LEIC/LETI 2014/15, Exame de Época Especial de Sistemas Distribuídos, 22/7/15

Responda no enunciado, apenas no espaço fornecido. Identifique todas as folhas. Duração: 2h30m

Grupo I [3v]

1) Considere um servidor em SUN RPC que permite aos seus clientes consultarem diferentes informações meteorológicas numa dada cidade.

A sua interface remota, descrita num ficheiro meteo.x, é a seguinte:

```
program METEO_PROG {
  version METEO_VERS {
    string GET_FORECAST(void) = 1;
    int GET_CURRENT_TEMPERATURE(void) = 2;
    int REPORT_METEO_EVENT(string) = 3;
  } = 1;
} = 1147765;
```

a) [0,5v] O número 1147765 acima tem de ser conhecido pelo programa cliente? Se sim, explique em que situação é que o cliente precisa saber o número. Se não, justifique.

b) [0,7v] Programe a função main de um cliente que invoca a função GET_FORECAST sobre um servidor a correr em meteo.ist.utl.pt e imprime o resultado no ecrã.
A invocação deve ser por UDP. Em caso de erros originados no RPC, o programa deve imprimir mensagem e terminar.
Caso precise de chamar a função clnt_create, apresenta-se de seguida a respetiva descrição das man pages:
*CLIENT *clnt_create(char *host, unsigned long prog,unsigned long vers, char *proto);*
Generic client creation routine. host identifies the name of the remote host where the server is located. proto indicates which kind of transport protocol to use. The currently supported values for this field are "udp" and "tcp".

```
int main ( int arc, char **argv ) {




}
```

c) [0,6v] No seu programa cliente, há linhas que podem originar erros relacionados com o RPC. Descreva em detalhe 2 dessas situações.

2) Considere agora a função remota *REPORT_METEO_EVENT*, que permite aos clientes reportarem um evento meteorológico. Quando executada, esta função associa um número único ao evento reportado e acrescenta-o numa fila mantida no servidor; além disso, incrementa um contador de eventos pendentes na fila e devolve ao cliente o novo valor desse contador.

Nas alíneas seguintes, assuma que o servidor tem a fila de eventos vazia e respetivo contador a zero. Considere que um programa cliente invoca a função *REPORT_METEO_EVENT* para reportar um dado evento.

a) [0,6] Preencha a tabela seguinte Indicando 2 situações distintas que são possíveis caso a semântica seja *Talvez*.

Resultado obtido pelo programa cliente	Valor do contador no servidor	Explicação do que aconteceu (usando diagrama de mensagens)
1		
Erro RPC		

b) [0,6] Partindo do estado inicial (contador a zero), considere agora que a semântica era *Pelo-menos-uma-vez*. Indique de novo 2 situações distintas, completando a tabela seguinte.

Resultado obtido pelo programa cliente	Valor do contador no servidor	Explicação do que aconteceu (usando diagrama de mensagens)
2		
Erro RPC		

Grupo II [2,8v]

1. Durante a época balnear, instalaram-se computadores em cada praia com bandeira azul. Cada computador corre uma máquina virtual Java onde existe um objeto que conhece o estado da praia. Esse objeto oferece um método *int bandeiraAtuall()* que permite consultar o tipo de bandeira atualmente na praia (0 - bandeia verde, 1 – amarela, 2 – vermelha, 3 - xadrez). Esse objecto é um objecto remoto Java RMI.

   a. [0,5v] Defina em Java a interface remota IMonitorPraia que os objectos remotos em cada praia oferecem.

   b. [0,7v] Apresente o método main de cada praia. Este método deverá criar o objecto remoto que monitoriza a praia e registar o objecto no RMI Registry com o nome indicado em *args[0]*. Assuma que existe uma classe *SDPraiaServant* que implementa a interface IMonitorPraia que definiu acima. Simplificação: omita do seu programa a definição do SecurityManager.

```
public static void main(String args[]){









 while (true) ; //ciclo infinito para não terminar
}
```

   c. [0,6v] Construa agora um programa cliente que verifica regularmente as condições no nó-sensor registado com o nome "\\carcavelos.praias.pt\carcavelos". O programa deverá consultar a bandeira nessa praia. Caso seja vermelha (valor 2), deve chamar o método *Alarme.alertaBandeira("carcavelos")*. Simplificação: omita do seu programa a definição do SecurityManager.

```
public static void main(String args[]){



 while (true) {




} }
```

2. [0,5] O Java RMI suporta o carregamento dinâmico de código. Descreva sucintamente uma situação em que esse mecanismo ocorra.

3. [0,5] "Em Java RMI, é possível um mesmo objeto ser passado por valor ou por referência, consoante o método remoto em que é passado." A afirmação é verdadeira ou falsa? Justifique.

Grupo III [3,8v]

Considere a mensagem SOAP abaixo:

```
POST /Customer HTTP/1.1
Host: www.example.org
Content-Type: text/xml; charset=utf-8
Content-Length: nnn
SOAPaction: "http://www.example.org/GetCustomer"

<?xml version="1.0"?>
<soap:Envelope
xmlns:soap="http://www.w3.org/2001/12/soap-envelope"
soap:encodingStyle="http://www.w3.org/2001/12/soap-encoding">

<soap:Body xmlns:m="http://www.example.org/customer">
  <m:GetNextCustomer>
</soap:Body>

</soap:Envelope>

HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: nnn

<?xml version="1.0"?>
<soap:Envelope
xmlns:soap="http://www.w3.org/2001/12/soap-envelope"
soap:encodingStyle="http://www.w3.org/2001/12/soap-encoding">

<soap:Body xmlns:m="http://www.example.org/stock">
  <m:GetNextCustomerResponse>
    <m:Name>ABCD</m:Name>
    <m:Balance>1234.15</m:Balance>
  </m:GetNextCustomerResponse >
</soap:Body>

</soap:Envelope>
```

1. A partir desta mensagem pode inferir diversas informações do documento WSDL que deve ter servido para o especificar.
    a. [0,6] Escreva em XML o excerto da secção PortType que a mensagem acima permite conhecer.

b. [0,7] A partir da mensagem defina o *XML schema* do parâmetro de saída do serviço. Defina a informação que não estiver explícita de acordo com o que lhe parece mais provável em conformidade com a mensagem.

2. Da mensagem pode também identificar elementos da parte concreta do WSDL.
   a. [0,4] Explique a diferença entre a parte abstrata e concreta do WSDL.
   b. [0,5] Que informação pode inferir relativamente à secção *binding*? Seja explícito referindo os itens que essa secção considera.
   c. [0,3] O URL *http://www.example.org/customer* deveria estar especificado em que secção?

3. [0,5] Os Web Services podem ser invocados de forma síncrona (request-response) ou assíncrona (one way). Diga em qual destas forma de invocação o excerto acima se insere e porquê.

4. Explique como é que o protocolo SOAP resolve os seguintes problemas:
   a. [0,4] Poder ser usado na internet e não ser barrado pelos *firewalls*.
   b. [0,4] Heterogeneidade de dados entre diversos processadores/ sistemas na rede.

Grupo IV [4,2v]

Considere a seguinte mensagem trocada entre a Alice e o Bob (da Alice para o Bob) no âmbito de um protocolo seguro, em que o Kerberos é usado como entidade autenticadora segura.

$$H(M+K_{AB})\ \ ticket_{A,B}\ Aut_{A,B}\ \{M\}_{KAB}$$

1. Identifique que componentes da mensagem acima permitem garantir os seguintes requisitos. Caso um requisito não seja garantido, indique-o e justifique.
    a. [0,5] Autenticar a Alice. Justifique.

    b. [0,5] Garantir a Integridade da mensagem. Justifique.

    c. [0,5] Garantir a frescura da mensagem. Justifique.

    d. [0,5] Garantir a confidencialidade. Justifique.

    e. [0,5] Garantir o não repúdio pela Alice da mensagem. Justifique.

2. [0,3] O $ticket_{A,B}$ é enviado pela Alice, mas esta não deve ter possibilidade de mudar o seu conteúdo. Como é que este requisito é implementado?

3. $H(M+K_{AB})$
   a. [0,6] Explique quais as dificuldades que terá um atacante para fazer $H(M'+K_{AB})=H(M+K_{AB})$ em que M' é obviamente uma mensagem falsificada?

4. $\{M\}_{KAB}$. Esta cifra poderia ser efetuada em modo Cipher Block Chaining (CBC).
   a. [0,4] Como é que o Bob obtém a chave para decifrar a mensagem?

   b. [0,4] Como funciona o CBC?

Grupo V [3v]

Considere a figura abaixo:

1. Suponha que a réplica 3 responde ao FE com X=0, pid=3, seq=20 e os restantes enviam os valores corretos.
    a. [0,3] O FE aceita a resposta? Justifique.

    b. [0,2] Como classifica essas situações em termos das características das faltas?

2. [0,5] Suponha que a réplica 3 não responde por atraso, respondendo as restantes duas. Que informação vai o FE enviar ao cliente? Justifique.

3. O cliente pretende escrever 50. Assuma agora que nenhuma réplica está em falta e responde sempre corretamente.
    a. [0,5] Considere o estado na figura acima. Quando a escrita se efetuar qual será o valor de sequência da réplica 2 admitindo que todo o protocolo decorreu sem faltas e que o pedido de escrita já chegou à réplica 2? Justifique.

    b. Em alternativa ao cenário da alínea anterior, considere que a escrita se efetuou apenas na Réplica 1 e os restantes não responderam ainda:
        i. [0,5] O FE pode concluir a operação? Justifique.

4. Considere que para além desta réplica, o sistema conta com uma réplica 4 que se executa numa máquina de elevada fiabilidade em relação a estas 3 que são idênticas.
    a. [0,5] Atribua pesos às réplicas de forma a que seja possível completar uma operação (leitura ou escrita) após receber: ou respostas da réplica 4 e de uma outra réplica qualquer; ou respostas das réplicas 1, 2 e 3.

        Réplica 1 ☐ Réplica 2 ☐ Réplica 3 ☐ Réplica 4 ☐

    b. [0,5] Justifique com base nas fórmulas de modelo de quórum com pesos os valores escolhidos.

Grupo VI [1,9v]

1. Considere uma aplicação em Java RMI que registou um objeto remoto no endereço *rmi://tecnico.ulisboa.pt:9090/sdObj.* Como classifica este nome?

    a) [0,3v] Quanto ao âmbito? Justifique.

    b) [0,3v] Quanto à pureza? Justifique.

    c) [0,3v] Quanto à heterogeneidade? Justifique.

2. Na organização hierárquica do DNS, resolver o nome en.wikipedia.org é possível contatando a sequência de servidores de nomes desde a raiz até ao domínio wikipedia.org: primeiro SNraiz, depois SNorg, finalmente SNwikipedia.
    a) [0,5] A resolução acima pode acontecer em modo recursivo ou modo iterativo. O que as distingue?

    b) [0,5] A resolução acima tem o problema de sobrecarregar o servidor dos domínios superiores. Que mecanismos no DNS evitam essa sobrecarga? Ilustre a sua resposta com um exemplo.

Grupo VII [1,3v]

1. Considere o seguinte programa cliente (em pseudo-código), em que S1 e S2 são proxies para serviços remotos distintos.

```
1 openTransaction();
2 x = S1.dequeue()
3 S2.enqueue(x);
4 closeTransaction();
```

Considere que é usado o protocolo 2-phase commit.

a. Ao chegar à linha 4:
   i. [0,2] Quantas transações locais existem nos participantes?

   ii. [0,2] Para cada transação local que indicou na alínea anterior, em que linha (1-4) é que a transação foi iniciada?

   iii. [0,2] Qual o estado das transações locais antes de executar a linha 4?

b. [0,7v] Represente no diagrama seguinte todas as mensagens trocadas durante a execução da linha 4. Assuma uma situação em que S1 está em falha silenciosa quando se executam as ações do protocolo correspondente à linha 4, não havendo outras falhas nem atrasos.

Cliente	Coordenador	S1	S2