

Introdução a questões de segurança de banco de dados

Tipos de segurança

- A segurança do banco de dados tenta resolver muitos problemas, incluindo os seguintes:
 - Diversas questões legais e éticas com relação ao direito de acessar certas informações.
 - Questões políticas quanto aos tipos de informações que não devem se tornar públicas.
 - Questões relacionadas ao sistema, como **níveis de sistema** em que várias funções de segurança devem ser impostas.
 - A necessidade, em algumas organizações, de identificar vários níveis de segurança e categorizar os dados e usuários com base nessas classificações.

Introdução a questões de segurança de banco de dados

Ameaças aos bancos de dados

- As ameaças aos bancos de dados podem resultar na perda ou degradação de alguns ou de todos os objetivos de segurança comumente aceitos:
 - **Integridade**
 - **Disponibilidade**
 - **Confidencialidade**

Introdução a questões de segurança de banco de dados

Ameaças aos bancos de dados

- Em um sistema de banco de dados multiusuário, o SGBD precisa oferecer técnicas para permitir que certos usuários acessem partes selecionadas de um banco de dados sem que obtenham acesso ao restante dele.
- Um SGDB normalmente inclui dois tipos de mecanismos de segurança de banco de dados:
 - **Mecanismos de segurança discricionários**
 - Usados para conceder privilégios aos usuários
 - **Mecanismos de segurança obrigatórios**
 - Usados para classificação de dados e usuários em vários níveis de segurança (AS, S, C e NC)

Medidas de controle

- Quatro medidas de controle principais são usadas para fornecer segurança nos bancos de dados:
 - **Controle de acesso**
 - **Controle de inferência**
 - **Controle de fluxo**
 - **Criptografia de dados**

Segurança de banco de dados e o DBA

- O DBA tem uma **conta de DBA** no SGBD, também conhecida como **conta do sistema** ou **conta de superusuário**, que oferece capacidades poderosas que não estão disponíveis às contas e usuários comuns do banco de dados.
- Os comandos privilegiados dos DBA realizam os seguintes tipos de ações:
 - Criação de conta
 - Concessão de privilégio
 - Revogação de privilégio
 - Atribuição de nível de segurança

Controle de acesso discricionário

Tipos de privilégios discricionários

- Existem dois níveis para atribuição de privilégios na utilização do sistema de banco de dados:
 - **Nível de conta**
 - Podem incluir os privilégios CREATE SCHEMA, CREATE TABLE, ALTER, DROP, SELECT.
 - **Nível de relação (ou tabela)**
 - Podem incluir o privilégio SELECT, modificação em R (U/D/I), especificar restrições de integridade referencial em R .
- A concessão e revogação de privilégios costuma seguir um modelo de autorização conhecido como **modelo de matriz de acesso**.
 - Linhas de uma matriz representam sujeitos
 - Colunas representam objetos

Controle de acesso discricionário

Especificando privilégios por meio do uso de visões

- O mecanismo de **visões** (views) é um importante mecanismo discricionário por si só.
 - Por exemplo, se o proprietário *A* de uma relação *R* quiser que outra conta *B* seja capaz de recuperar apenas alguns campos de *R*, então *A* pode criar uma visão *V* de *R* que inclua apenas os atributos e depois conceda SELECT em *V* para *B*.
 - **CREATE VIEW** vfuncionario **AS**
SELECT Nome, Datanasc, Endereco
FROM FUNCIONARIO
WHERE Dnr = 1;
 - **GRANT SELECT ON** vfuncionario **TO** 'B' @'localhost';

Controle de acesso discricionário

Revogação de privilégios

- Em alguns casos, é desejável cancelar privilégios.
 - Por exemplo, o proprietário de uma relação pode querer conceder o privilégio SELECT a um usuário para uma tarefa específica e, depois, revogar esse privilégio quando a tarefa for concluída.
 - **REVOKE SELECT ON FUNCIONARIO FROM 'B'@'localhost';**

Controle de acesso discricionário

Propagação de privilégios usando a GRANT OPTION

- Sempre que um proprietário A de uma relação R concede um privilégio em R para outra conta B com a GRANT OPTION, isso significa que B também pode conceder esse privilégio em R para outras contas.
- Se a conta de proprietário A revogar o privilégio concedido a B , todos os privilégios que B propagou com base nesse privilégio deverão ser revogados automaticamente pelo sistema.

Controle de acesso discricionário

Limites de propagação de privilégios

- **Propagação horizontal:** para um número inteiro i significa que uma conta B que recebe a GRANT OPTION pode conceder o privilégio a , no máximo, i outras contas.
- **Propagação vertical:** se a conta A concede um privilégio à conta B com propagação vertical definida para um número inteiro j , isso significa que a conta B tem a GRANT OPTION sobre esse privilégio, mas pode conceder o privilégio a outras contas somente com uma propagação vertical *menor que* j .

Controle de acesso discricionário

Exemplos para ilustrar o controle de acesso discricionário no Mysql

FUNCIONARIO

Nome	<u>Cpf</u>	Data_nasc	Endereco	Sexo	Salario	Dnr
------	------------	-----------	----------	------	---------	-----

DEPARTAMENTO

<u>Dnumero</u>	Dnome	Cpf_ger
----------------	-------	---------

Figura 24.1

Esquemas para as duas relações, FUNCIONARIO e DEPARTAMENTO.

Controle de acesso discricionário

Exemplos para ilustrar a criação de contas de usuários no Mysql

- Para criar conta de usuário A1 com a senha 'root':
 - **CREATE USER** 'A1'@'localhost' **IDENTIFIED BY** 'root';
- Para alterar a senha do usuário A1 para 'admin':
 - **SET PASSWORD FOR** 'A1'@'localhost'=**PASSWORD**('admin');
- Para renomear o usuário A1 para A2:
 - **RENAME USER** 'A1'@'localhost' **TO** 'A2'@'localhost';
- Para excluir o usuário A2:
 - **DROP USER** 'A2'@'localhost' ;
- Para consultar todos os usuários cadastrados:
 - **SELECT** host, user **FROM** mysql.user;

Controle de acesso discricionário

Exemplos para ilustrar a concessão de privilégios

- Para conceder à conta A1 o privilégio de criar relações na base EMPRESA:
 - **GRANT CREATE ON EMPRESA TO 'A1'@'localhost';**
- Para conceder à conta A2 o privilégio de inserir tuplas na relação DEPARTAMENTO:
 - **GRANT INSERT ON DEPARTAMENTO TO 'A2'@'localhost';**

Controle de acesso discricionário

Exemplos para ilustrar a concessão de privilégios

- Para conceder à conta A3 o privilégio para excluir tuplas na relação FUNCIONARIO, e que também possa **propagar o privilégio DELETE** para outras contas:
 - **GRANT DELETE ON FUNCIONARIO TO 'A3'@'localhost' WITH GRANT OPTION;**

Controle de acesso discricionário

Exemplos para ilustrar a concessão de privilégios

- Para conceder à conta A4 o privilégio para recuperar apenas os atributos Pnome, Datanasc e Endereco e somente para as tuplas com Dnr = 4 na relação FUNCIONARIO, e que também possa propagar o privilégio SELECT para outras contas:
 - **CREATE VIEW A4FUNCIONARIO AS
SELECT Pnome, Datanasc, Endereco
FROM FUNCIONARIO
WHERE Dnr = 4;
GRANT SELECT ON A4FUNCIONARIO TO 'A4'@'localhost'
WITH GRANT OPTION;**

Controle de acesso discricionário

Exemplos para ilustrar a concessão de privilégios

- Para conceder à conta A4 o privilégio para atualizar apenas o atributo Dnome de DEPARTAMENTO:
 - **GRANT** UPDATE (Dnome) **ON** DEPARTAMENTO **TO** 'A4'@'localhost';
- Para conceder à conta A2 todos os privilégios para as relações da base EMPRESA:
 - **GRANT** ALL **ON** EMPRESA **TO** 'A2'@'localhost' ;

Controle de acesso discricionário

Exemplos para ilustrar a revogação de privilégios

- Para revogar o privilégio DELETE na relação FUNCIONARIO de A3:
 - **REVOKE DELETE ON FUNCIONARIO FROM 'A3'@'localhost';**

Controle de acesso obrigatório

- Em muitas aplicações, uma *política de segurança* adicional é necessária para classificar dados e usuários com base nas classes de segurança: AS, S, C, NC.
 - **Propriedade de segurança simples:** Um sujeito S não tem permissão para acesso de leitura a um objeto O a menos que classe $(S) \geq$ Classe (O) .
 - **Propriedade de estrela:** Um sujeito S não tem permissão para gravar um objeto O a menos que classe $(S) \leq$ Classe (O) .

Controle de acesso obrigatório

■ Exemplo:

(a) EMPREGADO

Nome		Salario		DesempenhoFuncao		CT
Smith	NC	40.000	C	Regular	S	S
Brown	C	80.000	S	Bom	C	S

(b) EMPREGADO

Nome		Salario		DesempenhoFuncao		CT
Smith	NC	40.000	C	null	C	C
Brown	C	null	C	Bom	C	C

(c) EMPREGADO

Nome		Salario		DesempenhoFuncao		CT
Smith	NC	null	NC	null	NC	NC

(d) EMPREGADO

Nome		Salario		DesempenhoFuncao		CT
Smith	NC	40.000	C	Regular	S	S
Smith	NC	40.000	C	Excelente	C	C
Brown	C	80.000	S	Bom	C	S

Figura 23.2 Uma relação multinível para ilustrar a segurança multinível. (a) As tuplas originais de EMPREGADO. (b) Aparência de EMPREGADO após a filtragem para usuários de classificação C. (c) Aparência de EMPREGADO após a filtragem para usuários de classificação NC. (d) Polinstantciação da tupla Smith.

Controle de acesso baseado em papéis

- Surgiu para gerenciar e impor a segurança em sistemas de grande escala por toda a empresa.
- Os papéis podem ser criados/destruídos usando os comandos **CREATE ROLE** e **DESTROY ROLE**.
- Para conceder o papel *tempo_integral* para o *funcionario_tipo1*:
 - **GRANT ROLE** tempo_integral **TO** funcionario_tipo1;
- O MySQL não tem suporte a controle de acesso baseado em papéis.

Controle de acesso baseado em papéis

Exemplos para ilustrar a concessão de privilégios

- Para criar o papel *gerente_vendas*
 - **CREATE ROLE** *gerente_vendas*;
- Para conceder as permissões de inserir, excluir e alterar ao papel *gerente_vendas*:
 - **GRANT ROLE** INSERT, DELETE, UPDATE **TO** *gerente_vendas*;
- Para conceder o papel *gerente_vendas* para os funcionários A1, A2, A3 e A4:
 - **GRANT** *gerente_vendas* **TO** A1, A2, A3, A4;

Referências bibliográficas

- **ELMASRI, R.; NAVATHE, S. B. Sistemas de Banco de Dados.** 6ª ed., Addison Wesley, 2010.
- **MySQL – Manual de Referência do MySQL 4.1.**
Disponível em: <http://downloads.mysql.com/docs/refman-4.1-pt.pdf>.
- **MySQL – Manual de Referência do MySQL 5.6.**
Disponível em: <http://dev.mysql.com/doc/refman/5.6/en/index.html>