Segurança

Josino Rodrigues Neto
josinon@gmail.com

Introdução

- O subsistema de segurança é responsável por proteger o BD contra o acesso não autorizado.
- Formas de acesso não autorizado:
  - leitura não autorizada
  - modificação não autorizada
  - destruição não autorizada

Introdução

- O DBA tem plenos poderes para dar e revogar privilégios a usuários.
- *Segurança em SGBD*, também chamada *Autorização*, diz respeito a um conjunto de regras e mecanismos de proteção de acesso a um banco de dados.

Introdução

- A segurança em banco de dados pode ser classificada em duas categorias:
  - **Segurança de sistema:**
    Cobre o acesso e o uso do banco de dados no nível de sistema, como por exemplo, nome de usuário e senha.
  - **Segurança de banco de dados:**
    Cobre o acesso e o uso dos objetos de banco de dados e as ações que esses usuários possam ter sobre os objetos.

Segurança de Acesso

- Além do procedimento clássico de segurança dos Sistemas Operacionais baseado em Identificação (Login) + Autenticação (Password), *os* SGBD's oferecem segurança em dois níveis:
  - Tabelas
  - Visão

Regras de Autorização

- Expressam os mecanismos de autorização em relações e visões
- São compiladas e armazenadas no dicionário de dados
- São expressas em linguagem de alto nível (Ex. SQL)
  - Formas de autorização:
    - autorização de leitura (select)
    - autorização de inserção (insert)
    - autorização de atualização (update)
    - autorização de remoção (delete)

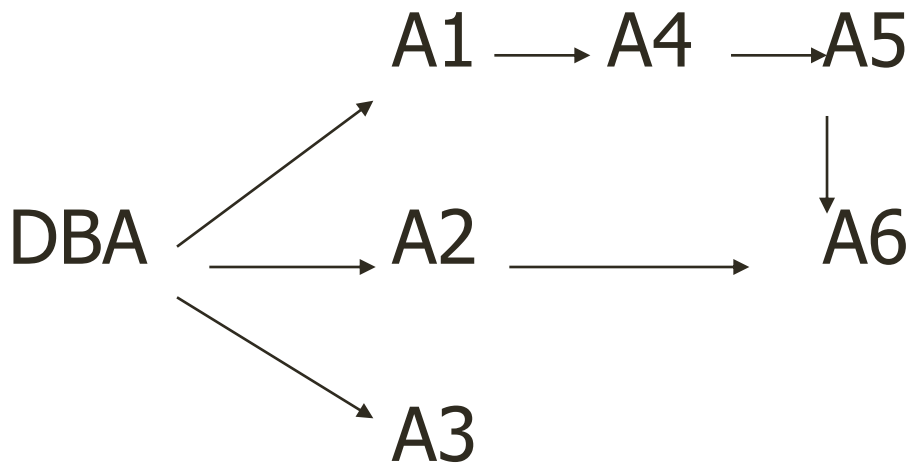
Regras de Autorização

- O DBA fornece ou revoga as autorizações de leitura, inserção, atualização e remoção aos usuários nas diversas tabelas/visões, e estes podem repassá-los caso receba autorização para tal.

- É criado um grafo de concessão de autorização, cujo nodo inicial é o DBA.

Grafo de Concessão

- Exemplo:



- Este grafo representa, por exemplo, que o DBA concedeu acesso a A2, que por sua vez, concedeu acesso à A6

Grafo de Concessão

- E se o DBA revogar o privilégio de A3 ?
- E se o DBA revogar o privilégio de A2 ?
- E se o DBA revogar o privilégio de A1 ?

Regras de Autorização

- **Um modelo de segurança**
  - O Administrador de Banco de Dados (DBA) cadastra os usuários.
    - usuário-id, grupo-id, grupo-id/usuário-id
  - O usuário não possui privilégios nesse ponto.

Regras de Autorização

- **Privilégios a nível de banco de dados**

Privilégio-BD ::= **GRANT** privilégio **TO**
lista-de-usuários

lista-de-usuários ::= **PUBLIC** | grupo-id |
lista-de-usuários-id

- **GRANT** - comando que tem o propósito de ceder privilégios aos usuários.

Regras de Autorização

- privilégios-em-tabela ::=

  GRANT privilégios ON tabela TO

  lista-de-usuários [WITH GRANT OPTION]

privilégios ::= ALL [PRIVILEGES] | lista-de-operações

operação ::= SELECT | INSERT | DELETE | UPDATE [(lista-de-colunas)]

Regras de Autorização

- REVOKE
  - Revoga autorização de privilégios
  - Se o usuário A tiver concedido o privilégio P para o usuário B, então A poderá, posteriormente, revogar o privilégio P de B, através do comando REVOKE
- Sintaxe:
- REVOKE <privilégios>

  ON <relação/visão> FROM <usuários>

Regras de Autorização

- Exemplo:
  - REVOKE delete ON projeto FROM Marta, Ana
  - REVOKE update ON Empregado FROM Ana

Referência

- **Livro Elmasri/Navathe (4ª Edição)**
  - Aspectos de segurança **(Cap.23)**