Contribution ID: **292** Type: **not specified**

TPM 2.0 Linux sysfs interface

Wednesday, September 11, 2019 6:05 PM (25 minutes)

At the time of writing this paper the Linux kernel supported TPM 1.2 functionalities in sysfs. To these functionalities we include:

$ls/sys/devices/pnp0/00:04/tpm/tpm0activecapsdeviceenabledpcrsppisubsystemtimeoutscanceldevdurationsownedpower$
ls /sys/devices/pnp0/00:04/tpm/tpm0/ppi
request response tcg_operations transition_action version vs_operations

We would expect the same or similar level of support for TPM 2.0. At least kernel should be able to request localities, change PCR banks, list PCRs, extend PCRs, clear TPM, take ownership. For now, the TPM2.0 is unusable in any way. Despite enabling all TPM options in the kernel configuration. There is a TPM 2.0 software stack, however, it has many dependencies and has to be compiled by anyone who would like to utilize TPM2.0 (packages in package managers was broken for certain distros at the time of writing the document).

Additionally, Linux has Integrity Measurement Architecture which utilizes TPM to attest the rootfs whether it has been maliciously modified. However, the only supported TPM is the one in version 1.2. Enabling it is as simple as adding a single kernel cmdline parameter: ima_tcb and defining a policy. However, it will only work with TPM 1.2 tools like tpm-tools, trousers.

I agree to abide by the anti-harassment policy

Yes

I confirm that I am already registered for LPC 2019

Primary authors: Mr PIOTR, Król (3mdeb Embedded Systems Consulting); Mr MICHAŁ, Żygowski (3mdeb Embedded Systems Consulting)

Presenters: Mr PIOTR, Król (3mdeb Embedded Systems Consulting); Mr MICHAŁ, Żygowski (3mdeb Embedded Systems Consulting)

Session Classification: System Boot and Security MC