



FACULDADE DE
CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE NOVA DE LISBOA

Departamento de Informática

Licenciatura em Engenharia Informática
Sistemas Distribuídos – 1ª chamada, 19 de Janeiro de 2011
1º Semestre, 2011/2012

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) Explique como pode a utilização de máquinas virtuais simplificar a criação dum sistema distribuído.

- 2) Suponha que pretende desenvolver um sistema tipo Facebook, em que é mantido um conjunto de mensagens, e para cada mensagem um conjunto de comentários associados. Suponha que apenas podem ser efectuadas duas operações – criar mensagem e adicionar comentário a uma mensagem. Os dados do sistema devem ser mantidos replicados em vários centros de dados distribuídos geograficamente pelo mundo (cada centro de dados tem todos os dados do sistema). Suponha por simplicidade que cada centro de dados tem apenas um computador. Os utilizadores executam as suas operações contactando um centro de dados (em princípio, aquele geograficamente mais próximo).
- a) Suponha que as operações são propagadas entre os vários centros de dados usando um sistema de comunicação em grupo. Pretende-se que a informação em cada centro de dados seja sempre consistente – i.e., não deve haver um comentário a uma mensagem não existente. Indique qual a semântica do mecanismo de comunicação em grupo que deve ser usada relativamente à fiabilidade e ordenação das mensagens. Justifique.

Fiabilidade: _____ **porque** _____

Ordenação das mensagens: _____ **porque** _____

- b) Uma arquitectura alternativa para o sistema seria manter a informação de cada utilizador em apenas um centro de dados, usando uma estratégia de cliente/servidor particionado. Discuta as vantagens e desvantagens desta aproximação face à aproximação indicada.

Vantagens:

Desvantagens:

- c) Um centro de dados é composto por um conjunto de computadores. Para manter a informação das mensagens e respectivas respostas, seria interessante usar um arquitectura tipo DHT? Se sim, explique como organizaria a informação. Se não, explique as razões.

Sim / Não , porque ...

- 3) Suponha que pretende fornecer uma semântica “pelo menos uma vez” (at least once) num sistema de invocação remota de procedimentos/métodos. Para tal, usa um mecanismo de retransmissão dos pedidos. Neste caso, será necessário usar um mecanismo de filtragem de duplicados ? Justifique.

Sim, porque... / Não, porque...

- 4) Assinale com **[V]erdadeiro** ou **[F]also** as seguintes afirmações (**nota: as respostas erradas descontam**):
- Em Java RMI, invocações de diferentes clientes executam concorrentemente.
 - Em Java RMI, um objecto servidor será recolhido (garbage collected) se não houver nenhum referência para ele (local ou remota).
 - O WSDL inclui informação sobre as mensagens que são enviadas para invocar um método e devolver uma resposta.
 - O WSDL inclui informação da localização do servidor, incluindo o nome da máquina (ou IP) e porta.
 - No .NET remoting a semântica de invocação é “pelo menos uma vez” (at least once).

- 5) Considere um sistema que permite a um utilizador disponibilizar ficheiros imutáveis de grandes dimensões para outros utilizadores – exemplo: ficheiros multimédia. Neste sistema, o utilizador que pretende disponibilizar a informação deve efectuar o envio (upload) da informação para um servidor, a qual poderá ser acedida pelos outros utilizadores. Assim, considere que um utilizador C pretende disponibilizar para vários utilizadores C1, C2, ..., Cn um ficheiro F com conteúdo *Cont* (de grandes dimensões). Para garantir a segurança do sistema, cada utilizador partilha uma chave simétrica com todos os outros utilizadores com os quais pretende partilhar a informação (K1 entre o utilizador C e o utilizador C1, K2 entre C e C2, etc.).

Por simplicidade assuma que C apenas pretende partilhar a informação com dois utilizadores – C1 e C2. Indique que informação deve enviar o utilizador C para o sistema de forma a partilhar o ficheiro F com conteúdo *Cont* com C1 e C2 de forma eficiente e segura, i.e., garantindo o secretismo das mensagens e do conteúdo do ficheiro e a autenticação dos parceiros de comunicação (i.e., C1 e C2 devem ter a certeza que receberam o ficheiro de C e C deve ter a certeza que apenas C1 e C2 podem obter o conteúdo do ficheiro). Na sua solução, minimize a informação transmitida na rede e armazenada no sistema e o poder computacional necessário para executar o protocolo. O protocolo de envio (upload) de informação deve ter, no máximo, 1 mensagem, efectuando a seguinte interacção: C->sistema. 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.

C -> sistema:

O que garante o secretismo?

Como é que C1, C2 tem a certeza que recebeu o ficheiro de C?

Como é que C tem a certeza que apenas C1 e C2 podem obter o conteúdo do ficheiro?

Explique como é que se minimiza a comunicação e espaço ocupado?

Explique como é que se minimiza a capacidade computacional necessária?

Definição dos símbolos usados (complete, se necessário):

F – nome do ficheiro a pedir; *Cont* – conteúdo do ficheiro

K1 – chave secreta partilha entre C e C1

K2 – chave secreta partilha entre C e C2

- 6) Explique o que se entende por segurança futura perfeita e de que forma o algoritmo Diffie-Hellman pode contribuir para que um sistema apresente esta propriedade.

- 7) Considere um sistema de partilha de mensagens relativas a artistas semelhante ao implementado no trabalho prático, implementado usando uma arquitectura com um servidor único. Para cada artista o sistema mantém uma lista de eventos, contendo cada evento uma lista de recursos. O servidor permite: (a) adicionar um evento à lista de eventos dum artista; (b) adicionar um recurso a um evento; (c) listar os eventos dum dados artista; (d) para evento, listar a informação do evento, incluindo a lista de recursos; (e) obter um recurso.. Indique como poderia implementar cada operação usando REST (indique a operação, e o URL).

a.

b.

c.

d.

e.

- 8) Explique como é efectuada tipicamente a resolução de nomes no sistema DNS (iterativa, recursiva, multicast, combinação das anteriores), discutindo as razões para a solução adoptada.

- 9) Considere um ambiente de rede local em que um conjunto de utilizadores usa um sistema distribuído de ficheiros para partilhar ficheiros multimédia de grande dimensão.
- a) Considere que os ficheiros multimédia são acedidos apenas para leitura. Neste caso, o mecanismo de controlo de caching do sistema CIFS/SMB permite um funcionamento eficiente? Justifique.

Sim, porque... / Não, porque...

- b) Considere que os ficheiros multimédia são acedidos para escrita, mas que os utilizadores, em geral, se coordenam de forma a modificar diferentes partes do ficheiro. Proponha uma possível modificação ao sistema de controlo de *caching* do sistema CIFS/SMB que tornasse mais eficiente o acesso aos ficheiros nestas condições.