systemd-boot, systemd-stub, UKIs

FOSDEM 2024, Brussels

Lennart Poettering, Microsoft

systemd-boot

Note quite a boot loader

Fancy boot menu

Doesn’t actually load binaries into memory, just chain loads them

Finds boot menu entry drop-in files in a directory, sorts them by version, shows them in a menu, boots newest.

systemd-boot

UEFI Only

Implements Boot Loader Spec

`$BOOT/loader/entries/*.conf` (Type #1)

`$BOOT/EFI/Linux/*.efi` (Type #2)

Eligible for being signed by Shim (since the day before yesterday, Feb 2nd)

systemd-boot, Part 2

Automatic, no configuration

Also auto-discovers Windows/MacOS/EFI Shell/Firmware Setup

Many APIs towards userspace, mostly via EFI variables

Early boot Random Seed

Automatic Enrollment of Secure Boot keys

Automatic Loading of driver modules from drop-in dir

Automatic Boot Assessment/Boot counter support

bootctl

Primarily installer for systemd-boot

But also OS command line interface to talk to systemd-boot, to pick menu entries, list menu entries, update random seed, and more.

Automatically run on boot, to make sure copy of boot loader in ESP is always up to date.

systemd-stub

UEFI boot stub

systemd-stub + kernel + initrd + … = UKI (aka “Type #2 Boot Loader Spec Entry”)

UKI = Unified Kernel Image

PE Sections: .linux, .osrel, .cmdline, .initrd, .splash, .dtb, .uname, .sbat, .pcrsig, .pcrpkey

Optionally loads side-cars: *.cred, *.addon.efi, *.sysext.raw, *.confext.raw

TPM PCR Measurements

Kernel Command Line from SMBIOS Type 11

ukify

Script that glues together UKIs from systemd-stub, kernel, initrd, …

Predicts TPM PCR measurements when UKI is booted, adds this into the UKI

SecureBoot signs the result

systemd-measure

Precalculates PCR measurements of UKI

Used by ukify to do the hash predictions

kernel-install

Tool that installs kernels into the ESP

Idea: rpms/debs ship kernels in /usr/lib/, and they are copied/installed to ESP/$BOOT with kernel-install

Plugins for generating Type #1 and Type #2/UKI boot menu entries at RPM/DEB install time

Can also list available kernels

systemd-pcrlock

Very new addition to the toolset

Manages local PCR-based policies, covers local firmware, extension cards, configuration, … as well as boot loader, UKI, …

Highly extensible, creates dynamic access policy, can process UKIs, PEs, UEFI event log.

Closes gap of PCR protection that is not covered by integrity protection of resources supplied by OS vendor.

Summary

systemd-boot + systemd-stub + bootctl + ukify + systemd-measure + kernel-install + systemd-prlock

=

What is all this not

Not for legacy, non-UEFI systems

No boot scripts run by interpreter in boot loader

Not just yet another boot loader

Security, Signing, TPM is *not* an afterthought

Distribution Roadmap

Available in all relevant distributions

Increasing adoption, in particular systemd-stub, kernel-install, UKIs, ukify, …

In particular in the Confidential Computing world

Big distribution with default to systemd-boot soon? (OpenSUSE first)

The End