Relatório do Projeto de Segurança Informática

Grupo: Alessandro Aguiar 202200272
Bernardo Vaz 202200278

Laboratório: Ambos a quinta-feira

UC: Segurança Informática

Objetivo: Implementar um sistema de controle de acesso baseado no modelo **Bell-LaPadula**, garantindo segurança e integridade da informação.

1. Introdução

Este relatório documenta detalhadamente a implementação de um sistema de controle de acesso baseado no modelo **Bell-LaPadula**. O modelo foi escolhido pelo seu foco na **confidencialidade**, garantindo que os utilizadores de níveis inferiores **não possam ler** informações de níveis superiores e que os utilizadores de níveis superiores **não possam escrever** em níveis inferiores.

1.1. Escolha do Modelo de Segurança

O modelo **Bell-LaPadula** foi escolhido em detrimento do modelo **Biba**, pois o principal objetivo do projeto é **garantir a proteção contra fuga de informações**. No contexto da segurança da informação, esse modelo é amplamente utilizado em sistemas militares e governamentais para impedir acesso não autorizado a dados confidenciais.

O modelo Bell-LaPadula se baseia em duas regras principais:

1. **"No Read Up" (NRU):** Utilizadores de um nível inferior não podem ler informações de um nível superior.
2. **"No Write Down" (NWD):** Utilizadores de um nível superior não podem escrever informações em um nível inferior.

A escolha desse modelo foi feita para garantir que cada utilizador tenha **acesso apenas às informações adequadas ao seu nível de segurança**, prevenindo a fuga de informações sensíveis.

2. Planeamento e Configuração

2.1. Estrutura Inicial do Sistema

Criamos três diretórios correspondentes a cada nível de segurança:

- `/dados/alto_grupo_72_78` (acesso restrito ao grupo de alto nível)
- `/dados/médio_grupo_72_78` (acesso restrito ao grupo de médio nível)
- `/dados/baixo_grupo_72_78` (acesso restrito ao grupo de baixo nível)

Cada diretório possui permissões específicas para impedir o acesso indevido.

2.2. Criação de Utilizadores e Grupos

Foram criados três utilizadores e grupos correspondentes:

Utilizador	Grupo	Nível de Acesso
user_grupo_72_78_alto	grupo_72_78_alto	Alto
user_grupo_72_78_medio	grupo_72_78_medio	Médio
user_grupo_72_78_baixo	grupo_72_78_baixo	Baixo

Cada utilizador foi adicionado ao grupo correspondente para garantir que apenas ele e os seus pares tivessem acesso ao respetivo nível de informações.

2.3. Configuração de Permissões

As seguintes permissões foram aplicadas:

- `chmod 770` para **alto** (apenas grupo pode ler e escrever)
- `chmod 750` para **médio** (impede leitura por níveis inferiores)
- `chmod 755` para **baixo** (público pode ler, mas apenas grupo pode escrever)

Essas configurações garantem o cumprimento do modelo **Bell-LaPadula**.

3. Implementação das Regras de Segurança

As regras do modelo foram implementadas conforme os princípios do **Bell-LaPadula**:

- **"No Read Up"** foi garantido removendo permissões de leitura para utilizadores de níveis inferiores.
- **"No Write Down"** foi aplicado restringindo permissões de escrita para níveis superiores.

Exemplo de aplicação de permissões:

```
sudo chmod 550 /dados/médio_grupo_72_78
sudo chmod 555 /dados/baixo_grupo_72_78
```

Isso garante que os utilizadores superiores não possam escrever em níveis inferiores.

4. Utilização de Chaves Assimétricas

Cada nível recebeu um par de chaves RSA (**privada e pública**) gerado via OpenSSL. A chave privada é utilizada para desencriptação e assinatura digital, enquanto a chave pública é usada para encriptação e verificação de assinaturas.

O processo de geração envolveu:

```
openssl genrsa -aes256 -out
/chaves_grupo_72_78/user_grupo_72_78_alto_private.pem 2048
```

```
openssl rsa -in /chaves_grupo_72_78/user_grupo_72_78_alto_private.pem -
pubout -out /chaves_grupo_72_78/user_grupo_72_78_alto_public.pem
```

Os mesmos passos foram realizados para os níveis **Médio** e **Baixo**.

A encriptação dos ficheiros foi feita com:

```
openssl rsautl -encrypt -inkey
/chaves_grupo_72_78/user_grupo_72_78_alto_public.pem -pubin -in
/dados/alto_grupo_72_78/confidencial_72_78.txt -out
/dados/alto_grupo_72_78/confidencial_72_78.txt.enc
```

A desencriptação ocorre apenas com a chave privada:

```
openssl rsautl -decrypt -inkey
/chaves_grupo_72_78/user_grupo_72_78_alto_private.pem -passin
pass:passphrasea -in /dados/alto_grupo_72_78/confidencial_72_78.txt.enc -
out ~/confidencial_72_78_decrypted.txt
```

5. Criação do Programa de Consulta Restrita

O programa de consulta restrita foi desenvolvido para garantir que cada utilizador acesse **apenas** os seus próprios arquivos encriptados. Ele solicita a passphrase e verifica permissões antes de realizar a desencriptação.

```
sudo -u user_grupo_72_78_medio /usr/local/bin/consulta_segura.sh
```

O script valida o utilizador e impede acesso a níveis não autorizados.

6. Testes e Validação

Os testes realizados confirmaram que:

- Utilizadores de níveis inferiores não conseguiam ler ficheiros superiores (**NRU aplicada corretamente**).
- Utilizadores de níveis superiores não conseguiam escrever em diretórios inferiores (**NWD aplicada corretamente**).
- Os ficheiros encriptados foram corretamente desencriptados apenas pelo utilizador autorizado.

7. Conclusão

O projeto implementou corretamente o modelo **Bell-LaPadula**, garantindo **confidencialidade e segurança** no controle de acesso aos dados. No entanto, o programa de consulta restrita apresentou dificuldades na configuração de permissões de acesso às chaves privadas, impedindo o seu total funcionamento.

Nota: Na pasta em que está o material todo não conseguimos copiar os ficheiros que faltam devido a um erro. Ao tentar copiar alguns dos ficheiros para uma pasta dava a mensagem de erro **"Permission denied"** devido à falta de tempo não conseguimos resolver esse problema.

```
[01/20/25]seed@VM:~$ # Copiar chaves
[01/20/25]seed@VM:~$ cp /chaves_grupo_72_78/*.pem ~/projeto_grupo_72_78/chaves/
cp: cannot stat '/chaves_grupo_72_78/*.pem': Permission denied
[01/20/25]seed@VM:~$
[01/20/25]seed@VM:~$ # Copiar ficheiros encriptados
[01/20/25]seed@VM:~$ cp /dados/alto_grupo_72_78/*.enc ~/projeto_grupo_72_78/fich
eiros_encriptados/
cp: cannot stat '/dados/alto_grupo_72_78/*.enc': Permission denied
[01/20/25]seed@VM:~$ cp /dados/médio_grupo_72_78/*.enc ~/projeto_grupo_72_78/fic
heiros_encriptados/
cp: cannot stat '/dados/médio grupo 72 78/*.enc': Permission denied
```