Toshiba Wipe Technology: Better Data Security for the Digital Age

Introduction

In April 2011 Toshiba announced Wipe2 technology (later mention) Toshiba's unique set of enhanced features for TCG-Opal self-encrypting disk drive (SED) models. Toshiba's Wipe Technologies strengthen data security by providing data invalidation capabilities that can be set to automatically trigger if an un-expected host is detected by the SED. Use cases that benefit from this enhanced security include multi-function printers (MFP) and copiers, personal computers and IT storage assets that may be at risk as a result of improper de-commissioning, re-purposing, component servicing or asset disposal.

Increasing Risks to Data Security

Digital information and communication technologies are everywhere, enabling us to access the data we need wherever we go. These technologies power today's business processes, email, e-commerce, infrastructure monitoring and security, document and medical imaging, global communications, personal entertainment, digital photography – the list goes on and on... The massive amounts of digital storage in use today (as well as the growth in the capacity of individual storage devices) have greatly increased the security risks for sensitive business information and personal information subject to privacy regulations.

Today so many copies of sensitive data exist across so many systems that we must guard against unintentional data leakage in addition to guarding against malicious security attacks by identity thieves and other evil doers. Data privacy regulations and well-publicized data breaches have prompted many institutions, public and private, to improve their ability to safeguard private information from cyber attacks and unintentional leakage. These same organizations are also seeking legal "safe harbor" from the potential burden of data breach notification requirements. It is no surprise then that encryption technologies are becoming more widely deployed to help secure "data at rest" on digital systems.

Existing Encryption"Best Practices" May Not be Sufficient

Many policy makers and IT professionals are increasingly aware of how security gaps and risks may evolve over the usage lifecycle of computers, copiers and other systems used to process, transmit and store digital data. For example, many organizations have policies in place that require the encryption of storage in client PC machines. Traditionally (meaning over the last 10 or so years...) many organizations have used software encryption products which run as "background" applications using processing cycles from the PC's CPU to perform the encryption. This is not only inefficient it is also less secure than self-encrypting storage devices. Consider that software encryption must also perform an initial encryption "pass" on a new PC – prior to deployment all the data loaded during new system configuration must be encrypted by the crypto-software before the PC is ready to be deployed. Because it takes time to complete the software encryption operation, a "compliance gap" may exist during the first hours of system operation. Software encryption also robs systems performance and may result in application compatibility issues, thus resulting in the risk that knowledgeable users may disable the encryption to gain performance or to remedy real or perceived compatibility issues. Obviously, this creates a compliance gap and puts sensitive data at risk. Consider also that multiple copies of encryption keys must be managed for software encryption, resulting in additional key management overhead and the increased risk of key management security risks over the life-time of system use, and especially during system de-commissioning, re-deployment or disposal.

Secure Data Disposal - Better Data Erase Methods

In addition to client data security, policy makers are increasingly concerned about the compliance of data erasure and data purge operations with security policy and accepted best practice. It is currently common practice to use multiple data erase and overwrite passes to ensure that sensitive data has been rendered unrecoverable for magnetic or solid-state storage media. The downside is that such overwrite processes often need 5 – 6 hours to complete, tying up the equipment and

burdening the personnel required (cost) to oversee such operations. Because of the risks and expense associated with data overwrite operations, the risk of "shortcuts" increases which raises the risk of data leakage. Some security policies may mandate physical destruction of otherwise useable or re-saleable equipment. But such physical destruction requires special equipment or services (cost) and depends on people to certify that the disk media has been effectively erased or destroyed (risk). A better approach is required.

Stronger Security at the Source – Self-Encrypting Drives and Wipe Technologies

Hard disk drive makers now offer on-board encryption and access authentication features in Self-Encrypting Drive (SED) models. When properly integrated within securely designed host systems, SEDs offer advantages over software encryption that may reduce the costs and risks associated with data security, especially during initial deployment of protected systems and when protected systems and storage hardware are re-purposed or retired from service.

Today's SEDs provide many advantages over legacy storage encryption technologies. But what about protection from more sophisticated thieves? Consider the following:

- **What if a thief removes the hard drive from a stolen PC to defeat the access security safeguards?**
- **What if the hard drive is removed for maintenance and finds its way into the hands of an evil-doer?**

Toshiba studied such scenarios and worked with system makers to develop Wipe Technology as an enhanced set of security features for Toshiba SED models. Toshiba first announced Wipe1 technology in August 2010.

Wipe1 was mainly aimed at the MFP / copier use case – such systems store document images on disk drives – documents that may contain sensitive information. Wipe 1 enabled protected data partitions to be instantly invalidated (crypto-erased) whenever power is cycled to the HDD interface. This covers risk cases such as system theft or HDD removal from the MFP / copier system.
Toshiba SEDs with Wipe1 may be used as follows:

- **Create data areas protected by Wipe security, and separate data areas (for example for system boot and operational code) that will not be protected by Wipe security. (Both areas protected by data encryption.)**
- **Use the protected areas for sensitive Print, Scan and Copy data. Use the non- protected areas for system boot files and activity log data.**

Whenever the system's power is turned off all of the user data in the protected areas will be crypto-graphically erased, thus preventing any evil doer from recovering sensitive document images that may reside on a copier system that has been stolen, scraped or simply returned from to a leasing company.

Wipe2: Toshiba's Customers Ask for Additional Security

Toshiba's announcement of Wipe1 received a lot of positive feedback from systems designers, who requested that Toshiba develop additional Wipe features to cover additional threat scenarios.

For example, some uses cases needed to preserve user data across a system power cycle event, but still provide for automatic crypto-erase if the system's SED storage device were to be stolen or removed from service.

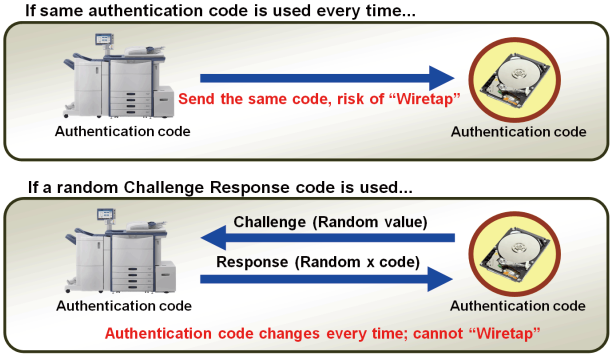
After further work with systems designers, Toshiba announced Wipe2, which added the ability to "pair" a host system with the attached SED storage.

With Wipe2, during system boot the host and the SED perform an authentication sequence. If the SED is unable to authenticate the attached host, then access to the SED remains locked and data areas protected with Wipe2 are cryptographically erased.
The authentication capabilities added with Wipe2 significantly improve the ability to protect sensitive data while preserving the ability to perform system maintenance operations. For example, if the Wipe2 SED is removed from the original system and later

reinstalled in the same original system, then protected areas are preserved. On the other hand, if the Wipe2 SED is removed from its original system and connected to another system, then areas protected by Wipe2 will be cryptographically erased, thus ensuring the security of the protected data.

Safe system authentication

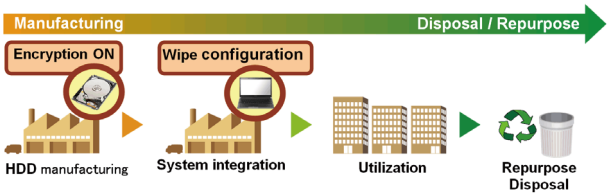
Toshiba's Wipe2 uses a challenge and response sequence protocol for secure authentication between a Wipe2 enabled host system and the Wipe2 SED. The method used randomizes the authentication code each time so that a "Wiretap" cannot be used to discover and defeat the Wipe2 security.



The Wipe2 SED is able to judge the authentication code from a Wipe2 enabled host by comparing the completing the pre-determined challenge and response protocol process inside the secure SED device.

Data protection throughout a system's life cycle

Toshiba Wipe Technology greatly improves the ability to protect against sensitive data leakage throughout the usable life cycle of systems using secure, efficient SED storage devices. Wipe Technology provides additional security against improper data access if a system is lost or stolen, and after storage assets are retired from service. Evil doers are unable to access protected data by attaching a stolen SED to another host system, or by using forensic tools because protected areas of the SED will be automatically crypto-graphically erased if there is any deviation from the SED's expected access protocols.



Target market and use case

Toshiba's Wipe Technology SED models provide Wipe1 and Wipe2 capabilities, in addition to the standard security command capabilities supporting the SED's ability to invalidate data by system command (one of the SED's native functions which Toshiba refers to as Wipe0).

Market segments that may benefit significantly from Toshiba's Wipe Technology include:

- **PC market:** Enhanced data security for mobile and desktop computing.
- **MFP market:** Enhanced data security digital data images in office equipment.
- **IT system with transient data:** Enhanced data security for digital data that may still reside on disk storage within a system after the data is no longer required for local processing by the system.
- **IT system with shared client environment:** Enhanced data security for session data that may still reside on disk storage within a shared client system after the prior user session has ended.

Data Protection Scenarios include:

- **Protection against HDD removal from IT systems**
  - Data invalidation on power down of HDD or HDD removal from powered system. (Wipe1)
  - Data invalidation when HDD is connected to an unauthorized system. (Wipe2)
- **System disposal and repurposing**
  - Data invalidation by system command to SED storage device. (Wipe0)
- **Thin client / Multi-User Secure PC**
  - Data invalidation on logical session termination (Wipe0) or thin-client power down. (Wipe1)

Summary

Toshiba's Wipe Technology feature set for self-encrypting drives provide enhanced security capabilities to help protect sensitive data throughout the life cycle of systems using SED storage. Systems designers can select from several Wipe Technology capabilities to fit different data leakage protection scenarios:

- **Wipe0:** Data invalidation by system command.
- **Wipe1:** Data invalidation on power down of the HDD, such as HDD removal from host.
- **Wipe2:** Data invalidation by host authentication failure.

Using the capabilities of Toshiba Wipe Technology, the security of sensitive user data may be improved against unexpected attacks on lost, stolen, or discarded HDDs. Using on-board encryption and secure crypto-erase capabilities, Toshiba's Wipe Technology SED models may significantly lower the cost associated with data encryption during system life, as well as reducing the costs associated with securely erasing data during system disposal and repurposing.
It is Toshiba's goal to contribute to a peaceful and safe society by providing storage products that enhance data security.

Reference use case

Data leak prevention at MFP

● **< Scene 1 > Leak prevention at HDD theft**

- Overview: When connected unknown host, HDD will invalidate protected data immediately
- Before: System supports encryption but data invalidation is not integrated. –risk of unauthorized data access
- After: Even if HDD is stolen, data breach is prevented by automatic data invalidation.

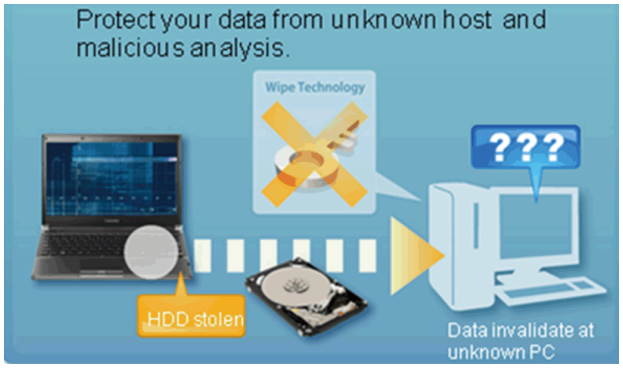
● **< Scene 2 > Invalidation at system retirement**

- Overview: System menu provides instant data invalidation feature for use during system return or disposal.
- Before: Data erase / overwrite took 2 to 5 hours
- After: Data invalidation completes within seconds, saving hours of operation and encouraging policy enforcement. Strong TCO reduction.

Data leak prevention at PC

● **< Scene 1 > Leak prevention if HDD theft**

- Overview: Stolen HDD connected to unkown host remains locked. HDD unlocks only on original PC.
- Before: HDD stolen and HDD password cause risk of data leak.
- After: HDD needs both host authentication and Password. Even if Password leaks, HDD invalidates protected data if host authentication fails.



● **< Scene 2 > Invalidation at system retirement**

- Overview: Administrator or Special software tool invalidates HDD data immediately.
- Before: Data erase / overwrite took 2 to 5 hours
- After: Data invalidation completes within seconds, saving hours of operation and encouraging policy enforcement. Strong TCO reduction.

* Before creating and producing designs and using, customers must also refer to and comply with the latest versions of all relevant TOSHIBA information and the instructions for the application that Product will be used with or for.

* All other names and brands mentioned herein may be trademarks of their respective owners.

Website: http://www.toshibastorage.com