Anna Plust, 36148

Zaufana Infrastruktura Obliczeniowa

Laboratorium 3, Sprawozdanie

Testy platformyTPM2- Engine & OpenSSL

1. Kontynuacja poprzedniego laboratorium

```
┌──(root㉿kali)-[/lab2]
└─# ./provision.out
Context: 0×559fa6339190
... fapi provision

┌──(root㉿kali)-[/lab2]
└─# ./random.out
Context: 0×5627cd86a190
... fapi get random
0×5627cd90f9e0: 0×4b 0×d0 0×7e 0×64 0×cd 0×72 0×3f 0×48 0×a5 0×75 0×1d 0×20 0×3 0×6f 0×63 0×86 0×f1 0×1b 0×78 0×b0 0
xfd 0×82 0×49 0×4f 0×86 0×a0 0×14 0×48 0×23 0×8 0×a8 0×bf
```

2. TPM2-ENGINE

Opis narzędzia/modułu. Co można przy jego pomocy zrobić?

Implementuje silnik kryptograficzny dla OpenSSl dla TPM2.0 za pomocą stosu programowego tpm2-tss.
Do komunikacji w dół wykorzystuje interfejs Enhanced System API (ESAPI) TSS 2.0. Obsługuje deszyfrowanie i podpisy RSA oraz podpisy ECDSA.

Umożliwia aplikacjom korzystanie z usług kryptograficznych dostarczanych przez TPM, takich jak generowanie i podpisywanie certyfikatów cyfrowych, bez konieczności znajomości szczegółów dotyczących sprzętu TPM.

Działa poprzez dostarczenie wtyczki do OpenSSL. Kiedy aplikacja żąda wykonania operacji kryptograficznej, takiej jak podpisanie wiadomości, biblioteka OpenSSL przekazuje żądanie do TPM2-ENGINE. Silnik komunikuje się z urządzeniem TPM w celu wykonania żądanej operacji i zwraca wynik do aplikacji.

```
┌──(root㉿kali)-[/tpm2-tss-engine]
└─# openssl engine -t -c tpm2tss
(tpm2tss) TPM2-TSS engine for OpenSSL
 [RSA, RAND]
     [ available ]
```

3. Podpis RSA

```
┌──(root㉿kali)-[/lab2]
└─# echo "my data" > mydata.txt

┌──(root㉿kali)-[/lab2]
└─# tpm2tss-genkey -a rsa -s 2048 mykey.key

┌──(root㉿kali)-[/lab2]
└─# openssl rsa -engine tpm2tss -inform engine -in mykey.key -pubout -outform pem -out mykey.pub
Engine "tpm2tss" set.
writing RSA key

┌──(root㉿kali)-[/lab2]
└─# openssl pkeyutl -engine tpm2tss -keyform engine -inkey mykey.key -sign -in mydata.txt -out mysig
Engine "tpm2tss" set.

┌──(root㉿kali)-[/lab2]
└─# openssl pkeyutl -pubin -inkey mykey.pub -verify -in mydata.txt -sigfile mysig
Signature Verified Successfully
```

4. **Szyfrowanie i deszyfrowanie RSA**

```
┌──(root㉿kali)-[/lab2]
└─# echo "my data" > mydata.txt

┌──(root㉿kali)-[/lab2]
└─# tpm2tss-genkey -a rsa -s 2048 mykey.key

┌──(root㉿kali)-[/lab2]
└─# openssl rsa -engine tpm2tss -inform engine -in mykey.key -pubout -outform pem -out mykey.pub
Engine "tpm2tss" set.
writing RSA key

┌──(root㉿kali)-[/lab2]
└─# openssl pkeyutl -pubin -inkey mykey.pub -in mydata.txt -encrypt -out mycipher

┌──(root㉿kali)-[/lab2]
└─# openssl pkeyutl -engine tpm2tss -keyform engine -inkey mykey.key -decrypt -in mycipher -out out_mydata.txt
Engine "tpm2tss" set.

┌──(root㉿kali)-[/lab2]
└─# cat mydata.txt & cat out_mydata.txt
[1] 16535
my data
[1]  + done       cat mydata.txt
my data
```

5. **Podpis danych z wykorzystaniem klucza TPM2 / weryfikacja podpisu z OpenSSL**

```
┌──(root㉿kali)-[/lab2]
└─# openssl dgst -verify sub-pub.der -keyform der -sha1 -signature hash.plain msg.txt
Verified OK
```