Exam without consultation of documentation (*closed-book* exam) **Normal Exam**
Duration: 1,5 hours **4.June.2024**
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 English or in Portuguese.

---

1. [1 pt]

In the Introductory chapter of the course unit, it was presented a table: «*Threats/attacks to computer systems: classification, examples, "solutions"*». An excert of it is here reproduced:

Perspective (type):	Intent	Origin	Operation mode	Predictability	Severity
(Sub)type:	none	internal	passive	normal	normal
	on-purpose	external	active	difficult	catastrophic

Using the table, classify the following recent security issue:[1]

«*The t:connect mobile app works with the t:slim X2 insulin pump* (...)». The app is «*used as a method of viewing pump information and limited control of the pump* (...)»; the pump «*is intended to deliver insulin under the skin (subcutaneous delivery)* (...)». App's version 2.7 was distributed «*from February 12, 2024 to March 13, 2024*» and recalled starting on «*March 18, 2024*»; users were requested to update it «*to version 2.7.1 or later* (...)». «*The reason for the recall is (...) an issue with the software that may cause the mobile app to crash (...) and may lead to the pump shutting down sooner (...) which could lead to an under-delivery of insulin and may result in hyperglycemia or even diabetic ketoacidosis, which can be a life-threatening condition*(...)».
«*There have been 224 reported injuries as of April 15, 2024 and no reports of death.*»

2. [1 pt]

Complete the following table that was presented in its entirety in the review of basic cryptography concepts as "*Key types of cryptographic keys*".

Designation	***"Owner" entity***	***Main application***	***Cryptographic type***	***Longevity***	***Efficiency***
personal	?	authentication	?	?	?
session	communication channel	?	shared-key	?	?

3. [1 pt]

As presented in class, the integrity "problem" for the transmission of documents can, in principle, be cryptographically solved with any of the three techniques below. Briefly present the essential *pros* and *cons* of each technique.

1- encipherment ; 2- integrity (authentication) codes ; 3- digital signatures

4. [1 pt]

«*Randomness is essential in Cryptography*»! This was stated in one of the classes, is written in the support slides, and even was addressed in one of the proposed SEED experiments.

a) Give a real or realistic example that supports the sentence.

b) For 2 of the following types of ENT[2] tests conducted in the mentioned SEED experiment, present the result expected for a generated series of (good) random numbers:

1- frequency distribution ; 2- entropy ; 3- compression ; 4- Chi-square ; 5- arithmetic mean ; 6- Monte Carlo value for Pi ; 7- serial correlation coefficient.

---

[1] https://www.fda.gov/medical-devices/medical-device-recalls/tandem-diabetes-care-inc-recalls-version-27-apple-ios-tconnect-mobile-app-used-conjunction-tslim-x2

[2] ENT, A Pseudorandom Number Sequence Test Program

5. [1 pt]

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

a) Why are they necessary instead of just using *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]

Two parties (users or computers), connected by a network, share an asymmetric key, where the first knows the private key, and the second knows the public key.

a) In the context of the authentication mechanism explain the threat known as a *replay attack*.

b) Indicate the steps and messages, in a protocol to authenticate the first party with the second, using the shared asymmetric key, and immune to the replay attack.

7. [1 pt]

One of the fundamental mechanisms behind application security is authorization, also known as access control.

a) State the main differences between two strategies for implementing the authorization mechanism: the DAC (Discretionary Access Control) and the MAC (Mandatory Access Control)

b) Using MAC, characterized by a security level S, and a set of compartments C, state the usual conditions for a label L1 to be in a higher level than another label L2. Explain.

8. [1 pt]

The TLS protocol allows a communication channel to exchange messages maintaining confidentiality and integrity.

a) What guarantees the integrity property provides to the two ends in this context? Explain.

b) How is it usually achieved in TLS? Give an example.

9. [1 pt]

Some authentication and authorization mechanisms in web applications rely on emission and verification of tokens, like Open ID and OAuth.

a) Those mechanisms define and use identification tokens, authorization codes, access tokens, and refresh tokens. Explain the purpose of each of those tokens.

b) Access tokens can be represented in two different ways, maintaining confidentiality relatively to the client application. Explain why it is convenient to have that confidentiality, and what are those two representations.

10. [1 pt]

A rising exploitation in web applications is a consequence of the possible vulnerability known as SSRF (Server Side Request Forgery).

a) Explain what is SSRF and the impact it could have.

b) State two SSRF prevention techniques. Explain.

APM/JMC