Linux Plumbers Conference 2019

Contribution ID: **276** Type: **not specified**

TrenchBoot - how to nicely boot system with Intel TXT and AMD SVM

Wednesday, 11 September 2019 16:05 (25 minutes)

TrenchBoot is a cross-community OSS integration project for hardware-rooted, late launch integrity of open and proprietary systems. It provides a general purpose, open-source DRTM kernel for measured system launch and attestation of device integrity to trust-centric access infrastructure. TrenchBoot closes the the measurement gap and reduces the need to trust system firmware. This talk will introduce TrenchBoot architecture and recent work within Oracle to launch the Linux kernel directly with Intel TXT or AMD SVM Secure Launch. It will propose mechanisms for integrating a Linux distro into a TrenchBoot system launch. DRTM-enabled capabilities for client, server and embedded platforms will be presented for consideration by the Linux community.

I agree to abide by the anti-harassment policy

Yes

I confirm that I am already registered for LPC 2019

Primary author: KIPER, Daniel

Presenter: KIPER, Daniel

Session Classification: System Boot and Security MC