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.
   (a) True
   (b) False
   Score: 1 point
   Accepted Answers: True

2) SDL Excludes cannot protect from invasive attacks.
   (a) True
   (b) False
   Score: 1 point
   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 TrustZone.
   (a) True
   (b) False
   Score: 1 point
   No, the answer is incorrect. Score: 0
   Accepted Answers: False

4) Monitor mode is only responsible for isolating the values of normal mode while switching between normal to secure world. Restoration of values is not done by the monitor.
   (a) True
   (b) False
   Score: 1 point
   No, the answer is incorrect. Score: 0
   Accepted Answers: False

5) A TEE in an ARM TrustZone has the following fields.
   (a) NSIO bit, NS bit
   (b) NTIO bit, Virtual Address
   (c) NS bit and the virtual address
   (d) Virtual Address, Physical Address and the NS bit
   (e) NTIO bit = Virtual Address, NS bit = Physical Address
   Score: 1 point
   No, the answer is incorrect. Score: 0
   Accepted Answers: False

6) What is the correct security checking order for implementing the chain of trust?
   (a) Root of trust → Root Loader → Base OS → Root OS
   (b) Root of trust → Boot Loader → Secure OS
   (c) Root of trust → Secure OS → Root Loader
   (d) Root of trust → Secure OS → Root Loader → Root OS
   Score: 1 point
   No, the answer is incorrect. Score: 0
   Accepted Answers: False

7) SGD can be effective even when OS, BIOS and ARM of a system has been compromised.
   (a) True
   (b) False
   Score: 1 point
   No, the answer is incorrect. Score: 0
   Accepted Answers: False

8) Match the following in connection to SBox:

<table>
<thead>
<tr>
<th>a. Encrypt</th>
<th>b. Decipher</th>
<th>c. Execute</th>
<th>d. Receive</th>
<th>e. Decrypt</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. AES-128</td>
<td>2. AES-256</td>
<td>3. RSA-512</td>
<td>4. MD5</td>
<td>5. SHA-256</td>
</tr>
</tbody>
</table>

   Score: 1 point
   No, the answer is incorrect. Score: 0
   Accepted Answers: False

9) If an interrupt occurs while performing some operations in the kernel then that interrupt can’t be handled by AZX.
   (a) True
   (b) False
   Score: 1 point
   No, the answer is incorrect. Score: 0
   Accepted Answers: False

10) Comment about the validity of the following statements in connection to PUs:

    (a) Exploiting a PU's design to implement a secure feature should mean the feature being made more secure
    (b) Capability of CMSO2 Transistors determines the delay of transistors, this property can be used to design PUs because delay is less

    Score: 1 point
    No, the answer is incorrect. Score: 0
    Accepted Answers: False