Contribution ID: **192** Type: **not specified**

Enhancing Trust: The Evolution of Trusted Keys in the Linux Kernel

Thursday, 19 September 2024 17:45 (45 minutes)

Embedded System-on-Chips (SoCs) provide unique, device-specific keys for encrypting and decrypting user data, serving as a Root of Trust (ROT) store crucial for security. Historically, the Trusted Keys framework in the Linux Kernel was tightly integrated with Trusted Platform Module (TPM), limiting the ability to incorporate additional sources of trust like Trusted Execution Environments (TEE). Starting from v5.13, the Kernel now supports a flexible Trusted Keys framework, enabling the integration of various underlying trust sources. Initial efforts have integrated TPM and TEE into this framework.

Over the last three years, significant progress has been made with the addition of hardware sources of trust such as CAAM and DCP (introduced in 6.10). This presentation dives into the evolution of trusted keys, current framework capabilities, and supported trust sources (TPM, TEE, CAAM, DCP). It also outlines ongoing efforts, planned for v6.12, to incorporate Hardware Unique Keys (HUK) for STM32 platforms. Additionally, the talk explores the implementation of the trusted keys retention service in the Kernel, including applications in DM-Crypt and fscrypt from userspace.

Primary author: N, Parthiban (Linumiz)

Presenter: N, Parthiban (Linumiz)

Session Classification: LPC Refereed Track

Track Classification: LPC Refereed Track