ONIE
Securing the Install Process

Curt Brune
Principal Engineer
Cumulus Networks
Talk Overview

• Quick Annual Roundup
• Root of Trust Concepts
• Booting ONIE Securely
• Verifying Installers
Since Last Year’s Summit

Contributions

• New machine definitions: 49 (more than 4 per month)
• Contributing individuals: 24
• Contributing organizations: 20

New Developments

• Improved Documentation
• Reduced Build Times
• Support Common CPU modules
• Moved to Linux kernel 4.9.y
• Hooks for Network ASIC drivers
ONIE Project Statistics

Git Commits vs. Year

Year

2013 2014 2015 2016 2017

Commits

0 100 200 300 400 500

Git Commits
ONIE Project Statistics

Machines Per Year and Cumulative

Year

2013 2014 2015 2016 2017

Machines Per Year

Machines Cumulative

2013: 3
2014: 23
2015: 37
2016: 31
2017: 49
ONIE Project Contributors – Thanks!!

- Cumulus Networks
- Mellanox
- Lenovo
- Celestica
- NXP (Qualcomm)
- Alpha Networks
- Inventec
- Juniper Networks
- Canonical
- Foxconn
- Ingrasys Technology
- Accton / Edgecore
- DELL EMC
- Delta Networks
- Quanta
- Interface Masters
- Centec Networks
- Ciena
- Intel
- Broadcom
- Platina Systems
Securing the ONIE Boot Process
Root of Trust, Chain of Trust

Each component verifies the next component
ONIE Secure Boot on x86_64

- Unified Extensible Firmware Interface (UEFI) firmware
  - Maintains a database of authorized public keys - 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
ONIE Secure Boot on x86_64, Cont.

- UEFI verifies shimx64.efi
- shimx64.efi is signed by a private key, whose public key is in the UEFI db
ONIE Secure Boot on x86_64, Cont.

- shimx64.efi verifies grubx64.efi using one of:
  - Internal key
  - UEFI db, dbx
  - MOK db, dbx
- Registers verification interface for grubx64.efi to use
• **grubx64.efi** verifies Linux kernel
• **Uses interface provided by shimx64.efi for verification**
  - consults UEFI db, dbx, MOK db, MOK dbx
ONIE 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.
ONIE Secure Boot Available Today

• Includes Build System Modifications:
  ▪ create shimx64.efi for external signing
  ▪ sign grubx64.efi with ONIE vendor key
  ▪ sign Linux kernel with ONIE vendor key

• For testing see the `kvm_x86_64` virtual machine
  ▪ QEMU with OVMF Tiancere UEFI Firmware
  ▪ Pre-made keys and certificates
  ▪ Exercises the entire secure boot flow
Future: Verifying Installers

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

- 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
Future: Installer Root of Trust

- NOS Vendors Sign Their Installers
- NOS Vendors Publish Their Public Key Certificate
- End User Enrolls NOS Vendor Cert into MOK database
- ONIE Verifies NOS Vendor Signature on the Installer
- ONIE Runs the Installer
Thank you!

Visit us at cumulusnetworks.com or follow us @cumulusnetworks

© 2018 Cumulus Networks. Cumulus Networks, the Cumulus Networks Logo, and Cumulus Linux are trademarks or registered trademarks of Cumulus Networks, Inc. or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. The registered trademark Linux® is used pursuant to a sublicense from LMI, the exclusive licensee of Linus Torvalds, owner of the mark on a world-wide basis.
Further Reading

• ONIE Secure Boot Proposal
  ▪ Version 2, April 217
  ▪ http://mirror.opencompute.org/onie/docs/ONIESecureBootv2.pdf

• Unified Extensible Firmware Interface Specification