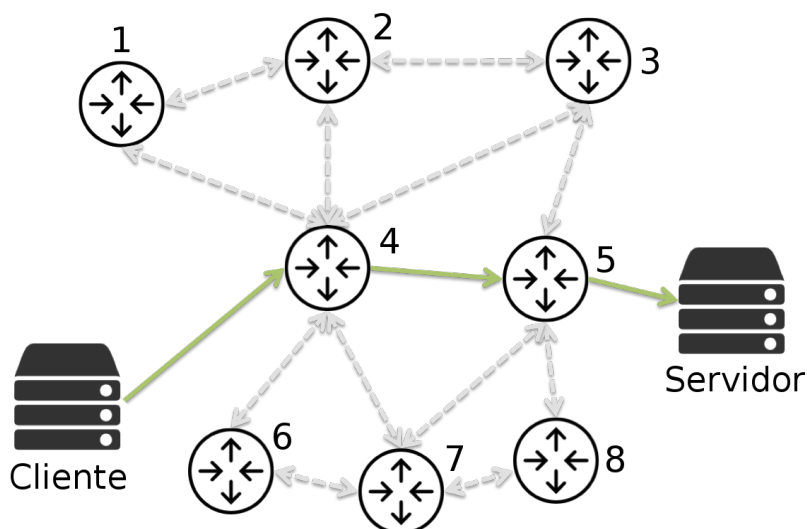


LETI/LEIC 2015-2016, Repescagem do 2º Teste de Sistemas Distribuídos 28 de junho de 2016

Responda no enunciado, usando apenas o espaço fornecido. Identifique todas as folhas.
Uma resposta errada numa escolha múltipla com N opções desconta $1/(N-1)$ do valor da pergunta.
Duração da prova: 1h30m

Grupo I [8 valores]

Considere o seguinte sistema de encomendas eletrônicas baseado na tecnologia de Web Services. O Cliente e o Servidor estão interligados através da Internet, por nós de rede em que não confiam. O fornecedor recebe encomendas através da operação `placeOrder` invocada por HTTP.



1) Um **atacante** capturou o seguinte pedido a caminho do servidor:

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
  <S:Header/>
  <S:Body>
    <ns2:placeOrder xmlns="http://tempuri.org/PurchaseOrderSchema.xsd"
xmlns:ns2="http://ws.example/">
      <ns2:order OrderDate="2016-06-17+01:00">
        <ShipTo>
          <name>Warehouse</name>
          <street>22nd st</street>
          <city>Springfield</city>
          <state>MA</state>
          <zip>1105</zip>
        </ShipTo>
        <BillTo>
          <name>Headquarters</name>
          <street>Vassar St</street>
          <city>Cambridge</city>
          <state>MA</state>
          <zip>2139</zip>
        </BillTo>
      </ns2:order>
    </ns2:placeOrder>
  </S:Body>
</S:Envelope>
```

- a) [0,6] Descreva os passos necessários para realizar um ataque que leve a encomenda a ser entregue noutra endereço postal. Indique explicitamente onde se deve posicionar o atacante.

- b) [0,5] Se o pedido estivesse a ser enviado via HTTPS em vez de HTTP, continuaria a ser possível o mesmo ataque? Responda esclarecendo se a segurança oferecida pelo HTTPS é “ponto-a-ponto” ou “extremo-a-extremo” explicando a diferença.

Não, o ataque deixaria de ser possível porque o HTTPS garante segurança extremo-a-extremo
(end-to-end), ou seja, estabelece um canal seguro entre o cliente e o servidor.
Se a segurança fosse ponto-a-ponto, a mensagem seria decifrada em cada nó no caminho.
O HTTP não garante segurança alguma.

- 2) Considere agora que tem à sua disposição **criptografia assimétrica**.

- a) [0,9] O que acrescentaria à mensagem para garantir *apenas* a **integridade**.
Use { } para representar cifra e Kpub e Kpriv para indicar chave pública e privada.
Acrescente uma legenda para outros elementos adicionais, caso sejam necessários.

```
<soap:envelope>
  <soap:header>
    <id-emissor>Cliente</id-emissor>
    <assinatura> { hash(body) } Kpriv emissor </assinatura>

  </soap:header>
  <soap:body>
    <placeOrder .../>
  </soap:body>
</soap:envelope>
```

- b) [0,9] Pretende-se agora garantir a **confidencialidade** recorrendo *apenas* a cifra assimétrica.
Represente as etiquetas XML de forma simplificada.

```
<soap:envelope>
  <soap:header>
    <id-emissor>Cliente</id-emissor>
    <cifra> { body } Kpub destinatário </cifra >
  </soap:header>

  <soap:body /> <!-- vazio -->
</soap:envelope>
```

- c) [0,5] Qual seria a distribuição de chaves que permitiria garantir o **não-repúdio** dos pedidos de encomenda?
- i) A chave pública deve ser certificada por 2 níveis hierárquicos de CA.
 - ii) A chave pública deve ser apenas do conhecimento do destinatário.
 - iii) Deve usar-se um par de chaves diferente para cada mensagem.
 - iv) A chave privada deve ser apenas do conhecimento do próprio.

- d) Pretende-se agora usar **cifra híbrida** da seguinte forma:
 $\{ M \} K1, \{ K1 \} K2$ onde M representa a mensagem, { } cifra, e K1 e K2 são chaves criptográficas.

- i) [0,4] Escolha um algoritmo de cifra para K1. Justifique.

- ii) [0,4] Escolha um algoritmo de cifra para K2. Justifique.

- iii) [0,6] O que sucede se o tamanho de M não for um múltiplo exato do tamanho do bloco da cifra?
Como trataria o último bloco?

- 3) Considere agora que está a utilizar o sistema **Kerberos V5**.

- a) [0,4] Do ponto de vista do cliente, qual é o resultado final **após** executar integralmente o protocolo Kerberos?

- b) [0,4] Que chaves devem ser partilhadas entre um cliente e o Kerberos **antes** de se poder executar o protocolo?

- c) [0,5] Seguindo o protocolo Kerberos V5, um cliente C obteve um **ticket** para sessão com o serviço S. O cliente pretende agora enviar um pedido confidencial a S. Para tal, a mensagem deve incluir:

- i) $\{ \text{pedido} \} K_{\text{pub } s}$
- ii) $\{ \text{pedido} \} K_{\text{cs}}$
- iii) $\{ \text{pedido} \} K_{\text{priv } s}$
- iv) $\{ \text{pedido} \} K_{\text{saut}}$

- d) [0,8] Usando a chave escolhida na resposta anterior, poderia garantir a **integridade** da mensagem?
Se sim, indique o nome do mecanismo e explique-o sucintamente.
Se não, indique a razão que impede a garantia.

Sim. A chave Kcs é apenas do conhecimento do cliente e do servidor (e do Kerberos).

Seria possível calcular um MAC da mensagem, que consiste num resumo (hash) da mensagem

cifrado com a chave simétrica partilhada. Uma alternativa seria usar um HMAC que faz um resumo

com um bloco secreto, correspondente à chave.

- e) [0,5] Considere o **autenticador** usado no Kerberos V5: $\text{auth}_{x,y} = \{x, T_{\text{req}}\}_{K_{x,y}}$
- x é o resumo do nome do cliente, T_{req} é um valor numérico, $K_{x,y}$ é uma chave simétrica.
 - x é um nonce, T_{req} é marca temporal para garantir frescura, $K_{x,y}$ é a chave pública de Y.
 - x é a chave do cliente, T_{req} é marca temporal para garantir frescura, $K_{x,y}$ é a chave de sessão.
 - x é o nome do cliente, T_{req} é marca temporal para garantir frescura, $K_{x,y}$ é a chave de sessão.

iv

- f) [0,6] Que implicação tem a utilização do valor **Treq** sobre os clientes e servidores envolvidos?

Implica que os relógios dos clientes e dos servidores têm que estar sincronizados entre si,

de modo a que os tickets apenas sejam usados dentro do prazo de validade estabelecido.

Grupo II [6 valores]

- 1) Considere um sistema cliente-servidor com **replicação ativa** com *quorum consensus*.
Onde: C1 – cliente com id 1; C2 – cliente com id 2; FE1 – *Front-end* de C1; FE2 – *Front-end* de C2;
R1, R2, R3 – réplicas do servidor; x uma é variável inteira.

Registaram-se as seguintes mensagens:

- C1 -> FE1 read(x)
- FE1 -> R1 read(x)
- FE1 -> R2 read(x)
- FE1 -> R3 read(x)
- R2->FE1 $x=0, <1,33>$
- R3->FE1 $x=-100, <2,31>$

- a) [0,5] O que são os valores $<... , ...>$ (exemplificados acima por $<1,33>$ e $<2,31>$)? E para que servem?

Id cliente, número de sequência.

Servem para ser possível determinar qual a resposta correta no quórum consensus,

Permitindo escolher a resposta com maior número de sequência ou, em caso de empate, o cliente com maior prioridade.

- b) [0,5] Considera que a leitura de C1 poderia ser finalizada no passo seguinte a R3->FE1? Justifique.

Para ter quórum basta receber a maioria das respostas (neste caso, 2 em 3).

Como no passo seguinte já se receberam 2 respostas,

seria possível responder ao cliente com o resultado.

c) [0,9] C1 pretende agora executar **write(x, 10)** e C2 **write(x, 20)**.

Considere que:

- A leitura anterior já terminou e nenhuma outra operação se executou entretanto.
- R2 teve uma falta silenciosa (R2 KO) e antes não tinham ocorrido outras faltas.
- A ligação de rede do FE1 a todas as réplicas tem aproximadamente o dobro da latência da ligação de rede de FE2 a todas as réplicas.

Construa uma possível sequência de mensagens até à conclusão das duas escritas, caso seja possível. Inclua os meta-dados <... , ...> relevantes na sua resposta e pode acrescentar mais • se necessário.

- **R2 KO** •
- C1 -> FE1 write(x, 10)
- C2 -> FE2 write(x, 20)
-
-
-
-
-
-
-
-
-
-
-
-
-

Seria necessário fazer um read prévio para determinar a maxtag, e depois poder fazer a escrita com maxtag+1

Os valores <...,...> deveriam ser representados

d) [0,7] O cliente C3 pretende agora executar **read(x)** após as duas escritas anteriores terem sido concluídas. Considere que R2 está recuperado (R2 OK) e que R1 teve uma falta silenciosa (R1 KO).

Construa uma possível sequência de mensagens até à conclusão da leitura, caso seja possível.

- **R2 OK** •
- **R1 KO**
- C3 -> FE3 read(x)
-
-
-
-
-
-
-
-
-

2) Considere agora um outro sistema replicado, baseado no protocolo **primary-backup** com um servidor de nomes. Onde: C – cliente; FE – front-end; S – serviço; R1 – réplica primária; R2 – réplica secundária; NS – servidor nomes. *a* é uma variável inteira.

O *front-end* resolve *sempre* o nome do servidor antes de o contactar através da função *resolve* que devolve o endereço de uma réplica (*addressOf*).

Registaram-se as seguintes mensagens:

- C -> FE read(*a*)
- R1 -> R2 ...
- FE -> NS resolve(*S*)
- NS -> FE addressOf(R1)
- FE -> R1 read(*a*)
- R1 -> FE *a*=100
- R1 -> R2 ...
- FE -> C *a*=100

a) [0,5] Qual é o conteúdo e propósito das mensagens R1 -> R2 ... ?

b) [0,6] Antes da resposta ao cliente, não deveria ter surgido R1 -> R2 read(*x*)? Considera este comportamento normal ou uma falta? Justifique.

c) [0,9] O cliente pretende agora executar **write(*a*, 300)**.

Complete uma possível sequência de mensagens sendo que R1 KO representa a falta silenciosa de R1. Complete a sequência até que o sistema recupere da falta (caso recupere).

- C -> FE write(*a*, 300) •
- FE -> NS resolve(*S*)
- NS -> FE addressOf(R1)
- FE -> R1 write(*a*, 300)
- **R1 KO**
-
-
-
-
-
-
-
-

- d) [0,4] Qual é o cálculo correto para o tempo de recuperação do serviço assumindo *primary-back com naming server*?
- i) $(P + t_{max}) + (t_{publishNS} + t_{resolveNS}) + t_{retryFE}$
 - ii) $P + t_{publishNS} + t_{retryFE}$
 - iii) $(P + t_{max}) + t_{publishNS} + t_{retryFE} + t_{response}$
 - iv) $(P + 3 * t_{max}) + (t_{publishNS} + t_{resolveNS}) + t_{retryFE}$

- e) [0,4] Qual é o ponto central de falha da solução global de *primary-backup com naming server*? Considere que cada FE corre no mesmo processo que cada C.

- f) [0,6] Que solução proporia para evitar um ponto central de falha na solução?

Grupo III [3 valores]

Numa plataforma de *crowdfunding* cada projeto proposto recebe promessas de donativos monetários vindas de diferentes interessados em apoiar o projeto. Após um projeto angariar o montante pretendido, é realizada a transferência de cada donativo para a conta do proponente do projeto.

Assuma que para um dado projeto as promessas de donativos foram recolhidas na lista *donativos*, diferentes donativos podem vir de diferentes bancos (*d.bank*). Cada banco tem um serviço remoto que oferece a operação *transfer* e mantém as suas contas num sistema de dados transacional.

```
1 boolean collectDonations(List<Donation> donations, Account proponentAccount) {
2     Object tx = openTransaction();
3     for each (Donation d in donations) {
4         d.bank.transfer(d.account, d.amount, proponentAccount, tx);
5         if (error) {
6             return error;
7         }
8     }
9     return closeTransaction(tx);
10 }
```

- 1) O programa acima poderá violar a propriedade da Atomicidade.

- a) [0,2] Defina o conceito de Atomicidade.

b) [0,5] Indique como corrigiria o programa para garantir a propriedade.

Programa as alterações indicando o número ou números das linhas a modificar ou a corrigir.

6	d. abort (tx);
7	return error;

2) [0,4] No programa não há qualquer menção explícita à utilização de mecanismos para garantir isolamento porque:

a) O isolamento é garantido pelo coordenador.

b) O isolamento é garantido pela transação local do participante.

c) O isolamento é garantido pelo 2PC que chega a uma decisão única.

d) O isolamento se necessário é garantido pela programação da sincronização no código.

b

3) O valor retornado na linha 2 (tx)

a) [0,3] Quem atribui o valor a tx?

b) [0,4] Que utilidade tem tx na sequência da transação, no caso concreto da linha 4? Justifique.

Permitirá ao participante contactar o coordenador para fazer o join à transação com o id fornecido.

c) [0,4] Que utilidade tem tx na sequência da transação, no caso concreto da linha 9. Justifique.

Permite ao coordenador identificar qual a transação a concluir e iniciar o 2PC com os participantes que

fizeram join à transação

4) Assuma que o programa é executado com 4 bancos participantes (B1, B2, B3, B4) e chega à linha 9 do programa. Indique qual a decisão tomada pelo coordenador em cada uma das seguintes situações:

a) [0,4] Após enviar canCommit(tx), o coordenador recebeu voto Yes de todos os participantes exceto do B1 que não respondeu tendo expirado o *timeout*.

i) O Coordenador envia doAbort a todos.

ii) O Coordenador envia doCommit a todos.

iii) O Coordenador envia doCommit aos participantes que votaram Yes e doAbort a B1.

iv) O Coordenador não toma nenhuma decisão neste caso ficando bloqueado.

i

b) [0,4] Após enviar canCommit(tx), o coordenador recebeu voto Yes de todos os participantes e agiu em conformidade, B1 não volta a contactar o coordenador.

i) O Coordenador envia doAbort a todos.

ii) O Coordenador envia doAbort a B1.

iii) O Coordenador mantém a transação aberta esperando que B1 recupere.

iv) O Coordenador envia uma excepção ao cliente e fecha a transação.

iii

Grupo IV [3 valores]

Considere o seguinte extrato de uma mensagem SOAP:

```
<soap:Body>
  <m:GetPrice xmlns:m="http://www.w3schools.com/prices">
    <m:Item>Apples</m:Item>
  </m:GetPrice>
</soap:Body>
```

- 1) [0,4] O URI `http://www.w3schools.com/prices` indicado neste pacote SOAP serve para:
- Localizar o WSDL do serviço.
 - Identificar um *namespace*.
 - Não é um *namespace* porque é uma mensagem SOAP e não um documento XML.
 - Localizar um *namespace*.

- 2) [0,4] Considere o seguinte binding em Java RMI e o nome `"//xpto.jogox"`

```
Jogo j = (DeckofCards) Naming.lookup("//xpto.jogox");
```

- É um URL que localiza diretamente o objeto servidor
- O nome identifica o objeto no RMI registry local e permite obter a sua referência remota
- O nome é local à máquina virtual onde está a correr o servidor
- O nome é puro e pode estar localizado em qualquer RMI registry

O seguinte excerto faz parte da página de informação do Fénix. A informação apresentada deve ser percebida tendo em conta o que aprendeu na cadeira de Sistemas Distribuídos.

Sistema de Autenticação Centralizada

O sistema de autenticação centralizada do IST inclui:

O diretório central do IST através do [protocolo LDAP](#);

O sistema de autenticação [Kerberos](#);

- 3) Um serviço de diretório é diferente de um serviço de nomes
- a) [0,5] Indique claramente a principal diferença entre um serviço de diretório e um serviço de nomes.

Um serviço de nomes tem como objetivo traduzir um nome num nome/ identificador de outro espaço de nomes. Um serviço de diretório para além da função de tradução de nomes permite obter informação sobre diversos atributos do objeto, tendo para tal um esquema de dados associado.

- b) [0,5] A que se refere o protocolo LDAP da página do IST? Explique claramente o que deverá conter este diretório. Procure ilustrar com a sua informação como utente do IST.

O LDAP é um serviço de diretório dos utilizadores de um sistema informático. Normalmente contém a informação dos utentes, endereço de email, telefone, categoria, sala de trabalho, etc. No caso do IST tem, entre outros, número de aluno, nome, email, curso, ano. (Atenção: O LDAP não tem as notas nem as informações do Fénix, como também não tem as informações de segurança como palavras-chave que estão no Kerberos.)

c) No seu projeto usou também um serviço de diretório

i) [0,3] Qual a principal vantagem que obteve da sua utilização. Justifique.

Utilizou-se o UDDI que teve como principal vantagem ter um nome para um serviço e
traduzir em tempo de execução esse nome no URL. No caso concreto da replicação permitia
substituir o servidor mantendo o mesmo nome do serviço.

ii) [0,5] Procure evidenciar com 2 exemplos que outras funções poderia obter desse diretório que não fosse a mera tradução do nome do serviço.

O UDDI poderia permitir obter os serviços de entidades a partir de um atributo, por exemplo,
serviços de empresas transportadoras, ou empresas transportadoras de uma dada região.
Poderia também armazenar os certificados X509 de cada entidade. Poderia guardar a lista de endereços
de várias réplicas para otimizar a mudança em protocolos de tolerância a faltas.

4) [0,4] LDAP e certificados digitais

a) O diretório pode ter os certificados digitais X509 dos utilizadores.

b) Não pode colocar certificados no diretório porque existe a possibilidade de ataque de “*man-in-the-middle*”.

c) O LDAP não resulta da evolução do X500 pelo que não consegue armazenar certificados X509 que apenas podem existir nesse diretório.

d) O LDAP tem os certificados porque é uma *Certification Authority* (neste caso do IST).

a
