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 do 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 principais aspectos de segurança que foram considerados.

Capítulo 2

Solução desenvolvida

2.1 Arquitectura e Estrutura da ferramenta

A solução desenvolvida 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, tem de aceder a rota *http://localhost:3000/auth/register* e indicar o seu nome, e-mail, password e o unix username. Os dados fornecidos serão guardados numa base de dados mongoDB, ficando disponíveis para serem acedidos por parte do sistema operativo. Em seguida, precisa de iniciar sessão na conta previamente criada, sendo redireccionado para a sua página pessoal.

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 da ação que esta a ser executada, incluindo o username unix do utilizador que à esta a realizar e o path do ficheiro que se pretende aceder. Colocando-se por fim à 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 o código é eliminado e retorna-se false à função open().

Por outro lado, se o utilizador inserir o código (ou clicar no link presente no corpo da mensagem que possui o código na query string) antes de se esgotarem os 30 segundos, este é comparado com o que foi gerado e se coincidirem é concedida autorização para abertura do ficheiro pretendido.

A imagem 2.1, apresentando um esquema síntese do funcionamento da ferramenta desenvolvida.

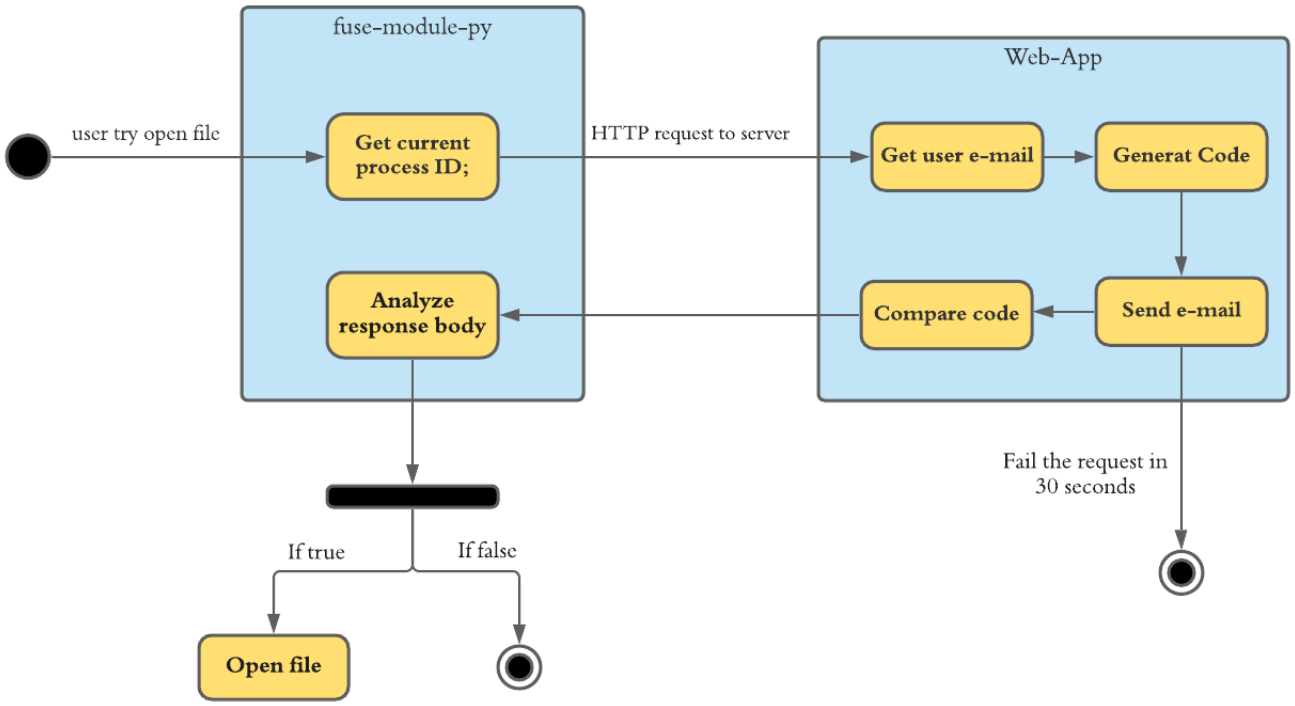

Figura 2.1: Diagrama de estados da ferramenta.

2.2 Utilização da Ferramenta

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

1. Criar o sistema de ficheiros. Na pasta *fuse-module-py* deve executar-se o comando:

   python3 passthroughfs.py <directoria a replicar> <directoria replicada>

2. Iniciar o servidor Web. Na pasta Web-app, deve-se executar: *npm start*.

   Sendo necessário que o utilizador, inicie sessão ou se registe.

3. Por fim, num terminal, aceder a um ficheiro que se encontra na directoria replicada apenas é possível se o código de autorização recebido for inserido correctamente no tempo disponível.

Capítulo 3

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 as principais vulnerabilidade ou fraquezas conhecidas. Deste modo, podemos afirmar que a ferramenta possui às seguintes 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 **Disponibilidade** (a informação esta sempre disponível para acesso aos utilizadores que demonstram possuir o código gerado).

Além disto, durante o desenvolvimento desta solução tentou-se mitigar algumas das fraquezas mais comuns, como é o caso:

- *CWE-287: Autenticação impropria* - Antes da realização de cada ação o utilizador necessita de iniciar sessão de modo a ser possível garantir que é quem diz ser.
- *CWE-200 : Exposição de informações confidenciais a um usuário não autorizado* - O envio de um código por e-mail introduz um nível extra de segurança, garantindo que apenas usuários autorizados tem acesso a informação.
- *CWE-862: Missing Authorization* - Com o sistema desenvolvido, evita-se que mesmo quando as verificações de controle de acesso não são aplicadas, os usuários para aceder aos ficheiros ou realizar qualquer ação, necessitam de introduzir um código de segurança.