Storage Security – Year in Review

Eric Hibbard, CISSP, FIP, CISA
Samsung Semiconductor, Inc.

SNIA COMPUTE, MEMORY, AND STORAGE SUMMIT

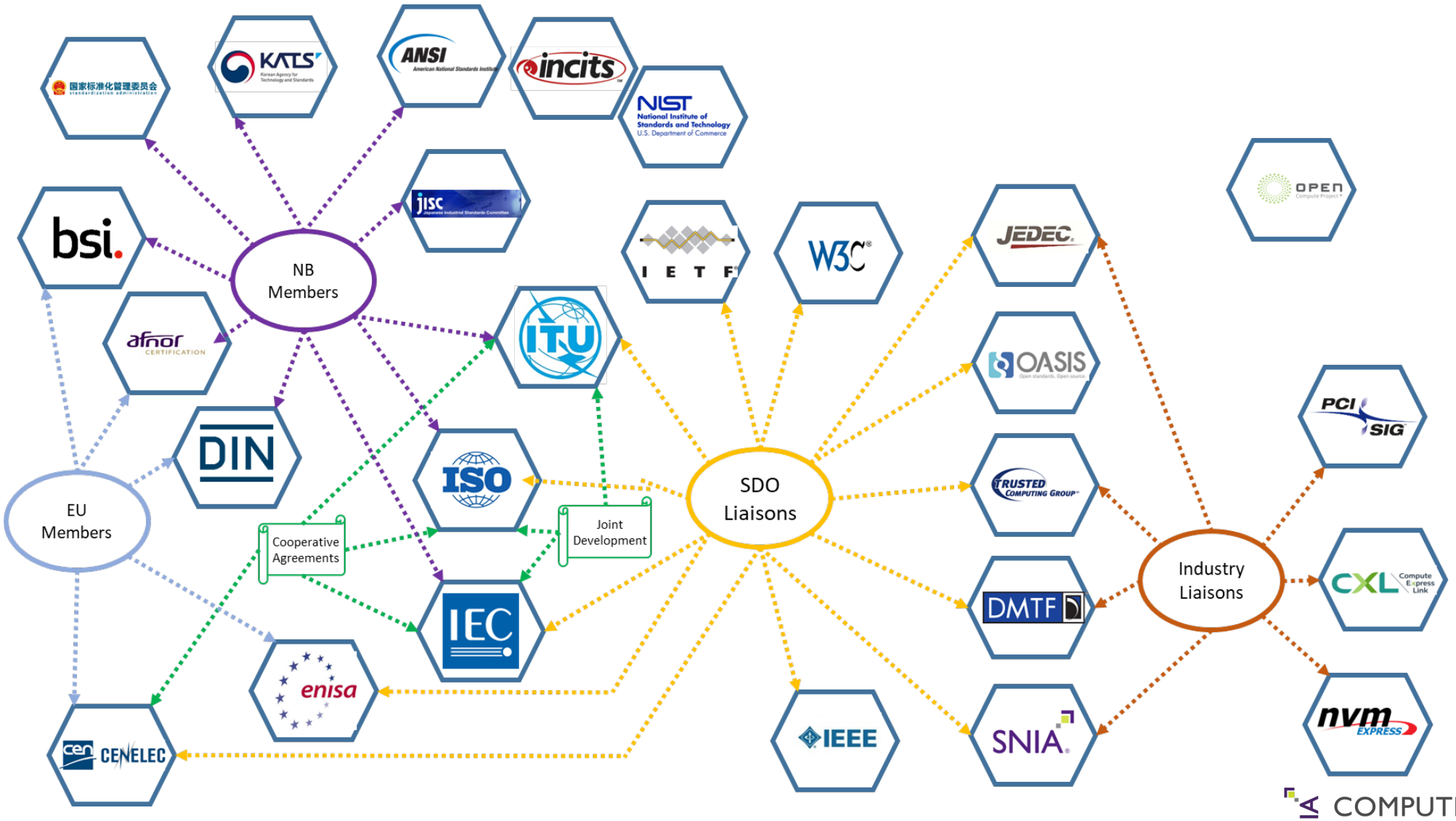
Solutions, Architectures, and Community
VIRTUAL EVENT, MAY 21-22, 2024

Threat Summary

- Ransomware with data exfiltration (hybrid attacks)
- Supply chain attacks (service providers)
- Cyber attacks
  - Critical infrastructure (nation state actors)
  - Healthcare
  - Banking & finance or government (organized crime)
- Data breaches (new malware, vulnerabilities, etc.)

- AI is emerging as a new tool for attackers

Standards and Industry Players



ISO/IEC 27040:2024-01 (Storage security)

- Comprehensive coverage of storage security
- Includes both requirements and guidance (includes auditor checklists)
- Covers organizational, people, physical, and technological controls
- Defers to IEEE Std 2883 for media-specific sanitization (old Annex A removed); verification and cryptographic erase clarified
- Many new controls (e.g., IPMI, NVMe-oF™, storage systems security, data archives and repositories, and cyber-attack recoveries)

- ISO/IEC 27002:2022 references to ISO/IEC 27040 for backup security and media sanitization, resulting in increased visibility of storage security

IEEE Security in Storage (SISWG)

- Building upon IEEE 2883-2022 (Storage Sanitization)
  - Draft P2883.1 Recommended Practice for Use of Storage Sanitization Methods
  - Draft P2883.2 Recommended Practice for Virtualized and Cloud Storage Sanitization
  - Draft P3406 Standard for a Purge and Destruct Sanitization Framework
  - P1667 Standard for Discovery, Authentication, and Authorization in Host Attachments of Storage Devices (Revision)
- Revision of IEEE 1619 (XTS-AES)
  - Draft P1619 Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices
  - Working with NIST for a future update of NIST SP 800-38E

Trusted Computing Group

- Storage WG
  - TCG Key Per I/O (SSC and AppNote published; Test Cases under development)
  - TCG Opal SSC (errata for v2.02; v2.3 under development)
  - Revision of TCG Storage Architecture Core Specification v3.0 initiated
  - Multiple feature sets under revision/development
- Attestation
  - TCG Attestation Framework – Part 1: Terminology, Concepts, and Requirements under development
- DICE
  - TCG DICE Protection Environment Specification v1.0 under development
  - TCG DICE Concise Evidence Binding for SPDM v1.0 published
  - TCG Hardware Requirements for a Device Identifier Composition Engine v1.0 published

OCP – Security & Storage

- *OCP Datacenter NVMe® SSD Specification* v2.5 published; significant update to security requirements
- *OCP Caliptra: A Datacenter System on a Chip (SOC) Root of Trust (RoT)* v1.0 published
- *OCP Layered Open-source Cryptographic Key-management (L.O.C.K.)* under development
- OCP Security Appraisal Framework and Enablement (S.A.F.E.) program established

SNIA – Security/Data Protection

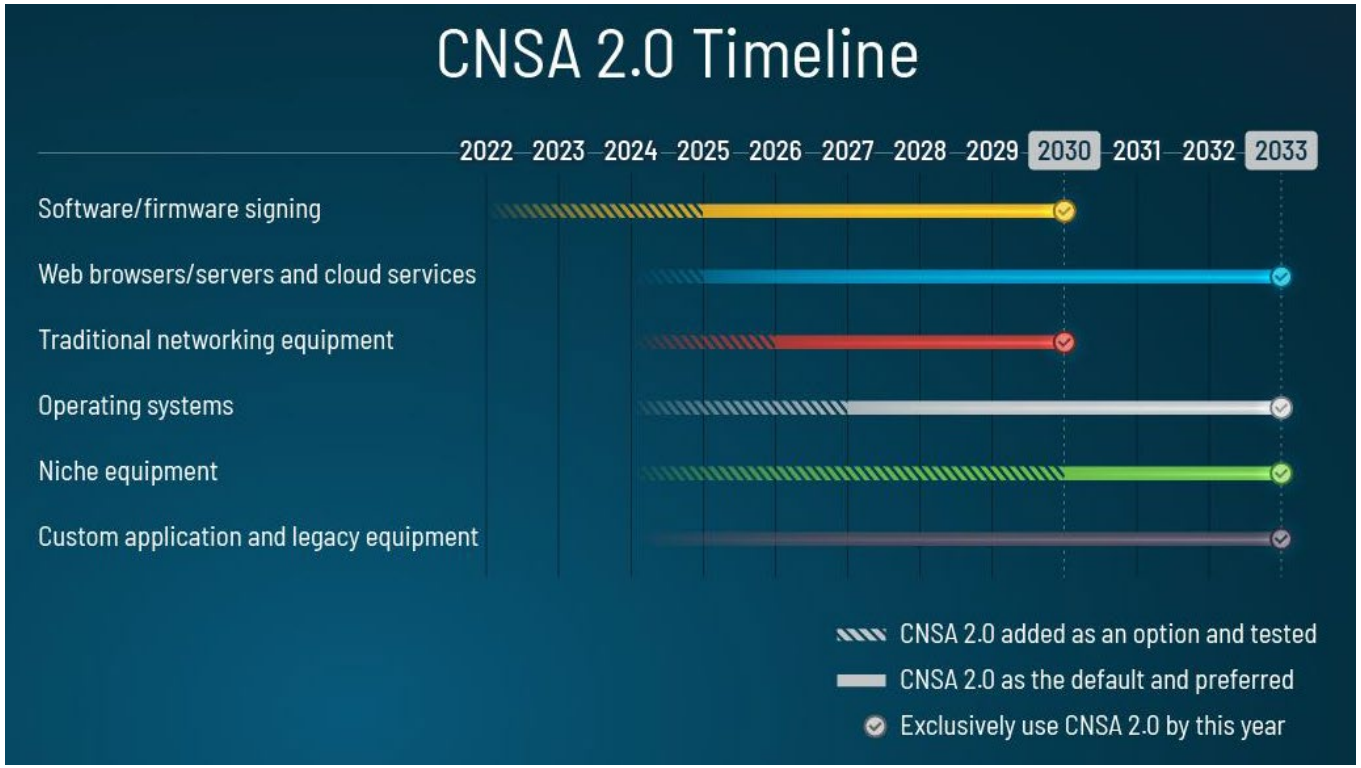
- *SNIA Storage Security: Encryption and Key Management* technical paper published
- *SNIA Storage Security: Fibre Channel Security* technical paper published
- Revision of *SNIA TLS Specification for Storage Systems* v2.2 and ISO/IEC 20648 (2nd ed.) underway
- Revision of *SNIA Data Protection Best Practices* technical paper underway

Additional Relevant Activities

- DMTF
  - Component Measurement and Authentication (CMA)/SPDM and PCIe IDE
  - DMTF Secure Protocol and Data Model (SPDM) v1.3 published; v1.3.1 under development
- Peripheral Component Interconnect Special Interest Group (PCI-SIG™)
  - PCI Express® (PCIe®) Integrity and Data Encryption (IDE)
  - PCIe TEE Device Interface Security Protocol (TDISP)
- Compute Express Link® (CXL®) 3.1 Specification
- NVM Express® over Fabric (NVMe-oF™)

Post Quantum Cryptography (PQC)

- NIST released draft FIPS 203 (CRYSTALS-Kyber), FIPS 204 (CRYSTALS-Dilithium) and FIPS 205 (SPHINCS+)
- NSA released Commercial National Security Algorithm Suite (CNSA) v2.0



Summary

- The threat landscape continues to evolve
- Security requirements for storage are increasing
  - Attestation and link encryption
  - Platform and device security
- Complexities and interdependencies are increasing

- PQC requirements and timelines are poised to be disruptive to both customers and vendors

Please take a moment to rate this session.

Your feedback is important to us.