



Catarina Pereira
Inês Neves
Leonardo Martins
Miguel Gonçalves
Rui Barbosa

TP2 - Modelação do Controlo de Acesso

Uminho | 2024

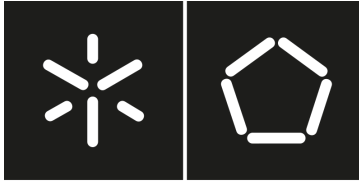


Universidade do Minho
Escola de Engenharia

Catarina da Cunha Malheiro da Silva Pereira
Inês Cabral Neves
Leonardo Dias Martins
Miguel José Mendes Gonçalves
Rui Fernando dos Santos Barbosa

TP2 - Modelação do Controlo de Acesso

2 de março de 2024



Universidade do Minho

Escola de Engenharia

Catarina da Cunha Malheiro da Silva Pereira
Inês Cabral Neves
Leonardo Dias Martins
Miguel José Mendes Gonçalves
Rui Fernando dos Santos Barbosa

TP2 - Modelação do Controlo de Acesso






Relatório Prático de Cibersegurança
Mestrado em Engenharia
Telecomunicações e Informática

Trabalho efetuado sob a orientação de:

Professor Doutor Henrique Manuel Dinis Santos

Identificação do Grupo

O Grupo 05 é constituído por cinco membros, sendo que quatro deles são do 1º ano do Mestrado em Engenharia de Telecomunicações e Informática (METI), sendo identificados por Pós-Graduação (PG) seguido dos seus números mecanográficos, enquanto o quinto membro pertence ao 4º ano de Mestrado Integrado em Engenharia de Telecomunicações e Informática (MIETI) e é identificado pelo código Aluno (A) seguido do seu número mecanográfico.

Imagem	Nome / Número Mecanográfico / E-mail institucional
	Catarina da Cunha Malheiro da Silva Pereira PG53733 pg537336@alunos.uminho.pt
	Inês Cabral Neves PG53864 pg53864@alunos.uminho.pt
	Leonardo Dias Martins PG53996 pg53996@alunos.uminho.pt
	Miguel José Mendes Gonçalves PG54101 pg54101@alunos.uminho.pt
	Rui Fernando dos Santos Barbosa A89370 a89370@alunos.uminho.pt

Índice

Identificação do Grupo	ii
Índice de Figuras	iv
Índice de Tabelas	v
Lista de Acrónimos	vi
1 Introdução	1
2 Revisão da Literatura	2
3 Recursos e Instrumentos Utilizados	3
4 Problema ao utilizar o modelo Bell-LaPadula	4
4.1 Análise do Modelo	5
4.2 Análise da Dinâmica de Fraude entre Alunos e Professores	6
5 Implantação Automática de Modelos em Infraestruturas TIC	7
5.1 Criação de utilizadores	7
5.2 Criação de grupos	8
5.3 Atribuição das Restrições	8
5.4 Resultados	9
6 Conclusão	11
Referências Bibliográficas	12

Índice de Figuras

1	<i>Lattice</i> de controlo de acesso do modelo BLP	4
2	Esquema das permissões.	7
3	Criação do utilizador correspondente à Reitoria.	7
4	Criação do utilizador correspondente aos Professores.	7
5	Criação do utilizador correspondente aos seguranças do Campi Universitário.	8
6	Criação dos grupos.	8
7	Associação dos modos de confidencialidade aos utilizadores.	8
8	Criação da pasta e atribuição de dono e grupo.	8
9	Atribuição de permissões sobre a pasta aos grupos.	9
10	Verificação das alterações realizadas.	9
11	Leitura e escrita por parte do utilizador reitor.	9
12	Criação, escrita e leitura do ficheiro do utilizador professor.	9
13	Leitura e escrita por parte do utilizador segurança.	10
14	Simulação de ataque por parte do segurança.	10
15	Simulação de ataque por parte do reitor.	10

Índice de Tabelas

Tabela 1: Associação das Entidades com as <i>labels</i>	5
---	---

Acrónimos

A Aluno.

AS Academic Services.

BLP Bell-LaPadula.

C Confidential.

METI Mestrado em Engenharia de Telecomunicações e Informática.

MIETI Mestrado Integrado em Engenharia de Telecomunicações e Informática.

P Public.

PG Pós-Graduação.

SC Strictly Confidential.

ScS Scientific Services.

TIC Tecnologia da Informação e Comunicação.

UC Unidade Curricular.

1 Introdução

Este relatório faz parte da Unidade Curricular (UC) Cibersegurança, do 2º semestre do 1º ano do Mestrado (Integrado) em Engenharia de Telecomunicações e Informática. Este projeto foi desenvolvido como resposta a um problema apresentado pelo docente.

O presente relatório aborda a construção de uma *lattice* de rótulos de segurança para os níveis de segurança Public (P) , Confidential (C) e Strictly Confidential (SC), e as categorias Academic Services (AS) e Scientific Services (ScS) num contexto universitário. O exercício é composto por duas partes distintas, sendo a primeira a construção de uma *lattice* e a verificação da possibilidade de prevenir a ocorrência de fraude por parte de um aluno em relação a um professor, considerando as propriedades fundamentais do modelo BLP e a classificação dos professores e alunos. A segunda parte aborda um possível processo de implantação automática desse modelo numa infraestrutura típica de Tecnologia da Informação e Comunicação (TIC).

O relatório baseia-se em conceitos formais do modelo Bell-LaPadula (BLP) , bem como em princípios de controlo de acesso, e tem como objetivo fornecer uma compreensão abrangente e prática da aplicação desses conceitos num ambiente universitário.

A seguir, serão apresentados os resultados da construção da *lattice*, a análise da viabilidade de prevenção de fraude no contexto universitário e as considerações sobre o processo de implantação automática do modelo numa infraestrutura de TIC.

2 Revisão da Literatura

O modelo BLP é um modelo formal de política de segurança informática introduzido por David Elliott Bell e Leonard J. LaPadula em 1973. Preocupa-se principalmente em manter a confidencialidade das informações e prevenir a divulgação não autorizada de dados confidenciais. O modelo BLP é baseado numa estrutura de rede matemática e define um conjunto de regras que governam como os indivíduos (utilizadores ou processos) podem aceder objetos (arquivos, recursos) com base nas autorizações de segurança.

Os principais componentes do modelo Bell-LaPadula incluem, [1, 2, 3]:

- 1. Regra de Não Divulgação (No Read Up):** Um indivíduo num nível de segurança mais baixo não pode ler informações num nível de segurança mais alto para evitar divulgação de informações confidenciais.
- 2. Regra de Não Escrita (No Write Down):** Um indivíduo num nível de segurança mais alto não pode escrever informações num nível de segurança mais baixo para evitar a contaminação de informações menos confidenciais.

Estas duas regras são essenciais para garantir a integridade, confidencialidade e disponibilidade dos dados em sistemas que requerem altos níveis de segurança, como ambientes militares e governamentais [4].

Existe também algumas propriedades do modelo Bell-LaPadula:

- Foco na confidencialidade dos dados e controlo de acesso.
- Divide o sistema em sujeitos e objetos, definindo um estado seguro e regras de transição.
- Utiliza rótulos de segurança para classificar informações, como *Top Secret*, *Secret*, *Confidential* e *Public*.

As maiores vantagens deste modelo BLP são as seguintes:

- Grande ênfase na confidencialidade, negligenciando a integridade dos dados.
- Dificuldade de implementação na prática e complexidade elevada.
- Possibilidade de alterações nos níveis de confidencialidade dos dados, tornando a gestão desafiadora.

Estas características ressaltam a importância do modelo Bell-LaPadula na proteção da confidencialidade dos dados, mas também destacam as limitações e desafios associados à sua aplicação prática.

O ataque BlindWrite [5] é um método de explorar vulnerabilidades remotas de *stack buffer* de pilha sem a necessidade do binário alvo ou do código-fonte. Este ataque é particularmente eficaz contra serviços que reiniciam após uma falha. Blind Write Protocol [6] é um método de lidar com operações de gravação intercaladas num sistema de banco de dados relacional sem a necessidade de bloqueio. Este protocolo pode aumentar significativamente o rendimento do banco de dados.

3 Recursos e Instrumentos Utilizados

Neste capítulo explora-se em detalhe os elementos que desempenham um papel fundamental na condução deste trabalho. O conjunto de recursos utilizados abrange uma ampla variedade de aplicações, cada uma desempenhando um papel específico e vital no desenvolvimento do trabalho.

Os recursos utilizados são:

- **Miro:** Utiliza-se a plataforma Miro para criar diagramas e esquemas, facilitando a visualização e a comunicação de conceitos complexos.
- **Plataformas de Comunicação:** Para facilitar a comunicação, colaboração e organização do trabalho desenvolvido pelo grupo, utiliza-se as plataformas Discord e Whatsapp.
- **OverLeaf:** Para a elaboração de relatórios em formato \LaTeX , utiliza-se a plataforma OverLeaf, que simplifica a formatação e a colaboração em documentos técnicos.

4 Problema ao utilizar o modelo Bell-LaPadula

Para abordar esta questão, desenvolveu-se uma *lattice* de segurança baseada no modelo Bell-LaPadula, conforme ilustrado na Figura 1. Esta estrutura considera três níveis de segurança: P (Public), C (Confidential) e SC (Strictly Confidential), juntamente com as categorias AS (Academic Services) e ScS (Scientific Services). É importante compreender como estas relações são estabelecidas.

O objetivo desta *lattice* é demonstrar as várias relações de dominância, começando com a etiqueta $(SC, \{AS, ScS\})$, que domina todas as outras. As etiquetas restantes seguem uma hierarquia, onde dominam as que estão abaixo delas, ou, no caso de pertencerem ao mesmo nível de segurança, dominam aquelas que possuem mais categorias.

Após a definição desta *lattice*, surge a necessidade de analisar cada etiqueta e remover aquelas que se mostram desnecessárias para o sistema. Com este propósito, elabora-se uma tabela que relaciona as etiquetas definidas com os utilizadores/objetos do sistema, visando excluir as etiquetas não pertinentes.

Além disso, foi estabelecida uma associação entre as etiquetas e cargos reais para uma melhor compreensão do modelo, respondendo também a questões relacionadas com alunos, professores e a possibilidade de fraude.

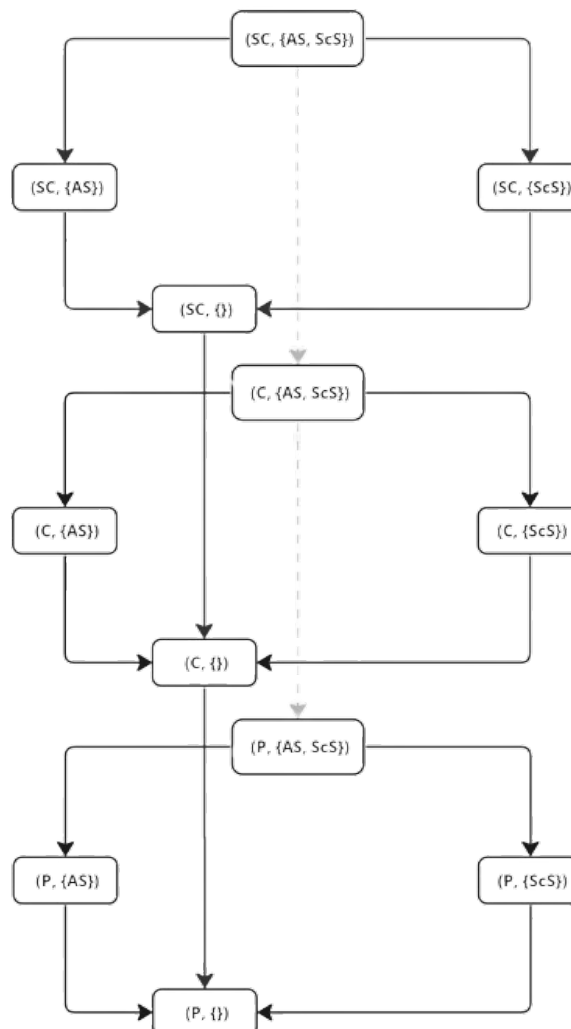


Figura 1: *Lattice* de controlo de acesso do modelo BLP

4.1 Análise do Modelo

Após a criação da *lattice*, torna-se imperativo analisar cada etiqueta e remover aquelas que se revelam dispensáveis para o sistema. Com esse propósito, elaborou-se uma tabela na qual foram estabelecidas correspondências entre as *labels* definidas e as entidades do sistema. Esta abordagem visa identificar e excluir etiquetas que não acrescentam valor ou não são relevantes para os objetivos do sistema, contribuindo assim para uma estrutura mais refinada e eficiente.

Tabela 1: Associação das Entidades com as *labels*.

Nível de Segurança	Label	Entidades
Strictly Confidential	$(SC, \{As, ScS\})$	Reitoria
	$(SC, \{As\})$	Diretores dos Serviços Académicos
	$(SC, \{ScS\})$	Diretores dos Serviços de Investigação
	$(SC, \{\})$	Diretores dos Serviços de Ação Social
Confidential	$(C, \{As, ScS\})$	Docentes
	$(C, \{As\})$	Estudantes
	$(C, \{ScS\})$	Investigadores
	$(C, \{\})$	Dados Logísticos dos Campi
Public	$(P, \{As, ScS\})$	Seguranças dos Campi Universitário
	$(P, \{As\})$	Novos Estudantes
	$(P, \{ScS\})$	RepositórioUM

A tabela apresentada ilustra a associação de entidades com níveis e *labels* de segurança. Esta associação é crucial para manter a integridade do sistema de controlo de acesso. As relações de dominância entre os *labels* indicam uma estrutura hierárquica, com a Reitoria a ocupar a posição mais elevada. A escolha das entidades para cada *label* é baseada nas suas funções e responsabilidades dentro da universidade, garantindo que cada entidade tenha o acesso necessário para desempenhar eficazmente as suas funções. A presença da Reitoria como *label* dominante sublinha a sua influência e a necessidade de manter todos os rótulos para um controlo de acesso eficaz. A remoção de qualquer etiqueta poderá comprometer a integridade do sistema. Portanto, a manutenção de todas as etiquetas é essencial para a segurança e funcionalidade do sistema.

Para explicar as escolhas das relações entre as etiquetas e as entidades:

- $(SC, \{AS, ScS\})$: A Reitoria foi escolhida porque gere toda a universidade, precisando de acesso amplo às informações académicas e de investigação para tomar decisões abrangentes.
- $(SC, \{AS\})$: Os Serviços Académicos possuem esta etiqueta devido à sua responsabilidade pela gestão dos registos dos alunos e questões académicas, necessitando de acesso completo a essas informações.
- $(SC, \{ScS\})$: Os Diretores dos Serviços de Investigação foram escolhidos por supervisionarem atividades de investigação, precisando de acesso a informações confidenciais relacionadas à investigação.

4.2. ANÁLISE DA DINÂMICA DE FRAUDE ENTRE ALUNOS E PROFESSORES

- $(SC, \{\})$: Os Diretores dos Serviços de Ação Social são responsáveis pelo suporte social aos alunos (por exemplo, residências), necessitando de acesso a recursos e informações relevantes.
- $(C, \{As, ScS\})$: Os docentes possuem esta etiqueta devido à sua responsabilidade tanto no ensino quanto na investigação, requerendo acesso a informações confidenciais em ambos os domínios.
- $(C, \{As\})$: Os estudantes foram atribuídos a esta etiqueta para aceder a informações confidenciais sobre o seu próprio desempenho académico.
- $(C, \{ScS\})$: Esta etiqueta foi atribuída aos Investigadores, indica que eles têm acesso a informações confidenciais relacionadas à investigação. Isso permite que conduzam estudos académicos e científicos, coordenem projetos e colaborem com outros investigadores de forma eficaz.
- $(C, \{\})$: Os Dados Logísticos dos Campi não estão associados a nenhum nível específico de segurança, ou seja, não têm restrições de acesso. Isto significa que são informações gerais sobre logística dos campi universitários, como gestão de infraestrutura e distribuição de recursos, que estão disponíveis para consulta sem restrições. Estes dados podem ser acessados por várias partes interessadas dentro da universidade para facilitar a gestão eficiente dos recursos e a operação dos campi.
- $(P, \{As, ScS\})$: Os seguranças dos campi universitários possuem esta etiqueta para garantir a segurança das instalações e responder a incidentes, necessitando de acesso a informações administrativas e sensíveis relacionadas à segurança.
- $(P, \{As\})$: Os novos estudantes possuem esta etiqueta para acessar informações gerais e orientações específicas para novos alunos.
- $(P, \{ScS\})$: O RepositórioUM que é um repositório de publicações académicas para a comunidade universitária. Ao ter esta etiqueta, o RepositórioUM está disponível para acesso público, mas também pode conter informações sensíveis ou restritas, como teses de mestrado ou doutoramento.

4.2 Análise da Dinâmica de Fraude entre Alunos e Professores

Após a análise do modelo de Bell-LaPadula, é possível inferir a existência de uma relação de dominância entre o professor $(C, \{AS, ScS\})$ e o aluno $(C, \{AS\})$. No contexto deste modelo, duas condições chave são utilizadas para assegurar a confidencialidade. Uma etiqueta num nível hierárquico superior pode visualizar dados das etiquetas inferiores, mas não pode escrever nelas (regra “no write down”). Por outro lado, uma etiqueta num nível hierárquico inferior só pode escrever em níveis superiores, sem capacidade de leitura (regra “no read up”).

Qualquer arquivo disponibilizado pelo professor, como testes ou notas, será classificado com a sua etiqueta. Isto implica que alguém com um nível de segurança inferior, como o aluno, não terá permissão para aceder a esses arquivos de acordo com a regra “no read up”. No entanto, esta regra não impede o aluno de escrever em arquivos acima do seu nível hierárquico, permitindo assim a possibilidade de fraude e comprometimento da integridade dos arquivos contendo informações sensíveis das avaliações.

Nesta perspetiva, em caso de tentativa de fraude, onde o aluno procura aceder aos dados do professor, o modelo oferece proteção, uma vez que as condições mencionadas anteriormente garantem a confidencialidade e previnem ataques à integridade dos dados. No entanto, o aluno tem a capacidade de escrever, o que coloca em risco a integridade do sistema e abre a possibilidade de fraude, como escrever em arquivos com notas falsas sem o conhecimento do professor. Sim, é possível o aluno cometer fraude.

Na prática, o aluno poderia modificar um arquivo contendo as notas de uma disciplina para o seu próprio benefício, adulterando assim a sua própria avaliação. Esta vulnerabilidade destaca a importância da implementação cuidadosa e monitorização constante das políticas de segurança para mitigar riscos e garantir a integridade e confidencialidade dos dados no ambiente universitário.

5 Implantação Automática de Modelos em Infraestruturas TIC

Neste exercício, propõe-se a elaboração de um processo de implementação automática, numa infraestrutura de TIC, do modelo construído. A implementação foi realizada num ambiente Linux (Ubuntu). Para exemplificar a resolução deste problema, foram utilizadas apenas três *labels*: ($SC, \{AS, ScS\}$), ($C, \{AS, ScS\}$) e ($C, \{AS, ScS\}$). Conforme o modelo Bell-LaPadula, onde a primeira *label* tem precedência sobre a segunda e a segunda sobre a terceira, no contexto do ambiente Linux (Ubuntu), as *labels* serão representadas por grupos com diferentes permissões de um arquivo contido numa pasta criada por uma entidade de *label* ($C, \{AS, ScS\}$).

O objetivo deste exercício é desenvolver um processo viável de implementação automática numa infraestrutura de TIC conforme o modelo Bell-LaPadula. Para ilustrar este processo com um exemplo prático, optou-se por utilizar as entidades: Reitoria, Docentes e Seguranças dos Campi Universitário, que estão associados aos níveis *Strictly Confidential*, *Confidential* e *Public*, respetivamente.

A Figura 2 ilustra as permissões, onde a Reitoria possui permissão de leitura, os docentes têm permissão de leitura e escrita, e os Seguranças dos Campi Universitários possuem apenas permissão de escrita.

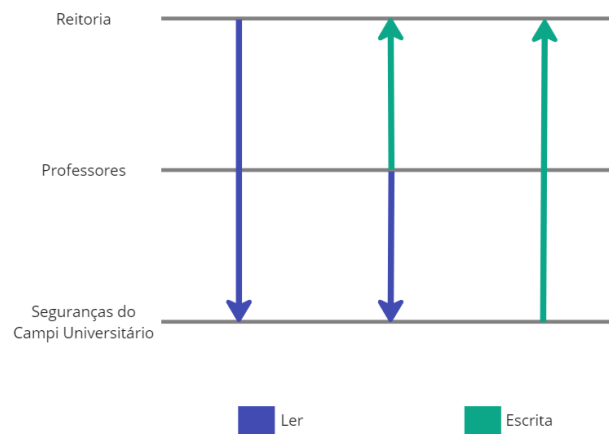


Figura 2: Esquema das permissões.

5.1 Criação de utilizadores

Primeiramente, foram criados utilizadores correspondentes a cada uma das entidades: Reitoria (Reitor Rui Vieira de Castro), Docentes (Professor Henrique Santos) e Seguranças do Campi Universitário (Segurança Nuno Silva). Estes utilizadores foram criados com os seguintes nomes de utilizador: `reitor`, `professor` e `seguranca`.

A Figura 3 representa a entidade da Reitoria. A Figura 4 representa a entidade dos docentes, e a Figura 5 representa a entidade dos Seguranças do Campi Universitário.

```
lnes@lnes-VirtualBox:~$ sudo adduser reitor
A adicionar o utilizador 'reitor' ...
A adicionar o novo grupo 'reitor' (1002) ...
A adicionar o novo utilizador 'reitor' (1002) com grupo 'reitor' ...
A criar directório home '/home/reitor' ...
A copiar ficheiros de '/etc/skel' ...
Nova palavra-passe:
Digite novamente a nova palavra-passe:
passwd: a palavra-passe foi actualizada com sucesso
A alterar a informação de utilizador de reitor
Introduza o novo valor, ou carregue em ENTER para o valor pré-definido
Nome Completo []: Rui Vieira De Castro
Número da Sala []:
Telefone do Emprego []:
Telefone de casa []:
Outra Informação []:
Esta informação é correcta? [Y/n] y
lnes@lnes-VirtualBox:~$
```

Figura 3: Criação do utilizador correspondente à Reitoria.

```
lnes@lnes-VirtualBox:~$ sudo adduser professor
A adicionar o utilizador 'professor' ...
A adicionar o novo grupo 'professor' (1003) ...
A adicionar o novo utilizador 'professor' (1003) com grupo 'professor' ...
A criar directório home '/home/professor' ...
A copiar ficheiros de '/etc/skel' ...
Nova palavra-passe:
Digite novamente a nova palavra-passe:
passwd: a palavra-passe foi actualizada com sucesso
A alterar a informação de utilizador de professor
Introduza o novo valor, ou carregue em ENTER para o valor pré-definido
Nome Completo []: Henrique Santos
Número da Sala []:
Telefone do Emprego []:
Telefone de casa []:
Outra Informação []:
Esta informação é correcta? [Y/n] y
lnes@lnes-VirtualBox:~$
```

Figura 4: Criação do utilizador correspondente aos Professores.

5.2. CRIAÇÃO DE GRUPOS

```
ines@ines-VirtualBox:~$ sudo adduser seguranca
A adicionar o utilizador 'seguranca' ...
A adicionar o novo grupo 'seguranca' (1004) ...
A adicionar o novo utilizador 'seguranca' (1004) com grupo 'seguranca' ...
A criar directório home '/home/seguranca' ...
A copiar ficheiros de '/etc/skel' ...
Nova palavra-passe:
Digite novamente a nova palavra-passe:
passwd: a palavra-passe foi actualizada com sucesso
A alterar a informação de utilizador de seguranca
Introduza o novo valor, ou carregue em ENTER para o valor pré-definido
Nome Completo []: Nuno Silva
Número da Sala []:
Telefone do Emprego []:
Telefone de Casa []:
Outra Informação []:
Esta informação é correcta? [Y/n] y
ines@ines-VirtualBox:~$
```

Figura 5: Criação do utilizador correspondente aos seguranças do Campi Universitário.

5.2 Criação de grupos

Foram estabelecidos grupos correspondentes a diferentes níveis de confidencialidade. Na Figura 6, apresenta-se a criação dos três grupos distintos de confidencialidade.

```
ines@ines-VirtualBox:~$ sudo groupadd StrictlyConfidential
ines@ines-VirtualBox:~$ sudo groupadd Confidential
ines@ines-VirtualBox:~$ sudo groupadd Public
ines@ines-VirtualBox:~$
```

Figura 6: Criação dos grupos.

Sendo depois inseridos em cada grupo os diferentes os utilizadores criados na Figura 6, de modo a que cada um deles atenda as restrições que irão ser associadas a cada grupo ilustradas na Figura 7.

```
ines@ines-VirtualBox:~$ sudo usermod -g StrictlyConfidential reitor
ines@ines-VirtualBox:~$ sudo usermod -g Confidential professor
ines@ines-VirtualBox:~$ sudo usermod -g Public seguranca
ines@ines-VirtualBox:~$
```

Figura 7: Associação dos modos de confidencialidade aos utilizadores.

5.3 Atribuição das Restrições

Neste passo foi criada uma pasta com o nome *ciberseguranca* e posteriormente foi lhe atribuída como dono da pasta o utilizador *professor* e o grupo do tipo *Confidential* como ilustrada na Figura 8. O intuito desta pasta será o docente *professor* guardar as pautas da UC de Cibersegurança.

```
ines@ines-VirtualBox:~$ mkdir Ciberseguranca
ines@ines-VirtualBox:~$
ines@ines-VirtualBox:~$ sudo chown -R professor Ciberseguranca/
ines@ines-VirtualBox:~$ sudo chown -R :Confidential Ciberseguranca/
```

Figura 8: Criação da pasta e atribuição de dono e grupo.

De seguida, foi atribuído a cada grupo de utilizadores diferentes tipos de acesso à pasta conforme a hierarquia criada no diagrama *lattice*, demonstrado na Figura 9:

- **StrictlyConfidential** – acesso de leitura.
- **Confidential** – acessos de leitura e escrita.
- **Public** – acesso de escrita.

5.4. RESULTADOS

```
ines@ines-VirtualBox:~$ sudo setfacl -R -d -m g:StrictlyConfidential:rx Ciberseguranca/
ines@ines-VirtualBox:~$ sudo setfacl -R -d -m g:Confidential:rwX Ciberseguranca/
ines@ines-VirtualBox:~$ sudo setfacl -R -d -m g:Public:wx Ciberseguranca/
```

Figura 9: Atribuição de permissões sobre a pasta aos grupos.

Para averiguar sobre as alterações realizadas ao longo dos comandos realizados representados na Figura 10.

```
ines@ines-VirtualBox:~$ getfacl Ciberseguranca/
# file: Ciberseguranca/
# owner: professor
# group: Confidential
user::rwX
group::rwX
other::r-x
default:user::rwX
default:group::rwX
default:group:StrictlyConfidential:r-x
default:group:Confidential:rwX
default:group:Public:-wx
default:mask::rwX
default:other::r-x
ines@ines-VirtualBox:~$
```

Figura 10: Verificação das alterações realizadas.

5.4 Resultados

Os resultados mostram que o utilizador com permissões de leitura e escrita (docente) pode adicionar e visualizar conteúdo na pasta, Figura 12. No entanto, outros utilizadores com permissões diferentes, como o reitor (apenas leitura), Figura 11, e o segurança (sem acesso), não conseguem modificar o conteúdo da pasta, Figura 13, conforme o esperado de acordo com as restrições definidas.

Na Figura 11 observa-se a tentativa de escrita por parte do utilizador “reitor”, como este pertence à reitoria, ele possui apenas permissão de leitura no ficheiro, a operação de escrita é negado devido ao facto do utilizador encontrar-se num nível superior de *lattice*. Ao analisar a Figura 11, nota-se que, quando o utilizador “reitor” tenta escrever no ficheiro, a permissão é recusada, refletindo a implementação eficaz das restrições de acesso.

```
professor@ines-VirtualBox:/home/ines$ su reitor
Palavra-passe:
reitor@ines-VirtualBox:/home/ines$ cd Ciberseguranca
reitor@ines-VirtualBox:/home/ines/Ciberseguranca$ echo "Catarina - 18 valores" >> resultados.txt
bash: resultados.txt: Permissão recusada
reitor@ines-VirtualBox:/home/ines/Ciberseguranca$ cat resultados.txt
Ines - 16 valores
reitor@ines-VirtualBox:/home/ines/Ciberseguranca$
```

Figura 11: Leitura e escrita por parte do utilizador reitor.

Na Figura 12 observa-se o que utilizador “professor”, detém permissões para ler e escrever no ficheiro “resultados.txt”, dado o seu nível de segurança. Pode-se observar o professor a adicionar uma nova nota aos resultados e a observar o conteúdo da pasta.

```
ines@ines-VirtualBox:~$ su professor
Palavra-passe:
professor@ines-VirtualBox:/home/ines$ cd Ciberseguranca
professor@ines-VirtualBox:/home/ines/Ciberseguranca$ echo "Ines - 16 valores" >> resultados.txt
professor@ines-VirtualBox:/home/ines/Ciberseguranca$ cat resultados.txt
Ines - 16 valores
professor@ines-VirtualBox:/home/ines/Ciberseguranca$
```

Figura 12: Criação, escrita e leitura do ficheiro do utilizador professor.

A Figura 13 observa-se a tentativa de leitura por parte do utilizador “segurança”, como este pertence aos Seguranças dos Campi Universitário, ele possui apenas permissão de escrita no ficheiro, a operação de leitura é negado devido ao facto do utilizador encontrar-se num nível inferior de *lattice*. Ao analisar a Figura 13, nota-se

5.4. RESULTADOS

que, quando o utilizador “segurança” tenta ler no ficheiro, a permissão é recusada, refletindo a implementação eficaz das restrições de acesso.

```
reitor@ines-VirtualBox:/home/ines$ su segurança
Palavra-passe:
seguranca@ines-VirtualBox:/home/ines$ cd Ciberseguranca
seguranca@ines-VirtualBox:/home/ines/Ciberseguranca$ echo "Catarina - 18 valores" >> resultados.txt
seguranca@ines-VirtualBox:/home/ines/Ciberseguranca$ cat resultados.txt
cat: resultados.txt: Permissão recusada
seguranca@ines-VirtualBox:/home/ines/Ciberseguranca$
```

Figura 13: Leitura e escrita por parte do utilizador segurança.

A Figura 14 apresenta uma simulação de um ataque *blindwrite* utilizando o utilizador “segurança”, que possui permissões de escrita no ficheiro “resultados.txt”, é possível constatar como o utilizador “segurança” consegue apagar integralmente o conteúdo do ficheiro de texto e substituí-lo por uma frase qualquer, na figura no utilizador “professor” verifica-se que o ataque ocorreu com sucesso.

```
seguranca@ines-VirtualBox:/home/ines/Ciberseguranca$ echo ataque > /home/ines/Ciberseguranca/resultados.txt
seguranca@ines-VirtualBox:/home/ines/Ciberseguranca$ su professor
Palavra-passe:
professor@ines-VirtualBox:/home/ines/Ciberseguranca$ cat resultados.txt
ataque
professor@ines-VirtualBox:/home/ines/Ciberseguranca$
```

Figura 14: Simulação de ataque por parte do segurança.

A Figura 15 apresenta uma simulação de um ataque *blindwrite* utilizando o utilizador “reitor”, que possui permissões de leitura no ficheiro “resultados.txt”, é possível constatar que o utilizador “reitor” não consegue apagar integralmente o conteúdo do ficheiro de texto ou substituí-lo por uma frase qualquer, o que significa que o ataque não é concretizado com sucesso, o que valida as permissões existentes no utilizador “reitor”.

```
professor@ines-VirtualBox:/home/ines/Ciberseguranca$ su reitor
Palavra-passe:
reitor@ines-VirtualBox:/home/ines/Ciberseguranca$ echo ataque > /home/ines/Ciberseguranca/resultados.txt
bash: /home/ines/Ciberseguranca/resultados.txt: Permissão recusada
reitor@ines-VirtualBox:/home/ines/Ciberseguranca$
```

Figura 15: Simulação de ataque por parte do reitor.

6 Conclusão

Com a conclusão deste trabalho prático, é evidente que o modelo Bell-LaPadula apresenta limitações significativas no que diz respeito à segurança. Ao concentrar exclusivamente na confidencialidade dos sistemas operativos, o modelo enfrenta desafios consideráveis diante do crescente número de vulnerabilidades encontradas nesses sistemas e nas redes de computadores. Este cenário atual torna possível diversas formas de alteração dos níveis de segurança, comprometendo assim a própria confidencialidade proposta pelo modelo. Portanto, é necessário considerar que o modelo Bell-LaPadula pode não ser adequado aos tempos atuais, dada a sua limitação em lidar com os desafios emergentes em cibersegurança.

Além disso, este trabalho proporcionou ao grupo uma oportunidade valiosa de aprofundar o conhecimento sobre o modelo Bell-LaPadula e outros modelos de controlo de acesso. O processo de implementação prática durante o projeto contribuiu significativamente para o desenvolvimento das habilidades necessárias para aplicar os conceitos aprendidos em aulas de Cibersegurança. Assim, conclui-se que este trabalho não apenas aumentou o entendimento teórico, mas também melhorou as capacidades práticas de implementação dos conhecimentos adquiridos.

Em resumo, a realização deste trabalho prático destacou não apenas as limitações do modelo Bell-LaPadula em relação à segurança, mas também proporcionou uma valiosa experiência de aprendizado para o grupo. Ao expandir o conhecimento sobre modelos de controlo de acesso e suas fragilidades, este trabalho contribuiu para uma compreensão mais ampla e aprofundada do funcionamento dos sistemas de segurança em ambientes de TI contemporâneos.

Referências Bibliográficas

- [1] Henrique Santos. *Segurança em Redes de Computadores (MIETI 4º Ano/S2-H208N4) Access Control and Authentication*. Dpt. Sistemas de Informação, Ext. 3302. 2017.
- [2] Andrés Jiménez-Ramírez et al. "Automatic generation of questionnaires for supporting users during the execution of declarative business process models". Em: vol. 176 LNBIP. Springer Verlag, 2014, pp. 146–158. ISBN: 9783319066943. DOI: 10.1007/978-3-319-06695-0_13.
- [3] Carlos Maziero. "Modelos de controle de acesso". Em: *Lecture Notes in Business Information Processing* 176 LNBIP (2019), pp. 55–72.
- [4] Rafael Rodrigues Obelheiro. *Modelos de Segurança baseados em papéis para Sistemas de Larga Escala: A Proposta RBAC-JACOWEB*. <https://core.ac.uk/download/pdf/30362882.pdf>. Acedido em 28 de fevereiro de 2024. Fevereiro de 2001.
- [5] Andrea Bittau et al. "Hacking Blind". Em: *2014 IEEE Symposium on Security and Privacy*. 2014, pp. 227–242. DOI: 10.1109/SP.2014.22.
- [6] Khairul Anshar, Nanna Suryana e Noraswaliza Binti Abdullah. "Blind Write Protocol". Em: 2018, pp. 868–879. DOI: 10.1007/978-3-319-76348-4_83.