DATA STORAGE SECURITY SUMMIT

01010011 01001110 01001001 01000001

SEPTEMBER 24, 2015
SANTA CLARA, CA

SNIA

Advances in Storage Security Standards

Jason Cox

Intel Corporation

Objectives

- Overview of Trusted Computing Group (TCG) Storage Work Group
- Review of TCG Document types and Goals
- Describe recent specifications and new work
- Discuss work in progress to align with NVMe
- Review the importance of Opal assurance
- Highlight other recent, storage-related security specifications, goals, and benefits

Trusted Computing Group

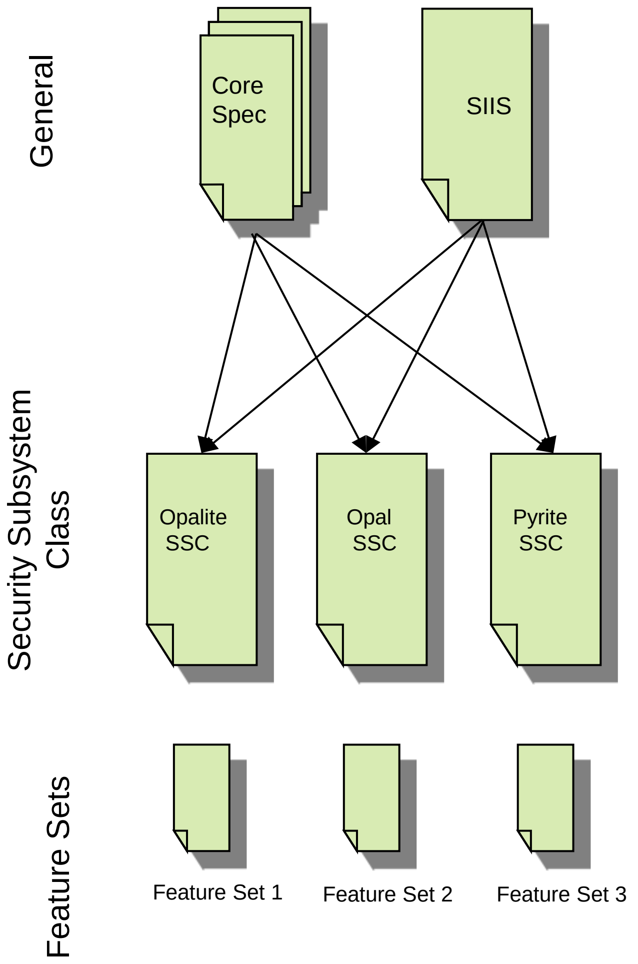
- Trusted Computing Group (TCG)
  - Cross-industry organization formed to develop, define, and promote standards
    - Work Groups focused on TPM, Storage, Networking, Mobile, and more
  - TCG Storage Work Group
    - Defines specifications related to Storage Device-based security features

www.trustedcomputinggroup.org

TCG Storage Specifications

- **Core Specification (Core Spec)**
  - Overall architecture – a description of the underlying constructs to be used in the device specifications.
- **Storage Interface Interactions Specification (SIIS)**
  - Describes the interactions of the TCG SWG specifications with the underlying storage interface protocols, such as ATA, SCSI, USB, etc.
- **Security Subsystem Class (SSC)**
  - Device specifications, consist primarily of a subset of the functionality contained in the Core Spec.
  - Opal, Opalite, Pyrite, Enterprise
- **Feature Sets**
  - These are documents that define extensions to the basic functionality of SSCs.
    - Created to allow for simple extensions to be added to the SSC at a faster pace.
    - Additionally, it allows for features that only appeal to a subset of the market to be standardized.
    - Generally "Optional", may be "Mandatory" by spec (e.g., PSID)

TCG Storage Specifications can be downloaded here: http://www.trustedcomputinggroup.org/developers/storage



TCG Storage WG Goals

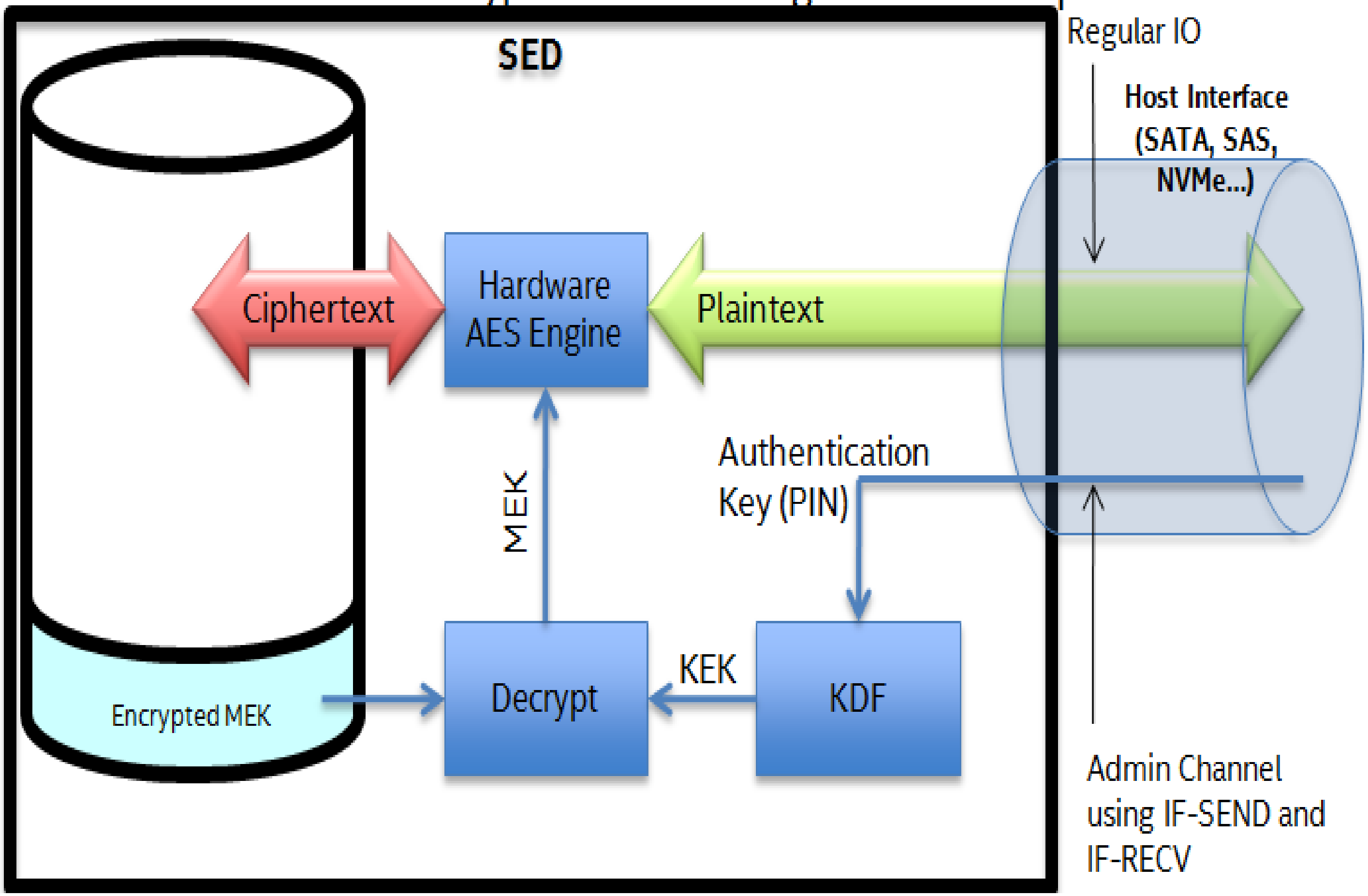
- Expand current use cases
  - Opalite SSC, Pyrite SSC
- Enhance deployability and assurance
  - NVMe/Namespace interactions
  - TCG Storage Opal Test Cases, Collaborative Protection Profile
- Introduce new features based on IT, OEM, IHV, ISV pain points
  - Secure Messaging, PSID
- Expand Opal Threat Model
  - CRAM and TPE

Opal SSC

- 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**
    - **Drive powered off and user has been de-authenticated from system**
- Primary Features:
  - 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.

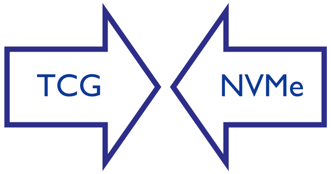
Self-Encrypting Drive (SED)

How the Crypto Works: A High-Level Example



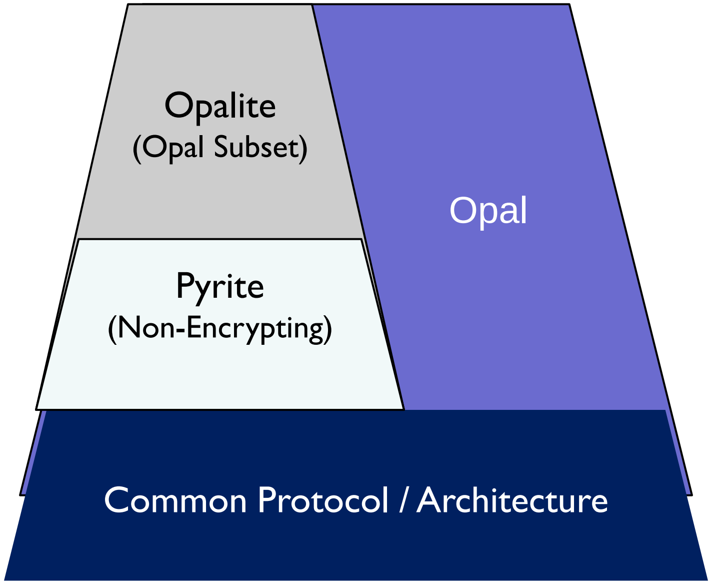
2015 SNIA Data Storage Security Summit. © Intel Corporation. All Rights Reserved.

Opalite SSC and Pyrite SSC



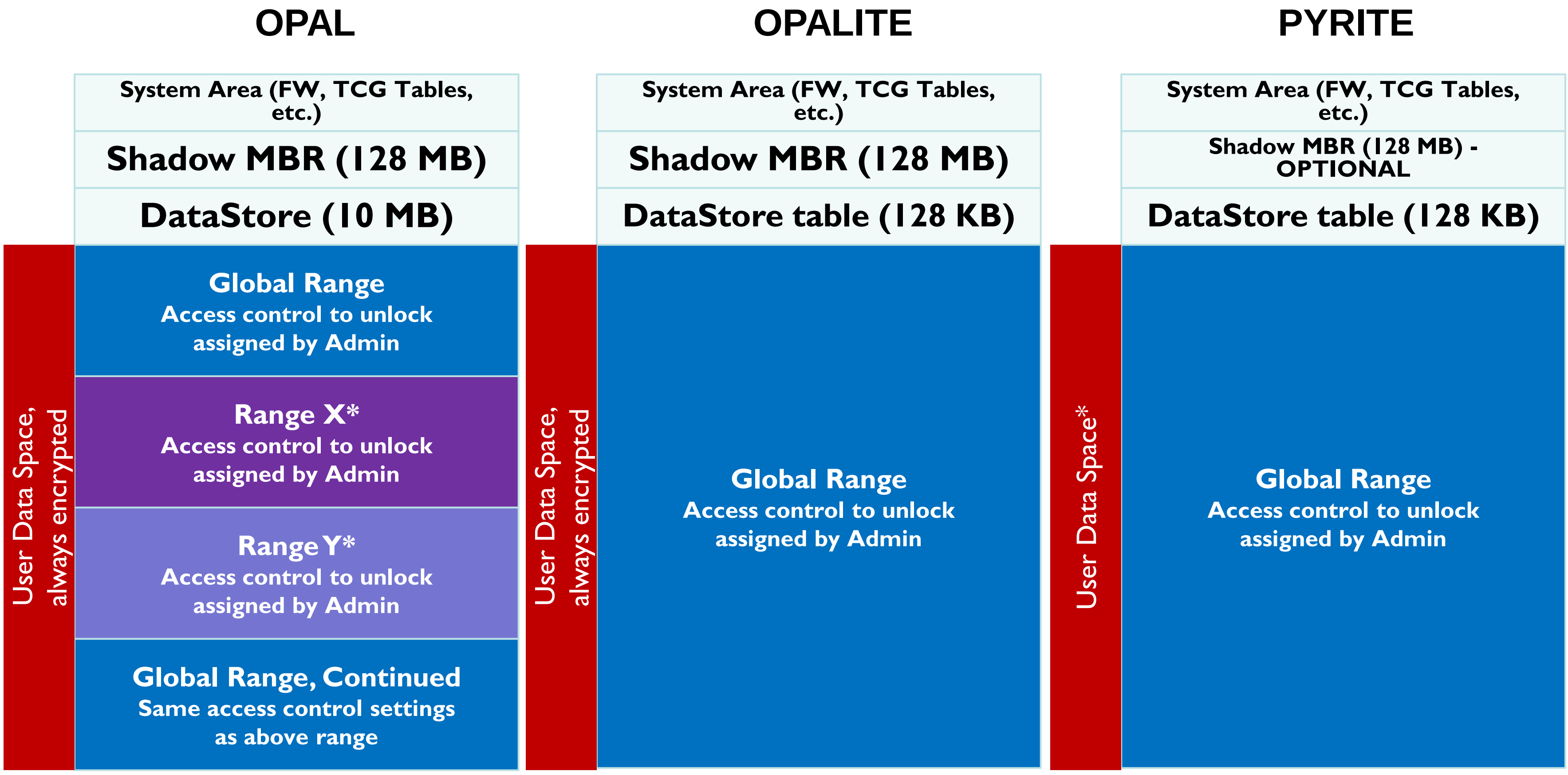
- NVMe's strategy: align on Opal SSC-based solutions for security management
    - Scale across the needs of NVMe in different Client and Enterprise (data center) solutions
- TCG has developed a "family" of specifications to scale across the needs of NVMe in different Client and Enterprise solutions
- SKL Reference BIOS slated to support simple password management via Opal over NVMe

Opal "Family"



Consumers, Enterprise Client Users, and Data Centers are able to take advantage of Encryption via Opal "Family" on NVMe using the same, standardized interface

Opal, Opalite, Pyrite Comparison



OPAL

System Area (FW, TCG Tables, etc.)

Shadow MBR (128 MB)

DataStore (10 MB)

User Data Space, always encrypted

Global Range
Access control to unlock assigned by Admin

Range X*
Access control to unlock assigned by Admin

Range Y*
Access control to unlock assigned by Admin

Global Range, Continued
Same access control settings as above range

OPALITE

System Area (FW, TCG Tables, etc.)

Shadow MBR (128 MB)

DataStore table (128 KB)

User Data Space, always encrypted

Global Range
Access control to unlock assigned by Admin

PYRITE

System Area (FW, TCG Tables, etc.)

Shadow MBR (128 MB) - OPTIONAL

DataStore table (128 KB)

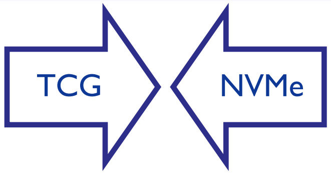
User Data Space*

Global Range
Access control to unlock assigned by Admin

*Opal 2.00 supports Global Range plus at least 8 configurable ranges

*Pyrite SSC does not specify encryption of user data

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

Opalite	
Range	Namespace
Global	NS1
	NS2
	...NSN
Pyrite	
Range	Namespace
Global	NS1
	NS2
	...NSN
Opal	
Range	Namespace
Global	NS1
	NS2
	...NSN
Range1	"Blocked"
Range2	"Blocked"
Range3	"Blocked"
Range4	"Blocked"
Range5	"Blocked"
Range6	"Blocked"
Range7	"Blocked"
Range8	"Blocked"

If multiple namespaces are created, then locking of all are controlled together.

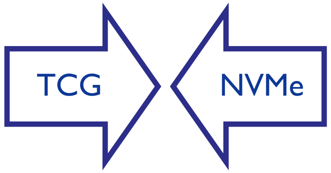
Multiple Locking Ranges

Opalite	
Range	Namespace
Global	NS1
Pyrite	
Range	Namespace
Global	NS1
Opal	
Range	Namespace
Global	NS1
Range1	NS1
Range2	NS1
Range3	NS1
Range4	NS1
Range5	NS1
Range6	NS1
Range7	NS1
Range8	NS1

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.

Range	Namespace
Global	NS1 NS3 NS7
Range1	NS2
Range2	NS4
Range3	NS4
Range4	NS5
Range5	NS6
Range6	NS6
Range7	NS8
Range8	NS9

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

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.

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 or interference with operations
- Use Cases:
  - Protects TCG Storage management traffic
    - Allows for secure, remote updates of Opal configuration
    - Traffic could be protected starting at a back-end management/key server all the way to the storage device

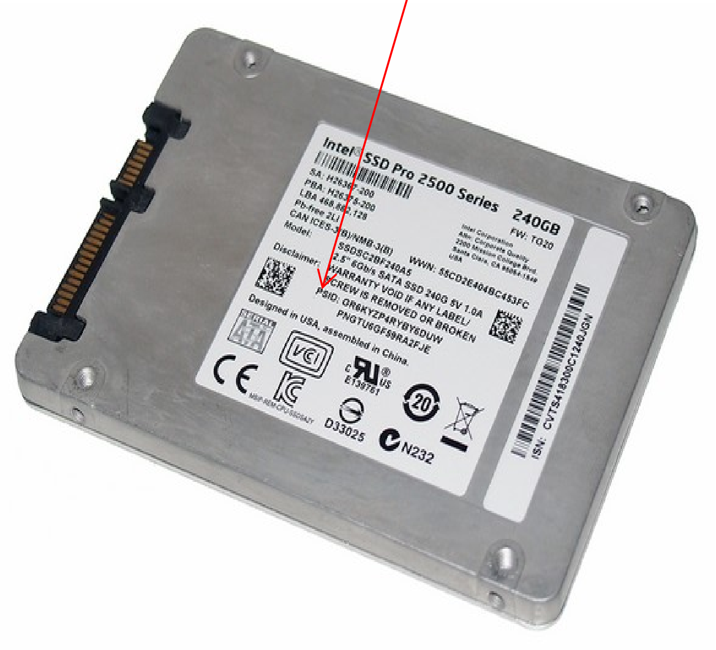
Developing new features and expanding the Opal threat model to increase value.

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

- 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



PSID

Intel SSD Pro 2500 Series
240GB
FW: TG20
Model:
SSDSC2BF240A5
2.5" 6Gb/s SATA SSD 240G 5V 1.0A
WWN: 55CD2E404BC453FC
Disclaimer: WARRANTY VOID IF ANY LABEL/
SCREW IS REMOVED OR BROKEN
PSID: GR6KYZP4RYBY6DUW
PNGTU6GF59RA2FJE
Designed in USA, assembled in China.
D33025
N232
ISN: CVTS418300C1240JGN

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

Storage Integration Guidelines

- TCG Storage Integration Guidelines
  - Reference document intended to provide guidance to IHVs, ISVs, and OEMs related to integration of Opal SEDs into systems.
  - ***Currently in pre-publication review***

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 for more information on IEEE 1667

Opal/SED Enhancements: Expanding the Opal Threat Model

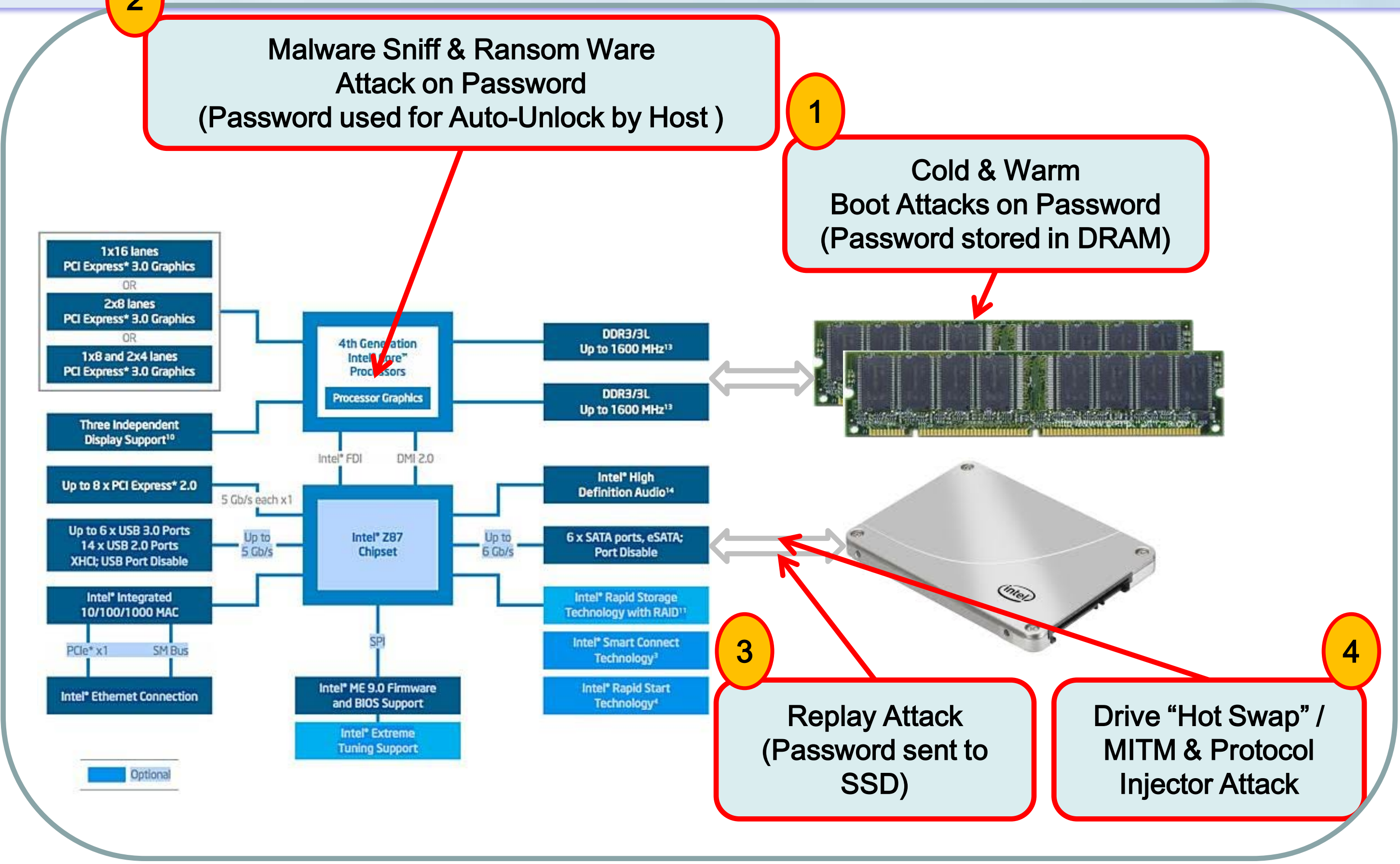
- Recall the Opal Threat Model:
  - **Protect confidentiality of stored user data against unauthorized access once it leaves the owner's control**
    - **Drive powered off and user has been de-authenticated from system**

- Classic conflict between User Experience (UX) and Security exists with SEDs
- Platforms containing SEDs are vulnerable when the SED is unlocked and the user is not present
  - I.e. Stolen laptop in S3 state
- This is due to End User Experience (UX) Expectations:
  - Ease of data access (passwords - ugh!)
  - Fast responsiveness (S3 Resume)
- Which led to Tradeoffs: Auto-Unlock SED during…
  - S3 resume (open lid) & Connected Standby/Always on Always Connected
  - S4/S5 resume still requires user password

User Experience Favored over Platform Security

Exposures in Responsiveness

Note: Password is Handled in clear txt


1x16 lanes PCI Express* 3.0 Graphics
OR
2x8 lanes PCI Express* 3.0 Graphics
OR
1x8 and 2x4 lanes PCI Express* 3.0 Graphics
Three Independent Display Support[10]
Up to 8 x PCI Express* 2.0
5 Gb/s each x1
Up to 6 x USB 3.0 Ports 14 x USB 2.0 Ports XHCI; USB Port Disable
Up to 5 Gb/s
Intel® Integrated 10/100/1000 MAC
PCIe* x1
SM Bus
Intel® Ethernet Connection
Optional
4th Generation Intel® Core™ Processors
Processor Graphics
Intel® FDI
DMI 2.0
Intel® Z87 Chipset
SPI
Intel® ME 9.0 Firmware and BIOS Support
Intel® Extreme Tuning Support
DDR3/3L Up to 1600 MHz[13]
DDR3/3L Up to 1600 MHz[13]
Intel® High Definition Audio[14]
Up to 6 Gb/s
6 x SATA ports, eSATA; Port Disable
Intel® Rapid Storage Technology with RAID[11]
Intel® Smart Connect Technology[3]
Intel® Rapid Start Technology[4]
intel

2 Malware Sniff & Ransom Ware Attack on Password (Password used for Auto-Unlock by Host)

1 Cold & Warm Boot Attacks on Password (Password stored in DRAM)

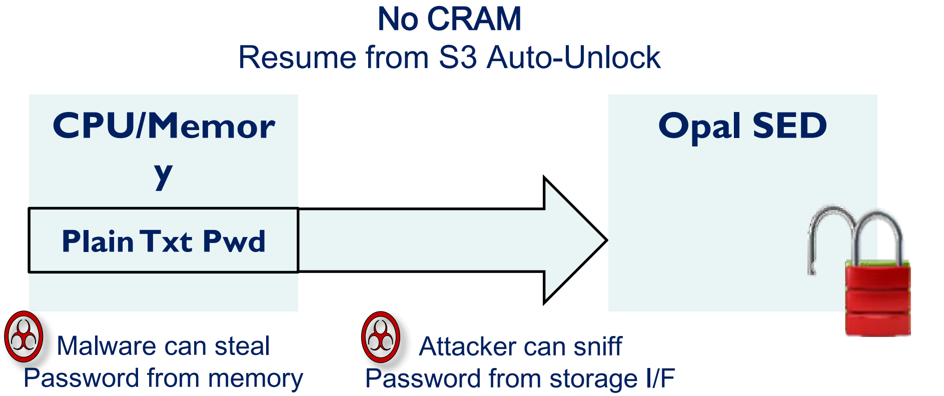
3 Replay Attack (Password sent to SSD)

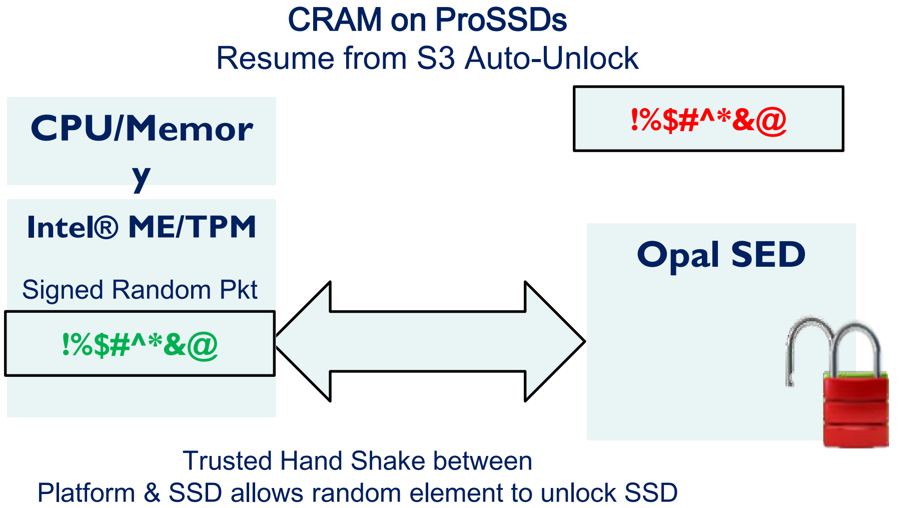
4 Drive “Hot Swap” / MITM & Protocol Injector Attack

Auto-Unlock Provides UX Benefits, but Opens Data Access Security Gaps!

Challenge Response Authentication Method (CRAM)

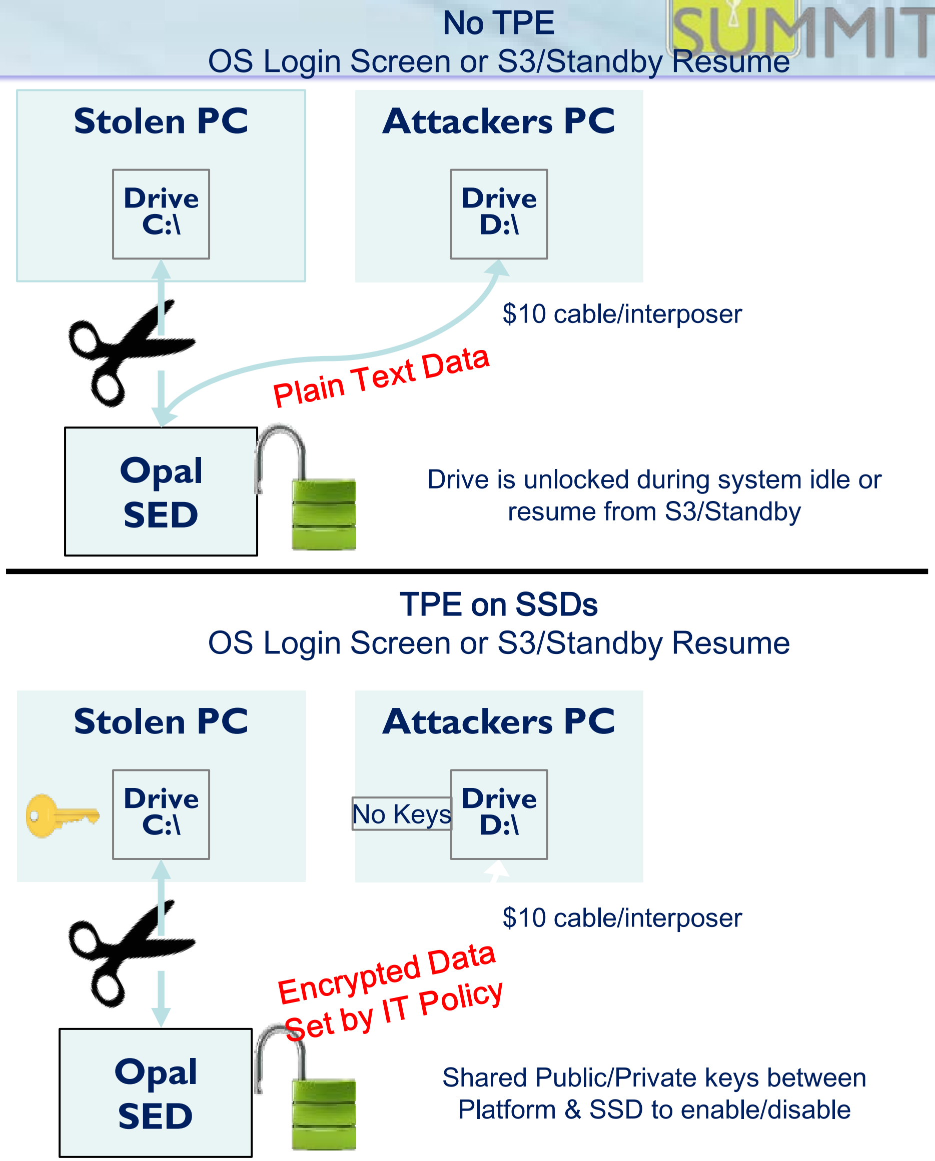
- CRAM introduces a random element into the authentication process
- Prevents sniff/replay of the authentication credential to the drive
- Removes the need to store the password in DRAM
- Signing key can be held securely in a TEE (such as Intel® ME/TPM)


No CRAM
Resume from S3 Auto-Unlock
CPU/Memory
Plain Txt Pwd
Opal SED
Malware can steal Password from memory
Attacker can sniff Password from storage I/F

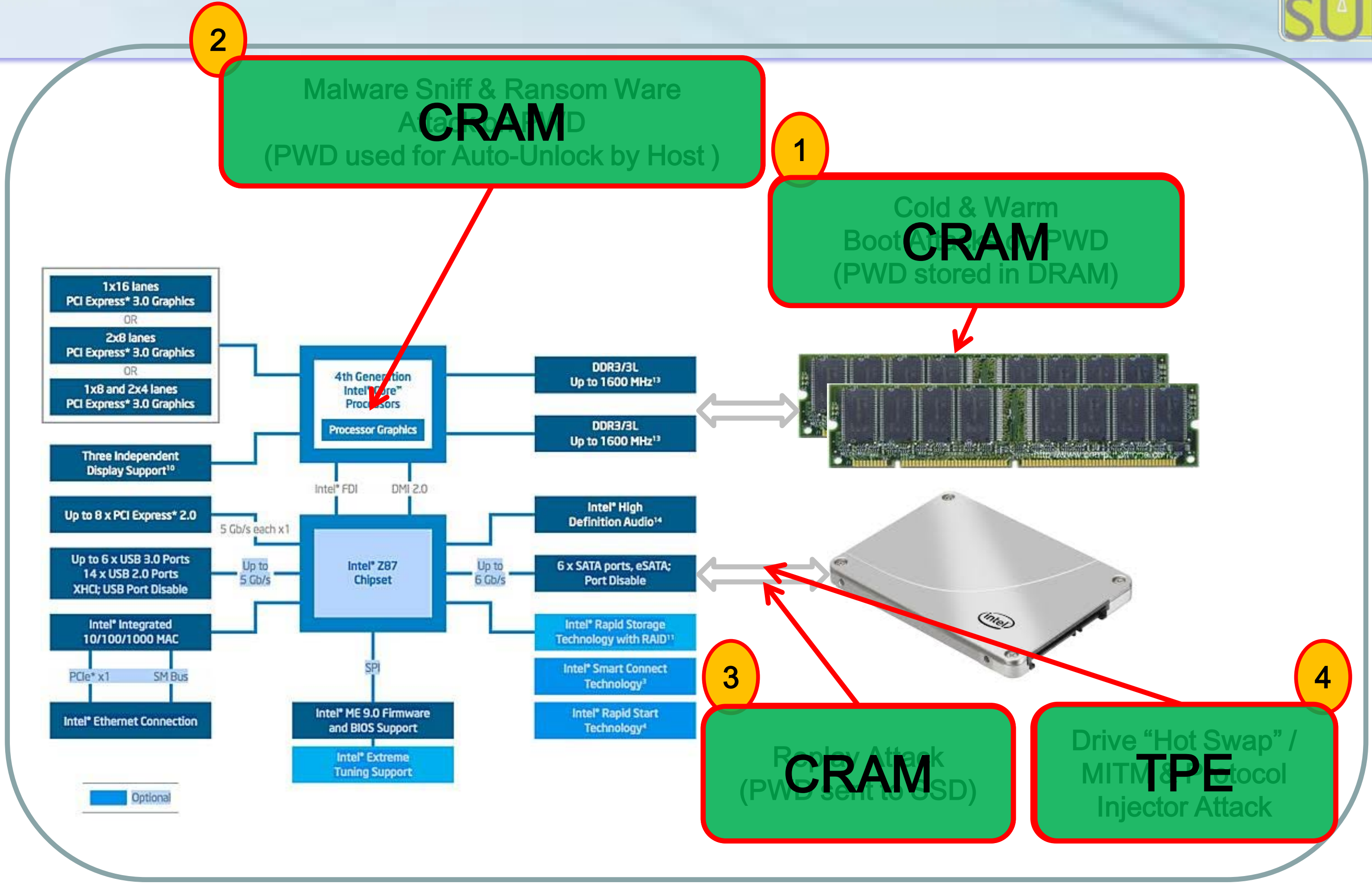

CRAM on ProSSDs
Resume from S3 Auto-Unlock
CPU/Memory
Intel® ME/TPM
Signed Random Pkt
!%$#^*&@
!%$#^*&@
Opal SED
Trusted Hand Shake between Platform & SSD allows random element to unlock SSD

Transport Encryption (TPE)

- TPE encrypts all data over the interface in platform “vulnerable states”
- Enable/Disable of TPE requires cryptographic authentication
- Encryption disabled while user is logged in to the OS (maintains performance)
- Encryption enabled at OS lock screen



Responsiveness with Enhancements



2

Malware Sniff & Ransom Ware Attack on PWD
(PWD used for Auto-Unlock by Host)

CRAM

1

Cold & Warm Boot Attack on PWD
(PWD stored in DRAM)

CRAM

3

Replay Attack
(PWD sent to SSD)

CRAM

4

Drive "Hot Swap" / MITM & Protocol Injector Attack

TPE

1x16 lanes PCI Express* 3.0 Graphics
OR
2x8 lanes PCI Express* 3.0 Graphics
OR
1x8 and 2x4 lanes PCI Express* 3.0 Graphics
Three Independent Display Support
Up to 8 x PCI Express* 2.0
5 Gb/s each x1
Up to 6 x USB 3.0 Ports 14 x USB 2.0 Ports XHCI; USB Port Disable
Up to 5 Gb/s
Intel® Integrated 10/100/1000 MAC
PCIe* x1
SM Bus
Intel® Ethernet Connection
Optional
4th Generation Intel® Core™ Processors
Processor Graphics
Intel® FDI
DMI 2.0
Intel® Z87 Chipset
SPI
Intel® ME 9.0 Firmware and BIOS Support
Intel® Extreme Tuning Support
DDR3/3L Up to 1600 MHz
DDR3/3L Up to 1600 MHz
Intel® High Definition Audio
Up to 6 Gb/s
6 x SATA ports, eSATA; Port Disable
Intel® Rapid Storage Technology with RAID
Intel® Smart Connect Technology
Intel® Rapid Start Technology

Proposed Features Address Exposures while Introducing Minimal Platform Performance Degradation

Bonus: 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

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.
  - http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44404
- 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

Questions?

- Thank you!