Contribution ID: **201** Type: **not specified**

Towards Secure Unified Kernel Images for Generic Linux Distributions and Everyone Else

Monday, 12 September 2022 17:00 (40 minutes)

In this talk we'll have a look at:

- systemd-stub (the UEFI stub for the Linux kernel shipped with systemd)
- unified kernels (i.e. kernel images glued together from systemd-stub, the kernel itself, an initrd, and more)
- systemd-sysext (an extension mechanism for initrd images and OS images)
- systemd service credentials (a secure way to pass authenticated and encrypted bits of information to services, possibly stored on untrusted media)
- systemd's Verity support (i.e. setup logic for file system images authenticated by the kernel on IO, via dm-verity)
- systemd's TPM2 support (i.e. ability to lock credentials or disks to TPM2 devices and software state)
- systemd's LUKS support (i.e. ability to encrypt disks, possibly locked to TPM2)

And all that with the goal of providing a conceptual framework how to implement simple unified kernel images, that are immutable, yet extensible and parameterizable, are fully authenticated and measured, and that allow binding the root fs encryption or verity to them, in a reasonably manageable way.

The intention is to show a path for generic distributions to make use of UEFI SecureBoot and actually provide useful features for a trusted boot, putting them closer to competing OSes such as Windows, MacOS and ChromeOS, without losing too much of the generic character of the classic Linux distributions.

I agree to abide by the anti-harassment policy

Yes

Primary author: POETTERING, Lennart

Presenter: POETTERING, Lennart

Session Classification: Service Management and systemd MC

Track Classification: LPC Microconference: Service Management and systemd MC