Contribution ID: **25** Type: **not specified**

System Boot and Security MC

In the fourth year in a row, we are going to bring together people interested in the
firmware, bootloaders, system boot, security, etc., and discuss all these topics
during the System Boot and Security microconference. This year we would like to focus on better communication and closer cooperation between Free Software and Open Source projects which are building blocks of Free OSes. Past months and even years showed us that the lack of one or both very often delays introduction of very interesting and important features. A good example is the TrenchBoot project. Lack of or sporadic communication and cooperation between the TrenchBoot project and Linux kernel developers made it difficult to understand each other's requirements and needs. This has resulted in the TrenchBoot project being stuck in limbo. This situation is improving due to the interactions from last year's System Boot and Security MC, but there are still areas for improvement. As such we think the System Boot and Security MC is a good place to discuss technical and organizational problems which may happen due to not ideal communication and cooperation. Though we do not limit this MC to this kind of problems and want to encourage all stakeholders to bring and discuss issues that they are encountering in broadly understood system boot and security.

Below is the list of topics that would be nice to cover. This is not exhaustive and can be extended if needed.

Expected topics:
- TPMs, HSMs, secure elements
https://trustedcomputinggroup.org/work-groups/pc-client/
- Roots of Trust: SRTM and DRTM
https://trustedcomputinggroup.org/resource/d-rtm-architecture-specification/
- Intel TXT, SGX, TDX
https://software.intel.com/content/www/us/en/develop/articles/intel-sdm.html
https://ww.intel.com/content/www/us/en/software-developers/intel-txt-software-development-guide.html
https://software.intel.com/content/dam/develop/external/us/en/documents/intel-tdx-module-1eas.pdf
- AMD SKINIT, SEV,
https://www.amd.com/system/files/TechDocs/24593.pdf
- ARM DRTM
- Growing Attestation ecosystem,
- IMA,
https://www.redhat.com/en/blog/how-use-linux-kernels-integrity-measurement-architecture
- TrenchBoot, tboot,
https://github.com/TrenchBoot
https://sourceforge.net/projects/tboot/
- UEFI, coreboot, U-Boot, LinuxBoot, hostboot,
- Measured Boot, Verified Boot, UEFI Secure Boot, UEFI Secure Boot Advanced Targeting (SBAT),
- shim,
https://github.com/rhboot/shim
- boot loaders: GRUB2, SeaBIOS, network boot, PXE, iPXE,
- u-root,
- OpenBMC, u-bmc,
https://github.com/openbmc/openbmc
https://github.com/u-root/u-bmc
- legal, organizational and other similar issues relevant for
people interested in system boot and security.

If you are interested in participating in this microconference and have topics

to propose, please use the CFP process. Please note that submissions should be targeted at new developments, innovations and solving new problems on the boundary of firmware, bootloader and operating system. Be sure to explain well why and what is going to be discussed.

I agree to abide by the anti-harassment policy

Primary authors: KIPER, Daniel; ŻYGOWSKI, Michał (3mdeb Embedded Systems Consulting); GARRETT, Matthew (Google); KRÓL, Piotr (3mdeb Embedded Systems Consulting)

Presenters: KIPER, Daniel; ŻYGOWSKI, Michał (3mdeb Embedded Systems Consulting)

Track Classification: LPC Microconference Track (CLOSED)