Contribution ID: **38** Type: **not specified**

System Boot and Security MC

The System Boot and Security Microconference has been a critical platform for enthusiasts and professionals working on firmware, bootloaders, system boot, and security. This year, once again, we want to focus on the challenges that arise when upstreaming boot process improvements to the Linux kernel and bootloaders. Our experience shows that the introduction of new and/or not well-known technologies into the kernel are especially difficult. The TrenchBoot project is a very good example here, but we think others are also impacted. So, it would be good to take all project stakeholders in one room and think what does not work, what can be improved, etc. Though we are also happy to hear and discuss what is currently happening in other areas related to platform initialization and OS boot. Especially discussion about obstacles, not only technical ones, during upstreaming and finding solutions during the MC can be very valuable for various projects and the audience.

We welcome talks on the following things that can help achieve the goals mentioned above:
- TrenchBoot, tboot,
- TPMs, HSMs, secure elements,
- Roots of Trust: SRTM and DRTM,
- Intel TXT, SGX, TDX,
- AMD SKINIT, SEV,
- ARM DRTM,
- Growing Attestation ecosystem,
- IMA,
- TianoCore EDK II (UEFI), SeaBIOS, coreboot, U-Boot, LinuxBoot, hostboot,
- Measured Boot, Verified Boot, UEFI Secure Boot, UEFI Secure Boot Advanced Targeting (SBAT),
- shim,
- boot loaders: GRUB, systemd-boot/sd-boot, network boot, PXE, iPXE,
- UKI,
- u-root,
- OpenBMC, u-bmc,
- legal, organizational, and other similar issues relevant to people interested in the system boot and security.

Primary authors: KIPER, Daniel; KRÓL, Piotr (3mdeb)

Presenters: KIPER, Daniel; KRÓL, Piotr (3mdeb)