Number: Name:

Segurança Informática em Redes e Sistemas / Network and Computer Security

MEIC, MEIC

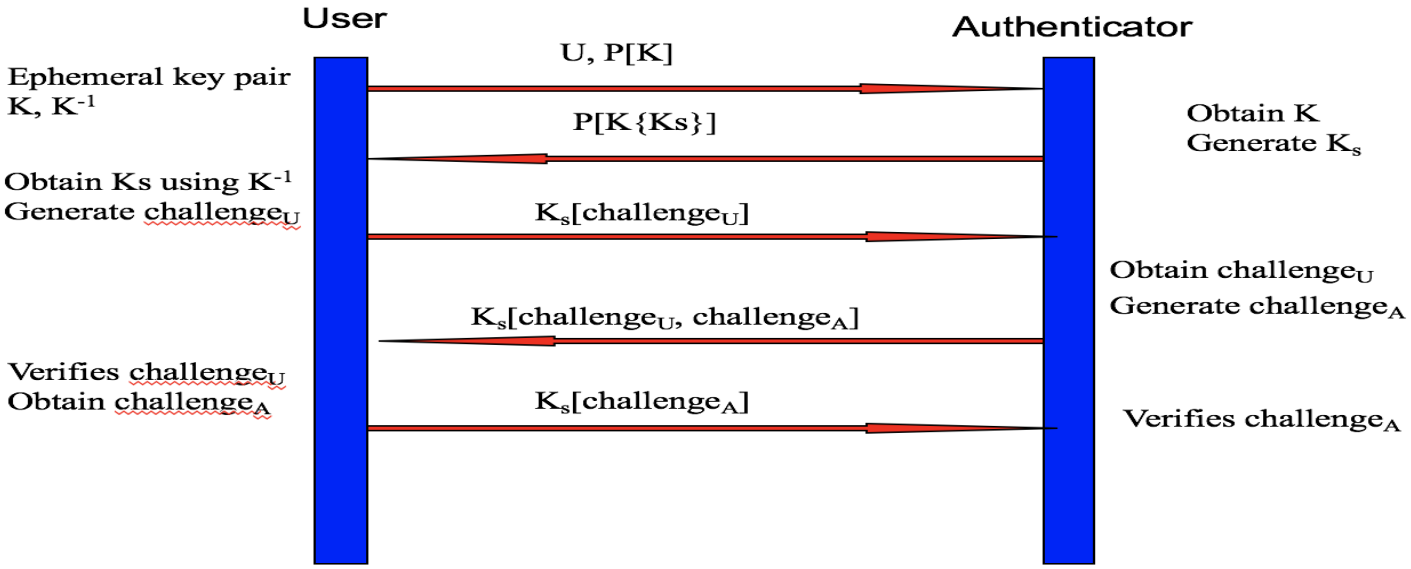
2nd Test, January 8th, 2018

- 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. Biometric Systems
    a. Suppose you are in charge of deploying a biometric system in an airport and in a metro station. How should each deployment prioritize the False Acceptance Rate or False Rejection Rate? Justify.

    b. What is the difference between Identification and Authentication? Provide an example of a biometric system usage for each case.

2. Regarding Authentication Systems:
    a. Consider a system that uses the S/Key authentication protocol with passwords sent in plaintext. Consider also a passive attacker that is able to sniff two consecutive authentication requests by a client. Is the attacker able to guess the next authentication request? Justify.



Notation

P – Password, known by U and A
K[m] – Cipher m with the **secret** key K
K^{-1}[m] – Decipher m with the secret key K
K{ m } – Cipher m with the **public** key K
K^{-1}{ m } – Decipher m with the **private** key K^{-1}

K - Secret key generated during the protocol
$challenge_U$, $challenge_A$ – integer values generated during the protocol

b. Consider the Encrypted Key Exchange Diagram with RSA presented above. Present the steps necessary for an attacker to conduct a Man-in-the-Middle Attack. If this is not possible, justify.

c. What is the purpose of the last message in the protocol?

3. On Wireless communication protocols:
   a. Consider an Access Point with four legit clients connected using Wired Equivalency Privacy. Are they able to sniff each other's messages in plaintext? If yes, how can this be prevented? If no, justify.

b. Suppose an attacker places a rogue Access Point close to the clients to fool them. What can they do to prevent successful attack?

c. Now suppose the AP is upgraded to use WiFi Protected Access. Is it possible for clients to sniff each other's traffic? And can an attacker successfully install a rogue AP?

Client Sniffing:

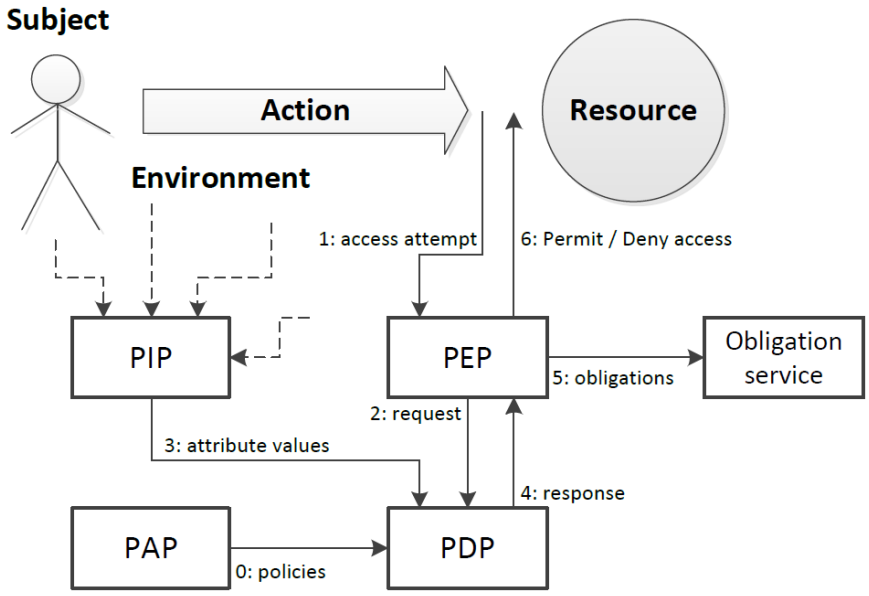
Rogue AP:

4. On Wireless communication protocols:
   a. Both WEP and Bluetooth 2.0 encrypt data with weak cipher algorithms, however Bluetooth 2.0 is more resistant to attacks to the encryption algorithm than WEP, why? Relate your answer with the techniques added to WEP in WPA.

   b. The adopted measures against attacks to the data encryption algorithms in WPA 2.0 and UMTS, differ from the previous ones, describe them briefly and how data integrity was improved.

   c. In GSM the frame number is fed to the A5 algorithm together with the encryption key to generate the keystream. What is the role of the frame number in this process? Relate your answer with the cipher modes that you have learned.

5. The following diagram represents the XACML processing model.



a. XACML is a standard for ABAC (Attribute-Based Access Control). Describe in what way ABAC allows for a precise and fine-grained authorization definition.

b. What is the PDP and what is its role in the processing of a request?

c. State which operation is not allowed in the Bell-LaPadula access control model what is not allowed, *write down* or *write up*? Justify why?

6. In the TLS protocol the Master secret (MS) is generated as:

$$MS = MD5(PMS||SHA(‘A’||PMS||R1||R2))||$$
$$MD5(PMS||SHA(‘BB’||PMS||R1||R2))||$$
$$MD5(PMS||SHA(‘CCC’||PMS||R1||R2))$$

where || represent the concatenation of values, PMS is the Pre-Master Secret.

a. Explain the use and need for the exchanged random values (R_i).

b. State which **one** of the following services in not provided by TLS (a wrong answer will count with -50% of the question value):
   - ☐ - Confidentiality.
   - ☐ - Key distribution.
   - ☐ - Non-repudiation.
   - ☐ - All of the above.

c. For each TLS session how many session keys are used?
   - ☐ - None, the *master secret is used as the session key.*
   - ☐ - 1.
   - ☐ - 2.
   - ☐ - 4.

Grading:

1:	a) 1	b) 1		T= 2
2:	a) 1	b) 1	c) 1	T= 3
3:	a) 1	b) 1	c) 1	T= 3
4:	a) 1.2	b) 1.3	c) 1	T= 3.5
5:	a) 1	b) 1	c) 1.5	T= 3.5
6:	a) 1	b) 1	c) 1	T= 3