Contribution ID: **251** Type: **not specified**

Measured Boot, Secure Attestation & co, with systemd

Wednesday 18 September 2024 12:40 (20 minutes)

systemd has gained various TPM-related components in the recent past, to make measured boot on generic Linux reality.

In this talk I'd like to shed some light on recent developments in this area, and what comes next. Some of the topics touched will (probably) be:

- Additional PCRs via nvindexes
- Measurement logs
- An API for quotes of system state, and remote attestation
- Dynamically managed, local PCR policies with systemd-pcrlock
- Setting the TPM's clock
- Measuring more resources and events

Primary author: POETTERING, Lennart

Presenter: POETTERING, Lennart

Session Classification: System Boot and Security MC

Track Classification: System Boot and Security MC