Protecting the Device: Cisco Trustworthy Systems & Embedded Security

David Lapier
Senior Product Manager
dlapier@cisco.com
@LapierDee

Stephen Lynn
Consulting Architect
stlynn@cisco.com
CCIE 5507 (R&S/WAN/Security)
CCDE 2013::56
@netw0rkStlynn
Cisco Spark

Questions?
Use Cisco Spark to communicate with the speaker after the session

How
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

cs.co/ciscolivebot#BRKSEC-1010
David lives in Palo Alto, CA

Likes to sailboat race. Reads too much Sci Fi.

Stephen lives in Washington DC

Like skiing and scuba diving.
Abstract

Malware installed on network devices is a real threat. This presentation addresses how Cisco builds trust into its products to mitigate attacks on the infrastructure. We also introduce best practices for the network administrator for “securing the device”
Apple Fights Order to Unlock San Bernardino Gunman’s iPhone
By ERIC LICHTBLAU and KATIE BENNER  FEB. 17, 2016

Putin Ordered ‘Influence Campaign’ Aimed at U.S. Election, Report Says
By DAVID E. SANGER  JAN. 6, 2017

Security experts say 'Vault 7' leak describes common, public hacks

Fresh Wikileaks Dump Shows CIA Was Hacking iPhones A Year After Launch

NSA's powerful Windows hacking tools leaked online

SYNful Knock router exploit isn’t going away soon
By Tim Greene

The Athens Affair
How some extremely smart hackers pulled off the most audacious cell-network break-in ever
By VASSILIS PREVELAKIS and DIOMIDIS SPINELLIS

HOW A CRYPTO ‘BACKDOOR’ PITTED THE TECH WORLD AGAINST THE NSA

Edward Snowden: Leaks that exposed US spy programme
© 2018  Cisco and/or its affiliates. All rights reserved.   Cisco Public
Security Landscape

“How do we trust the network and devices? How do we verify it?”

- DDoS
- MACsec
- Protocol Security
- Run time Defense
- Certifications
- Detection and Recovery
- Network Security
- Security
- Hardware Security
- Infrastructure Security
- Remote Attestation
- TAm
- Secure Storage
- Chip Guard
- Secure Asset Transfer
- Image Signing
- BIOS / Boot Loader Protection
- Secure Boot
- IPC Authentication
Agenda

- Anatomy of an Attack
- Trustworthy Systems
  - Built-In Security and Trust
  - Cisco Cloud Offerings
- Trustworthy Technologies
  - Image Signing and Secure Boot
  - Trust Anchor Module
  - Hardware Authenticity Check
  - Integrity Verification
  - Secure Zero-Touch Deployment
  - Best Practices
  - Runtime Defenses
  - Quality Crypto
- Summary
Anatomy of an Attack
Anatomy of An Attack

Recon

Attacker looks for weakness

Infiltration

Attacker uses info from recon to exploit the network device

Compromise

Network device is accessed

Data Exfiltration

Data is acquired from target devices

Cleanup

Attacker cleanup evidence of compromise
The Attack – IOS Modifications

Malware: 6 Observed Variants

- **Incident 0**: Static infection, Crypto (DH keys)
- **Incident 1**: Static infection, Crypto (DH keys)
- **Incident 2**: Runtime infection, C&C data exfil., Line cards
- **Incident 3**: Runtime infection, C&C; data exfil. multi-arch
- **Incident 4**: Runtime infection, C&C data exfil. ROMMON modular
- **Synful Knock**: Static infection, C&C; modular

Years:
- 2011
- 2012
- 2013
- 2014
- 2015
- 2016
Today’s Products for Today’s Threats

Risk

10 Years Ago

- Physical Isolation
- Locked Cabinets
- Limited staff access
- Proprietary HW & SW

Today

- Attackers are Professional
- Staff Related Breaches Grow
- Physical Barriers Break Down

- Nation-State
- Criminal
- Political
- Insider

- Social Engineering
- Outsourcing

- Internet
- Cloud
- Virtualization
- Open-Source
Trustworthy Systems
“Security is and will remain one of our absolute highest priorities.”

Chuck Robbins, CEO Cisco Systems
Cisco Trustworthy Systems Levels

<table>
<thead>
<tr>
<th>Protect the Network</th>
<th>Device Level Attack Protection</th>
<th>Solution Level Attack Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Snooping</td>
<td>Port Security</td>
<td>TrustSec</td>
</tr>
<tr>
<td>Intrusion Detection</td>
<td>IP Source Guard</td>
<td>ISE</td>
</tr>
<tr>
<td></td>
<td>uRPF</td>
<td>Stealthwatch</td>
</tr>
<tr>
<td></td>
<td>ACLs</td>
<td>FnF</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Platform Integrity</th>
<th></th>
<th>Secure Device Onboarding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Boot</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Image Signing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Counterfeit Protections</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware Trust Anchor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Runtime Defenses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OS Validation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modern Crypto</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Culture</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supply Chain Management</td>
<td></td>
<td>Product Security Baseline</td>
</tr>
<tr>
<td>Open Source Registration</td>
<td></td>
<td>PSIRT Advisories</td>
</tr>
<tr>
<td>Security Training</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Modeling</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Cisco Secure Development Lifecycle
Trust for Cisco Cloud Offerings
Cloud Services Vulnerability Attack Types

The first line of defense against threats on the Internet wherever users go

Web based attacks – XSS, CSRF, Unprotected API’s, Misconfigured ACL

Backdoors through unknown service accounts or hardcoded default credentials.

Command Injection through input validation weakness.
Trustworthy Cloud

From Product to Service
Continuous Security

Hosting Infrastructure
Share responsibilities
Ongoing operations

DevOps Model
Scale & Responsiveness
Automate Security

Build, operate, and monitor with trust
Continuous Security – Validate Regularly

Misconfigured AWS S3 bucket exposes millions of Verizon customers' data

Dow Jones Data Leak Results from an AWS Configuration Error

Security pros expect to see more incidents like the Dow Jones leak, which exposed customers' personal information following a public cloud configuration error.
Cisco Meraki Trust

Security, reliability & privacy information for Meraki cloud services

Overview

- 99.99% Reliability SLA
- Two-factor Authentication
- Highly Available Redundant Architecture
- SSAE16 Type II Audited Datacenters

Ready to see for yourself?
Start Trial

Have questions? We've got answers: 1 (888) 490-0918

https://meraki.cisco.com/trust
Administrative Tools & Best Practices

- Two Factor Authentication for Admin Access
- Password strengthening
- Role Based Access
- Alerting on configuration change
- Audit of configuration and logging
- SSL Certificate verification
- Idle Timeouts
- Security Rewards Program
Image Signing and Secure Boot
“In a troubling new development, threat actors looking for different ways to break into and remain undetected on enterprise networks appear to have begun targeting routers connecting businesses to the Internet.”

- Jay Vijajan, DARKReading.
Mitigations at Boot Time

Malware: 6 Observed Variants

- **Incident 0**
  - Static infection
  - Crypto (DH keys)

- **Incident 1**
  - Static infection
  - Crypto (DH keys)

- **Incident 2**
  - Runtime infection
  - Crypto
  - C&C data exfil.

- **Incident 3**
  - Runtime infection
  - C&C; data exfil.
  - multi-arch Line cards

- **Incident 4**
  - Runtime infection
  - C&C data exfil.
  - ROMMON modular

- **Synful Knock**
  - Static infection
  - C&C; modular

Timeline:
- 2011
- 2012
- 2013
- 2014
- 2015
- 2016
Mitigations at Boot Time

Malware: 6 Observed Variants

- **Incident 0**: Static infection, Crypto (DH keys), Image Signing, Secure Boot
- **Incident 1**: Static infection, Image Signing, Secure Boot
- **Incident 2**: Runtime infection, C&C data exfil.
- **Incident 3**: Runtime infection, C&C; data exfil. multi-arch Line cards
- **Incident 4**: Runtime infection, C&C data exfil. ROMMON modular
- **Synful Knock**: Static infection, Image Signing, Secure Boot
Mitigations at Boot Time

Malware: 6 Observed Variants

**Incident 0**
- Static infection
- Crypto (DH keys)
- Secure Boot

**Incident 1**
- Static infection

**Incident 2**
- Runtime infection
- C&C; data exfil.

**Incident 3**
- Runtime infection
- C&C; data exfil. multi-arch Line cards

**Incident 4**
- Runtime infection
- C&C

**Synful Knock**
- Static infection

SynFu! Knock

- Persistent malware that relies on stolen admin credentials to install cunning backdoor
- Gaining access to the ROMMON boot loader allows the malware to persist through reboots
- Modified image allows hacker to install independent executables on routers
- Attacker manipulates infected device behavior via HTTP C&C packets sent to the targeted device
- Found on ISR G1
  - 1841/2811/3825
- Static Infection to modify Cisco IOS.

https://www.talosintelligence.com/scanner
Image Signing: How It Works

Signing

1. Hash Function
2. Signing Hash With Cisco Private Key
3. Embed Signature to the Software
Image Signing: How It Works

Verification

Hash Function

Verify Signature Hash With Cisco Public Key

Hash is Compared to Verify Authenticity
Generic Boot Sequence

Bootloader

Fetch Hardware Instruction set. Initialize Basic Input/Output System (BIOS)

Operating System

Start-up Operating System
Infection Points to Generic Boot Sequence

- Changing the boot interface
- Booting from alternate device
- Bypassing Integrity checks
- Adding persistent code
Secure Boot Starts from Protected Code

Hardware Instruction Set (Boot Code) must be protected against an unauthorized modification from outside
Trust Anchor for Secure Boot

- Stores the initial instructions securely
- Point of trust where validation can begin.
- Cryptographically validates the integrity of ROMMON
- Ensures integrity for the boot sequence
Cisco Secure Boot
Anchors Secure Boot in Hardware to Create a Chain of Trust

Software Authenticity:

- Only authentic signed Cisco software boots up on a Cisco platform
- The boot process stops if any step fails to authenticate
- IOS “show software authenticity” command illustrates the results
Cisco Secure Boot and UEFI Secure Boot

Hardware-anchored Secure Boot

Step 1: Hardware Anchor
- Microloader

Step 2: Microloader checks Bootloader
- CPU

Step 3: Bootloader checks OS
- CPU

Step 4: OS launched
- CPU

Cisco Secure Boot
- Anchors Secure Boot process to hardware
- Resists supply chain and physical possession-based firmware tampering attacks
  - More difficult to modify hardware than software
  - More expensive
  - Hardware modification is more visible

Unified Extensible Firmware Interface (UEFI)
- Not anchored in hardware
- Nothing validates Bootloader
  - Susceptible to Bootloader rootkits
  - Susceptible to easy modifications in supply chain or with physical possession
Trust Anchor Module (TAm)
Cisco Trust Anchor Module (TAm)

- HW Authenticity Check
- Secure PnP
- Integrity Verification

Integrity Applications
TAM Services Libraries

Crypto Functions
Tamper-Proof Storage

- Anti-Tamper Chip Design
- Built-In Crypto Functions
- Secure Storage

Boot Measurements SUDI

BRKSEC-1010 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Platform Integrity: TPM and TAm Compared

TPM & TAm Capabilities

- Anti-tamper
- Non-volatile secure storage
- Crypto engine
- Key storage
- Random number generation
- Policy & Configuration

Cisco Trust Anchor Module

- Hardware designed to provide both end-user and supply chain protections
- Ideal for specialized network devices

Trusted Platform Module (TPM)

- Typically focused on providing end-user capabilities
- Ideal for general purpose computing
Secure Unique Device Identification (SUDI)

- Tamperproof ID for the device
- Binds the hardware identity to a key pair in a cryptographically secure X.509 certificate PID during manufacturing
- Connections with the device can be authenticated by the SUDI credential
- IEEE 802.1AR Compliant
Uses for SUDI

- Internal checks in the box
- Authentication Bootstrap Identity
- Remote Attestation
Cisco Trust Anchor Module

- Tamper Proof Storage
- Embedded Crypto Functions

Applications

Built-In Security

- Hardware Authenticity Check
- Integrity Verification
- Secure Zero-Touch Provisioning
Hardware Authenticity Check
Integrity Verification
Counterfeiting is Real
Cisco Secure Boot and Trust Anchor Module
Validating the Authenticity of Software Followed by Hardware

Step 1
- Hardware Anchor
- Microloader checks Bootloader

Step 2
- CPU
- Microloader
- Bootloader checks OS

Step 3
- CPU
- Bootloader
- OS launched

Step 4
- CPU
- OS
- Authenticity and license checks

Step 5
- Trust Anchor module

Step 6
- Trust Anchor module
- CPU
- OS

* The first instructions that run on a CPU are either stored in immutable hardware so that they cannot be tampered with or are validated by the hardware

Software authenticity check

Hardware authenticity check
Verifying that I can trust the device
Boot Integrity Visibility

Store Boot Measurements

Step 1: Hardware Anchor
- Microloader

Step 2: Microloader checks bootloader
- CPU

Step 3: Bootloader checks OS
- CPU

Step 4: OS launched
- CPU

Write Measurements

Tamper Proof Storage

TAm
Boot Integrity Visibility = Remote Attestation
Report Results Securely

Client

Integrity Verification App

Known Good Values (KGV)

Request SUDI [Nonce]…

… SUDI is.

Request Integrity Measures…

… Values Are.

TAm

Crypto Functions

Tamper-Proof Storage

Boot Measurements

SUDI
Boot Integrity Visibility
Attestation of the Identity and Boot Status

Network Device

Extract & Sign Measurements with SUDI

Secure Boot

Measurements

Trust Anchor

Integrity Verification App

Decrypt & Verify Measurements

“Nonce” to prevent re-play attacks

Verifies:
- Identity of the device
- running authenticate Cisco SW
- on authentic Cisco HW.

Cisco Development Cycle

Software Development

Known Good Value Collection

Known Good Value Collection

Software Development
Integrity Verification Demo
Secure Zero-Touch Deployment
Step 1: SUDI unique device identifier and serial number installed at manufacturing
Step 2: Secure boot of signed images at start-up verifies platform integrity
Step 3: Verification of device authenticity and integrity
Step 4: Network device sends its credentials to the Plug and Play server
Step 5: Plug and Play server verifies the identity of the device to be provisioned
Step 6: Two-way trust and secure communications established
Step 7: Secure provisioning of Cisco network device
Cisco SD-WAN
Platform for Digital Transformation
Cisco SD-WAN Zero Touch Provisioning

Certificate-Based Trust

- Bi-directional certificate-based trust between all elements
  - Public or Enterprise PKI
- White-list of valid vEdges and controllers
  - Certificate serial number as unique identification

<table>
<thead>
<tr>
<th>Controller Type</th>
<th>Hostname</th>
<th>System IP</th>
<th>Certificate Serial</th>
</tr>
</thead>
<tbody>
<tr>
<td>vBond</td>
<td>vBond1</td>
<td>1.1.1.2</td>
<td>46FD1AC2B1465B8E2EB5D7F7E10E1FEC</td>
</tr>
<tr>
<td>vBond</td>
<td>vBond2</td>
<td>1.1.1.11</td>
<td>640A8B654F391EE30E1CA13A97F06</td>
</tr>
<tr>
<td>vManage</td>
<td>vManage</td>
<td>1.1.1.1</td>
<td>074B7AE1DA4F9678FA42CA766845EF</td>
</tr>
<tr>
<td>vSmart</td>
<td>vSmart1</td>
<td>1.1.1.3</td>
<td>10CC1C0871C37758558F8B0F3E79ECC7</td>
</tr>
<tr>
<td>vSmart</td>
<td>vSmart2</td>
<td>1.1.1.10</td>
<td>0E4782A4EBCF42DA47EB0D9AE097C9A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Device Model</th>
<th>Serial No./Token</th>
<th>Hostname</th>
<th>IP Address</th>
<th>Validate</th>
</tr>
</thead>
<tbody>
<tr>
<td>vEdge Cloud</td>
<td>19EB7510F570D6BD235C1E576230...</td>
<td>RemoteSite2</td>
<td>1.1.1.8</td>
<td>Invalid</td>
</tr>
<tr>
<td>vEdge Cloud</td>
<td>585A0084DEA839ED7BB6F22BAE...</td>
<td>RemoteSite1</td>
<td>1.1.1.4</td>
<td>Invalid</td>
</tr>
<tr>
<td>vEdge Cloud</td>
<td>368ED9249E64F2C5ADF68C430F7E...</td>
<td>RegionalHub</td>
<td>1.1.1.7</td>
<td>Invalid</td>
</tr>
<tr>
<td>vEdge Cloud</td>
<td>0334D73E5EC036F87ABE132FE1CE4...</td>
<td>DataCenter</td>
<td>1.1.1.5</td>
<td>Invalid</td>
</tr>
</tbody>
</table>
Best Practices
Best Practices For Securing Infrastructure Devices

- Monitor Cisco Security Advisories and Responses
- Strengthen login credential by leveraging Authentication, Authorization, and Accounting (AAA)
- Centralized Log Collection and Monitoring
- Establish baseline and instrument the network to gain traffic visibility with NetFlow
- Control Plane & Management Plane Hardening
PSIRT Cisco Security Advisories and Response

Vulnerability Management
Evaluate and drive resolution of Cisco product & Cloud Services vulnerabilities

Incident Response
Assist customers with network-impacting security events

Proactive Engagement
Provide feedback and influence product design
Cisco PSIRT Openvuln API

Stay informed about security vulnerabilities

<table>
<thead>
<tr>
<th>PSIRT</th>
<th>Discover</th>
<th>Learn</th>
<th>Latest Threats and Vulnerabilities</th>
<th>Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communities</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Security Portal</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access our GitHub Repository</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

1 Overview
Find out how Cisco PSIRT openVuln API help.

2 Getting Started
Watch videos and technical documentation to get started with the Cisco PSIRT openVuln API.

3 Try the API Now!
Access the Cisco openVuln API to obtain Cisco Security Vulnerability information here.

https://developer.cisco.com/site/PSIRT/
A Modern Approach to Security Vulnerability Disclosures

This API allows technical staff and programmers to build tools that help them do their job more effectively. In this case, it enables them to easily keep up with security vulnerability information specific to their network.

https://developer.cisco.com/site/PSIRT

Community Support

Collaborate, learn, share and interact with Cisco PSIRT and other industry experts at the Cisco PSIRT Developer Community:

http://cs.co/psirt_community

Open Source Tools

Access our GitHub Repository and open source tools at:

https://github.com/CiscoPSIRT/openVulnAPI

Cisco Security Center

Access numerous security resources, white papers, vulnerability reports, blog posts, RSS feeds, and other information at:

https://cisco.com/security
“Attackers Use Stolen Credentials to Hack Cisco Networking Devices”
SecurityWeek August 13, 2015

“65 percent of companies expect to suffer a breach due to compromised credentials”
2016, Cloud Security Alliance

“81% of hacking-related breaches leveraged either stolen and/or weak passwords”
2017 Verizon Data Breach Investigations Report
Prevent Unauthorized Access
Better and Stronger Authentication

• Better / stronger Password Using enable secret (single factor)

• Public/private key (single factor)

• One Time Password/Token System (2-factor)

• CAC/smartcard with X.509v3 certificate RFC 6187 (2-factor)
CAC/smartcard with X.509v3 SSH Authentication

- Most secure access to command line
- Two-factor authentication
- X.509v3 certificate & PIN

- Government Certified
- Standard RFC-6187
- First End-to-end solution with Cisco and Pragma Systems
Gain visibility and intelligence of your network

Network as a Sensor

**Stealthwatch**

Provides unique visibility into what's happening across your entire network

Detects anomalies and threats faster with real-time analysis and advanced forensics capabilities

Generates notifications automatically when anomalies are detected on the network

Leverage information from other solutions to gain complete network visibility and security analytics

- Company Host
- Access
- Audit
- Posture
- Detect

- Everything must touch the network
- Know every host
- Record every conversation
- Understand what's normal
- Get alerted to change

Stealthwatch
Hardening the Device

- Enable SSH and Disable Telnet

  hostname <hostname>
  ip domain-name <domainname>
  crypto key generate rsa general-keys modulus 2048
  ip ssh time-out 60
  ip ssh source-interface <Source Interface>
  ip ssh logging events
  ip ssh version 2
  ip ssh dh min size 2048

  line vty 0 15
  access-class 100 in !!!Control access to VTY terminal
  transport input ssh !!!Specify SSH as the only
  transport output ssh !!!access to VTY
Hardening the Device

- Enable Data at Rest Protection with AES-128 Algorithm
  
  ```
  service password-encryption
  password encryption aes
  ```

- Disable Unused Services
  
  ```
  no service pad
  no service config
  no ip source-route
  no ip gratuitous-arps
  no service dhcp
  no ip http server
  no ip http secure-server
  no ip source-route
  no ip gratuitous-arps
  no ip bootp server
  ```
Hardening the Device

- Protect routed interfaces from spoofing and probing
  
  no ip proxy arp
  no ip unreachable
  no ip redirects
  ip verify unicast source reachable-via rx
  no ipv6 unreachables
  no ipv6 redirects
  ipv6 verify unicast source reachable-via rx
Hardening the Device

- Use SNMPv3 to secure access to devices by authenticating and encrypting data packets
  
  `snmp-server group <group name> v3 priv`
  
  `snmp-server trap-source <interface>`
  
  `snmp-server enable traps <trap type>`
  
  `snmp-server group <Group Name> v3 priv`
  
  `snmp-server view <View Name> iso included`
  
  `snmp-server trap-source <Source Interface>`
  
  `snmp-server host <Ipv4 address> version 3 priv admin`
  
  `snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart`
  
  `snmp-server enable traps config`
Runtime Defenses
Vulnerabilities in Running Software

- Attacker wants to exploit the Operating System when the software is running.

- Build software so that the possibility for exploitation is reduced.

- Use Compiler, kernel, and HW capabilities to provide protections.
Mitigations at Runtime

Malware: 6 Observed Variants

Incident 0
- Static infection
- Crypto (DH keys)
- Image Signing
- Secure Boot
- Runtime Defenses

Incident 1
- Static infection
- Image Signing
- Secure Boot

Incident 2
- Runtime infection
- C&C data exfil.
- Runtime Defenses

Incident 3
- Runtime infection
- C&C data exfil.
- Modular Line cards

Incident 4
- Runtime infection
- C&C
- Secure Boot
- Image Signing

Synful Knock
- Static infection
- Image Signing
- Secure Boot
Heartbleed: Buffer Overflow Attack

1. TLS Heartbeat Request
   - abc
   - Request Length = 30,000 bytes
   - Actual Length = 3 bytes

2. TLS Heartbeat Response
   - abc<garbage>mycertificatepassphrase<garbage>username & password, etc
   - Response Length = 30,000 bytes

3. Heap
   - Other stuff on the heap, including possibly certificate passphrase, accounts and passwords of web site users, credit card info, etc.
   - data="abc"
   - len=30,000 bytes
Computer Scientists Take Over Electronic Voting Machine

- Return Oriented Programming Attack
- Overrun data buffers to bypass normal execution
- Method of “Code Reuse Attack”
- Use libc “gadgets” to manipulate the system

UC San Diego, August 11, 2009
Stephen Checkoway, Ph.D.
Cisco Runtime Defenses

Address Space Layout Randomization (ASLR)

Object-Size Checking

X-Space

Hardware, Operating System, Compiler, and Development Best Practices

To protect against Buffer-Overflow and Return-Oriented Programming Attacks
Quality Cryptography
Why Quality Crypto Matters

Drivers

- Privacy
- Data Protection

Enablers

- Compatibility
- Simplification
- Efficient
- Secure Storage
- Secure Cryptography

Drivers:
- Why Quality Crypto Matters
- Data Protection
- Privacy

Enablers:
- Compatibility
- Simplification
- Efficient
- Secure Storage
- Secure Cryptography

Drivers and Enablers:
- Privacy
- Data Protection
- Secure Storage
- Secure Cryptography
- Efficiency

Cisco Live!
Quality Crypto - CiscoSSL

OpenSSL

- Hardened Crypto Library
- Feature Enhancements
- Certification Support
Quality Crypto - CiscoSSL

Hardened Crypto Library

- RC4 TLS cipher suites disabled
- GOST ciphers disabled
- SP800-90A DRBG enabled by default
- SSLv2 and SSLv3 are disabled

Feature Enhancements

- Improved ECC performance with FEC deprecation
- International ECC support
  - IETF Curve25519
- Deterministic ECDSA enhancements to improve security posture.
- Side-channel attack mitigation for ECDSA signature generation
- Entropy Enhancements
  - RDRAND support
  - 800-90A DRBG

Certification Support

- FIPS Object Module Support
  - FIPS mode
  - Includes support for updated NIST requirements
- Common Criteria Support
  - CC mode
  - Alignment with new NIAP and Protection Profile requirements

industry best practices

improving security and usability

compliance for public sector
Quality Crypto - CiscoSSL

Hardened Crypto Library

- Industry best practices
- RC4 TLS cipher suites disabled
- GOST ciphers disabled
- SP800-90A DRBG enabled by default
- SSLv2 and SSLv3 are disabled

Feature Enhancements

- Improving security and usability
- Improved ECC performance with FEC deprecation
- International ECC support
  - IETF Curve25519
- Deterministic ECDSA enhancements to improve security posture.
- Side-channel attack mitigation for ECDSA signature generation
- Entropy Enhancements
  - RDRAND support
  - 800-90A DRBG

Certification Support

- FIPS Object Module Support
  - FIPS mode
  - Includes support for updated NIST requirements
- Common Criteria Support
  - CC mode
  - Alignment with new NIAP and Protection Profile requirements

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
# Quality Crypto - CiscoSSL

## Hardened Crypto Library
- Industry best practices
- RC4 TLS cipher suites disabled
- GOST ciphers disabled
- SP800-90A DRBG enabled by default
- SSLv2 and SSLv3 are disabled

## Feature Enhancements
- Improving security and usability
- Improved ECC performance with FEC deprecation
- International ECC support
  - IETF Curve25519
- Deterministic ECDSA enhancements to improve security posture.
- Side-channel attack mitigation for ECDSA signature generation
- Entropy Enhancements
  - RDRAND support
  - 800-90A DRBG
- Deterministic ECDSA enhancements to improve security
- Side-channel attack mitigation for ECDSA signature generation
- Entropy Enhancements
  - RDRAND support
  - 800-90A DRBG

## Certification Support
- Compliance for public sector
  - FIPS Object Module Support
    - FIPS mode
    - Includes support for updated NIST requirements
  - Common Criteria Support
    - CC mode
    - Alignment with new NIAP and Protection Profile requirements
  - Hardened Crypto Library Feature Enhancements
  - Certification Support
    - Improving security and usability
    - Improved ECC performance with FEC deprecation
    - International ECC support
      - IETF Curve25519
    - Deterministic ECDSA enhancements to improve security posture.
    - Side-channel attack mitigation for ECDSA signature generation
    - Entropy Enhancements
      - RDRAND support
      - 800-90A DRBG
Summary
Direct attacks on network devices are a real threat

**Keep Malware Out**
- Exploit the Network
- Steal Intellectual Property
- Steal Customer Data

**Block Tampering**
- Money Laundering
- Insider Trading
- Identity Theft

**Stop Counterfeiting**
- Attack Customers
- Ransomware
- Brand Damage
Trustworthy Systems

Organizations require a secure, resilient network foundation for digitization

https://trust.cisco.com
Questions?
Use Cisco Spark to communicate with the speaker after the session

How
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

cs.co/ciscolivebot#BRKSEC-1010
• Please complete your Online Session Evaluations after each session

• Complete 4 Session Evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt

• All surveys can be completed via the Cisco Live Mobile App or the Communication Stations

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at www.ciscolive.com/global/on-demand-library/.
Continue Your Education

- Demos in the Cisco campus
- Walk-in Self-Paced Labs
- Tech Circle
- Meet the Engineer 1:1 meetings
- Related sessions
Thank you
Backup Slides
Feature Support
# Feature Support

<table>
<thead>
<tr>
<th>Feature Support</th>
<th>ASR 1001-HX</th>
<th>ASR 1002-HX</th>
<th>ASR 1000-RP3</th>
<th>ASR 1001-X</th>
<th>ASR 1002-X</th>
<th>ASR 1000-RP2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Signing</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HW-Anchored Secure Boot</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Trust Anchor Module</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>HW Authenticity Assurance</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Boot Integrity Visibility</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Runtime Defenses</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Simplified Factory Reset</td>
<td>Yes (16.7.1)</td>
<td>Yes (16.7.1)</td>
<td>Yes (16.7.1)</td>
<td>Yes (16.7.1)</td>
<td>Yes (16.7.1)</td>
<td>Yes (16.7.1)</td>
</tr>
<tr>
<td>Secure Storage</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Secure Guest Shell</td>
<td>Yes (16.7.1)</td>
<td>Yes (16.7.1)</td>
<td>Yes (16.7.1)</td>
<td>Yes (16.7.1)</td>
<td>Yes (16.7.1)</td>
<td>Yes (16.7.1)</td>
</tr>
</tbody>
</table>

## Solution Support

<table>
<thead>
<tr>
<th>Feature Support</th>
<th>ASR 1001-HX</th>
<th>ASR 1002-HX</th>
<th>ASR 1000-RP3</th>
<th>ASR 1001-X</th>
<th>ASR 1002-X</th>
<th>ASR 1000-RP2</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUDI authentication for Cisco Network PnP*</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>APIC EM Integrity Visibility App Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

*See Release Notes for Network Plug and Play

**For specific models, see Cisco 800 Series Integrated Services Routers Software Configuration Guide
# Feature Support

<table>
<thead>
<tr>
<th>Feature Support</th>
<th>ISR 4451-X</th>
<th>ISR 4431</th>
<th>ISR 4351</th>
<th>ISR 4331</th>
<th>ISR 4321</th>
<th>ISR 4221</th>
<th>CSR 1000V</th>
<th>ENCS-5400</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Signing</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HW-Anchored Secure Boot</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Trust Anchor Module</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>HW Authenticity Assurance</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Boot Integrity Visibility</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Runtime Defenses</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Simplified Factory Reset</td>
<td>Yes (16.6.1)</td>
<td>Yes (16.6.1)</td>
<td>Yes (16.6.1)</td>
<td>Yes (16.6.1)</td>
<td>Yes (16.6.1)</td>
<td>Yes (16.6.1)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Secure Storage</td>
<td>Yes (16.6.1)</td>
<td>Yes (16.6.1)</td>
<td>Yes (16.6.1)</td>
<td>Yes (16.6.1)</td>
<td>Yes (16.6.1)</td>
<td>Yes (16.6.1)</td>
<td>Yes (16.6.1)</td>
<td>No</td>
</tr>
<tr>
<td>Secure Guest Shell</td>
<td>Yes (16.5.1)</td>
<td>Yes (16.5.1)</td>
<td>Yes (16.5.1)</td>
<td>Yes (16.5.1)</td>
<td>Yes (16.5.1)</td>
<td>Yes (16.5.1)</td>
<td>Mar '18 (16.8.1)</td>
<td>Nov '17 (16.7.1)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Solution Support</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SUDI authentication for Cisco Network PnP*</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>APIC EM Integrity Visibility App Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

*See Release Notes for Network Plug and Play

** For specific models, see Cisco 800 Series Integrated Services Routers Software Configuration Guide
## Feature Support

<table>
<thead>
<tr>
<th>Feature Support</th>
<th>IR 809</th>
<th>ISR 819</th>
<th>ISR 829</th>
<th>ISR 840</th>
<th>ISR 860</th>
<th>ISR 880</th>
<th>ISR 890</th>
<th>ISR 1900</th>
<th>ISR 2900</th>
<th>ISR 3900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Signing</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HW-Anchored Secure Boot</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Trust Anchor Module</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>HW Authenticity Assurance</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Boot Integrity Visibility</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Runtime Defenses</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Simplified Factory Reset</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Secure Storage</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes**</td>
<td>Yes**</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Secure Guest Shell</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Solution Support

<table>
<thead>
<tr>
<th>Solution Support</th>
<th>IR 809</th>
<th>ISR 819</th>
<th>ISR 829</th>
<th>ISR 840</th>
<th>ISR 860</th>
<th>ISR 880</th>
<th>ISR 890</th>
<th>ISR 1900</th>
<th>ISR 2900</th>
<th>ISR 3900</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUDI authentication for Cisco Network PnP*</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>APIC EM Integrity Visibility App Support</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*See Release Notes for Network Plug and Play

** For specific models, see Cisco 800 Series Integrated Services Routers Software Configuration Guide
# Feature Support & Roadmap

<table>
<thead>
<tr>
<th>Feature Support</th>
<th>Cat 9500</th>
<th>Cat 9400</th>
<th>Cat 9300</th>
<th>Cat 3850</th>
<th>Cat 3850 Fiber</th>
<th>Cat 3650</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Signing</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HW-Anchor Secure Boot</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Trust Anchor Module</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HW Authenticity Assurance</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Boot Integrity Visibility</td>
<td>Mar ’18 (16.8.1)</td>
<td>Mar ’18 (16.8.1)</td>
<td>Mar ’18 (16.8.1)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Runtime Defenses</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Secure Guest Shell</td>
<td>Yes (16.5.1)</td>
<td>Yes (16.6.1)</td>
<td>Yes (16.5.1)</td>
<td>Yes (16.5.1)</td>
<td>Yes (16.5.1)</td>
<td>Yes (16.5.1)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Solution Support</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SUDI authentication for Cisco Network PnP*</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>APIC EM Integrity Visibility App Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

*See Release Notes for Network Plug and Play*
# Feature Support

<table>
<thead>
<tr>
<th>Feature Support</th>
<th>Cat 3750-X</th>
<th>Cat 3560-X</th>
<th>Cat 3560-CX</th>
<th>Cat 6800 Sup6T</th>
<th>Cat 6800 Sup2T</th>
<th>Cat 4500 Sup8E</th>
<th>Cat 4500 Sup7E/LE</th>
<th>Cat 4500-X</th>
<th>Cat 4500 Sup6E/LE</th>
<th>Cat 2960-X</th>
<th>Cat 2960-L</th>
<th>Cat 2960-CX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Signing</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes -</td>
<td>Yes -</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>15.3(1)E</td>
<td>Yes</td>
<td>15.3(1)E</td>
<td></td>
</tr>
<tr>
<td>HW-Anchored Secure Boot</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Trust Anchor Module</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HW Authenticity Assurance</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Boot Integrity Visibility</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Runtime Defenses</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Simplified Factory Reset</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Secure Storage</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Secure Guest Shell</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Solution Support**

| SUDI authentication for Cisco Network PnP* | No | No | No | No | Yes | Yes | Yes | No | No | No | No | No |
| APIC EM Integrity Visibility App Support | No | No | No | No | Yes | Yes | Yes | No | No | No | No | No |

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
# Feature Support

<table>
<thead>
<tr>
<th>Feature</th>
<th>Aironet 1560</th>
<th>Aironet 1815</th>
<th>Aironet 2800</th>
<th>Aironet 3800</th>
<th>Aironet 1830</th>
<th>Aironet 1850</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Signing</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HW-Anchored Secure Boot</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Trust Anchor Module</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>HW Authenticity Assurance</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Boot Integrity Visibility</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Runtime Defenses</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

## Solution Support

<table>
<thead>
<tr>
<th>Solution Support</th>
<th>Aironet 1560</th>
<th>Aironet 1815</th>
<th>Aironet 2800</th>
<th>Aironet 3800</th>
<th>Aironet 1830</th>
<th>Aironet 1850</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUDI authentication for Cisco Network PnP*</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>APIC EM Integrity Visibility App Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
# Feature Support

<table>
<thead>
<tr>
<th>Feature</th>
<th>8500 Series WLC</th>
<th>Cisco 5500 Series WLC</th>
<th>Cisco 3504 WLC</th>
<th>Cisco 2500 Series WLC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Signing</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HW-Anchored Secure Boot</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Trust Anchor Module</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HW Authenticity Assurance</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Boot Integrity Visibility</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Runtime Defenses</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Solution Support**

<table>
<thead>
<tr>
<th>Feature</th>
<th>8500 Series WLC</th>
<th>Cisco 5500 Series WLC</th>
<th>Cisco 3504 WLC</th>
<th>Cisco 2500 Series WLC</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUDI authentication for Cisco Network PnP*</td>
<td>No</td>
<td>No</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>APIC EM Integrity Visibility App Support</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

*See Release Notes for Network Plug and Play*
# Feature Support

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Signing</td>
<td>Yes</td>
<td>yes</td>
<td>Yes for Most Models++</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Runtime Defenses</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HW-Anchored Secure Boot **</td>
<td>No</td>
<td>No</td>
<td>Yes for Most Models++</td>
<td>2100 Series</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Trust Anchor Module **</td>
<td>No</td>
<td>Yes</td>
<td>Yes for Most Models++</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>HW Authenticity Check **</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

** Applies to HW / Appliances only
++ Except 5525-X, 5545-X, 5555-X, and 5585-X
Feature Support Questions

• Ask your acct team
• Email “ask-trustworthy@cisco.com”
Further Reading

- *Cisco IOS Software Integrity Assurance*
  - Methods to compromise Cisco devices, best practices to protect against attempts to modify HW or SW
- Cisco Guide to Harden Cisco IOS Devices
- Telemetry Based Infrastructure Device Integrity Monitoring
- Cisco Security Response Center Home
  - [https://tools.cisco.com/security/center/home.x](https://tools.cisco.com/security/center/home.x)
Further Reading

- *Cisco Event Response: SYNful Knock Malware*

- *Digitally Signed Cisco Software*

- *Cisco IOS Software Integrity Assurance*
  - Methods to compromise Cisco devices, best practices to protect against attempts to modify HW or SW