Obrana proti útokům

na samotné směrovače a přepínače a nejen na ně

4.8.2020

Security Foundation – TrustWorthy Systems

Protect the Network

Device Level Attack Protection

DHCP Snooping | Port Security | uRPF
Intrusion Detection | IP Source Guard | ACLs

Solution Level Attack Protection

TrustSec | ISE | Stealthwatch | FnF

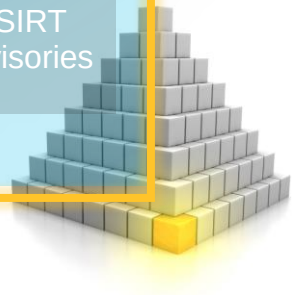
Platform Integrity

Secure Boot | Image Signing | Counterfeit Protections | Hardware Trust Anchor | Runtime Defenses | OS Validation | Modern Crypto | Secure Device Onboarding (SUDI, …)

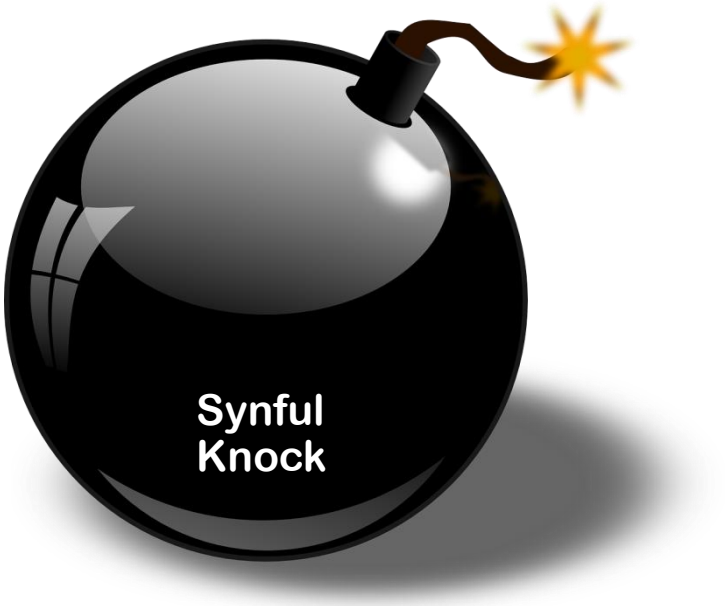
Security Culture

Supply Chain Management | Open Source Registration | Security Training | Threat Modeling | Product Security Baseline | PSIRT Advisories

Cisco Secure Development Lifecycle

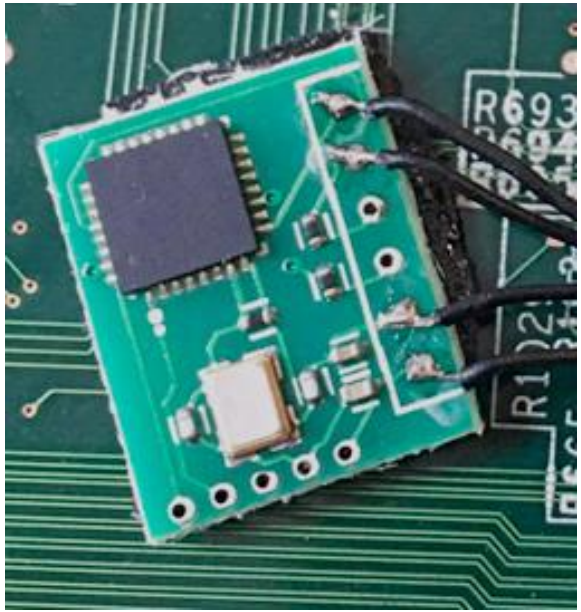


SynFul Knock



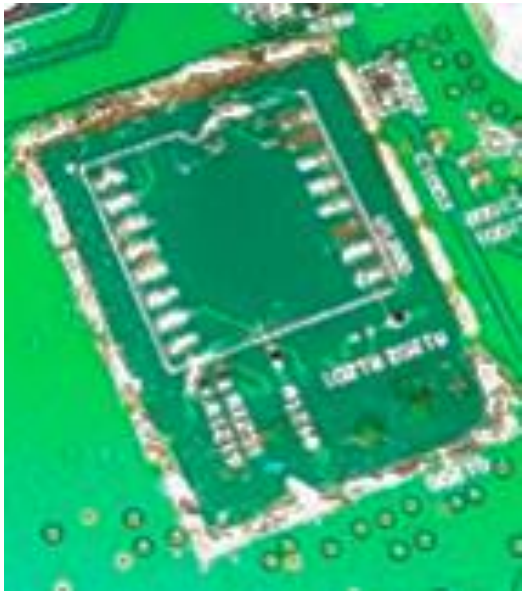
- Persistent malware that relies on stolen admin credentials to install cunning backdoor
- Gaining access to the ROMMON boot loader allows the malware to persist through reboots
- Modified image allows hacker to install independent executables on routers
- Attacker manipulates infected device behavior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

Counterfeiting



- Occurs on regular basis
- Mostly switching or volume products. Adding ports, or bypassing licensing.
- Not just Cisco's problem – It is bad for customer's too.
- (Quality, performance, support… possible tampering?)

Physical Tampering



- Lost critical data with forensic attacks

E.g. Top Trends for 2018

(Annual Security Report)

Embedded Security

Built for Today's Threats

Verification of Integrity

Security Expertise and Innovation

For Your Reference

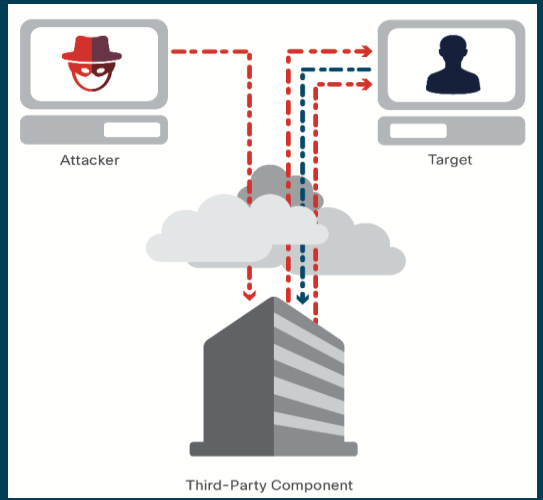
- Targeting (critical) infrastructure devices in the network
  - Network based malware
  - Exploitation of EoL network infrastructure
- Attacks on the supply chain (counterfeiting)
- Exploiting end of life and outdated hardware/software/ protocols
- Exploitation of third party and open source software
- Abuse of cloud services

E.g. Top Network Vulnerabilities for 2018

(Annual Security Report)

For Your Reference

- Buffer Overflow Errors
- Input Validation
- Permissions Privileges, Access
- Cryptographic Issues
- Reflection Amplification (DDoS) Attacks
- Exploitation of Open Source Software



Cisco’s response to escalating threats…

Embedded Security

Trustworthy Solutions: The Foundations of Trust

CSDL

Product Vulnerabilities

- New version in place, recommitment to SRCs
- Rigorous, evolving product security standards
- Consistent security standards
- Stop-ship if non compliant

Supply Chain Security

Compromised During Transit

Technical, Behavioral, Physical, & Logical Security Implementations

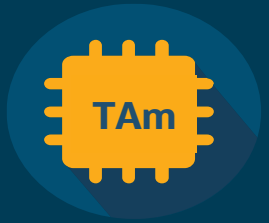
- Smart Chips
- PCB Labels
- Vendor Auditing

Secure Boot & Run Time Defenses

Compromised Software

- Only genuine SW boots on a Cisco platform
- Automated integrity checks
- Monitors startup & shuts down if compromised
- Faster identification of threats

Trust Anchor Module



Compromised Hardware

- Verifies that hardware is genuine
- Protects against counterfeit and data manipulation
- Enables secure, encrypted communications
- Enables zero-touch provisioning, minimizes deployment costs

History of Malware Found on Cisco IOS Devices

	Incident 0	Incident 1	Incident 2	Incident 3	Incident 4	Incident 5

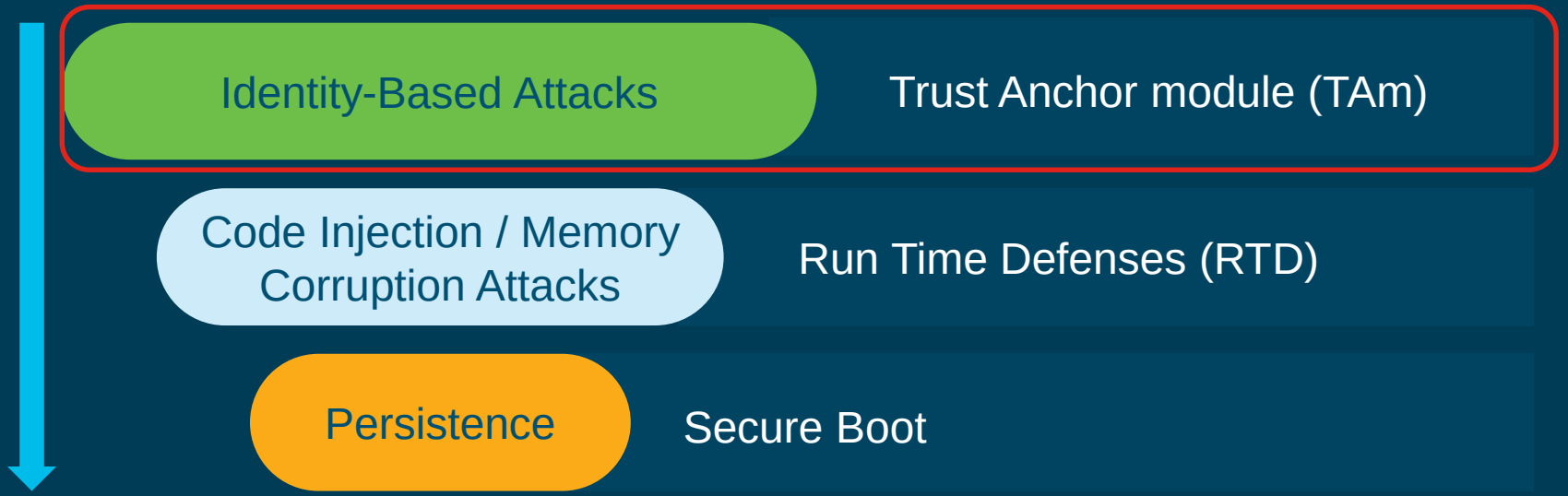
“Evolution of Attacks on Cisco IOS Devices”, Graham Holmes
https://blogs.cisco.com/security/evolution-of-attacks-on-cisco-ios-devices

Attacking a Network

Multilayered security protections to create defense-in-depth

Attacking a Network

Multilayered security protections to create defense-in-depth



Trust Anchor Module (TAm)

- Hardware-Based Anchor
- Anti-Tamper Chip
- Secure Storage
- Built-In Crypto Functions
- Random Number Generator
- Hardware Authenticity Check
- Integrity Verification
- Verifiable Entropy

Secure Unique Device ID (SUDI)
X.509 Certificate = Device's Identity

- Manufacturer installed certificate
- Hardware serial numbers
- Device-unique public key

Key Use Cases

- Verifying the integrity of a device's identity
- Onboarding a new device – Secure Zero Touch Provisioning
- Secure enrollment within an organization's PKI

TAm vs Trusted Platform Module

TAm and TPM: Common Features

Anti-tamper protection

Nonvolatile secure storage

Policy and configuration

Key store

Random-number generation

Crypto engine

Crypto services

Cisco Trust Anchor Module (TAm)

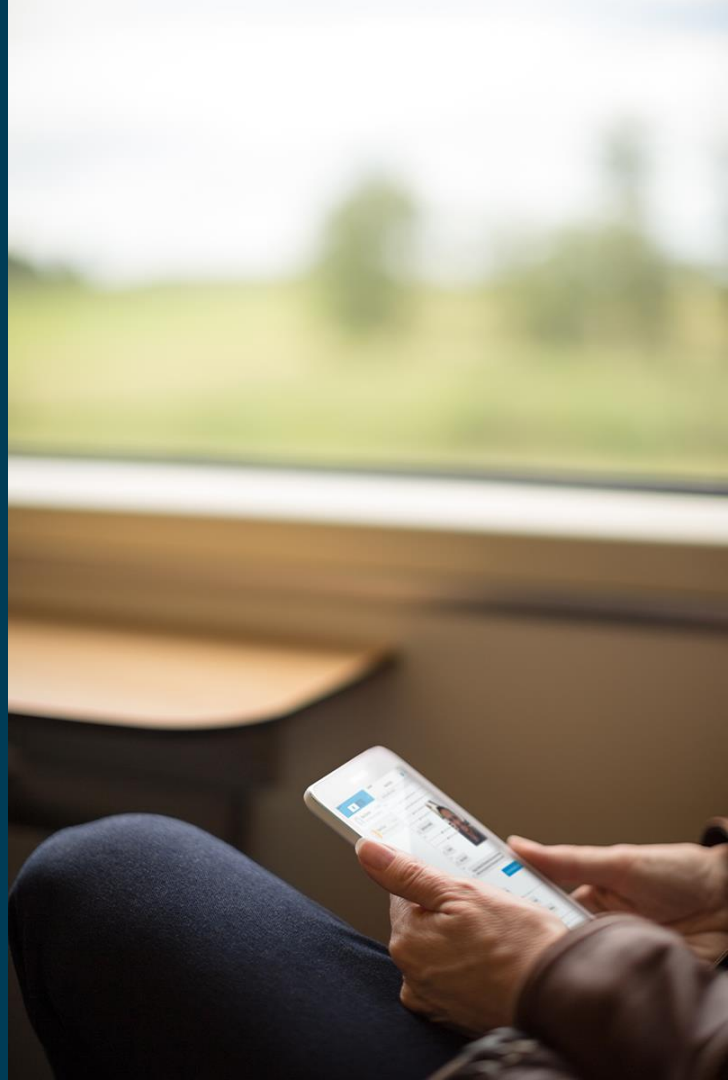
- Hardware designed to provide both end-user and supply chain protections
  - End-user protections include highly secure storage of user credentials, passwords, settings
  - Supply chain protections -- Cisco SUDI (secure unique device identifier) inserted during manufacturing
- Secured at manufacturing → no user intervention required
- Ideal for embedded computing like routers and Wi-Fi access points

Trusted Platform Module (TPM)

- Typically focused on providing end-user capabilities
  - Hardware protection for user certificates
  - Hardware protection for integrity information
- Custom development required for use
- Ideal for general-purpose computing like servers and PCs

Customer Benefits

- Allows customers to accurately, consistently and electronically identify Cisco products for asset management
- Enables service entitlement by serial number, quality feedback by version, and inventory management
- Consistent device identity and certificates across secured products
- SPs: Enables custom deployments, allows for use of a Cisco provisioning service



Now Let's See What Happens With TAm....

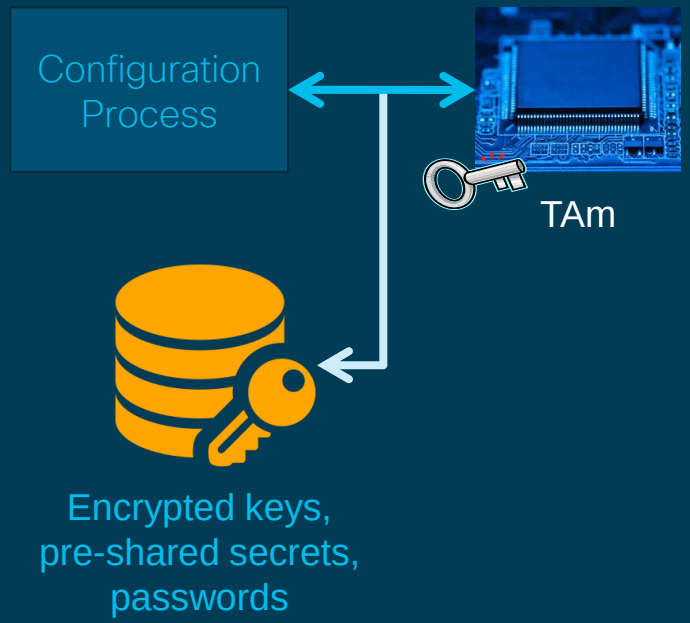
An Example of How SUDI can be Seen on the Command Line...

Let's Watch What Happens
Without TAm Secure Storage…

TAm Secure Storage

At-Rest Protection of Sensitive Configuration Data

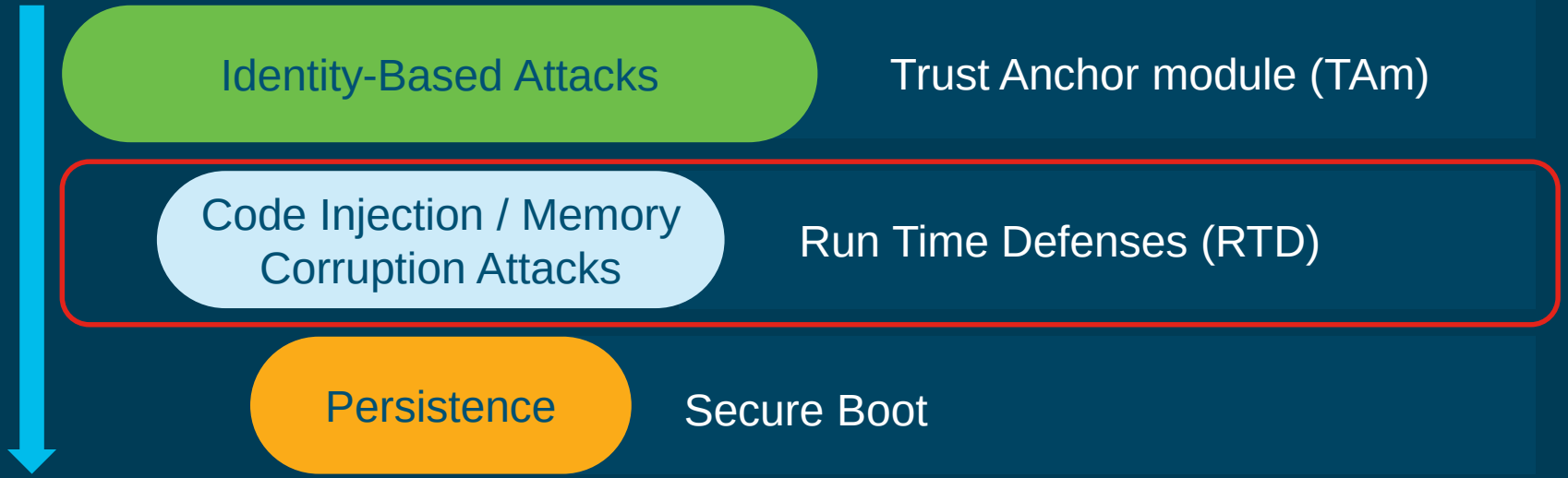
- Unique AES-256 key securely-stored in TAm encrypts sensitive configuration data stored in flash
- Protected data includes:
  - Crypto PKI keys
  - Type 6 passwords (e.g. AAA)
  - Routing protocol shared secrets
  - Remote server credentials
- Feature support emerging



Let's Watch What Happens With TAm Secure Storage...

Attacking a Network

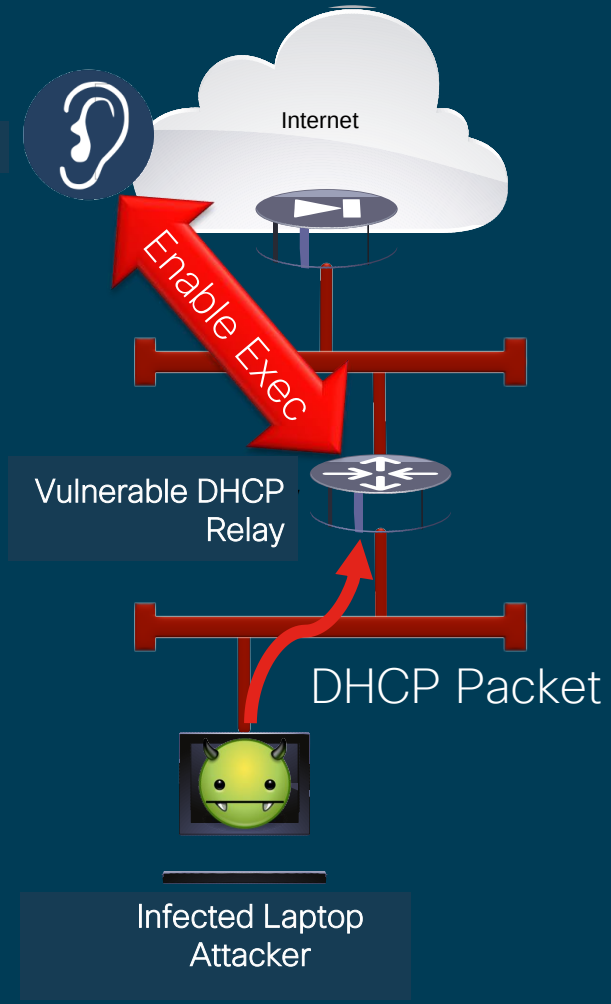
Multilayered security protections to create defense-in-depth



Let's Watch What Happens When We Attempt to Access a Device Without Run Time Defenses In Place...

Scenario: Attacker exploits DHCP relay

- Laptop is infected with malware
- Attacker uses infected laptop to hit Cisco Catalyst 3850 with a single DHCP packet that triggers a buffer overflow vulnerability in the DHCP relay
- Switch calls home to Listener, providing the attacker with an Enable prompt and foothold into the customer network



Code Injection Attack Demo

root@attacker: ~ (ssh) ⌘1 root@attacker: ~ (ssh) ⌘2 root@listener: ~ (... ⌘3

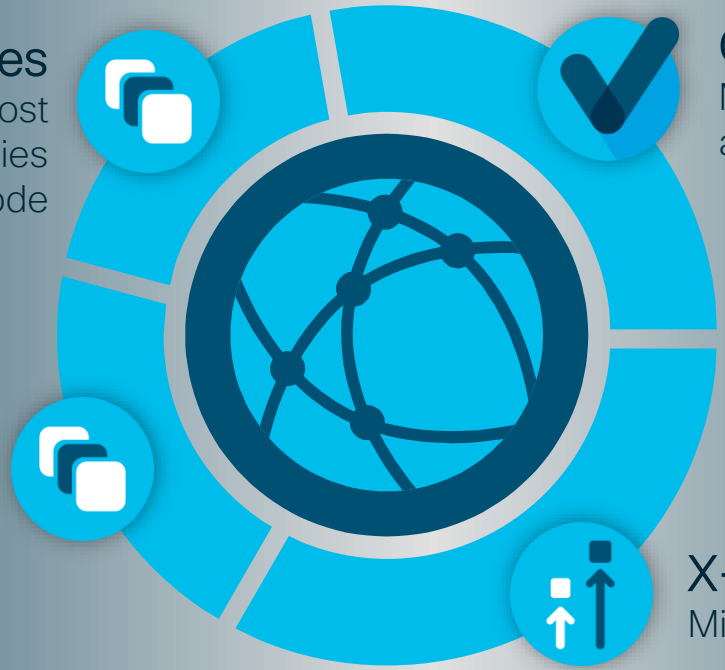
```
Cat3850#
Cat3850#
Cat3850#
Jul 11 16:15:14.151: %DATACORRUPTION-1-DATAINCONSISTENCY: Attempt to me
mcpy 212 bytes should have been 92 bytes,  -PC= :AAAAAAA000+4BB4F4C
-Traceback= 1#89ca4c68b59a0b4410c4a014c684606e  :AAAAAAA000+4B43A80 :AA
AAAAA000+4B42BEC :AAAAAAA000+4B42F9C :AAAAAAA000+4B7FE60 :AAAAAAA000+82
BA49C :AAAAAAA000+4BB4F4C :AAAAAAA000+4BB5DDC :AAAAAAA000+4BB5F58 :AAAA
AAA000+4BB6AFC :AAAAAAA000+4BB79F4 :AAAAAAA000+4BB7F50
```

Switch Console

Run-Time Defenses

Safe C Libraries

Ensure only the most secure coding libraries are used in code



Object Size Checking

Mitigate buffer overflow attacks

ASLR

Mitigate code injection attacks

X-Space

Mitigate code injection attacks

Let's Watch What Happens With Run Time Defenses...

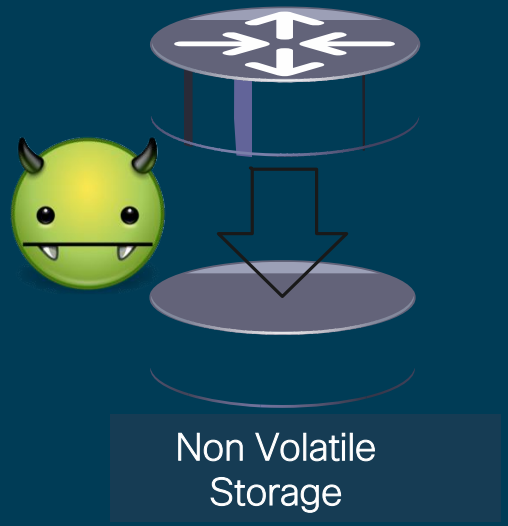
Attacking a Network

Multilayered security protections to create defense-in-depth

Let's Watch What Happens When We Try to Boot a Modified Image Without Secure Boot in Place...

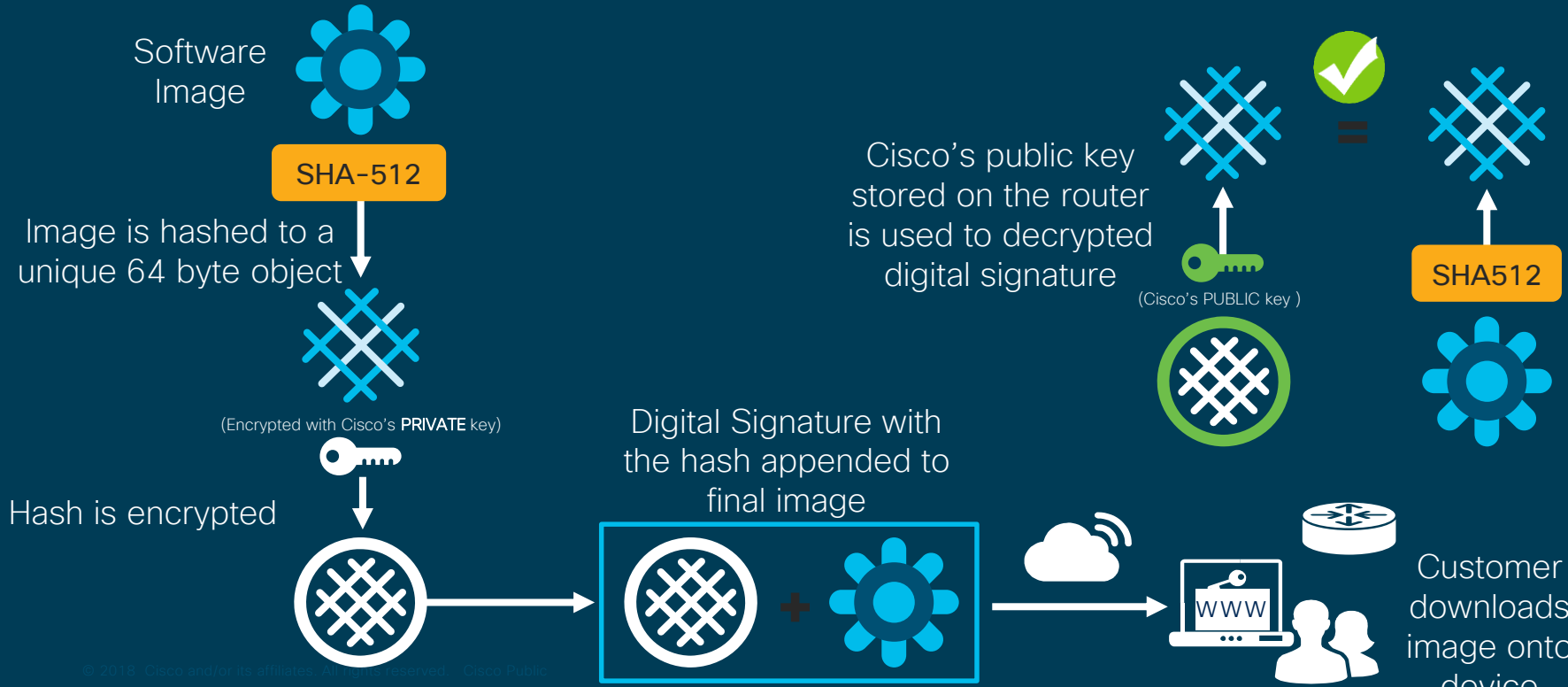
Scenario: Attacker becomes persistent

- Attacker, having gained a foothold into the customer network, desires persistence
- Modifies IOS XE code on disk or golden image to disable **all** password checking
- When router boots, it will load code that weakens all password checking on box:
  - SSH
  - Console
  - Enable



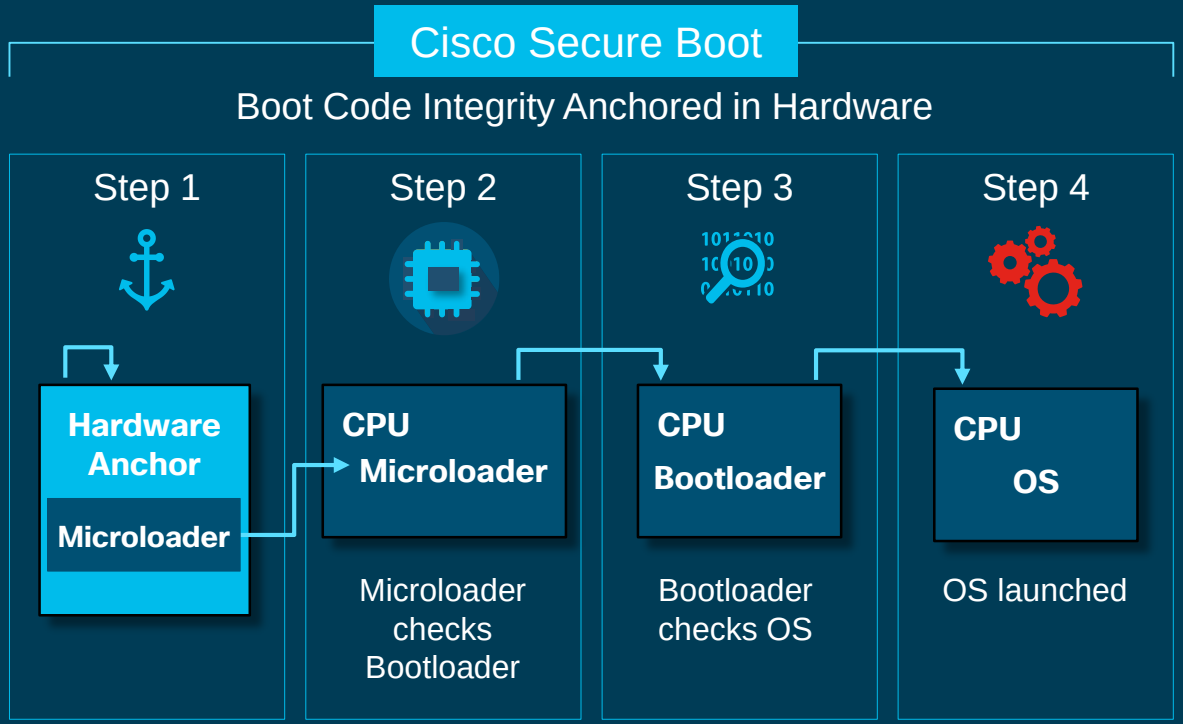
Booting a Modified Image

Image Signing: Integrity & Non Repudiation



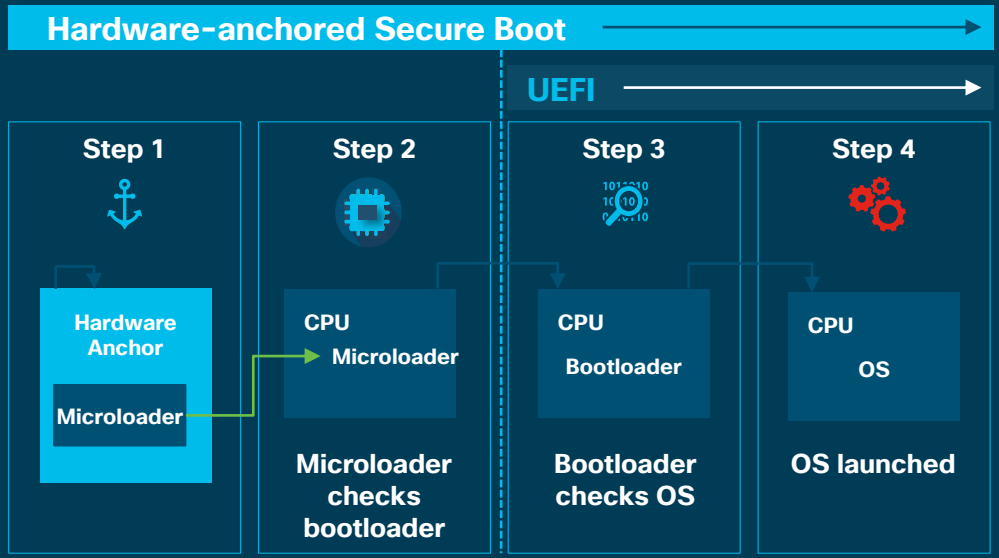
Secure Boot

Ensuring authentic Cisco software is executed by anchoring assurance in hardware



- Secure Boot takes **image signing to the next level.**
- Anchoring the boot sequence chain of trust to hardware **at the CPU level**.
- Only authentic signed Cisco software boots up on a Cisco platform
- The boot process will not allow tampered software to boot
- Protects against persistent firmware implants through use of run time attacks
- Resists supply chain and physical possession based firmware tampering attacks

Cisco Secure Boot vs Industry UEFI



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)

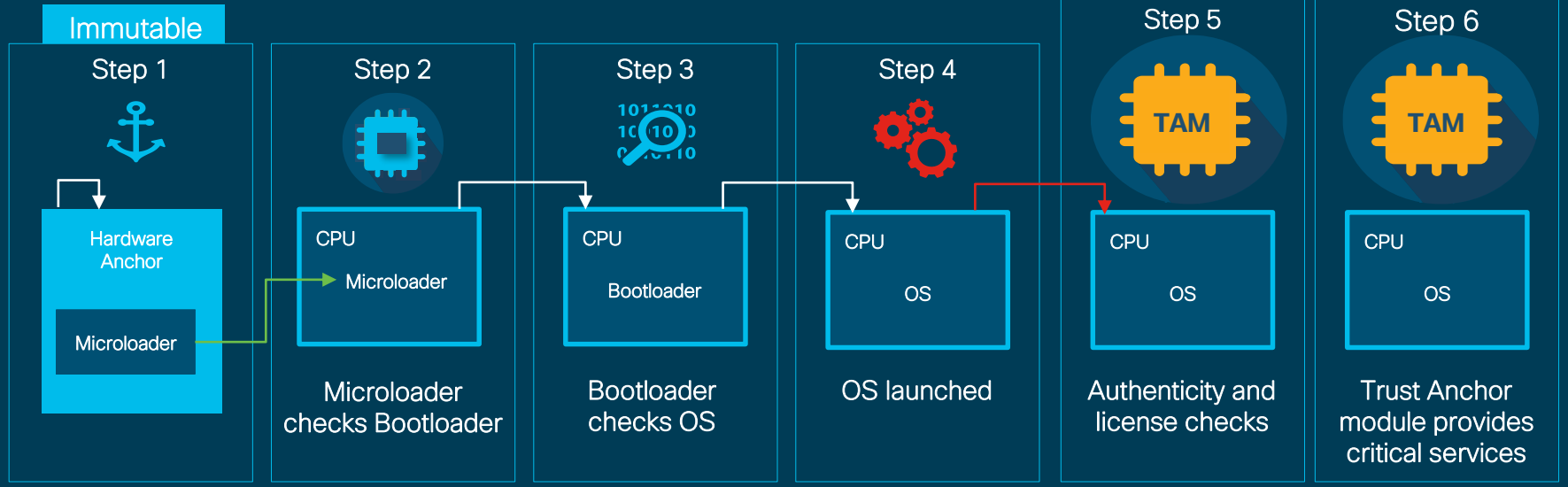
- Not anchored in hardware
- Nothing validates BIOS
  - Susceptible to BIOS rootkits
  - Susceptible to easy modifications in supply chain or with physical possession

Let's Watch What Happens When We Try to Boot a Modified Image With Secure Boot in Place...

Secure Boot Protects System

How Cisco Secure Boot & TAM Come Together

Validating the Authenticity of Software Followed by Hardware



The first instructions run on CPU and stored in immutable hardware → they cannot be tampered with

Software authenticity check

Hardware authenticity check

Trust Anchor module is a Cisco specific chip with anti-tamper features:

- **Secure unique device ID (SUDI)**
- **Secure storage (keys and objects)**
- **Certifiable entropy source**
- **Secure crypto assist**
- **Secure zero touch provisioning**

Attack Scenario

- Will the counterfeit card boot?

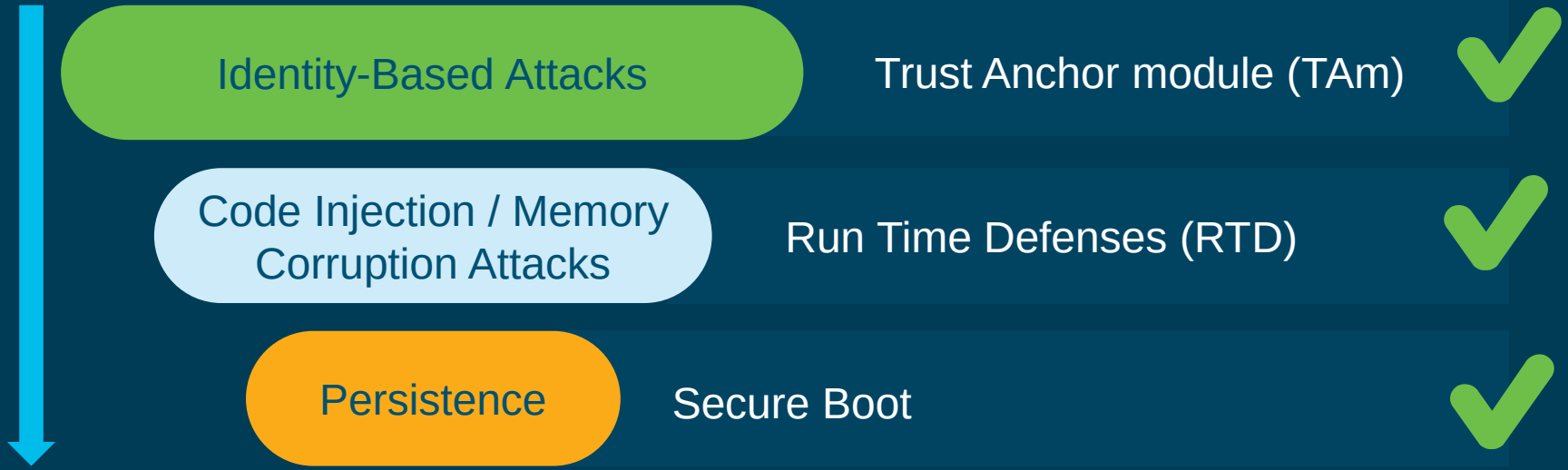
No SUDI

Good SUDI

```
Switch#
*Jun  4 19:19:24.441: %PLATFORM_PM-6-FRULINK_INSERTED: 2x40G uplink module inserted in the switch 1 slot 1
Switch#show mod
Switch  Ports    Model                Serial No.   MAC address     Hw Ver.       Sw Ver.
------  -----   ---------             -----------  --------------  -------       --------
 1       50     C9500-40X            FCW2133A4NB  00a3.d145.7800  V01           16.8.1a
Switch#show inventory
NAME: "c95xx Stack", DESCR: "c95xx Stack"
PID: C9500-40X          , VID: V01  , SN: FCW2133A4NB

NAME: "Switch 1", DESCR: "C9500-40X"
PID: C9500-40X          , VID: V01  , SN: FCW2133A4NB

NAME: "Switch 1 - Power Supply A", DESCR: "Switch 1 - Power Supply A"
PID: PWR-C4-950WAC-R    , VID: 000  , SN: APS2139000J

NAME: "Switch 1 - Power Supply B", DESCR: "Switch 1 - Power Supply B"
PID: PWR-C4-950WAC-R    , VID: 000  , SN: APS2139004B

NAME: "Switch 1 FRU Uplink Module 1", DESCR: "2x40G Uplink Module"
PID: C9500-NM-2Q        , VID: V00  , SN: FOC21172QCE


Switch#
```

Attacking a Network

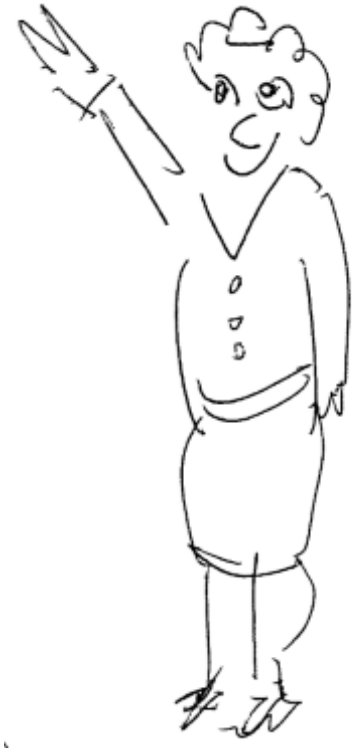
Multilayered security protections to create defense-in-depth



Best Practices

Best Practices at the “Device” level

- Protect the command line and WebUI
- Follow Hardening Guides
- Remove “Service Internal” from configs
- Monitor Security Advisories (PSIRT)
- Upgrade to latest IOS images
- Gain visibility
- Maintain logs
- Verify software integrity
- Purchase from Authorized Resellers
- Factory Reset when re-purposing



PSIRT Security Advisories

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

Open Source Tools

Access our GitHub Repository and open source tools at:
https://github.com/CiscoPSIRT/openVulnAPI

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

Cisco Security Center

Access numerous security resources, white papers, vulnerability reports, blog posts, RSS feeds, and other information at:
https://cisco.com/security

For Your Reference

Hardening the Device

- *Cisco Guide to Harden Cisco IOS Devices*
- http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html
- *Cisco IOS Software Integrity Assurance*
- http://www.cisco.com/c/en/us/about/security-center/integrity-assurance.html
- *Cisco IOS XE Software Integrity Assurance*
- https://tools.cisco.com/security/center/resources/ios_xe_integrity_assurance.html
- *Cisco Security Advisories and Alerts*
- http://www.cisco.com/go/psirt
- *Cisco Security Response Center Home*
- https://tools.cisco.com/security/center/home.x
- *Security Advisory Software Checker*
- https://tools.cisco.com/security/center/softwarechecker.x

Summary

Cisco TRUSTworthy Infrastructure – Security Foundation

Protect the Application, Data, IT, …

Protect the Network

Device Level Attack Protection

- DHCP Snooping
- Intrusion Detection
- Port Security
- IP Source Guard
- uRPF
- ACLs

Solution Level Attack Protection

- TrustSec
- ISE
- Stealthwatch
- FnF

Platform Integrity

- Secure Boot
- Image Signing
- Counterfeit Protections
- Hardware Trust Anchor
- Runtime Defenses
- OS Validation
- Modern Crypto
- Secure Device Onboarding (SUDI, …)

Security Culture

- Supply Chain Management
- Open Source Registration
- Security Training
- Threat Modeling
- Product Security Baseline
- PSIRT Advisories

Cisco Secure Development Lifecycle

Shrnutí: TrustWorthy Systems

- Bez bezpečných základů nelze vybudovat bezpečný systém
- Bezpečnost stojí na důvěře v komponenty
- I drobné detaily mohou způsobit bezpečnostní incident
- https://trust.cisco.com


CISCO