A Trustworthy Framework for Cisco 8000 Series Routers

Building secure networks with hardware designed to handle threats and attacks

Securing the underlying infrastructure is key

Networking is evolving because of the rising tide of bandwidth generated by ever-increasing demand from users, devices, and applications. To address network growth, operators around the world are considering network architectures with an emphasis on scale, latency, resiliency, automation, and security. As operators expand their networks, security is taking on greater importance. As network infrastructure resources become more dispersed, operators need to have tighter control over the resources to better serve their customers. Securing the network is paramount because service providers operate critical infrastructure that supports healthcare, finance, utilities, and governmental systems. If the network for any, or all, of these sectors were subject to a cyberattack, the effects could be catastrophic and crippling to operations and even the economy.

Contents

As networks grow, so does their threat exposure

With the current advances in the Internet of Things (IoT) and the availability of network infrastructures, more devices are going online. According to the Cisco Visual Network Index (VNI), by the year 2022 there will be 4.8 billion global Internet users. At the same time, around 26 billion network devices will be connected and 82% of all IP traffic will be video.[1] In addition, Mind Commerce projects that by 2020 two billion personal devices (bring your own device or BYOD) will be in the workplace.[2]

With all of that growth, it will be challenging to build secure networks unless the underlying infrastructure hardware is built to handle and circumvent the threats and attacks. Each device added to the network creates another point of vulnerability. To support the rapid growth in 5G deployments, infrastructure elements are being deployed in more diverse and sometimes less secure locations, which creates additional risk.

In the Cisco 2018 Annual Cybersecurity Report, evidence shows that cyberattacks are more sophisticated in nature and have more significant financial impacts. Recent cyber breaches have demonstrated how hackers exploited software vulnerabilities and were able to steal millions of dollars, permanently erase computer data, or hack into corporate networks to steal valuable consumer information.[3] The Cisco 2018 Security Capabilities Benchmark study revealed that more than half (53 percent) of all attacks resulted in financial damages of more than US $500,000.[4] The extent of damages goes beyond the financial. Businesses have lost customers and partners and damaged their reputations along with their ability to capture new opportunities.

The Cisco 2018 Annual Cybersecurity report also points out that cybercriminals are exploiting supply chain vulnerabilities to replace hardware components or software. Cybercriminals could act from within the network from day one, potentially with full access to sensitive data sets. Operators need to expand their security policies to review hardware and software vulnerabilities that could arise during the manufacturing and supply chains. The impact of supply chain attacks can be quite massive and remain undetected for a long period of time.

To curb supply chain attacks, operators need to work with vendors who issue Common Vulnerabilities and Exposures (CVE) reports and have a comprehensive supply and value chain security program to protect their systems from compromise. Vendors must also be capable of quickly addressing any system-level vulnerabilities and provide ways for service providers to validate the integrity of the hardware against malicious code.

Cisco 8000 Series Routers

The Cisco 8000 Series Router (8000 Series) is the foundational routing device to support the next evolution of the Internet, and Cisco has addressed security throughout the entire development cycle of the product. We have led the industry with a secure development using the Cisco Secure Development Lifecycle (CSDL). With CSDL, Cisco products have security features embedded throughout their product lifecycle and have resiliency against today's sophisticated manufacturing supply chain attacks.

Cisco routers are designed with foundational security capabilities that verify devices for authenticity and integrity. This verification offers evidence that network devices are operating as intended and are unaltered from their manufactured state. The idea is similar to design for testability (DFT) and design for manufacturability (DFM). From concept to production, Cisco routing platform products are based on a trustworthy framework, and now the Cisco 8000 Series uses this established methodology as well.

Cisco trustworthy framework

The trustworthy framework addresses security at every phase of the product lifecycle, from concept to end of life. The framework explores the following concepts:

- What is the product's threat model?
- What attack vectors are specific to this product?
- What measures can be taken to make this product robust and threat resistant?
- What is the product's security operational model?
- What type of security measures need to be provisioned? (For example, pre-boot, post-boot, runtime, and supply chain security.)

A critical step in designing resilient networking solutions is to design hardware from the outset with embedded security features. Cisco uses a Trust Anchor module chip that implements a number of security features in a standards-based way. The Trust Anchor module is used to enable the following security features in the Cisco 8000 platform:

- Secure boot and image signing
- Run-time defenses
- Supply chain security (Cisco Chip Protection)

The first step in establishing platform security is platform identity, which is performed using the Trust Anchor module (TAm). The TAm is similar to the Trusted Platform Module (TPM) from the Trusted Computing Group, which was accepted as a standard by ISO and IEC in 2009. Originally developed to protect against counterfeiting and supply chain attacks, the Trust Anchor module is

a tamper-resistant chip that provides secure on-chip storage, random number generation for encryption, and a secure unique device identity for authentication.

During manufacturing, device identification is programmed into the TAm using a Secure Unique Device Identification (SUDI), an X.509 certificate that is globally unique per device. SUDI is an extension of device identity as defined by the IEEE 802.1 working group. The 802.1 AR standard defines a secure device identifier as a cryptographic identity that is bound to a device and used to assert device identity. SUDI is permanently programmed into the Trust Anchor module and logged by Cisco manufacturing and is used for device authentication purposes. Cisco has a secure business-to-business network with its silicon, software, and manufacturing partners to exchange critical system information such as SUDI between suppliers and the Cisco back-end process.

Cisco secure boot and UEFI secure boot

With the TAm storing critical device identity information, the first priority becomes to begin device authentication at boot time. The hardware-anchored secure boot process is designed to ensure that only genuine, unmodified code is allowed to boot on the Cisco 8000 Series platform. It is anchored in hardware using the information in the Trust Anchor module to provide a robust security framework built on a hardware root of trust. With the establishment of root of trust, secure boot monitors all stages of the boot process.

At boot time the secure boot process authenticates a micro-loader, bootloader, and the bootloader authenticates the operating system. The micro-loader is encrypted and signed by Cisco private keys, with the private key information being stored in the Trust Anchor module. The bootloader and operating systems have digital signature information stored in the TAm as well.

This process creates a chain of trust from the micro-loader to the operating system, which establishes the software authenticity and integrity. All of these signatures are verified using keys that are securely stored in the Trust Anchor module at manufacturing time. This verification ensures the authenticity of hardware and software during boot time, which prevents hardware and software counterfeiting. If any of the digital signature checks fail, the Cisco device will not allow the software to boot.

Extending trust to run-time applications

After the verification of all the steps in the boot sequence, it is crucial to extend the integrity verification to run-time applications. The integrity measurement architecture (IMA) is intended to assure that executables preparing to load have not been modified from their original form. IMA maintains a run-time measurement list and anchored in the TAm, an aggregate integrity value over this list. The benefit of anchoring the aggregate integrity value in the TAm is that any software attack on the measurement list would be detectable. On a trusted boot system, IMA can be used to attest to the system's run-time integrity.

IMA can work in two modes:

- Logging mode: The system logs a message if the appraisal fails.
- Appraisal mode: The system blocks applications if the appraisal fails.

In the Cisco 8000 series, the IMA signatures for all applications will be included in the routing processor modules for IOS XR packages.

Trusting hardware components in critical infrastructure

With processes working to ensure only genuine software and code can run within a Cisco device, the next layer to protect is the JTAG interface of the components of those devices. Most embedded devices provide a JTAG interface for debugging purposes. However, if left unprotected, this interface can become an important attack vector on the system.

JTAG refers to the IEEE 1149.1, Standard Test Access Port and Boundary Scan Architecture. Silicon devices that are IEEE 1149.1-compliant may be connected together on a PCB to form a scan chain, which is typically driven by external test equipment or a debugger. The original application for JTAG was to be used by manufacturing to validate PCB wiring and IC functionality in an effort to improve quality. JTAG has also been adopted to program Field Programmable Gate Arrays (FPGAs) and to provide a CPU debug access port. Most CPU vendors including Intel, Freescale, Marvell, and AMD, allow for a debugger to be connected to the CPU's JTAG port to assist with code debugging.

Using JTAG to provide a CPU debug access port presents a security risk. A laptop and a JTAG debugger are all that is required to provide access to an embedded CPU. An attacker can then retrieve firmware images, dump memory, and monitor software execution. The small size coupled with a sophisticated tool set gives attackers a portable and yet powerful way to exploit a system. Potentially malicious uses of JTAG include:

- Intellectual property theft. It is easier to reverse engineer than perform static binary analysis.
- Counterfeiting. Reverse engineering of anti-counterfeit mitigations and licensing schemes or modification of firmware to circumvent licensing.
- Embed malware. Can be performed statically or dynamically (dynamic can evade image signing).
- Theft of secrets. Private or symmetric cryptographic keys can be retrieved from memory, or passwords can be retrieved from memory.

While this attack vector may seem far-fetched, counterfeit Cisco products have been examined and found to contain modified software images that were designed to circumvent protections. Although the exact tools and techniques of real-world attacks are often unknown, JTAG makes it significantly easier to reverse engineer, modify, and test software. A proof-of-concept attack was demonstrated by a German university team who used the JTAG interface on Cisco routers to monitor memory during run-time operation to extract private information.

To combat these attacks, the Cisco IP Secure JTAG monitor and strobe function is a specialized logic block that is designed to prevent the use of JTAG debuggers to probe and modify CPU memory contents. Secure JTAG both monitors the JTAG bus for activity and also periodically checks the continuity of the JTAG chain during run-time operation. When unauthorized activity is detected or the chain integrity is compromised, the host system is notified, and corrective action is taken by the host.

Cisco Chip Protection for embedded silicon

Attacks on supply chains include the replacement of application specific integrated circuits (ASICs) with ASICs containing trojans or malware code. For hackers to complete an attack of this magnitude would require physical help during the manufacturing process. Some people have theorized that agencies influence CPU and ASIC vendors to get them to put trojans onto chips.

Learn more

To learn more about the Cisco 8000 Series Routers, please visit the 8000 Series product page.

To learn more about the Trustworthy hardware, please visit the Built-in-Trust page.

Other people have suggested that a trojan might be added to silicon while on board the assembled hardware unit. Cisco Chip Protection helps mitigate this threat with the use of unique identifiers stored inside the Trust Anchor module as a way to identify and track components through the product lifecycle.

Cisco Chip Protection is applicable to all field replaceable units (FRUs). An imprint database is a master list within the Trust Anchor module that stores the unique identification of Cisco ASICs, CPUs, systems on a chip, and other devices with their device types specific to a board. In most cases, the unique identification is device serial number or appropriate value of that device. The imprint database is a known good values database unique to the board it is loaded on, and it is used by the authentication process to validate the components. These values are programmed on to a Trust Anchor module during the manufacturing process, similar to the SUDI and secure boot processes.

Observed component identifications are collected by firmware every time the board is booted and is measured against the imprint database in the Trust Anchor module. If the observed identification does not match the imprint database, then it is an indication of breach and is reported into the host for appropriate action.

Keep the network safe

Cybersecurity is a growing challenge for service providers across the globe who want to offer trustworthy networks for critical infrastructure services. Cisco has taken unprecedented steps to address this challenge using its trustworthy framework based upon the Cisco Secure Development Lifecycle. Security is the cornerstone of our development strategy, and the Cisco 8000 Series includes built-in features that allow only verified authentic components, software, and hardware to operate. With these built-in-security features, the Cisco 8000 Series Router family is ready to circumvent security threats and keep the network resilient against today's sophisticated manufacturing and supply chain attacks.

1. Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper
2. BYOD in Enterprise Applications and Cloud Environment: Market Challenge and Opportunity Analysis 2015 – 2020
3. Cisco 2018 Annual Cybersecurity Report
4. Cisco 2018 Annual Cybersecurity Report Reveals Security Leaders Rely on and Invest in Automation, Machine Learning and Artificial Intelligence to Defend Against Threats