**Segurança Informática**

**Grupo 25**

**Entrega 2**

**Gonçalo Ventura Cruz 54959**

**Renato Ramires 54974**

**Tiago Teodoro 54984**

**Objetivos concretizados**

O programa foi testado exaustivamente pelo grupo e o grupo acredita que todos os requisitos descritos no enunciado foram cumpridos, não se verificando qualquer falha ou mau funcionamento do sistema.

Em relação às funcionalidades concluídas na primeira etapa do projeto o grupo melhorou alguns aspectos que não considerou 100% correctos, tais como:

* Quando o cliente lista os seus ficheiros e estes não existem o servidor apresenta uma mensagem ao indicar o mesmo, ao invés de uma lista vazia;
* A *sandbox* é agora mais restritiva sendo que o utilizador apenas poderá manipular ficheiros na pasta bin/files no diretório do projeto, restringindo assim o acesso de um utilizador ao sistema de ficheiros;
* Foi também retirada a opção de *write* às *propertyPermissions* no diretório *user*.*dir*, visto que esta não era necessária;
* A procura por um utilizador no ficheiro das passwords é também agora mais eficiente, visto que esta é interrompida assim que o ciclo encontra o utilizador pretendido;

No que respeita as novas funcionalidades, todas foram realizadas com sucesso, enumerando:

* Na criação de um novo utilizador o servidor cria um par de chaves RSA para o utilizador e guarda-o numa keystore privada do utilizador;
* No envio de ficheiros para o servidor, o servidor cria a assinatura digital do ficheiro com a chave privada do cliente, guarda ambos o ficheiro e a assinatura e envia para o cliente a assinatura;
* Na receção de ficheiros do servidor, o cliente recebe agora para além do ficheiro também a sua assinatura digital;
* O servidor tem agora a opção de criar uma assinatura digital através de uma síntese de ficheiro enviada pelo cliente;
* O servidor tem também a capacidade de verificar a assinatura digital de um ficheiro;
* As passwords são armazenadas no servidor protegidas por um hash com salt, de forma a que não sejam comprometidas pela visualização de terceiros;
* A integridade do ficheiro das passwords é agora também protegida por um MAC que é verificado frequentemente e encerra o programa assim que deteta que o ficheiro possa ter sido corrompido;
* A autenticidade e confidencialidade na comunicação são assegurados por canais seguros utilizando o protoco TLS/SSL;
* Os ficheiros armazenados no fornecedor são também protegidos da observação do seu conteúdo por terceiros através de criptografia hibrida com base nas chaves assimétricas do cliente;

**Problemas encontrados**

Não existiram nenhuns problemas de que o grupo tenha conhecimento ou que gostaria de realçar.

**Segurança da aplicação**

A aplicação implementa vários mecanismos de segurança, tais como:

* Comunicação segura através do protocolo TLS/SSL;
* Sínteses simples de texto com o algoritmo SHA;
* Sínteses seguras que utilizam uma chave secreta partilhada combinando o HMac com o SHA;
* Proteção da confidencialidade através de criptografia hibrida e assimétrica que utilizam os algoritmos AES e RSA;
* Criação de assinaturas digitais de ficheiros, permitindo garantir a autenticidade do seu autor.

O grupo espera que não existam quaisquer fraquezas associadas à segurança da aplicação e pensa que quaisquer melhorias que poderiam ser feitas à aplicação não seriam associadas ao tema deste trabalho mas sim a outros temas de segurança.