

Filipe da Silva Sousa – RA: 163610

Verificando o TPM no Windows

Abre-se o Prompt de Comando como administrador, e executa-se o seguinte código:

```
CA: Administrador: Prompt de Comando
Microsoft Windows [versão 10.0.22621.1265]
(c) Microsoft Corporation. Todos os direitos reservados.

C:\Windows\System32>wmic /namespace:\\root\cimv2\Security\MicrosoftTpm path Win32_TPM get /value

IsActivated_InitialValue=TRUE
IsEnabled_InitialValue=TRUE
IsOwned_InitialValue=TRUE
ManufacturerId=1229870147
ManufacturerIdTxt=INTC
ManufacturerVersion=500.14.0.0
ManufacturerVersionFull120=500.14.0.0
ManufacturerVersionInfo=Intel
PhysicalPresenceVersionInfo=1.3
SpecVersion=2.0, 0, 1.38

C:\Windows\System32>echo filipe
filipe

C:\Windows\System32>
```

Demonstrando-se que o TPM utilizado é o 2.0

Verificando o TPM no Linux

Utilizou-se o seguinte comando no terminal do Linux:

```
facens@Teste:~$ journalctl -k --grep=tpmt
Mar 11 08:58:42 Teste kernel: ACPI: SSDT 0x000000007FFF0320 000124 (v01 VBOX VBOXTPMT 00000002 INTL 20100528)
facens@Teste:~$ echo Filipe
Filipe
facens@Teste:~$
```

A saída indica que foi detectada uma ACPI referente ao TPM, indicando que o SSDT começa no endereço 0x7FFF0320, possui 124 bytes, e possui assinatura VBOXTPMT.

O seguinte comando também pode ser utilizado para verificar a versão:

```
facens@Teste:~$ cat /sys/class/tpm/tpm0/tpm_version_major
2
facens@Teste:~$ echo filipe
filipe
facens@Teste:~$
```

Comprovando-se novamente a versão 2 do TPM

Criando uma chave AES através do TPMS

É possível através do TPM realizar a criação de uma chave criptográfica utilizada para cifrar e decifrar dados através de um algoritmo AES, um algoritmo de cifragem simétrica.

O seguinte comando demonstra a criação da chave primária:

```
root@Teste:/home/facens# echo Criando a chave Primária
Criando a chave Primária
root@Teste:/home/facens# tpm2_createprimary -C primary.ctx
name-alg:
  value: sha256
  raw: 0xb
attributes:
  value: fixedtpm|fixedparent|sensitivedataorigin|userwithauth|restricted|decrypt
  raw: 0x30072
type:
  value: rsa
  raw: 0x1
  exponent: 65537
  bits: 2048
  scheme:
    value: null
    raw: 0x10
  scheme-halg:
    value: [null]
    raw: 0x0
  sym-alg:
    value: aes
    raw: 0x6
  sym-mode:
    value: cfb
    raw: 0x43
  sym-keybits: 128
  raw: b227aa880f33574fc8770e1bada09e93ecc2585fcd962a09d2b099d7d7d3e31976d7d9ecf3b4340d2cccc7e0e583cee4433a3094511e1e4f8f04b06c1631f4d460fa161fb4dda7d971b6ee63d72c9e631a705f436f48eb5b9d949e44d8425c13ce46e66ac12fa5647481b94dc28ffc61d
  0b912b6d0eb53054000909185f0d74a1ff5ce1d59132921913109f3a6dcaec90e1e24fbc3ff742346288027d94f2194c4f18005830427781d37c74192306f4fa29ebc56373a0323c82c64833c7807f23990180c175a372ecc76d8191a409fca0ff720430727084a3c81c1e6a780b4963e063b
  6f6e43e5e5d43f423afcdc3089a79493739280b
```

Nessa chave primária estão contidas informações sobre a chave primária, incluindo seu identificador único e seus atributos.

Utiliza-se então a chave primária para criar uma nova chave no TPM, através do seguinte comando:

```
root@Teste:/home/facens# echo Criando a chave no dispositivo TPM usando a chave primária armazenada no primary.ctx
Criando a chave no dispositivo TPM usando a chave primária armazenada no primary.ctx
root@Teste:/home/facens# tpm2_create -C primary.ctx -Gaes128 -u key.pub -r key.priv
name-alg:
  value: sha256
  raw: 0xb
attributes:
  value: fixedtpm|fixedparent|sensitivedataorigin|userwithauth|decrypt|sign
  raw: 0x60072
type:
  value: symcipher
  raw: 0x25
sym-alg:
  value: aes
  raw: 0x6
sym-mode:
  value: null
  raw: 0x10
sym-keybits: 128
symcipher: 816415791f0d0c807758caf3d0f00ae3f7d5ce5cb4570e735c138f9d4492c983
root@Teste:/home/facens#
```

Nesse comando, têm-se:

- Especificação do arquivo que contém a chave primária, através do “-C primary.ctx”
- Especificação do algoritmo AES-128 para criptografar a nova chave
- Especificação do nomes dos arquivos contendo as chaves públicas e privadas

Para carregar a chave criptográfica gerada no TPM e armazená-la em um novo arquivo, utilizou-se o seguinte comando:

```
root@Teste:/home/facens# tpm2_load -C primary.ctx -u key.pub -r key.priv -c key_filipe.ctx
name: 000b64ca0d01c1ca47ac56a4976682d0dbf014a3f6b157ec2b5335f1f4c9bc20ec4
```

Encriptar e decryptar com TPM

Pode-se também utilizar o TPM para encriptar/decryptar mensagens, conforme demonstrado a seguir:

```
root@teste:/home/facens# echo "frase confidencial a ser encriptada" > virus.dat
root@teste:/home/facens# ls
Desktop  Documents  Downloads  key.ctx  key.filep.ctx  key.priv  key.pub  Music  Pictures  primary.ctx  Public  Templates  Videos  virus.dat  Warpinator
```

Criou-se um arquivo de dados denominado “virus.dat”, contendo a frase “frase confidencial a ser encriptada”. Utiliza-se então o tpm2_encryptdecrypt para criptografar este arquivo, e criar o arquivo “secret.dat”, conforme demonstrado a seguir:

```
root@Teste:/home/facens# rpm2crypto --decrypt -c key_filipe.ctx -o secret.enc virus.dat
WARN: Using a weak IV, try specifying an IV
root@Teste:/home/facens# ls
Desktop Documents Downloads  key.ctx  key_filipe.ctx  key.priv  key.pub  Music  Pictures  primary.ctx  Public  secret.enc  Templates  Videos  virus.dat  Warpinator
root@Teste:/home/facens# cat secret.enc
0S-0w[
0d?Y667ZB0v06S060root@Teste:/home/facens#
```

Utilizando-se da chave gerada anteriormente, criou-se um arquivo contendo uma mensagem criptografada, que não pode ser visualizada caso não se tenha a respectiva chave.

Para demonstrar o funcionamento da chave, utilizou-se novamente o `tpm2_encryptdecrypt` para, com a chave especificada, revelar o conteúdo da mensagem deste arquivo criptografado:

```
root@Teste:/home/facens# tpm2_encryptdecrypt -d -c key_filipe.ctx -o secret.dec secret.enc
WARN: Using a weak IV, try specifying an IV
root@Teste:/home/facens# ls
Desktop Documents Downloads key.ctx key_filipe.ctx key.priv key.pub Music Pictures primary.ctx Public secret.dec secret.enc Templates Videos virus.dat Warginator
root@Teste:/home/facens# cat secret.dec
frase confidencial a ser encriptada
root@Teste:/home/facens#
```