Universidade do Minho
Escola de Engenharia

Mestrado Integrado em Engenharia de Telecomunicações e Informática

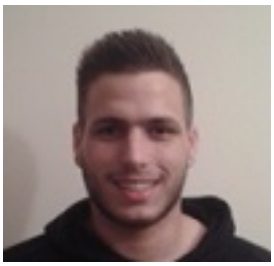
Segurança em Redes de Computadores

Trabalho Prático Nº2

Modelação do Controlo de Acesso

Grupo 5

Fernando Guimarães
A70012



Hélder Veloso
A70017

Luís Ferreira
A70016

14 de Março de 2017

Índice

Lista de Figuras

Página

1. Introdução

O mecanismo de controlo de acesso visa garantir o acesso autorizado a determinada propriedade. Este mecanismo é composto por três processos distintos, a autenticação, autorização e auditoria.

A autenticação trata-se da identificação do utilizador que pretende ter acesso ao sistema através de credenciais, como por exemplo um endereço eletrónico e a respetiva palavra-chave. A autorização define os direitos e permissões que o utilizador tem no sistema que implementa o controlo de acesso. Por fim a auditoria permite através da análise de dados relativos à utilização dos recurso do sistema, concluir a natureza dessa mesma utilização.

Estes processos são utilizados consoante as técnicas de controlo acesso implementadas, estas técnicas podem ser discricionárias, obrigatórias ou *Role-Based*. O controlo de acesso discricionário é uma política de controlo de acesso determinada pelo proprietário do recurso. É este que atribui as permissões de acesso à sua propriedade. Por outro lado a política de controlo de acesso obrigatório é o sistema que determina as propriedades de acesso aos seus recursos e não os proprietários desses mesmos recursos. Existe uma terceira política, o controlo baseado em papéis, esta define os direitos e permissões consoante o papel que determinado utilizador tem dentro da sua organização. Esta técnica visa a simplificar a gestão de permissões dadas aos utilizadores dentro da mesma organização.

Para este trabalho prático é requerido a conceptualização de um modelo de controlo de acesso no contexto académico tendo como referência o modelo Bell - LaPadula.

2. Modelo Bell-LaPadula

O modelo Bell-LaPadula foi inicialmente adotado para o controlo de acessos em assuntos militares e governamentais. Nestes casos, utilizadores e objetos são divididos em diferentes níveis de segurança, isto é, os utilizadores apenas acedem a informação que corresponde ao seu nível de segurança. Duas afirmações de controlo de acesso que correspondem às duas regras em que o modelo de Bell-LaPadula assenta são por exemplo: "O público não pode ter acesso a dados confidenciais" e mais um exemplo, "Dados secretos não podem ser escritos em ficheiros de acesso público".

É este tipo de divisão para controlar os acessos que o modelo Bell-LaPadula cria, sendo que os níveis de acesso vão de `público` a `confidencial` e `estritamente confidencial`, por exemplo.

Estes diferentes níveis que garantem o controlo de acesso são atribuídos a utilizadores e a objetos. Entenda-se que um utilizador pode ser um ser humano, um computador ou uma organização, e um objeto poderá ser dispositivos de *input/output*, ficheiros e documentos.

2.1 *Mandatory Access Control*

Uma *Mandatory Access Control* (MAC), ou em português, um controlo de acessos obrigatório é um tipo de política que corresponde a atribuir os direitos de acesso baseados nos regulamentos da organização. Este tipo de políticas assentam no facto da informação pertencer à organização e não ser apenas de carácter individual, sendo assim da competência da organização garantir o controlo da política de segurança. Este tipo de políticas esforça-se para combater e evitar ataques do tipo cavalo de Troia.

A forma de restringir o acesso de utilizadores a objetos baseia-se numa *label*

com a informação dos dados contidos nos objetos e do nível de autorização dos utilizadores a informação dessa sensibilidade.

Estas diferentes *labels* são então dispostas numa espécie de grafo, *lattice* onde é necessário garantir a dominância entre diferentes *labels*, ou seja, *labels* de um nível superior têm de ser de um nível de segurança mais restrito e conter a informação da *label* abaixo. Em termos matemáticos, esta dominância pode ser exemplificada da seguinte forma:

Tendo duas *labels* diferentes, $L1 = (S1, C1)$ e $L2 = (S2, C2)$, se tivermos que $L1 \leq L2$, significando que $L1$ não é mais restritivo que $L2$ e que $C1 \subseteq C2$, fica claro que *label* $L2$ tem então dominância sobre a *label* $L1$.

Neste trabalho prático, é pedido que na construção da *lattice* se tenha em conta que os professores são classificado com a *label* `(C,{AS,ScS})` e os alunos com a *label* `(C,{AS})`, sendo que existem três níveis de segurança, **P** para o nível Público, **C** para o nível Confidencial e por último **SC** para *Strictly Confidential*, com as categorias **AS** para os Serviços Académicos e **ScS** para os serviços científicos. Com isto em mente, a *lattice* criada para este trabalho prático está demonstrada na Figura 2.

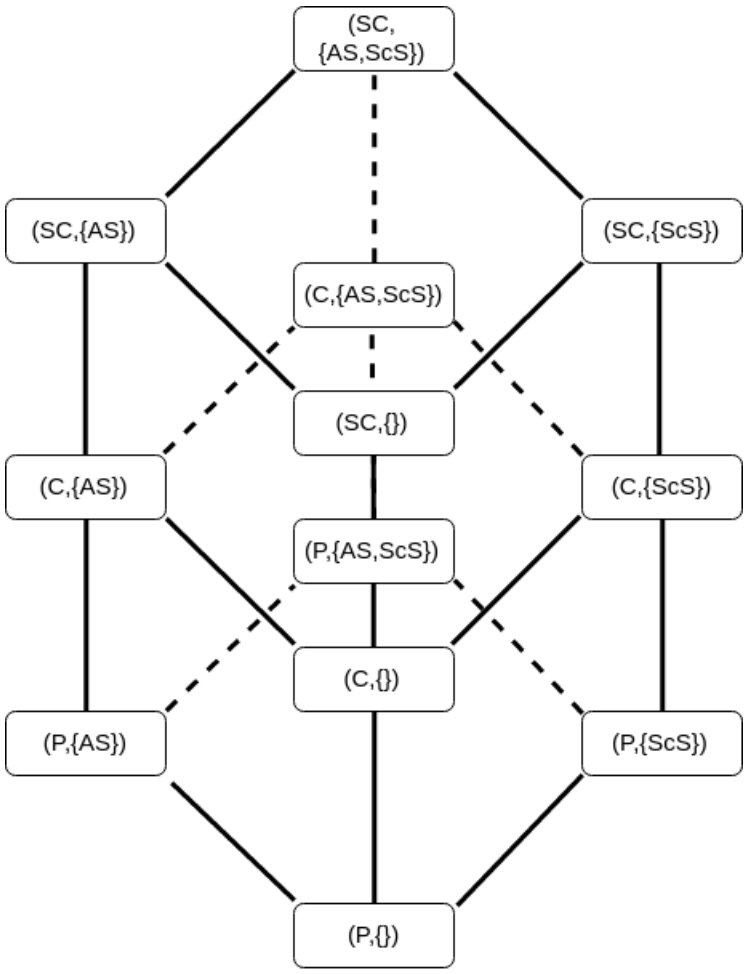


Figura 2: *Lattice* criada neste trabalho prático.

No diagrama anterior podemos verificar a existência destas dominâncias entre diferentes *labels*. Por exemplo a *label* `(SC,{AS,ScS})` é dominante sobre as *labels* `(SC,{ScS})`, `(SC,{AS})` e `(C,{AS,ScS})`. A *label* `(SC,{AS,ScS})` acaba por ser dominante sobre todas as restantes *labels* por consequência da demonstração anterior. Como este trabalho é desenvolvido no contexto universitário, podemos dizer que a *label* com dominância sobre as restantes poderia ser o Reitor da Universidade, por exemplo.

É importante notar que as regras de controlo da informação são garantidas. Seja $L(x)$ a *label* da relação x, um utilizador U apenas pode ler ficheiros F se $L(F) \leq L(U)$, ou seja, os utilizadores não conseguem "ler para cima". Um utilizador U poderá escrever num ficheiro F apenas se $L(U) \leq L(F)$, ou seja, os utilizadores não podem "escrever para baixo".

De forma a compreender visualmente este tipo de regras, temos na Figura 3

um exemplo com quatro nível de segurança, **TS** para *Top-Secret*, **S** para *Secret*, **C** para *Classified* e por fim **U** para *Unclassified*.

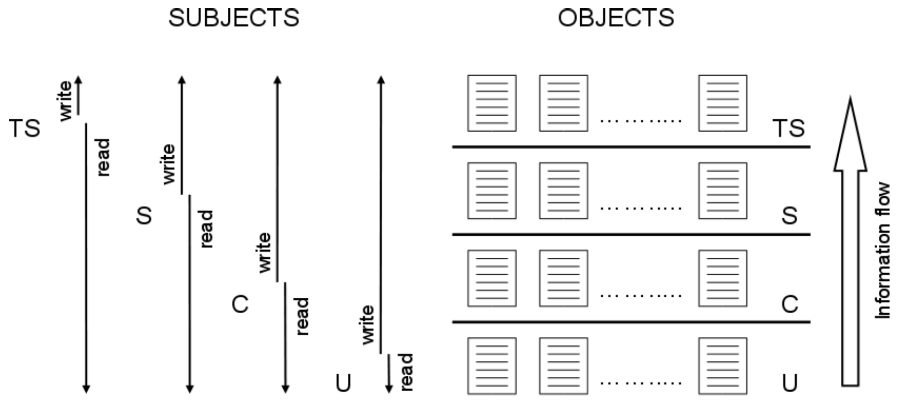


Figura 3: Regras que estabelecem a *Mandatory Access Control*.

2.2 *Discretionary Access Control*

A *Discretionary Access Control* (DAC) é a política onde são atribuídos as diferentes permissões baseada nas regras de cada utilizador. Este tipo de política inclui o modelo das permissões dos ficheiros que são utilizadas pela maioria dos sistemas operativos.

Para além dos utilizadores, a DAC utiliza os objetos e ações associadas a esses objetos.

Os utilizadores definidos neste trabalho prático são os professores e os alunos, e como objetos o grupo escolheu o trabalho realizado pelo aluno e a nota final atribuída pelo professor ao aluno. Como ações temos a ação **R** para leitura e a ação **W** para escrita. Com estes objetos e ações, foi possível construir a matriz seguinte, onde através das duas ações utilizadas, leitura e escrita, podemos combater teoricamente, o problema dos professores interferirem com o trabalho dos alunos, será impossível garantir que os alunos copiem entre si uma vez que o modelo apenas garante a confidencialidade do sujeitos envolvidos.

Utilizadores \Objetos	Trabalho	Nota final
Aluno	W	R
Professor	R	W

2.3 Considerações sobre o modelo de segurança

É necessário ter em conta determinadas características desta implementação.

- A possibilidade de o nível de segurança atribuído a um utilizador ser alterado durante uma sessão poderá afetar o fluxo de informação que se pretende preservar.

- Este modelo apenas garante a confidencialidade. A integridade de qualquer conteúdo poderá estar sujeito ao que se chama "blind write" ou seja, o reescrever de um ficheiro por parte de um processo que não tem permissão de leitura.

- Existe também um outro inconveniente, quando um determinado processo com permissões acima do nível de segurança do objeto que pretende escrever não tem permissão, devido à característica deste modelo de não permitir *write down*. Como tal é necessário a autenticação a níveis de segurança inferiores (ao nível de segurança do objeto) para que possa efetuar a operação pretendida.

3. Processo automático para implementação da *lattice* numa infraestrutura TIC típica

A tecnologia *Multi-Level Security* refere-se a um esquema de segurança que impõe o *Mandatory Access Model* Bell-La Padula. A aplicação de um sistema informático para processar informações com sensibilidades diferentes, isto é, a diferentes níveis de segurança (Figura 4), permite o acesso simultâneo de utilizadores com diferentes autorizações de segurança e necessidades de conhecimento e impede que os utilizadores obtenham acesso a informações para as quais não têm autorização.

Figura 4: Níveis de segurança.

As regras de acesso MLS são sempre combinadas com permissões de acesso convencionais (permissões de ficheiros). Por exemplo, se um utilizador com um nível de segurança de *"Secret"* usa o *Discretionary Access Control* (DAC) para bloquear o acesso a um ficheiro para outros utilizadores, isso também bloqueia o acesso a utilizadores com um nível de segurança de *"Top Secret"*. É importante lembrar que as regras de política do SELinux MLS são verificadas após as regras do DAC. Uma autorização de segurança mais elevada não dá automaticamente permissão para procurar arbitrariamente um sistema de ficheiros.

Os utilizadores com autorizações de nível superior não adquirem automatica-

mente direitos administrativos aos sistemas de vários níveis. Embora eles possam ter acesso a todas as informações no computador, isso é diferente de ter direitos administrativos.

As seguintes etapas são utilizadas para habilitar a política SELinux MLS no sistema, é um serviço bastante complexo daí ser apenas fornecida uma breve explicação de como este é configurado de forma a funcionar num sistema Linux.

1. Instalação do pacote selinux-policy-mls.

```
~]# yum install selinux-policy-mls
```

2. Antes da diretiva MLS ser habilitada, cada ficheiro no sistema deve ser classificado com um rótulo MLS de acordo com o modelo BLP elaborado acima. Depois do sistema de ficheiros ser classificado, domínios confinados podem ter acesso negado, o que pode impedir o sistema de iniciar corretamente. Para evitar que isso aconteça, é necessário a configuração `SELINUX = permissivo` no ficheiro `/etc/selinux/config`. Além disso, é também necessário a habilitação da diretiva MLS configurando `SELINUXTYPE = mls`.

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of these two values:
#       targeted - Targeted processes are protected,
#       mls - Multi Level Security protection.
SELINUXTYPE=mls
```

3. Configuração do SELinux em execução no modo permissivo.

```
~]# setenforce 0
```

```
~]$ getenforce
Permissive
```

4. Criação de um ficheiro *.autorelabel* na diretoria de raiz para garantir que os ficheiros sejam classificados na reinicialização seguinte do sistema.

```
~]# touch /.autorelabel
```

5. Reinicialização do sistema, durante a próxima inicialização, todos os sistemas de ficheiros serão classificados de acordo com a política MLS. O processo classifica todos os ficheiros com um contexto SELinux apropriado.

```
*** Warning -- SELinux mls policy relabel is required.
*** Relabeling could take a very long time, depending on file
*** system size and speed of hard drives.
***********
```

   Os caracteres " * " na linha inferior representa 1000 ficheiros que foram classificados. No exemplo acima, onze caracteres representam 11000 ficheiros já classificados. O tempo necessário para esta operação depende do número de ficheiros no sistema e da velocidade das unidades de disco rígido. Em sistemas modernos, esse processo pode levar apenas 10 minutos. Quando o processo de classificação terminar, o sistema será reinicializado automaticamente.

6. No modo permissivo, a política SELinux não é aplicada, mas as tentativas de acesso negadas ainda são registadas. Antes de mudar para o modo de *"enforcing"*, como *root*, é necessário a execução do seguinte comando para confirmar que o SELinux não negou ações durante a última inicialização. Se o SELinux não negou ações durante o último arranque, este comando não retorna nenhuma saída.

```
~]# grep "SELinux is preventing" /var/log/messages
```

7. Se não houver mensagens de negação no ficheiro `/var/log/messages`, ou se tiver resolvido todas as recusas existentes, é necessário a configuração do `SELINUX = enforcing` no ficheiro `/etc/selinux/config`.

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these two values:
#       targeted - Targeted processes are protected,
#       mls - Multi Level Security protection.
SELINUXTYPE=mls
```

8. Por fim, é necessário a reinicialização do sistema, verificando que o SELinux está em execução no modo de *"enforcing"* e a política MLS está habilitada.

```
~]$ getenforce
Enforcing
```

```
~]# sestatus |grep mls
Policy from config file:       mls
```

As seguintes etapas são utilizadas para criar um novo utilizador com um intervalo MLS específico.

1. Criação de um novo utilizador usando o comando *useradd* e mapeamento deste para um utilizador SELinux existente, neste caso, *user_ u*.

```
~]# useradd -Z user_u john
```

2. Atribuição de uma palavra passe ao utilizador recém-criado.

```
prompt~]# passwd john
```

3. Execução do seguinte comando como *root* para visualizar o mapeamento entre os utilizadores do SELinux e do Linux, o resultado deve ser parecido com o seguinte.

```
~]# semanage login -l

Login Name           SELinux User         MLS/MCS Range        Service

__default__          unconfined_u         s0-s0:c0.c1023       *
john                 user_u               s0                   *
root                 unconfined_u         s0-s0:c0.c1023       *
system_u             system_u             s0-s0:c0.c1023       *
```

4. Definição de um intervalo específico para o utilizador.

```
~]# semanage login --modify --seuser user_u --range s2:c100 john
```

5. Visualização novamente o mapeamento entre os utilizadores do SELinux e do Linux, agora o utilizador tem um intervalo MLS específico definido.

```
~]# semanage login -l

Login Name           SELinux User         MLS/MCS Range        Service

__default__          unconfined_u         s0-s0:c0.c1023       *
john                 user_u               s2:c100              *
root                 unconfined_u         s0-s0:c0.c1023       *
system_u             system_u             s0-s0:c0.c1023       *
```

6. Correção do rótulo na diretoria pessoal do utilizador executando o seguinte comando.

```
~]# chcon -R -l s2:c100 /home/john
```