Universidade do Minho
Departamento de Informática

Mestrado Integrado em Engenharia Informática

Network Security

TP2 - Controlo de Acesso: Aplicação do modelo de Bell-LaPadula

Grupo 5
A86617 Gonçalo Nogueira
A74806 João Amorim
A75876 Jorge Cardoso
A78566 Marcos Silva
A82529 Carlos Afonso

Braga
Novembro, 2020

Conteúdo

Lista de Figuras

1 Introdução

No âmbito da unidade curricular de Segurança de Redes foi-nos proposto a realização de um trabalho com o objetivo de desenhar uma política de controlo de acesso num contexto de ensino universitário. Os mecanismos de controlo de acesso têm como objetivo principal a autorização ou bloqueio de acesso a recursos consoante o que a entidade tenta aceder. Além disso, permite ainda distinguir o tipo de permissões que cada entidade possui sobre diferentes objetos, como por exemplo, acesso apenas de leitura ou de leitura e escrita.

2 Conceitos Importantes

2.1 Políticas de Controlo de Acesso

2.1.1 Discretionary Access Control

É uma política de controlo de acesso definida como um meio de garantir ou restringir o acesso a objetos com base na identidade dos sujeitos e/ou grupos aos quais eles pertencem. Os controlos são discricionários no sentido em que o sujeito com uma certa permissão de acesso seja capaz de passar esta permissão (talvez indiretamente) para qualquer outro sujeito.

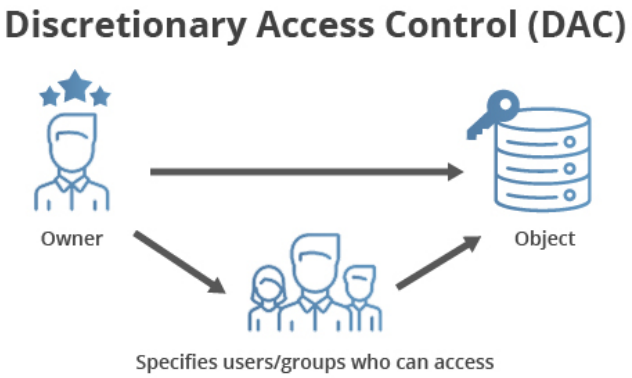

Figura 1: Política DAC

2.1.2 Mandatory Access Control

É uma estratégia de controlo de acesso que restringe a possibilidade que os proprietários têm para permitir ou negar acesso a serviços num sistema de ficheiros. Os critérios MAC são definidos pelo administrador do sistema e são impossíveis de sofrerem alterações por parte do utilizador normal ou comum. Esta estratégia é predominantemente implementada por organizações governativas ou militares e funciona baseando-se na designação de classificações para cada objeto como por exemplo confidential, secret ou Top secret e cada utilizador tem um nível de acesso semelhante podendo aceder apenas a objetos que a sua designação o permite.

2.2 Modelo de Especificação Formal

2.2.1 Modelo Bell-LaPadula

O modelo foca-se na confidencialidade de dados e no controlo de acesso à informação privada onde as entidades de um sistema são divididas em processos/objetos. Neste modelo é definida a noção de nível de segurança, onde se demonstra que numa transição de nível para outro se preserva a segurança. Este nível de segurança é só considerado totalmente seguro se os acessos aos objetos de um sistema estiverem de acordo com a política de segurança implementada. Os utilizadores sujeitos a este modelo apenas podem criar/escrever conteúdo no seu nível de segurança ou o nível acima, mas apenas podem ver conteúdo no seu nível ou abaixo.

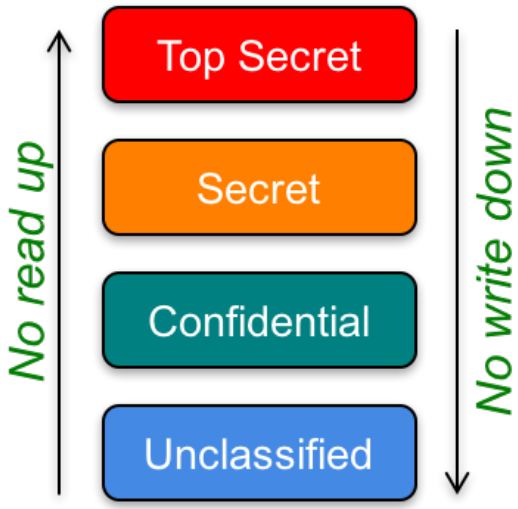

Figura 2: Representação do Modelo Bell-LaPadula

3 Lattice num Contexto Universitário

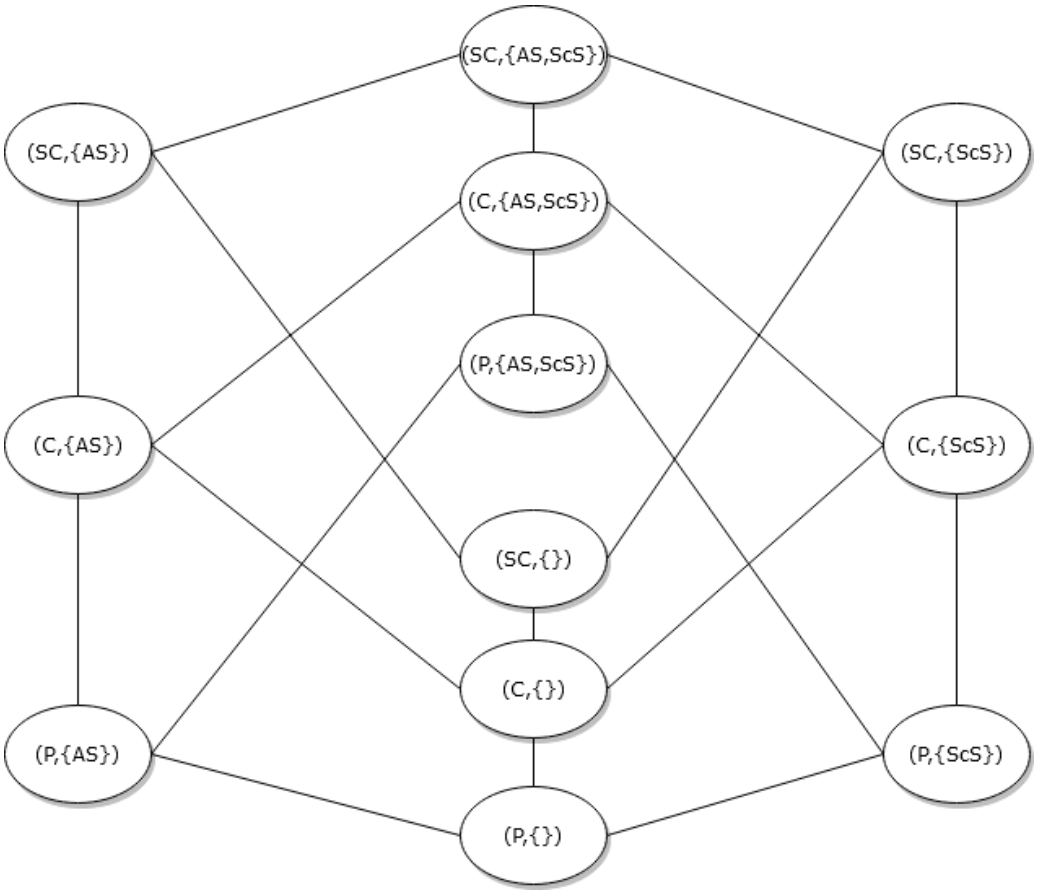

Figura 3: Lattice de Níveis de Segurança

É-nos pedido no trabalho, que consideremos duas condições importantes na construção da lattice, as labels de aluno (C, {AS}) e professor (C, {AS,ScS}). É importante também referir que é necessário que as labels de um nível superior têm de ter um nível de segurança mais restrito e conter a informação de uma label abaixo sempre garantindo a dominância entre labels diferentes. No caso específico de aluno e professor, uma vez que estão ambos no nível confidencial, o aluno não tem permissão para ler ou escrever nesse nível na label do professor, logo não é possível o aluno modificar objetos inseridos pelo professor. Para a atribuição de notas pelo professor e necessário também que este possua uma label (C, {AS}) equivalente á do aluno.

3.1 É possível um aluno ser fraudulento para com o Professor?

Tendo em consideração a lattice acima, numa primeira vista, parece ser praticamente impossível um aluno ser capaz de ser fraudulento. No entanto, isto pode não ser verdade. Partindo do princípio que os utilizadores podem criar/escrever conteúdo no seu nível de segurança ou o nível acima e apenas podem ver conteúdo no seu nível ou abaixo, podemos simular o seguinte caso. Um professor (C,{AS,ScS}) escreve as notas finais para um nível de acesso superior(Serviços Academicos). Após a aprovação por parte dos serviços académicos, estes irão divulgar, sob domínio publico, as notas, de forma a que os alunos possam ter acesso. Posto isto, uma das formas de ser fraudulento, seria o chamado *blindwrite*, segundo o qual, o aluno poderia escrever na pauta das notas, antes de esta ser aprovada pelos funcionários dos serviços académicos, uma vez que está a escrever para um nível de segurança superior, sendo então possível apagar os dados todos, ou alterar a sua própria nota, sendo isto algo complexo de concluir com sucesso.

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

WO: Write-Only
RO: Read-Only

Figura 4: Tabela de Permissões baseada na lattice definida

4 Processo de Desenvolvimento Automático do Modelo numa Infraestrutura Típica TIC

Por último era-nos pedido que elaborássemos uma possível implementação da lattice para o sistema universitário em questão. Nesta tarefa recorremos ao uso dos comandos acl (*Access Control Lists*, já presentes no Linux, que providenciam mecanismos de permissão para sistemas de ficheiros. Possibilita a permissão, a qualquer utilizador, para um determinado recurso. Usa a política *Discretionary Access Control.*

Como exemplo prático, iniciámos o processo com a criação de grupos, e seus respetivos utilizadores, para Reitoria UM e Corpo Docente, considerando que estes pertencem às labels **(SC,AS,ScS)** e **(C,AS,ScS)**, respetivamente.

Figura 5: Criação de Utilizadores para os Grupos Reitoria e Corpo Docente

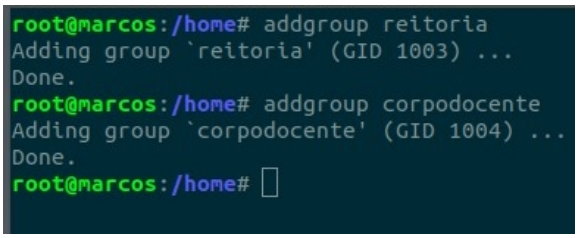

Figura 6: Criação de Grupos

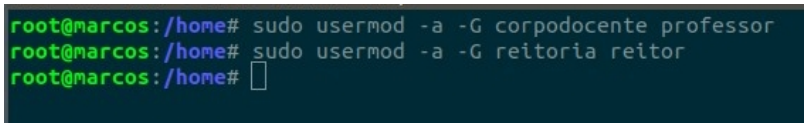

Figura 7: Atribuição dos Utilizadores aos Grupos

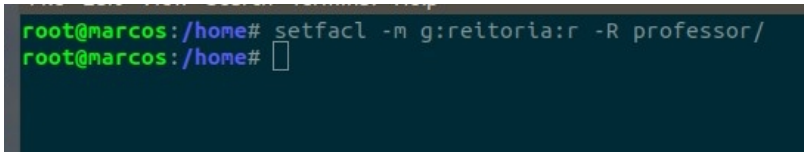

Figura 8: Reitoria tem permissão de leitura sobre o conteúdo de Professor

Figura 9: Corpo docente tem permissão de escrita sobre o conteúdo de Reitor

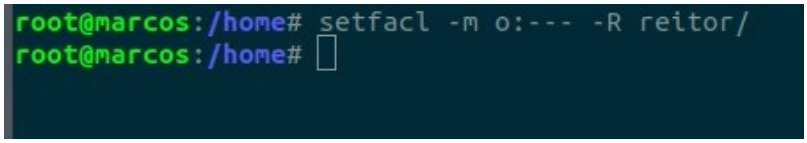

Figura 10: Grupos não têm acesso ao conteúdo de Reitor

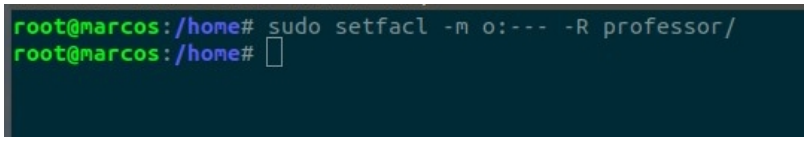

Figura 11: Grupos não têm acesso ao conteúdo de Professor

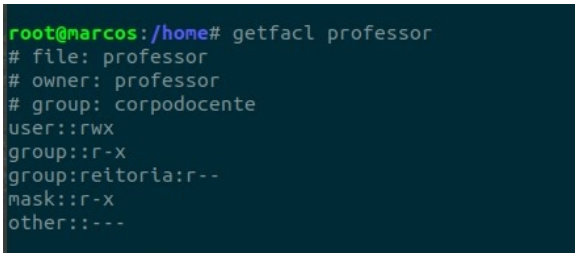

Figura 12: Estado Final de Professor

Figura 13: Estado final de Reitor

Nesta nossa implementação foi usada a gestão de controlo de acesso já implementada no Sistema Operativo Linux para uma configuração mais especifica poderia ser utilizada a ferramenta *Security Enhanced Linux* (SELinux) que implementa MAC (*Mandatory Access Control*)por cima de DAC(*Discretionary Access Control*) que o Linux já implementa.

5 Conclusão

Após a conclusão deste trabalho prático, sentimos-nos satisfeitos com os resultados alcançados e com os conhecimentos mais consolidados acerca de mecanismos de segurança no controlo de acesso, conseguindo na nossa opinião implementar corretamente o modelo de segurança proposto.

Conseguimos também criar um processo que implementa a lattice criada no primeiro momento do trabalho numa infraestrutura TIC típica, em ambiente Linux, onde usámos as regras de acesso e permissões de acesso a objetos definidas na lattice.

Concluindo, os elementos do grupo ficaram com a noção da complexidade e das necessidades de controlo de acesso aos recursos de uma instituição académica neste caso mas que representa todo o tipo de instituições independentemente do tipo e objetivos.

6 Bibliografia

Pfleeger, Charles P., Pfleeger, Shari L., *Security in Computing*, Fourth Edition, Prentice Hall PTR, 2007

`http://www.cs.cornell.edu/courses/cs5430/2011sp/NL.accessControl.html`

`http://www.cs.unc.edu/~dewan/242/f96/notes/prot/node1.html`

`https://www.redhat.com/sysadmin/linux-access-control-lists`