Haute école d'ingénierie et d'architecture Fribourg
Hochschule für Technik und Architektur Freiburg

TPM laboratory

Hes·so
Haute Ecole Spécialisée
de Suisse occidentale
Fachhochschule Westschweiz

Jean-roland.schuler@hefr.ch

Install software TPM swtpm

Install on your PC

```
git clone https://github.com/stefanberger/swtpm.git
cd swtpm
```

Install swtpm

```
see: https://github.com/stefanberger/swtpm/wiki
sudo dnf -y install libtasn1-devel expect socat python3-twisted fuse-devel glib2-devel
gnutls-devel gnutls-utils gnutls json-glib-devel

sudo dnf install libtpms-devel
sudo dnf install libseccomp-devel
./autogen.sh --with-openssl --prefix=/usr
make -j4
make -j4 check
sudo make install
export TPM2TOOLS_TCTI="swtpm:port=2321"
```

Start swtpm

```
swtpm socket --tpmstate dir=/home/schuler/work/tpm/swtpm2  --tpm2 --server type=tcp,port=2321 --ctrl
type=tcp,port=2322 --flags not-need-init,startup-clear
```

Install TPM2 tools

Install on your PC

```
sudo dnf install tpm2-tss
sudo dnf install tpm2-tools
```

Question 1, create-load-save primary keys

Create primary key in owner hierarchy, key parameter: rsa 2048 bits

Check the handles-transient, handles-persistent areas

Flush the handle-transient area

Save the primary key to the NV-Ram

Check the handles-transient, handles-persistent areas

Question 2, create-load-save child keys

Create child key in owner hierarchy, key parameter: rsa 2048 bits

Check the handles-transient, handles-persistent areas

Flush the handle-transient area

Save the child key to the NV-Ram

Check the handles-transient, handles-persistent areas

Question 3, decrypt on TPM

The file `encryptedtext` has been encrypted by the public key `rsa_key.pem`

Decrypt this file on the TPM

Question 4, PCR policy

U-boot has not yet integrated the TPM. The goal of this question is to simulate on your PC how u-boot can integrate the tpm in order to check the Linux kernel integrity.

1) With the tpm2 commands and graphics, simulate how u-boot shoud check the Linux kernel integrity with PCR registers and prcpolicy.

2) With the tpm2 commands and graphics, simulate how it is possible to install a new Linux kernel and update PCR registers and prcpolicy