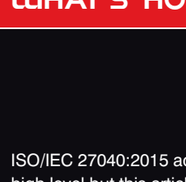
STORAGE SECURITY AND FIBRE CHANNEL SECURITY

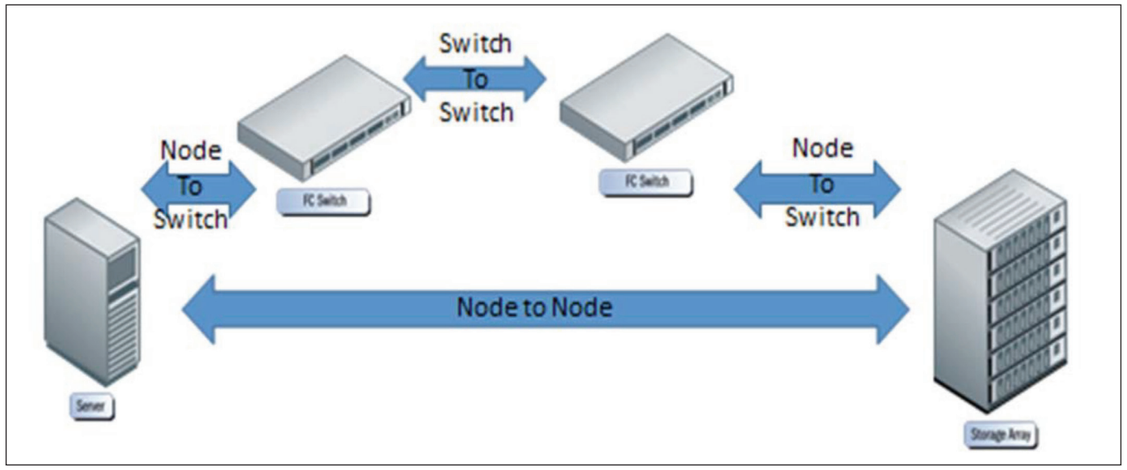


Fibre Channel is often viewed as a specialized form of networking that lives within data centers and neither has or requires special security protections. Neither of these assumptions is true, but finding the appropriate details to secure Fibre Channel infrastructure can be challenging. This SNIA storage security article 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. By Eric Hibbard, SNIA Storage Security TWG Chair, Hitachi, and SNIA Storage Security TWG team members.

ISO/IEC 27040:2015 addresses storage security risks and threats at a high level but this article is written in the context of Fibre Channel. The following list is a summary of the major threats 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 monitorin g revealing data, metadata, and storage protocol signaling. If the sniffed traffic includes authentication details, it may be possible for the attacker to replay9 (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.
- **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.

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.

A core element of Fibre Channel security is the ANSI INCITS 496-2012, Information Technology - Fibre Channel - Security Protocols - 2 (FC-SP-2) standard, which 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 several authentication infrastructures: secret-based, certificate-based, password-based, and pre-shared key based authentication.
- **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 using one of the following protocols:

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: storage networking and block-based storage.

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. Similarly, ISO/IEC 27040 provides limited guidance associated with Fibre Channel devices, above and beyond what may be implemented within FC SANs, including:

- 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 (when possible. For sensitive information that leaves protected areas use link encryption
- For sensitive/regulated or high-value data, implement data at rest encryption and the appropriate key management measures on the storage device or media.
- 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 more in-depth information about Storage Security and Fibre Channel, please see SNIA's whitepaper on Storage Security: Fibre Channel Security. This SNIA whitepaper, which was written by the Security Technical Working Group, is one in a series from SNIA that addresses various elements of storage security, and it 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.

For more information about SNIA and Security visit:
http://www.snia.org/security