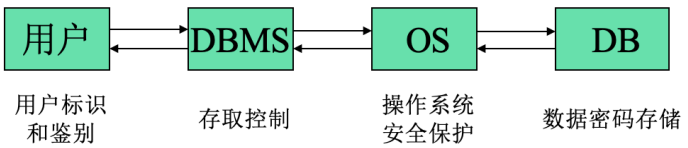
第四章 数据库的安全性

- 计算机安全性概述
  - 数据库的安全性
    - 是指保护数据库以防止不合法使用所造成的数据泄露、更改或破坏
  - 三类安全性问题
    - 技术安全类
      - 采用**具有一定安全性的硬件、软件**来实现对计算机系统及其所存数据的安全保护。
    - 管理安全类
      - **软硬件意外故障，场地的意外事故**，计算机设备和数据介质的**物理破坏**、丢失等安全问题。
    - 政策法律类
      - 政府部门建立的有关**计算机犯罪、数据安全保密**的法律道德准则和政策法规、法令
- 数据库安全性控制
  - 在一般计算机系统中，安全措施是一级一级层层设置的



  - 用户标识与鉴别（最外层安全保护措施）
  - 存取控制
    - 数据库安全性所关心的主要是**DBMS的存取控制机制**
    - 确保**只有合法用户才能访问数据库**，一般通过**授权**来实现
    - 存取控制机制
    - **自主存取控制 DAC**
      - Discretionary Access Control
      - 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
      - 灵活
      - 具体内容
        - 定义一个用户的存取权限就是要定义这个用户可以在那些数据对象上进行哪些类型的操作
        - 用户权限是由两个要素组成的

- 存取权限定义为**授权**

	数据对象	操作类型
模式(建表)	模式 外模式 内模式	建立、修改、检索 建立、修改、检索 建立、修改、检索
数据	表 属性列	查找、插入、修改、删除 查找、插入、修改、删除

  - 授权与回收
  - 数据库角色
- **强制存取控制 MAC**
  - 每一数据对象被标以一定的密级，每一个用户也被授予某一个级别的许可证。
  - 对于任一个对象，只有具有合法许可证的用户才可以存取。
  - 有些DBMS也支持B1级中的强制存取控制(MAC)
  - 具体内容
    - DBMS管理的全部实体分为主体和客体两大类
      - **主体**
      - **客体**
    - 对于主体和客体，DBMS为它们每个实例（值）指派一个**敏感度标记（Label）**
    - MAC机制就是通过对比主体的Label和客体的Label，最终确定主体是否能够存取客体
      - 当某一用户（一主体）以标记label注册入系统时，系统要求他对任何客体的存取必须遵循如下规则：
        - 1. 仅当主体的许可证级别大于或等于客体的密级时，该主体才能读取相应的客体；
        - 仅当主体的许可证级别等于客体的密级时，该主体才能写相应的客体
  - 视图机制
- 审计
- 数据加密
  - 对于高度敏感性数据，除以上安全性措施外，还可以采用数据加密技术
  - 数据加密是防止数据库中数据在**存储和传输**中**失密**的有效手段
  - DES，RSA
- 统计数据库的安全性