FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE NOVA DE LISBOA

Departamento de Informática

Licenciatura em Engenharia Informática
Sistemas Distribuídos I – época de recurso, 24 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 2h30 min**.
O enunciado contém **5** páginas que devem ser entregues com a resposta ao exame.

NOME: _____ **NÚMERO**.: _____

1. Apresente duas vantagens de desenvolver um sistema distribuído recorrendo a uma linguagem cujo código executa sobre uma máquina virtual (e.g. Java) face a desenvolver numa linguagem que deve ser compilada em código nativo.

2. Indique se é verdadeira ou falsa a seguinte afirmação: "Num sistema tolerante a falhas é importante recuperar os componentes falhados". Justifique.

Verdadeira, porque... / **Falsa,** porque... (risque o que não interessar)

3. Explique em que consiste a activação de objectos remotos e em que condições é que a mesma é interessante.

4. Seria interessante implementar um sistema de invocação remota de procedimentos com semântica oneway (em que o cliente não aguarda pelo resultado) usando um sistema de *message-queueing*? Explique porquê, indicando as propriedades do sistema assim implementado, ou porque não.

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

5. Considere um sistema distribuído, que mantém arrays de bytes de grandes dimensões (e.g. ficheiros) associados a chaves (e.g. nomes simbólicos únicos), composto por: (1) um servidor S1 que mantém o mapeamento entre a chave e um identificador, o qual permite conhecer o servidor que contém o array de bytes associado a essa chave; (2) um conjunto de servidores que mantém os arrays de bytes armazenados no sistema, os quais podem ser acedidos pelos identificadores guardados no servidor S1 (cada servidor contém apenas um subconjunto dos arrays de bytes). Quando se pretende obter o array de bytes associado a uma chave, contacta-se primeiro o servidor S1 e de seguida o servidor que armazena o array de bytes.

    1. Indique, dos algoritmos distribuídos estudados, qual (se algum) seria interessante usar na implementação do sistema. Justifique.

    2. Apresente uma alternativa para a resolução de nomes em que não fosse necessário usar o servidor S1. Indique uma vantagem e uma desvantagem dessa aproximação face à indicada.

6. Considere o contexto de um sistema peer-to-peer de partilha de ficheiros multimédia. Neste sistema, cada peer tem um conjunto de outros peers nos quais confia e com os quais partilha uma chave secreta (uma chave com cada peer em que confia). Quando um peer P1 pretende obter o conteúdo de um ficheiro, pede a um dos peers em que confia (e.g P2) o conteúdo do ficheiro, enviando-lhe o nome do ficheiro F. Caso o peer P2 não tenha o ficheiro, pode solicitar a um peer em que (P2) confie (e.g. P3) para enviar o conteúdo do ficheiro para P1 – P3 envia o conteúdo C do ficheiro F directamente para P1. Suponha que P1 e P2 partilham a chave Ks1 e P2 e P3 partilham a chave Ks2.
    1. Apresente um protocolo que permita a um peer P1 obter o conteúdo C do ficheiro F de forma segura a partir de P3, mas comunicando inicialmente com P2, o qual comunica com P3, como explicado anteriormente. O protocolo deve garantir o secretismo das mensagens trocadas e a autenticação mútua dos peers (i.e., os peers devem ter a certeza com quem estão a comunicar – **não se esqueça de garantir que P3 sabe que foi P1 que fez o pedido e P1 sabe que foi P3 que enviou a resposta**). 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->P3->P1. Explique como seriam garantidas as propriedades indicadas. Use as notações sintéticas de descrição de protocolos criptográfico 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 -> P3:

O que garante o secretismo?

_____

P3 -> P1:

O que garante o secretismo?

_____

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

Como é que P3 tem a certeza que foi P1 que pediu F?

Como é que P1 sabe a identidade de quem enviou F e como tem a certeza dessa informação?

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

2. Apresente, justificando, um protocolo que permita a P1 obter o conteúdo C do ficheiro F a partir de P2 garantindo o secretismo, autenticação e a segurança futura perfeita (inclua o número de interacções necessárias – P1 e P2 partilham Ks1).

P1->P2:

O que garante o secretismo?

O que garante a autenticação?

O que garante a segurança futura perfeita?

7. Considere um sistema composto por três processos, os quais comunicam através da troca de mensagens ponto-a-ponto e multi-ponto usando um sistema de middleware que garante a fiabilidade da entrega das mensagens. Neste contexto, indique se cada uma das seguintes afirmações é **[V]erdadeira** ou **[F]alsa**. **Nota: as respostas erradas descontam.**

i. Dados dois eventos, e1 e e2, ocorridos em diferentes processos e estampilhados com um relógio lógico de Lamport, C(e1)=5 e C(e2)=5, sabe-se que e1 é concorrente com e2.

ii. Dados dois eventos, e1 e e2, em que e2 não é um evento de recepção de uma mensagem, ocorridos em diferentes processos e estampilhados com um relógio lógico de Lamport, C(e1)=5 e C(e2)=6, sabe-se que e1 aconteceu antes de e2.

iii. Dados dois eventos de envio de mensagem multi-ponto, e1 e e2, ocorridos em processo diferentes e estampilhados com um relógio lógico de Lamport, C(e1)=5 e C(e2)=8, é necessário entregar e1 antes de e2 em todos os processos para respetiar a ordem FIFO.

iv. Dados dois eventos, e1 e e2, com e1 o envio da mensagem m no processo 1 e e2 a recepção da mensagem m2 no processo 2, é possível que os mesmos fossem estampilhados com as seguintes estampilhas vectoriais: C(e1)=[5 2 3] e C(e2)=[5 4 7]?

v. Dados dois eventos de envio de mensagem multi-ponto, e1 e e2, com e1 a ocorrer no processo 1 e e2 no processo 3, e sabendo que os mesmos foram estampilhados com as seguintes estampilhas vectoriais: C(e1)=[5 2 3] e C(e2)=[5 4 7], respeita-se sempre a ordem causal se se entregar a mensagem correspondente a e1 antes da mensagem correspondente a e2 em todos os processos.

NOTA: em iv e v, assume-se que as estampilhas vectorias são actualizadas na emissão e recepção de mensagens, assim como quando ocorrem outros eventos no sistema.

8. Suponha que existe um grupo de servidores que mantém réplicas dum conjunto de valores associados a variáveis do tipo inteiro. Estas variáveis são acedidas, possivelmente ao mesmo tempo, por um conjunto de clientes, submetendo operações difundidas por *multicast.*
    1. Assumindo que a única operação disponível para actualizar uma variável é "*incremental*" e que a operação é executada no servidor, qual a ordem de entrega das mensagens mais fraca que garante a convergência das réplicas (sem ordem < ordem FIFO < ordem causal < ordem total)? Justifique.

Sem ordem/Ordem/FIFO/Ordem causal/Ordem total, porque... (risque o que não interessar)

    2. Assumindo que estão disponíveis as operações "*adicionar constante*" e "*multiplicar por constante*" para actualizar uma variável e que estas operações são executadas no servidor, qual a ordem de entrega das mensagens mais fraca que garante a convergência das réplicas (sem ordem < ordem FIFO < ordem causal < ordem total)? Justifique.

Sem ordem/Ordem FIFO/Ordem causal/Ordem total, porque... (risque o que não interessar)

9. Considere o sistema de ficheiros NFS. Sabendo qual o servidor a contactar, explique de forma breve mas completa (**i.e. indicando todos os passos**) como é feita a resolução do nome dum ficheiro (e.g. /dir/subdir/f). Indique, justificadamente, as características da solução, em termos de desempenho.

10. Suponha que pretende utilizar um sistema distribuído de ficheiros para armazenar ficheiros multimédia acedidos por vários utilizadores numa instituição. Como é habitual, os ficheiros multimédia têm, geralmente, uma grande dimensão e são modificados muito raramente. É comum os utilizadores acederem aos mesmos ficheiros no mesmo dia ou em dias consecutivos.
    Neste contexto, indique, jutificadamente, qual o sistema distribuído de ficheiros que seria mais apropriado usar para armazenar os ficheiros multimédia.

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