LEIC/LETI, 2014/15, 2º Exame de Sistemas Distribuídos, 30 de Junho de 2015

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

Grupo I [3,5v]

Considere o seguinte programa servidor, que funcionará sobre o SUN RPC. Este servidor armazena pares chave-valor (*key-value*), que podem ser escritos ou lidos através das funções remotas apresentadas abaixo.

```
struct store_args {
        char *key;
        char *val;
};
typedef struct store_args store_args;

void *store_1_svc(store_args *argp, struct svc_req *rqstp)
{
static char * result;
       putInLocalStorage(argp->key, argp->val) ;
return (void *) &result;
}

char **
load_1_svc(char **argp, struct svc_req *rqstp)
{
static char * result;
       result = getFromLocalStorage(*argp);
return &result;
}
```

1. [0,7] Apresente o conteúdo do IDL relativo a este programa. Assuma PROGRAM=62015 e VERSION=1.

2. [0,4] Uma hipotética alternativa a ter descrito a interface remota do serviço no IDL anterior teria sido definir os tipos de dados e assinaturas das funções num simples ficheiro .h. Apresente um exemplo da sua resposta anterior que ilustrem porque é que o .h não é solução.
   Caso não tenha respondido à alínea anterior, apresente um exemplo livre (cotação limitada a 70% neste caso).

3. [0,7] Considere o seguinte esboço de um programa cliente em SUN RPC, ainda em construção, que invoca o serviço anterior:

```
int main(...) {
        char *load_res;
        store_args args;

        /* We copy the contents of key1 to key2 */
        load_res = load_1("key1", NULL);

        args.key = "key2";
        args.val = load_res;
        store_1(&args, NULL);

        return 0;
}
```

Ajude o programador, indicando-lhe 2 aspetos de programação de SUN RPC que são fundamentais para o programa funcionar em SUN RPC. Proponha as alterações necessárias.

4. O servidor acima, quando usado sobre UDP, oferece a semântica pelo-menos-1-vez.
   a) [0,6] Pode uma invocação nesta semântica devolver "erro de RPC" devido a faltas na comunicação ou no servidor? Se sim, apresente num diagrama um exemplo em que uma invocação do cliente devolve "erro de RPC". Se não, justifique.
   Assuma que a rede não é fiável e que o nó servidor pode falhar.

   b) [0,5v] Para esta aplicação, seria vantajoso mudar para no-máximo-1-vez?

5. [0,6] Considere o módulo de comunicação de um servidor RPC que oferece a semântica no-máximo-1-vez. Apresente a sequência de passos (pode ser pseudo-código) que descreve o que esse módulo faz quando recebe um pedido vindo do cliente.

Grupo II [3v]

1. Considere o seguinte excerto de um programa em Java RMI, em que x referencia um objeto remoto:

```
1 try {
        2 TypeY y = x.receive();
        3 String name = y.getName();
        4 int val = y.getBalance("cash");
5 } catch (RemoteException e) {…}
```

a) [0,7] O retorno do método *receive* deve ser passado por referência. Apresente a declaração do tipo TypeY da forma o mais completa possível.

b) No programa acima é criado pelo menos um proxy.

i. [0,4] Que interface oferece esse proxy?

ii. [0,4] Onde é o proxy usado pela primeira vez no programa acima? Indique a linha.

iii. [0,5] Resuma as etapas que acontecem localmente quando um método do proxy é chamado por este programa.

2. Indique se cada afirmação seguinte sobre "garbage collection" é verdadeira ou falsa e justifique.

a) [0,5] "O uso de leases implica cliente e servidor com relógios sincronizados."

b) [0,5] "Em Java RMI, um objeto remoto é libertado assim que já não tenha referências locais a apontar para ele; independentemente do número de referências remotas que tenha."

Grupo III [3,5v]

1. [0,4] Considere o caso de uma empresa que decidiu evoluir a sua infra-estrutura de interoperação utilizando Web Services. A empresa tem já descrita a grande maioria das entidades informacionais como XML schemas em ficheiros .xsd. Poderá reaproveitar este trabalho na definição dos Web Services? Seja claro na resposta relacionando com o documento WSDL e respectivas secções.

2. Considere o extracto de XML schema definido na empresa para normalizar as mensagens de erro.

```
<xsd:complexType name="Fault">
<xsd:sequence><xsd:element minOccurs="0" name="reason" type="xsd:string"/>
</xsd:sequence>
</xsd:complexType
```

[0,4] Explique sucintamente o significado dos principais elementos deste XML schema: name, element, sequence ,minOccurs, name e type.

3. Considere o seguinte extrato de WSDL com a definição de um serviço.

```
<wsdl:portType name="Interface">
   <wsdl:operation name="op1">
    <wsdl:input name="op1Request" message="tns:op1RequestMsg"/>
    <wsdl:output name="op1Response" message="tns:op1ResponseMsg"/>
   </wsdl:operation>
</wsdl:portType>
```

a. [0,4] Explique onde se encontram declarados os parâmetros da operação e os respetivos tipos no documento WSDL.

b. O que deveria acrescentar para existir a possibilidade do cliente receber uma exceção lançada pelo servidor cujo **formato correspondesse ao formato genérico da alínea 2**?

   i. [0,3] Descreva o XML a acrescentar à secção portType.

   ii. [0,3] Descreva o XML a acrescentar à secção message.

c. Suponha que a empresa usa Kerberos para autenticar os utilizadores e os servidores. Pretende-se incluir o Ticket e o Autenticador na invocação dos web services.

a. [0,3] Que alterações deve efectuar no WSDL?

b. [0,3] Em que secção da mensagem SOAP devem ser enviados o Ticket e Autenticador?

c. [0,3] Que componente do sistema deverá executar a validação do ticket e autenticador do lado do servidor?

d. O Java RMI tem diversos conceitos que usam nomes semelhantes aos da tecnologia de Web Services mas mesmo quando usada com Java–WS diferem substancialmente.
Um objecto em Java quando interactua com um objecto remoto fá-lo através de um proxy.

i. [0,4] Indique uma diferença fundamental dos proxies em Web Services relativamente aos proxies de Java RMI quando são invocados por um objecto cliente. Justifique.

ii. [0,4] Indique uma semelhança. Justifique.

Grupo IV [3,7v]

Considere a seguinte mensagem genérica transmitida num canal seguro entre a Alice (emissor) e o Bob (receptor), em que M é o conteúdo da mensagem (*payload*) enviada e K1, K2, K3 e K4 designam genericamente chaves utilizadas no protocolo, H é uma função de resumo (digest).

$$\{H(M)\}_{K1}, \{K2\}_{K3}, \{M\}_{K4}$$

Tanto a Alice como o Bob dispõem de um par de chaves assimétricas: $K_{pub(A)}$, $K_{priv(A)}$, $K_{pub(B)}$, $K_{priv(B)}$, respetivamente. As chaves públicas foram previamente partilhadas entre os interlocutores de forma segura.

Nota: K1, K2, K3 e K4 não são necessariamente todas distintas entre elas.

1) O campo $\{H(M)\}_{K1}$, entre outras funções, garante o não-repudio do emissor da mensagem.
   a) [0,2] A cifra que é executada neste campo é, na sua opinião:

   ☐ Simétrica ☐ Assimétrica ☐ Híbrida

   b) [0,4] Indique quais os requisitos de segurança que este campo assegura no protocolo, justificando cada um.

   c) [0,4] Explique, em função dos intervenientes no canal e da cifra utilizada, qual é o significado da chave K1.

2) Considere o campo $\{K2\}_{K3}$
   a) [0,4] Qual a função deste campo?

   b) [0,4] Explique, em função dos intervenientes no canal e da cifra utilizada, qual é o significado da chave k3.

3) A expressão menciona quatro chaves.
   a) [0,1] São todas diferentes? Sim ou Não?

   b) [0,4] Se sim justifique porquê, senão indique quais as que são idênticas.

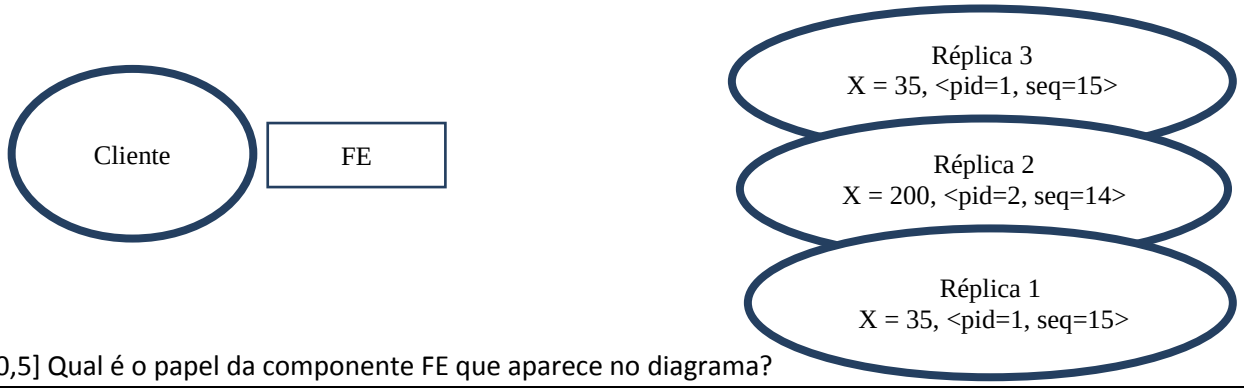
c) [0,4] Na receção da mensagem, quais as chaves que o Bob já deveria ter e quais deverá obter para executar o protocolo?

4) Um algoritmo de cifra assimétrica de grande utilização é o RSA.
   a) A segurança do algoritmo baseia-se na execução de operações de difusão e mistura dos dados com a chave?
      i) [0,1] ☐ Concordo ☐ Discordo
      ii) [0,4] Justifique.

5) [0,5] Assuma que se usava Kerberos para autenticar a Alice e o Bob, sendo a Alice um cliente e Bob um servidor registado no Kerberos. Apresente o protocolo que a Alice seguiria para enviar pedido M ao Bob.
   Omita da sua resposta as interações com o Saut e TGS respetivo.

Grupo V [3,3v]

Considere o seguinte sistema que está a funcionar com uma replicação baseada no protocolo de replicação com quóruns de maioria e com base nos pressupostos temporais e de faltas desse protocolo. Por simplificação o sistema replica apenas uma variável X com os valores iniciais representados abaixo.



1) [0,5] Qual é o papel da componente FE que aparece no diagrama?

2) Indique que tipo de faltas tolera.
   a) [0,2] Bizantinas dos servidores, quantas?

   b) [0,2] Silenciosas dos servidores, quantas?

   c) [0,2] Permanentes da rede impedindo o FE de comunicar com duas réplicas?

   d) [0,2] Silenciosas do FE, quantas?

3) Se o cliente pretender ler o valor de X.
   a) [0,5] Que valor vai ler? Justifique.

   b) [0,5] Poderá suceder um cliente na leitura obter o valor 200 devido a atrasos significativos da resposta da réplica 1 e 3? Justifique.

4) Assuma que o FE com pid=3 pretende efetuar uma escrita em X do valor 250.
   a) [0,5] Qual deverá ser a primeira etapa do protocolo? Justifique porquê.

   b) [0,5] Assuma que a escrita decorreu sobre o estado do sistema ilustrado na figura acima (ou seja, não aconteceram outras escritas entretanto). Indique o estado final das réplicas se na atualização a Réplica 1 estiver em falha silenciosa (as restantes réplicas estão corretas e receberam o pedido).

Réplica	X	Tag

Grupo VI [1,5v]

Um determinado web service S recebeu o seguinte pedido SOAP.

```
<?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:Header>
  <distributed-transaction-id>234
  </distributed-transaction-id>
</soap:Header>
<soap:Body xmlns:m="http://www.example.org/stock">
  <m:SetStockPrice>
    <m:StockName>IBM</m:StockName>
    <m:StockPrice>67</m:StockPrice >
  </m:SetStockPrice>
</soap:Body>

</soap:Envelope>
```

O pedido foi enviado por um cliente que está a executar uma transação distribuída, na qual S ainda não participa. Assuma que o web service S mantém o seu estado numa base de dados com suporte transacional.

1. [0,5] Indique os passos (pode ser pseudo-código) que S executa ao receber este pedido.

2. [0,5] Apresente o excerto do programa cliente até ao instante em que saiu o pedido acima. Na sua resposta, apresente apenas aquilo que a informação neste enunciado lhe permite conhecer.

3. [0,5] Algum tempo depois de responder ao pedido acima, chegou um pedido *canCommit* a S. Assuma que S respondeu *Yes*. Tal como S, os restantes participantes (assuma que são 2: S2 e S3) responderam *Yes* também. No entanto, a ligação entre S e o coordenador está com problemas e o voto de S atrasa-se para além do *timeout* usado pelo coordenador.

Apresente num diagrama a execução desde o canCommit enviado aos 3 participantes até à decisão final sair do coordenador.

Cliente	Coordenador	S	S2	S3

Grupo VII [1,5v]

1. Ao longo da cadeira estudou 3 principais tecnologias de programação distribuída: SUN RPC, Java RMI, Web Services com JAX-WS.

   Em cada um destes casos, recorreu a um serviço de nomes para programar as suas aplicações distribuídas.

   b. [0,4] Indique que serviços de nomes usou em cada um dos 3 casos.

   c. [0,4] Cada serviço de nomes referido na alínea anterior permitia a um programa cliente localizar os endereços dos serviços remotos a partir de um nome.
   Dê um exemplo de cada um destes nomes para cada serviço de nomes.

2. Em DNS, considere o nome op.cm-lisboa.pt.
   Considere um cliente ligado a uma rede local no campus do IST, configurado para usar um servidor DNS local, SNist. Este cliente pretende resolver o nome op.cm-lisboa.pt. Explique o que aconteceu em cada um dos seguintes cenários:

   a. [0,35] Pedido de resolução chegou a SNist, depois a SNpt, depois a SNcmlisboa.

   b. [0,35] Pedido foi imediatamente respondido pelo SNist.

