数据库原理

王兴梅
计算机科学与技术学院
Email:wangxingmei@hrbeu.edu.cn

第四章　数据库安全性

- 问题的提出
  - 数据库的一大特点是数据可以共享
  - 但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

例：军事秘密、国家机密、新产品实验数据、市场需求分析、市场营销策略、销售计划、 客户档案、医疗档案、银行储蓄数据

数据库安全性（续）

- 什么是数据库的安全性
  - 数据库的安全性是指保护数据库，防止因用户非法使用数据库造成数据泄露、更改或破坏。
- 什么是数据的保密
  - 数据保密是指用户合法地访问到机密数据后能否对这些数据保密。
  - 通过制订法律道德准则和政策法规来保证。

第四章 数据库安全性

4.1 计算机安全性概论

4.2 数据库安全性控制

4.3 统计数据库安全性

4.4 小结

4.1 计算机安全性概论

4.1.1 计算机系统的三类安全性问题

4.1.2 可信计算机系统评测标准

4.1.1 计算机系统的三类安全性问题

- 什么是计算机系统安全性
  - 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。

计算机系统的三类安全性问题（续）

- 计算机安全涉及问题
  - 计算机系统本身的技术问题
    - 计算机安全理论与策略
    - 计算机安全技术
  - 管理问题
    - 安全管理
    - 安全评价
    - 安全产品
  - 政策法规

4.1 计算机安全性概论

4.1.1 计算机系统的三类安全性问题

4.1.2 可信计算机系统评测标准

4.1.2 可信计算机系统评测标准

- 为降低进而消除对系统的安全攻击，各国引用或制定了一系列安全标准
  - TCSEC (桔皮书)
  - TDI (紫皮书)

可信计算机系统评测标准（续）

- TCSEC/TDI安全级别划分

安全级别	定　　义
A1	验证设计（Verified Design）
B3	安全域（Security Domains）
B2	结构化保护（Structural Protection）
B1	标记安全保护（Labeled Security Protection）
C2	受控的存取保护（Controlled Access Protection）
C1	自主安全保护（Discretionary Security Protection）
D	最小保护（Minimal Protection）

可信计算机系统评测标准（续）

- 四组(division)七个等级
  - D
  - C（C1，C2）
  - B（B1，B2，B3）
  - A（A1）
- 按系统可靠或可信程度逐渐增高
- 各安全级别之间具有一种偏序向下兼容的关系，即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要求，同时提供更多或更完善的保护能力。

可信计算机系统评测标准（续）

不同安全级别对安全指标的支持情况

	自主存取控制	客体重用	标记完整性	标记信息的扩散	主体敏感度标记	设备标记	强制存取控制	标识与鉴别	可信路径	审计	系统体系结构	系统完整性	屏蔽信道分析	可信设施管理	可信恢复	安全测试	设计规范和验证	配置管理	可信分配	安全特性用户指南	可信设施手册	测试文档	设计文档
C1	■							■			■	■				■				■	■	■	■
C2	▨	■						▨		■	■	□				▨				□	▨	□	□
B1	□	□	■	■			■	▨		▨	▨	□				▨	■			□	▨	□	▨
B2	□	□	□	□	■	■	▨	□	■	▨	▨	□	■	■		▨	▨	■		□	▨	▨	▨
B3	▨		□	□	□	□	□	□	▨	▨	▨	□	▨	▨	■	▨	▨	□		□	▨	□	▨
A1	□	□	□	□	□	□	□	□	□	□	□	□	▨	□	□	▨	▨	▨	■	□	□	▨	▨

可信计算机系统评测标准（续）

- 表示该级不提供对该指标的支持；
- 表示该级新增的对该指标的支持；
- 表示该级对该指标的支持与相邻低一级的等级一样；
- 表示该级对该指标的支持较下一级有所增加或改动。

第四章 数据库安全性

4.1 计算机安全性概论

4.2 数据库安全性控制

4.3 统计数据库安全性

4.4 小结

4.2 数据库安全性控制

4.2.1 数据库安全性控制概述
4.2.2 用户标识与鉴别
4.2.3 存取控制
4.2.4 自主存取控制方法
4.2.5 强制存取控制方法
4.2.6 视图机制
4.2.7 审计
4.2.8 数据加密

4.2.1 数据库安全性控制概述

- 非法使用数据库的情况
  - 用户编写一段合法的程序绕过DBMS及其授权机制，通过操作系统直接存取、修改或备份数据库中的数据；
  - 直接或编写应用程序执行非授权操作；

数据库安全性控制概述（续）

- 通过多次合法查询数据库从中推导出一些保密数据

  例：某数据库应用系统禁止查询单个人的工资，但允许查任意一组人的平均工资。用户甲想了解张三的工资，于是他：

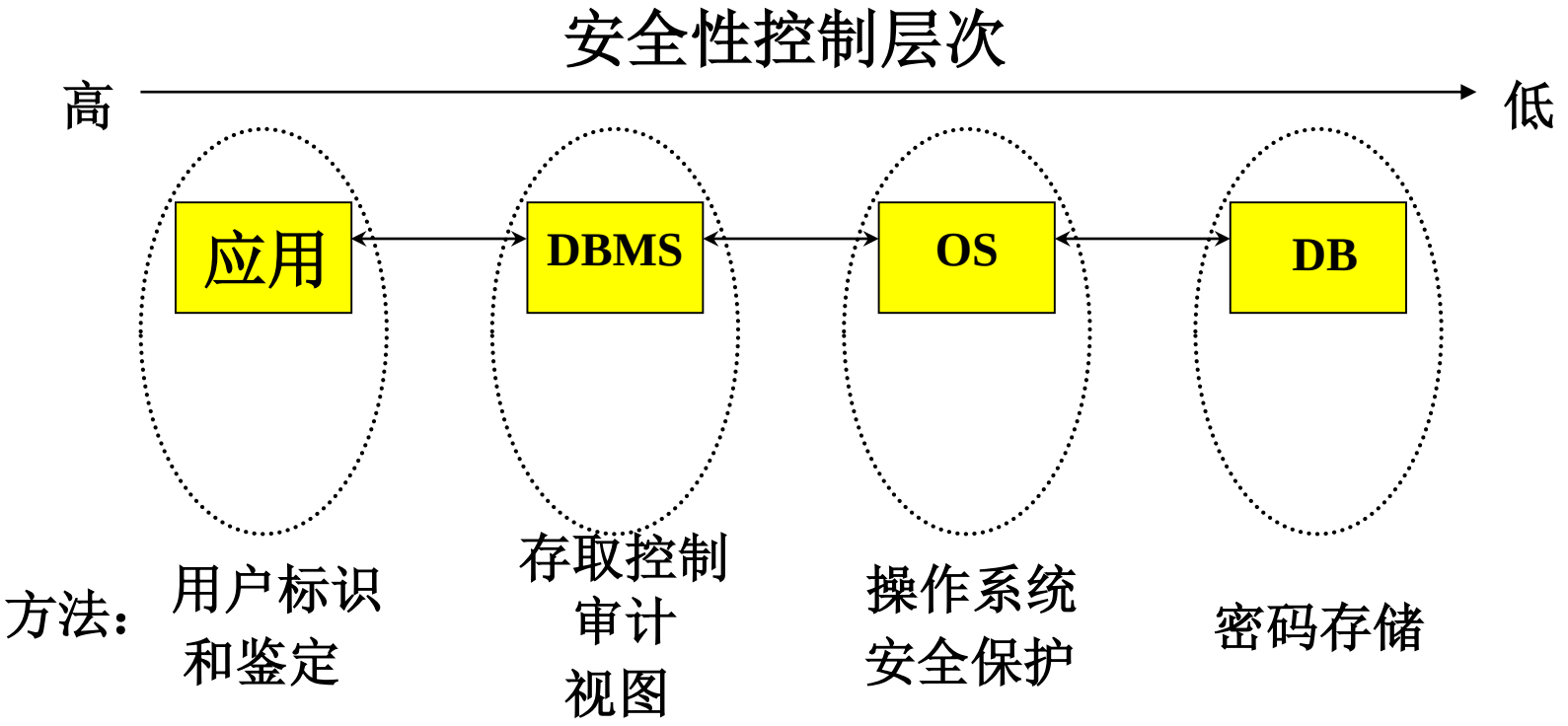
  首先查询包括张三在内的一组人的平均工资

  然后查用自己替换张三后这组人的平均工资

  从而推导出张三的工资

- 破坏安全性的行为可能是无意的，故意的，恶意的。

计算机系统中的安全模型



数据库安全性控制概述（续）

- 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
  - 密码存储

4.2 数据库安全性控制

4.2.1 数据库安全性控制概述

4.2.2 用户标识与鉴别

4.2.3 存取控制

4.2.4 自主存取控制方法

4.2.5 强制存取控制方法

4.2.6 视图机制

4.2.7 审计

4.2.8 数据加密

4.2.2 用户标识与鉴别

- 用户标识与鉴别（Identification & Authentication）
  - 系统提供的最外层安全保护措施

4.2.2 用户标识与鉴别

基本方法

- 系统提供一定的方式让用户标识自己的名字或身份；
- 系统内部记录着所有合法用户的标识；
- 每次用户要求进入系统时，由系统核对用户提供的身份标识；
- 通过鉴定后才提供机器使用权。
- 用户标识和鉴定可以重复多次

用户标识自己的名字或身份

- 用户名/口令
  - 简单易行，容易被人窃取
- 每个用户预先约定好一个计算过程或者函数
  - 系统提供一个随机数
  - 用户根据自己预先约定的计算过程或者函数进行计算
  - 系统根据用户计算结果是否正确鉴定用户身份

4.2 数据库安全性控制

4.2.1 数据库安全性控制概述

4.2.2 用户标识与鉴别

4.2.3 存取控制

4.2.4 自主存取控制方法

4.2.5 强制存取控制方法

4.2.6 视图机制

4.2.7 审计

4.2.8 数据加密

4.2.3 存取控制

- 存取控制机制的功能
  - 存取控制机制的组成
    - 定义存取权限
    - 检查存取权限

    用户权限定义和合法权检查机制一起组成了DBMS的安全子系统

存取控制（续）

- 定义存取权限
  - 在数据库系统中，为了保证用户只能访问他有权存取的数据，必须预先对每个用户定义存取权限。
- 检查存取权限
  - 对于通过鉴定获得上机权的用户（即合法用户），系统根据他的存取权限定义对他的各种操作请求进行控制，确保他只执行合法操作。

存取控制（续）

- 常用存取控制方法
  - 自主存取控制（Discretionary Access Control，简称DAC）
    - C2级—— 灵活
  - 强制存取控制（Mandatory Access Control，简称 MAC）
    - B1级——严格

4.2 数据库安全性控制

4.2.1 数据库安全性控制概述
4.2.2 用户标识与鉴别
4.2.3 存取控制
4.2.4 自主存取控制方法
4.2.5 强制存取控制方法
4.2.6 视图机制
4.2.7 审计
4.2.8 数据加密

4.2.4 自主存取控制方法

- 定义存取权限
  - 存取权限
    - 存取权限由两个要素组成
      - 数据对象
      - 操作类型

自主存取控制方法（续）

- 关系系统中的存取权限
  - 类型

	数据对象	操作类型
模　式	模　式	建立、修改、删除、检索
	外模式	建立、修改、删除、检索
	内模式	建立、删除、检索
数　据	表	查找、插入、修改、删除
	属性列	查找、插入、修改、删除

自主存取控制——授权与回收

- 概述
- 授权
- 收回权限
- 小结

安全性(续)

- 谁定义？

  DBA和表的建立者（即表的属主）

- 如何定义？

  SQL语句：

  GRANT

  REVOKE

授 权

- GRANT语句的一般格式：

  GRANT <权限>[,<权限>]...

  [ON <对象类型> <对象名>]

  TO <用户>[,<用户>]...

  [WITH GRANT OPTION];

- 谁定义？DBA和表的建立者（即表的属主）
- GRANT语义功能：将对指定操作对象的指定操作权限授予指定的用户。

(1) 操作权限

对　象	对象类型	操　作　权　限
属性列	TABLE	SELECT, INSERT, UPDATE DELETE, ALL PRIVILEGES
视　图	TABLE	SELECT, INSERT, UPDATE DELETE, ALL PRIVILEGES
基本表	TABLE	SELECT, INSERT, UPDATE DELETE ALTER, INDEX, ALL PRIVILEGES
数据库	DATABASE	CREATE TABLE

(2) 用户的权限

- 建表（CREATETAB）的权限:属于DBA
- DBA授予-->普通用户
- 基本表或视图的属主拥有对该表或视图的一切操作权限
- 接受权限的用户:

  一个或多个具体用户

  PUBLIC（全体用户）

(3) WITH GRANT OPTION子句

- 指定了WITH GRANT OPTION子句:
  获得某种权限的用户还可以把这种权限再授予别的用户。

- 没有指定WITH GRANT OPTION子句:
  获得某种权限的用户只能使用该权限，不能传播该权限

例题

［例］把查询Student表权限授给用户U1

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

例题（续）

[例] 把对表SC的INSERT权限授予U5用户，并允许他再将此权限授予其他用户

```
GRANT INSERT
ON TABLE SC
TO U5
WITH GRANT OPTION;
```

传播权限

执行例5后，U5不仅拥有了对表SC的INSERT权限，还可以传播此权限：

```
GRANT INSERT ON TABLE SC TO U6
WITH GRANT OPTION;
```

同样，U6还可以将此权限授予U7：

```
GRANT INSERT ON TABLE SC TO U7;
```

但U7不能再传播此权限。

U5--> U6--> U7

例题（续）

[例] DBA把在数据库S_C中建立表的权限授予用户U8

```
GRANT CREATE TABLE
ON DATABASE S_C
TO U8;
```

授权与回收

- 概述
- 授权
- 收回权限
- 小结

收回权限的功能

- REVOKE语句的一般格式为：

```
REVOKE <权限>[,<权限>]...
[ON <对象类型> <对象名>]
FROM <用户>[,<用户>]...
[CASCADE|RESTRICT];
```

- 功能：从指定用户那里收回对指定对象的指定权限

例题

［例］把用户U4修改学生学号的权限收回

```
REVOKE UPDATE(Sno)
ON TABLE Student
FROM U4;
```

例题（续）

［例］把用户U5对SC表的INSERT权限收回

```
REVOKE INSERT
ON TABLE SC
FROM U5 CASCADE;
```

权限的级联回收

系统将收回直接或间接从U5处获得的对SC表的INSERT权限:

-->U5--> U6--> U7

收回U5、U6、U7获得的对SC表的INSERT权限:

<--U5<-- U6<-- U7

小结:SQL灵活的授权机制

- DBA拥有对数据库中所有对象的所有权限，并可以根据应用的需要将不同的权限授予不同的用户。
- 用户对自己建立的基本表和视图拥有全部的操作权限，并且可以用GRANT语句把其中某些权限授予其他用户。
- 被授权的用户如果有“继续授权”的许可，还可以把获得的权限再授予其他用户。
- 所有授予出去的权力在必要时又都可以用REVOKE语句收回。

4.2 数据库安全性控制

4.2.1 数据库安全性控制概述
4.2.2 用户标识与鉴别
4.2.3 存取控制
4.2.4 自主存取控制方法
4.2.5 强制存取控制方法
4.2.6 视图机制
4.2.7 审计
4.2.8 数据加密

4.2.5 强制存取控制方法

- 什么是强制存取控制
  - 强制存取控制(MAC)是指系统为保证更高程度的安全性，按照TDI/TCSEC标准中安全策略的要求，所采取的强制存取检查手段。
  - MAC不是用户能直接感知或进行控制的。
  - MAC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

强制存取控制方法（续）

- 主体与客体
  - 在MAC中，DBMS所管理的全部实体被分为主体和客体两大类
  - 主体是系统中的活动实体
    - DBMS所管理的实际用户
    - 代表用户的各进程
  - 客体是系统中的被动实体，是受主体操纵的
    - 文件
    - 基表
    - 索引
    - 视图

强制存取控制方法（续）

- 敏感度标记
  - 对于主体和客体，DBMS为它们每个实例（值）指派一个敏感度标记（Label）
  - 敏感度标记分成若干级别
    - 绝密（Top Secret）
    - 机密（Secret）
    - 可信（Confidential）
    - 公开（Public）

强制存取控制方法（续）

- 主体的敏感度标记称为许可证级别（Clearance Level）
- 客体的敏感度标记称为密级（Classification Level）
- MAC机制就是通过对比主体的Label和客体的Label，最终确定主体是否能够存取客体

强制存取控制方法（续）

- 强制存取控制规则
  - 当某一用户（或某一主体）以标记label注册入系统时，系统要求他对任何客体的存取必须遵循下面两条规则：

（1）仅当主体的许可证级别大于或等于客体的密级时，该主体才能读取相应的客体；

（2）仅当主体的许可证级别小于或等于客体的密级时，该主体才能写相应的客体。

4.2 数据库安全性控制

4.2.1 数据库安全性控制概述
4.2.2 用户标识与鉴别
4.2.3 存取控制
4.2.4 自主存取控制方法
4.2.5 强制存取控制方法
4.2.6 视图机制
4.2.7 审计
4.2.8 数据加密

4.2.6 视图机制

- 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，
- 视图机制更主要的功能在于提供数据独立性，其安全保护功能太不精细，往往远不能达到应用系统的要求。

视图机制（续）

- 视图机制与授权机制配合使用:
- 首先用视图机制屏蔽掉一部分保密数据
- 视图上面再进一步定义存取权限
- 间接实现了支持存取谓词的用户权限定义

4.2 数据库安全性控制

4.2.1 数据库安全性控制概述
4.2.2 用户标识与鉴别
4.2.3 存取控制
4.2.4 自主存取控制方法
4.2.5 强制存取控制方法
4.2.6 视图机制
4.2.7 审计
4.2.8 数据加密

4.2.7 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
  - DBA可以利用审计日志中的追踪信息

    找出非法存取数据的人
  - C2以上安全级别的DBMS必须具有审计功能

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（续）

- 强制性机制:

  用户识别和鉴定、存取控制、视图

- 预防监测手段:

  审计技术

4.2 数据库安全性控制

4.2.1 数据库安全性控制概述
4.2.2 用户标识与鉴别
4.2.3 存取控制
4.2.4 自主存取控制方法
4.2.5 强制存取控制方法
4.2.6 视图机制
4.2.7 审计
4.2.8 数据加密

4.2.8 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（术语为明文，Plain text）变换为不可直接识别的格式（术语为密文，Cipher text）
  - 不知道解密算法的人无法获知数据的内容

数据加密（续）

- 加密方法
  - 替换方法
    - 使用密钥（Encryption Key）将明文中的每一个字符转换为密文中的一个字符
  - 置换方法
    - 将明文的字符按不同的顺序重新排列
  - 混合方法

    美国1977年制定的官方加密标准：数据加密标准（Data Encryption Standard，简称DES）

第四章 数据库安全性

4.1 计算机安全性概论

4.2 数据库安全性控制

4.3 统计数据库安全性

4.4 小结

4.3 统计数据库安全性

- 统计数据库的特点
  - 允许用户查询聚集类型的信息（例如合计、平均值等）
  - 不允许查询单个记录信息

例：允许查询“程序员的平均工资是多少？”

不允许查询“程序员张勇的工资？”

统计数据库安全性（续）

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

第四章 数据库安全性

4.1 计算机安全性概论

4.2 数据库安全性控制

4.3 统计数据库安全性

4.4 小结

4.4 小结

- 随着计算机网络的发展，数据的共享日益加强，数据的安全保密越来越重要
- DBMS是管理数据的核心，因而其自身必须具有一整套完整而有效的安全性机制。

小结（续）

- 《可信计算机系统评测标准》TCSEC/TDI是目前各国所引用或制定的一系列安全标准中最重要的一个。
- CSEC/TDI从安全策略、责任、保证和文档四个方面描述了安全性级别的指标

小结（续）

- 实现数据库系统安全性的技术和方法有多种，最重要的是存取控制技术和审计技术。
  - 目前许多大型DBMS 达到了C2级，其安全版本达到了B1
  - C2级的DBMS必须具有自主存取控制功能和初步的审计功能
  - B1级的DBMS必须具有强制存取控制和增强的审计功能
  - 自主存取控制功能一般是通过SQL 的GRANT语句和REVOKE语句来实现的