FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE NOVA DE LISBOA

Departamento de Informática

Licenciatura em Engenharia Informática
Sistemas Distribuídos – ep. recurso, 11 de Fevereiro de 2008
1º Semestre, 2007/2008

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 2h30 min**.
O enunciado contém **4** páginas que devem ser entregues com a resposta ao exame.

NOME: _____ **NÚMERO**.: _____

1. Apresente duas vantagens de desenvolver um sistema distribuído recorrendo a um sistema de *middleware* face a desenvolver sobre a interface nativa dos sistemas de operação.

1:

2:

2. Considere o sistema BitTorrent.
   i. Apresente uma razão pelas qual o mecanismo de toma-lá-dá-cá (tit-for-tat), em que um peer envia um bloco dum ficheiro apenas em troca de um bloco recebido, é fundamental para o bom funcionamento do sistema.

   ii. Na informação relativa a cada ficheiro a ser partilhado, o sistema mantém um hash seguro de cada bloco. Explique a razão desta opção face a ter um hash seguro do ficheiro completo.

3. Comente a afirmação: "a utilização de meios de comunicação assíncronos e persistentes contribui para a escalabilidade dum sistema distribuído", indicando se concorda com a mesma ou não e justificando.

Concordo, porque... | **Não concordo,** porque...

4. Considere um sistema de *chat*, com múltiplas salas nas quais os utilizadores podem trocar mensagens. Numa sala de chat, cada utilizador visualiza todas as mensagens inseridas por todos os utilizadores. A única operação disponível é a inserção de uma nova mensagem (que pode ser a respostas a uma mensagem enviada por outro utilizadores).
   Explique como poderia implementar este sistema recorrendo a comunicação multicast. NOTA: na sua resposta, caracterize a solução de multicast usada relativamente à fiabilidade e ordenação de mensagens (optando pelas soluções mais simples que permitem obter as propriedades minímas desejáveis).

Solução base:

Fiabilidade: **, porque**

Ordenação: **, porque**

5. A solução do sistema Java RMI de apenas permitir registar no *RMI registry* servidores/objectos remotos a executar na própria máquina contribui para a segurança do sistema. Indique se a afirmação anterior é verdadeira ou falsa justificando.

Verdadeira, porque.... | **Falsa**, porque....

6. Assinale com **[V]erdadeiro** ou **[F]also** as seguintes afirmações (**nota: as respostas erradas descontam**):
   i. Para resolver o nome "rmi://asc.di.fct.unl.pt/rmiServer" é necessário consultar dois serviços de nomes.
   ii. Uma referência remota inclui informação sobre a máquina em que o servidor executa.
   iii. Nos protocolos de invocação remota, mesmo quando as operações definidas no servidor são idempotentes é importante filtrar os duplicados.
   iv. No sistema Java RMI, os servidores têm uma organização interno do tipo "thread-por-objecto".
   v. Uma descrição WSDL inclui o formato das mensagens trocadas entre o cliente e o servidor.
   vi. Os dados transmitidos numa conexão SSL podem ser comprimidos pelo protocolo SSL.

7. Suponha que pretende implementar um cliente de correio electrónico com interface web (a executar num browser). Apresente duas vantagens da utilização dum sistema que suporte um mecanismo de invocação remota assíncrona de procedimentos (e.g. GWT) na criação do sistema (face a um interface web tradicional em que as interacções com o servidor são consequência da selecção de algum elemento da interface - botão, lista, etc.).

1.

2.

8. Considere o contexto de um sistema peer-to-peer de disseminação de fotografias. Neste sistema, um peer pode enviar o conteúdo de uma fotografia a qualquer outro peer – para tal, deve enviar a identificação do ficheiro F a enviar e o seu conteúdo C (de grandes dimensões). Para ajudar a garantir a segurança do sistema, existe um servidor de segurança (SS) que conhece a chave pública de cada peer (Kpub1 para o peer P1, Kpub2 para o peer P2, etc.) – cada peer tem um par de chaves assimétricas. O servidor de segurança possui um par de chaves assimétricas. Todos os peers conhecem a chave pública de SS.
   a) Apresente um protocolo que permita a um peer P1 enviar o ficheiro F com conteúdo C ao 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, 3 mensagens, efectuando a seguinte interacção: P1->P2->SS->P2. 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?

Como é que P2 tem a certeza que recebeu F e C enviado por P1 (e que estes não foram alterados)?

Como é que P1 tem a certeza que só P2 pode obter F e C?

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
Kpub1/Kpriv1 – chave pública/privada de P1
Kpub2/Kpriv2 – chave pública/privada de P2
KpubSS/KprivSS – chave pública/chave privada de SS

b) Caso P1 e P2 partilhassem uma chave secreta K, apresente o conteúdo da mensagem enviada por P1 a P2 para transmitir o ficheiro F com conteúdo C de forma a garantir **apenas** que P2 tenha a certeza que foi P1 que enviou a mensagem e que esta não foi modificada. Use as notações sintéticas de descrição de protocolos criptográficos que aprendeu nas aulas.

Mensagem:

Como sabe P2 que foi P1 que enviou a mensagem:

Como sabe P2 que recebeu o conteúdo correcto do ficheiro F:

9. No DNS, a resolução de nomes é geralmente iterative, controlada por um servidor. Apresente motivos pelos quais a solução normalmente usada não é puramente recursiva.

10. Suponha que um programa actualiza sucessivamente e em exclusividade um ficheiro de registo (log), adicionando linhas de texto de pequena dimensão – até 100 bytes. Caso o ficheiro de registo esteja guardado num sistema NFS, considera que o mecanismo de *write-back* que o NFS implementa contribui para o bom funcionamento do sistema. Justifique.

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

11. Suponha que, num ambiente semelhante ao dos laboratório do DI, em que existe um conjunto de PC e um servidor de ficheiros, se pretende partilhar um conjunto de ficheiros imutáveis – neste caso, programas e bibliotecas, de dimensão variada. Para cada um dos seguintes sistemas – NFS, SMB/CIFS, Coda, apresente, se alguma, uma característica do sistema que contribui para o seu bom funcionamento. Justifique.

NFS:

SMB/CIFS:

Coda: