Controlo de Acessos

Notas para a UC de “Segurança Informática”

Inverno de 10/11

Rui Joaquim (rjoaquim *em* cc.isel.ipl.pt)

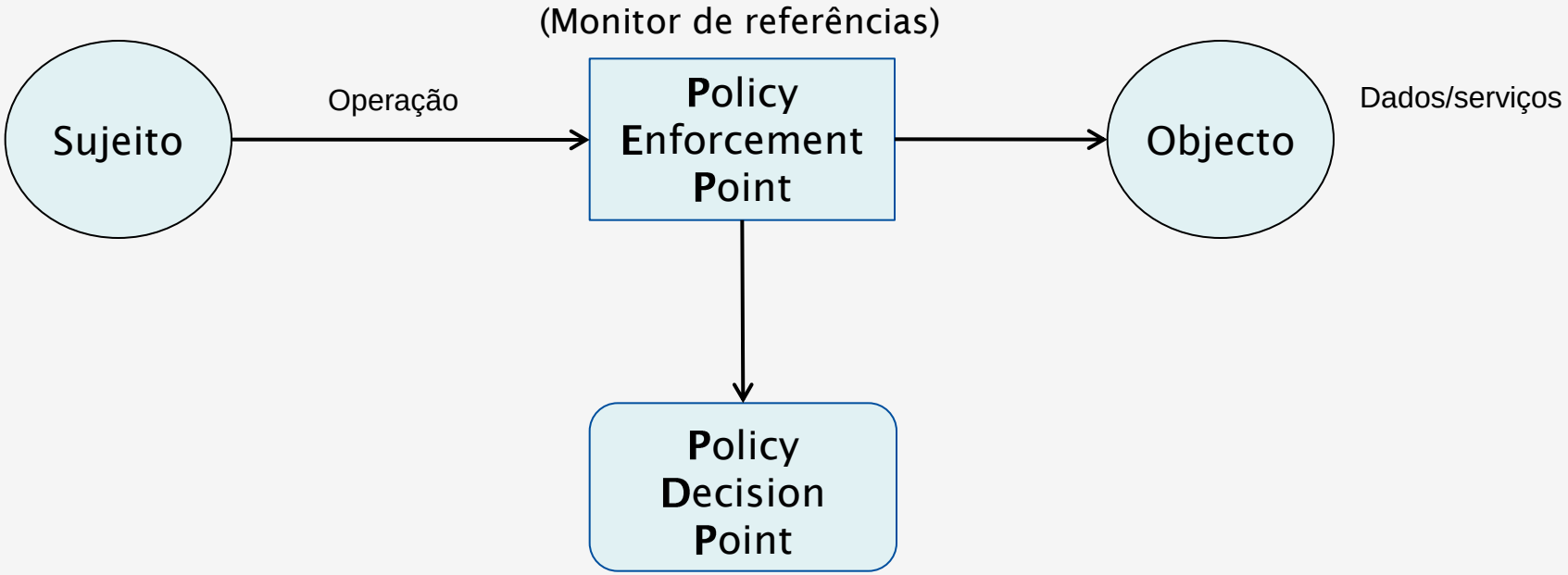
Instituto Superior de Engenharia de Lisboa

Introdução

- Controlo de acessos (autorização) é o processo de mediação de pedidos a recursos (objectos) mantidos pelo sistema, decidindo se o pedido é aceite ou não.

- Motivações:
  - Proteger o acesso a recursos (dados/serviços).
  - Garantir a integridade dos recursos.

Arquitectura base

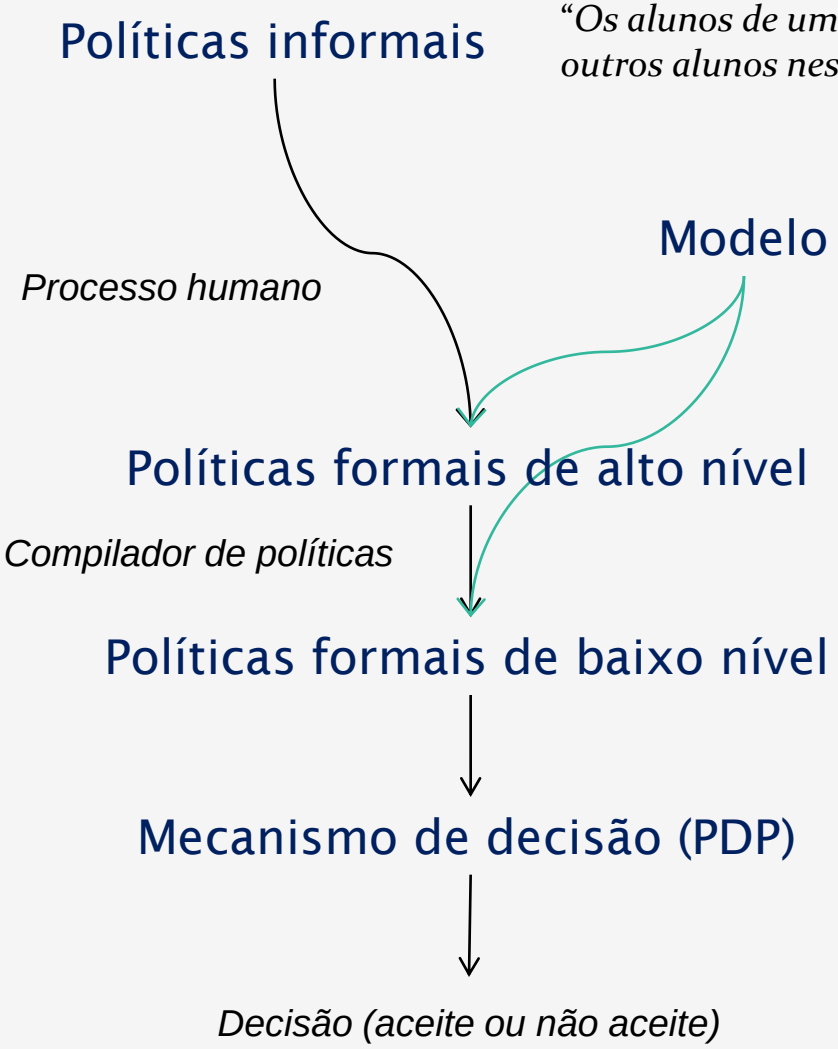


- Propriedades do PEP:
  - Não deve ser possível alterá-lo.
  - Não deve ser possível contorná-lo.
  - Deve ser pequeno e estar confinado ao núcleo de segurança do sistema por forma a facilitar a verificação da sua correcção.

Introdução II

- Componentes:
  - Politica de segurança: define as regras do controlo de acessos.
  - Modelo de segurança: formalização da forma de aplicação das políticas de segurança.
  - Mecanismos de segurança: funções de baixo nível (software/hardware) que dão suporte à implementação de modelos e políticas de segurança.

Políticas, modelos e mecanismos



Tipos de políticas de controlo de acessos

- Discricionárias: baseadas na identidade do sujeito e em regras que definem o que cada sujeito pode (ou não) fazer. Em geral, as regras são definidas pelo dono (*owner*) do recurso/objecto.

- Mandatórias: baseadas na identidade do sujeito e em regras que definem o que cada sujeito pode (ou não) fazer. As regras são definidas por uma autoridade central.

- Baseadas em papéis (*roles*): baseadas no papel que o utilizador possui no sistema e em regras que definem o que os utilizadores que pertencem a cada papel podem fazer.

- Uma política de controlo de acesso pode ter aspectos de vários tipos (exemplo: controlo de acesso no windows).

Matriz para controlo de acessos

Rui Joaquim
José Simão

Modelo Matriz de Acessos

- Matriz de acessos.
  - Define um triplo (*S,O,A*), onde:
    - *S* é o conjunto de sujeitos.
    - *O* é o conjunto de objectos.
    - *A é o conjunto de operações*
    - M_{SO} é a matriz de operações, onde as linhas representam os sujeitos, as colunas os objectos e cada entrada *M*[*s,o*] as permissões do sujeito *s* sobre o objecto *o*.

	File1	**File2**	**File3**	**Program1**
Alice	read write	read write		execute
Bob	read		read write	
Charlie		read		execute write

Proposta inicial por Lampson (Protection, In 5th Princeton Symposium Information Science and Systems, 1971)

Formalizado por Harrison, Ruzzo e Ullmann (Protection in Operating Systems, Communications of the ACM, 19(8), 1976

Implementação da matriz de acessos I

Tabela de autorização

Sujeito	Permissão	Objecto
Alice	read	File1
Alice	write	File1
Alice	read	File2
Alice	write	File2
Alice	execute	Program1
Bob	read	File1
Bob	write	File3
Bob	read	File3
Charlie	read	File2
Charlie	execute	Program1
Charlie	write	Program1

Implementação da matriz de acessos II

Capacidades:

- As permissões são guardadas junto dos sujeitos.
- A capacidade (*capability)* de cada sujeito corresponde à sua linha na matriz:
  - Alice *capability*: File1: read, write; File2: read, write; Program1: execute
  - Bob *capability*: File1: read; File3: read, write
  - Charlie *capability*: File2: read; Program1: execute, write

- Vantagens:
  - Facilidade na obtenção das permissões associadas a um sujeito.
  - Ao eliminar um sujeito elimina-se automaticamente todas as suas permissões.
  - Em ambientes distribuídos elimina a necessidade de múltiplas autenticações.

- Desvantagens:
  - Para saber quem tem acesso a um objecto é necessário pesquisar todas as capacidades.
  - Se a reutilização dos identificadores de objectos for possível é necessário, na eliminação de um objecto, eliminar todas das permissões sobre o mesmo de todas as capacidades no sistema.
  - A eliminação de capacidades pode ser problemática (especialmente no caso de politicas discricionárias)
  - Possibilidade de cópia e uso fraudulento.

Implementação da matriz de acessos III

Lista de controlo de acessos (ACL):

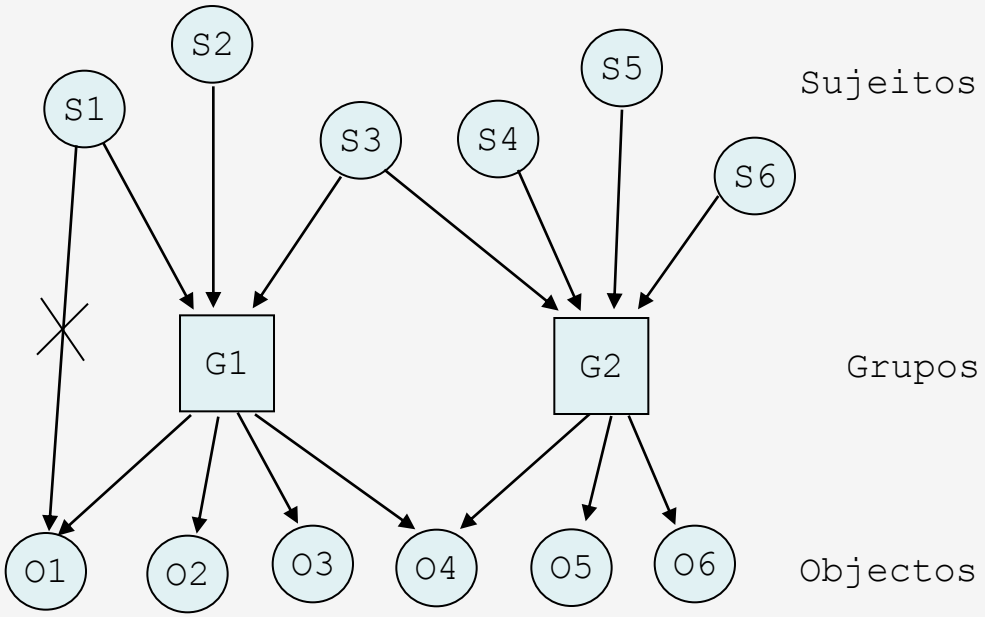
- As permissões são guardadas junto dos objectos.
- A ACL de cada objecto corresponde à sua coluna na matriz:
  - ACL para File1: Alice: read,write; Bob: read
  - ACL para File2: Alice: read, write; Charlie: read
  - ACL para File3: Bob: read, write
  - ACL para Program1: Alice: execute, Charlie: execute, write

- Vantagens:
  - Facilidade na obtenção das permissões associadas a um objecto.
  - Ao eliminar um objecto elimina-se todas as permissões a ele associadas.

- Desvantagens:
  - Para saber todas as permissões de um sujeito é necessário pesquisar todas as ACLs.
  - Se a reutilização dos identificadores de sujeitos for possível é necessário, na eliminação de um sujeito, eliminar todas das permissões do mesmo de todas as ACLs no sistema.

Permissões para grupos

- Motivação: facilitar a gestão de sujeitos, agrupando sujeitos com permissões semelhantes num grupo.
- Os grupos funcionam como uma camada intermédia na definição de controlos de acesso.
- Regra geral as permissões são associadas aos grupos e não individualmente aos sujeitos.
- A verificação de controlo de acesso passa a ser feita em função do sujeito ser membro ou não de um grupo.
- Pode ser necessário "afinar" as permissões de um determinado sujeito dentro de um grupo com permissões ou permissões negativas para esse sujeito em particular.
- Dependendo da política pode ser possível definir hierarquias de grupos, bem como atribuir um sujeito a mais que um grupo.
- Também é possível agrupar objectos?



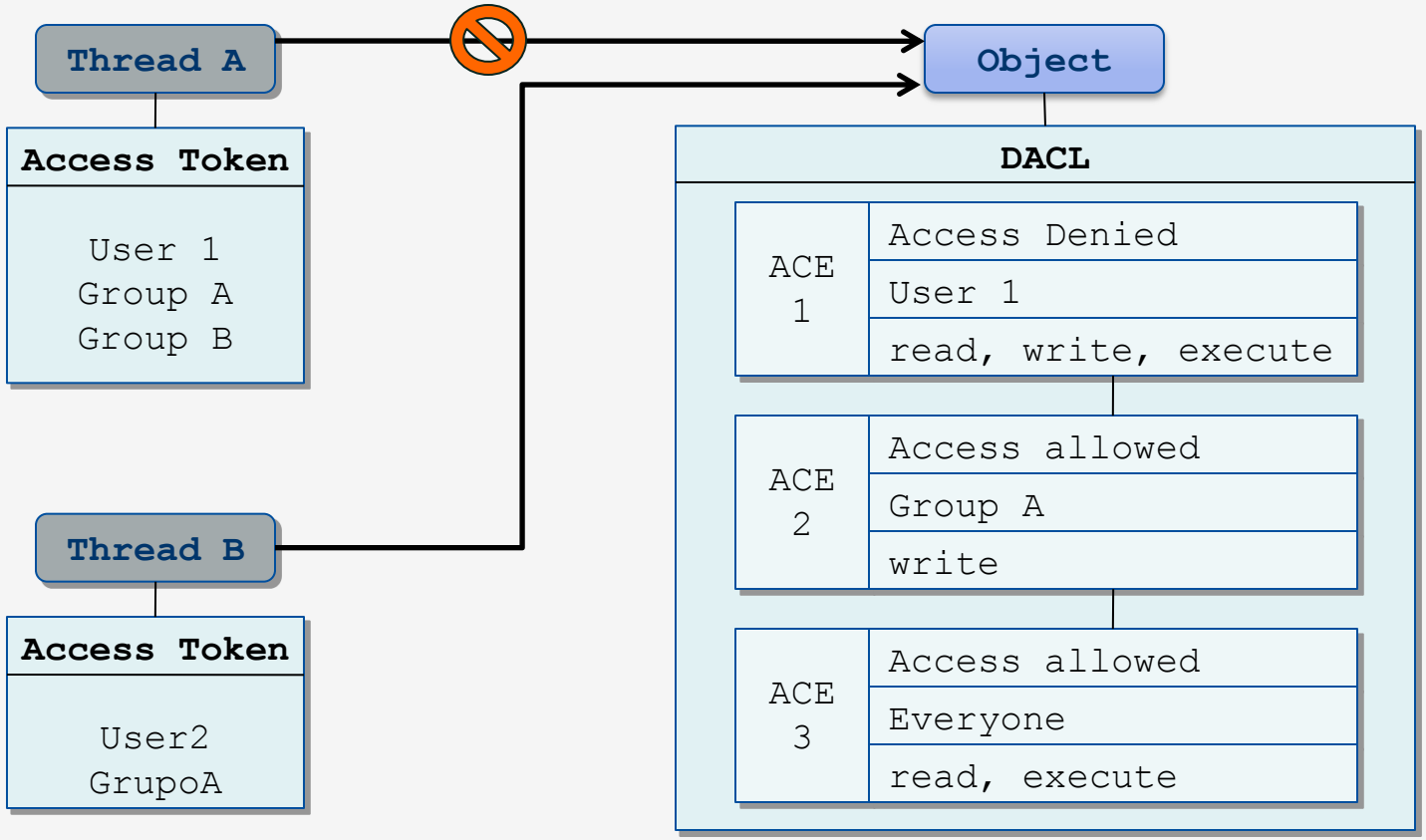
Caso prático: Componentes para controlo de acessos (Windows)

- Após *login* é atribuído ao utilizador um *access token*
  - Em cada *access token* estão presentes *security identifiers (SID)* com a identificação do utilizador e dos grupos a que pertence

- Após a criação de um objecto (recurso) é lhe associado um *security descriptor* com:
  - O SID do seu dono
  - Discretionary Access Control List (DACL)
  - System Access Control List (SACL) com a política do sistema para auditar o acesso ao objecto e o “nível de integridade” do mesmo

- Uma ACL é uma lista de Access Control Entry (ACE), onde consta:
  - SID (utilizador ou grupo), Permissão ou Negação, Acções

Controlo de acessos através de DACL



- Para determinar se o acesso é autorizado ou não, a DACL é percorrida até à negação de uma das acções ou permissão de todas as acções requeridas
- À cabeça ficam as ACE que negam