

**Universidade do Minho**  
Escola de Engenharia

## CIBERSEGURANÇA

# TP2 - CONTROLO DE ACESSO

*Autores:*

Inês Barreira Marques - a84913@alunos.uminho.pt

José Carlos Peixoto Ferreira - a85497@alunos.uminho.pt

Marcos Alexandre Ferreira Martins a84481@alunos.uminho.pt

Rui Filipe Ribeiro Freitas pg47639@alunos.uminho.pt

Tiago João Pereira Ferreira pg47692@alunos.uminho.pt

20 de março de 2022

# Índice

<b>1</b>	<b>Introdução</b>	<b>3</b>
<b>2</b>	<b>Modelo Bell-LaPadula</b>	<b>4</b>
<b>3</b>	<b><i>Lattice</i> dos níveis de segurança</b>	<b>5</b>
<b>4</b>	<b>Fraude por parte do Aluno</b>	<b>8</b>
<b>5</b>	<b>Processo de implementação automático</b>	<b>9</b>
<b>6</b>	<b>Conclusão</b>	<b>12</b>

## Lista de Figuras

1	Modelo Bell-LaPadula . . . . .	4
2	<i>Lattice</i> dos níveis de segurança . . . . .	5
3	Exemplo Serviços Académicos . . . . .	10
4	Exemplo Funcionário . . . . .	11
5	Exemplo Visitante . . . . .	11

## Lista de Tabelas

1	Entidades de nível Strictly Confidential. . . . .	6
2	Entidades de nível Confidential. . . . .	6
3	Entidades de nível Public. . . . .	7

# 1 Introdução

No âmbito da unidade curricular de cibersegurança foi proposto o desenvolvimento de um modelo de controlo de acesso, num contexto universitário, baseado no modelo de Bell-LaPadula.

Os mecanismos de controlo de acesso têm como objetivo autorizar ou bloquear o acesso a informações tendo em conta o sujeito que tenta aceder, tendo por base este conceito teremos que realizar a sua aplicação num contexto universitário. Para isso vai ser necessário primeiramente identificar as entidades e atribuir as *labels* para cada uma delas, de seguida vai ser realizada uma *lattice* com o objetivo de dividir os vários indivíduos de uma universidade tendo em conta o seu grau de confiança. Por último deverá ser elaborada uma implementação automática do modelo BLP numa estrutura TIC baseada na *lattice* criada.

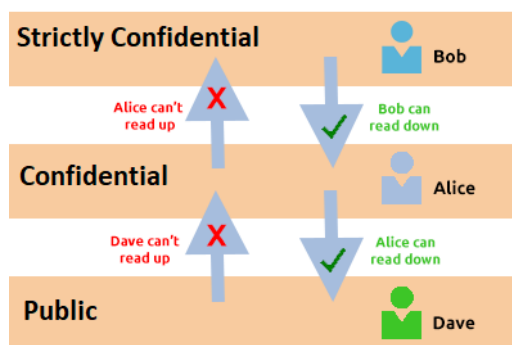
De modo a sermos capazes de cumprir com o proposto no enunciado foi necessário um estudo aprofundado do que é o modelo BLP e como realizar a sua implementação num contexto real.

## 2 Modelo Bell-LaPadula

O Modelo Bell-LaPadula (BLP) é um modelo que garante a confidencialidade da informação, uma vez que não permite o acesso não autorizado da mesma. Este modelo é composto por um conjunto de regras que se baseiam em níveis de segurança para objetos e autorizações para assuntos.

Este modelo baseia-se em 3 regras principais, que seguidas ao pormenor garantem a confidencialidade pretendida. As regras são as seguintes:

- Uma pessoa num determinado nível de segurança não pode ler um objeto com um nível de segurança mais alto;
- Uma pessoa num determinado nível de segurança não pode escrever em qualquer objeto de nível de segurança mais baixo;
- Uma pessoa num determinado nível de segurança pode ler e escrever em qualquer objeto do seu nível de segurança.



**Figura 1:** Modelo Bell-LaPadula

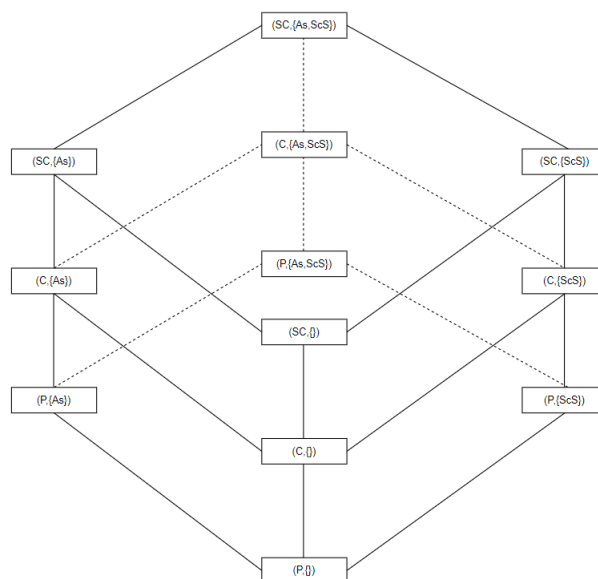
Na figura 1 é possível observar o funcionamento deste modelo. Um sujeito que pertença ao grupo *Confidential* terá permissões para ler informações do seu nível e inferiores mas não de níveis superiores. Quando à escrita este tem permissões de escrever no seu nível e superiores mas não em inferiores. Estas regras são a base para que haja confidencialidade em qualquer que seja o ambiente em que este modelo é aplicado.

### 3 *Lattice* dos níveis de segurança

De acordo com o enunciado foi proposta a elaboração de uma *lattice* de níveis de segurança tendo em conta 3 níveis de acesso, estritamente confidencial(SC), confidencial(C) e público(P) sendo que o nível SC tem dominância sobre o nível C e o nível C sobre o nível P. Por consequência o nível SC possui dominância sobre o nível P.

- **Strictly Confidential (SC)** - Nível mais alto da *lattice*, estritamente confidencial
- **Confidential (C)** - Nível intermédio da *lattice*, confidencial
- **Public (P)** - Nível mais baixo da *lattice*, publico

Para além dos níveis de segurança também temos de ter em conta 2 categorias que permitem identificar os serviços presentes no contexto universitário, os **serviços académicos(As)** e os **serviços científicos(ScS)**. A conjunção dos níveis de segurança com as categorias criam *labels* que no nosso caso em particular são criadas 12 *labels* em que cada uma tem dominância sobre a label inferior. No contexto universitário era possível adicionar pelo menos mais uma categoria como por exemplo os serviço administrativo mas caso este fosse adicionado, em vez de 12 *labels* seriam criadas 48 *labels*. De seguida é apresentada a *lattice* desenvolvida para o contexto universitário tendo em conta o problema proposto.



**Figura 2:** *Lattice* dos níveis de segurança

De acordo com a *lattice* apresentada anteriormente foram atribuídas entidades a cada nível de acesso, de forma a ser possível obter uma análise mais aprofundada do problema. As tabelas seguintes mostram a atribuição feita pelo grupo.

Tal como foi previamente descrito, a *lattice* possui relações de dominância entre níveis de segurança, no entanto, essas relações acontecem também dentro do mesmo nível.

Label	Entidade
(SC,{As,ScS })	Reitoria
(SC,{As})	Serviços Acadêmicos
(SC,{ScS})	Serviços de Investigação
(SC,{ })	Diretores de Curso

**Tabela 1:** Entidades de nível Strictly Confidential.

No nível Strictly Confidential, a Reitoria possui relação de dominância sobre os Serviços Acadêmicos e os Serviços de Investigação, e estes dois possuem dominância sobre os Diretores de Cursos. Consequentemente, a Reitoria tem dominância sobre os Diretores de Curso. Foi atribuída à Reitoria a label **(SC,{As,ScS})**, uma vez que esta é a entidade com maior poder e gere todas as entidades abaixo. Para os Serviços Acadêmicos foi atribuída a label **(SC,{As})** uma vez que gerem a parte Acadêmica da Universidade. Aos Serviços de Investigação foi atribuída a label **(SC,{ScS})** uma vez que é onde ocorre a gestão da parte Científica, como trabalhos e artigos. Para os Diretores de Curso foi atribuída a label **(SC { })**, uma vez que tem de comunicar com os serviços acima sobre o estado do curso e fazer a gestão do curso, que inclui professores e alunos.

Label	Entidade
(C,{As,ScS })	Professores
(C,{As})	Alunos
(C,{ScS})	Alunos/Pessoas externas a fazer investigação
(C,{ })	Funcionários

**Tabela 2:** Entidades de nível Confidential.

Neste nível a entidade com mais poder são os Professores, que dominam os Alunos e os Alunos/Pessoas em Investigação, e estas duas possuem dominância sobre os Funcionários o

que faz com que os Professores possuam dominância sobre os Funcionários. Nos Professores foi colocada a *label*  $(C, \{As, ScS\})$ , uma vez que estes podem atuar tanto a nível académico através de aulas como a nível científico através de trabalhos/orientação de investigação. Os Alunos atuam ao nível Académico, nas aulas, daí a sua *label*  $(C, \{As\})$ . Quanto aos funcionários foi colocada a *label*  $(C, \{ \})$  devido ao facto de eles não se encontrarem nem na categoria Académica nem Científica mas ao mesmo tempo existirem vários tipos de funcionários na universidade para ajudar e fornecer serviços a alunos e professores.

Label	Entidade
$(P, \{As, ScS\})$	Visitantes/Leitores de artigos

**Tabela 3:** Entidades de nível Public.

Pela análise desta última tabela que representa o nível de Public foram retiradas três das labels originais, existindo apenas a label de  $(P, \{AS, ScS\})$  devido ao facto de não existirem muitas informações públicas disponíveis sobre a universidade, sendo que as que existem pertencem a ambas as categorias (Académica e Científica) e são meramente informativas ou sobre aspetos da própria universidade ou sobre ofertas educativas e/ou documentos publicados por pessoas dentro da instituição. Daí termos definido como Visitantes/Leitores de artigos.



## 4 Fraude por parte do Aluno

Seguindo o modelo de Bell-LaPadulla baseado puramente na confidencialidade e a *lattice* realizada pelo grupo, tanto o Professor como o Aluno encontram-se no mesmo nível de segurança, Confidential, porém o nível do Professor possui dominância sobre o Aluno.

No modelo BLP existem as regras de No Read Up e a regra No Write Down, que ditam que um usuário não pode ler de um nível superior ao seu, e não pode escrever para um nível inferior ao seu.

Tendo em conta estas características do modelo, um Aluno pode explorar a hipótese de fazer batota, como por exemplo a modificação de uma pauta depois de a ter recebido do professor. Esta batota basear-se-ia na escrita de um novo ficheiro, copiado do ficheiro original, alterando valores falsos conforme o pretendido pelo Aluno. Há a possibilidade de este exemplo acontecer, uma vez que o Professor e o Aluno pertencem ao mesmo nível e pertencem aos Academic Services. Isto significa que o aluno pode ler os documentos que são escritos pelo Professor, e copiando um desses documentos, poderá enviá-lo para os Serviços Académicos que estão no nível acima. Os Serviços Académicos por sua vez não se irão aperceber quem terá enviado o novo documento devido à confidencialidade imposta pelo modelo.

Caso os documentos fossem do tipo Scientific Services (ScS), o Aluno não conseguiria cometer fraude uma vez que na sua label  $(C, \{As\})$  não possui a categoria dos ScS. Deste modo, é possível afirmar que a batota pode acontecer, desde que as condições sejam as descritas anteriormente. Apesar de o modelo fornecer confidencialidade, este não consegue garantir a integridade dos dados que o usuário pode introduzir ao escrever em níveis superiores, daí ser explorada essa vulnerabilidade dos sistemas que implementam o modelo BLP.

## 5 Processo de implementação automático

O segundo objetivo desta TP é a implementação automática do modelo BLP numa estrutura TIC, para tal, seguimos como estrutura base a lattice apresentada anteriormente.

A *lattice* desenvolvida possui três níveis de segurança, o Strictly Confidential (SC) que é o primeiro nível, ou nível mais alto, o Confidential (C) que corresponde ao segundo nível, ou nível intermédio e o Public (P) que corresponde o terceiro o nível, ou o nível mais baixo.

Para implementar o modelo foi criada uma diretoria onde são registadas as entradas na Universidade. Foram criados três utilizadores, em que cada um possui um nível diferente de segurança. Foi criado o utilizador Serviços Académicos, que conta com o nível de acesso SC, o utilizador funcionário, com o nível de acesso C, e o utilizador visitante com o menor nível de acesso, o P. Na diretoria criada os Serviços Académicos possuem apenas a opção de ler os ficheiros, o funcionário pode ler e escrever no ficheiro e o visitante apenas escrever no mesmo.

Abaixo encontram-se os comandos efetuados para a criação dos diferentes utilizadores e grupos.

- `sudo adduser servicos_academicos_uminho`
- `sudo adduser funcionario_entrada_uminho`
- `sudo adduser visitante_uminho`
- `sudo addgroup SC`
- `sudo addgroup C`
- `sudo addgroup P`

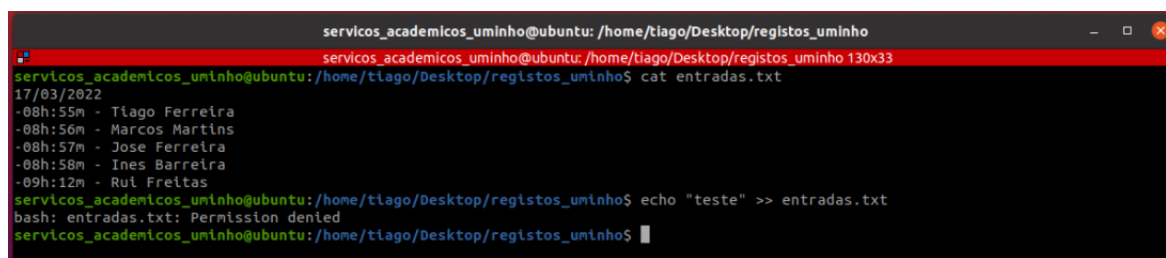
O passo seguinte foi a atribuição a cada user o seu respetivo grupo.

- `sudo usermod -g SC servicos_academicos_uminho`
- `sudo usermod -g C funcionario_entrada_uminho`
- `sudo usermod -g P visitante_uminho`

O último passo é a criação e atribuição de permissões na diretoria através dos comandos seguintes.

- `mkdir registos_uminho`
- `sudo chown -R funcionario_entrada_uminho registos_uminho`
- `sudo chown -R :C registos_uminho`
- `sudo setfacl -R -d -m g:SC:rx registos_uminho`
- `sudo setfacl -R -d -m g:C:rwX registos_uminho`
- `sudo setfacl -R -d -m g:P:wx registos_uminho`

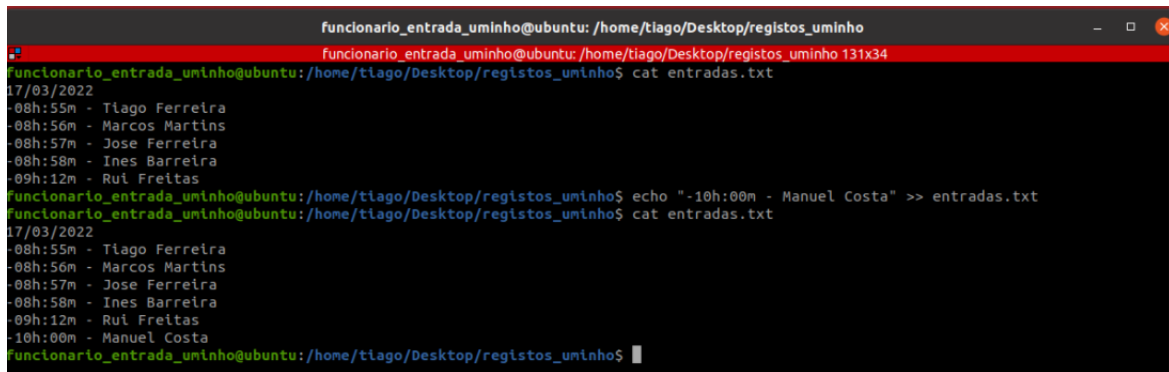
De seguida são apresentadas capturas de ecrã a comprovar a implementação do modelo Bell-LaPadula numa estrutura de dados. Primeiramente é realizado a leitura do ficheiro por parte dos serviços académicos, como demonstrado na figura 3. Depois é realizada uma tentativa de escrita no ficheiro por parte desta entidade cujo acesso é negado visto encontrar-se num nível da *lattice* superior ao do ficheiro.



```
servicos_academicos_uminho@ubuntu: /home/tiago/Desktop/registos_uminho
servicos_academicos_uminho@ubuntu: /home/tiago/Desktop/registos_uminho 130x33
servicos_academicos_uminho@ubuntu: /home/tiago/Desktop/registos_uminho$ cat entradas.txt
17/03/2022
-08h:55m - Tiago Ferrelra
-08h:56m - Marcos Martins
-08h:57m - Jose Ferrelra
-08h:58m - Ines Barreira
-09h:12m - Rui Freitas
servicos_academicos_uminho@ubuntu: /home/tiago/Desktop/registos_uminho$ echo "teste" >> entradas.txt
bash: entradas.txt: Permission denied
servicos_academicos_uminho@ubuntu: /home/tiago/Desktop/registos_uminho$
```

**Figura 3:** Exemplo Serviços Académicos

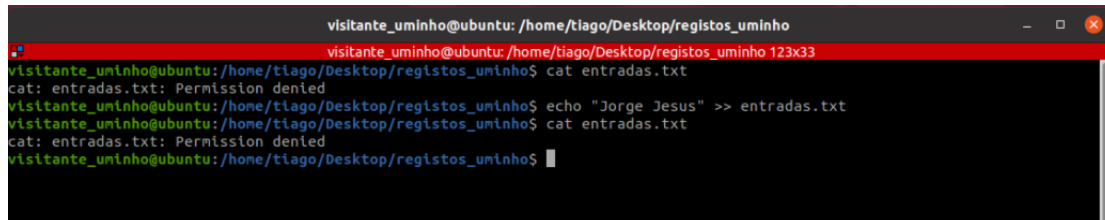
Quanto ao funcionário da universidade este tem permissões para ler e escrever no ficheiro visto ter sido neste nível de segurança que ocorreu a criação do ficheiro. É comprovado na figura 4, que representa o terminal de um funcionário, este pode efetivamente realizar a leitura do ficheiro e posterior escrita através da adição do aluno Manuel Costa à lista de entradas.



```
funcionario_entrada_uminho@ubuntu: /home/tiago/Desktop/registos_uminho
funcionario_entrada_uminho@ubuntu: /home/tiago/Desktop/registos_uminho 131x34
funcionario_entrada_uminho@ubuntu: /home/tiago/Desktop/registos_uminho$ cat entradas.txt
17/03/2022
-08h:55m - Tiago Ferreira
-08h:56m - Marcos Martins
-08h:57m - Jose Ferreira
-08h:58m - Ines Barreira
-09h:12m - Rui Freitas
funcionario_entrada_uminho@ubuntu: /home/tiago/Desktop/registos_uminho$ echo "-10h:00m - Manuel Costa" >> entradas.txt
funcionario_entrada_uminho@ubuntu: /home/tiago/Desktop/registos_uminho$ cat entradas.txt
17/03/2022
-08h:55m - Tiago Ferreira
-08h:56m - Marcos Martins
-08h:57m - Jose Ferreira
-08h:58m - Ines Barreira
-09h:12m - Rui Freitas
-10h:00m - Manuel Costa
funcionario_entrada_uminho@ubuntu: /home/tiago/Desktop/registos_uminho$
```

**Figura 4:** Exemplo Funcionário

Por último é apresentada uma captura de ecrã da tentativa de leitura do ficheiro por parte de um visitante da universidade. Este como se encontra num nível de acesso inferior não lhe é possível realizar a leitura do ficheiro. Quanto à escrita no ficheiro é comprovado que pode ser realizado através do comando *echo*.



```
visitante_uminho@ubuntu: /home/tiago/Desktop/registos_uminho
visitante_uminho@ubuntu: /home/tiago/Desktop/registos_uminho 123x33
visitante_uminho@ubuntu: /home/tiago/Desktop/registos_uminho$ cat entradas.txt
cat: entradas.txt: Permission denied
visitante_uminho@ubuntu: /home/tiago/Desktop/registos_uminho$ echo "Jorge Jesus" >> entradas.txt
visitante_uminho@ubuntu: /home/tiago/Desktop/registos_uminho$ cat entradas.txt
cat: entradas.txt: Permission denied
visitante_uminho@ubuntu: /home/tiago/Desktop/registos_uminho$
```

**Figura 5:** Exemplo Visitante

## **6 Conclusão**

Após a conclusão deste trabalho prático foi possível retirar que o modelo Bell-LaPadula poderá não ser o mais adequado em termos de integridade das informações mas excelente relativamente à confidencialidade. Por conseguinte, aos olhos do grupo este poderá não ser um balanço propriamente adequado numa rede de segurança atual em que para além de confidencialidade dos dados também é necessário existir a integridade destes.

Este trabalho prático foi importante para expandir o nosso conhecimento na área da cibersegurança, uma área cada vez mais relevante nos dias de hoje. Para além disso serviu também para melhorar as capacidades de implementação dos conhecimentos adquiridos.