



Universidade do Minho

Escola de Engenharia

Mestrado Integrado em Engenharia de Telecomunicações e Informática

Segurança em Redes de Computadores

## Trabalho Prático Nº 3

# Modelação do Controlo de Acesso

Elementos do grupo:

Hélder Duarte A75121

Hugo Pereira A48319

Manuel Coutinho A76569

26 de Março de 2018

# Índice

|  |    |
|--|----|
| Índice de figuras .....                        | 3  |
| Índice de tabelas .....                        | 3  |
| Índice de abreviaturas.....                    | 3  |
| Introdução.....                                | 4  |
| 1. Controlo de acesso .....                    | 5  |
| 1.1. Modelo Bell-LaPadula.....                 | 6  |
| 1.1.1. Mandatory Access Control.....           | 7  |
| 1.1.2. Discretionay Access Control.....        | 9  |
| 1.1.3. Possibilidade de fraude.....            | 9  |
| 2. Implementação numa infraestrutura TIC ..... | 10 |
| Conclusão .....                                | 15 |

## Índice de figuras

|   |    |
|---|----|
| Figura 1 - Propriedades do modelo Bell-LaPudula. <sup>1</sup> ..... | 6  |
| Figura 2 - Lattice. ....  | 8  |
| Figura 3 - Criação dos ficheiros de teste. ....                     | 10 |
| Figura 4 - Permissões da categoria AS.. ....                        | 11 |
| Figura 5 - Comandos para atribuição das permissões.....             | 11 |
| Figura 6 -Permissões da categoria ScS.....                          | 12 |
| Figura 7 - Erro de permissão de leitura do ficheiro.....            | 13 |
| Figura 8 - Erro de permissão de escrita no ficheiro.....            | 13 |
| Figura 9 - Permissão de leitura e escrita.....                      | 14 |

## Índice de tabelas

|                                    |   |
|------------------------------------|---|
| Tabela 1 - Matriz acessos DAC..... | 9 |
|------------------------------------|---|

## Índice de abreviaturas

AS

Academic Services, 7

DAC

Discretionary Access Control, 5

MAC

Mandatory Access Control, 5

MLS

Multi-Level Security, 5

ScS

Scientific Services, 7

# Introdução

No âmbito da Unidade Curricular de Segurança de Redes de Computadores foi-nos proposto que desenvolvêssemos um modelo de controlo de acesso tendo como contexto a hierarquia de acessos de uma universidade.

Para este trabalho, foi-nos pedido, numa primeira fase para desenvolver uma *lattice* de níveis de segurança que respeite as propriedades fundamentais do modelo *Bell-LaPadula* e averiguar a possibilidade de enganar esse sistema.

A segunda fase pede para elaborar sobre a possibilidade de criação de um processo automatizado de implementação do sistema criado na primeira fase numa infraestrutura típica de TIC.

# 1. Controlo de acesso

O controlo de acesso assenta em três propriedades: autenticação, autorização e auditoria:

- A autenticação consiste no processo de verificar a identidade do sujeito tendo um certo grau de confiança neste processo. Isto é feito através do uso de uma palavra-passe ou de um endereço de email, sendo que o sujeito pode consistir num ser humano ou numa máquina. Este processo pode envolver dois casos típicos: um computador requer acesso a um computador partilhado e um utilizador requer acesso a uma máquina;
- A autorização consiste em verificar se o utilizador tem ou não autoridade para efetuar certas tarefas;
- A propriedade de auditoria serve para medir a quantidade de recursos que o utilizador gasta durante o seu acesso.

Associados ao controlo de acesso existem políticas tais como a MAC (*Mandatory Access Control*) e a DAC (*Discretionary Access Control*):

- A política MAC é uma forma de garantir direitos de acesso sendo estes regulados por uma entidade central. Uma implementação da política MAC é o MLS (*Multi-Level Security*);
- A política DAC por sua vez é a forma de garantir direitos de acesso tendo por base regras criadas pelos utilizadores. Um mecanismo que implemente a política DAC deverá ser capaz de dar resposta à seguinte questão:

“Um sujeito S tem direito R sobre um objeto O?”

## 1.1. Modelo Bell-LaPadula

Este modelo foi a primeira formalização do controlo de acesso mandatário. A principal intenção do modelo *Bell-LaPadula* é aumentar os controlos de acesso discricionários com controlo de acesso mandatário, de forma a implementar políticas de fluxo de informação. Este modelo conceptualiza duas propriedades fundamentais:

1. Propriedade simples de segurança: um sujeito  $S$  apenas consegue ler um objeto  $O$  se  $L(O) \leq L(S)$ . Por outras palavras, os sujeitos não têm permissão para ler informação que esteja num nível de segurança superior ao deles.
2. <sup>1</sup>Propriedade da estrela: um sujeito  $S$  pode escrever no objeto  $O$  apenas se  $L(S) \leq L(O)$ . Por outras palavras, um sujeito não pode escrever em níveis de segurança inferiores ao que esteja classificado.

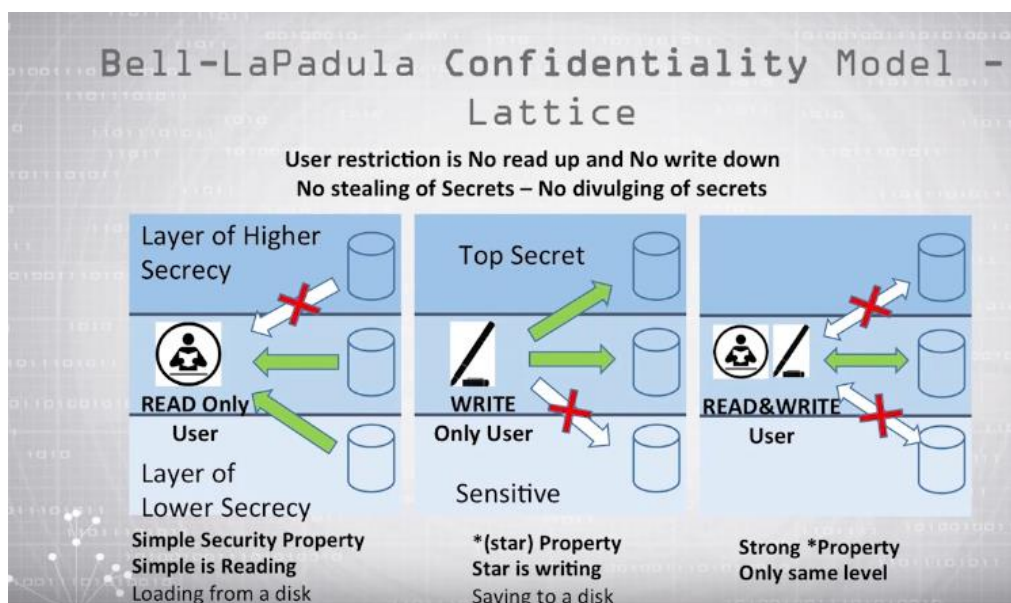


Figura 1 - Propriedades do modelo Bell-LaPadula.<sup>1</sup>

O modelo *Bell-LaPadula* apenas se preocupa com a confidencialidade da informação e não com a sua integridade. O modelo permite que um sujeito escreva no sentido ascendente dos níveis hierárquicos, contudo, apesar de um sujeito não poder ler um objeto, este pode fazer alterações no mesmo. Esta ação é chamada de "*blindwrite*".

<sup>1</sup> Figura 1 extraída do vídeo <https://www.youtube.com/watch?v=SfryxGRXoVg&t=182s>

De realçar que neste modelo o acesso de escrita é interpretado apenas como acesso de escrita e não como acesso de leitura e escrita como noutros modelos nos quais a escrita assume uma maior conotação em relação à leitura.

### 1.1.1. Mandatory Access Control

A política MAC é uma forma de garantir direitos de acesso sendo estes regulados por uma entidade central visto que os dados são propriedade desta mesma entidade e não são dados pessoais. Estas políticas têm como preocupação evitar ataques do tipo cavalo de Troia.

Para controlar os acessos, a política MAC etiqueta os documentos tendo em conta a sensibilidade que a sua informação contém e os riscos associados à fuga da informação. É possível observar frequentemente esta etiquetagem da informação no sector militar e governamental.

Associando um nível de segurança a uma compartimentalização é criada uma *label*. Estas *labels* são dispostas sob a forma de grafo, e o conjunto destas é conhecido por *lattice* no qual é fundamental garantir a hierarquia entre elas de forma a que uma *label* de nível superior tenha um nível de segurança mais elevado de modo a que a sua informação seja de acesso apenas a utilizadores com as credenciais para tal. Os utilizadores são também etiquetados de acordo com o seu certificado de segurança. Isto pode ser explicado pela seguinte demonstração matemática:

- dadas duas *labels*  $L1 = (S1, C1)$  e  $L2 = (S2, C2)$ , pela política MAC,  $L1 \leq L2$  logo  $L1$  não é mais restritiva que  $L2$  e quem tiver acesso a  $L1$  não pode ler os objetos com a *label*  $L2$ , quando se verificam as seguintes condições:
  - $S1 \leq S2$ ;
  - $C1 \subseteq C2$ , onde se entende que o conteúdo de  $C1$  tem um nível de segurança  $\leq$  que o conteúdo de  $C2$ .

No contexto do nosso trabalho que tem como base o ambiente universitário, os níveis de segurança exigidos foram: Público, Confidencial e Estritamente Confidencial enquanto que a informação é compartimentalizada em AS (*Academic Services*) e ScS (*Scientific Services*). Um dos requisitos consiste que na *lattice* os professores sejam classificados com a *label*  $(C, \{AS, ScS\})$  e os alunos com a *label*  $(C, \{As\})$ . Na Figura 2 abaixo, podemos ver a *lattice* que o grupo criou para este trabalho.

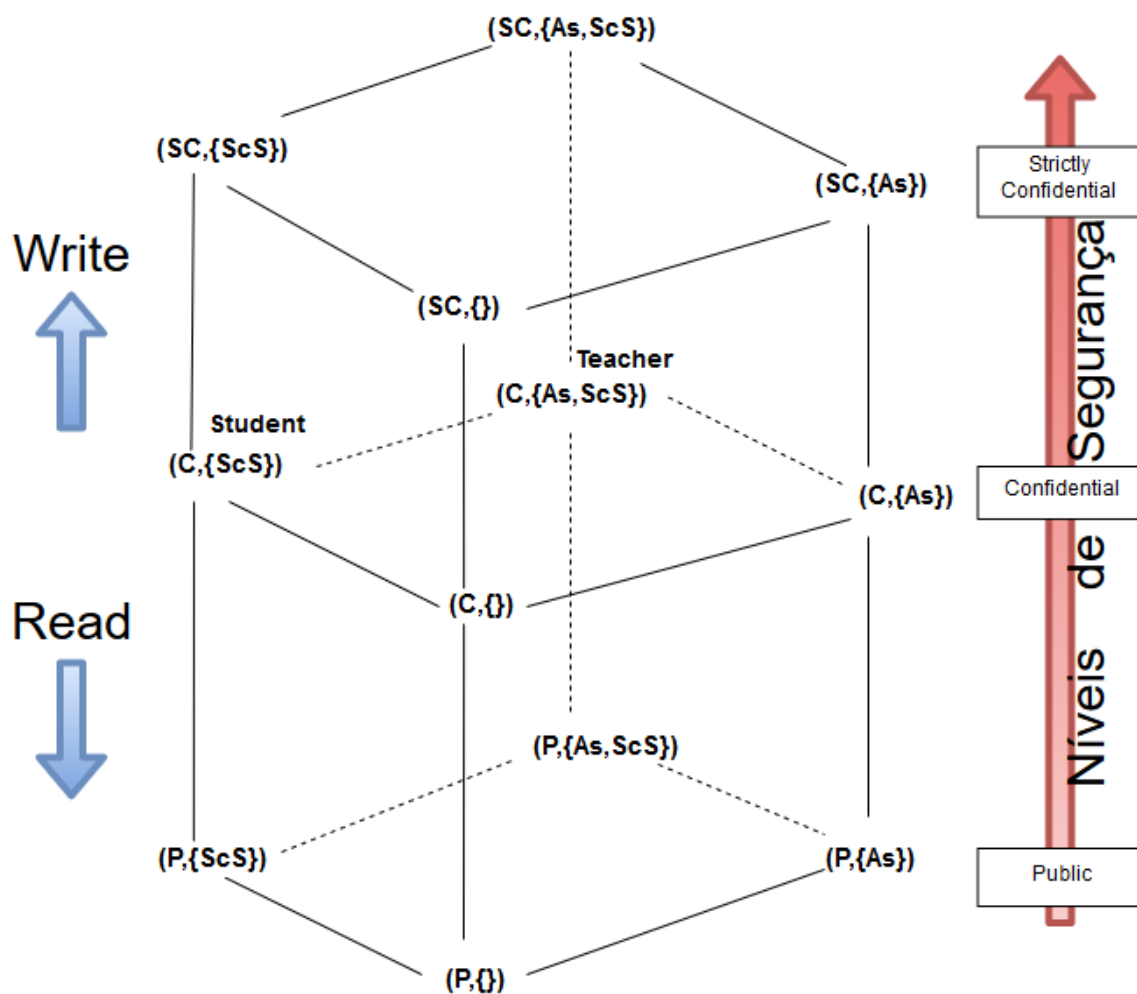


Figura 2 - Lattice.

É de notar que os utilizadores com a *label*  $(SC, \{As, ScS\})$  têm permissão para ler todos os documentos existentes que tenham as *labels* que se encontram presentes na lattice enquanto que no sentido oposto temos os utilizadores com a *label*  $(P, \{\})$  são os mais restringidos no que toca ao acesso à leitura de documentos.

Tendo em conta as propriedades do modelo Bell-LaPadula associadas à escrita, são precisamente os utilizadores com a *label*  $(P, \{\})$  que têm permissão para escrever por cima em todos os documentos, independentemente do nível de segurança que lhes esteja associado.



### 1.1.2. Discretionary Access Control

A política DAC (*Discretionary Access Control*) é uma forma de atribuir direitos de acesso a objetos tendo por base regras especificadas pelos utilizadores. Os utilizadores podem alterar as permissões dos objetos por eles criados tendo em conta o sujeito em questão fazendo deste um modelo discricionário. Esta política deverá ser capaz de dar a resposta à questão: "O sujeito *S* tem direito *D* sobre o objeto *O*?". A resposta a esta pergunta pode ser facilmente respondida através de uma matriz de controlo de acesso. Nesta matriz são atribuídas permissões ao conjunto Sujeito / Objeto. Nas linhas constam os sujeitos e nas colunas os objetos.

Tabela 1 - Matriz acessos DAC.

| Objeto<br>Sujeito | Dados pessoais<br>do aluno | Processo do<br>aluno | Trabalhos<br>submetidos | Notas dos<br>trabalhos |
|-------------------|----------------------------|----------------------|-------------------------|------------------------|
| Professor         | R                          | W/R                  | R                       | W/R                    |
| Aluno             | W/R                        | R                    | W/R                     | R                      |

### 1.1.3. Possibilidade de fraude

Quanto à questão colocada no enunciado deste trabalho prático sobre se os alunos conseguem fraudar os professores, o grupo chegou à conclusão que com a implementação do modelo de controlo de acesso Bell-LaPadula, é possível que tal aconteça. Como já foi referenciado, o foco deste modelo prende-se com a confidencialidade dos dados e não com a sua integridade.

Visto que na categoria dos AS os alunos e os professores têm o mesmo nível de acesso (C), então têm as mesmas permissões nesta categoria. Assim por exemplo um aluno poderia alterar as notas emitidas pelo professor o que não é aceitável no contexto universitário.

## 2. Implementação numa infraestrutura TIC

É pretendido elaborar sobre uma implementação automática do modelo numa estrutura TIC. Tendo em conta que os objetos e os sujeitos estariam classificados de acordo com os seguintes níveis de acesso: P (Public), C(Confidential) e SC (Strictly Confidential).

A abordagem do grupo passava por desenvolver um script com o seguinte algoritmo:

Entradas:

- Todos os ficheiros e respetivos níveis de segurança
- Todos os utilizadores e respetivos níveis de segurança

Para cada utilizador:

- Para cada ficheiro:
  - ❖ Se  $\text{nível}(\text{utilizador}) \geq \text{nível}(\text{ficheiro})$ 
    - Permissão para ler
  - ❖ Se  $\text{nível}(\text{utilizador}) \leq \text{nível}(\text{ficheiro})$ 
    - Permissão para escrever

Para simular a implementação deste *script* utilizamos os comandos **setfacl** e o **getfacl** para atribuir permissões aos utilizadores. Foram criados ficheiros para as categorias AS e ScS em que o nome representa o nível de acesso do ficheiro, tal como descrito na Figura 3.

```
manuel@manuel-VirtualBox:~/Desktop/SRC$ touch P,{AS}
manuel@manuel-VirtualBox:~/Desktop/SRC$ touch C,{AS}
manuel@manuel-VirtualBox:~/Desktop/SRC$ touch SC,{AS}
manuel@manuel-VirtualBox:~/Desktop/SRC$ touch SC,{ScS}
manuel@manuel-VirtualBox:~/Desktop/SRC$ touch C,{ScS}
manuel@manuel-VirtualBox:~/Desktop/SRC$ touch P,{ScS}
```

Figura 3 - Criação dos ficheiros de teste.

Tendo em conta que os utilizadores têm um nível de segurança C, foram atribuídas as permissões de acordo com o algoritmo supra mencionado, usando o comando **setfacl** descrito na Figura 5:

```

manuel@manuel-VirtualBox:~/Desktop/SRC$ setfacl -m u:aluno:rw C,{AS}
manuel@manuel-VirtualBox:~/Desktop/SRC$ setfacl -m u:aluno:r P,{AS}
manuel@manuel-VirtualBox:~/Desktop/SRC$ setfacl -m u:aluno:w SC,{AS}
manuel@manuel-VirtualBox:~/Desktop/SRC$ setfacl -m u:professor:w SC,{AS}
manuel@manuel-VirtualBox:~/Desktop/SRC$ setfacl -m u:professor:rw C,{AS}
manuel@manuel-VirtualBox:~/Desktop/SRC$ setfacl -m u:professor:r P,{AS}
manuel@manuel-VirtualBox:~/Desktop/SRC$ setfacl -m u:professor:r P,{ScS}
manuel@manuel-VirtualBox:~/Desktop/SRC$ setfacl -m u:professor:rw C,{ScS}
manuel@manuel-VirtualBox:~/Desktop/SRC$ setfacl -m u:professor:w SC,{ScS}
manuel@manuel-VirtualBox:~/Desktop/SRC$ setfacl -m u:aluno:- SC,{ScS}
manuel@manuel-VirtualBox:~/Desktop/SRC$ setfacl -m u:aluno:- C,{ScS}
manuel@manuel-VirtualBox:~/Desktop/SRC$ setfacl -m u:aluno:- P,{ScS}

```

Figura 5 - Comandos para atribuição das permissões.

A definição das permissões dos ficheiros para os utilizadores Aluno e Professor como estabelecido na Figura 2 do modelo de Bell-LaPadula, estão descritas nas Figura 4 e Figura 6:

```

manuel@manuel-VirtualBox:~/Desktop/SRC$ getfacl P,{AS}
# file: P,{AS}
# owner: manuel
# group: manuel
user::rw-
user:aluno:r--
user:professor:r--
group::rw-
mask::rw-
other::r--

manuel@manuel-VirtualBox:~/Desktop/SRC$ getfacl C,{AS}
# file: C,{AS}
# owner: manuel
# group: manuel
user::rw-
user:aluno:rw-
user:professor:rw-
group::rw-
mask::rw-
other::r--

manuel@manuel-VirtualBox:~/Desktop/SRC$ getfacl SC,{AS}
# file: SC,{AS}
# owner: manuel
# group: manuel
user::rw-
user:aluno:-w-
user:professor:-w-
group::rw-
mask::rw-
other::r--

```

Figura 4 - Permissões da categoria AS..

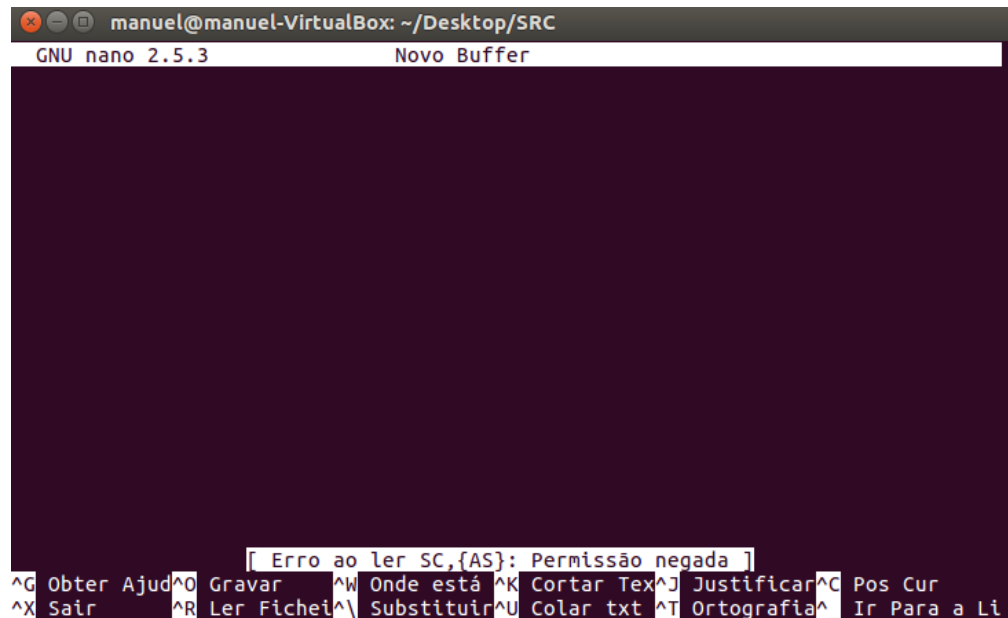
```
manuel@manuel-VirtualBox:~/Desktop/SRC$ getfacl P,{ScS}
# file: P,{ScS}
# owner: manuel
# group: manuel
user::rw-
user:aluno:---
user:professor:r--
group::rw-
mask::rw-
other::r--

manuel@manuel-VirtualBox:~/Desktop/SRC$ getfacl C,{ScS}
# file: C,{ScS}
# owner: manuel
# group: manuel
user::rw-
user:aluno:---
user:professor:rw-
group::rw-
mask::rw-
other::r--

manuel@manuel-VirtualBox:~/Desktop/SRC$ getfacl SC,{ScS}
# file: SC,{ScS}
# owner: manuel
# group: manuel
user::rw-
user:aluno:---
user:professor:-w-
group::rw-
mask::rw-
other::r--
```

*Figura 6 -Permissões da categoria ScS.*

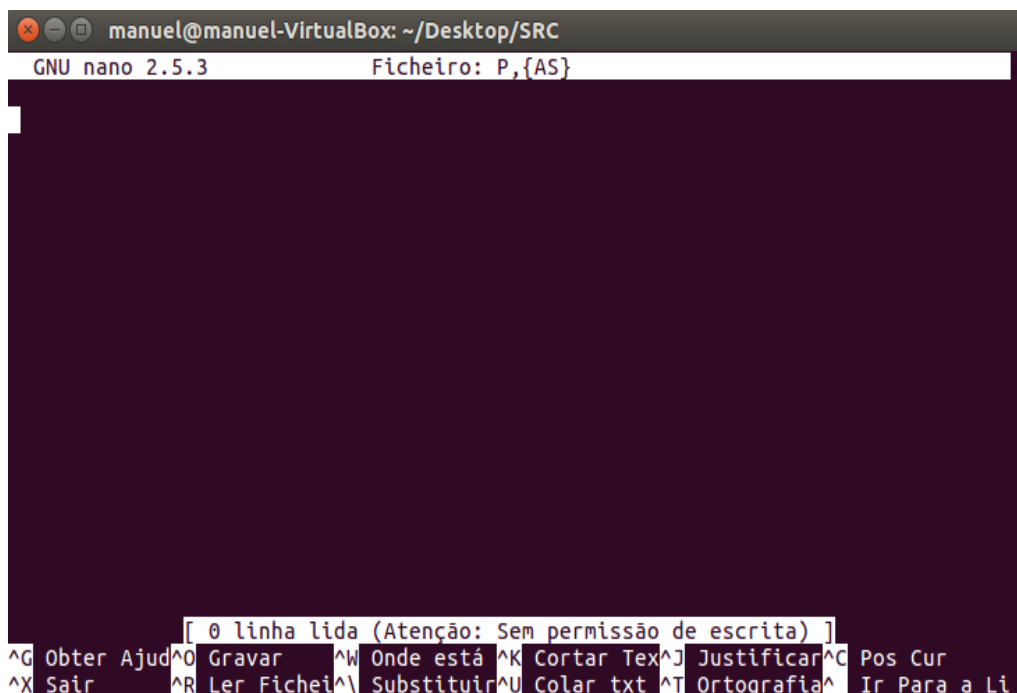
Como podemos ver nas Figura 7 e Figura 8, um aluno não tem permissão para escrever em objetos que estejam classificados com um nível de segurança inferior a Confidencial, nem têm permissão para ler em objetos que estejam classificados com um nível de segurança superior a Confidencial.



```
manuel@manuel-VirtualBox: ~/Desktop/SRC
GNU nano 2.5.3          Novo Buffer

[ Erro ao ler SC,{AS}: Permissão negada ]
^G Obter Ajud^O Gravar ^W Onde está ^K Cortar Tex^J Justificar^C Pos Cur
^X Sair ^R Ler Fichei^_ Substituir^U Colar txt ^T Ortografia^_ Ir Para a Li
```

Figura 7 - Erro de permissão de leitura do ficheiro.



```
manuel@manuel-VirtualBox: ~/Desktop/SRC
GNU nano 2.5.3          Ficheiro: P,{AS}

[ 0 linha lida (Atenção: Sem permissão de escrita) ]
^G Obter Ajud^O Gravar ^W Onde está ^K Cortar Tex^J Justificar^C Pos Cur
^X Sair ^R Ler Fichei^_ Substituir^U Colar txt ^T Ortografia^_ Ir Para a Li
```

Figura 8 - Erro de permissão de escrita no ficheiro.

Na Figura 9, podemos ver que o aluno tanto pode escrever e ler um objeto que esteja classificado com o mesmo nível de segurança que o sujeito tem.

```
manuel@manuel-VirtualBox: ~/Desktop/SRC
GNU nano 2.5.3      Ficheiro: C,{AS}

[ 1 linha lida ]
^G Obter Ajuda  ^O Gravar      ^W Onde está   ^K Cortar Tex  ^J Justificar  ^C Pos Cur
^X Sair         ^R Ler Fichei  ^_ Substituir  ^U Colar txt   ^T Ortografia  ^_ Ir Para a Li
```

Figura 9 - Permissão de leitura e escrita.

## Conclusão

O conhecimento adquirido durante a realização do trabalho, nomeadamente as propriedades deste modelo permite-nos afirmar que este modelo não perfaz os requisitos de segurança atuais. Não faz sentido confiar num sujeito ao ponto de o deixar alterar informação quando não lhe é depositada confiança para ler essa mesma informação.

Apesar desta falha no modelo, o grupo percebeu a necessidade que o modelo teve na altura que foi criado e através do algoritmo descrito neste relatório, conseguimos recriá-lo e implementá-lo num sistema atual.