M.EIC Segurança em Sistemas Informáticos (Computer Systems Security) – 2024/25 FEUP

Exam without consultation of documentation (*closed-book* exam)
Duration: 1,5 hours
Weight in course final grade: 50%

Normal Exam
20.June.2025

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 may answer in English or in Portuguese.

---

1. [1 pt]

In the Introductory chapter of the course unit, one of the points considered for projecting a security system was establishing *trustiness*. In that respect, comment on the following situation:
When a teacher or student wants to use one of the computers administered by FEUP's Informatics staff, he/she has to login in the machine by typing his/her name and password on the keyboard that is attached to the computer.

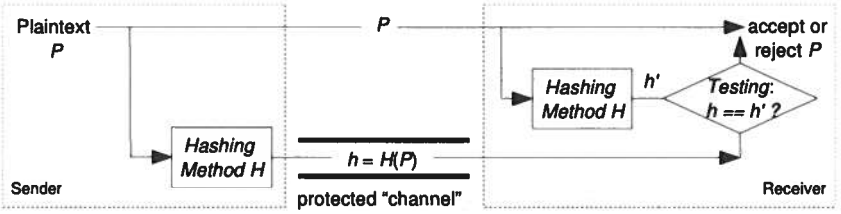
2. [1 pt]

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

a) What security properties should the "protected channel" shown have?

b) Why does *P* is not transmitted through the "protected channel" as well?

c) Why is a '*Hashing Method*' used in the scheme shown? Is it inevitable in that scheme?



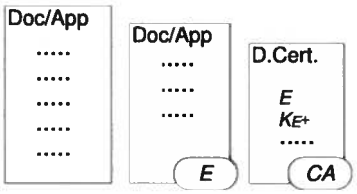
3. [1 pt]

For the secure distribution of documents (Doc) or software (App), the usual procedure followed by the Emmiter (E) is to:

. digitally sign the Doc/App, by generating $[Doc/App]_E$
. append to the signature a digital certificate (DC) with the public key of E, signed by a Certificate Authority (CA): $[DC(E)]_{CA}$
. send "everything" (shown in the picture) to the Receiver (R)

a) Present the procedure followed by the Receiver in order to use with confidence the just received "package".

b) Suppose the Receiver does not possess the public key of that specific Certificate Authority. Would that be a problem?

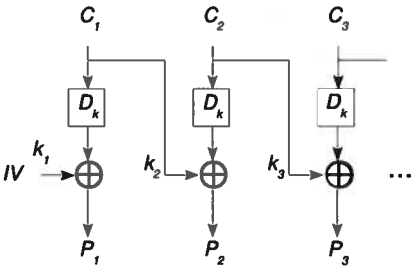


4. [1 pt]

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 the practical classes' SEED labs.

a) What is 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.



5. [1 pt]

«*Authenticated Enciphering Modes*» was one of the class subtopics of the course unit.

a) Why are they necessary instead of using just *Enciphering Modes*?

b) There are two main approaches to their implementation: «*(external) combination of protective techniques*» and «*"intrinsic" combination*». For each approach, sketch a picture that illustrates the general principles behind it.

6. [1 pt]

An important vulnerability that can happen in the design of distributed applications is the use of serialized objects, especially in Java.
Explain in what can consist this vulnerability and some of their exploitations. How can, in general, such an exploitation be avoided?

7. [1 pt]

One of the authorization mechanisms is known as MAC (mandatory access control). It is characterized by defining a label for subjects and objects and establishing a hierarchy between those labels. Labels can have several components, such as a value denoting a security level, and a set of topics (compartments).

a) What are the conditions for a user (subject) to be authorized to write (create or append) to a resource (object) ? Explain what that rule tries to accomplish.

b) In a concrete situation we have 3 users and 1 document with the following labels (s–security level, C-compartments):
User A (s=3; C={economy})
User B (s=4; C={economy, deficit})
User C (s=1; C={economy})
Doc A (s=3; C={economy})
Who is authorized to add information to it? And who is authorized to edit it? Explain.

8. [1 pt]

Recently the FIDO (Fast Identity Online) initiative pretends to standardize a password less cryptographic authentication mechanism, allowing e.g., the use of external devices (like a smartphone) to verify the presence and authenticate a user. It needs a previous registration operation. Describe the steps and cryptography involved in this registration operation.

9. [1 pt]

In many protocols the message content between two nodes in a network needs to have confidentiality and integrity guarantees.

a) How can you also guarantee the origin of the message? Explain a mechanism to have it.

b) What is transport level security and message level security? Explain. What should you prefer if you know that two nodes have a direct network connection? Why?

10. [1 pt]

Web servers supplying web applications usually delegate authentication and/or authorization to another service/server. Also, many times, protected resources used by a web application are kept separate in a resource server.

a) Describe how a web application user, requiring user authentication, can do that operation on a separate authentication server.

b) A technique for representing a token is a PoP (proof of purchase) token. Describe one possible form for these type of tokens. Explain how the resource server can know for sure that it was supplied to the web server in a legitim way.

APM/JMC