Instituto Superior de Engenharia de Lisboa

LEIRT, LEIC e LEIM

Segurança Informática

Época Normal, Semestre de Inverno, 2021/22 – 28 de janeiro 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 em bloco (ex: DES, AES):

   ☐ A mesma primitiva pode ser usada com diferentes modos de operação

   ☐ Estas primitivas são determinísticas, ou seja, usando a mesma chave k, e o mesmo bloco b, $DES(k)(b)$ dá o mesmo resultado

   ☐ Os modos de operação ECB e CBC só funcionam com chaves de dimensão superior a 64 bits

   ☐ O modo de operação GCM dá garantias de autenticidade da mensagem cifrada, sendo possível detetar modificações antes da decifra

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 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 derivadas da chave privada do servidor

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

   ☐ Em ambos os protocolos, o termo aplicação cliente, ou *relying party*, designa o *browser* através do qual o utilizador acede ao serviço

   ☐ A estrutura designada como `access_token` tem de ser usada nos pedidos ao servidor de recursos

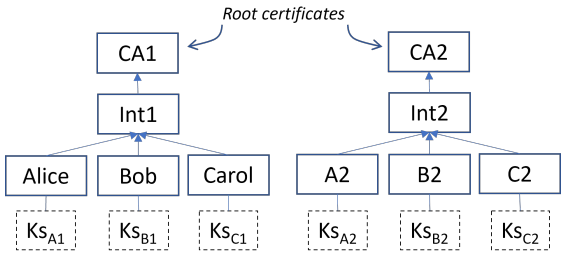
   ☐ Em ambos os protocolos, a aplicação cliente e o servidor de autorização partilham uma chave privada de longa duração para assinar mensagens

   ☐ Neste protocolos, e tendo em conta o fluxo *authorization code grant*, o endereço designado de *callback* refere-se a um dos *endpoints* disponíveis no servidor de autorização.

4. (2) Considere que, em virtude de uma vulnerabilidade detectada na função de *hash* MD5, é computacionalmente fazível, dado x, obter $x' \neq x$ tal que $MD5(x') = MD5(x)$. Quais as implicações deste ataque caso esta função seja usada para gerar a assinatura digital de um certificado X.509?

5. (2) Assume that *Alice* intends to establish a TLS connection to the server $C2$, using both client and server authentication. Indicate, using the identifiers in the figure, the minimum set of certificates and private keys that must be installed, both on the client and on the server.

   Considere o diagrama da figura, onde são apresentadas duas hierarquias de certificados semelhantes às usadas no trabalho. $CA1$ e $CA2$ são raízes de confiança, e $Ks_{A1}...Ks_{C2}$ são chaves privadas associadas aos respetivos certificados.



6. (2) No contexto da JCA (*Java Cryptography Architecture*) e da classe Cipher, explique dois motivos para existirem os métodos `update` e `doFinal`, e não apenas o método `update`.

7. (1,5) Considere uma aplicação que guarda *passwords* (p) usando um salt (s) diferente por utilizador, e uma função de *hash* (H), na forma $v_u = H(p_u||s_u)$, sendo v_u a informação armazenada para o utilizador u e $||$ a operação de concatenação.

   Qual a vantagem desta solução para proteger o armazenamento de *passwords* comparando com uma solução que usa cifra simétrica ou assimétrica para proteger a *password*.

8. (2) Considere uma aplicação *web* que pretende garantir a autenticidade dos *cookies* que usa para manter estado de sessão entre *browser* e servidor HTTP. Quais as vantagens/desvantagens entre usar um esquema de MAC ou um de assinatura digital.

9. (1,5) No modelo RBAC, qual a motivação para haver o conceito de sessão sabendo que a relação UA já relaciona utilizadores e roles?

10. (3) No contexto das normas OAuth 2.0 e OpenID Connect, responda às seguintes questões:

    10.1. Como é obtido o `client_id` e o `client_secret`?

    10.2. Qual o mecanismo que permite à aplicação cliente relacionar um pedido de autorização com a resposta entregue pelo servidor de autorização, e como é usado?