Proposta do Projeto - Segurança de Redes

Alunos:
Leonardo Garcia dos Santos
Ronaldo Ávila de Arruda Junior

Objetivo: Desenvolvimento de um WebChat em tempo real com criptografia de ponta a ponta usando o protocolo WebSokcet.

Em um primeiro viés foi planejado o desenvolvimento de um chat em tempo real que utiliza uma criptografia de ponta a ponta com o protocolo WebSocket, o projeto será um monolito com frontend em Javascript e backend em Golang(“Golang foi escolhido devido sua capacidade ágil em lidar com o protocolo websocket”). A aplicação será dockerizada, onde a princípio terá dois containers um para subir o servidor Golang que já tem a capacidade de renderizar páginas web em HTTP sem a necessidade de um Apache ou Nginx e um com o Wireguard que vai criar e estabelecer um “túnel” seguro entre o cliente e o servidor utilizando VPN.

O projeto busca entender como a criptografia é usada nas trocas de mensagens e como os dados se comportam em todo o tráfego pela rede.

A VPN é uma forma de garantir confidencialidade entre o tráfego da rede, porém a aplicação terá uma camada de criptografia adicional, ainda não foi decidido o tipo de algoritmo que será utilizado e nem a implementação, mas uma opção no frontend é a JWT.io onde nela existem os principais tipos de algoritmos como o RSA e ECDSA que utilizam um modelo de par de chaves, a forma de manipulação dos dados é via JSON. Abaixo segue o diagrama da aplicação: