Engenharia de Computadores e Telemática

47232

Segurança

Sistema seguro de transmissão de mensagens instantâneas

Autor:
Rafael Almeida

Número de estudante:
68486

November 6, 2016

Contents

0.1 Introdução

O presente relatório elaborou-se no âmbito da unidade curricular de Segurança com vista a apresentar e explicar as soluções encontradas em resposta aos objectivos impostos para a realização do projecto que consiste no desenvolvimento de um sistema de troca de mensagens entre utilizadores sendo que estas não deverão de forma alguma ser acessíveis a sujeitos que não os intervenientes na conversação.

Este tipo de sistemas são atualmente muito utilizados sendo fundamental garantir a segurança e privacidade dos seus utilizadores de forma a detetar e evitar o sucesso de qualquer tipo de actividade ilícita.

Relativamente a redes P2P existem vários aspectos a serem explorados dependendo do tipo de aplicação e do grau de segurança exigido. Os principais aspectos investigados são os seguintes:

- Disponibilidade - garantir que uma entidade está disponível quando necessário.
- Autenticidade - determinar se alguém é realmente quem diz ser.
- Confidencialidade - proteger dados contra entidades não autorizadas.
- Integridade - proteger dados contra corrupção.
- Autorização - restringir o acesso de uma entidade a recursos do sistema.
- Reputação - determinar o grau de confiança das demais entidades intervenientes no sistema.
- Anonimidade - manter desconhecida a identidade de uma entidade.
- Negabilidade - ofuscar dados de forma a proteger a entidade que os detém de ser responsabilizada.
- Não-repúdio - evitar que uma entidade negue responsabilidade por ação executada.

Em resposta ao problema proposto implementaram-se métodos de negociação de chaves entre os utilizadores e também algoritmos de cifra/decifra de forma a possibilitar a cifragem/decifragem das mensagens enviadas e recebidas pelos diferentes utilizadores do sistema.

Sendo este o principal objectivo do projecto, existem outras funcionalidades implementadas tais como a hierarquização de utilizadores, impossibilitando assim que a um utilizador de hierarquia inferior não seja dada a possibilidade de envio de mensagens para um utilizador hierarquicamente superior, entre outras.

0.2 Estado de Arte

Actualmente a segurança de redes informáticos é indispensável embora em alguns casos muito dispendiosa dependendo do nível de segurança exigida por cada tipo de rede. Particularmente em redes P2P estas dividem-se em várias categorias, tais como:

- Partilha de arquivos
- Sistemas de armazenamento de arquivos em rede
- Computação distribuída
- Comunicação entre utilizadores

Relativamente à última categoria apresentada, existe ainda uma subcategoria referente a aplicações de mensagens instantâneas sendo nesta subcategoria que o presente projecto incide. Algumas das aplicações deste tipo existentes no mercado atual são como por exemplo o MSN Messenger [MSN, 2006] e o Yahoo Messenger [Yahoo, 2006].

0.3 Funcionamento

O sistema propriamente dito funciona com base na troca de mensagens entre cliente-servidor e servidor-cliente. Assim sendo, cada utilizador do sistema estabelece inicialmente uma sessão TCP com o servidor de forma a possibilitar a troca de mensagens entres estas entidades. Após o estabelecimento de uma sessão TCP com o servidor atribui-se a cada utilizador a possibilidade de requerer a lista de utilizadores com os quais é possível estabelecer comunicação e assim salvaguardar informações relevantes relativas a cada cliente listado.

Nesta fase, com o envio de uma mensagem com características específicas para o efeito, efectua-se o pedido de conexão para outro cliente. Uma vez enviado o pedido inicia-se a troca de mensagens entre os clientes intervenientes na comunicação, sendo que por cada mensagem enviada inicia-se um processo de negociação de chaves referentes à mensagem enviada e também de um segredo que permitirá avaliar a autenticidade dos intervenientes da sessão. Para além das mensagens anteriormente referidas, existem ainda mensagens de término de sessão e confirmação de receção.

0.4 Solução

A solução encontrada baseia-se na estrutura de cada tipo de mensagem existente no sistema, sendo usado objetos json para agrupar os diferentes atributos que constituem cada mensagem enviada.

Tipo de mensagens possíveis e principais atributos:

- "Connect":

  Tipo de mensagem utilizada para comunicar a presença de um novo utilizador ao servidor, partilhando com este informações como:

  - "phase": fase do processo de comunicação
  - "name": nome do utilizador
  - "id": identificador do utilizador
  - "ciphers": modo de cifra utilizada
  - "data":
    - "level": nível hierárquico do utilizador
    - "public": chave pública única proprietária de cada utilizador

- "List":

  Tipo de mensagem utilizada para requisitar a lista de utilizadores com os quais se pode estabelecer sessão, ao servidor.

  - "data":
    - "id": número de identificação do utilizador sobre o qual se pretende obter informação, em caso de ser null servidor lista todos os utilizadores com os quais é possível estabelecer sessão.
    - "level": nível hierárquico do utilizador que envia o pedido.

- "Client-connect":

  Tipo de mensagem necessária para estabelecer uma sessão com outro cliente

  - "src": identificador do emissor da mensagem
  - "dst": identificador do receptor da mensagem
  - "phase": fase do processo de comunicação
  - "ciphers": modo de cifra utilizada

  - "data":
    - "AESKeyEncrypted": chaves simétrica gerada e cifrada com chaves pública do cliente emissor
    - "A","p","g": valores gerados para o processo diffie-hellman

- "Client-com":

  Tipo de mensagem necessária para efectuar a comunicação propriamente dita entre dois utilizadores

  - "src": identificador do emissor da mensagem
  - "dst": identificador do receptor da mensagem
  - "data":
    - "AESKeyEncrypted": chaves simétrica gerada e cifrada com chaves pública do cliente emissor.
    - "encryptedText": mensagem propriamente dita e segredo do emissor devidamente encriptados com chaves simétrica negociada no campo anterior.

- "Ack":

  Tipo de mensagem enviada pelo receptor para informar o emissor da receção da mensagem correspondente.

  - "src": identificador do emissor da mensagem
  - "dst": identificador do receptor da mensagem
  - "data": campo com informação diversa de acordo ao tipo de mensagem ao qual a mensagem ack se refere

- "Client-disconnect":

  Tipo de mensagem enviada com o intuito de terminar sessão entre dois utilizadores.

  - "src": identificador do emissor da mensagem
  - "dst": identificador do receptor da mensagem
  - "data": campo com informação auxiliar

Aquando a recepção de uma mensagem efectua-se de imediato a análise da informação existente na mesma e consequente actualização das variáveis internas de cada cliente seguido do envio da mensagem de confirmação de receção.

A Figura 1 apresenta todo o processo necessário para que comunicação de texto em claro seja possível entre dois clientes e também alguma informação relevante que caracteriza cada fase do processo.

Relativamente ao processo de cifragem e decifragem de informação para que esta não seja compreendida por qualquer entidade externa com acesso ao servidor usou-se algoritmos de cifra por blocos, assimétrica (RSA) e simétrica (AES). Para o algoritmo simétrico recorreu-se a um gerador de chaves simétricas de 128 bits sendo que a chaves resultante é utilizada para cifrar/decifrar a mensagem (texto em claro) enviada/recebida de forma a gerar o criptograma partindo do texto em claro (cifragem) ou gerar o texto em claro partindo do criptograma (decifragem). Para que que este processo seja possível é necessário que anteriormente ocorra um processo de negociação da chave simétrica gerada. Uma vez que esta não pode ser interceptada no servidor, empregou-se o referido processo de cifragem/decifragem desta chave simétrica com a chaves pública/privada gerada para o algoritmo de cifra assimétrico (RSA). Este processo garante a Confidencialidade das mensagens enviadas entre utilizadores.

Para garantir a Autenticidade da comunicação usou-se um método de criptografia específico para troca de chaves desenvolvido por Whitfield Diffie e Martin Hellman. Após o processo de negociação das variáveis envolvidas no processo de cálculo do segredo e aquando da receção de um criptograma por parte do receptor e após a decifragem deste criptograma efectua-se a comparação do segredo transmitido e o segredo que este detém. Esta comparação , em caso de igualdade, comprova que os clientes intervenientes na sessão são realmente quem dizem ser.

A Figura 2 representa o processo de negociação e cálculo de segredo entre dois utilizadores usado neste projecto.

0.5 Interface gráfica

Para auxiliar o processo de comunicação criaram-se interfaces gráficas para gerir e controlar as ações de cada cliente.

A Figura 3 apresenta a interface de gestão de utilizadores, onde é possível especificar os atributos gerais de um novo utilizador a instânciar e também atributos do socket associado a este novo utilizador. É ainda possível visualizar os utilizadores

disponíveis no sistema.

As Figura 4 e 5 apresentam a interface de controlo de fluxo da aplicação, ou seja, é nesta fase que todo o processo de estabelecimento de sessão seguido de comunicação propriamente dita é efectuado. Todo o processo desencadeia-se com eventos despoletado pelo "click" dos diferentes componentes da interface.

- Start: instância o socket utilizado pelo cliente.
- Connect: envia uma menssagem "connect" para o servidor
- Available Users: envia uma mensagem "list" para o servidor de forma a solicitar a lista de utilizadores disponíveis
- Destination user-name: permite escolher o utilizador com o qual se pretende estabelecer uma ligação
- Send: envia mensagens "client-connect" se este cliente ainda não estabeleceu uma ligação com o destinatário e também mensagem "client-com"
- Disconnect: envia mensagem "client-disconnect" para o servidor para terminar a sessão com um determinado cliente

0.6 Conclusão

Ao término da primeira parte deste projecto e elaboração deste relatório concluiu-se que existem diversos aspectos de segurança a serem considerados em redes P2P sendo que neste apenas surgiram resoluções e tentativas de resolução para alguns aspectos necessários neste tipo de redes.

Uma vez que não se utilizaram cifras perfeitas dado que estas são pouco práticas é expectável que um ataque do tipo MitM obtenha resultados favoráveis para o atacante embora que as vulnerabilidades das cifras utilizadas não permitem a sua criptoanálise em tempo útil, em casos normais.

Assim sendo é possível afirmar que algumas das funcionalidade exigidas neste tipo de redes não foram completamente implementadas e/ou contém algumas falhas que deverão ser solucionadas em versões futuras.

0.7 Bibliografia

1. André Zúquete,Segurança em Redes Informáticas,4ª Ed.Aumentada, FCA, Lisboa.

0.8 Anexo

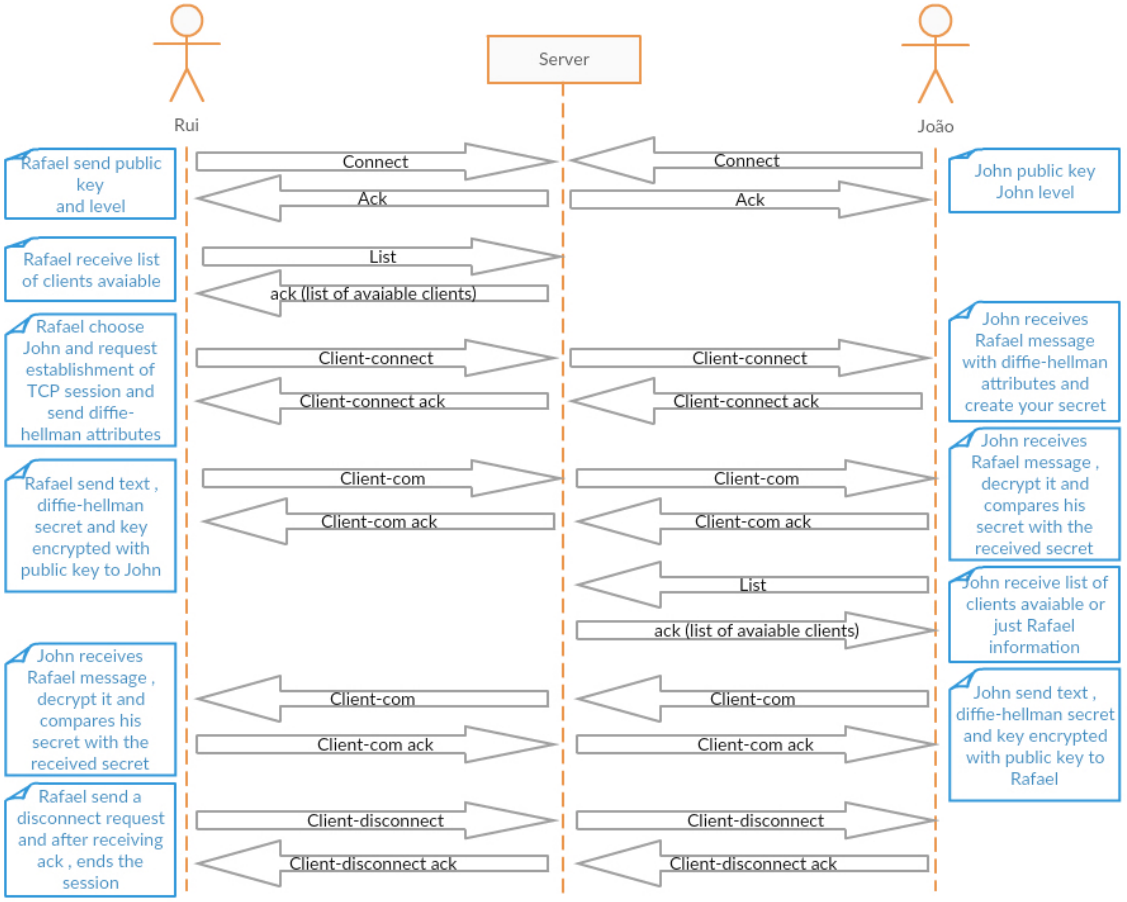

Figure 1: Diagrama de fluxo do processo de comunicação entre dois clientes

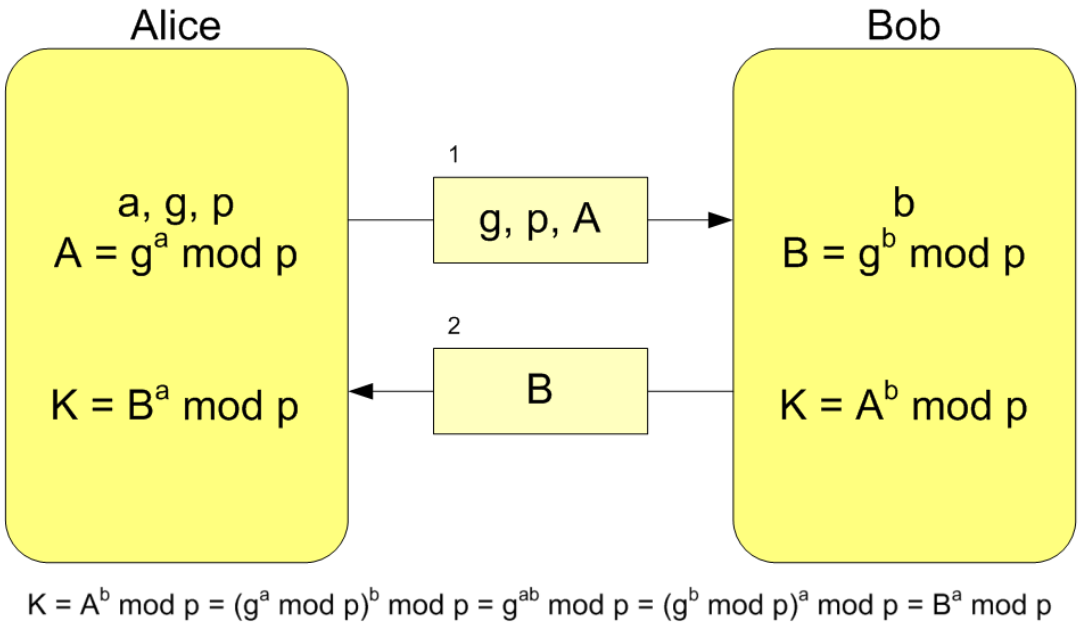

Figure 2: Processo de negociação Diffie-Hellman

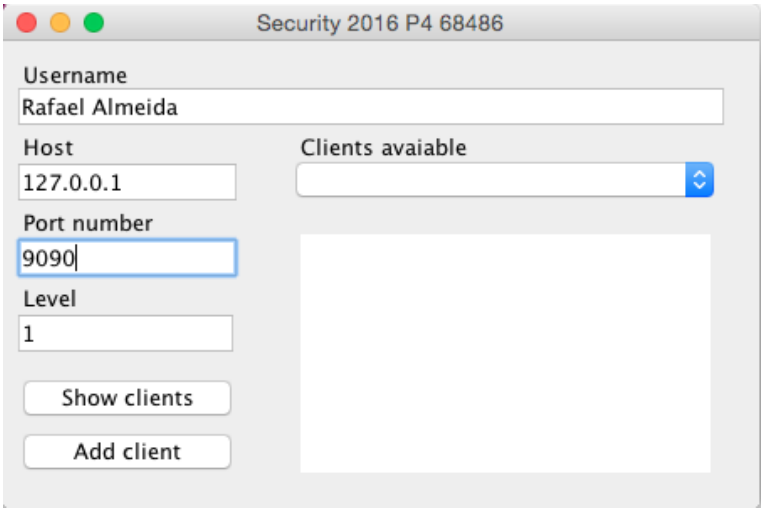

Figure 3: Interface de gestão de clientes

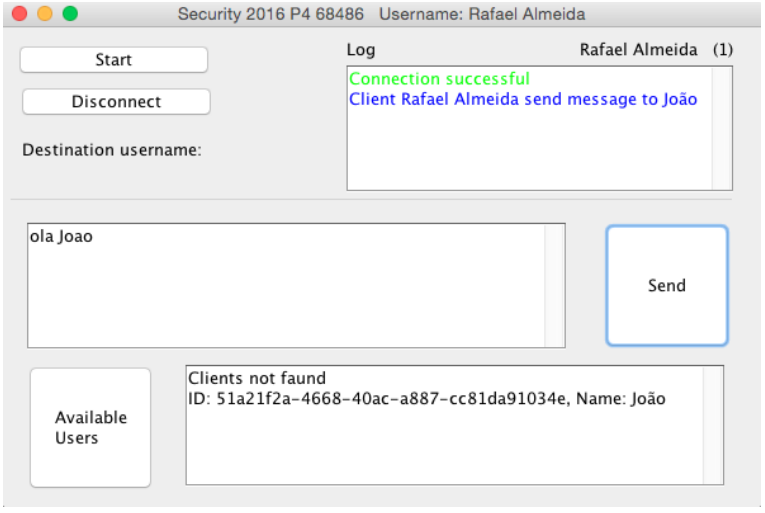

Figure 4: Interface do cliente (emissor)

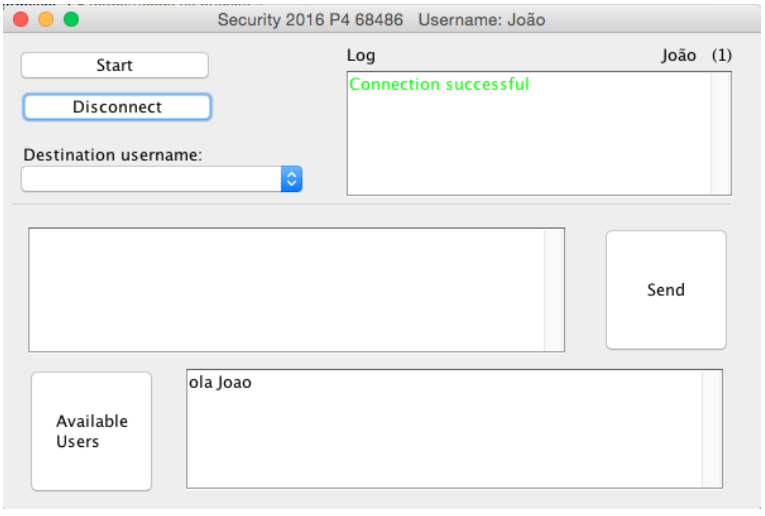

Figure 5: Interface do cliente (receptor)