Contribution ID: **293** Type: **not specified**

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

Wednesday, September 11, 2019 5:40 PM (25 minutes)

The main issue in using TPM2.0 in such measured boot solution is that at the moment of writing this abstract neither Trusted Grub, nor Linux kernel has TPM2.0 implementation. There are of course implementations based on UEFI systems, where bootloaders can utilize TCG EFI protocol to handle TPM. However other non-UEFI based solutions suffer from lack of TPM2.0 drivers in the bootloaders. Taking, for example, coreboot with vboot and measured mode the chain of trust ends on at verifying and measuring the MBR code. This limits the trusted boot technology for firmware solutions that do not base on UEFI specification.

As TPM2.0 is already supported in coreboot, the next stage would be enabling it in GRUB2. As a matter of fact that TPM1.2 has already been enabled in its derivative, Trusted GRUB2.0, but we consider it much unsatisfying.

Chain of trust:

coreboot + payload -(chain cuts here)-> Trusted GRUB -> kernel

Establishing a chain of trust will make SRTM (Static Root of Trust for Measurement) based on coreboot fully featured. As security solutions are used more and more widely it will help coreboot to stay up to date with all the competitor's proprietary solutions.

I agree to abide by the anti-harassment policy

Yes

I confirm that I am already registered for LPC 2019

Primary authors: KRÓL, Piotr (3mdeb Embedded Systems Consulting); Mr MICHAŁ, Żygowski (3mdeb Embedded Systems Consulting)

Presenters: KRÓL, Piotr (3mdeb Embedded Systems Consulting); Mr MICHAŁ, Żygowski (3mdeb Embedded Systems Consulting)

Session Classification: System Boot and Security MC