Number: Name:

Segurança Informática em Redes e Sistemas / Network and Computer Security

MEIC, MEIC

1st Test, November 24th, 2017

- The duration of the test is of 1:00 hour.
- **Identify all sheets.**
- Read all paragraphs of each question before you answer the first one.
- Be objective and concise in your answers. Use only the space given for each question.
- The exam can be answered in Portuguese or in English.
- **Justify all answers.**

1. What is the difference between a *threat* and a *vulnerability*?
   Give an example of each one in regard to an application running in your smartphone.

2. Consider the following recommendations from the IEEE Center for Secure Design.
   a. *"Strictly separate Data and Control instructions"*
      Give a specific example of how you would apply this recommendation in the design of a recent software project that you did (can be the SIRS project or another project).

Project topic:

Example:

   b. *"All data must be explicitly validated"*.
      Give a specific example of how this recommendation can be applied in web applications to prevent injection attacks.

3. Which two (and only two) of the following sentences are true, regarding certification
   (a wrong answer will count with -50% of the question value):

□ - In Common Criteria (CC) the EAL depends either on the Protection Profile (PP) or on the Security Target (ST), both cannot be simultaneously used.
□ - If two products have the same EAL value they must have the same functionalities.
□ - TCSEC evaluates functionality not assurance.
□ - ITSEC evaluates both functionality and assurance.
□ - CC can be used to evaluate Operating Systems (OS).
□ - CC can evaluate all systems except OS. For OS evaluation TCSEC must be used.

4. In regards to Network Security
   a. Comment the following sentence with true of false and explain why:
   "Since Switches only send data to the port where the respective MAC address of the destination machine is registered, sniffing attacks are not possible when using Switches."

   b. At which OSI layer do Switches operate? Justify.

   c. The DNS vulnerability know as Kaminski vulnerability, is similar to the vulnerability in TCP/IP that can be explored to hijack a TCP session. Describe briefly what makes both vulnerabilities similar.

   d. Describe a possible solution (can be the one discussed in the lectures) that mitigates the above vulnerability and why it works?

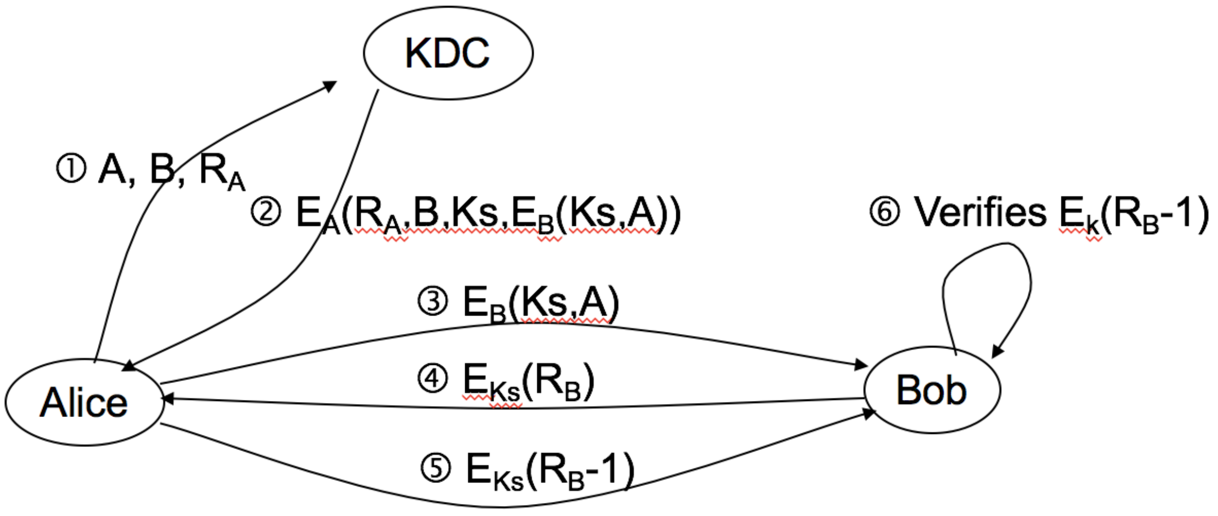
5. Consider the cryptographic service of Authentication.
   a. Is it possible to provide authentication using Cyclic Redundancy Codes? Justify.

   b. "MACs provide Authentication and Non-Repudiation." Do you agree with the previous sentence? Justify.

6. Consider the “Surreptitious Forwarding” and “Message Stealing” problems.
   a. Provide an example of each problem with users Alice, Bob and Mallory.

   b. Present a solution to the two problems above. Use the notation $\{M\}_{Ku\_A}$ and $\{M\}_{Kv\_A}$ to represent the encryption of message M with A’s public and private key, respectively.

7. Below is a diagram for the Needham-Schroeder protocol.



   a. What is the role of the KDC? Does Bob need to trust it?

b. Why are steps 4 and 5 needed?

c. Identify the main vulnerability in the protocol. How could an attacker exploit it? Justify.

8. Alice wants to send a message M1 to Bob and receive a confirmation message M2.
over an unsecure public channel. Assume that Alice and Bob share a 128 bit key. Design a diagram of the messages exchanged such that the following properties are ensured: confidentiality, freshness, message authentication. Use the following nomenclature: $[M\}_{K}$ to represent the cipher of message M with key K, and || to represent concatenation.

a. Is perfect forward secrecy assured in the above protocol?

Grading:

1:	1	T= 1
2:	a) 1 b) 1	T= 2
3:	a) 1	T= 1
4:	a) 1 b) 1 c) 1.5 d) 1.5	T= 5
5:	a) 1 b) 1	T= 2
6:	a) 1 b) 1	T= 2
7:	a) 1 b) 1 c) 1	T= 3
8:	a) 3 b) 1	T= 4