Linux Plumbers Conference 2019

Contribution ID: **77**

Type: **not specified**

Enabling TPM based system security features

Tuesday 10 September 2019 15:00 (45 minutes)

Nowadays all consumer PC/laptop devices contain TPM2.0 security chip (due to Windows hardware requirements). Also servers and embedded devices increasingly carry these TPMs. It provides several security functions to the system and the user, such as smartcard-like secure keystore and key operations, secure secret storage, bruteforce-protected access control, etc.

These capabilities can be used in a multitude of scenarios and use cases, including disk encryption, device authentication, user authentication, network authentication, etc. of desktops/laptops, servers, IoTs, mobiles, etc.
Utilizing the TPM requires several layers of software; the driver (inside the kernel), tpm middleware (a TSS implementation), security middleware (e.g. pkcs11), applications (e.g. ssh).

This talk first gives an architectural overview of the hard-/software components involved in typical use cases. Then we will dive into a set of concrete use cases and on different ways in which they can be built up; these use cases will be related to device/user authentication around pkcs11 and openssl implementations.

The talk will end with a list of software and works in progress for introducing TPM functionality to core applications. Finally, a list of potential projects for extending the utilization of the TPM in core software is presented. This latter list shall then drive the discussion on which software is missing or which software has cotributors attending that would like to include such features or which software is currently missing on the list. The current lists of core software are available and updated at https://tpm2-software.github.io/software

Keywords: core libraries, device support, security, tpm, tss

I agree to abide by the anti-harassment policy

Yes

Primary author: Mr FUCHS, Andreas (Fraunhofer SIT)

Presenter: Mr FUCHS, Andreas (Fraunhofer SIT)

Session Classification: LPC Refereed Track