Instituto Superior de Engenharia de Lisboa

LEIC, LEIRT e LEIM

Segurança Informática

Época de Recurso, Semestre de Inverno, 2023/24 – 23 de janeiro de 2024

Duração: 2 horas

- **Respostas às questões 4 a 9 em grupos de folhas diferentes, como indicado no enunciado**
- **Todas as respostas às perguntas de desenvolvimento têm de ser justificadas. Valoriza-se a objetividade 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 verdadeira ou falsa. A indicação errada desconta 50% da cotação atribuída à afirmação.**

Número: _____ **Nome**: _____

1. (2) Considere os 4 esquemas criptográficos abordados:

   ☐ Considerando os usos modernos típicos, as chaves simétricas têm uma quantidade de bits menor do que as chaves assimétricas.

   ☐ Os esquemas de MAC e de assinatura digital produzem marcas cuja dimensão depende da mensagem a autenticar.

   ☐ Na cifra simétrica quando se usa um modo de operação em bloco é preciso um algoritmo de *padding*.

   ☐ Os esquemas de assinatura digital não garantem o não-repúdio de uma mensagem previamente assinada.

2. (2) No contexto dos certificados X.509 e da biblioteca JCA:

   ☐ Dois certificados A e B, se tiverem o mesmo nome de sujeito (ex: CN=www.isel.pt) têm sempre a mesma assinatura.

   ☐ A classe Mac, que implementa o esquema MAC, recebe como parâmetro um certificado de onde obtém a chave pública para gerar a marca.

   ☐ A classe *TrustStore* é utilizada para armazenar certificados de raiz, que podem ser utilizados na autenticação do servidor numa ligação TLS.

   ☐ Tendo o certificado R emitido o certificado F, isso significa que foi usada a chave pública de R para cifrar alguma parte do certificado F.

3. (2) No contexto dos modelos de controlo de acessos e dos protocolos OAuth2 e OpenID Connect no fluxo *Authorization Code Grant*:

   ☐ O protocolo OpendID Connect tem semelhanças com o OAuth2, nomeadamente nos objetivos do parâmetro *scope* e do *access token*.

   ☐ O parâmetro *scope* deve, no mínimo, incluir o valor *oauth2* quando se esteja a usar o protocolo OAuth2.

   ☐ Na aplicação *web* desenvolvida no segundo trabalho, o controlo de acessos é feito antes da interação com o fornecedor de identidade.

   ☐ Uma vantagem do uso de *Access Control List* é que simplifica o processo de listagem das permissões associadas a um objeto.

Grupo 1

4. (2) No RFC 7516, parcialmente implementado no primeiro trabalho, o texto em claro é cifrado com um algoritmo simétrico e modo de operação *Galois Counter Mode* (GCM). Este sistema criptográfico deve ser complementado com um esquema que garanta autenticidade, como é o caso do MAC? Se sim, porquê, se não, de que forma a autenticidade é garantida?

5. (2) Considere o protocolo Transport Layer Security (TLS) e HTTP sobre TLS (HTTPS). Um *browser* liga-se a uma aplicação *web* através de HTTPS. Considerando os dois sub-protocolos do TLS, explique qual deles é responsável pela confidencialidade e autenticidade dos *cookies* nos pedidos e respostas HTTP.

Grupo 2

6. (2) Considere a implementação de um sistema informático que permite aos utilizadores assinar digitalmente contratos em formato PDF. O sistema é composto por um programa chamado *assinante* que recebe como entrada o contrato e gera a assinatura do utilizador — posteriormente, ambos, contrato e assinatura, são colocados num ficheiro PDF. Há outro programa, chamado *verificador*, que realiza a verificação dos contratos assinados pelo primeiro.

   6.1. Identifique uma das primitivas criptográficas utilizadas pelo sistema como parte da implementação da assinatura digital e explique o seu objetivo.

   6.2. Qual ou quais chaves são utilizadas pelo *assinante* e qual ou quais são usadas pelo *verificador*?

   6.3. Discuta a afirmação: "Os objetivos deste sistema poderiam ser igualmente atingidos se o método empregado fosse um MAC, ao invés de uma assinatura digital."

7. (3) Considere novamente o sistema descrito na questão anterior. Um desafio na sua implementação é a distribuição segura de chaves — em particular, como o programa *verificador* obtém a chave correta para verificar as assinaturas geradas pelo programa *assinante*. Assuma que o sistema em questão utiliza uma solução baseada em Infraestrutura de Chave Pública com certificados X.509, na qual uma CA raiz CA_A certifica uma CA intermédia CA_{int} que, finalmente, emite os certificados folha.

   7.1. Para os propósitos do sistema, devem ser emitidos certificados folha para cada um dos utilizadores, para o programa verificador ou para o programa assinante?

   7.2. Seria seguro que o programa *assinante* anexasse também ao PDF gerado o certificado associado à chave utilizada para geração da assinatura?

   7.3. Qual ou quais certificados o programa *verificador* deve possuir no seu repositório de confiança?

Grupo 3

8. (2) Considere a seguinte política definida sobre o modelo $RBAC_1$:

   - $U = \{u_1, u_2, u_3\}$, $R = \{r_0, r_1, r_2, r_3, r_4\}$, $P = \{p_1, p_2, p_3, p_4, p_5\}$
   - $RH = \{r_0 \preceq r_1, r_0 \preceq r_2, r_1 \preceq r_3, r_1 \preceq r_4\}$
   - $UA = \{(u_1, r_1), (u_2, r_3), (u_3, r_4)\}$
   - $PA = \{(r_1, p_1), (r_2, p_2), (r_3, p_3), (r_3, p_5), (r_4, p_4)\}$

   Indique o conjunto de permissões que podem existir numa sessão associada a cada utilizador (u_1, u_2, u_3).

9. (3) Considere os protocolos OAuth2 e OpenID Connect no fluxo *Authorization Code Grant*:

   9.1. Sobre o parâmetro *state*, existente em ambos os protocolos: Qual é o objetivo deste parâmetro? Que preocupações deve ter a aplicação cliente para que seja usado de forma segura?

   9.2. Explique sucintamente as ações realizadas pela aplicação cliente para conseguir aceder ao *UserInfo Endpoint*.