Relatório da atividade 1 – Comunicação segura

Disciplina: Segurança e auditoria de sistemas (EC38D)

Formato: ADNP (Atividade didáticas não presenciais)

Professor(a): Lucas Dias Hiera Sampaio

Turma: C81 / Engenharia da computação

O código foi desenvolvido com base em na linguagem Java, utilizando a IDE (Integrated Development Environment) Netbeans 8.2 e os testes de sniffers de rede feito com o programa Wireshark 3.2.5.

O método de criptografia utilizado foi o RSA. Neste sistema de transmissão segura de dados, a chave é pública e é diferente da chave de decriptação que é privada.

Tela de celular com texto preto sobre fundo branco

Descrição gerada automaticamente

O projeto tem 4 classes, são elas Server, Usuario, message e RSACripto.

A classe Server será realizada a conexão, por meio de um socket, com a classe Usuario. Além disso, será responsável pelo envio de mensagens criptografadas para o servidor (Server). A classe automaticamente, assim que iniciada, abre um socket na porta TCP 8002.

A classe Usuario é responsável pelo envio de mensagens do usuário para o servidor. Utilizada também para criptografar e decifrar mensagens e gerar as chaves necessárias durante o processo.

A classe RSACripto é responsável pela criação do RSA.

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente- Coleta de dados no Wireshark

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

Uma imagem contendo screenshot, texto

Descrição gerada automaticamente

Referências:

<http://docs.oracle.com/javase/7/docs/technotes/guides/security/crypto/CryptoSpec.html>

<http://www.javamex.com/tutorials/cryptography/rsa_encryption.shtml>