TrenchBoot

Project description

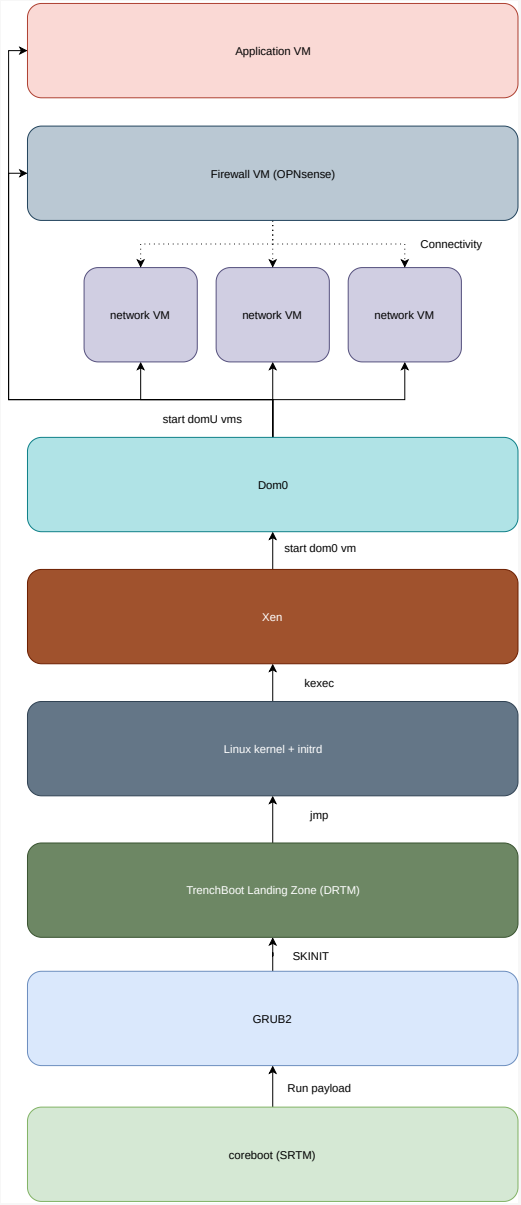
TrenchBoot is a project that aims to increase the security of firmware and software running on machines with measured launch environment aka Dynamic Root of Trust for Measurement (DRTM). There are known reference implementations of measured launch like tboot, however it supports only Intel Trusted Execution Technology (TXT). The main advantage of TrenchBoot is the support for both measured launch technologies AMD Secure Startup and Intel TXT. It can be fully integrated with most popular bootloader GRUB2. What is more the implementation for AMD is fully open-source in contrast to Intel's TXT, which require BIOS and SINIT ACM's.

Modern practices for building less-insecure systems leverage virtualization, for isolation properties and flexible support of narrow component interfaces. The Trusted Platform Module (TPM), an IC for critical cryptographic functions, is now more usable by OSS software. TPMs provide a Root of Trust for Dynamic (DRTM) and Static (SRTM) measurements for platform integrity.

These are supported by the apu2, a reliable, Low-SWaP x86 device from Swiss OEM PC Engines. Usable as SOHO firewall or industrial edge device, it has nearly-open hardware, coreboot firmware, mPCIe extensibility and an extended support lifecycle for the embedded CPU and motherboard.

The demonstration presents a software architecture design leveraging TrenchBoot capabilities and comprises:

1. Open-source firmware:
   - coreboot
   - measured and verified boot mode
   - TPM 2.0 support
   - Static Root of Trust for Measurement (SRTM)
   - permanently write protected SPI flash
2. Open-source bootloader:
   - GRUB with TrenchBoot support
   - Dynamic Root of Trust for Measurement (DRTM)
   - built from meta-measured
3. Open-source hypervisor:
   - Xen
   - built from meta-virtualization
4. Isolation through network VM based on OpenXT work
5. Open-source virtualized firewall:
   - OPNsense launched by Xen
   - NICs passed through via Xen


Application VM
Firewall VM (OPNsense)
Connectivity
network VM
network VM
network VM
start domU vms
Dom0
start dom0 vm
Xen
kexec
Linux kernel + initrd
jmp
TrenchBoot Landing Zone (DRTM)
SKINIT
GRUB2
Run payload
coreboot (SRTM)

coreboot is an open-source firmware development framework capable of enabling verified and measured boot mode with TPM 2.0. It allows to launch almost everything, starting with SeaBIOS, GRUB, Linux kernel, tianocore UEFI payload. PC Engines apu2 has been supported in coreboot for over 3 years. The verified and measured boot mode solution with coreboot has been utilized to provide Static Root of Trust for Measurement.

One is not limited to trust the firmware only. Dynamic Root of Trust for Measurement, delivered by TrenchBoot measured launch modules in GRUB, already assumes that the platform is not trusted. With this assumption hardware architecture is leveraged to establish the Root of Trust and TrenchBoot by invoking special processor instructions like SKINIT for AMD and SENTER for Intel. These technologies allow to securely measure the software like operating system or hypervisor despite the firmware may be compromised.

Xen is a type 1 hypervisor. This means it runs directly on a bare metal and is responsible for controlling the hardware and managing the guest virtual machines. It is a specialized piece of system software that manages and runs operating systems. In this demonstration Xen is launched in the measured launch environment established by TrenchBoot.

The whole design is aimed to be as secure as possible thus utilizing every security feature possible and present on the hardware. Starting with the coreboot firmware, which provides Static Root of Trust for Measurement, then move to measured launch of the Xen hypervisor with TrenchBoot modules in GRUB providing Dynamic Root of Trust for Measurement, ending with virtualized firewall with passed through network controllers. Finally we provide power and performance benchmarks for virtualization overhead.

Due to various environments the components are built in, they have been integrated into OpenEmbedded meta layers for ease of use and complexity reduction. The proposed build is a qualified industrial grade secure firewall solution. The usage of simple and widely available low cost hardware makes the whole solution the most attractive choice in the world.