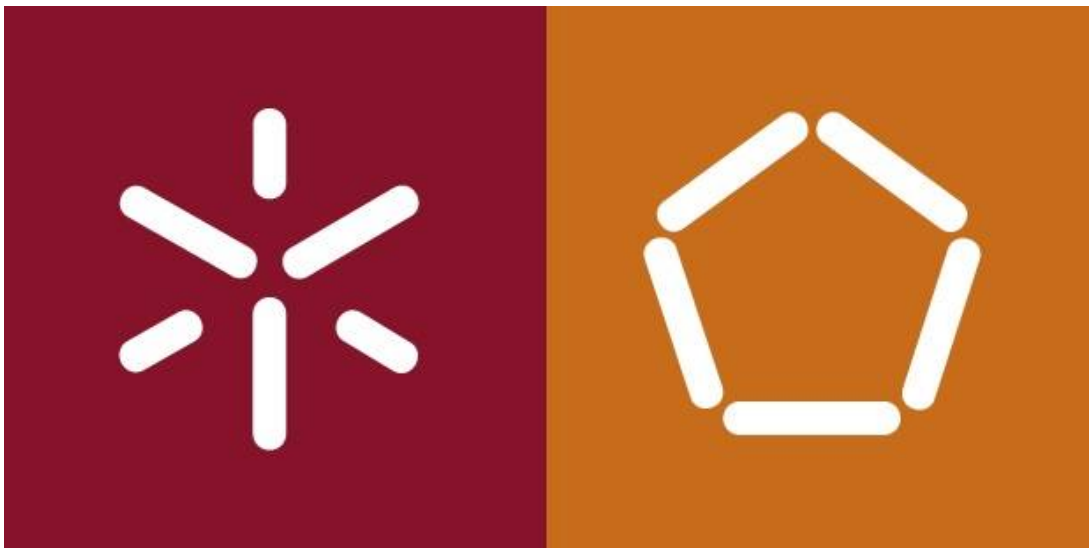
Universidade do Minho



Autorização de operações ao nível do sistema de ficheiros

Mestrado Integrado em Engenharia Informática

Tecnologias de Segurança
1º Semestre , 2018/2019

Grupo 6
A77070 - João Pedro Pereira Alves
A70132 - Nuno André Lopes Leite

Gualtar,Braga
15 de Janeiro de 2019

Conteúdo

1 Introdução

Neste trabalho prático, foi pedido ao grupo que implementasse um sistema de ficheiros que permitisse autorização de operações ao nível do mesmo, ou seja, construir uma camada adicional de segurança especificamente na operação de abertura de ficheiros.

O objetivo é que um utilizador, ao executar uma acção com a intenção de abrir um ficheiro para ver o seu conteúdo, tenha que obrigatoriamente se autenticar via um código que lhe é enviado para o seu contacto de correio eletrónico.

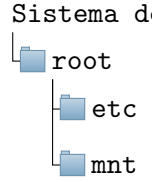
Neste sentido, a solução desenvolvida será composta pelo próprio sistema de ficheiros com a camada extra de segurança e por um web server que permitirá a introdução do código de autorização. Estas ferramentas irão comunicar entre si para o bom funcionamento da ferramenta desenvolvida.

2 Arquitetura e Estrutura da Solução

Com o intuito de implementar um sistema de ficheiros seguro, com base nas permissões e modos de ficheiros e diretorias do **Unix**, foi desenvolvida uma solução composta por:

- Um **web server**, desenvolvido em *NodeJS*, que escuta pedidos no *localhost* na porta 4500 feitos pelo sistema de ficheiros, contendo uma simples interface web, que permite ao utilizador inserir o código de autenticação enviado por email;
- Uma implementação, partindo do *passthrough* em *Python*, de um sistema de ficheiros que integra a biblioteca *libfuse*, através de uma API específica em *Python*, que será abordada na secção própria.

Seguindo ainda este modelo, considerou-se então que a estrutura do sistema de ficheiros deveria ser de tal forma que, um determinado utilizador tivesse acesso aos seus dados pessoais necessários, aquando da execução da aplicação. Para tal, foi criada a seguinte organização de diretorias:



Posto isto, a autenticação de um utilizador é feita, sempre que este tentar montar o sistema de ficheiros, executando a aplicação, sendo que, se esta não for garantida, a sessão criada é apenas temporária, pelo que o utilizador terá que inserir o seu contacto quando iniciar novamente a aplicação. A autenticação é feita recorrendo às bases de dados dos utilizadores do sistema **Unix**, no qual está a ser executada a aplicação.

NOTA: São permitidas sessões temporárias para efeitos de avaliação académica, para que possam ser avaliados todos os restantes aspetos mesmo que a autenticação falhe. Num cenário real, a ferramenta abortaria, visto que, do seu ponto de vista, não reconheceria o utilizador.

A informação de contacto do utilizador, necessária para o correto funcionamento desta ferramenta, é introduzida pelo mesmo na primeira vez que este utiliza o sistema de ficheiros. Essa informação é encriptada e armazenada na diretoria **etc** criada, num ficheiro que apenas o utilizador que o criou tem permissões de leitura e escrita.

Aquando da chamada da função `open()`, é exigido uma autenticação extra do utilizador, que consiste na geração de um código aleatório de 6 dígitos e o seu envio numa mensagem de correio eletrónico, para o contacto do utilizador que está a utilizar o sistema de ficheiros, altura em que também é iniciado um alarme de 30 segundos, permite a autenticação até, no máximo, 30 segundos. Posteriormente, abre uma página web com um pedido ao **web server** criado, onde o utilizador deve inserir o código que recebeu. Finalmente, se os 30 segundos ainda não passaram, compara o código inserido com o código gerado e concede ou não autorização para a abertura do ficheiro pedido.

A comunicação entre web server e o sistema de ficheiros para operações de autenticação é feita através de um ficheiro, sendo que o web server nunca sabe qual foi o código gerado, apenas fornece um meio de introdução de um código que irá depois ser comparado na função do sistema de ficheiros, com o código gerado.

A figura 1 mostra uma forma abstrata de visualizar as componentes desta ferramenta e as interações entre si.

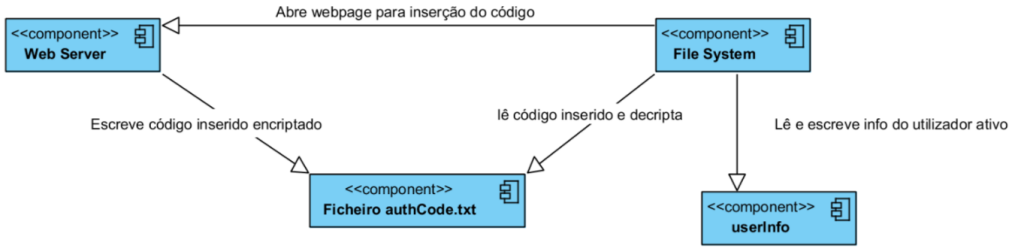


Figura 1: Diagrama de componentes do sistema

3 Bibliotecas utilizadas

Na solução em *python*, que implementa o sistema de ficheiros, utilizámos as seguintes bibliotecas:

- **pyfuse3** - biblioteca que fornece uma API em *Python* que permite a integração com a libfuse3;
- **python-pam** - que permite autenticar o utilizador, no momento da execução, recorrendo às bases de dados de utilizadores *Unix*;
- **smtplib** - biblioteca que fornece uma API para comunicação com correio eletrónico simples;
- **Cryptography** - biblioteca utilizada para a encriptação e decriptação dos dados de contacto do utilizador.

Além disso, para executar o sistema de ficheiros é necessário instalar (se ainda não a possuir) a versão 3.X de *Python* e ter o *pip*, o package manager de *Python* também instalado, que pode ser feito recorrendo ao seguinte comando:

```
sudo apt-get install python3-pip
```

De forma a preparar o ambiente *Python* com todas as bibliotecas instaladas, execute o seguinte comando dentro na diretoria inicial do projeto:

```
sudo pip install
```

Na solução em *NodeJS*, que implementa o web server, não foram utilizadas nenhumas bibliotecas externas, visto que a interface desenvolvida é extremamente simples e é feita recorrendo apenas a módulos do *NodeJS*.

4 Utilização da ferramenta

Para utilizar esta ferramenta é necessário iniciar o web server em primeiro lugar, para que possa escutar pedidos. Assim, deve-se navegar até a pasta authServer e, dentro desta, executar o seguinte comando:

```
npm start
```

A partir desta altura, o web server já está ativo. De seguida, deve-se iniciar/montar o sistema de ficheiros. Neste sentido, deve-se navegar até a pasta pyfuse3 e, dentro desta, executar o seguinte comando:

```
python3 passthrough.py test/ root/mnt
```

No comando acima executado, o argumento test/ é a pasta raíz do sistema de ficheiros que irá ser criado e o argumento root/mnt é onde o sistema de ficheiros será montado.

Após a execução do comando, deverá seguir as instruções de autenticação e informação pedidas.

Finalmente, para experimentar a ferramenta, basta abrir um terminal normal e aceder à pasta root/mnt que está dentro da pasta pyfuse3/ e, apartir daí, é possível navegar no sistema de ficheiros, tendo sempre que se autenticar através do código de autorização quando quiser ver o conteúdo de um ficheiro.

5 Conclusões

Tendo terminado a concepção desta ferramenta, é da nossa opinião que o resultado apresentado neste relatório é bastante satisfatório, visto que o sistema de ficheiros implementado, em conjugação com o web server, permite operações ao nível do sistema de ficheiros com funcionalidades de autorização bem definidas, tendo em conta que, para saber o conteúdo de um ficheiro, é sempre necessário introduzir um código de autorização que é enviado apenas para o contacto do utilizador que está a usar a ferramenta.

Assim, podemos referir que a ferramenta concebida apresenta as seguintes propriedades de segurança:

- **Autenticidade e autorização** - Estas duas propriedades de segurança são garantidas pelo facto que o acesso apenas é permitido a um utilizador autenticado, cuja identidade está bem definida (em termos do sistema operativo) e a autorização também está bem definida, visto que o acesso ao conteúdo apenas é permitido a um utilizador que seja autorizado para o efeito, ao introduzir o código de autenticação;
- **Confidencialidade** - O ficheiro de cada utilizador tem o seu conteúdo (forma de contacto) encriptado.

Para finalizar, é da opinião do grupo que os objetivos propostos foram cumpridos, apesar de que existiram algumas dificuldades, principalmente no que diz respeito a entender como trabalhar com as operações que integram com a *libfuse* de forma a retornar os resultados corretos.