Building Trustworthy Network Infrastructure

Rakesh Kandula
Technical Marketing Engineer, Cisco Systems

16th October 2023
About Me

• Technical Marketing Engineer @ Cisco

• 16+ Years in Cisco

• Current Focus Areas
  • Trustworthy Systems
  • Platform Security Chips
  • Secure Boot
  • Post Quantum Security
  • DDoS Solutions, etc.

• Outdoor enthusiast & marathoner who loves trail ultras
“People need stories in order to cooperate, and they can change the way they cooperate by changing the stories they believe”

Yuval Noah Harari
Agenda

1. Service Provider Security Concerns
2. Trustworthy Platforms – Challenges & Solutions
3. Strengthening Operational Security
Threat Landscape For Service Provider Networks

Deployment Challenges For Service Providers

- Untrusted Remote Locations
- Support Critical Infrastructure
- Global Scale

Impact of Attacks on Service Providers

- Loss of Revenue
- Brand Reputation Loss
- Impact to SLAs
- Legal Implications
Threats to Network Devices – Layered View

NOS

- Integrity Visibility (Boot & Run-time)
- NOS Runtime
  - (Maintain Trust at Run-time)
- BSP & Linux Kernel
  - (Establish Trustworthy NOS)

RP BIOS  LC BIOS

X86 - CPU
- (Establish Trust in Hardware)

Protection against

- Ransomware
- MitM attacks
- Credential Theft
- Known Vulnerabilities
- Malware Attacks
- Boot Vulnerability
- Malware Attacks
- Compromised Hardware
- Counterfeit Hardware
Trustworthy Platforms Overview

- Trust Begins in Hardware
  - Ensuring Hardware Integrity

- Enabling Trust in the Network OS
  - Ensuring Integrity of the Boot Process

- Maintaining Trust at Runtime
  - Run-time Defenses, Data Protection, DDoS Protection

- Visualize and Report on Trust
  - Continuous Posture Evaluation
Components of Trustworthy Platforms

Hardware Integrity
Ability to detect counterfeit hardware and act as a trust anchor

Boot Integrity
Ensuring integrity of the boot process

Runtime Integrity
Ensuring the integrity of the NOS runtime

Trust Visibility
Providing visualization of Trust
Components of Trustworthy Platforms

**Hardware Integrity**
Ability to detect counterfeit hardware and act as a trust anchor

**Boot Integrity**
Ensuring integrity of the boot process

**Runtime Integrity**
Ensuring the integrity of the NOS runtime

**Trust Visibility**
Providing visualization of Trust
Tampering of Critical Components

- Increase in Supply Chain Attacks
- Increasing attempts to put Trojans on Chips

- CPU Integrity
- ASIC Integrity
- Detect in-transit tamper
- Validate Mission Critical Components
Counterfeit Hardware & Unique Hardware Identity

1. Counterfeit hardware from illegal markets.
2. Tampered hardware sold in resale markets

1. Ability to cryptographically identify a device uniquely
2. Adoption of secure & standards-based device onboarding / enrollment
Solutions To Ensure Hardware Integrity

A tamper-proof, cryptographic unique identity to establish hardware identity remotely

A platform security chip to ensure integrity of critical hardware components

Ability to detect tampering, built-in crypto functions, providing entropy for RNGs, etc.

Ability to support remote attestation (identity challenge-response, boot measurements, etc.)
Components of Trustworthy Platforms

**Hardware Integrity**
Ability to detect counterfeit hardware and act as a trust anchor

**Runtime Integrity**
Ensuring the integrity of the NOS runtime

**Boot Integrity**
Ensuring integrity of the boot process

**Trust Visibility**
Providing visualization of Trust
Attacking the Boot Sequence

1. Changing the boot interface
2. Booting from alternate device
3. Bypassing Integrity checks
4. Adding persistent code
Ensuring Boot Integrity

Secure boot anchored in an immutable hardware root of trust must be mandatory

Ability to validate boot artifacts and record boot measurements inside a TPM or similar security chip

Ability to prevent an adversary from disabling secure boot

Ability to prevent revoked images from booting (image downgrade protection)
Components of Trustworthy Platforms

- **Hardware Integrity**: Provides counterfeit hardware protection and act as a trust anchor.
- **Runtime Integrity**: Ensure integrity of the NOS runtime.
- **Boot Integrity**: Ensures integrity of the boot process.
- **Trust Visibility**: Provides visualization of Trust.
Runtime Integrity Challenges

1. Detecting tampering of Network Operating System (NOS) after secure boot process.
2. Ability to prevent processes from accessing unauthorized resources.
3. Ensuring the integrity of files before a process executes.
4. Preventing unverified 3rd party applications from running on the routers.
Maintaining Trust at Run-time

Application Containment and Policy

**SELinux**
- A Mandatory Access Control (MAC) facility built into the Linux Kernel
- Protection from malicious or misbehaving compromising the system

Integrity Visibility and Secure Measurement

**Linux Integrity Measurement Architecture**
- All processes executed by the kernel are securely measured and reported
- Kernel checks process signature to prevent unsigned code from executing
Linux Integrity Measurement Architecture (IMA)

IMA Logging

• IMA which ensures every file loaded during runtime goes through a measurement / appraisal
• Kernel must have the ability to measure and verify the signature and extend the PCRs in TPM chip
• IMA violations must be logged in audit.log

IMA Log: /sys/kernel/security/ima/ascii_runtime_measurements
Components of Trustworthy Platforms

- **Hardware Integrity**: Provides counterfeit hardware protection and act as a trust anchor
- **Runtime Integrity**: Ensure integrity of the NOS runtime
- **Boot Integrity**: Ensures integrity of the boot process
- **Trust Visibility**: Provides visualization of Trust
Trust Visibility Components

1. Boot Integrity Visibility (BIV)
2. Runtime Integrity Visibility
3. Remote Attestation Workflow
How to establish Trust?
Boot Integrity Visibility (BIV)
Boot Integrity Visibility (BIV) – Validate Trust

- Measure each boot stage
- Securely store measurements
- Retrieve signed measurements from TPM Chip
- Compare against reference measurements

External service to Verify trust

Attestation

Reference Measurement Database

Validate

Attestation Server

PCR
Remote Attestation Workflow
Remote Attestation Workflow

1. Attestation server securely requests and collects signed evidence from network devices

2. Collected evidence must be verified and added to timeline of running hardware and software

3. Trust data verified against Known-Good-Values (KGV) for hardware and software integrity

4. Dashboard for monitoring the posture of all devices in the network

5. Additionally provide ability for closed loop automation to take actions based on the device posture
What About Operational Security?
Operational Security Focus Areas

User Identity Access
Adopting Passwordless SSH, MFA, AAA controls, etc.

Ownership Establishment
Ownership Vouchers & MASA Service

Data Protection
Data-at-rest protection & data sanitization

Secure Device Onboarding
RFC8572 compliant secure zero touch provisioning of routers

Consent Based Security Features
Additional consent for critical security features

Quantum Security
Challenges posed by Quantum Computers
### User Identity & Access Controls

<table>
<thead>
<tr>
<th>SSH</th>
<th>Multi Factor Authentication</th>
</tr>
</thead>
</table>
| 1. Adopting Password less SSH  
   a) Public-Key based authentication  
   b) Certificate-based authentication | 1. Two-factor authentication for admins accessing the devices |
| 2. Disabling weaker ciphers | 2. Additional consent-based security* mechanism for sensitive features |

<table>
<thead>
<tr>
<th>AAA Controls</th>
<th>Other Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Using dynamic authentication and proper segregation of roles for users</td>
<td>1. Using stronger password hashing mechanisms (Type-8, 9, 10)</td>
</tr>
<tr>
<td>2. Implementing stronger password policies</td>
<td>2. Adopting secure transport methods (syslogs over TLS, SNMPv3, etc.)</td>
</tr>
</tbody>
</table>

*Discussed in later slides
Operational Security Focus Areas

User Identity Access
Adopting Passwordless SSH, MFA, AAA controls, etc.

Ownership Establishment
Ownership Vouchers & MASA Service

Consent Based Security Features
Additional consent for critical security features

Data Protection
Data-at-rest protection & data sanitization

Secure Device Onboarding
RFC8572 compliant secure zero touch provisioning of routers

Quantum Security
Challenges posed by Quantum Computers
Sensitive Data Protection

1. Need data-at-rest protection
2. Full / Partial Disk Encryption
3. Encryption key protected by hardware
4. Support deletion of encryption keys
Data Protection and the missing element

Data At Rest

Data In Transit

Data In Use

And...
Data Protection and the missing element

Data At Rest  
Data In Transit  
Data In Use  
Data Sanitization
Data Sanitization

1. Setup de-commissioning process for data-bearing components
2. Ensure all persistent data storage devices are safely erased
3. Implement an audit process for safe decommissioning of hardware
4. Critical for sustainability initiatives ensuring data protection

Data sanitization must be part of your organization’s data security policies
Operational Security Focus Areas

User Identity Access
Adopting Passwordless SSH, MFA, AAA controls, etc.

Ownership Establishment
Ownership Vouchers & MASA Service

Consent Based Security Features
Additional consent for critical security features

Data Protection
Data-at-rest protection & data sanitization

Secure Device Onboarding
RFC8572 compliant secure zero touch provisioning of routers

Quantum Security
Challenges posed by Quantum Computers
What is Ownership Establishment?

Physical World Example

- Customer purchases a car from a car dealer.
- Car delivered to the customer.
- Customer initiates registration request with the transport authority, providing Chassis S/N and Customer SSN, etc.
- Owner identity verified.
- Customer receives registration card.
- Customer ownership established.
What is Ownership Establishment?

Networking World Example

Purchases a router

Router delivered to customer

Initiate Ownership Voucher request

Receives ownership voucher

Install ownership voucher on the router

Customer Ownership Established

MASA - Manufacturer Authorized Signing Authority

Transport Authority

Chassis S/N

SSN / user identity

Registration Card

becomes

becomes

becomes

becomes

MASA Service

Router S/N

Owner Certificate

Ownership Voucher

Customer

MASA Service
Ownership Voucher (O.V) (RFC 8366)

Yang model for O.V.

```yaml
module: ietf-voucher

yang-data voucher-artifact:
  +---- voucher
      +---- created-on           yang:date-and-time
      +---- expires-on?          yang:date-and-time
      +---- assertion            enumeration
      +---- serial-number        string
      +---- idevid-issuer?        binary
      +---- pinned-domain-cert   binary
      +---- domain-cert-revocation-checks? boolean
      +---- nonce?               binary
      +---- last-renewal-date?    yang:date-and-time
```

- **Serial Number**: Serial number of the router/pledge being bootstrapped
- **Pinned-domain-cert (PDC)**: The owner cert is rooted to the chain of trust leading to the pinned-domain cert. This means PDC can be the root cert for OC or an intermediate cert for OC or the same as OC (self-signed).

Operational Security Focus Areas

**User Identity Access**
Adopting Passwordless SSH, MFA, AAA controls, etc.

**Ownership Establishment**
Ownership Vouchers & MASA Service

**Consent Based Security Features**
Additional consent for critical security features

**Data Protection**
Data-at-rest protection & data sanitization

**Secure Device Onboarding**
RFC8572 compliant secure zero touch provisioning of routers

**Quantum Security**
Challenges posed by Quantum Computers
Security Considerations for Zero Touch Provisioning (ZTP)

**Router/Client Validation**
Server must validate router/client cert (SUDI cert) before offering artifacts/secrets/configs

**Server Validation**
Router/client must validate the server offering artifacts

**Artifact Validation**
The artifact downloaded from the ZTP/Web server must be validated before being loaded/executed
Secure ZTP (RFC8572): Router Validation

SZTP Artifacts (RFC 8572): ZTP Server + Artifact Validation

- Device needs Bootstrapping Data to validate Server and Artifacts
- Order of validation: CIA signature → owner cert → O.V.
- O.V. is signed by vendor, so ultimate trust established by manufacturer / device vendor

CIA contains scripts/configs/redirect-URLs

Conveyed Information artifact (CIA)

CIA signature based on owner cert

Owner cert validated using O.V

Ownership Voucher (O.V)

References: https://tools.ietf.org/html/rfc8572
Operational Security Focus Areas

User Identity Access
Adopting Passwordless SSH, MFA, AAA controls, etc.

Ownership Establishment
Ownership Vouchers & MASA Service

Data Protection
Data-at-rest protection & data sanitization

Secure Device Onboarding
RFC8572 compliant secure zero touch provisioning of routers

Consent Based Security Features
Additional consent for critical security features

Quantum Security
Challenges posed by Quantum Computers
CLI Challenge / Response – Consent Workflow

1) Enable / Disable a feature

2) Generate unique nonce

3) Send nonce for signing

4) Return signed nonce

5) Validate & enable / disable the feature

Network Admin

Network Operator Signing Service

Off-box workflow

On-box workflow

Operator’s Public Key*

Operator’s Private Key*
Operational Security Focus Areas

User Identity Access
- Adopting Passwordless SSH, MFA, AAA controls, etc.

Ownership Establishment
- Ownership Vouchers & MASA Service

Consent Based Security Features
- Additional consent for critical security features

Data Protection
- Data-at-rest protection & data sanitization

Secure Device Onboarding
- RFC8572 compliant secure zero touch provisioning of routers

Quantum Security
- Challenges posed by Quantum Computers
People are making incremental efforts in developing a **Quantum Computer**.

Once they have one which is sufficiently large and reliable, they could use it to **Break Current Encryption!** (public key algorithms)
Quantum Computing Impact on Cryptography

Secure Session (MACsec/IPsec/TLS)
- Public-private key-pairs
- Authentication
- Key establishment
- Data encryption & integrity

Asymmetric Cryptography
- Based on **mathematically related** public-private key-pairs
- Used for control plane operations
  - Authentication, Key establishment
- Example: RSA, DH, ECC

Symmetric Cryptography
- Based on shared key
- Used for bulk data encryption & integrity
- Protection level based on key strength
  - Key size & entropy
- Example: AES-GCM

Quantum-Resistant?
- Large reliable Quantum computers can break RSA, DH, ECC!

- Symmetric crypto with large and high-entropy keys is resistant to Quantum computer attacks
Why should we care about Quantum Threats now?

1. Attackers can tap the flows **today** and store them to be decrypted in the **future**.

2. Any sensitive deployments that need forward secrecy for 5+ years must act now!!!
   a) Military or other defense networks
   b) Federal or other government agencies
   c) Financial institutions and banks
   d) Service provider networks catering to enterprises having sensitive data

3. Less critical or short-lived sessions without long-term significance can wait.
Available Options

- **Symmetric Cryptography**
  - Long symmetric keys are Quantum Safe
  - Issues with distributing keys and trust

- **Quantum Key Distribution**
  - Use Quantum Mechanics to protect the data
  - Some limitations

- **Postquantum Cryptography**
  - Replace current public key algorithms with new ones
  - Still need to vet the algorithms and update the protocols
To Summarize...
Threats to Network Devices & Solutions

**NOS**

- **Integrity Visibility (Boot & Run-time)**
- **NOS Runtime** (Maintain Trust at Run-time)
- **BSP & Linux Kernel** (Establish Trustworthy NOS)
- **RP BIOS** | **LC BIOS**
- **X86 - CPU** (Establish Trust in Hardware)

**Protection against**

- Ransomware
- MitM attacks
- Credential Theft
- Known Vulnerabilities
- Malware Attacks
- Boot Vulnerability
- Malware Attacks
- Compromised Hardware
- Counterfeit Hardware

**Solutions**

- Disk Encryption
- Remote Attestation
- Secure Onboarding
- Operational Security Features
- Measured Boot
- Security Enhanced Linux
- Integrity Measurement Arch.
- Unique Hardware Identity
- Platform Security Chip like TPM
- Hardware anchored Secure Boot
Questions?