Contribution ID: **334** Type: **not specified**

Oak stage0: a minimal firmware for (confidential) virtual machines

Oak stage0 is a VM firmware, mainly targeting QEMU microvm and Q35 machines (and compatible VMMs) that is simpler (and less featureful) than the traditional choices of EDK2/OVMF and SeaBIOS. The main purpose of stage0 is to provide a smaller and simpler method of booting confidential virtual machines to reduce the TCB. To that end, stage0 supports AMD SEV-SNP and Intel TDX; stage0 is the first step in how Project Oak provides falsifiable claims about confidential workloads via remote attestation.

We go over the basic design decisions behind stage0, what features it has and equally importantly what features it doesn't have. We will also touch on issues that we've encountered in the Linux kernel, as stage0 is not an EFI firmware.

Stage0 is written in Rust and is available in the Oak repository, https://github.com/project-oak/oak/

Primary author: Mr SAAR, Andri (Google)

Presenter: Mr SAAR, Andri (Google)

Session Classification: System Boot and Security MC

Track Classification: System Boot and Security MC