Storage Networking Industry Association
Technical White Paper

Storage Security: Sanitization

August 27, 2015

Abstract: *The ISO/IEC 27040:2015 (Information technology - Security techniques - Storage security) standard provides detailed technical guidance on controls and methods for securing storage systems and ecosystems. This whitepaper provides an overview of the sanitization guidance in the standard as applied to disk-type media and provides guidance to organizations in developing a sanitization program to meet their particular needs.*

USAGE

The SNIA hereby grants permission for individuals to use this document for personal use only, and for corporations and other business entities to use this document for internal use only (including internal copying, distribution, and display) provided that:

1. Any text, diagram, chart, table or definition reproduced shall be reproduced in its entirety with no alteration, and,

2. Any document, printed or electronic, in which material from this document (or any portion hereof) is reproduced shall acknowledge the SNIA copyright on that material, and shall credit the SNIA for granting permission for its reuse.

Other than as explicitly provided above, you may not make any commercial use of this document, sell any or this entire document, or distribute this document to third parties. All rights not explicitly granted are expressly reserved to SNIA.
Permission to use this document for purposes other than those enumerated above may be requested by e-mailing tcmd@snia.org. Please include the identity of the requesting individual and/or company and a brief description of the purpose, nature, and scope of the requested use.

All code fragments, scripts, data tables, and sample code in this SNIA document are made available under the following license:

BSD 3-Clause Software License

Copyright (c) 2014, The Storage Networking Industry Association.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of The Storage Networking Industry Association (SNIA) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

DISCLAIMER

The information contained in this publication is subject to change without notice. The SNIA makes no warranty of any kind with regard to this specification, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The SNIA shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this specification.

Suggestions for revisions should be directed to http://www.snia.org/feedback/.

Revision History

Revision	Date	Sections	Originator:	Comments
V1.0 R0	*3/4/2015*	All	Richard Austin	Initial Draft
V1.0 R1	*3/5/2015*	All	Richard Austin	Final Draft
V1.0 R2	*8/10/2015*	All	Richard Austin	Updated title and inserted Appendix A to harmonize with other papers in series.

Suggestion for changes or modifications to this document should be submitted at http://www.snia.org/feedback/.

Foreword

This is one of a series of whitepapers prepared by the SNIA Security Technical Working Group to provide an introduction and overview of important topics in ISO/IEC 27040:2015, *Information technology – Security techniques – Storage security*. While not intended to replace the standard, they provide additional explanations and guidance beyond that found in the actual standard.

Executive Summary

Sanitization addresses a risk as old as reusable storage devices themselves: disclosure of information via reuse or disposal of storage media. Though originally as easy as assuring that magnetic media was degaussed before reuse or disposal, advances in technology and new storage media types have increased the complexity of the sanitization process while society as a whole is becoming increasingly intolerant of data stewards who put their information at risk.

This document provides an overview of the sanitization guidance provided in ISO/IEC 27040 and will assist organizations in developing a sanitization program that meets their needs. As sanitization decisions may have implications for retention, discovery holds and other regulatory or legal matters, the users of this document are advised to consult with competent legal counsel before implementing its guidance. Nothing in this document should be construed as legal advice or opinion.

1 Introduction

The purpose of sanitization is, not too surprisingly, to sanitize storage media. "Sanitize" means rendering the data on the media infeasible to recover for a given level of effort.[1] The "level of effort" is an important concept as it will motivate decisions regarding the sanitization process and its implementation. As will be covered later, the more valuable the information, the more effort an adversary might be willing to invest in recovering it and the more careful an organization must be in its choice of a sanitization method.

Sanitization is required by four basic types of concerns:

1. In many jurisdictions, loss of control of media containing protected information is being regarded as equivalent to disclosing that information. This may mean that breach notifications must be performed and liability for regulatory or other legal penalties may be incurred.
2. Developing privacy requirements (such as the European Union "Right to be forgotten") may require that data not be just "deleted" but also sanitized to assure it is resistant to recovery.
3. It may be a requirement. Defense contractors and other agencies that deal in national security information must comply with regulations governing sanitization.
4. Limiting the scope of information subject to electronic discovery – organizations generally want to limit the amount of information that is potentially subject to

[1] ISO/IEC 27040, p. 5

electronic discovery requests. This may be accomplished by assuring that all data at end-of-life (including retention periods) and not subject to a current duty to preserve is sanitized.[2]

Whether, and how, these concerns apply to your organization is determined through consultation with competent legal counsel. As this is a rapidly developing area of law, this consultation should be regular and ongoing rather than a one-time occurrence.

This whitepaper will primarily focus on disk-type media not because other storage types are less important or ISO/IEC 27040 lacks guidance for other media types but because readers will likely be more familiar with disk-type media. A sound grasp of sanitization concepts in the familiar disk-media context will prepare readers to successfully apply ISO/IEC 27040's guidance for other storage types.

1.1 History

As noted earlier, sanitization is as old as reusable storage media. An early (1991) discussion of the problem revolved around "remanence" – "the residual information that remains on storage media after erasure."[3] Remanence recognized that operations intended to delete data (such as a file system delete operation) might leave recoverable parts of the data behind that could be recovered by an interested party. Though the Trusted Computer System Evaluation Criteria (TCSEC) has been superseded, this document is the source for much of the terminology for sanitization methods.

An influential study of how data could be reconstructed from its remanence and effective methods for accomplishing sanitization was conducted by Peter Gutmann in 1993.[4] Gutmann also described sophisticated laboratory-style data recovery methods such as magnetic force microscopy and developed the Gutmann algorithm for sanitizing media that provided assurance against them. This method of overwriting multiple times with varying data patterns became the recommended guidance for many sanitization products and was incorporated in mandatory guidance such as the 1995 version of the NISP Operating Manual or DoD 5220.22-M. However, as noted in an epilogue to his original paper, later technological developments have modified the need for multiple overwrites in many cases.

---

[2] As noted earlier, sanitization goes beyond simple deletion and includes resistance to some level of effort.

[3] Trusted Computer System Evaluation Criteria *A Guide to Understanding Data Remanence in Automated Information Systems*, the "forest green" book. http://fas.org/irp/nsa/rainbow/tg025-2.htm Accessed 30 January, 2015

[4] Peter Gutmann, *Secure Deletion of Data from Magnetic and Solid-State Memory*. Sixth USENIX Security Symposium. https://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html with epilogue accessed 30January, 2015.

Though sanitization was a concern for the national security and military establishments, the private sector and individuals had much less understanding of its requirements. This was graphically changed when Simpson Garfinkel purchased a large number of used disk drives and did a study of the data that was easily retrieved from them.[5] Garfinkel retrieved a trove of confidential data such as medical and financial records.

A major modern study of disk sanitization was conducted at the Center for Magnetic Recording Research (CMRR) at UCSD in 2007.[6] This study provides an excellent overview of the various requirements for sanitization, effective methods for sanitizing disk media and is notable for its coverage of the new device commands in modern drives that provide sanitization capability and also debunks a number of exaggerated claims regarding the ability to recover data from sanitized disk media. It is also notable for identifying the limitations of degaussing as a sanitization method due to the increasing use of solid-state memory for storage devices (and as performance-enhancing caches in magnetic storage devices).

NIST's Special Publication 800-88, *Guidelines for Media Sanitization* (newly revised in December of 2014) provides detailed guidance for sanitizing many forms of media ranging from disks to paper. Though its guidance is binding only on US federal agencies, it is an excellent resource for private sector organizations.

ISO/IEC 27040 provides extensive guidance for storage security in general and includes sanitization as a major topic. Its normative (i.e., describing what should be done) Annex A: *Media Sanitization* provides detailed guidance on how to properly sanitize many types of storage based on the risk profile of the organization.

1.2 Implement sanitization as a process

Sanitization is not a one-off activity but rather should be implemented as a normal part of the information management process. A process implementation should also include appropriate proof of sanitation to both satisfy audit requirements and justify exclusion from electronic discovery requests (e.g., if user workstation disks are automatically sanitized within 30 days of termination of employment, no legal duty to preserve or produce information from Jane Doe's workstation would be created by a lawsuit filed 60 days after her termination[7]).

---

[5] Simpson Garfinkel and Abhi Shelat, *Remembrance of Data Passed: A Study of Disk Sanitization Practices*. IEEE Security & Privacy, January/February 2003. pp. 17-27.

[6] Gordon Hughes and Tom Coughlin, *Tutorial on Disk Drive Sanitization*, 2007. http://cmrr.ucsd.edu/people/Hughes/documents/DataSanitizationTutorial.pdf Accessed January 6, 2015

[7] This is an overly simplified example – if the organization reasonably expected the litigation to be filed earlier than 30 days after Jane's termination, a duty to preserve might already exist in advance of the lawsuit. This is the type of legal issue that mandates regular consultation with legal counsel on sanitization decisions and processes.

1.2.1 Legal Considerations

As noted earlier, the sanitization process must comply with both retention periods (whether mandated by law, regulation or policy) and the duty to preserve. If a given type of information (e.g., executive email) must be retained for some period, then the sanitization process must exclude it until the retention period has expired.

Duty to preserve deals with the responsibility of a party to a litigation to preserve any information relevant to that litigation. Though there is a general good-faith acceptance that normal sanitization processes may destroy potentially relevant information, there is a requirement to suspend sanitization when the litigation is filed or even when a reasonable expectation of litigation arises. This implies that there should be a means for the organization's legal staff to request suspension of sanitization activities and for that suspension to be implemented in a timely fashion.

This is an active and developing area of law and regular consultation with legal counsel is required.

2 Methodology

2.1 Considerations in choosing a methodology

Choosing a sanitization methodology requires balancing the value of the information against the capabilities and intent of an adversary[8] as well as deciding on the desired final disposition of the media.

Valuing information can be a difficult process as most private sector organizations are not subject to the strict classification protocols of the national security establishment. Private sector organizations tend to think in terms of contractual, legal and regulatory mandates that require certain levels of protection for specific types of information (e.g., PCI DSS for payment card information, HIPAA for protected health information and privacy requirements for personally identifiable information). Information on new products, significant inventions, etc., also have a direct value that must be protected. Even when information is valued, the identification of storage media holding specific types of information can be difficult. In many cases, this state of affairs, unfortunately, requires sanitizing storage to a level appropriate to the most sensitive information it ***might*** contain.

[8] "Adversary" is used generically to represent anyone desiring illicit access to valuable information whether they are cybercriminals, operatives of a state-sponsored intelligence operation, cyber-activists, etc.

Adversary intent and capability also vary. Cybercriminals seek to monetize pilfered payment card information either directly by making fraudulent purchases or indirectly by selling it to those who will make those purchases. Nation states may use pilfered intellectual property for competitive advantage. Capability can range from use of simple undelete utilities to modern forensic tools to techniques available only in a well-funded and equipped laboratory.

The importance of the final disposition of media revolves around whether the sanitized media will remain under organizational control or be sold, recycled[9], returned to the vendor, etc.

Though there are many variables and their values may be nebulous, the choice of sanitization methodology revolves around two simple questions:

1. Will your organization retain control of the media after it is sanitized?
2. What level of technical capability do potential adversaries have?

2.1.1 Retaining Control

If the media will be reused within your organization, then its exposure to outside entities is limited. Your risk here is more on the lines of the curious employee or contractor rather than a cybercriminal gang with significant technical expertise and capability. In this case a less strenuous sanitization method would be appropriate.

On the other hand, if the sanitized media is leaving your control, you have no idea who may attempt to retrieve information. Used hard drives from a financial institution would likely attract the interest of cybercriminals hoping to recover payment card or other valuable financial information. Similarly, used media from a defense contractor would be of interest to nation states engaged in espionage.

A sometimes overlooked case involves media that is returned to a vendor under a warranty claim or service contract. This case is complicated by the possibility that the device may not be functional at the time it is returned.

Media leaving an organization's control should be subjected to a more stringent sanitization regimen.

2.1.2 Adversary capability

Attempts to recover data from sanitized media break down into two basic categories: logical methods and physical methods such as sophisticated laboratory attacks.

[9] Storage devices contain many useful materials (such as rare earth elements) that can be recovered by a suitably equipped recycling center.

Logical methods range from using a file undelete utility to common digital forensic tools. These tools are readily available and any adversary may be assumed to have access to them.

Physical methods are open ended and depend solely on the technical expertise of the adversary and the effort they are willing to expend. As noted earlier, Gutmann described the use of Magnetic Force Microscopy to retrieve data from magnetic disks (though this technique no longer works with modern drives). A modern example would be using laser drills to access the internal circuitry of a logic chip and a logic analyzer to decode its operation.[10] These potential attacks are particularly relevant to solid state storage where wear-leveling may leave significant information extant at hardware levels below the storage controller.

When adversary capability is high and the information is valuable enough to justify use of those advanced capabilities, the media should be subjected to the most stringent sanitization regimens.

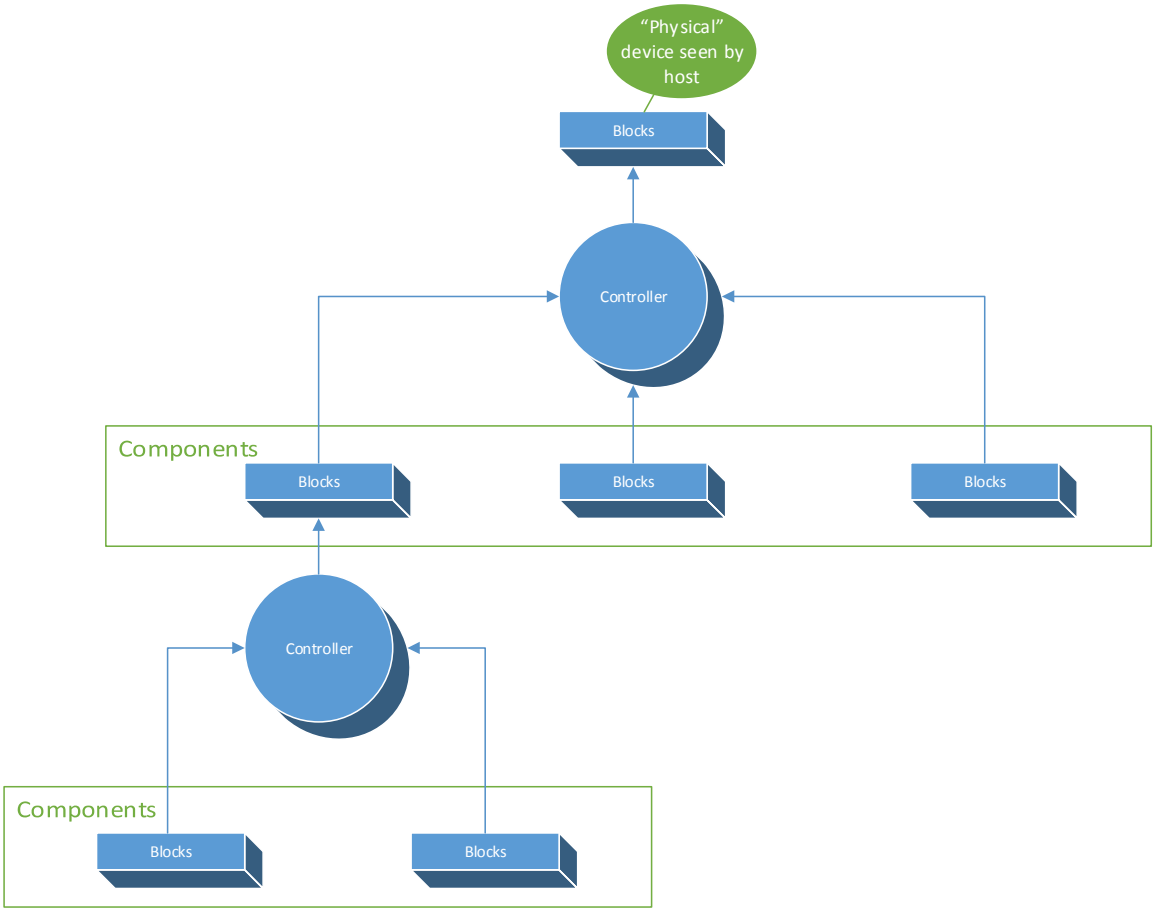


Figure 1: Levels of Virtualization in Storage Ecosystems

[10] For a good overview of such laboratory attacks, see Chapter 16 of Ross Anderson's *Security Engineering: A Guide to Building Dependable Distributed Systems* (2nd ed). 2008.

2.2 Logical versus Media-Aligned Sanitization

Modern storage ecosystems can be complex environments that implement several layers of virtualization in presenting what appears to be a disk device to a host. Looking at Figure 1, at the top are a collection of blocks presented to a host as a storage LUN. Below that is a controller which combines chunks of storage blocks (possibly from multiple independent devices) to create that LUN seen by the host. Perhaps one of those devices (the one on the left) is a solid state drive so the physical "device" is actually a virtual creation made up of a collection of blocks that are managed by a subsidiary controller (for purposes of wear-leveling, etc.).

Sanitization can be applied at any of these levels and ISO/IEC 27040 uses the terminology logical and media-aligned to differentiate between them. If one were to sanitize the virtual drive (the LUN), that would be an example of *logical* sanitization. If one were to identify the subsidiary devices used by the controller in creating the virtual drive and sanitize those, this would be *media-aligned sanitization*.

Logical sanitization is more commonly done because it is much easier to identify and access the virtual devices dedicated to a particular host than to parse out which chunks of storage on which physical drives contribute space to the higher level entity.

2.3 Terminology

Sanitization methodologies fall into three general classes: clear, purge and destruct. Clear is the least stringent while destruct, not too surprisingly, is the most stringent. Clear and purge leave the media in a reusable state while destruct does not.

2.3.1 Clear

ISO/IEC 27040 defines clear as "sanitize using logical techniques on data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques using the same interface available to the user". The clear operation is most often implemented using an overwriting process which fills every user-addressable block of the device with non-sensitive data (such as binary 0's). As noted earlier, on modern magnetic disks, a single overwrite pass is sufficient.

Clear is appropriate for media that must withstand logical attacks but will not be subject to physical attacks. This is basically due to the limitations inherent in only overwriting the user-addressable portions of the media as it excludes portions of the media that may be reserved and sections that may have been deleted from the usable space by sparing operations.

A clear operation is also not appropriate for solid state drives as technological features such as wear leveling may transparently (at the host level) move logically accessible data to different physical locations while leaving the previous location's content intact.

Though it may seem a bit confusing, organizations may choose to use the device specific commands (or even cryptographic erase) normally considered as appropriate for purge operations (see below) to perform a clear. This is basically due to convenience as these techniques typically execute much faster than an overwriting process. To help avoid confusion, remember that these techniques can be used for clear operations as a *matter of convenience* while purge operations rely on them because of their increased *effectiveness*.

2.3.2 Purge

ISO/IEC 27040 defines purge as "sanitize using physical techniques that make recovery infeasible using state of the art laboratory techniques, *but which preserves the storage media in a potentially reusable state*". A significant characteristic of purge operations is that they sanitize both user-addressable and non-user-addressable storage locations. This may be accomplished using specialized device commands or degaussing (for magnetic media).

Purge operations are appropriate when the media will be passing out of organizational control (recycled, donated, resold) as the organization cannot be sure of what level of effort a potential adversary may devote to retrieving information potentially remaining on the media.

Cryptographic erase

As media has become larger and as new technologies such as solid-state storage have come into widespread use, organizations have sought to minimize the time required to perform sanitization even on devices having sanitization commands. The increasing use of encryption for data at rest has provided a very fast technique for cryptographic erasure. Cryptographic erasure basically involves destroying the encryption key for the data and thus forcing an adversary to conduct an attack against the cryptologic implementation in order to gain access to the sanitized data. Another advantage of cryptographic erase is its high granularity. For example, it is theoretically possible to cryptographically erase a single field in a database by encrypting it under a random key that is immediately sanitized.

Cryptographic erase may also be the only effective technique for sanitizing certain types of media (such as flash-based solid-state storage).

Though it sounds deceptively easy to implement and very attractive because of its speed, there are a number of critical requirements that must be met:

Encryption must be applied before any data is written to the drive – this requirement assures that there is no data on the media in clear-text form.

High-pedigree encryption is required. This requires that the cryptographic algorithms themselves and their implementation must be reliable. This requirement is usually met by using only a well-vetted cryptographic implementation such as those that have met FIPS140-2 (or equivalent) certification. This is to assure that there are no weaknesses in the implementation that would make it easier for an adversary to access the encrypted information.

Effective key management is required. In order to conduct cryptographic erasure, ***all*** copies of the relevant key must be sanitized (including those in escrow or a centralized key management solution).[11]

Proof of encryption is required. In order for cryptographic erase to be accepted as a sanitization method, it must be reliably documented that the data was encrypted appropriately in the first place.

Meeting these requirements assures that a potential adversary must either mount a brute-force attack on the encrypted data or find a weakness in the algorithm or its implementation (highly unlikely in a well-vetted implementation).

2.3.3 Destruct

ISO/IEC 27040 defines destruct as "sanitize using physical techniques that make recovery infeasible using state of the art laboratory techniques and *results in the subsequent inability to use the media for storage*." Destruct is commonly implemented by means such as incineration, shredding, etc.

Though it sounds deceptively simple (and possibly even fun), care must be taken in selecting an appropriate method to match the risk of data exposure. Field expedient means such as firing a bullet through a disk might preclude its being put back in a server to read the data but the damaged platters might still provide useful data to a well-funded and technically adept adversary.

Whatever method is chosen should also consider environmental impacts accruing to what is done with the media (e.g., landfill waste), possible toxic fumes produced during incineration, etc.

[11] For further information, please refer to the whitepaper in this series: Storage Security: Encryption and Key Management

2.3.4 Summary

Selecting a sanitization method, like many other decisions in information security, is based on risk. Table 1 provides a concise summary of where each method is appropriate.

Method	Media End State	Adversarial Risk Level
Clear	Reusable	Low-Medium
Purge	Potentially Reusable	High
Destruct	Not Reusable	Very High

Table 1 Method vs. Adversarial Risk

Adversarial risk reflects media exposure (under/out of organization control), content information value and adversary capability.

Once the appropriate method has been identified, *Annex A* of ISO/IEC 27040 provides guidance in choosing the appropriate technique for a specific type of media.

3 Conclusion

Sanitization is a critical component of information lifecycle management to assure that information is not inadvertently disclosed when storage is reused, recycled or discarded. ISO/IEC 27040 provides extensive guidance in selecting methods and techniques for many types of storage based on the risk profile of the organization.

4 Acknowledgments

4.1 About the Author

Richard Austin has worked in the IT industry for over 35 years in positions ranging from software developer to security architect. He currently works in the Technology Office of HP Cyber Security. He is a senior member of both the IEEE and ACM and also holds the CISSP certification. In addition to active participation in SNIA's Security Technical Working Group, he participates in international standardization activities through INCITS/CS1.

4.2 Reviewers and Contributors

The Security TWG wishes to thank the following for their contributions to this whitepaper:

Eric Hibbard, CISSP, CISA	Hitachi Data Systems
Walt Hubis	Hubis Technical Associates
Dr. Alan Yoder	Huawei Technologies Co. Ltd.
Wayne Adams	EMC Corporation

5 For More Information

Additional information on SNIA security activities, including the Security TWG, can be found at http://www.snia.org/security.

Suggestion for revision should be directed to http://www.snia.org/feedback/.

The ISO/IEC 27040 standard can be purchased at http://www.iso.org.

Appendix A. Overview of ISO/IEC 27040

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 completions of a standard to address storage security. This is noteworthy since a major element of SC27's program of work (see Appendix B) 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*. 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

  Note 1 to entry: Storage security is focused on protecting data (and its storage infrastructure) against unauthorized disclosure, modification, or destruction while assuring its availability to authorized users.

  Note 2 to entry: These controls may be preventive, detective, corrective, deterrent, recovery, or compensatory in nature.

- ***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).

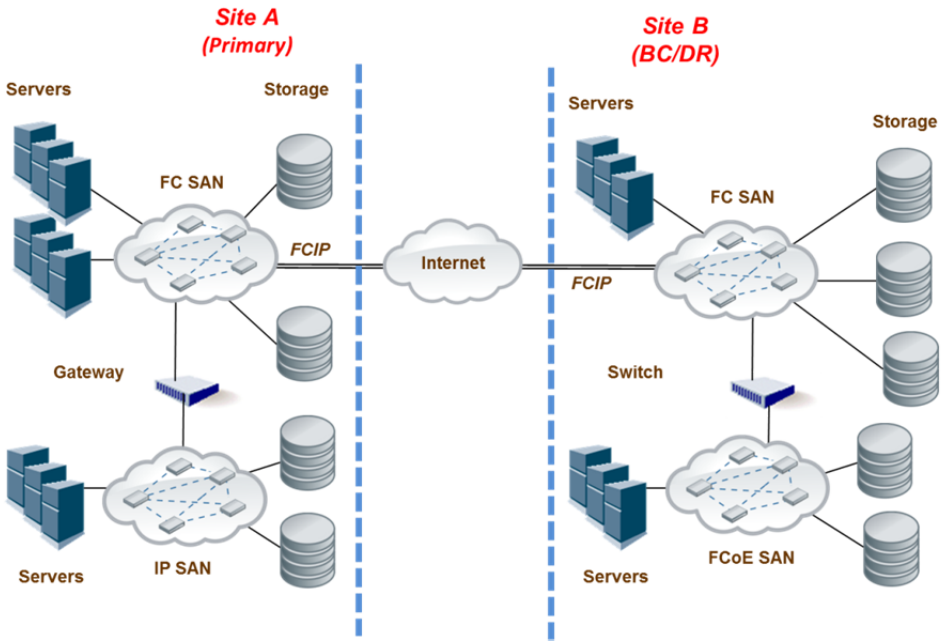
ISO/IEC 27040 approaches storage security guidance from two angles: 1) supporting controls and 2) design and implementation of storage security. Both are addressed in sufficient detail that storage professional with limited security knowledge and security/audit professionals with little storage background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



(Source: ISO/IEC 27040:2014, Figure 2; developed by SNIA Security TWG)

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 providing detailed coverage of this topic and it is structured such that it can be referenced like the 1995 version of DoD 5220.22-M document, which 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.

Summary

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).

Appendix B. Overview of ISO/IEC JTC 1/SC27

The International Organization for Standardization (ISO) is the world's largest developer of voluntary International Standards and it is an independent, non-governmental organization made up of members from the national standards bodies of 164 countries and 3,368 technical bodies.[12] Since its founding in 1947, ISO has published over 19,500 International Standards covering almost all aspects of technology, business, and manufacturing (e.g., from food safety to computers, and agriculture to healthcare).

Founded in 1906, the International Electrotechnical Commission (IEC) is the world's leading organization that prepares and publishes International Standards for all electrical, electronic and related technologies, collectively known as "electrotechnology."[13] "Over 10,000 experts from industry, commerce, government, test and research laboratories, academia and consumer groups participate in IEC Standardization work."

ISO and IEC are two of the three global sister organizations (International Telecommunication Union, or ITU, being the third) that develop International Standards for the world. When appropriate, some or all of these SDOs cooperate to ensure that International Standards fit together seamlessly and complement each other. "Joint committees [e.g., JTC 1] ensure that International Standards combine all relevant knowledge of experts working in related areas." All ISO/IEC International Standards are fully consensus-based and represent the needs of key stakeholders of every nation participating in ISO/IEC work. "Every member country, no matter how large or small, has one vote and a say in what goes into an [ISO or] IEC International Standard."

Subcommittee 27 (SC27)

Within JTC 1, SC27 has responsibility for the development of standards for the protection of information as well as information and communications technology (ICT). This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as

- Security requirements capture methodology;
- Management of information and ICT security; in particular information security management systems (ISMS), security processes, security controls and services;
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;

[12] *About ISO*, INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, http://www.iso.org/iso/home/about.htm (last visited September 15, 2014).
[13] *About the IEC*, INTERNATIONAL ELECTROTECHNICAL COMMISSION, http://www.iec.ch/about/?ref=menu (last visited September 15, 2014).

- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;
- Conformance assessment, accreditation and auditing requirements in the area of information security;
- Security evaluation criteria and methodology.[14]

Since convening its first plenary session in April 1990, SC27 has published more than 120 standards and it currently has in excess of seventy-five active projects. To manage these projects and the on-going maintenance associated with the published standards, SC27 is organized into the following working groups (WGs)[15]:

- WG 1: Information security management systems (ISMS)
- WG 2: Cryptography and security mechanisms
- WG 3: Security evaluation, testing, and specification
- WG 4: Security controls and services
- WG 5: Identity management and privacy technologies
- SWG-M: Special working group on management items.
- SWG-T: Special working group on transversal items.

[14] International Organization for Standardization/ International Electrotechnical Commission [ISO/IEC], *SC 27 Business Plan October 2013—September 2014*, at 1.2, ISO/IEC JTC 1/SC 27 N12830 (Sept. 30, 2013).

[15] *ISO/IEC JTC 1/SC 27 IT Security techniques*, INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, http://www.iso.org/iso/iso_technical_committee?commid=45306 (last visited May 15, 2014).