Sistema de Ficheiros com Garantia de Integridade

Sistemas de Elevada Confiabilidade

Grupo 10

Rui Peres 73831
Carlos Macedo73919
João Costa 85652

Limitações

Devido à formação tardia do nosso grupo, os requisitos do sistema de ficheiros foram reduzidos de forma a respeitar a entrega do projeto. Portanto, a interface deste sistema de ficheiros sofreu as seguintes alterações: Na escrita no ficheiro do cliente apenas é passado como argumento o conteudo do ficheiro, e no caso da leitura apenas se indica o id do ficheiro pretendido. No lado do servidor, só existem blocos K, sendo a função *put_h* não utilizada. No entanto é enviado juntamente com o projeto duas classes que implementam a funcionalidade de escrita e leitura nos blocos K e H, mas que não nos foi possivel integrá-la com o resto do projeto.

Interação Cliente/Servidor

A interação entre o cliente e servidor foi contruida usando RMI, devido à sua facilidade de implementação. A interface remota é constituida pelas funções do serviddor de blocos (*get*, *put_k*, *put_h*).

Implementação

Cada cliente é representado por uma biblioteca (FSLibrary), e no servidor de blocos, cada ficheiro é guardado apenas num unico bloco, usando a função remota put_k. O id de cada bloco é um resumo da chave publica do cliente que identifica não só cada bloco mas também identifica o ficheiro do cliente e o proprio cliente, facilitando assim todas as verificações necesssarias.

Confiabilidade

A arquitetura usada neste sistema de ficheiros, garante autenticação, não-repudiação, integridade e segurança dos dados. No caso de autenticação e não-repudiação, quem escreveu num ficheiro não pode negar ter sido ele próprio a escrever, pois a função *put_k* antes de inserir informação num bloco, verifica se a assinatura recebida é válida. No caso de integridade da informação, quando um cliente pretende ler um ficheiro, os dados devolvidos pelo servidor correspondem aos dados originais, pois a função *get* verifica a assinatura do bloco pretendido antes de enviar o conteudo desse bloco. E no caso da segurança, o conteudo de um ficheiro é encriptado antes de ser enviado para o servidor (na função *FS_write*) com a chave privada do dono do ficheiro, e desencriptado quando um cliente pretende ler desse ficheiro (na função *FS_read*) . Isto garante que não seja revelada a informção dos ficheiros a quem o dono do ficehiro não tenha dado permissões de leitura, ou seja que tenha acesso não tenha a chave publica correpondente.