Inhaltsverzeichnis

Download und install 3
PreRequisites 3
herunterladen, konfigurieren und kompilieren 3

Trusted Platform Module

Der TPM Chip ist praktisch eine erweiterte SmartCard. Warum also nicht den TPM benutzen zum speichern der privaten Keys für z.B. SSH oder TLS Zertifikate oder für die HDD Verschlüsselung mit LUKS?

Andreas Fuchs erklärt das am 36c3 in einem halbstündigen Vortrag.

"Don't ask what you can do for TPMs, Ask what TPMs can do for you" Hacking (with) a TPM

TPM2 Software Community Homepage: tpm2-software.github.io

Download und install

PreRequisites

```
sudo apt -y install \
  autoconf-archive \
  libcmocka0 \
  libcmocka-dev \
  procps \
  iproute2 \
  build-essential \
  git \
  pkg-config \
  gcc \
  libtool \
  automake \
  libssl-dev \
  uthash-dev \
  autoconf \
  doxygen \
  libjson-c-dev \
  libini-config-dev \
  libcurl4-openssl-dev \
  libuuid-dev \
  libltdl-dev
```

Es kann sein, dass das Paket statt libuuid-dev uuid-dev heisst.

herunterladen, konfigurieren und kompilieren

```
sudo chmod go+rw /dev/tpmrm0
for i in tss tss-engine pkcs11 totp tools; do
git clone --depth=1 \
https://github.com/tpm2-software/tpm2-${i}.git \
```

```
&& pushd tpm2-${i} \
&& ./bootstrap \
&& ./configure --enable-plymouth --sysconfdir=/etc \
&& make -j$(nproc) \
&& sudo make -j install \
&& popd
done
tpm2_getcap properties-fixed
```