Changes on the Final Project

Luís Silva, lfssilva@ua.pt, 76585

February 4, 2018

1 Introduction

I really liked to score 20 in a class at least one time while in the University, this is my best shot at it. Fingers crossed.

2 Changes

2.1 Protection of User Keys in Client

Previously I did not implement any kind of security in the RSA keys generated by the program for the client to use. It was obviously a flaw because even the key is on the client computer the bare minimum was to protect the private key with a password. For the protection of the private RSA key of the client I encrypted with AES with a key of 256 bit, this key was generated using an password facilitated by the user and the use of *PBKDF2* a key derivation function.

2.2 Add another key agreement protocol

Before the user could not choose the Key Agreement protocol with the server. Now we can choose both from Elliptic Curves and the Standard Diffie Hellman .

2.3 Add another method for encryption of messages

Before the user could not choose the symmetric encryption protocol for the messages. Now we can choose both from the standard AES or TripleDES.

2.4 Overall cleanup and bug finding

Very fun project to do, definitely a field in which I would like to dig deeper