Unit 7 - Week 6

Assignment 6

The due date for submitting this assignment has passed.
As per our records you have not submitted this assignment.

Due on 2020-03-11, 23:59 IST.

1) We use Trusted Execution Environment for achieving security even when the operating system is compromised. *1 point*

- True
- False

No, the answer is incorrect.
Score: 0
Accepted Answers:
True

2) SGX Enclaves cannot protect from Invasive attacks. *1 point*

- True
- False

No, the answer is incorrect.
Score: 0
Accepted Answers:
False

3) There are separate page tables maintained for the normal world and the secure world for the ARM Trustzones. *1 point*

- True
- False

No, the answer is incorrect.
Score: 0
Accepted Answers:
True

4) Monitor mode is only responsible for saving the values of normal mode while switching between normal to secure world. Restoration of values is not done by the monitor. *1 point*

- True
- False

No, the answer is incorrect.
Score: 0
Accepted Answers:
False

5) A TLB in a ARM trust-zone has the following fields *1 point*

- NSTID bit , NS bit
- NSTID bit, Virtual Address
- NS bit and the virtual address.
- Virtual Address, Physical Address and the NS bit
- NSTID bit + Virtual Address, NS bit + Physical Address

No, the answer is incorrect.
Score: 0
Accepted Answers:
NSTID bit + Virtual Address, NS bit + Physical Address

6) What is the correct security checking order for implementing the chain of trust *1 point*

- Root of trust -> Boot Loader -> Secure OS -> Rich OS
- Root of trust -> Boot Loader -> Secure OS
- Root of trust -> Secure OS -> Boot Loader
- Root of trust -> Secure OS -> Boot Loader -> Rich OS

No, the answer is incorrect.
Score: 0
Accepted Answers:
Root of trust -> Boot Loader -> Secure OS -> Rich OS

7) SGX can be effective even when OS, BIOS and VMM of a system has been compromised. *1 point*

- True
- False

No, the answer is incorrect.
Score: 0
Accepted Answers:
True

8) Match the following in connection to SGX *1 point*

I. PRM	a. encryption
II. EPCM	b. Restores all the registers after an interrupt
III. Secure output from processor	c. not accessible memory for non-trusted devices
IV. SECS	d. Contains global metadata of enclave
V. EERESUME instruction	e. Management related aspects for EPC

- I-a, II - b, III-d , IV - e, V - c
- I - c, II- a , II- e, IV - d, V - b
- I - e, II - a III - b, IV -c, V - d
- I - c , II - e, III - a , IV - d, V-b

No, the answer is incorrect.
Score: 0
Accepted Answers:
I - c , II - e, III - a , IV - d, V-b

9) If an interrupt occurs while performing some operations in the enclave then that interrupt can't be handled by AEX *1 point*

- Ture
- False

No, the answer is incorrect.
Score: 0
Accepted Answers:
False

10) Comment about the validity of the following statements in connection to PUFs *1 point*

I. Exposing a PUF device to extreme temperature should impact its behaviour making it more secure
II. Capacitance of CMOS transistors determines the delay of transistors, this property can be used to design PUFS because a pair of N number of inverters might not have same delay

- I - True II- True
- I - False II - False
- I- False II- True
- I - True II - False

No, the answer is incorrect.
Score: 0
Accepted Answers:
I- False II- True