Contribution ID: **254** Type: **not specified**

reference Integrity measurements for TPM2 security policy

Wednesday, 11 September 2019 17:20 (20 minutes)

Firmware on commodity PCs have used the TPM to store integrity measurements from security relevant components as part of the boot process for some time. Grub2 has recently merged patches that extend this integrity measurement chain through to the launching of the OS kernel. Collecting and storing these measurements in the TPM is a necessary precondition for implementing authorization policy based on the state of the system, but this alone is insufficient.

This talk will begin by discussing the current state of boot-time integrity measurement collection in UEFI firmware and Grub2. We'll then present a notional use-case implementing security controls based on TPM2 policy mechanisms while describing the plumbing required to enable interaction with the TPM2 device. The remainder of this talk will then discuss the existing gaps in software and tooling required to implement workflows for managing configuration of the relevant security controls across system install and update operations.

I agree to abide by the anti-harassment policy

Yes

I confirm that I am already registered for LPC 2019

Primary author: TRICCA, Philip (Intel)

Presenter: TRICCA, Philip (Intel)

Session Classification: System Boot and Security MC