数据库第四章

数据安全性

- 概念：保护数据库以**防止不合法使用所造成的数据泄漏 更改或破坏**
- 不安全因素
  - 非授权用户对数据库的恶意存取和破坏
  - 数据库中重要或敏感的数据被泄漏
  - 安全环境的脆弱性

数据库安全性控制

用户身份鉴别

方法：

- 静态口令鉴别：密码
- 动态口令鉴别：短信密码
- 生物特征鉴别：指纹 虹膜
- 智能卡鉴别：智能卡

存取控制

自主存取控制

定义用户权限---授权

- 概念：用户对某一数据对象的操作权利称为权限 select/update/insert/delete
- 操作
  - GRANT
    - **grant 权限名 on 对象类型 对象名 to 用户**
    - **WITH GRANT OPTION**：可以把获得的权限再授予其他的用户
  - REVOKE：收回存取权限
    - **revoke 权限 on 对象类型 对象名 from 用户**
    - cascade/RESTRICT：收回当户及被当前用户授权的权限/当前用户权限
  - CREATE：只有超级用户dba才有权创建一个新的数据库用户；模式的创建/修改/删除 也需要安全性控制
    - 权限
      - CONNECT：不能创建新用户 不能创建模式 不能创建基本表 只能登录数据库
      - RESOURCE：能创建基本表和视图 不能创建模式 不能创建新用户
      - DBA：可以创建新的用户 创建模式 创建基本表 视图
  - UPDATE：对表中存在的某一列的值进行修改
- 数据库角色
  - 概念：是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
  - 语句：**create role 角色名；grant 权限on 对象类型 对象名 to 角色名；grant 角色名 to 用户 with admin option；** 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

合法权限检查：若用户的操作请求超出了定义的权限 系统将拒绝执行此操作

强制存取控制

- 概念：对于任意对象 只有具有合法许可证的用户才可以存取
- 实体
  - 主体
  - 客体：系统中的被动实体 是受主体操纵的
- 敏感度标记
  - 分类：绝密 机密 可信 公开
  - 规则
    - 当主体的许可证级别大于或等于客体的密级时 主体才能读取相应的客体
    - 当主体的许可证级别小于或等于客体的密级时 主体才能写相应的客体

审计

- 概念：把用户对数据库所有操作自动记录下来放入审计日志；
- 语句
  - AUDIT：设置审计功能
  - NOAUDIT：取消审计功能
- 引入原因：因为任何系统的安全保护措施都不是完美无缺的利用审计功能 DBA可以根据审计跟踪的信息找到非法存取的数据
- 事后检查的安全机制

视图机制

通过视图机制把要保密的数据对无权存取的用户隐藏起来

数据加密

- 概念：将明文变换为密文 从而使得无法获知数据的内容
- 防止数据库中的数据在存储和传输中失密的有效手段
- 分类
  - 存储加密
    - 透明：对用户完全透明
    - 非透明：通过多个加密函数实现
  - 传输加密
    - 链路加密：在数据链路层加密
    - 端到端加密：在发送端加密 在接收端解密

扫码听课，视频讲解更清晰