Instituto Superior de Engenharia de Lisboa

Licenciatura em Engenharia Informática e de Computadores

Licenciatura em Engenharia Informática, Redes e Telecomunicações

Segurança Informática

Teste final, Época normal, Semestre de Inverno, 2019/20

Duração: 2 horas e 30 minutos

Justifique todas as respostas.

1. (1) No contexto das primitivas de cifra simétrica em bloco, foi proposto um algoritmo de *padding* que preenche os *bytes* em falta no último bloco com zeros (0). Quais as limitações desta solução?

2. (1,5) Considere um novo esquema criptográfico AE. O objectivo é fazer uma cifra simétrica com garantias de integridade, ou seja, caso os criptogramas sejam modificados no canal de comunicação, tal seria detetado pelo destinatário.

   As funções AE_e e AE_d realizam a cifra e decifra autenticada, sendo E uma primitiva de cifra simétrica, H uma função de *hash* criptográfica e $||$ a concatenação.

   $AE_e(k)(m) = E(k)(m) \,||\, H(E(k)(m))$

   $AE_d(k)(c,h) = (\textbf{se } H(c) == h \textbf{ então } m = D(k)(c) \textbf{ senão}$ falha de integridade)

   Note que a função de decifra opera sobre criptogramas (c) e o valor de hash (h) que foram colocados no canal de comunicação pela função de cifra.

   Descreva de que forma pode ser comprometida a propriedade de integridade do esquema.

3. (2) Considere os certificados digitais X.509 e as infra-estruturas de chave pública:

   3.1. A assinatura de um certificado folha tem em conta toda a cadeia de certificados?

   3.2. Existem campos num certificado que estejam protegidos por um esquema de cifra (simétrica ou assimétrica)?

4. (1,5) Um dos princípios da JCA é ter uma API independente dos algoritmos que implementam cada um dos esquemas criptográficos. Dê um exemplo de como este princípio é concretizado.

5. (3) Considere a fase de *handshake* do protocolo TLS:

   5.1. Durante a fase inicial de negociação um atacante tenta modificar ou inserir mensagens, com o objectivo de cliente e servidor usarem algoritmos criptográficos mais fracos. Como é que esse ataque seria detectado?

   5.2. O RFC 7525, *Recommendations for Secure Use of Transport Layer Security*, classifica como inseguro a troca do *pre-master secret* usando chaves públicas e privadas. Qual a justificação?

6. (1,5) Considere um sistema onde a informação de validação da *password* do utilizador u é armazenada usando a seguinte função:

   $v_u = SHA1(password_u \,||\, SHA1(password_u)_{1..32})$

   Tendo em conta que $SHA1(password_u)_{1..32}$ representa os primeiros 32 bits do *hash* da *password* do utilizador u e $||$ representa concatenação de bits, descreva sucintamente como é que este sistema pode ser atacado com o objectivo de encontrar a *password* de qualquer utilizador assumindo que o atacante sabe a construção.

7. (1,5) No sistema Moodle os professores podem assumir o papel de "professor", "professor não editor", "aluno" ou "visitante" mas, para cada professor, apenas um destes papéis pode estar ativo em cada interação com o sistema. Assuma que os papéis não estão relacionados entre si. Explique sucintamente como o RBAC pode, em geral, ser usado para especificar esta política.

8. (3) Considere a norma OAuth 2.0 e o fluxo *authorization code grant*:

   8.1. O valor indicado no *scope* é escolhido pelo cliente ou pelo dono de recursos?

   8.2. Em que situações o cliente e o servidor de autorização comunicam indiretamente através do *browser* do dono de recursos?

9. (3) Considere o protocolo OpenID Connect:

   9.1. Qual a diferença entre o *access_ token* e o *id_ token*?

   9.2. Considere a aplicação W com uma vulnerabilidade no processo de autenticação. Um atacante inicia a autenticação em W com um fornecedor de identidade (e.g., Google), interrompendo esse processo quando a resposta passa pelo seu *browser*. Explique como, a partir deste ponto, o atacante conseguiria que uma dada vítima fique autenticada em W como sendo o atacante.

10. (2) Um cliente de *e-mail* poderia ser alvo de um ataque de XSS? Se não explique porquê, se sim indique as características desse cliente e como poderia ser feito o ataque.

28 de Janeiro de 2020