Unidad 2: Control de acceso

Estado de protección del sistema

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Estado de un sistema

Es el conjunto de los valores actuales de todas las posiciones de memoria, de todo el almacenamiento secundario, de todos los registros del procesador y de otros componentes del sistema.

Estado de protección del sistema

Es el subconjunto de estados relacionado con la seguridad y protección del sistema.

Definiciones

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Sujetos

Entidades (usuarios, grupos, roles y procesos) que modifican los objetos y en consecuencia cambian el estado del sistema.

Objetos

Todas las entidades que son relevantes para el estado de protección del sistema. Es decir que deben ser protegidas. Por ejemplo: memoria, archivos o datos en dispositivos de almacenamiento secundario, directorios, programas, dispositivos de hardware, etc.

Definiciones

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Permisos

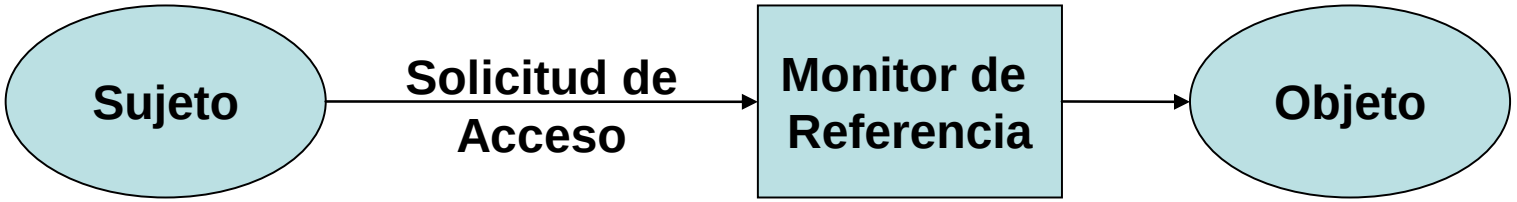
Acciones autorizadas que un sujeto puede realizar sobre un objeto.

Solicitud de acceso

Es una acción solicitada al sistema por un sujeto sobre un objeto con el fin de acceder al mismo .

Monitor de referencia (MR)

Mecanismo responsable de “mediar” cuando los sujetos intentan realizar operaciones sobre los objetos en función de una política de acceso.



Propiedades del MR

- Intermediación obligatoria

  Debe intervenir en todos los accesos.

- Aislamiento

  Tanto el MR como sus datos deben ser incorruptibles, sin posibilidad de modificaciones no autorizadas.

- Verificabilidad

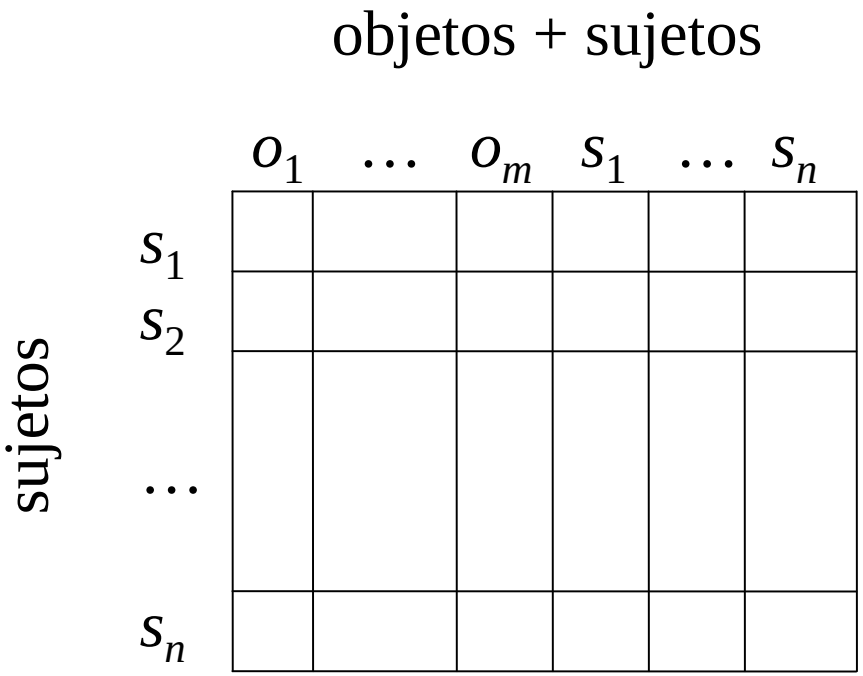
  Debe poder demostrarse que su funcionamiento es correcto.

Matriz de control de accesos

- Es un modelo conceptual que describe el estado de protección de manera precisa.

- Matriz que describe los permisos de los sujetos (usuarios o procesos) sobre los objetos.

Modelo conceptual



- Sujetos $S = \{ s_1,\ldots,s_n \}$
- Objetos $O = \{ o_1,\ldots,o_m \}$
- Permisos $R = \{ r_1,\ldots,r_k \}$
- Entradas $A[s_i, o_j] \subseteq R$

$A[s_i, o_j] = \{ r_x, \ldots, r_y \}$
Es decir el sujeto s_i tiene permisos $r_x, \ldots, r_y$ sobre el objeto o_j

Ejemplo

- Procesos proc1, proc2
- Archivos arch1, arch2
- Permisos r=read, w=write, x=execute, a=append, o=own

	arch1	arch2	proc1	proc2
proc1	*rwo*	*r*	*rwxo*	*w*
proc2	*a*	*ro*	*r*	*rwxo*

Ejemplo

- Usuarios alice, bob
- Archivos memo.doc, demo.exe, backup.pl
- Permisos r = read, w = write, x = execute

	memo.doc	demo.exe	backup.pl
alice	---	*x*	*rx*
bob	*rw*	*x*	*rwx*

Otro ejemplo

- Funciones inc_ctr, dec_ctr, manage
- Variable counter
- Permisos +, –, call

	counter	inc_ctr	dec_ctr	manage
inc_ctr	+			
dec_ctr	-			
manage		*call*	*call*	*call*

Implementación

Dos formas de implementar la matriz de control de accesos:

- Lista de control de accesos (ACL):

  Hay una lista por objeto. Indica los permisos que posee cada sujeto sobre el objeto.

- Lista de capacidades:

  Hay una lista por sujeto. Indica los permisos que posee el sujeto sobre cada objeto.

Lista de control de accesos

- Consiste en almacenar la matriz de control de accesos por columnas.

- Dado un objeto, tenemos las siguientes ventajas :
  - Es fácil ver los permisos del mismo para todos los sujetos.
  - Es fácil revocar todos sus accesos, reemplazando su ACL por una vacía.
  - Es fácil darlo de baja, borrando su ACL.

- Problemas:
  - ¿Cómo chequear a que puede acceder un sujeto?

Lista de capacidades

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

- Consiste en almacenar la matriz de control de accesos por filas.

- Dado un sujeto, tenemos las siguientes ventajas:
  - Es fácil de chequear todos los permisos que posee.
  - Es fácil de revocar sus permisos, reemplazando su lista de capacidades por una vacía.
  - Es fácil darlo de baja, eliminando su lista de capacidades.

- Problemas:
  - ¿Cómo chequear quien puede acceder a un objeto?

Tipos de control de acceso

Objetivo: controlar quien accede al sistema, quien accede a los recursos del sistema y cómo accede a los mismos.

Dos áreas bien diferenciadas:

- Control de acceso al sistema
- Control de acceso a los recursos

Control de acceso al sistema

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Objetivo: es permitir el acceso al sistema solo a aquellos usuarios autorizados.

Se utiliza un mecanismo que consiste de dos pasos:

- Identificación: el usuario le indica al sistema quien es.
- Autenticación: el sistema verifica la identidad del usuario.

Lo vamos a ver en la Unidad 4.

Control de acceso a los recursos

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Objetivo: establecer cuáles usuarios pueden acceder a los distintos recursos que provee el sistema y de que manera pueden hacerlo.

Hay dos reglas principales:

- Los recursos deben ser accedidos sólo por los usuarios autorizados. Es decir los que tienen permisos explícitos.
- Las acciones sobre los recursos deben ser las que están permitidas para esos usuarios.

Clasificación

Las técnicas de control de acceso generalmente se clasifican en:

- Control de acceso discrecional (DAC)
- Control de acceso mandatorio (MAC)

En la década del 90 surge:

- Control de acceso basado en roles (RBAC)

Control de acceso discrecional

El control de acceso discrecional (Discretionary Access Control - DAC) es una política de control de acceso determinada por el dueño de un recurso (un archivo, una impresora).

Es discrecional porque el dueño del recurso decide de manera arbitraria a quien le permite acceder al mismo y con que permisos.

Control de acceso discrecional

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

- Conceptos

  Propiedad: cada objeto en el sistema debe tener un dueño. La política de acceso es determinada por el dueño del recurso.

  En teoría un objeto sin dueño no se encuentra protegido.

  Normalmente el dueño de un recurso es el usuario que lo crea.

  Permisos: derechos de acceso que el dueño de un recurso asigna a usuarios individuales o a grupos de usuarios.

Control de acceso discrecional

- Conceptos

  Sujetos: usuarios o grupos de usuarios.

  Objetos: recursos del sistema

  Permisos: derechos de acceso para el par ordenado (S_i, O_j).

  Significa que el sujeto S_i puede acceder al objeto O_j de acuerdo con los derechos (read, write, execute, etc.) otorgados.

Control de acceso discrecional

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

- Ventajas

  Flexible y adaptable a muchos sistemas y aplicaciones.

  Ampliamente usado, especialmente en ambientes comerciales e industriales.

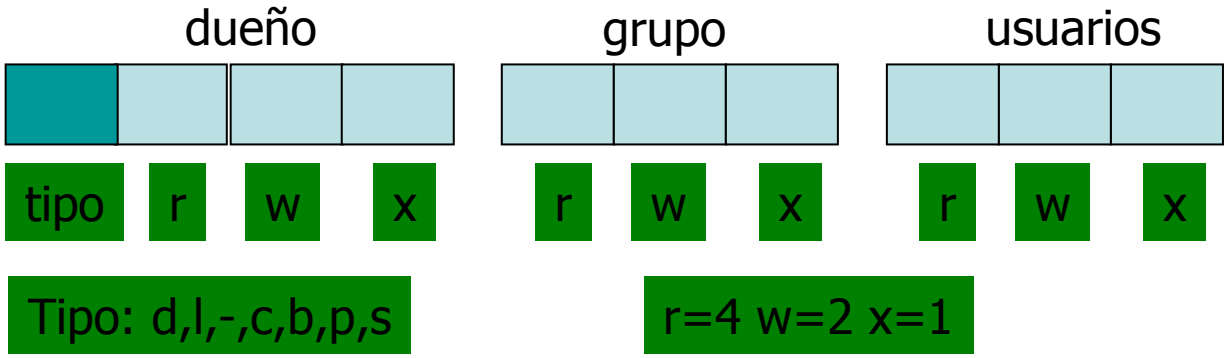
- Principal problema:

  Discrecionalidad para la cesión de derechos.

Permisos básicos en UNIX

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

- **Permisos de archivos**



192.168.234.139 - PuTTY

```
-rw-r----- 1 root shadow   928 Feb 14 08:23 shadow
-rw------- 1 root root     928 Feb 14 08:23 shadow-
-rw-r--r-- 1 root root     165 Feb 13 22:05 shells
drwxr-xr-x 2 root root    4096 Feb 13 22:05 skel
drwxr-xr-x 2 root root    4096 Mar  1 15:30 snmp
drwxr-xr-x 3 root root    4096 Feb 14 08:14 snort
drwxr-xr-x 2 root root    4096 Feb 13 23:06 ssh
drwxr-xr-x 4 root root    4096 Feb 15 14:44 ssl
-rw-r--r-- 1 root root    2082 Feb 24  2010 sysctl.conf
drwxr-xr-x 2 root root    4096 Feb 13 22:06 sysctl.d
drwxr-xr-x 2 root root    4096 Feb 13 22:05 terminfo
drwxr-xr-x 3 root root    4096 Feb 13 23:05 texmf
-rw-r--r-- 1 root root      21 Feb 13 22:06 timezone
-rw-r--r-- 1 root root    1260 May 30  2008 ucf.conf
drwxr-xr-x 4 root root    4096 Feb 13 22:06 udev
drwxr-xr-x 3 root root    4096 Feb 13 23:05 ufw
-rw-r--r-- 1 root root     274 Nov  4  2009 updatedb.conf
drwxr-xr-x 2 root root    4096 Feb 13 22:06 vim
drwxr-xr-x 2 root root    4096 Feb 13 23:06 w3m
drwxr-xr-x 2 root root    4096 Feb 24 11:07 webalizer
-rw-r--r-- 1 root root    4496 Sep  5  2010 wgetrc
drwxr-xr-x 3 root root    4096 Feb 13 22:06 X11
drwxr-xr-x 2 root root    4096 Feb 13 23:06 xml
root@debian6:/etc#
```

Permisos especiales

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

SETUID y SETGID son permisos de acceso que pueden asignarse a archivos o directorios en un sistema operativo basado en Unix. Se utilizan principalmente para permitir a los usuarios del sistema ejecutar binarios con privilegios elevados temporalmente para realizar una tarea específica.

Si un archivo tiene activado el bit "Setuid" se identifica con una “s” en un listado de la siguiente forma:

```
-rwsr-xr-x 1 root shadow 27920 ago 15 22:45 /usr/bin/passwd
```

Otros permisos en linux

- **Chattr.**

  Agrega atributos (append only, immutable, etc)

- **Posix ACLs (getfacl, setfacl) y NFSv4 ACLs**

  Flexibilizan las ACLs standard, posibilitando dar permisos a usuarios específicos, a más de un grupo, etc.

Componentes Seguridad Windows

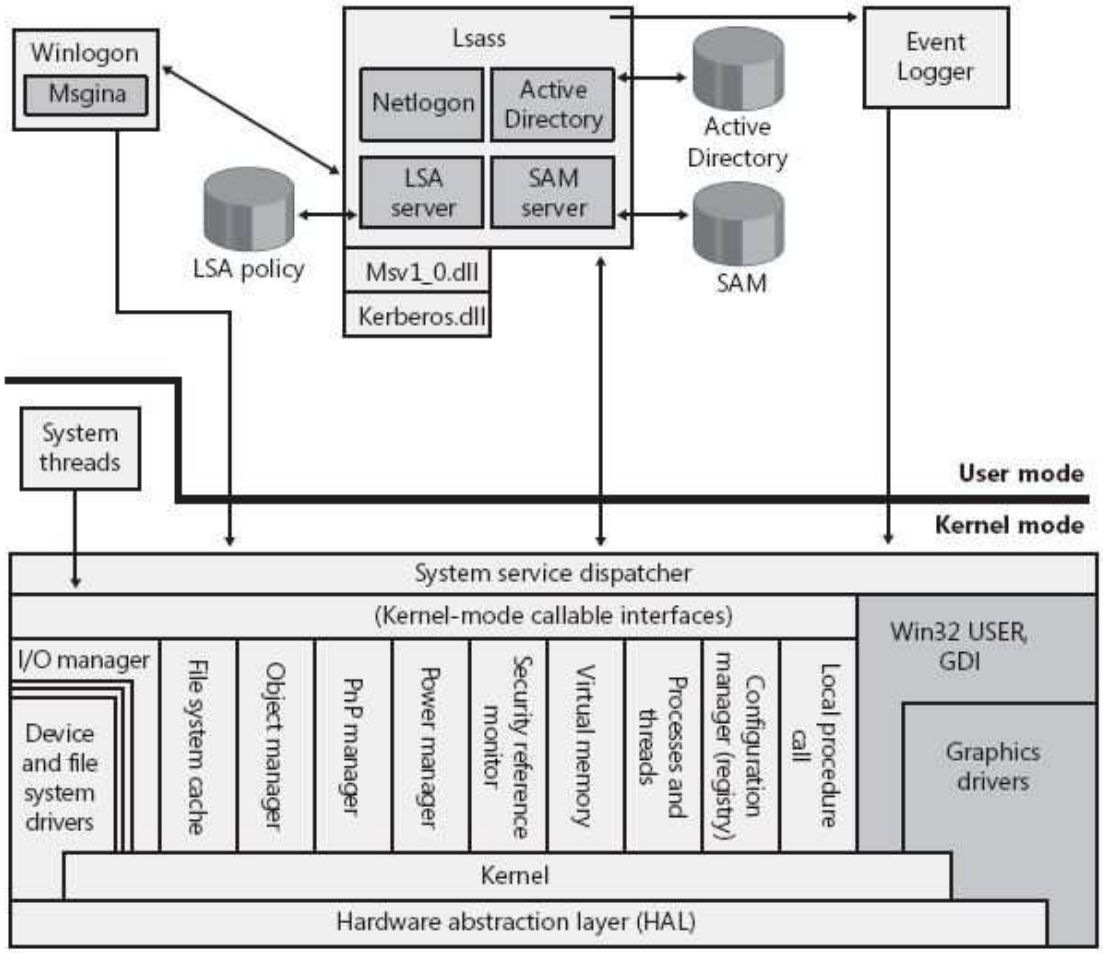


Figure 8-1 Windows security components

Fuente: Microsoft Windows Internals, 4th. edition

Control de acceso en Windows

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Windows NT4 o superior

SID (Windows security identifier): secuencia numérica que se utiliza para identificar usuarios, grupos y cuentas del sistema.

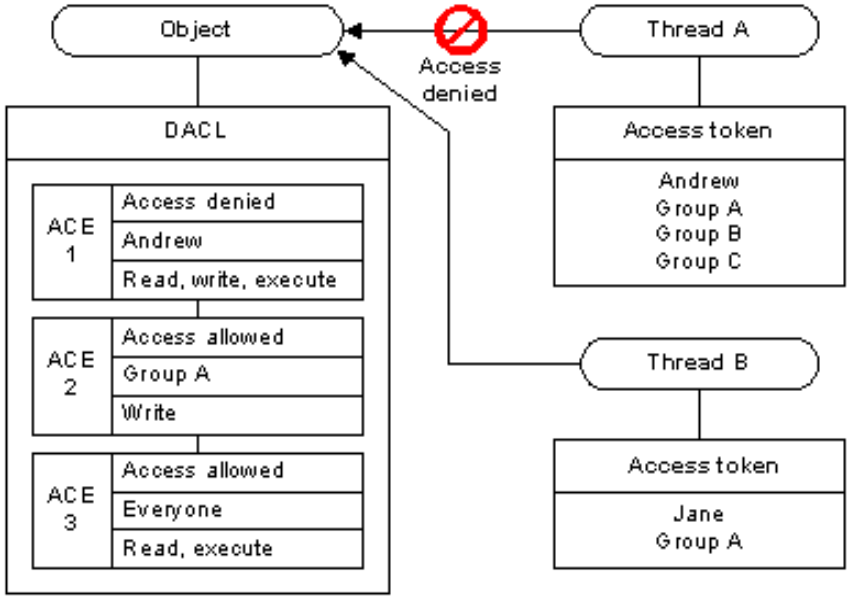
SID S-1-1-0 = grupo Everyone

A un objeto se le asigna una DACLs (Discretionary access-control list) que se compone de ACEs (Access Control Entry).

```
ace (denied, aceType(['ACCESS_DENIED_ACE_TYPE']),
                aceFlags,
                aceMask(['READ_CONTROL', 'SYNCHRONIZE']),
                sid('S-1-1-0')).
```

Ejemplo

- Thread A: el sistema lee ACE 1 y deniega el acceso. El sistema no chequea ACE 2 ni ACE 3.
- Thread B: ACE 1 no se aplica, el sistema toma ACE 2, que permite acceso de escritura y ACE 3 que permite lectura y ejecución.



Control de acceso mandatorio

El control de acceso mandatorio (Mandatory Access Control – MAC) es una política de control de acceso determinada por el sistema no por el dueño de un recurso. Clasifica a sujetos y objetos en niveles de seguridad.

Se utiliza en sistemas multinivel que procesan información altamente sensible.

Sistema multinivel: es un sistema de computadoras que maneja múltiples niveles de clasificación entre sujetos y objetos, como por ejemplo información gubernamental o militar.

Control de acceso basado en roles

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

RBAC (Role Based Access Control) surge a fines de la década del 80 y toma un fuerte impulso en los 90. Combina aspectos de DAC y de MAC, pero con una visión más orientada a la estructura organizacional.

Básicamente consiste en la creación de roles para los trabajos o funciones que se realizan en la organización.

Los miembros del staff se asignan a roles y a través de estos roles adquieren permisos para ejecutar funciones del sistema.

Control de acceso basado en roles

Los sujetos acceden a los objetos en base a las actividades que (los sujetos) llevan a cabo en el sistema. Es decir, considerando los roles que ocupan en el sistema.

Rol: es el conjunto de acciones y responsabilidades asociadas con una actividad en particular.

Control de acceso basado en roles

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Para implementar RBAC se necesitan mecanismos que permitan:

- Identificar los roles en un sistema y asignar los sujetos a los roles definidos.
- Establecer los permisos de acceso a los objetos para cada rol.
- Establecer permisos a los sujetos para que puedan adoptar roles.

Control de acceso basado en roles

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

- **Características de RBAC:**
  - Administración de autorizaciones
  - Jerarquía de roles
  - Menor privilegio
  - Separación de responsabilidades
- **Desventaja**
  - Dificultad de establecer los roles y definir sus alcances.

Control de acceso basado en roles

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Administración de autorizaciones:

- La asignación de permisos a usuarios tiene dos partes:
  - asociar usuarios a roles
  - asignar permisos para objetos a roles.
- Si un usuario cambia de tareas, solo basta con cambiarle el rol.

Es más sencillo que en DAC o en MAC.

Control de acceso basado en roles

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Jerarquía de roles:

- Los roles también poseen relaciones de jerarquía.
- Pueden heredar privilegios y permisos de otros roles de menor jerarquía, simplificando la administración de las autorizaciones.

Control de acceso basado en roles

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Menor privilegio:

- Permite implementar la política del menor privilegio posible.
- Si una tarea no va a ser ejecutada por un usuario, entonces su rol no tendrá los permisos para hacerla, de esta manera se minimizan riesgos de daños.

Control de acceso basado en roles

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

División de responsabilidades:

- Se basa en el principio de que ningún usuario tenga suficientes privilegios para usar el sistema en su propio beneficio.
- Por ejemplo, una persona encargada de autorizar un pago no debe ser el beneficiario de ese pago.

Se puede establecer de dos formas:

- Estáticamente: definiendo los roles excluyentes para un mismo usuario;
- Dinámicamente: realizando el control al momento de acceso.

Algunos estándares de RBAC

- **INCITS 359-2012**
- ***eXtensible Access Control Markup Language*. (XACML)**
- **XACML RBAC Profile**

Más información: http://csrc.nist.gov/groups/SNS/rbac/index.html

Algunas implementaciones de RBAC

- **Sun Solaris**
- **Microsoft Active Directory**
- **Base de datos Oracle**
- **Base de Datos MS Sql Server**

RBAC en Solaris

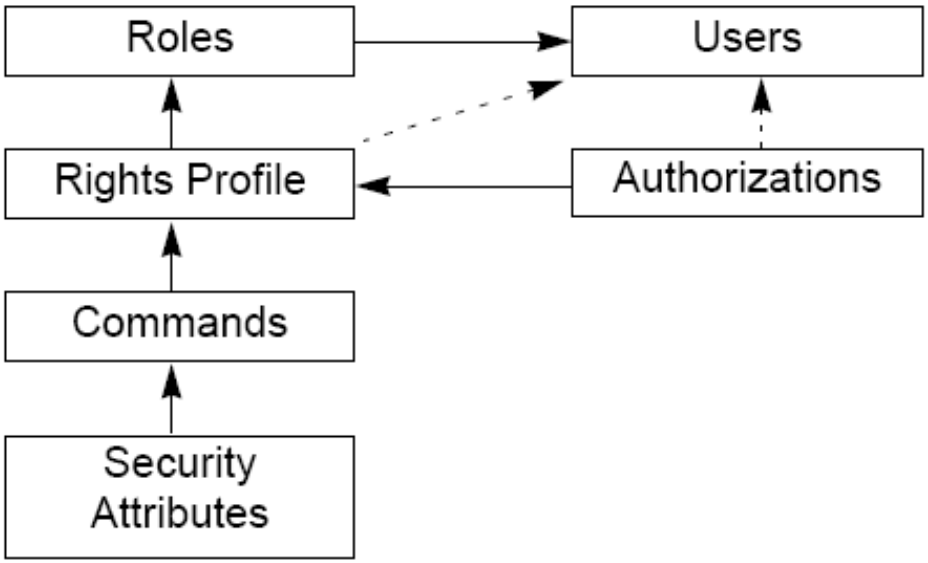
DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Rol:
Identidad especial asumida por los usuarios asignados.

Autorización:
Permiso que es asignado a un rol o a un usuario para realizar una cierta clase de acciones.

Perfil de permisos:
Se asignan a los roles y consisten de autorizaciones, comandos con atributos de seguridad, atributos de seguridad adicionales (en la forma de perfiles de permisos anidados)

RBAC en Solaris



Roles

Se crean de la misma manera que las cuentas (home directory, grupos, password, etc.)

Los usuarios que pueden asumir un mismo rol tienen el mismo home del rol, operan en el mismo entorno y tienen acceso a los mismos archivos.

Los usuarios asumen roles utilizando el comando “*su*”, no es posible ingresar al sistema con un rol de manera directa.

Cuando un usuario asume un rol pierde todos sus atributos y asume los del rol.

Perfiles de roles predefinidos:

- Primary Administrator
- System Administrator
- Operator

Autorizaciones

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

- Tienen un nombre, por ej.: *solaris.admin.usermgr.pswd*, y una descripción corta "*Change passwords*", esta convención permite que se manejen las autorizaciones en forma jerárquica y tambien utilizar "*"

- Ejemplo: acceso a configuracion de usuarios del sistema.
  - Operator: *solaris.admin.usermgr.read*
  - System Administrator: *solaris.admin.usermgr.read*
    solaris.admin.usermgr.write
  - Primary Administrator: *solaris.admin.usermgr.read*
    solaris.admin.usermgr.write
    solaris.admin.usermgr.pswd

Delegación de autorizaciones

- Si una autorización finaliza con el sufijo “*grant*” permite al rol delegar las autorizaciones que comienzan como el mismo prefijo.
- Por ejemplo, un rol con*: solaris.admin.usermgr.grant* y *solaris.admin.usermgr.read*, puede delegar el permiso de lectura a otro usuario.

Perfiles de permisos

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

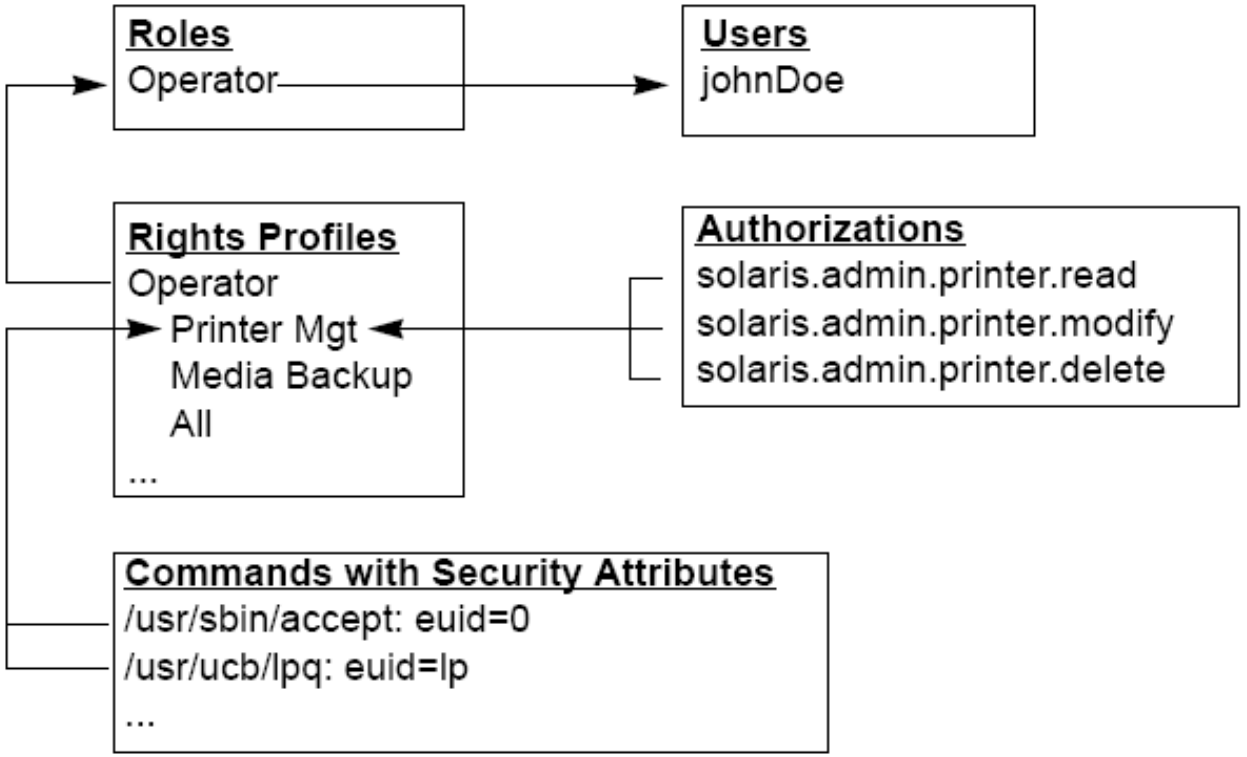
Primary Administrator: puede realizar todas las tareas administrativas

- Autorizaciones: *solaris.*, solaris.grant*
- Comandos: **:uid=0;gid=0*

Printer Manager: maneja impresoras.

- Autorizaciones: *solaris.admin.printer.delete*
  solaris.admin.printer.modify
  solaris.admin.printer.read
- Comandos: */usr/ucb/lpq:euid=0,*
  /etc/init.d/lp:euid=0,
  /etc/init.d/lpstat:euid=0,
  /etc/init.d/lpsqued:euid=0, etc.

Ejemplo


Roles
Operator
Users
johnDoe
Rights Profiles
Operator
Printer Mgt
Media Backup
All
...
Authorizations
solaris.admin.printer.read
solaris.admin.printer.modify
solaris.admin.printer.delete
Commands with Security Attributes
/usr/sbin/accept: euid=0
/usr/ucb/lpq: euid=lp
...