ONIE and Secure Boot

Curt Brune
Principal Engineer
Cumulus Networks, Inc.
Talk Overview

- A Question of Trust
- Cryptographic Concepts
- Secure Technologies
- Applying it to ONIE
A Question of Trust

- Trusting Hardware
  - CPU
  - FPGA / CPLD
  - Boot Firmware

- Trusting Software
  - ONIE
  - Network OS Installer
  - Network OS Runtime
Security and Cryptographic Concepts

- Lots of Terminology
- Lots of Specifications
- Lots of Jargon
Security and Cryptographic Building Blocks

• Secure Hash (Digest)
  ▪ digest = sha256(message)

• Hash Extend
  ▪ A = hash(original A || message)

• Public / Private Key Crypto
  ▪ encrypt(key_public, message) => M'
  ▪ decrypt(key_private, M') => message
Digital Signatures

• Creating a Signature, sender
  ▪ \( \text{signature} = \text{encrypt}(\text{key}_{\text{private}}, \text{hash(message)}) \)

• Send original message and signature to recipient

• Verifying Signature, recipient
  ▪ \( \text{digest} = \text{hash(message)} \)
  ▪ \( \text{claimed_digest} = \text{decrypt}(\text{key}_{\text{public}}, \text{signature}) \)
  ▪ does \( \text{claimed_digest} == \text{digest} \) ??
Root of Trust, Chain of Trust

• Ultimately a core component of the system is “trusted”

• The trusted core verifies the next stage of the boot process before handing off control

• The next stage continues the trust relationship, verifying the next stage before handing off control

• Repeat
Each component verifies the next component.
CPU Security Technologies

- Varies by CPU Manufacturer
  - x86_64 - Intel Boot Guard, UEFI, TXT
  - ARM - Trust Zone, UEFI / Verified Boot
  - NXP
  - Thousands of pages of specifications

- All verify digital signatures in one form or another. Forms the root of trust for measurement.
Trusted Platform Module (TPM)

• Does a lot. Thousands of pages of specification.

• Measured Boot
  ▪ Platform Configuration Registers
  ▪ Hash Extend Platform State
Linux Secure Boot on x86_64

- Unified Extensible Firmware Interface (UEFI) firmware
  - Maintains a database of authorized public keys - **kek, db**
  - Maintains a database of blacklisted (revoked) keys - **dbx**
- **shimx64.efi**
  - Thin EFI application, signed by private key whose public key is in UEFI db
  - Contains a public key for verifying the next stage
  - Verifies and loads next stage
- **MokManager.efi**
  - Machine Owner Key (MOK) database
  - Supplementary database of keys for verification
  - Used by shimx64.efi during image verification
• UEFI verifies shimx64.efi
• shimx64.efi is signed by a private key, whose public key is in the UEFI db
shimx64.efi verifies grubx64.efi using one of:
  ▪ Internal key
  ▪ UEFI db, dbx
  ▪ MOK db, dbx

• Provides verification interface for grubx64.efi to use
• Measures grubx64.efi image and MOK database into TPM PCRs
• **grubx64.efi** verifies Linux kernel
• **Uses interface provided by shimx64.efi for verification**
  ▪ consults UEFI kek, db, dbx, MOK db, MOK dbx
Linux Secure Boot on x86_64, All Together

- UEFI verifies shimx64.efi
- shimx64.efi verifies grubx64.efi
- grubx64.efi verifies Linux kernel
- Linux kernel verifies kernel modules, etc.
Applying to ONIE

• ONIE is a Linux based operating system
  ▪ Linux Kernel
  ▪ initramfs

• The ONIE Secure Boot flow will follow the shim model
  ▪ ONIE shimx64.efi
  ▪ ONIE grubx64.efi
  ▪ ONIE kernel and initramfs
ONIE Image Discovery Waterfall - NEW

• Locate an installer via the image discovery waterfall
  ▪ Local file
  ▪ DHCP options
  ▪ etc...

• NEW - Verify the signature on the installer before execution
  ▪ UEFI kek, db, dbx
  ▪ MOK db, dbx
  ▪ Continue waterfall if verification fails

• Execute the Installer
  ▪ NOS installer prepares its NOS for Secure Boot
Collaboration and Input Needed

• Open Questions and Details:
  ▪ What about secure firmware updates?
  ▪ Build system modifications
  ▪ PKI, Certificate Authorities and key management
Further Reading

- Unified Extensible Firmware Interface Specification

- Platform Initialization Specification: Volume 1
  - Pre-EFI Initialization Core Interface

- TCG PC Client Platform Firmware Profile Specification
  - Level 00 Revision 00.21, March 30, 2016
  - https://trustedcomputinggroup.org/

- TCG PC Client Specific TPM Interface Specification
  - Version 1.3, 21 March 2013
  - https://trustedcomputinggroup.org/
Thank you!

Visit us at cumulusnetworks.com or follow us @cumulusnetworks