Contribution ID: **137** Type: **not specified**

Using DICE Attestation for SEV and SNP Hardware Rooted Attestation

Tuesday, 13 September 2022 11:00 (20 minutes)

Device Identifier Composition Engine (DICE) is a measured boot solution for systems without a TPM or similar hardware based capabilities. DICE is a layered approach meaning that each layer or software component of a boot takes inputs from the previous layer, its measurement and certificate, and then generates the same for the next phase of the boot. The output of this layering provides a strong code identity of all components of the boot. Since not all Confidential VM hardware contains TPM-like capabilities for attestation, DICE may be a solution for providing a meaningful attestation story for linux workloads in these environments.

I agree to abide by the anti-harassment policy

Yes

Primary author: GONDA, Peter (Google)

Presenter: GONDA, Peter (Google)

Session Classification: Confidential Computing MC

Track Classification: LPC Microconference: Confidential Computing MC