Segurança
1º Semestre, 2009/10

2º Exame
29 de Janeiro de 2010

- Todas as perguntas têm a mesma cotação.
- 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. Numa arquitectura x86, qual é o problema causado pela alteração das cópias de registos EBP salvaguardadas na pilha?
    b. Quais as vantagens que adviriam da incapacidade de executar instruções localizadas em zonas de memória afectas à pilha?

2. Considere o modelo geral de operação de uma cifra contínua concretizada por uma cifra por blocos em modo CFB (*Cipher Feedback*) e CTR (*Counter*). Compare-os quanto aos seguintes aspectos:
    a. Comprimento do ciclo da chave contínua produzida.
    b. Tolerância a erros em *bits* do criptograma.

3. Considere a cifra assimétrica RSA. Explique:
    a. Como são constituídas as suas chaves privada e pública?
    b. Como são usadas as suas chaves privada e pública no âmbito da troca confidencial de dados?

4. Um MAC (*Message Authentication Code*) é um meio de autenticação de dados. Explique que vantagens e desvantagens podem existir quando se compara as seguintes opções no seu cálculo: (i) cifra de uma síntese dos dados, ou (ii) síntese conjunta dos dados e da chave de cifra.

5. É normal as assinaturas digitais conterem alguma meta-informação, i.e. serem constituídas por mais dados do que o simples resultado da cifra da síntese do documento com uma chave privada. Indique as vantagens da seguinte meta-informação:
    a. Certificado de chave pública do assinante.
    b. Cadeia de certificação desse certificado.

6. Descreva com pormenor o modelo de protecção de ficheiros com cifra do EFS (*Encrypted File System*).

7. Considere a gestão de chaves públicas. Explique, justificando, qual é a importância das Entidades Certificadoras raiz (*Root Certification Authorities*) para o processo global de confiança nessa gestão.

8. As chaves privadas protegidas dentro de *smartcards* podem ser geradas dentro dos mesmos ou podem ser geradas externamente e inseminadas nos *smartcards*. Discuta as vantagens e desvantagens dos dois métodos tendo em conta as seguintes utilizações dessas chaves:
    a. Assinatura digital
    b. Comunicação confidencial.

9. Considere o padrão PKCS #11. Explique:
    a. Em que consiste?
    b. Como é que o mesmo é explorado na prática?

10. Explique o modelo geral de exploração dos *Pluggable Authentication Modules* (PAM) do Linux.

11. Descreva e dê exemplos dos 3 modelos genéricos de autenticação de pessoas.

12. Descreva como funciona o modelo de autenticação do GSM, focando todas entidades e trocas de dados envolvidas.

13. Imagine que pretende controlar o acesso a áreas protegidas usando fechaduras activadas através do Cartão de Cidadão. Indique que cuidados deve ter, na interacção com o Cartão de Cidadão, para tornar o controlo de acesso tão fidedigno quanto possível.

14. Considere uma política de separação de deveres (*Separation of Duties*). Explique:
    a. Em que consiste.
    b. Qual é a sua relevância para a segurança de uma organização.

15. Considere o modelo de controlo de integridade de Clark-Wilson, que usa regras de certificação e regras de implantação (*enforcement*). Explique:
    a. O princípio geral do modelo.
    b. A diferença entre regras de certificação e implantação.

16. Explique em que consiste o problema da inferência quando se utiliza uma base de dados contendo itens de informação sensível protegidos.

17. A cifra de itens de informação sensível numa base de dados com segurança multi-nível pode não ser suficiente para evitar o problema da inferência. Explique porquê.

18. Uma vulnerabilidade identificada através de um registo CVE (*Common Vulnerabilities and Exposures*) pode ajudar um atacante? Justifique a sua resposta?

19. Explique o que é um ataque do dia 0 (*Zero-day attack*) e quais os seus riscos.

20. No âmbito do Java e do seu ambiente de execução (*Java Run-time Environment*, JRE), qual é a relevância dos domínios de protecção (*protection domains*) para a implantação de contextos de execução confinados (*sandboxes*).