Contribution ID: **230** Type: **not specified**

TrenchBoot Update

Monday, September 12, 2022 12:55 PM (35 minutes)

Presented here will be an update on TrenchBoot development, with a focus on the Linux Secure Launch upstream activities and the building of the new late launch capability, Secure ReLaunch. The coverage of the upstream activities will focus on the redesign of the Secure Launch start up sequence to accommodate efi-stub's requirement to control Linux setup on EFI platforms. This will include a discussion of the new Dynamic Launch Handler (dl-handler) and the corresponding Secure Launch Resource Table (SLRT). The talk will then progress into presenting the new Secure ReLaunch capability and its use cases. The conclusion will be a short roadmap discussion of what will be coming next for the launch integrity ecosystem.

I agree to abide by the anti-harassment policy

Yes

Primary authors: SMITH, Daniel (Apertus Solutions, LLC); PHILIPSON, Ross (Oracle)

Presenter: SMITH, Daniel (Apertus Solutions, LLC)

Session Classification: System Boot and Security MC

Track Classification: LPC Microconference: System Boot and Security MC