Self-Encrypting Hard Drives: From Laptops to the Data Center

Jason Cox, Seagate Technology
The material contained in this tutorial is copyrighted by the SNIA.

Member companies and individuals may use this material in presentations and literature under the following conditions:

- Any slide or slides used must be reproduced without modification
- The SNIA must be acknowledged as source of any material used in the body of any document containing material from these presentations.

This presentation is a project of the SNIA Education Committee.

Neither the Author nor the Presenter is an attorney and nothing in this presentation is intended to be nor should be construed as legal advice or opinion. If you need legal advice or legal opinion please contact an attorney.

The information presented herein represents the Author's personal opinion and current understanding of the issues involved. The Author, the Presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.
Abstract

- Trusted Computing Group (TCG) Storage Specifications
  - The Trusted Computing Group (TCG) Storage Work Group recently published formal specifications for security and trust services on storage devices, including hard drives, flash, and tape drives. The majority of hard drive and other storage device manufacturers participated. Putting security directly on the storage device avoids the vulnerabilities of platform OS-based software security. The details of the Specification will be highlighted, as well as various use cases, including Self Encrypting Drives with enterprise key/credential management.
TCG Storage Work Group Structure

- **Storage WG**
  - Jorge Campello
  - HGST

- **Key Management Services**
  - Walt Hubis
  - LSI

- **Storage Interface Interactions**
  - James Hatfield
  - Seagate

- **Optical Storage**
  - Bill McFerrin
  - DataPlay

- **Storage Conformance**
  - Cyril Guyot-HGST/
  - Dmitry Obukhov-Samsung
Document Roadmap

- Trusted Storage Core Architecture Specification 1.0
  - Published May 2007
- Optical Storage Subsystem Class Specification
  - Published September 2008
- Enterprise Security Subsystem Class Specification
  - Published January 2009
- Storage Interface Interactions Specification
  - Published January 2009
- Trusted Storage Core Architecture Specification 2.0
  - Published April 2009
- Opal Security Subsystem Class Specification
  - Published April 2009
Core Spec/SSC Relationship

General Documents
- TCG Storage Core Architecture Specification v1.0
- Storage Interface Interactions
- TCG Storage Core Architecture Specification v2.0

Specific Documents
- Enterprise SSC
- Opal SSC

Auxiliary Documents (currently in progress)
- Compliance
- App Note
- Compliance
- App Note

Storage Developer Conference 2009
© 2009 All rights reserved.
Self-Encrypting Drive Basics

- The storage device LOCKS when it powers OFF.
- The storage device remains LOCKED when it is powered back ON.
- Authentication UNLOCKS the storage device.
- The storage devices Reads and Writes data normally while drive is unlocked.
- The plaintext data sent to the device is encrypted before being written.
- The encrypted data read from the device is decrypted before being returned.

Data protected from loss, disclosure.

100% performance encryption engine in the drive.
Enterprise SSC Motivation

- Provide a solution to address current market needs:
  - Protect the confidentiality of stored data.
  - Minimize the time to bring devices online.
  - Provide secure disposal / end of life.
SED in the Data Center

- Enterprise SSC Threat Model
  - Unauthorized access to data on the device once it leaves the owner’s control.

- Features
  - Encryption
  - Drive Locking with Password-based authorization
  - Ranges
  - Fast Secure Erase
  - Static Access Control Model
SED in the Client

- Opal SSC Motivation
  - Provide a solution to address current market needs:
    - Stolen / lost laptop data leakage.
    - End of life / disposal.
  - Trade-off between time-to-market and feature addition.
    - Simple password based authentication.
    - Provide encryption and locking
SED in the Client

- Opal SSC Threat Model
  - Offline leakage of data.

- Features
  - Encryption
  - Drive Locking with PW access control
  - Ranges
  - MBR Shadowing
  - Fast Secure Erase
  - Dynamic Access Control Model
Encryption & Locking

- Independent Locks for read and write.

Storage Device

- Keys are generated internally.

Secure (Cryptographic) Erase performed by erasing the key.

User
LBA Ranges

Independent encryption and access control for each range.

Ranges are not necessarily aligned with partitions, though we expect that will be the case in the majority of uses in the client space.
MBR Shadowing

- **Initial Power-up**
  - When the system first requests the MBR, the HDD returns the pre-boot code (the MBR shadow).

- **Authentication and Unlock**
  - The pre-boot code manages the authentication process with both internal and external authorities.
  - After the appropriate authentications, the management software unlocks the regular user space.

- **Resume Normal Boot**
  - After the HDD is unlocked, the management software sends the system back to the boot process.
  - The system's request for the MBR now returns the true MBR and the OS is loaded completing the boot process.
Define an architecture that:

- Enables application of access control over select device features
- Permit configuration of these capabilities in conformance to the platform security policy
The host platform, applications, devices, local end users, or remote users/service providers can gain exclusive control of selected features of the storage device. This allows them to simultaneously and independently extend their trust boundary into the storage device or trusted peripheral (TPer).
Security Providers (SPs)

TCG Storage specifications are intended to provide a comprehensive command architecture for putting selected features of storage devices under policy-driven access control.

- Features are packaged into individual functionality containers called “SECURITY PROVIDERS (SPs).”

- Each SP is a “sand box” exclusively controlled by its owner. SP functionality is a combination of pre-defined functionality sets called SP TEMPLATES:
  - Base
  - Admin
  - Crypto
  - Log
  - Clock
  - Locking

- SPs are a collection of TABLES and METHODS that control the persistent trust state of the Storage Device (SD).
  - Method invocation occurs under access control.
  - The SP has a list of authorities and their respective credentials for access control.
Tables provide data storage in SPs. Each template defines a set of tables. Capabilities provided by the Base template allow the host to create additional tables.

- Two types of tables:
  - Object – organized storage
  - Byte – raw data

UID column contains SP-wide unique, addressable value for that row.

Rows associate column values.

Object Table

<table>
<thead>
<tr>
<th>UID</th>
<th>Col2</th>
<th>Col3</th>
<th>Col4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>Data</td>
<td>Data</td>
<td></td>
</tr>
<tr>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
</tr>
</tbody>
</table>

Each column stores data all of the same type.

Byte tables have a single column.

Byte tables have 0 or more rows indexed by position in the table.

<table>
<thead>
<tr>
<th>Index</th>
<th>Column</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0x41</td>
</tr>
<tr>
<td>1</td>
<td>0x42</td>
</tr>
<tr>
<td>2</td>
<td>0x43</td>
</tr>
<tr>
<td>…</td>
<td>…</td>
</tr>
</tbody>
</table>

Each cell stores one byte.
Methods are remote procedure calls invoked by the host to manipulate SP state. Methods operate on tables or the SP itself, and are used for session startup, authentication, table manipulation, and access control customization.

**InvokingUID.MethodUID [ Method Parameters ] => [ Method Result ]**

- UID of the table or object upon which the method is being invoked.
- UID of the invoked method.
- List of method parameters sent by host.
- List of results generated by TPer

**Key Methods**

- **Get** – Retrieve values stored in tables.
- **Set** – Change values stored in tables.
- **Authenticate** – Prove host knowledge of a secret

**Other methods provide capability to:**

- Create/delete tables/table rows
- Generate encryption keys on the device
- Perform cryptographic operations on the device
Access control defines the authorization required to invoke specific methods. Access control permissions apply at the SP, table, or table row level. Access control settings are configurable and assignable.

Authorities are authentication agents. Each authority has a unique identifier and credential. Authorities are required authentication operations.

The Host Application invokes the **Authenticate** method, identifying the Authority to be authenticated and the required proof (password, signed challenge, etc.).
Ranges are individually encrypted with different encryption keys.
The access to a range is given from the Admin to any combination of users either for read, write, or both.
The secure erase capability of a range is given from the Admin to any combination of users.
Enterprise SSC Range Encryption & Locking

Ranges are individually encrypted with different encryption keys.
The access to ranges is assigned at manufacturing and non-modifiable.
Minimum support requires Global Range, and EraseMaster and BandMaster0 authorities.

<table>
<thead>
<tr>
<th></th>
<th>EraseMaster</th>
<th>BandMaster0</th>
<th>BandMaster1</th>
<th>BandMaster2</th>
<th>BandMasterN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Global Range</strong></td>
<td>Read Un/Lock</td>
<td>Read Un/Lock</td>
<td>Read Un/Lock</td>
<td>Read Un/Lock</td>
<td>Read Un/Lock</td>
</tr>
<tr>
<td>K0</td>
<td>Write Un/Lock</td>
<td>Write Un/Lock</td>
<td>Write Un/Lock</td>
<td>Write Un/Lock</td>
<td>Write Un/Lock</td>
</tr>
<tr>
<td></td>
<td>Secure Erase</td>
<td>Secure Erase</td>
<td>Secure Erase</td>
<td>Secure Erase</td>
<td>Secure Erase</td>
</tr>
</tbody>
</table>

| **Range 1**     | Read Un/Lock| Read Un/Lock| Read Un/Lock| Read Un/Lock| Read Un/Lock|
| K1              | Write Un/Lock| Write Un/Lock| Write Un/Lock| Write Un/Lock| Write Un/Lock|
|                 | Secure Erase | Secure Erase | Secure Erase | Secure Erase | Secure Erase |

| **Range 2**     | Read Un/Lock| Read Un/Lock| Read Un/Lock| Read Un/Lock| Read Un/Lock|
| K2              | Write Un/Lock| Write Un/Lock| Write Un/Lock| Write Un/Lock| Write Un/Lock|
|                 | Secure Erase | Secure Erase | Secure Erase | Secure Erase | Secure Erase |

| **Range N**     | Read Un/Lock| Read Un/Lock| Read Un/Lock| Read Un/Lock| Read Un/Lock|
| KN              | Write Un/Lock| Write Un/Lock| Write Un/Lock| Write Un/Lock| Write Un/Lock|
|                 | Secure Erase | Secure Erase | Secure Erase | Secure Erase | Secure Erase |

Fixed, not configurable
The SSCs define two SPs. The Admin SP is used for retrieving device information and configurations. The Locking SP is used to control the data encryption and locking/unlocking of LBA ranges in the storage device.

User authenticates to the SP and retrieves configuration information using App A.

App A invokes Get to retrieve configurations.
The storage device can have only one SP with Locking capability. Access control to user data can be configured. The storage device will support a certain number of independent ranges of user data.

Independent encryption and access control for each range.

App is responsible for configuring encryption and access control for all users.

There can only be one Locking SP per Storage Device.
Locking Ranges

The Locking SP enables independent ranges of the user data space to be separately configured for read/write access control.

Separately configured portions of user data space

App Authenticates and then invokes Set to configure the starting address and length of each range.

Range settings are stored in the Locking table.
Configuring Passwords

Each user can be assigned a separate password that is used for authentication to the Locking SP.

Passwords are stored in the C_PIN table.

App Authenticates and then invokes **Set** to change the password.
The user authenticates with a password and then unlocks the ranges accessible ranges.

App authenticates and then invokes `Set` to change the locking values of the appropriate ranges.

Range settings are stored in the `Locking` table.
Secure Erase

The Locking SP provides the host with the ability to erase data, securely and quickly, by replacing the encryption key for a range with a new key randomly generated securely in the drive.

App Authenticates and then invokes **GenKey** (Opal) or **Erase** (Enterprise) to generate a new key for the range.
The Future…

- **Encryption**
  - Automatic performance scaling, manageability, security

- **Standards-based**
  - Multiple vendors; interoperability

- **Unified key management**
  - Handles all forms of storage
Thank You!

www.trustedcomputinggroup.org
Q&A / Feedback

Please send any questions or comments on this presentation to SNIA: tracksecurity@snia.org

Many thanks to the following individuals for their contributions to this tutorial.
- SNIA Education Committee

Robert Thibadeau
Michael Willett
Jorge Campello
All Storage Manufacturers (contributors)