DI/FCT/UNL
Mestrado Integrado em Engenharia Informática

Confiabilidade de Sistemas Distribuídos
2º Semestre, 2015/2016

Teste de Avaliação nº 2 (4/Junho/2016)
Componente: Teste da Parte Teórica

A preencher pelo aluno

Nº Aluno	
Nome	
Nº Total de Páginas com respostas (sem contar com capa): (deve numerar todas as páginas)	

A preencher pelos docentes

Avaliação da parte I – Sem Consulta							
Avaliação da parte II – Com Consulta							

DI/FCT/UNL
Mestrado Integrado em Engenharia Informática

Confiabilidade de Sistemas Distribuídos
2º Semestre, 2015/2016
Teste de Avaliação nº 2 (4/Junho/2016)
Componente: Teste da Parte Teórica
PARTE I (Sem Consulta, 1h00 m)

De entre as seguintes cinco questões pode descartar uma, escolhendo apenas quatro para responder.

Questão 1

Para lidar com intrusões num sistema computacional é possível usar técnicas de *pro-active recovery* ou de *reactive recovery*.

a) Discuta as vantagens e desvantagens de ambas as soluções num contexto de um sistema tolerante a falhas bizantinas.
b) A partir das vantagens e desvantagens que apresentou em a) diga como se repercutem as mesmas na decisão de optar com vantagens por uma ou outra técnica no contexto do projeto realizado, partindo dos requisitos e pressupostos de implementação.

Questão 2

Considere o contexto do estudo de sistemas de detecção de intrusões (ou IDS – *Intrusion Detection Sytems*)

a) Qual a diferença entre um sistema de detecção de intrusões que se baseia no princípio da detecção anómala e um sistema que se baseia em assinaturas ou heurísticas de intrusão.
b) Em que tipo de ambientes de computação distribuída considera mais vantajosa uma ou outra aproximação ?
c) Que motivações e vantagens encontra na adopção de arquiteturas de sistemas de detecção de intrusões do tipo "*Distributed and Hybrid Detection Systems*"? Que componentes podem integrar este tipo de arquiteturas e qual o objetivo de cada um desses componentes ?

Questão 3

Considere o contexto do sistema COCA, apresentado como caso representativo de uma proposta que utiliza técnicas de replicação combinadas com um mecanismo de *pro-active recovery*. Qual a motivação e objetivo da utilização do mecanismo criptográfico de assinaturas de limiar (ou *threshold signatures*) no contexto desse sistema? Na sua explicação refira que vantagens encontra na utilização desse mecanismo de segurança.

Questão 4

O sistema Byzantium permite replicar, de forma tolerante a falhas Bizantinas, um sistema de base de dados relacional. No contexto deste trabalho, responda às seguintes perguntas.
a) Explique porque é que apenas é necessário executar as operações de *begin* e *commit* (ou *rollback*) como operações BFT?
b) Explique porque é que é necessário executar as operações de leitura em mais do que uma réplica.

Questão 5

No contexto do estudo do sistema DepSky, responda às seguintes perguntas.
a) Explique o objetivo da utilização de *Erasure Codes* neste sistema.
Indique qual a técnica alternativa que poderia ter sido usada e qual a vantagem da utilização de *Erasure Codes*.
b) Explique o objetivo da utilização de técnicas de *Secret Sharing* neste sistema e que vantagens encontra na sua utilização

PARTE II (Com Consulta): 1h00 m

Deve responder obrigatoriamente à questão 1 e optar por uma das seguintes questões desta PARTE II

Questão 1 (30 min)

O sistema PBFT inclui um mecanismo de *pro-active-recovery*, apresentado nas aulas teóricas. Discuta em que condições o mecanismo é interessante na prática e como é que se pode construir um sistema a partir dessas condições.
Tente estruturar a sua resposta tendo em conta as condições, critérios de concepção e aspetos de concepção relevantes no sistema PBFT para implementação desse tipo de solução. Na organização da sua resposta, tente delinear uma argumentação cobrindo, entre outros pontos que considere relevantes, os seguintes (como secções da sua argumentação):

- Efetividade do mecanismo na solução PBFT de acordo com os seus objetivos;
- Hipótese ou delimitação do modelo de adversário para que a recuperação seja efetiva e garanta as propriedades do consenso;
- Em que medida as garantias anteriores podem ou não colocar em causa a disponibilidade permanente de serviço neste tipo de solução;
- Enriquecimentos da solução para mitigar as hipóteses de um adversário bizantino
- Aspetos limitativos da solução, por exemplo, quantas réplicas podem estar a recuperar ao mesmo tempo e porquê.

Questão 2 (30 min)

Considere o contexto de salvaguarda da privacidade de dados em bases de dados remotas bem como o contexto de operação e utilização do sistema CryptDB.

a) De acordo com o seu estudo, elabore sobre cinco potenciais limitações da solução que considere poderem ser insuficiências face a tipologias de ataques à privacidade de operações e dados críticos mantidos na base de dados. Para o efeito, pode considerar o alargamento do modelo de adversário tal como definido pelos autores da solução.

b) Tendo em conta uma das limitações discutidas em a), apresente uma possível abordagem de solução para ultrapassar a mesma.

Questão 3 (30 min)

Considere a funcionalidade base (ou os serviços de segurança de base) de módulos de hardware do tipo TPM (considerando como referência módulos TPMv2.0).

Considere também o contexto de desenvolvimento do seu trabalho (projeto) e a identificação da base de confiança da sua solução (face ao modelo de falhas e adversário considerados).

Supondo que iria realizar o *deployment* da sua solução em servidores que possuem módulos do tipo TPM (ex., TPM 2.0), responda às seguintes questões:

a) Como se proporia utilizar e tirar partido desse suporte a partir da funcionalidade TPM? (Pode partir da ideia de eventual extensão da sua solução para esse efeito).
b) Que benefícios poderia extrair desse tipo de suporte e que confiabilidade acrescida isso asseguraria à sua solução.
c) Identificados os componentes da base de confiança da sua solução, refira-se às limitações da funcionalidade providenciada por um módulo TPM para cobrir todos os requisitos dessa base de confiança.

QUESTÃO SOBRE IMPLEMENTAÇÂO DO PROJETO (Com Consulta, 30m)

Questão TP (30 min): Questão com consulta, sobre enquadramento do projeto prático. Deve responder com base no código desenvolvido, com consulta e em articulação com o template-relatório correspondente à submissão do mesmo.

Considere o desenvolvimento do seu projeto e o código de detalhe da implementação.

a) Explique em que consiste, como foi implementado e onde está codificado o mecanismo de *pro-active-recovery*, referindo em que se baseia o mesmo e como opera no caso de uma réplica ter sido atacada por um adversário bizantino.

   Na sua resposta deve referenciar a sua resposta concretamente e rigorosamente a partir do código desenvolvido, clarificando de forma detalhada onde e como está implementada a solução (tendo por base os *packages*, classes – linhas de código, métodos, APIs, funcionalidade utilizada da biblioteca BFTsmart, ou outros aspectos relevantes que clarifiquem a sua resposta a partir do código da sua implementação).

b) Dada a sua implementação e sua avaliação experimental, apresente uma análise crítica sobre pressupostos, garantias ou limitações da mesma, em relação a conseguir por um lado assegurar a operação correta do sistema tolerando intrusões bizantinas ou ataques de disponibilidade às réplicas (que provoquem a sua paragem) e ao mesmo tempo garantir disponibilidade permanente de serviço de forma transparente para os clientes.