FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE NOVA DE LISBOA

Departamento de Informática

Licenciatura em Engenharia Informática
Sistemas Distribuídos I – 1ª chamada, 29 de Junho de 2007
2º Semestre, 2006/2007

NOTAS: Leia com atenção cada questão antes de responder. A interpretação do enunciado de cada pergunta é um factor de avaliação do teste. **O exame é SEM consulta**. **A duração do exame é de 2h00 min + 30min**. O enunciado contém **5** páginas que devem ser entregues com a resposta ao exame.

NOME: _____ **NÚMERO**.: _____

1. Para aceder ao ficheiro indicado pelo URL `nfs://fatdata.berkley.edu/students/ze`, indique quais os nomes que devem ser resolvidos e qual o serviço (de nomes) usado para a sua resolução.

2. Considere que se utilizavam URNs em substituição de URLs para identificar recursos na Internet. Esta aproximação permite contribuir para que um cliente forneça transparência de falhas? Em caso afirmativo, explique como. Em caso negativo, explique porque não.

Sim, porque... / **Não,** porque... (risque o que não interessar)

3. Compare o desempenho e complexidade (do código necessário) do processo de codificação dos dados nas invocações remotas em Corba e usando Web Services. Justifique a resposta.

4. Suponha que pretende desenvolver um sistema que permita explorar os recursos computacionais (capacidade de processamento) disponíveis nos computadores duma instituição. Neste sistema, qualquer máquina poderia requerer a execução dum trabalho (fornecendo a sua descrição) e decidir executar um trabalho (obtendo a descrição do trabalho e devolvendo o seu resultado).
    1. Para implementar este sistema seria mais interessante usar um modelo de interacção do tipo produtor/ consumidor (publish/subscribe) ou de interacção indirecta (e.g. espaço de tuplos ou memória partilhada distribuída). Justifique.

Produtor/consumidor, porque... / **Interacção indirecta,** porque... (risque o que não interessar)

    2. Indique, justificadamente, quais as características do sistema Java e Java RMI que poderiam ser importantes para facilitar a implementação deste sistema.

5. Seria apropriado implementar um sistema de comunicação multicast (1 para N) usando um sistema de message-queuing? Explique como ou porque não.

Sim, porque... / **Não,** porque... (risque o que não interessar)

6. Considere o contexto de um sistema peer-to-peer de partilha de ficheiros multimédia. Neste sistema, cada peer pode obter o conteúdo de um ficheiro a partir de qualquer outro peer – para tal, deve enviar a identificação do ficheiro pretendido F e receber o conteúdo C (de grandes dimensões). Para ajudar a garantir a segurança do sistema, existe um servidor de segurança (SS) que partilha com cada peer uma chave simétrica (Ks1 para o peer P1, Ks2 para o peer P2, etc.).
   a) Apresente um protocolo que permita a um peer P1 obter o conteúdo de um ficheiro de um peer P2 de forma segura, i.e., garantindo o secretismo das mensagens trocadas e a autenticação mútua dos peers (i.e., os peers devem ter a certeza que estão a comunicar entre si). Na sua solução, tenha em atenção possíveis ataques por "*replaying*" e minimize a informação transmitida na rede. O protocolo deve ter, no máximo, 4 mensagens, efectuando a seguinte interacção: P1->P2->SS->P2->P1. 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.

P1 -> P2:

O que garante o secretismo?

P2 -> SS:

O que garante o secretismo?

SS -> P2:

O que garante o secretismo?

P2 -> P1:

O que garante o secretismo?

Como é que P2 tem a certeza que recebeu F de P1?

Como é que P1 tem a certeza que recebeu C de P2?

Como é que os ataques por *replaying* são evitados?

Definição dos símbolos usados (complete, se necessário):
F – nome do ficheiro a pedir; C – conteúdo do ficheiro
Ks1 – chave secreta partilha entre P1 e SS
Ks2 – chave secreta partilha entre P2 e SS

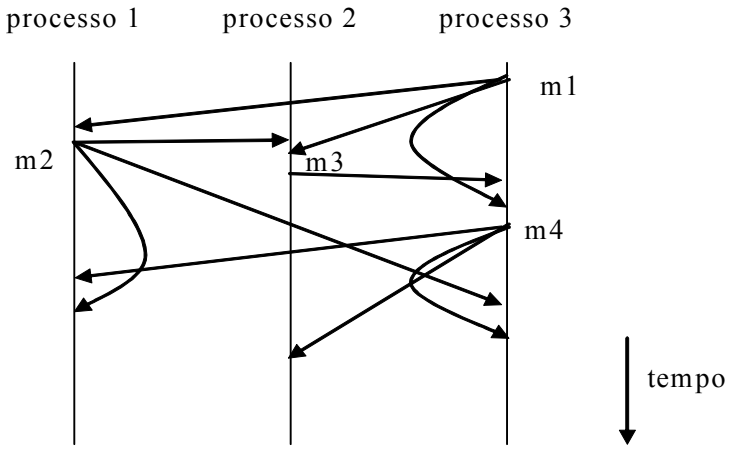
b) No contexto deste sistema, seria interessante evitar os ataques por *replaying*? Justifique.

Sim, porque... / **Não,** porque... (risque o que não interessar)

c) Supondo que não é um requisito do protocolo que P1 autentique P2 e vice-versa, seria suficiente executar o protocolo de Diffie-Hellman entre P1 e P2 para negociar uma chave que garanta o secretismo das mensagens trocadas entre P1 e P2 (assim removendo a necessidade de manter o servidor SS no sistema)?

Sim, porque... / **Não,** porque... (risque o que não interessar)

7. Considere o seguinte esquema temporal representando a propagação de mensagens num sistema composto por três processos. As setas indicam a propagação de mensagens entre os vários processos. O início de uma seta indica o envio de uma mensagem. O fim de uma seta representa a recepção de uma mensagem num processo. Suponha ainda que os processos comunicam usando um sistema de *middleware* capaz de atrasar a entrega das mensagens recebidas para garantir a sua entrega por uma dada ordem.



Com base na informação anterior, indique se cada uma das seguintes afirmações é **[V]erdadeira** ou **[F]alsa**. **Nota: as respostas erradas descontam.**

i. É possível respeitar a ordem total entregando a mensagem m1 depois da mensagem m3 no processo 3.
ii. Para garantir a ordem FIFO, é necessário entregar a mensagem m2 antes da mensagem m3 no processo 3.
iii. Supondo que a mensagem m2 é entregue antes do envio de m3 no processo 2, para garantir a ordem causal é necessário entregar a mensagem m2 antes da mensagem m3 no processo 3.
iv. É possível respeitar a ordem causal entregando a mensagem m4 antes da mensagem m2 no processo 1.
v. Supondo que a mensagem m1 é entregue antes do emissão da mensagem m2, para garantir a ordem causal é necessário entregar m1 antes de m2 no processo 2.

8. Considere o algoritmo de exclusão mútua baseado num servidor central (considere um modelo assíncrono e falhas fail-stop).
   a) Indique, justificadamente, se este algoritmo garante a *safety* (i.e., que o algoritmo em nenhum caso transita para um estado incorrecto)?

SIM porque / NÃO porque (risque o que não interessar)

   b) Como sabe, este algoritmo não garante a *liveness* (i.e., o algoritmo não consegue fazer progresso) quando o servidor falha. Caso um processo detecte a falha do servidor poderia tomar o seu lugar? Justifique, explicando porque não ou em que condições é que o poderia fazer.

SIM porque / NÃO porque (risque o que não interessar)

9. Suponha que pretende utilizar um sistema de bases de dados que armazena o conteúdo da base de dados num ficheiro armazenado num sistema distribuído de ficheiros. O sistema de bases de dados mantém o ficheiro do conteúdo aberto durante um período de tempo elevado e produz os seguintes acessos típicos:
   - Existem blocos do ficheiro que são lidos com grande frequência (enquanto muitos outros raramente ou nunca são lidos);
   - As escritas afectam apenas alguns blocos guardados aleatoriamente no disco (e são feitas por sobreposição).

   Considere ainda que apenas um utilizador acede ao conteúdo da base de dados (numa única máquina, i.e., ignore os problemas que poderiam advir do acesso concorrente).

   a) Supondo que utilizava a base de dados para leitura e escrita, qual o mecanismo mais eficiente: o do sistema SMB/CIFS ou o do sistema NFS? Justifique.

SMB/CIFS porque / NFS porque (risque o que não interessar)

   b) Supondo que utilizava a base de dados apenas para leitura, qual o mecanismo mais eficiente: o do sistema Coda ou o do sistema NFS? Justifique.

Coda porque / NFS porque (risque o que não interessar)