systemd & TPM in 2025

Lennart Poettering

FOSDEM 2025
Brussels, Belgium

30 min

Goals

- Catch up with other OSes
- Default to Measured Boot
- Disk Encryption locked to TPM2
- Service Credentials locked to TPM2
- Secure Parameterization of the Boot
- Confidential Computing
- Open up TPM2 usage for other purposes
- Good enough to be turned on by default on generic Linux

Components

systemd-cryptsetup, systemd-cryptenroll, systemd-pcrextend, systemd-pcrphase, systemd-pcrmachine, systemd-pcrfs, systemd-stub, systemd-measure, ukify, systemd-pcrlock, systemd-repart, systemd-creds & ImportCredentials=, systemd-sbsign, systemd-keyutil

Primary Security Model

- Focus on Measured Boot, not on Secure Boot
- More democratic and compatible with image-based systems, where minor code changes would otherwise always require fresh Secure Boot signing
- *(Security benefit of Secure Boot is limited, a very wide net, a very slow deny list for code at best)*
- TOFU model: lock down system on install, protect for all future boots
- Consider SecureBoot an add-on, but not the primary hook for security
- *(This is Lennarts take on things. Others, including my employer, of course have very different takes on this, and that's fine)*

Combined `systemd-pcrlock` + Signed PCR Policies

Finally: `systemd-pcrlock` policies can be combined with signed PCR policies

This means disk can be protected by local policies on equal footing with OS vendor policies

Tough nut to crack (i.e. TPMs don’t really allow combining `PolicyAuthorizeNV` + `PolicyAuthorize`). Simple solution: key sharding

tpm2.target

There’s now a clear synchronization point in place where TPMs have to have shown up at boot

Supports late probed kernel drivers (kmods…)

Supports TPMs that require userspace code (OPTEE supplicant…)

System Credentials now Available Unprivileged

With v257, systemd-creds can be used to encrypt/decrypt per-user credentials

With v258 (upcoming), `ImportCredentials=` in user services supports this too

Other Stuff

Multi-profile UKIs (see other talk)

`systemd-cryptenroll` can unlock and enroll with TPM2, in one (but use `systemd-pcrlock` instead)

`systemd-keyutil` now available to do certain HSM key operations, for use in environments where systemd-measure and `systemd-sbsign` are used later. (Can cache PINs)

Much better build-time tooling

Other Stuff #2

`systemd-stub` measures into CC pseudo-PCRs

`systemd-measure` works in “offline” mode + PKCS#11/HSM support

`systemd-sbsign` is now a thing

Varlink IPC API for measuring arbitrary stuff (writes CEL log)

`systemd-pcrlock` now supports policies on root fs

Other Stuff #3

`systemd-pcrlock` now supports policies for root fs, too

TPM 1.2 gone

`ConditionSecurity=measured-uki`

`systemd-cryptenroll` can do offline enrollment + explicit hash value enrollment

`systemd-tpm2-setup` runs at boot and initializes SRK explicitly

Soon

NVIndex range assigned to systemd/Linux

→ Measurement of sysext, context, portable services, …

The End