Relatório de Projeto: *Programação utilizando sockets*

Felipe Durant (fdf)[1], Matheus Victor (mvas2)[1], Morgana Galamba (mbfg2)[1]

[1]Centro de Informática – Universidade Federal de Pernambuco (UFPE)

Abstract. *This report outlines the development of a secure communication system using a Certificate Authority (CA) to manage public keys within a network. The system employs a hybrid cryptography approach, merging AES for data encryption with RSA for the secure exchange of keys. The implementation faced challenges, including anomalous behavior related to the use of the UDP protocol and limitations in the CA's registration management. Despite these challenges, the project proved to be an effective solution for ensuring security and privacy in network communications. This report discusses the design decisions, encountered challenges, and provides an analysis of the outcomes, suggesting areas for future enhancements.*

Resumo. *Este relatório detalha o desenvolvimento de um sistema de comunicação segura utilizando uma Autoridade Certificadora (CA) para gerir as chaves públicas em uma rede. O sistema adota uma abordagem de criptografia híbrida, combinando AES para encriptação de dados e RSA para o intercâmbio seguro de chaves. A implementação enfrentou desafios, incluindo comportamentos anômalos associados ao uso do protocolo UDP e limitações na gestão de registros pela CA. Apesar desses desafios, o projeto demonstrou ser uma solução eficaz para garantir a segurança e a privacidade das comunicações em rede. Este relatório aborda as decisões de design, os desafios encontrados e fornece uma análise dos resultados, sugerindo áreas para futuras melhorias.*

1. Introdução

Esta introdução estabelece o cenário para a discussão detalhada que se segue, cobrindo as motivações, as decisões de design tomadas, os desafios enfrentados durante a implementação e a análise dos resultados obtidos.

2. Decisões de Design

2.1. Escolha da Criptografia Híbrida

O projeto adota uma abordagem híbrida de criptografia, combinando AES e RSA. A decisão de permitir que cada nó gere sua própria chave AES para a encriptação de dados foi motivada pela limitação do RSA em encriptar dados de tamanho considerável. O AES é utilizado para a encriptação de mensagens devido à sua eficiência e capacidade de trabalhar com grandes volumes de dados, enquanto o RSA é empregado para a encriptação segura das chaves AES, facilitando o intercâmbio seguro das chaves sem expor a chave privada da CA ou dos nós.

2.2. Roteamento no Sentido Horário

A decisão pelo roteamento no sentido horário visa simplificar a implementação do algoritmo de roteamento, evitando a necessidade de manter estados complexos ou implementar lógicas de roteamento avançadas. Essa simplicidade ajuda na manutenção do código e na estabilidade do sistema, facilitando a identificação e correção de problemas.

2.3. Simulação da Topologia de Rede

Utilizando o Docker Compose, o projeto simula uma topologia de rede em anel, representando a conexão entre os nós. Esta escolha permite testar o sistema em um ambiente controlado, replicando uma estrutura de rede realista e simplificando o processo de desenvolvimento e teste. As redes do Docker oferecem uma abstração conveniente para simular a comunicação entre os componentes do sistema.

3. Desafios e Soluções

3.1. Comportamento Anômalo com UDP

Durante o desenvolvimento, observou-se que a utilização de UDP como protocolo de transmissão podia levar a comportamentos anômalos, especialmente após várias iterações de comunicação. Em certos momentos, as mensagens não eram entregues, impactando a confiabilidade do sistema. Este comportamento é atribuído às características inerentes do UDP, que não garante a entrega de pacotes, ordem ou integridade dos dados.

3.2. Limitações no Registro com a CA

A Autoridade Certificadora, ao lidar com múltiplos registros dos mesmos nós, apresentou limitações, deixando de responder após várias tentativas de registro. Isso pode ser devido ao acúmulo de entradas no registro da CA ou à gestão ineficiente dos recursos. A implementação não foi inicialmente projetada para lidar com um alto volume de solicitações de registro em um curto período de tempo, revelando a necessidade de otimização nessa área.

4. Conclusão

O projeto de comunicação segura com Autoridade Certificadora foi bem-sucedido em demonstrar a viabilidade de uma abordagem híbrida de criptografia para a segurança de comunicações em rede. Apesar dos desafios enfrentados, especialmente relacionados ao uso do protocolo UDP e ao gerenciamento de registros na CA, o sistema cumpriu seu objetivo principal de garantir a encriptação e a privacidade das mensagens. As observações sobre o comportamento anômalo do UDP e as limitações no registro com a CA são valiosas para a fase de revisão e otimização do projeto. Futuras iterações deverão abordar esses desafios, possivelmente explorando alternativas ao UDP para a transmissão de mensagens e aprimorando o sistema de registro da CA para suportar um maior volume de solicitações.