Non-UEFI-aware measured boot using coreboot, GRUB and TPM2.0

LPC 2019: System Boot and Security MC

Piotr Król

3MDEB

About me

Piotr Król
Founder & Embedded Systems Consultant

- open-source firmware
- platform security
- trusted computing

@pietrushnic
piotr.krol@3mdeb.com
linkedin.com/in/krolpiotr
facebook.com/piotr.krol.756859

Problem statement

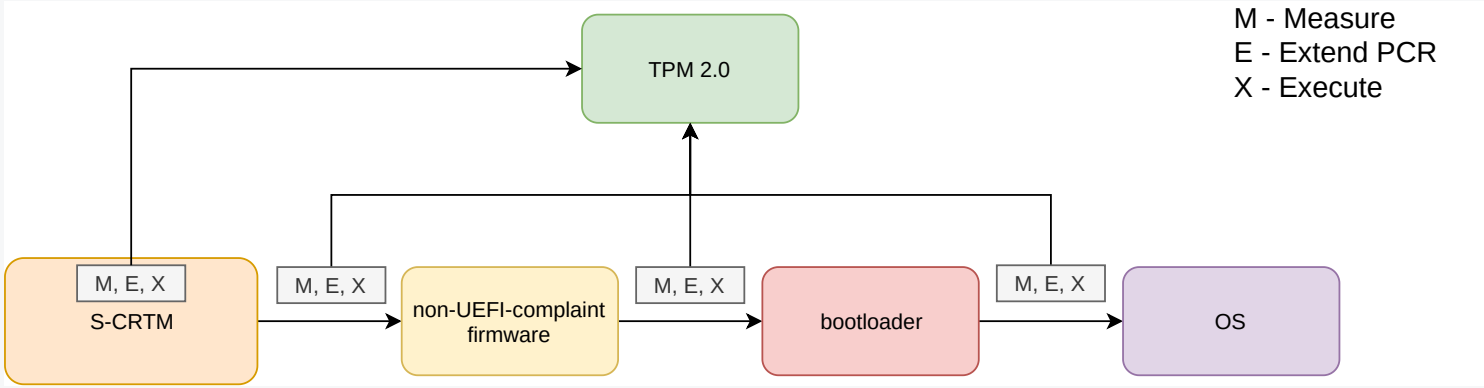
- boot process integrity works for UEFI-compliant systems
- there are boot firmware implementations that are natively non-UEFI-compliant
  - coreboot/libreboot/oreboot
  - U-Boot
  - LinuxBoot
  - SeaBIOS
  - Legacy BIOS/UEFI CSM
  - skiboot
- existing solutions
  - petitboot - measured kexec to Linux
  - TrustedGRUB2 - use INT 1Ah, only TPM 1.2 implementation, not widely adopted
- other effort
  - HardenedBSD Call for Participations to unify and collaborate on security issues

https://twitter.com/HardenedBSD/status/1170040875075985408

Who should care

- Chrombooks users who want to repurpose the device
- Users of previously mentioned firmware stacks
- All distros supporting non-UEFI/legacy boot
- Cloud providers using QEMU with SeaBIOS (?)
    - Xen
    - Proxmox

What is needed?



- **S-CRTM** - Static Code/Core Root of Trust for Measurement
- **bootloader** - GRUB/GRUB2, SeaBIOS
- **OS** - Linux, BSD, L4 based OSes, multiboot, ReactOS

State of various components

- coreboot
  - can M,E,X since it was proven through Vboot implementation
  - finally measures payload and jumps to it
  - question is if payload can take that further?
- LinuxBoot
  - typically starts as jump from UEFI PEI
  - pre UEFI PEI phases can implement Intel Boot Guard or similar method
  - there is no official way to provision system in compliance with Intel documentation and keep chain of trust
  - if starts from coreboot then M,E,X should work without problem
  - if start from U-Boot SPL situation highly depends on proprietary hardware implementation
  - seem to be from kexec camp

State of various components

- GRUB2
  - depends what and how it boots (bootloader in SPI vs HDD/SSD/eMMC)
  - there is no support for measured boot for MBR based boot
- SeaBIOS
  - supports TPM 1.2 and 2.0
  - expose INT 1Ah interface
  - TrustedGRBU2 seem to be the only user

TrustedGRUB2

- Use API INT 1Ah from **TCG PC Client Specific Implementation Specification for Conventional BIOS**
- Supports only TPM 1.2
- INT 1Ah (...) allows the caller of the interface to have direct access to a limited set of TSS functions and a pass-through to the TPM.
- TrustedGRUB2 can leverage previously installed interface, the only known BIOS implementation that do it is SeaBIOS
- Topic is extensively discussed here: https://github.com/Rohde-Schwarz/TrustedGRUB2/issues/23

Others

petitboot

- How petitiboot manage to perform measured kexec?

LinuxBoot

- It is possible to extend kexec to use already implemented support for TPM in LinuxBoot (Go)

Open questions

- Is there any other solution that we missing?
- Does adoption of INT 1Ah still make sense in light of expanding kexec based solutions?
- Can we really kexec everything and keep chain of trust?

Summary

- It looks like we have 2 camps
  - INT 1Ah
  - kexec
- BSD-world may be not exactly happy with kexec'ing
  - https://forums.freebsd.org/threads/kexec-into-freebsd.59123/
- We doubt that Legacy BIOS/UEFI CSM with INT 1Ah exist
- Both solutions would require implementation in bootloader for cases where bootloader is included in firmware (e.g. coreboot)

Q&A