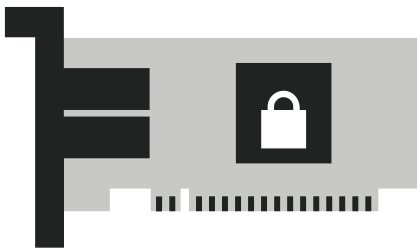
Securing Fibre Channel with Silicon Root of Trust

QLogic 2870 64GFC and 2770 Enhanced 32GFC HBAs



Cryptographically Secured Firmware on QLogic Fibre Channel (FC) HBAs Ensures SAN Integrity

Key Benefits

Here are some of the ways Marvell® QLogic® FC HBAs delivers value to an enterprise and/or MSP data center:

- To harden platform attack surfaces, security technologies should be rooted in hardware
- Such hardening is critical as attackers are increasingly launching sophisticated attacks on hardware
- Marvell QLogic 64GFC and Enhanced 32GFC incorporates an immutable silicon-based hardware root of trust
- Silicon/hardware embedded keys ensure only validated firmware executes on the FC HBA
  - Delivers additional layers of Defense in Depth
  - Prevents malicious firmware from hijacking the Fibre Channel adapter
- Ensures both integrity and authenticity during adapter firmware updates
  - Protects firmware updates in critical environments and at remote locations
- Eliminates threat vectors and protects servers by leveraging strong public key cryptography

Executive Summary

Marvell QLogic 2870 Series of 64GFC and 2770 Series Enhanced 32-Gigabit Fibre Channel (GFC) Adapters incorporate silicon Root of Trust (RoT) technology that prevents malicious firmware from hijacking the Fibre Channel adapter. Hardware-based security provides a “chain of trust” rooted in silicon that makes the Fibre Channel Host Bus Adapter (HBA) and extended storage area network (SAN) more trustworthy and secure.

Business Drivers for Securing Fibre Channel Adapter Firmware

Security threats continue to evolve and increase, driving Chief Information Officers towards securing the server all the way down to the firmware at the lowest layers of the server platform, where attacks can be the most difficult to detect.

- To minimize the security threat of unauthorized software accessing and changing configuration of storage networking components, server vendors are looking to restrict and control write accesses to on board non-volatile memory, both on the motherboard and in adapters like FC HBAs. Robust public key security technology guarantees utilized to protect servers.

FC HBA Platform Integrity with Secure Firmware

Marvell QLogic 2870 Series of 64GFC and 2770 Series Enhanced 32GFC Adapters deliver additional layers of Defense in Depth with the new secure firmware download feature, which provides both integrity and authenticity during adapter firmware updates, and every time the adapter is restarted. Marvell QLogic adapters verify strong signatures before committing downloads and passing control to operational code. This ensures only validated firmware executes and protects firmware updates in critical environments and at remote locations.

Platform Security Technologies – Firmware Verification

Marvell QLogic 64GFC and Enhanced 32GFC adapters contain Marvell's public key and receive Marvell Fibre Channel firmware appended with a strong signature. These adapters perform an RSA (cryptosystem) verification operation using the Marvell public key to authenticate the signed firmware. Verification can be thought of as "decryption with the public key". Marvell FC adapters first compute the SHA-256 hash of the firmware update while decrypting the appended signature with the Marvell public key. These adapters then compare the SHA-256 computation (aka "Digest") with the RSA decryption of the appended signature. If the comparison is successful, then it proves two facts, illustrated in Figure 1. First, the firmware has integrity, because the hashes match. More importantly, the firmware is authentic and could only have been generated by Marvell, because RSA's mathematical property virtually guarantees that only Marvell's private key could have generated that signature.

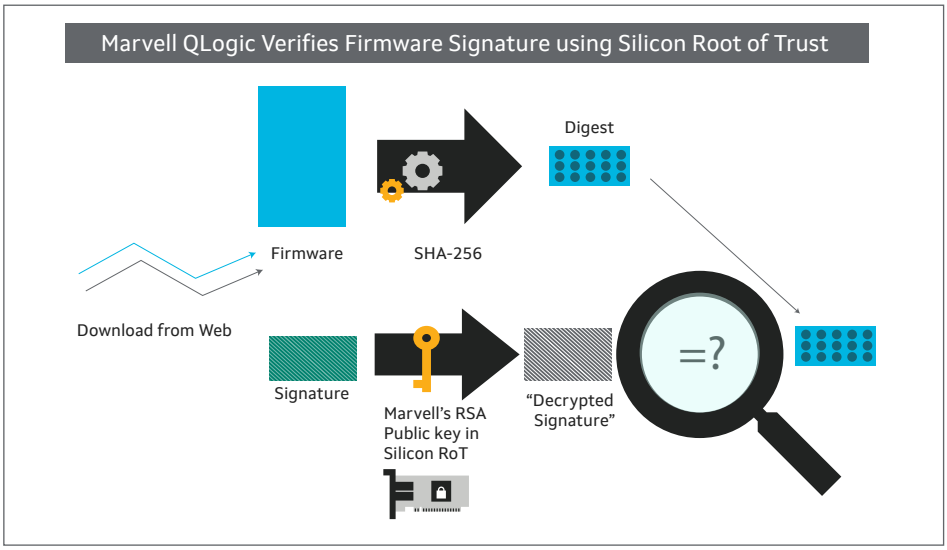


Figure 1. Marvell QLogic 2870 and 2770 Series firmware verification using RSA public key

Platform Security Technologies – Signing Trusted Firmware

Marvell's public key encryption utilizes two mathematically-related keys, which have a special inverse property when performing public key cryptography. Marvell creates the RSA private / public key pair, keeps one key secret and protected, and distributes the other on all Marvell QLogic 64GFC and Enhanced 32GFC adapters. In Figure 2, Marvell uses the private key to sign a 32-byte SHA-256 hash (aka "Digest") of the firmware. Think of signing as "encrypting with the private key". Marvell distributes the firmware appended by this signature. Marvell burns its public key into these adapters, so they can verify Marvell's firmware signatures.

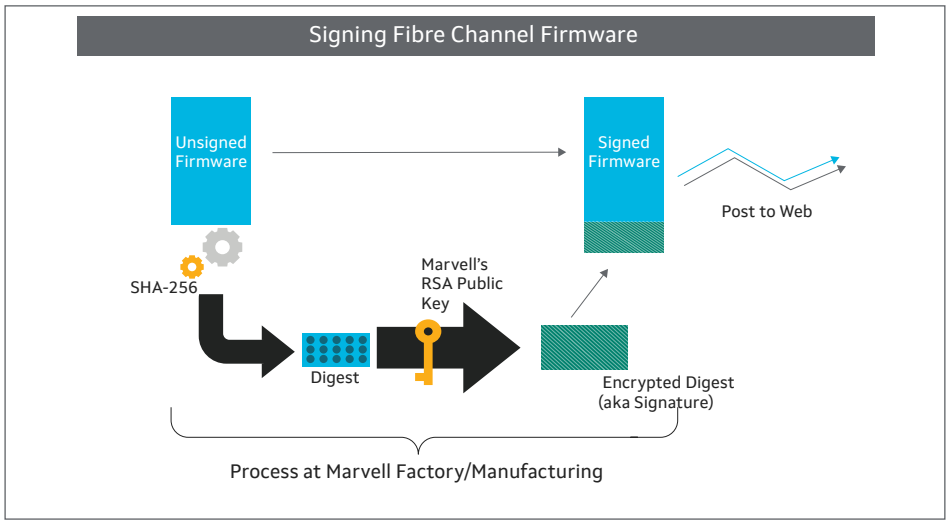


Figure 2. Marvell signing trusted firmware using RSA private key

Best Practices

To harden hardware-based attack surfaces against firmware exploits, servers must secure their own firmware, along with the firmware of all adapters. This enables a chain of trust that extends from the motherboard across all adapters providing a cohesive security architecture that protects the server against hardware-based threat vectors. This in turn provides a trusted foundation for additional layers of security, such as secure boot.

The Marvell QLogic 2870 Series of 64GFC and 2770 Series Enhanced 32GFC Adapters are designed from the ground up to secure mission-critical servers with hardware based Root of Trust (RoT) and protect against rouge firmware exploits. The Marvell QLogic FC HBAs extends the server's secure hardware-based RoT allowing only trusted firmware to download and execute by utilizing strong public key authentication.

Summary

To secure servers down to the firmware at the lowest layers of the server platform, the Marvell QLogic Adapters incorporate hardware RoT technology that prevents malicious firmware from hijacking the Fibre Channel adapter. Marvell QLogic 2870 and 2770 Series ensures both integrity and authenticity by validating firmware signatures with strong embedded cryptographic keys so that only authentic firmware executes, while protecting firmware updates that are applied over public networks.