Universidade do Minho
Escola de Engenharia

Trabalho Prático III

Tecnologia de Segurança

Trabalho realizado por:
Filipe Freitas (PG42828)
Maria Barbosa (PG42844)

Janeiro de 2021

Índice

Capítulo 1

Introdução

O objectivo deste trabalho é a implementação de um sistema de ficheiros, complementar ao tradicional do sistema operativo Linux. Procuramos criar um mecanismo capaz de autorizar a operação de abertura de um ficheiro apenas depois da introdução de um código de segurança único enviado via e-mail, para o utilizador que o despoletou. Assim, quando um utilizador realiza uma ação que demonstra a sua intenção de abrir um ficheiro, tem de obrigatoriamente iniciar sessão na app e inserir o código que lhe foi enviado para o seu endereço de e-mail.

Para isso, criou-se um sistema de ficheiros, baseado no lifuse, e um servidor web que permite a comunicação com o utilizador e a inserção da código atribuído para posteriormente ser validado pela app.

Neste relatório, descrevemos as estratégias adotadas, a estrutura e os comandos necessários para executar a ferramenta criada. Além disso, terminamos com uma breve reflexão sobre o trabalho realizado, explicando os aspectos de segurança que foram considerados.

Capítulo 2

Arquitectura e Estrutura da solução

A solução criada para o problema previamente identificado pode ser dividida em dois pequenos programas que se completam e interagem entre si. São eles:

- **Web-App -** Um servidor Web que funciona como interface da nossa solução, permitindo ao utilizador registar-se, iniciar sessão, gerar o código, envia-lo por e-mail e inserir o código recebido verificando se o mesmo é válido. Foi desenvolvido em NodeJs e encontra-se a escuta de pedidos no endereço *http://localhost:3000/*.
- **Fuse-module** - Utiliza o ficheiro *passthroughfs.py* que tem por base a biblioteca libfuse.

Tendo isto em conta um user que se encontre a utilizar pela primeira vez a App deve começar por se registar. Para isso, deve aceder a rota *http://localhost:3000/auth/register* e indicar o seu nome, e-mail, password e o seu unix username. Os dados fornecidos serão guardados numa base de dados, ficando disponíveis para serem acedidos por parte do sistema operativo. Em seguida, ao iniciar sessão na conta previamente criada é redireccionado para a sua página pessoal. A autenticação é feita com auxilio de uma base de dados mongoDB.

Sempre que é detectada a intenção do utilizador abrir um ficheiro, no fuse-module-py é invocada a função open() que vai instaurar o processo de autenticação complementar do utilizador. Este processo começa pela obtenção e envio para o web server, dos dados do processo que esta a ser executado, incluindo o username unix do utilizador que esta a realizar a ação e o path do ficheiro que se pretende aceder. Colocando-se por fim a escuta da resposta enviada pelo servidor.

Ao servidor web, cabe procurar os dados do utilizador identificado pelo seu Unix username, na base de dados, gerar um código aleatório com 6 dígitos e proceder ao seu envio para o endereço de e-mail do utilizador que desencadeou todo este processo. Este código, é guardado localmente. Após o envio do e-mail, inicia-se a contagem de 30 segundos, após os quais se não houver resposta se elimina o código e

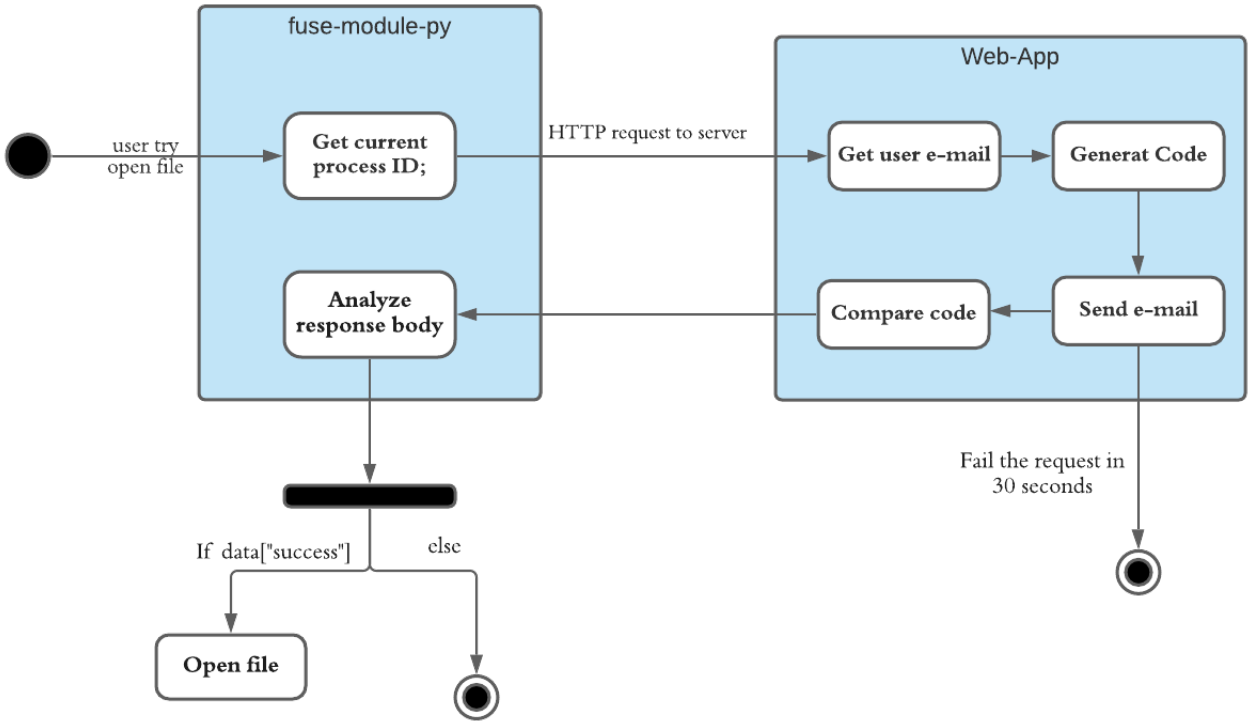

Figura 2.1: Diagrama de estados da ferramenta

retorna-se a false à função open(). Por outro lado, se o utilizador inserir o condigo, antes dos 30 segundos passarem, este será comparado com o que foi gerado e se coincidirem é concedida autorização para abertura do ficheiro pedido. Em alternativa, para simplificar o trabalho do utilizador, este pode optar por pode clicar no link que surge no corpo da mensagem (como mostra a figura ...) que contem o código gerado na query string.

A imagem 2.1 esboça a estrutura da solução, apresentando um esquema simples do funcionamento da nossa ferramenta.

Capítulo 3

Utilização da Ferramenta

Para utilizar e testar a ferramenta devem executar-se os seguintes passos:

1. Iniciar o servidor Web. Na pasta Web-app executar: *npm start*
2. Agora, com o servidor web funcional, o utilizador, deve registar-se
3. (...)

Capítulo 4

Conclusão

O objectivo principal deste trabalho, desenvolver um sistema de ficheiros complementar ao do SO Linux que garante um mecanismo de autenticação extra, foi atingido com sucesso.

Durante a sua execução, procuramos garantir que a ferramenta desenvolvida tem em atenção às principais propriedades de segurança e garanta que o sistema não se encontra sujeito a nenhuma vulnerabilidade ou fraqueza conhecida. Deste modo, a ferramenta possui às propriedades de segurança: **Autorização** (através do código enviado, garante-se que o acesso ao ficheiro apenas é permitido ao utilizador que tem autorização para o aceder), **Autenticação** (todos os usuários estão devidamente identificados pela ferramenta) e **Confidencialidade**.