FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE NOVA DE LISBOA

Departamento de Informática

Licenciatura / Mestrado em Engenharia Informática
Sistemas Distribuídos – 2º teste, 14 de Dezembro de 2012
1º Semestre, 2012/2013

NOTAS: Leia com atenção cada questão antes de responder. **O teste é sem consulta e tem a duração de 1h30min**. O teste contém **4** páginas.

NOME: _____ **NÚMERO**: _____

1) Para cada pergunta, assinale como **V[erdadeira]** ou **F[alsa]** cada uma das afirmações. **As respostas erradas descontam**.

___ O IP Multicast implementa uma solução de comunicação em grupo (multicast) não fiável.

___ Um sistema de comunicação em grupo pode respeitar a ordem total sem respeitar a ordem FIFO.

___ Num sistema de comunicação em grupo fiável que tolere K > 1 falhas de máquinas, o middleware pode ter a necessidade de atrasar, em alguns nós, a entrega duma mensagem recebida.

___ O UDDI é um serviço de diretório.

___ Um pedido SOAP é tipicamente mais "pesado" que um pedido REST, devido à maior dimensão das mensagens trocadas.

___ Fazer *caching* duma resposta a um pedido SOAP é simples porque basta indexar o conteúdo da resposta HTTP com base no URL do pedido.

___ Fazer *caching* duma resposta a um pedido REST é simples porque basta indexar o conteúdo da resposta HTTP com base no URL do pedido.

___ A técnica de cifra por blocos encadeados (*cipher block chaining*) permite reduzir o perigo de ataques por análise de padrões repetidos no texto cifrado.

___ No sistema Kerberos, os servidores que fornecem serviços têm de conhecer as chaves dos utilizadores para os autenticarem.

___ Quando se acede a um servidor Web usando https, a autenticação do cliente é tipicamente efectuada recorrendo a certificados dos clientes.

___ Para permitir a revogação de certificados, quando um programa valida um certificado devia verificar se o certificado tinha sido revogado (e.g. contactando a entidade de certificação).

___ O sistema NFS implementa um modelo de *caching* de blocos.

___ Para funcionar corretamente, o sistema de *caching* do NFS necessita que os clientes e os servidores tenham os relógios sincronizados.

___ Para funcionar corretamente, o sistema de *caching* SMB/CIFS necessita que os clientes e os servidores tenham os relógios sincronizados.

___ Num sistema de replicação primário/secundário, se o primário devolver o resultado antes de propagar o resultado para o servidor secundário não existe garantia que a operação seja executada nos secundários.

___ Num serviço de nome com múltiplos servidores, a pesquisa recursiva exige mais recursos nos servidores que a pesquisa iterativa.

___ Um URL é sempre um nome global.

2) Considere um serviço de nomes em que a informação está replicada de forma completa num conjunto de servidores. Para cada pergunta, risque o que não interessa. **As respostas erradas descontam**.

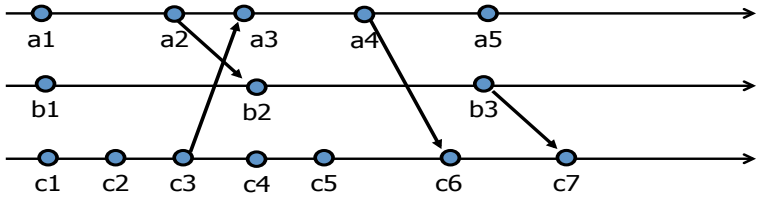
   a) A solução mais eficiente para implementar uma operação de leitura é utilizar: broadcast / multicast / anycast.

   b) Uma operação de escrita deve ser implementada usando: multicast não fiável / multicast fiável / multicast fiável com sincronia virtual.

   c) Uma operação de escrita deve ser implementada usando: ordenação total / ordenação FIFO / sem ordem.

3) 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, assinale como **V[erdadeira]** ou **F[alsa]** cada uma das afirmações. **As respostas erradas descontam**.



___ A2 aconteceu antes de C7.

___ A4 aconteceu antes de B3.

___ C4 aconteceu antes de A5.

   b) Suponha que pretende identificar os eventos com relógios lógico. Indique um possível valor para cada um dos seguintes eventos, sabendo que o primeiro evento será identificado com o relógio 1

A2: _____ A3: _____ B3: _____ C6:_____ C7: _____

4) Considere um sistema similar ao Twitter, com um muito elevado número de utilizadores. Para cada utilizador, mantém-se uma sequência de mensagem adicionadas pelo utilizador. Cada utilizador pode seguir um conjunto de outros utilizadores. A página pessoal dum utilizador apresenta a lista de mensagens dos utilizadores que ele segue. Um utilizador pode re-emitir ou responder a uma mensagem de outro utilizador.
   Neste contexto responda às seguintes questões:

   a) Se os clientes estivessem sempre a executar e apenas acedessem à sua página pessoal, poderia implementar este sistema usando um sistema de disseminação de eventos? Justifique indicando porque não é apropriado ou como é que o implementaria.

Sim, porque… / Não, porque… (risque o que não interessa)

b) Neste sistema seria interessante manter a informação causal relativa às mensagens submetidas? Justifique.

Sim, porque… / Não, porque… (risque o que não interessa)

4) Considere um ambiente de rede local em que um conjunto de utilizadores usa um sistema distribuído de ficheiros para partilhar um ficheiro de uma base de dados, de grande dimensão.
   a) Considere que o ficheiro da base de dados é acedido apenas para leitura (não sendo necessário fazer nenhuma escrita em disco). Neste caso, o mecanismo de controlo de *caching* do sistema CIFS/SMB permite um funcionamento eficiente? Justifique.

Sim, porque… / Não, porque…

   b) Considere que a base de dados é acedida para escrita, mas que as escritas dos utilizadores são refletidas tipicamente em zonas diferentes dos ficheiros. Proponha uma possível modificação ao sistema de controlo de *caching* do sistema CIFS/SMB que tornasse mais eficiente o acesso aos ficheiros nestas condições.

5) Uma empresa U9A que tem um conjunto de clientes aos quais pretende fornecer um serviço de correio electrónico. Cada cliente tem um registo na empresa, o qual contém o seu nome e uma palavra chave. Para fornecer o serviço de correio electrónico, a empresa U9A recorre a uma segunda empresa Jêmeile que mantém o serviço através dum servidor Smail. Por questões de segurança, a empresa U9A não pretende fornecer as palavras chaves dos utilizadores à empresa Jêmeile.
   Para ajudar a segurança do sistema, a empresa U9A tem um servidor de autenticação SAut que conhece os nomes e passwords de todos os clientes.
   Os servidores SAut e Smail têm um par de chaves assimétricas KpubSaut/KprivSaut e KpubSmail/KprivSmail, respectivamente. As chaves públicas são conhecidas por todas as entidades do sistema (incluindo os clientes).
   Apresente um protocolo que permita a um cliente C com palavra-chave pwd autenticar-se e estabelecer um canal seguro, com segurança futura perfeita, com o servidor Smail. Na sua solução, minimize a informação transmitida na rede e o poder computacional necessário para executar o protocolo. O protocolo deve ter, no máximo, 4 mensagens, efetuando a seguinte interação: C->Saut; Saut->C; C->Smail; Smail->C. Explique como seriam garantidas as propriedades indicadas. Use as notações sintéticas de descrição de protocolos criptográficos que aprendeu nas aulas.

   NOTA: Caso não consiga resolver o problema assumindo que os elementos do sistema **apenas conhecem inicialmente** as chaves indicadas, indique explicitamente as chaves adicionais que assume serem conhecidas para cada um dos elementos do sistema **no início do protocolo**.

C -> Saut:

Saut -> C:

C -> Smail:

Smail -> C:

Qual a chave a usar em posteriores comunicações entre C e Smail?

O que é que garante o secretismo das mensagens seguintes?

O que garante a segurança futura perfeita do sistema?

Como é que Smail tem a certeza que está a comunicar com o utilizador C?

Como é que o utilizador C tem a certeza que está a comunicar com o servidor Smail?

Como é que se evita o replaying?

Definição dos símbolos usados (complete):
C – nome do utilizador; pwd – palavra chave do utilizador (conhecida por C e Saut)
KpubSaut/KprivSaut – chave pública e privada do servidor de autenticação
KpubSmail/KprivSmail – chave pública e privada do servidor de mail

---

Chaves adicionais conhecidas no início do protocolo (complete, se usar):