Control de acceso

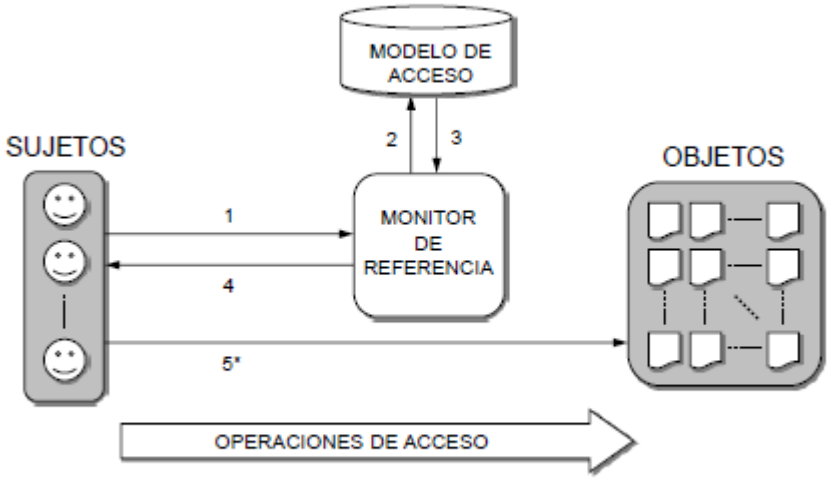
UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat d'Informàtica de Barcelona

inLab FIB
talent & tech

Matriz de accesos

- Sujetos o dominios: usuarios, grupos, roles y procesos que modifican objetos

- Objetos: entidades relevantes para el estado de protección. Memoria, archivos, datos, programas, etc



Matriz de accesos

Dom/Obj	F1	F2	F3	F4
D1	Read		Read	
D2				Print
D3		Read	Execute	
D4	Read Write		Read Write	

- Una matriz de acceso es una matriz donde las filas son sujetos/dominios y las columnas objetos
- Un acceso son las operaciones/permisos que un proceso ejecutado en un dominio puedo invocar en un objeto.
- Si un proceso de un dominio intenta hacer una operación esa operación debe estar en la tabla

	Memo.doc	Demo.exe	Backup.pl
Alice	---	**x**	**rx**
Bob	**Rw**	**x**	**rwx**

Clasificación

- Control de acceso discrecional (DAC)
  - Política determinada por el dueño del recurso. El dueño de la impresora decide quien accede y con qué permisos.
    - Permisos de unix
- Control de acceso mandatorio (MAC)
  - Politica determinada por el sistema. Clasifica a sujetos y objetos según niveles de seguridad.
    - Información gubernamental
- Control de acceso basado en roles (RBAC)
  - Combina aspectos de DAC y MAC

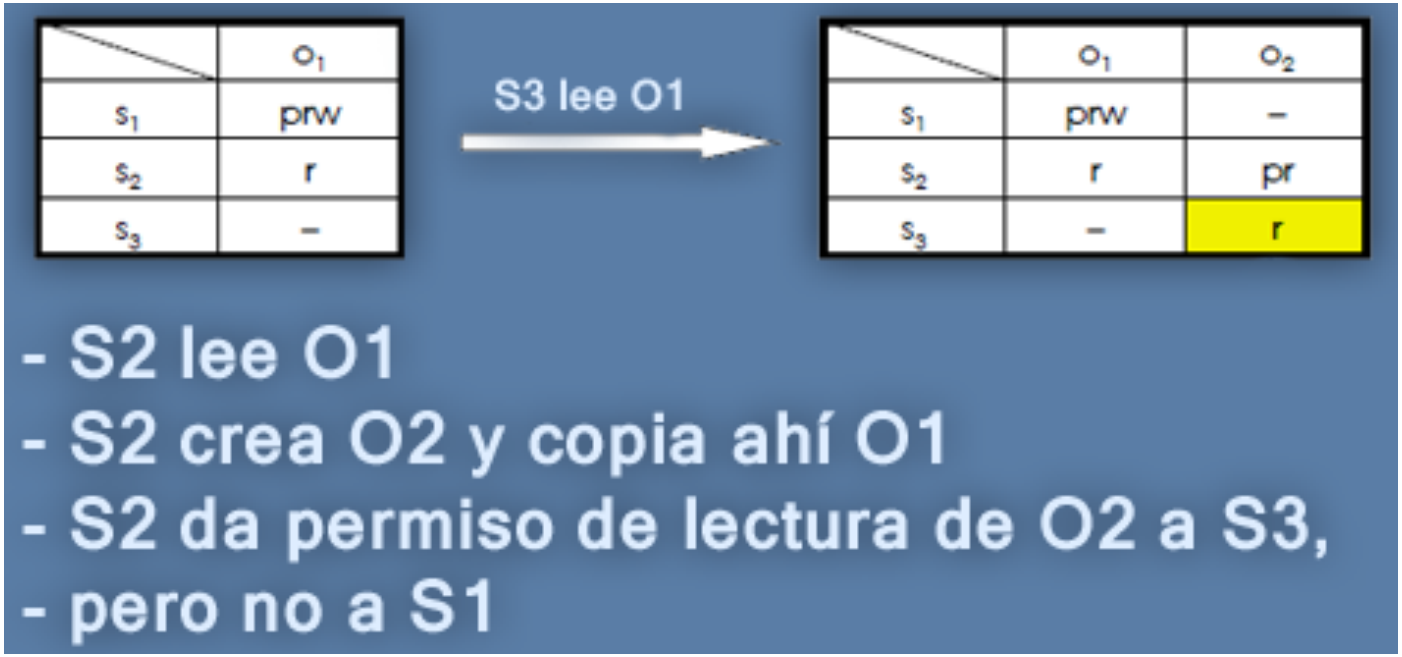
Control de acceso discrecional (DAC)

- El usuario que crea un objeto define la columna
- Es posible realizar una protección dinámica:
  - Dueño del objeto
  - Copy. Copiar una opearción de un Objeto A a un Objeto B
  - Control. El Dominio A puede modificar los derechos de un Domino B
  - Transfer. Es posible cambiar de Dominio

ACM incorpora 'p' (propietario) a las propiedades de acceso

	$Objeto_1$	$Objeto_2$	$Objeto_3$	...	$Objeto_M$
$Usuario_1$	prwx	rw	prwx	...	rw
$Usuario_2$	x	prwx	X	...	rw
$Usuario_3$		rw	rwx	...	pwr
...	...	...	...	...	...
$Usuario_N$	x	rw	x	...	w

Control de acceso discrecional (DAC). Caballo de troya

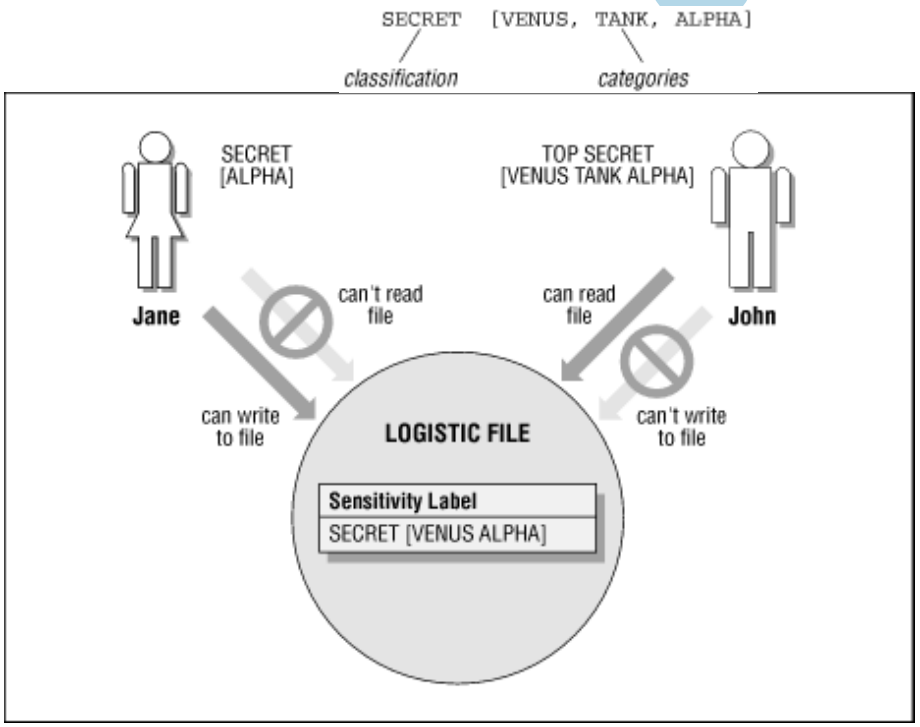


Mandatory access control MAC

- Lectura
  - Clasificación (sensitividad) mayor o igual a la propuesta
  - Contener todas las categorías

- Escritura
  - Categoria incluida en la del objeto
  - Clasificacion menor o igual

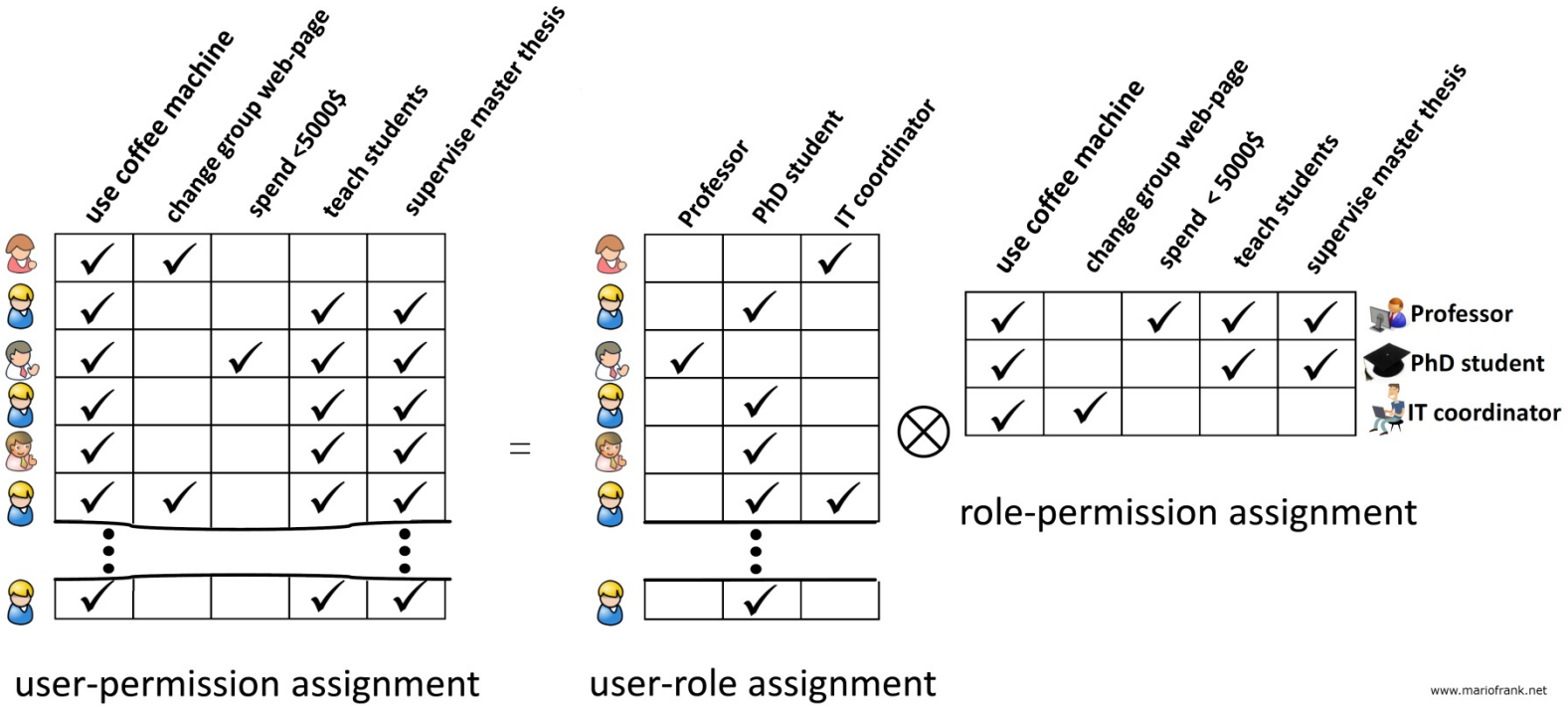
- Downgrade:
  - Si algo es top-secret no se puede
  - Copiar en unclassified



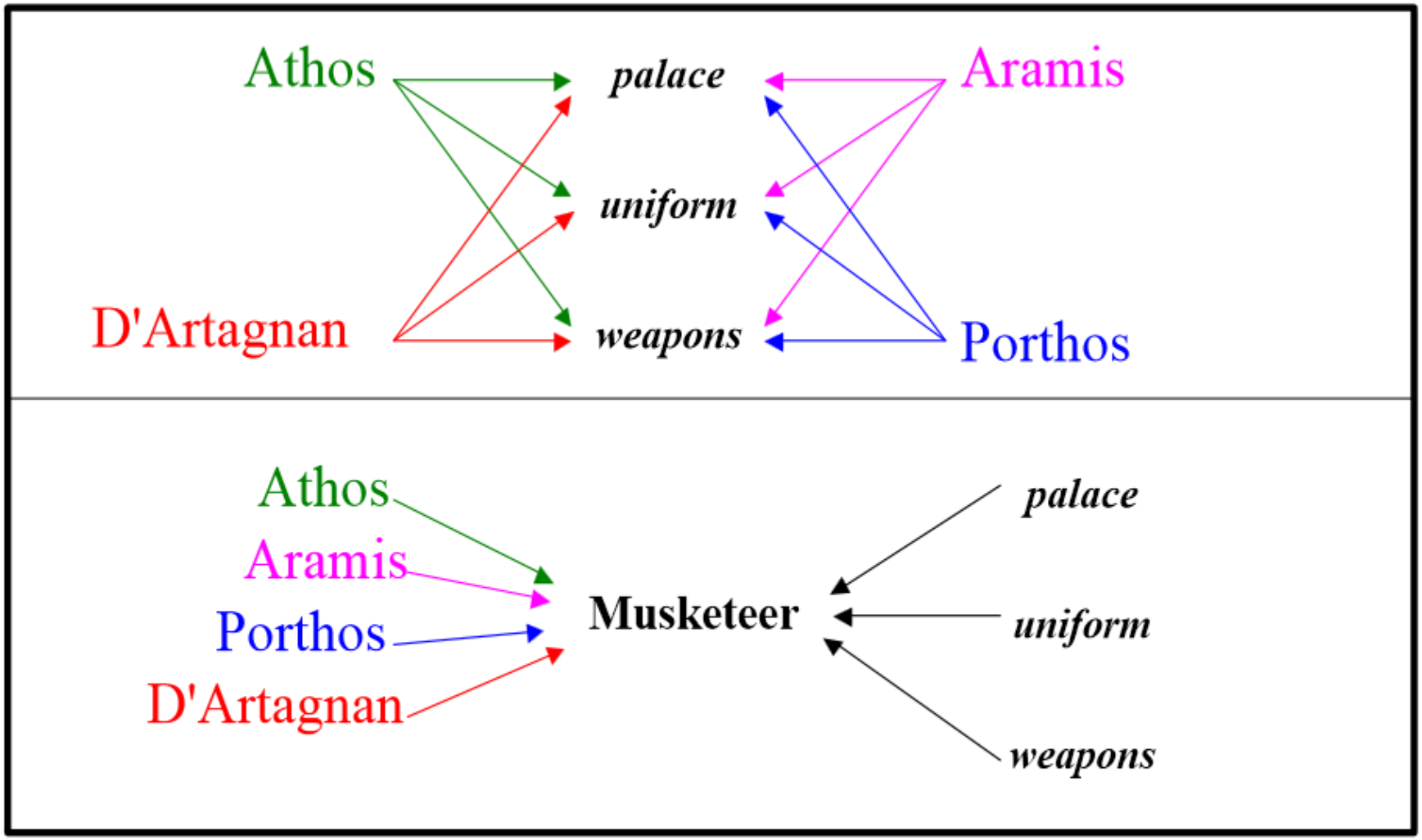
Role based authorization

- Todo empezó en 1990…Ferraiolo and Khun
- Un rol incluye unan serie de permisos
- Se asignan roles a los usuarios
- Reduce la complejidad y el coste de la administración de seguridad
- Se reducen el número de relaciones

Role based authorization



Role based authorization



Referencias

- http://ingenieriadelaseguridad.blogspot.com.es/p/control-de-accesos.html
- http://oreilly.com/catalog/csb/chapter/ch03.html