Unit 7 - Week 6

Course outline	Assignment 6
How does an NPTEL online	The due date for submitting this assignment has passed.
course work?	As per our records you have not submitted this assignment.
Week 1	We use Trusted Execution Environment for achieving security even when the operating system is compromise
Week 2	○ True
Week 3	○ False
Waste 4	No, the answer is incorrect. Score: 0
Week 4	Accepted Answers:
Week 5	True
Veek 6	SGX Enclaves cannot protect from Invasive attacks.
Trusted Execution	○ True
Environments	False
ARM Trustzone	No, the answer is incorrect. Score: 0
SGX (part 1)	Accepted Answers: False
SGX (part 2)	
PUF (part 1)	<ol> <li>There are separate page tables maintained for the normal world and the secure world for the ARM Trustzones</li> </ol>
PUF (part 2)	○ True
PUF (part 3)	O False
Quiz : Practice Assignment 6	No, the answer is incorrect. Score: 0
Quiz : Assignment 6	Accepted Answers: True
Week 6 Feedback	4) Manitar made is only responsible for equing the values of narmal made while quitables between narmal to see
eek 7	<ol> <li>Monitor mode is only responsible for saving the values of normal mode while switching between normal to se values is not done by the monitor.</li> </ol>
eek 8	○ True
ownload Vidaca	○ False
ownload Videos	No, the answer is incorrect. Score: 0
ext Transcripts	Accepted Answers: False
	raise
	5) A TLB in a ARM trust-zone has the following fields
	O NSTID bit , NS bit
	NSTID bit, Virtual Address
	NS bit and the virtual address.  Virtual Address. Physical Address and the NS bit.
	Virtual Address, Physical Address and the NS bit     NSTID bit + Virtual Address, NS bit + Physical Address
	No, the answer is incorrect.
	Score: 0

Assignment 6		
The due date for submitting this assignment As per our records you have not submitted		1, 23:59 IST.
We use Trusted Execution Environment for	achieving security even when the operating system is compromised.	1 point
○ True		
O False		
No, the answer is incorrect. Score: 0 Accepted Answers: True		
2) SGX Enclaves cannot protect from Invasi	ve attacks.	1 point
○ True		
No, the answer is incorrect.		
Score: 0 Accepted Answers:		
False		
<ol> <li>There are separate page tables maintained</li> </ol>	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		
	g the values of normal mode while switching between normal to secure world. Restoration of	1 point
○ True		
False		
No, the answer is incorrect. Score: 0 Accepted Answers:		
Accepted Answers: False		
5) A TLB in a ARM trust-zone has the followi	ng fields	1 point
NSTID bit , NS bit		
NSTID bit, Virtual Address  NS bit and the virtual address.		
Virtual Address, Physical Address and the		
NSTID bit + Virtual Address, NS bit + Phy No, the answer is incorrect.	sical Address	
Score: 0 Accepted Answers:		
NSTID bit + Virtual Address, NS bit + Physical	Address	
<ol><li>What is the correct security checking order</li></ol>	r for implementing the chain of trust	1 point
Root of trust -> Boot Loader -> Secure O     Root of trust -> Boot Loader -> Secure O		
Root of trust -> Secure OS -> Boot Load		
Root of trust -> Secure OS -> Boot Load	ler -> 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		
No, the answer is incorrect.		
Score: 0 Accepted Answers:		
True		
Match the following in connection to SGX		1 point
I. PRM II. EPCM	a. encryption     b. Restores all the registers after an interrupt	
III. Secure output from processor IV. SECS	c. not accessible memory for non-trusted devices 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 sor  Ture	ne operations in the enclave then that interrupt can't be handled by AEX	1 point
False		
No, the answer is incorrect. Score: 0 Accepted Answers: False		
10) Comment about the validity of the following	g statements in connection to PUFs	1 point
	e temperature should impact its behaviour making it more secure	, pont
	determines the delay of transistors, this property can be used to design PUFS because a pair of	N
I - True II- True		
I- False II- True		
I - True II - False		
No, the answer is incorrect. Score: 0 Accepted Answers:		
I- False II- True		