Security
1st Semester, 2009/10

2nd Test / 1st Exam
January 15, 2010

- All questions have the same grade.
- Total duration time of test is 1 hour and 30 minutes (last 10 questions).
- Total duration time of exam is 3 hours (20 questions).

1. Consider the *stack smashing attack*s using C. Explain:
    a. What is the vulnerability of the C programming language that allows such attacks?
    b. Describe a process to detect such attacks.

2. Explain the general operation model of a stream cipher implemented by a block cipher working in Counter mode (CTR), providing an illustrating diagram.

3. The Counter mode (CTR) allows the implementation of stream ciphers with uniform random access time in the encryption/decryption of large data sets. Explain:
    a. Why does CTR possesses this characteristic?
    b. What make this cipher mode particularly interesting for the encryption of file contents in file systems with security of file's contents?

4. Digest functions must complicate the discovery of a second pre-image. Explain:
    a. What does it mean such discovery?
    b. Why it is critical for the validation of digital signatures calculated over values computed with digest functions?

5. A MAC (*Message Authentication Code*) is a data authentication method. Explain:
    a. What is the general model of generation and validation of a MAC?
    b. How can it be implemented exclusively with a cipher function?

6. What are the basic mathematical assumptions of the RSA security?

7. Consider the file system with file content encryption capabilities. Explain:
    a. Why may not be enough the ordinary file access control mechanisms, such as access control lists (ACL), for controlling the access to files' contents?
    b. What are the implications of content encryption in the file sharing among several users?

8. Explain, providing an example with Cartão de Cidadão, why smartcards are useful for implementing a Public Key Infrastructures (PKI).

9. Consider the management of public keys. Explain:
    a. What is a Certification Authority (CA)?
    b. How can users assess, at a given moment, their confidence in a particular Certification Authority?

10. Consider the issue of the lifetime of a public key certificate. Explain:
    a. How is the lifetime controlled?
    b. Which mechanisms are available for users to check if a certificate has not yet expired?

11. Consider the challenge-response authentication protocols. Explain:
    a. Why must the challenge be a value never used before (*nonce*)?
    b. How can they be implemented using the Cartão de Cidadão?

12. Explain how does the S/Key authentication protocol works, referring these specific details:
    a. Data initialization at the authenticator (or authentication server).
    b. Authentication protocol.

13. Consider the authentication protocols with a shared secret. Explain:
    a. What is a dictionary attack?
    b. Why are the GSM and RSA SecurID protocols immune to such attacks?

14. Consider the discretionary access control (DAC) and the mandatory access control (MAC).
    a. Explain the difference between them.
    b. Give examples for each of them considering an operating system as an access control monitor.

15. A role-based access control (RBAC) policy is different from an access control policy using access control lists (ACL) based on groups. Explain why.

16. Explain the general operating principle of an information flow control policy.

17. Explain the general operation principle of Biba's integrity control policy.

18. Consider the databases with multi-level security. Explain:
    a. What is their general operation model?
    b. How can we implement them using encryption of sensitive values?

19. What is the goal of the universal records of common vulnerabilities and exposures (CVE)?

20. Explain why Java Virtual Machines (or Java Run-time Environments) do not allow java.* classes to be loaded from the network.