Segurança
1º Semestre, 2008/09

2º Exame
30 de Janeiro de 2008

- Todas as perguntas têm a mesma cotação.
- A duração total do exame é de 3 horas.

1. Explique a diferença entre uma política de segurança e um mecanismo de segurança. Dê um exemplo envolvendo autenticação de pessoas.
2. Descreva o modo como se processa um ataque por esmagamento da pilha (*stack smashing attack*).
3. Explique qual o modelo geral de operação de uma cifra contínua, ilustrando-o com um diagrama.
4. Uma cifra contínua propaga erros na decifra de um criptograma com erros? Justifique a sua resposta.
5. Uma cifra assimétrica como a RSA é uma cifra por blocos. Indique como são definidos os blocos, nomeadamente qual é a dimensão dos mesmos.
6. Quando se considera a cifra de dados de ficheiros ao nível dos sistemas de ficheiros, há diversos metadados desses ficheiros que não podem ser cifrados, porque precisam de ser analisados por terceiros. Dê 2 exemplos desses metadados e explique porque não podem ser cifrados.
7. Indique as vantagens e desvantagens de usar ECB (*Electronic Code Book*) ou CBC (*Cipher Block Chaining*) na cifra de conteúdos de ficheiros.
8. Explique o que é o padrão PKCS #11.
9. O Cartão de Cidadão é um *smartcard* que permite efectuar assinaturas digitais qualificadas. Por omissão, essa funcionalidade está desactivada no acto de entrega do cartão, podendo ser solicitada a sua activação pelo dono. Explique como, tecnicamente, essa activação é concretizada.
10. Um *smartcard* não é um mero circuito de memória, mas possui um processador e inclusive capacidades de execução de funções criptográficas complexas e de geração de valores aleatórios. Explique a utilidade destas duas últimas capacidades.
11. Explique de que forma a arquitectura PAM permite a integração de diferentes paradigmas de autenticação de pessoas (com senha, com o Cartão de Cidadão, etc.) com diversas aplicações Unix.
12. Um ataque a senhas de acesso com dicionários é um ataque exaustivo? Justifique a sua resposta.
13. Explique em que consiste um protocolo de autenticação com desafio-resposta e porque razão se usa.
14. Explique como funciona o protocolo de autenticação com senhas únicas S/Key.
15. Discuta a sensibilidade do protocolo S/Key a ataques com dicionários.
16. Explique como funciona o protocolo de autenticação do GSM.
17. Descreva três problemas da autenticação biométrica que não se verificam com outros paradigmas de autenticação.
18. O que é um certificado auto-assinado e qual o seu valor (ou utilidade)?
19. Explique para que serve o protocolo OCSP (*Online Certificate Status Protocol*) e em que circunstância deve ser usado.
20. Explique o que é, para que serve e como é usada uma cadeia de certificação.