Ochrona Centrów Danych

Raport 4

Politechnika Wrocławska

Anna Płecha, 241446

Wrocław, 2021

1. Cel ćwiczeń

Celem ćwiczenia było zainstalowanie dwóch programów symulujących TPM, jeden od IBM (SWTPM) oraz jeden od Microsoft (MSSIM) oraz uruchomienie ich celem potwierdzenia poprawności instalacji.

2. Przebieg ćwiczenia

Na maszynie wykorzystywanej do tej pory uprzednio zainstalowany był Docker. Dzięki temu możliwe było uruchomienie kontenera z obrazem Docker 20.0.4. Następnie na utworzonym kontenerze należało zainstalować wymagane narzędzia w kolejności oraz wersjii:

* libtpms v0.9.0
* swtpm v0.7.0
* mssim (master)
* tss 3.1.0
* tabrmd 2.4.0
* tools 5.2

Wszystkie narzędzia były instalowane według określonego schematu - na początku należało za pomocą git clone pobrać repozytorium, następnie doinstalować wymagane pakiety i/lub wykonać niezbędne komendy. Ponieważ każdy z procesów wyglądał bardzo podobnie i udokumentowanie tego wymagałoby dużej ilości screenów, przykładowe działanie ukazano na przykładzie poniżej (instalacja tpm2-tools):

Rys 1. Pobieranie repozytorium tpm2-tools.

```
root@a860e66386de:/tpm2-tools# git checkout 5.2
Note: switching to '5.2'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to false

HEAD is now at ebd59ef8 doc/CHANGELOG.md: updated to version 5.2
```

Rys 2. Wykonanie komendy dotyczącej wersji narzędzia.

```
root@a860e66386de:/tpm2-tools# ./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
```

Show Applications

Rys 3. Wykonanie komendy ./bootstrap.

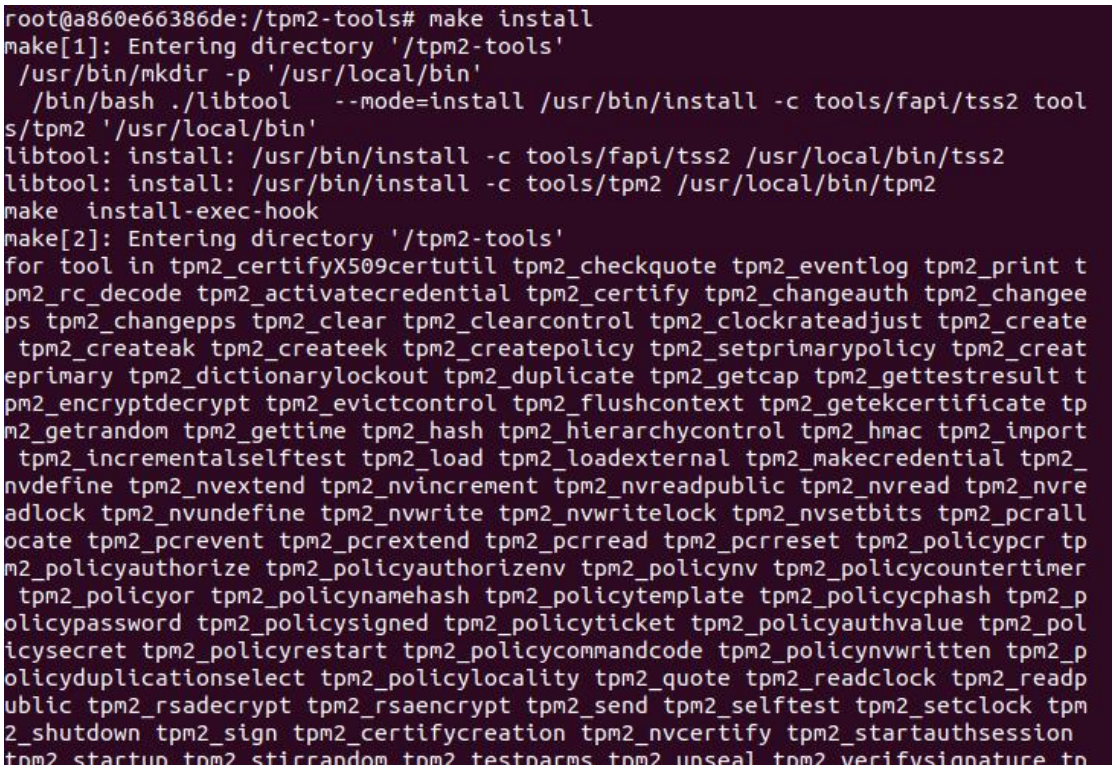
```
root@a860e66386de:/tpm2-tools# ./configure
checking whether to enable debugging... no
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
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 ln -s works... yes
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
checking how to print strings... printf
checking for a sed that does not truncate output... /usr/bin/sed
checking for grep that handles long lines and -e... /usr/bin/grep
checking for egrep... /usr/bin/grep -E
checking for fgrep... /usr/bin/grep -F
checking for ld used by gcc... /usr/bin/ld
checking if the linker (/usr/bin/ld) is GNU ld... yes
checking for BSD- or MS-compatible name lister (nm)... /usr/bin/nm -B
checking the name lister (/usr/bin/nm -B) interface... BSD nm
checking the maximum length of command line arguments... 1572864
```

Help

Rys 4. Wykonanie komendy ./configure.

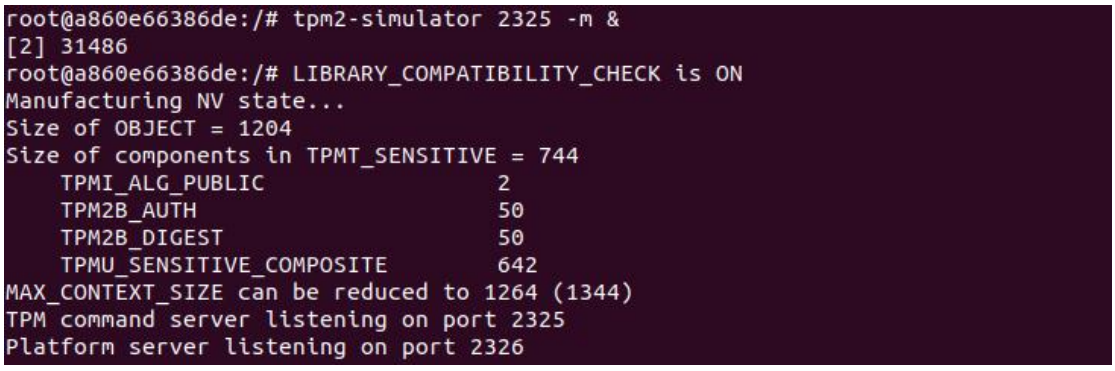
```
root@a860e66386de:/tpm2-tools# make
  CC       tools/fapi/tss2-tss2_template.o
  CC       tools/fapi/tss2-tss2_decrypt.o
  CC       tools/fapi/tss2-tss2_encrypt.o
  CC       tools/fapi/tss2-tss2_list.o
  CC       tools/fapi/tss2-tss2_changeauth.o
  CC       tools/fapi/tss2-tss2_delete.o
  CC       tools/fapi/tss2-tss2_import.o
  CC       tools/fapi/tss2-tss2_getinfo.o
  CC       tools/fapi/tss2-tss2_createkey.o
  CC       tools/fapi/tss2-tss2_createseal.o
  CC       tools/fapi/tss2-tss2_exportkey.o
  CC       tools/fapi/tss2-tss2_getcertificate.o
  CC       tools/fapi/tss2-tss2_getplatformcertificates.o
  CC       tools/fapi/tss2-tss2_gettpmblobs.o
  CC       tools/fapi/tss2-tss2_getappdata.o
  CC       tools/fapi/tss2-tss2_setappdata.o
  CC       tools/fapi/tss2-tss2_setcertificate.o
  CC       tools/fapi/tss2-tss2_sign.o
  CC       tools/fapi/tss2-tss2_verifysignature.o
  CC       tools/fapi/tss2-tss2_verifyquote.o
  CC       tools/fapi/tss2-tss2_createnv.o
  CC       tools/fapi/tss2-tss2_nvextend.o
  CC       tools/fapi/tss2-tss2_nvincrement.o
  CC       tools/fapi/tss2-tss2_nvread.o
  CC       tools/fapi/tss2-tss2_nvsetbits.o
  CC       tools/fapi/tss2-tss2_nvwrite.o
```

Rys 5. Wykonanie komendy make.

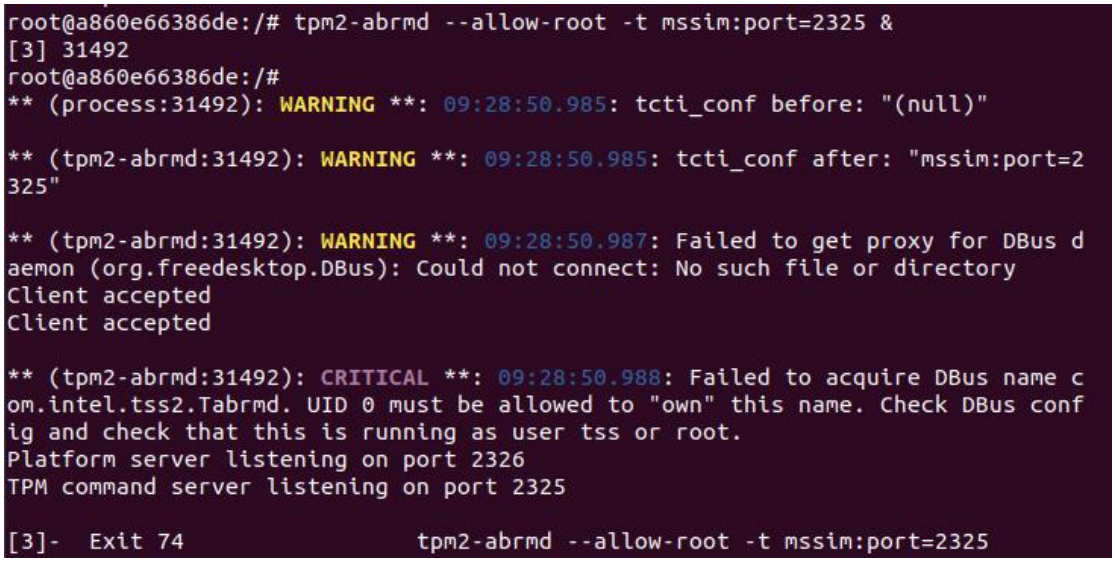


Rys 6. Wykonanie komendy make install - instalacja narzędzia.

Następnie uruchomiono oba symulatory, tym samym sprawdzając, czy proces instalacyjny przebiegł prawidłowo. Jako pierwszy uruchomiono MSSIM (Microsoft):



Rys 7. Uruchomienie symulatora MSSIM.



Rys 8. Inicjalizacja MSSIM TPM.

Rys 9. Odczyt rejestrów PCR - MSSIM.

Kolejnym krokiem było uruchomienie drugiego z zainstalowanych symulatorów, czyli SWTPM firmy IBM.

```
root@a860e66386de:/# rm -rf /tmp/mytpm && mkdir /tmp/mytpm && swtpm socket --tp
mstate dir=/tmp/mytpm --tpm2 --ctrl type=tcp,port=2324 --server type=tcp,port=2
323 --flags not-need-init &
[3] 31519
root@a860e66386de:/# ps aux | grep tpm
root      31483  0.0  0.0  24372  1448 pts/0    Tl   09:23   0:00 tpm2-simulator
 -m
root      31486  0.0  0.0  89908  1516 pts/0    Sl   09:27   0:00 tpm2-simulator
 2325 -m
root      31522  0.0  0.0   9028  5276 pts/0    S    09:36   0:00 swtpm socket -
-tpmstate dir=/tmp/mytpm --tpm2 --ctrl type=tcp,port=2324 --server type=tcp,por
t=2323 --flags not-need-init
root      31524  0.0  0.0   3304   728 pts/0    S+   09:36   0:00 grep --color=a
uto tpm
```

Rys 10. Uruchomienie SWTPM oraz potwierdzenie działania procesu.

```
root@a860e66386de:/# TPM2TOOLS_TCTI="swtpm:port=2323" tpm2_startup -c
```

Rys 11. Inicjalizacja SWTPM.

```
root@a860e66386de:/# TPM2TOOLS_TCTI="swtpm:port=2323" tpm2_pcrread
  sha1:
    0 : 0x0000000000000000000000000000000000000000
    1 : 0x0000000000000000000000000000000000000000
    2 : 0x0000000000000000000000000000000000000000
    3 : 0x0000000000000000000000000000000000000000
    4 : 0x0000000000000000000000000000000000000000
    5 : 0x0000000000000000000000000000000000000000
    6 : 0x0000000000000000000000000000000000000000
    7 : 0x0000000000000000000000000000000000000000
    8 : 0x0000000000000000000000000000000000000000
    9 : 0x0000000000000000000000000000000000000000
   10: 0x0000000000000000000000000000000000000000
   11: 0x0000000000000000000000000000000000000000
   12: 0x0000000000000000000000000000000000000000
   13: 0x0000000000000000000000000000000000000000
   14: 0x0000000000000000000000000000000000000000
   15: 0x0000000000000000000000000000000000000000
   16: 0x0000000000000000000000000000000000000000
   17: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
   18: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
   19: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
   20: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
   21: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
   22: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

Rys 12. Odczyt rejestrów PCR - SWTPM.