Contribution ID: **69** Type: **not specified**

New design for initrds

Monday, 12 September 2022 17:45 (40 minutes)

Distributions ship signed kernels, but initrds are generally built locally. Each machine gets a “unique” initrd, which means they cannot be signed by the distro, the QA process is hard, and development of features for the initrd duplicates work done elsewhere.

Systemd has gained “system extensions“ (sysexts, runtime additions to the root file system), and “credentials“ (secure storage of secrets bound to a TPM). Together, those features can be used to provide signed initrds built by the distro, like the kernel. Sysexts and credentials provide a mechanism for local extensibility: kernel-commandline configuration,
secrets for authentication during emergency logins, additional functionality to be included in the initrd, e.g. an sshd server, other tweaks and customizations.

Mkosi-initrd is a project to build such initrds directly from distribution rpms (with support for dm-verity, signatures, sysexts). We think that such an approach will be more maintainable than the current approaches using dracut/mkinitcpio/mkinitramfs. (It also assumes we use systemd to the full extent in the initrd.)

During the talk I want to discuss how the new design works at the technical level, but also how distros can use it to provide more secure and more managable initrds, and the security assumptions and implications.

I agree to abide by the anti-harassment policy

Yes

Primary author: JĘDRZEJEWSKI-SZMEK, Zbigniew (Red Hat)

Presenter: JĘDRZEJEWSKI-SZMEK, Zbigniew (Red Hat)

Session Classification: Service Management and systemd MC

Track Classification: LPC Microconference: Service Management and systemd MC