Instituto Superior de Engenharia de Lisboa

LEIC

Segurança Informática

Época de Recurso, Semestre de Verão, 2021/22 – 11 de julho de 2022

Duração: 2 horas

- **Todas as respostas às perguntas de desenvolvimento têm de ser justificadas. Valoriza-se a objetividade e a síntese das respostas.**
- **Nas questões 1, 2 e 3, indique V, F, ou deixe a caixa em branco se não tiver a certeza que a afirmação é (V)erdadeira ou (F)alsa. A indicação certa soma 0,5 valores, a indicação errada desconta 0,25 valores.**

Número: _____ **Nome**: _____

1. (2) No contexto das primitivas de cifra simétrica em bloco (ex: DES, AES) e dos modos de operação:

   ☐ O modo de operação *Electronic Code Book* (ECB) não precisa de vetor inicial (IV), ao contrário do modo de operação *Cipher Block Chaining* (CBC)

   ☐ Na prática, as chaves usadas nestas primitivas são normalmente reutilizadas várias vezes, sendo as mesmas chaves usadas ao longo de vários meses ou anos

   ☐ Um esquena criptográfico que use a primtiva AES pode usar modos de operação diferentes para cifrar e para decifrar (ex: ECB para cifrar e CBC para decifrar)

   ☐ Estas primitivas usam chaves de pequena dimensão (poucos bits) quando comparadas com as primitivas de cifra assimétrica

2. (2) No contexto dos certificados X.509, do protocolo TLS e da biblioteca JCA:

   ☐ Num certificado folha ou intermédio, a assinatura desse certificado é verificada pela chave pública existente no mesmo

   ☐ A classe `X509Certificate` da JCA tem os métodos `getPublicKey()` (para obter a chave pública do certificado) e `getPrivateKey()` (para obter a chave privada que existe dentro do certificado)

   ☐ No *handshake* do TLS, cliente e servidor enviam os números `client_random` e `server_random`, sobre um canal inseguro. Se os números forem modificados no canal, tal será detetado nas mensagens finais do *handshake*

   ☐ As chaves usadas no *record protocol* são chaves privadas semelhantes à que o servidor usa para se autenticar perante o cliente

3. (2) No contexto das normas OAuth 2.0 e OpenID Connect:

   ☐ Na *framework* OAuth 2.0, o valor a colocar no parâmetro *scope* é introduzido pelo dono de recursos

   ☐ No protocolo *OpenID Connect*, a estrutura `id_token` é usada pela aplicação cliente para obter mais informações sobre o utilizador (ex: foto de perfil), através do *userinfo endpoint*

   ☐ Na *framework* OAuth 2.0, o `access_token` tem informação sobre o dono dos recursos cujo objetivo é ser consultada pela aplicação cliente.

   ☐ Nestes protocolos, e tendo em conta o fluxo *authorization code grant*, o endereço designado de *callback* refere-se a um dos *endpoints* da aplicação cliente

4. (2) O método `init` da engine classe `Cipher` tem várias sobrecargas mas todas elas recebem como primeiro parâmetro o modo de utilização, os quais são:

   - `ENCRYPT_MODE`
   - `DECRYPT_MODE`
   - `WRAP_MODE`
   - `UNWRAP_MODE`

   Explique sucintamente o objetivo e forma de utilização dos modos ENCRYPT/DECRYPT e dos modos WRAP/UNWRAP.

5. (2) Nos certificados X.509 a verificação de autenticidade do certificado é feita com um esquema de assinatura digital. Este objetivo poderia ser obtido com um esquema MAC aplicado ao conteúdo do certificado?

6. (2) No contexto dos certificados X.509 e do protocolo TLS, considere que o cliente C estabelece ligações ao servidor S. O certificado do servidor S foi emitido pela autoridade de certificação CA_0, na qual o cliente C confia.

   Como é que um ataque a uma autoridade de certificação diferente da CA_0 pode contribuir para se realizar um ataque *man-in-the-middle* entre o cliente C e o servidor S.

7. (1,5) Comente a seguinte afirmação sobre autenticação baseada em *passwords*:

   > A utilização de um *salt* de 64 bits em vez de 16 bits para armazenar a informação de validação na base de dados aumenta em 4 vezes a dificuldade de realizar um ataque através da interface de autenticação.

8. (1,5) Considere uma aplicação *web* que pretende garantir a autenticidade dos *cookies* que usa para manter estado de sessão entre *browser* e servidor HTTP. É mais adequado usar um esquema de MAC, um esquema de assinatura digital, ou qualquer um deles? Porquê?

9. (2) Comente a seguinte afirmação sobre o modelo RBAC1:

   > O conjunto designado por PA relaciona utilizadores e permissões. Através deste conjunto, uma política pode indicar que determinado utilizador é hierarquicamente superior a outro e por isso herda as suas permissões.

10. (3) No contexto dos protocolos OAuth 2.0 e OpenID Connect:

    10.1. A interação entre a aplicação cliente e o *Resource Server* é em algum caso feita usando o URL de *callback* da aplicação cliente?

    10.2. Na proteção contra ataques de *Cross-Site Request Forgery* (CSRF) de que forma a aplicação cliente deve validar o parâmetro `state` recebido na resposta ao pedido de autorização?