Documento de Funcionamento do Sistema de Comunicação Segura Cliente-Servidor com Entidade Certificadora (CA)

Introdução

Este documento descreve o funcionamento do sistema de comunicação segura entre cliente e servidor, com um foco especial na segurança provida pela Entidade Certificadora (CA). O sistema usa criptografia assimétrica (RSA) e simétrica (AES), além de um protocolo de troca de chaves (Diffie-Hellman), para garantir a confidencialidade, autenticidade e integridade das mensagens trocadas entre os clientes.

Componentes do Sistema

- Cliente
- Servidor
- Entidade Certificadora (CA)

Funcionamento Geral do Sistema

1. Estabelecimento de Conexão

Inicialização do Servidor: O servidor é iniciado e aguarda conexões na porta especificada. Ele também inicializa a CA e carrega ou cria o arquivo de chaves criptografadas.

Conexão do Cliente: O cliente se conecta ao servidor utilizando o endereço IP e porta do servidor.

2. Troca de Chaves Diffie-Hellman

Envio de Parâmetros: O servidor envia os parâmetros Diffie-Hellman (primo e gerador) para o cliente.

Geração e Troca de Chaves: Ambos, cliente e servidor, geram suas chaves públicas e privadas Diffie-Hellman.

O cliente envia sua chave pública para o servidor.

O servidor calcula a chave compartilhada e envia sua chave pública para o cliente.

O cliente também calcula a chave compartilhada.

3. Geração e Troca de Chaves RSA

Geração de Chaves RSA no Cliente: O cliente gera um par de chaves RSA (pública e privada).

Envio do Nome e Chave Pública RSA do Cliente: O cliente criptografa seu nome usando a chave simétrica compartilhada e envia para o servidor.

O cliente também envia sua chave pública RSA.

4. Certificação pela CA

Recepção e Certificação no Servidor: O servidor recebe o nome e a chave pública RSA do cliente.

O servidor gera um par de chaves RSA para o cliente e salva as chaves criptografadas.

A CA assina a chave pública do cliente, gerando um certificado.

Envio do Certificado para o Cliente: O servidor envia o certificado assinado pela CA para o cliente.

5. Comunicação Segura

Envio de Mensagens: O cliente envia mensagens criptografadas para o servidor, especificando o destinatário.

O servidor descriptografa a mensagem e verifica o destinatário.

Se o destinatário estiver conectado, o servidor reencapsula a mensagem e a envia ao destinatário.

Recepção de Mensagens: O cliente receptor descriptografa a mensagem recebida e a exibe.

Segurança Provida pela CA

1. Criação de Chaves Seguras

A CA gera um par de chaves RSA de 2048 bits, que são usadas para assinar as chaves públicas dos clientes.

As chaves são armazenadas de forma segura no servidor e protegidas por criptografia AES.

2. Assinatura Digital

A chave pública do cliente é assinada pela chave privada da CA, garantindo a autenticidade da chave pública do cliente.

A assinatura digital impede que um atacante substitua a chave pública do cliente por uma chave maliciosa.

3. Armazenamento Seguro

O arquivo de chaves (chaves.txt) é criptografado utilizando AES com uma chave derivada de uma senha fornecida pelo usuário. Isso garante que mesmo se o arquivo for comprometido, as chaves permanecem seguras.

4. Verificação de Integridade

A integridade das mensagens e das chaves é garantida pelo uso de HMAC (Hash-based Message Authentication Code), que verifica se a mensagem foi alterada durante a transmissão.

5. Troca de Chaves Segura

A troca de chaves Diffie-Hellman proporciona um método seguro de estabelecimento de uma chave simétrica compartilhada entre cliente e servidor, protegendo contra ataques de interceptação.

Conclusão

Este sistema de comunicação segura garante que as mensagens trocadas entre os clientes sejam confidenciais, íntegras e autênticas. A Entidade Certificadora (CA) desempenha um papel crucial na garantia da autenticidade das chaves públicas dos clientes, prevenindo ataques de intermediários (man-in-the-middle) e outras formas de

comprometer a segurança do sistema. A utilização de criptografia híbrida (assimétrica e simétrica) proporciona uma comunicação eficiente e segura entre os participantes.

Código dos Arquivos

Os arquivos envolvidos no sistema são servidor.py, cliente.py, ca.py, cliente_manager.py, e criptografia.py. Cada um desses arquivos contém a implementação das funcionalidades descritas acima, garantindo a segurança e a eficiência da comunicação entre os clientes.