Escola de Engenharia
Universidade do Minho

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA
Mestrado Integrado em Engenharia Informática
Segurança de Sistemas Informáticos

Trabalho Prático

TP3

Grupo 17


Ricardo Canela - A74568


Tiago Baptista - A75328

Braga, 12 de Janeiro de 2020

Conteúdo

1 Introdução **2**

2 Fuse **3**

3 Autenticação e Segurança **4**

4 Conclusão **5**

4.1 Desfecho 5

1. Introdução

O presente foi elaborado no âmbito da disciplina de Segurança de Sistemas Informáticos e teve como principal objectivo complementar os mecanismos de controlo de acesso de um sistema tradicional do sistema operativo Linux com um mecanismo adicional de autorização de operações de abertura de ficheiros. O mecanismo pretendido deveria ser concretizado sob a forma de um novo sistema de ficheiros baseado em *libfuse*.

O mecanismo abordado e desenvolvido autoriza a operação de abertura de um ficheiro apenas após a inserção de um código de segurança devidamente definido para cada utilizador e enviado por correio electrónico para o mesmo.

2. Fuse

O *FUSE (Filesystem in Userspace)* é uma interface que permite a um utilizador o desenvolvimento de um *filesystem* sobre o *kernel* do *Linux*.

Com recurso a esta ferramenta pode-se personalizar

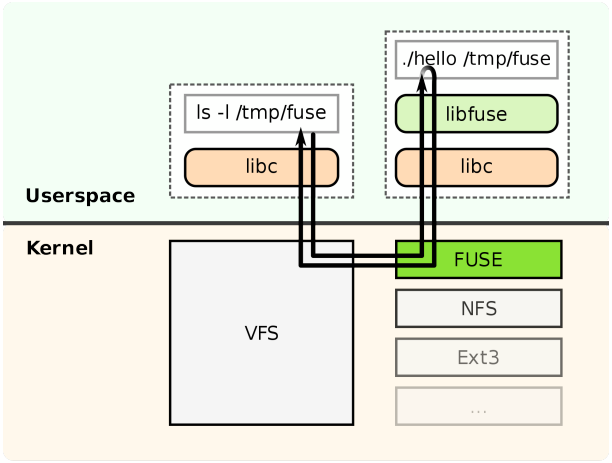

Figura 2.1: Esquema da arquitetura do *Fuse*.

3. Autenticação e Segurança

Como mecanismo de autenticação e controlo de acesso recorreu-se ao desenvolvimento de um servidor em *node* com interface em *pug* e uma base de dados em *MongoDB*.

Quando o *filesystem* desenvolvido com recurso ao *Fuse* recebe um pedido para abertura de um ficheiro, o utilizador é imediatamente apresentado com uma interface *web* de maneira a efetuar o *login*.

Após a realização do login através do mail e password, é encaminhado para uma página onde pode solicitar o envio automático de um código de confirmação, desta maneira estamos a introduzir segurança adicional no acesso aos ficheiros do *filesystem*.De seguida o utilizador tem de introduzir o código que lhe foi enviado, ficando assim desbloqueado o acesso ao ficheiro.

O *servidor web* é responsável pela autenticação com recurso às credenciais na base de dados,pela geração do código de verificação, assim como do seu envio com recurso ao *nodemailer*.

Por seu lado o *filesystem* fica bloqueado durante 1 minuto à espera do *input* realizado num ficheiro comum com o servidor.Caso o servidor efetue uma auntenticação (*mail,password* e código de verificação) com sucesso, escreve uma mensagem nesse ficheiro,que desbloqueia ação do filesystem permitindo o acesso ao ficheiro que o utilizador pretendia visualizar/editar.

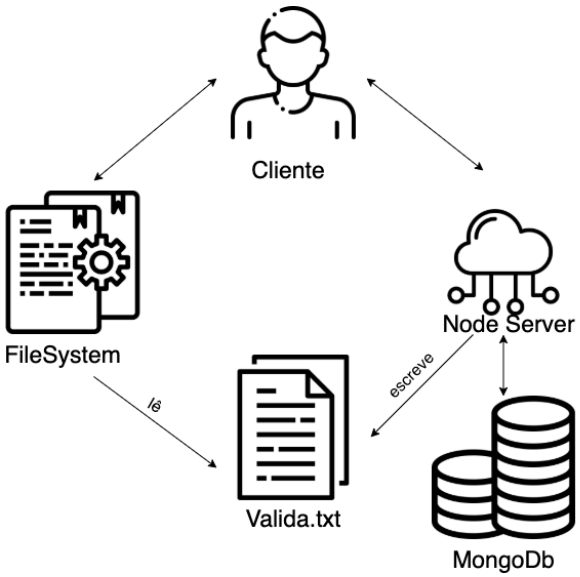

Figura 3.1: Esquema simplificado da arquitetura adotada.

4. Conclusão

4.1 Desfecho

Este projecto permitiu-nos conhecer a ferramenta *Libfuse*, que nos permitiu o desenvolvimento do *filesystem*. A abordagem seguida possui algumas vulnerabilidades, nomeadamente no que diz respeito ao ficheiro de configuração que serve como comunicação entre o servidor e o *filesystem*.