第四章　数据库安全性

数据库的一大特点是数据可以共享

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**

如何限定有些用户只能访问特定的数据表或视图;

如何使有些数据库只对指定的用户开放;

以及如何阻止非法帐号登录？

……这些问题都和数据库数据保护息息相关。

数据的安全性　　**数据的完整性**

本章主要内容

- 计算机安全性概述
- 数据库安全性控制
- 数据库其他安全机制

一、计算机安全性概述

数据的安全性是指保护数据以防止因不合法的使用而造成数据的泄露、更改和破坏。

计算机系统也存在安全性问题。

计算机系统安全性：为计算机系统建立和采取的各种安全保护措施，以保护计算机系统中的硬件、软件及数据，防止其因偶然或恶意的原因使系统遭到破坏，数据遭到更改或泄露等。

数据库的安全性和计算机系统的安全性，包括计算机硬件、操作系统、网络系统等的安全性，是紧密联系、相互支持的。

计算机安全不仅涉及到计算机系统本身的技术问题、管理问题，还涉及法学、犯罪学、心理学的问题。

二、数据库安全性控制

1、用户标识与鉴别

用户标识：用户名（User Name）、用户标识号（UID）

2、存取控制

数据库安全性主要指DBMS的存取控制机制。

① 定义用户权限，并登记到数据字典中（安全规则/授权规则）；

② 合法权限检查。


用户权限
定义
合法权限
检查
DBMS安
全子系统

目前，大型的DBMS一般都支持自主存取控制（DAC）；有些DBMS同时还支持强制存取控制（MAC）。

（1）自主存取控制：用户可以“自主”地决定将数据的存取权限授予何人，决定是否也将“授权”的权限授予别人；

（2）强制存取控制：通过对比用户的许可证级别和数据库对象的密级，最终确定用户是否能够存取数据库对象。

3、自主存取控制（DAC）

目前，大型的DBMS几乎都支持DAC，SQL通过GRANT语句和REVOKE语句对DAC提供支持。

用户权限包括：数据库对象和操作类型。

在数据库系统中，定义存取权限称为授权。

4、授权和回收

- GRANT

语句格式：

```
GRANT { ALL [ PRIVILEGES ] }
    | permission [ ( column [ ,...n ] ) ] [ ,...n ]
    [ ON [ class :: ] securable ] TO principal [ ,...n ]
    [ WITH GRANT OPTION ] [ AS principal ]
```

权限的名称

指定授予其权限的对象

被授予权限的对象

允许被授权者在获得指定权限的同时还可以将指定权限授予其他用户、角色或Windows组。

指定当前数据库中执行GRANT语句的用户所属的角色名或主名。

EG：给PXSCJ数据库上的用户david和wang授予创建表的权限。

```
GRANT CREATE TABLE
TO david,wang
```

数据库级的权限不需要指定ON子句。

EG：把查询XSB表的权限授给用户zhang。

```
GRANT SELECT ON XSB
TO zhang;
```

EG：把对XSB表和KCB表的全部操作权限授予用户lily和zhao。

```
GRANT ALL PRIVILEGES ON XSB,KCB
TO lily,zhao;
```

SQL Server 2008不推荐使用此选项，保留此选项仅用于向后兼容。它不会授予所有可能的权限。

EG：把对XSB表的查询权限授予所有用户。

```
GRANT SELECT ON XSB
TO PUBLIC;
```

Public :所有用户都拥有此用户权限，可以浏览数据表、视图和执行存储过程，但没有访问权限。

EG：把查询XSB表和修改学生总学分的权限授给用户fang。

```
GRANT UPDATE(Tcredit),SELECT ON XSB
TO fang;
```

EG：把查询XSB表的权限授给用户zhang，并允许将此权限再授予其他用户。

```
GRANT SELECT ON XSB
TO zhang
WITH GRANT OPTION;
```

- REVOKE

语法格式：

```
REVOKE [ GRANT OPTION FOR ]
    { [ ALL [ PRIVILEGES ] ]
      |permission [ ( column [ ,...n ] ) ] [ ,...n ]
    }
    [ ON [ class :: ] securable ]
    { TO | FROM } principal [ ,...n ]
    [ CASCADE] [ AS principal ]
```

将撤消授予指定权限的能力

权限的名称

指定表中将撤消其权限的列的名称

指定将撤消其权限的安全对象

主体的名称

指示当前正在撤消的权限也将从其他被该主体授权的主体中撤消。

指定一个主体，执行该查询的主体从该主体获得撤消该权限的权利。

EG：收回用户zhang对查询XSB表的权限。

```
REVOKE SELECT ON XSB
FROM zhang CASCADE;
```

EG：收回用户fang修改XSB表学生总学分的权限。

```
REVOKE UPDATE(Tcredit) ON XSB
FROM fang;
```

EG：收回所有用户对XSB表的查询权限。

```
REVOKE SELECT ON XSB
FROM PUBLIC;
```

5、数据库角色

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。

在SQL Server中，通过角色可以将用户分为不同的类，相同类用户（相同角色的成员）进行统一管理，赋予相同的操作权限。

（1）创建角色

CREATE ROLE role_name [AUTHORIZATION owner_name]

AUTHORIZATION owner_name：将拥有新角色的数据库用户或角色。如果未指定用户，则执行 CREATE ROLE 的用户将拥有该角色。

EG：创建用户 zhang 拥有的数据库角色 r_zhang。

```
CREATE ROLE r_zhang AUTHORIZATION zhang;
```

（2）给角色授权

GRANT <权限>[，<权限>]…

ON <对象类型>对象名

TO <角色>[，<角色>]…

（3）将一个角色授予其他的角色或用户

GRANT <角色1>[，<角色2>]…

TO <角色3>[，<用户1>]…

[WITH ADMIN OPTION]　　--可将权限授予其他角色

（4）角色权限的收回

REVOKE <权限>[，<权限>]…

ON <对象类型> <对象名>

FROM <角色>[，<角色>]…

EG：通过角色实现将一组权限授予一个用户。

```
CREATE ROLE R1;                          /*创建角色R1*/
GO
GRANT SELECT,UPADATE,INSERT
ON XSB
TO R1;                    /*授予R1对XSB表的SELECT,UPADATE,INSERT权限*/
GO
GRANT R1 TO A1，A2，A3;          /*将该角色授予A1、A2、A3*/
GO
REVOKE R1 FROM A1;                /*收回A1的三个权限*/
```

EG：角色R2在XSB表上拥有SELECT权限，用户li是R2的成员，li使用WITH GRANT OPTION子句将SELECT权限转移给了用户huang，用户huang不是R2的成员。请以用户li的身份撤销用户huang的SELECT权限。

以用户li的身份登录SQL Server服务器：

```
REVOKE SELECT
ON XSB
TO huang
AS R2;
```

三、其他数据库安全性控制

- 强制存取控制方法（MAC）
- 视图机制
- 审计
- 数据加密
- 统计数据库安全性

1、强制存取控制方法

（1）自主存取控制（DAC）缺点：

- 可能存在数据的“无意泄露”；
- 原因：这种机制仅仅通过对数据的存取权限来进行安全控制，而数据本身并无安全性标记；
- 解决：对系统控制下的所有主客体实施强制存取控制策略。

（2）强制存取控制（MAC)

- 保证更高程度的安全性
- 用户不能直接感知或进行控制
- 适用于对数据有严格而固定密级分类的部门

  军事部门

  政府部门

2、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。

- 先建立视图；
- 再定义存取权限。

3、审计（Audit）

- 创建审计日志（Audit Log）将用户对数据库的所有操作记录在上面；
- DBA利用审计日志找出非法存取数据的人、时间和内容；
- C2以上安全级别的DBMS必须具有审计功能。

审计分为：

- 用户级审计

  针对自己创建的数据库表或视图进行审计；

  记录所有用户对这些表或视图的一切成功和（或）不成功的访问要求以及各种类型的SQL操作。

- 系统级审计

  由DBA设置；

  监测成功或失败的登录要求；

  监测GRANT和REVOKE操作以及其他数据库级权限下的操作；

4、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）变换为不可直接识别的格式（密文），使得不知道解密算法的人无法获知数据的内容。

加密方法：替换方法（密钥）、置换方法以及混合方法。

5、统计数据库安全性

统计数据库允许用户查询聚集类型的信息（如合计、平均值等），不允许查询单个记录信息。

统计数据库中特殊的安全性问题：存在隐蔽的信息通道，能从合法的查询中推导出不合法的信息。

三大规则：

规则1：任何查询至少要涉及N(N足够大)个以上的记录；

规则2：任意两个查询的相交数据项不能超过M个；

规则3：任一用户的查询次数不能超过1+(N-2)/M；