Storage Networking Industry Association
Technical White Paper

Storage Security: Fibre Channel Security

Version 1.01

September 6, 2016

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 Fibre Channel (FC) security guidance in the standard as applied to Storage Area Networks (SAN). It also provides additional SNIA guidance in developing a FC 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/.

Revision History

Revision	Date	Sections	Originator:	Comments
V0.1	*4/2/2015*	All	Eric Hibbard	Initial Draft
V1.0	*5/20/2016*	All	Eric Hibbard	Final 1.0 Text
V1.01	*9/6/2016*		Eric Hibbard	Minor Edits

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

Fibre Channel is often viewed as a specialized form of networking that lives with data centers and neither has or requires special security protections. Neither of these assumptions is true, but finding the appropriate details to secure Fibre Channel infrastructure can be challenging. This SNIA storage security whitepaper leverages the guidance in the ISO/IEC 27040 standard and provides value added information on Fibre Channel as it relates to storage systems and ecosystems.

1 Introduction

ISO/IEC 27040:2015 *Information technology - Security techniques - Storage security* provides detailed technical guidance in securing storage systems and ecosystems (see Appendix A for an overview). While the coverage of this standard is quite broad it lacks details for certain important topics.

This whitepaper, one in a series from SNIA that addresses various elements of storage security, is intended to leverage the guidance in the ISO/IEC 27040 standard and enhance it with a specific focus on Fibre Channel (FC) security. The whitepaper provides background information on Fibre Channel, summarizes the FC security options, explores the relevant ISO/IEC 27040 guidance, and offers additional information to help secure FC-based storage.

2 Storage Technology Overview

This section briefly describes key storage technologies with the intent of setting the stage for the security descriptions and guidance.

2.1 Storage Area Networks (SAN)

A Storage Area Network (SAN) is a specialized, high-speed network that provides block-level network access to storage. SANs are typically composed of hosts, switches, storage elements, and storage devices that are interconnected using a variety of technologies, topologies, and protocols. SANs may also span multiple sites.

SANs are often used to

- improve application availability (e.g., multiple data paths),
- enhance application performance (e.g., off-load storage functions, segregate networks, etc.),

- increase storage utilization and effectiveness (e.g., consolidate storage resources, provide tiered storage, etc.), and
- improve data protection and security.

In addition, SANs typically play an important role in an organization's Business Continuity Management (BCM)[1] activities.

A SAN presents storage devices to a host such that the storage appears to be locally attached. This simplified presentation of storage to a host is accomplished through the use of different types of virtualization.

SANs are commonly based on Fibre Channel (FC) technology[2] that utilizes the Fibre Channel Protocol (FCP) for open systems and proprietary variants for mainframes. In addition, the use of Fibre Channel over Ethernet (FCoE) makes it possible to move FC traffic across existing high-speed Ethernet infrastructure and converge storage and IP protocols onto a single cable. Other technologies like Internet Small Computing System Interface (iSCSI), commonly used in small and medium sized organization as a less expensive alternative to FC, and InfiniBand, commonly used in high performance computing environments, can also be used. In addition, it is possible to use gateways to move data between different SAN technologies.

2.2 Fibre Channel (FC)

According to the SNIA Dictionary, Fibre Channel is

> *A serial I/O interconnect capable of supporting multiple protocols, including access to open system storage (FCP), access to mainframe storage (FICON), and networking (TCP/IP).*

It supports point to point, arbitrated loop, and switched topologies with a variety of copper and optical links running at a variety of speeds.

The Fibre Channel Protocol (FCP) is described in ANSI INCITS 470–2011 (FC-FS-3) as a network architecture organized into five layers or levels. The following table provides a brief summary for each of the levels:

[1] "Business Continuity Management (BCM)" is used in ISO/IEC 27002:2013 to cover topics such as Disaster Recovery (DR) and the broader issue of Business Continuity (BC). In the past, DR and BC were addressed differently by the security community, but the current trend is to handle them as elements under BCM.

[2] SANs that are based on the Fibre Channel switched fabric (FC-SW) topology are sometimes referred to as FC fabrics.

FC-4	Protocol-mapping layer (application protocols, such as SCSI, IP or FICON, are encapsulated into a protocol data unit for delivery to FC-2)
FC-3	Common services layer
FC-2	Network layer (core of Fibre Channel, and defines the main protocols)
FC-1	Data link layer (implements line coding of signals)
FC-0	Physical layer (cabling, connectors etc.)

The FC-2 level defines the FC frame format, the transport services, and control functions required for information transfer. Fibre Channel Generic Services share a Common Transport (CT) at the FC-4 level defined in ANSI INCITS 463–2010 (FC-GS-6). The CT provides access to a Service (e.g., Directory Service) with a set of service parameters that facilitates the usage of Fibre Channel constructs.

A Fibre Channel port is a hardware pathway into and out of a node that communicates over an FC link (sometimes called a channel). FC defines many different types of ports, but the following are relevant to this whitepaper (see Figure 1):

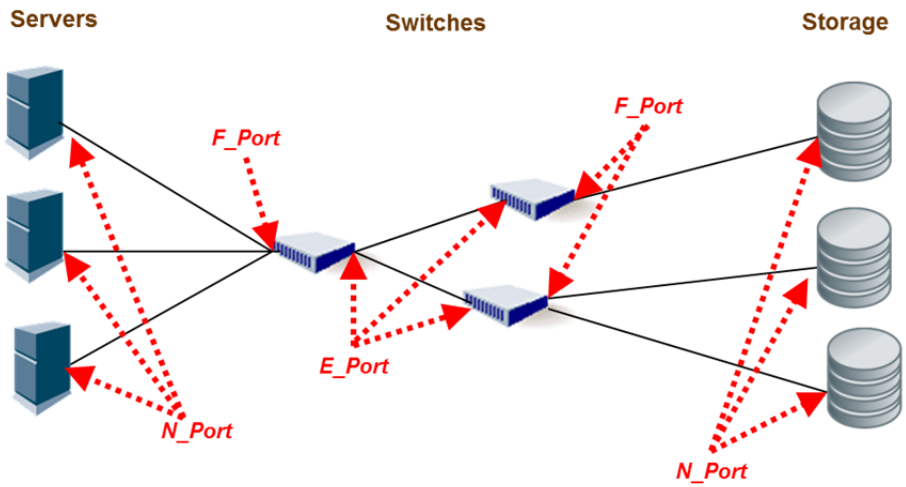


Figure 1 — FC Port Types

— **N_Port:** A network or node port used to connect a node to a FC switch. This could be an initiator HBA (Host Bus Adapter) in a host or a target port on a storage array.

— **F_Port:** A switch port used to connect the FC fabric to a node (N_Port).

- **E_Port:** An extender port used to connect (cascade) FC switches together; the connection between two E_Ports forms an Inter-Switch Link (ISL).

- **NP_Port:** A switch port that function as a proxy for multiple physical N_Ports. When the switch is operating in NPV mode (described below), the interfaces that connect the switch to the core network switch are configured as NP_Ports.

2.3 FC Virtualization

Within FC SANs, two complementary virtualization technologies are used and are described in this section. They are known as are NPIV (N_Port ID Virtualization) and NPV (N_Port Virtualization).

2.3.1 N_Port_ID Virtualization (NPIV)

Keeping in mind that an N_Port has a single N_Port_ID associated with it in a non-virtualized context, NPIV enables a single physical N_Port to have multiple World Wide Port Names (WWPNs), and therefore multiple N_Port_IDs, associated with it. After the normal FLOGI process, an NPIV-enabled physical N_Port can subsequently issue additional commands to obtain and register more WWPNs and receive more N_Port_IDs (one for each WWPN). The Fibre Channel switch also needs to support NPIV, as the F_Port on the other end of the link would "see" multiple WWPNs and multiple N_Port_IDs coming from the host and need to know how to handle this behavior.

Once all the applicable WWPNs have been registered, each of these WWPNs can be used for SAN zoning or LUN presentation. There is no distinction between the physical WWPN and the virtual WWPNs; they all behave in exactly the same manner and they can be used in exactly the same ways.

With NPIV in place it is possible to create a zone in a FC SAN that only one virtual machine can access, even though the underlying server may have numerous other virtual machines. In addition, virtual machines that migrate from one host to another require no special changes to make sure the target host has the correct access to the LUN because the virtual WWN follows the virtual machine. This means that the virtual machine has that access and as a result the host inherits the ability to access the LUN.

It is important to note that each N_Port_ID created by NPIV consumes resources in the host, network fabric and storage, so care should be exercised when a potentially large number of virtual hosts are used to avoid scaling problems.

Depending on the functionality offered by the manufacturer, NPIV can be used in conjunction with other Fibre Channel security mechanisms described in 3.3.

2.3.2 N port virtualization (NPV)

While NPIV is primarily a host-based solution, NPV is primarily a switch-based technology. It is designed to reduce switch management and overhead in larger SAN deployments.

In a non-virtualized context, a SAN may need a large number of edge switches (e.g., large-scale blade server deployments with built in switches) that exceed the limit of 239 domain IDs[3], which translates into the SAN having a limit of 239 switches.[4] NPV alleviates the domain ID limit by sharing the domain ID of the core switch among multiple edge switches[5] that appear as Fibre Channel hosts to the core switch and as regular Fibre Channel switches to their connected devices. The core switch provides F_Port functionality (such as login and port security) and all the Fibre Channel switching capabilities.

Key to NPV's functionality is the introduction of a new type of Fibre Channel port, the NP_Port, which connects to an F_Port and acts as a proxy for other N_Ports on the NPV-enabled switch (typically an edge switch); the NP_Port "looks" like an NPIV-enabled host to the F_Port on the other end. An NPV-enabled switch will register additional WWPNs (and receive additional N_Port_IDs) via NPIV[6] on behalf of the N_Ports connected to it. The physical N_Ports don't have any knowledge this is occurring and don't need any support for it; it's all handled by the NPV-enabled switch.

NPV also enables network administrators to connect FCoE hosts to non-FCoE-enabled SANs and simplifies third-party interoperability concerns because the NPV enabled Fibre Channel module does not participate in domain operations or perform local switching. This enables multivendor topologies to be implemented without the restrictions the interoperability mode may require.

Some vendor switch implementations build on Fibre Channel NPV, by supporting NPV for Fibre Channel over Ethernet (FCoE-NPV) as well. FCoE-NPV brings similar benefits as the Fibre Channel NPV mode to a pure FCoE implementation. The switch still uses FIP snooping[7] to identify FCoE traffic and to maintain separation and provide security. FCoE NPV also creates a new port type for the VNP (Virtual NPV Port).

---

[3] A number identifying a specific switch in the fabric.

[4] Not all vendors support the maximum of 239 domain IDs.

[5] The switches that connect directly to end-user devices are called "edge" or "access" switches. Generally, the backbone of the network is where switching ends and routing begins, with core switches serving as both switching and routing engines (and possibly firewall capabilities).

[6] A key component to enable the proper operation of NPV is the need for N-Port ID Virtualization (NPIV) on the core/upstream Fibre Channel switch.

[7] FIP snooping is used in multi-hop FCoE environments and it is a frame inspection method that can be used by FIP snooping capable Data Center Bridge (DCB) devices to monitor FIP frames and apply policies based on the information in those frames.

Depending on the functionality offered by the manufacturer, NPV can be used in conjunction with other Fibre Channel security mechanisms described in 3.3.

3 FC and SAN Security Background

This section provides a description of the more common forms of threats and security measures for SANs and Fibre Channel specifically.

3.1 Threats

ISO/IEC 27040:2015 addresses storage security risks and threats at a high level, but this white paper contains more specific information in the context of Fibre Channel. The following list is a summary of the major threats[8] that may confront Fibre Channel implementations and deployments.

- *Storage Theft*: Theft of storage media or storage devices can be used to access data as well as to deny legitimate use of the data.
- *Sniffing Storage Traffic*: Storage traffic on dedicated storage networks or shared networks can be sniffed via passive network taps or traffic monitoring revealing data, metadata, and storage protocol signaling. If the sniffed traffic includes authentication details, it may be possible for the attacker to replay[9] (retransmit) this information in an attempt to escalate the attack.
- *Network Disruption*: Regardless of the underlying network technology, any software or congestion disruption to the network between the user and the storage system can degrade or disable storage.
- *WWN Spoofing*: An attacker gains access to a storage system in order to access/modify/deny data or metadata.
- *Storage Masquerading*: An attacker inserts a rogue storage device in order to access/modify/deny data or metadata supplied by a host.
- *Corruption of Data*: Accidental or intentional corruption of data can occur when the wrong hosts gain access to storage.

[8] Risk cannot be discussed as it is specific to the circumstances in your particular environment. Risk refers to the probability of something unfortunate happening and the resulting impact to your organization. Threats can be more generally cataloged but you must assign the likelihood of a threat being instantiated and the resulting impact based on your environment.

[9] A *replay attack* is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated.

- *Rogue Switch*: An attacker inserts a rogue switch in order to perform reconnaissance on the fabric (e.g., configurations, policies, security parameters, etc.) or facilitate other attacks.
- *Denial of Service (DoS)*: An attacker can disrupt, block or slow down access to data in a variety of ways by flooding storage networks with error messages or other approaches in an attempt to overload specific systems within the network.

3.2 SAN Security

Security controls relevant to a SAN are grouped into the following categories:

- **Access Control:** Access control on a SAN is implemented through application of zoning, Logical Unit (LUN) masking, and port binding mechanisms. Access control in a SAN is based on machine identities rather than on the more familiar user and group identity types.
  - **Port Binding:** World Wide Names (WWN) are used for identification in a SAN. Port binding is a SAN security mechanism that specifies which WWNs are permitted to connect through that physical port. This association can mitigate snooping or spoofing attempts by an adversary and should be used whenever possible.
  - **Zoning:** A SAN fabric can be segmented into separate zones to restrict the visibility of portions of a SAN to specific hosts and storage devices. Soft zoning is based on limiting SAN fabric nameserver responses to queries based on the assumption that hosts will not contact storage devices that are not discovered via the nameserver. Some modern switches allow “hard” (switch ASIC) zoning based on WWN that uses physical port numbers on SAN switches to restrict traffic forwarding and is a more secure zoning method because it does not rely on correct host behavior and in particular is not vulnerable to spoofing of host identity.
  - **LUN masking:** A storage device can be divided into logical units that are identified by logical unit numbers (LUNs[10]). LUN masking refers to making a LUN visible to some hosts while remaining invisible to others.
- **Authentication:** For SANs it is important for a switch to verify the identity of other switches in the SAN with which it communicates to prevent rogue switches from joining a SAN. Likewise, the nodes in a SAN (e.g., storage devices and hosts) need to employ authentication to guard against unauthorized access to data.
- **Encryption:** There are two major use cases for encryption in assuring data confidentiality on a SAN: 1) data in motion and 2) data at rest. Sensitive and high-value data[11] needs to be

[10] A common source of confusion in the industry is the practice of referring to a Logical Unit (a contiguous array of logical block addresses) as a "LUN". Usually, when people refer to a LUN, they mean the underlying Logical Unit, i.e. the storage itself, not the arbitrary number assigned to it for presentation to a host.

cryptographically protected in SANs when it is in motion as well as when it is at rest on a storage device.

3.3 Overview of Fibre Channel Security

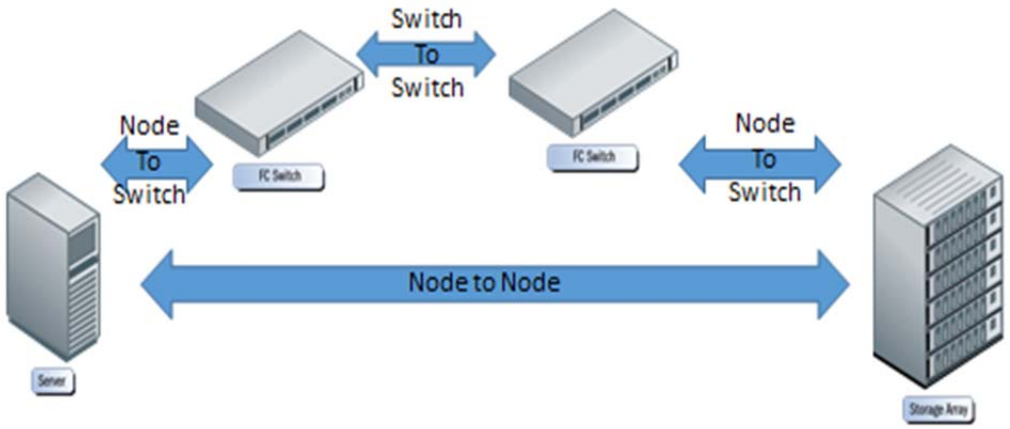
Fibre Channel fabrics may be deployed across multiple, distantly separated sites which make it critical that security services be available to assure consistent configurations and proper access controls.

ANSI INCITS 496-2012, *Information Technology - Fibre Channel - Security Protocols - 2* (FC-SP-2) defines protocols to authenticate Fibre Channel entities, set up session encryption keys, negotiate parameters to ensure frame-by-frame integrity and confidentiality, and define and distribute policies across a Fibre Channel fabric. It is also worth noting that FC-SP-2 includes compliance elements, which is somewhat unique for FC standards.

The security architecture defined by FC-SP-2 encompasses the following components:

a) *Authentication infrastructure* –Defines an architecture for several authentication infrastructures: secret-based, certificate-based, password-based, and pre-shared key based authentication.

b) *Authentication* – Defines authentication protocols allowing entities to assure the identity of communicating entities. Two entities may negotiate whether authentication is required and which authentication protocol may be used. Authentication is defined for switch-to-switch, node-to-switch, and node-to-node (see Figure 2), using one of the following protocols:



[11] "Sensitive and high-value" assumes that organizations classify their data or know what's actually stored where. Otherwise, they have to protect to an appropriate level for the most sensitive data that might be stored there.

Figure 2 — FC Authentication

- Diffie-Hellman Challenge Handshake Authentication Protocol (DH-CHAP), which is mandatory (see 3.3.1);
- Fibre Channel Certificate Authentication Protocol (FCAP);
- Fibre Channel Password Authentication Protocol (FCPAP);
- Fibre Channel Extensible Authentication Protocol (FCEAP);
- The Security Association Management Protocol (IKEv2-AUTH).

Security associations – A subset (i.e., the Security Association Management protocol) of the Internet Key Exchange Protocol Version 2 (IKEv2)[12] protocol suitable for Fibre Channel is defined (see 3.3.4) in order to establish Security Associations between entities.

Cryptographic integrity and confidentiality – Frame by frame cryptographic integrity and confidentiality, replay protection, and traffic origin authentication (verification that the traffic came from a given endpoint) is achieved by using the ESP_Header (see 3.3.2). CT_Authentication (see 3.3.3) may be leveraged to provide cryptographic integrity and confidentiality, replay protection, and traffic origin authentication to Common Transport Information Units. ESP_Header processing and CT_Authentication processing are independent.

Authorization (access control) – Fabric policies provide basic authorization controls and are of two types:

- policies that contain fabric-wide data and are distributed to every switch of the fabric;
- policies that contain per switch data and are sent to an individual switch.

Fabric policies may be used to control which switches are allowed to comprise a fabric and which nodes are allowed to connect to a fabric. Policies may be further used to specify topology restrictions within the fabric environment (e.g., which switches may connect to which other switches or which nodes may connect to which switches).

Fabric policies also provide the mechanism for controlling management access to the fabric, the ability to control authentication choices and to specify optional security attributes for fabric entities (e.g., nodes and switches). Management access to the fabric may be controlled for Common Transport or IP access.

[12] IKEv2 is described in IETF RFC 7296, *Internet Key Exchange Protocol Version 2 (IKEv2).*

Figure 2, which is from clause 4.5 of the FC-SP-2 standard, shows the relationship between the authentication protocols and security associations. The defined authentication protocols are able to perform mutual authentication with optional shared key establishment. The shared key computed at the end of an authentication transaction may be used to establish security associations.

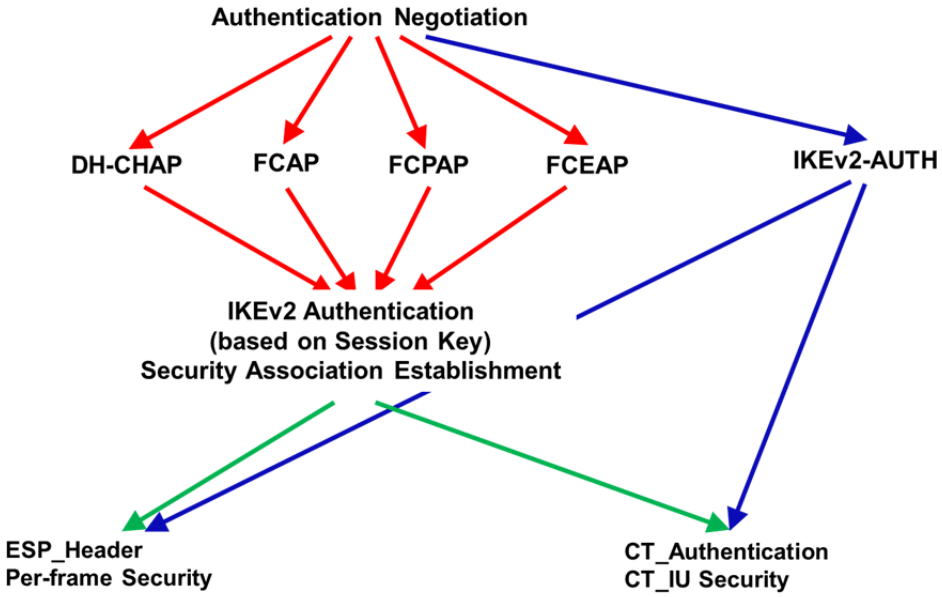


Figure 2 — Relationship between FC-SP-2 Authentication Protocols and Security Associations

3.3.1 DH-CHAP authentication

DH-CHAP is a secret-based authentication and key management protocol that uses the CHAP algorithm with an optional Diffie-Hellmann algorithm. DH-CHAP provides unidirectional or bidirectional authentication between an *Authentication Initiator* and an *Authentication Responder*. When the Diffie-Hellmann part of the protocol is not used, DH-CHAP reduces its operations to those of the CHAP protocol, and it is referred to as DH-CHAP with a NULL DH algorithm. All FC-SP-compliant implementations are required to support DH-CHAP with a NULL DH algorithm. To claim FC-SP-2 compliance, an implementation is required to support the AUTH-A Compliance Element (described in Annex A of FC-SP-2), which includes the 2048-bit DH algorithm.

In addition to identifying the authentication algorithm, FC-SP-2 specifies that authentication is defined for Switch-to-Switch, Device-to-Switch, and Device-to-Device entities (see Figure 2), and that the protocols are able to support mutual authentication. Thus, conformant or compliant products are required to also implement each of the following when applicable:

- **Switch-to-Switch**—Products that include authentication between these types of entities must be able to authenticate a switch as well as be authenticated by a switch.

- **Device-to-Switch**—Products that include authentication between these types of entities must be able to authenticate a switch as well as be authenticated by a switch, from a device perspective, or be able to authenticate a device as well as be authenticated by a device, from a switch perspective.

- **Device-to-Device**—Products that include authentication between these types of entities must be able to authenticate a device as well as be authenticated by a device. In addition, each device must complete the appropriate Device-to-Switch authentication prior to performing this authentication.

Products conformant to FC-SP-2 must also implement re-authentication such that the entity can be re-authenticated by the other entity at any time.

3.3.2 ESP_Header

ESP_Header is a security protocol for FC-2 Fibre Channel frames that provides origin authentication, integrity assurance, anti-replay protection, and confidentiality.

ANSI INCITS 470–2011, *Information Technology — Fibre Channel — Framing and Signaling-3* (FC-FS-3) defines optional headers that can be used within Fibre Channel frames. Of these optional headers, the ESP_Header and ESP_Trailer play an important security role because they are the mechanism used to support encryption of frame payloads.

The Encapsulating Security Payload (ESP), defined in RFC 4303, is a generic mechanism to provide confidentiality, data origin authentication, and anti-replay protection for IP packets. FC-SP-2 defines how to use ESP in Fibre Channel.

FC-FS-3 states that "End-to-end ESP_Header processing shall be applied to FC frames in transport mode (see RFC 4303[13], and Link-by-link ESP_Header processing shall be applied to FC frames in tunnel mode[14] (see RFC 4303). The Authentication option shall be used, Confidentiality may be negotiated by the two communicating FC_Ports (see FC-SP-2)."

NOTE - An intended application of Link-by-link ESP_Header processing is to secure a link in a Fabric or between Fabrics without requiring use of ESP by every Nx_Port[15].

[13] IETF RFC 4303, IP Encapsulating Security Payload (ESP) describes an updated version of ESP, which is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic flow confidentiality.

[14] In "tunnel mode" the internal routing information is protected by encrypting the header of the original packet/frame whereas "transport mode" only protects the payload with encryption.

[15] The term Nx_Port is used to refer to either an N_Port (node port) or an NL_Port (node loop port).

3.3.3 CT_Authentication

Fibre Channel defines two security protocols that provide security services for different portions of Fibre Channel traffic: the ESP_Header (see 3.3.2) and CT_Authentication defined in ANSI INCITS 463–2010, *Information Technology — Fibre Channel — Generic Services — 6 (FC-GS-6)*. The CT_Authentication protocol provides origin authentication, integrity assurance, anti-replay protection, and optionally, confidentiality protection for Common Transport Information Units, which are used to convey control information.

Unlike ESP_Header, which operates at the FC frame level, CT_Authentication operates at the Common Transport (CT) level and provides access to a service (e.g., directory service) with a set of service parameters that facilitates the usage of Fibre Channel constructs.

3.3.4 Fibre Channel Security Association

As described earlier, two mechanisms are available to protect specific classes of traffic: the ESP_Header is used to protect Fibre Channel frames, and CT_Authentication is used to protect Common Transport Information Units. Security associations for the ESP_Header and CT_Authentication protocols between two Fibre Channel entities (hosts, storage, or switches) are negotiated by the Fibre Channel Security Association Management Protocol (defined in FC-SP-2). The protocol is a modified subset of the Key Exchange Protocol Version 2 (IKEv2) that performs the same core operations, but uses the Fibre Channel AUTH protocol to transport IKEv2 messages. IETF RFC 4595, *Use of IKEv2 in the Fibre Channel Security Association Management Protocol* provides additional information on Fibre Channel use of IKEv2.

NOTE - Only one protocol (either ESP_Header or CT_Authentication) is applicable to any Fibre Channel Security Association.

3.3.5 FC-SP Zoning

In order to preserve backward compatibility with existing zoning definitions and implementations, FC-SP-2 describes a variant of the Enhanced Zoning model defined in ANSI INCITS 461–2010, *Information Technology — Fibre Channel - Switch Fabric — 5* (FC-SW-5) and ANSI INCITS 463–2010, *Information Technology — Fibre Channel — Generic Services — 6* (FC-GS-6), denoted as FC-SP Zoning, that follows the general concepts of the Enhanced Zoning model, but keeps zoning management and enforcement completely independent from other policy management and enforcement.

Fabric policies and zoning policies allow an asymmetric distribution of policy information in the Fabric with the definition of three types of switches:

a) Host Switches: Switches that retain all policy objects and all node to node (zoning) information;

b) Autonomous Switches: Switches that retain their own per switch policy objects, all fabric-wide policy objects, and all node to node (zoning) information;

c) Client Switches: Switches that retain their per switch policy objects, all fabric-wide policy objects and the subset of the node to node (zoning) information relevant for their operations, which is pulled from a host switch when needed.

4 Summary of FC Guidance in ISO/IEC 27040

When using ISO/IEC 27040 to identify relevant Fibre Channel controls, it is important to remember that these materials are located in at least two places: 1) storage networking, and 2) block-based storage.

4.1 FC SAN Security

The ISO/IEC 27040 guidance associated with using Fibre Channel as part of a SAN focuses on controlling FCP nodes (e.g., hosts, storage), implementing switch-based controls, and controlling the interconnection of FC SANS. The following is a summary of the guidance:

— Control FCP node access by restricting host access on the switches using techniques such as Access Control Lists (ACLs), binding lists, and FC-SP-2 fabric policies. For virtualized hosts, use NPIV (N_Port_ID Virtualization) enabled HBAs to assign individual N_Port_IDs to virtual hosts.

— Implement switch-based controls by restricting switch interconnections using techniques such as ACLs, binding lists, and FC-SP-2 fabric policies. In addition, zoning should be used in FC SAN fabrics with a preference for hard zoning; carefully use default zones and zone sets (assume a least privilege posture). If basic zoning is a not a strong enough security measure for the target environment, use stronger techniques like FC-SP Zoning where supported by the vendor. Last, but not least, disable unused ports on switches.

— Interconnect different FC SANs securely by configuring switches, extenders, routers, and gateways necessary to meet requirements. Unfortunately, ISO/IEC 27040 does not provide additional details on what is meant by "to meet requirements."

Overall, ISO/IEC 27040 does not provide extensive guidance on securing FC SANs.

4.2 FC Device Security

The ISO/IEC 27040 guidance associated with Fibre Channel devices is above and beyond what may be implemented within FC SANs. The following is a summary of the guidance:

— Use LUN masking, WWN filtering, and other access control mechanisms to restrict access to storage.

— Utilize FCP security measures such as mutual authentication using FC-SP-2 AUTH-A with all hosts and switches, leveraging centralized authentication services (RADIUS[16]) when possible. For sensitive information that leaves protected areas (e.g., confines of a physically controlled data center), use link encryption (e.g., ESP_Header with GCM encryption[17]).

— For sensitive/regulated or high-value data, implement data at rest encryption and the appropriate key management measures on the storage device or media. For additional information on this topic, consult the *SNIA Storage Security: Encryption and Key Management* whitepaper.

— Similar to data at rest encryption, use media-aligned or logical sanitization measures to protect sensitive/regulated or high-value data. The latter can be particularly helpful for virtualized storage, especially when the actual storage devices and media cannot be determined. For additional information on this topic, consult the *SNIA Storage Security: Sanitization* whitepaper.

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

[17] Fibre Channel frame integrity or confidentiality can be provided with ESP_Header optional headers, which are defined in ANSI INCITS 470–2011, *Fibre Channel – Framing and Signaling-3 (FC-FS-3).*

5 SNIA Observations and Guidance for FC

Fibre Channel standards specify a wide range of features and functionality that are not universally available. This section highlights some of the known FC security challenges and issues as well as offering guidance above and beyond what is offered in ISO/IEC 27040.

5.1 FCP Link Encryption

Link encryption is the data security process of encrypting all the data along a specific communication path. Link encryption typically occurs at the data link and physical layers between two communication points (e.g., routers). It is also important to note that link encryption is not the same as end-to-end encryption, which protects communications between the originating and receiving devices.

Within the context of Fibre Channel, link encryption can show up as part of the FCP (e.g., ESP_Header) or as an external mechanism (e.g., IPsec protecting FCIP). Link encryption is typically only used to protect FCP connections between sites that employ Fibre Channel over IP (FCIP) as the transport. Few storage vendors have implemented ESP_Header encryption, so it is difficult, if not impossible, to implement link encryption within Fibre Channel SANs. This situation may change if customers begin demanding this functionality.

Assuming link-level encryption is available, it is important to remember that its use can have a major impact on data reduction technologies (i.e., compression and de-duplication) that might be employed between data centers.

As of this writing, FCIP with IPsec is the only form of link encryption available for Fibre Channel.

5.2 Data At-rest Encryption

Data at-rest encryption is not an element of Fibre Channel security, but it is briefly mentioned here because it can have an impact on data reduction technologies in a similar way as link encryption.

It is important to always remember that encryption within storage ecosystems provides media-level protection and can be a safety net, but for real confidentiality protections the data needs to be encrypted near its source or use (i.e., by a host, application, etc.). Additional details on data at-rest encryption can be found in the SNIA *Storage Security: Encryption and Key Management* whitepaper.

5.3 Maintaining FC Security with FCoE

A Fibre Channel over Ethernet (FCoE) device that has a converged network adapter (CNA) uses the FCoE Initialization Protocol (FIP) process to log in to the FC network as an FCoE Node (ENode). The login process establishes a dedicated virtual link between a virtual N_Port (VN_Port) on the ENode and a virtual F_Port (VF_Port) on the FC switch. This dedicated virtual link emulates a point-to-point connection. The emulated connection is called a virtual link and virtual links pass transparently through the transit switch (i.e., The transit switch is invisible to the ENode VN_Port and the FC switch VF_Port and virtual links appear to be direct point-to-point links.).

It is important to note that FCoE exposes FC frames on Ethernet networks, which may not have the same level of security as native FC networks. To mitigate potential risks, a security mechanism known as FIP snooping, designed to prevent unauthorized access and data transmission to a Fibre Channel (FC) network, should be implemented to filter traffic via one of the following mechanisms:

- VN_Port to VF_Port (VN2VF_Port) FIP snooping[18] on an FCoE VLAN, the system (e.g., transit switch) snoops VN_Port to VF_Port packets and enforces security only on VN2VF_Port virtual links.
- VN_Port to VN_Port (VN2VN_Port) FIP snooping[19] on an FCoE VLAN, the system (e.g., transit switch) snoops VN_Port to VN_Port packets and enforces security only on VN2VN_Port virtual links.

Note: An FCoE VLAN can support either VN2VF_Port FIP snooping or VN2VN_Port FIP snooping, but not both.

5.4 Additional Considerations

The materials in this section highlight issues and problems that could impact successful use of FC security mechanisms.

5.4.1 Number of Shared Secrets for FC Authentication

On enterprise-class storage systems and director-class FC switches it may be possible to have a very large number (greater than 50,000) of entities authenticating using FC-SP-2 AUTH-A. Keeping in mind that a pair of shared secrets is necessary for mutual authentication between any two of these entities (hosts to switches, storage to switches, and hosts to storage), this large number of shared secrets can result in operational challenges to correctly generate,

[18] Specified in FC-BB-5
[19] Specified in FC-BB-6

distribute, and implement the shared secrets necessary to secure such an environment. To minimize overhead and avoid down time due to misconfigurations, it may be preferable to have the various devices use RADIUS to reduce the number shared secrets that have to be managed.

5.4.2 Composition of FC Shared Secrets

The FC-SP-2 standard does not address user interface issues, but it turns out this situation results in some ambiguity with regards to shared secrets. The particular problem stems from the fact that both end-points have to use the same shared secret. However, the manner in which a shared secret is entered into each can result in an incompatibility. For example, one device may require the user to enter a 128-bit hexadecimal entry while another may require an alpha-numeric value to be entered. Even in the latter case, there can be differences in the acceptable characters. These differences can severely restrict or prevent interoperability in heterogeneous environments. These limitations can also have an impact on the entropy of the shared secrets.

6 Summary

Fibre Channel security mechanisms are specified in a range of standards, which can make them difficult for vendors to implement and customers to use. In addition, some of the specified mechanisms are optional for vendors to implement, so the available of security capabilities is not assured. Lastly, those FC security features that are available may have interoperability issues in heterogeneous FC SANs.

7 Acknowledgments

7.1 About the Author

Eric Hibbard is the HDS CTO Security & Privacy and he has 30 years of experience in ICT infrastructure with a specialty in data/storage security. He is a Co-Chair of the SNIA Security TWG and holds leadership positions in ABA, IEEE, CSA, and INCITS. He is and has served as the editor of multiple ISO/IEC and IEEE standards, ISO/IEC 27040 (Storage security) and the ISO/IEC 20648 (TLS Specification for Storage Systems). Hibbard currently holds the $(ISC)^2$ CISSP and CCSP certifications as well as the ISSAP, ISSMP, and ISSEP concentrations credentials along with the ISACA CISA certification.

7.2 Reviewers and Contributors

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

Richard Austin, CISSP	HPE
Walt Hubis	Hubis Technical Associates
Dr. Alan Yoder	
Gary Sutphin	
Tim Hudson	Cryptsoft
Thomas Rivera	Hitachi Data Systems

8 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 this 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 update).

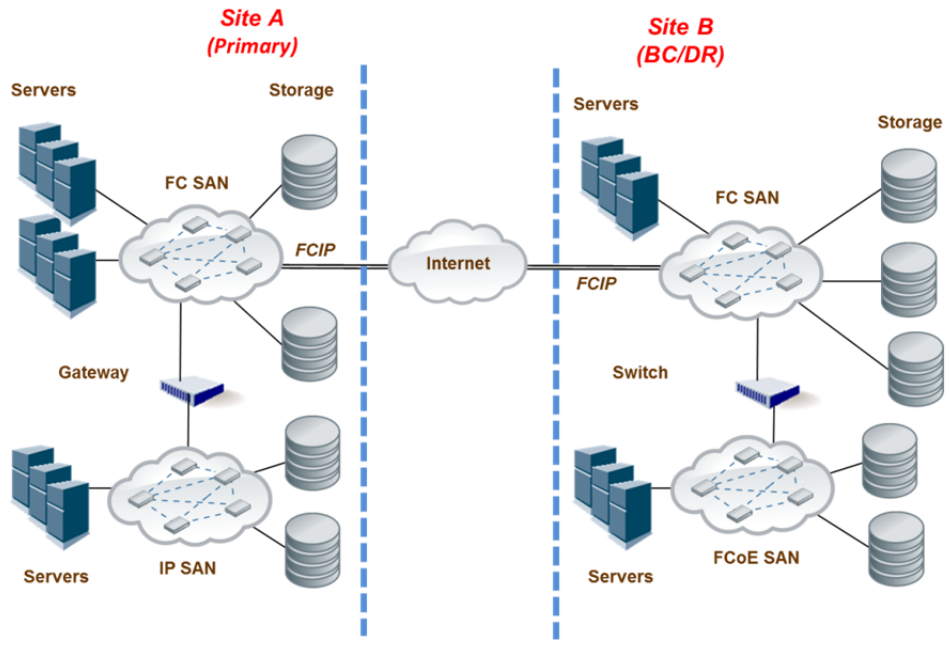
ISO/IEC 27040 approaches storage security guidance from two angles: 1) supporting controls and 2) design and implementation of storage security. Both are addressed in sufficient detail that storage professional with limited security knowledge and security/audit professionals with little storage background 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.[20] 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."[21] "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;

[20] *About ISO*, INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, http://www.iso.org/iso/home/about.htm (last visited September 15, 2014).
[21] *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.[22]

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)[23]:

- 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.

[22] 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).
[23] *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