LEIC/LETI – 2014/15, 2º Teste de Sistemas Distribuídos, 16 de Junho de 2015

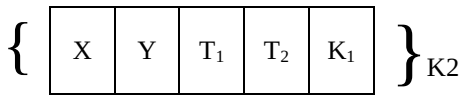
Responda no enunciado, apenas no espaço fornecido. Identifique todas as folhas. Duração: 1h30m

Grupo I [8,5v]

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) [0,8] 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:



   Explique para a chave K_1:
   i) [0,3] A função desta chave no protocolo.

   ii) [0,3] Quando é gerada?

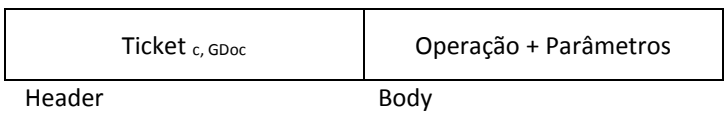
   iii) [0,3] Onde deve ser guardada?

   c) Explique para a chave K_2:
   i) [0,3] A função desta chave no protocolo.

   ii) [0,3] Quando é gerada?

   iii) [0,3] Onde deve ser guardada?

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



a) [0,7] A invocação representada pode ser alvo de um *replay attack*. Explique como se materializa este ataque.

b) [0,7] O que deveria fazer para evitar o ataque referido na alínea anterior? Considere que o atacante tem a possibilidade de escutar as mensagens e repeti-las por completo

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

a) [0,6] Escolha um protocolo de cifra. Justifique a escolha.

b) [0,6] Como faria a distribuição da chave de forma segura utilizando o mínimo de recursos?

c) Pretende-se usar uma cifra contínua (*stream*).

i) [0,6] Qual a vantagem? Justifique.

ii) [0,6] ”Um protocolo do tipo stream obriga a partilhar mais informação pelos utilizadores do canal”. Explique esta afirmação e indique qual a informação e porquê.

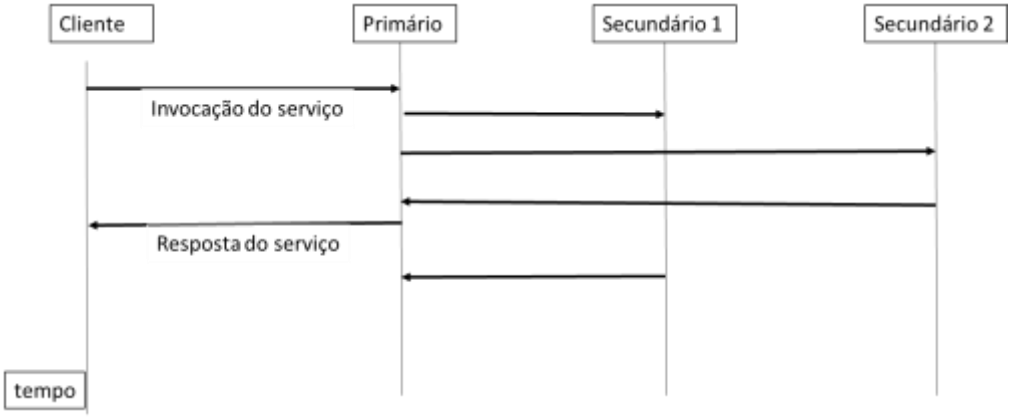
4) Existe a preocupação de, em relação aos documentos enviados na invocação dos serviços, garantir que são **íntegros, autenticados e não repudiáveis**.

a) [0,7] 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) [0,7] A validação da assinatura pode ser sujeita a várias ataques. Identifique claramente um, mostrando como materializa.

c) [0,7] Como poderia evitar o ataque que indicou na alínea anterior?

Grupo II [4,4v]



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 T_{max} 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) [0,6] Explique o que é uma falta silenciosa.

   b) [0,8] Exemplifique porque tolera 2 faltas.

2) Como existem 3 réplicas, o protocolo tolera também 1 falta bizantina.
   a) [0,3] Concordo ☐ Discordo ☐
   b) [0,5] Justifique a sua escolha.

3) Uma importante característica de avaliação dos protocolos é o incremento de tempo na resposta ao cliente.
   a) [0,8] 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

   b) [0,7] Compare a resposta anterior com o *primary backup* exposto nas aulas teóricas e explique a diferença.

c) [0,7] Vê alguma vantagem neste protocolo? Justifique.

Grupo III [3v]

Considere um sistema de compras online. 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) [0,8v] 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) Da resposta dada à alínea anterior, indique:
   a) [0,5v] Quais linhas são invocações diretas sobre o coordenador da transação distribuída?
   b) [0,5v] Quais linhas são invocações diretas sobre os participantes?

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. O protocolo 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) [0,4v] 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) [0,4v] Após enviar canCommit(tx), o coordenador recebeu voto Yes de todos os participantes exceto do E, cuja resposta não chegou ao coordenador ao fim do *timeout* definido por este.

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.

c) [0,4v] 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 IV [4,1v]

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) [0,7v] Sob a forma de um diagrama, resuma o modelo de dados do UDDI que o código acima reflete. Apresente os conceitos e as relações entre estes.

2.2. [0,7v] 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, instanciando o modelo de dados que apresentou antes.

2.3. [0,7v] 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) [0,7v] 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.

i) [0,6v] Detalhe agora a sua resposta anterior sabendo que a resolução foi feita em modo recursivo.

b) [0,7v] 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 2 situações distintas que possam 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.