

**Relatório de Segurança e Confiabilidade**

Trabalho 2

Engenharia Informática

Grupo 51

João David n49448

João Marques n49038

Luís Moreira n49531

Índice

[Concretização 2](#_Toc7295797)

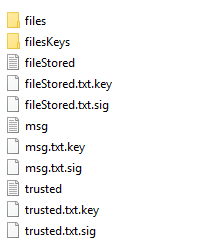
[Problemas encontrados 3](#_Toc7295798)

[Segurança 3](#_Toc7295799)

# Concretização

…

Cada utilizador registado tem uma pasta como seu nome com a seguinte estrutura no seu interior:



# Problemas encontrados

…

# Segurança

O ficheiro que contém a informação de login dos utilizadores (usersInfo.txt) encontra-se protegido com um MAC, este MAC é posteriormente guardado num ficheiro userInfoMAC.txt, sempre que o programa UserManager pretenda alterar algo no ficheiro, para efeitos de criação, actualização e remoção de utilizador, é previamente verificada a integridade do ficheiro, se for detectada alguma alteração maliciosa, a aplicação lança uma excepção e pára a execução, caso contrário altera o conteúdo do ficheiro e volta a calcular um novo MAC.

No caso do MsgFileServer, vai haver verificação da integridade deste ficheiro ao ligar o servidor, e sempre que um utilizador conectado faça uma operação remota, caso seja detectada uma alteração maliciosa, vai ser lançada uma excepção e abortada a execução.

Sempre que um utilizador envia um ficheiro F para o servidor (independentemente do tipo de ficheiro), este é cifrado com uma chave simétrica K AES gerada aleatoriamente, a chave K é posteriormente cifrada com a chave pública do servidor e armazenada dentro de um ficheiro com o mesmo nome que o ficheiro enviado pelo utilizador com a extensão “.key”, o ficheiro que contém a chave não pode ser guardado na mesma pasta que o ficheiro F, visto que se tal acontecesse, o utilizador conseguiria transferir este ficheiro, por isso, é guardado na pasta “fileKeys”, enquanto que o ficheiro F fica na pasta “files”. Existe uma pasta “filesKeys” para cada utilizador, tal como acontece para a pasta “files”.

Após o ficheiro ter sido cifrado e armazenado com sucesso, é adicionado ao ficheiro de controlo “fileStored.txt”, o nome do ficheiro que acabou de ser guardado pelo utilizador. Desta forma, mesmo que o ficheiro F e o ficheiro que contem a chave que foi usada para cifrar forem apagados, o servidor tem forma de saber que era suposto estar la o ficheiro e lançar excepção referente a violação de integridade dos ficheiro. Sem o “fileStored.txt” a fazer este controlo, um hacker poderia apagar os ficheiros de todos os utilizadores, e o servidor nunca saberia dessa ocorrência.

Relativamente aos ficheiros de controlo do utilizador (trusted.txt, msg.txt e fileStored.txt), estes são gerados sempre que um utilizador é criado, são assinados (a assinatura é guardada num outro ficheiro com a extensão “.sig”), e são depois cifrados de forma idêntica aos ficheiros enviados pelo utilizador (como explicado anteriormente).

Sempre que uma operação remota evocada por um utilizador necessite de recorrer a estes ficheiros, estes são previamente decifrados e é verificada a assinatura. Caso seja necessário serem alterados, por exemplo na adição de uma nova mensagem, ou utilizador amigo, são novamente assinados e cifrados.

Ao iniciar o servidor, a integridade de todos os ficheiros são verificada, nomeadamente os ficheiros dos utilizador, os seus ficheiros de controlo e o ficheiro que contém a informação de login de todos os utilizadores registados no servidor.

Cada utilizador registado tem uma pasta como seu nome com a seguinte estrutura no seu interior: