Departamento de Informática

Faculdade de Ciências e Tecnologia

UNIVERSIDADE NOVA DE LISBOA

Licenciatura em Engenharia Informática
PROVA DE TESTE PRÁTICO – Sistemas Distribuídos I
2º Semestre, 2002/2003

Leia com atenção cada questão antes de responder. A interpretação do enunciado de cada pergunta é um factor de avaliação do teste. O exame tem 7 questões e 5 páginas.
Não pode utilizar elementos pessoais de consulta. **A duração do exame é 3h00**.

Atenção: os alunos devem colocar o nome e o número em todas as páginas.

1) Como sabe o sistema Java/RMI baseia-se numa forma de comunicação síncrona do tipo pergunta / resposta em que o programa que realiza a invocação fica bloqueado à espera da resposta do objecto remoto. A implementação que utilizou da invocação remota Java/RMI é realizada sobre um canal TCP. Acha que faria sentido implementar a invocação remota do sistema Java/RMI sobre um sistema de troca persistente de mensagens? Justifique a sua resposta.

2) Comente a seguinte afirmação: "um sistema distribuído que se encontra disponível a 99.9% não pára mais do que 7 horas por mês".

3) No contexto de um sistema de multicasting fiável diga qual a diferença entre uma "ordem total" e uma "ordem total temporal" de entrega de mensagens.

4) Suponha que num sistema distribuído se está a usar o sistema Java/RMI para que os diferentes objectos se possam invocar uns aos outros. Suponha uma situação em que o objecto que implementa o objecto remoto A tem um método que invoca o objecto remoto B. Suponha que o objecto implementação de B tem um método que invoca o objecto remoto C. Suponha que o objecto implementação de C tem um método que invoca o objecto A.

a) O sistema Java/RMI permite que o cenário descrito seja possível ? Justifique a sua resposta.

b) Admitindo que o cenário era possível, podia o sistema ficar bloqueado num "deadlock" ou ter qualquer outro comportamento igualmente desastroso ? Justifique a sua resposta.

5) Considere um cenário em que o cliente C pretende estabelecer um canal seguro com um servidor S.

a) A seguir lista-se o conjunto de trocas de mensagens realizadas segundo o protocolo de Needham/Schroeder com chaves simétricas para autenticação e estabelecimento de um canal seguro entre um cliente e um servidor. As trocas de mensagens indicadas estão desordenadas. Ordene-as. C designa o cliente, S o servidor, KDC o Key Distribution Center, Ks e Kc são as chaves simétricas do servidor e do cliente e K é a chave de sessão, M, N e P são números que por hipótese nunca mais serão reutilizados.

1. C -> S: {P-1}K
2. KDC -> C: {N, S, K, {K, C}Ks }Kc
3. C -> S: {K, C}Ks, {M}K
4. S -> C: {M-1, P}K
5. C -> KDC: C, S, N

b) Descreva um protocolo que permite ao cliente autenticar-se perante o servidor e estabelecer um canal seguro com o mesmo, sabendo que o servidor já conhece uma chave simétrica secreta do cliente. É claro que a chave secreta do cliente não deverá passar em claro na rede e ambos não poderão recorrer a terceiras partes. Considere que o cliente tem a certeza de que está a dialogar com o servidor S e não é possível nenhum impostor tomar o lugar de S. Descreva as fases do protocolo com a nomenclatura da a).

c) Descreva um protocolo que permite ao cliente autenticar-se perante o servidor e estabelecer um canal seguro com o mesmo, sabendo que o servidor já conhece uma chave simétrica secreta do cliente e o cliente conhece uma chave pública assimétrica do servidor. O cliente não tem a certeza de que está a dialogar com o servidor certo. Descreva as fases do protocolo com a nomenclatura da a).

6) Quais das seguintes questões são verdadeiras ou falsas ? Justifique a sua resposta no caso das falsas. Em cada resposta, riscar a opção que não interessa.

a) Um mecanismo de "locks" de ficheiros pode ser implementado facilmente num servidor de ficheiros "stateless".

Verdadeiro. Falso porque:

b) Os sistemas de ficheiros "stateless" não têm de incluir necessariamente um parâmetro "file offset" nas suas operações de leitura e escrita de ficheiros remotos.

Verdadeiro. Falso porque:

c) Os sistemas de ficheiros "stateful" têm uma interface de manipulação de ficheiros baseada em operações idempotentes.

Verdadeiro. Falso porque:

d) O "crash" dos servidores "stateless" pode ser mais facilmente transparente aos seus clientes.

Verdadeiro. Falso porque:

e) A gestão da cache no sistema SMB é completamente transparente ao servidor.

Verdadeiro. Falso porque:

7) Verdade ou falso ? Justifique a sua resposta quando é falso. Em cada resposta, riscar a opção que não interessa.

a) Um nome do tipo identificador pode ser reutilizado com frequência, ou seja, a associação entre o nome e a entidade que o mesmo designa pode variar frequentemente.

Verdadeiro. Falso porque:

b) Dois identificadores distintos, no mesmo espaço, designam sempre duas entidades distintas.

Verdadeiro. Falso porque:

c) Dois nomes distintos no mesmo contexto, designam necessariamente duas entidades distintas.

Verdadeiro. Falso porque:

d) Um identificador, dada a sua não reutilização, tem necessariamente de ser afectado por uma entidade única e centralizada.

Verdadeiro. Falso porque:

e) A concatenação de uma data com resolução adequada com um endereço de rede é um método comum de geração de identificadores únicos e não reutilizáveis.

Verdadeiro. Falso porque: