#dcsarticle http://www.dcseurope.info/n/sstj

SNIA™
Security Technical Work Group
www.snia-europe.org

Storage security comes of age

By Eric A. Hibbard, CISSP, CISA; Chair, SNIA Security TWG
and ISO Editor of ISO/IEC 27040, HDS.

MANY ORGANIZATIONS face the challenge of implementing data protection and security measures to meet a wide range of requirements, including statutory and regulatory compliance. All too often, the implemented measures fail to address the security associated with storage systems and infrastructure (i.e., storage security) 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.

A contributing factor to the limited use of storage security measures is the lack of generally available information and guidance. The Storage Networking Industry Association (SNIA) has attempted to fill some of this void with its best practices, whitepapers, and tutorials on the subject. Unfortunately, security professionals and auditors are frequently unaware of these materials and thus have only focused on a few elements (e.g., at rest encryption, media sanitization, etc.). This situation is about to change because the International Organization for Standardization (ISO), in conjunction with the International Electrotechnical Commission (IEC), under Subcommittee 27 (SC 27) of the Joint Technical Committee 1 (JTC 1) is nearing completion of a standard to address storage security. This is noteworthy since a major element of SC27's program of work includes International Standards for information security management systems (ISMS), often referred to as the ISO/IEC 27000-series, including ISO/IEC 27001 (criteria used for ISMS certification of organizations).

The full title of the new SC27 storage security standard is ISO/IEC 27040:2014, Information technology — Security techniques — Storage security, which is currently at the Final Draft International Standard (FDIS) stage and is expected to be published before the end of 2014. The purpose of ISO/IEC 27040 is to provide security guidance for storage systems and ecosystems as well as for protection of data in these systems; it supports the general concepts specified in ISO/IEC 27001. It is relevant to managers and staff concerned with data storage and information security risk management within an organization and, where appropriate, external parties supporting such activities.

The standard provides relevant terminology, including the following important definitions:

- **Storage security -** application of physical, technical and administrative controls to protect storage systems and infrastructure as well as the data stored within them
- **Data breach -** compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed

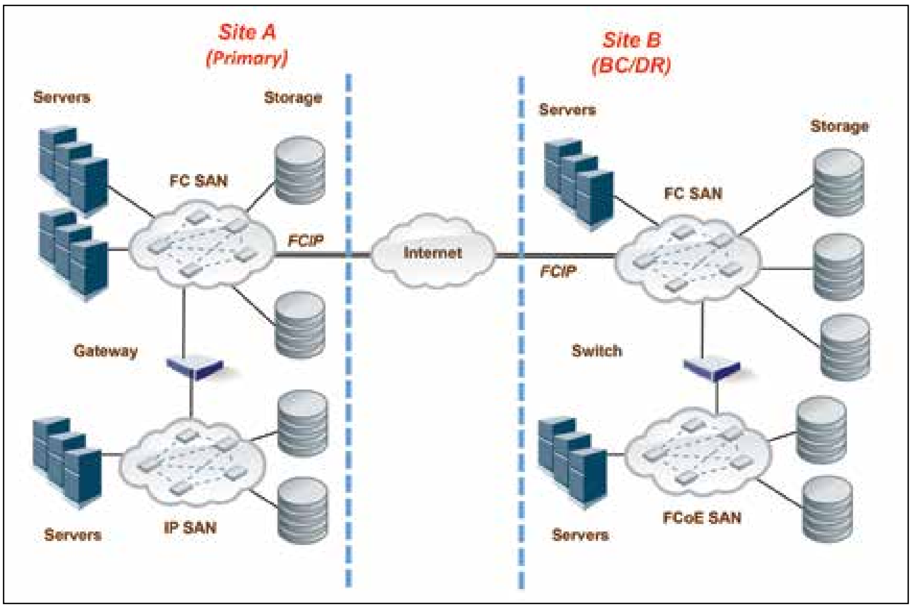
Since data breaches are a major area of concern (common types are addressed in this standard), this definition plays a pivotal role throughout the standard. Historically, the storage industry was only worried about unauthorized disclosure/access, but his new definition, which is aligned with the new EU General Data Protection Rules, adds destruction, loss, and alteration. This potentially means that individuals involved with storage could now be a party to a data breach due to an action that causes data loss or corruption (e.g., from a failed microcode updated).

ISO/IEC 27040 approaches storage security guidance from two angles: 1) supporting controls and 2) design and implementation of storage security. Both are addressed in sufficient detail that storage professional with limited security knowledge and security/audit professionals with little storage background can leverage the materials.

Storage security - supporting controls

The supporting controls clause in ISO/IEC 27040 identifies the controls (measures) that support storage security architectures, their related technical controls, and other controls (technical and non-technical) that are applicable beyond storage. Each of the following is addressed:

- Direct Attached Storage (DAS)
- Storage networking (multiple flavors of SAN and NAS)
- Storage management



(Source: ISO/IEC 27040:2014; Figure 2)

- Block-based storage (Fibre Channel and IP)
- File-based storage (NFS, SMB/CIFS, pNFS)
- Object-based storage (cloud, OSD, CAS)
- Storage security services (sanitization, data confidentiality, and data reductions)

No storage technology is recommended over another. Instead, the guidance is provided in a manner that makes it clear as to what is needed/expected from a security perspective when particular storage technologies are selected or deployed. The standard also considers complex scenarios shown here.

Storage security - design and implementation

Designing and implementing storage solutions requires adherence to core security principles. ISO/IEC 27040 addresses these design principles from a storage security perspective and leverages the supporting controls to counter storage security threats and vulnerabilities. The basic premise is that design failures can lead to significant problems (i.e., data breaches). The materials in this clause cover the following:

- Storage security design principles (defense in depth, security domains, design resilience, and secure initialization)
- Data reliability, availability, and resilience (including backups and replication as well as disaster recovery and business continuity)
- Data retention (long-term and short/medium-term retention)
- Data confidentiality and integrity
- Virtualization (storage virtualization and storage for virtualized systems)
- Design and implementation considerations (encryption and key management issues, alignment of storage and policy, compliance, secure multi-tenancy, secure autonomous data movement)

The secure multi-tenancy and secure autonomous data movement (similar to ILM security) are advanced issues and they are likely to have broader applicability (e.g., cloud computing).

Value-added elements of ISO/IEC 27040

A significant effort was made to enhance the applicability and usability of ISO/IEC 27040, which lead to the incorporation of the following:

- **Media Sanitization -** The standard includes an annex that provides detailed information (similar to NIST SP 800-88r1) on ways to sanitize different types of storage media. The techniques span the use of overwriting approaches through cryptographic erasure (key shredding). This is the only International Standard covering this issue and it was structured such that it can be referenced like the 1995 version of DoD 5220.22-M is often used by vendors.

- **Selecting Storage Security Controls -** It was recognized that organizations would not be able to address the 330+ controls provided in ISO/IEC 27040. To avoid an all-or-nothing scenario, an annex was developed to help prioritize the selection and implementation of storage security controls, based on security criteria (i.e., confidentiality, integrity, availability) or data sensitivity (low or high). This annex can also be used as a checklist by auditors for storage systems and ecosystems.

- **Important Security/Storage Concepts -** Given the disparate target audiences (security, storage, and audit), it became clear that certain “tutorial” materials needed to be provided to ensure a common understanding of certain concepts. As such, these details are provided in an annex, which briefly covers topics such as authentication, authorization and access control, Self-Encrypting Drives (SED), sanitization, logging, N_Port_ID Virtualization (NPIV), Fibre Channel security, and OASIS KMIP. The Fibre Channel materials are especially important because this is one of the few places FC-SP-2 and other FC security mechanisms are explained.

- **Bibliography -** Normally, the bibliography of a standard is of marginal value. In ISO/IEC 27040, however, this is not the case because it represents the go-to list for relevant storage security information. One might consider it the core source material for storage security.

Conclusions

As data breaches persist, organizations are scrambling to find additional ways to protect their systems and data. Storage security is often overlooked and may be pressed into service as a last line of defense. ISO/IEC 27040 provides the details that can help accomplish this.

ISO/IEC 27040 is a “guidance” standard (i.e., everything is specified as “should”).

It is relatively easy to turn this guidance into requirements by specifying that some or all of the guidance shall be implemented, or in the case of materials directed towards a vendor (e.g., RFP), the vendor shall provide the capabilities/functionality necessary to implement the ISO/IEC 27040 guidance (some or all).

Look for an up-tick in interest in storage security in early 2015, following on the heels of the publication of ISO/IEC 27040.

For more information about the Storage Networking Industry Association (SNIA) and its technical security work, please visit **http://www.snia.org/tech_activities/work/twgs** and all of our activities in SNIA Europe at **http://www.snia-europe.org**