FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE NOVA DE LISBOA

Departamento de Informática

Licenciatura em Engenharia Informática
Sistemas Distribuídos – 1ª chamada, 7 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**.
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: "É mais fácil a quem desenvolve um sistema adicionar novas funcionalidades caso o sistema seja aberto (em vez de ser proprietário)".

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

2) Suponha que numa instituição existe um conjunto elevado de máquinas que se encontram permanentemente conectadas, as quais têm uma capacidade de armazenamento livre bastante elevada (na ordem das centenas de GB). Suponha que pretende implementar um sistema de recepção e armazenamento de correio electrónico, o qual deve armazenar as mensagens de todos os utilizadores da instituição sem que estes tenham necessidade de as apagar (como no gmail) e fornecer uma interface IMAP/POP3 para acesso ao email pelos clientes.

   a) Apresente uma solução eficiente para implementar este sistema, considerando que é impossível armazenar as mensagens de todos os utilizadores em apenas uma máquina. NOTA: Não se preocupe com questões de fiabilidade. Na sua resposta deve indicar o tipo de arquitectura usado, como são armazenadas as mensagem (em que computadores) e como é que os utilizadores acedem a essas mensagens de forma eficiente.

b) Discuta como poderia adicionar tolerância a falhas na sua solução.

3) Suponha que se pretende manter a informação sobre o stock dum conjunto de produtos replicada num conjunto de servidores (cada qual mantendo a informação sobre o stock de todos os produtos). Considere que apenas é possível efectuar duas operações sobre o stock: adicionar um valor positivo ou subtrair um valor positivo. Considere que o valor do stock pode (temporariamente) ter um valor negativo.
Suponha que se pretende implementar este sistema propagando as operações com recurso a comunicação multicast.

a) Neste caso, seria importante que fosse utilizado multicast fiável? Justifique.

Sim, porque... | **Não,** porque...

b) Neste caso, seria importante garantir a ordenação total das mensagens? Justifique.

Sim, porque... | **Não,** porque...

4) No Java RMI, na invocação remota de um método, os objectos (e.g. um objecto do tipo Hashtable) são passados por valor ou por referência? Apresente uma justificação para esta decisão.

Valor, porque... | **Referência,** porque...

5) Considere o contexto de um sistema distribuído de ficheiros, em que um conjunto de servidores de ficheiros (SF) disponibilizam diferentes ficheiros. Neste sistema, existe um servidor principal (SP) que conhece a localização de cada ficheiro (por simplicidade, assuma que cada ficheiro apenas se encontra presente num servidor de ficheiros). O servidor SP conhece ainda as permissões de cada utilizador relativa a cada ficheiro – nenhuma, leitura, escrita, leitura/escrita. Para ajudar a garantir a segurança do sistema, o servidor SP partilha uma chave simética com cada servidor de ficheiros (K_{SF1},...) e com cada utilizador (K_{U1},...).

Apresente um protocolo que permita a um utilizador U executar uma operação Op com resultado R no ficheiro F de forma segura, comunicando inicialmente com o servidor principal, SP, para conhecer o servidor de ficheiros, SF, em que o ficheiro se encontra. O protocolo deve garantir o **secretismo** das mensagens trocadas, a **autenticação** e **controlo de acessos** na execução da operação do utilizador no servidor de ficheiros (i.e., o servidor de ficheiros deve conseguir decidir se uma dada operação pode ser efectuada ou não). 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: U->SP->U->SF->U. **O protocolo deve ainda permitir a execução de uma sequência de diferentes operações por repetição da interacção entre U e SF, sem necessitar de voltar a contactar SP (i.e. (**U->SP->U->SF->U->SF->U->SF->U...)**.** 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.
Caso não consiga resolver o problema para permitir a execução de uma sequência de operações, resolva para permitir a execução de apenas uma operação.

U -> SP:

O que garante o secretismo?

SP -> U:

O que garante o secretismo?

U -> SF:

O que garante o secretismo?

SF -> U:

O que garante o secretismo?

Como é que SP tem a certeza que receber F de U?

Como é que SF tem a certeza da identidade do utilizador que está a executar a operação?

Como é que SF consegue executar controlo de acessos?

Como é que SF consegue executar controlo de acessos nas operações seguintes?

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

Definição dos símbolos usados (complete, se necessário):
F – nome do ficheiro a pedir; Op – operação a executar; R – resultado da operação
K_{SF} – chave simétrica partilhada entre SP e SF
K_U – chave simétrica partilhada entre SP e U

6) Comente a seguinte afirmação, indicando justificadamente se a mesma é verdadeira ou falsa: "Os problemas de segurança dum sistema que utilize código móvel podem ser resolvidos através da utilização de canais seguros".

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

7) Assinale com **[V]erdadeiro** ou **[F]also** as seguintes afirmações (**nota: as respostas erradas descontam**):
   i. Os web services utilizam, geralmente, como protocolo de transporte o HTTP (sobre TCP).
   ii. Um servidor implementado em Java RMI pode estar registado em mais do que um servidor rmiregistry.
   iii. Em Java RMI, uma referência remota inclui a fábrica de sockets do servidor.
   iv. Um servidor RMI pode implementar múltiplas interfaces remotas.
   v. O .NET remoting usa, geralmente, uma semântica de invocação "at least once".

8) Explique porque razões é que um sistema baseado em REST permite um melhor desempenho que um sistema baseado em web services SOAP num ambiente de Internet.

9) Considere o sistema de descoberta de serviços Jini.
   a) Assinale com **[V]erdadeiro** ou **[F]also** as seguintes afirmações (**nota: as respostas erradas descontam**):
      i. Um cliente começa por enviar uma mensagem multicast para localizar os servidores de *lookup*.
      ii. Um serviço pode estar registado em mais do que um servidor de *lookup*.
   b) O cliente contacta o serviço final utilizando um objecto recebido do serviço de *lookup* (descoberta). Apresente potenciais vantagens desta aproximação.

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.

a) Neste contexto, apresente um cenário de utilização realista em que fosse mais interessante efectuar *caching por blocos* e outro em que fosse mais interessante usar *caching de ficheiro completo.* Justifique a sua resposta.

Caching por blocos:

Caching de ficheiro completo:

b) Supondo que quando um ficheiro era alterado, apenas era alterado parcialmente (por exemplo, os primeiros segundos num ficheiro de aúdio de vários minutos), indique que (se alguma) alterações introduziria ao mecanismo de gestão de cache usado pelo sistema NFS para se adaptar ao cenário apresentado (tenha em consideração apenas o modo como o sistema adiciona e remove dados da cache). Justifique a resposta.