DI/FCT/UNL
Mestrado Integrado em Engenharia Informática

Confiabilidade de Sistemas Distribuídos
2º Semestre, 2015/2016

Teste sobre o Trabalho Prático (9/Abri/2016)

Considere o contexto relacionado com os requisitos, especificações e estado de desenvolvimento do trabalho prático nº 1 que entregou para avaliação, para endereçar e responder às seguintes questões.

1) Implementação da PARTE I

a) Aponte na seguinte tabela (colocando S (SIM), N (NÃO) ou P (PARCIALMENTE) nas duas colunas indicadas para esse efeito), sobre a completude de requisitos e sobre a robustez testada da implementação e correção com que avalia a sua implementação.

	Aspetos de implementação	Implementação com completude das especificações pedidas no enunciado	Robustez e correção de funcionamento, aferida com base em testes que realizei da implementação feita e que foi entregue
A	A aplicação cliente *SIFTClient* que permite ter acesso ao servidor via *sockets* TCP (ou via JAVA-RMI). A aplicação base segue assim o modelo básico Cliente/Servidor permitindo que o servidor execute *standalone* numa máquina remota suportando um número não limitado de clientes que podem executar em máquinas diferentes na Internet.		
B	Cada cliente identifica-se e autentica-se com um ID único (ex., uma *string*), e pode ter várias diretorias partilhadas com diferentes utilizadores. Estes clientes mantêm os ficheiros sincronizados entre si através do uso de um servidor comum.		
C	Implementei o mecanismo de partilha e controlo de acessos, de acordo com a especificado no enunciado. Para cada uma das diretorias, o cliente periodicamente obtém automaticamente a lista dos ficheiros presentes na sua diretoria local e do servidor a lista dos ficheiros desta diretoria e copia (sincroniza) de/para o servidor os ficheiros cuja data de alteração for posterior à dos ficheiros que se encontram no cliente/servidor		

D	A implementação do SIFTBox atende concorrentemente vários clientes que com ele interagem (atendendo invocações remotas em paralelo)		
E	A implementação consegue suportar uma estrutura hierárquica de ficheiros (diretorias de ficheiros, subdiretorias, etc.), sincronizando essa hierarquia e, especificamente, os ficheiros alterados		
F	Garante-se que o ficheiro que determina a política de controlo de acessos definida por cada utilizador para efeitos de controlo de partilha, nunca pode ser modificado (escrita) a não ser pelo dono dos ficheiros		

b) Clarifique os aspectos (A, B, C, ... G), explicando no caso de ter indicado P (Parcialmente), justificando a sua solução. Se indicou em todos os casos SIM (completamente) ou NÃO (Não Implementado), não necessita de justificar.

c) Apresente os aspectos que considera valorativos da sua implementação, no que diz respeito a extensões de requisitos, optimizações ou aspectos a destacar na sua implementação da FASE 1.

2) Implementação da PARTE II

a) Apresente agora na seguinte tabela a caracterização da sua implementação da Fase 2

	Aspetos de implementação	Indique: SIM, NÃO, PARCIALMENTE	Robustez, aferida com base em testes que realizei da implementação feita e que foi entregue
A	Procedi à integração do suporte *BFTSmart*, garantindo assim que a implementação do componente do lado do servidor permite replicar os ficheiros, mantendo toda a funcionalidade da implementação da Fase I		
B	A implementação anterior (A) foi testada executando o componente *BFTsmart* em nós distribuídos em computadores diferentes, embora não possa suportar clientes em todos os nós		
C	A implementação anterior (A) foi testada executando o componente *BFTsmart* em nós distribuídos em computadores diferentes, e é possível ter vários clientes executando concorrentemente utilizando diversos servidores, mantendo os clientes toda a funcionalidade tal como indicada no quadro da Fase 1		

b) Clarifique os aspectos (A, B, C), explicando no caso de ter indicado P (Parcialmente). Se indicou em todos os casos SIM (completamente) ou NÃO (Não Implementado), não necessita de justificar.

c) Apresente os aspectos que considera valorativos da sua implementação, no que diz respeito a extensões de requisitos, optimizações ou aspectos a destacar na sua implementação da FASE 2.

3) Questões sobre o trabalho

a) Indique no código de implementação do seu trabalho, que estrutura(s) de dado(s) utiliza para escrever/ler os objetos que são replicados na solução BFTsmart, indicando de forma rigorosa a partir do seu código as estruturas de dados envolvidas quando as operações (*read* / *write*) são submetidas ao protocolo de consenso.

b) Diga quais as diferenças entre o modelo de adversário que considera na proteção do canal que suporta as operações do(s) cliente(s) e servidor(es), o modelo de adversário no canal de comunicação entre as instâncias – réplicas BFTsmart, tal como a sua solução utiliza a solução BFTsmart, bem como o modelo de ataques por intrusão que são suportados. Nota: tenha em conta na sua resposta a proteção implícita do BFTsmart que está subjacente à própria implementação do protocolo de consenso e deve definir os modelos de adversário de forma rigorosa, a partir das propriedades de segurança que são asseguradas.

c) Indique na sua implementação, quando e onde (indicando no código) um servidor (réplica) tem a certeza que um objecto já foi replicado no número de réplicas correto, assegurando consenso mesmo face a potenciais atacantes ou falhas bizantinos. Deve indicar o local do código em que a replicação foi concluída corretamente após o protocolo de consenso.

d) Suponha que um atacante atuando por intrusão num servidor onde executa a sua implementação decide injetar código malicioso, modificando a implementação de forma a impedir a execução correta do protocolo de replicação (SMR) subjacente à implementação BFTsmart. Que efeito isso poderia ter no contexto da sua aplicação ? Justifique.

e) Suponha que um atacante atuando por intrusão num servidor onde executa a sua implementação decide injetar código malicioso, modificando incorretamente a implementação do código do servidor que implementa a funcionalidade da aplicação (atendimento dos clientes e funcionalidade executada pelo servidor RMI/SSL SIFTBox). Que efeito isso teria? Justifique.

f) Uma das possibilidades para optimizar e melhorar o desempenho de uma implementação como a que fez no TP1, seria tentar implementar uma estratégia do tipo FAST READS (com *One-Trip-Time*). Como poderia implementar esta estratégia tendo em conta que está a usar a biblioteca BFTsmart e de acordo com a discussão teórica dessa opção num protocolo com as características do protocolo PAXOS (subjacente à implementação no suporet BFTsmart) ? O que poderia esperar deste tipo de implementação e como se proporia endereçar esta estratégia?