Contribution ID: **420** Type: **not specified**

Challenges in developing trustworthy Linux-based systems in an open-source way

Wednesday, 18 September 2024 10:00 (20 minutes)

The presentation highlights five challenging areas and activities to address those in various communities over the last two years.

- Lack of OS awareness about hardware security capabilities leads to the inability to evaluate and improve system security posture. Platform security and the challenges of closing System Management Mode (SMM) created a gap in an open-source way.
- The growth of hardware and firmware components like AMD SMM Supervisor, Intel PPAM, or MS Pluton and how effectively those block building trustworthy systems in parallel, creating an ecosystem in which we cannot leverage the full potential of hardware and firmware in our machines.
- Plans for defeating the lack of consistent assessment, implementation, and provisioning of Root of Trust on very different hardware configurations through Caliptra, DICE, SPDM, and more, as well as what impact it may have on the OS.
- Lessons learned from making DRTM for Intel CPUs a first-class citizen in Linux kernel impact on support for AMD.

The topics will be considered in the context of other presentations planned for the 2024 edition of System Boot and Security MC.

Primary author: KRÓL, Piotr (3mdeb)

Presenter: KRÓL, Piotr (3mdeb)

Session Classification: System Boot and Security MC

Track Classification: System Boot and Security MC