Faculdade de Ciências da Universidade de Lisboa
Departamento de Informática
Mestrado em Segurança Informática

RELATÓRIO

Privacidade e Segurança dos Dados

First Part

Hélio José (Nª64417)

Matias Pickett (Nº54705)

Kevin Dos Santos (Nº64874)

Repositório GitHub: Repositório grupo 24

Professor: **Bernardo Ferreira**

1º Semestre Letivo 2024/2025

Introdução

Este relatório descreve a implementação de um sistema de chat seguro ponto-a-ponto (P2P) que utiliza criptografia Diffie-Hellman para estabelecer comunicações seguras entre pares (peers). A solução desenvolvida oferece uma interface gráfica simples para facilitar a interação dos usuários e funcionalidades de segurança que garantem a confidencialidade das mensagens trocadas.

Descrição da Solução

1. **Estrutura do Código**

A implementação é composta por duas classes principais: Peer e PeerGUI.

- Peer: Esta classe representa um par (peer) que realiza a troca de mensagens com outros peers. Cada instância de Peer possui métodos para armazenar mensagens, enviar e receber mensagens, e estabelecer chaves de criptografia.
- PeerGUI: Esta classe implementa a interface gráfica, que permite que o usuário selecione um destinatário e envie mensagens para ele. A interface exibe o histórico de mensagens de cada conversa em uma janela de chat.
- PeerHandler: Esta classe lida com a comunicação direta entre dois peers, gerenciando a troca de mensagens criptografadas.

2. **Funcionalidades Desenvolvidas**

- **Envio e Recebimento de Mensagens**: A aplicação permite que os peers enviem e recebam mensagens de texto. Cada mensagem é exibida na interface gráfica, com o histórico completo da conversa.
- **Armazenamento de Mensagens**: As mensagens trocadas entre os peers são armazenadas com uma identificação de origem ("Você:" para mensagens enviadas e o ID do remetente para mensagens recebidas). Isso permite um histórico de conversa unificado, acessível a qualquer momento.
- **Interface Gráfica**: A interface facilita o uso, permitindo ao usuário escolher o destinatário e enviar mensagens diretamente pela aplicação. A interface também exibe o histórico de conversas e atualiza os contatos disponíveis.

3. **Criptografia Diffie-Hellman**

Para garantir a segurança da comunicação, foi implementada a troca de chaves Diffie-Hellman, um protocolo de criptografia assimétrica que permite que duas partes estabeleçam uma chave secreta compartilhada sem a necessidade de trocá-la diretamente.

A chave secreta gerada com Diffie-Hellman é então utilizada para criptografar as mensagens entre os peers usando o algoritmo AES (Advanced Encryption Standard). A chave simétrica é guardada localmente e se por acaso comunicarmos com o mesmo peer numa sessão ele usa a mesma chave.

Processo de Criação da Chave:

1. Os peers trocam chaves públicas geradas com Diffie-Hellman.

2. Cada peer utiliza a chave pública do outro peer e sua chave privada para gerar uma chave secreta compartilhada.

3. Esta chave secreta é usada para criptografar e descriptografar as mensagens trocadas entre os peers.

Análise das Garantias de Segurança

1. **Confidencialidade**

- A criptografia Diffie-Hellman garante que a chave secreta para a criptografia AES é conhecida apenas pelos dois peers envolvidos na comunicação. Como a chave não é transmitida, é extremamente difícil para um atacante interceptar ou descobrir essa chave.
- A confidencialidade das mensagens é garantida pelo uso do AES, que protege o conteúdo das mensagens ao criptografá-las antes do envio.

2. **Integridade**

- Embora a criptografia Diffie-Hellman e AES protejam a confidencialidade, a implementação atual não inclui verificação de integridade explícita, como assinaturas digitais ou códigos de autenticação de mensagens (MAC).

3. **Autenticidade**

- A solução não implementa autenticação formal para verificar a identidade dos peers. O foco desta implementação é na confidencialidade das mensagens trocadas. No entanto, a falta de autenticação significa que um peer mal-intencionado poderia potencialmente se passar por outro.
- Para uma solução completa, futuras versões poderemos implementar autenticação utilizando certificados digitais ou uma infraestrutura de chave pública (PKI).

4. **Resistência a Ataques do Homem-no-Meio (MitM)**

- O protocolo Diffie-Hellman é vulnerável a ataques MitM se não houver autenticação dos pares. Na implementação atual, não há verificação da identidade dos peers. No entanto, em um ambiente controlado ou com uma camada de autenticação adicional, a resistência a esses ataques poderia ser significativamente melhorada.

Como Usar

Iniciando a Aplicação

1. Compile o projeto em sua IDE ou use o terminal para compilar os arquivos .java.
2. Execute a classe principal do programa. Uma janela gráfica será aberta.
3. Para compilar:

javac -d bin src/main/java/*.java

- Para correr:

java -cp bin main.java.Peer

- Para limpar o /bin:

rm -rf bin/*

Conclusão

A solução desenvolvida implementa um sistema de chat seguro entre pares utilizando criptografia Diffie-Hellman para garantir a confidencialidade das mensagens. A escolha do protocolo Diffie-Hellman permite que os peers gerem uma chave secreta compartilhada sem trocá-la diretamente, reduzindo o risco de interceptação da chave.

Embora a solução ofereça boas garantias de confidencialidade, ela poderia ser melhorada no que diz respeito à autenticidade e integridade das mensagens, para proteger contra ataques de MitM e manipulação de dados. Futuras melhorias poderiam incluir autenticação por certificados digitais e verificação de integridade das mensagens.

Este projeto demonstra a viabilidade de uma comunicação segura entre pares em um ambiente de chat, implementando os princípios fundamentais de criptografia de chave pública para proteger a troca de mensagens.