Instituto Superior de Engenharia de Lisboa
LEIC, LEIRT e LEIM
Segurança Informática
Época Normal, Semestre de Inverno, 2023/24 – 5 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) Considerando que se pretende cifrar um ficheiro de 50 bytes com um esquema de cifra simétrica:

   ☐ O criptograma final pode ter mais de 50 bytes se for usado um modo de operação em bloco (ex: *Cipher Block Chaining*).

   ☐ Se for usado vetor inicial (IV), o seu valor terá de ser conhecido antes de iniciar o processo de decifra.

   ☐ A dimensão da chave depende da dimensão do ficheiro.

   ☐ A cifra e a decifra são feitas com chave pública e privada, respetivamente.

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

   ☐ Um certificado auto-assinado é universalmente considerado de confiança.

   ☐ No certificado fornecido no segundo trabalho, para representar o servidor `www.secure-server.edu`, a sua chave pública não é usada para verificar a assinatura desse certificado.

   ☐ A classe Mac da JCA produz uma marca cuja dimensão depende do algoritmo indicado no método fábrica `getIntance`.

   ☐ O *record protocol* garante a integridade das mensagens com um esquema assimétrico de assinatura digital.

3. (2) No contexto dos mecanismos para autenticação e autorização de utilizadores de um sistema computacional:

   ☐ O controlo de acessos é normalmente feito antes de autenticar o utilizador.

   ☐ Os modelos de controlo de acessos têm em conta utilizadores específicos do sistema.

   ☐ Os modelos RBAC consideram apenas permissões positivas na relação *Permission-Assignment*.

   ☐ A biblioteca Casbin, usada no segundo trabalho, é específica para o controlo de acessos em aplicações web.

Grupo 1

4. (3) No RFC 7516, parcialmente implementado no primeiro trabalho, existem duas chaves: a chave de cifra do texto (CE_k) e a chave pública do destinatário da mensagem (K_e). A chave K_e é usada para cifrar a chave CE_k, a qual cifra a mensagem de texto t.

   4.1. Indique uma razão para serem usadas duas chaves para o processo de cifrar o texto t.

   4.2. Qual é, resumidamente, o processo de decifra?

5. (3) Considere o protocolo *Transport Layer Security* (TLS).

   5.1. Considere que um atacante modifica as mensagens iniciais trocadas durante o *handshake protocol* entre um cliente e um servidor, com o objetivo de que ambos usem versões mais antigas dos algoritmos criptográficos. De que forma é este ataque detetado?

   5.2. A propriedade *perfect forward secrecy* tem como objetivo resolver possíveis ataques a qual ou quais partes do sistema: i) cliente, ii) servidor, iii) canal de comunicação?

Grupo 2

6. (2) No Bitcoin, uma ou mais transações financeiras são organizadas em blocos que por sua vez são encadeados numa lista. Entre os campos do *header* de cada bloco, são armazenados o valor do *hash* do *header* do bloco anterior (h_1) e um *hash* do conjunto de transações do bloco atual (h_2).

   Por exemplo, dado os bloco b_i e b_{i-1}, e as transações t_1 e t_2 armazenadas no bloco b_i, o *header* do bloco b_i seria composto pelos hashs $h_1 = H(b_{i-1})$ e $h_2 = H(t_1, t_2)$.

   Explique como um atacante poderia tentar alterar as transações de um determinado bloco **sem alterar nenhum outro bloco da cadeia**. A resposta deve explicitar quais campos do *header* do bloco alterado mudam (se algum). Além disto, considerando que o Bitcoin utiliza uma boa função de *hash* criptográfico, diga se este ataque é computacionalmente fazível justificando a resposta.

7. (2) Considere uma aplicação web onde as *passwords* dos utilizadores são armazenadas na forma

$$p_u = E(k)(pwd_u)$$

   onde E é uma função de cifra simétrica conhecida, k é a chave simétrica usada para todos os utilizadores e pwd_u a palavra-passe de um utilizador u. Tanto os valores de p_u como o valor de k são armazenados na base de dados da aplicação.

   Assumindo que um atacante obteve acesso a uma cópia recente da base de dados, descreva as implicações para a segurança da aplicação e dos seus utilizadores. De que forma poderiam as *passwords* ter sido armazenadas para mitigar o risco associado à situação descrita e em simultâneo mitigar ataques de dicionário e de pré-computação do dicionário? Apresente na sua resposta uma função alternativa para p_u.

Grupo 3

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

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

   Sendo s_0 um identificador de sessão, e $user(s_0) = u_2$, é possível que $r_1 \in roles(s_0)$? E que $r_0 \in roles(s_0)$?

9. (3) Considere os protocolos OAuth2 e OpenID Connect:

   9.1. O parâmetro *scope* existe nos dois protocolos? Qual é o seu objetivo?

   9.2. Considere os endpoints *authorization endpoint* e o *token endpoint*. De que forma a aplicação cliente acede a cada um destes endpoints?