M.EIC **Computer System Security – 2021/22** **FEUP**

Closed book exam **1st call (Normal)**
Duration: 1h30m **20.June.2022**
Weight in course final grade: 50%

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 **Portuguese** or in **English**

---

1. [1 pt]

Right in the Introductory chapter of the course unit, it was stated that the ultimate goal of Computer Systems Security was providing access control to resources (owned by someone).
Connect that ultimate goal to the classical goals of providing protection of Confidentiality, Integrity, Availability and Authentication.

2. [1 pt]

Consider a company whose Informatics' security system is structured following Bell-LaPadula's model. Each Subject and each Object pertaining to the system is classified along the security levels: SECRET, CONFIDENTIAL, PUBLIC and the security categories: {DEVELOPMENT, OPERATIONS, PRODUCTION}.
Suppose that Robert is an employee of the company that has clearance (SECRET, {OPERATIONS}) and, apparently, needs to access `Blue Manual #2`, document classified as (CONFIDENTIAL, {DEVELOPMENT, OPERATIONS}). Explain if Robert can access `Blue Manual #2` and, if he can, with what type of access.

3. [1 pt]

In the review study of basic Cryptography, a table for a tentative classification of cryptographic systems was presented. An excerpt of that table is hereby reproduced.

a) Explain the meaning of the "on the method" perspective for the operation of a cryptographic system.

b) What sense does it make to have the RSA primitive mentioned as an example of a (pure) "block" method of operation?

Perspective	***Variant***	***Sub-variant***	***Examples***
on the secret	...		
on the method	stream		RC4, One-time pad
	block	(pure)	AES, RSA (in ECB)
		mixed	AES (in CBC)
on the purpose	...		

c) Why is the AES primitive, in CBC mode, mentioned as an example of a *mixed* "block" method of operation?

4. [1 pt]

Some hashing techniques, namely SHA256, have an inherent structure that eases the hash calculation of a sequence (concatenation) of messages: e.g. *hash* ($P_1 \| P_2$) = *hash* (*hash* (P_1), P_2), where P_1 and P_2 are messages.[1] This "concatenation" feature enables, in certain conditions, the so-called *length extension attack*, which was exemplified in a SEED lab conducted in the practical classes, for Message Authentication Codes calculated as *hash* ($K \| P$), being K a (secret!) key.
The mentioned attack can be defeated by the use of certain hashing constructs, such as HMAC (as also seen in the SEED Lab), that implies *double hashing*.
But what if a simpler construct is used, such as SHA256 ($P \| K$)? Would the attack be also averted or not?

5. [1 pt]

The (simple) confidentialy protection of a message provided by a symmetric-based crytographic primitive, such as AES, might not be adequate to prevent attacks that modifiy the content of the message.
Present a construct that is able to provide dual protection (confidentiality and integrity) to a message sent from Alice to Bob.

[1] And this in spite of the techniques having a (kind of) padding "protection" which includes message length.

6. [1 pt]

We say that a remote authentication operation is executed whenever a communication channel between two nodes is involved.

a) Refer two of the main weaknesses/attacks that could be present in the design of a protocol for this operation. Justify why and how could they be exploited.

b) Refer ways to mitigate the weaknesses indicated previously, in the design and implementation of this type of protocols. Explain why they are effective.

7. [1 pt]

One type of authorization mechanism is known as MAC (mandatory access control).

a) What is the sensitivity level? To what entities is it defined? And, what are compartments (need to know)?

b) Explain how the conjugation of these two values is used to determine if a subject has read access to an object.

8. [1 pt]

The OAuth authorization protocol is based on the emission of access tokens, allowing a web application to use a protected resource on behalf of a user.

a) Access tokens can be totally opaque (just a random value). Describe how those tokens can be verified by the resource server? What is required to obtain that verification and token content?

b) How can the resource server be sure that an access token is not stolen (the sender is the one that is entitled to it)? Explain a possible mechanism to avoid token theft.

9. [1 pt]

Recently the FIDO (Fast Identity Online) initiative pretends to standardize a passwordless authentication mechanism and ecosystem, allowing e.g. the use of external devices (like a smartphone) to verify the presence and authenticate a user.

After a registration operation, authentication with the remote service is done based on a cryptographic operation. Describe the cryptography involved in this process.

10. [1 pt]

The Kerberos system is used in the authentication/authorization mechanisms in large distributed systems. After authentication, a client obtains from the Authentication Server (AS) a **ticket (Ttgs)**, giving it access to the Ticket Granting Server (TGS). When the client needs to request access to a resource server it asks the TGS for a specific ticket, sending the one obtained from the AS. In Kerberos V4 this message contains also an authenticator, defined as: $E_{Kc,tgs}$(IDc, ADc, TS), where IDc and ADc are identifiers of the client C (the sender), and TS is a time stamp. Kc,tgs is a symmetric key generated by the AS, sent to C in the first phase, and included in Ttgs.

a) What is the purpose of the authenticator, and why was it included in V4? Explain.

b) Explain how it achieves its purpose.

APM/JMC