数据库系统概论

An Introduction to Database System

浙江农林大学

主讲：刘丽娟

数据库安全性

浙江农林大学
ZHEJIANG A&F UNIVERSITY

- 问题的提出
  - 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

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**

数据库安全性（续）

- 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 。
- 系统安全保护措施是否有效是数据库系统主要的性能指标之一。

第四章 数据库安全性

浙江农林大学
ZHEJIANG A&F UNIVERSITY

4.1 数据库安全性概述

4.2 数据库安全性控制

4.3 视图机制

4.4 审计（Audit）

4.5 数据加密

4.6 其他安全性保护

4.7 小结

4.1 数据库安全性概述

浙江农林大学
ZHEJIANG A&F UNIVERSITY

4.1.1 数据库的不安全因素

4.1.2 安全标准简介

4.1.1 数据库的不安全因素

浙江农林大学
ZHEJIANG A&F UNIVERSITY

1.非授权用户对数据库的恶意存取和破坏

- 一些黑客（Hacker）和犯罪分子在用户存取数据库时猎取用户名和用户口令，然后假冒合法用户偷取、修改甚至破坏用户数据。
- 数据库管理系统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。

数据库的不安全因素（续）

- 2.数据库中重要或敏感的数据被泄露
  - 黑客和敌对分子千方百计盗窃数据库中的重要数据，一些机密信息被暴露。
  - 数据库管理系统提供的主要技术有强制存取控制、数据加密存储和加密传输等。
  - 审计日志分析

数据库的不安全因素（续）

浙江农林大学
ZHEJIANG A&F UNIVERSITY

- 3.安全环境的脆弱性
  - 数据库的安全性与计算机系统的安全性紧密联系
    - 计算机硬件、操作系统、网络系统等的安全性
  - 建立一套可信（Trusted）计算机系统的概念和标准

4.1 数据库安全性概述

浙江农林大学
ZHEJIANG A&F UNIVERSITY

4.1.1 数据库的不安全因素

4.1.2 安全标准简介

第四章 数据库安全性

浙江农林大学
ZHEJIANG A&F UNIVERSITY

4.1 数据库安全性概述

4.2 数据库安全性控制

4.3 视图机制

4.4 审计（Audit）

4.5 数据加密

4.6 其他安全性

4.7 小结

4.2 数据库安全性控制

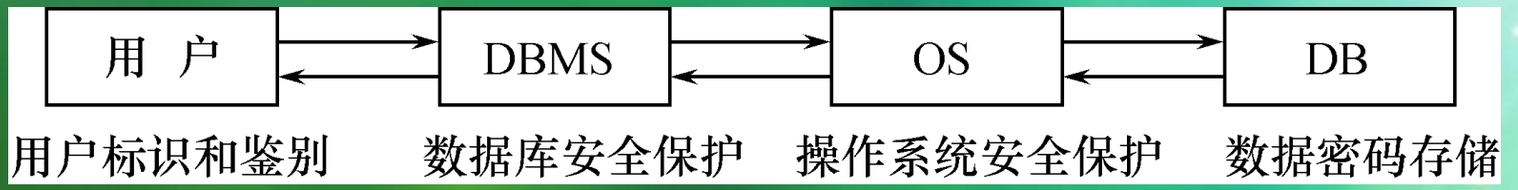
浙江农林大学
ZHEJIANG A&F UNIVERSITY

- 非法使用数据库的情况
  - 编写合法程序绕过数据库管理系统及其授权机制
  - 直接或编写应用程序执行非授权操作
  - 通过多次合法查询数据库从中推导出一些保密数据

数据库安全性控制（续）

浙江农林大学
ZHEJIANG A&F UNIVERSITY

- 计算机系统中，安全措施是一级一级层层设置



计算机系统的安全模型

数据库安全性控制（续）

浙江农林大学
ZHEJIANG A&F UNIVERSITY

- 系统根据用户标识鉴定用户身份，合法用户才准许进入计算机系统
- 数据库管理系统还要进行存取控制，只允许用户执行合法操作
- 操作系统有自己的保护措施
- 数据以密码形式存储到数据库中

数据库安全性控制（续）

浙江农林大学
ZHEJIANG A&F UNIVERSITY

- 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**

4.2 数据库安全性控制

浙江农林大学
ZHEJIANG A&F UNIVERSITY

4.2.1 用户身份鉴别

4.2.2 存取控制

4.2.3 自主存取控制方法

4.2.4 授权：授予与回收

4.2.5 数据库角色

4.2.6 强制存取控制方法

4.2.1 用户身份鉴别

浙江农林大学
ZHEJIANG A&F UNIVERSITY

- 用户身份鉴别

  （Identification & Authentication）

  - 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

    （用户标识号在系统整个生命周期内唯一）

用户身份鉴别（续）

- 用户身份鉴别的方法

1.静态口令鉴别

- 静态口令一般由用户自己设定，这些口令是静态不变的

2.动态口令鉴别

- 口令是动态变化的，每次鉴别时均需使用动态产生的新口令登录数据库管理系统，即采用一次一密的方法

3.生物特征鉴别

- 通过生物特征进行认证的技术，生物特征如指纹、虹膜和掌纹等

4.智能卡鉴别

- 智能卡是一种不可复制的硬件，内置集成电路的芯片，具有硬件加密功能

4.2 数据库安全性控制

4.2.1 用户标识与鉴别

4.2.2 存取控制

4.2.3 自主存取控制方法

4.2.4 授权：授予与回收

4.2.5 数据库角色

4.2.6 强制存取控制方法

4.2.2 存取控制

- 存取控制机制组成
  - 定义用户权限，并将用户权限登记到数据字典中
    - 用户对某一数据对象的操作权力称为**权限**
    - DBMS提供适当的语言来定义用户权限，存放在数据字典中，称做安全规则或授权规则
  - 合法权限检查
    - 用户发出存取数据库操作请求
    - DBMS查找数据字典，进行合法权限检查
- 用户权限定义和合法权检查机制一起组成了数据库管理系统的存取控制子系统

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
    - 用户对不同的数据对象有不同的存取权限
    - 不同的用户对同一对象也有不同的权限
    - 用户还可将其拥有的存取权限转授给其他用户

存取控制（续）

浙江农林大学
ZHEJIANG A&F UNIVERSITY

- 常用存取控制方法（续）
  - 强制存取控制（Mandatory Access Control，简称 MAC）
    - B1级
    - 每一个数据对象被标以一定的密级
    - 每一个用户也被授予某一个级别的许可证
    - 对于任意一个对象，只有具有合法许可证的用户才可以存取

4.2 数据库安全性控制

浙江农林大学
ZHEJIANG A&F UNIVERSITY

4.2.1 用户标识与鉴别

4.2.2 存取控制

4.2.3 自主存取控制方法

4.2.4 授权：授予与回收

4.2.5 数据库角色

4.2.6 强制存取控制方法

4.2.3 自主存取控制方法

- 通过 SQL 的GRANT 语句和REVOKE 语句实现
- 用户权限组成
  - 数据对象
  - 操作类型
- 定义用户存取权限：定义用户可以在哪些数据库对象上进行哪些类型的操作
- 定义存取权限称为授权

自主存取控制方法（续）

浙江农林大学
ZHEJIANG A&F UNIVERSITY

- 关系数据库系统中存取控制对象

对象类型	对象	操作类型
数据库模式	数据库	CREATE DATABASE
	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
	属性列	SELECT，INSERT，UPDATE

关系数据库系统中的存取权限

4.2 数据库安全性控制

浙江农林大学
ZHEJIANG A&F UNIVERSITY

4.2.1 用户标识与鉴别

4.2.2 存取控制

4.2.3 自主存取控制方法

4.2.4 授权：授予与回收

4.2.5 数据库角色

4.2.6 强制存取控制方法

4.2.4 授权：授予与回收

浙江农林大学
ZHEJIANG A&F UNIVERSITY

1.GRANT

- GRANT语句的一般格式：

  GRANT <权限>[,<权限>]...

  ON <对象名>

  TO <用户>[,<用户>]...

  [WITH GRANT OPTION];

- 语义：将对指定操作对象的指定操作权限授予指定的用户

GRANT（续）

浙江农林大学
ZHEJIANG A&F UNIVERSITY

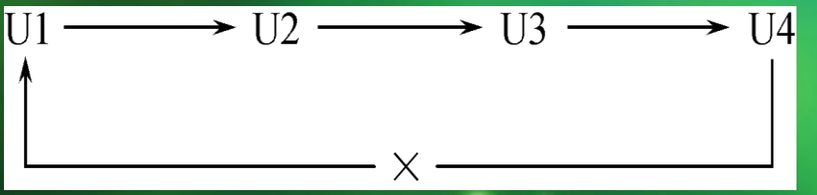
- 发出GRANT:
  - 数据库管理员
  - 数据库对象创建者（即属主Owner）
  - 拥有该权限的用户
- 按受权限的用户
  - 一个或多个具体用户
  - PUBLIC（即全体用户）

WITH GRANT OPTION子句

浙江農林大學
ZHEJIANG A&F UNIVERSITY

- WITH GRANT OPTION子句:
  - 指定：可以再授予
  - 没有指定：不能传播

- 不允许循环授权



例题

[例4.1] 把查询S表权限授给用户U1

```
GRANT   SELECT
ON   S
TO   U1;
```

例题（续）

[例4.2] 把C表的增、删、改权限授予用户U2和U3

```
GRANT INSERT,DELETE,UPDATE
ON C
TO U2,U3;
```

例题（续）

[例4.3] 把对表SC的查询权限授予所有用户

```
GRANT SELECT
ON  SC
TO PUBLIC;
```

例题（续）

浙江农林大学
ZHEJIANG A&F UNIVERSITY

[例4.4] 把查询Student表和修改学生学号的权限授给用户U4

```
GRANT UPDATE(Snum), SELECT
ON  S
TO U4;
```

- 对属性列的授权时必须明确指出相应属性列名

例题（续）

浙江农林大学
ZHEJIANG A&F UNIVERSITY

[例4.5] 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  SC
TO U5
WITH GRANT OPTION;
```

传播权限

执行例4.5后，U5不仅拥有了对表SC的INSERT权限，还可以传播此权限：

[例4.6] GRANT INSERT
ON SC
TO U6
WITH GRANT OPTION;

同样，U6还可以将此权限授予U7：

[例4.7] GRANT INSERT
ON SC
TO U7;

但U7不能再传播此权限。

传播权限（续）

执行了例4.1~例4.7语句后学生-课程数据库中的用户权限定义表

授权用户名	被授权用户名	数据库对象名	允许的操作类型	能否转授权
DBA	U1	关系Student	SELECT	不能
DBA	U2	关系Student	ALL	不能
DBA	U2	关系Course	ALL	不能
DBA	U3	关系Student	ALL	不能
DBA	U3	关系Course	ALL	不能
DBA	PUBLIC	关系SC	SELECT	不能
DBA	U4	关系Student	SELECT	不能
DBA	U4	属性列 Student.Sno	UPDATE	不能
DBA	U5	关系SC	INSERT	能
U5	U6	关系SC	INSERT	能
U6	U7	关系SC	INSERT	不能

授权：授予与回收（续）

浙江农林大学
ZHEJIANG A&F UNIVERSITY

2.REVOKE

- 授予的权限可以由数据库管理员或其他授权者用REVOKE语句收回
- REVOKE语句的一般格式为：

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

REVOKE（续）

浙江农林大学
ZHEJIANG A&F UNIVERSITY

[例4.8] 把用户U4修改学生学号的权限收回

```
REVOKE UPDATE(Snum)
ON  S
FROM U4;
```

REVOKE（续）

浙江農林大学
ZHEJIANG A&F UNIVERSITY

[例4.9] 收回所有用户对表SC的查询权限

```
REVOKE SELECT
ON  SC
FROM PUBLIC;
```

REVOKE（续）

浙江农林大学
ZHEJIANG A&F UNIVERSITY

[例4.10] 把用户U5对SC表的INSERT权限收回

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

- 将用户U5的INSERT权限收回的时候应该使用CASCADE，否则拒绝执行该语句
- 如果U6或U7还从其他用户处获得对SC表的INSERT权限，则他们仍具有此权限，系统只收回直接或间接从U5处获得的权限

REVOKE（续）

浙江农林大学
ZHEJIANG A&F UNIVERSITY

执行例4.8~4.10语句后学生-课程数据库中的用户权限定义表

授权用户名	被授权用户名	数据库对象名	允许的操作类型	能否转授权
DBA	U1	关系Student	SELECT	不能
DBA	U2	关系Student	ALL	不能
DBA	U2	关系Course	ALL	不能
DBA	U3	关系Student	ALL	不能
DBA	U3	关系Course	ALL	不能
DBA	U4	关系Student	SELECT	不能

MySQL的权限管理

浙江农林大学
ZHEJIANG A&F UNIVERSITY

```
USE mysql
-- 查询账户信息
SELECT * FROM user
-- 删除用户
DROP USER 'user1'@'localhost'
-- 刷新权限
FLUSH PRIVILEGES
-- 创建用户
CREATE USER 'user1'@'localhost' IDENTIFIED WITH
mysql_native_password  BY '123456'
-- 查询用户
SELECT user,host,plugin FROM user
```

MySQL的权限管理

浙江农林大学
ZHEJIANG A&F UNIVERSITY

```
-- 授权
GRANT  SELECT(snum,sname,ssex,sbirth),update,delete ON
test.s TO 'user1'@'localhost'
-- 查看用户权限
SHOW GRANTS FOR 'user1'@'localhost'
-- 收回（撤销）用户权限
REVOKE SELECT(sbirth),delete ON test.s FROM 'user1'
@'localhost'
```

小结:SQL灵活的授权机制

浙江农林大学
ZHEJIANG A&F UNIVERSITY

- 数据库管理员：
  - 拥有所有对象的所有权限
  - 根据实际情况不同的权限授予不同的用户
- 用户：
  - 拥有自己建立的对象的全部的操作权限
  - 可以使用GRANT，把权限授予其他用户
- 被授权的用户
  - 如果具有“继续授权”的许可，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用REVOKE语句收回

4.2 数据库安全性控制

浙江农林大学
ZHEJIANG A&F UNIVERSITY

4.2.1 用户标识与鉴别

4.2.2 存取控制

4.2.3 自主存取控制方法

4.2.4 授权：授予与回收

4.2.5 数据库角色

4.2.6 强制存取控制方法

4.2 数据库安全性控制

浙江农林大学
ZHEJIANG A&F UNIVERSITY

4.2.1 用户标识与鉴别

4.2.2 存取控制

4.2.3 自主存取控制方法

4.2.4 授权与回收

4.2.5 数据库角色

4.2.6 强制存取控制方法

自主存取控制缺点

浙江农林大学
ZHEJIANG A&F UNIVERSITY

- 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

4.2.6 强制存取控制方法

浙江农林大学
ZHEJIANG A&F UNIVERSITY

- 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

强制存取控制方法（续）

浙江农林大学
ZHEJIANG A&F UNIVERSITY

❖在强制存取控制中，数据库管理系统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
  - 数据库管理系统所管理的实际用户
  - 代表用户的各进程

- 客体是系统中的被动实体，受主体操纵
  - 文件、基本表、索引、视图

强制存取控制方法（续）

浙江农林大学
ZHEJIANG A&F UNIVERSITY

- 敏感度标记（Label）
  - 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，TS）
    - 机密（Secret，S）
    - 可信（Confidential，C）
    - 公开（Public，P）
    - TS>=S>=C>=P
- 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）

强制存取控制方法（续）

- 强制存取控制规则

  （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

强制存取控制方法（续）

浙江农林大学
ZHEJIANG A&F UNIVERSITY

- 强制存取控制（MAC）是对数据本身进行密级标记，无论数据如何复制，标记与数据是一个不可分的整体，只有符合密级标记要求的用户才可以操纵数据。
- 实现强制存取控制时要首先实现自主存取控制
  - 原因：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

第四章 数据库安全性

浙江农林大学
ZHEJIANG A&F UNIVERSITY

4.1 数据库安全性概述

4.2 数据库安全性控制

4.3 视图机制

4.4 审计（Audit）

4.5 数据加密

4.6 其他安全性保护

4.7 小结

4.3 视图机制

浙江农林大学
ZHEJIANG A&F UNIVERSITY

- 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

- 间接地实现支持存取谓词的用户权限定义

视图机制（续）

浙江农林大学
ZHEJIANG A&F UNIVERSITY

[例4.14] 建立计算机系学生的视图，把对该视图的SELECT权限授于王平，把该视图上的所有操作权限授于张明

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）

浙江农林大学
ZHEJIANG A&F UNIVERSITY

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

浙江农林大学
ZHEJIANG A&F UNIVERSITY

4.1 数据库安全性概述

4.2 数据库安全性控制

4.3 视图机制

4.4 审计（Audit）

4.5 数据加密

4.6 其他安全性保护

4.7 小结

4.4 审计

浙江农林大学
ZHEJIANG A&F UNIVERSITY

- 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，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

4.4 审计

- 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）

1.审计事件

- 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）

浙江农林大学
ZHEJIANG A&F UNIVERSITY

- 2.审计功能
  - 基本功能
    - 提供多种审计查阅方式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）

浙江农林大学
ZHEJIANG A&F UNIVERSITY

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（续）

- 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

审计（续）

浙江农林大学
ZHEJIANG A&F UNIVERSITY

[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

浙江农林大学
ZHEJIANG A&F UNIVERSITY

4.1 数据库安全性概述

4.2 数据库安全性控制

4.3 视图机制

4.4 审计（Audit）

4.5 数据加密

4.6 其他安全性保护

4.7 小结

4.5 数据加密

浙江农林大学
ZHEJIANG A&F UNIVERSITY

- 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

4.5 数据加密

浙江农林大学
ZHEJIANG A&F UNIVERSITY

❖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）

浙江农林大学
ZHEJIANG A&F UNIVERSITY

- 传输加密
  - 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
  - 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

数据加密（续）

浙江农林大学
ZHEJIANG A&F UNIVERSITY

- 基于安全套接层协议SSL传输方案的实现思路：
  - （1）确认通信双方端点的可靠性
    - 采用基于数字证书的服务器和客户端认证方式
    - 通信时均首先向对方提供己方证书，然后使用本地的CA 信任列表和证书撤销列表对接收到的对方证书进行验证
  - （2）协商加密算法和密钥
    - 确认双方端点的可靠性后，通信双方协商本次会话的加密算法与密钥

数据加密（续）

浙江农林大学
ZHEJIANG A&F UNIVERSITY

- （3）可信数据传输
  - 业务数据在被发送之前将被用某一组特定的密钥进行加密和消息摘要计算，以密文形式在网络上传输
  - 当业务数据被接收的时候，需用相同一组特定的密钥进行解密和摘要计算

第四章 数据库安全性

浙江农林大学
ZHEJIANG A&F UNIVERSITY

4.1 计算机安全性概述

4.2 数据库安全性控制

4.3 视图机制

4.4 审计（Audit）

4.5 数据加密

4.6 其他安全性保护

4.7 小结

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
- 隐蔽信道
  - 处理强制存取控制未解决的问题

其他安全性保护（续）

浙江农林大学
ZHEJIANG A&F UNIVERSITY

- 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等各个阶段

第四章 数据库安全性

浙江农林大学
ZHEJIANG A&F UNIVERSITY

4.1 数据库安全性概述

4.2 数据库安全性控制

4.3 视图机制

4.4 审计（Audit）

4.5 数据加密

4.6 其他安全 性保护

4.7 小结

4.7 小结

- 数据的共享日益加强，数据的安全保密越来越重要。
- 数据库管理系统是管理数据的核心，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）

- 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