STORAGE DEVELOPER CONFERENCE
SDC 21
BY Developers FOR Developers
Virtual Conference
September 28-29, 2021
A SNIA Event

Emerging Storage Security Landscape

Presented by:

Eric A. Hibbard, CISSP, CIPP/US, CISA

Director, Product Planning – Storage Networking & Security, Samsung Semiconductor, Inc.

About the Speaker

Eric Hibbard
CISSP-ISSAP, ISSMP, ISSEP, CIPP/US, CIPT, CDPSE, CISA, CCSK

eric.hibbard@samsung.com

Chair, SNIA Security Technical Work Group
Chair, INCITS TC Cybersecurity and Privacy
Chair, IEEE Computer Society, Cybersecurity & Privacy Standards Committee (CPSC)
Co-Chair, Cloud Security Alliance (CSA) – International Standardization Council (ISC)
Member, American Bar Association – Science & Technology (SciTech) Law Council
Member, American Bar Association – Cybersecurity Legal Task Force
Co-Chair, American Bar Association – SciTech Law – Internet of Things (IoT) Committee
ISO Editor: ISO/IEC 27040, ISO/IEC 27050 (multi-part), ISO/IEC 17788, ISO/IEC 22123 (multi-part), ISO/IEC 20648
IEEE Editor: IEEE Std 1619 (XTS-AES)

Abstract

This session outlines the storage security landscape from the perspective of storage becoming the last line of defense.

Highlights new and emerging storage security elements that may further enhance data security.

Background

Common Threat Actors

- Cyber Terrorists
- Government-sponsored/State-sponsored Actors
- Organized Crime/Cybercriminals
- Hacktivists
- Insiders
- Script Kiddies
- Internal User Errors

Common Motivations

- Political, Economic, Technical, and Military Agendas
- Profit/Financial Gain
- Notoriety
- Revenge
- Multiple/Overlapping

Security is a People Problem!

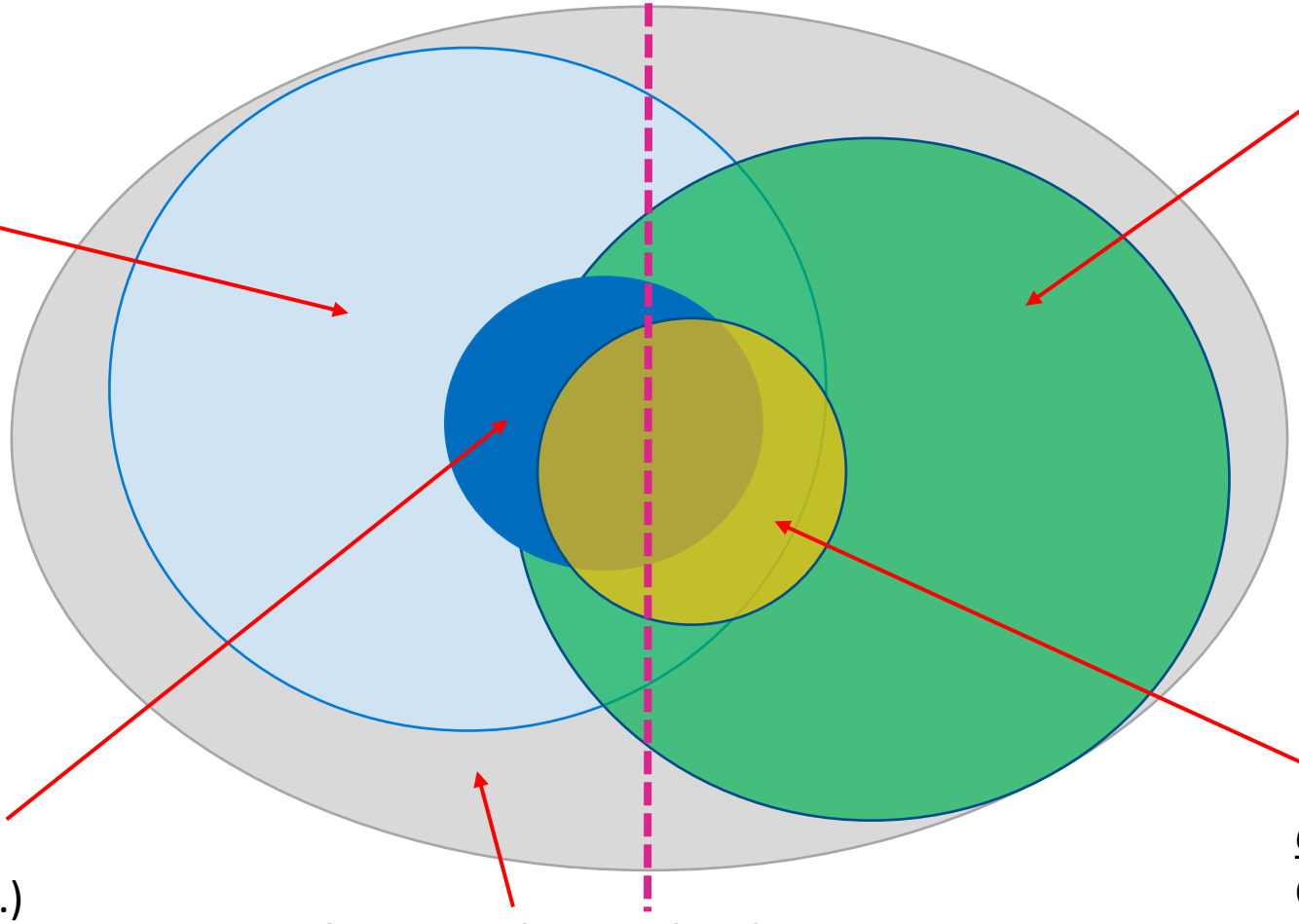
Current Threat Landscape

- Social Engineering
- Advanced Persistent Threat (APT)
- Ransomware/Malware
- Unpatched/Updated Systems
- Security Misconfiguration
- Denial of Service
- Sensitive Data Exposure
- Injection Flaws
- Cryptojacking
- Cyber Physical Attacks
- Broken Authentication
- Broken Access Control
- Third Party (Supplier)
- Insider Theft
- Mobile Malware
- Physical Loss of Devices
- Cross-site Scripting (XSS)
- Man-in-the-Middle Attacks
- IoT Weaponization

Heavily Regulated

Privacy: Collection Limitations, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, accountability

Information Security: Ensures confidentiality, integrity, and availability (CIA) of information



Personal Data Protection: Safeguards applying under various laws and regulations to personal data (PII, PHI, etc.) about individuals that organizations collect, store, use and disclose

Ethics: Moral principles that govern Person's behavior or the conducting of an activity

Cybersecurity: Confidentiality, integrity, and availability of data; identify, protect, detect, respond, recover

Current Storage Security Standards

ISO/IEC JTC 1/SC 27 *Information Security, Cybersecurity, Privacy Protection*

- ISO/IEC 27040:2015 *Storage Security*
  - Guidance standard providing 330+ recommendations/controls
  - Addresses broad range of storage technologies
  - Only international standard addressing storage sanitization
- ISO/IEC 27050-4:2021 *Electronic discovery — Part 4: Technical readiness*
  - Guidance standard that addresses retention and preservation
- ISO/IEC 27031:2011 *Guidelines for ICT technology readiness for business continuity*
  - Guidance standard that includes concepts and principles
  - Provides a framework of methods and processes for improving business continuity

National Institute of Standards and Technology (NIST)

- NIST SP 800-88 Revision 1 *Guidelines for Media Sanitization*
  - Guidance standard or sanitization and disposition
  - Minimum sanitization recommendations & cryptographic erase device guidelines
  - Only international standard addressing storage sanitization
- NIST SP 800-209 *Security Guidelines for Storage Infrastructure*
  - Security guidance for storage deployments
- NIST SP 800-111 *Guide to Storage Encryption Technologies for End User Devices*
  - Guidance for common types of storage encryption technologies

Emerging Storage Security Standards & Specifications

ISO/IEC 27040 *Storage Security* (2nd Ed.)

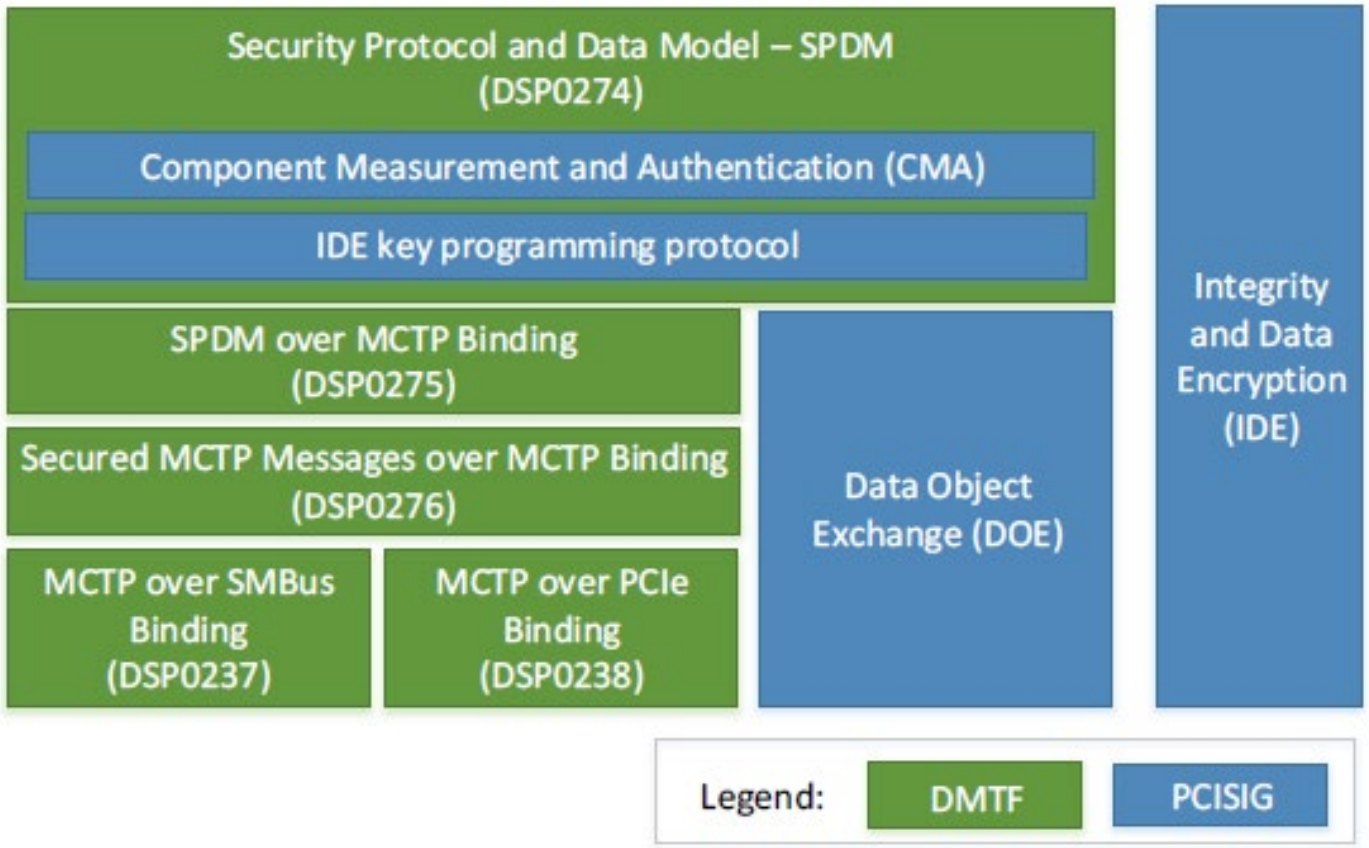
- New standard includes guidance as well as requirements (conformance)
- Target audience is consumers of storage technologies; indirectly impacts vendors
- Updates include:
  - Removal of niche (e.g. FCoE and pNFS) and obsolete technologies (e.g., floppies)
  - New material for securing NVMe-oF and IPMI
  - Significant consolidation of information
  - Removal of technology-specific sanitization annex; leverages IEEE Std. 2883
  - Removal of controls prioritization annex; requirements now the baseline
- Controls restructured to align with new ISO/IEC 27002 (to be published in early 2022)
- Publication anticipated in mid-2022

IEEE 2883 Standard for Storage Sanitization

- Requirements-based standard for sanitizing non-volatile storage (currently just media)
- Identifies three sanitization methods (clear, purge, and destruct)
- For covered media types:
  - Identifies applicable sanitization methods
  - Provides sanitization technique options (when available) for the sanitization methods
  - Specifies the minimum required for each sanitization technique
- Addresses specific techniques such as cryptographic erase and degaussing
- Provides guidance on verification of sanitization outcomes

- Note: When published in early 2022, it is expected to be the go-to standard for sanitization

PCI-SIG® & DMTF Specifications for Security



Source: PCI-SIG

SPDM defines a "toolkit" for authentication, measurement, and other security capabilities

CMA defines how SPDM is applied to PCIe devices/systems

DOE supports Data Object transport between host CPUs & PCIe components over PCIe

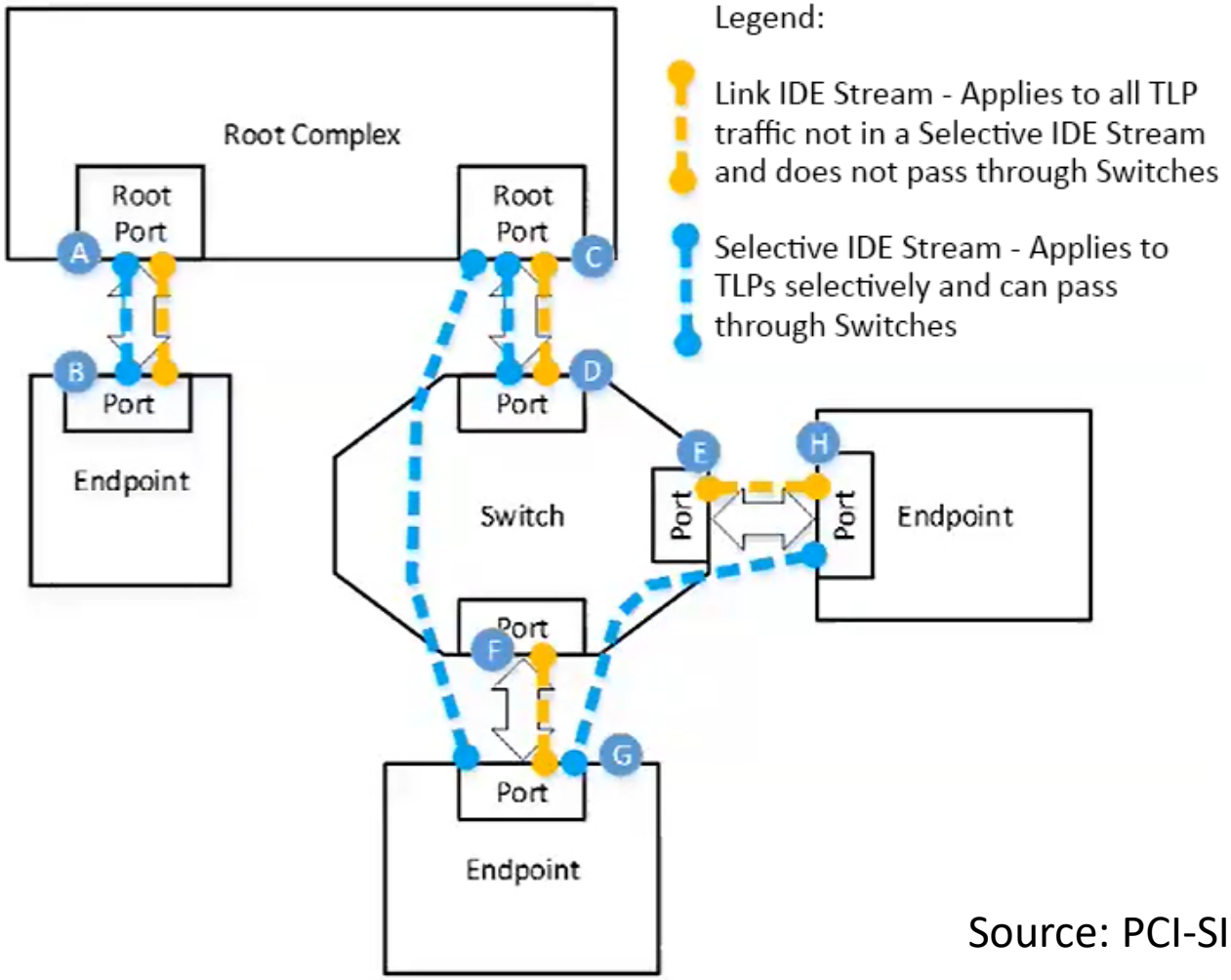
Various MCTP bindings support Data Object transport over different interconnects

IDE will typically use this toolkit for key exchange, but can use other mechanisms for keys

PCIe® Component Authentication

- To effectively validate authenticity, component authentication needs to support the five phases in a component's lifecycle:
  - **Component Manufacturing**: Each component needs to be authenticatable at any time during the manufacturing process by an appropriate test device.
  - **Component Integration:** Prior to installing a component in an enclosure or an enclosure into a rack or larger enclosure, the integrator or manufacturer needs to verify its authenticity.
  - **Initialization and Power Cycle Events**: Authentication needs to be performed whenever a component or enclosure is initialized or power cycled.
  - **Runtime**: Authentication needs to be performed on-demand to support application or customer-specific validation prior to or during application or service operation. Further, authentication needs to be initiated whenever a component exits a deep low-power state.
  - **Component Addition or Replacement**: Authentication needs to be performed whenever a component is added or replaced.
- Component authentication via industry standard security data objects enables vendors and customers to verify that every component is genuine and from a trusted manufacturer.

PCIe® Technology Integrity and Data Encryption (IDE)



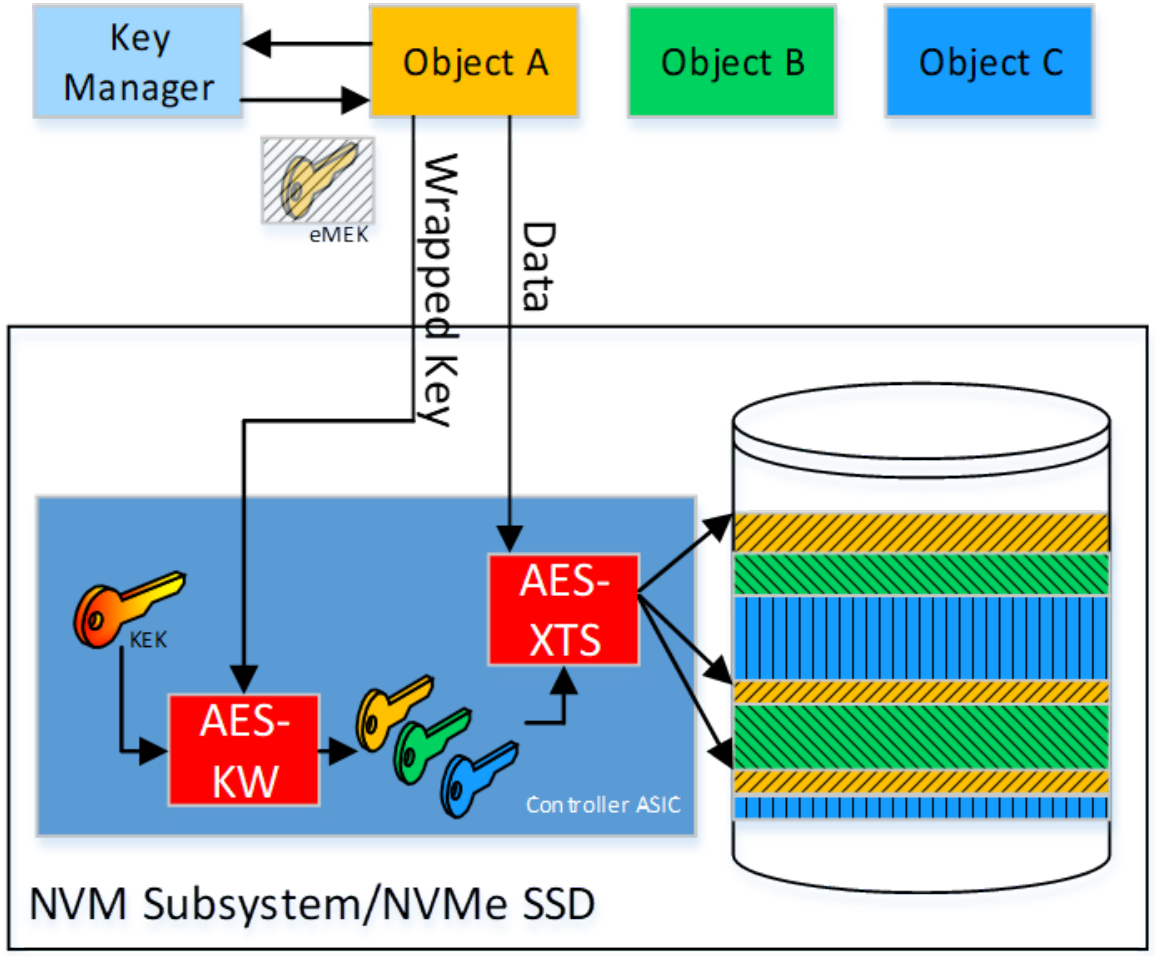
Source: PCI-SIG

Provide confidentiality, integrity, and replay protection for PCIe Transaction Layer Packets (TLPs)

Link level encryption protects against physical attacks by prevention of reading confidential data, modification of TLP contents, and reorder or deletion of TLPs

AES-GCM is used as the encryption for the TLP Data Payload.

NVMe & TCG Key Per IO (KPIO)



Source: NVM Express

Leverage high speed encryption in the storage device, but centrally generate and manage keys external to the device.

Encrypted Media Encryption Keys (MEKs) are wrapped and injected into Self Encrypting Drive key cache (volatile memory) and assigned a “Key Tag”

Subsequent I/O can use the “Key Tag” to encrypt/decrypt data to/from the storage device in a non-contiguous fashion

NVMe spec adds capability; TCG Key Per IO SSC provides most of the details

Miscellaneous/Noteworthy

- US Government encouraged to use Zero Trust Architectures; others looking at “trustworthiness”
- ISO/IEC 27001 to undergo revision
  - Annex A controls to be aligned with new ISO/IEC 27002
  - Leveraging an amendment approach; minimizing changes
  - Publication anticipated in 2022
  - Existing ISO/IEC 27001:2013 certifications expected to be invalid after 12-month phase-in; necessitate many new recertifications in 2022/2023
- Adoption of TLS 1.3 is progressing; probably one black-swan event away from abandoning earlier TLS versions

Thank you for Your Time!

Please take a moment to rate this session.

Your feedback is important to us.

