Education

STORAGE SECURITY - THE ISO/IEC STANDARD

Eric A. Hibbard, CISSP, CISA
Hitachi Data Systems

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA Education Committee.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.
  NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

Abstract

Storage Security - The ISO/IEC Standard

Many organizations face the challenge of implementing protection and data security measures to meet a wide range of requirements, including statutory and regulatory compliance. Too often the security associated with storage systems and infrastructure has been missed because of misconceptions and limited familiarity with the storage technology, or in the case of storage managers and administrators, a limited understanding of the inherent risks or basic security concepts. The net result of this situation is that digital assets are needlessly placed at risk of compromise due to data breaches, intentional corruption, being held hostage, or other malicious events.

To help combat this situation, ISO/IEC Joint Technical Committee 1 / Subcommittee 27 (IT Security techniques) has undertaken a new standardization project, ISO/IEC 27040 "Storage security." This standard seeks to provide detailed technical guidance on the protection (security) of information where it is stored and to the security of the information being transferred across the communication links; it includes the security of devices and media, the security of management activities related to the devices and media, the security of applications and services, and security relevant to end-users.

This session introduces the new draft standard, highlights key elements of the guidance, and describes how it can be leveraged by an organization (RFPs, policy, skills, etc.).

What is Storage Security?

- Technical controls, which may include integrity, confidentiality and availability controls, that protect storage resources and data from unauthorized users and uses.

  – SNIA Dictionary

- ***Convergence*** of storage, networking, and security.

- Simply a part of ***Information Assurance***
  - Measures that protect and defend information and systems
  - Encompasses system reliability and strategic risk management
  - Provides for restoration of information systems through protection, detection, and reaction capabilities

Why a Storage Security Standard?

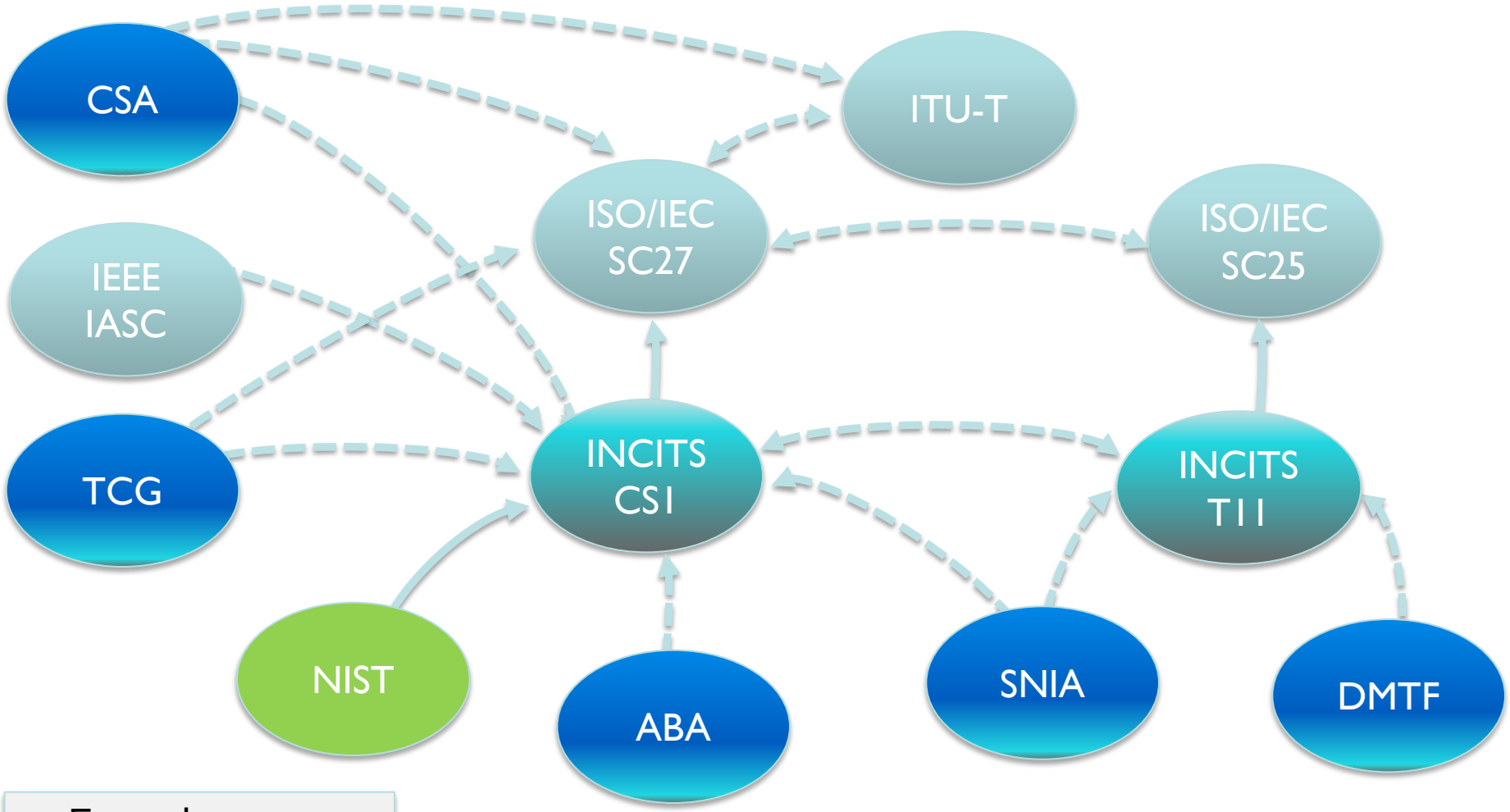
- Organizations live and die based on the availability and integrity of their data
- Mishandling of sensitive data can result in severe consequences
- Cybercrime is both highly profitable and less dangerous than traditional organized crime activities such as drug trafficking
- Cyberterrorism and cyberwarfare agents are targeting digital assets in a broad range of organizations
- Data is no longer safely tucked away behind servers; it may be readily available

- Security and storage professionals need consistent guidance

The Road to an ISO Standard?

- SNIA Activities:
  - Chartered the Security Technical Work Group (2000)
  - Formed the Storage Security Industry Forum (2002)
  - Conducted several storage security summits (2002-2008)
  - Published key guidance documents:
    - *Storage Security: The SNIA Technical Tutorial (2004)*
    - *Storage Security Best Current Practices (2008)*
    - *Storage Security Professional's Guide to Skills and Knowledge (2009)*
- ISO/IEC JTC 1 SC27 (IT Security Techniques):
  - Initiated a study period on storage security (Oct-2009)
  - Approved Storage Security New Work Item Proposal (Oct-2010)
  - Distributed 1st Working Draft of ISO/IEC 27040 (Jun-2011)
  - Distributed 2nd Working Draft of ISO/IEC 27040 (Feb-2012)
  - Distributed 1st Committee Draft of ISO/IEC 27040 (Jun-2012)
  - Projected International Standard (Jan-2014)

Relationships of Key Standards Development Organization (SDO)



Introduction to ISO/IEC 27040
Storage security

NOTE: ISO/IEC 27040 is a draft standard and subject to change.

Overview of ISO/IEC 27040

Education SNIA

Scope:

Provides detailed technical ***guidance*** on how organizations may define an appropriate level of risk mitigation by employing a well-proven and consistent approach to the planning, design, documentation and implementation of data storage security.

Applicability:

- Security of devices and media,
- Security of management activities related to the devices and media,
- Security of applications and services, and
- Security relevant to end-users

Relevance

- Anyone owning, operating or using data storage devices, media and networks
- Senior managers, acquirers of storage product and service, and other non-technical managers or users
- Information/storage security focused managers and administrators
- Anyone involved in the planning, design and implementation of the architectural aspects of storage network security

Project Objectives

- Common set of guidance for security and storage professionals
- Identify the real and perceived risks
- For storage systems and ecosystems, address
  - the physical, technical and administrative controls
  - the preventive, detective and corrective controls
- Facilitate compliance with statutory and regulatory requirements as well as other legal issues (e.g., data authenticity, digital forensics, etc.)

Relevant Storage Technologies

- Computers with host controller, host adapter, or host bus adapter (HBA)
- Storage Arrays with storage network interfaces
- Storage Network Switches
- Cable Plant for Storage Networks
- Storage Management
- Backup Systems (tape, virtual tape, disk)
- Storage Network Gateways
- Network Attached Storage (NAS)
- Content Addressable Storage (CAS)
- Continuous Data Protection (CDP)
- Long-term Storage (on-line and off-line)
- Storage Replication (including DR/BC)
- Media Sanitization
- Virtualization
- Self-encrypting Media (hard disk drives, solid state disks, etc.)
- Cloud Storage
- Specialized Services (encryption, compression, and de-duplication)

Structure of ISO/IEC 27040 (1)

- Front Matter (scope, references, terms, etc.)
- *Overview & Concepts* – Introduces the storage security topic.
  - Overview of Storage Concepts
  - Introduction to Storage Security
  - Storage Security Risks
- *Supporting Controls* – Technology/control specific guidance.
  - Storage Networking
  - Storage Management
  - Block-based Storage
  - File-based Storage
  - Object-based Storage (cloud storage & OSD)
  - Storage Security Services (sanitization, confidentiality, data reductions)

Structure of ISO/IEC 27040 (2)

- *Design/Implementation Guidelines* – as the title suggests
  - Storage Security Design Principles
  - Data Reliability, Availability, and Resilience
  - Data Retention
  - Data Confidentiality and Integrity
  - Virtualization
  - Design and Implementation Considerations
- *Annexes*
  - Media Sanitization
  - Media Sanitization Based on Protection Class
  - Important Security Concepts

Major Changes to Draft

- **Sanitization:**
  - The media sanitization materials were moved to Annex A to make them easier to reference like the long-obsolete DoD 5220.22-M (1995)
  - Preliminary descriptions of Cryptographic Erase and the associated verification process were added
  - A new Annex B (experimental) was added to identify the media sanitization methods to be used, based on Protection Classes and Security Levels
- **Object-based Storage**
  - Includes a new section on cloud storage, with specific guidance on CDMI
  - Includes a new section on OSD along with guidance on using it securely
- **Archives (Long-term Retention):**
  - ISO references (from TC 65/68) for long-term references are identified
  - Guidance for securing short- and medium-term archives (e.g., evidence repositories) was added

Open Issues

- **Sanitization:**
  - NIST has released its update to NIST SP 800-88 *Media Sanitization* and this content needs to be reflected in the new Annex A
  - Additional materials are needed to fully integrate Cryptographic Erase
  - The use of both Protection Classes and Security Levels for media sanitization in Annex B is considered too complex by some, so adjustments are necessary
- **Levels of Security**
  - As currently written, the storage controls and guidance are written as all-or-nothing
  - A new annex has been proposed to identify all the storage security controls and then show their applicability based on levels of security (probably 3 categories)
- **Miscellaneous**
  - Security controls and guidance for CAS are still missing
  - Security controls and guidance for pNFS are still missing
  - Further detail on availability, reliability, and resilience along with how they relate to storage security is needed
  - The are questions as to whether identified ISO references provide adequate details for securing long-term data

What to Expect in the Near-term

- National bodies submitted votes (and comments) on 1stCD by 10/10/2012

- Comments/contributions to be dispositioned at SC27 meeting in Rome, Italy (10/22-26/2012)
- Next draft (CD/DIS) due to ISO around 1/1/2013
- National bodies to review and vote on draft (4/2013)
- Comments/contributions dispositioned at SC27 meeting in France (5/2013)

The Potential Role of ISO/IEC 27040

Raising the Security Bar for Storage

- The sheer existence of ISO/IEC 27040 is causing the security community to take note of the security needs and posture of storage infrastructure
- ISO/IEC 27040 will help identify other important and related standards and specifications (e.g., FC-SP)
- Specific criteria (like media sanitization methods) will be documented in a way that they can be used by both vendors and customers
- ***BOTTOM LINE:*** ISO/IEC 27040 will define best practices that ultimately set the minimum expectations for storage security.

Spotters Guide to Storage Security

Education SNIA

- Securing Storage Management
- Securing Storage Networks
- Short- and Medium-term Retention Security
- Virtualization Security
- At-rest Encryption & Key Management
- Data/Media Sanitization

- ***Possibly:*** Selection of storage security controls based on data sensitivity and/or criticality

Exploiting ISO/IEC 27040

- Customer Perspective
  - Internationally recognized guidance
  - Can be an important reference for RFPs for storage products and service contracts (guidance can be turned into requirements)
- Vendor Perspective
  - Major threats and risks identified
  - Insight into how technology-specific controls fit into an overall storage security approach

Final Thoughts

Final Thoughts

- Storage security is finally getting the attention that it has needed for a very long time
- Security controls within deployed storage infrastructures are frequently in need of attention; adoption of ISO/IEC 27040 is likely to involve some pain
- Although a *guidance* standard, ISO/IEC 27040 could easily become a source of *requirements*, which introduce compliance issues.
- Get involved early. Leverage organizations like SNIA, TCG, and INCITS/CS1 to participate.

SNIA Security Organizations

- SNIA Security Technical Work Group (TWG)
  - Focus: Requirements, architectures, interfaces, practices, technology, educational materials, and terminology for storage networking.
  - http://www.snia.org/tech_activities/workgroups/security/
- Storage Security Industry Forum (SSIF)
  - Focus: Educational materials, customer needs, whitepapers, and best practices for storage security.
  - http://www.snia.org/ssif

Attribution & Feedback

The SNIA Education Committee would like to thank the following individuals for their contributions to this Tutorial.

Authorship History

Eric A. Hibbard – March 2012

Updates:
Eric A. Hibbard – September 2012

Additional Contributors

SNIA Security TWG

Andrew Nielsen, CISSP
Walter Hubis
Richard Austin, CISSP
Roger Cummings

Please send any questions or comments regarding this SNIA Tutorial to
tracktutorials@snia.org