Ochrona Centrów Danych
Raport 5

Wykorzystanie symulatorów TPM

Politechnika Wrocławska

Anna Płecha, 241446

Wrocław, 2021

Cel ćwiczenia

Celem przeprowadzonego ćwiczenia było zapoznanie się w praktyce z zainstalowanymi na poprzednich zajęciach symulatorami TPM. Należało przedstawić własne przykłady użycia podstawowych usług TPM. Na te potrzeby wybrano narzędzie tpm2-totp: Attest the trustworthiness of a device against a human using time-based one-time passwords.

Przebieg ćwiczenia

Rozpoczęto od pobrania głównego repozytorium oraz doinstalowania niezbędnych pakietów. Należało się upewnić, że symulator jest włączony i działający.

Rys 1. Odczyt rejestrów PCR działającego symulatora.

```
root@a860e66386de:/# git clone https://github.com/tpm2-software/tpm2-totp
Cloning into 'tpm2-totp'...
remote: Enumerating objects: 884, done.
remote: Counting objects: 100% (183/183), done.
remote: Compressing objects: 100% (102/102), done.
remote: Total 884 (delta 95), reused 108 (delta 66), pack-reused 701
Receiving objects: 100% (884/884), 245.69 KiB | 2.21 MiB/s, done.
Resolving deltas: 100% (519/519), done.
root@a860e66386de:/#
```

Rys 2. Pobranie repozytorium dla wybranego oprogramowania.

```
root@a860e66386de:/tpm2-totp# sudo apt -y install build-essential autoconf auto
conf-archive automake m4 libtool gcc pkg-config libqrencode-dev pandoc doxygen
liboath-dev iproute2 plymouth libplymouth-dev
bash: sudo: command not found
root@a860e66386de:/tpm2-totp# apt -y install build-essential autoconf autoconf-
archive automake m4 libtool gcc pkg-config libqrencode-dev pandoc doxygen liboa
th-dev iproute2 plymouth libplymouth-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
autoconf is already the newest version (2.69-11.1).
automake is already the newest version (1:1.16.1-4ubuntu6).
gcc is already the newest version (4:9.3.0-1ubuntu2).
iproute2 is already the newest version (5.5.0-1ubuntu1).
libtool is already the newest version (2.4.6-14).
m4 is already the newest version (1.4.18-4).
pkg-config is already the newest version (0.29.1-0ubuntu4).
autoconf-archive is already the newest version (20190106-2.1ubuntu1).
doxygen is already the newest version (1.8.17-0ubuntu2).
pandoc is already the newest version (2.5-3build2).
build-essential is already the newest version (12.8ubuntu1.1).
The following additional packages will be installed:
  dmsetup libargon2-1 libcryptsetup12 libdevmapper1.02.1 libdrm-common
  libdrm2 libip4tc2 libkmod2 liboath0 libplymouth5 libpng16-16 libqrencode4
  networkd-dispatcher plymouth-theme-ubuntu-text python3-dbus python3-gi
```

Rys 3. Doinstalowanie niezbędnych pakietów.

Następnie następuje pobranie repozytorium github z tpm2-tss oraz wykonanie komendy ./bootstrap oraz ./configure.

```
root@a860e66386de:/tpm2-totp# git clone --depth=1 http://www.github.com/tpm2-so
ftware/tpm2-tss
Cloning into 'tpm2-tss'...
warning: redirecting to https://github.com/tpm2-software/tpm2-tss.git/
remote: Enumerating objects: 831, done.
remote: Counting objects: 100% (831/831), done.
remote: Compressing objects: 100% (712/712), done.
remote: Total 831 (delta 413), reused 232 (delta 111), pack-reused 0
Receiving objects: 100% (831/831), 1.20 MiB | 6.72 MiB/s, done.
Resolving deltas: 100% (413/413), done.
root@a860e66386de:/tpm2-totp# cd tpm2-tss
```

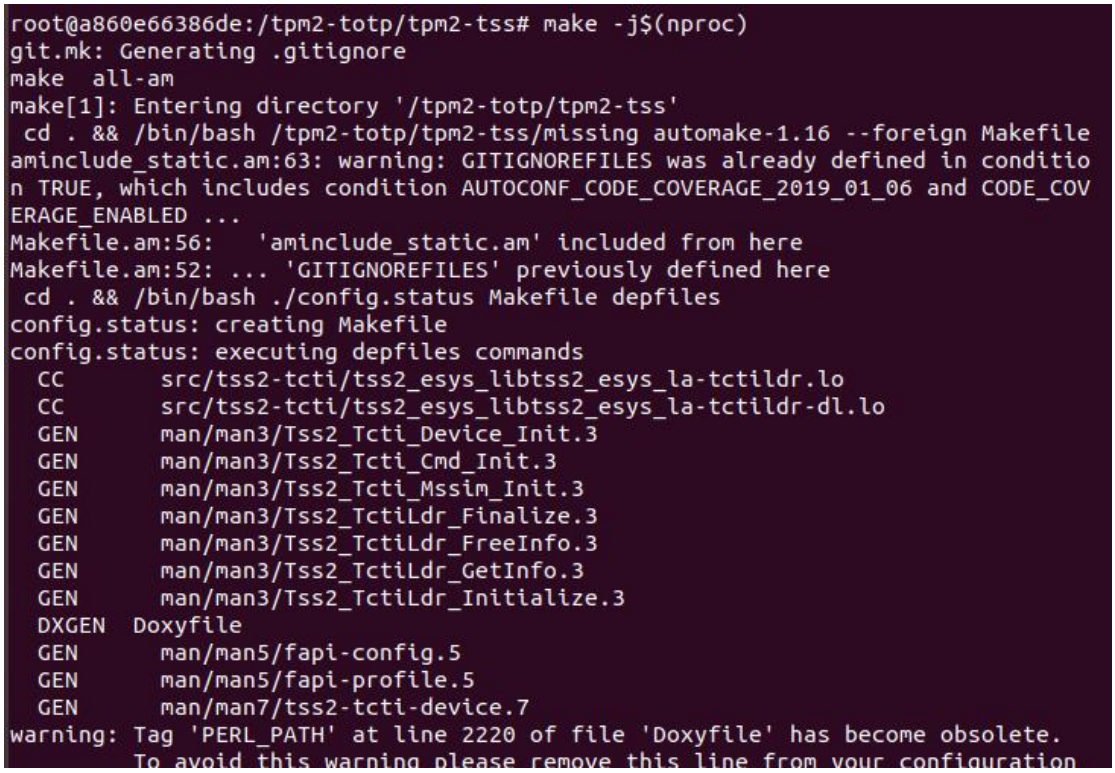
Rys 4. Pobranie repozytorium z tpm2-tss.

```
root@a860e66386de:/tpm2-totp/tpm2-tss# ./bootstrap
Generating file lists: src_vars.mk
aclocal: installing 'm4/ax_ac_append_to_file.m4' from '/usr/share/aclocal/ax_ac
_append_to_file.m4'
aclocal: installing 'm4/ax_ac_print_to_file.m4' from '/usr/share/aclocal/ax_ac_
print_to_file.m4'
aclocal: installing 'm4/ax_add_am_macro_static.m4' from '/usr/share/aclocal/ax_
add_am_macro_static.m4'
aclocal: installing 'm4/ax_add_fortify_source.m4' from '/usr/share/aclocal/ax_a
dd_fortify_source.m4'
aclocal: installing 'm4/ax_am_macros_static.m4' from '/usr/share/aclocal/ax_am_
macros_static.m4'
aclocal: installing 'm4/ax_check_compile_flag.m4' from '/usr/share/aclocal/ax_c
heck_compile_flag.m4'
aclocal: installing 'm4/ax_check_enable_debug.m4' from '/usr/share/aclocal/ax_c
heck_enable_debug.m4'
aclocal: installing 'm4/ax_check_gnu_make.m4' from '/usr/share/aclocal/ax_check
_gnu_make.m4'
aclocal: installing 'm4/ax_check_link_flag.m4' from '/usr/share/aclocal/ax_chec
k_link_flag.m4'
aclocal: installing 'm4/ax_code_coverage.m4' from '/usr/share/aclocal/ax_code_c
overage.m4'
aclocal: installing 'm4/ax_file_escapes.m4' from '/usr/share/aclocal/ax_file_es
capes.m4'
aclocal: installing 'm4/ax_is_release.m4' from '/usr/share/aclocal/ax_is_releas
e.m4'
aclocal: installing 'm4/ax_normalize_path.m4' from '/usr/share/aclocal/ax_norma
lize_path.m4'
aclocal: installing 'm4/ax_prog_doxygen.m4' from '/usr/share/aclocal/ax_prog_do
```

Rys 5. Wykonanie komendy ./bootstrap.

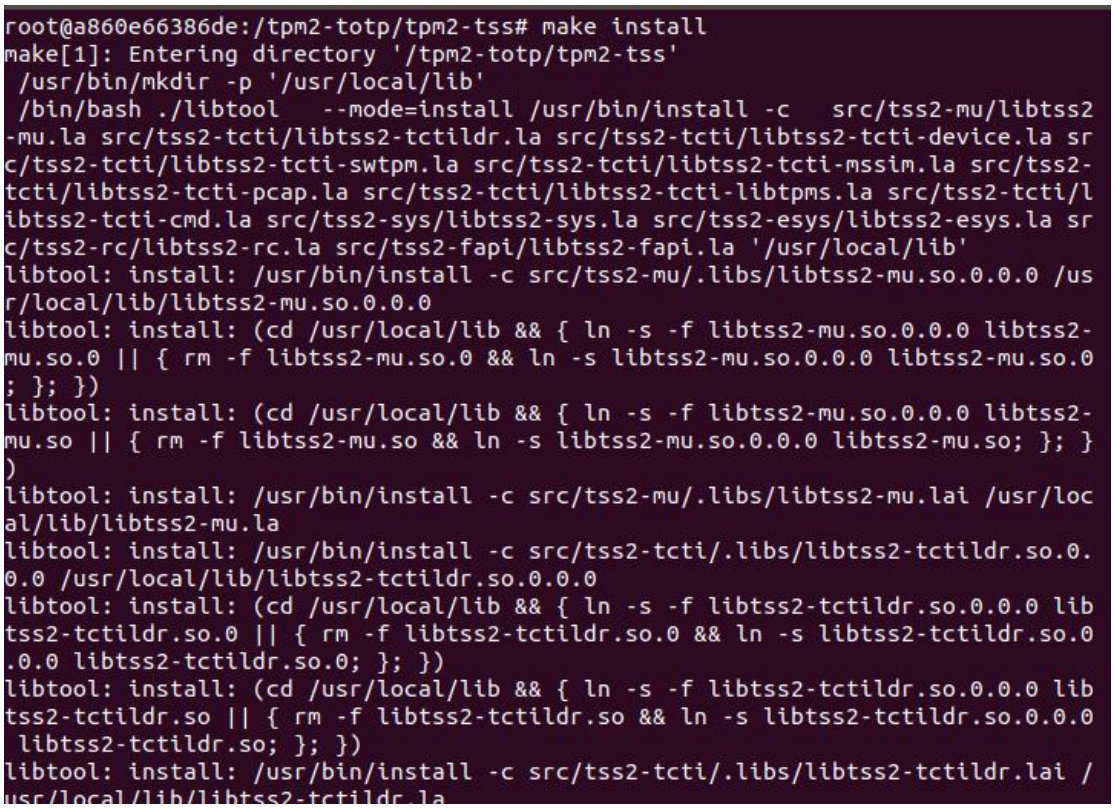
```
root@a860e66386de:/tpm2-totp/tpm2-tss# ./configure
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... gawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking whether make supports nested variables... (cached) yes
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
checking whether to enable debugging... no
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking whether make supports the include directive... yes (GNU style)
checking dependency style of gcc... gcc3
checking for g++... g++
checking whether we are using the GNU C++ compiler... yes
checking whether g++ accepts -g... yes
checking dependency style of g++... gcc3
checking whether ln -s works... yes
```

Rys 6. Wykonanie komendy ./configure.



Rys 7. Wykonanie komendy make -j$(nproc)

Następnie komendą make install zainstalowano wybrane oprogramowanie tpm2-totp.

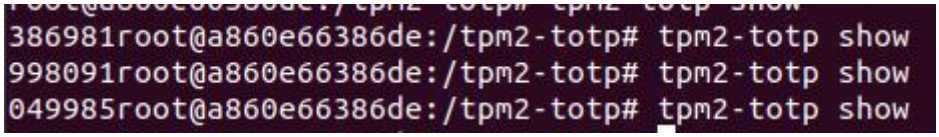


Rys 8. Wykonanie komendy make install - proces instalacji.

Do poprawnego działania aplikacji konieczna była komenda ldconfig. Następnie uruchomiono tpm2-totp.

Rys 9. Wykonanie komendy tpm2-totp init

Na telefonie instalujemy aplikację Last Pass Authenticator i po kodzie QR lub secret code dodajemy użytkownika. Następnie komendą tpm2-totp show wyświetlamy aktualny kod użytkownika w kontenerze i porównujemy z jednorazowym kodem w naszej aplikacji. Jeśli są takie same to znaczy, że wszystko działa poprawnie.



Rys 10. Widoczne przy użytkowniku aktualne jednorazowe kody.