Contribution ID: **124** Type: **not specified**

Passing and retrieving information from bootloader and firmware

Thursday, August 27, 2020 10:25 AM (25 minutes)

Each operating system relies on the information exposed to it by the firmware. It consists of various data like memory map, device structure (either ACPI or devicetree), firmware version, vendor, etc. But passing information from operating system bootloader has been neglected for many years. In this presentation, we will mainly focus on retrieving information from firmware and bootloader by Linux kernel with a special focus on bootloader log and DRTM TPM event log.

I agree to abide by the anti-harassment policy

I agree

Primary authors: Mr KIPER, Daniel (Oracle); Mr ŻYGOWSKI, Michał (3mdeb Embedded Systems Consulting)

Presenters: Mr KIPER, Daniel (Oracle); Mr ŻYGOWSKI, Michał (3mdeb Embedded Systems Consulting)

Session Classification: System Boot and Security MC

Track Classification: System Boot and Security MC