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.

1. Introduction

The importance of information security is increasing. To address the needs for information security, the IT industry has continuously explored and developed new technologies. These technologies are crucial in protecting information stored in storage devices.
Previously, security technologies were primarily used to prevent information leakage in the event of loss or theft of Universal Serial Bus (USB) memory sticks or PCs. However, now with the prevalence of cloud storage, protecting personal information stored in data centers is also becoming increasingly important. This article outlines the information security required for diverse storage products as well as Toshiba's initiatives to fulfill such requirements.

2. Current Self-Encrypting Drives (SEDs)

2.1 SED Market Sectors and Market Demands

The HDD/SSD market is broadly divided into two sectors: mobile storage primarily for personal use and enterprise storage mainly for data center and other business servers. These market sectors have different requirements for cryptographic technologies.
In the field of mobile devices, internal and external HDDs and SSDs for notebook PCs are the major concern for information protection. It is necessary to prevent data leakage in the event of loss or theft of a mobile device. To prevent unauthorized access to the stored data, mobile devices need password-based user authentication and data encryption mechanisms.
In contrast, storage products for enterprise use do not need any robust protection against loss or theft because they are generally placed in secure rooms in data centers and elsewhere. Rather, the market for enterprise storage products places higher priority on low-cost data protection solutions in the event of hardware failure or at the time of disposal of HDDs and SSDs. Therefore, enterprise storage products must provide a data encryption mechanism and a capability to cryptographically lock up and invalidate data by means of key zeroization.
Conventionally, users had no choice but to rely on lengthy data overwrite operations or physical destruction of a drive in order to prevent data leakage when disposing of HDDs and SSDs.
However, data cannot be overwritten in the event of a drive failure. Additionally, the ever increasing storage capacity is posing an issue in terms of the time, and therefore the cost, taken to overwrite the entire data. Storage products incorporating cryptographic technology deliver several advantages in terms of data security. Encryption allows data to be securely protected in the event of any hardware failure. Furthermore, the entire data in HDDs and SSDs can be invalidated instantaneously just by changing the encryption key (Crypto Erase); this is a secure and low-cost means of disposing of the entire data on drives. The data invalidation capability makes it possible for data centers offering cloud storage services to quickly reallocate sanitized storage spaces to new customers.
Under these circumstances, market demand is increasing for SEDs that automatically encrypt data as it is written to the drive.

2.2 Security Standards for SEDs

Table 1 lists the security standards with which SEDs should comply in order to address security concerns, and the functions of these security standards.
Key features of the Trusted Computing Group (TCG) standard include data encryption and a capability for creating multiple storage ranges with each having its own access control (range management). Additionally, the TCG Opal Security Subsystem Class (SSC) standardizes pre-boot authentication[(1)].
HDD and SSD controllers must incorporate a

Table 1 Security standards for self-encrypting drives (SEDs)

Field	Security Standard	Function
Mobile	ATA Security Feature Set	Password authentication Data encryption Range management
	TCG Opal SSC	
	IEEE 1667	
Enterprise	TCG Enterprise SSC	Range management Crypto Erase
	T10 & T13 Sanitize	Crypto Erase

ATA: Advanced Technology Attachment

cryptographic circuit to encrypt data as it is written and decrypt it as it is read out. The TCG standard relies on the XTS and CBC modes of the Advanced Encryption Standard (AES). Although the TCG standard only requires the use of a 128-bit or longer key, Toshiba's SEDs use a 256-bit key to ensure long-term data security.

The range management feature of the TCG standard divides the disk space of an HDD or SSD into several address ranges for the purpose of security control. Each range is protected by its own encryption key, allowing only the authorized users to manage the associated range (Fig. 1). Although the Institute of Electrical and Electronics Engineers (IEEE) 1667 standard stipulates the use of the eDrive specification adopted by the Microsoft® BitLocker® (*1), it is incompatible with the TCG Opal SSC provided by independent software vendors (ISVs). It is still unclear which security standard will prevail in HDDs and SSDs.

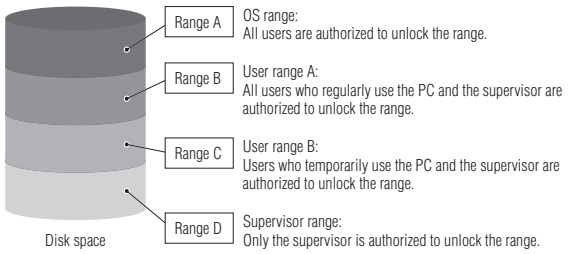

Figure 2 Example of use of logical block address (LBA) ranges in disk space —
Only the authorized users can access the associated LBA ranges unless they are unlocked. Range locking protects user's information.

2.3 Toshiba's SED Implementation

Toshiba has consolidated its storage security design & development departments. The newly established division develops enterprise and mobile storage products compliant with various security standards described in Section 2.2.

It is responsible for perusing these security standards to create libraries that implement basic functionality common to them such as password authentication, access control, random number generation and key management. These libraries are designed for common use by multiple HDDs and SSDs. They are utilized to create range locking/unlocking and other higher level security functions required by the security standards. The new division is also creating common firmware for enterprise or mobile storage products, which is designed to process the TCG Trusted Send/Receive and Security Protocol In/Out commands for both T10 and T13. This firmware helps improve the HDD/SSD development efficiency. Furthermore, it makes the behaviors of security-related commands on all storage products look identical from the host as long as they support the same security standard; this simplifies replacing HDDs with SSDs and vice versa.

Fig. 2 shows the structures of HDDs/SSDs and the password (PIN) authentication sequence. For example, in the TCG Opal SSC sequence, a PIN is sent as a parameter to the Trusted Send command, decoded by the TCG processor and then acknowledged by the basic security processor during the PIN authentication process. Once the PIN is authenticated, the associated range is unlocked for both read and write accesses.

2.4 Certification of Toshiba's Security Functions by Third-Party Organizations

Conformance to TCG and other security standards is necessary but insufficient to proclaim that a given storage product is secure. Third-party authentication is necessary as an independent, objective assurance on its security quality. The Cryptographic Module Validation Program (CMVP) based on the U.S. NIST FIPS 140(*2) is most widely used in the field of HDDs, SSDs and other storage products.

Because the CMVP certification is compulsory for products for use by the U.S. government, more and more storage product vendors are seeking to have their products certified for CMVP. Additionally, vendors of firewall and other networking equipment and software encryption libraries are also seeking CMVP certification.

The CMVP validation program requires that an encryption algorithm approved by the U.S. government be implemented properly and that encryption keys and other sensitive information used by the cryptographic function be safeguarded. Its security testing covers numerous areas, including proper implementation of an encryption algorithm; a capability for wiping sensitive information from an actual product; assessment of entropy sources; resistance against physical attacks to the PCB via visual and probe examinations, etc. (Fig. 3).

Based on our experience with Japan CMVP (JCMVP), we began seeking CMVP certification in August 2012. To start with, we created the common libraries described in Section 2.3, taking the FIPS 140 requirements into consideration early in the design stage, such as the implementation of encryption algorithms and the handling of encryption key and other parameters. Our design team dedicated to security authentication is striving to minimize the CMVP certification cost by using a common security implementation as a basis of all HDDs and SSDs for both enterprise and mobile use. Our

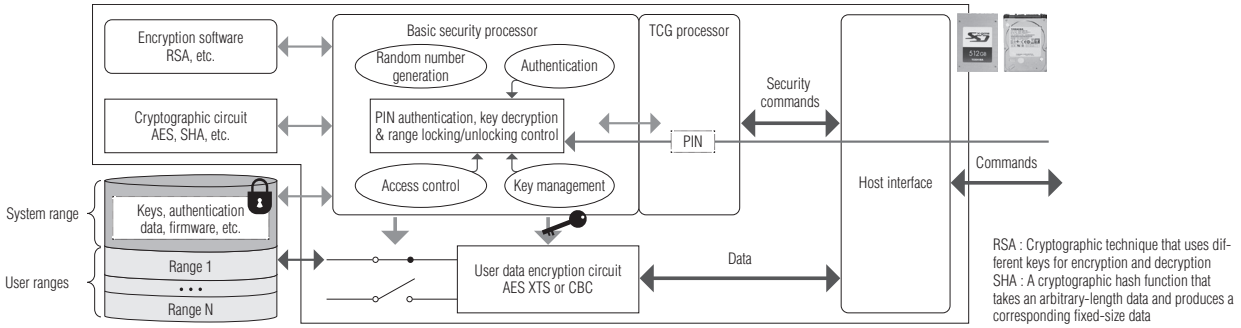

Figure 2 Configuration and personal identification number (PIN) authentication of HDD and SSD —
User authentication, key allocation and range locking/unlocking are performed using PINs.

mobile HDDs incorporating TCG Opal SSC and Toshiba-proprietary Wipe™ encryption technology were certified by an accreditation organization and have been brought to the NIST for final assessment as of December 2013. We are also preparing to have our enterprise HDDs and SSDs and mobile SSDs certified for CMVP successively. The know-how needed to obtain CMVP certification for HDDs and SSDs can also be applied to Universal Flash Storage (UFS), *e*•MMC™ (*3) and other memory products.

Figure 2 Example of use of logical block address (LBA) ranges in disk space —
Only the authorized users can access the associated LBA ranges unless they are unlocked. Range locking protects user's information.

3. SED Issues To Be Tackled in the Years Ahead

3.1 Challenges Facing Mobile Storage Products

The challenges to be resolved in the field of storage products for mobile devices are as follows:

(1) Unclear course of TCG Opal SSC

ISVs have led the development of the TCG Opal SSC. The use cases of corporate mobile devices envisaged by them are inconsistent with those of mobile PCs envisaged by Microsoft that prioritize personal data protection. Because of these differences in use cases, the TCG Opal SSC defines multiple compliance tests and thus incurs higher test costs. In order to fulfill the need for a unified test procedure, it is crucial to predict which use case will become mainstream and to interface with all parties concerned.

(2) Improvement in the resistance against physical attacks

People frequently use a mobile device in an environment where anyone can reach for it. Therefore, mobile devices have lower physical security than enterprise storage products. At present, a security issue exists concerning the bus trace through which a PIN is sent and received without being encrypted. The HDD or SSD could also be removed from a mobile device for unauthorized analysis and tampering. Toshiba's storage products incorporating Wipe TM technology provide a solution for these data protection issues(1).

(3) DEVSLP support

In order to support DEVSLP, Intel's ultra-low-power device sleep mode, a storage drive must be allowed to return to normal operating mode without requiring user authentication. This means that DEVSLP has significant security implications; if a notebook PC is stolen while in DEVSLP mode, the thief can easily retrieve any data stored in it. It is necessary to strengthen the security on exit from the DEVSLP mode in order to prevent security problems.

3.2 Challenges Facing Enterprise Storage Products

The challenges to be resolved in the field of storage products for enterprise use are as follows:

(1) Common secure failure analysis technique

It is contradictory to provide robust data protection to SEDs and, at the same time, to simplify the collection of log and trace data in the event of a failure or repair. Our common firmware requires further enhancement to make it possible to collect failure analysis data in a secure manner. The data collection method should be applicable to as many scenarios as possible.

(2) Data erasure technique considering the remote copy function

Storage systems designed for data center applications have a remote copy capability to maintain a mirror image of data at remote sites so that no data is lost in

the event of an earthquake or other disaster or a major device failure. Therefore, multiple copies of exactly the same data reside on different HDDs or SSDs. In order to maintain data consistency among all copies, it is important that when certain data is erased from primary storage, the same data is also erased from all its mirror images.

3.3 Challenges Concerning the Acquisition of CMVP Certification

The challenges to be resolved to obtain CMVP certification are as follows:

(1) Measures to work around various restrictions

In order to have a storage product certified for CMVP, the vendor must specify the version numbers of both its hardware and firmware. When either the hardware or the firmware is updated, it is necessary to have it recertified. Because it is often required to tailor enterprise HDDs and SSDs to suit the needs of specific customers, maintaining their CMVP certifications could be costly. Moreover, it currently takes eight to ten months to obtain CMVP certification; most of this time is spent waiting for the NIST to assess a test report, and thus it is difficult for a vendor or an accreditation organization to shorten the certification process. Nevertheless, product life cycles are becoming shorter and shorter; once a product is certified for CMVP, its market window could be limited. Certification and sales strategies must take these restrictions into consideration.

(2) Incorporating security requirements into controller designs

It takes six months to a full year to design a controller to be embedded in a storage product. Any design iterations would considerably impact the design schedule and cost. If any functions requiring CMVP validation are to be incorporated into a controller, a thorough investigation is necessary. It is therefore essential to keep track of new cryptographic requirements that may arise in the future because of a revision to a security standard or FIPS 140(*2), or a revision to an encryption standard (e.g., changes to entropy evaluation techniques related to the SHA3 addition

or NIST SP800-90B (Special Publication 800-90B)). Any new requirements must be fed back to a controller design in a timely manner. To reduce the workload incurred, we need not only to use the same firmware but also to reuse the same hardware design for the security function.

4. Conclusion

Nowadays, with many news reports breaking out about information breaches, consumers are becoming more concerned about information protection. To address such concerns, we have been developing storage products with enhanced security features.

However, many challenges remain to be solved, as described in Section 3. Because the market for storage security technology is still developing, it is of primary importance to find solutions to current issues and then to predict and meet future customer needs. Additional features that are unrelated to information security may also be required for storage products. For example, the European Union suggests the "right to be forgotten"; so a possible addition may include a capability to search for and delete personal information on the network. Another example may be a capability to optimize the HDD and SSD performance in terms of the search speed.

Information security has growth potential in terms of both technology and market. We will continually strive to create innovative storage products with new and enhanced security features that will address the security concerns of society.

(*1) Microsoft and BitLocker are registered trademarks of Microsoft Corporation in the U.S. and other countries.

(*2) Tested in accordance with Federal Information Processing Standard (FIPS) 140-2 of the U.S. National Institute of Standards and Technology (NIST) published in 2001 (as of September 2013). FIPS 140-2 will be revised and released as FIPS 140-3 within 2014.

(*3) *e*•MMC is a trademark of JEDEC Solid State Technology Association.

References

(1) Self-Encrypting 2.5-inch Hard Disk Drives Equipped with Wiping Technology to Reduce Information Security Risks.
TOSHIBA Review 66, 8, 2011, pp. 44-46

YAMAKAWA Teruji
Storage Products Div.

ARAMAKI Yasuto
Storage Products Div.

UMESAWA Kentaro
System & Software Solution Center