

数据库安全性

2020年4月16日

数据库安全性 – 问题的提出

* 数据库特点：数据共享

1. 数据共享所引发的数据库安全问题
2. 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 – 基本概念

- * 由DBMS统一提供数据库的**数据保护**功能
 - * 保证数据库内数据的**安全可靠和正确有效**
 - * **安全性**：防止因用户非法使用数据库造成数据泄露、更改或破坏。
 - * **完整性**：防止出现不正确的数据（不符合语义的数据）
- * 共享的庞大数据的安全问题尤为重要！
- * 系统安全保护措施是否有效，是数据库系统的重要技术指标之一。

主要内容

- 一 计算机安全性概论
- 二 数据库安全性控制
- 三 统计数据库安全性
- 四 小结

三类安全性问题
安全标准简介

1.1 三类安全性问题 - 基本概念

* 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。

* 计算机安全涉及：

- * 计算机系统本身的技术问题、管理问题、.....
- * 法学、犯罪学、心理学、.....

1.1 三类安全性问题

- * 技术安全类

- * 采用具有一定安全性的硬件、软件来实现对计算机系统及其所存数据的安全保护，当计算机系统受到无意或恶意的攻击时仍能保证系统正常运行，保证系统内的数据不增加、不丢失、不泄露。

- * 管理安全类

- * 政策法律类

1.2 安全标准简介

- * TCSEC (桔皮书)
 - * 1985年美国国防部（DoD）正式颁布《DoD可信计算机系统评估准则》（简称TCSEC或DoD85）
- * TDI (紫皮书) – 将TCSEC扩展到DBMS
 - * 1991年4月美国NCSC（国家计算机安全中心）颁布了《可信计算机系统评估标准关于可信数据库系统的解释》（Trusted Database Interpretation 简称TDI）
- * CC – 目前已基本取代TCSEC
 - * 1993年，为满足全球IT市场互认标准化安全评估结果的需要，合成一组单一的、能被广泛使用的IT安全准则。于2001年被我国采纳为国家标准。
 - * 特点：结构开放，表达方式通用

1.2 安全标准简介 - TCSEC

- * 桔皮书
- * TCSEC的目的
 - * 提供一种标准，使用户可以对其计算机系统内敏感信息安全操作的可信程度做评估；
 - * 给计算机行业的制造商提供一种可循的指导规则，使其产品能够更好地满足敏感应用的安全需求。

1.2 安全标准简介 - TDI

- * 紫皮书
- * TDI: 将TCSEC扩展到数据库管理系统。
- * TDI中定义了数据库管理系统设计与实现中需满足和用以进行安全性级别评估的标准。

1.2 安全标准简介 – TCSEC/TDI – 1

- * 从四个方面来描述安全性级别划分的指标
 - * 安全策略
 - * 自主存取控制、客体重用、标记、强制存取控制
 - * 责任
 - * 标识与鉴别、审计
 - * 保证
 - * 操作保证、生命周期保证
 - * 文档
 - * 安全特性用户指南、可信设施手册、测试文档、设计文档、等

1.2 安全标准简介 – TCSEC/TDI – 2

* 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）

1.2 TCSEC/TDI – 安全级别说明

- * 四组(division)七个等级
 - * A (A1)
 - * B (B1, B2, B3)
 - * C (C1, C2)
 - * D
- * 按系统可靠或可信程度逐渐增高
- * 安全级别之间可向下兼容。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，且提供更多或更完善的保护能力。

1.2 安全级别说明 - D级

A (A1)
B (B1、B2、B3)
C (C1、C2)
D

- * 将一切不符合更高标准的系统均归于D组
- * 典型例子：DOS是安全标准为D的操作系统
 - * 在安全性方面几乎没有什么专门的机制来保障

1.2 安全级别说明 – C级

A (A1)
B (B1、B2、B3)
C (C1、C2)
D

* C1级

- * **非常初级的自主安全保护**

- * 实现对用户和数据的分离，进行自主存取控制（DAC），保护或限制用户权限的传播。

* C2级

- * **安全产品的最低档次**

- * 提供受控的存取保护，将C1级的DAC进一步细化，以个人身份注册负责，并实施审计和资源隔离

- * 达到C2级的产品在其名称中往往不突出“安全” (Security)这一特色

- * 如，Windows 2000，Oracle 7

1.2 安全级别说明 – B级

A (A1)
B (B1、B2、B3)
C (C1、C2)
D

* B1级

- * **标记安全保护**。可称为：“安全”或“可信的”产品。
- * 对系统的数据加以标记，对标记的主体和客体实施强制存取控制（MAC）、审计等安全机制
- * **Trusted** Oracle 7, **Secure** SQL Server version 11.0.6,

1.2 安全级别说明 – B级（续）

A (A1)
B (B1、B2、B3)
C (C1、C2)
D

* B2级

- * **结构化保护**。建立形式化的安全策略模型并对系统内的所有主体和客体实施DAC和MAC。
- * 经过认证的B2级以上的安全系统较少。

* B3级

- * **安全域**。该级的TCB必须满足访问监控器的要求，审计跟踪能力更强，并提供系统恢复过程。

1.2 安全级别说明 - A级

A (A1)
B (B1、B2、B3)
C (C1、C2)
D

* A1级

- * **验证设计**，即提供B3级保护的同时，给出系统的形式化设计说明和验证，以确信各安全保护真正实现。

* B2以上的系统





- * 还处于理论研究阶段
- * 应用多限于一些特殊的部门，如军队等
- * 目前也有研究机构正在大力发展安全产品，试图将目前仅限于少数领域应用的B2安全级别下放到商业应用中来，并逐步成为新的商业标准。

1.2 安全标准简介 – 各安全级别对安全指标的支持情况

表 9.2 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 and 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																							

1.2 安全标准简介 – 各安全级别对安全指标的支持情况 – 符号说明

	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

主要内容

- 一 计算机安全性概论
- 二 数据库安全性控制
- 三 统计数据库安全性
- 四 小结

概述

用户身份鉴别

存取控制

自主存取控制

数据库角色

强制存取控制

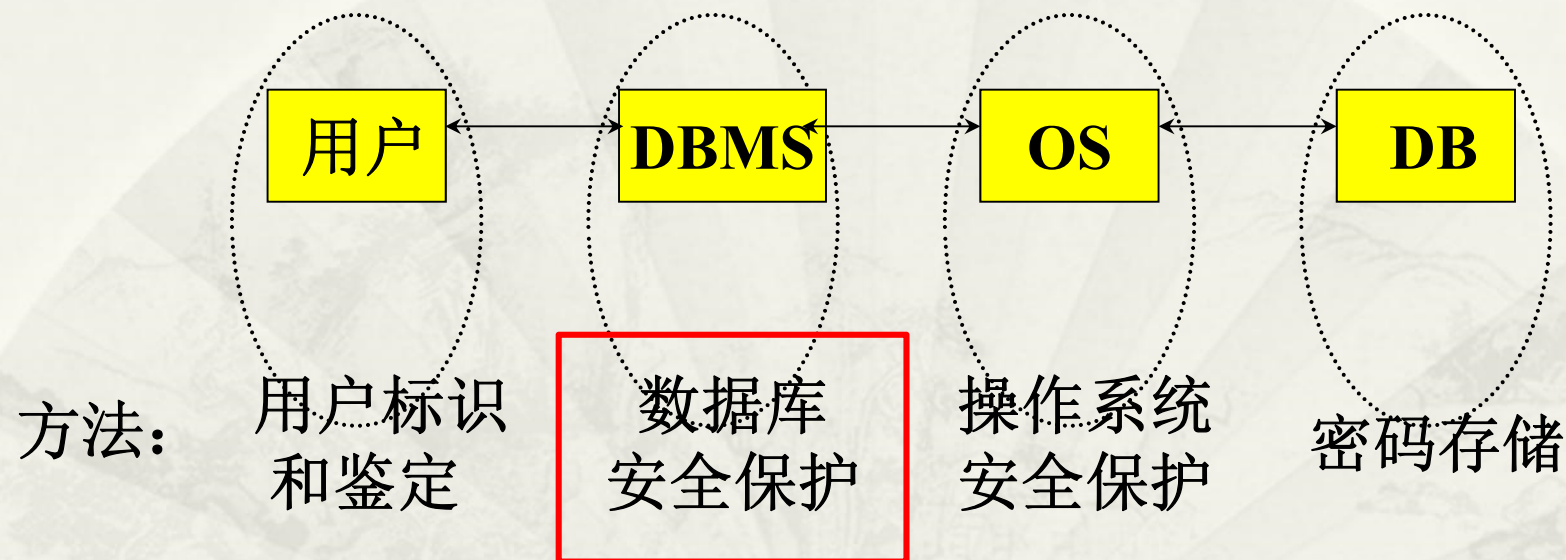
视图机制

审计

数据加密

2.1 数据库安全性控制概述

* 计算机系统的安全模型



2.1 数据库安全性控制概述

- * 非法使用数据库
 - * 编写程序，非法操作数据库
- * 通过多次合法操作，导出保密数据
 - * 统计数据库中，通过有意识多次组合，导出个人数据，或其他保密数据
- * 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、.....

2.2 用户身份鉴别

- * 系统提供的**最外层安全保护措施**
- * 基本思路
 - * 系统提供一定的方式让用户标记自己的名字或身份。用户登录时系统进行核对。
- * 常用方法
 - * 用户标识 UID
 - * 口令
 - * 静态口令、动态口令
 - * 验证码（防止恶意登录）
 - * 生物特征鉴别、智能卡鉴别、.....

2.3 存取控制

- * 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
- * 定义存取权限，并存入数据字典
 - * 预先定义每个用户对库内数据对象的操作权限。是管理问题，而不是技术问题。
- * 合法权限检查
 - * 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。

2.3 存取控制 – 常用方法

A (A1)
B (B1、 B2、 B3)
C (C1、 C2)
D

- * 自主存取控制DAC (Discretionary Access Control)

- * C2级

- * 灵活

- * 强制存取控制MAC (Mandatory Access Control)

- * B1级

- * 严格

2.3 存取控制 – 自主存取控制DAC

- * 同一**用户**对于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

2.3 存取控制 – 强制存取控制MAC

- * 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

2.4 自主存取控制方法 – DAC

- * 定义存取权限
 - * 用户权限的两个要素；SQL语句；授权表
- * 检查存取权限
- * 授权粒度
- * 与数据值有关的授权
- * DAC的优缺点

2.4 DAC – 定义存取权限（授权）

- * 用户权限的两个要素
 - * 数据库对象：数据库、模式、表、视图、索引、属性列、.....
 - * 操作类型：建立、查找、插入、修改、删除
- * 授权与回收
 - * SQL语句：GRANT/REVOKE
 - * 非技术问题

2.4 DAC – 定义存取权限 – RDBS的存取权限

对象类型	对象	操作类型
数据库	模式SCHEMA	<i>CREATE</i>
	基本表TABLE	<i>CREATE、ALTER</i>
模式	视图VIEW	<i>CREATE</i>
	索引INDEX	<i>CREATE</i>
数据	基本表和视图	<i>SELECT、INSERT、UPDATE、DELETE、REFERENCES、ALLPRIVILEGES</i>
数据	属性列	<i>SELECT、INSERT、UPDATE、REFERENCE、ALLPRIVILEGES</i>

2.4 DAC – 定义存取权限 – SQL语句

- * **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];
- * 将对指定操作对象的指定操作权限授予指定的用户。
- * 发出命令者：DBA、该对象创建者、已拥有权力的用户

2.4 DAC – 定义存取权限 – SQL语句

- * **GRANT *SELECT* ON *TABLE Student* TO *U1*;**
- * **GRANT *ALL PRIVILEGES***
ON *TABLE Student, Course* TO *U2,U3*;
- * **GRANT *SELECT***
ON *TABLE SC* TO *PUBLIC*;
- * **GRANT *UPATE(Sno), SELECT***
ON *TABLE Student* TO *U4*;
- * **GRANT *INSERT* ON *TABLE SC***
TO *U5* *WITH GRANT OPTION*;
- * **GRANT *INSERT* ON *TABLE SC***
TO *U6* *WITH GRANT OPTION*;
- * **GRANT *INSERT* ON *TABLE SC* TO *U7*;**

2.4 DAC – 定义存取权限 – 用户授权表

授权用户名	被授权用户名	数据库对象	允许操作	能否转授权
DBA	U1	关系Student	SELECT	No
DBA	U2	关系Student	ALL	No
DBA	U2	关系Course	ALL	No
DBA	U3	关系Student	AL	No
DBA	U3	关系Course	ALL	No
DBA	PUBLIC	关系SC	SELECT	No
DBA	U4	关系Student	SELECT	No
DBA	U4	属性列S.Sno	UPDATE	No
DBA	U5	关系SC	INSERT	Yes
U5	U6	关系SC	INSERT	Yes
U6	U7	关系SC	INSERT	No

2.4 DAC – 定义存取权限 – SQL语句

- * **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];
- * 将指定的用户对指定操作对象的指定操作权限收回。

2.4 DAC – 定义存取权限 – REVOKE

- * **REVOKE *UPDATE(Sno)***
ON *TABEL Student* FROM *U4*;
- * **REVOKE *SELECT***
ON *TABLE SC* FROM *PUBLIC*;
- * **REVOKE *INSERT***
ON *TABLE SC* FROM *U5* *CASCADE*;

2.4 DAC – 定义存取权限 – 用户授权表 – 收回部分授权后的表格

授权用户名	被授权用户名	数据库对象	允许操作	能否转授权
DBA	U1	关系Student	SELECT	No
DBA	U2	关系Student	ALL	No
DBA	U2	关系Course	ALL	No
DBA	U3	关系Student	AL	No
DBA	U3	关系Course	ALL	No
DBA	PUBLIC	关系SC	SELECT	No
DBA	U4	关系Student	SELECT	No
DBA	U4	属性列S.Sno	UPDATE	No
DBA	U5	关系SC	INSERT	Yes
U5	U6	关系SC	INSERT	Yes
U6	U7	关系SC	INSERT	No

2.4 DAC – 检查存取权限

- * 对于获得上机权后又进一步发出存取数据库操作的用户
 - * DBMS查找数据字典（系统目录），根据其存取权限对操作的合法性进行检查
 - * 若用户的操作请求超出了定义的权限，系统将拒绝执行此操作

2.4 自主存取控制 – 授权粒度

- * 授权粒度：可以定义的数据对象的范围
 - * 衡量授权机制灵活性的一个重要指标。
 - * 数据对象的粒度越细，即可以定义的数据对象的范围越小，授权子系统就越灵活。
- * 关系数据库授权粒度
 - * 数据库、表、属性列、行
 - * 能否提供与数据值有关的授权？
 - * 授权子系统的精巧程度

2.4 自主存取控制 – 存取谓词 – 补充

* 实现与数据值有关的授权

- * 存取谓词可以很复杂

- * 可以引用系统变量，如终端设备号，系统时钟等，实现与时间地点有关的存取权限，这样用户只能在某段时间内，某台终端上存取有关数据。

- * 例：规定“教师只能在每年1月份和7月份星期一至星期五上午8点到下午5点处理学生成绩数据”。

2.4 自主存取控制-存取谓词 – 补充 – 例

例：扩充后的授权表

用户名	数据对象名	允许的操作类型	存取谓词
王平	关系Student	SELECT	Sdept='CS'
张明霞	关系Student	UPDATE	Sname='张明霞'
张明霞	关系 Course	ALL	空

2.4 自主存取控制 – 创建数据库模式的权限

- * **CREATE USER** <username> [WITH]
[DBA|RESOURCE|CONNECT] ;
- * 只有系统的超级用户才有权创新一个新的数据库用户。
- * 新创建的用户权限： DBA、RESOURCE、CONNECT（默认）
- * RESOURCE权限的用户可以创建基本表和视图。
- * DBA权限的用户为超级用户。
- * 注：该命令不是SQL标准。

2.4 自主存取控制 - 小结

- * 定义存取权限：用户
- * 检查存取权限：DBMS
- * 授权粒度：即数据对象粒度，数据库、表、属性列、行
- * 数据值粒度：存取谓词
 - * 授权粒度越细，授权子系统就越灵活，能够提供的安全性就越完善。
 - * 但是，因数据字典变大变复杂，系统定义与检查权限的开销也会相应地增大。
- * 数据库模式的创建权限

2.4 自主存取控制 – 优缺点

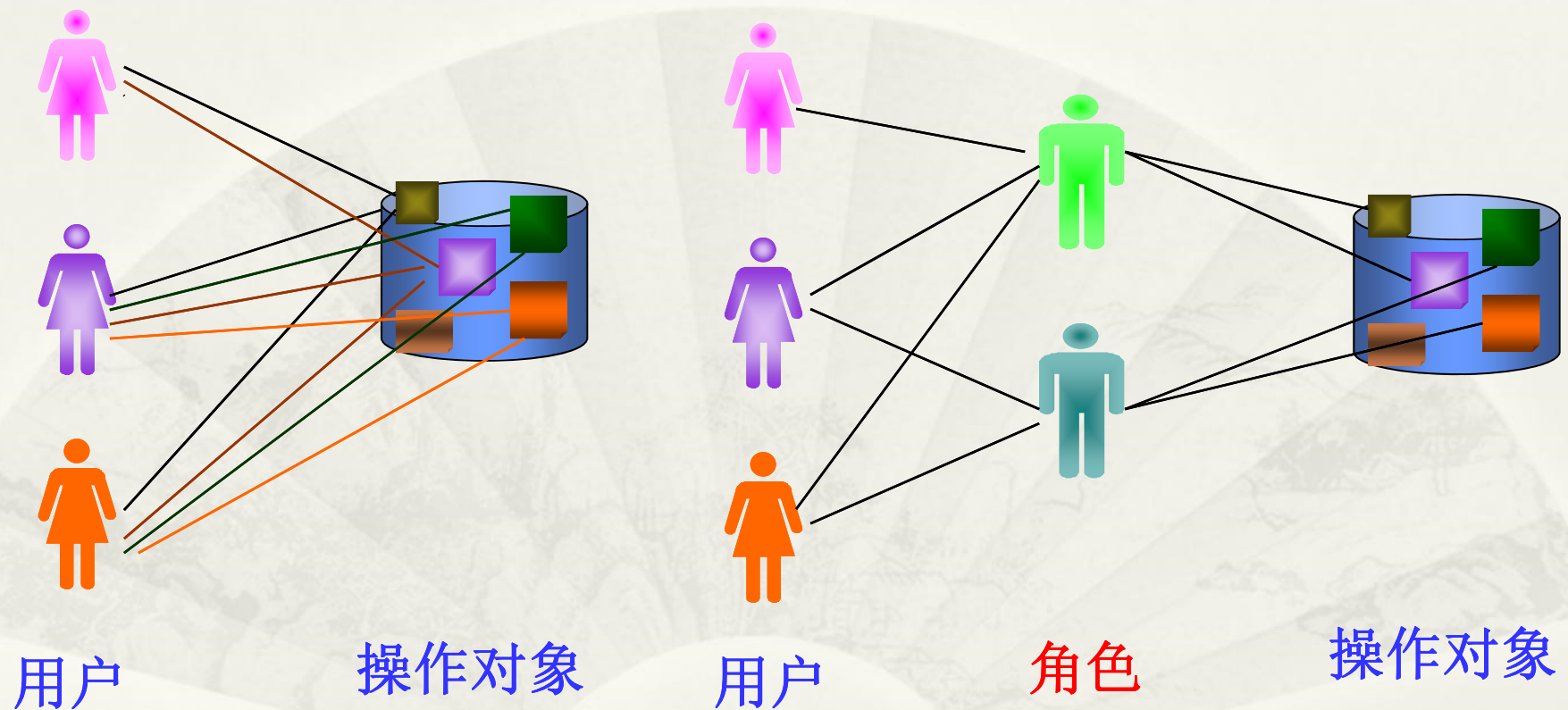
- * 优点

- * 能够通过授权机制**有效地控制其他用户**对敏感数据的存取

- * 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。

2.5 数据库角色 - 操作权限的集合



2.5 数据库角色 – 操作权限的集合 – 示例

- * 角色的创建

- * **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>]...

- * 将一个角色赋予其他角色或某用户

- * **GRANT** <角色1> [,<角色2>] ...
TO <角色3> [,<用户1>] ... [WITH ADMIN OPTION]

- * 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>] ...

- * 数据库角色是一组权限的集合。简化授权过程，使自主授权更加灵活方便。

2.6 强制存取控制MAC

- * 定义：系统为保证更高层次的安全性，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、

2.6 强制存取控制MAC – 基本概念

* 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、等

2.6 强制存取控制MAC – 基本概念

* 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）

2.6 强制存取控制MAC – 机制

- * 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

2.6 强制存取控制MAC – 控制规则

* 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**等于**客体的密级时，该主体才能**写**相应的客体。

2.6 强制存取控制MAC – 控制规则 – 修正规则

- * 某些系统的规定：保密性准则 [下读、上写]
 - * 主体的许可证级别 \leq 客体的密级
 - 主体能写客体
 - * 用户可为写入的数据对象赋予高于自己的许可证级别的密级
 - * 一旦数据被写入，该用户自己也不能再读该数据对象了。
- * 规则共同点：禁止了拥有高许可证级别的主体更新低密级的数据对象

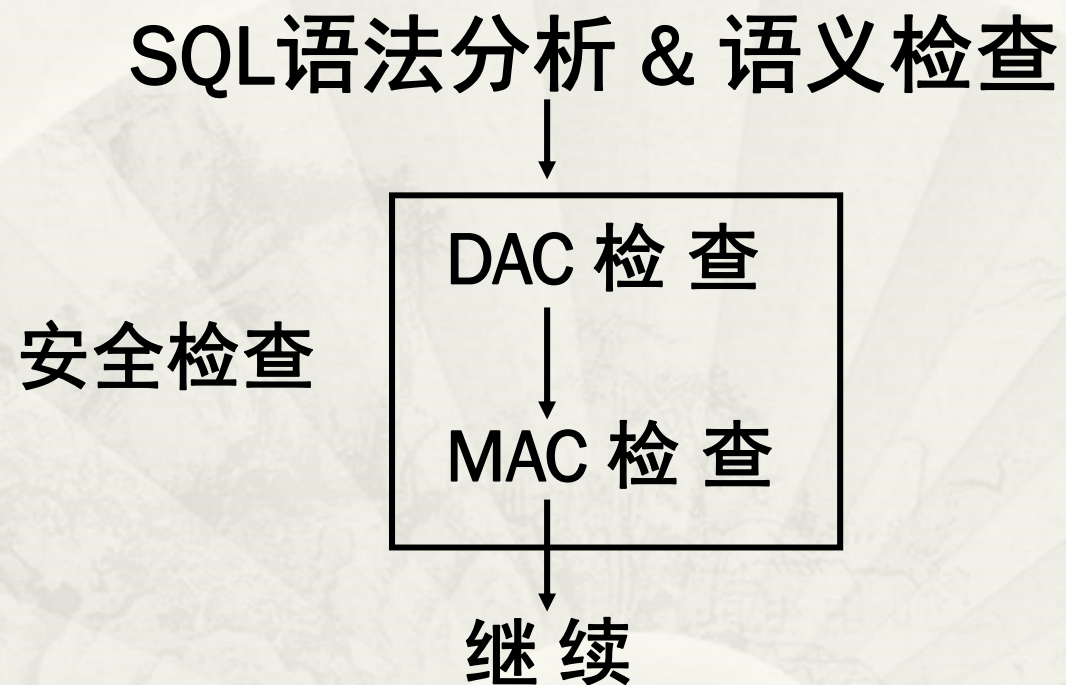
2.6 强制存取控制MAC - 特点

- * MAC是对数据本身进行密级标记，可提供更高级别的安全性。
- * 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

2.6 强制存取控制MAC与自主存取控制DAC

- * DAC与MAC共同构成DBMS的安全机制
 - * 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
- * 先进行DAC检查，通过DAC检查的数据对象再由系统进行MAC检查，只有通过MAC检查的数据对象方可存取。

2.6 DAC+MAC安全检查示意图



2.7 视图机制

- * 视图机制：保证数据独立性；可对用户隐藏保密的数据。但安全保护功能不够精细。
- * 与授权机制的结合
 - * 定义视图：屏蔽一部分保密数据；
 - * 视图之上再定义存取权限；
 - * 可间接实现了支持存取谓词的用户权限定义

2.7 视图机制 – 例

例：王平只能检索计算机系学生的信息

1. **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';
```

2. **在视图上进一步定义存取权限**

```
GRANT SELECT  
ON CS_Student  
TO 王平 ;
```


2.8 审计

A (A1)
B (B1、 B2、 B3)
C (C1、 C2)
D

* 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自动记录在日志中。
- * 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

* 审计功能的可选性：

- * 时间空间需求高
- * DBA可根据应用对安全性的要求，灵活打开或关闭审计功能。

2.8 审计 – 两级审计

- * 用户级审计
 - * 面向数据库用户
 - * 用户可针对自己创建的库表或视图进行审计
- * 系统级审计
 - * 由DBA设置
 - * 监测：登录、GRANT/REVOKE操作、其他数据库级权限下的操作。
- * 操作语句：AUDIT、NOAUDIT
- * 提供了事后检查的安全机制。

2.9 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
- * 存储加密：透明、非透明，两种方式
- * 传输加密：链路加密、端到端加密
- * 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）
 - * 不知道解密算法的人无法获知数据的内容

2.9 数据加密 - 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）

2.9 数据加密 – DBMS中的数据加密

- * **实现方法**

- * 有些数据库产品提供了数据加密例行程序
- * 有些数据库产品本身未提供加密程序，但提供了接口

- * **数据加密功能通常也作为可选特征，允许用户自由选择**

- * 数据加密与解密是比较费时的操作
- * 数据加密与解密程序会占用大量系统资源
- * 应该只对高度机密的数据加密

其他

* MySQL安全机制

- * 用户权限和访问控制：杜绝匿名用户
- * 数据保护：数据加密、数据备份/恢复/数据导入导出/审计
 - * 补充“备份”：物理备份、逻辑备份、增量备份
- * 日志文件：错误日志、查询日志、二进制日志、慢查询日志
- * 仲裁
- * 防范SQL注入攻击

主要内容

- 一 计算机安全性概论
- 二 数据库安全性控制
- 三 统计数据库安全性
- 四 小结

3.1 统计数据库 – 基本概念

- * 概念：管理统计数据的数据库系统
 - * 统计数据库的特点
 - * 包含大量数据内容
 - * 目的：向用户提供各种统计汇总信息，而不是单个记录信息。
 - * 操作：允许用户查询聚集类型的信息（例如合计、平均值等），但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？”

3.2 统计数据库 - 安全性问题

* 统计数据库中特殊的安全性问题

- * 可能存在**隐蔽的信息通道**，使得用户能从合法的查询中推导出不合法的信息。

例：下面两个查询都是合法的：

1. 本公司共有多少女高级程序员？
2. 本公司女高级程序员的工资总额是多少？

规则1：任何查询至少要涉及 N (N 足够大)个以上的记录。

3.2 统计数据库 – 安全性问题 – 例

例2：用户A发出下面两个合法查询：

1. 用户A和其他N个程序员的工资总额是多少？
2. 用户B和其他N个程序员的工资总额是多少？

若第一个查询的结果是X，第二个查询的结果是Y，
由于用户A知道自己的工资是Z，
那么他可以计算出用户B的工资= $Y-(X-Z)$ 。

原因：两个查询之间有很多重复的数据项

规则2：任意两个查询的相交数据项不能超过M个

3.2 统计数据库 - 安全性问题 - 例

可以证明，在上述两条规定下，如果想获知用户B的工资额，A至少需要进行 $1+(N-2)/M$ 次查询

规则3：任一用户的查询次数不能超过 $1+(N-2)/M$

如果两个用户合作查询就可以使这一规定失效

3.2 统计数据库 – 安全机制的设计目标

试图破坏安全的人所花费的代价

>>

得到的利益

3.3 其他安全性保护

* 推理控制

- * 非法操作：利用列间的函数依赖关系，从低安全等级获取无权访问的高等级安全信息。
- * 如：职员信息中，低安全等级（姓名、职位）、高安全等级（工资）——行业薪资等

* 隐蔽信道

- * 非法操作：利用数据库的数据/属性控制特性，导致高等级敏感数据泄露。

* 数据隐私

主要内容

- 一 计算机安全性概论
- 二 数据库安全性控制
- 三 统计数据库安全性
- 四 小结

4 小结

- * 数据安全问题的重要性
- * 计算机系统安全问题及安全标准 – TCSEC 及扩展到数据库的标准TDI
- * 数据库安全性控制机制：用户标识与鉴别、存储控制（DAC、MAC）、视图机制、审计、数据加密、等
- * 统计数据库的安全性问题及其他安全问题

作业

* P.154 1、4、6、7(1-4-6-7)、11

