谢艺婕 10162551 应数161

第4章 数据库安全性

1. 什么是数据库的安全性?

答: 数据库的安全性是指保护数据库以防止不合法的使用所造成的数据泄露、更改或破坏。

5. 试述实现数据库安全性控制的常用方法和技术。

答: ①用户标识和鉴别: 该方法由系统提供一定的方式让用户标识自己的名字或身份。每次用户要求进入系统时,由系统进行核对,通过鉴定后才提供系统的使用权。

②存取控制: 通过用户权限定义和合法权检查确保只有合法权限的用户访问数据库,所有未被授权的人员无法存取数据。例如C2级中的自主存取控制(DAC),B1级中的强制存取控制(MAC)。

③视图机制: 为不同的用户定义视图,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,从而自动地对数据提供一定程度的安全保护。

④审计: 建立审计日志,把用户对数据库的所有操作自动记录下来放入审计日志中。DBA可以利用审计跟踪的信息,重现导致数据库现有状况的一系列事件,找出非法存取数据的人、时间和内容等。

⑤数据加密: 对存储和传输的数据进行加密处理,从而使得不知道解密算法的人无法获知数据的内容。

8. 请用SQL的GRANT和REVOKE语句(加上视图机制)完成以下授权定义或存取功能:

(a) 用户王明对两个表有SELECT权力

解: GRANT SELECT ON 职工, 部门
TO 王明

(b) 用户李勇对两个表有INSERT和DELETE权力

解: GRANT INSERT, DELETE ON 职工, 部门
TO 李勇

(c) 每个职工只对自己的记录有SELECT权力

解: GRANT SELECT ON 职工
WHEN USER() = NAME
TO ALL

(d) 用户刘星对职工表有SELECT权力,对工资字段具有更新权力

解: GRANT SELECT, UPDATE(工资) ON 职工
TO 刘星

(e) 用户张新具有修改这两个表的结构的权力

解: GRANT ALTER TABLE ON 职工, 部门
TO 张新

(f) 用户周平具有对两张所有权力(读、插、改、删数据),并具有给其他用户授权的权力

解: GRANT ALL PRIVILIGES ON 职工, 部门
TO 周平
WITH GRANT OPTION

(g) 用户杨兰具有从每个部门职工中SELECT最高工资、最低工资、平均工资的权力,他不能查看每个人的工资

解: CREATE VIEW 部门工资 AS
SELECT 部门.名称, MAX(工资), MIN(工资), AVG(工资)
FROM 职工, 部门
WHERE 职工.部门号 = 部门.部门号
GROUP BY 职工.部门号
GRANT SELECT ON 部门工资
TO 杨兰

9. 把上题中(a)~(g)的每一种情况,撤销各用户所授予的权力

解: (a) REVOKE SELECT ON 职工, 部门 FROM 王明
(b) REVOKE INSERT, DELETE ON 职工, 部门 FROM 李勇
(c) REVOKE SELECT ON 职工
WHEN USER() = NAME
FROM ALL
(d) REVOKE SELECT, UPDATE ON 职工 FROM 刘星
(e) REVOKE ALTER TABLE ON 职工, 部门 FROM 张新
(f) REVOKE ALL PRIVILIGES ON 职工, 部门 FROM 周平
(g) REVOKE SELECT ON 部门工资 FROM 杨兰
DROP VIEW 部门工资