LEIC/LETI, 2014/15, Repescagem do 2º Teste de Sistemas Distribuídos
30 de Junho de 2015

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

Grupo I [7,5v]

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) [0,3] A cifra que é executada neste campo é, na sua opinião:

   ☐ Simétrica ☐ Assimétrica ☐ Híbrida

   b) [0,7] Indique quais os requisitos de segurança que este campo assegura no protocolo, justificando cada um.

   c) [0,6] 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) [0,6] Qual a função deste campo?

   b) [0,6] 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) [0,2] São todas diferentes? Sim ou Não?

   b) [0,7] Se sim justifique porquê, senão indique quais as que são idênticas.

   c) [0,7] Na receção da mensagem, quais as chaves que o Bob já deveria ter e quais deverá obter para executar o protocolo?

   d) [0,8] Este protocolo pode ser alvo de um ataque de man-in-the middle? Se não porquê, se sim como se efectua.

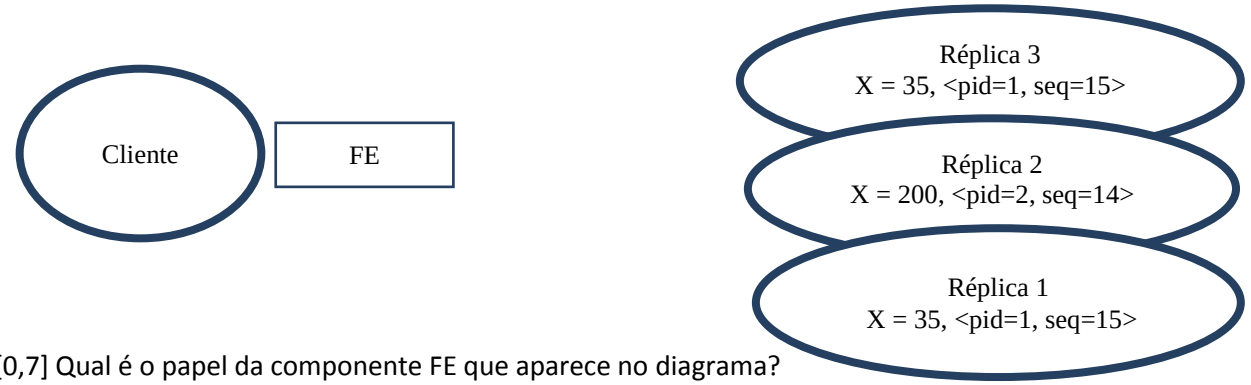
4) Um algoritmo de cifra assimétrica de grande utilização é o RSA.
   a) A segurança do algoritmo baseia-se na execução de operações de difusão e mistura dos dados com a chave?
      i) [0,3] ☐ Concordo ☐ Discordo
      ii) [0,5] Justifique.

   b) [0,7] Este algoritmo poderia ser usado na cifra do campo $\{M\}_{K4}$? Indique uma vantagem ou uma desvantagem relativamente a usar AES.

5) [0,8] 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 II [6,5v]

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) [0,7] Qual é o papel da componente FE que aparece no diagrama?

2) Indique que tipo de faltas tolera.
   a) [0,3] Bizantinas dos servidores, quantas?

   b) [0,3] Silenciosas dos servidores, quantas?

   c) [0,3] Permanentes da rede impedindo o FE de comunicar com duas réplicas?

   d) [0,3] Silenciosas do FE, quantas?

3) Se o cliente pretender ler o valor de X.
   a) [0,7] Que valor vai ler? Justifique.

   b) [0,7] 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) [0,8] Qual deverá ser a primeira etapa do protocolo? Justifique porquê.

   b) [0,8] 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

5) Considerando o mesmo caso da alínea 4 em que pretende escrever em X 250 mas que, para além da Réplica 1 estar em falta de paragem, o pedido de escrita ainda não tiver chegado à Réplica 3 devido a um atraso considerável na rede (ou seja, a única réplica que recebeu o novo valor escrito é a Réplica 2).

   a) [0,7] Enquanto este estado se mantiver, o FE do cliente considera que a escrita se efectuou ou não? Justifique.

   b) [0,9] Enquanto este estado se mantiver, as leituras que aconteçam podem devolver valores diferentes. Explique que valores são esses.

Grupo III [3v]

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. [0,7] Indique os passos (pode ser pseudo-código) que S executa ao receber este pedido.

2. [0,8] 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. [0,7] Algum tempo depois de responder ao pedido acima, chegou um pedido *canCommit* a S. Indique 2 situações concretas que podem levar S a responder *No*.

4. [0,8] Pelo contrário, assuma agora 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 IV [3v]

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.
   a. [0,7] Indique que serviços de nomes usou em cada um dos 3 casos.

   b. [0,7] 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.

   c. Entre os 3 nomes apresentados acima, indique um que seja:
      i. [0,2] Impuro.

      ii. [0,2] Heterogéneo.

      iii. [0,2] De âmbito local a uma máquina apenas.

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. [0,5] Pedido de resolução chegou a SNist, depois a SNpt, depois a SNcmlisboa.

   b. [0,5] Pedido foi imediatamente respondido pelo SNist.
