FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE NOVA DE LISBOA

Departamento de Informática

Licenciatura em Engenharia Informática
Sistemas Distribuídos – época de recurso, 28 de Janeiro de 2009
1º Semestre, 2008/2009

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**.
O enunciado contém **5** páginas que devem ser entregues com a resposta ao exame.

NOME: _____ **NÚMERO**.: _____

1) Comente a seguinte afirmação, indicando justificadamente se a mesma é verdadeira ou falsa: "Num sistema distribuído é sempre possível a um coimponente saber se um outro componente (computador) está a funcionar correctamente ou se falhou".

Verdade, porque... | **Falso,** porque...

2) Comente a seguinte afirmação, indicando justificadamente se a mesma é verdadeira ou falsa: "O Java RMI fornece às aplicações transparência relativamente às falhas".

Verdade, porque... | **Falso,** porque...

3) Suponha que se pretende implementar um sistema de chat que possa ser usado por **milhões de utilizadores**. Este sistema deve permitir a um utilizador comunicar com outro utilizador – apenas são permitidas comunicações ponto-a-ponto.

   a) Assumindo que cada utilizador conhece um identificador de cada utilizador com que pretende comunicar, seria interessante utilizar um sistema do tipo DHT, que implementa uma tabela de hash distribuída, para facilitar o contacto inicial entre os utilizadores? Explique como ou porque não.

Sim, porque... | **Não,** porque...

b) Apresente uma arquitectura que permita suportar de forma eficaz a pesquisa de um utilizador dada uma parte do seu nome – por exemplo, usar "Pregui*" para pesquisar "Preguiça" – assumindo que, normalmente, um utilizador pesquisa utilizadores que se encontram próximos da sua localização. Justifique.

4) Numa arquitectura orientada a serviços, as aplicações necessitam de procurar serviços existentes numa rede, dada a sua descrição e não sabendo a sua localização. A aplicação liga-se a este serviços para executar operações necessárias ao seu funcionamento – por exemplo, uma aplicação pode necessitar dum serviço de computação e de um serviço de envio de mensagens SMS fornecidos em diferentes computadores da rede.

a) Considera que a utilização do *rmiregistry* seria apropriada para permitir à aplicação descobrir e contactar os serviços necessários? Explique como poderia ser usado ou apresente razões que tornam desaconselhável esta solução.

Sim, porque... | **Não,** porque...

b) Considera que a utilização do serviço UDDI (dos web services) seria apropriada para permitir à aplicação contactar os serviços necessários? Explique como poderia ser usado ou apresente razões que tornam desaconselhável esta solução.

Sim, porque... | **Não,** porque...

5) Considere o contexto dum sistema de abertura automática de portas usando cartões com RFIDs, como o existente na faculdade para controlar as portas do edifício. Suponha as seguintes características do sistema:
   - os cartões têm associado um identificador;
   - os cartões têm capacidade de processamento (incluindo a capacidade para executar operações criptográficas) e comunicação, podendo estabelecer com um leitor associada à porta n (L_n) um protocolo de comunicação;
   - existe um servidor (S) que conhece, para cada identificador de cartão as permissões para cada porta.

   Suponha que o leitor associado a uma porta L_n partilha com S uma chave simétrica K_{Ln}.

   O objectivo do sistema desenvolver é permitir ao leitor (L_n) de uma porta saber de forma segura, na presença dum cartão C_I com identificador I, se a porta deve ser aberta ou não.

a) Quais as propriedades de segurança que este protocolo deve garantir para ser seguro?

b) Apresente um protocolo que permita alcançar o objectivo do sistema, i.e., que permita ao leitor (L_n) associado à porta n, verificar de forma segura se deve abrir a porta a um utilizador que apresenta um cartão C_I com identificador I.

O protocolo deve garantir as propriedades que indicou na alínea anterior. O protocolo deve ter, no máximo, 4 mensagens, efectuando a seguinte interacção: L_n->C_I->L_n->S->L_n. Explique como seriam garantidas as propriedades indicadas. Use as notações sintéticas de descrição de protocolos criptográficos que aprendeu nas aulas.
Comece por indicar que chaves (além de K_{Ln}) devem existir para que seja possível resolver o problema. Na sua solução não se esqueça de considerar que o cartão tem uma capacidade de processamento extremamente reduzida.

Chaves adicionais:

L_n -> C_I:

C_I -> L_n:

L_n -> S:

S -> L_n:

Como é que S sabe de forma segura qual o cartão apresentado?

Como é que L_n sabe de forma segura que deve abrir a porta (ou não)?

Explique como as propriedades indicadas na alínea anterior são alcançadas.

Definição dos símbolos usados (complete, se necessário):
I – identificador do cartão C_I; sim/não – decisão de abrir a porta (ou não)
K_{Ln} – chave simétrica partilhada entre L_n e S

6) Explique em que consiste o problema da "segurança futura perfeita".

7) Assinale com **[V]erdadeiro** ou **[F]also** as seguintes afirmações (**nota: as respostas erradas descontam**):

   i. Em Java RMI, uma referência remota inclui a fábrica de sockets do cliente.

   ii. O mecanismo de codificação dos dados do Corba é mais eficiente que o mecanismo de codificação dos dados usado no Java RMI.

   iii. Um servidor Java RMI usa a política: *thread por objecto.*

   iv. O .NET remoting pode usar um mecanismo de ligação por configuração directa, em que no cliente se indica explicitamente a localização do servidor.

   v. O WSDL de um serviço remoto SOAP inclui a definição das mensagens usadas para aceder ao serviço.

8) Explique porque razão é possível utilizar os proxies HTTP para fazer cache dos resultados num sistema de invocação remota baseada em REST e não é possível (ou é muito difícil) fazer o mesmo num sistema de invocação remota SOAP.

9) No sistema NFS, nem todas as operações são idempotentes. Apresente um exemplo e explique como é que o sistema lida com a situação para usar um protocolo de invocação remota "at least once".

10) Considere um ambiente semelhante ao dos laboratórios do DI, com um número elevado (na ordem das 100) de máquinas com suficiente espaço em disco. Suponha que se pretendia instalar um sistema de ficheiros distribuído para partilhar uma hierarquia d directoria com ficheiro executáveis (que são modificados muito raramente). Qual dos mecanismos de cache que estudou pensa ser mais apropriado para este objectivo. Justifique.

NFS, porque... / **SMB/CIFS – op locks -** , porque... / **"Callback promise**", porque...