Departamento de Informática

Faculdade de Ciências e Tecnologia

UNIVERSIDADE NOVA DE LISBOA

Licenciatura em Engenharia Informática
Sistemas Distribuídos I – 6 de Julho de 2004
2º Semestre, 2003/2004

Exame sem consulta com a duração de 2h30

Aluno nº _____Nome: _____

1) Um serviço tolerante a falhas está disponível, por especificação, 99,99%. A especificação da disponibilidade desse serviço indica que a mesma é avaliada todos os meses.

a) Qual o período máximo seguido durante o qual o sistema pode estar não disponível num mês para não violar a especificação ?

b) Qual o período máximo seguido durante o qual o sistema pode estar não disponível num ano para não violar a especificação ?

c) Qual o período máximo durante o qual o sistema pode dar resultados errados num mês para não violar a especificação ?

2) Comente a seguinte afirmação: “um sistema distribuído consegue reproduzir o comportamento de um sistema centralizado e tornar transparente, isto é esconder, a distribuição, independentemente da capacidade dos canais de comunicação que utiliza”.

3) Um mecanismo de comunicação por mensagens multiponto (“multicasting”) geralmente disponibiliza uma sincronização entre o emissor e os receptores de tipo assíncrono, isto é, o emissor apenas sabe que os receptores vão receber a sua mensagem depois da mesma ter sido emitida, e os receptores sabem que receberam uma mensagem também após a sua emissão.

a) É possível conceber uma forma de comunicação multiponto de tipo síncrona unidireccional ? Descreva em que consistiria a mesma.

b) É possível conceber uma forma de comunicação multiponto de tipo pedido / resposta síncrona ? Descreva em que consistiria a mesma.

c) Estes tipos de comunicação referidos em a) e b) introduzem problemas delicados de realização?

4) Desenhe um protocolo para que dois programas A e B comuniquem de forma segura segundo o modelo pedido / resposta através de um sistema de comunicação persistente, isto é, assegurando a hipótese de comunicação mesmo que B ou A não estejam activos quando as mensagens forem enviadas. As mensagens trocadas são de dimensão significativa.

a) Deve ser usada uma chave de criptografia simétrica Ks, gerada para cada nova troca de mensagens entre A e B. Ks não pode ser gerada por nenhuma terceira parte. No protocolo só são enviadas duas mensagens, uma de A para B e outra de B para A. Só B consegue ler a mensagem que A lhe enviou. B consegue verificar que foi A que lhe enviou a mensagem. Só A consegue ler a resposta de B e tem possibilidade de verificar que foi B que lha enviou. A e B podem também verificar a integridade das mensagens que receberam. A mensagem de A para B é a M1, a mensagem de B para A é a M2.

Mensagem de A para B:

Mensagem de B para A:

Significado dos símbolos usados (para além de Ks, M1 e M2) e justificação:

b) Discuta de que forma é possível garantir a possibilidade de evitar ataques por "replaying" no seu protocolo.

5) Explique de forma justificada como é que se pode desenhar um protocolo de invocação remota baseado em UDP que garanta a semântica "at most once" (no máximo uma vez) e que mascare as falhas de omissão do canal de comunicação entre o cliente e o servidor. Indique formas que possam servir para minorar o mais que possível a carga do protocolo sobre o servidor, nomeadamente em ocupação de memória.

6) Considere um sistema de processos comunicantes em que se conhece o valor $\partial 1$ que denota o erro máximo que os relógios dos processos podem ter e em que se conhece o valor $\partial 2$ que denota o tempo máximo de encaminhamento de qualquer mensagem. Nesse sistema não se perdem mensagens. É possível, em determinadas condições particulares, um processo ordenar quaisquer mensagens que receba em função do momento real da emissão das mesmas e, eventualmente, em função de algum outro dado. Indique quais são essas condições e dados e indique também se as mesmas introduzem algumas limitações no funcionamento do sistema.

7) a) Considere o código seguinte, o qual representa um esboço de uma classe Java que implementa alguma da funcionalidade básica associada a um certificado. Preencha o código em falta.

Nota: Por questões de espaço e simplicidade, o código foi editado de modo a eliminar o tratamento das excepções.

```
import java.io.* ;
import java.util.* ;
import SD1.Security.* ;

public class Certificate implements [          ] {

    private String id ;
    private String ca_id ;
    private long expiration ;
    private byte[] keyData ;
    private byte[] [          ];

    public Key [          ]() {
        return new [          ]( keyData ) ;
    }
    public boolean isValid() {
        if( expiration > System.currentTimeMillis() ) {
            Digest d = new Digest() ;
            d.update( keyData ) ;
            d.update( (id + ca_id + expiration).getBytes() ) ;
            Certificate c = Certificate.get( [          ] ) ;
            return Arrays.equals( d.getBytes(), c.[          ]().[          ]( sigData ) ) ;
        } else return false ;
    }

    public static Certificate get( String owner ) {
        FileInputStream fis = new FileInputStream("certificates/" + owner + ".cer") ;
        return (Certificate) new ObjectInputStream( fis ).[          ]();
   }
}
```

b) Considere as seguintes afirmações, responda cada uma delas assinalando com **V**[erdadeiro] ou **F**[also]. As respostas erradas descontam até _ do valor de cada alínea.

☐ 1) A classe Certificate contém toda a informação criptográfica necessária para negociar um canal seguro.

☐ 2) A classe Certificate pode ser usada para autenticar uma entidade.

☐ 3) A classe Certificate, tal como está escrita, impede que o próprio emita um certificado a si próprio, devido à utilização de uma função de síntese.

☐ 4) A classe Certificate não deverá ser "serializável" porque tal seria uma enorme falha de segurança.

☐ 5) A classe Certificate contém informação de natureza privada que não deve ser passada a estranhos.

☐ 6) Na classe Certificate, a informação contida em keyData é de natureza sensível e privada e por isso deve estar guardada cifrada no disco.

☐ 7) Na classe Certificate, a informação sigData terá uma dimensão apreciável, da ordem do megabyte.

☐ 8) A classe Certificate não contempla a revogação de certificados mas tal é desnecessário, dado que a inclusão de uma assinatura digital garante que o certificado foi emitido por uma entidade de certificação idónea.

☐ 9) A classe Certificate, não contém a informação adequada para verificar assinaturas em que a data de emissão respectiva é importante.