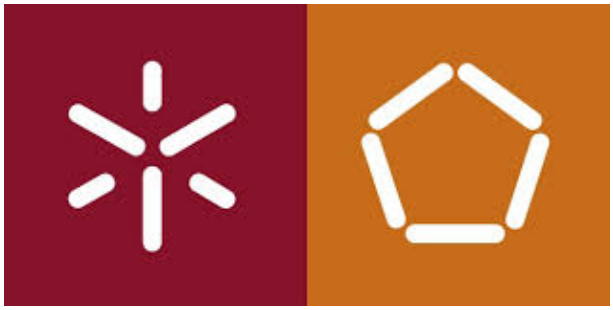
Universidade do Minho



Trabalho Prático

Controlo de Acesso

Mestrado Integrado em Engenharia Informática

Segurança em Redes

(1º Semestre - 2018/2019)

a70565	Bruno Arieira
a73883	Cesário Perneta
a73974	Daniel Vieira
a78494	José Dias

27 de Outubro de 2018

Resumo

"To control the acess conditions of a ***subject*** to an ***object***, in particularly what the first can do (authorization) - Read, Write, Execute..."

Este trabalho prático foi realizado no âmbito da unidade curricular Segurança em Redes, e tem como principal objetivo a implementação de um modelo que permita o controlo de acesso de segurança, num contexto universitário.

Conteúdo

1 Introdução 3

2 Contextualização 4

3 Modelo de Bell-LaPadula 5

4 Modelo de Bell-LaPadula num sistema operativo 6

5 Conclusão 8

1 Introdução

Neste segundo trabalho prático, temos como principal objetivo aplicar o conhecimento adquirido nas aulas de Seguranças em Redes, relativamente á matéria lecionada sobre Controlo de Acesso, com principal objetivo da modelação de um sistema de Controlo de Acesso, num ambiente simplificado de uma universidade.

De acordo com o enunciado proposto, para a realização deste trabalho, inicialmente é necessário o estudo aprofundado das propriedades fundamentais e aspetos formais do modelo BLP (***Bell-LaPadula***), por forma a permitir a confidencialidade de um sistema *Multi-User*, numa infraestrutura **TIC**. Este é um modelo formal de transição de estado para políticas de segurança de computador que descreve um conjunto de regras de controlo de acesso, usando etiquetas de segurança em objetos e autorizações para os utilizadores.

Para o desenvolvimento deste trabalho, foi delineado que todos os elementos deviam analisar e entender as propriedades do modelo já mencionado (BLP), assim como outros conceitos imprescindíveis, para a posterior discussão e elaboração das tarefas propostas, onde todos os elementos trabalharam de forma uniforme.

2 Contextualização

Controlo de acesso consiste numas das medidas mais importantes para a proteção da informação, impedindo acessos não autorizados a utilizadores de um determinado sistema. Podem se definir como principais objetivos para o controlo de acesso:

- Proteção da privacidade de dados pessoais, evitando o acesso de sujeitos sem autorização a informações sensíveis;
- Evita a indevida criação, eliminação ou alteração de informação por parte de utilizadores que não têm autorização para o efeito;
- Permite a autenticação, através da identificação de sujeitos legítimos para aceder á informação;

As três propriedades principais para a segurança são a **Confidencialidade**, **Integridade** e **Disponibilidade**, como foi abordado no trabalho prático anterior:

- Confidencialidade: Impedir o acesso a informação por entidades não autorizadas.
- Integridade: Impedir a alteração de informação por entidades não autorizadas para o efeito.
- Disponibilidade: Garantir que toda a informação esteja disponível para todas as entidades que tenham esse direito.

O modelo de *Bell-LaPadula*, tem como fundamento a garantia da primeira propriedade descrita, baseada em vários padrões, incluindo os Critérios de Avaliação do Sistema de Computação Confiável. Este modelo destina-se á confidencialidade, uma vez que utilizadores de níveis inferiores (menos importantes numa determinada infraestrutura) não têm autorização a aceder a informação de utilizadores de níveis superiores, que por outro lado, impossibilita a fuga de informação sensível, pois os utilizadores de nível superior não podem escrever para níveis inferiores. Para interligar por outras palavras com a definição de confidencialidade, se C for um conjunto de entidades e I for alguma informação, então I tem a propriedade de confidencialidade em relação a C caso nenhum elemento de C obtenha alguma informação de I. Um exemplo que achamos importante referenciar neste relatório, foi o processo de escrita e leitura num ambiente militar referenciado pelo professor.

Figura 1: Exemplo de autorização de leitura/escrita

Pela figura podemos estabelecer relações de confidencialidade, em que um soldado apenas pode escrever para os graus hierárquicos superiores mas não ler, pois caso isso acontecesse, teria acesso a informações que poderiam ser confidenciais e que apenas o Coronel ou o Tenente (dependendo do nível de importância) teriam autorização para aceder.

3 Modelo de Bell-LaPadula

O modelo de Bell-LaPadula apresentado na figura 2, tem em conta as categorias, **AS** (*Academic Services*) e **ScS** (*Scientific Services*) e níveis das *labels*, **P** (*public*), **C** (*confidential*) e **SC** (*strictly confidential*).

Num contexto universitário, o aluno está classificado como (C, AS), numa posição hierárquica inferior à do professor, o que faz com que este não possa alterar diretamente dados do professor, no entanto, nada o impede de escrever "às cegas", pois este modelo visa proteger a confidencialidade, isto é, quem está em níveis superiores não pode vazar informações para níveis inferiores, porém, quem está em níveis inferiores, não está impedido de escrever para níveis superiores, somente está impedido de ler.

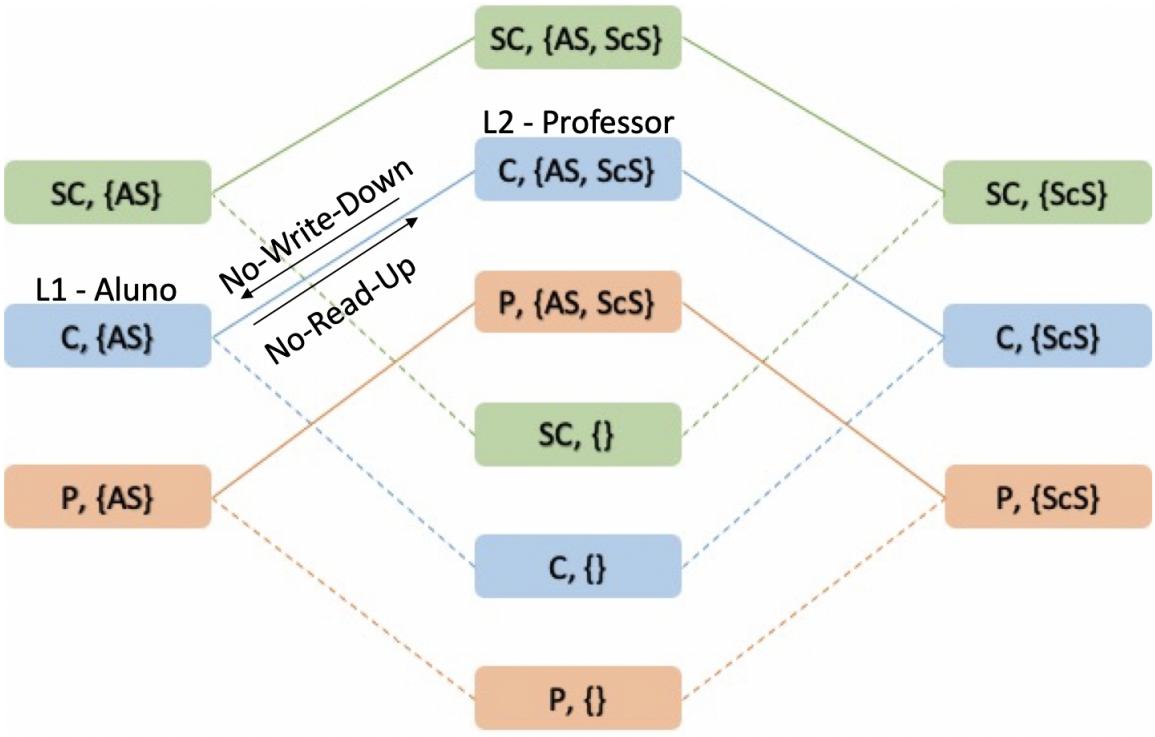


Figura 2: Controlo de acesso baseado no modelo de Lattice aplicado a Bell-Lapadula

Podemos comprovar o que foi anteriormente dito, através da figura 2, onde se pode verificar que L1 $\leq$ $L2, resumindo$:

- C $\leq C$
- AS $\subseteq AS, ScS$
- Professor - *No-Write-Down*
- Aluno - *No-Read-Up*

Com este modelo e tomando como exemplo as *labels* do aluno e do professor, podemos agora definir todas as permissões do modelo anteriormente apresentado:

	P{}	P{AS}	P{ScS}	P{AS,ScS}	C{}	C{AS}	C{ScS}	C{AS,ScS}	SC{}	SC{AS}	SC{ScS}	SC{AS,ScS}
P{}	RO/ WO	WO	WO	WO	WO	WO	WO	WO	WO	WO	WO	WO
P{AS}	RO	RO/ WO		WO	WO	WO		WO	WO	WO		WO
P{ScS}	RO		RO/ WO	WO	WO		WO	WO	WO		WO	WO
P{AS,ScS}	RO	RO	RO	RO/ WO	WO	WO	WO	WO	WO	WO	WO	WO
C{}	RO				RO/ WO	WO	WO	WO	WO	WO	WO	WO
C{AS}	RO	RO		RO	RO	RO/ WO		WO	WO	WO		WO
C{ScS}	RO		RO	RO	RO		RO/ WO	WO	WO		WO	WO
C{AS,ScS}	RO	RO	RO	RO	RO	RO	RO	RO/ WO	WO	WO	WO	WO
SC{}	RO				RO				RO/ WO	WO	WO	WO
SC{AS}	RO	RO		RO	RO	RO		RO	RO	RO/ WO	WO	WO
SC{ScS}	RO		RO	RO	RO		RO	RO	RO		RO/ WO	WO
SC{AS,ScS}	RO	RO	RO	RO	RO	RO	RO	RO	RO	RO	RO	RO/ WO

Permissões: RO – Read Only; WO – Write Only

Figura 3: Tabela de permissões baseada no modelo da figura 2

4 Modelo de Bell-LaPadula num sistema operativo

Numa segunda fase do nosso trabalho foi proposta a discussão quanto á implementação deste modelo. O objetivo final seria obter uma estrutura com níveis de segurança bem definidos para cada grupo bem como a sua *clearance*.

Temos como exemplo o que encontramos anteriormente onde encontrávamos o seguinte:

- Niveis de segurança: *Public*, *Confidential* e *Strictly Confidential*
- *Clearance*: *Academic Services*, *Scientific Services*

Utilizamos para exemplificar o sistema uma adaptação que podemos encontrar em "https://github.com/achintverma/Bell-LaPadula"utilizando os ficheiros:

- `BLPwrite`
- `BLPread`
- `BLP_permissions.txt`
- `BLP_user_levels.txt`

Além dos ficheiros acima, criamos um ficheiro para exemplificar denominado de `Avaliação.txt`. Esse ficheiro foi posteriormente adicionado ao ficheiro `BLP_permissions.txt`.

Para obter os resultados esperados tivemos de alterar no ficheiro `BLP_user_levels.txt`, de modo a simular utilizadores diferentes, o nível de permissão no caso do *userid* 1000, pois na maquina em que testamos era esse a identificação do utilizador, para 3 no caso do professor (figura 5) e 2 no caso dos alunos (figura 4).

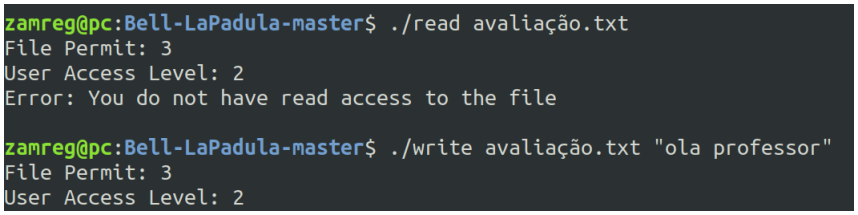


Figura 4: Tentativas de leitura e escrita efetuadas por um aluno

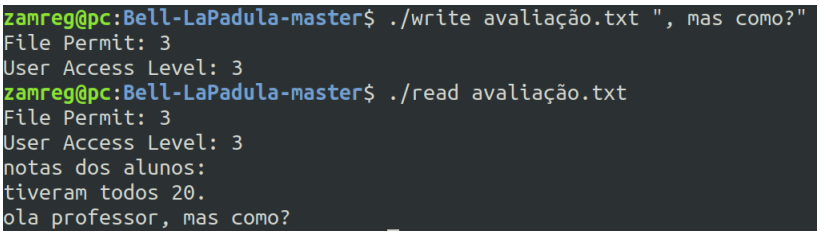


Figura 5: Tentativas de leitura e escrita efetuadas por um professor

5 Conclusão

Chegando à parte final deste trabalho, há que fazer uma revisão de todo trabalho efetuado. Devido ao conhecimento que adquirimos nas aulas e a pesquisas efetuadas, o capitulo que intitulamos de **Contextualização** foi realizado sem nenhum problema relevante, onde apresentamos uma explicação teórica do tema **Controlo de acesso**.

Em relação ao Modelo de Bell-LaPadula sentimos mais dificuldades, visto que não estávamos a conseguir transfigurar o nosso conhecimento teórico nesta parte prática. Depois de algumas conversas com o professor, conseguimos entender este exercício e elabora-lo.
Antes de efetuarmos qualquer trabalho, dividimos o mesmo de acordo com a disponibilidade de cada elemento para o realizar, tornando assim este trabalho mais aprazível de o fazer.

Para concluir, visto que chegamos a conclusões satisfatórias, achamos que este foi um bom trabalho, sucinto, objetivo e que nos levou a melhorar todo o nosso conhecimento em **Segurança em Redes**, mais precisamente em **Controlo de Acesso**.