Universidade do Minho

Segurança de Sistemas Informáticos

Trabalho Prático 3

2019/2020

Implementação de um File System em FUSE

Trabalho realizado por:

Ricardo Ponte
António Machado

Número de Aluno:

A79097
ID8236

16 de Janeiro de 2020

Conteúdo

1 Introdução

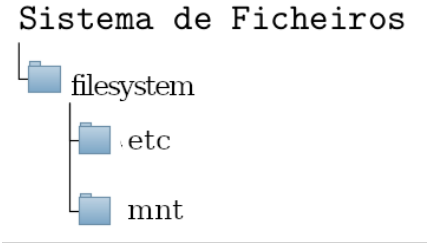
Este trabalho foi proposto no âmbito da Unidade Curricular de Segurança de Sistemas Informáticos da Universidade do Minho. Neste trabalho prático, foi pedido ao grupo que implementasse um sistema de ficheiros com introdução de uma camada adicional de segurança na operação de abertura de ficheiros.

O objetivo é que quando um utilizador abra um ficheiro qualquer , recorrendo à *system call open()* , tenha que obrigatoriamente se autenticar através de 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 , à qual foi adicionada a funcionalidade de deteção e remoção de virus no momento de acesso , sendo que o utilizador irá interagir com a ferramenta pela linha de comandos.

2 Arquitetura e Estrutura da Solução

A solução foi desenvolvida, partindo do *passthrough* em *Python*, de um sistema de ficheiros que integra a biblioteca *libfuse*, através da API *pyfuse3* (referida na secção seguinte). Esta solução integra-se com o *daemon* do *ClamAV* , o qual terá de ser devidamente instalado e configurado para fazer *scan* (no momento de acesso) aos ficheiros presentes no sistema de ficheiros montado , atraveś da biblioteca *pyClamd*.

Considerou-se que a estrutura do sistema de ficheiros deveria ser construída de modo a permitir a um qualquer utilizador do sistema de ficheiros ter 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 a partir da ferramenta,caso a autenticação falhe e não exista ficheiro de configuração para o utilizador, é criada uma sessão temporária, em que o utilizador tem de inserir o seu contacto (email) para montar o sistema de ficheiros. A autenticação é feita recorrendo às bases de dados dos utilizadores do sistema Unix, no qual está a ser executada a ferramenta.

NOTA: São permitidas sessões temporárias apenas para efeitos de avaliação académica, para que os outros elementos da ferramenta possam ser avaliados possam ser avaliados independen-

temente da autenticação. Num cenário real, a ferramenta abortaria pois não seria capaz de reconhecer o utilizador.

A informação de contacto do utilizador, necessária para o correto funcionamento desta ferramenta, é introduzida pelo mesmo na primeira utilização do sistema de ficheiros. Essa informação é cifrada e armazenada na diretoria **etc** criada, num ficheiro que tem o nome do utilizador no sistema de ficheiros nativo, sendo que apenas este tem permissões de leitura e escrita.

Sempre que é feita uma chamada à *system call open()*, é pedido ao utilizador que insira o código de acesso, que consiste num código aleatório de 6 digitos que será enviado por mensagem de correio eletrónico para o contacto do utilizador do sistema de ficheiros. De seguida, é iniciado um alarme com duração de 30 segundos, sendo que após este tempo a autenticação falha. Caso seja introduzido um código errado mas dentro dos 30 segundos definidos , são dadas 3 tentativas ao utilizador antes da autenticação ser abortada, se o código for correto é indicado que o acesso foi autorizado e que proceder-se-à ao *scan* do ficheiro. Caso o ficheiro não contenha virus aparecerá uma mensagem a indicar esse facto , caso contrário , será enviado mail com o resultado do *scan* , para o email de contacto do utilizador , e posteriormente o ficheiro será removido do sistema de ficheiros.

3 Bibliotecas Utilizadas

Na solução que implementa o sistema de ficheiros , desenvolvida em Python, que são utilizadas as seguintes bibliotecas:

- **pyfuse3** - Fornece uma API em *Python* que permite a integração com a *libfuse3*;
- **python-pam** - Permite autenticar o utilizador, em *runtime*, recorrendo às bases de dados de utilizadores Unix ;
- **smtplib** - Fornece uma API para comunicação com correio eletrónico através do protocolo SMTP;
- **Cryptography** - Utilizada para a cifra e decifra dos dados de contacto do utilizador.
- **pyClamd** - Permite comunicar com o *daemon* do ClamAV para uso das suas funcionalidades de antivirus.

Para se poder executar o sistema de ficheiros é necessário instalar (caso não possua) a versão 3.X de Python juntamente com o pip, o *package manager* do *Python* , que pode ser feito recorrendo ao seguinte comando:

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

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

```
sudo pip3 install .
```

4 Utilização da ferramenta

Para iniciar/montar o sistema de ficheiros é necessário aceder à pasta *pyfuse3* e, dentro desta, executar o seguinte comando:

```
python3 passthrough.py tests/ filesystem/mnt
```

No comando mencionado acima, o argumento *tests/* é a pasta de raíz do sistema de ficheiros que irá ser montado e o argumento *filesystem/mnt* é onde o sistema de ficheiros será montado.Após a execução do comando, deverão ser seguidas as instruções de autenticação e informação pedidas.

Para testar o funcionamento da ferramenta basta abrir o terminal e aceder à pasta *filesystem/mnt* que está dentro da pasta *pyfuse3/* e, a partir daí, é possível navegar no sistema de ficheiros, tendo sempre que se autenticar através do código de autorização para abrir um ficheiro.

5 Conclusão

Tendo terminado a concepção desta ferramenta, o grupo considera que o resultado obtido é satisfatório, visto que o sistema de ficheiros implementado,permite operações ao nível do sistema de ficheiros com funcionalidades de autorização bem definidas, sendo 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. Além disso a funcionalidade de deteção e remoção de virus reforça a robustez do sistema de ficheiros , não permitindo que um ficheiro seja malicioso seja aberto , sendo este removido após a sua deteção.

Sendo assim, pode-se dizer que a ferramenta concebida tem o seguinte impacto nas propriedades de segurança abaixo mencionadas:

- **Autenticidade e Autorização** - O acesso apenas é permitido a um utilizador autenticado, cuja identidade está bem definida (em termos do sistema operativo), devidamente autorizado, após introdução correta do introduzir o código de autenticação envido;
- **Confidencialidade** - O ficheiro de cada utilizador tem o seu conteúdo (forma de contacto) cifrado.
- **Integridade e Disponibilidade** - Deteção e remoção de ficheiros maliciosos permite evitar ataques que possam por em causa o funcionamento do sistema de ficheiros bem como o conteúdo dos seus ficheiros.