SNIA STORAGE SECURITY SUMMIT

Wednesday, May 11, 2022 • Virtual

ISO Storage Security Standard Gets a Refresh

Eric Hibbard, CISSP, CIPP/US, CISA

Samsung Technologies, Inc.

A SNIA Event

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 containin material from these presentations.
- This presentation is a project of the SNIA.
- 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

- The ISO/IEC 27040 storage security standard was originally published in 2015 as a guidance standard that expanded upon the earlier SNIA storage security best practices and focused on existing and emerging storage technologies. During the intervening years, the threat landscape has morphed significantly, storage technologies and practices continue to change, and the regulatory obligations increase with each wave of attacks. In response, ISO initiated an early revision of ISO/IEC 27040, which included transitioning it from a guidance standard to one that includes both requirements and guidance as well as other changes to help ensure the standard remains relevant.

- This session will highlight the anticipated changes for the second edition of ISO/IEC 27040, position it within the ISO 27000 series security standards, and provide a timeline for its availability. While the standard is written primarily for storage consumers, this session will also provide vendors with insights into what they can expect once the standard is published.

Storage Security Standardization

Background

A Little History

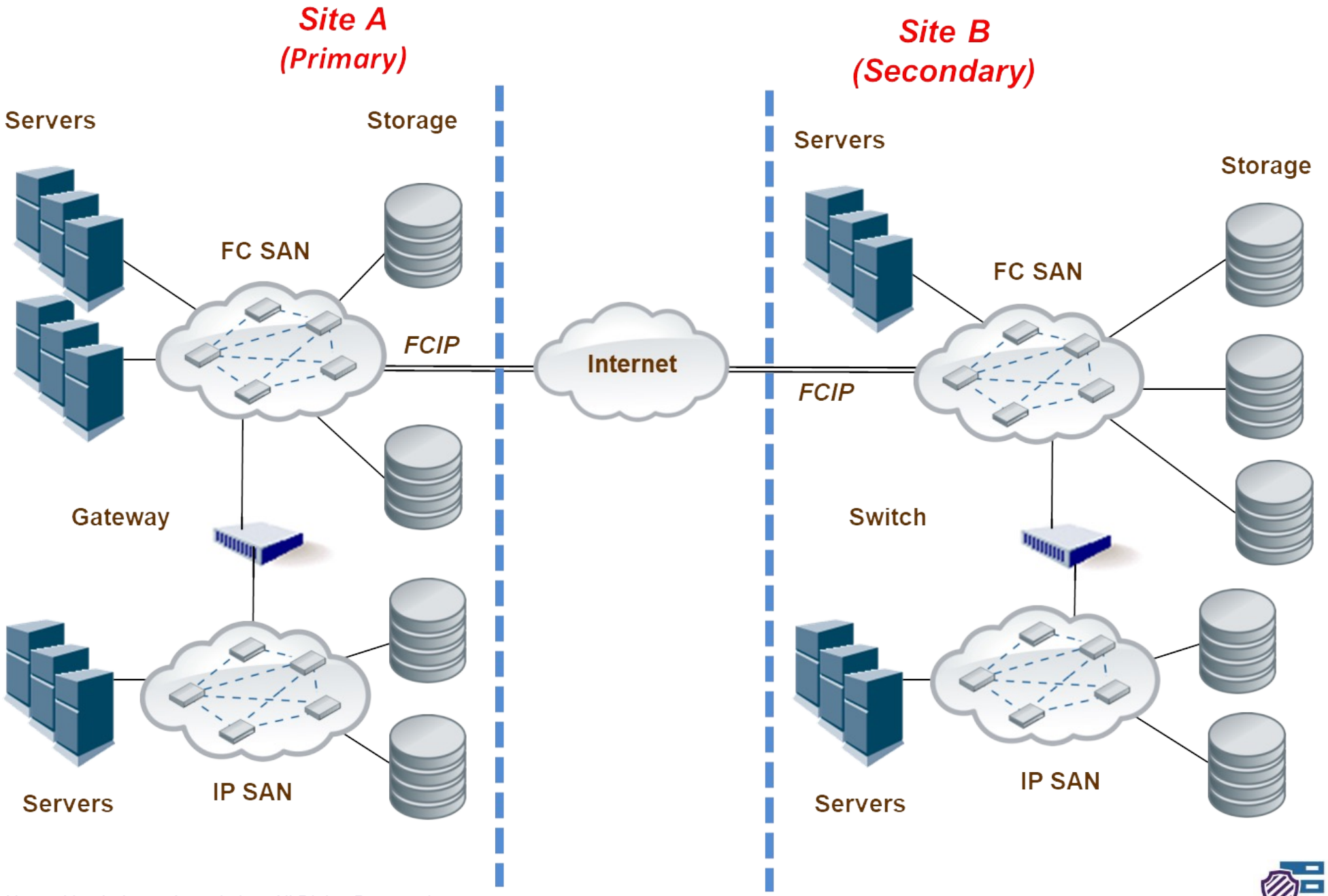
- Roots of ISO Storage Security Project:
  - SNIA Storage Security BCPs (circa 2008)
  - U.S. proposed a Study Period on Storage Security (February 2010)
  - ISO/IEC JTC 1/SC 27/WG 4 initiated New Work Item Proposal (October 2010)
- ISO/IEC 27040 (1st Edition) published January 2015
- SC 27/WG initiates Study Period on the early revision of ISO/IEC 27040 (April 2019)
- ISO/IEC 27040 (2nd Edition)
  - New Work Item Proposal approved
  - 3 Working Drafts (WD) and 1 Committee Draft (CD) balloted
  - Text for Draft International Standard (DIS) submitted May 2022
  - DIS ballot (last opportunity for technical changes) anticipated to close by October 2022

Storage-oriented Data Breaches

Security threats	Potential forms of data breach
Theft or loss of storage device or storage media	Unlawful or unauthorized disclosure, data loss, or data destruction
Accidental configuration changes (e.g., storage management, storage/network resources, and incorrect patch management) by authorized personnel	Accidental access, accidental disclosure, accidental data destruction, accidental data alteration, or removal/denial of access
Malicious configuration changes (storage management, storage/network resources, and application tampering) by external or internal adversaries	Unlawful access, unlawful disclosure, unlawful data destruction, unlawful data alteration
Privileged user abuses by authorized users (e.g., inappropriate data snooping)	Unlawful/unauthorized access or disclosure
Malicious data tampering by external or internal adversaries	Unlawful data destruction or alteration
Denial of service attacks	Loss of access by legitimate users and unavailability of storage and data
Malicious monitoring of network traffic	Unlawful/unauthorized disclosure

Overview of ISO/IEC 27040:2015

- Direct Attached Storage (DAS)
- Storage networking
  - Storage Area Networks (SAN)
  - Network Attached Storage (NAS)
- Storage management
- Block-based storage (Fibre Channel and IP)
- File-based storage (NFS, SMB/CIFS, parallel NFS)
- Cloud storage
- Object-based storage
- Storage virtualization
- Storage security services
  - Sanitization,
  - Data confidentiality
  - Secure multi-tenancy
  - Secure autonomous data movement



Challenges with ISO/IEC 27040:2015

- As a guidance standard, there were no requirements
  - No basis for compliance
- 330+ controls made it difficult to establish priorities; Annex B profiled the controls (C/I/A versus data sensitivity)
- Technology specific media sanitization guidance (Annex A) of diminishing value
  - Many listed storage media were already obsolete; no easy way to add new media types
  - Techniques/procedure were not appropriate to new technologies
- Alignment with ISO/IEC 27000-series was weak
- Missing guidance on data protection and archives/repositories
- Several included storage technologies were niche (very limited adoption)

Refreshing ISO/IEC 27040

Information technology – Security techniques – Storage security

Key Drivers for ISO/IEC 27040 Revision

- Establish a baseline of storage security controls
- Improved alignment with ISO/IEC 27002 (and ISO/IEC 27001)
- Remove the controls for obsolete/niche storage technologies; address new storage technologies
- Eliminate the extensive tutorial material (Annex C) that required significant maintenance
- Improve the maintenance of the storage media sanitization materials

Major Changes for ISO/IEC 27040 (2nd Ed.)

- New structure tracks ISO/IEC 27002:2022 structure
  - Organization, people, physical, and technological controls
- Scope was modified to include requirements
  - Organizational (1)
  - Physical (1)
  - Technological (30)
    - System hardening (2)
    - Storage management (5)
    - Encryption/key management (7)
    - Sanitization (9)
    - NFS (2) / SMB (3)
    - Cloud storage – CDMI (2)

Major Changes for ISO/IEC 27040 (2nd Ed.) [cont.]

- Significant changes to sanitization materials
  - Defers to IEEE Std 2883 for media-specific sanitization; old Annex A removed
  - Verification and cryptographic erase clarified
- New labeling scheme for controls and clusters of controls
  - Differentiates requirements from guidance
  - Control labels summarized (Annex A)
- Tutorial materials (old Annex C) eliminated
  - Necessary descriptions moved to normative text
  - Leverage industry whitepapers

Major Changes for ISO/IEC 27040 (2nd Ed.) [cont.]

- New controls added for:
  - Expertise of storage administrators
  - Design and implementation of storage security
    - Integrity as well as retention, preservation, and disposal of data
  - Storage systems security
    - Storage vulnerability management
  - Management of Intelligent Platform Management Interfaces (IPMI)
  - NVMe over Fabrics (NVMe-oF)
  - Storage backups – cyber-attack recovery
  - Data archives and repositories

Summary

- The ISO/IEC 27040 requirements will be usable by vendors (conformance claims), customers (in tenders), and auditors (criteria)
- ISO/IEC 27002:2022 now references ISO/IEC 27040
  - Media sanitization
  - Backups

- Publication of ISO/IEC 27040 (2nd Ed.) is anticipated by February 2023

Please take a moment to rate this session.

Your feedback is important to us.

