第四章 数据库安全性

4.3 视图机制

- 把要保密的数据对无权存取这些数据的用户隐藏起来，对数据提供一定程度的安全保护

视图机制（续）

- 授予用户查询整个表的权限

```
GRANT SELECT
ON TABLE Student
TO U1;
```

- 授予用户查询某些列的权限

```
GRANT SELECT(Sno, Sname)
ON TABLE Student
TO U2;
```

- 授予用户查询某些行的权限？
  - 需要用存取谓词来定义用户权限
  - 无法直接用GRANT语句实现
  - 可以用视图机制间接地实现

视图机制（续）

[例4.14] 授权王平老师能查询计算机系学生的情况，授权系主任张明能对计算机系学生的信息进行所有操作。

(1) 先建立计算机系学生的视图CS_Student

```
CREATE VIEW CS_Student
AS
SELECT  *
FROM   Student
WHERE  Sdept='CS';
```

视图机制（续）

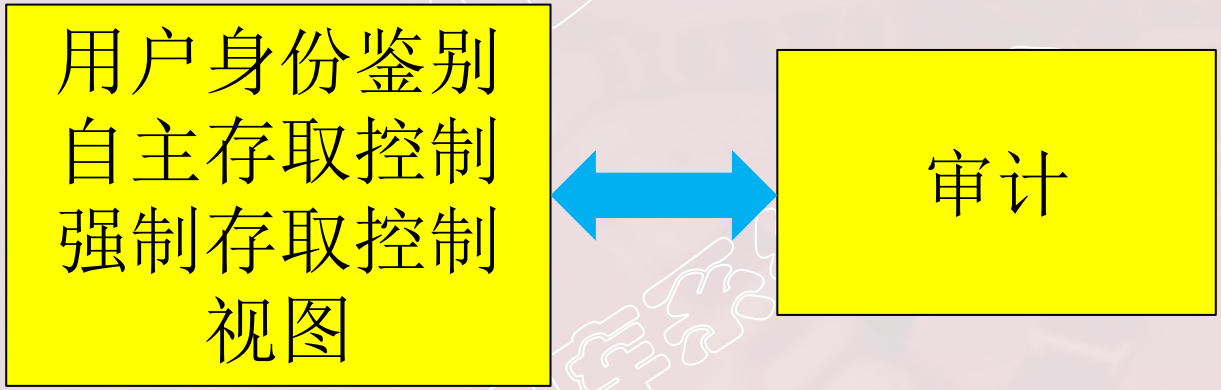
(2) 在视图上进一步定义存取权限

```
GRANT  SELECT
ON  CS_Student
TO 王平;

GRANT ALL PRIVILIGES
ON  CS_Student
TO  张明;
```

第四章 数据库安全性

数据库安全性控制措施



预防性措施　　监控措施

4.4 审计

- 什么是审计
  - 启用一个专用的审计日志（Audit Log）
    将用户对数据库的所有操作记录在上面
  - 审计员利用审计日志
    监控数据库中的各种行为
    发现非法存取，发现潜在威胁
  - C2以上安全级别的DBMS必须具有审计功能

审计（续）

- 可以被审计的事件
  - 服务器事件
    - 审计数据库服务器发生的事件
  - 系统权限
    - 对系统拥有的结构或模式对象进行操作的审计
    - 要求该操作的权限是通过系统权限获得的
  - 语句事件
    - 对SQL语句，如DDL、DML、DQL及DCL语句的审计
  - 模式对象事件
    - 对特定模式对象上进行的SELECT或DML操作的审计

审计（续）

- 审计日志管理
  - 基本功能: 提供多种审计查阅方式
  - 多套审计规则：一般在初始化设定
  - 提供审计分析和报表功能
  - 审计日志管理功能
    - 防止审计员误删审计记录，审计日志必须先转储后删除
    - 对转储的审计记录文件提供完整性和保密性保护
    - 只允许审计员查阅和转储审计记录，不允许任何用户新增和修改审计记录等
  - 提供查询审计设置及审计记录信息的专门视图

审计（续）

- 审计功能的可选性
  - 审计很费时间和空间
  - DBA可以根据应用对安全性的要求，灵活地打开或关闭审计功能
  - 审计功能主要用于安全性要求较高的部门

审计（续）

- 审计功能设置
  - AUDIT语句：设置审计功能
  - NOAUDIT语句：取消审计功能

设置审计功能

- 用户级审计
  - 任何用户可设置的审计
  - 主要是用户针对自己创建的数据库表和视图进行审计
- 系统级审计
  - 只能由数据库管理员设置
  - 监测成功或失败的登录要求、监测授权和收回操作以及其他数据库级权限下的操作

例题

[例4.15] 对修改SC表结构或修改SC表数据的操作进行审计

```
AUDIT ALTER,UPDATE
ON  SC;
```

[例4.16] 取消对SC表的一切审计

```
NOAUDIT  ALTER,UPDATE
ON  SC;
```

第四章 数据库安全性

4.5 数据加密

- 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—明文（Plain text）变换为不可直接识别的格式-—密文（Cipher text）
- 加密方法
  - 存储加密
  - 传输加密

数据加密（续）

- 存储加密
  - 透明存储加密
    - 内核级加密保护方式，对用户完全透明
    - 将数据在写到磁盘时对数据进行加密，授权用户读取数据时再对其进行解密
    - 数据库的应用程序不需要做任何修改，只需在创建表语句中说明需加密的字段即可

    内核级加密方法: 性能较好，安全完备性较高
  - 非透明存储加密
    - 通过多个加密函数实现

数据加密（续）

- 传输加密
  - 链路加密
    - 传输信息由报头和报文两部分组成
      报头:路由选择信息；报文:要传送的数据信息
    - 报文和报头均加密
  - 端到端加密
    - 在发送端加密，接收端解密
    - 只加密报文不加密报头
    - 所需密码设备数量相对较少，容易被非法监听者发现并从中获取敏感信息

数据加密（续）

用户

可信通讯模块

第一步：创建可信连接

第二步：确认通信双方端点的可靠性

第三步：协商加密算法和密钥

第四步：可信传输数据

第五步：关闭可信连接

可信通讯模块

数据库服务器

数据库管理系统可信传输示意图

第四章 数据库安全性

4.6 其他安全性保护

❖ 推理控制

- 处理强制存取控制未解决的问题，避免用户利用能够访问的数据推知更高密级的数据
- 常用方法
  - 基于函数依赖的推理控制
  - 基于敏感关联的推理控制

用户A

公开

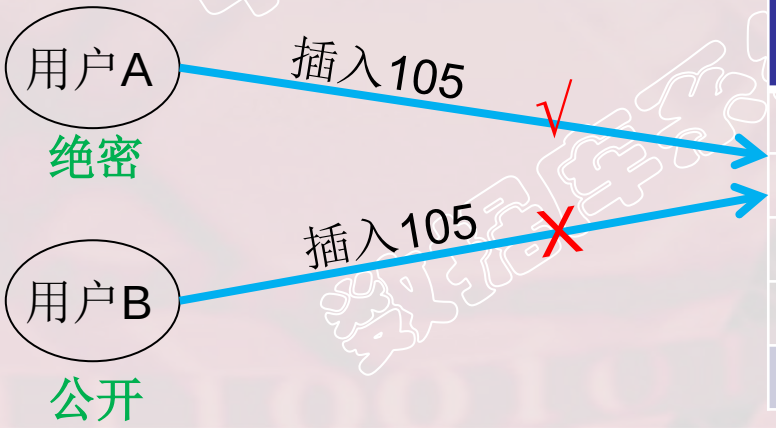
职工表

职工号	姓名	职务	工资
101	A	部门经理	5000
102	B	部门经理	5000
103	C	销售员	3000
……	……	……	……
公开	公开	公开	机密

4.6 其他安全性保护

❖隐蔽信道

- 处理强制存取控制未解决的问题
- 高安全等级用户按事先约定方式主动向低安全等级用户传输信息，从而导致高安全等级敏感信息泄露。



X（UNIQUE）	……
101	……
102	……
103	……
……	……
绝密	……

表T

第四章 数据库安全性

4.7 小结

- 实现数据库系统安全性的技术和方法
  - 用户身份鉴别
  - 存取控制技术：自主存取控制和强制存取控制
  - 视图技术
  - 审计技术
  - 数据加密：加密存储和加密传输

小结（续）

- 本章目标
  - 掌握什么是数据库的安全性问题
  - 牢固掌握数据库管理系统实现数据库安全性控制的常用方法和技术
- 本章重点
  - 使用GRANT 语句和 REVOKE 语句实现自主存取控制功能
  - 使用CREATE ROLE语句创建角色，用GRANT 语句给角色授权
  - 掌握视图机制在数据库安全保护中的作用
- 本章难点
  - 强制存取控制机制中确定主体能否存取客体的存取规则
  - 要理解并掌握存取规则为什么要这样规定