Contribution ID: **194** Type: **not specified**

Protected KVM: Memory protection of KVM guests in Android

Monday, August 24, 2020 10:30 AM (15 minutes)

This talk outlines a proposal to re-factor and extend the arm64/KVM implementation in order to enable the execution of guest VMs in memory carveouts protected from the host kernel, as well as potential use-cases in the Android world. Using this architecture, we intend to remove the host kernel from the Trusted Computing Base, hence protecting guest secrets, such as private user data, against attacks targeting the host.

I agree to abide by the anti-harassment policy

I agree

Presenter: PERRET, Quentin (Google)

Session Classification: Android MC

Track Classification: Android MC