Education

STORAGE SECURITY - THE ISO/IEC STANDARD

Eric A. Hibbard, CISSP, CISA, ISSAP, ISSMP, ISSEP, SCSE
Hitachi Data Systems

Author: Eric A. Hibbard, 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

Storage and security professionals don't typically move in the same technology and management circles within an organization, and as a result, storage frequently plays a diminished role in protecting the organization's digital assets. This situation is unfortunate because storage systems and infrastructure could be an effective weapon in the organization's war chest against cybercrime, cyberwarfare, and other less insidious types of incidents. One might say that storage could be the last line of defense in an organization's defense-in-depth strategy.

The pressure to change is already there from the statutory and regulatory requirements, but the catalyst for this change could come from a new standard being developed by ISO/IEC Joint Technical Committee 1 / Subcommittee 27 (IT Security techniques). The new ISO/IEC 27040 "Storage security" project 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?

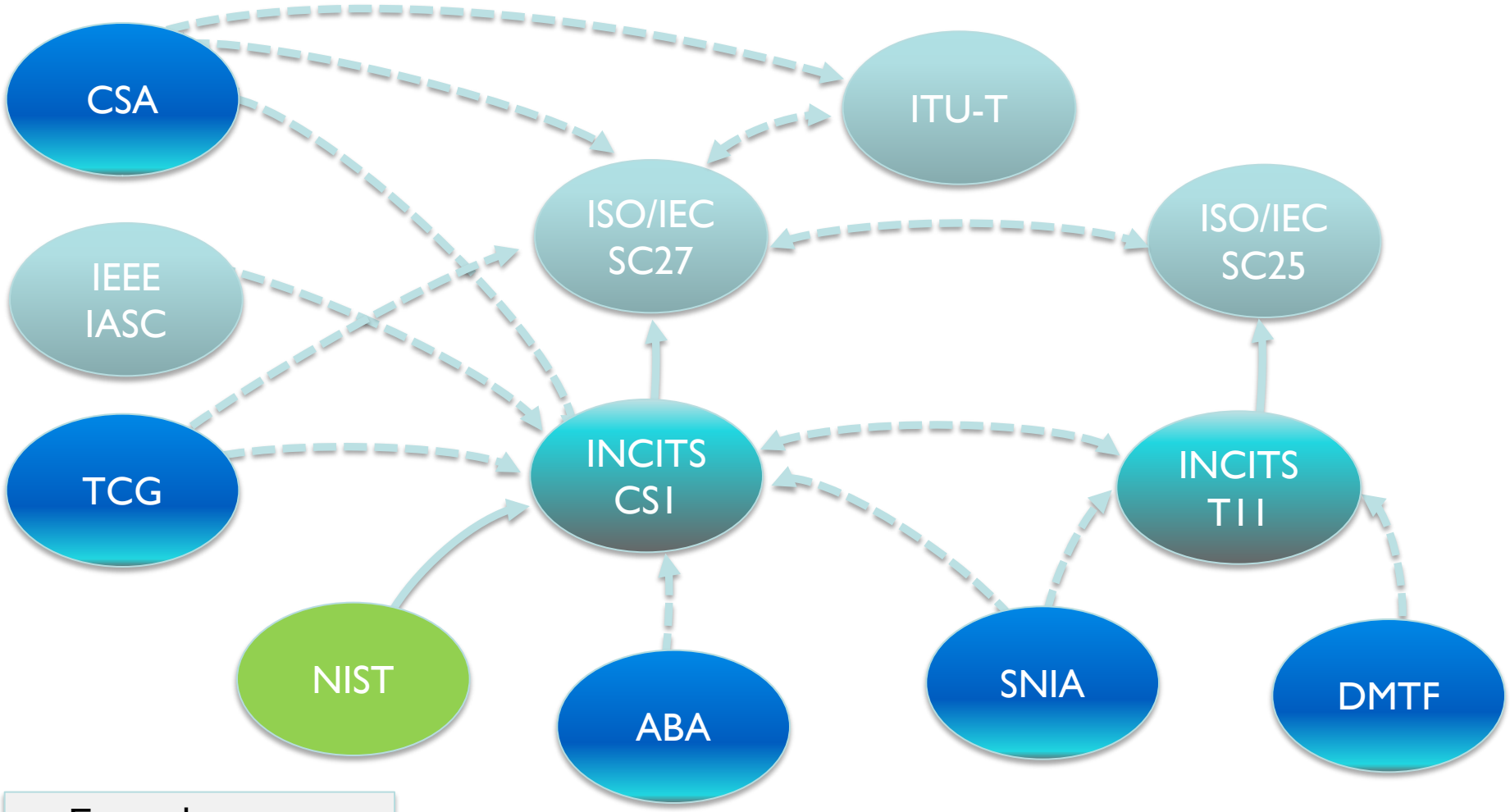
- Organizations live and die based on the availability and integrity of their data
- Mishandling of sensitive data can result in severe consequences
- Cybercrime is both highly profitable and less dangerous than traditional organized crime activities such as drug trafficking
- Cyberterrorism and cyberwarfare 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)
  - Projected International Standard (Oct-2013)

Key SDO Relationships



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)

* The specific role of these technologies are being defined.

Structure of ISO/IEC 27040 (1)

- Front Matter (scope, references, terms, etc.)
- *Overview & Concepts* – Introduces the storage security topic.
  - Overview of Storage
  - Introduction to Storage Security
  - Storage Security Risks
  - Relationship with 27000 series of international standards
- *Supporting Controls* – Technology/control specific guidance.
  - Storage Networking
  - Storage Management
  - Block-based Storage
  - File-based Storage
  - Object-based Storage
  - 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* – Cross-references Between 27001/27002 and 27040

Open Issues

- **Cloud Storage**
  - Both SC27 (IT Security Techniques) and SC38 (Distributed Application Platforms & Services) are developing cloud standards
  - At least one national body has expressed concerns about including general cloud storage in ISO/IEC 27040; an exception may be made for those storage issues that are needed to support cloud (e.g., virtualization)
- **Archives (Long-term Retention):**
  - At least one national body has asserted that archives are handled by other ISO committees (TC 65/68) and should be out of scope for ISO/IEC 27040
  - There is agreement that short- and medium-term archives (e.g., evidence repositories) are in scope of ISO/IEC 27040
- **Sanitization:**
  - Recent work in the U.S. may make cryptographic erasure an acceptable method of sanitization for certain forms of media (e.g., SSDs)
  - NIST is in the process of updating NIST SP 800-88 *Media Sanitization*

What to Expect in the Near-term

- National bodies to review and comment on 2ndWD (due to ISO on 4/10/2012)
- Comments/contributions dispositioned at SC27 meeting in Stockholm, Sweden (5/7-11/2012)
- Next draft (CD) due to ISO around 7/1/2012
- National bodies to review and vote on draft (9/2012)
- Comments/contributions dispositioned at SC27 meeting in Italy (10/2012)
- Next draft (DIS) due to ISO around 1/1/2013

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

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

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 has been 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
- ISO/IEC 27040 may be the first of several storage security related standards; future standards may take the form of *requirements* standards, which introduce compliance issues.
- Get involved early. Leverage organizations like SNIA, TCG, and INCITS/CS1 to participate.

Other SNIA Security Tutorials

- Wednesday (April 4th @ 11:40): *A Hype-free Stroll through Cloud Storage Security*
- Thursday (April 5th @ 11:15): *Implementing Stored-Data Encryption*

Q&A / Feedback

- Please send any questions or comments on this presentation to SNIA: tracktutorials@snia.org

Many thanks to the following individuals for their contributions to this tutorial.

- SNIA Education Committee

Eric A. Hibbard, CISSP, CISA

SNIA Security TWG

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