Solution Brief

NetXtreme® E-Series: Industry's Most Secure Ethernet Adapters

Building data center security on BroadSAFE™ Silicon Root of Trust

Thor 2x100G Ethernet Network Adapter (NIC) and Whitney+ 2x25G Ethernet Network Adapter (NIC)

Executive Summary

Ethernet adapters occupy a strategic location in the data center and their operational integrity is a critical component of data center security.

Industry best practice security solutions use an unalterable, hardware root of trust to guarantee the integrity of adapter firmware and its secure configuration, operation and management while deployed in the data center.

Broadcom adapters provide a comprehensive set of security features, centered around a silicon root of trust, making them the most secure adapters in the industry.

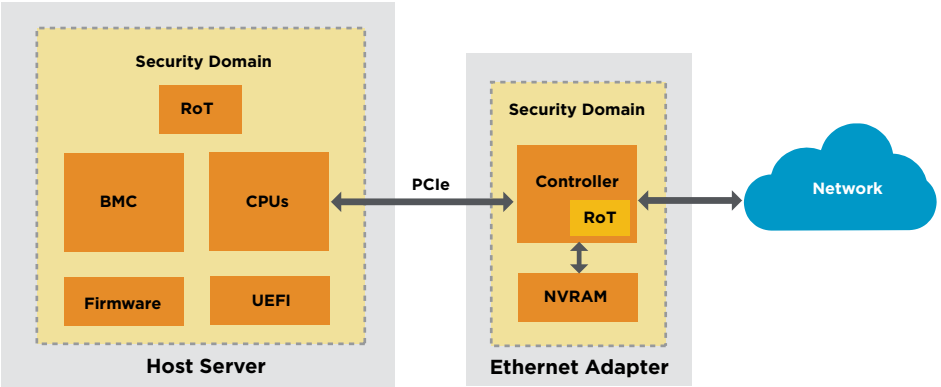
Introduction

With direct access to the data center network, Ethernet adapters occupy a strategic location in the server and can uniquely compromise a data center's security. A single compromised Ethernet adapter could impact thousands of unsuspecting users by snooping or blocking application traffic, inserting malicious messages or diverting traffic from its intended destination. A larger scale hack involving multiple network adapters could wreak havoc in the data center, potentially affecting millions of users.

To address this potential security vulnerability, Broadcom has integrated BroadSAFE security technology including a silicon Root of Trust (RoT) into its NetXtreme E-Series Ethernet adapters, helping to make them the industry's most secure network adapters. This RoT, first introduced to the E-Series with the BCM574xx (Whitney+) controller in 2016, provides an unalterable hardware foundation for a comprehensive suite of adapter security features.

This paper will describe how a hardware root of trust operates and how it enables a host of features essential to the secure operation of network adapters in the data center.

Figure 1. Ethernet adapters reside in an independent security domain



Security Risks in Ethernet Adapters

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

From a security standpoint, the adapter is a standalone system built around a System on Chip (SoC) known as the controller and non-volatile memory (NVRAM) containing the controller firmware. While the adapter is connected to the host via a PCIe interface, it is entirely outside of the motherboard's security domain. Preventing unauthorized firmware from executing on the controller is therefore of paramount importance and is only possible if adequate security is available on the adapter itself.

Adapter firmware presents attack surfaces resembling that of other electronic systems. The small form factor and ease of replacement of Ethernet adapters in the field could increase the risk of hardware modification or adapter swapping.

Drawing lessons from recent history, other possible types of hardware attacks include interception and modification during shipment[1] and the alleged insertion of surveillance chips during manufacturing[2]. By making modification to an adapter, an attacked could compromise firmware by inserting malware into NVRAM.

Direct firmware attacks are also on the rise. Cyber-espionage groups have begun to exploit UEFI firmware in laptops with the LoJax attack[3]. Research has exposed similar firmware vulnerabilities in servers. In February 2019, security experts showed that the Cloudbourne attack could "brick" a server or hijack a bare-metal cloud server through BMC firmware[4].

Even an isolated, secure data center is not immune to such breaches, A malicious insider with sufficient privileges could exploit their access to modify adapter hardware or load unauthorized firmware onto the adapter[5].

Given the growing sophistication of the attackers, attacks upon adapter firmware are likely. Therefore, adapter security solutions must prevent malware insertion via hardware or firmware attacks.

BroadSAFE Security Technology Pedigree

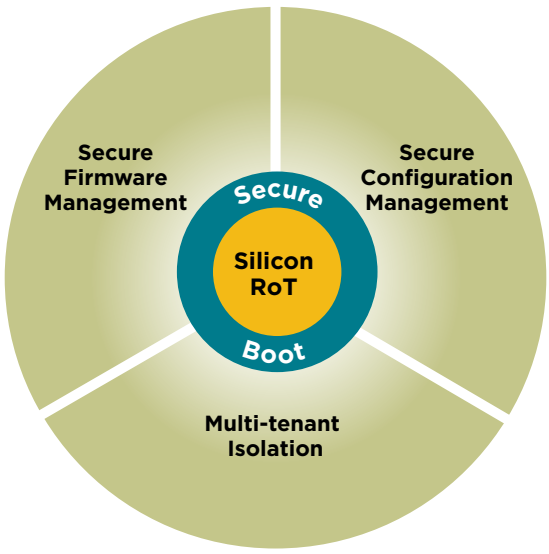
NetXtreme leverages BroadSAFE security technology. BroadSAFE is a suite of security solutions used across Broadcom product lines, including network adapters, switches, secure processors, and systems-on-a-chip (SoCs) and has tracked security best practices for more than 15 years. BroadSAFE has been hardened by deployment in the most demanding of security environments, such as Point of Sale (POS) terminals where it routinely protects remote payment processing from physical, firmware and side-channel attacks.

Security Framework in NetXtreme E-Series Adapters

Securing Ethernet adapters requires a holistic approach to security. To prevent hardware and firmware tampering on adapter firmware, the foundation of any security approach for Ethernet controllers must be a silicon Root of Trust. This hardware protects the firmware which in turn implements and controls key software and hardware security features.

Figure 2 shows the NetXtreme E-series security solution architecture, centered around its integrated silicon RoT.

Figure 2. Silicon Root of Trust is the foundation for adapter security

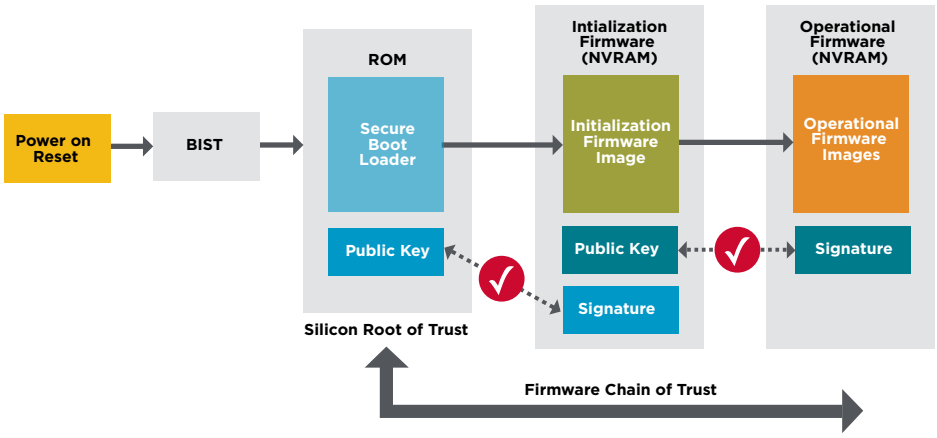


1. https://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden
2. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies
3. https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/
4. https://www.zdnet.com/article/hackers-can-hijack-bare-metal-cloud-servers-by-corrupting-their-bmc-firmware/
5. https://www.securityweek.com/tesla-breach-malicious-insider-revenge-or-whistleblowing

BroadSAFE Silicon RoT protection

Adapter firmware must be secured by a lower-level protection mechanism, 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 section describes the boot process of Whitney+, Broadcom's market-leading dual-port 25G NetXtreme Ethernet controller.

Figure 3. Whitney+ Silicon RoT and Secure Firmware Loading



Whitney+ Adapter Boot Sequence

The adapter begins to boot when the server applies power, which initiates the card's reset sequence. Immediately after the device exits reset and before any code executes, the controller verifies the integrity of all of its internal memories with hardware-based Built-in-Self-Test, or "BIST". A BIST failure aborts the boot process as it might indicate tampering with the device.

Once BIST completes, the controller's processor executes Secure Boot Loader (SBL) code from an integrated, unchangeable ROM. This code locates the first firmware image in NVRAM and copies it to internal memory. Then, the SBL authenticates this firmware image using a public key, 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 or ECC algorithm. 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 BIST, SBL, and public key, act as the core silicon RoT, ensuring the authenticity and integrity of the first firmware image.

The first image loaded during boot contains the initialization firmware which continues to initialize device hardware and loads additional operational firmware images that provide the complete functionality of the adapter. The initialization firmware authenticates each operational firmware image using its own public/private key pair. This extends a chain of trust, authentication traceable to the silicon RoT, to all firmware and completes the secure boot process.

NetXtreme E-Series Security Feature Summary

Once the secure boot process completes, the operational firmware provides a variety of features that enable secure adapter operations. Several features rely on controller hardware mechanisms configured by the firmware, while others are functions of the firmware itself. These features include the following.

Table 1. NetXtreme E-Series BroadSAFE security features

Secure Firmware Management	Chain of trust extended to all operational firmware via authentication, preventing malware insertion. Firmware authenticated at boot and during updates. All updates logged.
Secure Configuration Management	Firmware encrypts sensitive configuration data such as passwords. All modifications logged. Configuration deleted with secure wipe.
Multi-tenant Isolation	Firmware manages several hardware protection mechanisms for the PCIe interface and RoCE DMA to isolate PCIe functions, VMs and applications.

Secure Firmware Management

Firmware updates in the field must be securely managed through remote mechanisms at data center scale. New firmware images are authenticated and verified by operational firmware, secured via the chain of trust prior to being written into NVRAM. The controller maintains an audit log of all update events, both successful and unsuccessful. This cryptographically protected process is FIPS 186-3 and NIST SP800-131A compliant.

Secure Configuration Management

Adapter operational firmware stores user and OEM configuration data in NVRAM. Sensitive data, such as iSCSI CHAP passwords, is encrypted. A configuration reset will erase user configuration data and restore the adapter's default configuration, enabling the safe redeployment or decommissioning of the adapter without exposing sensitive user data.

Multi-tenant Isolation

Multiple host tenants, virtual machines (VMs) and RDMA over Converged Ethernet (RoCE) applications, often share an adapter. The adapter must isolate tenants from one another to ensure fair sharing of the network and prevent cross-tenant interference by any misbehaving tenants. The adapter firmware abstracts and virtualizes controller hardware resources and allocates authorized resources to individual tenants to establish a secure configuration of the adapter. Once the firmware has configured the adapter, hardware protection mechanisms enforce the isolation between tenants.

Conclusion

With the expected increase of hardware and firmware security threats, data center architects must address Ethernet adapter security to design a reliable and trusted infrastructure. Today, the industry best practice includes the use of an immutable, silicon RoT to protect from these attacks.

The BroadSAFE silicon RoT in NetXtreme E-series adapters provides strong, hardware-based security. The unalterable RoT protects adapter initialization and operational firmware from being compromised. This maintains the integrity of all adapter security features, making the NetXtreme E-series the most secure Ethernet adapters in the industry.

BROADCOM®
connecting everything®

For more product information: broadcom.com

BC-0537EN 06.14.2019