White paper
Cisco public

What Do Cable Operators Need to Know about Trust?

Why trust matters in cable networks

Cable operators can’t grow market share without a foundation of trust

Today, cable operators and multiple system operators (MSOs) have some of the most dense and farthest-reaching networks. The companies operating these networks have the potential to reach the growing Internet of Things (IoT) and upcoming 5G markets. The ability to capture market share by supporting this expansion depends on the ability for MSOs to demonstrate that their networks can transport sensitive data sets without being compromised. MSOs must ensure that their network infrastructure is safe from attack, and trust is the key. Every component of their critical infrastructure must be authentic, so untrustworthy hardware can’t become rooted in ways that could jeopardize customer data, services, and reputation. To achieve this level of security, networks must be built with trust from the inside out.

Contents

What's the risk?

Trusted networks require trusted infrastructure

Because software can lie

How Cisco delivers trust for MSOs

Trust, but verify

The need for trusted platforms

Learn more

What's the risk?

Today's network infrastructures are under threat, and essential services and customer data must be protected. Sophisticated actors are looking to silently gain access and compromise network services and customer data. These actors are well-funded, persistent; they work to silently hijack network infrastructure components to establish a persistent foothold in the network. They can take control of network assets to affect traffic flows, enable surveillance by rerouting traffic, or mirror traffic to remote receivers.

Attacks on network infrastructures are no longer theoretical. Since 2015, the United States Computer Emergency Readiness Team (US-CERT) and other entities have seen more attempts and attacks on network infrastructure elements. Infrastructure attacks have been able to disrupt Internet traffic in Europe, Asia, Latin America, and the United States. You should assume that the attackers are motivated, and have access to "zero-day" vulnerabilities in existing network operating systems from all vendors. Although MSOs already perform the required patching, secure operations, and recommended hardening, any infrastructure could potentially be under threat from unknown vulnerabilities or exposed interfaces, which never can be 100 percent covered. An innovative approach to protecting critical infrastructure is needed.

Trusted networks require trusted infrastructure

Today's network backbones are the critical infrastructure for the successful operation and growth of not only enterprises, but also a nation's economy. Without access to high-speed connections and the trust that those connections are secure, business operations and transactions would halt. The only way to deliver a secure network is to establish trust in the core infrastructure. A trusted system is based on clear criteria, which can be measured, verified, reported, and audited.

A trusted network component must provide assurance that:

- The hardware running your network is authentic and that processes are in place to protect network devices from corruption and modification.
- The network operating system and its associated services are trusted and haven't been modified.
- The management of the network device is properly authenticated and audited.
- Any secrets stored within the network device can't be extracted or changed without authorization.

Because software can lie

Software relies on its firmware and hardware for validation, and software reports back whatever it's told by that underlying architecture. Existing practices of verifying software through hashes and code signatures are an important part of establishing a trusted system, but software systems can be affected or compromised by the underlying architecture. For instance, a known-good application can't be trusted if the underlying operating system doesn't maintain effective protection and sandboxing of that process. Similarly, an operating system can be compromised through attacks based in the firmware or the underlying hardware.

Attacks on the underlying hardware or firmware of a system are commonly used to establish persistence in compromised systems after a breach. Often, they're designed to persist even after an operating system has been reinstalled. Examples of these types of attacks include hypervisor-based attacks such as "Blue Pill", which can invisibly compromise the running operating system (OS) kernel. And attacks such as "ThunderStrike" have already demonstrated persistent compromise through firmware.

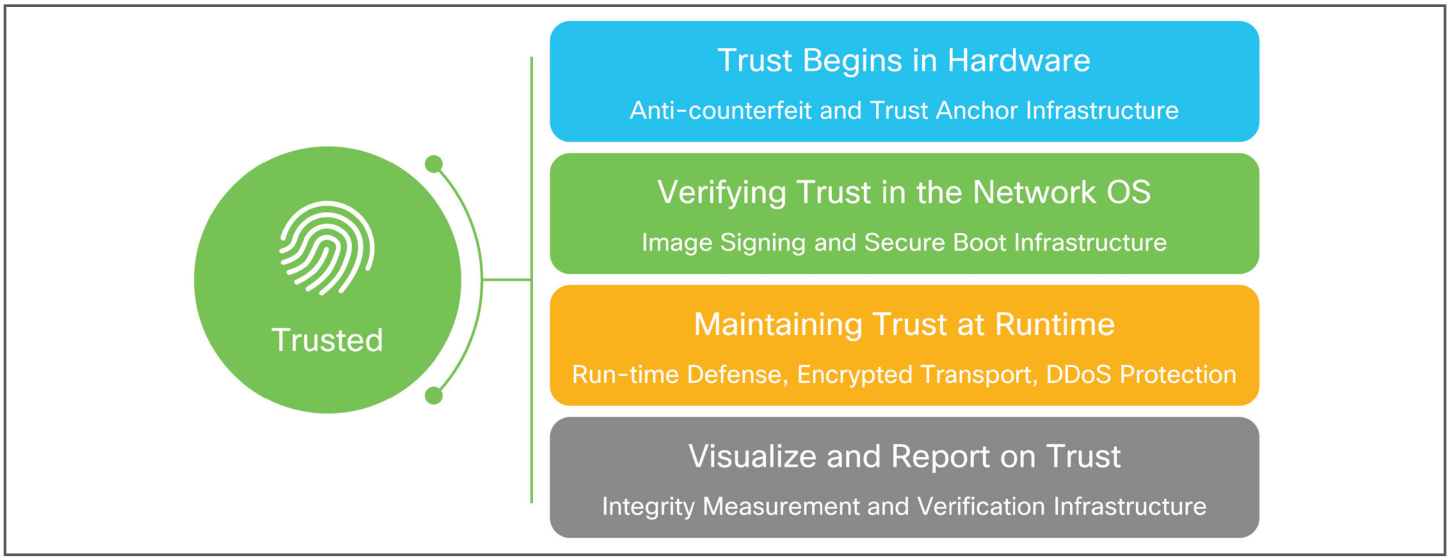
Trusted infrastructure must be based in trusted hardware

Because software alone can't prove its integrity, truly establishing trust can only be done in hardware, using a hardware root of trust. To be effective, this root of trust must be based on an immutable hardware component that establishes a chain of trust at boot time. Each piece of code in the boot process measures and checks the signature of the next stage of the boot process before the software boots. Without a hardware root of trust, no amount of software signatures or secure software development can protect against a compromise of the underlying system.

How Cisco delivers trust for MSOs

As MSOs work to further monetize their HFC Networks and evolve them from analog to digital elements, they need to decide how they will scale services in the future. Migrating from analog to digital will require new hardware and interfaces throughout the cable access network for interconnectivity. With this transition, MSOs have an opportunity to build an end-to-end foundation

Figure 1. Trusted network.


Trusted
Trust Begins in Hardware
Anti-counterfeit and Trust Anchor Infrastructure
Verifying Trust in the Network OS
Image Signing and Secure Boot Infrastructure
Maintaining Trust at Runtime
Run-time Defense, Encrypted Transport, DDoS Protection
Visualize and Report on Trust
Integrity Measurement and Verification Infrastructure

of trust in the network. Being able to authenticate the hardware from the edge back to the core will help reduce the exposure of the MSO's distributed infrastructure.

Cisco leads the industry for building in the capabilities to establish, verify, and measure trust in our products and in the critical network infrastructures we support. We provide both hardware and software with embedded security features and a secure device identity that builds a trusted network. For us, establishing trust begins in our supply chain by ensuring our supply chain doesn't have vulnerabilities and that a secure boot process readily validates the firmware and components when you power the unit on.

Trusted hardware and supply chain

Maintaining control over the hardware components and the underlying supply chain behind the hardware product lifecycle is the key to establishing and maintaining a trusted networking device. Cisco has extensive controls and processes in its hardware supply chain management. These controls are designed to detect and prevent counterfeit hardware or unauthorized modifications to components within Cisco hardware products. Effective supply chain management answers the question: "How do I know this is authentic and trusted hardware?" and "How do I know that the hardware root-of-trust is authentic?"

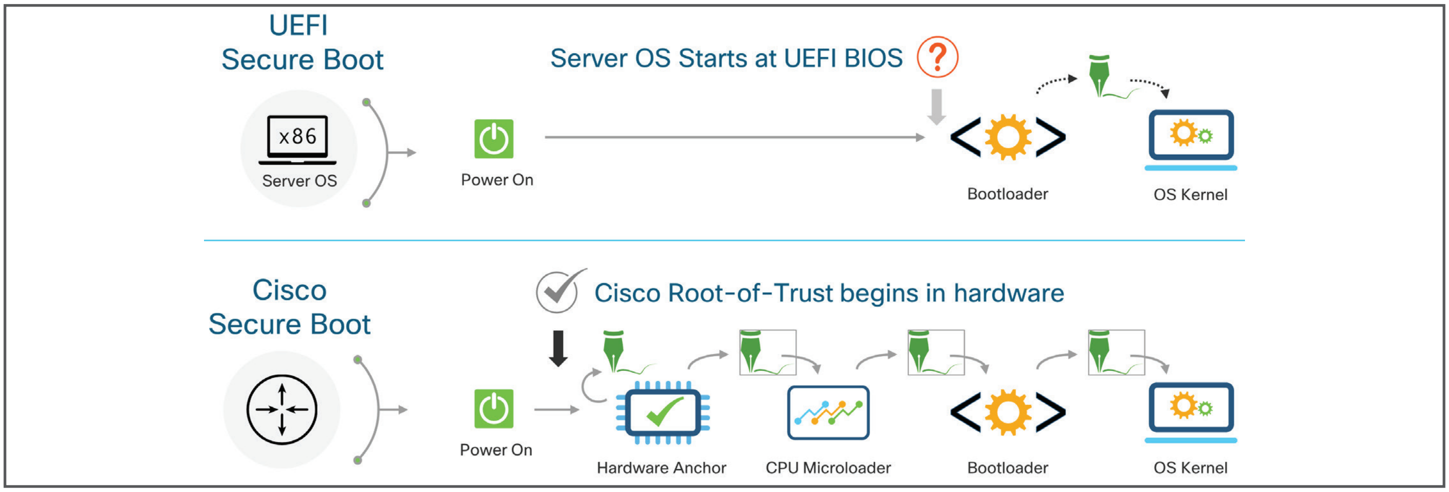
Hardware root-of-trust and secure boot

Many Cisco service provider routers use signed images and hardware-anchored secure boot to prevent inauthentic or compromised code from booting. Anchoring the first code in the boot sequence in hardware establishes a chain-of-trust and is the foundation of the Cisco secure boot process.

Secure boot is already a familiar term in the world of x86 servers. It's used to cryptographically verify the authenticity of the operating system (OS) boot loader and the OS kernel as part of the boot process. Secure boot is commonly used to protect against boot-kit attacks in server OSs like Linux or Microsoft Windows Server. In traditional x86 server systems, this secure boot process begins in UEFI BIOS and doesn't have a hardware root of trust or trust anchor.

Cisco's IOS XR software includes a more extensive boot process that is designed around a hardware trust anchor. This process begins before the CPU is allowed to boot and offers significant protections against hardware or firmware compromises. The Cisco IOS XR secure boot process establishes an extensive chain of trust that begins in hardware. The hardware anchor implements self-measurement, followed by measurement and signature verification of the CPU microloader. It then verifies the signature of the bootloader and the OS kernel.

Figure 2. Secure boot.



Secure hardware for strong cryptography

Cisco also uses a Trust Anchor module (TAm) which provides a secure unique device identity (SUDI) and other services. Within Cisco IOS XR, the TAm also provides critical cryptographic services such as:

- Unique cryptographic hardware identity (SUDI)
- Compliance with NIST SP 800-90B entropy source using a hardware random number generator
- Secure generation and storage of secret key material

Hardware root-of-trust is an industry best practice

Cisco leads the network industry in establishing trusted systems, but our approach isn't unique because security is an industry-wide challenge. Other industry-leading infrastructure providers use a similar hardware-based approach to establish a root of trust for their own trusted computing hardware such as Google Titan and Microsoft Olympus.

Trust, but verify

"Trust but verify" isn't just a proverb. It's critical to verify hardware, firmware, and software components of a system at boot-time to establish trust, but it's equally important to provide visibility and audit capabilities for trusted systems. Secure boot processes can provide valuable protections against compromise of the OS or underlying components, but once it's complete there needs to be an external reporting system that can prove a non-compromised environment. Trusted systems require effective measurement and trust posture reporting from external systems, where measured values from the system can be compared against "known-good values" (KGV) for that system.

Secure measurement

Hardware root-of-trust is critical to establishing trust in a critical system. MSOs should require that networking devices include access to external mechanisms that securely record and store measurements taken during the boot process. Hardware values measured during a system boot should be securely recorded into the configuration. These values can then be used as cryptographic proof that the system hasn't been compromised. MSOs are well positioned to support 5G and IoT services by leveraging their dense infrastructure. With externally validated trust anchor measurements, MSOs can prove the integrity or trust of their infrastructure systems.

In addition to secure boot processes, secure measurement can be extended to individual processes within the OS at run time. It can be important to extend trust measurements to the run-time environment to allow for comparisons against baselines. Cisco IOS XR software uses advanced capabilities to measure processes and critical files at run time. It then compares these measurements against known-good values (KGVs) of the IOS XR build process.

Maintaining trust throughout the network infrastructure requires an external service that can compare all measurements to known-good values (KGV) for boot integrity or individual process measurements. By providing secure measurement and reporting of measurements, a trusted system can enable remote attestation or the ability to cryptographically prove that measured values are accurate. It compares these values to known-good values on an external system. This approach provides visibility, trust posture assessment, and auditing of trustworthy systems.

Evaluating your vendors for secure software development practices

As establishing and maintaining trusted systems to power critical network infrastructure becomes a requirement in all carrier networks, it's important to consider how network hardware and software vendors manage their supply chain and development process. No amount of hardware trust verification helps if malicious code is inserted into the network operating system as part of the software development process. It's crucial to examine how your vendors implement secure development practices as well as the secure management and build processes of the network operating system.

It's important to consider how vendors balance maintaining secure software development with build practices, especially when custom production code can be developed outside of secure facilities in distributed environments.

The Cisco Secure Development Lifecycle (CSDL) is a repeatable and measurable process that is designed to increase Cisco product resiliency and trustworthiness. The combination of tools, processes, and awareness training introduced throughout the development lifecycle enhances security, provides a holistic approach to product resiliency, and establishes a culture of security awareness.

Security is a core part of the Cisco development process and includes:

- Product security requirements
- Management of third-party code
- Secure design processes
- Secure coding practices and common libraries
- Static analysis
- Vulnerability testing

Building on trust

Although the topic of secure services built on a trusted network infrastructure is beyond the scope of this white paper, trusted systems also supply mechanisms for secure key management and key storage using the hardware root of trust. Key management and storage provide a secure foundation for other security services built on the network infrastructure.

As requirements for additional data plane encryption services such as MACsec or IPsec and stronger authentication for control plane routing protocols increase, the requirement to securely store key material in a way that can't be compromised or extracted becomes increasingly important. As the proliferation of MSO access devices grows to meet the demand growth in 5G mobile backhaul networks, larger number of MSO access routers will be deployed in unsecured locations. This situation drives the need for secure automated provisioning tools and protection for keys against theft or compromise. Providing these secure services will require trusted platforms with hardware-rooted trust models and effective visibility and remote verification of trust.

The need for trusted platforms

In the current landscape of advanced, well-funded, and motivated adversaries, it's not enough to just keep software up to date and employ current best practices for hardening network devices. Attackers are seeking longer-term compromises in systems and using effective trade craft to compromise and silently persist within critical infrastructure devices. So the next step to secure your infrastructure involves building on a foundation of trusted platforms. We believe that establishing, maintaining, and verifying trust within network infrastructure devices and throughout Cisco IOS XR is the most effective strategy to deliver a trusted and secure digital network infrastructure.

Learn more

To learn more about Cisco trust factors for more secure networks, visit the Cisco Trust Center page.