FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE NOVA DE LISBOA

Departamento de Informática

Mestrado Integrado em Engenharia Informática
Sistemas Distribuídos – 2º teste, 14 de Junho de 2017
2º Semestre, 2016/2017

NOTAS: Leia as questões atentamente antes de responder. **O teste é sem consulta. A duração do teste é 2h00min**. O teste contém **8** páginas.

Nome: _____ **Número**: _____

1. Indique se cada afirmação é **[V]erdadeira** ou **[F]alsa** (**nota: respostas incorretas descontam 2/3 da cotação de uma resposta certa**):

___ Num sistema distribuído podem-se utilizar relógios físicos para ordenar eventos, mas tal exige um custo de comunicação elevado para sincronizar os relógios.

___ A relação "aconteceu antes" não pode ser definida para eventos que ocorrem em máquinas distintas.

___ Dados quaisquer dois valores **a** e **b**, de um relógio lógico , se **a** < **b** então pode-se concluir **a** precede **b**.

___ Dados quaisquer três valores **a**, **b** e **c** de um relógio lógico, onde **b** e **c** referem-se, respetivamente, aos eventos de envio e recepção de uma mensagem ***m***, então se **a < b** pode-se concluir **c** ocorreu depois de **a**.

___ O sistema NFS (Network File System) utiliza nos clientes uma cache que guarda os blocos dos ficheiros guardados remotamente. As escritas não tiram partido da cache pois os blocos escritos por um cliente são imediatamente enviados ao servidor, afim de minimizar escritas concorrentes.

___ O sistema NFS (Network File System) utiliza nos clientes uma cache que guarda os blocos dos ficheiros guardados remotamente. Neste sistema, as escritas concorrentes são endereçadas por via do mecanismo de "callback promise".

___ O mecanismo "callback promise" usado no sistema AFS não exige que os servidores guardem qualquer estado relativo aos ficheiros.

___ Um ataque por *replaying* consiste em um atacante guardar as mensagens trocadas por um cliente e um servidor e voltar a executar a comunicação repetindo as mensagens enviadas por um dos parceiros.

___ Usando criptografia assimétrica, cifrar uma mensagem com uma chave pública garante a confidencialidade dos dados.

___ O OAuth é um mecanismo para um utilizador comunicar de forma segura a um cliente as suas credenciais que permitem o acesso a recursos armazenados num dado servidor.

___ No protocolo TLS, o canal primeiro comprime e depois cifra a informação. A ordem destas operações é irrelevante.

___ Um MAC (Message Authentication Code) é uma forma de assinatura digital compacta que permite autenticar documentos/mensagens destinadas a um número reduzido de destinatários.

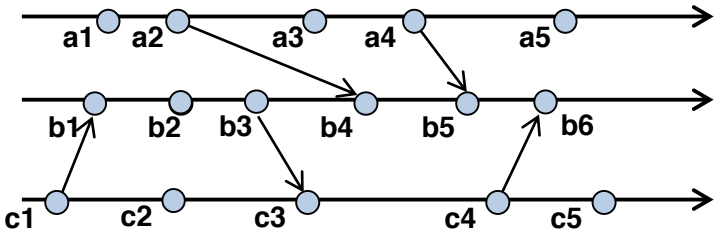
___ O sistema DNS pode retornar informação desatualizada a um cliente.

___ No sistema DNS, caso não exista informação em cache, a resolução de nomes começa sempre pelos servidores dos domínios de topo.

___ No sistema DNS, a resolução de nomes é tipicamente efetuada de forma recursiva e iterativa, em que o servidor de DNS local resolve um nome para o cliente contactando iterativamente os servidores necessários.

___ Um sistema de "message queueing" pode ser usado para implementar um sistema de comunicação *anycast*, em que um processo envia uma mensagem para um qualquer de um grupo de outros processos.

2. Considere um sistema distribuído com três processos, em que ocorrem os eventos assinalados a1, a2, ... As setas indicam o envio de uma mensagem.



a) Neste contexto, indique todos os eventos que aconteceram antes de:

b5:

c5:

b) Suponha que pretende identificar os eventos com **relógios vetoriais**. Indique o valor para cada um dos seguintes eventos, sabendo que cada processo incrementa a sua entrada pelo menor valor possível e inicialmente a sua entrada tem o valor 0.

a2: _____ b3: _____ c3: _____ a5:_____b6: _____

c) Considere que a imagem representa as comunicações relativas a um sistema de armazenamento de dados. As operações sem setas (a1, a3, a5, b2, c2, c5) representam escritas, i.e., são os eventos importantes. As setas representam a propagação do estado da réplica origem da seta para a réplica. O estado inicial das réplicas é representado pelo vetor versão [0 0 0].
Indique em que eventos se detetaram que existiram escrita concorrentes, e para cada situação indique o vetor versão de cada uma das réplicas (sabendo que as entradas são incrementadas pelo menor valor possível).

Situação 1:

Situação 2:

Situação 3:

Situação 4:

Situação 5:

Nome: _____ **Número**: _____

3. **Complete** as seguintes afirmações, ou **risque o que não interessar**:

   a) No protocolo de Needam-Schroeder com chaves simétricas é utilizado um centro de distribuição de _____.

   b) Nos protocolos de segurança utiliza-se o conceito de "nonce" para evitar ataques de _____.

   c) Para evitar ataques por interposição ("man in the middle") é necessário que a chave pública do servidor utilizada pelo cliente seja _____ .

   d) Num sistema seguro a *trusted computing* base deve ser _____.

   e) Evitar o repúdio de mensagens pode ser conseguido por recurso a _____ .

   f) Uma função síntese segura serve principalmente para garantir a _____ das mensagens.

   g) A Alice enviou uma mensagem secreta ao Bob. A mensagem foi cifrada com a chave pública / privada da Alice / do Bob.

   h) A Alice enviou uma mensagem ***m*** secreta ao Bob, usando o protocolo de Needam-Schroeder. A mensagem chave de sessão que cifrou a mensagem foi gerada pela Alice / pelo Bob / pelo KDC.

4. A Alice e a Sara fizeram um pacto para aumentar as compras nas suas lojas. Para tal, sempre que um cliente faz compras na loja da Alice recebe um cupão que lhe permite ter um desconto na loja da Sara e vice-versa, desde que efetuado nos 7 dias posteriores à compra. O desconto é proporcional ao somatório das compras efetuadas em cadeia. Quando fizeram esse acordo, a Alice e a Sara combinaram uma chave secreta Ks.

   Os cupões são emitidos pelas lojas e gravados num cartão que os clientes possuem. O cartão apenas tem capacidade para um cupão de cada vez e não tem nenhum mecanismo de segurança que impeça um atacante de alterar o seu conteúdo. Quando um cliente vai fazer uma compra, dá o cartão que possui o cupão gravado anteriormente.

   A Alice e a Sara pretendem garantir que não dão descontos superiores aos que devem. Para tal, é necessário proteger a informação do cupão. Apresente de seguida como guardaria a informação do cupão, considerando que o primeiro cupão é gerado na loja da Alice, sendo: A – Alice; S – Sara; V – soma das compras efetuadas.

   1) Geração do primeiro cupão: A, V1, [ ], **H**([ ])

   2) Geração do segundo cupão: S, V2, [ ], **H**([ ])

   …

a) Complete o protocolo indicado acima, sendo que em cada caixa não deve haver informação cifrada. Caso não saiba resolver o protocolo anterior, apresente uma solução alternativa.

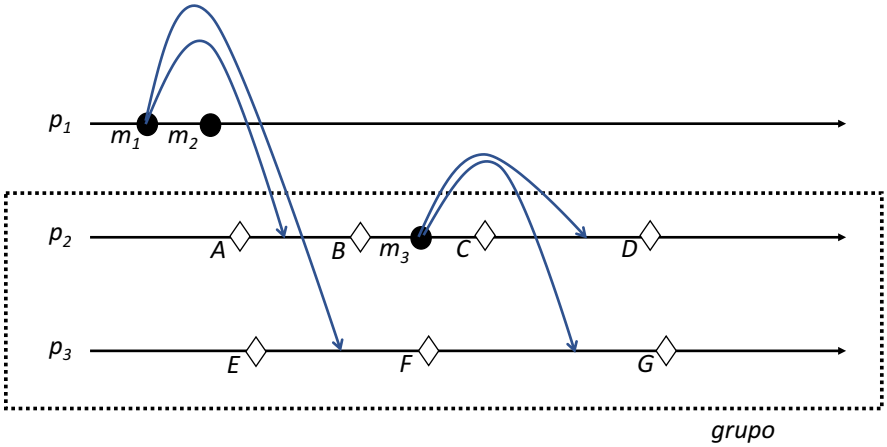
Geração do primeiro cupão:

Geração do segundo cupão:

b) Explique o que é que impede um atacante de levar uma loja a aplicar um desconto superior ao que tem direito, fingindo que a soma das compras é superior ao realizado até ao momento?

Nome: _____ **Número**: _____

5. Considere o seguinte diagrama que ilustra um padrão de comunicação em grupo, envolvendo três processos dos quais ***p₂*** *e* ***p₃*** pertencem ao grupo destinatário de todas as mensagens e **p1** que apenas participa como emissor. As setas indicam o momento em que ocorre a entrega da mensagem no processo, estando fixas para as mensagens **m1** e **m3**. Para a mensagem **m2** o momento de entrega pode ser um dos momentos indicados por A, B, C, D no processo ***p₂*** e E, F, G no processo ***p₃***.



a) Indique **todos os pares** possíveis para a entrega da mensagem **m2** que permitem que garantir que todas as mensagens são entregues por ordem total. [nota: as respostas devem ser do tipo (x,y) com x = A ou B ou C ou D e y = E ou F ou G]

b) Indique **todos os pares** possíveis para a entrega da mensagem **m2** que permitem que garantir que todas as mensagens são entregues por ordem total e causal.

6. Considere que pretende implementar um sistema de comunicação fiável com ordem causal. Caso os processos não falhem, será suficiente que cada processo estabeleça um canal fiável com cada um dos outros processos, no qual propaga as mensagens enviadas por ordem FIFO, sendo as mensagens entregues assim que são recebidas? (E.g., caso existam 3 processos, p1, p2 e p3, uma mensagem enviada por p1 é entregue localmente e enviada para os processos p2 e p3 por um canal que não perde mensagens e as entrega por ordem de envio) Justifique.

Sim, porque… / Não, porque…

7. Suponha que pretende implementar um sistema para armazenar informação sobre os servidores que executam num cluster. Este serviço fornece quatro operações: (1) ***write (app/name, props)***, para guardar um conjunto de propriedades sobre o servidor app/name, em que app é o nome da aplicação e name é o nome do servidor nessa aplicação; (2) **delete (app/name)**, para remover informação sobre o servidor app/name; (3) **get (app/name)**, para obter informação sobre o servidor app/name; e (4) **list (app)**, para listar os servidores registados cujo prefixo do nome é app.

   a) Este serviço é um serviço de nomes ou um serviço de diretório? **Justifique**.

Serviço de nomes, porque… / Serviço de diretório, porque…

Nome: _____ **Número**: _____

b) Suponha que, para ter tolerância a falhas, pretende fornecer o serviço com recurso a um conjunto de servidores que replicam a informação mantida recorrendo a um algoritmo primário/secundário.

i) Neste algoritmo, quando processa uma operação de escrita, o primário pode esperar pela confirmação (ack) de todos os secundários antes de enviar a confirmação para o cliente? Justifique.

Sim, porque… / Não, porque…

ii) Considere que tem um sistema com 5 servidores, um primário e quatro secundários, com a seguinte configuração: na escrita o primário envia a resposta ao cliente após receber a confirmação de três secundários; na leitura, um servidor (secundário) verifica que a versão dum outro servidor é igual à sua (ou mais antiga) antes de responder ao cliente. Neste caso, é possível que o cliente após fazer uma escrita, faça uma leitura que reflete um estado anterior ao estado da sua escrita? (i.e., o cliente escreve a versão *n* e a seguir lê a versão *n-1*)

Sim, porque… / Não, porque…

c) Suponha que os clientes querem fazer cache da informação relativa a um servidor, com garantias que recebem sempre a informação mais atual. Qual lhe parece a solução mais apropriada para fornecer esta propriedade – NFS, CIFS/op locks, callback promise? Justifique.

NFS /CIFS – op locks / Callback promise , porque…

d) Suponha que pretende permitir aos servidores serem notificados sempre que existem alterações na lista de servidores de uma dada aplicação. Poderia usar um sistema de publish/subscribe para fornecer esta funcionalidade? Se sim, apresente um esboço da solução indicando o tipo de sistema usado e como eram feitas as notificações. Se não, explique o motivo e apresente uma solução alternativa.

Sim,… / Não,…