LEIC/LETI – 2014/15, 1º Exame de Sistemas Distribuídos, 16 de Junho de 2015

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

Grupo I [3v]

Considere um servidor em SUN RPC que permite aos seus clientes consultarem a data atual em 2 formatos distintos - inteiro (binário) e string.

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

```
program DATE_PROG {
  version DATE_VERS {
    int INT_DATE(void) = 1;
    string STR_DATE(void) = 2;
  } = 1;
} = 897604;
```

1) [0,5v] O número 897604 acima é definido pelo programador que preparou o ficheiro apresentado acima. Esse número deve ser único dentro de determinado âmbito. Que âmbito é esse?

2) [0,5v] Quando usado sobre UDP, o SUN RPC oferece a semântica pelo-menos-uma-vez. Considera essa semântica adequada a este sistema? Justifique.

3) [0,7v] Programe a função main de um cliente que invoca a função STR_DATE sobre um servidor a correr em sigma.ist.utl.pt e a imprime 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 ) {




}
```

4) [0,7v] No seu programa cliente, há linhas que podem originar erros relacionados com o RPC. Descreva em detalhe 2 dessas situações.

5. [0,6v] Passados alguns meses desde o lançamento do servidor, o programador pretende adicionar uma terceira operação remota à interface, “string STR_TIME()”, que retorna apenas a hora atual.
Apresente as alterações que faria à interface de forma a manter a compatibilidade com clientes antigos da interface acima.

Grupo II [3,5v]

Em Java RMI considere um serviço distribuído de armazenamento de documentos, com parecenças com o serviço SDStore do projeto da cadeira. Neste serviço, cada utilizador tem um repositório invididual de documentos onde pode adicionar novos documentos e listar os documentos já existentes.
A sua interface remota é a seguinte:

```
public interface SDStoreI extends Remote {
        List<DocumentI> listDocs(String userdId);
        void createDoc(String userId, DocumentI newDoc);
}
```

1) [0,5v] A interface acima tem um erro. Indique como o corrigiria. Justifique explicando porque é que a correção que propõe é fundamental para o funcionamento do Java RMI.

2) [0,9v] Assuma que o serviço definido pela interface acima está instanciado e registado com o nome “rmi://rmi.ulisboa.pt/SDStore”.
Construa um programa que, a correr numa máquina remota, adiciona ao repositório do utilizador “Alice” um novo documento que é uma cópia do primeiro documento já existente no mesmo repositório.
Para tal, considere que existe uma classe Document que implementa DocumentI e que tem como métodos: *byte[] load()* e *void store(byte[]).*
Na sua resposta, pode omitir a configuração do SecurityManager. Não se esqueça de tratar eventuais erros da invocação remota.

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









}
```

3) O comportamento do seu programa é diferente consoante a classe Document seja remota ou não.
   a) Nos diagramas seguintes, indique onde residem os 3 objetos em causa (instância de SDStoreI, documento inicial do repositório de "Alice", novo documento criado no repositório de "Alice") e apresente as referências entre eles.
   Assuma que o documento inicial reside no mesmo processo que a instância de SDStoreI.
   A seguir a cada diagrama, justifique sucintamente a sua resposta.

      i) [0,6v] Caso Document seja classe remota.

Máquina que corre o programa da alínea 2	Máquina rmi.ulisboa.pt

      ii) [0,6v] Caso Document seja classe local.

Máquina que corre o programa da alínea 2	Máquina rmi.ulisboa.pt

   b) Na situação da alínea 3.1.i (Documento é classe remota), indique:
      i) [0,4v] Quantas instâncias de proxy tem a máquina rmi.ulisboa.pt? Justifique.

      ii) [0,5v] Considerando o programa que apresentou na alínea 2, indique uma linha que origine uma chamada addRef sobre algum garbage collector remoto. Justifique.

Grupo III [3,5v]

```
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>
```

Os excertos representam as mensagens de invocação e de resposta a um Web Service.

1) Da análise da mensagem inicial indique:
   a) [0,2] Qual o URL do serviço invocado.

   b) [0,2] Qual o nome da operação.

   c) [0,2] Quais os argumentos.

2) Da análise da resposta:
   a) [0,7] Escreva o protótipo da função em Java sem utilizar os elementos específicos do XML

   b) Em que secção do WSDL deveria estar:
      i) [0,2] A descrição do resultado explicitado na alínea anterior?

      ii) [0,2] A descrição da mensagem “GetNextCustomerResponse”?

      iii) [0,2] O SOAPaction: "http://www.example.org/GetCustomer""?

3) Suponha que o valor da informação de resposta deveria ser devolvida de forma confidencial.
   a) A melhor maneira é modificar o WSDL para cifrar os valores respetivos.
      i) [0,3] Concordo ☐ Discordo ☐
      ii) [0,6] Justifique.

4) Suponha que existe a exceção "No Client"
   a) [0,4] Como deveria em termos de web services ser tratada a exceção?

   b) [0,3] De que forma é incluída a excepção no pacote SOAP. Escolha a opção
      i) No header
      ii) Novo elemento do pacote com a tag fault
      iii) Tag fault dentro do body do pacote

☐

Grupo IV [4,5v]

Suponha que pretende desenvolver um sistema de gestão de arquivo de documentos seguros (GDoc) numa grande empresa usando web services e incorporando os requisitos de segurança necessários ao caso de negócio.

1) A Autenticação dos utilizadores utiliza um Active Directory suportado em Kerberos.
   a) [0,5] Na interação de autenticação do cliente com o Kerberos pode existir um ataque de man-in-the-middle? Se não, porquê? Se sim, explique o ataque.

   b) O Kerberos fornece um ticket para permitir utilizar o servidor de gestão documental, Gdoc. Considere o formato genérico de ticket enviado pelo cliente ao GDoc:

$$\{ \boxed{X} \boxed{Y} \boxed{T_1} \boxed{T_2} \boxed{K_1} \}_{K2}$$

   Explique para a chave K_1:
      i) [0,2] A função desta chave no protocolo.
      ii) [0,2] Quando é gerada?
      iii) [0,2] Onde deve ser guardada?

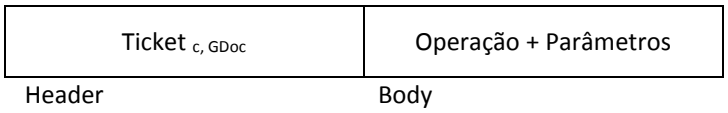
c) Explique para a chave K_2:

i) [0,2] A função desta chave no protocolo.

ii) [0,2] Quando é gerada?

iii) [0,2] Onde deve ser guardada?

2) [0,5] Na interação com o GDoc os clientes enviam um pacote SOAP que genericamente contém a seguinte informação:



A invocação representada pode ser alvo de um replay attack. Explique como se materializa este ataque.

3) Suponha que se pretende que o canal seja confidencial. No cenário descrito neste grupo, indique como poderia garantir a confidencialidade?

a) [0,5] Escolha um protocolo de cifra. Justifique a escolha.

b) [0,4] Como faria a distribuição da chave de forma segura utilizando o mínimo de recursos?

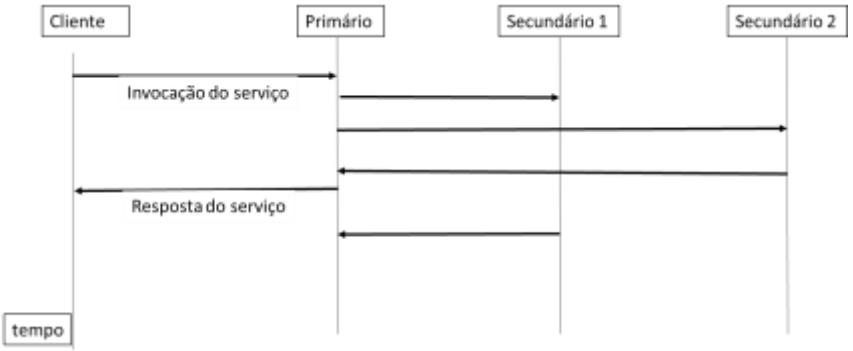
c) [0,4] Pretende-se usar uma cifra contínua (stream). Qual a vantagem? Justifique.

4) Existe a preocupação de, em relação aos documentos enviados na invocação dos serviços, garantir que são **íntegros, autenticados e não repudiáveis**.

a) [0,5] Suponha que o documento se chama ABC. Escolha uma assinatura adequada aos requisitos e mostre as operações que deveria realizar sobre o documento ABC para produzir essa assinatura.

b) [0,5] A validação da assinatura pode ser sujeita a várias ataques. Identifique claramente um, mostrando como materializa.

Grupo V [2,5v]



Considere o protocolo descrito na figura acima, que é uma variante do primary backup ensinado nas teóricas. O primário envia a mensagem aos secundários e responde ao cliente quando recebe a primeira confirmação de um dos secundários.

Todos os pressupostos do primary backup se mantêm, em particular o primário envia aos secundários em cada período P uma mensagem de "I'm alive". O sistema é síncrono com Tmax como limite de entrega de mensagens. Para além destes pressupostos existe um protocolo para na ausência de mensagem de I'm alive do primário, os secundários decidirem qual é o novo primário.

1) O protocolo tolera 2 faltas de nós silenciosas.
   a) [0,5] Explique o que é uma falta silenciosa.

   b) [0,5] Exemplifique porque tolera 2 faltas.

2) Como existem 3 réplicas, o protocolo tolera também 1 falta bizantina.
   a) [0,2] Concordo ☐ Discordo ☐
   b) [0,6] Justifique a sua escolha.

3) [0,7] Uma importante característica de avaliação dos protocolos é o incremento de tempo na resposta ao cliente. Procure calcular qual o incremento máximo de tempo na resposta ao cliente deste protocolo. Assuma que o tempo de execução dos pedidos é próximo de zero

Grupo VI [1,4v]

Considere um sistema de compras online que permite aos seus utilizadores comprar de diferentes fornecedores distribuídos. Ao longo de uma sessão, cada utilizador pode juntar itens ao seu carrinho de compras e, no final, fechar a compra conjunta desses itens junto dos respetivos fornecedores.
Cada fornecedor dispõe de um serviço remoto que permite ao sistema de compras online consultar e efetuar compras dos itens no stock de cada fornecedor.
O passo de fechar a compra (*check-out*) está descrito no seguinte pseudo-código:

```
boolean checkOut (list<Item> shoppingCart) {
        for each (Item i in shoppingCart) {
                Supplier s = getSupplierProxy(i);
                if (s.isInStock(i) == false)
                        return false;
                else
                        s.buy(i);
        }
        return true;
}
```

1) [0,4v] Apesar de desejável para o utilizador, o programa acima não garante a atomicidade da compra conjunta. Complemente o programa acima com uma transação distribuída que assegure essa propriedade.

```
boolean checkOut (list<Item> shoppingCart) {




}
```

2) [0,3v] Da resposta dada à alínea anterior, indique quais linhas são invocações diretas sobre o coordenador da transação distribuída?

3) Assuma que o programa acima é executado para fechar uma compra conjunta envolvendo 5 fornecedores participantes (A,B,C,D,E) e chega ao momento da terminação atómica. Assuma também que o protocolo usado é o 2-Phase Commit (2PC).
Indique qual a decisão tomada pelo coordenador em cada uma das seguintes situações.
Indique apenas uma opção. **Resposta errada desconta ¼ da cotação da alínea.**

a) [0,35v] Após enviar canCommit(tx), o coordenador recebeu voto Yes de todos os participantes exceto do E, que votou No.
   i) Coordenador envia doAbort a todos.
   ii) Coordenador envia doCommit a todos.
   iii) Coordenador envia doCommit aos participantes que votaram Yes e doAbort a E.
   iv) Coordenador não toma nenhuma decisão neste caso.

b) [0,35v] Após enviar canCommit(tx), o coordenador recebeu voto Yes de todos os participantes, incluindo E. No entanto, antes de receber a decisão do coordenador, E falhou temporariamente.
   i) Todos os participantes abortam a transação, incluindo E depois de recuperar.
   ii) Todos os participantes confirmam a transação, incluindo E depois de recuperar.
   iii) Os participantes A-D confirmam a transação; E aborta a transação assim que recuperar.
   iv) Participantes não confirmam nem abortam nesta situação.

Grupo VII [1,6v]

1) Considere o seguinte programa que, através da biblioteca JAX-R, permite a um cliente consultar no UDDI a informação relativa a uma organização (*orgName)*.

```
BulkResponse r = bqm.findOrganizations(…, orgName, …);
Collection<Organization> orgs = r.getCollection();

for (Organization o : orgs) {
    Collection<Service> services = o.getServices();

    for (Service s : services) {
        Collection<ServiceBinding> serviceBindinds = (Collection<ServiceBinding>) s
                .getServiceBindings();

        for (ServiceBinding sb : serviceBindinds) {
            result.add(sb.getAccessURL());
        }
    }
}
```

a) [0,4v] Num sistema replicado (como o serviço SDStore do projeto da cadeira), pretende-se registar no UDDI os *endpoints* dos diferentes gestores de réplica. Proponha uma forma de o fazer, descrevendo a sua solução com referência aos elementos apresentados no extrato acima.

b) [0,4v] O método getAccessURL() devolve um URL. Este nome é puro ou impuro? Justifique.

2. No serviço DNS, considere os servidores de nomes (SN) primários de uma sub-árvore de domínios.
Como a tabela mostra, cada SN conhece os SN dos seus sub-domínios e todos os SN de domínios ascendentes.

Servidor de nomes (SN)	**Zona gerida pelo SN**	**SN conhecidos por este SN**
SNpt	pt	SNulisboa
SNciencias	ciencias.ulisboa.pt	SNulisboa, SNpt
SNulisboa	ulisboa.pt	SNpt, SNtecnico, SNciencias
SNtecnico	tecnico.ulisboa.pt	SNtagus, SNulisboa, SNpt
SNtagus	tagus.tecnico.ulisboa.pt	SNtecnico, SNulisboa, SNpt

a) [0,4v] Assuma que um cliente na rede do Técnico - Taguspark está configurado para contactar o SNtagus sempre que precisa resolver um nome DNS.
Indique quais os SN que são contactados quando esse cliente tenta resolver o nome www.ciencias.ulisboa.pt. Justifique.
Assuma que as caches (tanto no cliente como nos servidores) estão limpas.

b) [0,4v] O endereço IP associado à máquina www.ciencias.ulisboa.pt era 194.117.42.133 e mudou para 194.117.42.140. A mudança de endereço IP foi atualizada nos registos do servidor de nomes primário do domínio em causa.
Indique 1 situação que possa levar a que, após essa atualização, haja clientes que continuam a observar o endereço IP antigo quando tentam resolver o nome www.ciencias.ulisboa.pt.