PBOX Client

MIECT

Mário Liberato, Jorge Oliveira

PBOX Client

DETI

MIECT

Mário Liberato, Jorge Oliveira
(nmec) mario@ua.pt, (84983) jorge.am.oliveira@ua.pt

21-04-2017

Resumo

Resumo do trabalho.....

Conteúdo

Capítulo 1

Introdução

O tema do seguinte trabalho é a criação de um cliente onde é possível realizar certas operações com um servidor. Este servidor contém um modelo de "boxes"com (ou sem) segurança onde é possível deixar comentário de curto comprimento para consulta do seu criador. Todos os utilizadores têm possibilidade de criar uma **caixa** com um certo nome, também sendo possível existir uma chave pública ao servidor. Além da criação de caixas, é possível **listar**,**receber** e **enviar** documentos para uma certa caixa.

O documento encontra-se dividido em cinco capítulos. Sendo que no **??** é apresentada a metodologia seguida para a criação do cliente e as funções do mesmo. No **??** são apresentados os resultados óbtidos no cliente e na **??** a análise dos resultados. Finalmente, no **??** são apresentadas as conclusões do trabalho.

Capítulo 2

Metodologia

Para a criação do cliente foi utilizada essencialmente programação em Python (para isto foi utilizado o PyCharm) e a interface do cliente foi adaptada em web.

Antes da realização de qualquer programação o grupo reuniu-se e discutiu como deveria ser realizado o trabalho, que caminhos seguir até ao produto final. Foi optado ser realizado uma pequena base do cliente onde seria possível listar as caixas disponíveis no servidor, de seguida foram sendo adicionadas as funções de criar caixas, dar segurança às mesma, receber e enviar documentos às caixas. Finalmente a interface gráfica e apelativa ao utilizador foi introduzida. Antes de prosseguir em cada etapa foram realizados testes para determinar erros ou falhas (em especial de segurança) para ser obtida uma experiência sem problemas.

2.1 Descrição do cliente

Nesta secção são apresentadas as funções do cliente e como foram adaptadas para o mesmo.

2.1.1 Listagem

É pretendido listar todas as caixas seguras existentes através do envio de uma mensagem **LIST**, sendo que o servidor responderá com todas caixas seguras existentes e, caso existam, as chaves públicas das mesmas.

2.1.2 Criação de caixas

Esta função permite criar uma caixa através do envio da mensagem **CREATE**, a mensagem deverá conter o nome da caixa e o seu timestamp. Ainda é possível ter uma chave pública e assinatura da mensagem. Para oferecer segurança, se for optado por fornecer uma chave pública essa caixa só pode ser modificada com mensagens seguras.

2.1.3 Envio de documentos para uma caixa

Para o envio de documentos para uma caixa é necessário o envio da mensagem **PUT** contendo um texto

2.1.4 Receção de um documento

A receção de um documento de uma certa caixa é realizado através da mensagem GET contendo o seu timestamp.

2.1.5 Segurança

Para segurança são utilizadas cifras Assimétricas **rsa!** (**rsa!**) com chaves de 2048 bits que são enviadas em formato **pem!** (**pem!**). Também são necessárias Assinaturas com chaves **rsa!** e síntesessha1, sendo isto visível na criação de caixas e obtenção dos documentos numa caixa.

2.1.6 Interface Web

Foi optado realizar uma interface web para o cliente ser mais apelativo e de uso simples ao utilizador

Capítulo 3

Resultados

Descreve os resultados obtidos.

Capítulo 4

Análise

Analisa os resultados.

Capítulo 5

Conclusões

Apresenta conclusões.

Contribuições dos autores

Acrónimos

RSA Rivest Shamir Adleman, Iniciais dos apelidos dos fundadores deste algorítmo de criptografia

PEM Privacy-enhanced Electronic Mail