第四章 数据库安全性

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。

数据库中数据的共享是在DBMS统一的严格的控制之下的共享，即只允许有合法使用权限的用户访问允许他存取的数据。

数据库系统的安全保护措施是否有效是数据库系统主要的性能指标之一。

数据库的安全性是指保护数据库，防止因用户非法使用数据库造成数据泄露、更改或破坏。

数据库系统的安全性包括计算机安全性和数据库的安全性。本章只讨论数据库的安全性。

第四章 数据库安全性

本章内容:

4.2 数据库安全性控制

4.2.1 用户标识与鉴别

4.2.2 自主存取控制—授权与回收

4.2.3 强制存取控制

4.2.4 视图机制

4.2.5 审计

4.2.6 数据加密

4.3 统计数据库安全性

4.2 数据库安全性控制

- **非法使用数据库的情况**
  - 用户编写一段合法的程序绕过DBMS及其授权机制，通过操作系统直接存取、修改或备份数据库中的数据；
  - 直接或编写应用程序执行非授权操作；
  - 通过多次合法查询数据库从中推导出一些保密数据

    例：某数据库应用系统禁止查询单个人的工资，但允许查任意一组人的平均工资。用户甲想了解张三的工资，于是他：

    (1)首先查询包括张三在内的一组人的平均工资

    (2)然后查用自己替换张三后这组人的平均工资

    从而推导出张三的工资
  - 破坏安全性的行为可能是无意的，故意的，恶意的。
- **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、数据加密。

4.2.1 用户标识与鉴别

- 用户标识与鉴别(Identification & Authentication)是系统提供的最外层安全保护措施。
- **基本方法**
  - 系统提供一定的方式让用户标识自己的名字或身份；
  - 系统内部记录着所有合法用户的标识；
  - 每次用户要求进入系统时，由系统核对用户身份标识；
  - 通过鉴定后才提供机器使用权；
  - 用户标识和鉴定可以重复多次。
- **用户名/口令**
  - 简单易行，容易被人窃取
- **每个用户预先约定好一个计算过程或者函数**
  - 系统提供一个随机数
  - 用户根据自己预先约定的计算过程或者函数进行计算
  - 系统根据用户计算结果是否正确鉴定用户身份