Contribution ID: **50** Type: **not specified**

TPMs and the Linux Kernel: unlocking a better path to hardware security

Friday 12 December 2025 15:00 (45 minutes)

TPMs have been present in modern laptops and servers for some time now, but their adoption is quite low. While operating systems do provide some security features based on TPMs (think of BitLocker on Windows or dm-verity on Linux) third party applications or libraries usually do not have TPM integrations.

One of the main reasons of low TPM adoption is that interfacing with TPMs is quite hard: there are competing TPM software stacks (Intel vs IBM), lack of key format standardization (currently being worked on) and many operating systems are not set up from the start to make TPM easily available (TPM device file is owned by root or requires privileged group for access). Even with a proper software stack the application may have to deal with low-level TPM communication protocols, which are hard to get right.

In this presentation we will explore a better integration of TPMs with some Linux Kernel subsystems, in particular: kernel keystore and cryptographic API. We will see how it allows the Linux Kernel to expose hardware-based security to third party applications in an easy to use manner by encapsulating the TPM communication complexities as well as providing higher-level use-case based security primitives.

Primary author: KORCHAGIN, Ignat (Cloudflare)

Presenter: KORCHAGIN, Ignat (Cloudflare)

Session Classification: LPC Refereed Track

Track Classification: LPC Refereed Track