



**Faculdade de Design,
Tecnologia e Comunicação**
Universidade Europeia

Proposta de trabalho para Sistemas Distribuídos

Sistema 2FA

Engenharia Informática

Sistemas Distribuídos

Professor Pedro Rosa

Realizado por:

Mafalda Quintas - 50036446

Rafael Pilré - 20190877

Tiago Silva - 20190878

Repositório de github: <https://github.com/mrquintas98/2FA>

Composição do Grupo			
Número / Nome	Esforço (Horas)		
	Pesqui. Web	Reunião	Implementação
50036446 – Mafalda Quintas	5	10	
20190877 – Rafael Pilré	5	10	
20190878 – Tiago Silva	5	10	

Enquadramento

A Autenticação de Dois Fatores (2FA) é um processo de verificação em duas etapas que visa proporcionar um nível adicional de segurança ao exigir que o utilizador se autentique a si próprio utilizando um meio secundário. Sem a utilização do 2FA, um hacker poderia obter acesso aos dispositivos ou contas de uma pessoa apenas conhecendo a palavra-passe da vítima, enquanto que com o 2FA sabendo apenas esta palavra-passe é insuficiente para passar a verificação de autenticação. O objetivo deste trabalho consiste em implementar uma solução de autenticação de dois fatores em conjunto com outro grupo de trabalho para que consigamos reforçar a segurança do sistema. Esperamos com este projeto, beneficiar a sociedade a aumentar o conhecimento geral do 2FA conduzindo a serviços mais seguros, como também ganhar experiência em trabalhar com equipas de projetos diferentes mas que se ligam ao mesmo tempo.

Casos de uso

1. Utilizador após autenticar-se corretamente é pedido um código
2. A aplicação envia um pedido de um token
3. O utilizador recebe o código
4. Digitar o código na janela de verificação da aplicação
5. Acesso é garantido
- 5.1 Caso o código esteja errado, selecionar opção de reenviar

Solução a implementar

i. Descrição genérica

Após a primeira autenticação no sistema de repositório de ficheiros (início de sessão com *Username* e *Password*), será enviado um pedido de geração de token para o nosso serviço de *Token* como também um identificador de utilizador para o qual o mesmo será gerado (e-mail, etc.). Após receber os dados necessários, irá ser gerado um *Token* de uma de duas formas (dependendo do que o docente aceitar): a partir de uma API que execute o algoritmo RFC4226(HOTP) ou algo mais simples como uma *OTP (One Time Password)* através de Nodejs. Com a conclusão desta fase este *Token* será enviado tanto para a aplicação *Mobile*, onde o código será visualizado em conjunto com um temporizador (passando a uma solução *TOTP - Time-based One Time Password*) referente à validade do mesmo, como a aplicação na qual o utilizador deseja efetuar o *Login*.

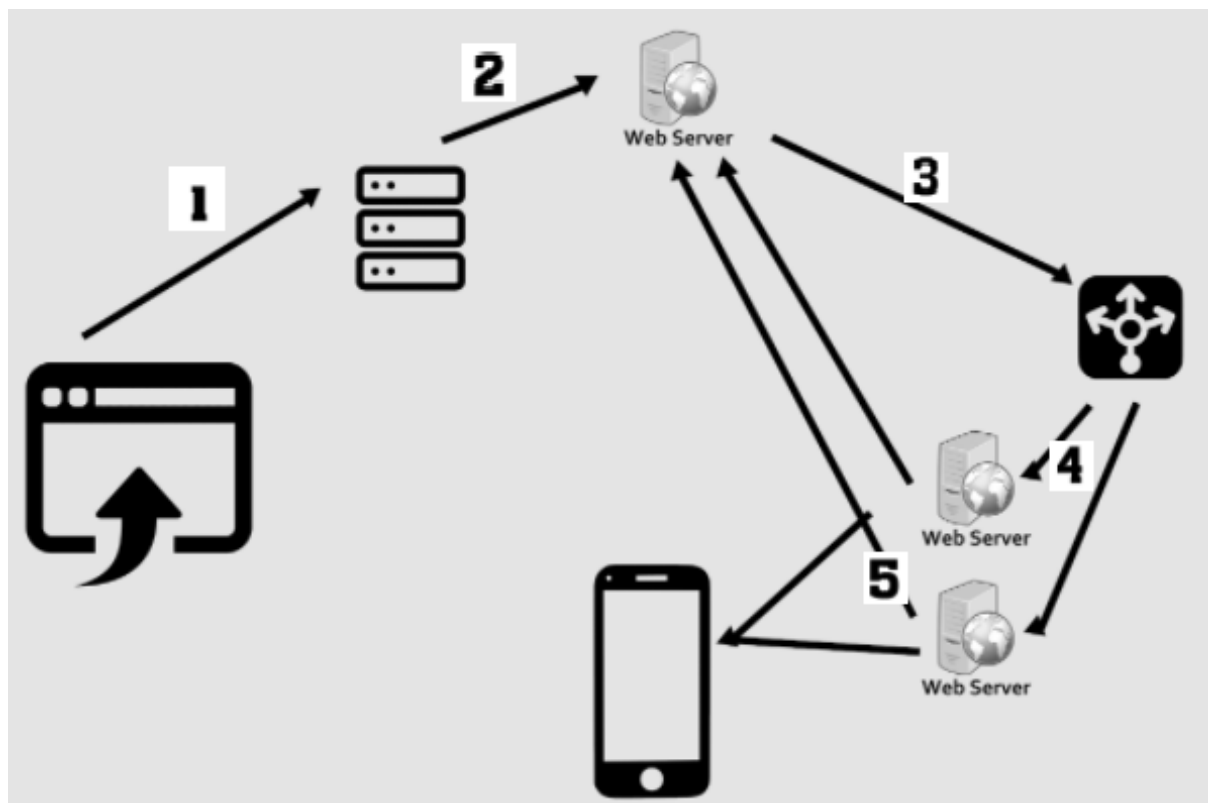
ii. Enquadramento nas áreas da unidade curricular

Quando se trata de segurança on-line, o fator de autenticação mais comum, de longe, é a combinação nome de utilizador/senha. Isso significa que a maioria dos sistemas está a usar apenas a autenticação de fator único. Também é importante lembrar que as pessoas têm mais contas on-line do que quando as senhas foram introduzidas pela primeira vez, o que significa que, muitas vezes, há muitas senhas para serem lembradas. Isso pode levar à “reciclagem de senha”, que é quando a mesma senha é usada para várias contas, facilitando o acesso a terceiros. Um sistema distribuído vai permitir também que tanto no servidor ou aplicação caso haja algum tipo de erro, este não comprometa o risco da operacionalidade do sistema.

iii. Requisitos técnicos

O sistema 2FA irá utilizar 1 HAProxy Load Balancer e pelo menos 2 Web Servers para geração de Tokens. Irá também ser construída uma aplicação mobile para apresentação do Token ao cliente que efetua Login na aplicação.

iv. Arquitetura da solução



Tendo em conta a integração do projeto com o grupo G04, a solução irá funcionar da seguinte forma:

1. O cliente efetua o login no Website de acesso ao sistema de ficheiros distribuídos(G04);
2. Após o pedido passar por um Proxy, o pedido é redirecionado para o Web Server referente à ação(G04);
3. Após validação de um Login bem feito, o Web server irá fazer um pedido para geração de Token 2FA(G04);
4. Após o pedido ser recebido por um HAProxy e distribuído para o Web Server com menor carga, irá ser gerado o Token 2FA;
5. Por fim, a informação referente ao Token 2FA (incluindo um temporizador) é tanto enviada ao Web Server que fez o pedido de Token como também à App Mobile do Cliente.

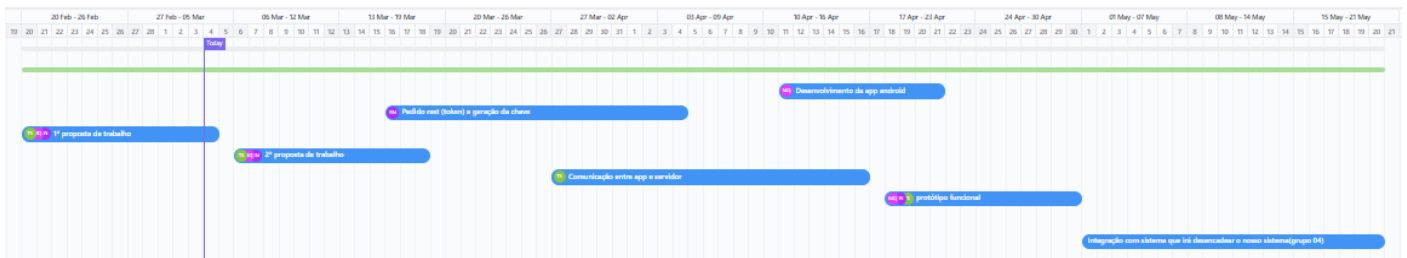
v. Tecnologias a utilizar

As tecnologias que identificámos podem não ser de todo definitivas para o trabalho, visto que para a implementação mobile estamos dependentes da resposta dos docentes de Project Factory.



Planeamento e calendarização

OPEN	8 TASKS	ASSIGNEE	DUE DATE	PRIORITY	
■	1ª proposta de trabalho	RN TS	Today	Flag	
■	2ª proposta de trabalho	RN TS	Mar 18	Flag	
■	Pedido rest (token) e geração da chave	RN	Apr 4	Flag	***
■	Desenvolvimento da app android	MQ	Apr 21	Flag	
■	Comunicação entre app e servidor	TS	Apr 16	Flag	
■	protótipo funcional	TS RN TS	Apr 30	Flag	
■	Sistema de anti-Ransomware	MQ RN TS		Flag	
■	Integração com sistema que irá desencadear o nosso sistema(grupo 04)		May 20	Flag	



Bibliografia

- M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., and O. Ranen, "HOTP: An HMAC-Based One-Time Password Algorithm", RFC 4226, DOI 10.17487/RFC4226, December 2005,
- Oliynyk, M. (2020, June 24). TOTP Algorithm Explained. Protectimus.
- Adding multi-factor authentication to your web app | Identity Platform Documentation | Google Cloud. (2022). Retrieved 4 March 2022, from <https://cloud.google.com/identity-platform/docs/web/mfa>