Número: Nome:

LEIC/LERC – 2010/11

1º Exame de Sistemas Distribuídos

6 de Junho de 2011

Responda no enunciado, apenas no espaço fornecido. Identifique todas as folhas.

Duração: 2h30m

Grupo I [2,5 v.]

Considere o seguinte programa local, uma variante simplificada do sistema *doodle*.

```
1  int main() {
2    char str1[DIM], str2[DIM];
3    while (1) {
4       printf("introduza o comando:");
5       readString(str1, DIM);
6       if (strcmp(str1, "votar")==0) {
7             printf("Indique o seu nome:");
8             readString(str1, DIM);
9             if (strlen(str1)<3)
10              printf("Nome tem de ter, pelo menos, 3 caracteres.");
11            else {
12              printf("Indique a sua opção:");
13              readString(str2, DIM);
14              votar(str1, str2);
15              printf("O seu voto foi registado. Se já votou antes, o voto anterior foi
                        substituído.");
16            }
17      } else if (strcmp(str1, "consultar")==0) {
18            int numvotos;
19            printf("Indique a opção:");
20            readString(str1, DIM);
21            numvotos = consultar(str1);
22            printf("A opção tem %d votos até ao momento.", numvotos);
23 } } }
```

Pretende-se construir uma versão distribuída do programa acima. Na versão distribuída, haveria um servidor que manteria o estado de cada opção, permitindo que múltiplos clientes distribuídos geograficamente votem e consultem o sistema.

1. [1,2v] Assuma que já existe um servidor que implementa os procedimentos remotos *votar* e *consultar*, usando Sun RPC. Indique as alterações necessárias ao programa acima para implementar o cliente remoto. Indique o pseudo-código da alteração e a linha onde a inseriria/substituiria. Indique até um máximo de 4 alterações.

Número da linha original:
Alteração/nova linha a introduzir antes da original:

Número da linha original:
Alteração/nova linha a introduzir antes da original:

Número da linha original:
Alteração/nova linha a introduzir antes da original:

Número da linha original:
Alteração/nova linha a introduzir antes da original:

2. [0,6v] Na versão distribuída, a verificação de que o nome tem pelo menos 3 caracteres podia ser feita no cliente, no servidor, ou em ambos. Que opção escolheria?
   Assuma que é prioritário minimizar mensagens enviadas pela rede e que o servidor pode ser invocado por diversas implementações de clientes. Suporte a sua resposta indicando desvantagens das outras opções.

3. [0,7v] Assuma que pode optar entre a semântica pelo-menos-uma-vez e a semântica no-máximo-uma-vez para este serviço. Qual escolheria? Justifique.

Grupo II [2,5 v]

1. Os Web Services podem ser vistos como uma plataforma de RPC, na mesma categoria de plataformas mais antigas como o SUN RPC ou o DCE RPC.
   a. [0,9v] Complete a figura que indica a descrição de um serviço, mas na linguagem WSDL, associando na tabela em baixo as letras ao texto correspondente (uma ou mais palavras) em falta no WSDL.

```
<?xml version="1.0" encoding="UTF-8"?>
<definitions name="Domotica"
  targetNamespace="http://exemploTesteSD.com/domotica/domotica"
  xmlns:tns="http://exemploTesteSD.com/domotica/domotica"
  xmlns="http://schemas.xmlsoap.org/wsdl/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">

<____A_____>
  <xsd:schema elementFormDefault="qualified"
targetNamespace="http://exemploTesteSD.com/domotica/domotica">
      <xsd:simpleType name="Resultado">
          <xsd:restriction base='xsd:string' >
            <xsd:enumeration value="SUCESSO" />
            <xsd: enumeration value="ERRO" />
          </xsd:restriction>
      </xsd:simpleType>
      <xsd: _______B_________ name="DadosTemperatura">
        <xsd:sequence>
          <xsd:element name="valor"  type="__E__:long"/>
          <xsd:element name="resOperacao  type="_F_:Resultado"/>
        </xsd:sequence>
      </xsd: _______B_________ >
  </xsd:schema>
</____A_____>


<_______I___  name="temperaturaInMessage">
    <_____H_____="id" type="___E__:long"/>
</_______I____>
<_______I___  name="temperaturaOutMessage">
    <_____H____="temperatura"
type="_F_:DadosTemperatura"/>
</_______I____>
```

```
<_____J_____ name="DomoticaPortType">
   <_____L_____ name="temperatura">
       <input  ___I_____="_F___:temperaturaInMessage"/>
       <output ___I_____="__F__:temperaturaOutMessage"/>
  </_____L_____>
</_____J _______>


<_____O_______ name=DomoticaHTTP_B
type=”tns:_______P_______”>
   <soap:binding style ="rpc"
                 __R_="http://schemas.xmlsoap.org/soap/http"/>
     <operation name="temperatura">
       <____S____> <soap:body use="literal"
         namespace="http://exemploTesteSD.com/domotica/domotica"/>
       </____S____>
       <output> <soap:body use="literal"
         namespace="http://exemploTesteSD.com/domotica/domotica"/>
       </output>
     </operation>
</___O_____>


 <_____U_____name="DomoticaS">
    <documentation>My exam one service</documentation>
    <__V__ name="DomoticaPort" _______X_______”>
        <soap:address location
    ="http://exemploTesteSD.com/ExemploDomoticaWS/endpoint"/>
    </__V__>
  </_____U_____>

</definitions>
```

portType			types			transport	
part name			binding			xsd	
Port			message			input	
complexType			operation			binding="tns:DomoticaHTTP_B”	
Tns			service			DomoticaPortType	

b. I [0,3v] Indique quais as secções da parte abstracta da parte concreta do WSDL.

II [0,3v] Qual a vantagem em separar a parte abstracta da concreta? E qual a vantagem em ter várias secções em cada uma delas? Justifique.

c. [0,4v] Qual a semântica de execução garantida para a invocação deste web service? Justifique com base no WSDL apresentado.

d. Assuma que o documento WSDL foi criado por um programador. Deu dois tipos de aproximação - contract-first ou Implementation first, que podem ser utilizadas na base do desenvolvimento do servidor e do cliente

   i. [0,15v] Qual o tipo de aproximação foi utilizada para este documento?

   ii. [0,45v] Descreva comparativamente as duas aproximações.

Grupo III [2,5 v]

```
1    package examples.RMIHumanHealth;
2    import java.rmi.*;
3    import java.rmi.server.*;
4
5    public class HealthObject implements Serializable{
6
7      public HealthObject() {……}
8      public void setHealthLevel(int l){
9            healthLevel = l;
10     }
11   }
12
13   public class HealthClient{
14     public static void main(String args[]){
15           System.setSecurityManager(new RMISecurityManager());
16           Population aPopulation = null;
17           Family aFamily = null;
18           Int sizeFamily = 0;
19           try{
20                    aPopulation  = (Population) Naming.lookup("//earth.net/Population");
21                    System.out.println("Found server");
22                    HealthObject h = new HealthObject();
23                    Human babyJohn=aPopulation.birth(h);
24                    aFamily  = (Family) Naming.lookup("//earth.net/Family");
25                    sizeFamily=aFamily.addMember(babyJohn).
26            }catch(RemoteException e) {System.out.println("HealthStatus: " + e.getMessage());}
27     }
28   }
29
30   public class FamilyClient{
31     public static void main(String args[]){
32           System.setSecurityManager(new RMISecurityManager());
33           Family aFamily = null;
34           Int sizeFamily = 0;
35           try{
36                    aFamily  = (Family) Naming.lookup("//earth.net/Family");
37                    HealthObject oldM = aFamily.olderMember();
38            }catch(RemoteException e) {System.out.println("FamilyStatus: " + e.getMessage());}
39     }
40   }
```

Considere o seguinte extracto acima de programas que descrevem a classe HealthObject e as classes de dois clientes de uma aplicação distribuída de gestão de dados de saúde de uma população (desenvolvimento do exemplo do teste 1 de 2011). As interfaces Human, Population e Family herdam da interface Remote. Considere ainda que as servants de Population e Family são intanciados no mesmo servidor.

1. [0,5v] Nas linhas 20, 24 e 36 o cliente invoca o serviço de nomes. Que informação é retornada por essas invocações? Explique que informação está armazenada no servidor de nomes e que relação tem com a informação retornada pela função de lookup. Justifique.

2. [0,5v] Como resultado dessas invocações, são instanciados objectos no espaço de endereçamento dos clientes. Quais? Justifique a resposta.

3. [0,5 v] No final de cada método Main, quantas referências remotas tem cada cliente? E para que objectos remotos?

4. [0,5v] O objecto `h` é usado na linha 22 como parâmetro da chamada ao método `birth` do objecto `aPopulation`. O objecto `oldM` por sua vez é retornado na linha 37 na chamada ao método `olderMember` do objecto `aFamily`. Como é que são passados estes objectos, e para que quem (servidor, HealthClient, FamilyClient)? Justifique.

5. [0,5v] A classe Human tem o método void setBI(int BI). Suponha que SetBI é invocado com um valor diferente do especificado na criação. O objecto no cliente e no servidor ficam com os mesmos valores? Justifique.

Grupo IV [2,5v]

Numa rede assíncrona e não fiável, existe um sistema replicado com N=5 réplicas de um dado registo.
O sistema replicado oferece aos clientes uma interface com duas operações: leitura e escrita.
Existem dois tipos de clientes: um único cliente (*single-thread*) que apenas emite pedidos de escrita (CW); e múltiplos clientes que apenas pedem leituras (CR1, CR2, …).
Assuma que as réplicas podem falhar silenciosamente, enquanto que os clientes nunca falham.
Considere o seguinte algoritmo para manter a consistência entre réplicas:

Algoritmo X

ler() {
1. CRi envia pedido de leitura a todas as réplicas;
2. Cada réplica que recebe o pedido responde com o valor da sua réplica;
3. Assim que CRi receber a primeira resposta, CRi retorna o respectivo valor à aplicação;

}

escrever(novoValor) {
1. CW envia pedido de escrita a todas as réplicas;
2. Cada réplica que receba o pedido de escrita aplica-o localmente e responde *ack*;
3. CW bloqueia-se até receber *ack* de todas as réplicas;

4. CW retorna à aplicação;

}

1. [0,6v] O algoritmo X tolera quantas falhas de réplicas na leitura? Justifique.

2. [0,7] A linha 3 da escrita parece demasiado limitativa para CW. Considere que era substituída por:
   "3. CW espera pelo primeiro ack recebido."
   Qual o problema desta modificação? Exemplifique com um exemplo.

3. [1,2v] Usando uma descrição análoga àquela usada acima para o algoritmo X, proponha um algoritmo alternativo que tolere mais falhas que X em operações de escrita.
   Assuma que existe apenas um escritor *single-thread* (CW).
   A sua solução pode diminuir a tolerância a faltas das leituras, desde que assegure que as leituras toleram pelo menos 1 réplica em falha.
   Penalizar-se-ão soluções mais complexas que o necessário.

Ler() {

Escrever() {

Grupo V [3v]

Considere o seguinte programa de um cliente.

O programa cliente invoca procedimentos remotos (LerSaldo e ActualizarSaldo) de dois servidores distintos (bancoA e bancoB), no âmbito de uma transacção distribuída.

O protocolo de confirmação atómica é o 2-Phase Commit.

```
1 transferência (bancoA, bancoB, Valor)
2 {
3   idDtx = openTransaction();
4   LerSaldo (bancoA, SaldoA, idDtx);
5   LerSaldo (bancoB, SaldoB, idDtx);
6   if (Valor > SaldoA)
7     closeTransaction(idDtx, abort);
8   else
9   {
10    ActualizarSaldo (bancoA, saldoA-Valor, idDtx);
11    ActualizarSaldo (bancoB, saldoB+Valor, idDtx);
12    closeTransaction(idDtx, commit);
13  }
14}
```

1. [0,6v] Quando o programa chega à linha 12, quantas transacções locais (em bancoA e bancoB) existem? Assumindo que não houve conflitos com outras transacções distribuídas, qual o seu estado (*activa/suspensa, confirmada* ou *abortada*)?

2. [0,6v] Considere que as rotinas de recepção da resposta à invocação remota da linha 11 têm um erro que coloca o cliente num ciclo infinito, não o permitindo chegar à linha 12. Os participantes envolvidos na transacção (bancoA e bancoB) podem desistir da transacção distribuída, ou são obrigados a esperar pela recuperação do coordenador? Justifique.

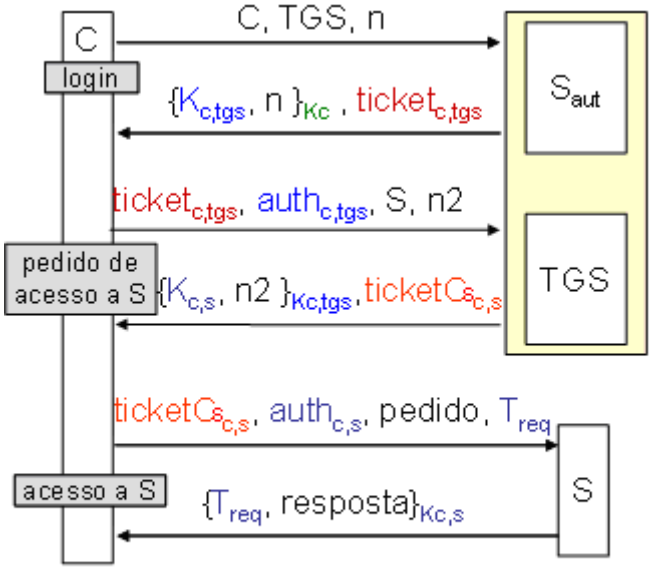
3. [0,6v] Descreva, em pseudo-código, a implementação da função *closeTransaction*. Considere apenas o caso em que o segundo argumento é *"commit".*

4. [0,6v] Descreva, em pseudo-código, a implementação da função *closeTransaction*. Considere apenas o caso em que o segundo argumento é *"abort"*. Caso a resposta seja igual à da alínea anterior, escreva apenas "igual".

5. [0,6v] Comente a afirmação "O 2-Phase Commit pode obrigar um participante no estado preparado a bloquear-se enquanto o coordenador não recuperar. No entanto, esse bloqueio não é grave pois outras transacções podem avançar em paralelo no mesmo participante."

Grupo VI [5v]

1. Considere uma plataforma integradora de serviços (por exemplo de IPTV e de Domótica), fornecidos por prestadores de serviços em servidores remotos.



$ticketCs_{c,s} = \{C, S, Cs, K_{c,s}\}_{Ks}$

A figura representa o protocolo de autenticação usado pela plataforma, que consiste numa variante do Kerberos, sobre o qual se introduziram pequenas alterações.
A plataforma é controlada por um operador de telecomunicações, o qual controla o servidor de autenticação Saut e o servidor TGS de distribuição de bilhetes (tickets).

O protocolo assegura que, se um cliente C contacta o sistema para pedir acesso a serviços fornecidos por um servidor prestador de serviços, S, então o cliente recebe um bilhete do TGS apenas se C for subscritor desses serviços.
O ticket retornado a C contém as capacidades Cs do cliente C em S. As capacidades incluem: a identificação de todos os objectos que o cliente pode aceder em S, e que operações tem autorização para efectuar sobre cada objecto em S.

a. [0,5v] Para as chaves referidas, assinale com um X na tabela seguinte quais as entidades que partilham as chaves permanentes, e com um Y as entidades que partilham as chaves temporárias.

	C	S	TGS	Saut
Kc				
Ks				
Kc,s				
Kc,tgs				
Ktgs				

b. [0,5v] Quais as diferenças entre os bilhetes deste protocolo e os do Kerberos?

c. [0,5v] Para que servem a informação n e n2 nas mensagens?

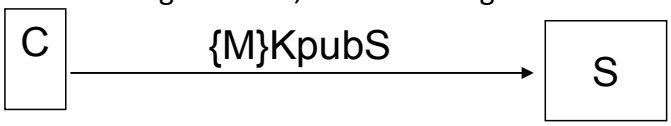
d. Um atacante teve acesso a um ficheiro em claro, M, e ao respectivo ficheiro cifrado C. Sabe-se que C foi cifrado usando o algoritmo DES usando uma chave de sessão Kerberos, Kcs. O atacante tenta descobrir qual foi a chave secreta utilizada através de um ataque de pesquisa exaustiva (*brute-force*) da chave Kcs.

- Cada chamada a encryptDES ou decryptDES demora 1 segundo. A mensagem original pode ser cifrada com uma única chamada a encryptDES.
- Assuma que a chave de sessão expira ao fim de 24h, sendo este o tempo máximo de uma sessão.
- O atacante só quebra a chave após de N/2 iterações da pesquisa exaustiva (em que N é o número de iterações).

i. [0,7v] Assuma que a chave Kcs é de 16 bits. O tamanho desta chave é seguro? Justifique indicando os cálculos.

ii. [0,6v] Assuma agora que Kcs tem 100 bits de tamanho, e que um atacante usando muitos recursos (por exemplo um grande cluster de computadores em rede) consegue descobrir Kcs após 2 anos de ataque de pesquisa exaustiva por força bruta. Conseguirá usar de forma ilegítima este sistema? Justifique.

2. Considere que um cliente C e um servidor S pretendem trocar mensagens de forma segura.
Para tal, S gerou um par de chaves privada e pública {KprivS, KpubS} e C gerou um par de chaves privada e pública {KprivC, KpubC}.
Sempre que C quer enviar uma mensagem M a S, envia-a da seguinte forma:



a. [0,3v] Como classifica a cifra acima: cifra simétrica ou assimétrica?

b. [0,3v] Indique o nome de um algoritmo que esteja na categoria de cifra que indicou.

c. [0,5v] Assuma que a chave pública de S foi enviada previamente num email para os clientes (em claro e sem qualquer informação adicional), usando um protocolo inseguro. Diga sucintamente como S poderia distribuir a sua chave pública a C de forma segura.

d. Um cliente C2, usando este protocolo, poderá enviar informação para o servidor fazendo passar-se pelo cliente C.

I. [0,6v] Descreva de que modo o cliente C deverá usar o seu próprio par de chaves, de modo a adicionar informação à mensagem que impeça este ataque. (Assuma que S conhece KpubC.)

II. [0,5v] Que propriedades de segurança são garantidas com a sua solução da alínea anterior?

Grupo VII [2v]

1. Jornal de Notícias, 26/5/2009:
   "Portadores do Cartão de Cidadão têm de procurar número de eleitor
   O recenseamento eleitoral automático está a criar dificuldades a milhares de cidadãos que não sabem onde terão de votar no dia 7 de Junho. […] Isto obrigou os cidadãos a terem de procurar saber qual o número que lhes foi atribuído para poderem votar [e o posto de voto onde deveriam votar]. Podem conhecê-lo na sua sede de junta de freguesia ou acedendo via internet ao sitewww.recenseamento.mai.gov.pt, ou ainda enviando uma sms gratuita para 3838 (RE, espaço, número de B.I. ou de Cartão de Cidadão, ano-mês-dia)."

   a. [0,5v] No contexto da gestão de nomes, a notícia refere a resolução de nomes necessária ao processo de voto. Indique quais os espaços de nomes envolvidos.

   b. Uma hipotética solução para simplificar o processo de voto seria adoptar um novo número de Bilhete de Identidade, que seria composto da seguinte forma:
   LLL:XXXXXXXXXX, em que L seriam caracteres alfabéticos que identificariam o posto de voto associado ao local de residência do cidadão e em que os dígitos X seriam algarismos decimais que identificariam univocamente o cidadão e seriam suficientes para ele votar no respectivo posto de voto.
      a. [0,5v] Como classificaria o antigo e a proposta de novo número de BI quanto à pureza? Justifique.

2. Considere o serviço de nomes DNS.
   a. [0,5v] Que vantagem(ns) traz o uso de caching à resolução de nomes no DNS? Indique no máximo 2, justificando.

   b. [0,5v] Que desvantagens traz o uso de caching ao registo de novas associações no DNS? Indique no máximo 2, justificando.
