Storage Security: Fibre Channel Security

Version 2.0

February 14, 2024

Eric A. Hibbard, CISSP, FIP, CISA

Table of Contents

List of Tables

List of Figures

Executive Summary

Fibre Channel (FC) is the premier transport for storage within and across datacenters, known for its reliability, resilience, and high-speed connectivity. Yet the capabilities available to provide security protections within a Fibre Channel network are neither well known nor well understood. In reality, in a Fibre Channel network both servers and storage systems provide many security capabilities themselves, while there are also other Fibre Channel-specific capabilities of the infrastructure that are available to provide additional security within the network. This SNIA/Fibre Channel Industry Association (FCIA) storage security paper provides information on Fibre Channel as it relates to storage systems and the Fibre Channel ecosystem.

1 Introduction

Storage security capabilities and practices have seen significant advances since their initial introductions. Storage systems (e.g., hard disk drives, solid state drives, storage arrays, and file servers) and storage ecosystems (e.g., storage devices and systems, storage networks, and storage management software) are able to protect data in a variety of ways.

This technical paper is intended to enhance understanding of Fibre Channel security. The whitepaper provides background information on Fibre Channel, summarizes the FC security options, 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 interconnects hosts and storage devices primarily for the purposes of data storage,data retrieval, and archival. 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, often in configurations intended to support high availability and disaster recovery configurations.

SANs are often used to:

- improve application availability (e.g., multiple paths on the SAN to the same storage),
- increase scalability (e.g., number of devices accessible to a host, number of hosts accessible to a storage device),
- enhance application performance (e.g., off-load storage functions, segregate networks, clustering, 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].

SANs are commonly based on Fibre Channel network technology[2] that interconnects hosts and devices supporting storage command sets such as SCSI, NVM Express®, and Single Byte (SB) command sets.

2.2 Fibre Channel (FC)

According to the SNIA Dictionary, Fibre Channel is:

> *A serial I/O interconnect capable of supporting multiple protocols. Protocols supported include FCP, NVMe, SB (FICON), and IP.*

Fibre Channel supports point-to-point and switched topologies with a variety of copper and optical links running at a variety of speeds and distances.

The Fibre Channel architecture is described in INCITS 562–2024 (FC-FS-6) [3] as a network architecture organized into five layers or levels. Table 1 provides a summary for each of the levels:

Table 1. Fibre Channel Layers

FC-4	Protocol mapping layer (upper level protocols, such as SCSI, NVMe, IP, or SB, are encapsulated into a protocol information unit for delivery to the FC-2 layer)
FC-3	Common services layer
FC-2	Network layer (core of Fibre Channel, and defines the framing and signaling 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 INCITS 548–2020 (FC-GS-8) [2]. 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.

Fibre Channel Link Services provide two sets of architected functions:

---

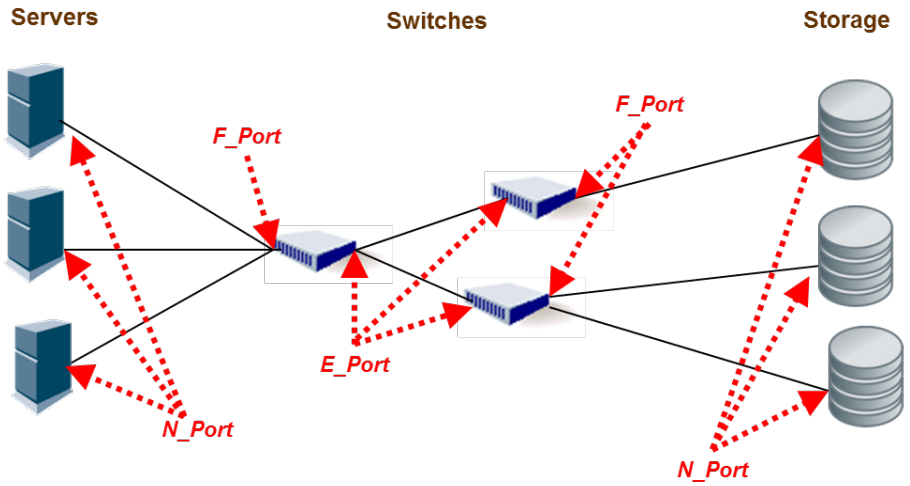
[1] "Business Continuity Management (BCM)" is used in ISO/IEC 27002:2022 to cover topics such as Disaster Recovery (DR) and the broader issue of Business Continuity (BC). In the past, DR and BC were addressed differently by the security community, but the current trend is to handle them as elements under BCM.

[2] SANs that are based on the Fibre Channel switched fabric [3] topology are referred to as FC fabrics.

- Basic Link Services (BLSs) (see FC-FS-6) define a set of basic control functions that operate within the context of an existing Exchange (e.g., Abort Exchange); and
- Extended Link Services (ELSs) (see FC-LS-5) define a set of functions that a Fibre Channel entity may use to request another FC entity to perform a service. ELSs are used for authentication and security association management.

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

Figure 1. FC Port Types



- **N_Port:** A node port used to connect a node to an FC switch, or another node in point-to-point topology. This is typically an initiator HBA (Host Bus Adapter) in a host or a target port on a storage array. An N_Port is associated with a World Wide Node Name, is identified by a World Wide Port Name, and is assigned an FC address identifier[3].
- **F_Port:** A switch port used to connect the FC fabric to a node (N_Port).
- **E_Port:** An extender port used to connect FC switches together; the connection between two E_Ports form an Inter-Switch Link (ISL).

2.3 FC Address Discovery and Access Control

In an FC fabric, an N_Port determines connectivity to other N_Ports by registering with and querying the FC fabric "Directory Service". Queries of the Directory Service return N_Port identifiers (e.g., WWN's,

[3] A physical FC Port minimally supports one N_Port. Additional N_Port's may share the physical FC Port via the use of the FC N_Port_ID Virtualization (NPIV) feature. Using NPIV, each of the N_Ports on the physical FC Port will have an independent FC address identifier.

their FC address identifiers, and FC-4 protocol attributes) for the other N_Ports attached to the FC fabric. The N_Port can then initiate communication to the other N_Ports if desired.

The FC fabric may be divided into "zones". A zone is a grouping of N_Ports that are allowed to communicate with each other. The FC Directory Service will limit an N_Port's query results to only the N_Port's that are in the same zone(s) as the querying N_Port.

One level of security is to construct zones to prohibit communication between particular nodes.

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

The following list is a summary of the major threats[4] 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[5] (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 unauthorized user 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.

[4] 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.

[5] 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, access control lists, 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.
  - Storage Device Access Control Lists - A storage device controls and varies the presentation and access to storage objects on the device based on the host communicating with the device. This includes items such as SCSI Logical Units (LUNs) with LUN masking, as well as NVM Express Subsystems and Namespaces. For example, a storage device may allow Host A to view/access SCSI LUNs A and B, but allows Host B to only view/access SCSI LUNs B and C.
- **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:** Sensitive and high-value data needs to be cryptographically protected when in motion in an FC fabric.

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 confidentiality of the data and proper access controls.

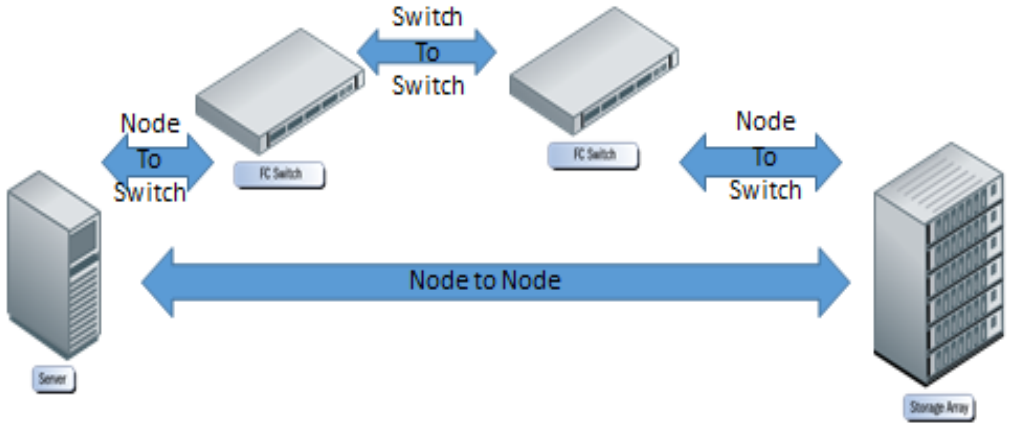
INCITS 496-2012 (FC-SP-2) [5] defines protocols to authenticate Fibre Channel entities, set up session encryption keys, negotiate parameters to ensure frame-by-frame integrity and confidentiality, and define

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:

- *Authentication infrastructure* – Defines an architecture for authentication infrastructures: secret-based and certificate-based.
- *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:

Figure 2. FC Authentication



  - Diffie-Hellman Challenge Handshake Authentication Protocol (DH-CHAP) (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) [9] 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:

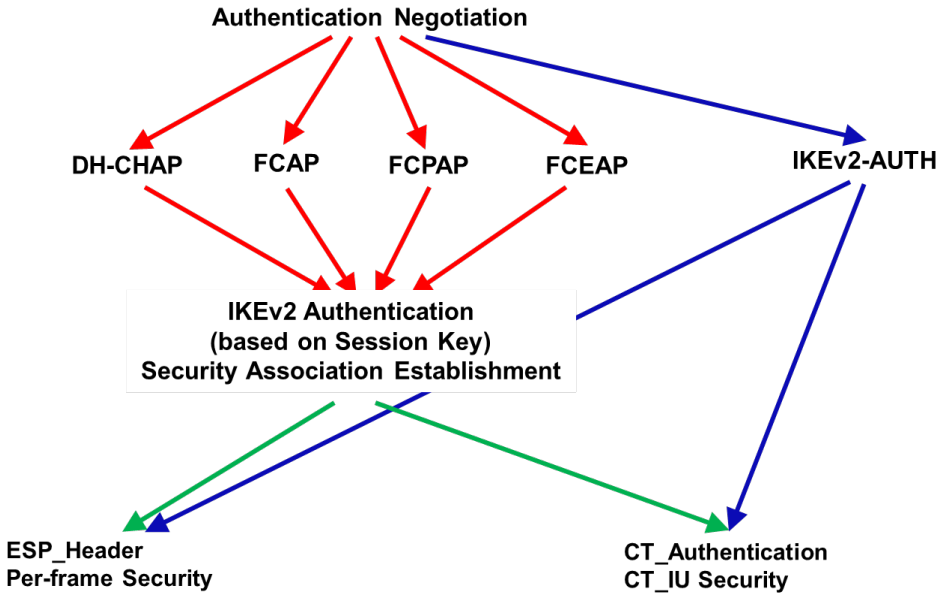
- policies that contain fabric-wide data and are distributed to every switch of the fabric;
- policies that contain per switch data and are sent to an individual switch.

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.

Figure 3, 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 3. 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.

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.

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.

INCITS 562–2024 (FC-FS-6) [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 [7], 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-6 states that "End-to-end ESP_Header processing shall be applied to FC frames in transport mode (see RFC 4303[6]), and Link-by-link ESP_Header processing shall be applied to FC frames in tunnel mode[7] (see RFC 4303). The Authentication option shall be used, and confidentiality (i.e., use of encryption) 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 N_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 INCITS 548–2020, (FC-GS-8) [2]. The CT_Authentication protocol provides origin authentication, integrity assurance, anti-replay

[6] IETF RFC 4303 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.

[7] 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.

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 functionality.

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) [9] that performs the same core operations, but uses the Fibre Channel AUTH protocol to transport IKEv2 messages. IETF RFC 4595 [8] provides additional information on Fibre Channel use of IKEv2.

NOTE - Only one protocol (i.e., 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 INCITS 547–2020 (FC-SW-7) [3] and INCITS 548–2020 (FC-GS-8) [2], 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:

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

When considering relevant Fibre Channel controls, it is important to remember that they can be applied in at least two places: 1) FC SAN security, and 2) FC device security.

4.1 FC SAN Security

When using Fibre Channel as part of a SAN, focus on controlling FC nodes (e.g., hosts, storage), through implementing switch-based controls, and controlling the interconnection of FC SANS. The following is a summary of the guidance:

- Control FC node access by restricting host access on the switches using techniques such as Zoning, Access Control Lists (ACLs), and FC-SP-2 fabric policies.
- 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 (e.g., preserving security domains).

4.2 FC Device Security

For Fibre Channel devices (above and beyond what may be implemented within FC SANs), the following guidance should be considered:

- Use Storage Device Access Control Lists (such as LUN masking), WWN filtering, and other access control mechanisms to restrict access to storage.
- Utilize FC security measures such as mutual authentication using FC-SP-2 AUTH-A with all hosts and switches, leveraging centralized authentication services (e.g., RADIUS [6]) when possible. For sensitive information transmitted on the FC fabric, especially if the data leaves protected areas (e.g., confines of a physically controlled data center), use link encryption (e.g., ESP_Header with GCM encryption[8]).

5 SNIA/FCIA Observations and Guidance for FC

Fibre Channel standards specify a wide range of features and functionality which may be used for security. This section highlights link encryption and data-at-rest encryption.

5.1 FC 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 FC framing protocols (e.g., ESP_Header) or as an external mechanism (e.g., IPsec protecting FCIP). Link encryption is typically only used to protect FC connections between sites that employ Fibre Channel over IP (FCIP) as the transport.

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.

[8] Fibre Channel frame integrity or confidentiality can be provided with ESP_Header optional headers, which are defined in INCITS 562–2024 (FC-FS-6) [4].

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 complements link and endpoint encryption security, but also 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.) through the fabric to its destination (target). Additional details on data at-rest encryption can be found in the SNIA *Storage Security: Encryption and Key Management* whitepaper.

6 Summary

System storage security is a critical, yet complex, topic with various solution options that may be implemented, each addressing one or more identified security threats. Fibre Channel offers methods for servers, storage devices, and SANs to authenticate identities and ensure rights to access as well as for the use of encryption to provide for the integrity and confidentiality of data transferred between entities. Security requirements evolve over time, and work is underway in the FC standards to produce a revised standard, FC-SP-3, that will provide updates to address the latest security developments in the industry.

7 Abbreviations

Abbreviations used in this paper:

ACL	Access Control List
BC	Business Continuity
BCM	Business Continuity Management
CHAP	Challenge Handshake Authentication Protocol
CNA	Converged Network Adapter
CT	Common Transport
DR	Disaster Recovery
DH	Diffie-Hellman
DOS	Denial of Service
ESP	Encapsulating Security Payload
FC	Fibre Channel
FC-SP	Fibre Channel - Security Protocols
FC-FS	Fibre Channel - Framing and Signaling
FC-GS	Fibre Channel - Generic Services
FCAP	Fibre Channel Certificate Authentication Protocol
FCIP	Fibre Channel over IP
FCP	Fibre Channel Protocol
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	IP Security
iSCSI	Internet Small Computer System Interface
LUN	Logical Unit
NPIV	N_Port ID Virtualization
RADIUS	Remote Authentication Dial In User Service
RFC	Request For Comment
SAN	Storage Area Network
SCSI	Small Computer System Interface
TCP/IP	Transmission Control Protocol/Internet Protocol
WWN	World Wide Name
WWPN	World Wide Port Name

8 Acknowledgments

10.1 About the Author

Eric A. Hibbard is the Director, Product Planning – Security at Samsung Semiconductor, Inc. and a cybersecurity and privacy leader with extensive experience in industry (PrivSec Consulting LLC, Hitachi, Raytheon, Hughes, OAO Corp), U.S. Government (NASA, DoE, DoD), and academia (University of

California). Mr. Hibbard holds leadership positions in standards development organization and industry associations, including ISO/IEC, INCITS, IEEE, SNIA, ABA, and CSA. He has also served as editor of ISO/IEC 27040, ISO/IEC 27050 series, ISO/IEC 22123 series, and IEEE 1619-2018.

Mr. Hibbard possesses a unique set of professional credentials that include the (ISC)2 CISSP-ISSAP, ISSMP, and ISSEP certifications; IAPP FIP, CIPP/US and CIPT certifications; ISACA CISA and CDPSE certifications; and CSA CCSK certification. He has a BS in Computer Science. Learn more at https://www.linkedin.com/in/ericahibbard/.

10.2 Reviewers and Contributors

The SNIA Security Technical Work Group (TWG) wishes to thank the following SNIA experts for their contributions to this technical paper:

Glen Jaquette, IBM

Thomas Rivera, VMware, Inc.

Paul Suhler, Kioxia Corporation

Mark Carlson, Kioxia Corporation

John Geldman, Kioxia Corporation

Sridhar Balasubramanian, NetApp

Jim Hatfield

Gary Sutphin

The SNIA Security Technical Work Group (TWG) wishes to thank the following FCIA experts for their contributions to this technical paper:

David Peterson, Broadcom

Roger Hathorn, IBM

James Smart, Broadcom

Patty Driever, IBM

Bibliography

[1] INCITS 509-2014, *Fibre Channel — Backbone - 6 (FC-BB-6)*
[2] INCITS 548–2020, *Fibre Channel — Generic Services - 8 (FC-GS-8)*
[3] INCITS 547–2020, *Fibre Channel — Switch Fabric - 7 (FC-SW-7)*
[4] INCITS 562–2024, *Fibre Channel — Framing and Signaling - 6 (FC-FS-6)*
[5] INCITS 496-2012, *Fibre Channel — Security Protocols - 2 (FC-SP-2)*
[6] IETF RFC 2865 *Remote Authentication Dial In User Service (RADIUS)*
[7] IETF RFC 4303 *IP Encapsulating Security Payload (ESP)*
[8] IETF RFC 4595, *Use of IKEv2 in the Fibre Channel Security Association Management Protocol*
[9] IETF RFC 7296, *Internet Key Exchange Protocol Version 2 (IKEv2)*
[10] Storage Networking Industry Association (SNIA), *Storage Security: Encryption and Key Management*

About SNIA

SNIA is a not-for-profit global organization made up of corporations, universities, startups, and individuals. The members collaborate to develop and promote vendor-neutral architectures, standards, and education for management, movement, and security for technologies related to handling and optimizing data. SNIA focuses on the transport, storage, acceleration, format, protection, and optimization of infrastructure for data.

About the Fibre Channel Industry Association (FCIA)

The Fibre Channel Industry Association (FCIA) is a non-profit international organization whose sole purpose is to be the independent technology and marketing voice of the Fibre Channel industry. We are committed to helping member organizations promote and position Fibre Channel, and to providing a focal point for Fibre Channel information, standards advocacy, and education.

SNIA
5201 Great America Parkway, Suite 320, Santa Clara, CA, 95054
Phone:719-694-1380 • Fax: 719-694-1385 • www.snia.org