Fundamentos de Segurança Informática 2021/2021 — Exame Final — 03/02/2022

Duração: 1h:30m

Número mecanográfico: | | | | | | | | | |

Nome completo: _____

Grupo 1 - Segurança Web

1.1. Preencha a seguinte tabela que estabelece uma analogia entre conceitos de segurança de sistemas operativos (SO) e conceitos de segurança Web.

Segurança de SO	Segurança Web
Processos	
	Cookies
Sockets/TCP	
Sub-processos	

1.2. Recorde o que estudou sobre Same Origin Policy (SOP).

a) O que significa *origem* para todos os recursos exceto cookies?

b) Indique se cada uma das seguintes afirmações é verdadeira ou falsa.

Afirmação	V/F
Código HTTP da origem A pode pedir recurso a servidor em origem B	
Código JavaScript da origem A pode enviar dados a servidor em origem B	
Código JavaScript da origem A pode enviar mensagem a iFrame com recursos de origem B na mesma aplicação	
Código JavaScript da origem A pode ler informação de cookie de origem B	

1.3. Descreva um ataque baseado em Cross-Site Request Forgery que permite a um atacante obter informação sobre os hábitos de pesquisa no Google de um utilizador alvo.

1.4. Considere o código seguinte, que prepara um query SQL. Identifique a vulnerabilidade que contém.

```
uName = getRequestString("username");
uPass = getRequestString("userpassword");

sql = 'SELECT * FROM Users WHERE Name ="' +
        uName + '" AND Pass ="' + uPass + '"'
```

1.5. Recorde o que estudou sobre ataques de Cross-Site Scripting (XSS). Qual é a diferença entre um ataque *reflected XSS* e um ataque *stored XSS*?

Grupo 2 - Criptografia e PKI

2.1. Recorde a construção de uma cifra simétrica que utiliza o AES em modo Electronic Code Book (ECB). Descreva esta construção e explique porque é insegura.

2.2. Recorde que um Message Authentication Code (MAC) tem a seguinte sintaxe $\mathsf{MAC}(k, m) = t$.

a) Como é utilizado um MAC, na prática, para garantir integridade e autenticidade no envio de uma mensagem m? Identifique, em particular, os papéis de k e t.

b) Como é utilizado um MAC para garantir integridade e autenticidade no envio de n mensagens $m_1, \ldots, m_n$ de A para B? Note que o objetivo aqui é garantir que, do lado B, apenas se aceita uma mensagem m_i transmitida por A, no caso de ser entregue na posição correta da sequência de mensagens.

2.3. Considere um sistema de gestão de chaves para N agentes com base num Key Distribution Center (KDC) e criptografia simétrica.

a) Clarifique a diferença entre chaves de longa duração e chaves de sessão, dando um exemplo de utilização para cada um destes tipos de chaves.

b) Apresente duas propriedades críticas do KDC para um funcionamento correto e seguro do sistema.

1.

2.

2.4. Recorde o que estudou sobre criptografia simétrica e assimétrica. Explique como se utiliza uma cifra construída de acordo com o paradigma híbrido para transferir informação confidencial de A para B?

2.5. Porque é que um Message Authentication Code (MAC) ao contrário de uma assinatura digital, não garante a propriedade de não repúdio?

2.6. Recorde o que estudou sobre Public Key Infrastructure (PKI).

a) Identifique a limitação fundamental da criptografia de chave pública que é resolvida através de uma PKI.

b) Indique duas alternativas a uma PKI para resolver o problema acima.

1.

2.

2.7. Indique, justificando, se a afirmação seguinte é verdadeira ou falsa.

Todos os certificados de chave pública podem ser transferidos por canais inseguros.

Grupo 3 - Autenticação

3.1. Considere o problema da autenticação.

a) Explique a diferença entre *autenticação de origem de mensagens* e *autenticação de entidades*.

b) Descreva um protocolo de autenticação de entidades que utilize, como componente, um mecanismo criptográfico que garanta autenticação de origem de mensagens.

3.2. Considere os seguintes servidores:

- Servidor A: armazena as credenciais dos seus utilizadores como $(username, password)$.
- Servidor B: armazena as credenciais dos seus utilizadores como $(username, H(password))$.
- Servidor C: armazena as credenciais dos seus utilizadores como $(username, salt, H(salt, password))$, em que *salt* é gerado independentemente para cada utilizador.

a) Descreva o processo típico de registo e autenticação neste tipo de serviço. (Recorde que, no caso de data breach, as garantias são usualmente $A < B < C$.)

b) Explique porque é que as garantias segurança, em caso de data breach, são superiores no caso do servidor C.

3.3. Descreva o funcionamento de um protocolo típico de autenticação que utiliza um one-time token como segundo factor de autenticação.

3.4. Explique os conceitos de False Accept Rate e False Reject Rate e que dificuldades coloca a sua parametrização, no contexto de autenticação biométrica.

Grupo 4 - Segurança de Redes

4.1. Caracterize um atacante *eavesdropper*, um atacante *on-path*, um atacante *off-path*, e um atacante *man-in-the-middle*.

4.2. Descreva um ataque de Rogue DHCP e explique porque pode ser útil no contexto de lançamento de ataques Man-in-the-Middle.

4.3. Descreva o modelo de segurança que motiva a definição de três regiões (interna, externa e zona desmilitarizada) na maioria das infra-estruturas de rede.

Grupo 5 - Transport Layer Security

5.1. Identifique a principal diferença entre os protocolos de handshake TLS utilizados no passado e o recomendado na versão TLS 1.3 com a motivação de garantir Perfect Forward Secrecy.

5.2. Explique um ataque de TLS Strip a uma aplicação web protegida com ligações HTTPS.