BROADCOM

Solution Brief

Emulex® HBAs Bring Zero Trust Enhancements to the World's Most Secure Data Centers

LPe35000/36000-Series Gen 7 32/64GFC PCIe 4.0 Fibre Channel Host Bus Adapters

Executive Summary

- The SPDM feature uses proven cryptographic methods to protect the authentication process.
- Silicon RoT in the Emulex Gen 7 HBAs creates a digital fingerprint in the hardware, ensuring the server never boots with compromised HBA firmware.
- SPDM and Silicon RoT combined with native Fibre Channel's air-gap network design makes Fibre Channel the most secure network available.

Overview

With ever increasing server-related security threats, it is imperative that data centers implement a more robust, reliable, and trusted infrastructure. This paper will address PCIe adapters, specifically storage adapters, and how implementing industry best practices for I/O adapter and firmware authentication is essential in securing servers in a modern Zero Trust data center.

Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data.

The Emulex Fibre Channel (FC) host bus adapters (HBAs) by Broadcom® play a strategic role in modern data center networks and are relied upon as a critical element of data center security. In order to address potential security vulnerability, Emulex FC HBAs have integrated two features that will be highlighted in this paper: the Security Protocol and Data Model (SPDM) feature, which is an industry standard defined by DMTF, and Silicon Root of Trust (RoT) firmware security.

For host servers, the combination of these two security features has the following implications:

- Broadcom adapters are trusted by the server by means of SPDM authentication
- Broadcom adapters contain certified and untampered with firmware content

Firstly, the DMTF SPDM provides an authentication mechanism to establish trust using proven cryptographic methods that protect the authentication process. As part of establishing trust between two endpoints, the SPDM specification enables the creation of a session to exchange secured messages between the server and the I/O adapter. The SPDM architecture focuses on securing server platforms against attacks facilitated by components of the platform. To enable this defense, the SPDM architecture allows components such as FC HBAs and Ethernet NICs to prove their identity and integrity, and to exchange keys for a secure communication.

The other key element of security for PCIe adapters that this paper will discuss is firmware authenticity. Emulex FC HBAs feature Silicon RoT to guarantee firmware security.

SPDM Attestation Certification-Based Authentication

The primary goal of the Broadcom implementation of the SPDM is to enable a server to cryptographically verify the identity of each Broadcom adapter. The Broadcom SPDM feature includes the following key benefits:

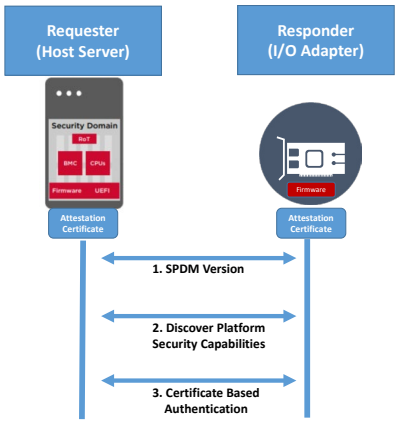
- Certificate-based authentication
- Privacy and data security communications

Emulex Fibre Channel HBAs are programmed at the factory with the X.509 v3 certificates, as defined by RFC 5280, to communicate identity information between the server and the Broadcom adapters. The firmware on the adapters enables the SPDM to be activated and does not require user activation.

Figure 1 shows the steps that are taken for the Requester (Server) and the Responder (I/O adapter) to establish a SPDM certificate attestation process. Adapter authentication steps include the following tasks:

1. Achieve both confidentiality and authenticity by verifying each other's identity.
2. Negotiate the cipher suites and crypto algorithms that are required to establish a secure connection.
3. Determine what version of SPDM will be used in the session.
4. Perform attestation certificate-based authentication.

Figure 1: SPDM Attestation Certificate Exchanges



The SPDM feature in Emulex Fibre Channel HBAs by Broadcom provides identity assurance and privacy and data security communications.

Silicon Root of Trust Firmware Security

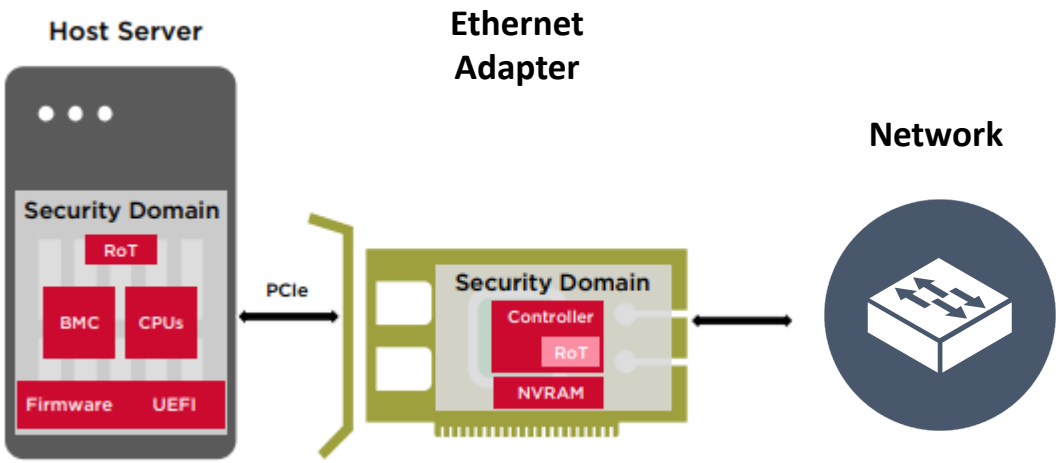
Protecting the firmware on server motherboards with hardware-based security has become a generally accepted data center best practice. However, the motherboard security does not protect the firmware of intelligent peripherals.

Adapter firmware must be secured by a lower-level protection mechanism, which is the silicon of the device itself. A true silicon RoT uses unalterable hardware to ensure the authenticity and integrity of all adapter firmware before it is allowed to execute on the controller. To make such an assurance, the RoT must guarantee the integrity of the controller boot process. The following paragraph explains this process.

The adapter begins to boot when the server applies power, or every time the server reboots. Immediately after the device exits reset, the Emulex HBA executes a Secure Boot Loader (SBL) code from an integrated, unchangeable ROM. This code locates the first firmware image in NVRAM. Then, the SBL authenticates this firmware image using a public key that is stored in the on-chip ROM. These authorized firmware images have been cryptographically signed with a SHA-256 hash of the image, encrypted with the private key using an RSA digital signature algorithm compliant with National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 186-4. During boot, the SBL authenticates this signature using its public key, also stored in on-chip ROM. Any modifications to the signed image will cause an authentication failure and prevent firmware execution. These unalterable elements, the SBL and public key, act as the core silicon RoT, ensuring the authenticity and integrity of the first firmware image.

The silicon RoT in Emulex Fibre Channel HBAs provide strong, hardware-based security. The unalterable silicon RoT protects adapter initialization and operational firmware from being compromised. The Emulex HBAs create a digital fingerprint in the hardware, ensuring the server never boots with compromised HBA firmware.

Figure 2: Silicon Root of Trust Process



Summary

With increased hardware and firmware security threats, data center architects must embrace enhanced Fibre Channel HBA security to deliver a more reliable and trusted infrastructure. Today, industry best practices includes the use of immutable, SPDM and silicon RoT features to protect from these attacks.

The combination of SPDM and silicon RoT in Emulex Fibre Channel HBAs provides strong security measures that result in host server assurances that the Emulex HBAs are trusted by the server and contain certified and untampered firmware content.

LPe3500x-Gen7-HBAs-SB102 March 27, 2023