

Assignment 2 – Part B

TPM-Based Secure Key Storage Simulation

November 3, 2025

1 Testbed

Commands were executed on Ubuntu with `tpm2-tools` using the software TPM backend exposed at `swtpm:host=localhost,port=2321`. The TPM was reset before each major stage to avoid stale transient handles.

2 Measured Boot Baseline

PCR Snapshot

Listing 1: Baseline PCR measurement (sha256:0,7)

```
sha256:  
 0 : 0x00000000000000000000000000000000  
 7 : 0x3E4DA56D9A01D334C46C6B7CEC006B06B85DB4B52242F149C2BAE2C6E7B97D9B
```

```
yuvan-raj-krishna@yuvan-raj-krishna-System-Product-Name:~/Documents/college/sem7/TC_ATTEMPT3$ tpm2_pcrread sha256:0,7 -o partb/pcr.bin | tee partb/pcr_snapshot.txt  
sha256:  
 0 : 0x00000000000000000000000000000000  
 7 : 0x3E4DA56D9A01D334C46C6B7CEC006B06B85DB4B52242F149C2BAE2C6E7B97D9B
```

Figure 1: PCR read command and console output

3 Key Hierarchy and Policy Creation

Primary Key under Owner Hierarchy

Listing 2: Primary key creation output

```
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
rsa: 8
  efd1ae5476e57719a4898e358a6f62bfd670e3d474f3631c7832d36fadfd8a2d362d39c1dac6fa918a3a9464749673b8ef6

```

```

yuvan-raj-krishna@yuvan-raj-krishna-System-Product-Name:~/Documents/college/sem7/TC_ATTEMPT:$ tpm2_createprimary -C o -G rsa -c partb/primary.ctx | tee partb/cr
eateprimary.txt
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
rsa: 8efd1ae5476e57719a4898e358a6f62bfd670e3d474f3631c7832d36fadfd8a2d362d39c1dac6fa918a3a9464749673b8ef659f15cb23699cf954de9bacea930d61958e71e0aac26c178fb59fc
B683fa2eb6e4164b39be705f901584b385cb7d1314015c4b8de36556d5562b1925fdbf19ac42e4becf31de426771a33c1f6b1a134248ad116fb235c146293f1bfafabae4cc029c977bc55aa6ec13
0cdf7ae04b3f6eb7971ab930f3f5f8d8e77azf2fc36af12f68a8d479026d8a7fb8a032ae9777a78e9fc8f2352915a23e281f3ae22def1c421eca4c5245920022fd9c75fd738702c2f69cd3443013d
6cb30f3a693e557b9a7c1794f58c644c3c615

```

Figure 2: Primary key creation (`tpm2_createprimary`)

PCR-Bound Policy Digest

Listing 3: Policy digest derived from PCRs

```
8b827c5b78588fb531a201acaff625d802fd7ed0adb88c2de5d7692f1624152a
```

```

0c030f138053e5570987c1794158c044cc5c013
yuvan-raj-krishna@yuvan-raj-krishna-System-Product-Name:~/Documents/college/sem7/TC_ATTEMPT:$ tpm2_startauthsession --policy-session --session partb/policy.session
7 --pcr partb/pcr.bin | tee partb/policy.hex
8b827c5b78588fb531a201acaff625d802fd7ed0adb88c2de5d7692f1624152a
yuvan-raj-krishna@yuvan-raj-krishna-System-Product-Name:~/Documents/college/sem7/TC_ATTEMPT:$ xxd -r -p partb/policy.hex partb/policy.digest
yuvan-raj-krishna@yuvan-raj-krishna-System-Product-Name:~/Documents/college/sem7/TC_ATTEMPT:$ tpm2_flushcontext partb/policy.session
yuvan-raj-krishna@yuvan-raj-krishna-System-Product-Name:~/Documents/college/sem7/TC_ATTEMPT:$ xxd -r -p partb/policy.digest | tr -d '\n'; echo
9b97c5b78588fb531a201acaff625d802fd7ed0adb88c2de5d7692f1624152a

```

Figure 3: Policy session and `tpm2_policypcr` digest

4 Sealing Confidential Data

Listing 4: Sealed object generation

```
name-alg:  
  value: sha256  
  raw: 0xb  
attributes:  
  value: fixedtpm|fixedparent  
  raw: 0x12  
type:  
  value: keyedhash  
  raw: 0x8  
algorithm:  
  value: null  
  raw: 0x10  
keyedhash: 1f31f3a4e5bf59ed46fab9e1e5738ff4c13057a1d1dfc271fe940823983232e4  
authorization policy: 8b827c5b78588fb531a201acaff625d802fd7ed0adb88c2de5d7692f1624152a
```

```
yuvan-raj-krishna@yuvan-raj-krishna-System-Product-Name:~/Documents/college/sem7/TC_ATTEMPT3$ tpm2_create -C partb/primary.ctx -L partb/policy.digest -i partb/secret.txt \  
  -u partb/seal.pub -r partb/seal.priv | tee partb/create.txt  
name-alg:  
  value: sha256  
  raw: 0xb  
attributes:  
  value: fixedtpm|fixedparent  
  raw: 0x12  
type:  
  value: keyedhash  
  raw: 0x8  
algorithm:  
  value: null  
  raw: 0x10  
keyedhash: 1f31f3a4e5bf59ed46fab9e1e5738ff4c13057a1d1dfc271fe940823983232e4  
authorization policy: 8b827c5b78588fb531a201acaff625d802fd7ed0adb88c2de5d7692f1624152a
```

Figure 4: Sealed object creation tied to the PCR policy

Listing 5: Loaded sealed object handle

```
name: 000bcb9cfbb61b41710939b10e0ac2cd4bf4f450185b3c1c8744774443b868ae2ece
```

```
yuvan-raj-krishna@yuvan-raj-krishna-System-Product-Name:~/Documents/college/sem7/TC_ATTEMPT3$  
  tpm2_load -C partb/primary.ctx -u partb/seal.pub -r partb/seal.priv -c partb/seal.ctx |  
  tee partb/load.txt  
name: 000bcb9cfbb61b41710939b10e0ac2cd4bf4f450185b3c1c8744774443b868ae2ece  
yuvan-raj-krishna@yuvan-raj-krishna-System-Product-Name:~/Documents/college/sem7/TC_ATTEMPT3$
```

Figure 5: Loading the sealed object into the TPM

5 Policy-Protected Unseal

Listing 6: Successful policy check and unseal

```
Confidential lab secret for Assignment 2
```

```

tpm2_getcap handles-transient
yuvan-raj-krishna@yuvan-raj-krishna-System-Product-Name:~/Documents/college/sem7/TC_ATTEMPT3$ tpm2_load -C partb/primary.ctx -u partb/seal.pub -r partb/seal.priv -c partb/seal.ctx | tee partb/load.txt
name: 000bcb9cfbb61b41710939b10e0ac2cd4bf4f450185b3c1c8744774443b868ae2ece
yuvan-raj-krishna@yuvan-raj-krishna-System-Product-Name:~/Documents/college/sem7/TC_ATTEMPT3$ tpm2_getcap handles-transient
- 0x800000000
- 0x800000001

```

Figure 6: Policy session prior to unsealing

```

- 0x800000000
yuvan-raj-krishna@yuvan-raj-krishna-System-Product-Name:~/Documents/college/sem7/TC_ATTEMPT3$ tpm2_readpublic -c partb/seal.ctx
name: 000bcb9cfbb61b41710939b10e0ac2cd4bf4f450185b3c1c8744774443b868ae2ece
qualified name: 000b95dc396323b43c079980389ba114eefa340bcb22b0823604f383d81531fad91
name-alg:
  value: sha256
  raw: 0xb
attributes:
  value: fixedtpm|fixedparent
  raw: 0x12
type:
  value: keyedhash
  raw: 0x8
algorithm:
  value: null
  raw: 0x10
keyedhash: 1f31f3a4e5bf59ed46fab9e1e5738ff4c13057a1d1dfc271fe940823983232e4
authorization policy: 8b827c5b78588fb531a201acaff625d802fd7ed0adb88c2de5d7692f1624152a

```

Figure 7: Recovered plaintext confirms unseal success

6 Policy Enforcement Demonstration

Listing 7: PCR extend simulating tampering

```
bba8b145c48336ddf892d83c78a61da62f580707a287b0060efcc70f5310379e
```

```

yuvan-raj-krishna@yuvan-raj-krishna-System-Product-Name:~/Documents/college/sem7/TC_ATTEMPT3$ tpm2_startauthsession --policy-session --session partb/policy.session
yuvan-raj-krishna@yuvan-raj-krishna-System-Product-Name:~/Documents/college/sem7/TC_ATTEMPT3$ tpm2_policypcr --session partb/policy.session --pcr-list sha256:0,7 | tee partb/policypcr_unseal.txt
8b827c5b78588fb531a201acaff625d802fd7ed0adb88c2de5d7692f1624152a
yuvan-raj-krishna@yuvan-raj-krishna-System-Product-Name:~/Documents/college/sem7/TC_ATTEMPT3$ tpm2_unseal -c 0x80000001 -p session;partb/policy.session | tee partb/unsealed.txt
Confidential Lab secret for Assignment 2
yuvan-raj-krishna@yuvan-raj-krishna-System-Product-Name:~/Documents/college/sem7/TC_ATTEMPT3$ tpm2_flushcontext partb/policy.session
yuvan-raj-krishna@yuvan-raj-krishna-System-Product-Name:~/Documents/college/sem7/TC_ATTEMPT3$ cat partb/unsealed.txt
Confidential Lab secret for Assignment 2

```

Figure 8: Tampering the PCR state via `tpm2_pcrextend`

Listing 8: Policy failure preventing unseal

```

yuvan-raj:krishna@yuvan-raj:krishna$ System-Product-Name:/Documents/college/sem7/TC_ATTEMPT3$ tpm2_pcrextend 7:sha256=$(echo -n "tamper" | sha256sum | cut -d' ' -f1)
yuvan-raj:krishna@yuvan-raj:krishna$ System-Product-Name:/Documents/college/sem7/TC_ATTEMPT3$ tpm2_startauthsession -policy-session session partb/policy.session
yuvan-raj:krishna@yuvan-raj:krishna$ System-Product-Name:/Documents/college/sem7/TC_ATTEMPT3$ tpm2_poltypcr --session partb/policy.session --pcr-lst sha256:0,7 | tee partb/policypcr_unseal_fail.txt
xt
bb8b8145c48336ddfb92d83x78a61da6f5f80870a287b0b960efcc707f5210379e
yuvan-raj:krishna@yuvan-raj:krishna$ System-Product-Name:/Documents/college/sem7/TC_ATTEMPT3$ tpm2_unseal -c 0x80000001 -p session:partb/policy.session | tee partb/unseal_fail.txt
WARNING:esys:src/tss2-esys/api/Esys_Unseal.c:295:Esys_Unseal_Finish() Received TPM Error
ERROR:esys:src/tss2-esys/api/Esys_Unseal.c:98:Esys_Unseal() Esys_Finish ErrorCode (0x0000099d)
ERROR: Esys_Unseal(0x99D) - tpm:session(1):: policy check failed
ERROR: Unable to run tpm2_unseal

```

Figure 9: Unseal attempt denied with TPM_RC_POLICY_FAIL

7 Artifact Summary

File	Description
partb/pcr_snapshot.txt	Baseline PCR measurements
partb/createprimary.txt	Owner primary key metadata
partb/policy.digest	Policy digest bound to PCR0/7
partb/seal.pub, partb/seal.priv	Serialized sealed object blobs
partb/seal.ctx	Loaded sealed object context (transient)
partb/unsealed.txt	Plaintext recovered when PCRs match
partb/unseal.fail.txt	Failure log after PCR tampering

Table 1: Generated artifacts retained for evaluation

8 Cleanup

All transient handles and sessions were flushed after the demonstration to leave the TPM in a clean state.