Sistema 2FA

Engenharia Informática

ANO/SEMESTRE: 2024-2025 / 5º Semestre

Unidade Curricular: Sistemas Distribuídos
Professor: Pedro Rosa

Carolyne Silva - 20210046
https://github.com/CMS77/sistema2fa

1. Descrição do Problema

A autenticação baseada apenas em nomes de utilizadores e senhas tem-se mostrado vulnerável a ataques, como phishing, força bruta e violações de bases de dados. Estes métodos de autenticação simples não são suficientes para garantir a segurança de sistemas críticos e informações sensíveis. Para mitigar esses riscos, o uso de autenticação de dois fatores (2FA) tem-se tornado um padrão. No entanto, para garantir robustez e continuidade do serviço, o sistema precisa ser tolerante a falhas e distribuído, evitando a dependência de um único ponto de falha. O objetivo deste projeto é desenvolver uma solução de 2FA que possa funcionar em ambientes distribuídos e que ofereça uma experiência de usuário simples e segura.

2. Casos de Uso

- **Login Seguro com 2FA**: O utilizador faz login na aplicação usando as suas credenciais habituais (nome de utilizador e senha). Após a validação inicial, o sistema solicita um segundo fator de autenticação, que pode ser gerado por um TOTP (Time-based One-Time Password) através de uma aplicação instalada no smartphone Android (Google Authenticator).
- **Distribuição de Autenticadores**: O sistema deverá ser capaz de distribuir a carga de autenticação em múltiplos servidores, garantindo disponibilidade mesmo em caso de falha de alguns componentes.

3. Enquadramento na Área da Unidade Curricular

Este projeto está diretamente relacionado com os conceitos abordados na Unidade Curricular de Sistemas Distribuídos, como:

- **Tolerância a Falhas**: Garantir que o sistema de 2FA continue a funcionar, mesmo quando algumas partes da infraestrutura falharem.
- **Replicação e Consistência**: A aplicação terá que lidar com a replicação de dados de autenticação entre vários nós distribuídos, mantendo a consistência dos dados para garantir uma experiência contínua e segura ao utilizador.

4. Arquitetura da Solução

A arquitetura do sistema 2FA será distribuída e composta pelos seguintes componentes:

- Servidor de Autenticação Centralizado:
  - **Função**: Valida as credenciais iniciais do utilizador (nome de utilizador e senha).
  - **Conexão**: Comunica-se com o Serviço Distribuído de 2FA para a segunda etapa de autenticação.
- Serviço Distribuído de 2FA (Google):
  - **Estrutura**: Replicado em múltiplos servidores para garantir disponibilidade e resiliência.
- Aplicação Android (Google Authenticator):
  - **Função**: Gera códigos TOTP (Time-based One-Time Password) para a segunda etapa de autenticação.
  - **Interação**: O utilizador insere o código gerado na aplicação para completar a autenticação.
- Banco de Dados Distribuído:
  - **Função**: Armazenar dados do utilizador e informações de autenticação.
  - **Benefícios**: Garante redundância e acessibilidade em caso de falhas.

5. Tecnologias a Utilizar

- **Android SDK**: Para o desenvolvimento da aplicação Android que gere TOTP ou receba notificações push.
- **Google Firebase (Cloud Messaging)**: Para o envio de notificações push.
- **OAuth 2.0**: Para o gerenciamento de tokens e autenticação segura.
- **Algoritmo TOTP (Time-based One-Time Password)**: Para a geração de senhas temporárias com base no tempo.
- **Docker**: Para a implementação e gestão de containers, permitindo a escalabilidade e distribuição dos componentes do sistema.
- **Protocolo HTTP/HTTPS**: Para comunicação segura entre os componentes distribuídos.
- **GitHub:** Controle de versão do código fonte.

6. Bibliografia

- https://www.microsoft.com/en-us/security/business/security-101/what-is-openid-connect-oidc

- https://br.developers.hubspot.com/beta-docs/guides/api/app-management/oauth/tokens?uuid=e96829b5-1798-4562-a2db-9506baf74d6e

- https://cloud.google.com/identity-platform/docs/admin/enabling-totp-mfa#java_2