Number: ______ Name: ______

Segurança Informática em Redes e Sistemas / Network and Computer Security

MEIC-A, MEIC-T, MSIDC

2nd Test, January 7th, 2019

- The duration of the test is of 1:00 hour.
- The exam can be answered in Portuguese or in English.
- **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.
- Wrong answers in multiple choice questions with N options, subtract 1/N of the value
- **Justify all answers.**

1. Consider a cloud-based document access system with *thousands* of users and *millions* of documents. The documents must be protected from unauthorized access attempts.

   a. Propose an authorization mechanism based on an ACL.
   Describe the data layout in the user device and in the server so that, for example, the user "Alice" can be checked to access the document "https://cloud.com/org/poems.doc".

   Authorization data on client:

   Authorization data on server:

   b. Could the use of RBAC be advantageous to this kind of system given its size?
   Explain what RBAC is and justify your answer.

   c. Propose an alternative authorization mechanism based on *capabilities*.
   Describe the data layout in the user device and in the server so that, for example, the user "Bob" can be checked to access the document "https://cloud.com/org/sales.xls".

   Authorization data on client:

   Authorization data on server:

2. Compare *password*-based authentication with *biometric* authentication using fingerprints. State one advantage of each one when compared to the other.

Password-based:

Fingerprints:

3. What is a password *salt*? How can it make password-based authentication more secure?

4. Match the following protocols/secure channel solutions with the security approach considered: (Each wrong answer will count with -1/8 of the question value)

___ - HTTPS
___ - WPA
___ - Bluetooth
___ - SSH

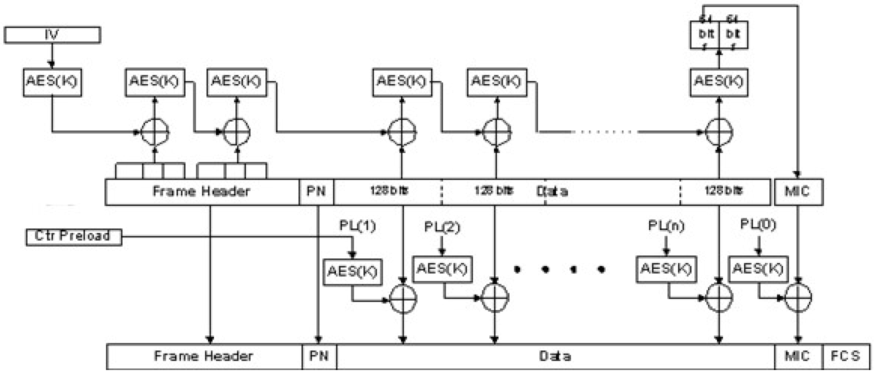
1) Link security
2) End-to-end security

5. State two vulnerabilities in GSM that have been corrected/mitigated in UMTS.

6. In Regard to the IEEE 802.11 protocol.
   a. In what way is the vulnerability of the WEP authentication approach similar to that of the original MSChap protocol?

   b. In what way does the 802.1X (EAP) protocol, in particular the EAPOL, improve on the above vulnerability?

7. Considering WPA2 protocol and the AES-CCMP protocol depicted in the figure below.



a. Does the AES-CCMP protocol allow for random access to the encrypted data?

b. Is the Frame Header of each packet ciphered? Justify why it is ciphered or not ciphered, depending on your answer.

c. Choose the best answer regarding what is provided by AES-CCMP:

□ confidentiality + non-repudiation
□ confidentiality + authenticity + non-repudiation
□ confidentiality without authenticity nor non-repudiation
□ none of the above are correct

8. A company has two offices, one in Lisbon and the other in Porto. For security reasons, all the communication between the two offices is protected using IPsec.

   a. Mark with an X all the security properties that can be guaranteed by IPsec:
   (no subtraction for wrong or incomplete answer in this question)
   □ - Confidentiality of the data exchanged over the IP protocol.
   □ - Integrity of the data exchanged over the IP protocol.
   □ - Authenticity of the packet sender.
   □ - Availability of the communication.

   b. In the two offices situation described, does it make sense to use IPsec in Transport mode or Tunnel mode?
   □ - Transport mode.
   □ - Tunnel mode.
   Justify you answer:

   c. What is the minimum number of Security Associations (SAs) that are needed in that situation?
   Answer: ____________ SAs
   Justify you answer:

   d. What is the parameter carried by an IPsec packet that allows deciding what SA shall be used to process that packet?
   □ - None, the recipient has that information before the packet is received.
   □ - The parameter is the Security Parameter Index.
   □ - The parameter is the Encapsulating Security Payload.
   □ - The parameter is the Sequence Number.

e. Consider a packet protected with the Authentication Header (AH) in Transport mode. The packet is represented below as a sequence of blocks of data (each block has a few bytes).

IP header	*AH header*	*TCP header*	*HTTP header*	*HTTP body*

AH protects the integrity of which of those blocks?
□ - None, because AH does not protect integrity.
□ - Only of the IP header.
□ - All the blocks.
□ - All the blocks except the IP header.

9. Consider the Transport Layer Security (TLS) protocol.

a. Which of the following phrases is the only one that is <u>true</u>?
□ - The TLS specification defines both a protocol and an API.
□ - In TLS it is possible to authenticate the client without authenticating the server.
□ - TLS uses a single session key to protect the communication.
□ - None of the above is true.

b. In relation to the choice of cryptographic algorithms used to protect the communication, mark with an X the only phrase that is <u>true</u>:
□ - The application defines one cryptographic algorithm for each purpose (for example, for encryption).
□ - First the client sends to the server the cryptographic algorithms that it supports, then the server selects one it supports and sends its decision to the client.
□ - First the server sends to the client the cryptographic algorithms that it supports, then the client selects the strongest it supports and sends its decision to the server.
□ - TLS only allows one set of cryptographic algorithms, e.g., AES for encryption.

Grading:

1:	a) 1,0 b) 1,0 c) 1,0	T= 3,0
2:	1,5	T= 1,5
3:	1,0	T= 1,0
4:	1,0	T= 1,0
5:	1,0	T= 1,0
6:	a) 1,0 b) 1,0	T= 2,0
7:	a) 1,0 b) 1,0 c) 1,0	T= 3,0
8:	a) 1,0 b) 1,5 c) 1,0 d) 1,0 e) 1,0	T= 5,5
9:	a) 1,0 b) 1,0	T= 2,0
	Total	= 20,0