Storage Networking Industry Association
Technical White Paper

Storage Security: An overview as applied to storage management

Version 1.0

August 2, 2016

Abstract: *The ISO/IEC 27040 (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 key security concepts as they relate to storage security and summarizes the security guidance in the standard as applied to storage management. It also provides additional SNIA guidance in developing a storage management security program to meet organizations' 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) 2016, 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/.

Copyright © 2016 SNIA. All rights reserved. All other trademarks or registered trademarks are the property of their respective owners.

Revision History

Revision	Date	Sections	Originator:	Comments
V0.1	*4/24/2016*	All	Richard Austin	Initial Draft
V0.2	*7/19/2016*	All	Richard Austin	Incorporate review comments
V1.0	*8/2/2016*	All	Richard Austin	Incorporate final editorial comments

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, *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

This SNIA whitepaper presents a gentle introduction to information security for the storage professional and its application in securing storage management as a case study. The intent is to equip the storage professional to make effective use of the guidance in ISO-IEC 27040 supplemented by industry best practices in assuring adequate security for the storage assets in their charge.

1 What is "security"?

"Security" is an often discussed word these days and most everyone agrees that having more of it is better as if one could walk into the nearest consultancy and say "I'd like 3 tons of security please." The problem is that security is not really a thing at all but rather a sort of condition. This "secure" condition can be said to exist when all the risks an organization faces are managed down to its risk tolerance at some point in time.

There are a lot of odd words in that last sentence "risk", "management" and "risk tolerance" and it turns out that most of the confusion about this thing called "security" is based on a lack of understanding of those terms.

1.1 Security is really about managing risk

We all have an idea of what risk is – we may have an auto accident on the way to work this morning, it may rain today, the stock market may move in an unexpected direction, our business competitor may introduce a significant new product. Each of those possible situations has some things in common:

- There is a particular potential loss[1] (we may be killed or injured in an auto accident; we may get wet unless we carry an umbrella …).
- There is something that can be done to reduce the loss (carry an umbrella, maintain auto insurance and drive carefully, diversify the stock portfolio …).
- There is a general idea of how likely the loss is (40% chance of rain today).

We could put those three factors together into a sort of equation that says that risk is determined by the likelihood of the loss and the size of the loss reduced by whatever we put in place to mitigate the risk[2].

[1] The risks we will think about are formally called "pure risks" because they lack an upside. For example, if I bet $10 on my poker hand, I may lose that $10 or may win several times that so there is both an upside and downside outcome I must consider. Information security risks only have loss outcomes so we focus on ways to avoid those losses.

$$Risk = f(Loss, Likelihood) - Mitigations$$

As you apply more mitigations, risk[3] will decrease so how do you know when you're done? Organizations have a tolerance for risk that varies – some are very conservative and have a very low tolerance for risk. Some, for example a dynamic start-up, have much higher tolerances. You are finished mitigating risks when the remaining risk is within the tolerance of your organization (or you run out of budget, whichever comes first).

1.2 Adversarial Risk

When we think about risks, we quickly realize that there are different types of risks. One which has muddied risk management in information security is the distinction between impersonal risk and adversarial risk.

A tornado in the area is not going to deliberately change course to destroy your main data center. This is an example of an impersonal risk – the tornado is a force of nature and is not targeting you in particular (though as Mr. Murphy frequently reminds us, it certainly seems that way sometimes). Impersonal risks tend to be better understood and have mature risk management processes (e.g., the insurance industry that can pay death benefits yet still make a profit).

However, Jane Hacker, in the employ of a multi-national criminal enterprise, may indeed be very interested in your organization specifically or even you personally as a stepping stone to her target. This is a targeted risk and is a horse of a very different color. Developing the basic factors for our risk equation becomes much more difficult and we tend to have to make do with qualitative estimates which often degenerate into truisms such as "store the information and they will come".

Unfortunately, most information security risk derives from human adversaries.

[2] Note that we do not say "eliminate" the risk as that is generally impossible except in trivial cases (e.g., we don't go out of our house; we never drive or ride in an automobile …). When we carry an umbrella to avoid getting wet in a rainstorm, there's still the chance that a strong wind gust may either blow our umbrella away or destroy it.
[3] Technically, residual risk since this is the risk remaining after the mitigations have been applied.

1.3 Risk management versus compliance

The information security industry today spends a lot of time talking about compliance which basically means verifiably doing what some (hopefully) knowledgeable and responsible body has decided is necessary. For example, if you process payment card information, you must comply with the PCI-DSS requirements. If you store or process personal health information in the USA, you must comply with HIPAA, and the list goes on.

However, "security" is a different thing than "compliance". Compliance basically means that you have followed all the applicable items on some checklist while security implies that all the important risks in your environment have been mitigated to an acceptable level.

Threats

While a catalog of specific threats can be quite lengthy, the effects of a threat typically involve compromising at least one of the following:

- Confidentiality – Information is available only to authorized entities
- Integrity – information is protected from unauthorized modification whether intentional or accidental
- Availability – information is available to authorized users when needed

These three categories are often called the C-I-A triad. To give some examples, a data breach is an example of compromising confidentiality; changing the amount of a payables check to be three thousand dollars instead of thirty dollars compromises integrity; and a denial of service attack compromises availability.

2 The ISO View of Risk

ISO has spent a lot of time thinking about risk in general and information security risk in specific. Because of this broad approach, the ISO view of risk is scattered across several standards in many contexts. The following is a general summary in the context of information security.

Figure 1 illustrates the important terms that give rise to risk ("effect of uncertainty on objectives", ISO/IEC 27000). Risk begins with a threat ("Potential cause of an unwanted incident that may cause harm to a system, individual or organization", ISO/IEC 27032). A tornado or a successful compromise of privileged logon credentials are examples of threats. Since we are particularly interested in adversarial risk, another important term (not shown in Figure 1) is threat agent ("Entity that can adversely act on assets", ISO/IEC TR 2004). Jane Hacker is an example of a threat agent.[4]

[4] Knowledge of threat agents is important because it helps us assess their motives and capabilities. A casual "hacker" might attempt to instantiate a threat for bragging rights in some online forum and only have access to known, mass-market attacks. An operative in the employ of a nation state might attempt to instantiate a threat to obtain valuable intellectual property and have access to sophisticated techniques and capabilities.

Threats make use of (exploit) vulnerabilities ("weakness of an asset or control[5] that can be exploited by a threat", ISO/IEC 27032). Examples of vulnerabilities are the ever-present software defects that keep our patch teams busy or a careless employee who clicks on a link in an EMAIL from a stranger with the subject "I Love You!"[6].

Successful exploit of a vulnerability causes an event ("identified occurrence of a system or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant", ISO/IEC 27000) which may have consequences that interest us (again, this isn't certain as, for example, the adversaries' desired consequence may be blocked by a control such as an anti-malware product blocking the malicious link in the "I Love You!" e-mail). Another useful concept when thinking about threat agents and vulnerabilities is threat vector (ISO refers to this as an attack vector "path or means by which an attacker can gain access to a computer or network server in order to deliver a malicious outcome", ISO/IEC 27032). A threat vector is the line that connects a threat agent to the vulnerability. In the "I Love You" example, the e-mail is the threat vector.

If the consequence is significant enough, it may give rise to a security incident ("single or series of unwanted information security events that have a significant probability of compromising business operations or threatening information security", ISO/IEC 27000). An incident indicates that the adversary likely has achieved their objective in penetrating our defenses.

Though the terms may seem foreign and somewhat cryptic, they embody an approach to estimating the likelihood and magnitude of a loss. Likelihood depends on threats and vulnerabilities (and how easily a threat may exploit a vulnerability) while consequences measure the loss.

[5] A control is what we called mitigations earlier.

[6] This is a necessary reminder that not all vulnerabilities are technical in nature (bug in software, misconfiguration of a firewall, etc.) but also include non-technical vulnerabilities such as human behavior.

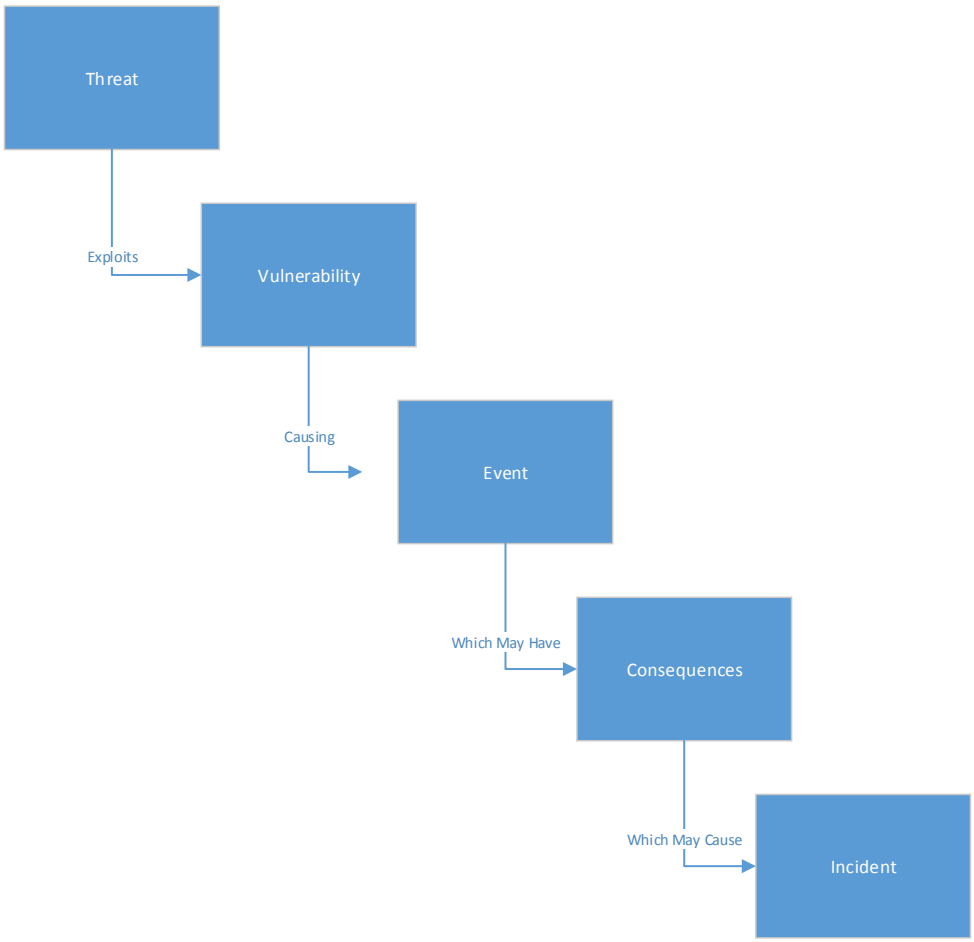


Figure 1 ISO Risk Model

2.1 Risk Management

Risk management is basically concerned with assuring that an organization identifies the risks in its environment and mitigates them as much as possible[7]. In an ideal world, there would be a risk assessment which produced an ordered list of risks, highest to lowest, and we would manage those risks by applying controls (mitigations). For example, we might purchase and install a firewall to limit the types of traffic incoming to our corporate webservers; we might purchase an e-mail gateway that could scan all the e-mails coming into our domain for malware and so on. These mitigations have costs both in acquiring them and operating them and our budget, supply of qualified people, etc., will always be limited so it's important that we apply mitigations where they will produce the greatest reductions in risk for our organization.

[7] The generic ISO risk management vocabulary and process are too opaque to introduce here.

Ideally, when our risk management is complete, we will have mitigated all known risks to within the risk tolerance of our organization. However, it is all too often the case that we mitigate until we run out of budget or available people with some risk items still remaining. This is unfortunate but we are still in a much better place for having assessed and attempted to manage our risks as we now know what risks remain and their probable impacts on our organization.

3 The Storage Threat Model[8]

ISO/IEC 27040 identifies several common classes of threats for storage and its supporting infrastructure:

- Unauthorized usage – use of storage capacity itself without authorization. An adversary might use storage as a depot to contain exfiltrated data from your own or other organizations prior to its being delivered to its final destination.
- Unauthorized access – access without authorization (or in excess of authorization) to information, management networks, management applications, etc. For example, an adversary might compromise a set of administrator's credentials and use them to access a management application to grant access to storage containing sensitive information.
- Liability due to regulatory non-compliance – there is a growing intolerance for loss of data (i.e., data breaches) and regulatory agencies may impose stiff fines or other penalties on organizations that fail to protect the information in their care.
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.
- Theft or accidental loss of media.
- Malware attack or introduction.
- Improper treatment or sanitization after end of use.

Likely results of the realization of these threats include data breaches, data corruption or destruction, temporary or permanent loss of access/availability and failure to meet statutory, regulatory or legal requirements.

Each of these results can cause a loss to the organization with the amount of loss depending on the scope and effect of the incident.

[8] The risks in a particular organization cannot be discussed in a general sense as they depend on the characteristics and circumstances pertinent to that specific organization. Threats, on the other hand, can be discussed much more generally. Users of this whitepaper will need to assess the threats, relevant vulnerabilities and the probable resulting impacts to determine their level of risk.

4 Why the security of storage management matters

As the astute reader will have already noticed, there is a common thread running through the classes of threats – storage management can be involved in most of them. A storage infrastructure is a complex structure made up of many interconnected devices that create the fiction of a flexible mass of SCSI cables that can connect any host to any storage. This fiction requires significant management to configure and assure its continued operation. When we talk about "storage management" we're talking about five general classes of activities (ISO/IEC 27040, section 6.4.1):

1. Operation – keeping the storage (and the services built on it) up and operating normally.
2. Administration – keeping track of resources in the storage infrastructure and how they are assigned.
3. Maintenance – performing repairs, upgrades and the general day-to-day tuning and adjustments that assure efficient operation.
4. Provisioning – preparing a system to provide services.
5. Sanitization – assuring that the previous contents of storage are rendered unreadable when it is either removed from service or repurposed.

Management can either be in-band, out-of-band or a hybrid of the two. In-band management uses the same network used to transport the data while out-of-band uses a separate management network (commonly TCP/IP). A hybrid solution uses in-band for some functions and out of band for others. For example, the actual management traffic may be in-band while an out-of-band network is used to communicate with an authentication server.

Out of band management networks are of particular concern as they commonly are implemented by a TCP/IP network and if there's one thing our adversaries have a great deal of experience doing, it's attacking across a TCP/IP network.

Consequences of compromising storage management can be quite severe. If an adversary can compromise a powerful set of storage administrator credentials, they achieve significant control over the SAN environment where they can modify zoning configurations, allocate/deallocate storage, perform a factory reset on an entire disk array, etc., with high impacts to the confidentiality, integrity and availability of storage assets.

5 Securing storage management

Storage management is quite powerful and also fairly exposed as it must be accessible to those charged with managing the storage infrastructure (whether present locally or remotely), vendor support personnel (usually remote) and auditors. Couple this with the common practice of out-

of-band management over a TCP/IP network and it becomes an attractive target for adversaries.

ISO/IEC 27040 provides solid guidance in securing storage management.

5.1 Authentication and Authorization

For authentication, ISO/IEC 27040 recommends the following best practices:

- All users should have a unique identifier – though this seems obvious, it is still sometimes possible to have a generic user identifier such as "Administrator" used by multiple entities when performing administrative tasks. The problem is that actions are no longer traceable to a specific person. This complicates responding to a credential compromise because, for example, changing the password now affects multiple users rather than just the affected user.
- Use a suitable authentication technique – this decision is based on both good practice and the risk associated with the credential being compromised (e.g., a credential with broad administrator capabilities poses much more risk than one with a restricted set of capabilities). Recommendations include:
    - Use strong passwords and enforce requirements for length, complexity (use of

What is "Authentication and Authorization"?

Authentication and authorization are two sides of a coin concerned with who is allowed to do what. Authentication is the proving of some asserted identity. When you log in to your banking website, you identify yourself by a user name, EMAIL address, mobile number or some other identifier that asserts who you are (your identity). You must then furnish proof that you are in fact who you say you are. This proof can take four general forms:

1. Something you know – a password or other secret information.
2. Something you have – a hardware token.
3. Something you are – usually a biometric such as a fingerprint, retinal scan or gesture.
4. Someplace you are – relies on the security controls applied in gaining access to a location (e.g., a SWIFT wire transfer terminal or the launch station for a ballistic missile).

These assurances may be used singly (single-factor) or in combination (multi-factor). An example of two-factor authentication would be a hardware token (something you have) that requires a PIN (something you know).

Authorization is concerned with what an authenticated identity is allowed to do. We're likely all familiar with running our laptops as a normal user and having to elevate our privileges (through sudo or User Account Control) to perform administrative tasks. Authorization is a means of implementing the security principle of least privilege (an entity should possess only the minimum set of privileges required to perform a task). This is important as it restricts the damage an adversary with a compromised set of credentials can inflict.

Authorization can take a number of forms ranging from the simple administrators-can-do-anything while users can do little to assigning specific capabilities to individual users to designing roles. While simple all-or-nothing authorization is easy to implement, it carries much more risk as a compromise of administrative credentials can be disastrous. Assigning individual capabilities to users (where permitted by the vendor) provides very granular control of user capabilities but can rapidly become a nightmare to manage. Roles (again, where implemented by the vendor) offer a good compromise. For example, one might define a zone-administrator role with the capability to manage zoning and then assign user Jane.Smith to that role. If Jane then leaves the organization or changes jobs, it is easy to just remove that role. This RBAC (Role Based Access Control) is attractive but engineering the role definitions (implementing the principle of least privilege and separation of duties) requires planning and discipline.

special characters, etc.) and periods of use.
    - Stronger authentication processes such as use of a challenge-response protocol (mitigates the possibility of replay attacks) or multi-factor authentication.
- Use a strong authentication technique for all remote access.
- Use a centralized authentication solution (such as RADIUS or some other single sign-on technology) – Managing user credentials can become a challenging task as the number of devices increases. Compared to managing the local user database on hundreds of devices, a centralized authentication solution allows all changes to be made once in one place.
- Use multi-factor authentication when managing sensitive and high-value data -- such data poses significant risk if an adversary should gain access to it and use of the strongest authentication processes mitigates the possibility of such a risk being realized.

For authorization, ISO/IEC 27040 recommends making use of roles implementing least privilege. Recall that least privilege seeks to restrict capabilities to the minimum required to perform a specific function. The idea here is to compartmentalize the damage that a credential compromise or other misuse can inflict. As a minimum the following roles are recommended:

- Security administrator – This role has the capabilities to create and manage accounts with their associated privileges, control audit logging configurations and content, establish trust relationships with IT infrastructure (e.g., which specific RADIUS server can authenticate users), manage certificates and key stores as well as other cryptographic infrastructure (such as key management[9]).
- Storage administrator – Having view and modify rights for all aspects of a storage infrastructure with the exception of capabilities reserved for the security administrator role. Note this this is usually considered to be a non-security role.
- Security auditor – This role has view (read-only) access to security relevant information to allow audit of entitlements (i.e., which users have which capabilities), verification of security-relevant configuration items, and audit logs. Note that this role does not have the capability to change anything.
- Storage auditor – Similar to the security auditor, this role has view access to enable verification of storage parameters and configurations and correct operation (e.g., viewing health/fault logs). This role cannot change any of the settings it may view.

SNIA recommends that each user should be associated with at most one of these roles. This helps with implementation of the principle of separation of duties as, for example, implementing a security sensitive operation such as adding a new authentication server requires cooperation of both the security and storage administrator roles.

[9] Though not specifically identified in the standard, in some environments the administration of cryptographic infrastructure is split out into a separate cryptographic officer role.

5.2 Secure the Management Interfaces

Most SAN devices expose physical management interfaces that allow their operations to be configured, controlled and monitored. Failure to protect these management interfaces, whether serial ports, modem (sometimes used for remote support access) or network (either in-band or out-of-band), can lead to unauthorized use with consequents of data destruction, corruption or denial of access.

To protect the physical management interfaces, ISO/IEC 27040 recommends:

- Restrict physical access to management interfaces – it should not be easy for an intruder to walk up to a SAN switch, for example, and plug in to its serial port.
- Disable and disconnect serial management ports when not in use.
- Segregate LAN interfaces used for management traffic from other LAN traffic – the intent is to limit access to the management LAN from the larger network. Physical isolation is preferred but virtual isolation (VLAN) may be used when necessary.

Beyond the physical interfaces, devices also provide software (or firmware) and API's (Application Programming Interface) that allow their operation to be managed and monitored through command-line tools, SNMP and GUI applications. ISO/IEC 27040 recommends the following best practices for securing these interfaces:

- Use firewalls or TCP wrappers to restrict access to management networks.
- Use entity authentication to establish trust relationships between storage systems and management systems – though the earlier discussion of authentication focused on users for ease of understanding, it is important for a storage system to be able to assure that the management stations attempting to control it are authentic.
- Leverage IDS and IPS to identify anomalous behavior and block it.
- Properly secure supporting infrastructure (DNS, SLS, NTP, etc.) to preclude their being used in an attack.
- Effectively use privileged user controls as discussed above under "Authentication and Authorization".
- Ensure that operating systems and applications are up-to-date and sufficiently hardened – software vulnerabilities, unfortunately, are pretty much of a given these days. It is important to assure that known vulnerabilities are remediated as quickly as possible to close potential vectors of attack. "Hardening" entails disabling unused services, prohibiting less secure protocols, etc., in order to minimize the possible vectors for attack (in the trade, we call this the "attack surface").

Remote management of storage systems is quite common (e.g., storage administrators may be centrally located while storage itself is decentralized). Enabling remote management while minimizing potential for malicious use involves the following additional security controls:

- Use secure channels for remote access -- These include VPN, TLS[10], or SSH. These protocols can mitigate the risk of interception, spoofing and tampering with remote management traffic.
- Require strong authentication such as multi-factor authentication.
- Follow the principle of least privilege to restrict remote access to the minimum capabilities required.

A specialized case of remote access occurs when vendors need remote access to storage systems for maintenance or support functions. Since these remote support sessions commonly use external networks or the phone system, the guidance for remote management should be followed with additions such as special authorization to enable a remote support session and specific audit logging of access and actions performed. When the phone system is used, a modem call-back protocol should be implemented and specifically authorized when a vendor session is necessary.

5.3 Security Auditing, Accounting and Monitoring

Storage systems are capable of generating many kinds of log records which can provide a detailed timeline of events in the storage infrastructure. Some of these events will be highly relevant from a security perspective whether used in compliance monitoring or as part of incident response or forensic investigation. While ISO/IEC 27002 (section 12.4) provides guidance on general event logging, ISO/IEC 27040 provides the following guidance specific to storage systems:

5.3.1 Include storage systems in the organization logging

Though it would seem obvious, many times storage infrastructures are largely ignored when organizations think of implementing audit logging. Given their criticality to the organization's operation, it is important that they be subject to and participate in the organization's logging processes.

- Mandate that storage systems comply with the organizational logging policy.
- All significant storage management events should be collected – identifying the significant events can be challenging as there are a large number of events to choose from and vendor documentation can sometimes be rather cryptic on just what a particular event actually represents. A common way to identify relevant events is to capture all events generated when an action is carried out (e.g., administrative logon, implementation of a zoning change, etc.) and review them to identify candidates for

[10] Recommendations for usage of TLS in storage systems is available in ISO/IEC 20648 which is also available as a SNIA Technical position.

collection. Some vendors also publish a "message manual" which lists all events generated by a particular product and this can be a good starting point as well.

- Log data is preserved – unfortunately, adversaries also know about log records and will attempt to prevent their generation or clear them from archival storage.
- Log data is archived and retained according to the organizational log data retention policy.
- Device time is synchronized with a reliable external source – many times an incident response will entail analyzing events from multiple sources and if the time is not consistent across all the potential sources, log analysis can become a nightmare.

5.3.2 Employ external (or centralized) event logging to a trusted remote source

By default, many devices maintain their event logs locally but forwarding them to a centralized point provides both better protection and easier correlation and analysis of events from multiple sources. The following practices are recommended:

- Implement centralized (i.e., events within a single security domain forward their events to a common point) audit logging to collect events from multiple sources in a single repository.
- Establish and use a common, accurate time source across the environment to assure that events from multiple sources can be arranged in an accurate timeline for correlation and analysis.
- Avoid use of device resident logs for anything other than health monitoring and problem resolution as they have a short lifespan (on-board storage is typically quite limited) and are more easily cleared or modified by an adversary.
- Use multiple log servers to collect events to provide redundancy.
- Use standard logging protocols such as syslog with preference for those versions that provide reliable delivery and secure transport (e.g., through use of TLS).
- Configure devices to forward events immediately rather than buffering them into batches prior to forwarding them to the collection points.
- Use correlation across multiple event sources during analysis to improve detection of incidents (e.g., correlating multiple invalid logon attempts recorded by an authentication server followed by a successful logon to a storage device using administrative credentials may indicate a successful brute forcing of a credential).
- Ensure that storage event logging is integrated into the Security Information and Event Management (SIEM) system when such a product is in use.

5.3.3 Ensure complete event logging

The audit logs of events occurring across a storage infrastructure (and its supporting technologies) provide a rich treasure trove of data for assessing compliance and supporting detection and investigation of security incidents. However, you can't use data which you don't

have so it is critical to assure that the audit logs are as complete as possible within the limits of capacity (e.g., audit logs require space and the more events you log and the longer you keep them, the more total space will be required). To provide for an effectively useful audit log, ISO/IEC 27040 provides the following recommendations:

- Once the set of events of interest has been determined, then all occurrences of those events should be logged (whether in-band or out-of-band).
- A *minimum* set of events should always be logged:
    - Failed and successful logon attempts – a series of failed logon attempts over a short period of time may indicate a brute-force compromise attempt while successful logons are useful in tying actions within the infrastructure to the entity that performed them.
    - Failed file and object access attempts for sensitive and high-value data – failed access attempts may indicate an adversary's conduct of reconnaissance within the infrastructure.
    - Account and group profile additions, changes and deletions – a very common adversary tactic after a successful intrusion is to elevate their privileges (e.g., by adding the credential they've compromised to the administrator's group). Adversaries may also create new credentials in the interest of maintaining access in case their compromised credential is discovered and disabled.
    - Changes to system security configurations such as log settings, network filtering rules, zoning configuration, etc. – This is another way an adversary elevates their access within an infrastructure.
    - Changes to security server usage (e.g., syslog, NTP, DNS, etc.) – For example, DNS is commonly used to map network names to their associated network address and an adversary might remap the organizational server name to the address of a server under their control.
    - System shutdowns and restarts – Unexpected shutdowns/restarts may indicate adversarial actions such as reconfiguration, etc.
    - Privileged operations.
    - Use of sensitive utilities.
    - Access to critical system files.
    - Movement of virtual servers between physical hosts.
- Each log entry should include at a minimum:
    - A timestamp that includes both date and time.
    - A severity level – this may or may not be significant from a filtering and analysis point of view as this is typically "designer's choice". For example, significant security events may be coded as "informational".
    - The source of the log entry – That is, the entity that generated the log record. This may be in the form of a name or even network address.

    - An event identifier as a well as a text identifier which may be localized in language (i.e., the event ID may be constant but the text identifier could be translated into the local language).
    - A description of the event – parsing the text description is the most challenging part of analyzing events as there is no widely accepted standard and the text is whatever was chosen by the vendor.
- Choose filters with care – as noted earlier, fields such as "severity" may be unreliable indicators of the importance of events. The organizational logging and retention policy should be the final arbiter of what events are relevant and for how long they should be retained.

5.3.4 Implement appropriate log retention and protection

As audit logs may be used to demonstrate compliance or to support an incident investigation, they must be retained and protected appropriately. ISO/IEC 27040 lists the following considerations:

- Audit log data that may have evidentiary value should be handled correctly – The prevailing legal system will impose requirements on data that may be used in legal proceedings such as chain of custody, verifiable integrity and authenticity, etc.
- Audit data with specific retention requirements (e.g., regulatory compliance) should be preserved using the organization's data retention process.
- Implement appropriate protections to preserve log integrity and protect them from unauthorized modification or destruction (whether intentional or accidental).
- When audit logs contain sensitive information (e.g., authentication information, cryptographic keys, etc.), the confidentiality of the data should be assured.
- For unique audit logging requirements (e.g., code signing), dedicated and especially hardened systems should be used.
- Leverage log relays and log filtering to minimize impact of specialized storage requirements (e.g., WORM).

5.4 System Hardening

Hardening is a process that seeks to minimize the attack surface of a system in order to limit opportunities for an adversary to attack it. Best practices in hardening a system include:

- Remove/disable un-needed/un-used software and services – Unfortunately, operating systems tend to include software and services (commonly in the name of usability) that are not required in all environments. Disabling or removing these un-needed items assures that any vulnerabilities found in them will not put the system at risk.
- Remove unnecessary accounts.
- Make changes (rename, disable, change default password, etc.) to default accounts.

- Only enable required network ports – If a port is closed or blocked, then any attack that makes use of that port will fail.
- Install patches from a trusted source in a timely fashion -- There is quite an industry devoted to reverse engineering vendor security bulletins to identify underlying vulnerabilities and develop exploits for them. It is important that patches be installed as quickly as possible. However, it is equally important to assure that patches are obtained from a trustworthy source as there have been several attacks where the vector was a supposed "security patch".
- Update firmware from a trusted source – Firmware is just another form of software and though it's typically obscure enough that we haven't seen (or recognized) attacks using malicious storage device firmware, it is best to use good update hygiene here as well.
- Install and maintain up-to-date malware protection – Malware remains a constant threat so protection against it is an important requirement. Adversarial innovation in this area is rapid and ongoing so it is critical for any malware protection to be continually updated.

6 Additional SNIA Guidance

Guidance regarding other security relevant topics can be found in the following SNIA publications[11]:

SNIA Storage Security: Sanitization – this whitepaper deals with the important topic of assuring that data that is no longer useful (or required to be retained) is rendered irrecoverable in a way matching the risk posed by inadvertent disclosure of the data.

SNIA Storage Security: Encryption and Key Management – Encryption plays a critical role in assuring the confidentiality of data, however, unless it is implemented correctly, it only creates the illusion of protection which can be more dangerous than no protection at all. This whitepaper provides useful guidance for properly implementing encryption and associated key management processes.

SNIA Storage Security: Fibre Channel Security -- The Fibre Channel Security Protocol (FC-SP) provides useful features such as entity authentication within a storage infrastructure. This whitepaper provides a useful introduction to FC-SP and recommendations for using it effectively in securing a storage infrastructure.

SNIA Technical Position, TLS Specification for Storage Systems – TLS (Transport Layer Security) is widely used in securing interactions with web applications and this whitepaper provides guidance on the proper use of TLS in storage systems (e.g., recommended cipher suites).

[11] Available for download at http://www.snia.org/securitytwg

Though primarily aimed at storage vendors, this document provides a useful guide for storage consumers in developing requirements. This document has also been standardized as ISO/IEC 20648.

SNIA Index for ISO/IEC 27040 – ISO standards, unfortunately, do not include an index which can make locating specific information difficult. This document provides an extensive index for the standard and makes it much easier to use in practice.

7 Conclusion

As a supplement to ISO/IEC 27040, this whitepaper has provided a gentle introduction to information security as the process of managing risk in a particular environment. After reviewing the common threat categories for storage systems, the guidance provided by ISO/IEC 27040 for securing storage management was reviewed.

The reader should be better prepared to assess the specific risks in their own environment and apply the security guidance from ISO/IEC 27040 in reducing those risks to an acceptable level.

8 Acknowledgments

8.1 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 security architecture for HPE 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.

8.2 Reviewers and Contributors

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

Eric Hibbard, CISSP	Hitachi Data Systems
Walt Hubis	Hubis Technical Associates
Gary Sutphin	
Tim Hudson	Cryptsoft
Thomas Rivera	Hitachi Data Systems

9 For More Information

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

Additional SNIA materials associated with ISO/IEC 27040 can be found at: http://www.snia.org/securitytwg.

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).

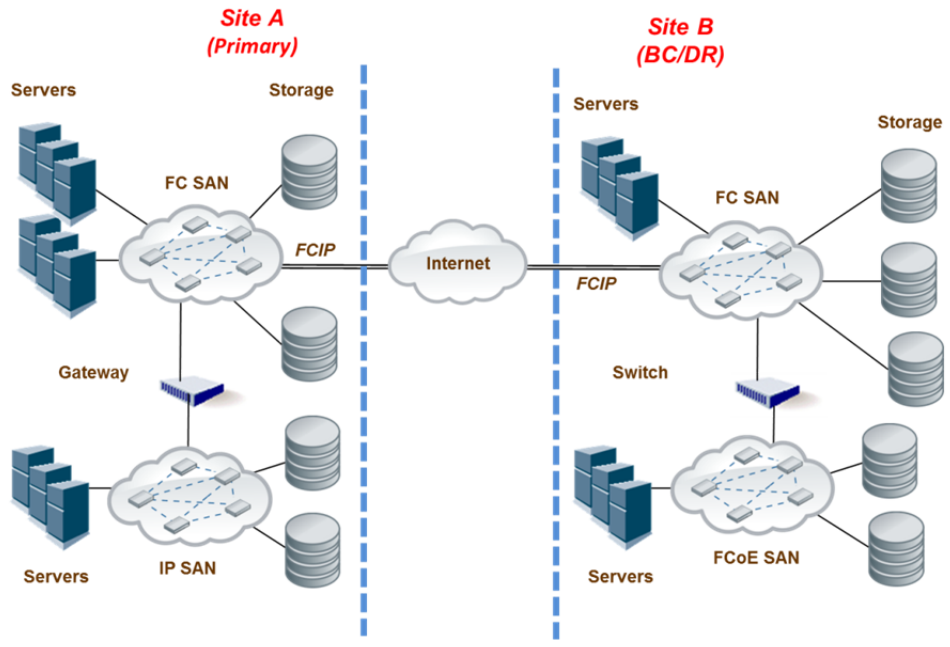
ISO/IEC 27040 approaches storage security guidance from two angles: 1) supporting controls and 2) design and implementation of storage security. Both are addressed in sufficient detail that storage professional with limited security knowledge and security/audit professionals with little storage background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

[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).

- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- 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).

Bibliography

[01] IETF RFC 2865 *Remote Authentication Dial In User Service (RADIUS)*

[02] IETF RFC 4303 *IP Encapsulating Security Payload (ESP)*

[03] IETF RFC 4595 *Use of IKEv2 in the Fibre Channel Security Association Management Protocol*

[04] IETF RFC 7296 *Internet Key Exchange Protocol Version 2 (IKEv2)*

[05] ANSI INCITS 461–2010, *Fibre Channel — Switch Fabric — 5 (FC-SW-5)*

[06] ANSI INCITS 462–2010, *Information Technology — Fibre Channel - Backbone — 5 (FC-BB-5)*

[07] ANSI INCITS 463–2010, *Fibre Channel — Generic Services — 6 (FC-GS-6)*

[08] ANSI INCITS 470–2011, *Fibre Channel — Framing and Signaling-3 (FC-FS-3)*

[09] ANSI INCITS 496–2012, *Information Technology — Fibre Channel — Security Protocols — 2 (FC-SP-2)*

[10] SNIA *Storage Security: Encryption and Key Management*, August 2015