第4章 数据库安全性

本章内容

- 4.1 基本原理

  概述、机制、方法
- 4.2 具体DBMS安全控制

4. 1 基本原理

4.1.1 概述

1. 概念

——防止对DB中的数据的非授权使用(避免泄露、恶意更改或破坏)。

可信计算机系统的概念和标准

三类安全性问题：

- 技术安全

  通过安全性硬件、软件对系统及数据实施保护

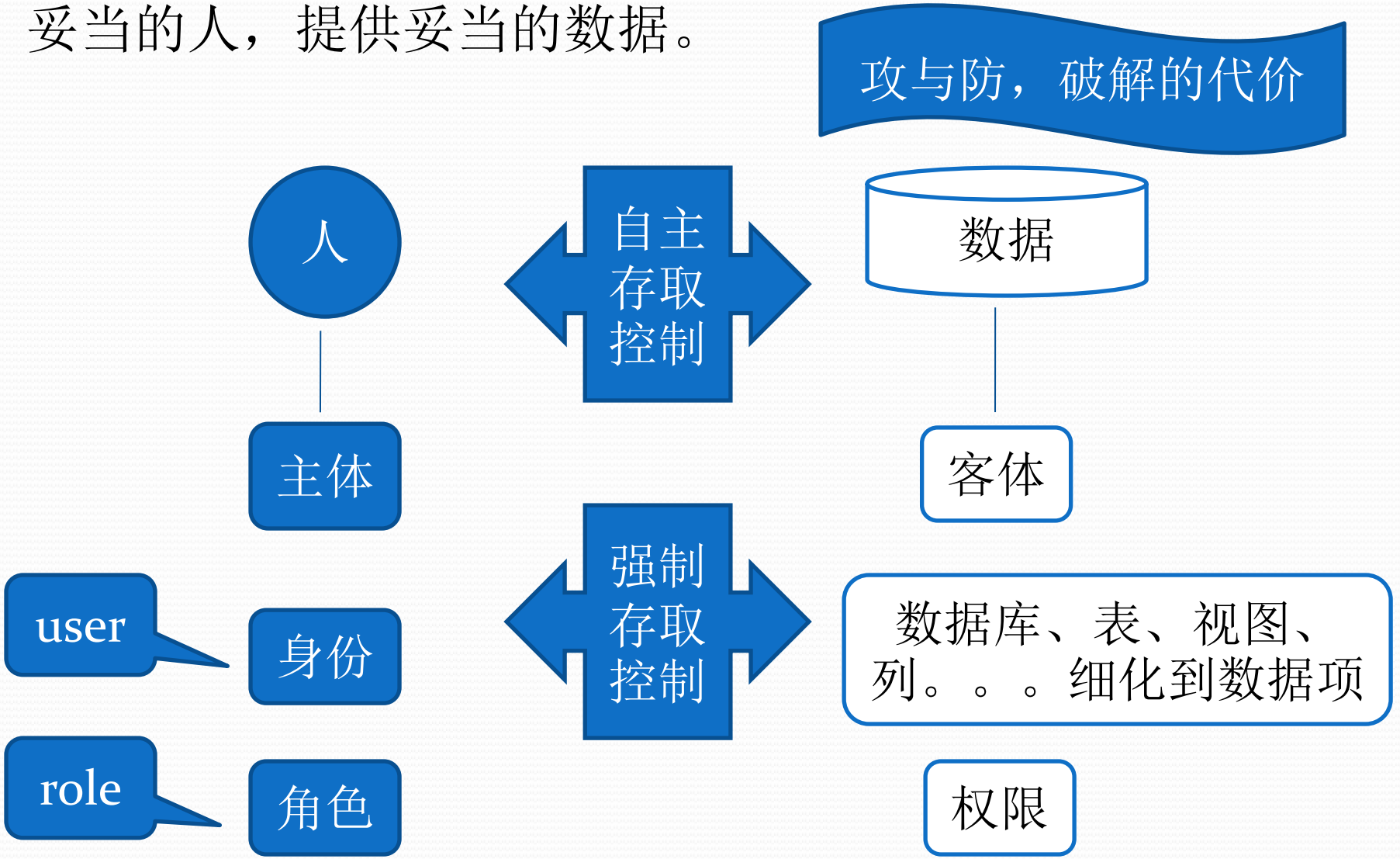
- 管理安全

  日常运行维护中对故障、意外的响应和管理机制

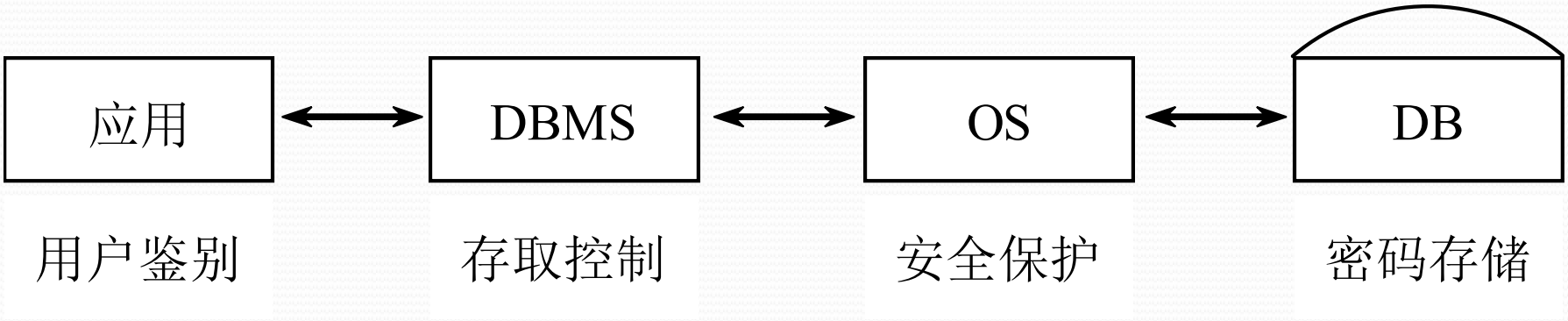
- 政策法律

  制定有关计算机犯罪、数据安全保密的法律准则

对数据安全的理解：在妥当的时刻，以妥当的形式，向妥当的人，提供妥当的数据。

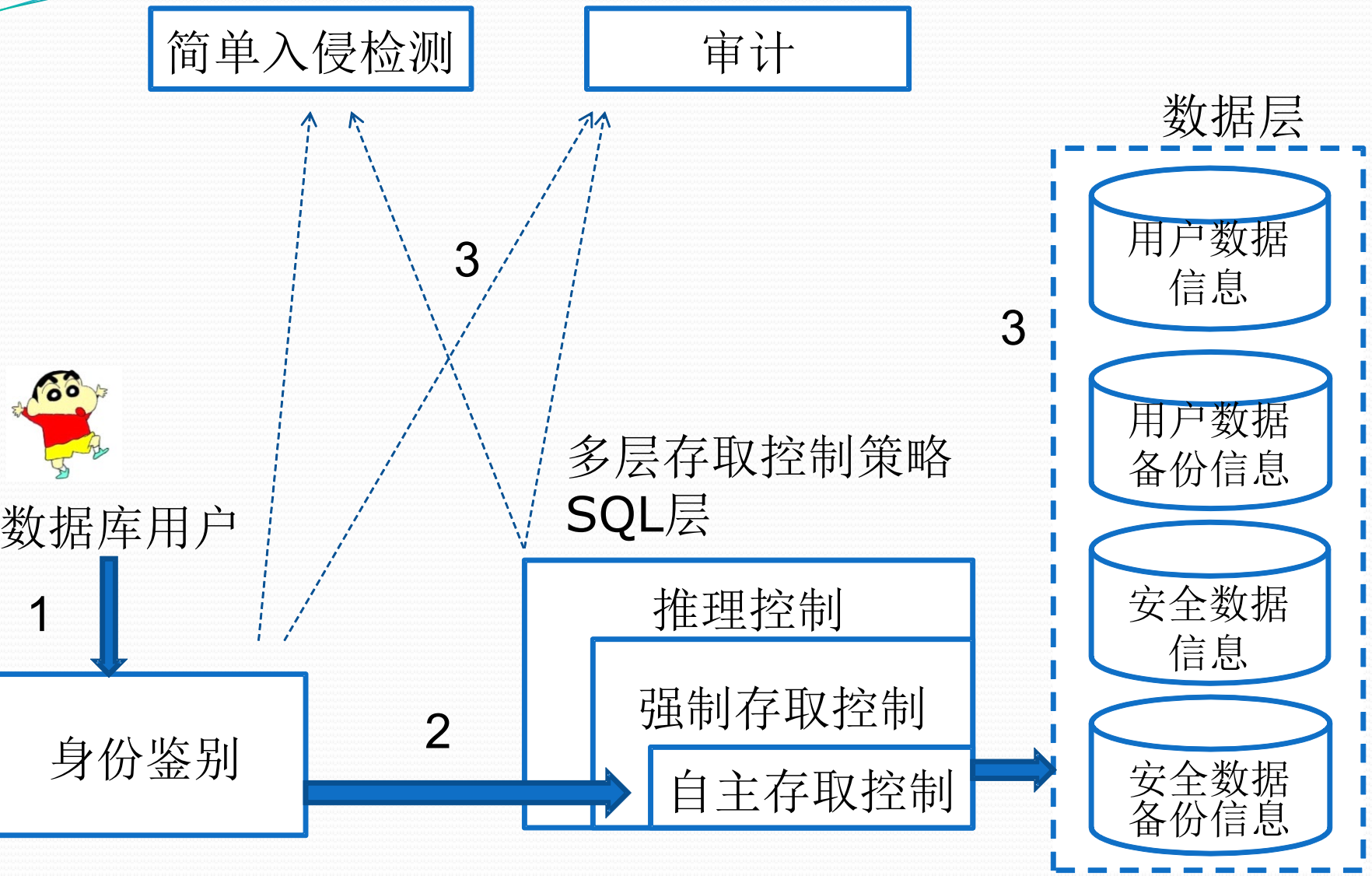


2. 计算机系统安全控制机制



3. DBS中的一般方法

1) 用户鉴别　2) 存取控制　3) 密码存储


简单入侵检测
审计
数据层
3
3
用户数据信息
用户数据备份信息
安全数据信息
安全数据备份信息
多层存取控制策略
SQL层
数据库用户
1
推理控制
强制存取控制
自主存取控制
2
身份鉴别

4.1.2 安全标准简介

桔皮书

- 最具影响力的两个标准：TCSEC和CC标准。

TCSEC(Trusted Computer System Evaluation Criteria)，美国国防部颁布。

欧洲的ITSEC信息技术安全评估准则

加拿大的CTCPEC可信计算机产品评估准则

美国的FC信息技术安全联邦标准草案

上述标准的发起组织联合发起了CC(Common Criteria)项目，产生了CC通用准则，被ISO作为国际标准，也是中国的国家标准。

安全标准简介

TCSEC(桔皮书)

《可信计算机系统评估准则关于可信数据库系统的解释》，TDI(Trusted Database Interpretation,紫皮书)

安全级别	定义
A1 (高)	被验证的设计（系统的形式化设计和验证）
B3	具有安全域（访问监控器、审计追踪能力、系统恢复过程）
B2	结构化保护（形式化的安全策略模型，全面DAC/MAC）
B1	标记安全保护（对被标记对象实施MAC）
C2	受控的存取保护（将C1级细化，实施审计 、资源隔离）
C1	自主安全保护
D (低)	最小保护，区别于其他级别

Discretionary

Mandatory

4.2 数据库安全控制机制

4. 2.1 用户身份鉴别

1） 口令

用户名	用户标识	……

口令是常用的一种用户标识手段

① 静态口令

② 动态口令

短信密码、动态令牌

③ 口令时限

2） 可读身份标识

①生物特征

声波、指纹、签名、图像（视网膜、人脸）

②智能卡

个人身份识别码（PIN）+智能卡

4. 2.2 存取访问控制

——防止非授权访问。

1)用户权限定义

生成安全规则或者授权规则。

用户名	数据对象名	操作类型	其它

数据对象名：模式、子模式、表、索引、视图、属性 (不同粒度)

操作类型： Create, Select, update, insert, all

其它： 如操作时间、范围，…

2）用户权限的检查

DBMS查找数据字典，并控制用户的存取权限。

上述这两部分合起来可以作为DBMS的一个安全子系统。

存取控制分为自主存取控制和强制存取控制，其中强制存取控制的安全级别较高。

自主存取控制（DAC，Discretionary）：不同的用户有不同的存取权限，而且用户可以自主的将自己的权限授予其它用户。

强制存取控制（MAC，Mandatory）： 依据密级实施权限控制。

相关概念（主体、客体、许可证级别、敏感度标记）

强制存取控制适用于对资料有严格而固定密级分类的部门。“资料”对象被标定以相应的保密级别，每个用户被授予相应每个保密级别的许可证。

强制存取控制的读写规则：用户只能

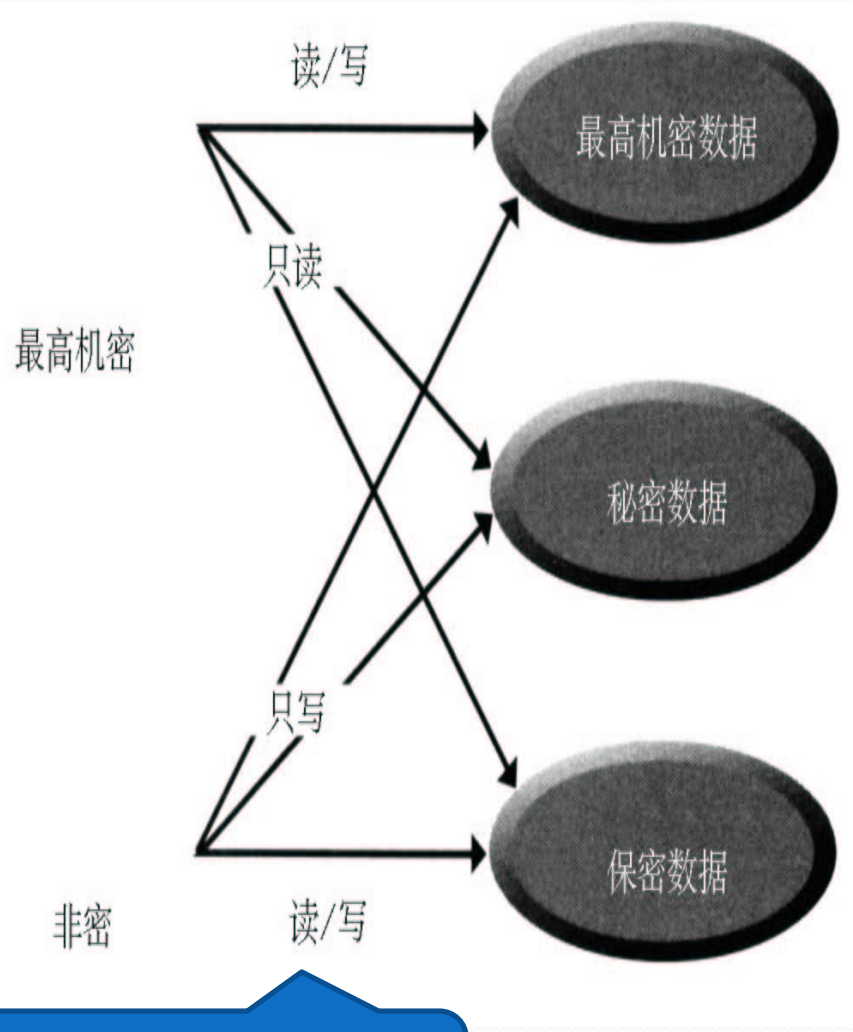
1）**读取**保密级别**小于或者等于**自身许可证级别的资料；

2）**修改**保密级别**大于或者等于**自身许可证级别的资料。

强制存取控制中密级标记和数据是不可分割的整体。

强制存取控制原理：

最高密级主体

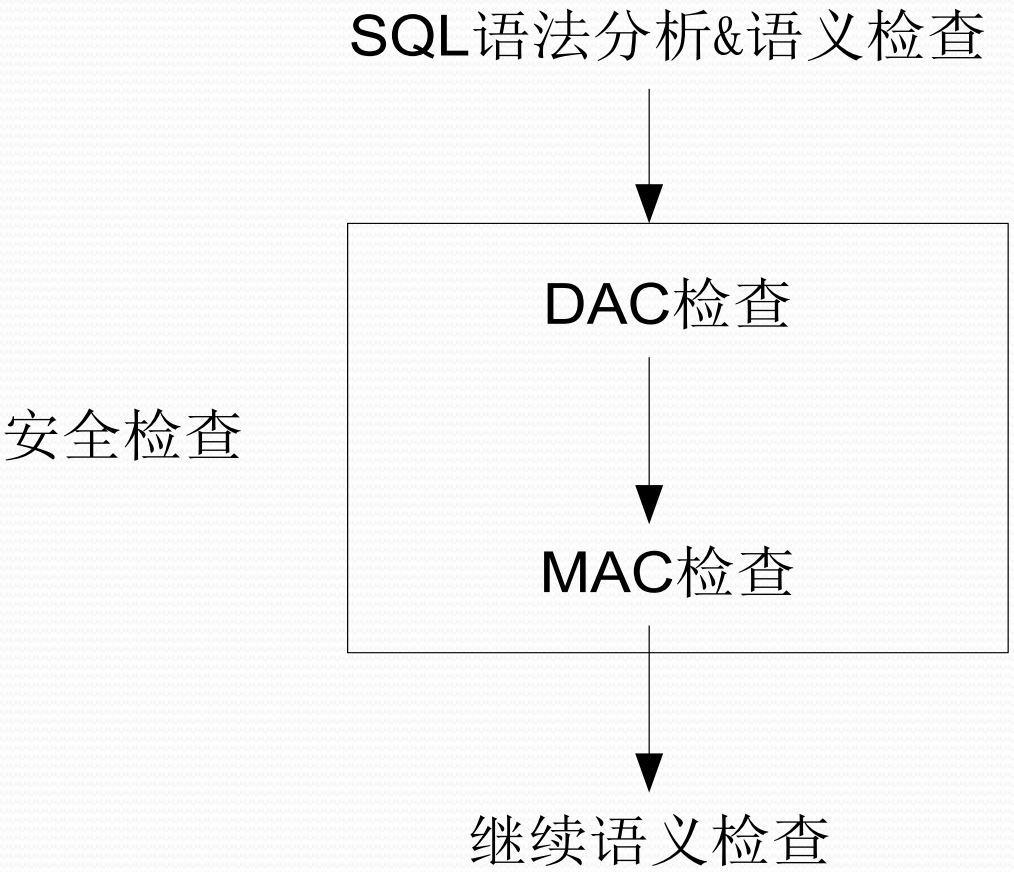


最低密级主体

防止信息泄露

系统设计原则（遵循安全保密标准）：

较高安全级别的数据保护要包含较低级别的所有保护，所以在实现强制存取控制（MAC，Mandatory）时首先要实现自主存取控制（DAC，Discretionary）



4.2.3 授权（Authorization）与回收

1）授权语句

grant 权限[，权限]...[on 对象类型　对象名] to 用户[，用户]...

[with grant option];

①权限：select, update, delete, alter, create index, create table, All,……

②对象名：关系名，视图名，db名

③对象类型：table, view，db

④with grant option:选用则表示可将它所拥有的权力转授其它用户。

⑤ 用户：用户名/public——所有用户。

⑥ 权限分配：

基本表	Select	Insert	update	Delete	CREATE INDEX	ALTER
视图	Select	Insert	update	Delete		ALTER
属性	Select	Insert	update	Delete		ALTER
DB	Create Table					
All Privileges . . .不同商用系统不尽相同						

例①：将student表的查询权授予所有用户

grant select on table student to public

例②：将student关系的所有权限授予用户1

grant all on table student to 用户1

例③：将对student的 delete 授予用户2，并给其再授权的权限

grant delete on table student to user2 with grant option

一个特殊的例子：为每位职工赋予查询自己信息的权限

GRANT SELECT ON TABLE 职工

WHEN USER( ) = NAME TO ALL; //某些DBMS支持

2）权力撤消

revoke 权力1[，权力2]...[on 对象类型 对象名]
from 用户1[，用户2]...[cascade|restrict]

若使用Restrict选项，且user2曾转授delete权限给其他人，则从user2处revoke失败。

例1：撤消user 2 对student表的delete 权力

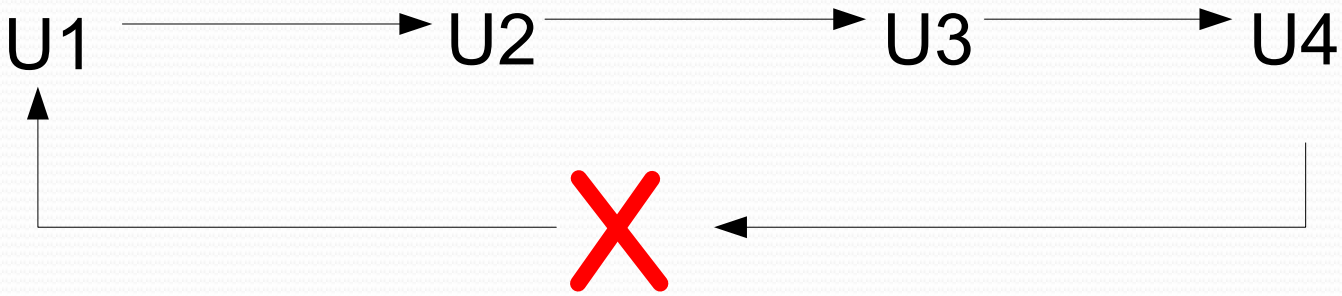
```
revoke delete on table student from user2
cascade;
```

若 user2 将delete权限转授u3，则u3被user2转授的该delete权限连带收回，但如果u3另外还从其他人获得该delete权限，则u3仍然拥有此权限，revoke只收回直接或间接从user2处获得的权限。

例2：撤消user 2 对student表sno属性的修改权限

```
revoke update(sno) on table student from user2;
```

SQL标准允许具有WITH GRANT OPTION的用户把相应权限传递授予其他用户，但是不允许循环授权。



? 影响祖先，不可控，安全性不可验证

关于角色的SQL语句

- 创建角色

  create role <角色名>

- 给角色授权

  grant <权限>[, <权限>]…
  on <对象类型> 对象名
  to <角色>[, <角色>]…

- 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>]…

- 将角色授予其他角色或用户

  grant <角色1>[, <角色2>]…
  to <角色3>[, <用户1>]…
  [with admin option]

例：创建角色R1

CREATE ROLE R1;

例：将对student表的查询、修改、插入权限赋予角色R1。

GRANT SELECT,UPDATE,INSERT ON TABLE STUDENT TO R1;

例：将R1角色授予用户李明和角色R2，并允许他们转授相应的权限。

GRANT R1 TO 李明, R2

WITH ADMIN OPTION

例：将R1角色从用户李明收回

REVOKE R1 FROM 李明

4.3 视图机制

通过外模式实现安全控制

4.4 审计控制

——对用户使用系统资源(Hardware、Software)情况的登记和审查，一般是基于审计日志，是DBMS达到C2级所必备的功能要求。

一种事后检查的
安全机制，增加运行开销

1. 功能

1) 设备安全审计

主要审查系统资源的安全策略、各种安全保护措施、故障恢复计划等。

2) 操作审计

各种操作的记录、分析(事务、操作类型、用户、终端、操作时间、审计时间、...)

审计事件的类别：

服务器事件（启动、停止、配置文件重新加载）、

系统权限（对系统拥有的结构、模式对象进行操作的审计）、

语句事件（DDL、DML、DCL）、

模式对象事件（针对特定模式对象上进行的sql语句的审计）

例：审计对SC关系的表结构修改和数据更新操作

AUDIT ALTER,UPDATE ON SC;

例：停止对SC关系的表结构修改和数据更新操作的审计

NOAUDIT ALTER,UPDATE ON SC;

3) 应用审计

应用系统功能、控制逻辑、数据流正确与否的审计。

4) 攻击审计

已发生攻击操作及危害系统安全事件的检测和审计。

2. 技术

1) 静态技术

利用软件设计说明书、流程图分析，明确易被攻击的环节。

2) 动态技术

实际运行测试(控制逻辑，...)

性能测试(测试用例、仿真程序)

3) 结果分析

数据的选择、收集和分析。

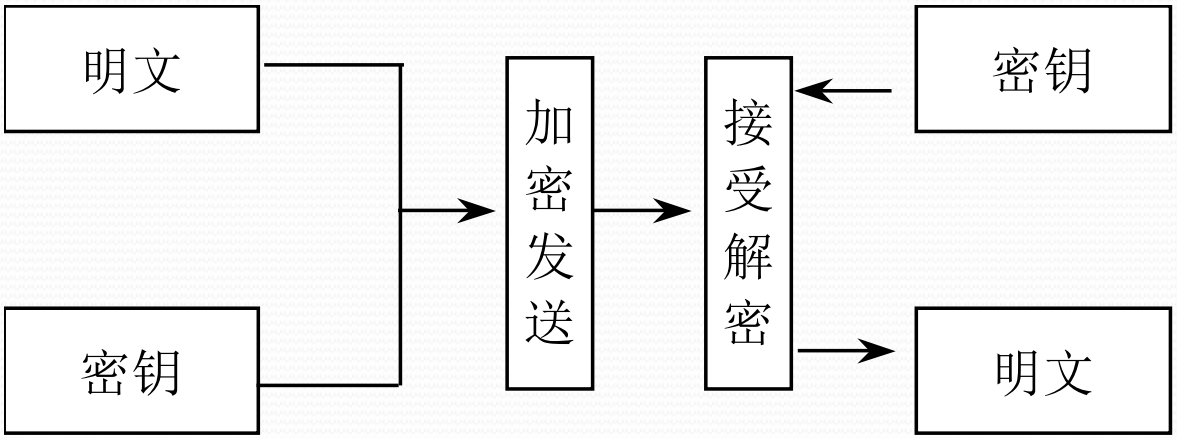
审计分析和报表、审计日志管理、审计设置、专门的审计视图

4. 5 数据加密

——以密码文形式存储和传输数据(只有知道密钥的用户才能访问)。

1. 处理流程

处理流程如下图所示：



2. 加密方法

1. 信息编码　2. 信息换位　3. 信息转换(密钥)

基于安全套接层协议（Security Socket Layer, SSL）的可信传输方案，一种端到端的传输加密方式。

——每次会话采用一个秘钥。

五个步骤：

1）创建连接（可信）；

2）基于数字证书认证（Certificate Authority, CA）双方互发自己的CA证书，确认对方通信端点的可靠性；

3）协商加密算法和秘钥，在此过程中利用公钥基础设施（Public Key Infrastructure, PKI）方式保证协商过程通信的安全可靠；

4）可信传输数据（密文+消息摘要，一次通讯一秘钥）；

5）关闭可信连接。

4.6 其他安全保护

4.6.1 推理控制（inference control, 统计安全性）

统计数据库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。

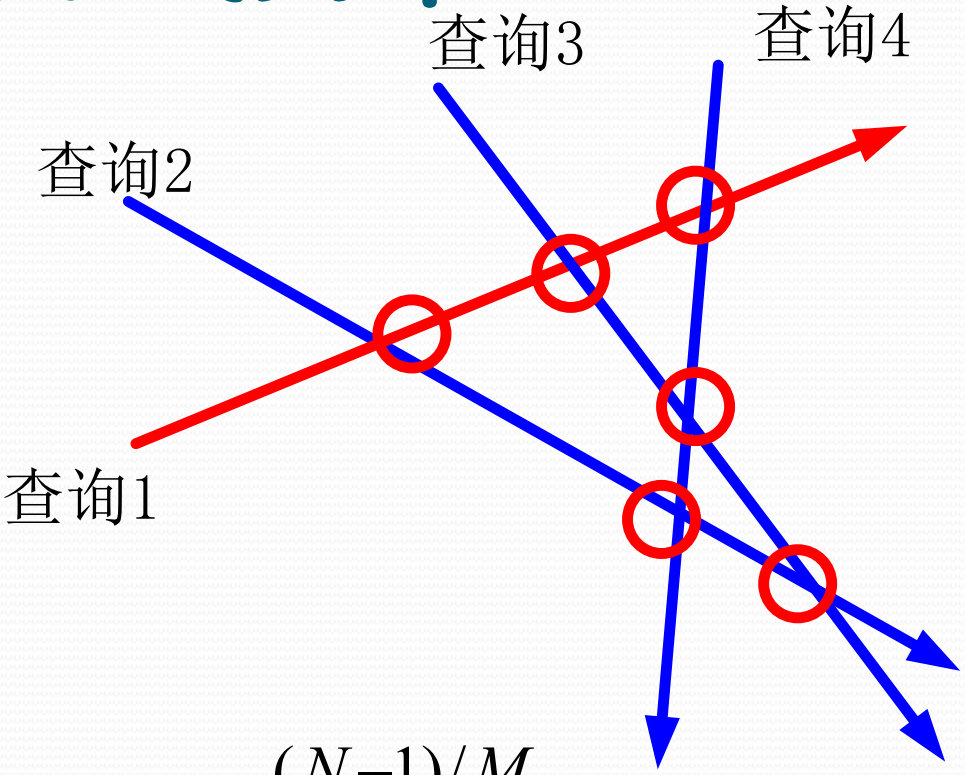
问题：存在隐蔽的信息通道可获得单个记录信息，例如由人数、最高值、总额、查询数据项的交集推算出个体信息。

解决办法：
规则1：查询至少要涉及N个以上记录。
规则2：任意两次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。

无法防止两个用户合作。

新的安全技术：隐私（标识信息、敏感信息、位置信息）保护。

如何理解3条规则？



欲求y，需有查询形如 $y + \sum_{i=1}^{(N-1)/M} A_i$

需有另外(N-1)/M次查询包含各个A_i，N-2？

4.6.2 隐蔽信道（covert channal）

约定信息的隐蔽传递方式可导致泄密。

例：甲乙双方约定向设置了主码的关系插入同一条记录，甲通过是否先插入来传递“有”或者“无”的信号，乙再其后插入同一条记录时通过能否成功插入即可获知甲的消息。

又例如通过CPU是否繁忙、系统的信号频率、电压的变化传递信息。

有专用保密插座

4.1.7.3 数据隐私（data privacy）保护

出于某种社会或科研需求的原因需要发布数据，但又要保护数据中涉及到的个人的隐私，相关技术有k-匿名，l-多样化等等。

定义1（*k*-匿名） 设PT(tid,A_{C1}, A_{C2},…, A_{Cm}, A_{N1}, A_{N2},…, A_{Nn}, s)是数据库表，属性集合{A_{C1}, A_{C2},…, A_{Cm}, A_{N1}, A_{N2},…, A_{Nn}}为准标识符属性，s为敏感属性，将PT划分为簇{C_1, C_2,…, C_p}, $|C_i| \geq k$, $1 \leq i \leq p$, C_i中的元组在各个A_i上有相同的值，则数据表PT满足k-匿名原则。

定义2（*l*-多样性） 设PT= $\sum_{i=1}^{p} C_i$ 是一个给定的数据集，

$|C_i| \geq l$， $|C_j| \geq l$， $C_i \cap C_j = \phi$ ， $1 \leq i \neq j \leq p$， s是簇C_i中最频繁的敏感值，$Num_{Ci}(s)$是簇C_i中敏感值s的个数。若$\forall C_i$ ，均有$Num_{Ci}(s) \geq l$，则数据集PT满足l-多样性原则。

案例分析：数据库安全问题频发

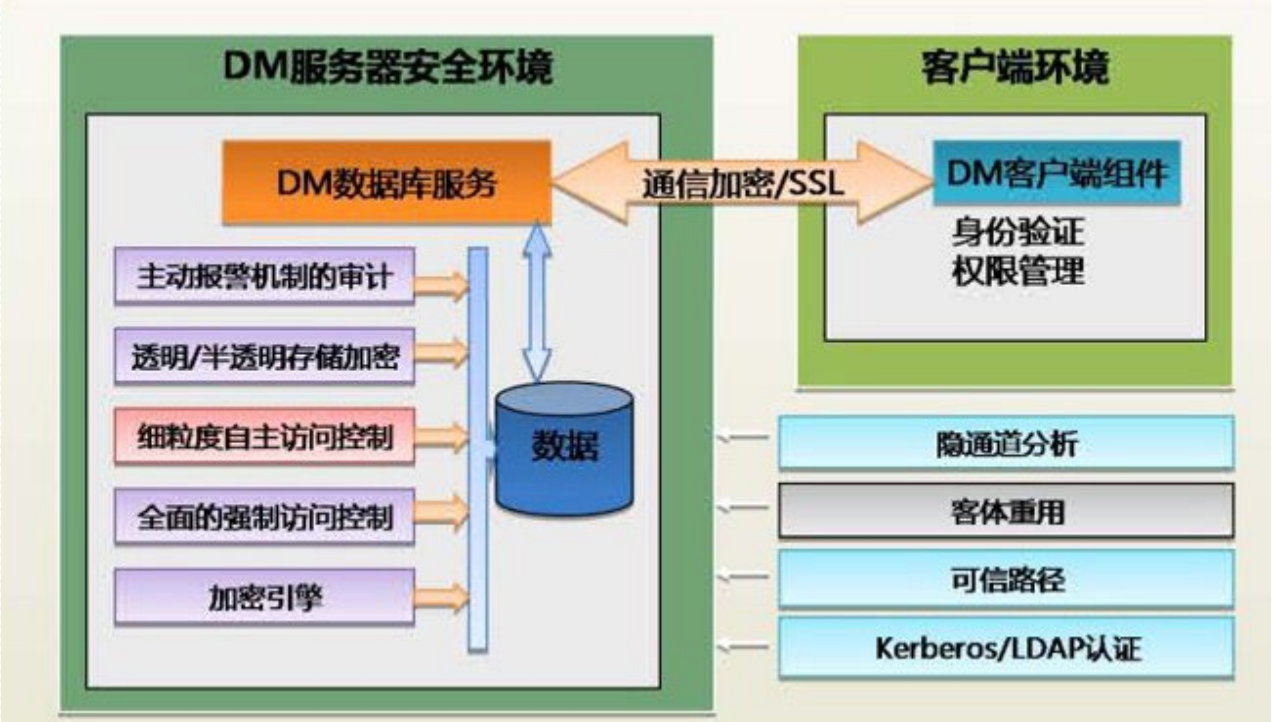
- 实例：Oracle数据库受到网络病毒攻击
- 现象：数据库遭遇重启失败（图为报错现场）

```
Total System Global Area  776646656 bytes
Fixed Size                  2257272 bytes
Variable Size             507514504 bytes
Database Buffers          264241152 bytes
Redo Buffers                2633728 bytes
Database mounted.
ORA-01092: ORACLE instance terminated. Disconnection forced
ORA-00704: bootstrap process failure
ORA-00704: bootstrap process failure
ORA-00600: internal error code, arguments: [16703], [1403], [20], [], [], [],
[], [], [], [], [], []
Process ID: 7425
Session ID: 1 Serial number: 5
```


数据库恶意注入攻击

- 原因查找：
  - Tab$中数据被清空，导致数据库启动时一致性检查失败；
  - 进一步定位：发现客户数据库中存在3个恶意存储过程和2个恶意触发器。

国产数据库-达梦数据库安全版（拓展学习）



达梦数据库安全版-安全体系结构图

数据库是数字产业的核心引擎，研发具有自主知识产权的基础软硬件设施，构建国产自主IT底层生态，是数字信息安全的底座，也是产业数字化转型的关键。

客体重用机制使DBMS能够清扫被重分配的系统资源，以保证数据信息不会因为资源的动态分配而泄露给未授权的用户。

国产数据库-openGauss安全机制 （拓展学习）

openGauss作为新一代自治安全数据库，提供了丰富的数据库基础安全能力，涵盖了访问登录认证、用户权限管理、审计与追溯及数据安全隐私保护等。

慕课讨论题

- 强制存取控制有哪些应用背景和系统需求？

什么样的数据库系统需要强制访问控制？具有强制存取控制的DBMS系统是否可以不需要自主存取控制能力？请论述原因。