Chapter4 数据库的安全性与完整性保护

4.1 数据库的安全性

4.1.1 数据库的安全与安全数据库

数据库的安全（database security）

防止非法使用数据库。即要求数据库的用户：通过规定的访问途径，按照规定的访问规则（规范）来访问数据库中的数据，并接受来自DBMS的各种检查

能适应网络环境下安全要求级别的数据库称为**安全数据库**（secure database），或称为可信数据库（trusted database）

4.1.2 数据库安全的基本概念与内容

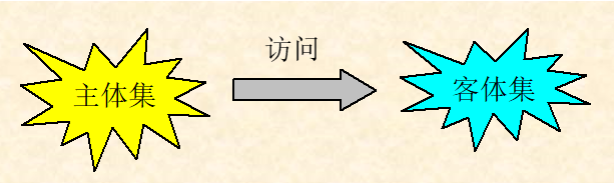
可信计算基TCB

它是为实现数据库安全所采用的所有实施策略与机制的集合；它是实施、检查、监督数据库安全的机构

主体、客体与主客体分离

客体——数据库中的数据及其载体，如：表、视图、快照、存储过程、数据文件等；

主体——数据库中数据的访问者



数据库安全就是研究有关实体的主/客体划分以及主/客体之间的访问关系的控制

在数据库安全中，主体访问客体时需进行一定的安全控制与检查，目前存在三种控制方式：

身份标识与鉴别

每个主体必须有一个标志自己身份的标识符（以区别不同的主体）以及一个用以验证其身份的访问口令

自主访问控制（DAC）

- 是一种基于存取矩阵的安全控制模型
- 此模型由主体、客体和存/取操作三部分内容构成了一个矩阵（如图所示）

	主体1	主体2	……	主体i	……
客体1	……	……	……	读/写	……
客体2	……	……	……	读/修改	……
……	……	……	……	……	……
客体j	插入	修改/删除	……	读/插入/删除	……
……	……	……	……	……	……

存取矩阵模型图

存取矩阵中的元素是可以随意改变的

主体可以通过授权（Grant）/回收（Revoke）操作变更某些操作权限

适合于单机方式下的访问控制

强制访问控制（MAC)

强制访问控制中的主、客体标记由专门的安全管理员设置，任何主体均无权设置与授权，它体现了在网上对数据库安全的强制性与统一性

数据完整性

防止非法使用插入（insert）、删除（delete）、修改（update）等影响数据完整性的操作

控制手段：–对存储数据错误的检测　–事务回卷功能

常用的控制手段：三类数据完整性：–实体完整性 –关联完整性　–用户定义完整性约束

公开通道

正规的、接受TCB的（自主/强制）访问控制检查的访问通道

隐蔽通道

非正规的、不受 TCB 控制的访问通道

审计

跟踪记录用户对数据的访问操作

–访问时间/访问内容/用户名/终端名/操作类型/操作结果

–并可根据审计结果给出报警信息

由于执行审计操作需要额外的时间和空间开销，因此在DBMS中，‘审计’通常是一个可选择的安全保护手段，主要用于安全性要求较高的部门

访问监控器

上述的安全策略须有一个网络中的实体来完成，即访问监控器。TCB是一个抽象的功能/策略集合，而访问监控器则是一个客观存在的实体，是TCB在网络中的实现。

4.1.3 数据库的安全标准

美国四类七级，中国五级，SQL92提供C1级别。具体的我不想记了，考到了算我倒霉。

4.1.4 SQL对数据库安全的支持

操作权限

- SELECT权
- INSERT权
- DELETE权
- UPDATE权
- REFERENCE权
- EXECUTE权
- USAGE权

Reference是指在完整性约束下引用关系的权利；Usage主要应用在关系和断言之外的多种模式元素上；Trigger是定义这个关系上的触发器的权利；Execute是执行如PSM过程或函数之类的代码的权利；Under是创建给定类型的子类型权利。

➢授权语句

GRANT <操作权限列表> ON <操作对象>
TO <用户名列表> [WITH GRANT OPTION]

–例：

- grant SELECT，UPDATE on S
  to XULIN with grant option
- grant UPDATE (G) on SC to XULIN

with grant option：给予其授予权限。

➢回收语句

REVOKE <操作权限列表> ON <操作对象>
FROM <用户名列表> [RESTRICT | CASCADE]

–CASCADE：连锁回收

–RESTRICT：在不存在连锁回收问题时才能回收权限，否则拒绝回收

–例：

- revoke UPDATE on S from XULIN cascade

4.2 数据库的完整性

指数据库中数据的正确性和一致性，包括：

正确性：数据的有效性、有意义

一致性：在多用户（多程序）并发访问数据库的情况下，保证对数据的更新不会出现与实际不一致的情况

4.2.1 数据库完整性保护的功能

三个基本功能

设置功能：-系统及用户对数据库完整性的基本要求

检查功能：-有能力检查数据库中的数据是否有违反约束条件的现象出现

处理功能：-出现违反约束条件时，有及时处理的能力

4.2.2 完整性规则的三个内容

实体完整性规则

—在一个基表的主关键字（主码）中，其属性的取值不能为空值

参照完整性规则

—关系R中的每个元组在外关键字F上的值或者是空值（NULL），或必须引用在关系S中存在的元组，即不能引用不存在的实体

用户定义的完整性规则

—由用户来定义的数据完整性要求

4.2.3 完整性约束的设置、检查与处理

看看课件就好吧，我真的不想记了。讲得太细了，要用的时候看手册不香么。考到了算我倒霉。

❑ 全局约束：断言

➢ 定义断言

```
CREATE ASSERTION <name> CHECK( <condition> )
```

➢ 撤消断言

```
DROP ASSERTION <assertion-name-list>
```

4.2.4 触发器

不考，欧耶！