Contribution ID: **258** Type: **not specified**

Kernel TEE subsystem evolution

Monday, September 12, 2022 11:15 AM (35 minutes)

A Trusted Execution Environment (TEE) is an isolated execution environment running alongside an operating system. It provides the capability to isolate security-critical or trusted code and corresponding resources like memory, devices, etc. This isolation is backed by hardware security features such as Arm TrustZone, AMD Secure Processor, etc.

This session will focus on the evolution of the TEE subsystem within the kernel, shared memory management between the Linux OS and the TEE, and the concept of the TEE bus. Later, we'll look at its current applications, which include firmware TPM, HWRNG, Trusted Keys, and a PKCS#11 token. Along with this, we will brainstorm on its future use-cases as a DRTM for remote attestation, among others.

I agree to abide by the anti-harassment policy

Yes

Primary author: GARG, Sumit

Presenter: GARG, Sumit

Session Classification: System Boot and Security MC

Track Classification: LPC Microconference: System Boot and Security MC