X

(https://swayam.gov.in) (https://swayam.gov.in/nc_details/NPTEL)

harshith.savanur01@gmail.com

NPTEL (https://swayam.gov.in/explorer?ncCode=NPTEL) » Information Security - 5 - Secure Systems Engineering (course)

Click to register for Certification exam (https://examform.nptel.ac.in/2025_01/exam_form/dashboard)

If already registered, click to check your payment status

Course outline

About NPTEL ()

How does an NPTEL online course work? ()

Week 1 ()

Week 2 ()

Week 3 ()

Week 4 ()

Week 5 ()

Week 6 ()

● Trusted Execution Environments (unit?

Week 6 : Assignment 6

The due date for submitting this assignment has passed.

Due on 2025-03-05, 23:59 IST.

Assignment submitted on 2025-03-03, 22:32 IST

1) Which of the following is NOT a feature of a Trusted Execution Environment? ***1 point***

○ Isolated execution
○ Confidentiality of assets
○ Hardware-based memory encryption
● Direct access to external peripherals without restrictions

Yes, the answer is correct.
Score: 1

Accepted Answers:
Direct access to external peripherals without restrictions

2) What is the primary role of the Secure Monitor in ARM TrustZone? ***1 point***

○ Encrypting data stored in the secure world
● Managing transitions between secure and non-secure states
○ Performing cryptographic operations
○ Isolating memory regions between processes

Yes, the answer is correct.
Score: 1

Accepted Answers:
Managing transitions between secure and non-secure states

3) In Intel SGX, what is the purpose of "sealed storage"? ***1 point***

○ To encrypt enclave code for secure execution
● To store secret data securely outside the enclave
○ To enable remote attestation for enclave verification

○ To partition memory into secure and non-secure regions

Yes, the answer is correct.
Score: 1

Accepted Answers:
To store secret data securely outside the enclave

4) Physical Unclonable Functions PUFs rely on which of the following for their uniqueness? ***1 point***

○ Cryptographic algorithms
◉ Random physical microstructure introduced during manufacturing
○ Software-defined randomness
○ External hardware sensors

Yes, the answer is correct.
Score: 1

Accepted Answers:
Random physical microstructure introduced during manufacturing

5) Which of the following correctly describes how ARM TrustZone enforces memory isolation? ***1 point***

○ By using software-based encryption mechanisms
◉ Through a TrustZone Address Space Controller
○ By executing all processes in the secure world
○ Using external cryptographic devices for isolation

Yes, the answer is correct.
Score: 1

Accepted Answers:
Through a TrustZone Address Space Controller

6) What is the key difference between Intel SGX and ARM TrustZone? ***1 point***

◉ SGX isolates specific application code and data, while TrustZone creates two virtual processors for secure and normal worlds.
○ SGX relies on cryptographic keys, while TrustZone does not use encryption.
○ TrustZone supports remote attestation, whereas SGX does not.
○ SGX is designed for embedded systems, while TrustZone is not.

Yes, the answer is correct.
Score: 1

Accepted Answers:
SGX isolates specific application code and data, while TrustZone creates two virtual processors for secure and normal worlds.

7) In PUFs, what is the term used to describe the input-output pair that defines its behaviour? ***1 point***

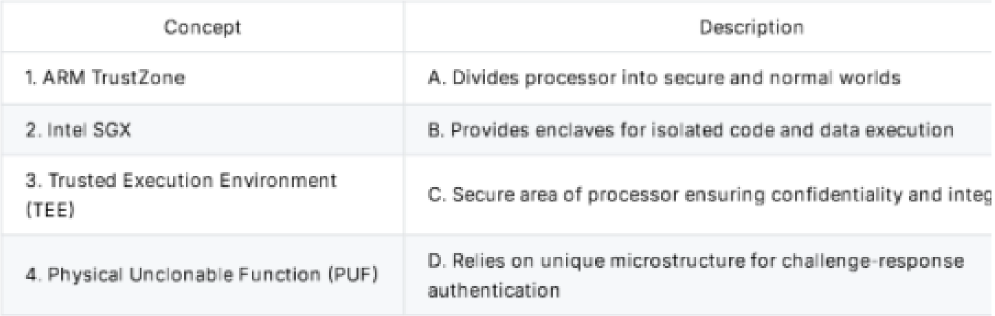
◉ Challenge-response pair
○ Encryption-decryption pair
○ Key-value pair
○ Stimulus-reaction pair

Yes, the answer is correct.
Score: 1

Accepted Answers:
Challenge-response pair

Lecture Material ()

8) Match the following with their descriptions: ***1 point***



Concept	Description
1. ARM TrustZone	A. Divides processor into secure and normal worlds
2. Intel SGX	B. Provides enclaves for isolated code and data execution
3. Trusted Execution Environment (TEE)	C. Secure area of processor ensuring confidentiality and integ
4. Physical Unclonable Function (PUF)	D. Relies on unique microstructure for challenge-response authentication

○ 1:A 2:D 3:C 4:B
○ 1:B 2:A 3:D 4:C
● 1:A 2:B 3:C 4:D
○ 1:B 2:C 3:D 4:A

Yes, the answer is correct.
Score: 1

Accepted Answers:
1:A 2:B 3:C 4:D

9) Assume an Intel SGX-enabled system has an enclave with a memory size limit of 128 MB due to Enclave Page Cache. If an application requires 256 MB of memory for its trusted operations, how much untrusted memory (in MB) will be required to store evicted EPC pages securely? (Assume 128 bytes of metadata for each page entry)

132

Yes, the answer is correct.
Score: 1

Accepted Answers:
(Type: Numeric) 132

1 point

10) State True or False: In ARM TrustZone, both secure and non-secure worlds share the same physical memory but use hardware-enforced isolation to prevent unauthorized access between them. ***1 point***

● True
○ False

Yes, the answer is correct.
Score: 1

Accepted Answers:
True