Anna Plust, 36148

Zaufana Infrastruktura Obliczeniowa

Laboratorium 1, Sprawozdanie

Podstawowe zasady posługiwania się modułem TPM

Testowanie zainstalowanych narzędzi.

```
┌──(root㉿kali)-[/]
└─# tpm2_selftest; echo $?
0

┌──(root㉿kali)-[/]
└─# tpm2_selftest --tcti=tabrmd; echo $?
0

┌──(root㉿kali)-[/]
└─# tpm2_selftest --tcti=device; echo $?
WARNING:tcti:src/tss2-tcti/tcti-device.c:439:Tss2_Tcti_Device_Init() Failed to open default TCTI device file /dev/t
pmrm0: No such file or directory
WARNING:tcti:src/tss2-tcti/tcti-device.c:439:Tss2_Tcti_Device_Init() Failed to open default TCTI device file /dev/t
pm0: No such file or directory
ERROR:tcti:src/tss2-tcti/tcti-device.c:444:Tss2_Tcti_Device_Init() Could not open any default TCTI device file
ERROR:tcti:src/tss2-tcti/tctildr-dl.c:169:tcti_from_file() Could not initialize TCTI file: device
ERROR:tcti:src/tss2-tcti/tctildr.c:430:Tss2_TctiLdr_Initialize_Ex() Failed to instantiate TCTI
ERROR: Could not load tcti, got: "device"
1

┌──(root㉿kali)-[/]
└─# tpm2_selftest --tcti=mssim
^C

┌──(root㉿kali)-[/]
└─#
```

```
┌──(root㉿kali)-[/]
└─# tpm2_testparms aes RSA ECC; echo $?
0
```

Odpytanie układu o udostępniane funkcje.

```
┌──(root㉿kali)-[/]
└─# tpm2_getcap -l
- algorithms
- commands
- pcrs
- properties-fixed
- properties-variable
- ecc-curves
- handles-transient
- handles-persistent
- handles-permanent
- handles-pcr
- handles-nv-index
- handles-loaded-session
- handles-saved-session
- vendor

┌──(root㉿kali)-[/]
└─# tpm2_readclock
time: 690796
clock_info:
  clock: 690796
  reset_count: 2
  restart_count: 0
  safe: yes
```

Generowanie losowych bajtów.

```
┌──(root㉿kali)-[/]
└─# tpm2_getrandom -o randomtpm.out 32
```

Wyświetlanie i ustawianie rejestrów PCR.
Wyświetlono dane dla następujących skrótów:

- sha1
- sha256
- sha384
- sha512

```
┌──(root㉿kali)-[/]
└─# 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
    23: 0x0000000000000000000000000000000000000000
  sha256:
    0 : 0x0000000000000000000000000000000000000000000000000000000000000000
    1 : 0x0000000000000000000000000000000000000000000000000000000000000000
    2 : 0x0000000000000000000000000000000000000000000000000000000000000000
    3 : 0x0000000000000000000000000000000000000000000000000000000000000000
    4 : 0x0000000000000000000000000000000000000000000000000000000000000000
    5 : 0x0000000000000000000000000000000000000000000000000000000000000000
    6 : 0x0000000000000000000000000000000000000000000000000000000000000000
    7 : 0x0000000000000000000000000000000000000000000000000000000000000000
    8 : 0x0000000000000000000000000000000000000000000000000000000000000000
    9 : 0x0000000000000000000000000000000000000000000000000000000000000000
    10: 0x0000000000000000000000000000000000000000000000000000000000000000
```