White Paper
Public

The bridge to possible

Cisco Trustworthy Technologies in Nexus 9000 Switches

© 2023 Cisco and/or its affiliates. All rights reserved.

Contents

© 2023 Cisco and/or its affiliates. All rights reserved.

Introduction

Trustworthy solutions encompass Cisco's commitment to deliver products and solutions with multilayered security that protect against today's threats. Trustworthy technologies provide a foundation of security and resilience across Cisco's solutions portfolio. Trustworthy technologies such as image signing, secure boot, Cisco Trust Anchor module (TAm), and runtime defenses help ensure that the code running on Cisco hardware platforms is authentic, unmodified, and operating as intended. A hardware-level root of trust, unique device identity, and validation of all levels of software during startup establish a chain of trust for the system.

Trustworthy Technologies in Nexus 9000 Switches

Today's sophisticated cyberattacks increasingly seek to compromise the network infrastructure by attacking devices such as routers and switches. By doing so, attackers can eavesdrop on sensitive communications, steal or manipulate data, and launch attacks against other parts of the network. This includes advanced persistent threats that modify the hardware or software of network devices. These threats can go unnoticed for months, or even years, inflicting devastating damage.

Cisco trustworthy technologies provide product assurance functionality as well as foundational security capabilities that enhance the security and resilience of Cisco solutions. To protect against device counterfeiting and malicious attacks on hardware and software, Cisco uses digitally signed software images, hardware-anchored secure boot, Secure Unique Device Identifier (SUDI), and other trustworthy technologies to verify the authenticity and integrity of our solutions. Among other functions, trustworthy technologies run automated checks of hardware and software integrity and can shut down the boot process if compromise is detected. The Cisco Trust Anchor module provides a Secure Unique Device Identifier, highly secure storage, a random bit generator, and secure key management. These added layers of security protect against counterfeit and software modification; enable secure, encrypted communications; and verify that Cisco network devices are operating as intended.

In this whitepaper, we will discuss some of the Trustworthy technologies that are adopted by Cisco Nexus 9000 switches used in a data center.

Cisco Secure Unique Device Identifier (SUDI)

The Cisco Secure Unique Device Identifier (SUDI) is an X.509 certificate whose private key is stored in the Trust Anchor Module at manufacturing time by Cisco to provide a tamperproof device ID. It is used for verifying the initial identity of the device during the onboarding process. More importantly, we also use it to verify the authenticity of the hardware and check against counterfeiting.

The SUDI is composed of the product ID + device S/N to uniquely identify a device. The SUDI is an IEEE 802.1AR compliant X.509v3 certificate that can be either RSA or ECC. This feature makes cloning or spoofing the identity information virtually impossible. The SUDI helps to avoid counterfeiting switches in the supply chain.

© 2023 Cisco and/or its affiliates. All rights reserved.

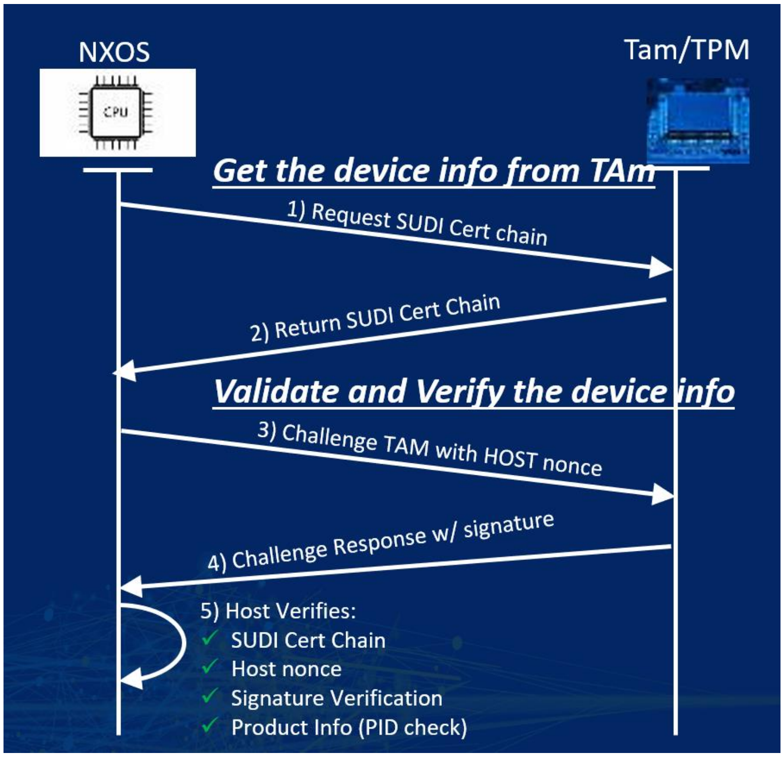

NXOS
CPU
Tam/TPM
Get the device info from TAm
1) Request SUDI Cert chain
2) Return SUDI Cert Chain
Validate and Verify the device info
3) Challenge TAM with HOST nonce
4) Challenge Response w/ signature
5) Host Verifies:
✓ SUDI Cert Chain
✓ Host nonce
✓ Signature Verification
✓ Product Info (PID check)

Figure 1. Hardware authenticity check with SUDI

Trust Anchor Module (TAm)

The Cisco Trust Anchor module (TAm) is a tamper-resistant chip that is built into Cisco Nexus 9000 switches. The TAm has nonvolatile secure storage and it is the root of the trust chain. The manufacture's public key is stored in the TAm chip for every Cisco Nexus switch.

ACT and ACT2 are hardware chips present in Nexus 9000 switches for bringing in Anti-Counterfeit Technology (ACT) to the gear.

The TAm includes the following things:

Identity
During product manufacturing, a product's ACT2 chip is filled with Cisco Secure Unique Device Identity (SUDI) in the form of an X.509v3 ECDSA or RSA certificate (or both), along with the associated keypairs and certificate chains. SUDI is the basis for Cisco's hardware anti-counterfeit check and is also used for establishing initial network identity.

Entropy
The ACT2 contains a NIST SP 800-90B compliant entropy source that is ideal for seeding host-based pseudo-random number generators.

Key Management
The ACT2 can generate symmetric keys and ECC and RSA asymmetric keypairs. The symmetric keys and the private portion of the keypairs are never released from the chip. Access to the protected keys is through crypto APIs. Certificates can be enrolled for the keypair generated by the ACT2.

Secure Storage
ACT2 can store about 50 KB of host data in a physically tamper-protected manner. This is an ideal location

© 2023 Cisco and/or its affiliates. All rights reserved.

for sensitive data such as licenses and secret data such as credentials. Important Nexus 9000 keys and passwords are saved in this secure storage.

TAm and SUDI in Nexus 9000 are similar to an IMEI (International Mobile Equipment Identity) number for a mobile device. This acts as a unique identifier for the hardware along with having other functionalities.

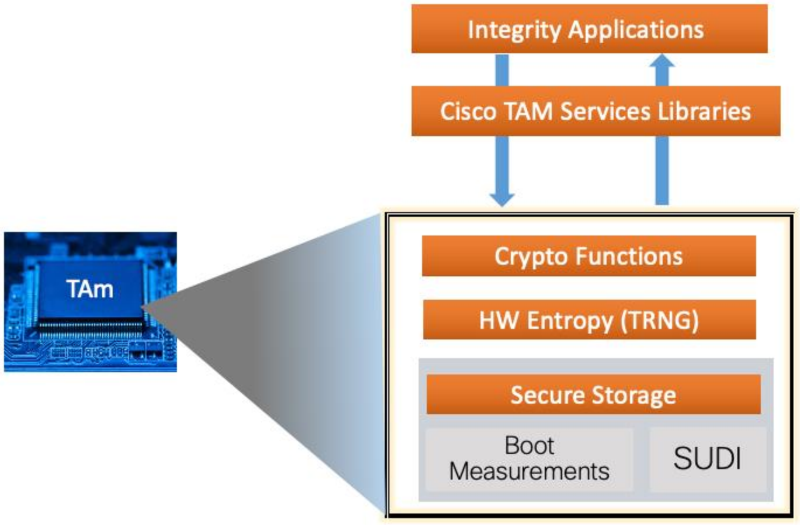


Figure 2. TAm in Nexus 9000 switches

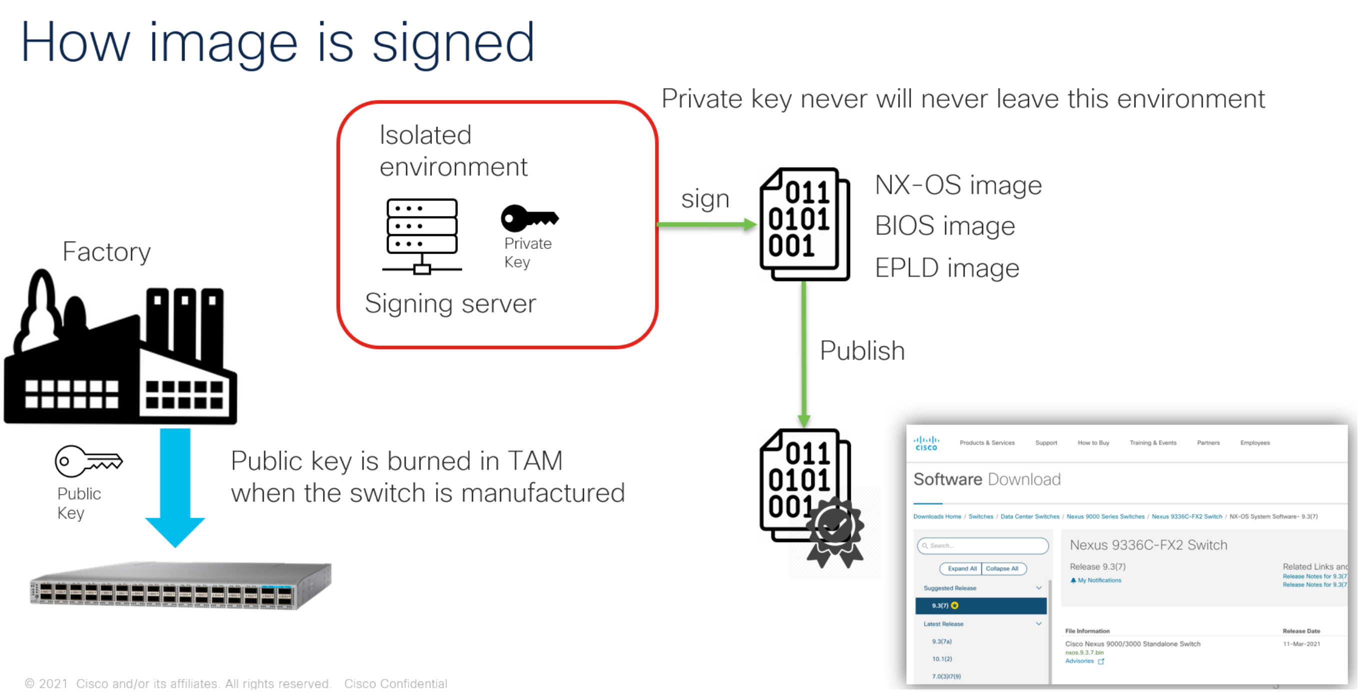
TAm has a secure nonvolatile storage for keys that are used for cryptographic algorithms. This storage is accessible to the applications using TAm libraries. The SUDI and boot measurements that are stored here are accessed during the switch bootup time to determine if the switch is legitimate and the booting process is executed as expected, or if someone tampered with it.

Secure Boot

Cisco Secure Boot helps to ensure that the code that executes on Nexus 9000 platforms is authentic and unmodified. Cisco hardware anchored secure boot protects the micro loader (the first piece of code that boots) in tamper-resistant hardware, establishing a root of trust that helps prevent Cisco network devices from executing tainted network software.

All images published by Cisco are signed by the manufacturer's private key. The environment is isolated, secured, and audited. The key pair is generated using RSA with a modulus of 2048.

After the device boots up, it authenticates the device with TAm using SUDI to verify that the device hardware is genuine Cisco hardware, not a counterfeit or compromised one.


How image is signed
Private key never will never leave this environment
Isolated environment
Private Key
Signing server
sign
NX-OS image
BIOS image
EPLD image
Publish
Factory
Public Key
Public key is burned in TAM when the switch is manufactured
011
0101
001
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Products & Services Support How to Buy Training & Events Partners Employees

Software Download

Downloads Home / Switches / Data Center Switches / Nexus 9000 Series Switches / Nexus 9336C-FX2 Switch / NX-OS System Software- 9.3(7)

Search...

Expand All | Collapse All

Suggested Release

9.3(7)

Latest Release

9.3(7a)

10.1(2)

7.0(3)I7(9)

Nexus 9336C-FX2 Switch

Release 9.3(7)

My Notifications

Related Links and

Release Notes for 9.3(7

Release Notes for 9.3(7

File Information	Release Date
Cisco Nexus 9000/3000 Standalone Switch nxos.9.3.7.bin Advisories	11-Mar-2021

Figure 3. Nexus OS images image signing process.

Public key is burned into the hardware, and this is accessible through the TAm libraries. Nexus OS images are signed through private keys that will never leave the build DevOps release environment. These keys are compared during the boot process, which confirms that the Nexus hardware and software are signed by Cisco.

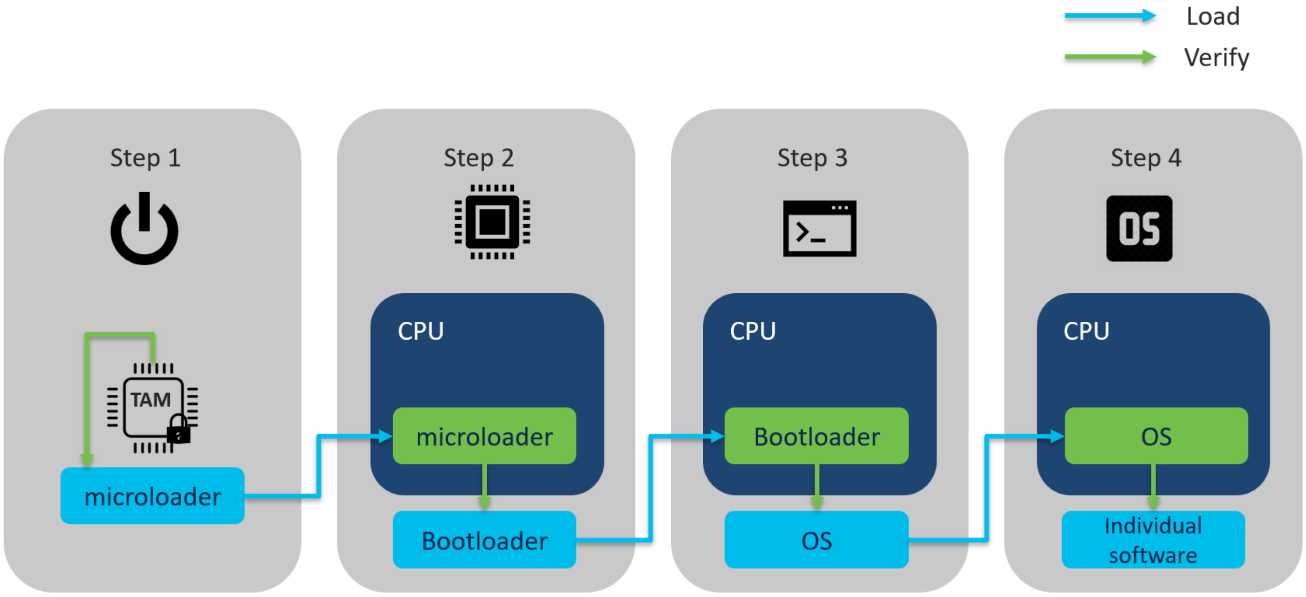


Figure 4. Secure boot at a glance

The secure chain starts from the TAm. The TAm verifies the integrity of the microloader before loading it to the CPU. The microloader verifies the BIOS/bootloader same way by calling the API of the TAm to verify the image of BIOS/bootloader before loading. The same thing applies when loading the NX-OS image.

After the image is loaded to the CPU, before activating the software, such as KLM, RPM, and ASIC SDK, the OS calls the API from the TAm to verify them.

Chip Guard (Chip Protection)

The chip protection feature available in Cisco Nexus 9000 DC switches ensures the integrity of the hardware. The chip protection takes the signature of each device at manufacturing time and compares the signature during every device bootup to ensure the peripherals on the Nexus 9000 are not counterfeited.

Manufacturing Time Database

The manufacturing time database is the original copy of the unique IDs of Cisco ASICs, CPUs, SoCs, and other devices with their device types specific to a board. In most cases, the unique ID is a device serial number or other appropriate value of that device. The manufacturing database is a Known Good Values (KGV) database specific to a board. It is programmed onto the TAm device as part of the manufacturing process.

Collected Database

The collected database is collected by the firmware whenever the board is booted and extended to the TAm device. Measurements are collected either through firmware or through system drivers.

The BIOS boot process integrates the TAm library to populate the collection database. The BIOS detects various hardware components as part of initialization and uses the TAm library APIs to record the device type and unique IDs if the detected devices are part of the manufacturing time database. After all the device types and unique IDs are written to the collected database, the platform operating system invokes the TAm library API to validate the collected database against the manufacturing time database. If there is a mismatch, the platform holds the boot process.

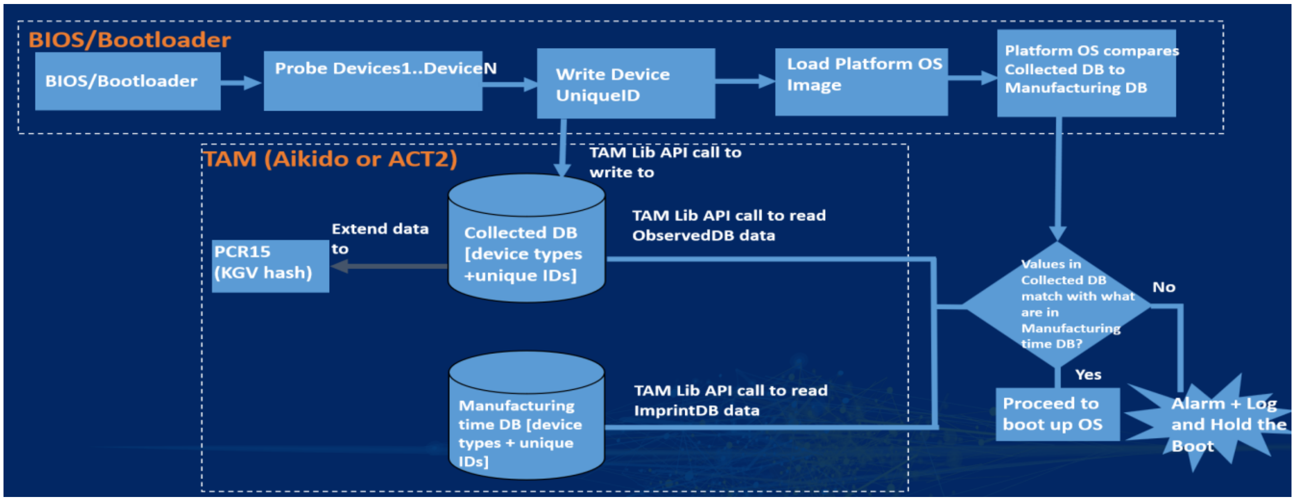
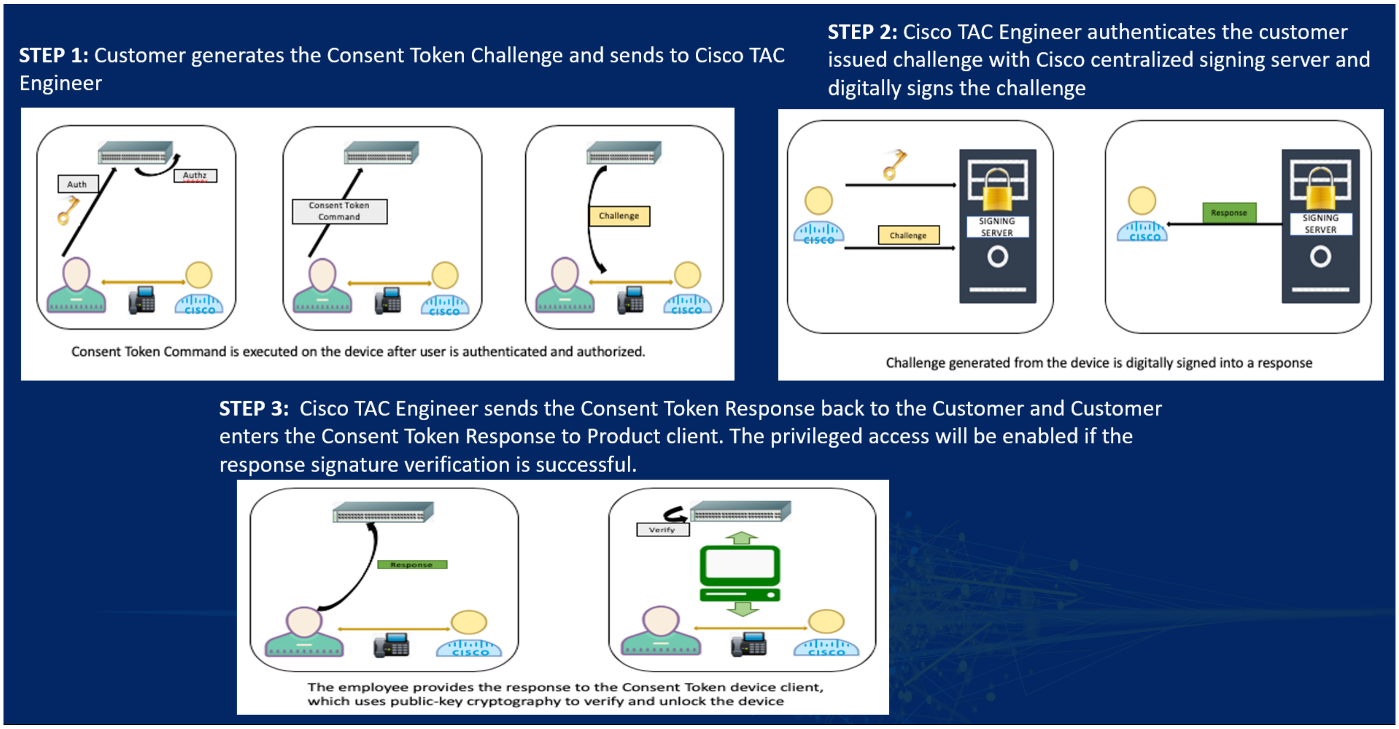

BIOS/Bootloader
BIOS/Bootloader
Probe Devices1..DeviceN
Write Device UniqueID
Load Platform OS Image
Platform OS compares Collected DB to Manufacturing DB
TAM (Aikido or ACT2)
TAM Lib API call to write to
Extend data to
PCR15 (KGV hash)
Collected DB [device types +unique IDs]
TAM Lib API call to read ObservedDB data
Values in Collected DB match with what are in Manufacturing time DB?
No
Yes
Manufacturing time DB [device types + unique IDs]
TAM Lib API call to read ImprintDB data
Proceed to boot up OS
Alarm + Log and Hold the Boot

Figure 5. Chip protection

Consent Token

A consent token is the centralized mechanism to provide secure, transparent, customer-authorized feature enablement on Cisco Nexus 9000 switches in an auditable and trackable process. A consent token is also a form of a multi-factor authentication system that creates a common client-server infrastructure to allow functionalities such as secure shell access on Cisco Nexus 9000 switches, leveraging the available digital signature verification infrastructure.

The secure shell access primary use case is to provide restrictive, time-bound root shell access to Cisco Nexus 9000 switches with customer consent.



STEP 1: Customer generates the Consent Token Challenge and sends to Cisco TAC Engineer

Consent Token Command is executed on the device after user is authenticated and authorized.

STEP 2: Cisco TAC Engineer authenticates the customer issued challenge with Cisco centralized signing server and digitally signs the challenge

Challenge generated from the device is digitally signed into a response

STEP 3: Cisco TAC Engineer sends the Consent Token Response back to the Customer and Customer enters the Consent Token Response to Product client. The privileged access will be enabled if the response signature verification is successful.

The employee provides the response to the Consent Token device client, which uses public-key cryptography to verify and unlock the device

Figure 6. Consent token for secure shell access

Random Number Generation and Entropy Source

Strong random number generation (RNG) is at the core of encryption, while weak RNG can undermine the entire encryption system. Random number generators play a key role in creating cryptographic keys, establishing highly secure communications between users and websites, and in resetting passwords for email accounts. Without assured randomness, an attacker can predict what the system will generate and undermine the algorithm. Cisco Nexus 9000 switches uses the RNG from Linux. The RNG is seeded with a random value, typically obtained from a hardware random number generator (HRNG), which makes it impossible to guess. Hardware also contains a Trust Anchor module that is compliant with NIST specifications and capable of providing much more effective RNG that extracts entropy from a true random source within the Trust Anchor.

© 2023 Cisco and/or its affiliates. All rights reserved.

Multistage BIOS

The BIOS is split into multiple, smaller pieces so that they can be loaded, validated, and executed entirely in the RAM to protect the BIOS from external modification (such as a Time-of-Check to Time-of-Use attack[1]). The BIOS is composed of the following things:

- Pre-EFI Initialization (PEI)
- Firmware Dependency Module (FDM)
- Driver Execution environment (DXE)

Having a multistage BIOS in Cisco Nexus OS switches makes it very hard to bypass the Cisco BIOS. Any intervention with the BIOS will stop the bootloader from loading the NXOS image.

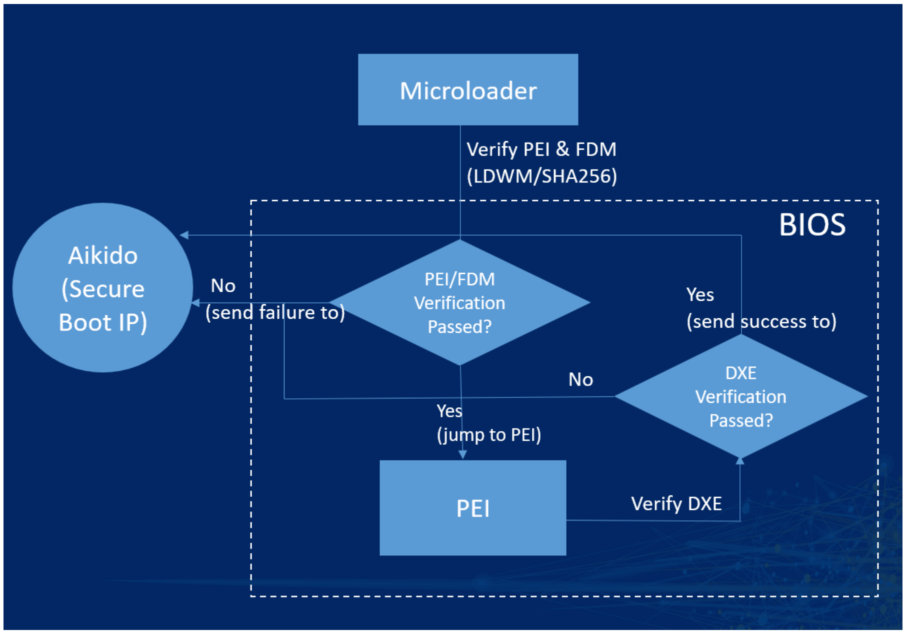


Figure 7. Multistage BIOS

Runtime Defenses (RTD)

Runtime defenses target injection attacks of malicious code into running software. Cisco Nexus 9000 switches runtime defenses include Address Space Layout Randomization (ASLR), Built-in Object Size Checking (BOSC), and X-space Runtime defenses. These defenses make it harder or impossible for attackers to exploit vulnerabilities in running software.

Address Space Layout Randomization (ASLR)

Address Space Layout Randomization (ASLR) is an important security hardening functionality that randomizes the locations of sections of all processes and the kernel for Cisco Nexus 9000 switches to

[1] A Time-of-Check to Time-of-Use (TOC/TOU) attack is a type of race condition vulnerability that occurs when a program checks a condition and then performs an action based on the result of that check. However, if another program modifies the condition between the time of the check and the time of the use, the action will be performed based on the modified condition, which could lead to unintended consequences.

© 2023 Cisco and/or its affiliates. All rights reserved.

make it more difficult for an attacker to exploit existing vulnerabilities. ASLR is a companion defense along with executable space protection, which prevents inadvertent execution of code from unauthorized areas and prohibits writing of code over executable areas.

ASLR functionality for processes can be categorized into Cisco binaries and 3rd party binaries, both of which need to support ASLR. For ASLR support, Cisco and 3rd party binaries and shared libraries need to be built with the correct flags. Cisco binaries including 3rd party shared objects must ensure the library is randomized so as not to compromise the randomization of the Cisco binary itself. 3rd party binaries and shared libraries might require vendor support to randomize them.

ASLR functionality for the Linux kernel brings support for address space randomization to running Linux kernel images by randomizing where the kernel code is placed at boot time. Kernel ASLR support is present in Cisco Nexus switches, making it hard for the hackers to perform malicious code injections.

Executable Space Protection (XSpace)

Executable space protection (X-space) is one of the most important security protections in Cisco Nexus switches. This feature ensures that executable space protection is enabled for Cisco Nexus gear, which prevents the execution of code from unauthorized areas and prohibits writing code over executable areas. X-space makes Cisco Nexus gear more robust at preventing hackers from penetrating into the switches.

Object Size Checking (OSC)

Buffer overflow is probably the best-known form of software security vulnerability. A buffer overflow condition exists when a program attempts to put more data in a buffer than the buffer can hold, or when a program attempts to put data in a memory area past a buffer. In this case, a buffer is a sequential section of memory allocated to contain anything from a character string to an array of integers. Writing outside the bounds of a block of allocated memory can corrupt data, crash the program, or cause the execution of malicious code. Nexus switches have full protection to determine buffer overflows in C/C++ code by having object size checks before a write call.

SafeC Libraries

Nexus software uses efficient library functions that promote safer, more secure C/C++ language programming and are based on the ISO/IEC 9989:2011 (C11) specification. Several standard C library functions are susceptible to vulnerabilities that can serve as launch points for more sophisticated attacks. While providing " safe" replacements for standard functions in a consistent naming schema, SafeC aims to mitigate security exploits due to buffer overflows, provides bound checks that may not be present in the native library, and prevents string termination and truncation errors. This SafeC safeguards Cisco Nexus 9000 hardware from buffer overflow attacks.

Cisco Signed Kernel Modules

Signed Kernel Modules ensure that any kernel modules loaded into the system are authentic and unmodified. This prevents unapproved and untrusted executable code from being loaded into the kernel by conventional means.

If the modules are not signed by Cisco, then they cannot be used with the Cisco Nexus OS. This feature stops unauthorized software from running on Cisco Nexus gear. All these hardening features make the Cisco Nexus OS and its peripheral components difficult to hack.

Secure JTAG (sJTAG)

JTAG was also adopted to program FPGAs and provide a CPU debug access port. A laptop and a JTAG debugger are often all that is required to provide access to an embedded CPU allowing for retrieval of

© 2023 Cisco and/or its affiliates. All rights reserved.

firmware images, dumping memory, and monitoring software execution. A small size interface coupled with a sophisticated toolset gives attackers a portable yet powerful means to exploit a system.

By having a secure JTAG on Cisco Nexus gear, we can mitigate intellectual property (IP) theft and avoid the stealing of passwords or keys from the memory.

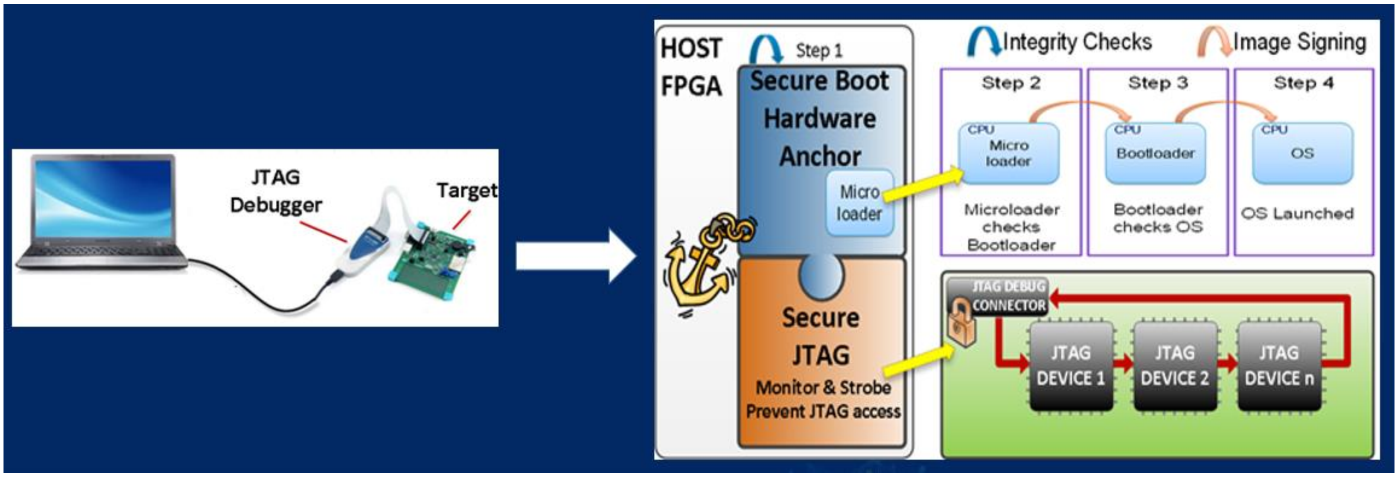


Figure 8. Secure JTAG

Secure Erase

The secure erase feature erases all customer information within Cisco Nexus 9000 switches. Secure erase is an operation that removes all the identifiable customer information in Cisco NX-OS devices for purposes of product removal due to Return Merchandise Authorization (RMA), upgrade or replacement, or system end-of-life.

- Return Material Authorization (RMA) for a device: If you must return a device to Cisco for RMA, remove all customer-specific data before obtaining an RMA certificate for the device.
- Recovering a compromised device: If the key material or credentials that are stored on a device are compromised, reset the device to the factory configuration, and then reconfigure the device.

Conclusion

Cisco's Nexus 9000 switches are fortified with a robust suite of trustworthy technologies that ensure the highest level of security. These technologies, including Secure Boot and the Cisco Trust Anchor Module (TAm), establish an unbreakable chain of trust, guaranteeing the authenticity and integrity of running software. The Secure Unique Device Identifier (SUDI) and consent token mechanisms thwart counterfeiting and provide controlled access, while advanced features such as random number generation, multistage BIOS, and secure erase ensure data privacy and system resilience. This comprehensive approach equips customers with an unparalleled level of protection, making Cisco Nexus 9000 switches an excellent choice for safeguarding their network infrastructure in data centers.

The availability of these features varies depending on the Cisco Nexus OS and the model of the switch hardware. Please contact your Cisco representative for more information.

References

Cisco Trustworthy Technologies Data Sheet

© 2023 Cisco and/or its affiliates. All rights reserved.