Contribution ID: **448** Type: **not specified**

The Future of Platform Security Measurement in Linux

Saturday 13 December 2025 10:25 (20 minutes)

The LVFS Host Security ID (HSI) has become the de facto standard for measuring platform security in Linux, with major distributions adopting it to present security posture to end users. Designed primarily around proprietary UEFI implementations, HSI may present edge cases for open-source firmware vendors working with diverse firmware stacks like coreboot and edk2.

This session examines platform security measurement approaches across operating systems and explores opportunities to enhance Linux implementation. We'll discuss potential kernel API extensions to simplify and unify the assessment of the advanced security features, such as SRTM or DRTM.

Primary author: PIJANOWSKI, Maciej (3mdeb)

Presenter: PIJANOWSKI, Maciej (3mdeb)

Session Classification: System Boot and Security MC

Track Classification: System Boot and Security MC