OpenXT Measured Boot with Xen, OE, TPM & Intel TXT

Rich Persaud | OpenXT.org

What is demonstrated

Security & Assurance Use Cases

- Cloud/Edge Infrastructure Integrity
- Guest Virtual Machine Integrity
- Application Integrity
- Hardware-Rooted Chain of Trust
- TPM-signed Measurements

OpenEmbedded Layers

- meta-virtualization
- meta-measured
- meta-selinux

Verified Software Integrity

- Intel TXT Measurements (DRTM)
  - Firmware
  - BIOS Configuration
  - Xen Hypervisor
  - Linux Kernel & initrd
- OpenXT Measurements
  - Virtual Machines

Hardware Information

- x86 Devices with Intel TXT-capable CPU & f/w
- Trusted Platform Module (TPM)

What was improved

New Features

- Management
  - Keys
  - Trusted Platform Module
  - Measured Launch
- TPM 2.0 Forward Seal
  - predict future measurements
  - unattended system update

Active Development

- tboot
- UEFI multi-boot modules
- Virtual TPM & attestation
- Xen dom0 disaggregation
- Extensible base platform

Source code or detail technical information availability

- http://OpenXT.org
- http://github.com/flihp/meta-measured
- http://github.com/starlab-io/meta-measured
- http://hg.code.sf.net/p/tboot/code