基础篇
第三章
数据库的安全性

主讲：高宏
海量数据计算研究中心

数据库安全性

- **Why?**
  - 数据库的一大特点是数据可以共享
  - 但数据共享必然带来数据库的安全性问题
  - 数据库系统中的数据共享不能是无条件的共享

例：军事秘密、国家机密、新产品实验数据、市场需求分析、市场营销策略、销售计划、客户档案、医疗档案、银行储蓄数据

- 1991年4月美国NCSC（国家计算机安全中心）颁布了《可信计算机系统评估标准关于可信数据库系统的解释》（Trusted Database Interpretation 简称TDI）
  - TDI中定义了数据库管理系统的设计与实现中需满足和用以进行安全性级别评估的标准。

- **TCSEC/TDI安全级别划分**

安全级别	定　　义
A1	验证设计（Verified Design）
B3	安全域（Security Domains）
B2	结构化保护（Structural Protection）
B1	标记安全保护（Labeled Security Protection）
C2	受控的存取保护（Controlled Access Protection）
C1	自主安全保护（Discretionary Security Protection）
D	最小保护（Minimal Protection）

按系统可靠或可信程度逐渐增高

安全级别具有向下兼容性

- 数据库安全性控制的常用方法：
  - 用户标识和鉴定
  - 存取控制
  - 视图
  - 审计
  - 加密存储

- 用户标识与鉴别(Identification & Authentication)
  - 系统提供的最外层安全保护措施
  - 用户名/口令
    - 简单易行，容易被人窃取

账号	口令
张明	1234
李丽	2345
……	……

- 存取控制机制
  - 存取控制机制的组成
    - 定义存取权限
    - 检查存取权限

    用户权限定义和合法权检查机制一起组成了DBMS的安全子系统

- 存取控制机制
  - 常用存取控制方法
    - 自主存取控制：C2级
      - 同一用户对于不同的数据对象有不同的存取权限
      - 不同的用户对同一对象也有不同的权限
      - 用户还可将其拥有的存取权限转授给其他用户

用Grant语句向用户授予对数据的操作权限

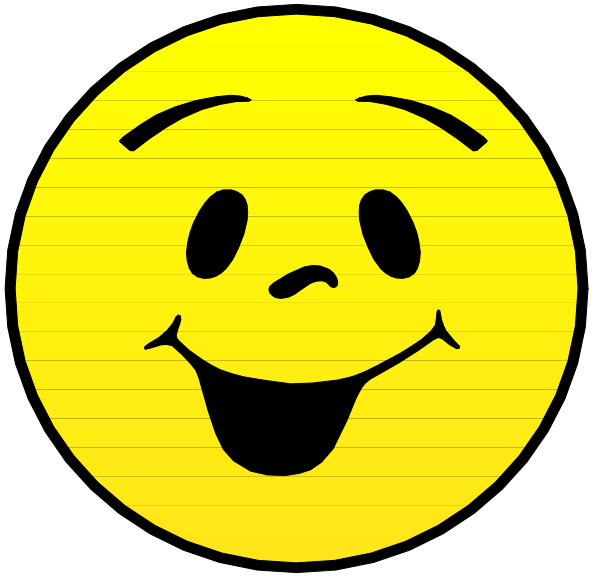
用Revoke语句收回授予的权限

- 数据库角色
  - 被命名的一组与数据库操作相关的权限
    - 角色是权限的集合
  - 可以为一组具有相同权限的用户创建一个角色
  - 使用角色来管理数据库权限可以简化授权的过程

- 审计
  - 审计功能启用一个专用的审计日志(Audit Log)，系统自动将用户对数据库的所有操作记录在上面
  - DBA可以利用审计日志中的追踪信息，重现导致数据库现有状况的一系列事件，以找出非法存取数据的人

C2以上安全级别的DBMS必须具有审计功能

- 数据加密
  - 防止数据库中数据在存储和传输中失密的有效手段
  - 加密的基本思想
    - 根据一定的算法将原始数据（术语为明文，Plain text）变换为不可直接识别的格式（术语为密文，Cipher text）
    - 不知道解密算法的人无法获知数据的内容



Now let's go to

Next Chapter