数据库安全模型及其应用研究

崔艳荣，文汉云
(长江大学 计算机科学学院，湖北 荆州 434103)

摘 要：在介绍了三种数据库安全模型——自主访问模型、强制访问模型和基于角色的访问模型的基础上，分析了它们的优点和不足，并给出了各种不同模型的应用场合。在车站售票管理系统中，给出了一种基于 BLP 安全模型的实现方法。

关键词：数据库；安全模型；自主访问模型；强制访问模型；基于角色的访问模型
中图法分类号：TP309 **文献标识码**：A **文章编号**：1001-3695(2005)07-0146-02

Research on Database Security Model and Its Application

CUI Yan-rong, WEN Han-yun
(School of Computer Science, Yangtse River University, Jingzhou Hubei 434103, China)

Abstract: Three kinds of database safe model (Discretionary Access Control, Mandatory Access Control and Role-Based Access Control) have been discussed. Some advantages and shortcomings existed on these safe model are analysed. So, the different application occasion for different safe model and an implementation method based on BLP safe model is given in this paper.

Key words: Database; Safe Model; Discretionary Access Control; Mandatory Access Control; Role-Based Access Control

数据库安全模型主要反映数据库系统的安全策略。随着对计算机数据库系统安全性研究的逐步深入，大量卓有成效的研究成果相继出现，在丰富了数据库系统安全模型的同时，将各种安全模型应用于系统的安全性设计也取得了大量的研究成果。依据存取控制策略、授权管理模式的不同，可以将安全模型分为三类，即自主访问控制模型(Discretionary Access Control, DAC)、强制访问控制模型(Mandatory Access Control, MAC)和基于角色的访问控制(Role-Based Access Control, RBAC)。本文将重点介绍这三种安全模型的基本概念，分析这三种模型的一些优点和不足，在此基础上给出各种不同模型的应用场合和一种基于 BLP 安全模型的应用实例。

1 自主访问控制模型(DAC)

自主访问控制模型是基于用户身份的访问和控制。在自主型访问安全模型中，每个用户都要被分配一定的权限，例如用户或者是被允许读取，或是被允许写入。也就是说，在自主型访问安全模型中，对资源对象的“拥有”是用户最核心的权限属性。当某个用户要求访问某个数据库资源时，系统检查该用户对该资源的所有权限，或衍生出来的访问权限，如果通过，则允许该访问在许可的方式下进行，如果不能通过，则拒绝继续访问系统。在自主型安全模型中，拥有某种权限的用户可以自主地将其所拥有的权限传授给其他任意在系统中登录的用户，它是该模型存在的致命缺点。自主访问安全模型的典型代表是存取矩阵。

DAC 模型可对用户提供灵活和易行的数据访问方式，但安全性相对较低。在该模型中，尽管访问控制只在授权后才能得到，但攻击者也很容易越过访问的授权限制。如当一个用户有权对某数据进行读操作时，它可以把这个权利传递给无权读此数据的人，而数据的所有者并不知道这一切。一旦某个信息为用户所获得，那么该模型策略对信息的使用是不加任何限制的。也就是说，在该模型中，尽管有自主型控制，对于非授权的人来说，非法读取数据是可能的，这样一来，系统就很容易受到类似特洛伊木马的攻击。特洛伊木马可以改变系统的保护状态，使系统安全受到威胁。

收稿日期：2004-05-06；修返日期：2004-09-08

2 强制访问控制模型(MAC)

强制访问控制模型通过无法回避的存取限制来防止各种直接和间接的攻击。在强制访问控制之下，系统给主体和客体分配了不同的安全属性，这些属性在安全策略没有改变之前是不可能轻易被改变的。这一点与存取矩阵中的条目可以直接和间接地被修改的情况完全不同。系统通过对主体和客体的安全属性进行匹配比较决定是否允许访问继续进行。用户以及代表用户的程序/进程等都不能以任何方式修改自身的或任何客体的安全属性。显然，用户无权将任何数据资源，哪怕是属于自己的数据资源的访问权“赠送”给别的用户，因此也就不能简单地分配数据的访问权限了。强制访问模型包括 BLP 模型及其一些改进的 BLP 模型。

2.1 BLP 模型

强制访问模型的典型代表是 Bell-LaPadula(BLP)安全模型。该模型是 D. Elliott Bell 和 Leonard J. LaPadula 于 1973 年创立的。现在大多数数据库安全系统都使用这种基于 BLP 模型的强制访问机制。该模型用主体(Subject)和客体(Object)来进行描述。一个客体可理解为一个文件、一条记录或一条记录中的某个字段。主体是一个请求访问客体的主动进程。每个客体被指派一个密级(Classification)，而每个主体被指派一

个许可证(Clearance) 。密级和许可证结合起来作为安全类别(Class) 并按偏序排列。

BLP 模型安全策略包括强制存取控制和自主存取控制两部分。强制存取控制部分由简单安全特性和 “* - 特性 ”组成, 通过安全级来强制性约束主体对客体的存取; 自主存取控制通过存取控制矩阵按用户的意愿来进行存取控制。BLP 还使用了可信主体的概念, 用于表示在实际系统中不受 “* - 特性 ”制约的主体, 以保证系统正常运行和管理。随着计算机安全理论和技术的发展, BLP 模型已不足以描述各种各样的安全需求, 主要表现在以下几个方面:

(1) 在 BLP 模型中, 可信主体不受 “* - 特性 ”约束, 其访问权限太大, 不符合最小特权原则, 应对可信主体的操作权限和应用范围进一步细化。

(2) BLP 模型主要注重保密性控制, 控制信息从低安全级向高安全级传递, 而缺少完整性控制, 不能控制 “向上写(Write up) ”操作, 而 “向上写 ”操作存在着潜在的安全问题。

(3) BLP 模型不能有效地限制隐藏通道。

2.2　改进的 BLP 模型

由于传统 BLP 模型的这些缺点, 人们提出了许多对 BLP 模型的改进方案[1], 其中 BLDM 和 MBLP 是影响比较大的两种。

2.2.1　BLDM 模型

BLDM(Bell&LaPadula Data Model) 是 T. Y. Lin 等人对 BLP 模型改进后得到的。该模型提出了数据簇的概念, 也就是要求不同安全级的原始数据必须存储在不同的物理卷中, 即每个原始数据属于且仅属于一个簇, 所有的簇物理地存放在一起, 不同安全等级的数据占有不同的卷。这就意味着整个模型不再允许任何从高安全级向低安全级的数据流动, 从而保证了系统的完全安全性。不过, 如果完全强调系统的安全, 那就牺牲了系统的可靠性, 所以应用 BLDM 系统的时候, 可以将下行的信息这样来处理: 先将高安全级的信息删除, 再将这个被删除的信息作为低安全级的信息插入。这项操作可以由不隶属于安全系统的工具软件辅助完成这种在 BLP 模型下属于可信主体的功能。

2.2.2　MBLP 模型

MBLP (Modified BLP) 模型主要解决了 BLP 模型中存在的几个问题:

(1) 针对 BLP 模型中可信主体不受 “* - 特性 ”约束致使其访问权限太大, 不符合最小特权原则的问题, MBLP 对可信主体的操作权限和应用范围进行了进一步的细化。

(2) BLP 模型注重保密性, 但缺少完整性控制, 不能控制低安全级主体对高安全级客体的 “向上写 ”, 所以 MBLP 对 “向上写 ”操作作出限制。

MBLP 模型对于普通用户域的主体, BLP 模型的基本安全公理仍然成立。对于可信用户域的主体, 满足二人原则。另外该模型可以有效地实现应用型病毒防护, 还可以有效地限制隐藏通道。

3　基于角色的访问控制(RBAC)

RBAC 是由美国 George Mason 大学的 Ravi Sandu 教授提出[2], 它提供了解决具有大量用户、数据库客体和访问权限系统中的授权管理问题。在 RBAC 中, 权限是和角色相联系的, 而用户则被指定到相应的角色作为其成员。这样就使权限的管理大大简化了。RBAC 涉及用户(User) 、角色(Role) 、访问权(Permission) 、会话(Session) 这几个主要概念。角色是访问权的集合, 当用户被赋予一个角色时, 用户具有这个角色所包含的所有访问权。用户和角色是多对多的关系, 角色与访问权也是多对多的关系。在 RBAC 模型系统中, 每个用户进入系统时得到一个会话, 一个用户会话可能激活的角色是该用户的全部角色的子集。对此用户而言, 在一个会话内可获得全部被激活的角色所包含的访问权。角色和会话的设置带来的好处是容易实施最小特权原则(Least-privilege Principle) 。RBAC 非常适用于数据库应用层的安全模型, 因为在应用层内角色的逻辑意义更为明显和直接。

RBAC 在不同的配置下可显示不同的控制功能, 它可以构造出 MAC 系统, 也可以构造出 DAC 系统, 甚至可构造兼备 MAC 和 DAC 的系统。RBAC 流行起来的原因在于它与策略无关, 可灵活适用于各种不同的安全策略。

4　一种基于 BLP 安全模型的实现

在某市的车站售票管理系统的安全性设计中, 应用 BLP 安全模型, 取得了比较好的效果, 该系统运行一年半以来, 还没有出现任何安全性问题。该模型有售票员、票房主任、系统一般管理员、系统高级管理员几个主体。系统高级管理员负责完成权限的管理和分配, 其他的主体被分配有不同的许可级别。被保护的客体, 即系统中的文件、字段、表格等被指派一个敏感标记 label, label{ 绝密, 秘密, 机密, 公开} , 售票员、票房主任、系统一般管理员不能改变自身或者任何客体的安全属性, 只有系统高级管理员可以确定用户和用户组的访问权限。当主体请求访问某个客体时, 系统通过比较客体和主体的安全属性来决定主体是否可以访问客体。其访问流程图如图 1 所示。

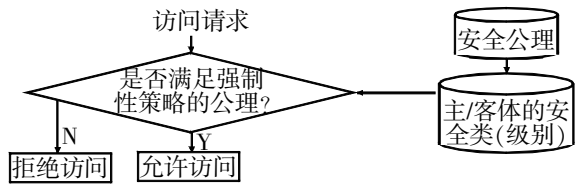

图 1　强制访问模型流程图

在车站售票管理系统中, 由于用户比较少, 很容易给所有的用户分配安全级别。客体数据的敏感级别也比较容易确定, 所以在系统的安全性设计中采用了基于对系统中的主、客体进行分类的强制存取模型。该模型可以有效地防止特洛伊木马类的恶意进攻, 同时还可以根据主体的不同权限, 修改了 “向上写 ”的特性, 从而控制了因向上写而带来的安全隐患。

5　结束语

数据库安全模型在具体应用时, 首先应分析清楚具体系统的特点, 如果安全级别不是要求很高, 可以用自主安全模型; 如果很重视系统的安全性, 则可以选用基于 BLP 的强制存取控制模型; RBAC 模型则比较合适基于角色的大型系统。在实际应用中, 还可以根据具体情况构造基于各种传统模型的复合安全模型来适应不同的需求。

参考文献:

[1]　王达昌, 鞠时光. BLP 安全模型及其发展[J] . 江苏大学学报(自然科学版) , 2004, 25(1) : 68-72.

[2]　施景超, 孙维祥, 许满武. 基于角色的存取控制及其实现[J] . 计算机应用研究 , 2000, 17(6) : 13-15.

作者简介:

崔艳荣(1968-) , 女, 讲师, 主要从事数据库系统方面的教学和科研工作。