第四章 数据库安全性

4.1 数据库安全性概述

数据库的安全性是指保护数据库以防止不合法使用所造成的数据泄露、更改或破坏

4.1.1 数据库的不安全因素

1、非授权用户对数据库的恶意存取和破坏

DBMS 提供的安全措施主要包括用户身份鉴别、存取控制和视图等技术

2、数据库中重要或民高的数据被泄露

DNMS 提供的主要啊技术有强制存取控制、数据加密存储和加密传输等

还可提供审计功能，审计日志分析

3、安全环境的脆弱性

数据库的安全性包括计算机硬件、操作系统、网络系统等的安全性与计算机系统的安全性紧密联系

解决：建立一套可信计算机系统的概念和标准

4.1.2 安全标准间简介

有 TCSEC 和 CC 两种

1、TCSEC 标准

TCSEC/TDI 从四个方面来描述安全性级别划分的指标：安全策略、责任、保护、文档 （P135）

2、CC 标准

提出国际公认的表述信息技术安全性的结构

把信息产品的安全要求分为：安全功能要求，安全保证要求

4.2 数据库安全性控制

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

存取控制流程

首先，数据库管理系统对提出 SQL 访问请求的数据库用户进行身份鉴别，防止不可信用户使用系统。然后，在 SQL 处理层进行自主存取控制和强制存取控制，进一步可以进行推理控制。还可以对用户访问行为和系统关键操作进行审计，对

异常用户行为进行简单入侵检测。

4.2.1 用户身份鉴别

系统提供的最外层安全保护措施

用户标识：由用户名和用户标识号组成，用户标识在系统生命周期中唯一

用户身份鉴别方法：

1、静态口令：由用户设定，不变

2、动态口令：口令动态变化，一次一密，短信验证码或动态令牌

3、生物特征识别：通过生物特征进行认证，指纹，虹膜等

4、智能卡识别：硬件，具有硬件加密的功能

4.2.2 存取控制

存取控制机制主要包括定义用户权限和合法权限检查两部分

定义用户权限和合法权限检查机制共同组成了数据库管理系统的存取控制子系统

4.2.3 自主存取控制方法

通过 SQL 的 GRANT 和 REVOKE 语句实现

用户权限由数据对象和操作类型两个要素：授权

对象类型	对象	操 作 类 型
数据库模式	模式	**CREATE SCHEMA**
	基本表	**CREATE TABLE，ALTER TABLE**
	视图	**CREATE VIEW**
	索引	**CREATE INDEX**
数据	基本表和视图	**SELECT，INSERT，UPDATE，DELETE，REFERENCES，ALL PRIVILEGES**
	属性列	**SELECT，INSERT，UPDATE， REFERENCES，ALL PRIVILEGES**

4.2.4 授权：授予与回收

GRANT 授予，REVOKE 回收

1、GRANT

GRANT <权限>[,<权限>]...

ON <对象类型> <对象名>[,<对象类型> <对象名>]…

TO <用户>[,<用户>]...

[WITH GRANT OPTION];

若有最后一句，则获得某种权限的用可以把该权限授予其他用户，若没有则不能允许传递授予，不能循环授予

例：GRANT ALL PRIVILIGES

ON TABLE Student,Course

TO U2,U3;

GRANT SELECT

ON TABLE SC

TO PUBLIC;

GRANT INSERT

ON TABLE SC

TO U5

WITH GRANT OPTION;

2、REVOKE

数据库管理员或其他授权者用 REVOKE 语句收回权限

REVOKE <权限>[,<权限>]...

ON <对象类型> <对象名>[,<对象类型><对象名>]…

FROM <用户>[,<用户>]...[CASCADE | RESTRICT];

3、创建数据库模式的权限

数据库管理员在创建用户时实现

CREATE USER <username>

[WITH][DBA|RESOURCE|CONNECT];

默认为 CONNECT 权限：啥也不能创建，只能登登录

RESOURSE：能创建基本表和视图，但是不能创建模式和新用户

DBA：超级用户，啥都行

4.2.5 数据库角色

数据库角色：被命名的一组与数据库操作相关的权限

可以为一组具有相同权限的用户创建一个角色，简化授权过程

1.角色的创建

CREATE　ROLE　<角色名>

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]

该语句把角色授予某用户，或授予另一个角色

授予者是角色的创建者或拥有在这个角色上的 ADMIN OPTION

指定了 WITH ADMIN OPTION 则获得某种权限的角色或用户还可以把这种权限授予其他角色

一个角色的权限：直接授予这个角色的全部权限加上其他角色授予这个角色的全部权限

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>]…

用户可以回收角色的权限，从而修改角色拥有的权限

REVOKE 执行者是角色的创建者，即拥有在这个（些）角色上的 ADMIN OPTION

4.2.6 强制存取控制的方法

资助存取控制仅仅通过对数据存取权限来进行安全控制，而数据本身并无安全性标记，或可能存在数据的“无意泄露”，可以对系统控制下的所有主客体实施强制存取控制策略

强制存取控制保证更高程度的安全性，用户不能最直接感知过进行控制，适合军事部门过政府部门

全部实体分为主体和客体：主体是系统中的活动实体，用户；客体是系统中的被

动实体，受主体操纵，文件基本表等

敏感度标记：绝密 TS，机密 S，可信 C，公开 P

主体敏感度标记叫许可证级别，客体敏感度标记叫密级

强制存取控制原则：

（1） 仅当主体许可证级别大于或等于客体密级，主体才能读取相应客体

（2） 仅当主体许可证级别小于或等于客体密级，主体才能写相应的客体

实现强制存取控制首先要实现资助存取控制，因为较高安全性级别提供的安全保护要包含较低级别的所有保护

自主存取控制与强制存取控制共同构成数据库管理系统的安全机制

系统应先进行自主存取控制检查，再进行强制存取控制检查

4.3 视图机制

视图把要保密的数据对无权存取这些数据的用户隐藏起来，从而对数据提供一定程度的安全保护，间接地实现支持存取谓词的用户权限定义

4.4 审计

启用有个专用的审计日志将用户对数据库的所有操作记录在上面，C2 以上安全级别的 DBMS 必须具有审计功能

审计功能是可选的，因为很费时间和空间

1、审计事件

服务器事件：服务器上发生的事件

系统权限：对系统拥有的结构或模式对象进行操作的审计，要求该操作是通过系统权限获得的

语句事件：对 SQL 语句，如 DDL ,DML, DQL, 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

2、审计功能

基本功能：提供多种审计查阅方式：基本的，可选的，有限的等

提供多套审计规则

提供审计分析和报表功能

审计日志管理功能 包括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

3、AUDIT 语句和 NOAUDIT 语句

AUDIT 语句：设置审计功能

NOAUDIT 语句：取消审计功能

审计分为系统级审计和用户级审计

用户级审计：任何用户都可设置，主要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，监测成果获失败的登录要求、监测授权和回收操作以及其他数据库级权限下的操作

例：AUDIT ALTER,UPDATE

ON SC;

NOAUDIT ALTER,UPDATE

ON SC;

4.5 数据加密

数据加密是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：把原始数据（明文）变换为不可直接识别的格式（密文）

加密方法分为存储加密和传输加密

1、存储加密

（1）透明存储加密

内核级加密保护方式，对用户透明

写数据时进行加密，授权用户读取数据时对其解密

应用程序不需做任何修改，只需说明加密字段即可

优点：性能较好，安全完备性较高

（2）非透明存储加密：通过多个加密函数实现

2、传输加密

（1）链路加密

在链路层进行加密；传输信息由报头和报文两部分组成；报文和报头均加密

（2）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

3、基于安全套层协议 SSL 传输方案的实现思路

（1）创建可信连接

用数字证书进行验证，用本地的 CA 信任列表和证书撤销列表进行验证

（2）确认通信双方端点的可靠性

（3）协商加密算法和密钥

双方协商本次会话的加密算法与密钥

（4）可信传输数据

数据以密文形式在网路上传输

（5）关闭可信连接

4.6 其他安全性保护

1、推理控制

利用用户之前访问的历史数据结合一些背景，推导出用户不能访问的数据

常用方法：基于函数依赖的推理控制

基于敏感关系的推理控制

2、隐蔽信道

3、数据隐私保护

描述个人控制其不愿他人知道或他人不便知道的个人数据的能力

范围很广：数据收集、数据存储、数据处理和数据发布各个阶段

总结：数据库管理系统是管理数据的核心

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

数据加密存储和加密传输