Contribution ID: **43** Type: **not specified**

System Boot and Security Microconference

In the third 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 System Boot and Security microconference. Last year BootHole events showed how crucial is platform initialization for the overall system security. These events exposed many weaknesses and shortcomings in current boot processes. However, they also allowed us to tighten cooperation between various companies and organizations and finally improve overall systems security. Now it is a good time to discuss lessons learned and what should be improved in the future. There is also a lot of room to explore new platform initialization methods and mechanisms provided by CPUs, motherboards, and other components to achieve this goal. Perfect sessions should discuss various designs and/or the issues and limitations of the available firmware, bootloaders, security technologies, etc., and solutions that were found during the development process. We are also welcome discussions about legal and organizational issues which hinder communities working on system boot and/or 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
- ways to improve attestation,
- 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.

Achivements:
-TrenchBoot AMD: 3mdeb obtained funds from NLNet foundation to contribute to TrenchBoot for AMD platforms:
https://nlnet.nl/project/OpenDRTM/
The funding covered various open-source contributions to LandingZone, GRUB2, and Linux kernel
https://xenbits.xen.org/gitweb/?p=xen.git;a=commit;h=e4283bf38aae6c2f88cdbdaeef0f005a1a5f6c78
https://github.com/ipxe/ipxe/pull/300
https://lists.gnu.org/archive/html/grub-devel/2020-11/msg00050.html
https://lkml.org/lkml/2020/11/13/1280

-TrenchBoot Steering Committee was created
-TrenchBoot Steering Committee participate with Arm D-RTM specification working group
-TrenchBoot Intel: Oracle implemented Intel TXT support in the Linux kernel and GRUB; a few version of RFC patches were posted and discussed; the design, except TPM driver in early kernel boot code, is mostly accepted at this point; next version of Linux kernel and GRUB patches are under development.
https://lkml.org/lkml/2020/9/24/844
https://lkml.org/lkml/2021/6/18/878
-GRUB: BootHole and further security developments; new UEFI LoadFile2 boot protocol implementation for GRUB - RFC patches posted; we want to discuss maintenance improvements and free software communities expectations.
https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html
https://lists.gnu.org/archive/html/grub-devel/2021-03/msg00007.html
-LVFS/fwupd - there was a lot of contribution over last 12 months, hard to point to everything:
https://github.com/fwupd/fwupd/pull/3420
https://github.com/fwupd/fwupd/pull/3343
https://github.com/fwupd/fwupd/pull/3258
https://github.com/fwupd/fwupd/pull/3274
https://github.com/fwupd/fwupd/pull/2874
https://github.com/fwupd/fwupd/pull/2710

Key people:

- Daniel Kiper,
- Piotr Król,
- Matthew Garret,
- Daniel P. Smith (ask for participation),
- Ross Philipson (ask for participation),
- Andrew Cooper (ask for participation),
- Lief Lindholm (ask for participation),
- Peter Jones (ask for participation),
- Javier Martinez (ask for participation),
- Ron Minnih (ask for participation).
- Lief Lindholm (ask for participation),

I agree to abide by the anti-harassment policy

I agree

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

Session Classification: System Boot and Security MC

Track Classification: System Boot and Security MC