SECURING FIBRE CHANNEL SANS WITH END-TO-END ENCRYPTION

By Robert Friend and Nishant Lodha, Marvell Semiconductor, Inc.

Fibre Channel is a purpose-built and proven storage network designed to meet the demands of enterprise data centers that require high availability, low latency, extreme reliability and seamless scalability. Fibre Channel (FC) SANs are deployed in over 90% of Fortune 1000 customer data centers that run mission-critical storage workloads. With ever increasing threat vectors both inside and outside the data center, a compromised customer dataset can quickly result in a torrent of lost business data, eroded trust, significant penalties, and potential lawsuits. There are potential vulnerabilities at every point in the enterprise infrastructure which requires data to be secured not only when it leaves the data center or is exposed to the internet, but every time it leaves a server or the storage media.

Existing SAN Security Mechanisms

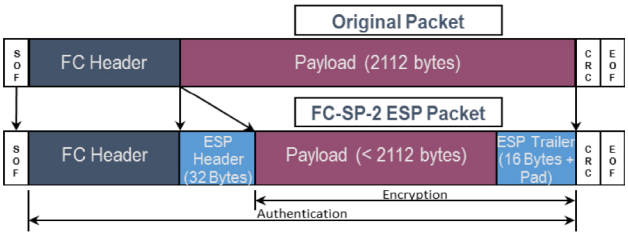
Fibre Channel SANs are inherently secure but are increasingly facing new and renewed threats. This is driving the industry to do more to secure Fibre Channel. The Fibre Channel protocol and a majority of Fibre Channel devices -- from HBAs to switches and storage devices, implement various security mechanisms ranging from access control via zoning, LUN Masking, and the security that physical segregation of storage and local area networks brings. However, with the increased risk of today's multi-tenancy environments that share Fibre Channel SAN resources across an increasing amount of host applications combined with increasing occurrences of insider attacks , make additional layers of protection required. In addition, government regulations including HIPAA, GDPR and ISO27001 A.10 increasingly require that transmission and storage of customer data be secured.

The level of security that will be required for Fibre Channel SANs is more than just encrypting storage media, as this only secures data against physical theft from the data center and does not protect against vulnerabilities while the data is in transit between host and storage media. During normal operations, data leaves shared storage devices unencrypted, which may pose a security risk. Adding defense in depth to the Fibre Channel SANs is prudent and provides excellent protection of mission-critical data that frequently traverse the Fibre Channel storage area network.

Fibre Channel Security Protocol FC-SP-2 standard provides the protocols and methods to extend the decades of proven security and storage networking technologies to the next level – encryption of data in flight.

Encrypting with Fibre Channel Security Protocol

Fibre Channel - Security Protocol (FC-SP-2), a stable and published standard, defines a security mechanism for FCP (Fibre Channel Protocol), FC-NVMe (NVMe over Fibre Channel) and FICON (Fibre Connection), developed by the Technical Committee T11 of the International Committee on Information Technology Standards (INCITS). It provides a security framework which includes authentication (using Diffie-Hellman Challenge Handshake Authentication Protocol (DHCHAP) or IKEv2), cryptographically secure key exchange, and cryptographically secure communication between Fibre Channel devices. The standard defines how to protect data in flight within a Fibre Channel SAN. It does not address the security of data at rest (in a storage device), for which other mechanisms already exist.



Within FC-SP-2, ESP_Header is a security protocol for Fibre Channel frames that provides origin authentication, integrity, anti-replay protection, and confidentiality. FC-SP-2 has adapted the IKEv2 protocol (used for IPsec) to provide authentication of Fibre Channel entities and setup of security associations. Within this framework, a Fibre Channel device can verify the identity of another Fibre Channel device and establish shared secrets that will be used to negotiate security associations for security protocols applied to Fibre Channel frames and information units.

Protections Provided by the Fibre Channel Security Protocol

When implemented, the FC-SP-2 standard will enable the following additional protections for Fibre Channel SANs:

- Origin authentication - verification that the traffic came from a given endpoint.
- Integrity assurance – assurance that the data transmitted was not tampered with before being received at the other end.
- Anti-replay protection – avoids a network attack in which a valid data transmission is maliciously or fraudulently repeated.
- Confidentiality – only the sender and receiver have access to the data contents of the frame.

Ecosystem and Market Dynamics

Encryption of data in flight seamlessly secures the entire SAN and is critical not only within, but also between, data centers for mirroring, backups, and remote replication to disaster recovery sites. Today, most Fibre Channel switches implement encryption for the data traffic that flows between Inter-Switch Links (link encryption), but an end-to-end solution between host/HBAs and storage devices is not yet generally available. Increased occurrences of insider attacks, theft of data while in transit, as well as government regulation is driving the Fibre Channel industry to productize an end-to-end Fibre Channel encryption and authentication implementation. It is expected that such implementations will work with existing SAN switch infrastructure. As defined in the FC-SP-2 specifications, payloads are encrypted, but the Fibre Channel header is sent in clear text, enabling encryption of data in flight to function with existing SAN switching.

A true secure SAN is one with end-to-end encryption and authentication! We expect that Fibre Channel HBAs with FC-SP-2 compliant, fully offloaded, end-to-end encryption capabilities will be generally available in early 2020.

---

[1] *https://fibrechannel.org/wp-content/uploads/2018/08/FCIA_SolutionsGuide2018_web.pdf*

[2] *https://www.forbes.com/sites/realspin/2016/08/30/the-future-of-insider-threats/#7e5270a47dcb*