Universidade do Minho
Escola de Engenharia

SEGURANÇA EM REDES DE COMPUTADORES

TP2 - CONTROLO DE ACESSO

MESTRADO INTEGRADO EM ENGENHARIA DE TELECOMUNICAÇÕES E INFORMÁTICA

Grupo 4:

70020 – José Pedro Afonso Rocha

73232 – Luís Pedro Lobo de Araújo

ÍNDICE

INTRODUÇÃO

No âmbito da Unidade Curricular de Segurança em Redes de Computadores foi-nos proposto desenhar uma política de controlo de acesso no contexto de uma instituição de ensino universitário.

Os mecanismos de controlo de acesso têm o intuito de autorizar ou bloquear o acesso a recursos consoante o sujeito que o tenta aceder. Permite ainda fazer a distinção ao tipo de permissões que cada sujeito tem sobre diferentes objetos, por exemplo, acesso só de leitura, ou leitura e escrita.

CONCEITOS TEÓRICOS

DISCRETIONARY ACCESS CONTROL

Discretionary Access Control, é um tipo de segurança de controlo de acesso que garante ou restringe o acesso a um objeto através de uma política de segurança determinada pelo grupo criador do objeto e, este mecanismo de controlo, normalmente é definido pela autenticação de um utilizador com credenciais válidas, como por exemplo, o nome de utilizador e respetiva password.

Os DAC's são discricionários porque o dono de um sistema que utilize esta estratégia (sujeito mais alto de uma hierarquia) pode transferir objetos autenticados ou permitir/determinar o acesso à informação para outros utilizadores neste sistema (privilégios de acesso ao objeto).

MANDATORY ACCESS CONTROL

Mandatory Access Control (MAC) é uma estratégia de segurança que restringe a possibilidade que os proprietários têm para permitir ou negar acessos a serviços num sistema de ficheiros.

Os critérios do MAC são definidos pelo administrador do sistema, estritamente implementadas pelo sistema que o está a utilizar e são impossíveis de alterar pelo utilizador final ou comum.

Esta estratégia de segurança é frequentemente implementada por organizações governativas ou militares e funciona baseando-se na designação de classificações para cada objeto de um sistema de ficheiro. Estas classificações podem ser *Confidential, Secret ou Top Secret* e cada utilizador ou dispositivo num sistema baseado nestas classificações tem um nível de designação e permissão semelhante.

Apesar de ser a estratégia de segurança de controlo de acesso mais segura disponível, esta precisa de um planeamento e de uma monitorização contínua para manter todos os recursos e classificações de utilizadores atualizados e pode ser conjugada com o controlo de acesso descrito anteriormente (DAC).

MODELO *BELL-LAPADULA*

O modelo Bell-Lapadula foca-se na confidencialidade de dados e no controlo de acesso à informação privada onde as entidades de um sistema de informação são divididas em *subjects/objects* (processos/objetos).

Neste modelo é definido a noção de "nível de segurança ", onde é provado que numa transição de um nível para outro preserva a segurança com transições que podem ser definidas por certas funções, o que satisfaz os objetivos deste modelo. Este nível de segurança só pode ser marcado como totalmente seguro se os acessos aos *objects* de um sistema estiverem de acordo com a política de segurança implementada.

Os utilizadores que estejam 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 no abaixo. Por exemplo, um investigador secreto pode criar ficheiros secretos ou muito secretos, mas não podem criar ficheiros públicos e apenas podem ver ficheiros púbicos ou secretos, sem poder visualizar ficheiros muito secretos.

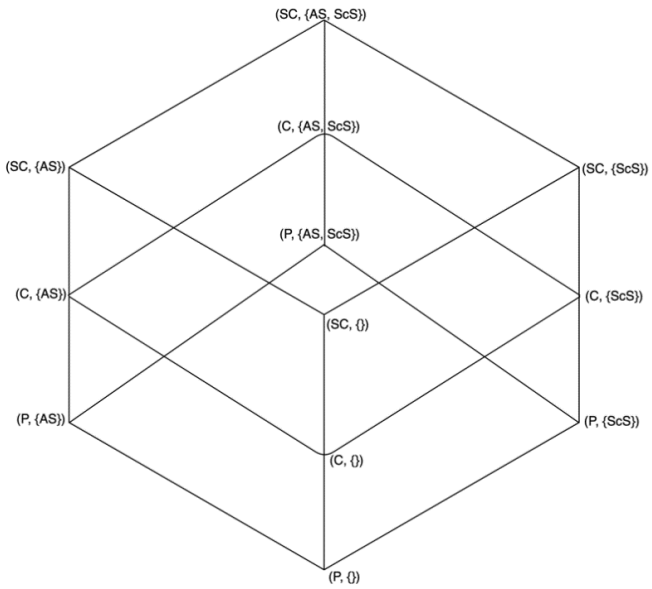

FIGURA 1 - *LATTICE* CRIADA PARA O CONTEXTO UNIVERSITÁRIO.

É pedido, neste trabalho prático, que sejam consideradas duas condições importantes para a construção da *lattice* (modelo onde as *designações/labels* estão num formato semelhante a um grafo) que são a classificação do professor e do aluno, onde o professor é classificado com a *label* (C,{AS,ScS}) e o aluno com a *label* (C,{AS}).

São três os níveis de segurança presentes neste trabalho, que são o P (*Public*), C (*Confidencial*) e SC (*Strictly Confidential*) com as categorias AS (*Academic Services*) e ScS (*Scientific Services*).

É também importante referir que é determinante e necessário que as *labels* de um nível superior têm de ter de um nível de segurança mais restrito e conter a informação de uma *label* abaixo sempre garantido a dominância entre *labels* diferentes. Matematicamente, isto pode ser explicado através de um caso óbvio e simples de duas *labels* diferentes, onde L1 = (S1, C1) e L2 = (S2, C2) e, se L1 ≤ L2 (L1 não é mais restritivo que L2) e C1 (contido) C2, então conclui-se que L2 tem dominância sobre L1.

No caso específico do Aluno e Professor, visto ambos estarem no nível *Confidential*, o Aluno não tem permissões de leitura e escrita nesse nível na *label* do Professor. Logo, não é possível o Aluno adulterar objetos inseridos pelo Professor.

Para a atribuição das notas pelo professor é necessário que este também possua uma *label* de (C,{AS}) equivalente à do aluno.

TABELA 1 - *LABELS* E UTILIZADORES ASSOCIADOS.

	{}	{AS}	{ScS}	{AS,ScS}
Strictly Confidential	-Ministério da Educação	-Serviços Académicos	-Departamentos	-Reitoria
Confidential	-Serviços de Ação Social	-Alunos	-Investigadores	-Professores
Public	-Visitantes	-Porteiros	- Investigadores externos	-Ficha de Candidatura

Na tabela acima foram inseridos os utilizadores associados às várias *labels* da *lattice*.

DESENVOLVIMENTO DA *LATTICE* NUMA INFRAESTRUTURA TIPICA DE TIC

Para a implementação da *lattice* criada para o contexto deste trabalho prático foram configurados no Linux 2 grupos de utilizadores, um para a Reitoria e outro para os Professores, como um exemplo prático.

Inicialmente foram criados os grupos e os respetivos utilizadores.

```
osboxes@osboxes:~$ sudo useradd -m prof
[sudo] password for osboxes:
osboxes@osboxes:~$ sudo useradd -m reitor
osboxes@osboxes:~$ sudo passwd prof
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
osboxes@osboxes:~$ sudo passwd reitor
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

FIGURA 2 - CRIAÇÃO DE UTILIZADORES.

```
root@osboxes:/home/osboxes# addgroup reitoria
Adding group `reitoria' (GID 1004) ...
Done.
root@osboxes:/home/osboxes# addgroup profs
Adding group `profs' (GID 1005) ...
Done.
root@osboxes:/home/osboxes# less /etc/gr
groff/  group   group-  grub.d/
root@osboxes:/home/osboxes# less /etc/group
root@osboxes:/home/osboxes# sudo usermod -a -G profs prof
root@osboxes:/home/osboxes# sudo usermod -a -G reitoria reitor
```

FIGURA 3 - CRIAÇÃO DE GRUPOS E ATRIBUIÇÃO DE UTILIZADORES.

Em seguida foram configuradas a permissões de acesso de cada grupo.

```
root@osboxes:/home# sudo chown -R :profs prof/
```

FIGURA 4 - ATRIBUIÇÃO DE GRUPO A PASTA DE UTILIZADOR PROF.

```
root@osboxes:/home# sudo chown -R :reitoria reitor/
```

FIGURA 5 - ATRIBUIÇÃO DE GRUPO A PASTA DE UTILIZADOR REITOR.

```
root@osboxes:/home# setfacl -m g:reitoria:r -R prof/
```

FIGURA 6 - REITORIA PODE LER O CONTEUDO DE PROF.

```
root@osboxes:/home# setfacl -m g:profs:w -R reitor/
```

FIGURA 7 - PROFESSORES PODEM ESCREVER PARA O REITOR.

```
root@osboxes:/home# sudo setfacl -m o:--- -R prof/
```

FIGURA 8 - TODOS OS OUTROS GRUPOS NÃO TÊM ACESSO AO CONTEUDO DO PROFESSOR.

```
root@osboxes:/home# setfacl -m o:--- -R reitor/
```

FIGURA 9 - TODOS OS OUTROS GRUPOS NÃO TÊM ACESSO AO CONTEUDO DO REITOR.

```
root@osboxes:/home# getfacl reitor/
# file: reitor/
# owner: reitor
# group: reitoria
user::rwx
group::rwx
group:profs:-w-
mask::rwx
other::---
```

FIGURA 10 - CONFIGURAÇÃO FINAL DO CONTEUDO DO REITOR.

```
root@osboxes:/home# getfacl prof/
# file: prof/
# owner: prof
# group: profs
user::rwx
group::rwx
group:reitoria:r--
mask::rwx
other::---
```

FIGURA 11 - CONFIGURAÇÃO FINAL DO CONTEUDO DO PROFESSOR.

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

CONCLUSÃO

Após conclusão deste trabalho prático, o grupo sente-se satisfeito com os conhecimentos consolidados acerca dos mecanismos de segurança no controlo de acesso, conseguindo implementar corretamente o modelo de segurança proposto, o que permitiu responder a uma questão pertinente colocada pelos docentes.

Conseguiu-se também criar um processo que implementa uma *lattice* numa infraestrutura TIC típica, em ambiente Linux, usando regras de acesso e permissões de acesso a objetos.

Com isto, os alunos ficaram com uma melhor noção das necessidades de controlo de acesso aos recursos de uma instituição.