Número: Nome:

Sistemas Distribuídos

Faculdade de Ciências e Tecnologia
2018/19
Teste 2 - Versão A
sem consulta - 1h 30 minutos

As respostas erradas às perguntas V/F descontam o equivalente ao valor da resposta certa correspondente. Para as perguntas de escolha de múltipla, o desconto é de 1/5. A penalização acumula apenas no contexto da mesma pergunta. Onde é permitido responder a uma fração das perguntas, caso o número de respostas seja superior ao solicitado, serão contabilizadas primeiro **as respostas erradas**.

Questão 1

Para cada uma das seguintes afirmações, indique se é `[V]`erdadeira ou `[F]`alsa. **Responda a 16 das 20 questões.**

1. TLS é um mecanismo de segurança que pode ser usado para autenticar os clientes de um sistema distribuído.
2. OAuth é um mecanismo de segurança onde estão envolvidos apenas dois principais.
3. O termo *trusted computing base* refere-se ao uso de *hardware* seguro, onde o CPU opera sobre dados cifrados e código assinado.
4. O termo *principal*, no âmbito de um sistema distribuído seguro, refere-se exclusivamente aos utilizadores do sistema.
5. Num sistema distribuído, controlo de acessos sem autenticação não é eficaz.
6. TLS confere proteção contra ataques de adulteração, mas ajuda pouco face a ataques de impedimento de prestação de serviço (*denial of service*).
7. A criptografia assimétrica é adequada para endereçar problemas do âmbito do *repúdio* de mensagens.
8. É impossível cifrar dados volumosos utilizando chaves de criptografia assimétrica.
9. Pode-se produzir uma assinatura digital sem cifrar os dados (assinados).
10. A técnica de cifra de blocos encadeados dificulta ataques de análise de tráfego.
11. Em geral, a dimensão do criptograma obtido por criptografia simétrica não é muito superior à dimensão do texto em claro (*plaintext*).
12. Dado um criptograma obtido à custa de uma qualquer chave RSA, se este for decifrado com a mesma chave, o resultado será o texto em claro (*plaintext*).
13. Dado um criptograma obtido à custa de uma chave pública RSA, se este for decifrado com a mesma chave, o resultado não será o texto em claro (*plaintext*).
14. Dado um criptograma obtido à custa de qualquer chave DES, se este for decifrado com a mesma chave, o resultado não será o texto em claro (*plaintext*).
15. Um gerador de números aleatórios seguros pode ser útil para evitar ataques de indiscrição (*eavesdropping*).
16. No algoritmo de Needham-Schroeder de criptografia simétrica, a chave de sessão K_s é gerada pelo principal que inicia a comunicação.
17. Um ataque de interposição fica facilitado quando não se utilizam chaves certificadas.
18. A *Web of trust* é um método para estabelecer a relação de confiança dos utilizadores na WWW, por recurso a certificados emitidos por entidades de confiança.
19. Um certificado deve ser aceite desde que esteja dentro do prazo de validade e a respetiva assinatura passar o processo de validação.
20. O algoritmo de Diffie-Hellman tem como objetivo dois principais autenticarem-se mutuamente.

Questão 2

Para cada uma das seguintes afirmações, indique se é [V]erdadeira ou [F]alsa. **Responda a 5 das 7 questões.**

21. A dimensão da codificação JSON de uma estampilha de Lamport depende do número de processos para os quais as relações de causalidade estão a ser seguidas.

22. É possível determinar se dois eventos são concorrentes por via das respetivas estampilhas de Lamport.

23. Num sistema distribuído não se justifica usar estampilhas vetoriais se este usar replicação primário/secundário.

24. Na replicação primário/secundário, o uso de estampilhas de Lamport permite acelerar as leituras.

25. Num serviço geo-replicado de armazenamento, com um número elevado de utilizadores, se forem usados vetores versão, é de esperar que a sua dimensão seja igual ao número de utilizadores que realizam escritas.

26. O sistema de ficheiros distribuídos NFS utiliza estampilhas temporais físicas para fazer a validação das *caches* dos clientes.

27. O sistema de ficheiros distribuídos CODA procura registar a história causal das escritas sobre os ficheiros que armazena.

Questão 3

Para cada uma das seguintes afirmações, indique se é [V]erdadeira ou [F]alsa. **Responda a 9 das 12 questões.**

28. Não é possível implementar geo-replicação com base em comunicação em grupo.

29. Num sistema geo-replicado, o melhor desempenho obtém-se quando quando se utiliza o mesmo número de réplicas em cada região.

30. É possível implementar um sistema geo-replicado por recurso a replicação primário/secundário.

31. Na replicação primário/secundário, tolerar partições de rede tem impacto no número de ACKs que o primário deve recolher antes de responder ao cliente.

32. Se o modelo de falhas admitir que os processos recuperam rapidamente e for usada memória secundária persistente, mesmo assim, o primário não pode confirmar uma operação ao cliente sem contactar qualquer secundário.

33. Na replicação primário/secundário qualquer secundário pode tomar o lugar do primário em caso de falha deste.

34. Na replicação *multi-master* poderá haver atualizações aos dados replicados que não serão consideradas (aplicadas).

35. A replicação *multi-master* está mais habilitada para implementar modelos de consistência forte.

36. Na replicação *multi-master*, com consistência eventual, uma réplica antes de responder está obrigada a propagar todas as suas alterações aos dados a pelo menos outra réplica.

37. —— *Caching* é uma forma de replicação.

38. Tendo em conta a consistência dos dados, o desempenho do *caching* é limitado pelo rácio entre o número de operações de leitura e o número de operações de escrita.

39. A comunicação em grupo tem aplicabilidade no âmbito dos sistemas de *caching*.

Questão 4

Para cada uma das seguintes afirmações, indique se é [V]erdadeira ou [F]alsa. **Responda a 6 das 9 questões.**

40. Um endereço é um nome.

41. Um endereço não pode ser um nome puro.

42. Um nome simbólico não pode ser em simultâneo um endereço e um identificador único.

43. Um URN é um nome e pode ser um identificador.

44. Os URLs e o URNs são classes de URIs.

45. O caminho absoluto num sistema de ficheiros local (eg., drive Windows) é um nome contextual.

46. Um serviço de nomes é interrogado fornecendo na pergunta um ou vários atributos do(s) objeto(s) procurado(s).

47. Uma resolução iterativa no âmbito de um sistema de nomes distribuído é a opção que sempre oferece a melhor latência das operações.

48. O Zookeeper é exemplo de um serviço de nomes replicado que suporta consistência forte.

Número: Nome:

Questão 5

Considere o contexto do segundo trabalho prático. Como sabe, no decurso da utilização da aplicação Microgram são carregados e descarregados ficheiros contendo imagens. Presentemente, qualquer cliente HTTP/HTTPS, desde que disponha do URI de uma imagem, poderá obter a mesma. Pretende-se evitar isso e só permitir que clientes autorizados possam descarregar as imagens armazenadas no serviço `MediaStorage`. Para tal, o cliente precisa de autenticar-se perante o serviço `MediaStorage`, juntando ao pedido uma *prova de autorização*, obtida do serviço `Profiles`.

Considere o protocolo de segurança, abaixo, cujos pressupostos são: (1) **as comunicações realizam-se sobre SSL/TLS**; (2) uma vez autenticado, o cliente poderá usar a mesma ligação TLS para efetuar novos pedidos ao serviço `MediaStorage`; (3) o serviço `Profiles` conhece a chave secreta, K_{Client}, de cada cliente; (4) os serviços Profiles e MediaStorage partilham uma chave K_{PM}.

tls! tls! tls! tls!

1. Client → Profiles: ☐
2. Profiles → Client: ☐, $\{N\}K_{Client}$
3. Client → MediaStorage: $\{$☐$\}_{K_{PM}}$, ☐
4. MediaStorage → Client: ☐
5. Client → MediaStorage: File2, ☐
6. MediaStorage → Client: ...

Indique a melhor resposta, tendo em conta o objetivo do protocolo e os pressupostos enunciados.
Responda a todas as questões.

49. No passo 1, a caixa deve ser preenchida com:

A) $Client$ B) N C) $\{Client\}_{K_{Client}}$ D) $\{N\}_{K_{Client}}$ E) $\{N\}_{K_{PM}}$ F) Nenhuma das anteriores

50. No passo 2, a caixa deve ser preenchida com:

A) $\{N\}_{K_{PM}}$ B) $\{N, K_{PM}\}_{K_{Client}}$ C) $\{N, Client\}_{K_{PM}}$ D) $\{N, K_s, K_{PM}\}_{K_{Client}}$ E) $\{N, Client, K_{PM}\}_{K_s}$ F) Nenhuma das anteriores

51. No passo 3, a primeira caixa deve ser preenchida com:

A) $File$ B) K_s C) N D) $N, Client$ E) $Hash(N + File)$ F) Nenhuma das anteriores

52. No passo 3, a segunda caixa deve ser preenchida com:

A) $\{N\}_{K_s}, File$ B) $File$ C) $\{N, File\}_{K_s}$ D) $File, N$ E) $File, Hash(File + N)$ F) Nenhuma das anteriores

53. No passo 4, a caixa deve ser preenchida com:

A) $FileContents$ B) $\{FileContents\}_{K_{Client}}$ C) $\{N, FileContents\}_{K_{Client}}$ D) $\{N, FileContents\}_{K_s}$ E) $\{FileContents\}_{K_s}$ F) Nenhuma das anteriores

54. No passo 5, a caixa deve ser preenchida com:

A) N B) $Nada$ C) $\{N\}_{K_{PM}}$ D) $\{N, Client\}_{K_{PM}}$ E) $\{File\}_{K_s}$ F) Nenhuma das anteriores

Para cada uma das seguintes afirmações, indique se é `[V]`erdadeira ou `[F]`alsa.
Responda a 6 das 8 questões.

55. A chave secreta K_{Client} é uma chave de criptografia simétrica.

56. A chave K_{PM} é uma chave privada e o cliente irá precisar da chave pública correspondente.

57. Uma função de N é proteger a plataforma de ataques de *Masquerading*.

58. O protocolo permite que o serviço `Profiles` possa esquecer os valores N, desde que não os repita.

59. O protocolo não permite que o serviço `MediaStorage` possa esquecer os valores N.

60. O protocolo seria mais eficiente, gastando menos memória, se forem gerados valores N sucessivos: 1, 2, 3, ...

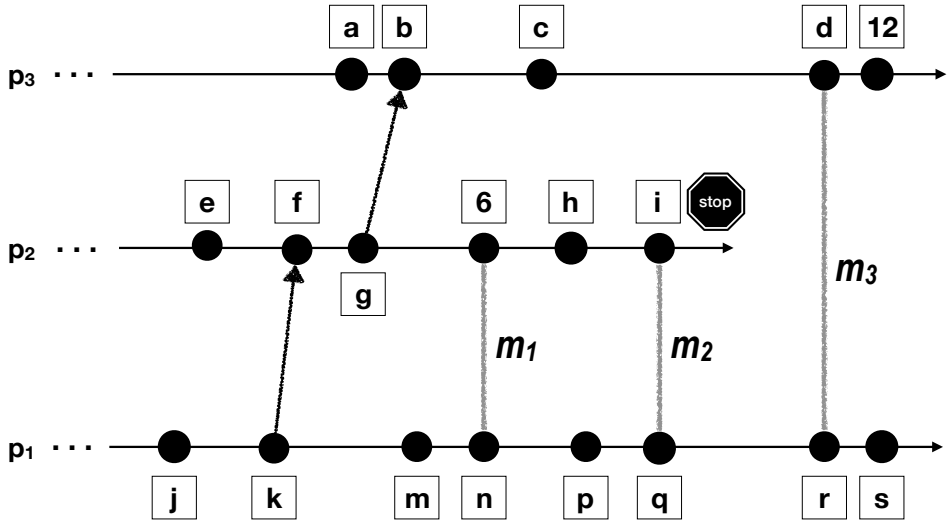
61. O cliente é autenticado mas não se impede que um atacante obtenha o conteúdo do ficheiro.

62. O cliente é autenticado e, também, se impede que um atacante altere o conteúdo do ficheiro, sem que cliente o detete.

Número: Nome:

Questão 6

Considere o seguinte diagrama temporal, onde está representado um padrão de comunicação ponto-a-ponto, envolvendo os processos p_1, p_2 e p_3. Para as mensagens, m_1, m_2 e m_3, desconhece-se o sentido da comunicação. Os eventos nos processos estão assinalados por círculos negros. Cada evento tem associado uma caixa, cujo valor é uma estampilha de um relógio de Lamport, de valores inteiros, atualizado pelo menor incremento possível.



Responda a cada pergunta de forma **independente**, escolhendo a resposta que pode ser explicada com base nos valores presentes no diagrama e as condições enunciadas na pergunta. **Responda a todas as questões.**

63. O maior valor admissível para `s` é:

A) 11 B) 10 C) 9 D) 12 →E) 13 F) Nenhum dos anteriores

64. O maior valor admissível para `a` é:

A) 4 B) 6 → C) 8 D) 7 E) 5 F) Nenhum dos anteriores

65. O maior valor admissível para `j` é:

→A) 2 B) 1 C) 5 D) 4 E) 3 F) Nenhum dos anteriores

66. O maior valor admissível para `i` é:

A) 8 B) 9 → C) 10 D) 11 E) 12 F) Nenhum dos anteriores

67. Se a mensagem m_2 for recebida em p_1, o valor de `i` será:

→A) 8 B) 9 C) 10 D) 11 E) 12 F) Nenhum dos anteriores

68. O menor valor possível para `p` é:

A) 4 B) 5 →C) 6 D) 7 E) 8 F) Nenhum das anteriores

Considerando, de novo, o diagrama, para cada uma das seguintes afirmações, indique se é `[V]`erdadeira ou `[F]`alsa. **Responda a 7 das 9 questões.** Considere as letras como identificando os eventos correspondentes.

69. As mensagens m_1 e m_2 não podem ambas ter sido recebidas em p_2.

70. O evento j *aconteceu antes* do evento e.

71. Os eventos a e k são concorrentes.

72. O evento d pode ser concorrente do evento m.

73. O valor do relógio de Lamport associado a i é necessariamente maior do que o valor de k.

74. Os eventos h e p são concorrentes, independentemente do sentido da comunicação das mensagens m_1 e m_2.

75. A relação *aconteceu antes* entre os eventos n e i depende do sentido da mensagem m_2.

76. O valor da estampilha de e é necessariamente inferior ao valor da estampilha de a.

77. O valor da estampilha de a pode ser superior ao valor da estampilha de m.