.

SmartConcierge$_{TM}$ Walkthrough Type Face Recognition System
ENOMOTO Nobuyoshi/SATO Toshio/YAMADA Takahiro
While the need for physical security systems is rising, conventional systems are not sufficiently convenient for users. Toshiba has improved its FacePass$_{TM}$ face recognition security system and remodeled it into the SmartConcierge$_{TM}$ walkthrough type face recognition system. SmartConcierge$_{TM}$ enhances security while maintaining convenience.

Traitor Tracing in Content Distribution
MATSUSHITA Tatsuyuki/YOSHIDA Takuya/AKIYAMA Koichiro/IMAI Hideki
In content distribution, a broadcaster encrypts and then broadcasts digital contents (e.g., movies) to subscribers. The subscribers decrypt the encrypted contents and play them using their decryption devices (decoders), which contain their decryption keys. In this application, malicious subscribers (known as "traitors") may redistribute their decryption keys to nonsubscribers. This allows nonsubscribers with a pirate decoder to gain illegal access to the content. Traitor tracing has been extensively studied as a deterrent to such piracy.
Toshiba, jointly with Chuo University and the National Institute of Advanced Industrial Science and Technology, has developed a traitor tracing scheme in which the pirate decoder can be traced back to at least one of the traitors, even if the pirate decoder does not respond any further when it detects itself being examined, while maintaining the transmission overhead at an efficient level.

Provably Secure Digital Signature Scheme with Additional Functionality
KOMANO Yuichi/SHIMBO Atsushi/OKADA Koji
Provable security is an index that ensures the security of fundamental cryptographic primitives such as public key encryption and digital signature schemes. It not only allows everyone concerned to confirm the security of the primitives, but also provides a criterion for establishing the relevant standard. In order to prove the security of a scheme, the scheme is first provided with a security model (attack scenario and security goal) and then it is shown that the scheme satisfies the model. However, the model needs to be formalized for each primitive (functionality).
Toshiba and the University of Electro-Communications have proposed a digital signature scheme with additional functionality that can achieve the shortest bandwidth among multisignature schemes having a trapdoor one-way permutation and security equivalent to that of the proposed scheme, by embedding the message (with practical length) to be signed into an initial multisignature.

High-Generation-Rate Random Number Generator Using Si-Rich SiN MOSFET
MATSUMOTO Mari/OHBA Ryuji/USHIJIMA Tomomi
Information security has recently been playing an increasingly important role in various ubiquitous applications such as integrated circuit (IC) cards and mobile equipment. Higher level random numbers have correspondingly been required as one of the fundamental elements of secure systems. Physical random number generators are most desirable because of their unpredictable" true" random numbers.
Toshiba has developed a silicon nitride metal-oxide-semiconductor field-effect transistor (SiN MOSFET)-based random number generator that can generate high-quality random numbers at high speed and can be embedded into small circuits.

Feature Articles

Degradation Mechanism and Lifetime Projection of HfSiON as Alternative High-k Gate Dielectric
HIRANO Izumi/YAMAGUCHI Takeshi/SEKINE Katsuyuki
Nitrided hafnium silicate (HfSiON) is one of the most promising gate dielectrics for further miniaturization of large-scale integrated circuits (LSIs).
Before highly reliable LSIs can be realized, however, it is necessary to establish reliability assessment in terms of device degradation including measurement techniques, as well as a lifetime prediction method.
Toshiba has clarified that pre-existing traps strongly affect the negative bias temperature instability (NBTI) of HfSiON. It is important to be able to estimate the NBTI lifetime, especially taking pre-existing bulk trap effects into consideration.

MAGNIATM LiTE40S Small Entry-Class Intel® Architecture (IA) Server
YOSHIDA Kazuhiko
Toshiba has developed a new server model, the MAGNIATM LiTE40S, as an addition to the MAGNIATM series of Intel® architecture (IA) servers. Featuring the dual-core Intel® Xeon® processor or the Intel® Pentium® 4 processor, it has ample functionality, performance, and expandability as an entry-level server. It is also downsized, with a chassis size reduced to 70 % by volume compared with the preceding models in the MAGNIATM LiTE series. It can be equipped with four serial advanced technology attachment II (SATA II) hard disk drives (300 Mbyte/s) to extend its capacity up to 2 Tbyte. Moreover, the new model is enhanced by the new version of MAGNIATM ATA RAID (advanced technology attachment/redundant array of inexpensive disks) technology.

TW-170VD Drum Type Washer-Dryer
IMAI Masahiro/KONO Tetsuyuki/MURASE Hiroki
Since Toshiba introduced the industry's first drum type washer-dryer equipped with a direct drive (DD) motor into the market in 2000, the demand for washer-dryers has rapidly expanded and they are expected to account for a 31% share of the washing machine market in FY2007. This is because people have become unwilling or unable to dry laundry in the open air due to inadequate living environments or changes in lifestyles. On the other hand, a need has still existed for further improvements in drying finish and reduction in washing costs. For these reasons, a heat pump drying method was introduced in addition to the conventional heater-drying method. The amalgamation of the two methods promises a considerable reduction in total power consumption and in water consumption because heat pump drying eliminates the use of cooling water for dehumidification when laundry is dried. Accordingly, the running cost is greatly reduced while, at the same time, laundry is free of wrinkles and damage because it is dried at a low temperature.
Toshiba Consumer Marketing Corporation. released the TW-2500/2000VC drum type washer-dryer in July 2006 after developing an exclusive heat pump unit. This model has the industry's lowest running cost and enjoys a good reputation. However, models equipped with a heat pump continue to face the issues of price and weight. To overcome these issues, reduction in running costs and improvements in drying finish of the heater drying method are still required in addition to further development of the heat pump method.
Against this background, we developed and released another type of drum type washer-dryer, model TW-170VD, in November 2006. This model is a reasonably priced heater-drying drum type washer-dryer that offers drying finish close to that of heat pump models.

Frontiers of Research & Development

Product Line Approach to Software Development

Supply and Demand Control Technology for Microgrid Power System