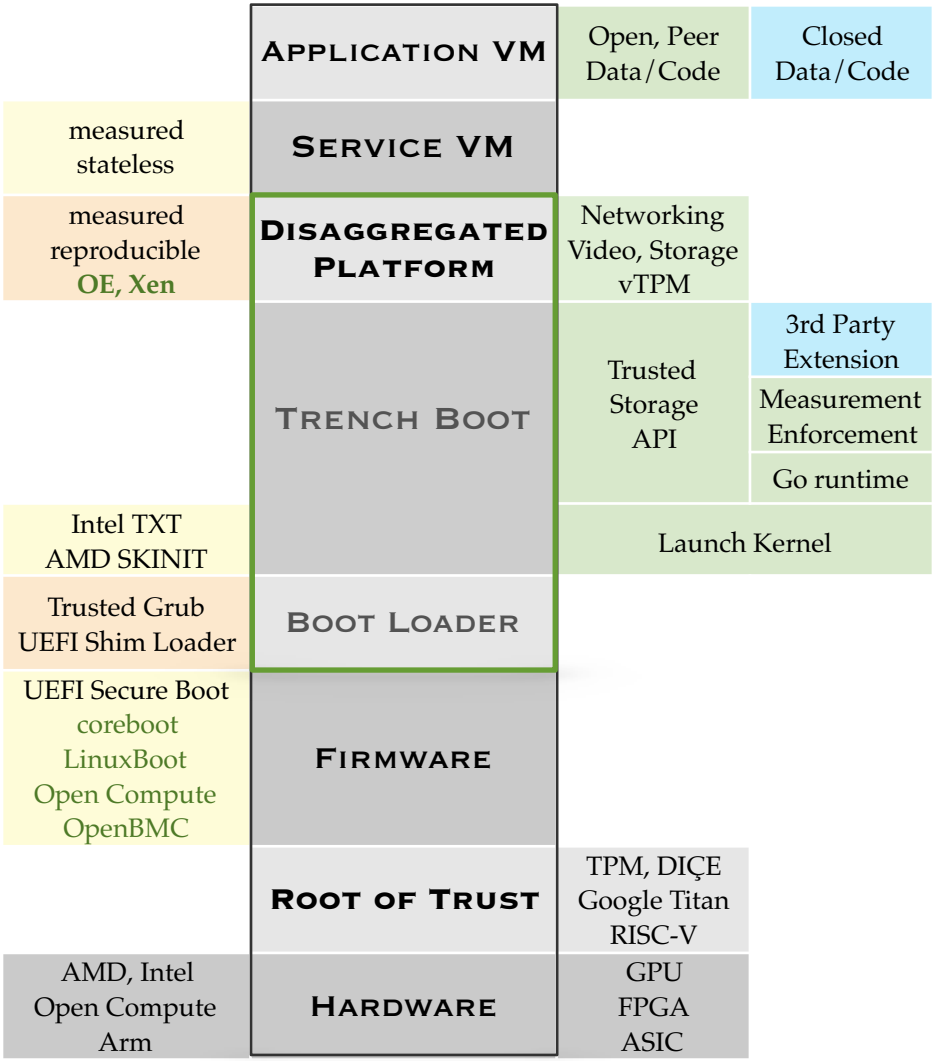
OpenXT Platform

Technical Showcase

Embedded Linux Conference Europe 2018

Trustworthy OE Devices and Software Supply Chain Integrity

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



Description

- Extensible platform based on Xen & OE meta-virtualization
- Upstream-first roadmap supports open+closed components
- Reproducible builds for critical open components
- Enables cloud, endpoint and edge use cases

Security & Assurance Use Cases

- Secure Over-The-Air (OTA) Updates
- Boot Integrity with Dynamic + Static Root of Trust
- Verify BIOS, firmware, hypervisor, OS
- TPM-signed Measurements & Attestation
- TPM 1.2 and 2.0

Industry Landscape

- HW / SW supply chain risks
- Open Compute Cerberus
- Pulp Platform RISC-V and Google Titan RoT
- Google Cloud Shielded VMs with vTPM
- Microsoft Linux and Azure Sphere IoT attestation

Source code and detailed technical information

- OE meta-virtualization layer
- OpenXT.org
- github.com/TrenchBoot
- PlatformSecuritySummit.com/2018/videos/