Status Report on Storage Security Initiatives

Eric A. Hibbard, CISSP, CISA
Sr. Director, Data Networking Technology
Hitachi Data Systems

Abstract

- This presentation will review the storage security initiatives that have been undertaken in various standards organizations subsequent to the first SNIA Security Summit held in 2002. It will present an overview of each activity, and compare and contrast the characteristics of the specifications being produced. It will also attempt to identify and prioritize any "gaps" that may exist, and propose future SNIA activities to address those issues.
- **Learning objectives:**
  - Learn about the storage security activities underway in a number of organizations, including INCITS (T10, T11, CS1), IEEE (P1619 & P1667), Trusted Computing Group (TCG), Distributed Management Task Force (DMTF) as well as SNIA
  - Identify the specific threats be addressed by each technology
  - Characterize each technology and identify its strengths and weaknesses
  - Identify best practices for the deployment of combinations of all of the technologies

Enter the *Wayback Machine*…

Back in 2000….

- SNIA formed a Security Technical Work Group (TWG) & started working on Storage Security
  - Very little awareness of security in the storage & SAN industries….
  - So started creating educational resources
    - SNW Tutorials
    - SNIA Technical Seminar Series booklets
    - SAN Risk Assessments
    - Best Practices
- Storage Security Industry Forum (SSIF) formed later to complement to TWG

Courtesy of Roger Cummings

….Then in 2002….

- SNIA organized the first Storage Security Summit
  - Held @ SNIA Tech Center, Colorado Springs
  - Brought key storage technical people and security experts together for the first time
- Started a twice yearly schedule in 2005
  - Slide presentations available at snia.org to SSIF members!

Courtesy of Roger Cummings

Fast Forward to Today…

SNIA Security Vision & Mission

- **Vision (SNIA desired future state):**

  The security vision of the SNIA is to enhance information assurance, optimize security investments while maintaining present operational effectiveness in the disparate technologies and standards that work together to form today's storage ecosystems.

- **Mission (what SNIA is trying to achieve):**

  The security mission of the SNIA is to produce high quality educational, technical and engineering collateral that influences the design, use, and management of storage networking technology to better protect and secure information.

  This may include participation in standards development, educational seminars, best practice documents, conferences, videos, and other activities to advance the SNIA security vision.

SNIA Security Goals

- **Goal #1:** Assist the SNIA membership in better understanding Information Assurance and how it applies to the storage ecosystem.
- **Goal #2:** Identify and incorporate prudent security mechanisms in all SNIA technical specifications.
- **Goal #3:** Continue striving to become a recognized expert/authority in data/information security

Storage Security Industry Forum

- 2008 Security Summit
  - Attempted to bring in ISSA and ISACA members
  - Key note address from ABA (e-Discovery)
  - R&D component from UC Santa Cruz
  - Status of future Security Summits is unknown
- Other Activities
  - Multiple talks for SNW
  - Data At-rest Solutions Guide
  - Recruiting security companies for membership
  - Outreach to storage security organizations (e.g., IEEE)
  - Awareness talks for SNIA affiliates

Security TWG

- Active Projects
  - Quarterly Report: *Standards Relevant to Storage Security*
  - Whitepaper: *SNIA Storage Security Best Current Practices (BCPs) v2.1*
  - Whitepaper: *Storage Security Professional's Guide to Skills and Knowledge*
  - Report: *Compliance and Storage Security – 2008*
  - Storage networking guidance for INCITS/CS1 *Small Organization Baseline Information Security Handbook (SOBISH)* activity
- Outreach to Affiliates
  - SNIA-Europe Collaboration on Compliance tutorial for SNW
  - SNIA-ANZ F2F briefing (Security Expo 2008) on storage networking security, encryption, storage security standardization (Aug-2008).
  - SNIA-J F2F Briefing on the BCPs v2.1 (Jul-2008)
- Internal SNIA Support
  - SMI-S 1.4.0, Part 1, Clause 13 – Security
  - Education Committee – Storage Security Exam

Meanwhile, Back At the Standards Ranch…

Relevant Standards Bodies

- *Internet Engineering Task Force (IETF)*
- *InterNational Committee for Information Technology Standards (INCITS)*
- *IEEE P1619 Security in Storage Working Group (SISWG)*
- *IEEE P1667*
- *ISO/IEC JTC1 SC27 IT Security Techniques*
- *Storage Networking Industry Association (SNIA)*
- *Distributed Management Task Force (DMTF)*
- *Trusted Computing Group (TCG)*

IETF

- Security
  - Numerous RFCs on security protocols, algorithms, authentication, and other security mechanisms (e.g., TLS, IPsec, Syslog, RADIUS)
- IT Infrastructure
  - Numerous RFCs on information & communications technology (ICT) infrastructure (e.g., DNS, NTP, LDAP, SLP)
- IP Storage
  - Multiple RFCs on *Internet Small Computer System Interface (iSCSI)*
  - RFCs on Fibre Channel over TCP/IP *(FCIP)* and *iFCP - A Protocol for Internet Fibre Channel Storage Networking*
  - RFCs detailing MIBs
  - RFCs on Network File System (NFS) protocol
- Long-Term Archive and Notary Services (LTANS)
  - *RFC4810 Long-Term Archive Service Requirements*

INCITS/T10

- SCSI Command Protocol
  - Draft *SCSI Primary Commands - 4 (SPC-4)*
- Security Support for Tape
  - Draft *SCSI Stream Commands - 3 (SSC-3)*
- *Object-based Storage Device*
  - *ANSI INCITS 400-2004 Information Technology - SCSI Object-Based Storage Device Commands (OSD)*
  - Draft *SCSI Objected-based Storage Device Commands–2 (OSD-2)*

INCITS/T11

- Fibre Channel
  - *ANSI INCITS 424–2007 Fibre Channel – Framing and Signaling-2 (FC-FS-2)*
  - *ANSI INCITS 426–2007 Fibre Channel Security Protocols (FC-SP)*
  - *ANSI INCITS 427–2007 Fibre Channel Generic Services - 5 (FC-GS-5)*
  - *ANSI INCITS 433–2007 Fibre Channel – Link Services (FC-LS)*
  - Draft *Fibre Channel Security Protocols Second Generation (FC-SP-2)*
- Others
  - *ANSI INCITS 388–2008 Storage Management*

ISO/IEC JTC1 SC27

- International security standards covering:
  - WG1 – Information security management systems
  - WG2 – Cryptography and security mechanisms
  - WG3 – Security evaluation criteria
  - WG4 – Security controls and services
  - WG5 – Identity management and privacy technologies
- Recent Standards:
  - ISO/IEC 11770-2:2008 Information technology -- Security techniques -- Key management -- Part 2: Mechanisms using symmetric techniques
  - ISO/IEC 15408-2:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components

ISO/IEC JTC1 SC27 (cont.)

- ISO/IEC 15408-3:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components
- ISO/IEC 24762:2008 Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services
- ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management

- Active Project of Potential Interest:
  - ISO/IEC FCD 15408-1.3 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model
  - ISO/IEC FCD 27000 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
  - ISO/IEC CD 27003 Information technology -- Information security management system implementation guidance
  - ISO/IEC FCD 27004 Information technology -- Security techniques -- Information security management measurements

ISO/IEC JTC1 SC27 (cont.)

- New Projects:
  - ISO/IEC NP 27012 Information technology - Security techniques -- ISM guidelines for e-government services
  - ISO/IEC NP 27032 Guidelines for cybersecurity.
  - ISO/IEC NP 27033 Information technology -- IT Network security
  - ISO/IEC NP 27034 Guidelines for application security
  - ISO/IEC WD 29100 Information technology -- Security techniques -- A privacy framework
  - ISO/IEC WD 29101 Information technology -- Security techniques -- A privacy reference architecture
  - ISO/IEC NP 29146 Information technology - Security techniques - A framework for access management
  - ISO/IEC NP 29147 Information technology - Security techniques - Responsible Vulnerability Disclosure
  - NWI Proposal - Evidence Acquisition Procedure for Digital Forensics

IEEE P1619 SISWG

- IEEE 1619–2007 Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices
- IEEE 1619.1–2007 Standard for Authenticated Encryption with Length Expansion for Storage Devices
- IEEE 1619.2 Draft Standard for Wide-Block Encryption for Shared Storage Media working to produce the first draft, which must include XCB.
- IEEE 1619.3 Draft Standard for Key Management Infrastructure for Cryptographic Protection of Stored Data

IEEE P1667

- IEEE 1667–2006 Standard Protocol for Authentication in Host Attachments of Transient Storage Devices
- Security for transient storage devices
  - Implemented @ low layer in USB stack
  - Windows OS support based on passphrase with hint
  - Can also be transported in SPC-4 Security Protocol In/Out commands

- Storage Management Initiative Specification (SMI-S)
- Object-based Storage Devices (OSD)
- XAM (eXtensible Access Method) Interface specification
- Common RAID Disk Data Format specification

DMTF

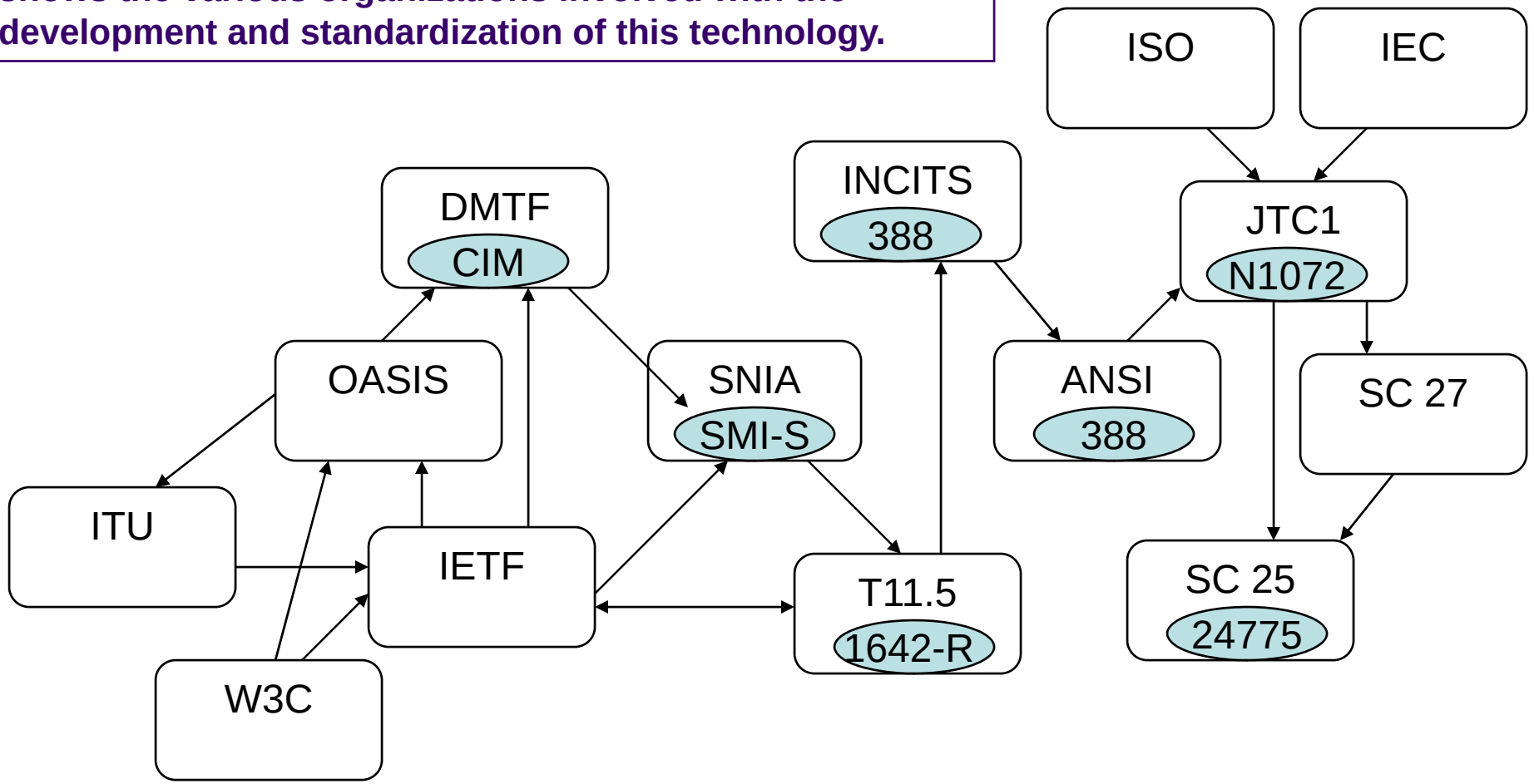
- Common Information Model (CIM)
  - DSP0004 – CIM Infrastructure Specification
  - DSP0200 – CIM Operations over HTTP
  - DSP0201 – Representation of CIM in XML
- Web-Based Enterprise Management (WBEM)
  - DSP0226 – WBEM Web Services for Management (WS-Management)
  - DSP0227 – WBEM WS-Management CIM Binding Specification
  - DSP0230 – WS-CIM Mapping Specification
- Management Profiles
  - DSP1017 – SSH Service Profile
  - DSP1034 – Simple Identity Management Profile
  - DSP1039 – Role Based Authorization Profile

Trusted Computing Group

- Storage
  - TCG Storage Architecture Core Specification Version 1.0
  - TCG Storage Working Group Application Note 1: Encrypting Drives in an Array Controller Version 1.0
- Others
  - Trusted Platform Module (TPM) Specifications
  - Trusted Network Connect (TNC) Specifications
  - Server Specifications
  - TCG Software Stack (TSS) Specifications
  - Infrastructure Specifications
  - Mobile Phone Specifications

Sample Interdependencies

Using SMI-S (see SNIA) as an example, the diagram shows the various organizations involved with the development and standardization of this technology.



Where Do We Go From Here…

What Do We Have…

- Protocol specifications (IETF, INCITS/T11)
- Transport security (IETF, INCITS/T11)
- Storage management objects (DMTF)
- Storage management (SNIA, INCITS/T11)
- Encryption algorithms for storage (IEEE P1619)

- In short…basic building blocks

What Is On The Way…

- Command specifications (INCITS/T10)
- Transport security (DMTF)
- Hard disk drive encryption and roots of trust (TCG)
- Storage management objects (DMTF)
- Storage management (SNIA, INCITS/T11)
- Encryption algorithms for storage (IEEE P1619)
- Key management elements for storage (INCITS/T10, IEEE P1619)

- In short…more building blocks

What Don't We Have…

- Consistent access controls for privileged users (includes separation of duties)
- Data and media sanitization standards (multiple governments have guidance and requirements)
- Standardized data authenticity and integrity (e-Discovery)
- Audit logging for storage
- End-user management controls for data access
- Standards for autonomous data movement (e.g., DLM/ILM)
- Security criteria for storage product certifications (e.g., Common Criteria Protection Profile)
- Long-term information security mechanisms

Thank You