White Paper

Data Center Server Security

Deploying Trusted Systems in Zero Implicit Trust Environment

Server Security is Fundamental to Data Center Security

Modern data centers must grapple with a wide variety of security threats from multiple vectors. To insulate against these vulnerabilities, several layers of both physical and digital security measures are typically employed. Typical digital security measures include network firewalls to prevent unauthorized accesses, protection against cyber attacks (phishing, malware, DDoS, and so on) and encrypting data in flight and at rest. While the scale is different, enterprise data centers and cloud providers face similar threats and employ similar countermeasures.

Implicit in these digital security measures is the trustworthiness of the servers themselves. Earlier generations of data centers trusted a server, its hardware, and software components. This presumption of trust is no longer acceptable. Today's data centers must expect and guard against unauthorized firmware components, malicious or otherwise, while tomorrow's data centers will be required to distrust hardware components till proven trustworthy.

Servers Must be Resilient Against Unauthorized Firmware Modification

At boot up, firmware binaries are the first software components that execute on a server and set it up for OS and other software services to load. Since a piece of software is typically mutable (changeable after compilation), a firmware can be compromised by modifying the binary code. A compromised firmware binary will compromise the server. For example, compromised firmware can facilitate misuse of the user data or expose the server to a range of attacks resulting in operational and reputational damage. There are several ways in which an attacker can modify the firmware binary of a server component:

- A malicious firmware is directly written to a flash part before or after it is mounted on the hardware
- A compromised server allows an unauthorized actor with physical or logical access to flash a malicious firmware using the normal update tools and mechanisms
- Load one OEM's customized firmware binary on another OEM's platform
- Load older firmware versions with known vulnerabilities

To be resilient to these types of binary modifications, a robust hardware solution must verify the following:

- The firmware is from the known and approved source (authenticity)
- It has not been modified after release by the source (integrity)
- It is allowed to run on that hardware (authorization)

Once booted, the firmware must also close all possible attack surfaces such as debug ports, JTAG ports, and any other out of band mechanisms through which an attacker with physical or logical access might gain access to the hardware and running firmware.

Any solution that is not rooted in the hardware or does not perform these checks is not resilient enough for enterprise and cloud data centers where security is paramount.

Broadcom® Hardware Root of Trust (RoT) and Secure Boot

Broadcom technology is leading the industry to make data center products highly secure by participating and contributing to the DMTF Security Task Force (SPDM), the OCP Security Project, and TCG. All current generation product lines across SAS I/O controllers, RAID controllers, SAS expanders, and PCIe switches implement hardware secure boot per NIST SP800-193 guidelines. The following product attributes are common across the Broadcom portfolio of products.

Identity and Integrity of Firmware Images

One of the fundamental goals of any secure boot solution is to verify the identity of the supplier of the firmware and that the firmware has not been modified since it was released by the supplier. To achieve these goals, Broadcom products implement the RSA Public Key Cryptography Standard (PKCS) Digital Signature scheme (approved by Federal Information Processing Standards, FIPS). The firmware binary is signed by computing its hash digest and encrypting the digest using a private key. The encrypted hash (signature) is then included in the final firmware image.

To verify the integrity of the firmware, one can recompute the firmware hash and compare it with the decrypted signature that is part of the image. If the hashes match, one can be assured of the firmware integrity. Since one has to use the public key to decrypt the signature, one can be assured of the identity of the signatory (firmware signer).

The security of the solution is as strong as the weakest link in the process. Broadcom uses a physically secure tamper-proof FIPS-2 compliant Hardware Security Module (HSM) in its data center to perform the firmware signing. The HSM ensures that the private key never leaves the HSM server and is protected from compromise. Firmware build and signing processes are fully automated and access limited.

Hardware-based Root of Trust

While a signed firmware proves the integrity of the binary and the identity of the signatory, that alone doesn't make the solution secure. The entity that verifies the signed firmware can be compromised and thus the verification process itself can be circumvented. A secure solution must include a verification and authentication mechanism that cannot be circumvented. That usually means a hardware-based mechanism.

All Broadcom current-generation SAS I/O controllers, RAID controllers and PCIe Switches implement hardware-based secure boot. All controller and switch hardware contains an immutable firmware image that verifies the mutable firmware identity and integrity before booting. As the name implies, the immutable code is part of the hardware. It is not a separate piece of code that is programmed into the hardware. Separate code is unreliable and creates another attack surface.

Hardware also contains a One Time Programmable (OTP) memory that contains the Public Keys. To be allowed to boot, a signed firmware binary must not only pass the identity and integrity verification, but must have also been signed by the private key that corresponds to the key in the OTP (authorization).

Broadcom products also offer the flexibility to customers to use their own public and private keys. Customers can securely migrate from Broadcom keys to Customer keys. Once migrated, hardware will boot only with customer signed firmware binary. Broadcom provides the tools and the knowhow to safely migrate the keys and sign the firmware.

Customers can be confident that Broadcom products meet all the criteria that the data center industry considers essential for a highly resilient secure solution.

Future of Server Security

The next step in the server security evolution is for a platform to verify and establish trust in all of the intelligent components. A trusted tamper-proof hardware component in a platform (system level root of trust) will attest the identity of the other system components (for example, I/O controllers and PCIe switches). The attestation process uses digital certificates to verify the identity and authenticity of the components, similar to how HTTPS uses certificates.

Broadcom has long been a long-time contributor to the DMTF standards body, working to define and grow the attestation standards. The result of that industry collaboration is the Security Protocol and Data Model (SPDM) standard for attestation. Broadcom has already started SPDM pilot projects with a few partners and all next-generation products will support SPDM.

Broadcom, a leading provider of data center solutions, has a comprehensive portfolio of network, server and storage connectivity. To learn more about Broadcom NVMe/SAS/SATA/PCIe storage connectivity solutions, visit broadcom.com/products/storage.

The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, please visit www.broadcom.com.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

BROADCOM®