



Trustworthy OE Devices and Software Supply Chain Integrity

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

	APPLICATION VM	Open, Peer Data/Code	Closed Data/Code
measured stateless	SERVICE VM		
measured reproducible OE, Xen	DISAGGREGATED PLATFORM	Networking Video, Storage vTPM	
	TRENCH BOOT	Trusted Storage API	3rd Party Extension
			Measurement Enforcement
			Go runtime
Intel TXT AMD SKINIT		Launch Kernel	
Trusted Grub UEFI Shim Loader	BOOT LOADER		
UEFI Secure Boot coreboot LinuxBoot Open Compute OpenBMC	FIRMWARE		
	ROOT OF TRUST	TPM, DIÇE Google Titan RISC-V	
AMD, Intel Open Compute Arm	HARDWARE	GPU FPGA ASIC	

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/