Security
1st Semester, 2015/16

Questions 1-20: Final Exam
Questions 11-20: 2nd Intermediate Test
January 18nd 2016

- All questions provide the same number of points.
- The total duration of the exam is 3 hours.
- The duration of the 2nd Intermedia Test is 1 hour and 30 minutes.

1) Describe how Mallory (a user) can execute a Reflected XSS (Cross Site Scripting) attack against Alice.

2) Describe the concepts of Policy and Mechanism and their relation in the context of a security domain.

3) Considering Information Security, comment the phrase "*To know your enemy, you must become your enemy*" by Sun Tzu, under the scope of the defence measures against attacks.

4) Define CVE (Common Vulnerabilities and Exposures) and CWE (Common Weaknesses Enumeration), and describe how they are related.

5) Considering a polyalphabetic cipher, what is considered its period?
   a) Describe the method that allows to determine the period from a cryptogram.

6) Considering the OFB and CBC cipher modes, when deciphering a cryptogram, please describe with reasonable detail:
   a) The effect of a communication error flipping 1 bit of the IV.
   b) The effect of a communication error flipping 1 bit of the first block of the cryptogram.

7) Describe how to construct a secure MAC (Message Authentication Code):
   a) Only using a cipher and XOR operations.
   b) Only using digest functions.

8) Considering the Vernam cipher, describe a practical approximation and compare its security and usability in relation to the original cipher.

9) In the context of the RSA cipher how the block size is defined, and what is its practical value?

10) What properties a hash function must have so that it can be used to create secure digital signatures?

11) For the purpose of authenticating a user wanting to access a valuable area (think of a bank vault), and considering that the communication channel is secure, compare the challenge-response approach using a smartcard and the direct approach using biometrics.

12) Describe the operation of the S/Key mechanism, including the setup and authentication processes.

13) Describe the certificates present in the Portuguese Citizen Card.
    a) Explain its relevancy in the context of a citizen validating a digital signature created by another citizen with a similar card (same year).

14) Define the ★ properties of the Biba and Bell-LaPadula models.
    a) They oppose each other in a system combining both approaches? Justify.

15) What are Security Labels and why they are important in the scope of multi-level object access.

16) In the context of the Linux Operating System
    a) What is a process?
    b) How are user permissions associated to a process and how this relates to the user creating the process?

17) In a login process into a Linux host and considering the content of the `/etc/shadow` file:
    a) How is the file content used to validate the user credentials without exposing them?

18) Considering the Plausible Deniability concept:
    a) Define the concept.
    b) Describe with detail how it can be implemented in a storage volume.

19) Describe a practical malleability attack in storage volumes ciphered with AES-CBC.
    a) How can this attack compromise a system?

20) Considering the EFS (Encrypting File System) in NTFS, and the structure of the file headers,
    a) Explain the choices made from the perspective of multi user access.
    b) Explain the choices made from the perspective of performant data access.