Número: Nome:

Sistemas Distribuídos

Faculdade de Ciências e Tecnologia
2017/18
Teste 2
sem consulta - 90 minutos

Questão 1

Leia com atenção as seguintes afirmações e assinale na folha de respostas se são verdadeiras ou falsas. Respostas incorretas descontam. Em caso de dúvida, justifique.

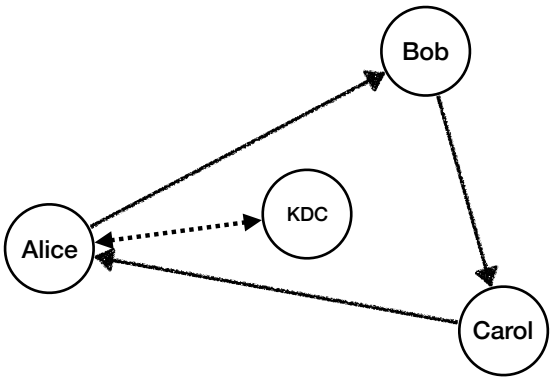
1. Para um sistema ser confiável (*dependable*) precisa de ser seguro e disponível, em simultâneo;
2. Num sistema distribuído, a *trusted computing base* deve ser tão abrangente quanto o possível;
3. O controlo de acessos pressupõe sempre alguma forma de autenticação;
4. Um canal seguro é um canal que fornece autenticidade e confidencialidade das comunicações e nada mais;
5. Um sistema distribuído não pode ser inseguro quando a especificação da sua *trusted computing base* é adequada/correcta.
6. Para comprimir o tráfego de um canal seguro, deve-se realizar a operação de cifra antes da compressão;
7. A criptografia opera sempre através da transformação dos dados de forma irreversível, de modo a ser impossível saber o conteúdo das mensagens;
8. A criptografia assimétrica é adequada para cifrar o conteúdo de ficheiros de dados grandes;
9. A criptografia simétrica só deve ser usada para cifrar o conteúdo de ficheiros de dados pequenos;
10. Cifrar com uma chave assimétrica pública o resultado de uma função de síntese, produz uma assinatura digital;
11. Um certificado de chave pública não deve passar em claro (desprotegido) num sistema de comunicações;
12. Através de uma função de síntese e um segredo apenas (string/chave simétrica) é possível produzir um objeto que fornece provas de autenticidade e de integridade;
13. Uma lista de revogação de certificados deve sempre ser assinada pela entidade que a emitiu.
14. O algoritmo de Diffie-Hellman permite estabelecer um canal privado entre dois principais sem a necessidade de partilhar segredos previamente;
15. O sistema OAuth oferece uma forma segura de passar as credenciais de um utilizador a outro site, usando um serviço confiável como intermediário (como por exemplo, o Google ou Facebook).
16. Em nenhum caso, o tempo físico serve para ordenar eventos de um sistema distribuído;
17. Através da consulta da estampilhas de um relógio de Lamport de um par de eventos, é possível determinar qual aconteceu antes do outro;
18. Combinando um relógio vectorial com o identificador do processo/máquina é possível definir uma ordem total para um conjunto de eventos;
19. Um relógio vectorial é uma forma de resumir os eventos importantes (escritas) que ocorreram num sistema distribuído;
20. É possível determinar se dois eventos são concorrentes comparando as respetivas estampilhas se estas forem obtidas através de um relógio vectorial;
21. Supondo que um processo contabiliza os seus eventos num relógio vectorial e num vector versão, cada entrada do relógio vectorial será sempre igual ou inferior à sua correspondente no vector versão;
22. Um relógio de Lamport oferece uma forma de resumir a *história causal* de um processo;
23. Os incrementos de um relógio de Lamport podem não ser inteiros;
24. Os incrementos de um relógio vectorial devem ser positivos e necessitam de ser sempre iguais (constantes);
25. Num sistema distribuído, quando são enviadas mensagens, pode não ser importante que todas sejam incluídas na sua história causal.
26. É possível implementar replicação de objetos por recurso a um mecanismo de comunicação em grupo, se a entrega das mensagens for fiável e respeitar a ordem total, mas não a ordem causal;
27. Em geral, a replicação é uma forma eficaz de equilibrar a carga de um sistema distribuído onde as escritas dominam;
28. Um sistema distribuído pode tolerar falhas mesmo que este não implemente replicação;

29. A replicação primário/secundário obriga que as escritas passem pelo primário, as leituras podem ser realizadas nos secundários;
30. Antes de responder ao cliente o resultado de uma escrita, o primário deve esperar até receber de todos os secundários uma confirmação;
31. Caso o primário falhe, qualquer secundário poderá tomar o seu lugar.
32. O desempenho de uma solução de replicação tende a aumentar se as garantias de consistência forem relaxadas;
33. A eficácia de uma cache não depende do rácio das operações de leitura e escrita num sistema distribuído;
34. A replicação baseada na consistência eventual tem que garantir que mais tarde ou mais cedo, ocorrerá a convergência dos dados, desde que as atualizações dos mesmos cessem;
35. O sistema de ficheiros NFS faz a gestão da sua cache com base em estampilhas lógicas;
36. No sistema de ficheiros CIFS, quando existem dois clientes com intenção de ler o ficheiro ao mesmo tempo, este não pode ser colocado em cache;
37. No sistema de ficheiros Coda, usam-se vetores de versão para detectar conflitos entre ficheiros alterados em modo *offline*;
38. Um serviço de nomes tem como objetivo registar apenas os nomes das entidades que compõem um sistema distribuído;
39. Um serviço de diretório pode substituir um serviço de nomes, o contrário não é verdade;
40. Um endereço de uma componente pode ser considerado um nome;
41. Na prática, aplicar uma função de síntese segura a um URL pode tornar o mesmo num identificador único;
42. Na prática, aplicar uma função de síntese segura ao conteúdo de um objeto apontado por um URL pode ser usado para construir um URN;
43. Um nome puro é um nome que não contém informação de localização, logo um URL é um nome puro.
44. Um nome puro é um nome que não contém informação de localização, logo aplicar uma função de síntese a um URL produz um nome puro.
45. O Zookeeper é um sistema de nomes que oferece consistência forte porque ordena totalmente as operações.

Número: Nome:

Questão 2

Considere o seguinte diagrama que descreve as interações dos principais de um sistema distribuído, a Alice, o Bob, a Carol e um KDC. Neste cenário, a Alice pretende enviar uma mensagem secreta ao Bob e à Carol, mas como ainda não sabe o contacto da Carol, precisa que seja o Bob a encaminhar essa mensagem à Carol. No final, a Alice espera receber da Carol uma mensagem que confirme que tanto o Bob como a Carol, receberam e leram a mesma mensagem. A Alice e o Bob conhecem a chave pública da Carol (K_{pubC}). O centro de distribuição de chaves, KDC, é de confiança.



O protocolo de segurança usado é o seguinte, onde se utiliza a notação usual para os símbolos:

1. Alice → KDC: $Alice, Bob, N_a$;
2. KDC → Alice: $\{N_a, Bob, K_s, \{K_s, Alice\}_{K_b}\}_{K_a}$
3. Alice → Bob: $\{K_s, Alice\}_{K_b}, \{N_b, M\}_{K_s}, Carol, \{Alice, K_s\}_{KpubC}$
4. Bob → Carol: $\{M, H(M + Nb)\}_{K_s}, \{Alice, K_s\}_{KpubC}$
5. Carol → Alice: $\{H(M + Nb), H(M)\}_{K_{privC}}$

Responda às seguintes questões de forma independente entre si, assinalando na folha de respostas se são verdadeiras ou falsas. Respostas incorretas descontam. Em caso de dúvida, justifique.

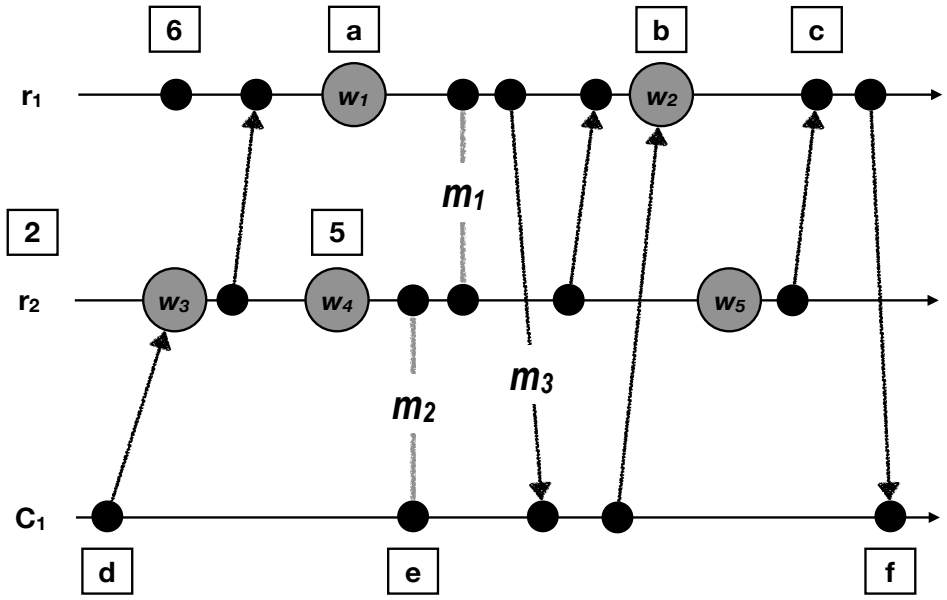
46. N_a é um segredo e tem como objetivo evitar ataques de indiscrição;
47. O Bob registou K_b no KDC previamente;
48. A chave K_s terá sido guardada previamente pela Alice no KDC;
49. No protocolo $\{...\}_{KpubC}$ serve para garantir a confidencialidade do conteúdo ...;
50. $\{H(M + Nb), H(M)\}_{K_{privC}}$ tem sempre uma dimensão comparável à da mensagem M;
51. $H(M + Nb)$ prova que o Bob leu a mensagem.
52. No passo 5, a Carol cometeu um erro, deveria ter enviado $\{H(M + Nb), H(M)\}_{K_{pubC}}$;
53. Com este protocolo, o Bob pode alterar a mensagem que envia à Carol, sem que a Alice se aperceba disso.
54. Com este protocolo, o Bob pode alterar a mensagem enviada pela Alice, sem que a Carol se aperceba disso.
55. Um pre-requisito dete protocolo é que os todos os principais se tenham registado no KDC.

Número: Nome:

Questão 3

Considere o seguinte diagrama temporal correspondente a um sistema de armazenamento de dados distribuído, composto por duas réplicas: r_1 e r_2, com as quais estão a interagir alguns clientes, entre eles C_1. As setas indicam eventos de comunicação ponto-a-ponto, uni-direcionais entre as componentes do sistema. As operações de escrita correspondem aos eventos: w_1, w_2, ...,w_5. m_1 e m_2 são mensagens para as quais a direcção de envio e recepção foi suprimida. Os valores contidos, nas caixas junto aos eventos, correspondem a estampilhas de um relógio de Lamport, sendo as letras também usadas para identificar os respetivos eventos.

Responda às seguintes questões de forma independente entre si, supondo que o incremento mínimo é de 1 unidade. Assinale na folha de respostas se as afirmações são verdadeiras ou falsas.



56. As escritas $\mathbf{w_1}$ e $\mathbf{w_4}$ são concorrentes, independentemente da direcção da comunicação de $\mathbf{m_1}$ ou $\mathbf{m_2}$;
57. As escritas $\mathbf{w_1}$ e $\mathbf{w_5}$ podem ser concorrentes, independentemente da direcção da comunicação de $\mathbf{m_1}$ ou $\mathbf{m_2}$;
58. As escritas $\mathbf{w_2}$ e $\mathbf{w_5}$ não são garantidamente concorrentes;
59. $\mathbf{w_2}$ aconteceu antes de $\mathbf{w_5}$;
60. $\mathbf{w_3}$ aconteceu antes de $\mathbf{w_5}$;
61. A relação *aconteceu antes* entre **e** e $\mathbf{w_2}$, depende da direcção da comunicação de $\mathbf{m_2}$;
62. O maior valor possível da estampilha **d** é 2;
63. O valor da estampilha **e** pode ser 3;
64. O valor da estampilha **c** é necessariamente inferior ao valor de **f**;
65. O valor da estampilha **f** não depende da direcção da comunicação de $\mathbf{m_1}$ ou $\mathbf{m_2}$;
66. Se a mensagem $\mathbf{m_3}$ se perder e não for entregue, o valor de **b** será 12;
67. Se **f** for a recepção do vector versão da réplica $\mathbf{r_1}$, o seu valor será [2, 3];
68. Supondo que $\mathbf{m_2}$ é entregue em $\mathbf{C_1}$, como o valor de **e** será menor que **a**, então **e** aconteceu antes de **a**;
69. Para o valor de **e** ser superior a 4, o evento correspondente terá de ser a recepção de $\mathbf{m_2}$.