Segurança
1º Semestre, 2009/10

2º Teste / 1º Exame
15 de Janeiro de 2010

- Todas as perguntas têm a mesma cotação.
- A duração total do teste é de 1 hora e 30 minutos (últimas 10 perguntas).
- A duração total do exame é de 3 horas (20 perguntas).

1. Considere os ataques por esmagamento da pilha (*stack smashing attack*) usando C. Explique:
    a. Qual é a vulnerabilidade da linguagem de programação C que permite tais ataques?
    b. Descreva um processo de detecção de tais ataques.

2. Explique qual o modelo geral de operação de uma cifra contínua concretizada por uma cifra por blocos em modo contador (*Counter*, CTR), ilustrando-o com um diagrama.

3. O modo contador (*Counter*, CTR) permite a concretização de uma cifra contínua com acesso aleatório uniforme na cifra/decifra de dados volumosos. Explique:
    a. Por que razão o modo CTR possui essa característica?
    b. O que torna este modo particularmente interessante para a cifra de conteúdos de ficheiros em sistemas de ficheiros com segurança dos conteúdos.

4. As funções de síntese devem dificultar a descoberta de uma segunda pré-imagem. Explique:
    a. Em que consiste essa descoberta?
    b. Por que razão tal é crítico no âmbito da validação de assinaturas digitais calculadas sobre valores calculados com funções de síntese?

5. Um MAC (*Message Authentication Code*) é um meio de autenticação de dados. Explique:
    a. Qual é o modelo geral de geração e validação de um MAC?
    b. Como pode ser concretizado apenas com uma função de cifra?

6. Quais são os pressupostos matemáticos base em que se baseia a segurança do RSA?

7. Considere os sistemas de ficheiros com capacidade de cifra de conteúdos de ficheiros. Explique:
    a. Por que razão podem não ser suficientes os mecanismos usuais de controlo de acesso aos ficheiros, como as listas de controlo de acesso (*Access Control Lists*, ACL), para controlar o acesso aos seus conteúdos?
    b. Quais as implicações da cifra dos conteúdos na partilha de ficheiros entre vários utentes?

8. Explique, exemplificando com o Cartão de Cidadão, porque razão os *smartcards* são úteis para a implantação de infra-estruturas de chave pública (*Public Key Infrastructures*, PKI).

9. Considere a gestão de chaves públicas. Explique:
    a. O que é uma Entidade Certificadora (*Certification Authority*, CA)?
    b. Como podem os utentes avaliar, em cada momento, a sua confiança numa dada Entidade Certificadora?

10. Considere o problema do tempo de vida de um certificado de chave pública. Explique:
    a. Como é que o mesmo é controlado?
    b. Que mecanismos existem para os utentes verificarem se um certificado ainda não expirou?

11. Considere os protocolos de autenticação com desafio-resposta. Explique:
    a. Por que razão o desafio tem de ser um valor nunca antes usado (*nonce*)?
    b. Como podem ser realizados estes protocolos usando o Cartão de Cidadão?

12. Explique como funciona o protocolo de autenticação S/Key, nomeadamente os seguintes aspectos:
    a. Iniciação dos dados no autenticador (ou servidor de autenticação).
    b. Execução da autenticação.

13. Considere os protocolos de autenticação com segredo partilhado. Explique:
    a. Em que consiste um ataque com dicionário?
    b. Por que razão o protocolos do GSM e do RSA SecurID não são vulneráveis a este tipo de ataques?

14. Considere os modelos de controlo de acesso discricionário (*Discricionary Access Control*, DAC) e obrigatório (*Mandatory Access Control*, MAC).
    a. Explique a diferença entre ambos.
    b. Dê exemplos de cada um considerando um sistema operativo como monitor de controlo de acesso.

15. Uma política de controlo de acesso por funções (*Role-Based Access Control*, RBAC) é diferente de uma política de controlo de acesso com listas de controlo de acesso (*Access Control Lists*) baseadas em grupos. Explique porquê.

16. Explique o princípio geral de operação de uma política de controlo de fluxos de informação.

17. Explique o modelo geral de operação da política de controlo de integridade de Biba.

18. Considere as bases de dados com segurança multi-nível. Explique:
    a. Qual é o seu modelo genérico de operação?
    b. Como se concretiza a mesma usando a cifra da valores sensíveis.

19. Qual é o propósito dos registos universais de vulnerabilidades comuns (*Common Vulnerabilities and Exposures*, CVE)?

20. Explique por que razão as Java Virtual Machines (ou os Java Run-time Environments) não permitem que as classes java.* sejam carregadas a partir da rede.