Exame de Sistemas Distribuídos I
Ano lectivo de 2001 / 2002

2ª Chamada - 04/Julho/2002

Notas:
- **Exame sem consulta. Duração: 2h45m**
- **A interpretação e duração do enunciado faz parte da avaliação.**

Nº de aluno: _____ Nome: _____

Nº Total de páginas entregues (sem rosto) : _____ (numere as páginas na forma Pág. / Total)

Classificação das questões (a preencher pelos docentes):

Questão 1	Questão 2	Questão 3	Questão 4	Questão 5

Questão 6	Questão 7	Questão 8	Questão 9	

1) Um mecanismo de comunicação ponto a ponto pode apresentar falhas de omissão, falhas temporais e falhas arbitrárias. Um mecanismo de comunicação multiponto ("multicasting") envia mensagens do emissor para o conjunto dos membros de um grupo. Como define os tipos de falhas anteriores no caso de um mecanismo de comunicação multi-ponto ? Existe mais algum outro tipo de falhas relevante neste caso ?

2) Um mecanismo de comunicação por mensagens multiponto ("multicasting") geralmente disponibiliza uma sincronização entre o emissor e os receptores de tipo assíncrono, isto é, o emissor sabe que os receptores vão receber a sua mensagem depois da mesma ter sido emitida, e os receptores sabem que receberam uma mensagem também após a sua emissão.

a) É possível conceber uma sincronização multiponto do tipo síncrono ? Descreva em que consistiria a mesma.
b) É possível conceber uma sincronização multiponto do tipo request / reply ? Descreva em que consistiria a mesma.
c) Estes tipos de sincronização referidos em a) e b) introduzem problemas delicados de realização?

3) Defina o que é um sistema distribuído aberto ("open system") e quais as vantagens e os defeitos desses tipos de sistemas.

4) Explique de forma justificada como é que se pode desenhar um protocolo de invocação remota baseado em UDP que garanta a semântica "at most once" (no máximo uma vez) que mascare as falhas de omissão e temporização do canal de comunicação entre o cliente e o servidor. Indique formas que possam servir para minorar o mais que possível a carga do protocolo sobre o servidor, nomeadamente em ocupação de memória. Discuta depois se o seu protocolo é capaz de mascarar as falhas do servidor ("crashs").

5) Suponha que foi escolhido para implementar uma aplicação de acesso remoto a uma base de dados de referências a documentos *World Wide Web*. A base de dados é pesquisável mediante um conjunto de palavras-chave, e as pesquisas têm como resultado uma lista de referências, ordenada segundo o número de palavras-chave que ocorrem no documento referido. Cada referência corresponde a uma *string* com o URL e o um pequeno excerto do texto com o máximo de 1 Kbyte.

a) Admitindo que tinha acesso a um objecto que realiza as pesquisas na base de dados, discuta como implementaria, através de Java/RMI, a aplicação pretendida. Ignore o objecto de pesquisa e defina as interfaces e objectos que julgar mais adequados ao RMI. Apresente um esquema global da aplicação (distribuída) e a(s) interface(s) remotas envolvidas.
b) Suponha que por razões de eficiência a base de dados foi dividida por diversas máquinas cuja identidade é conhecida *a priori*. Discuta quais as alterações necessárias à solução proposta em **a)** para que esta funcione de acordo com as novas especificações e tire partido do facto de uma pesquisa poder realizar-se em paralelo nas várias partições da base de dados. Apresente um esquema global da nova aplicação.
c) Que alterações seriam necessárias à(s) interface(s) proposta(s) em a) para implementar a mesma aplicação recorrendo no cenário descrito em b).

6) Descreva o protocolo de Needham-Schroeder para inicialização de um canal seguro utilizando apenas criptografia simétrica.

7) Num banco pretende-se aumentar o grau de segurança no controlo do acesso ao cofre. Dado que o cofre é moderno, o código a fornecer para que o cofre se abra é uma espécie de "palavra chave", a digitar no teclado associado à fechadura. Pretende-se, no entanto, que essa palavra chave mude constantemente. Na verdade, cada vez que alguém carrega no botão para anunciar que quer abrir o cofre, aparece um número aleatório "sempre diferente" no écran do cofre. A pessoa tem então que digitar o número dado pelo cofre numa máquina de calcular especial de bolso (de que só o gerente sabe o PIN - Personal Identification Numer com 8 digitos - que a máquina de calcular exige para se activar), a qual dá como resposta um novo número que o utilizador deve digitar no teclado do cofre em resposta ao primeiro número afixado. Se tudo estiver bem, isto é, se o número dado em resposta ao desafio mostrado inicialmente, a porta do cofre abre-se. Explique como funciona este sistema e que grau de confiança se pode ter no mesmo.

8) Nalguns sistemas distribuídos de acesso a ficheiros remotos, os clientes gerem uma cache de ficheiros remotos a que aplicam uma política, quando há alterações de ficheiros nos clientes, de "delayed write", que no extremo pode ser "write on close".

a) Este tipo de políticas introduz problemas quando há manipulações concorrentes do mesmo ficheiro? Quais ? Justifique.
b) De que forma ou formas se tenta minorar os potênciais problemas assinalados em a) ?
c) Para além dos problemas assinalados em a) podem surgir outros problemas relacionados com falhas. Quais ?

9) O "Registry service" do sistema Java / RMI pode ser assimilado a um sistema de designação ou "binding". Os sistemas de "binding" ou designação permitem geralmente localizar entidades ou recursos, ou obter dados sobre os atributos dessas entidades. No entanto, a operação "lookup", a única operação que permite obter informação registada no "Registry service", devolve um "proxy" para um objecto remoto.

a) Comente a situação e mostre que afinal não há nenhuma contradição.
b) Os nomes dos objectos registados pela "directory RMI" são contextuais ou globais ?
c) O serviço de descoberta do sistema Jini também permite descobrir serviços. Indique algumas semelhanças e diferenças do serviço de descoberta Jini e do serviço "Registry" do Java / RMI.