On firm footing with an extensible measured launch framework

Daniel Smith, Christopher Clark, Rich Persaud | OpenXT.org

What is demonstrated

- Intel tboot
- Trusted Grub
- UEFI Shim Loader
- UEFI Secure Boot
- AMD, ARM, Intel

Trench Boot

- Operating System
  - Trusted Storage API
  - 3rd Party Extension
  - Measurement Enforcement
  - Go runtime

- Boot Loader
  - Launch Kernel

- Firmware
  - Trusted Platform Module

- Root of Trust

Hardware Information

- PC Engines APU2 with AMD Jaguar CPU
- Trusted Platform Module (TPM) 1.2

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 Dynamic + Static Root of Trust
- Verify BIOS, firmware, hypervisor, OS
- TPM-signed Measurements

Components

- Grub patched to initiate AMD Secure Launch
- Linux kernel patched as AMD Secure Loader
- Go libraries for extensible measurement enforcement

Source code or detail technical information availability

- http://github.com/TrenchBoot
- http://openxt.org
- http://github.com/flihp/meta-measured