Advances in Storage Security Standards

Jason Cox
Security Architect, Intel Corporation
Co-Chair, TCG Storage WG
Objectives

- Provide background on Trusted Computing Group (TCG) Storage Work Group Goals
- How Use Cases are expanding
- Describe work in progress to align with NVMe
- The importance of Opal assurance
- Highlight other recent, storage-related security specifications, goals, and benefits
TCG Storage WG Goals

- Expand current use cases
  - Opalite, Pyrite
- Enhance deployability and assurance
  - NVMe/Namespace interactions
  - TCG Storage Opal Test Cases, Collaborative Protection Profile
- Introduce new features based on IT, OEM, IHV, ISV pain points; expand basic threat model
  - Secure Messaging, PSID
Opal SSC:
- Defines the full-featured interface for managing security features in a storage device, including device encryption.
- Threat model: protect confidentiality of stored user data against unauthorized access once it leaves the owner’s control (when drive and system are powered off)

Important Points:
- Supports division of Storage Device user data space into multiple “LBA Locking Ranges”
- Each LBA Locking Range has its own media encryption key.
- Locking Ranges are locked after a storage device power cycle.
- Admin assigns access to unlock Ranges to 0 or more Users.
- Each Locking Range can be independently cryptographically erased.
- The Shadow MBR region stores ISV SW “Pre Boot Environment” to capture unlock password and unlock Ranges to allow OS boot.
Self-Encrypting Drive (SED)
Opalite SSC and Pyrite SSC

- NVMe’s strategy: align on Opal SSC-based solutions
  - Scale across the needs of NVMe in different Client and Enterprise (data center) solutions
- At the request of NVMe WG, TCG Storage WG developed additional “Opal Family” specifications, to address additional Use Cases
  - **Opalite SSC**: Subset of and command compatible with Opal (functionally equivalent to ATA Security)
  - **Pyrite SSC**: Similar to Opalite, does not specify a requirement for media encryption
  - **Block SID Feature Set**: Provides function similar to “Freeze Lock”, to help control Take Ownership process

---

Opal and Pyrite expand use models beyond corporate client.
Opal and Assurance

- Opal SSC Test Cases Specification
  - Baseline for Opal Certification
    - Covers Opal 1.00, 2.00, and 2.01
  - *Currently in pre-publication review*

- Common Criteria Encryption Engine and Authorization Acquisition cPPs (Feb 2015)
  - Specifies security evaluation for Self-Encrypting Drives (SED) and SED management software

Opal compliance and assurance are high priority OEM/customer requests.
WIP: Namespace Interactions

- TCG Storage Interface Interactions
  - Updates to Namespace Interactions in progress (targets SIIS v1.05)
- Specifies required support for 2 scenarios:
  - Multiple namespaces can be supported with all mapped to the Opal Global Range
  - A single namespace can be supported with multiple Opal “Locking ranges” all mapped within the 1 namespace

Multiple Namespaces

<table>
<thead>
<tr>
<th>Range</th>
<th>Namespace</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>Opal</td>
</tr>
<tr>
<td>NS1</td>
<td></td>
</tr>
<tr>
<td>NS2</td>
<td></td>
</tr>
<tr>
<td>.NSN</td>
<td></td>
</tr>
</tbody>
</table>

Multiple Locking Ranges

<table>
<thead>
<tr>
<th>Range</th>
<th>Namespace</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>Opal</td>
</tr>
<tr>
<td>NS1</td>
<td></td>
</tr>
<tr>
<td>NS2</td>
<td></td>
</tr>
<tr>
<td>.NSN</td>
<td></td>
</tr>
</tbody>
</table>

If multiple namespaces are created, then locking of all are controlled together.
If multiple locking ranges are configured, then they all are within a single namespace, and additional namespaces cannot be created.

WIP to align with NVMe to enable a strong collaboration between the organizations.
WIP: Namespace Interactions

- Architecture of enhanced configurability also in progress
  - When namespaces are created, the Global Range settings apply.
  - Namespaces can be associated with one or more Locking objects, to enable separate locking of that namespace or LBA ranges within that namespace.
- TCG SWG is seeking input on use cases.

<table>
<thead>
<tr>
<th>Range</th>
<th>Namespace</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>NS1</td>
</tr>
<tr>
<td></td>
<td>NS3</td>
</tr>
<tr>
<td></td>
<td>NS7</td>
</tr>
<tr>
<td>Range1</td>
<td>NS2</td>
</tr>
<tr>
<td>Range2</td>
<td>NS4</td>
</tr>
<tr>
<td>Range3</td>
<td>NS4</td>
</tr>
<tr>
<td>Range4</td>
<td>NS5</td>
</tr>
<tr>
<td>Range5</td>
<td>NS6</td>
</tr>
<tr>
<td>Range6</td>
<td>NS6</td>
</tr>
<tr>
<td>Range7</td>
<td>NS8</td>
</tr>
<tr>
<td>Range8</td>
<td>NS9</td>
</tr>
</tbody>
</table>

One or more locking ranges associated with “configured” namespaces, allowing these namespaces to be unlocked separately, with differently configurable access controls.
Secure Messaging

• When managing Opal configuration, the authentication credential is sent from a host (local or network) to the storage device
  • The credential is sent in the clear across the storage interface
    • Could result in capture of an admin credential

• Use Cases:
  • Protects TCG Storage management traffic
    • Allows for secure, remote updates of Opal configuration
    • Traffic could be protected from a back-end management/key server all the way to the storage device
Secure Messaging Specs

• New Specs:
  • Core Spec Addendum: Secure Messaging
    • Maps TLS v1.2 handshake protocol to TCG Storage session startup
      – ISV Opal Management SW is the TLS “Client”, Opal SED is the “server”
  • PSK (Pre-Shared Keys) Feature Sets
    • Map TLS PSKs configuration and usage to the TCG Storage communications protocol
• **PSID Feature Set**
  • PSID = “Physical Security Identifier”
  • The specifies a means to implement a *physical presence credential* (e.g. a password printed on a label).
    • This enables recovery/repurpose/end-of-life in the event of lost/unavailable password
    • Use Cases/Benefits for IT departments, OEMs, IHVs, and ISVs
IEEE 1667 and NVMe

- IEEE 1667 TCG Transport Silo is a requirement for “eDrive” support
  - eDrive in 30 seconds:
    - Starting with Windows 8, MS BitLocker is able to manage SEDs that implement Opal 2.00, Single User Mode Feature Set, and the IEEE 1667 TCG Transport Silo

- IEEE 1667 has begun working on a IEEE 1667 transport technical proposal for NVMe
  - Enables general access to IEEE 1667 silos over NVMe, including 1667 TCG Transport Silo
    - TCG Transport Silo – alternate transport for TCG Opal commands
  - Enables management of Windows eDrive for NVMe Opal SEDs which use Opal 2.00

See [www.ieee1667.com](http://www.ieee1667.com) for more information on IEEE 1667
Plus: Other Recent Storage Security Standards Releases

- **NIST SP 800-88 rev. 1 (Dec 2014)**
  - Provides guidelines for media sanitization, including provisions for NAND-based devices, NVMe interface, and cryptographic erase

- **ISO 27040 (2015)**
  - Provides security guidance for storage systems and ecosystems as well as for protection of data in these systems.

- **TCG Enterprise SSC: Locking LBA Ranges Control Feature Set (May 2014)**
  - Defines mechanisms for additional locking criteria for Locking ranges
Storage Interface Interactions Spec

- TCG Storage Interface Interactions Specification:
  - SIIS v1.03: mappings for UFS, eMMC
  - SIIS v1.04: enhances interactions with T10/T13 Sanitize Feature Sets, minor updates to NVMe interactions
Summary

• A variety of new storage security standards enable broader applicability of TCG Opal and other specs; introduce enhancements to features; and enable increased assurance of implementation.
References

- TCG Storage Specifications
  - http://www.trustedcomputinggroup.org/developers/storage/specifications
- Opal Test Cases Specification (Public Review)
  - http://www.trustedcomputinggroup.org/resources/specifications_in_public_review
    - http://www.trustedcomputinggroup.org/files/resource_files/99188CB2-1A4B-B294-D0DB1CF3A7136274/Opal_SSC_Certification_Test_Cases_v2_00_r1_85_Public%20Review.pdf
- Common Criteria Collaborative Protection Profiles
  - http://www.commoncriteriaportal.org/pps/?cpp=1
- NIST SP 800-88 rev. 1 (Dec 2014)
  - Provides guidelines for media sanitization, including provisions for NAND-based devices, NVMe interface, and cryptographic erase
    - http://csrc.nist.gov/publications/PubsSPs.html
- ISO 27040 (2015)
  - Provides security guidance for storage systems and ecosystems as well as for protection of data in these systems.
- TCG Enterprise SSC: Locking LBA Ranges Control Feature Set (May 2014)
  - Defines mechanisms for additional locking criteria for Locking ranges
    - http://www.trustedcomputinggroup.org/resources/tcg_storage_enterprise_ssc_feature_set_locking_lba_ranges_control_specification
Thank you!
TCG Booth #550