Contribution ID: **117** Type: **not specified**

# Securely booting confidential VMs with encrypting disk

*Tuesday, September 13, 2022 10:40 AM (20 minutes)*

Confidential Computing technologies offer guest memory encryption, but there's no standard way to securely start a confidential VM with encrypted disk. Such VMs must unlock the disk inside the guest, so the passphrase is not accessible to the host. However, in TDX and SEV-SNP guest attestation and secure secret injection depend on guest kernel features, so grub cannot be used for unlocking. Unlocking the encrypted disk later during boot is possible, but may allow various passphrase-stealing attacks to sneak into the boot stages before unlocking, and therefore requires stricter guest measurement. Unlocking at a later stage also means that upgrading the kernel and initrd inside the guest is more complex.

The talk will present various options for securely starting a confidential VM with encrypted disk for SEV, SEV-ES, SEV-SNP and TDX using embedded grub, measured direct boot, or secure vTPMs. We'd like to gather feedback from plumbers working on the kernel and adjacent projects (QEMU, OVMF, and other guest firmware) towards defining a mechanism for starting confidential VMs with encrypted disk in a way that is secure, works on different TEEs, easy to maintain and upgrade, and open-source.

## I agree to abide by the anti-harassment policy

Yes

**Primary authors:** MURIK, Dov (IBM); FELDMAN-FITZTHUM, Tobin (IBM)

**Presenters:** MURIK, Dov (IBM); FELDMAN-FITZTHUM, Tobin (IBM)

**Session Classification:** Confidential Computing MC

**Track Classification:** LPC Microconference: Confidential Computing MC