ASPECTOS OPERACIONAIS

SEGURANÇA

Segurança

- Aspectos a serem considerados
  - Éticos e legais relacionados ao direito de acesso a certas informações
  - Políticos, a nível governamental, institucional ou corporativo, relativo às informações que não devem estar publicamente disponíveis
  - Relativos ao sistema tais como os níveis nos quais as funções de segurança devem ser manipuladas
  - A necessidade, em algumas organizações, de identificar vários níveis de segurança e categorizar os dados e os usuários de acordo

    → Sub-sistema de Segurança e Autorização no SGBD

Segurança

- Dois tipos de mecanismos de segurança
  - Mecanismo Arbitrário

    Usado para dar privilégios a usuários para acessar arquivos, registros ou campos de dados
  - Mecanismo Obrigatório

    Usado para garantir a segurança classificando dados e usuários nas diversas classes de segurança
- Prevenir contra pessoas não autorizadas

Controle de acesso

Segurança

- Segurança em BD Estatísticos

  Deve garantir que informações individuais não possam ser acessadas
- Dados Encriptados

  Usados para proteger dados sensíveis que estão sendo transmitidos via rede ou para prover proteção adicional a partes do BD

↓

Codificado por algum tipo de algoritmo

Segurança no BD e o DBA

- Responsabilidades do DBA
  - Dar privilégios a usuários
  - Classificar usuários e dados de acordo com a política da organização

    Conta privilegiada (root, super-usuário)
- Ações do DBA
  - Abrir contas

    Conta e password permitindo o acesso ao SGBD
  - Atribuir privilégios

    Atribuir certos privilégios a certas contas

Segurança no BD e o DBA

- Ações do DBA (Cont.)
  - Retirar privilégios

    Cancelar privilégios atribuídos anteriormente
  - Definir níveis de segurança

    Define as contas do usuário nos níveis de segurança apropriado

Responsável pela Segurança Geral do Sistema de BD

Acesso

- Proteção de acesso

  Número de conta e password são verificados quando do login
- Controle de login

  Seqüência de operações feitas por um dado usuário - do login ao logout

  ↓
- Modificar o arquivo de log

  Incluir a identificação da conta do usuário e a identificação do terminal onde está logado

  Qualquer Problema → AUDITORIA DO BD

Controle de Acesso Arbitrário

- Baseado em Privilégios

  Considerar o contexto relacional
- Método Típico
  - ➪ Dar (GRANT)
  - ➪ Retirar (REVOKE)

  } PRIVILÉGIOS
- A nível de Conta

  Privilégios particulares de uma conta independente das relações do BD
  - ➪ Privilégios
    - ➙ Criar esquemas ou tabelas
    - ➙ Criar visão

Controle de Acesso Arbitrário

- ➪ Privilégios (Cont.)
  - ➙ Alterar tabelas ou atributos
  - ➙ Remover tabelas ou visões
  - ➙ Modificar tuplas
  - ➙ Acessar o BD (SELECT)
- A nível de Relação

  Controle de acesso a cada relação em particular ou visão do BD
  - ➪ Para controlar o acesso à relação (ou visão), é criada uma conta associada a cada uma

  Conta do Proprietário ➡ Dá privilégio de acesso à relação

Controle de Acesso Arbitrário

- Em SQL temos os seguintes privilégios para uma relação R
  - ➪ SELECT - privilégio de acesso
  - ➪ MODIFY - capacidade de modificar tuplas em R
  - ➪ REFERENCES - capacidade de referenciar a relação R quando especificando restrições de integridade
- Para criar uma visão, a conta deve ter o privilégio SELECT em todas as relações envolvidas na definição da visão

Controle de Acesso Arbitrário

- Especificando autorizações através de visões

  Mecanismo de autorização importante por permitir o acesso à parte (sub-conjunto de atributos ou tuplas) de uma relação
  - ➪ Ex.:
    - ❶ A é proprietário da relação R
    - ❷ A cria uma visão V com alguns atributos de R
    - ❸ A dá a B o privilégio SELECT em V
- Retirando privilégios

  Em alguns casos é desejável dar privilégios temporariamente (ex.: uma dada tarefa). Um mecanismo de REVOKE privilégios é necessário

Controle de Acesso Arbitrário

- Propagação de privilégios

  Quando se dá privilégios a uma conta, pode-se dar ou não a ela a opção de dar privilégios a outras, através da

  GRANT OPTION

  ↓
  - ➪ Propagação de privilégios sem o conhecimento do proprietário
  - ➪ Se o privilégio da primeira conta for retirado, todas as outras também serão automaticamente retiradas

Controle de Acesso Arbitrário

- Técnicas para limitar a propagação de privilégios
  - Propagação horizontal

    Limitada a i significa que uma conta à qual foi dado o privilégio com GRANT OPTION pode dar privilégios a no máximo i outras contas
  - Propagação vertical

    Associada a j significa que uma conta tem o privilégio GRANT OPTION mas só pode dar privilégios a outras contas com propagação vertical < j

Controle de Acesso Arbitrário

- Exemplos
  - grant createtab to A1;

    Dá a A1 a capacidade de criar novas tabelas no BD
  - create schema Example authorization A1;

    A1 só está autorizado a criar tabelas em Example
  - Supor que A1 criou as tabelas

    EMPREGADO(nome, id, data_nasc, end, sexo, salário, num_dep)

    DEPARTAMENTO(num_depto, nome, id_gerente)

Controle de Acesso Arbitrário

- A1 é o proprietário e portanto pode dar privilégios nessas tabelas
  - grant insert, delete on EMPREGADO, DEPARTAMENTO to A2;

    A2 não pode dar privilégios a outras contas
  - grant select on EMPREGADO, DEPARTAMENTO to A3 with grant option;

    A3 pode dar privilégios a outras contas
    - grant select on EMPREGADO to A4;
  - revoke select on EMPREGADO from A3;

    Automaticamente o privilégio de A4 é retirado

Controle de Acesso Arbitrário

- create view A3EMPREGADO as select nome, data_nasc, end from EMPREGADO where num_dep=5;

  É criada uma visão de EMPREGADO para A3
  - grant select on A3EMPREGADO to A3 with grant option;

    É dado privilégio a A3 com propagação
  - grant uptade on EMPREGADO(salário) to A4;

    É dado privilégio a A4 de atualizar apenas salário

Controle de Acesso Arbitrário

- É possível para uma conta receber um certo privilégio de duas ou mais fontes, só perdendo o privilégio quando todas o retirarem

Controle de Acesso Obrigatório

- Baseado em Segurança Multinível

Mecanismo de segurança que classifica dados e usuários baseado em classes de segurança

- Pouco utilizado em SGBDs comerciais

Controle de Acesso Obrigatório

- Classes de segurança usuais
  - Muito secreta (TS)
  - Secreta (S)
  - Confidencial (C)
  - Não classificada (U)

  Onde TS > S > C > U
- Noções de segurança multinível no relacional
  - A cada atributo é associado um atributo de classificação e cada valor de atributo com sua classificação de segurança correspondente

Controle de Acesso Obrigatório

- A cada tupla é adicionado um atributo de classificação de tuplas para classificar a tupla como um todo

  R(A1, C1, A2, C2, ..., An, Cn, TC)

NOME	SALÁRIO	PERFORMANCE	TC
Smith U	4000 C	Fraco	S S
Brown C	8000 S	Bom	C S

Controle de Acesso Obrigatório

- Chave Aparente

  Equivalente à chave primária
- Filtragem

  Armazenar tuplas com nível de classificação maior e produzir tuplas correspondentes com nível menor
- Poli-instanciação

  Armazenar duas ou mais tuplas em diferentes níveis de classificação com a mesma chave