Contribution ID: **310** Type: **not specified**

Extending EFI support in Linux to new architectures

Tuesday, September 13, 2022 12:30 PM (30 minutes)

An overview will be presented of recent work in the Linux/EFI subsystem and associated projects (u-boot, Tianocore, systemd), with a focus on generic support for the various new architectures that have adopted EFI as a supported boot flow. This includes UEFI secure boot and/or measured boot on non-Tianocore based EFI implementations, generic decompressor support in Linux and early handling of RNG seeds provided by the bootloader.

Note that topics related to confidential computing (TDX, SEV) will not be covered here: there are numerous other venues at LPC and the KVM Forum that already cover this in more detail.

I agree to abide by the anti-harassment policy

Yes

Primary authors: BIESHEUVEL, Ard (Google); APALODIMAS, Ilias

Presenters: BIESHEUVEL, Ard (Google); APALODIMAS, Ilias

Session Classification: linux/arch MC

Track Classification: LPC Microconference: linux/arch MC