M.EIC **Computer System Security – 2022/23** **FEUP**

Closed book exam
Duration: 1h30m
Final weight: 50%

1st call (Normal)
June.06.2023

Note: Answer in separated sheet sets the following two question groups:
Group 1: Questions 1, 2, 3, 4, and 5
Group 2: Questions 6, 7, 8, 9, and 10
You can answer in **Portuguese** or in **English**

1. [1 pt]

In the Introductory chapter of the course unit, it was stated that the human factor, because of its importance, should be considered in the project of any security system. Give a concrete example of the importance of this factor for each of the following situations:

a) system's normal use;

b) system's administration.

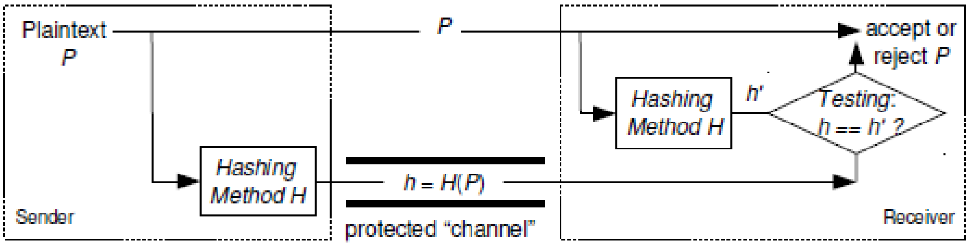
2. [1 pt]

In the review study of basic Cryptography, the nearby picture was presented, illustrating a way of achieving a specific type of protection among the group of possibilities: Confidentiality, Integrity, Availability.

a) Which specific type of protection is intended to be achieved?

b) Exemplify how can the *protected "channel"* be implemented.

c) Based on the picture presented, sketch another one that shows how to achieve <u>two</u> of the listed types of protection.

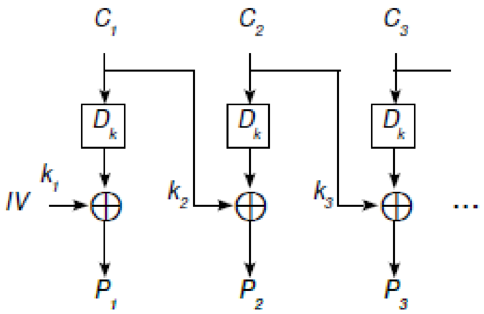


3. [1 pt]

The picture nearby represents the deciphering phase of one of the studied techniques used in the confidential transmission of "long texts": *Cipher Block Chaining*. The technique needs "padding", and there is an ingenious attack that takes advantage of that: the *Padding oracle attack*, which was exemplified in one of the practical classes' SEED labs.

a) Present the fundamental premise for the possibility of application of that attack.

b) Present the essence of the attack procedure, following the notation used in the nearby picture.



4. [1 pt]

Suppose you want to transmit to a partner a confidential long document. You both have already exchanged each other's cryptographic public keys, pertaining to a specific cryptographic algorithm.
Present:

a) your better proposal of a technique for performing the transmission – sketch an elucidating picture;

b) another, alternative, technique, pointing out its possible disadvantage.

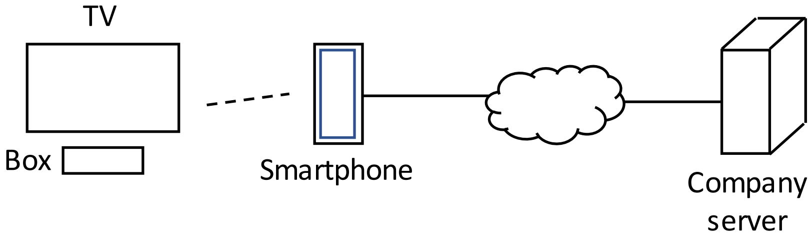
5. [1 pt]

The integrity protection solutions realistically available were presented in the chapter on "*Cryptography: general protection techniques*": 1- usage of integrity/authentication codes; 2- usage of digital signatures.

a) Distinguish the two approaches, pointing at least one strong point and one weaker point of one approach over the other.

b) Generally, in both approaches, a hashing function is used within the procedures. For each approach, explain how and why its use is deemed necessary.

6. [1 pt]



In the above illustrated scenario, a TV cable box holds a private key and the public key of the cable company. Assume also that a client mobile TV application can talk to the company server (which knows about the deployed boxes including their public keys). For the subscriber to be able to see a TV channel from the box in his smartphone app, he needs first to do a pairing (authentication) operation between the box and the smartphone app. After a successful pairing, the box transmits the TV channel wirelessly to the smartphone app.

a) The pairing initiates requesting it in the box and then reading with the app a QR-code shown on the TV. What information should that **QR-code contain** to be transmitted to the company server to establish the identity of the box and prevent valid replay attacks?

b) A while after reading the QR-code and obtaining information from the server the box and the smartphone establish a wireless connection. Before starting the transmission of the TV channel, the smartphone sends a message to the box. What should that **message contain** in order for the box to know for sure that it is a reply to the initial QR-code and it is authorized to transmit the TV channel? Explain.

7. [1 pt]

When transmitting information securely between two nodes on a network, we can use two different general methods, known as transport-level security and message-level security.

a) What security properties are intended to be guaranteed with these methods?

b) State the main difference between the two methods. Is anyone better than the other? If so, what is a possible weakness of the one considered less secure?

8. [1 pt]

The most common authorization information or rules specify, for each user, the operations he can perform in each protected resource, on a computing system or application.

a) In DAC (*discretionary access control*) that information can be provided in two different ways: the *access control list* (ACL) or the *capability list*. State the differences, and give the reason why those representations are used, instead of a full *access matrix* indexed by users and resources?

b) RBAC (*role-based access control*) is another way of specifying and enforcing authorization rules. What is the main difference relative to DAC? Is this difference advantageous? Explain why or why not.

9. [1 pt]

In a web application, many times the authentication mechanism is delegated to another server.

a) Describe the way to accomplish that in the web application server. How is the result delivered to the application?

b) The authorization information is many times represented in a token. What are the differences between a JWT (Json web token) and an opaque token? How a separated resource provider, receiving such a token, can verify if a requested operation can be performed or not? Explain.

10. [1 pt]

A rising vulnerability and exploitation in web applications is the one known as SSRF (*server-side request forgery*).

Explain in what it consists of, and what can be the consequences of its exploitation. How a developer can avoid it?

JMC/APM