TrenchBoot

Less-insecure Virtual Firewall Appliance
Piotr Król | coreboot, TrenchBoot, OpenEmbedded, Xen, OpenXT

What is demonstrated

**Theory**

- Firmware → Boot Loader → TrenchBoot → Operating System

**Practice**

- SPI flash:
  - coreboot (SRTM)
  - GRUB2
  - SKINIT (DRTM)
  - TrenchBoot Landing Zone
  - jmp
  - Linux+initramfs

- kexec

- Storage:
  - Xen
    - create VM → dom0
    - create VM → NDVM
    - create VM → OPNsense

Hardware Information

- PC Engines apu2 with AMD Jaguar CPU GX-412 TC
- Infineon Trusted Platform Module (TPM 2.0) SLB 9665

What was improved

**Description**

- Unifying framework for Boot Integrity Technologies (BIT)
- Advanced Measurement Collection
- Extensible, Fine Grained Verification
- Remote Attestation

**Security & Assurance Use Cases**

- Secure Over-The-Air (OTA) Updates
- Boot with Static + Dynamic Root of Trust
- Verify BIOS, firmware, hypervisor, OS
- TPM-signed Measurements

**Components**

- Coreboot-fast, secure, open-source firmware with SRTM
- GRUB2 patched to initiate AMD Secure Launch
- Open-source TrenchBoot Landing Zone implementation for AMD
- Go libraries extensible measurement enforcement + Linux kernel patched as AMD Secure Loader
- Xen Hypervisor
- NDVM (Network Driver VM) provides isolation that separate NIC and its driver from security critical firewall

Source code or detail technical information availability

- [http://github.com/TrenchBoot](http://github.com/TrenchBoot)
- [http://openxt.org](http://openxt.org)
- [http://github.com/flihp/meta-measured](http://github.com/flihp/meta-measured)