Segurança
1º Semestre, 2011/12

2º Teste / Exame de Época Normal
13 de Janeiro de 2012

- 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 com pormenor como os mesmos podem ser mitigados alterando o endereço base de início da pilha de cada vez que um programa inicia a sua execução.

2. Explique qual o modelo geral de funcionamento de uma cifra contínua concretizada explorando uma cifra por bloco. Ilustre a sua resposta com um diagrama.

3. Explique, ilustrando a sua resposta com um diagrama e com provas matemáticas, por que razão uma cifra por blocos em modo CBC (*Cipher Block Chaining*) é comparável, em termos de resultado final, a uma cifra polialfabética.

4. Explique como opera a cifra assimétrica RSA, ilustrando a sua explicação com as expressões matemáticas da cifra (não precisa de explicar processo de geração das chaves, apenas a sua constituição).

5. Qual é relação entre o Paradoxo do Aniversário e a aferição do limite máximo da robustez de uma função de síntese à descoberta de colisões? Ilustre a sua resposta com um exemplo.

6. Um MAC (*Message Authentication Code*) é um meio de autenticação de dados. Explique como pode ser usado para garantir uma sequência correta de mensagens enviadas e recebidas (e.g. pacotes UDP) num fluxo de mensagens bidirecional entre duas entidades.

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

8. Considere o problema da validação de um certificado de chave pública. Explique, com pormenor, quais as vantagens e desvantagens de usar listas de certificados revogados (*Certificate Revocation List*, CRL) ou serviços OCSP (*Online Certificate Status Protocol*) pela entidade validadora.

9. Um certificado de chave pública X.509 certifica, para além de uma chave pública, o fim a que a mesma se destina.
    a. Qual é, de entre vários existentes, o interesse primordial da certificação de uma chave pública?
    b. Indique três tipos de fins a que se pode destinar uma chave pública certificada (lembre-se do Cartão de Cidadão).

10. As cadeias de certificação terminam quando se atingem certificados declarados como confiáveis. Explique:
    a. Porque terminam nestes certificados?
    b. Quem define quem são estes certificados?

11. Explique como funciona o sistema de cifra de conteúdos de ficheiros do EFS (*Extended File System*) do Windows.

12. Considere os protocolos de autenticação com desafio-resposta. Explique, ilustrando com um diagrama, como pode realizar um protocolo unilateral desse tipo usando as operações de cifra assimétricas do Cartão de Cidadão (do autenticado).

13. O protocolo de autenticação S/Key é vulnerável a ataques com dicionários à senha do autenticado? Justifique, considerando duas situações distintas:
    a. Acesso do atacante aos dados mantidos pelo autenticador.
    b. Acesso do atacante aos dados trocados remotamente entre autenticador e autenticado.

14. Por regra, os mecanismos de controlo de acesso implicam alguma forma de autenticação prévia do sujeito controlado. Explique esta afirmação tendo em conta o mecanismo geral de controlo de acesso.

15. Considere o modelo de controlo de acesso discricionário (*Discricionary Access Control*, DAC). Explique:
    a. Qual a diferença entre posse de direitos (positivos), ausência de direitos ou posse de direitos negativos.
    b. Dê um exemplo de aplicação prática útil de direitos negativos.

16. Explique em que consiste uma política de controlo de acesso por funções (*Role-Based Access Control*, RBAC).

17. O modelo de integridade de Clark-Wilson considera a existência de dois tipos de dados: UDI (*Unconstrained data Item*) e CDI (*Constrained Data Item*). Explique a diferença entre ambos no âmbito de aplicação do modelo.

18. Considere as bases de dados com segurança multi-nível. Indique duas formas de evitar que uma aplicação com um nível de segurança consiga usar dados classificados com níveis de segurança superiores.

19. Considere o registo universal de vulnerabilidades (*Common Vulnerabilities and Exposures*, CVE). Indique:
    a. Que tipo de informação existe neste registo?
    b. De que forma esta informação pode ser útil para os gestores de sistemas computacionais em rede?

20. As classes Java carregadas numa *Java Virtual Machine* (ou *num Java Run-time Environment*) são segregadas por diferentes *Protection Domains*. Explique:
    a. Que vantagens advém dessa segregação?
    b. Qual é a política base para a sua realização?