Contribution ID: **30** Type: **not specified**

System Boot and Security MC

CFP closes on July 14th
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, the conference focuses on the challenges that arise when upstreaming boot process improvements to Linux kernel. Cryptography, which is an ever evolving field, poses unique demands on secure elements and TPMs as newer algorithms are introduced and older ones are deprecated. Additionally, new hardware architectures with DRTM capabilities, such as ARM's D-RTM specification, and the increased use of fTPMs in innovative applications, add to the complexity of the task. This is the fifth time in the last six years that the conference is being held.

Trusted Platform Modules (TPMs) for encrypting disks have become widespread across various distributions. This highlights the vital role that TPMs play in ensuring platform security. As the field of confidential computing continues to grow, virtual machine firmware must evolve to meet end-users demands, and Linux would have to leverage exposed capabilities to provide relevant security properties. Mechanisms like UEFI Secure Boot that were once limited to OEMs now empower end-users. The System Boot and Security Microconference aims to address these challenges collaboratively and transparently. We welcome talks on the following technologies that can help achieve this goal.

- TPMs, HSMs, secure elements
- Roots of Trust: SRTM and DRTM
- Intel TXT, SGX, TDX
- AMD SKINIT, SEV
- ARM DRTM
- Growing Attestation ecosystem,
- IMA
- TrenchBoot, tboot
- 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: GRUB2, 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 system boot and security.

If you want to participate in this microconference and have ideas to share, please use the Call for Proposals (CFP) process. Your submissions should focus on new advancements, innovations, and solutions related to firmware, bootloader, and operating system development. It's essential to explain clearly what will be discussed, why and what outcomes you expect from the discussion.

P.S. We can only make it on September 18 because of conflict with other event.

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

Co-author: GARRETT, Matthew (Google)

Track Classification: LPC Microconference Proposals