01.11.2025 07:46 Trusted Platform Module

Inhaltsverzeichnis

Download und install	
PreRequisites	3
herunterladen, konfigurieren und kompilieren	4

https://aha-it.ch/wiki/ Printed on 01.11.2025 07:46

01.11.2025 07:46 3/4 Trusted Platform Module

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

inst-prereq.sh

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

Es kann sein, dass das Paket bei euch auch uuid-dev statt libuuid-dev heisst. Ich habe es oben mal so angepasst. libqrencode wurde bei mir auch nicht gefunden, ich hab's durch quencode ersetzt.

Fehler habe ich bekommen, weil -enable-pymouth als Option nicht erkannt wurde. Und die ManPages

wurden nicht installiert, weil das Paket pandoc nicht installiert ist.¹⁾

Dann kommen Warnungen wegen OpenSSL 3.0 RAS_free, EC_KEY_free, ENGINE_by_id, ENGINE_init, ENGINE get name, ENGINE ctrl, EVP MD CTX md, ... is deprecated

herunterladen, konfigurieren und kompilieren

build.sh

```
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
```

Wenn alles geklappt hat, dann gibt der Befehl tpm2_getcap... die capabilities des TPM Chips aus. Ein einfacher Test ist z.B. der Zufallszahlengenerator, mit tpm2_getrand 4 werden 4 zufällige Bytes ausgegeben.

So, was können wir nun damit machen?

1)

ich hab's den PreRequisites bereits hinzugefügt

From:

https://aha-it.ch/wiki/ - AHa-IT

Permanent link:

https://aha-it.ch/wiki/lx/tpm?rev=1667938994

Last update: **08.11.2022 20:23**



https://aha-it.ch/wiki/ Printed on 01.11.2025 07:46