DI/FCT/UNL
Mestrado Integrado em Engenharia Informática

Confiabilidade de Sistemas Distribuídos, 2º Semestre, 2016/2017

PROVA DE EXAME (24/Julho/2017)
PARTE I (Parte Sem Consulta)

Questão 1

Na abordagem de construção de um sistema replicado (do tipo *replicated key-value store*) com tolerância a intrusões, estas que podem injetar comportamento incorreto originando falhas por paragem de réplicas ou indução de comportamento bizantino nas mesmas. Para tal vai desenhar-se um serviço de recuperação de intrusões, podendo seguir-se uma abordagem reativa ou uma abordagem pró-ativa.

a) Em que consiste cada uma das abordagens ? Na sua explicação indique vantagens ou desvantagens em cada uma das aproximações.
b) Argumente sobre dois cenários (tipologia de sistema a partir do seu modelo, modelo de consistência, características de concepção ou condições de operação) em que escolheria num caso uma abordagem de recuperação reativa e noutro caso recuperação pró-ativa.

Questão 2

a) Na variante do algoritmo Paxos, com um servidor primário (conhecido por Multi-Paxos), é possível que uma operação do primário não seja aceite? Apresente um *run* que mostre a situação e argumente sobre a necessidade deste comportamento.
b) Qual a diferença na definição das seguintes propriedades, na abordagem de um sistema SMR para consenso determinístico (com base no algoritmo PAXOS) e no caso do algoritmo BEN-OR.
Propriedades: (a) Validade; (b) Acordo; (c) Terminação; (d) Integridade

Questão 3

a) No protocolo ABD Tolerante a Falhas Bizantinas, as mensagens têm de incluir um *nonce*. Supondo que em vez de *nonces* se usassem *timestamps* que vantagens e desvantagens teria essa aproximação ? Justifique.
b) Comente a seguinte afirmação: "o algoritmo ABD com quóruns bizantinos permite uma melhor escalabilidade quando comparado com o algoritmo PBFT", indicando justificadamente se a mesma é verdade ou falsa.
Sugestão: analise o número de operações de escrita que cada réplica deve processar, considerando o total de operações de escrita que têm que ser executas pelos clientes, em cada caso.

Questão 4

Considere o sistema e protocolo Bitcoin / Blockchain.

a) Se não se gerasse um novo par de chaves sempre que se pretende receber uma transferência isso colocaria em perigo a correção do sistema? Justifique.
b) Como e com que verificações é possível evitar fraudes por "*double spending*" ou "*double-transfer*" de bitcoins (usando que um utilizador incorreto faça cópias de *bitcoins* antes obtidas e válidas em diferentes transações)

Questão 5

Considere o sistema Depsky

a) Que vantagens vê na utilização da técnica de *secret-sharing* face a uma solução em que os utilizadores obtivessem chaves criptográficas simétricas a partir de um sistema de autenticação e distribuição de chaves ? Justifique.
b) Em que contexto e que vantagens tem neste sistema a utilização da técnica de *erasure-coding*? Justifique.

Confiabilidade de Sistemas Distribuídos, 2º Semestre, 2015/2016

PROVA DE EXAME (24/Julho/2017)
PARTE II (Parte Com Consulta)

Questão 6

Considere o algoritmo de consenso probabilístico Ben-Or.

a) Apresente o *run* duma ronda em que no fim da ronda não existe uma maior probabilidade de se chegar ao consenso do que no início.
b) Apresente um *run* que mostre que um nó bizantino pode levar a um comportamento incorreto do algoritmo.

Questão 7

No algoritmo ABD para tolerar falhas bizantinas é possível usar quóruns de maiores dimensões, que se intersectem num maior número de réplicas, de forma a evitar que os clientes tenham de assinar as suas escritas (e que estas assinaturas sejam mantidas e retornadas nas leituras). Seria possível usar a mesma aproximação no algoritmo PBFT (aumentando simplesmente a dimensão dos quóruns)? Justifique.

Questão 8

Considere o sistema Byzantium. Será que para executar uma transação com apenas uma operação de leitura é necessário efetuar a operação de *begin transaction* recorrendo a uma operação PBFT (completando o protocolo de consenso) ou seria suficiente executar a operação de leitura imediatamente nas diferentes réplicas, desde que f+1 réplicas devolvessem o mesmo resultado.

Questão 9

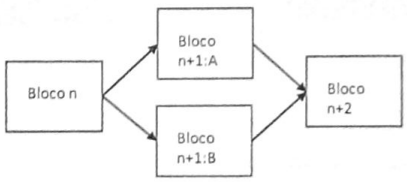
Considere o sistema CryptDB.

a) Porque é que o sistema permite suportar múltiplos utilizadores autenticados de forma independente permitindo aos mesmos realizarem operações SQL sobre os mesmos dados cifrados e a mesma base de dados, mesmo que não conheçam as chaves usadas para cifrar ou decifrar de acordo com o modelo de "*onion-encryption*" usado ? Justifique
b) Um dos problemas em aberto que pode ser levantado face à solução é que à medida que se vão suportando *queries*, a confidencialidade dos dados no servidor vai ficando mais vulnerável". Concorda ou não com esta afirmação? Justifique.

Questão 10. Das seguintes duas questões (10-A ou 10B) escolha opcionalmente uma para responder.

> Questão 10-A: Sistema Bitcoin / Blockchain

No protocolo Bitcoin podem ser gerados dois novos blocos concorrentemente. Nesta situação, um dos blocos acabará por ser descartado quando são gerados os próximos blocos, porque a blockchain é uma sequência de blocos. Para evitar que o trabalho efetuado na criação dum novo bloco se perde, suponha que se pretende alterar o protocolo Bitcoin para permitir que um bloco tenha como antecessores dois blocos, como apresentado na figura.



a) Indique que verificações é que seriam necessárias efetuar quando se juntam dois blocos concorrentes num novo bloco, como no caso apresentado na figura.
b) Considere o caso geral, em que um novo bloco poderia unificar não apenas dois blocos concorrentes mas várias sequências de blocos concorrentes. Neste caso, discuta se, aquando da criação dum novo bloco os *miners* deveriam tentar unificar todas as sequências concorrentes conhecidas ou se deveriam contribuir para aumentar uma das sequências.

> Questão 10-B: Plataformas para computação confiável, TPMs e TEEs

Considere o contexto da sua implementação do trabalho prático nº 2, nomeadamente o modelo e arquitetura do sistema. De modo a suportar um modelo de adversário com hipóteses estendidas, vai iterar a sua solução de modo a desenvolvê-la para servidores equipados com módulos TPM 2.0 e processadores Intel com suporte SGX. Neste reenquadramento pretende tirar partido deste tipo de suporte na sua nova infraestrutura.

a) Dada a solução atual (considerada como solução de partida) que iteração no modelo de adversário e no modelo de confiabilidade podia ser suportado (para além do seu modelo atual) ? Justifique.
b) Apresente uma arquitetura da solução que proporia implementar referindo particularmente que componentes do seu sistema seriam redesenhados/reimplementados e como tirariam partido da nova solução de modo a endereçar o novo modelo de adversário e o novo modelo de confiabilidade, nomeadamente:
   (b1) Que componente ou componentes tirariam partido do suporte TPM 2.0, como e para quê ?
   (b2) Que componente ou componentes tirariam partido do suporte SGX, como e para quê ?