UNIVERSIDADE FEDERAL DE ITAJUBÁ

Banco de Dados II

COM 231

Controle de Acesso

Vanessa Cristina Oliveira de Souza

Segurança

- Os dados armazenados no banco de dados precisam ser protegidos contra:
  - acessos não-autorizados
  - destruição ou alteração intencional
  - introdução ou alteração de inconsistência

Ameaças aos bancos de dados

- Perda de Integridade
  - A integridade é perdida se mudanças não autorizadas forem feitas nos dados por atos intencionais ou acidentais.
- Perda de Disponibilidade
  - Se um usuário ou um programa perde o acesso aos dados.
- Perda de Confidencialidade
  - A exposição não autorizada de um dado pode resultar em perda de confiança pública, constrangimento ou ação legal contra a organização mantenedora dos dados.

Ameaças aos bancos de dados

Segurança e informação são valores inseparáveis em computação!

Segurança X Integridade

- Segurança
  - Refere-se a segurança contra acessos maldosos.
    - Autorização
    - Visões
- Integridade
  - Refere-se ao ato de evitar a perda acidental de consistência.
    - Integridade referencial
    - Escalonamentos
    - Transações
    - Recuperação

Violações de Integridade

- Quebras durante o processamento de transações.
- Anomalias causadas por acesso concorrente ao banco de dados.
- Anomalias causadas pela distribuição de dados sobre diversos computadores.
- Um erro lógico que viola a suposição de que as transações preservam as restrições de consistência do banco de dados.

Violações de Segurança

- Leitura não-autorizada de dados (roubo de informação).
- Modificação não-autorizada de dados.
- Destruição não-autorizada de dados.

Medidas de Segurança

- A fim de proteger o banco de dados, medidas de segurança precisam ser tomadas em diversos níveis:
  - Físico
  - Humano
  - Sistema Operacional
  - Sistema de Banco de Dados
- A segurança de todos os níveis precisa ser mantida a fim de garantir a segurança do banco de dados.
- Uma fraqueza a um nível baixo de segurança (físico ou humano) permite contornar-se medidas de segurança de alto nível (banco de dados).

Medidas de Segurança

- Nível Físico
  - O local ou locais onde os sistemas de computador estão localizados precisam estar fisicamente protegidos contra assaltos ou intrusos.

Medidas de Segurança

- Bom fornecimento de energia
  - Instalação elétrica dedicada e balanceada;
  - No-breaks redundantes com carga compatível e bateria não vencida;
  - Geradores com carga compatível;
- Bom acondicionamento
  - Ar condicionado suficiente e redundante;
  - Boa acomodação (racks), bons gabinetes;
  - Segurança contra incêndio e desastres naturais;
- Equipe
  - Monitoramento constante dos sistemas;
- Backup

Medidas de Segurança

- Nível Humano
  - Os usuários devem ser cautelosamente autorizados para reduzir a chance de qualquer usuário dar acesso a um intruso em troca de suborno ou outros favores.

Medidas de Segurança

- Nível de Sistema Operacional
  - A fraqueza na segurança do sistema operacional pode servir como um meio para acesso não-autorizado ao banco de dados.
  - Uma vez que quase todos os sistemas de banco de dados permitem o acesso remoto através de terminais ou redes, a segurança no nível do *software* dentro do sistema operacional é tão importante quanto no nível físico.

Medidas de Segurança

- Nível de Sistema de Banco de Dados
  - Alguns usuários de banco de dados podem estar autorizados a fazer o acesso apenas a uma porção limitada do banco de dados.
  - A outros usuários pode ser permitida a formulação de consultas, mas proibida a modificação de dados.
  - É responsabilidade do sistema de banco de dados assegurar que essas restrições não sejam violadas.

UNIVERSIDADE FEDERAL DE ITAJUBÁ

Criação de Usuários

Usuários

- Todo **agrupamento de bancos de dados** possui um **conjunto de usuários** de banco de dados.

- Existem cinco tipos de usuários de banco de dados, segundo o modo como o qual interagem com o sistema:
  - DBA
  - Programadores de aplicativos
  - Usuários de alto nível
  - Usuários especializados
  - Usuários ingênuos

Criação de Usuários

- Para criar um usuário deve ser utilizado o comando SQL CREATE USER:

CREATE USER nome_do_usuário;

- Cria um usuário sem senha:

CREATE USER ‘nome_do_usuário’ WITH PASSWORD ‘senha’;

- Cria um usuário com senha:

Criação de Usuários

- Os usuários criados não possuem nenhum privilégio no banco. Apenas podem conectar no servidor.
  - Exceto superusuários

UNIVERSIDADE FEDERAL DE ITAJUBÁ

Concessão de Privilégios

Autorização de Acesso aos Dados

- Um usuário pode ter diversas formas de autorização a partes do banco de dados:
  - Autorização leitura
  - Autorização inserção
  - Autorização atualização
  - Autorização eliminação

- Todas, nenhuma ou uma combinação desses tipos de autorização pode ser concedida a um usuário.

Autorização de Esquema

- Além da autorização de acesso aos dados, pode ser concedidas autorizações para modificar o esquema do banco de dados:
  - Autorização índice
  - Autorização recursos
  - Autorização alteração
  - Autorização remoção

- Todas, nenhuma ou uma combinação desses tipos de autorização pode ser concedida a um usuário.

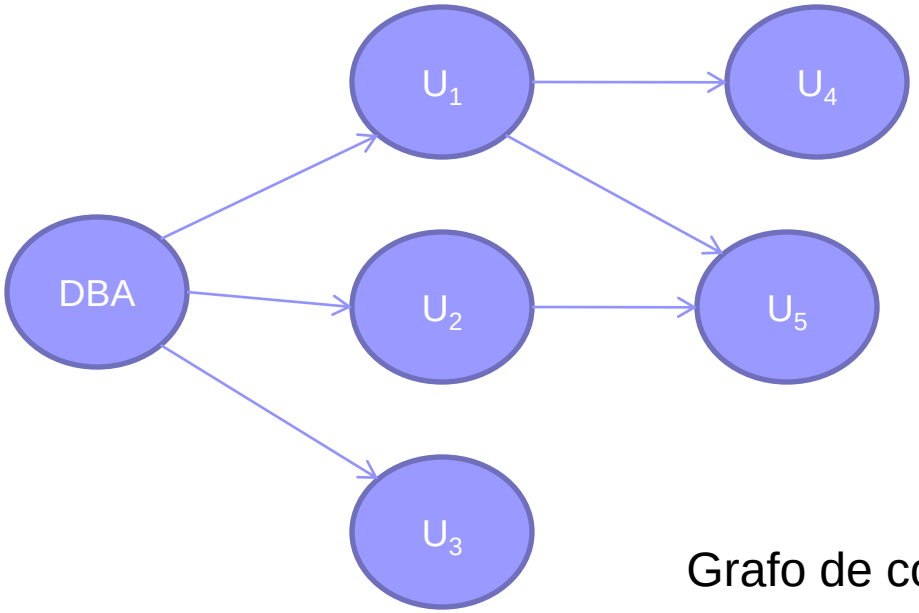
Concessão de Autorização

- Um usuário que tem concedida alguma forma de autoridade pode passar esta autoridade para outros usuários.

- Cuidados precisam ser tomados para assegurar que tal autorização possa ser revogada em momento futuro por quem a concedeu.

Concessão de Autorização

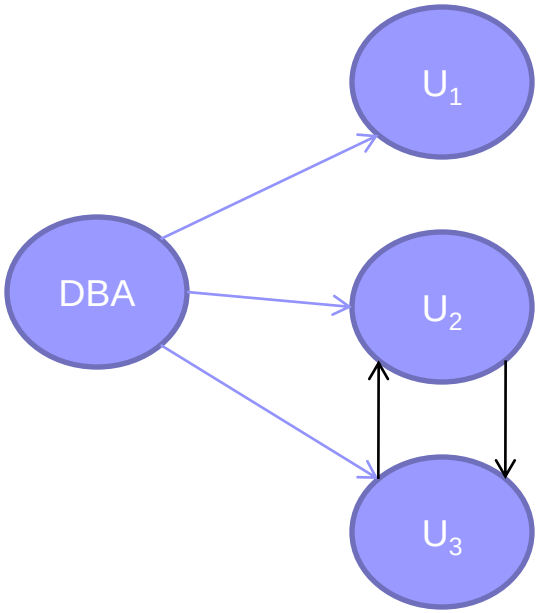
- Um usuário que tem concedida alguma forma de autoridade pode passar esta autoridade para outros usuários.



Grafo de concessão de autorização

Forma de burlar uma revogação de autorização

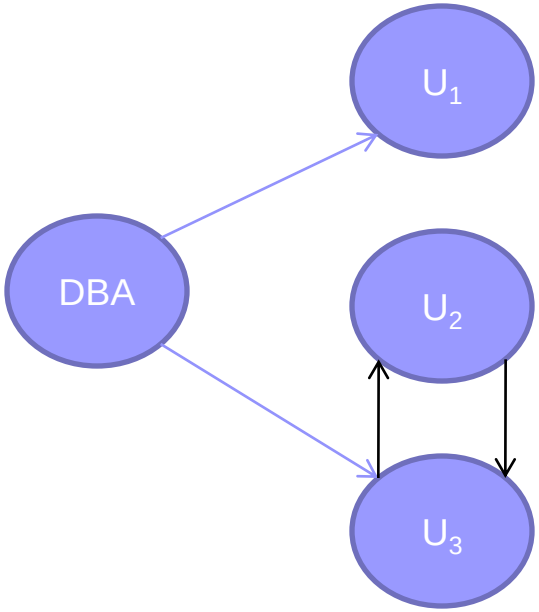
- O DBA concede autorização para os usuário 1, 2 e 3.
- O usuário 2 repassa seus direitos para o usuário 3.
- O usuário 3 repassa seus direitos para o usuário 2.



Grafo de concessão de autorização

Forma de burlar uma revogação de autorização

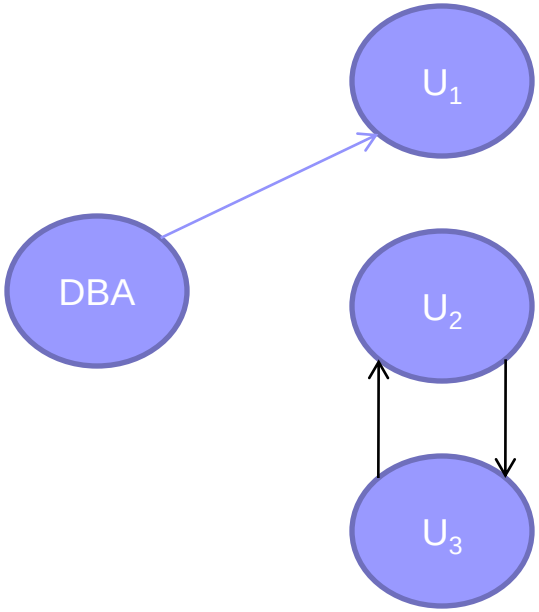
- O DBA revoga autorização para os usuário 2.
- O usuário 2 continua tendo os direitos concedidos pelo usuário 3.



Grafo de concessão de autorização

Forma de burlar uma revogação de autorização

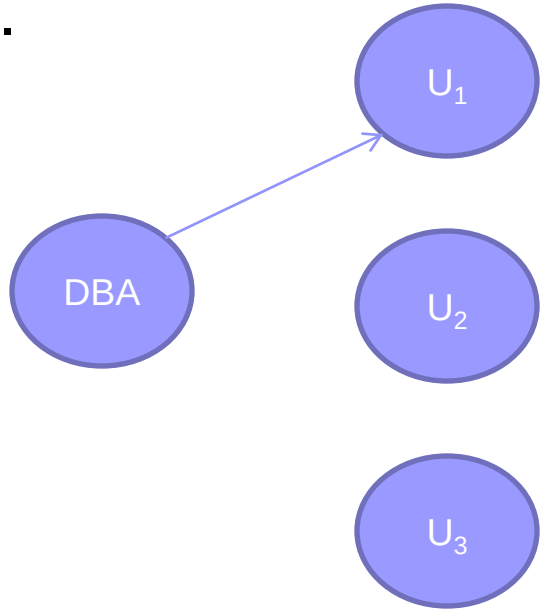
- O DBA revoga autorização para os usuário 3.
- O usuário 3 continua tendo os direitos concedidos pelo usuário 2.



Grado de concessão de autorização

Forma de burlar uma revogação de autorização

- Para evitar problemas como esse, requere-se que todas as arestas num grafo de autorização sejam parte de algum caminho originado no administrador do banco de dados.



Grafo de concessão de autorização

UNIVERSIDADE FEDERAL DE ITAJUBÁ

Concessão de Privilégios

O Comando GRANT

- O comando GRANT permite aos administradores do sistema criar usuários e conceder direitos aos usuários.

O Comando GRANT

- Existem quatro níveis de privilégios:
  - Nível Global
    - Aplicam privilégios para todos os bancos de dados em um determinado servidor.
  - Nível de Banco de Dados
    - Privilégios de bancos de dados aplicam-se a todas as tabelas em um determinado banco de dados.

O Comando GRANT

- Existem quatro níveis de privilégios:
  - Nível de Tabela
    - Privilégios de tabelas aplicam-se a todas as colunas em uma determinada tabela.
  - Nível de Coluna
    - Privilégios de colunas aplicam-se a uma única coluna em uma determinada tabela.

Exemplos Comando GRANT

- Nível de Banco de Dados

```
GRANT ALL ON DATABASE northwind TO vanessa;
```

  - CREATE, CONNECT and TEMPORARY

- Nível de Schema

```
GRANT ALL ON SCHEMA northwind TO vanessa;
```

- Nível de Tabelas

```
GRANT ALL ON TABLE northwind.customers TO vanessa;
GRANT SELECT(firstname) ON northwind.employees TO vanessa;
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA northwind TO vanessa;
```

Exemplos Comando GRANT

- Nível de Colunas

```
GRANT SELECT (col1), UPDATE (col1) ON mytable TO miriam_rw;
```

Sintaxe do Comando GRANT

GRANT <privilégios (colunas)>

ON <item>

TO <usuário>

(WITH GRANT OPTION)

- Se especificado, o usuário pode conceder seus privilégios a outros usuários.

O comando REVOKE

- O comando REVOKE permite aos administradores do sistema remover usuários e privilégios

Sintaxe do comando REVOKE

REVOKE <privilégios (colunas)>

ON item

FROM usuario

Exemplos Comando REVOKE

- **Privilégios a nível de Coluna.**

- Remover todos os privilégios do usuário “someuser” sobre a tabela “minhaTabela” do banco “MeuBanco”;

  - REVOKE ALL ON meuBanco.minhaTabela FROM someuser;

Exemplos Comando REVOKE

- REVOKE ALL ON DATABASE northwind FROM vanessa;

View + Grant

View x Grant

- O Grant garante um corte vertical na tabela, permitindo ao usuário manipular, no mínimo, uma coluna de uma tabela.

- Para permitir que um usuário tenha apenas acesso a um conjunto específico de registros, é preciso combinar a view com o grant.
  - Cria-se uma view
  - Concede ao usuário acesso apenas àquela view

View x Grant

- Exemplo:
  - Crie um novo grupo de usuários chamado ‘vendedoresMexico’;
  - Dê permissão de schema para esse grupo
  - Crie uma view chamada mexico sobre a tabela northwind.customers, filtrando por país (country like ‘Mexico’)
  - Dê permissão de select, insert, update e delete para o grupo vendedoresMexico sobre a view criada.
  - Crie o usuário vendedor1
  - Teste os privilégios para o vendedor1

Coisas importantes!

- Não confunda Integridade com Segurança!
- Usuários de aplicação não devem ser usuários de banco!!!!
- A definição dos usuários do banco e seus respectivos privilégios deve estar presente na documentação do banco

Segurança a nível de SGBD

1
- Criação de Usuários
- Quem? Perfil? PQ?
- Senha

2
- Autenticação
- Local/ Host
- Método de autenticação

3
- Concessão de Privilégios
- Quem? Perfil? PQ?
- Sem *Grant Option*

Para Casa

- Ler os itens 23.1, 23.2 e 23.3 do Elmasri e Navathe – 4ª Edição