数据库的安全性

北京理工大学

第六章数据库的安全性

- 数据库的安全性是指保护数据库防止不合法的使用造成数据库的泄露，更改和破坏
- 数据库的安全保护措施是否有效是数据库系统的主要指标之一
- 数据库系统安全性和计算机系统的安全性，操作系统的安全性以及网络的安全性是相互联系的

三类安全问题

- 计算机系统的安全性

  技术安全*-使用相应的硬件软件手段保证系统安全，在计算机系统受到有意或者无意的攻击的时候可以保证系统的正常运行，保证数据的安全

- 管理安全
- 政策法律安全

可信计算机系统的评估标准

- 1985—美国国防部（DOD）—《可信计算机系统的评估标准》—TCSEC (DOD85)-桔皮书
  - 评估计算机系统安全性的可信评估
  - 指导厂商对安全系统的设计
- 1991—NCSC 美国国家计算机安全中心—《TCSEC关于可信数据库系统的解释》—TDI—紫皮书

计算机系统的分级

- 根据TDI的相关指标，将系统分成4组7级

  D C1 C2 B1 B2 B3 A1

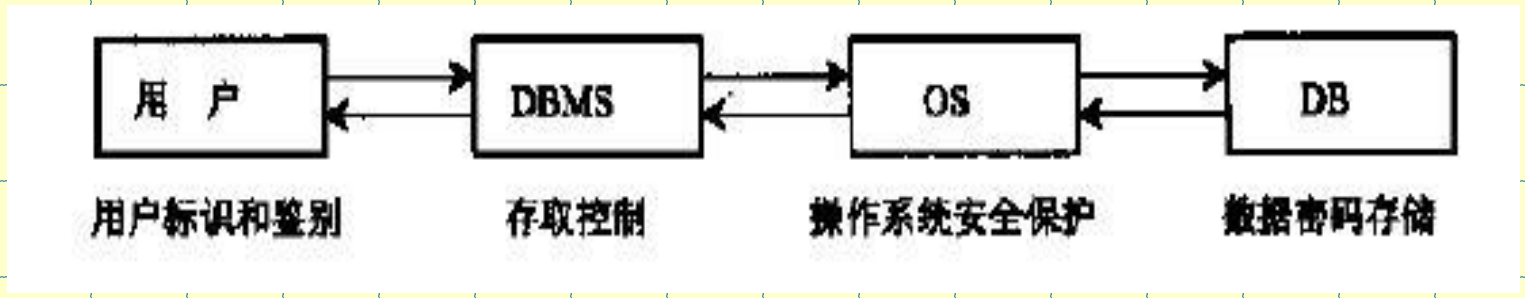
  不同的分级具有偏序向下兼容
- D 最低级别保留给不符合安全要求的系统
- C1 提供初级的自主安全保护
- C2 提供受控的存取保护
- B1 标记安全保护 提供 强制存取控制以及审计等安全机制

- B2 结构化保护 通过安全模型对系统的所有主体和客体实行DAC和MAC
- B3 安全域 提供访问监控器的功能，设计跟踪以及系统恢复过程
- A1 验证设计 在B3基础上给出形式化设计说明并得到验证各安全功能的真正实现
- CC标准中的评估保证级 参考p115表格
- B2以上的系统属于理论研究阶段，大多数系统处于B2以下级别

- B2级目前是大多数商业系统努力的目标
- 支持自主存取控制的DBMS 大致属于C级
- 支持强制存取控制的DBMS 原则可以达到B1级

数据库的安全性控制

- 计算机系统中，安全措施是一级一级的层层设置的



用鉴别户标识和鉴别

- 用户进入系统时候身份的识别机制
  - 用户名和口令
  - 数字证书
  - 动态口令

存取控制

- 什么样的用户对什么样的信息又什么访问权限的问题。

  定义用户权限，登记到数据字典当中

  合法权限的检查机制

  - 自主存取控制（DAC）—用户对不同的数据对象有不同的存取权限。不同的用户对相同的数据也有不同的存取权限
  - 强制存取控制（MAC）—每个数据对象被标以一个密级，某个用户被授予一个级别的访问许可

自主存取控制（DAC）

- 目前大多数的数据库产品支持自主存取控制 例如SQL语句中的GRANT 和REVOKE
- 用户权限包含两个要素

  数据对象和操作类型

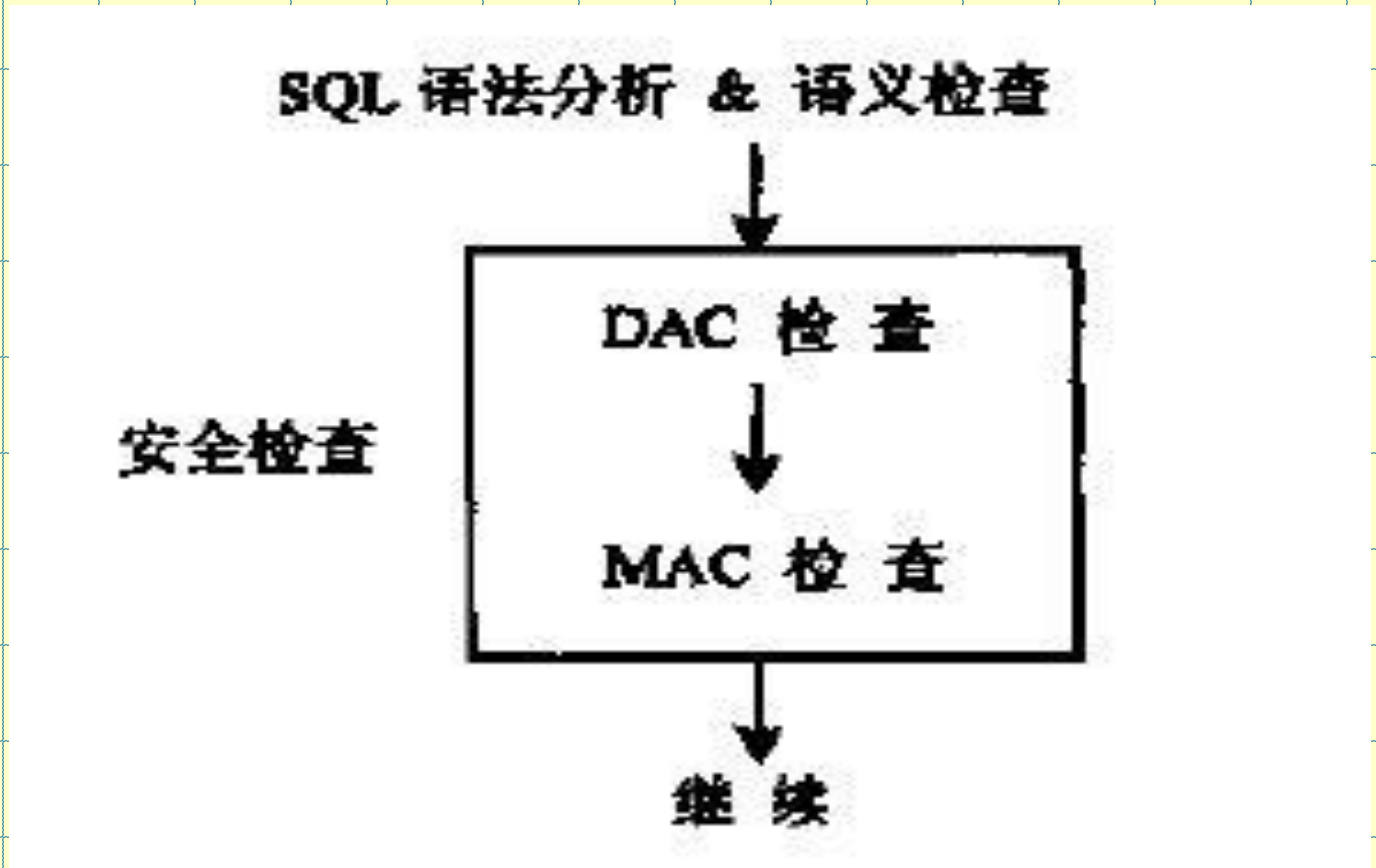
	数据对象	操作类型
模　式	模　式	建立、修改、检索
	外模式	建立、修改、检索
	内模式	建立、修改、检索
数　据	表	查找、插入、修改、删除
	属性列	查找、插入、修改、删除

- 用户权限定义过程中数据对象范围越小系统越灵活—例如有些系统可以支持字段级
- 有些系统可以提供于数值有关的授权（不仅根据数据的名称，可以根据数据的取值设置不同的权限）—存取谓词
- 系统授权还可以和某些系统参数相联系—比如时间段，终端号等因素
- 有的系统增加了角色的概念
- 授权和回收是自主的，系统无法完全控制

强制存取控制（MAC）

- 在MAC方法中，DBMS所管理的全部实体分为主体和客体
- 主体：系统中活动的实体（用户或者用户的进程）
- 客体：系统中被操作的对象
- DBMS对每个实体的实例分配敏感度标记
  - 主体的敏感度标记叫做 许可证级别
  - 客体的敏感度标记叫做 密级

- MAC是通过比较主体和客体的敏感度标记来确定存取权限
  - 主体的标记大于等于客体密级时才能读取相应的客体
  - 仅当主体的许可级别等于客体密级时才能写相应的客体*
- 标记跟随数据，即同一个数据的不同复本具有相同的存取控制
- DBMS实现MAC首先必须实现DAC


SQL 语法分析 & 语义检查
安全检查
DAC 检 查
MAC 检 查
继 续

- 视图机制

  通过视图机制可以保证一定程度的安全性
- 审计

  对数据库的所有访问操作记录在审计日志
- 数据加密

  将数据库中保存的信息从明文加密成密文
- 数据库统计功能安全性

  防止用户使用数据库统计（聚集函数）获得不被授权的单记录信息

- 教材上介绍了SQL server安全控制机制，请自行阅读了解。