LETI 2019/20, 2º Teste de Sistemas Distribuídos
17 de janeiro de 2020

Identifique todas as folhas. Responda no enunciado, usando apenas o espaço fornecido.

Nas perguntas de escolha múltipla assinaladas com EM existe apenas uma resposta certa.
Uma resposta errada desconta 1/(N-1) do valor de uma pergunta com N opções de resposta.

Duração da prova: **1h15m**

Grupo I [3 valores]

1) EM [0,6v] Qual é a sequência correta num sistema, de acordo com o modelo apresentado nas aulas?
   A. Falta, Erro, Falha.
   B. Falha, Erro, Falta.
   C. Erro, Falta, Falha.
   D. Falta, Falha, Erro.

2) Considere o contexto do seu **telefone móvel** (*smartphone*) pessoal.

   a) [0,7v] Dê um exemplo de uma falta **interna** e **temporária**. Justifique.

   b) [1,0v] A falta que descreveu anteriormente pode ser melhor modelada como uma falta **silenciosa** ou como uma falta **arbitrária**? Justifique, explicando a diferença de modelo entre estas duas.

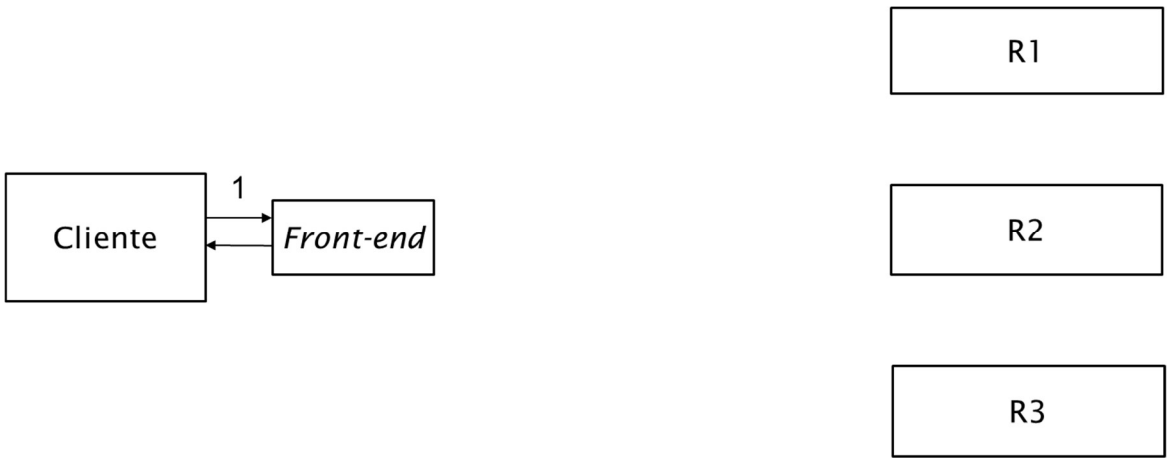
   c) [0,7v] Qual a métrica que faz mais sentido usar para o telefone móvel: **MTTF** ou **MTBF**? Justifique.

Grupo II [9 valores]

Considere um sistema replicado em que um cliente (C) comunica através de um *Front-end* (FE) com um conjunto de servidores: R1, R2, R3.

1) Nesta questão, o protocolo usado é o ***primary-backup***.
   O primário contacta diretamente os secundários e envia a cada secundário em cada período P uma mensagem de *"batimento cardíaco"*.

   a) [1,4v] Considere que o cliente quer escrever na variável inteira X o valor 227 – *write(X,227)*.
   Complete o diagrama abaixo indicando as mensagens através de **setas numeradas** e acrescente a **legenda** necessária para cada número. Não necessita de representar os "batimentos cardíacos".



1 – O cliente envia *write(X,227)* para o FE (*Front-End*)

2 –

   b) EM [0,8v] Quantas faltas de servidores pode este sistema tolerar?
   A. zero B. uma C. duas D. três

c) [0,8v] Qual será o tempo máximo de recuperação, **tRecuperação**, do sistema em caso de falha de R1? Defina todas as parcelas que terão que ser somadas.

tRecuperação = tMaxEscolha +
P - período das mensagens de "batimento cardíaco"
tMaxEscolha - o tempo máximo de escolha do novo primário

2) Considere agora que o protocolo usado é o ***quorum consensus*** e que o sistema é assíncrono.

a) EM [0,6v] No modelo de sistema assíncrono:

A. Pode considerar-se a existência de um limite superior no tempo de latência da rede.
B. É possível a deteção remota de falhas por paragem (*crash failures*).
C. Os pressupostos aproximam-se mais da realidade do que num sistema síncrono, em particular se houver uma partição na rede.
D. Nenhuma das anteriores é verdadeira.

b) Considere que há dois clientes – C1 e C2 – com os respetivos front-ends – FE1, FE2 – e que *Y* é uma variável inteira. Registaram-se as seguintes mensagens:

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

i) [0,8] O que são os valores <… , …> (exemplificados acima por <1,33> e <2,31>)? E para que servem?

ii) [0,8] Considera que a leitura de C1 poderia ser finalizada no passo seguinte a R3->FE1? Justifique.

iii) [0,8] *"Uma operação de escrita no quorum consensus implica uma leitura prévia"*.
Concorda com esta afirmação? Justifique.

3) Considere agora que o protocolo usado é o ***gossip*** e que o sistema é assíncrono.
Neste caso, existem vários clientes: C1, C2, C3. Cada cliente tem o seu *front-end*.

A aplicação guarda o conjunto de convidados para um evento, por exemplo, uma festa de aniversário.
As operações suportadas são *add()* que acrescenta um nome ao conjunto; *belongsTo()* que diz se um elemento pertence ao conjunto; e *count()* que devolve o número de elementos do conjunto.

Considere a seguinte sequência que foi executada:
C1 contacta R2 e faz *add("José")*;
C2 contacta R3 e faz *add("Maria")*;
C3 contacta R3 e faz *add("Salvador")*;

a) [0,7v] Indique o *timestamp* vetorial de cada réplica, assumindo que não houve ainda nenhuma ronda de *gossip*.

TS_R1 =
TS_R2 =
TS_R3 =

b) EM [0,7v] Assumindo que não houve *gossip*, se o cliente 2 contactar R2 e executar *belongsTo("Maria")* qual a resposta que obtém?

A. Falso, porque "Maria" está apenas no conjunto de R3.
B. Falso, porque R2 contacta R1 e não encontra "Maria".
C. Verdadeiro, porque R2 contacta R3 e encontra "Maria".
D. Verdadeiro, porque a atualização foi propagada de R3 para R2 logo no momento da inserção.

c) [1,0v] Pode acontecer C2 contactar R3 e ver um resultado e depois contactar R1 e ver um resultado diferente? Considera a resposta anterior uma anomalia? Se sim, proponha um mecanismo para impedir esta anomalia. Se não considera uma anomalia, justifique porquê.

É uma anomalia / Não é uma anomalia.

d) [0,6v] Assuma agora que decorreu uma ronda de *gossip* bidireccional entre R1 e R2, seguida de outra ronda entre R2 e R3. Quais são os vetores após a conclusão das duas rondas?

TS_R1 =
TS_R2 =
TS_R3 =

Grupo III – Segurança [8 valores]

1) O **P4E1** (*Privacy for Everyone*) é um mecanismo usado pela empresa SmallCo para cifrar e decifrar dados, oferecendo **confidencialidade** na comunicação de dados. É usado para a troca de mensagens de correio eletrónico entre um **remetente** e um **destinatário**.

a) [0,7v] No regulamento da empresa *SmallCo* consta o seguinte:
"Todos os colaboradores devem usar P4E1 na comunicação por correio eletrónico."
Trata-se de uma afirmação de política ou um mecanismo de segurança? Justifique.

b) [0,7v] Assuma que o sistema é usado para discutir detalhes sobre produtos inovadores que estão a ser desenvolvidos pela empresa, num mercado competitivo. Identifique e descreva um **adversário** do ponto de vista da segurança informática.

c) Considere agora os detalhes sobre o funcionamento do P4E1:

- Envio:
  - O P4E1 comprime os dados com o algoritmo ZIP para reduzir o volume de dados;
  - Depois cria uma chave de sessão;
  - A chave de sessão é cifrada com a chave pública do destinatário;
  - A mensagem é cifrada com a chave de sessão.
- Receção:
  - O destinatário usa a chave X para recuperar a chave de sessão;
  - A mensagem é decifrada com a chave Y;
  - O P4E1 descomprime os dados.

i) [1,0v] A que chaves se referem as incógnitas X e Y ?

X
Y

ii) [1,2v] *"O P4E1 é um sistema de cifra híbrida"*. Concorda com a afirmação?
Justifique explicando do que se trata este tipo de cifra e o que motiva a sua utilização.

Sim/não.

iii) [1,2v] Proponha algoritmos criptográficos concretos para as operações em que estão envolvidas as chaves X e Y. Justifique as suas escolhas.

Algoritmo onde é usado X:
Algoritmo onde é usado Y:

iv) [0,8v] *"A cifra com a chave de sessão deve usar o modo CBC para …"*.
Complete a frase e justifique a utilidade do **CBC**.

v) [1,5v] Estenda o protocolo do P4E1 com uma forma de **autenticar o remetente** e de garantir a **integridade** da mensagem. Desenhe um diagrama com legenda para especificar o que é enviado do remetente para o destinatário na versão estendida do protocolo.
.

vi) [0,9v] A extensão que propôs na alínea anterior é vulnerável a um ataque por repetição? Justifique a sua resposta, explicando em que consiste este ataque.

É vulnerável / Não é vulnerável.