SNIA COMPUTE + MEMORY + STORAGE SUMMIT

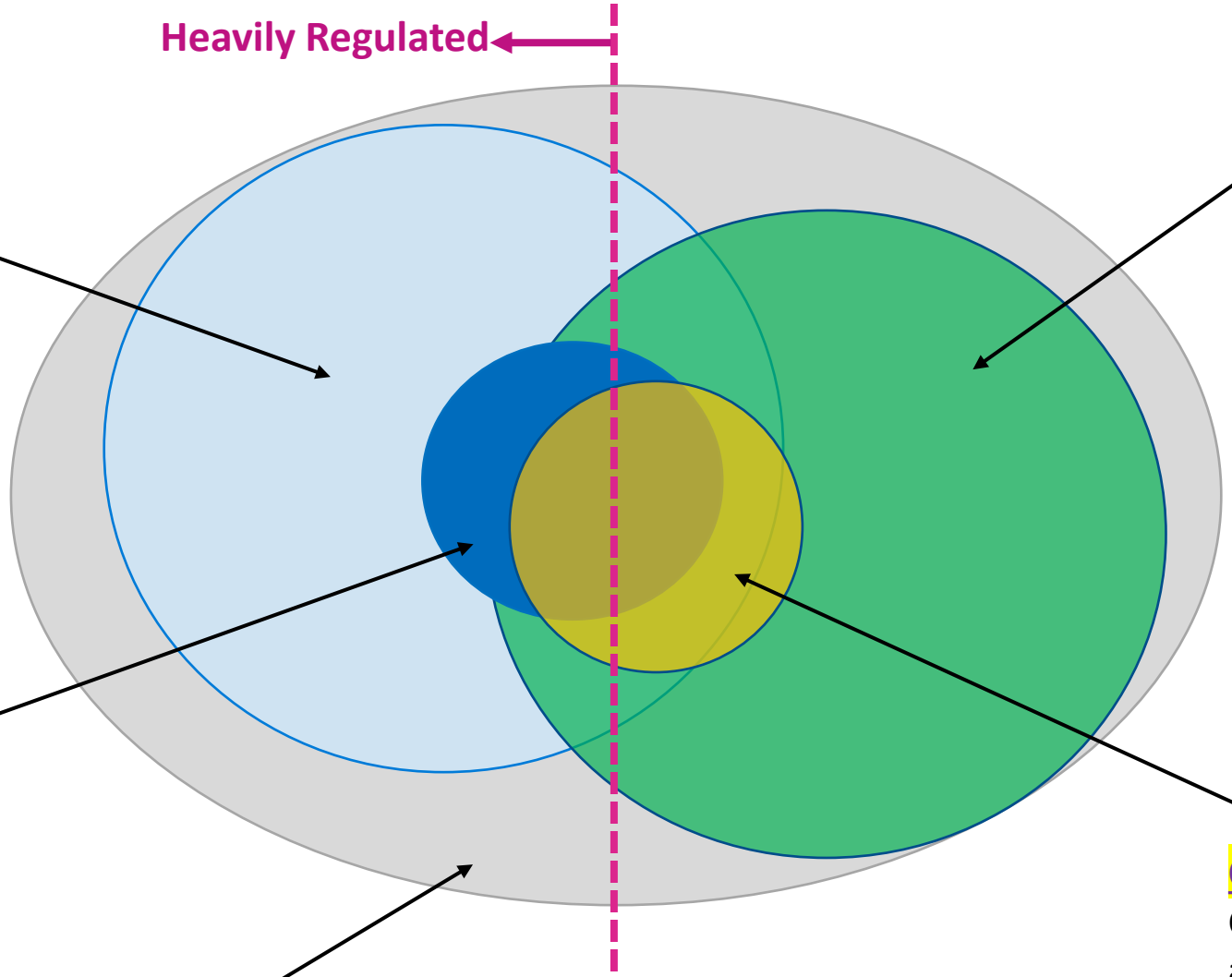
Architectures, Solutions, and Community
VIRTUAL EVENT, APRIL 11-12, 2023

Storage Security – Past, Present, and Future

Eric Hibbard, CISSP, FIP, CISA
Chair, SNIA Security TWG
eric.Hibbard@samsung.com

Privacy: Collection Limitations, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, Accountability

Heavily Regulated



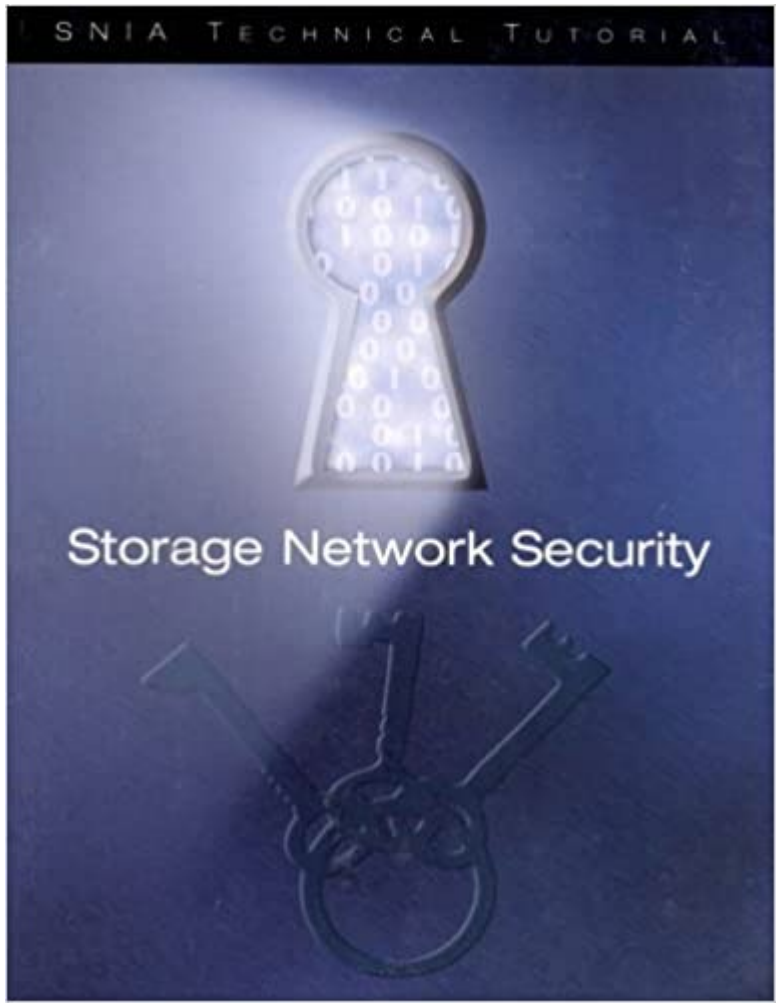
Information Security: Ensures Confidentiality, Integrity, and Availability (CIA) of information

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 a person's behavior or the conducting of an activity

Cybersecurity: Ensures Confidentiality, Integrity, and Availability of data; Identify, Protect, Detect, Respond, Recover

Storage Security – Past



SNIA Technical Tutorial: Storage Network Security

January 2003

by Roger Cummings and Hugo Fruehauf

Early SNIA Storage Security Adventures

- Storage Security Industry Forum (SSIF)
- Storage Security Summits [2005-2008, 2015-2016, 2022]
- SNIA Storage Security Tutorials (US, EU, JP, IN) [2003-2015]
- SNIA Best Current Practices [2007 & 2010]
- SNIA Storage Security Whitepaper (2008-2016)
- SNIA Technical Position: Storage Management Initiative Specification (SMI-S) v1.0 [2007]
- SNIA Technical Position: Cloud Data Management Interface (CDMI) v1.0 [2007]
- SNIA Standard: TLS Specification for Storage Systems v1.0.1 [2014]

- Early focus on securing storage networks, data at-rest encryption, and storage management

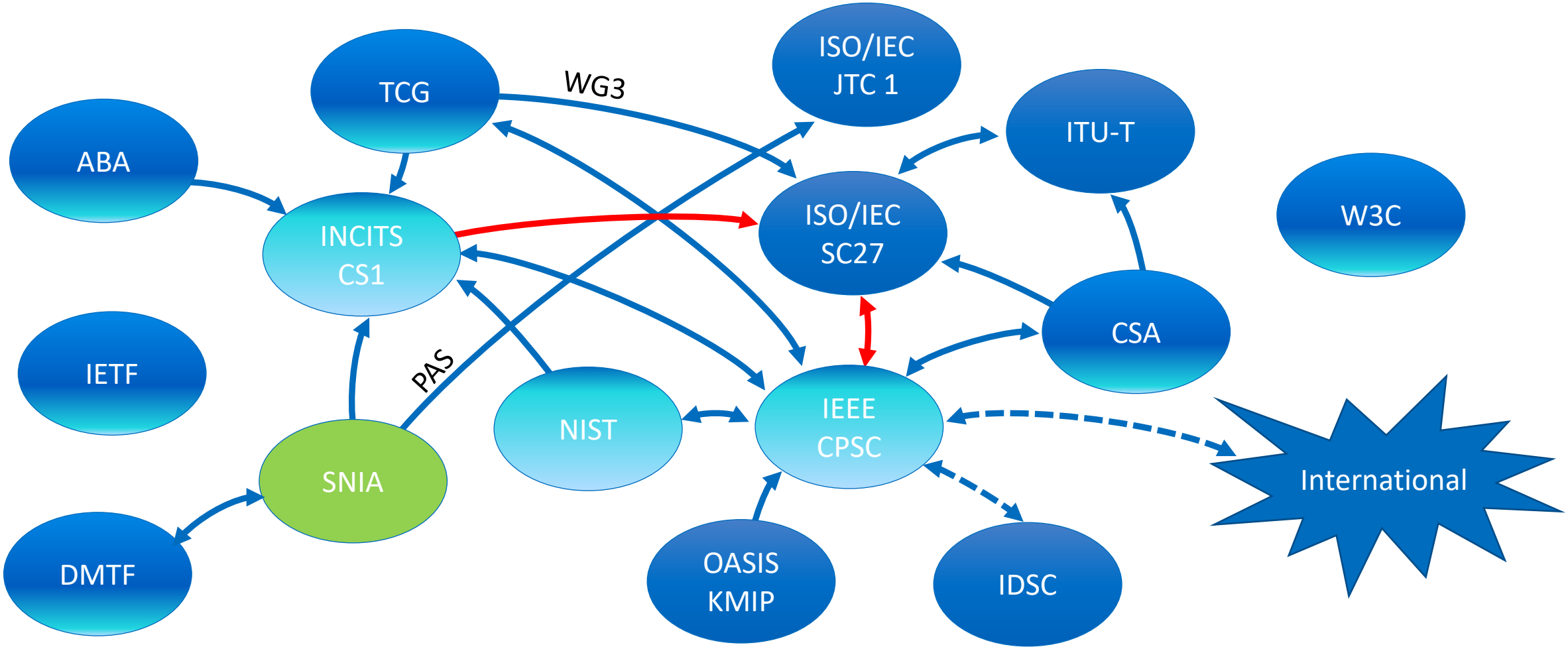
Early Standards Covering Storage Security

- ISO/IEC 27040:2015, *Information technology – Security techniques – Storage security*
- NIST SP 800-88 Revision 1 [2014], *Guidelines for Media Sanitization*
- NIST SP 800-209 [2020], *Security Guidelines for Storage Infrastructure*
- INCITS 496-2012, Information Technology - Fibre Channel - Security Protocols - 2 (FC-SP-2)
- TCG Storage Security Subsystem Class: Enterprise [2009]/Opal [2015]

- Broad security recommendations (optional) for storage systems and ecosystems as well as eradicating data on storage (storage sanitization)

Storage Security – Present

Key Storage Security Players



State of Storage Security

- Security controls are an element of all storage specification/standards
- Transitioning from guidance/recommendations (optional) to requirements for implementations; use is still optional
- Data at-rest encryption is ubiquitous; increased interest in data in-motion encryption
- Storage sanitization (clear, purge, destruct) is mandated in many jurisdictions; proof of data eradication is an area of concern
- Storage security is an element of information systems auditing

ISO Storage Security Standard Gets a Refresh

- The original ISO/IEC 27040 (Storage security) was published in January 2015 as a guidance standard
- ISO/IEC 27040 is being updated
  - Scope has been expanded to include requirements (baseline)
  - Restructured to align with ISO/IEC 27002:2022 (Organizational, People, Physical, Technological Controls)
  - Technology refreshed (NVMe-oF, IPMI, archives)
  - Defers to IEEE Std 2883 on specifics of media-sanitization
- Publication anticipated in mid-2023

Additional Considerations

- Product-based Security Certifications
  - Transition to FIPS 140-3
  - Transition to Common Criteria:2022 (ISO/IEC 15408)
- Open Compute Project (OCP)
  - Security – Attestation, measurements, change of ownership, recovery
  - Storage – NVMe SSD specifications (with security requirements)

Storage Security – Future

Storage Security Developments

- NVMe™ over Fabrics (NVMe-oF™)
  - Security can vary significantly based on the transports
- Computational Storage – Security Considerations in Architecture
  - Specific mechanisms (e.g., NVMe) are TBD
  - Multi-tenancy add complexities
- Key Per I/O
  - Fine-grain encryption using SSD encryption engine and host-based key management
- DMTF Security Protocols and Data Models (SPDM)
  - Authentication/attestation mechanism to establish trust
  - Communications security
- PCIe® Data Object Exchange (DOE) and Integrity and Data Encryption (IDE)
- Compute Express Link™ (CXL™) Security

Storage Security Event Horizon

- Privacy Preserving Computing Technology
  - Trusted Execution Environments (TEE)
  - Homomorphic Encryption
- OCP Caliptra
  - Silicon IP block for a Root of Trust for Measurement (RTM)
  - Targeting system on a chip (SoC) and ASICs in the hyperscaler/datacenter space

Summary

Concluding Remarks

- Storage security has matured significantly over the past 20 years
- Storage systems and ecosystems are now a viable part of a defense in-depth strategy and may serve as the last line of defense for data
- There are clear indications that new storage security capabilities may emerge over the next few years; “customer” adoption is uncertain
- Significant number of players and interdependencies; may complexities

- Bottom Line: Failure to secure storage could have legal and/or regulatory repercussions (reasonable security)

Where to Get Involved

- SNIA™ Security TWG and Data Protection & Privacy Committee
- IEEE Security in Storage WG (SISWG)
- INCITS Technical Committee Cybersecurity & Privacy
- Open Compute Project® (OCP) Security Project
- Trust Computing Group® (TCG) Storage WG
- PCI-SIG®
- NVM Express® (NVMe®)
- DMTF®
- Compute Express Link™ (CXL™) Consortium
- Confidential Computing Consortium™ (CCC)

SNIA COMPUTE + MEMORY + STORAGE SUMMIT

Architectures, Solutions, and Community
VIRTUAL EVENT, APRIL 11-12, 2023

Please take a moment to rate this session.

Your feedback is important to us.

