

# 基于访问控制的涉密信息管理安全解决方案

胡欣杰, 路 川

(装备学院 信息装备系, 北京 101416)

**摘 要:**将涉密信息放入共享的数据库中保存必须解决其安全问题,访问控制是一种基本方法。文中首先分析了自主访问控制、强制访问控制、基于角色的访问控制这三种经典的访问控制模型,然后分析了涉密信息本身的特点及其操作管理的需求,并考虑了数据库应用程序中的主体、客体等因素,最后提出并设计了一个综合利用这些策略管理涉密信息的实现方案。该方案设计了几个数据库表,分别保存实现这三种访问控制模型所需的信息和各种类型的涉密信息,给出了这些信息之间的相互关系,划分了程序模块及其实现方案。该方案符合理论要求,切实可行。

**关键词:**访问控制;数据库应用程序;信息安全

中图分类号:TP301

文献标识码:A

文章编号:1673-629X(2014)08-0131-04

doi:10.3969/j.issn.1673-629X.2014.08.030

## A Solution for Management Security of Secret Information Based on Access Controlling

HU Xin-jie, LU Chuan

(Department of Information Equipment, Institute of Equipment, Beijing 101416, China)

**Abstract:** Classified information to be included in the shared database must solve the security problem, access control is a kind of basic method. First, analyze the three classical access control models which are discretionary access control, mandatory access control and role-based access control, then analyze the characteristics of secret information and the requirements of operational management, considering the subject, object and other factors in a database application. Finally, propose and design a realizing scheme which comprehensively uses these strategies to manage classified information in database applications. The scheme designs several database table which to save the information needed and various types of classified information to achieve these three access control model. The relationship between the information is presented, dividing the program module and its implementation scheme. The scheme is practicable.

**Key words:** access control; database applications program; information security

### 1 访问控制及其模型

访问控制是信息安全领域的一项非常重要的安全机制,是指通过某种途径(授权、规则、约束)显式地允许或限制主体(用户)对客体(对象、资源)进行访问(操作)的能力与范围,以防止非法用户的侵入或合法用户的不慎操作而造成的破坏。访问控制主要有自主访问控制、强制访问控制、基于角色的访问控制。

#### 1.1 自主访问控制

自主访问控制(DAC)最早出现在20世纪60年代末的分时系统中。它是一种基于主体、客体所属关系的访问控制。规定客体的所有者或创建者主体具有访问客体的所有权限,其他主体必须被授予了某种权限才能对其他客体进行相应的访问,它允许主体可以自

主地把它对客体的访问权限授予给其他主体或从其他主体那里回收它被授予的访问权限。这种方式增加了授权管理的灵活性,分散了系统安全管理员的工作量,任何主体都可以根据工作的需要,在自己的权限范围内进行权限分配与回收。但存在局限性,如系统安全管理员可能很快失去对授权状况的控制。

通常利用访问控制矩阵模型来实现自主访问控制。访问控制矩阵如表1所示。表中每行表示一个主体 $S$ ,每列表示一个受保护的客体 $O$ ,矩阵中的元素表示主体可以对客体进行的访问模式 $M$ 或访问权限 $P$ 。 $M$ 或 $P$ 是一个集合,如创建、更改、读、写、执行等。

访问权限分为系统权限、对象权限。系统权限从系统管理角度允许用户做什么,用于系统结构的创建、

更改,系统资源的使用;对象权限是对象的创建者,允许其他用户在该对象上能做什么,是关于对象的读、写、执行、更改的权限<sup>[1-3]</sup>。

表 1 访问控制矩阵示例

主体 (Subject)	客体 (Object)			
	文件 1	文件 2	文件 3	程序 1
张三	读、写	读		执行
李四	读	读、写	读、写	
王五		写	读、写	执行

1.2 强制访问控制

强制访问控制 (MAC) 最早出现在 20 世纪 70 年代,是美国政府和军方源于对信息机密性的要求以及为防止特洛伊木马之类的攻击而提出的。它是一种基于安全级标记的访问控制方法,即它为客体指定一个内容敏感度的安全级别(如,绝密>机密>秘密>公开),为主体指定一个不泄漏敏感信息的信任度(如,高>中>低>无),并为保密指定一个保密强制性策略来控制主体对客体的访问:

- (1)防止上读,即主体的信任度高于或等于客体的安全级别时才能读客体;
- (2)防止下写,即主体的信任度低于或等于客体的安全级别时才能写客体。

强制访问控制如图 1 所示,图中表示安全的信息流通常是水平的(用户与自己的数据之间或同级用户及其数据之间的流向)和向上的(从用户低级流向高级用户)。

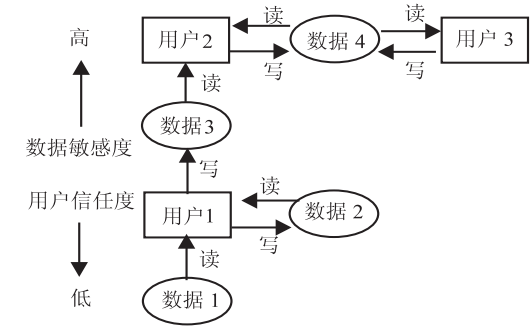


图 1 强制访问控制及其安全信息流模型

强制访问控制中最著名的模型是 BLP 模型。它是由 Bell 和 Lapadula 于 1973 年提出并于 1976 年修订、整合和完善的安全模型,是最典型的信息保密多级安全模型,通常是处理多级安全信息系统的设计基础。

1.3 基于角色的访问控制

20 世纪 90 年代以来,逐步产生了基于角色的访问控制 (RBAC)。其核心思想是在用户与权限之间引入角色的概念:一个角色是一组权限的集合,对用户的授权是通过赋予相应的角色来完成的,用户的权限是由该用户被授予的所有角色的权限集合的并集决定

的。

由 Sandhu 提出的 RBAC 的核心模型如图 2 所示。其中,用户集是系统中可以执行操作的用户;对象集是系统中需要保护的实体;操作集是定义在对象上的操作(权限);特定的对象集及其操作集构成了特定角色的特权集;角色是 RBAC 模型的核心,通过用户分配、特权分配等操作建立用户与特权的关联。

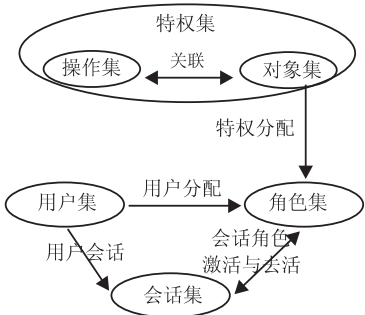


图 2 基于角色的访问控制模型

RBAC 适用于数量庞大的用户管理与权限管理的访问控制需求:它可以灵活地将用户从一个角色改变到另一个角色来实现特权的转换;在组织机构发生职能改变时,应用系统只需对角色重新分配特权,就可以使应用系统适应新的访问控制需求。

2 系统分析

上述访问控制模型是针对通用的、一般的计算机操作系统安全问题而提出的,但在处理涉密信息数据库应用程序的安全问题时,针对其保密需求和技术实现是可以扩展的。

1)系统保密需求方面。一条涉密信息以若干数据字段及其若干文档附件的形式保存在数据库表中。要综合利用上述访问控制模型,实现涉密信息的安全管理。即需要进行身份认证;用户分为涉密信息作者、涉密信息管理者两个角色,以便进行基于角色的访问控制;这两个角色和涉密信息都有保密级别,以便进行强制访问控制;涉密信息作者用户撰写的涉密信息与其角色的保密级别相同;同一保密级别的涉密信息作者用户之间不能相互访问各自的涉密信息,除非涉密信息作者用户将其撰写的涉密信息(对象资源)的某种操作权限授予给了另一个涉密信息作者用户,以便进行自主访问控制;涉密信息管理者用户可以查询等于或低于其角色的保密级别的涉密信息,但不能进行增加(插入)、更改、删除、保存操作。另外再安排一个安全管理员角色,由该角色的用户创建角色、用户,向角色分配或设置菜单(系统资源)的操作权限,向用户分配或设置角色<sup>[2]</sup>。

2)主体客体方面。主体不再是程序,而是具体的操作用户,所以保密不再是涉密信息“下读、上存”这

种安全信息流向的问题,而是操作用户相互之间需要保密的问题。客体不再是文件或程序,而是数据库表,并且由于 SQL 语句中可以有 WHERE 子句,使得客体的粒度可以进一步精细到记录行,尤其是每个用户的记录行或角色中具有相同保密级别的用户的记录行,换句话说,不同保密级别的涉密信息的创建者用户实际上可以在同一个数据库表中保存各自的涉密信息而且能做到相互保密<sup>[4-7]</sup>。

3)操作类型方面。读操作对应于查询操作,写操作对应于维护操作,即增加(插入)、更改、删除、保存操作。

4)技术实现方面。通过在数据库表中增加保密级别字段,可以实现对每个角色、每条涉密信息进行保密级别标记。然后通过动态构造 SQL 语句中的 WHERE 子句,即在其中添加对保密级别标记的判断条件,就可以实现按主体、客体的保密级别进行多级保密安全管理的策略,并符合系统保密需求<sup>[8-9]</sup>。

3 数据库表设计

为了在数据库应用程序中综合应用上述访问控制策略的优点,实现涉密信息保密或安全数据库应用程序,其关键是要设计出逻辑严密、维护方便、功能完备的数据库表,如图 3 所示。

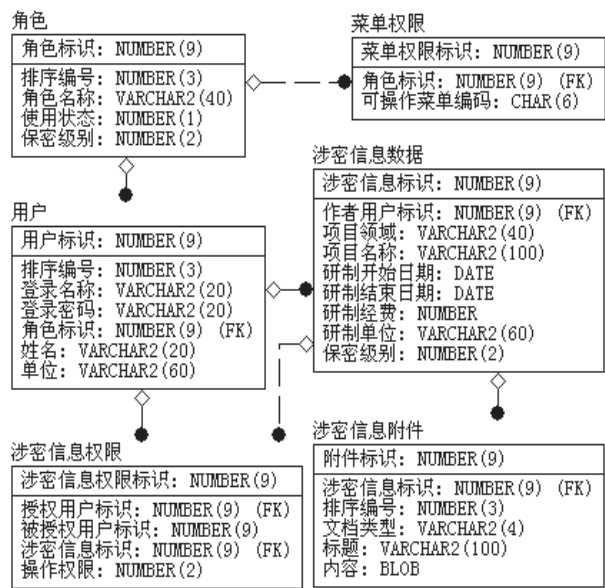


图 3 涉密信息管理系统数据库表逻辑模型

其中,“角色”表保存角色名称(如绝密作者、机密作者、秘密作者、公开作者,绝密管理员、机密管理员、秘密管理员、公开管理员,安全管理员),使用状态(如 1 为激活、0 为去活),角色的保密级别(如 3 为绝密、2 为机密、1 为秘密、0 为公开);“菜单权限”表保存角色被授予的、可操作菜单项的编码信息;“用户”表保存用户信息,包括身份验证所需的登录名称、登录密码,

以及用户的角色和其他个人信息;“涉密信息数据”表保存涉密信息的各种数据字段信息,涉密信息的保密级别(如 3 为绝密、2 为机密、1 为秘密、0 为公开);“涉密信息附件”表是涉密信息数据表的从表,保存与某条涉密信息相关的各种文档附件信息,文档类型可以是 doc、xls、pdf 等;“涉密信息权限”表保存涉密信息作者用户向其他涉密信息作者用户授予的、能操作的涉密信息及其操作权限(如 1 为查询、2 为维护)<sup>[10-12]</sup>。

4 程序模块设计

系统的各项功能模块或操作窗口可以分为三类,分别放入“系统安全维护”、“涉密信息撰写操作”、“涉密信息查询管理”三个一级菜单中。

在“系统安全维护”一级菜单中包括如下功能模块或菜单项,以便灵活方便地进行安全或保密权限的维护或定制。

1)角色维护模块。系统的安全管理员用该模块维护系统中的角色及其保密级别。

2)菜单操作权限授权模块。系统的安全管理员用该模块将系统的菜单操作权限向系统中的角色进行授予或回收。

3)用户维护模块。系统的安全管理员用该模块维护使用系统的用户。包括用户的登录名称、密码,角色,个人信息等。

4)涉密信息操作权限授权模块。涉密信息作者用户用该模块将自己撰写的涉密信息的操作权限向其他涉密信息创建者用户进行授予或回收。

5)更改密码模块。涉密信息作者用户用该模块更改自己的登录密码。

在“涉密信息撰写操作”一级菜单中,可以灵活安排几个功能模块或菜单项,以便涉密信息作者用户、获得授权的其他涉密信息作者用户能按各种方式撰写、操作各自的涉密信息<sup>[4]</sup>。

在“涉密信息查询管理”一级菜单中,可以灵活安排几个功能模块或菜单项,以便涉密信息管理者用户能按各种方式查询、管理各自的涉密信息<sup>[4]</sup>。

这些程序模块主要就是根据上述数据库表的设计及其数据库表中的当前数据,并综合应用上述访问控制模型,以及系统保密需求,在安全保密的前提下实现涉密信息的撰写管理功能<sup>[13-14]</sup>。

5 程序实现方案

在具体实现时除了通用技术之外,还应该根据所采用的数据库(如 Oracle)、程序开发工具(如 Power-Builder)的特殊技术,来解决相应的关键技术问题<sup>[3]</sup>。

1)主键标识方案。在 Oracle 数据库中创建一个 9



位数字的序列(sequence),在各个数据库表中增加记录时,记录的主键标识都从该序列中取 nextval 值。

2) 菜单编码方案。采用 6 位数字编码,每 2 位表示一级菜单,可以表示三级菜单,每级菜单可以有 99 个菜单项。如 010203 表示 01 号一级菜单中的 02 号二级菜单中的 03 号三级菜单。

3) 菜单操作权限控制方案。用户登录后,程序从用户表中获得该用户的角色标识,如果角色表中该角色的使用状态是启用,则通过 DataStore 对象,从菜单权限表获得该角色可操作的各个菜单项的菜单编码,然后根据菜单编码的编码规则,遍历各级菜单直到该菜单项,将该菜单项的 enabled 属性设置 True(可操作)或设置成 False(变灰色不可操作),即进行访问控制,直到处理完所有菜单项为止<sup>[5]</sup>。

4) 按钮操作权限控制方案。被其他涉密信息作者用户授予查询或维护其涉密信息的涉密信息作者用户在进入涉密信息撰写窗口后,程序将在该窗口的“信息列表”标签页的“涉密信息”数据窗口控件中同时显示授权用户、被授权用户的涉密信息。如果被授权用户选择到授权用户的涉密信息时,程序就根据被授予的操作权限是“查询”还是“维护”来设置该窗口的操作按钮的 enabled 属性,即进行访问控制。例如,当被授予的操作权限是“查询”时,则将该窗口的“信息列表”标签页的“查询”按钮的 enabled 属性设置为 True(可操作),而将“增加”、“插入”、“删除”、“保存”按钮的 enabled 属性设置为 False(变灰色不可操作);同时将该窗口的“附件列表”标签页的“查看编辑文档”按钮的 enabled 属性设置为 True,将“创建新文档”、“保存文档内容”按钮的 enabled 属性设置为 False<sup>[3]</sup>。

5) 文档撰写方案。当在涉密信息撰写窗口的“信息列表”标签页的“涉密信息”数据窗口控件中选择一条记录时,就在该窗口的“附件列表”标签页的“文档列表”下拉列表控件中逐个显示该记录的所有文档附件,当在其中选择一个文档附件时,程序用 selectblob 语句从涉密信息附件表中获得该文档附件的内容,并显示在该标签页的“文档内容”OLE 控件中。此时单击“查看编辑文档”按钮,程序根据该文档的类型,激活相应的 Windows 程序,然后用户在其中查看编辑文档的内容,保存后退出该 Windows 程序,单击“保存文档内容”按钮,最后程序用 updateblob 语句将 OLE 控件中的内容保存到涉密信息附件表中。


## 6 结束语

加强数据库应用程序的安全不仅仅是对数据库应用程序进行安全加固,而是要从设计阶段开始就要综合利用各种访问控制策略,从根本上保证数据库应用程序的安全,尤其是要将基于安全标记的 BLP 访问控制模型应用到数据库应用程序的安全解决方案中,使之达到 TCSEC 的 B1 级标准,成为一个安全数据库应用程序。

### 参考文献:

- [1] 陈越. 数据库安全[M]. 北京:国防工业出版社,2011.
- [2] Pfleer C P. 信息安全原理与应用[M]. 北京:电子工业出版社,2007.
- [3] 路川. Oracle 10g 宝典[M]. 北京:电子工业出版社,2011.
- [4] Whitten J L. 系统分析与设计导论[M]. 北京:机械工业出版社,2012.
- [5] 郭宝利. PowerBuilder 9.0 实用解析[M]. 北京:电子工业出版社,2004.
- [6] Yuan Changan, Tang Changjie, Wen Yuanguang, et al. Intelligent function model discovery system based upon gene expression programming[J]. Journal of Computational Information Systems, 2006, 2(4): 1299-1304.
- [7] Lopes H S, Weinert W R. Egipsys: an enhance gene expression programming approach for symbolic regression problems[J]. International Journal of Applied Mathematics and Computer Science, 2004, 14(3): 375-384.
- [8] Micali S. Simple and fast optimistic protocols for fair electronic exchange[C]//Proc of the twenty-second annual symposium on principles of distributed computing. New York, NY, USA: ACM, 2003: 12-19.
- [9] 李昕昕, 严张凌, 王赛兰. 改进的基于角色的通用权限管理模型及其实现[J]. 计算机技术与发展, 2012, 22(3): 240-244.
- [10] Pagnia H, Gartner C. On the impossibility of fair exchange without a trusted third party[R]. Darmstadt: Darmstadt University of Technology, 1999.
- [11] 季小明, 汪家常. 基于 NET 动态用户权限管理模型的设计与实现[J]. 计算机技术与发展, 2006, 16(10): 202-204.
- [12] 林庆, 王飞, 吴旻, 等. 基于专家系统的入侵检测系统的实现[J]. 微计算机信息, 2007, 23(9): 61-63.
- [13] 邓小善. 基于层次模型的网络数据库安全体系的构建[J]. 计算机技术与发展, 2009, 19(6): 175-178.
- [14] 李澜, 冯登国, 徐震. 多级安全 OS 与 DBMS 模型的信息流及其一致性分析[J]. 计算机学报, 2005, 28(7): 1123-1129.

# 基于访问控制的涉密信息管理安全解决方案

作者: [胡欣杰](#), [路川](#), [HU Xin-jie](#), [LU Chuan](#)  
作者单位: [装备学院 信息装备系, 北京, 101416](#)  
刊名: [计算机技术与发展](#)   
英文刊名: [Computer Technology and Development](#)  
年, 卷(期): 2014(8)

本文链接: [http://d.g.wanfangdata.com.cn/Periodical\\_wjtz201408030.aspx](http://d.g.wanfangdata.com.cn/Periodical_wjtz201408030.aspx)