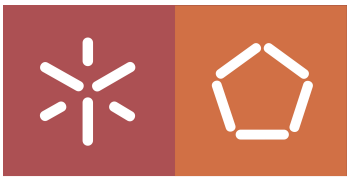

Universidade do Minho
Escola de Engenharia

GESTÃO E VIRTUALIZAÇÃO DE REDES
SEGURANÇA EM REDES
NETWORK SECURITY
(SR) - HOMEWORK TP2

CONTROLO DE ACESSO

GRUPO 2

A85308 Filipe Miguel Teixeira Freitas Guimarães
A79799 Gonçalo Nogueira Costeira
A84912 Joana Isabel Afonso Gomes
A75480 Marco Matias Pereira Gonçalves
A42040 Miriam Miranda Pinto
A57041 Simão Pedro Santa Cruz Oliveira

Braga,
13 de novembro de 2020

Conteúdo

1 Introdução

Para este segundo trabalho prático, no âmbito da unidade curricular de **Segurança de Redes**, foi-nos proposta a modelação de um sistema de Controlo de Acesso numa universidade simplificado, baseando-nos no conhecimento adquiridos nas aulas relativas à matéria de **Controlo de Acesso**.
Abordaremos assim uma forma de controlar os objetos a que um determinado sujeito tem acesso, seja para ler, escrever ou executar uma tarefa no sistema, recorrendo ao **modelo BLP**, o primeiro modelo matemático com uma política de segurança *multilevel*, cuja essência será aprofundada de seguida.

2 Contextualização

Foi-nos portanto proposto analisar e pôr em prática o **modelo BLP (Bell-La- Padula)**, um modelo formal de transição de estado para políticas de segurança de computador, que tem como principal obetivo alcançar a confidencialidade de um sistema com vários *users*, numa infraestrutura *CIT*. Neste modelo existe um conjunto de regras de controlo de acesso. A política que o define é que **a informação não pode passar para entidades a quem a informação não se destina.**

O **controlo de acesso** é uma das medidas mais importantes para a proteção dos sistemas de informação na atualidade, impedindo acessos não autorizados aos utilizadores, quando assim o deve ser.
Podem-se definir como principais **objetivos** para o **controlo de acesso**:

- **Autenticação**, através da identificação de utilizadores reconhecidos para aceder á informação
- **Prevenção** de criar ou modificar informação por parte de utilizadores que não têm autorização
- **Proteção** da privacidade de dados pessoais, evitando o acesso por utilizadores de niveis abaixo a informações sensíveis

Os utilizadores são identificados de acordo com as suas permissões de segurança. Assim como as etiquetas de um documento, as permissões de segurança são constituídas por um par (**nível de segurança**, **categoria**).
Se tivermos duas etiquetas `L1=(S1,C1)` e `L2=(S2,C2)`, escrevemos `L1`$\leqslant$`(S2,C2)` (que significa que L1 é menos restritivo que L2) quando:

- `S1`$\leqslant$`S2`, sendo que **Público < Confidencial < Estritamente Confidencial**
- `C1`$\subseteq$`C2`

No diagrama seguinte podemos ver algumas destas relações $\leqslant$, sendo que uma *label* L1 num nível mais baixo que uma *label* L2 dennota que `L1`$\leqslant$`L2`.

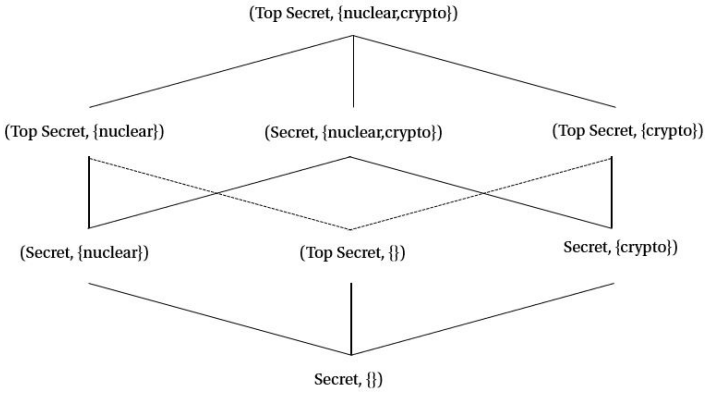

Figura 1: Ordem modelo BLP

Assim sendo, relembrando o previamente referido lema deste modelo (não permitir o vazamento de informação), se tomarmos `L(X)` como que denote uma *label* de uma entidade `X`, as **condições de segurança** do modelo BLP são:

- Uma entidade S pode ler um objeto `O` se `L(O)`$\leqslant$`L(S)` (ou seja, não pode ler "para cima")
- Uma entidade S pode escrever um objeto `O` se `L(S)`$\leqslant$`L(O)` (não pode escrever "para baixo")

3 Resposta ao problema proposto

3.1 *Bell-Lapadula* em contexto universitário

Em contexto universitário, e assumindo o modelo **BLP**, teremos então 3 etiquetas de níveis de segurança, seguindo a lógica que introduzimos na contextualização:

- **P** - Público
- **C** - Confidencial
- **SC** - Estritamente Confidencial

Em que $P < C < SC$.
E ainda as categorias:

- **AS** - Serviços Académicos
- **ScS** - Serviços Científicos

Se considerarmos duas etiquetas $L1 = (S1, C1)$ e $L2 = (S2, C2)$, tendo $L1 \leq L2$ então podemos dizer que L1 não é mais restritivo que L2 se,

$$(S1 \leq S2) \wedge (C1 \subseteq C2) \tag{1}$$

Podemos observar que L1 é parcialmente ordenado por C1, ou seja, é possível haver duas etiquetas que não são comparáveis (e.g. (Público, {Serviços Académicos}) e (Público, {Serviços Científicos})). Para organizar estas relações entre conjuntos criamos um reticulado (*lattice*) como podemos observar na seguinte figura.

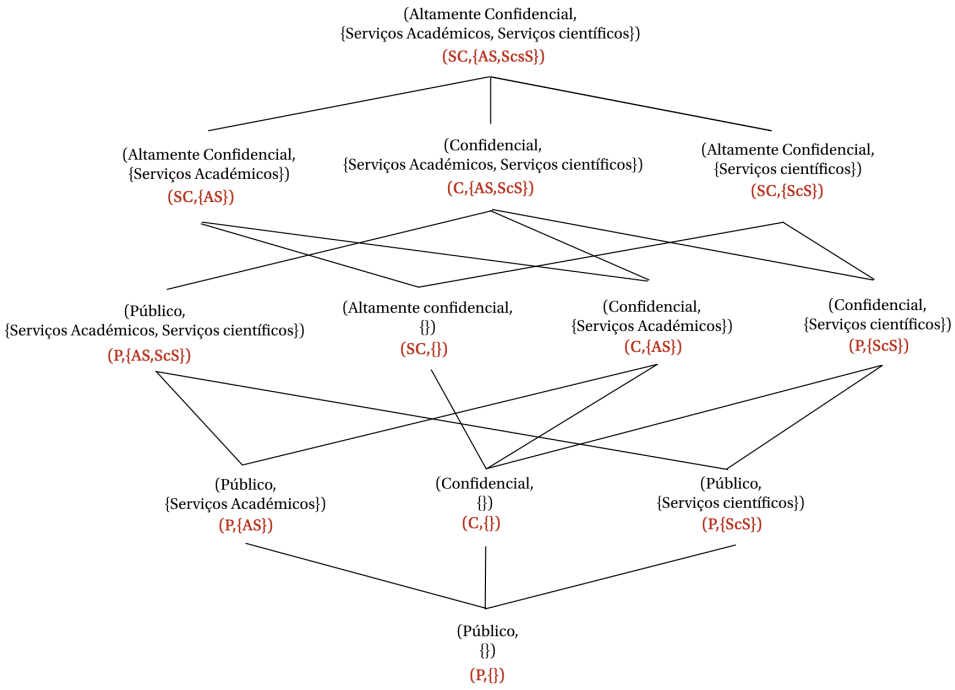

Figura 2: Reticulado com as relações entre conjuntos de controlo de acesso

Considerando que

$$etiqueta_{professor} = (C, \{AS, ScS\}) \tag{2}$$

$$etiqueta_{aluno} = (C, \{AS\}) \tag{3}$$

Observamos, a partir do reticulado que o aluno está a um nível inferior do que o professor provando que

$$etiqueta_{professor} \leq etiqueta_{aluno} \tag{4}$$

Ou seja,

$$(C \leq C) \wedge (As \subseteq AS, ScS) \tag{5}$$

Isto quer dizer que o professor não pode escrever para níveis abaixo, nem o aluno ler para níveis acima. Se o professor nunca partilhar informações para níveis abaixo, o aluno poderá apenas escrever "às cegas"nos ficheiros do professor.

3.2 Processo de *deployment* automático em *Linux*

Para um possível esquema de *deployment* automático deste modelo pode ser usado um sistema operativo baseado em Linux. Em Linux temos ferramentas para criar utilizadores e métodos de acesso, sendo possível também criar grupos.
Serão também definidos diferentes grupos, para ser possível testar os diferentes níveis de privacidade: *Público, Confidencial, Estritamente Confidencial.*
É possível também criar utilizadores, através do comando `(useradd <username>)`, definir a sua password `(passwd <username>)` e criar grupos `(groupadd <groupname>)`.

Também é necessário especificar o tipo de permissão em duas pastas que representam as categorias de acesso: **Serviços académicos** e **Serviços científicos**.
Num ambiente compartilhado, é preciso definir regras de acesso para que vários utilizadores possam compartilhar o acesso ao mesmo arquivo.
Será necessária a criação de várias associações entre os tipos de utilizador do sistema, bem como das permissões que cada um tem. Cada ficheiro tem um proprietário que , por sua vez, está associado a um grupo e mediante essa associação ter ou não acesso a um determinado ficheiro.
Para a realização de testes, e de forma a verificar se o modelo BLP está a ser corretamente aplicado, irá de seguida ser apresentada a forma como o algoritmo é aplicado.

Quanto à implementação do modelo BLP é necessário confirmar se a cada utilizador tem as suas categorias corretamente aplicadas.
Ao nível do sistema operativo Linux, é necessário verificar se o grupo a que utilizador pertence tem as respetivas permissões de acesso à pasta em questão.
Assumindo que o utilizador tem acesso à pasta onde faz o pedido, em seguida, o processo passa por saber a que grupo pertence esse utilizador (e.g. /etc/group).
Após confirmação do grupo são verificadas as permissões que o utilizador pode ter (leitura ou escrita).
No caso de ser leitura, o utilizador terá acesso se o grupo a que pertence for maior ou igual ao grupo que inicialmente criou o ficheiro.
Caso seja escrita, o processo será semelhante, sendo a única diferença o facto de o utilizador ter acesso caso seja menor ou igual ao grupo que criou o ficheiro.
Ambas estas decisões são feitas com base na análise do ficheiro que dite a hierarquia de segurança de todos os grupos definidos no sistema. Este ficheiro poderá ser um ficheiro de configuração ao qual apenas um administrador de sistemas tem acesso de escrita.

3.2.1 Implementação online

Ao lermos sobre **BLP** deparamo-nos com um projeto de implementação deste modelo que se encontra em `https://github.com/achintverma/Bell-LaPadula`.
Decidimos experimentar esta implementação e começamos por verificar qual é o identificador de utilizador com sessão iniciada.

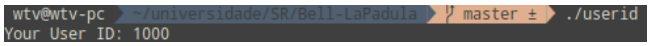

Figura 3: Verificação do userID da máquina

No ficheiro de níveis de permissão por utilizador adicionamos então ao utilizador 1000 com permissão 2 (aluno).

Figura 4: Ficheiro com os utilizadores do sistema e as respetivas permissões

Criamos também um ficheiro *enunciado.txt* com permissão de professor (nível 3).

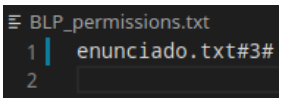

Figura 5: Ficheiro com as permissões de cada ficheiro

Testamos então a leitura deste ficheiro com permissão de aluno e verificamos, como esperado, que este não consegue ler o ficheiro.

```
wtv@wtv-pc ~/universidade/SR/Bell-LaPadula master ± ./BLPread enunciado.txt
File Permit: 3
User Access Level: 2
Error: You do not have read access to the file
```

Figura 6: Tentativa de leitura por parte do aluno no ficheiro *enunciado.txt*

Testamos também a escrita deste ficheiro com permissão de aluno e verificamos, mais uma vez como esperado, que este consegue escrever no ficheiro mas "às cegas", ou seja, não sabe bem para onde está a escrever.

```
wtv@wtv-pc ~/universidade/SR/Bell-LaPadula master ± ./BLPwrite enunciado.txt "Não con
igo abrir o enunciado"
File Permit: 3
User Access Level: 2
```

Figura 7: Tentativa de escrita por parte do aluno no ficheiro *enunciado.txt*

Agora, para testar as permissões de um professor modificamos o nosso utilizador para ser de nível 3 (professor).

Figura 8: Alteração de permissão para professor

Tentamos então a leitura deste ficheiro com permissão de professor e verificamos, como esperado, que este consegue ler o ficheiro e verificar que tem lá a frase que o aluno escreveu.

```
wtv@wtv-pc ~/universidade/SR/Bell-LaPadula master ± ./BLPread enunciado.txt
File Permit: 3
User Access Level: 3
Enunciado do teste n°1
Pergunta 1
.....................
Não consigo abrir o enunciado
```

Figura 9: Tentativa de leitura por parte do professor no ficheiro *enunciado.txt*

Testamos mais uma vez a escrita deste ficheiro, mas desta vez com permissão de professor e verificamos, mais uma vez como esperado, que este consegue escrever no ficheiro.

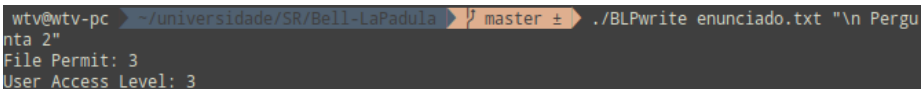

Figura 10: Tentativa de escrita por parte do professor no ficheiro *enunciado.txt*

Verificando lendo de novo este ficheiro.

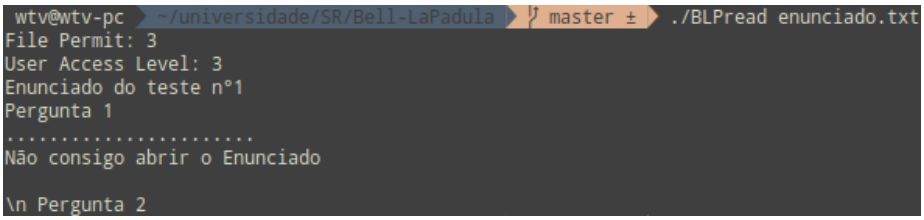

Figura 11: Confirmação da escrita do professor

Decidimos optar por testar esta ferramenta para verificar os conceitos apresentados anteriormente na prática sobre e confirmar que um aluno realmente não consegue "aldrabar"um professor.

4 Conclusão e Análise de Resultados

Concluído este trabalho prático, consideramos os resultados obtidos como satisfatórios.
Apercebemos-nos que ao desenvolvê-lo adquirimos muitos conhecimentos a nível do controlo de acessos e mais especificamente do modelo ***BLP***.
Inicialmente deparamos-nos com algumas dificuldades, dado ser um primeiro contacto com a análise deste modelo. Contudo, após alguma pesquisa e alguns esclarecimentos, foi-nos possível entender o conceito e seguir com a realização deste projecto.
Ao estudar este modelo, tanto ao nível teórico, como a nível experimental, consideramos ganhar as bases necessárias para um melhor controlo de acesso em qualquer rede ou sistema.

5 Bibliografia/Webgrafia

`http://www.cs.cornell.edu/courses/cs5430/2011sp/NL.accessControl.html`
`http://www.cs.unc.edu/~dewan/242/f96/notes/prot/node1.html`
`https://github.com/achintverma/Bell-LaPadula`