

Segurança Informática e nas  
Organizações  
1º Semestre, 2021/22  
1º Exame (1ª parte) [33]  
10 de fevereiro de 2022

Número de identificação: [redacted]  
Nome: [redacted]

Esta parte é única por aluno e tem 18 perguntas, sendo  
todas de resposta obrigatória.

Todas as perguntas de escolha múltipla valem 0,25 pontos.  
As perguntas de escolha múltipla têm 5 opções de resposta, sendo  
apenas uma correta. As respostas incorretas descontam-se do total. As respostas  
incorretas descontam-se do total de acordo com  $p = -0,25 \times$   
 $\frac{n}{5}$ , onde  $n$  representa o número de respostas incorretas.  
Os descontos serão aproximadamente 0,25 para  $n = 1$ ,  
0,5 para  $n = 2$ , 0,75 para  $n = 3$ , 1,0 para  $n = 4$ , 1,25 para  $n = 5$ .  
As perguntas de desenvolvimento valem 0,5 pontos cada.  
O teste possui a duração máxima de 150 minutos.

1. Identifique uma das principais fontes de vulnerabilidades  
em sistemas informáticos:
- (a) ☒ Comunicações não controladas
  - (b) Comunicações conhecidas
  - (c) Administradores
  - (d) Fornecedores

2. Identifique uma das dimensões principais a considerar  
numa estratégia de segurança:
- (a) ☒ As pessoas
  - (b) O treino
  - (c) As vulnerabilidades
  - (d) As políticas

3. Em relação à faceta ofensiva da segurança, assinale a correta:
- (a) ☒ Diz respeito ao software, mas não aos processos
  - (b) Consiste em ofender pessoas
  - (c) ☒ É de evitar, pois corresponde a atividades ilegais
  - (d) É usada pelos cibercriminosos

O OWASP Top 10 consiste: 10 vuln. mais importantes  
atuais

Nos 10 mecanismos mais relevantes a implementar  
fontes de vulnerabilidades mais populares em  
sistemas

fontes de vulnerabilidades mais populares em  
sistemas

comunicação com criminosos

12. Um MAC (Message Authentication Code) é calculado  
com uma chave secreta
- (a) ☒ Para que um atacante não consiga  
sugam a partir do seu MAC

- (b) ☒ Classifica a análise estatística para análise de  
aplicações em execução
- (c) ☒ Está limitada a vulnerabilidades conhecidas
- (d) ☒ Considera a análise estatística para análise de código  
fonte

8. Quando se usa uma cifra triple é normal usar o modo EDE  
(Encrypt, Decrypt and Encrypt). Porque?

- (a) ☒ Porque permite que decifra possa anular uma cifra,  
resultando numa única cifra simples
- (b) ☒ Porque caso se usasse 3 cifras seria mais simples de  
selecionar as 3 chaves
- (c) ☒ Porque aumenta a robustez da cifra, sem impacto de  
performance
- (d) ☒ Porque usar uma decifra entre cifras aumenta muito  
a confusão do processo de cifra

7. As técnicas de branqueamento em cifras:
- (a) ☒ Aumentam a difusão de uma cifra
  - (b) ☒ Aplicam chaves ao texto e/ou criptograma com XOR
  - (c) ☒ Anonimizam os dados depois de decifrados
  - (d) ☒ Removem a maioria dos padrões do texto, mesmo  
usando uma chave fixa

- Uma cifra híbrida consiste em:
- (a) ☒ Utilizar cifra com decifra  
contínua
  - (b) ☒ Utilizar uma combinação de cifras por blocos e  
cifra
  - (c) ☒ Cifrar um texto com uma chave simétrica aleatória,  
que é cifrada com a chave pública do destinatário
  - (d) ☒ Utilizar uma qualquer combinação de algoritmos de  
cifra

9. Qual dos seguintes modos de cifra permite paralelizar a  
cifra e a decifra?
- (a) ☒ CFB (Cipher FeedBack)
  - (b) ☒ GCM (Galois/Counter Mode)
  - (c) ☒ CBC (Cipher Block Chaining)
  - (d) ☒ CTR (Counter)

10. Ao utilizar o mecanismo PBKDF2, que informação deve  
ser privada?
- (a) ☒ A dimensão do resultado
  - (b) ☒ A senha
  - (c) ☒ O Pseudo Random Generator
  - (d) ☒ O tamanho dos blocos

11. Tendo em conta apenas a resistência à descoberta de co-  
lissões em funções de síntese, qual destas expressões é ver-  
dadeira?
- (a) ☒ Duas funções que implementem algoritmos distintos  
não vão colidir
  - (b) ☒ Se for reduzida, representa um risco caso a função  
seja usada num MIC (Message Integrity Code)
  - (c) ☒ Pode ser muito elevada com funções de síntese  
pseudo-aleatórias
  - (d) ☒ Se for reduzida, o autor de uma assinatura poderá  
produzir vários documentos para a mesma assi-  
natura

(b) Protege a mensagem transmitida com o MAC? *proteção da sua confidencialidade*

(c) Para evitar que uma mensagem possa validar um MAC?

(d) Para verificar que uma mensagem, e o seu MAC, provém de um interlocutor conhecido

15. Uma assinatura digital de uma mensagem usando RSA:

(a) Não tem qualquer relação em relação a uma autenticação com um MAC (Message Authentication Code)

(b) Permite que terceiros verifiquem a identidade de quem a envia

(c) Garante a identidade de quem a envia

(d) Garante a identidade de quem a cria

16. Para se verificar uma assinatura digital de um documento é preciso:

(a) A chave pública do verificador

(b) A identidade do assinante

(c) A chave pública do assinante

(d) O certificado de chave pública do verificador

17. Tendo em conta o uso de CRL (Certificate Revocation List), qual destas afirmações é verdadeira?

(a) As CRL delta constituem uma validação de integridade das CRL base

(b) As CRL base devem ser obtidas em conjunto com as CRL delta

(c) As CRL delta devem ser consultadas a cada acesso remoto

(d) Quando uma lista base é emitida, importa obrigatoriamente a lista delta imediatamente anterior

18. Em qual dos seguintes casos é possível um utente realizar uma verificação incompleta, mas válida, de uma cadeia de certificação?

(a) Existe uma Entidade Certificadora (CA) intermédia confiável no caminho de certificação

(b) Não é de todo possível

(c) O certificado de todas as Entidade Certificadoras (CA) intermédias ainda não expirou

(d) A data do certificado é válida

17. Uma cifra contínua não deve ser reutilizada com a mesma configuração inicial (IV e chave). Explique porque

18. Considere a gestão de chaves públicas. Explique por que razão não é necessário consultar o serviço de OCSP a cada validação realizada?

Um at-a-carre pode tentar encontrar padrões nos encriptações