Segurança
1º Semestre, 2010/11

2º Teste / 1º Exame
14 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 o conceito de ataque por esmagamento da pilha (*stack smashing attack*). Discuta a sua viabilidade caso existissem duas pilhas, e não apenas uma: uma para guardar parâmetros e variáveis locais, outra para guardar endereços de retorno e endereços de blocos de pilha (*stack frames*).
2. Considere o conceito de cifra tripla. Explique:
    a. O que motiva a sua utilização?
    b. Porque razão se usa a cifra tripla com a aproximação EDE?
3. A cifra RSA baseia a sua segurança em duas propriedades: dificuldade na factorização de grandes números e dificuldade no cálculo de logaritmos discretos de grandes números. Explique porquê?
4. Explique a aplicabilidade do Paradoxo do Aniversário à resistência à colisão das funções de síntese.
5. Descreva o modelo genérico de execução das funções de síntese (i.e. como são realizadas).
6. Considere o conceito de assinatura digital. Explique:
    a. Como é que a mesma é construída? Ilustre com um diagrama.
    b. Como é que a mesma é validada? Ilustre com um diagrama.
7. Considere o padrão de facto PKCS #11. Explique:
    a. Em que consiste?
    b. Porque razão ele não consegue abarcar todas as funcionalidades do Cartão de Cidadão?
8. Explique, de uma forma o mais completa possível, por que razão se usam certificados de chaves públicas.
9. Por que razão é fundamental que a chave privada de assinatura seja gerada dentro do Cartão de Cidadão e daí não possa sair?
10. Explique as vantagens que advém da hierarquia de certificação do Cartão de Cidadão possuir como raiz o certificado auto-assinado da Entidade Certificadora internacional GTE Cyber Trust Global Root.

11. Considere os paradigmas de autenticação com apresentação directa de credenciais e com desafio-resposta. Explique:
    a. Qual é a diferença fundamental entre as mesmas?
    b. Em que situações pode (deve) ser explorado cada um deles?
12. Considere o conceito de autenticação com senha única. Explique:
    a. Em que consiste?
    b. Quais as suas vantagens e desvantagens?
13. Considere o modelo de autenticação GSM. Explique:
    a. Como funciona?
    b. Que riscos podem advir de uma personificação de uma BTS (*Base Transceiver Station*) por um atacante?
14. Considere o conceito de monitor de controlos de acesso. Indique:
    a. Para que serve?
    b. Dê dois exemplos práticos da sua exploração.
15. Considere o conceito de matriz de controlo de acesso. Indique:
    a. Em que consiste a sua decomposição em Listas de Controlo de Acesso (*Access Control Lists*, ACLs)?
    b. Em que consiste a sua decomposição em capacidades (*capabilities)*?
16. Considere o conceito de controlo de acesso baseado em funções (*Role-Based Access Control*, RBAC). Explique:
    a. Em que consiste?
    b. Por que razão não pode ser concretizado com controlos de acesso baseados em grupos, usando um grupo por função?
17. Considere os modelos de controlo de fluxo. Explique:
    a. Em que consistem?
    b. Que informação é usada pelo monitor de controlo de acesso para tomar decisões?
18. Considere o modelo de controlo de integridade de Clark-Wilson. Explique em que consiste:
    a. Um CDI (*Constrained Data Item*) e um UDI (*Unconstrained Data Item*)
    b. Uma IVP (*Integrity Verification Procedure*) e uma TP (*Transformation Procedure*).
19. Considere o conceito de informação sensível. Explique:
    a. Em que consiste ser inerentemente sensível? Dê um exemplo.
    b. Em que consiste ser sensível por provir de uma fonte sensível? Dê um exemplo.
20. Considere o catálogo público de CVE (*Common Vulnerabilities and Exposures*). Explique:
    a. Que vantagem advêm da sua existência para as potenciais vítimas?
    b. Que riscos advém da sua publicitação para potenciais atacantes?