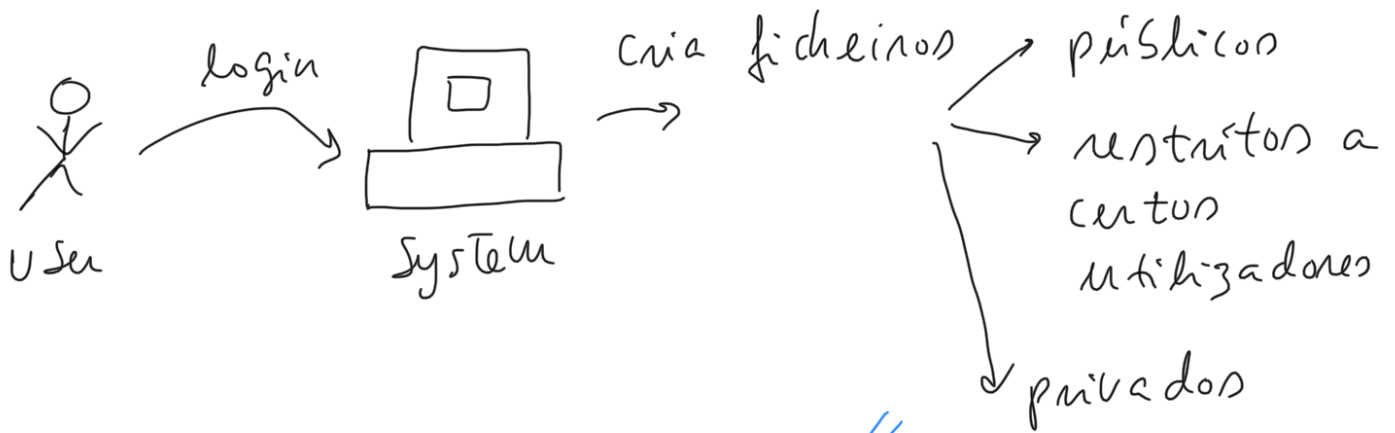


# Controlo de Acesso (Access Control) 1.



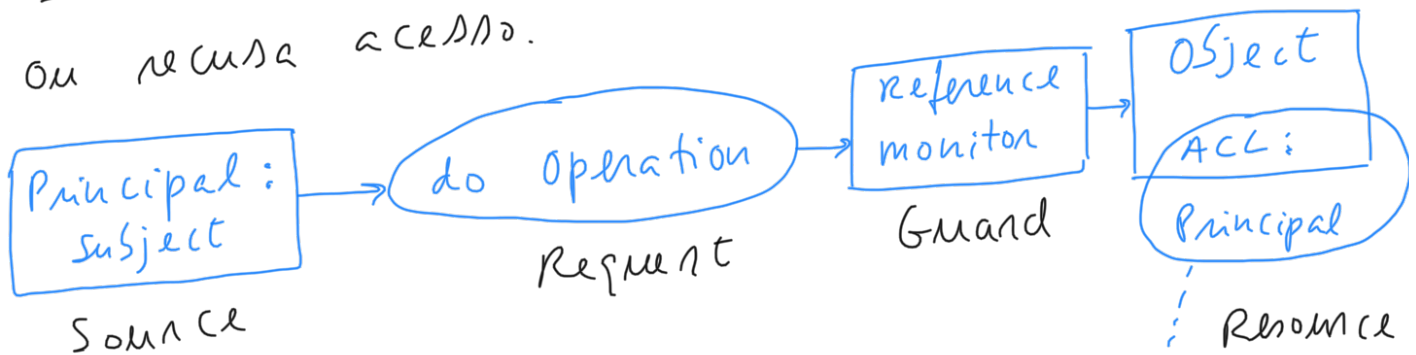
É necessária: 

- linguagem para exprimir política de controlo de acesso  
(access control policy)
- mecanismo para garantir controlo de acesso  
(enforce access control)

## Autenticação e Autorização

2

Controlo de acesso - uma entidade ativa, um subject ou principal, acede a um objeto passivo por meio duma operação de acesso, enquanto um reference monitor dá ou recusa acesso.



O controlo de acesso consiste em dois passos, autenticação e autorização.

↓  
O sistema tem que conhecer o principal/subject para permitir que este faça operações

↓  
O principal/subject tem que ter autorização para aceder a um objeto (recurso)

ACL - Access Control List  
de autorização a principal

Definição: "A Principal is an entity that can be granted access to objects or can make statements affecting access control decisions. A subject is an active entity within an IT System." 3.

Tipicamente: Principal → Utilizador / ID user  
entidade ligada Subject → Process / Thread  
Object → Recursos (e.g., memória, impressoras, ficheiros, directorias, nós na rede)

### Operações de Acesso

As políticas de controlo de acesso (acesso control policies - ACP) identificam aquilo que um dado Principal / Subject pode fazer

Ex: Representam operações de acesso  
- ler / escrever memória num sistema computacional  
- invocar métodos num sistema object-oriented  
- ler ficheiros / directorias num sistema operativo  
- etc.

## Administrative Access Rights

4.

No Unix, as ACP não expressam através de três operações:

|        | file              | diretório   |
|--------|-------------------|---|
| read   | ler ficheiro      | listar conteúdo diretório                         |
| write  | escrever ficheiro | criar/apagar ou renomear um ficheiro na diretório |
| execut | executar programa | procurar na diretório                             |

Ex: Para controlar quem pode criar/apagar ficheiros, basta controlar o acesso write na diretório onde está o ficheiro.

## Estruturas de Controlo de Acesso (Access Control Structures - ACS)

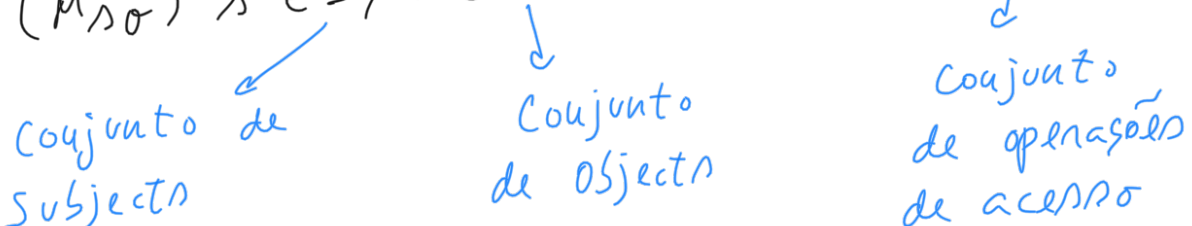
5.

↳ ACS ajudam a exprimir concretamente as ACP

### Access Control Matrix (ACM)

↳ Os access rights podem ser definidos individualmente para cada combinação de subject e object sob a forma de uma ACM:

$$M = (M_{\sigma\tau}) \quad \sigma \in S, \tau \in O \quad \text{com } M_{\sigma\tau} \subseteq A$$



conjunto de subjects      conjunto de objects      conjunto de operações de acesso

EX:

- bill.doc pode ser lido/escrito por Bill; Alice não tem nenhum acesso
- edit.exe pode ser executado por Alice e Bill, mas estes não têm outro acesso
- fun.com pode ser executado/lido por ambos mas apenas Bill pode escrever.

ACM:

| subject | bill.doc      | edit.exe  | fun.com                |
|---------|---------------|-----------|------------------------|
| Alice   | —             | {execute} | {execute, read}        |
| Bill    | {read, write} | {execute} | {execute, read, write} |

objects

- ACM não são práticas de implementar se o número de subjects e objetos for elevado, ou se os conjuntos de subjects e objetos mudam frequentemente.

## Capacidades (capabilities)

Existem duas formas de implementar uma

ACM:

- os access rights podem ficar junto com os subjects, ou junto com os objects

subject's capabilities

object's Access Control List

Alice's capability: edit.exe: execute; fun.com: execute, read;  
 Bill's capability: bill.doc: read, write;  
 edit.exe: execute; fun.com: execute, read, write;

Nota: Cada subject's capability  
corresponde à linha desse subject na  
ACM.

capabilities então tipicamente associadas  
com Discretionary Access Control

↓  
controle de acessos discricionário  
(ver adiante)

Vantagens:

- Facilidade na obtenção das permissões de um subject
- Ao eliminar um subject, eliminam-se todas as suas permissões
- em ambientes distribuídos, elimina a necessidade de múltiplas autenticações

Desvantagens:

- Para obter listas de acessos a objetos, obriga a pesquisar todos as capacidades (quem tem acesso a este objeto)



## Access Control Lists (ACL)

8.

Access Control Entries (ACEs)

- ACL para bill.doc: Bill: read, write;
- ACL para edit.exe: Alice: execute;  
Bill: execute;
- ACL para fun.com: Alice: execute, read;  
Bill: execute, read, write

↑  
coluna na ACM

### Vantagens:

- É fácil obter permissões associadas a um objeto
- Ao eliminar um objeto, eliminam-se todas as permissões associadas

### Desvantagens:

- Para saber todas as permissões dum subject, é necessário pesquisar todas as ACLs.

É comum colocar users em groups. P. ex., no Unix é possível indicar ACLs cada uma com três entradas, para indicar access rights a principais: user, group, others.



## Posse (ownership)

9.

No âmbito do controle de acesso, existem duas opções de declarar quem está encarregado de definir políticas de segurança:

- Política discricionária: definidas pelo dono (owner) do recurso; o dono decide quem pode aceder ao recurso (access control is at the discretion of the owner)  
(discrionary)
- Política mandatória: definidas por uma autoridade central (ex: sistema de defesa dum país)  
(mandatory)

Baseadas na  
identidade do sujeito

## Grupos e Permissões Negativas

10.

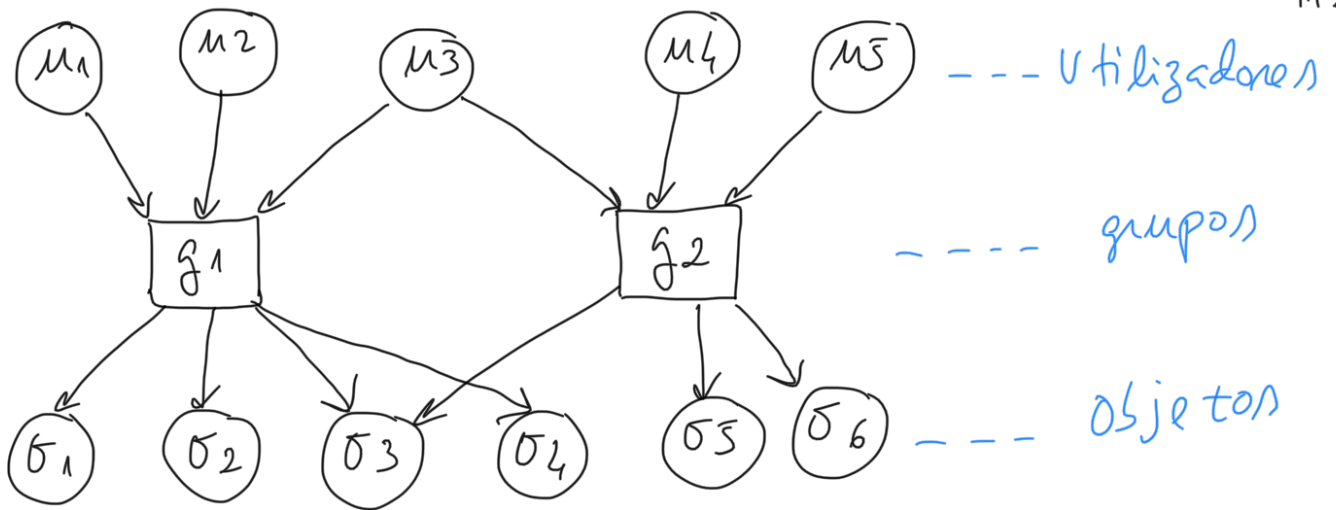
Os grupos (conjunto de utilizadores com direitos de acesso semelhantes) são uma forma de simplificar a definição de políticas de acesso de controle.

ex: um professor pretende dar acesso a material da disciplina aos seus estudantes.

OPÇÃO 1) Colocar estudantes individualmente numa ACL para cada material da disciplina

ou  
OPÇÃO 2) Colocar estudantes num grupo e colocar este grupo nas ACL de cada material da disciplina

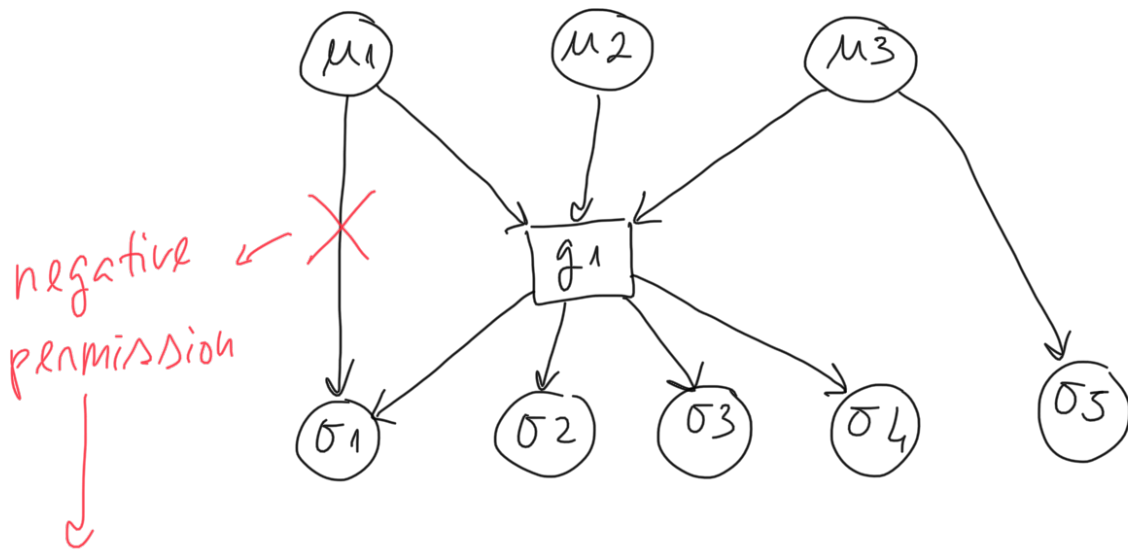
11.



As políticas de segurança podem ter exceções às regras gerais

ex: um utilizador deve ter acesso direto a um recurso (independentemente se pertence a um grupo), ou a um utilizador deve ser negado o acesso a um recurso embora pertença a um grupo que tem acesso a esse recurso.

negative permission



contradiz a permissão positiva dada ao grupo  $g^1 \Rightarrow$  policy conflict

$\Downarrow$   
resolvido pelo monitor de referências

Se as políticas forem definidas por ACLs, um algoritmo muito usado para resolver conflitos consiste em processar a ACL até ser encontrada uma entrada correspondente ao principal + acesso requerido. As restantes entradas em conflito são ignoradas.

Ex: windows ACL slide 13-14