第九章　数据库安全性

《概论》第九章详细介绍数据库安全性问题和实现技术。信息安全、计算机系统安全以及数据库系统安全是信息安全的重要内容。随着计算机特别是计算机网络的发展,数据的共享日益加强,数据的安全保密越来越重要。

一、基本知识点

数据库的安全性问题和计算机系统的安全性是紧密联系的,计算机系统的安全性问题可分技术安全类、管理安全类和政策法律类三大类安全性问题。我们讨论数据库的安全性,讨论数据库技术安全类问题,即从技术上如何保证数据库系统的安全性。

① 需要了解的:什么是计算机系统安全性问题;什么是数据库的安全性问题;统计数据库的安全性问题。

② 需要牢固掌握的: TDI/ TCSEC 标准的主要内容;C2 级 DBMS、B1 级 DBMS 的主要特征;实现数据库安全性控制的常用方法和技术有哪些;数据库中的自主存取控制方法和强制存取控制方法。

③ 需要举一反三的:使用 SQL 语言中的 GRANT 语句和 REVOKE 语句来实现自主存取控制。

④ 难点: MAC 机制中确定主体能否存取客体的存取规则,读者要理解并掌握存取规则为什么要这样规定,特别是规则(2)。

二、习题解答和解析

1. 什么是数据库的安全性?

答

数据库的安全性是指保护数据库以防止不合法的使用所造成的数据泄露、更改或破坏。

2. 数据库安全性和计算机系统的安全性有什么关系?

答

安全性问题不是数据库系统所独有的,所有计算机系统都有这个问题。只是在数据库系统中大量数据集中存放,而且为许多最终用户直接共享,从而使安全性问题更为突出。

系统安全保护措施是否有效是数据库系统的主要指标之一。

数据库的安全性和计算机系统的安全性,包括操作系统、网络系统的安全性是紧密联系、相互支持的,

3. 试述可信计算机系统评测标准的情况,试述 TDI/ TCSEC 标准的基本内容。

答

各个国家在计算机安全技术方面都建立了一套可信标准。目前各国引用或制定的一系列安全标准中,最重要的是美国国防部(DoD)正式颁布的《DoD 可信计算机系统评估标准》(Trusted Computer System Evaluation Criteria,简称 TCSEC,又称桔皮书)。(详细介绍参见《概论》9.1.2)。

TDI/ TCSEC 标准是将 TCSEC 扩展到数据库管理系统,即《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,又称紫皮书)。在 TDI 中定义了数据库管理系统的设计与实现中需满足和用以进行安全性级别评估的标准。

TDI 与 TCSEC 一样,从安全策略、责任、保证和文档四个方面来描述安全性级别划分的指标。每个方面又细分为若干项。这些指标的具体内容,参见《概论》9.1.2。

4. 试述 TCSEC(TDI)将系统安全级别划分为 4 组 7 个等级的基本内容。

答

根据计算机系统对安全性各项指标的支持情况,TCSEC(TDI)将系统划分为四组(division)7 个等级,依次是 D、C(C1,C2)、B(B1,B2,B3)、A(A1),按系统可靠或可信程度逐渐增高。

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)

这些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。

各个等级的基本内容为:

D 级　D 级是最低级别。一切不符合更高标准的系统,统统归于 D 组。

C1 级　只提供了非常初级的自主安全保护。能够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　实际是安全产品的最低档次,提供受控的存取保护,即将 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。

B1 级　标记安全保护。对系统的数据加以标记,并对标记的主体和客体实施强制存取控制(MAC)以及审计等安全机制。

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。

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。

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。

各个等级的基本内容请参见《概论》9.1.2。特别是《概论》上表 9.2 列出了各安全等级对安全指标的支持情况。希望读者掌握《概论》上的内容,这里就不重复了。

5. 试述实现数据库安全性控制的常用方法和技术。

答

实现数据库安全性控制的常用方法和技术有:

(1) 用户标识和鉴别:该方法由系统提供一定的方式让用户标识自己的名字或身份。每次用户要求进入系统时,由系统进行核对,通过鉴定后才提供系统的使用权。

(2) 存取控制:通过用户权限定义和合法权检查确保只有合法权限的用户访问数据库,所有未被授权的人员无法存取数据。例如 C2 级中的自主存取控制(DAC),B1 级中的强制存取控制(MAC)。

(3) 视图机制:为不同的用户定义视图,通过视图机制把要保密的数据对无权存取的用户隐藏起来,从而自动地对数据提供一定程度的安全保护。

(4) 审计:建立审计日志,把用户对数据库的所有操作自动记录下来放入审计日志中,DBA 可以利用审计跟踪的信息,重现导致数据库现有状况的一系列事件,找出非法存取数据的人、时间和内容等。

(5) 数据加密:对存储和传输的数据进行加密处理,从而使得不知道解密算法的人无法获知数据的内容。

具体内容请参见《概论》9.2。

6. 什么是数据库中的自主存取控制方法和强制存取控制方法？

答

自主存取控制方法:定义各个用户对不同数据对象的存取权限。当用户对数据库访问时首先检查用户的存取权限。防止不合法用户对数据库的存取。

强制存取控制方法:每一个数据对象被(强制地)标以一定的密级,每一个用户也被(强制地)授予某一个级别的许可证。系统规定只有具有某一许可证级别的用户才能存取某一个密级的数据对象。

解析

自主存取控制中自主的含义是:用户可以将自己拥有的存取权限“自主”地授予别人。即用户具有一定的“自主”权。

7. SQL 语言中提供了哪些数据控制(自主存取控制)的语句？请试举几例说明它们的使用方法。

答

SQL 中的自主存取控制是通过 GRANT 语句和 REVOKE 语句来实现的。如:

```
GRANT SELECT, INSERT ON Student
TO 王平
WITH GRANT OPTION;
```

就将 Student 表的 SELECT 和 INSERT 权限授予了用户王平,后面的“WITH GRANT OPTION”子句表示用户王平同时也获得了“授权”的权限,即可以把得到的权限继续授予其他用户。

```
REVOKE INSERT ON Student FROM 王平 CASCADE;
```

就将 Student 表 的 INSERT 权限从用户王平处收回,选项 CASCADE 表示,如果用户王平将 Student 的 INSERT 权限又转授给了其他用户,那么这些权限也将从其他用户处收回。

8. 今有两个关系模式:

职工(职工号,姓名,年龄,职务,工资,部门号)

部门(部门号,名称,经理名,地址,电话号)

请用 SQL 的 GRANT 和 REVOKE 语句(加上视图机制)完成以下授权定义或存取控制功能:

(1) 用户王明对两个表有 SELECT 权力。

```
GRANT SELECT ON 职工,部门
TO 王明;
```

(2) 用户李勇对两个表有 INSERT 和 DELETE 权力。

```
GRANT INSERT,DELETE ON 职工,部门
TO 李勇;
```

(3) * 每个职工只对自己的记录有 SELECT 权力。

```
GRANT SELECT ON 职工
WHEN USER() = NAME
TO ALL;
```

这里假定系统的 GRANT 语句支持 WHEN 子句和 USER()的使用。用户将自己的名字作为 ID。注意,不同的系统这些扩展语句可能是不同的。读者应该了解你使用的 DBMS 产品的扩展语句。

(4) 用户刘星对职工表有 SELECT 权力,对工资字段具有更新权力。

```
GRANT SELECT,UPDATE(工资) ON 职工
TO 刘星;
```

(5) 用户张新具有修改这两个表的结构的权力。

```
GRANT ALTER TABLE ON 职工,部门
TO 张新;
```

(6) 用户周平具有对两个表所有权力(读,插,改,删数据),并具有给其他用户授权的权力。

```
GRANT ALL PRIVILIGES ON 职工,部门
TO 周平
WITH GRANT OPTION;
```

(7) 用户杨兰具有从每个部门职工中 SELECT 最高工资、最低工资、平均工资的权力,他不能查看每个人的工资。

首先建立一个视图。然后对这个视图定义杨兰的存取权限。

```
CREATE VIEW 部门工资 AS
  SELECT 部门.名称,MAX(工资),MIN(工资),AVG(工资)
  FROM 职工,部门
  WHERE 职工.部门号 = 部门. 部门号
  GROUP BY 职工.部门号;
GRANT SELECT ON 部门工资
TO 杨兰;
```

9. 把习题 8 中(1)～(7) 的每一种情况,撤销各用户所授予的权力。

答

(1)

```
REVOKE SELECT ON 职工,部门
FROM 王明;
```

(2)

```
REVOKE INSERT,DELETE ON 职工,部门
FROM 李勇;
```

(3)

```
REOVKE SELECT ON 职工
WHEN USER() = NAME
FROM ALL;
```

这里假定用户将自己的名字作为 ID,且系统的 REOVKE 语句支持 WHEN 子句,系统也支持 USER()的使用。

(4)

```
REVOKE SELECT,UPDATE ON 职工
FROM 刘星;
```

(5)

```
REVOKE ALTER TABLE ON 职工,部门
FROM 张新;
```

(6)

```
REVOKE ALL PRIVILIGES ON 职工,部门
FROM 周平;
```

(7)

```
REVOKE SELECT ON 部门工资
FROM 杨兰;
DROP VIEW 部门工资;
```

10. 为什么强制存取控制提供了更高级别的数据库安全性?

答

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,从而提供了更高级别的安全性。

11. 理解并解释 MAC 机制中主体、客体、敏感度标记的含义。

答

主体是系统中的活动实体,既包括 DBMS 所管理的实际用户,也包括代表用户的各进程。

客体是系统中的被动实体,是受主体操纵的,包括文件、基表、索引、视图等。

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)。敏感度标记被分成若干级别,例如绝密(Top Secret)、机密(Secret)、可信(Confidential)、公开(Public)等。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)。

12. 举例说明 MAC 机制如何确定主体能否存取客体。

答

假设要对关系变量 S 进行 MAC 控制,为简化起见,假设要控制存取的数据单元是元组,则每个元组标以密级,如下表所示:(4 = 绝密,3 = 机密,2 = 秘密)

S#	SNAME	STATUS	CITY	CLASS
S1	Smith	20	London	2
S2	Jones	10	Paris	3
S3	Clark	20	London	4

假设用户 U1 和 U2 的许可证级别分别为 3 和 2,则根据规则 U1 能查得元组 S1 和 S2,可修改元组 S2;而 U2 只能查得元组 S1,只能修改元组 S1。

解析

这里假设系统的存取规则是:(1) 仅当主体的许可证级别大于或等于客体的密级时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才能写相应的客体。

13. 什么是数据库的审计功能,为什么要提供审计功能?

答

审计功能是指 DBMS 的审计模块在用户对数据库执行操作的同时把所有操作自动记录到系统的审计日志中。

因为任何系统的安全保护措施都不是完美无缺的,蓄意盗窃破坏数据的人总可能存在。利用数据库的审计功能,DBA 可以根据审计跟踪的信息,重现导致数据库现有状况的一系列事件,找出非法存取数据的人、时间和内容等。

14. 统计数据库中存在何种特殊的安全性问题?

答

统计数据库允许用户查询聚集类型的信息,如合计、平均值、最大值、最小值等,不允许查询单个记录信息。但是,人们可以从合法的查询中推导出不合法的信息,即可能存在隐蔽的信息通道,这是统计数据库要研究和解决的特殊的安全性问题。

*15. 试述你了解的某一个实际的 DBMS 产品的安全性措施。

答

不同的 DBMS 产品以及同一产品的不同版本的安全措施各不相同,仁者见仁,智者见智,请读者自己了解。《概论》上 9.4 简单介绍了有关 Oracle 数据库的安全性措施。