How to Secure Network Equipment Against Attack
Webcast Logistics

No Sound?
This is a streaming audio event. Make sure the sound on your PC is turned on.

Questions?
Type your questions using the Ask a Question Text Box
Today’s Presenters

Bill Sulzen
Technical Leader
Cisco Systems

Michael Eckel
Security Technologist
Huawei Technologies

Steve Hanna
Senior Principal
Infineon Technologies
Agenda

• Threats to network equipment
• Locking down firmware
• Introduction to trusted computing
• Networking applications for trusted computing
• From guidance to reality
• Call to action
• References
THREATS TO NETWORK EQUIPMENT
Threats to Network Equipment

• Network equipment is critical infrastructure

• Threats include:
  • Data theft
  • Denial of service
  • Launch point for further attacks
  • Damage to network equipment

• Recent headlines:
  
  “Russian hackers mass-exploit routers in homes, govs, and infrastructure\(^1\)”
  
  “Over a million vulnerable fiber routers can be easily hacked\(^2\)”
  
  “Wikileaks Unveils ‘Cherry Blossom’ – Wireless Hacking System\(^3\)”

Securing Network Infrastructure

• Today’s scope: Embedded networking systems like routers, firewalls, switches, industrial and IoT gateways

• It’s important to consider security at all levels
  – But particularly firmware
LOCKING DOWN FIRMWARE
Firmware Attacks

• Why so much focus on firmware attacks?
• It’s the first link in the chain of trust
  – If you skip a link in the chain, the remaining links cannot be trusted
• Firmware hacks are usually persistent
  – Firmware is not usually updated or examined
    • Good for stealthy attacks!
  – Hacks can be un-removable*

*Without a hardware programmer
Securing Firmware

Two simple steps:

1. Make sure that the OS cannot modify firmware
   – This usually needs some kind of hardware help to lock boot flash memory

2. Make sure that the BIOS (or U-Boot or whatever) won’t update itself without checking a signature on the new image
Secure Boot

- Secure boot(*) is a process that ensures that the device boots unmodified, authorized software.
- Secure boot is achieved by providing an unbroken “chain of trust” from the first instruction executed after reset through to the OS prompt.

*aka Verified Boot
INTRODUCTION TO TRUSTED COMPUTING
What is a Trusted System?

• Predictable, even under stress
• Trust based on experience and/or evidence
• Trust based on fundamental properties:
  – Identity
  – Integrity
Trusted Computing Group (TCG)

*Open Standards for Trusted Computing*

- TCG is the *only* group focused on Trusted Computing standards

- You know TCG for our technical specs & guidance such as:
  - Trusted Platform Module (TPM = ISO 11889)
  - Self-encrypting drives (SED)
  - Trusted Network Communications (TNC)

- TPM specification implemented in more than a *billion* devices
  - Chips integrated into PCs, servers, printers, kiosks, industrial systems, and many embedded systems
Trusted Platform Module (TPM)

The Standard Hardware Root of Trust

• Trusted Platform Module (TPM)
  – Self-contained security processor
  – Inexpensive & small (~0.1 watt, ~$1)
  – Connects to inexpensive processor buses

• TPM provides:
  – Secure storage of boot state (= hashes of objects)
  – Secure storage of runtime state (= hashes of software applications)
  – Secure storage of cryptographic secrets (e.g. private keys)
  – Cryptographic-quality Random Number Generator
  – Resistance to physical attack (i.e. reverse-engineering) to keep private keys private

• Specified by Trusted Computing Group, a standards group
NETWORKING APPLICATIONS FOR TRUSTED COMPUTING
TCG Network Equipment Guidance

• *TCG Guidance for Securing Network Equipment* document
• Developed by TCG members, many involved in networking:
  – Cisco, HPE, Huawei, Juniper, and others
• Intended to help equipment vendors use TCG technology to secure network infrastructure
• Includes use cases, building blocks, and implementation guidance
• Published January 17, 2018

https://trustedcomputinggroup.org/tcg-guidance-securing-network-equipment
Applications for TPM in Networked Gear

• Cryptographic Random Number Generator (RNG)
  – Unpredictable numbers are critical to secure cryptography

• Sealing secrets
  – Keep VPN keys and other data-at-rest secure

• IEEE 802.1AR cryptographic device identification
  – Use spoof-resistant cryptographic means to identity devices

• Software attestation / health check
  – Use records kept by the TPM to fingerprint each software module run

• … and many others
Random Number Generator

*Essential for Secure Protocols*

- Protocols like IPsec, SSH, SSL and TLS use cryptographic keys
- Keys are often generated within the embedded device itself
- Keys are like passwords: *If you can guess the key, you can break the protocol.*
- Cryptographic keys are typically generated from random numbers
- Without hardware help, computer algorithms can only generate pseudo-random sequences, not truly random numbers
- Most TPMs contain a physical source of randomness (aka entropy) which can be used to generate reliable keys
Sealing Secrets

Ensure that secrets remain secret!

• The TPM can be used to protect secrets like:
  – VPN shared-secret keys
  – Disk Encryption keys

• Configure the TPM so it will only decrypt the secrets for use when the platform is in a specified state, e.g.
  – Known, unmodified OS
  – Specific platform configuration
  – User password
IEEE802.1AR Secure Device Identity

Proves Which Device is Which

- Many embedded devices are ‘remote’ and difficult to protect or even identify reliably.
- The TPM can be configured with a unique cryptographic identifier based on device serial number – based on IEEE spec 802.1AR (DevID)
- Public Key Cryptography allows the device to assert its identity
- ... and then prove possession of a difficult-to-steal private key stored inside the TPM
How Would a DevID be Used?

• Inventory
  – Ensure the devices you put in place are still there

• VPN login
  – Use DevID for remote login, so only authorized devices are allowed on your network

• Zero-Touch configuration
  – Ensure that only authorized devices can call in to obtain configuration
Attestation and Measured Boot

Proves What Software was Launched on your Device

- Secure boot works well for deterministic early stages of boot
- But multi-core processors tend to be less predictable once the OS layer starts up
- The TPM can be used to record “measurements” (= hashes) of each executable run
- The TPM can then return those measurements to a management station later, signed by a key that only the TPM can know
- “Attestation” provides cryptographic assurance of which executables actually were run.
FROM GUIDANCE TO REALITY
Real-World Implementations

• So we have a great document
  – TCG Guidance for Securing Network Equipment

• How is that becoming real?
RSA Conference 2015

*Cisco and Infineon Secure the IoT with TPM*

- Remote attestation with IoT gateway, router, and server
- TPM-Protected Identity on all systems
- Rejects unauthorized or compromised systems
RSA Conference 2016

*Huawei and Infineon Secure the IoT with TPM*

- Remote attestation with IoT gateway, router, server, and VMs
- ARM, PPC, and X86 platforms equipped with a TPM
- Server running QEMU/KVM with vTPM
- One VM acted as verifier for attestations
- Layer binding between VM and hypervisor
• Sensitive Data decrypted using key from TPM at boot time
• Decrypted secrets may be erased from DRAM when done to avoid exposure
• Secrets cannot be retrieved from a purloined system disk
What Can You Do?

• Review Network Equipment Guidance to learn more:

• If you **build** network equipment,
  – Consider adopting the described techniques

• If you **buy** network equipment,
  – Ask your network equipment providers what they’re doing about today’s advanced threats
REFERENCES
Relevant Documents

• Trusted Computing Group:
  – https://www.trustedcomputinggroup.org/

• Network Equipment documents:
  – https://trustedcomputinggroup.org/work-groups/network-equipment/

• TPM documents:
  – http://trustedcomputinggroup.org/work-groups/trusted-platform-module/

• TPM & Secure Boot:
TPM Software

- tpm2-tss
  - https://github.com/tpm2-software/tpm2-tss
- IBM TSS
  - https://sourceforge.net/projects/ibmtpm20tss/
- Mocana IoT Trust Platform
  - https://www.mocana.com/solutions
- OnBoard Security TSS
  - https://www.onboardsecurity.com/products/tss
Questions?
Post Your Questions Now

Thank You!
Contacting Trusted Computing Group

www.trustedcomputinggroup.org
admin@trustedcomputinggroup.org

LinkedIn Trusted Computing Group:
https://www.linkedin.com/groups/4555624

Twitter: @TrustedComputin

YouTube channel:
https://www.youtube.com/user/TCGadmin

BrightTalk webcasts (free): www.brighttalk.com,
search “trusted computing” for library of
demonstrations and presentations