Role-Based Access Control (RBAC)

Além das políticas discricionárias e mandatórias, estas também podem ser role-based.

Sujeitos derivam os seus direitos de acesso a partir do papel (papéis) que têm.

Role (papel) - Coleção de procedimentos (procedures)

Os papéis são atribuídos a utilizadores

pode executar procedimentos associados ao role.

Procedimentos - métodos de controle de acesso de alto nível com semântica mais complexa que uma leitura / escrita. Podem ser aplicados a objetos dum dado tipo, ex: transferência de fundos entre duas contas.

↓

data type

Exemplo de RBAC

Um professor pode criar o role Student para estudantes da disciplina com permissão de leitura.

O role Teacher pode ser criado com permissão de edição do material da disciplina.

Role hierarchies – define relacionamento entre roles.

↓
ex: hierarquia

Um role sénior pode fazer tudo o que um role júnior faz.

ex: Teaching Assistant júnior role → pode editar material de exercícios.

Princípio de Privilégios Mínimos – Quando um utilizador faz login, o processo corrente deriva as permissões a partir dos roles do utilizador. O Princípio de Privilégios Mínimos sugere que apenas os roles necessários à tarefa em mãos sejam ativados.

Separation of Duties – Separação de Responsabilidades

O modelo RBAC Tem um nível (RBAC_2) em que é possível definir restrições. A separação de responsabilidades é um tipo de restrição.

Exemplos:

- Num Departamento de compras, a pessoa que aprova a compra ≠ pessoa que emitiu ordem de compra
- um administrador não pode exercer direitos de acesso sobre ele próprio

4 níveis incrementais do RBAC

cada nível inclui as características do nível anterior

- Flat RBAC (RBAC_0): utilizadores e permissões são atribuídos a papéis, utilizadores obtêm permissões se pertencerem a um papel
  ex: um sujeito pode ser um estudante (student) e ser também um Teaching Assistant.
- Hierarchical RBAC (RBAC_1): hierarquia de papéis
  ex: Teacher role é um senior role de Teaching Assistant

- Constrained RBAC (RBAC_2):
  adiciona suporte para políticas de separação de responsabilidades e restrições várias.
  ex: estudante não pode ter o role Teaching Assistant numa disciplina que está a frequentar.
- Symmetric RBAC (RBAC_3): adiciona suporte para revisões de permissões (permission-role reviews)
  ex: averiguar que papéis têm acesso de escrita ao material da disciplina

- Pode ser difícil de implementar em sistemas complexos e distribuídos.