Security
1st Semester, 2010/11

2nd Exam
February 1, 2010

- All questions have the same grade.
- Total duration time of exam is 3 hours.

1. Why can we have buffer overflows in C and not in Java?
2. Consider the logic circuit known as LFSR (Linear Feedback Shift Register), used to implement stream ciphers. Explain:
    a. What is the maximum period of the bit sequence it produces?
    b. What does it means to have a primitive feedback polynomial?
3. Show, mathematically, why the RSA cipher would be insecure if it was possible to:
    a. Factorize easily big numbers.
    b. Calculate easily discrete logarithms of large numbers.
4. Using the Birthday Paradox, show what is, approximately, the maximum collision resistance of a digest function. Justify appropriately your answer.
5. Describe the execution model of the HMAC construction, used to compute a MAC (Message Authentication Code) of a message.
6. Consider the concept of digital signature. Explain the motive that justifies the inclusion of additional information in its construction (besides the document to sign, or its digest).
7. Explain, as completely as possible, why public key certificates are vital for supporting the validation of digital signatures.
8. Consider the concept of CRL (Certificate Revocation List). Explain:
    a. Who manages a CRL?
    b. Who, and when, should we use its information?
9. Explain, giving an example, which risks takes a user when its certificate repository is attacked by a virus introducing false information.
10. Explain, in detail, the Linux authentication process.

11. GSM uses an authentication process exploring, simultaneously, something a person has and something a person knows. Explain why, complementing your explanation with a diagram.
12. Considering that the Cartão de Cidadão (Citizen Card) does not perform decryptions with its private keys, but only signatures, how could you use it to perform a remote challenge-response authentication?
13. Consider the concept of mandatory access control. Show:
    a. How does it work?
    b. Give two practical examples of its use.
14. What are the practical advantages of the separation of duties principle for the security of a system?
15. Explain the principles of the Bell-LaPadula flow control model.
16. Consider the Clark-Wilson integrity model. Explain what is:
    a. A CDI (Constrained Data Item) and an UDI (Unconstrained Data Item)
    b. An IVP (Integrity Verification Procedure) and a TP (Transformation Procedure).
17. Explain why inference represents a problem for the security of a database management system.
18. Consider a multilevel database, where data is encrypted according to a security level. Explain:
    a. What is the consequence of this fact for the users of the database?
    b. Which particular good practices should be followed in the data encryption?
19. In the Internet there are sensors that evaluate the network risk level. Explain:
    a. What are those sensors?
    b. How do they evaluate the risk?
20. Explain why Java Virtual Machines (or Java Run-time Environments) impose restrictions to the places from where they load classes for the running applications?