

访问控制策略的研究

司莹莹¹, 王 洪²

(1. 北京交通大学 软件学院, 北京 100044;

2. 高等教育出版社, 北京 100011)

摘 要:访问控制策略在软件系统中起着重要的作用,与软件系统的安全性和可靠性有着直接的联系。选取何种访问控制策略,如何对系统的访问控制权限进行规划,是摆在软件分析设计人员面前的一个复杂课题。介绍了自主访问控制、强制访问控制和基于角色的访问控制三种主流的访问控制策略,并进行了对比分析。基于角色的访问控制策略依据两个重要的安全原则,强化了对访问资源的安全访问控制,并且解决了具有大量用户和权限分配的系统中管理的复杂性问题,广泛应用于当前流行的数据管理系统。

关键词:自主访问控制;强制访问控制;基于角色的访问控制;安全

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2007)04-0100-04

Research on Access Control Strategy

SI Ying-ying¹, WANG Hong²

(1. School of Software, Beijing Jiaotong University, Beijing 100044, China;

2. Higher Education Press, Beijing 100011, China)

Abstract: Access control strategy plays an important role in software system. It influences the security and reliability of software system. Which strategy will be applied, is a complex problem to plan and design authorization system. This paper presents three mainstream access control strategies: discretionary access control, mandatory access control and role-based access control, and compares with each other. Role-based access control policy strengthens access control to resources by two important security policies, and settles the management questions in a system of many users and permissions. It is applied to current data-management system widely.

Key words: discretionary access control; mandatory access control; role-based access control; security

0 引 言

早期的计算机系统没有对访问系统资源的用户作任何操作权限上的限制。但是随着计算机资源的不断丰富,一个用户不需要也不应该可以访问任何资源,这就需要利用访问控制来加以管理。访问控制的基本任务是在对主体进行识别和认证的基础上,判断是否允许主体访问客体,并以此限制主体对客体的访问。

由于所有的安全控制最终的目的是实现对资源的安全使用,访问控制策略便成为安全协议中的核心问题。为了便于理解,先简要说明后面要用到的几个概念。

资源:需要纳入安全管理的对象,可能是物理上的实体,也可能是逻辑对象,如告警数据、性能数据等。

操作:一组命令的集合。

权限:用户在系统中进行任何一个操作,对资源的任何一种访问都会受到系统的限制,用户对特定的资源进行特定操作的许可称为权限。

用户:只有安全管理认可的有效用户才能够登录到系统中。

授权:授予用户访问某种资源某种操作的权限。

1 访问控制策略的实现及分类

国际标准化组织(ISO)在其网络安全体系的设计标准(ISO7498-2)中,定义了五大安全服务功能:身份认证服务、访问控制服务、数据保密服务、数据完整性服务、不可否认性服务。作为五大安全服务之一的访问控制服务在网络安全体系结构中具有不可替代的作用,它可以限制对关键资源的访问,防止非法用户的侵入或者合法用户的越权操作所带来的破坏。

访问控制(Access Control)是通过某种途径显式地准许或限制访问能力及范围的一种方法。访问控制限

收稿日期:2006-06-13

作者简介:司莹莹(1982-),女,山东淄博人,硕士研究生,研究方向为软件工程;王 洪,教授,硕士生导师,研究方向为网络与数据库。

制访问主体(或称为发起者,一个主动的实体,如用户、进程、服务等)对访问客体(需要保护的资源)的访问权限,从而使计算机系统在合法范围内使用,访问控制机制决定用户及代表一定用户利益的程序能做什么以及做到什么程度。

从概念上说,访问控制总是可以通过使用和维护一个访问控制矩阵(ACM, Access Control Matrix)来实现。访问控制矩阵中每一行代表一个用户,每一列代表一项系统资源,矩阵中的每项内容则表示用户对资源访问的模式。显然,如果系统中用户和资源都非常多,而因为每个用户可能访问的资源有限,这将出现庞大的访问控制矩阵中存在很多空值的情况,从而造成存储矩阵空间的浪费。不仅如此,访问控制矩阵存放在何处也是一个问题。简单的解决方式是将访问控制矩阵按行或按列进行划分。

如果是按行划分,得到每个用户基于能力的访问控制表中指明可以使用的对象和对对象的访问能力。

如果是按列进行划分,可以得到已广泛被应用的访问控制列表(ACL, Access Control List)。对于每个资源,访问控制列表中列出可能的用户和用户的访问权限。基本访问控制列表的改进是将用户分成组,以三种层次提供访问权限(所有人、同组所有人、组中某个人)。该表由资源拥有方或系统加以维护。但不论是以哪一种方式,在构造表的时候须知道所有用户对使用所有可能资源的需求及访问能力。同时它还会带来所有集中式管理可能引起的效率问题^[1]。

通常根据访问控制矩阵中每一项的访问权限由谁来决定,可以将访问控制策略分为自主访问控制(DAC)和强制访问控制(MAC)。

目前,常用的访问控制策略主要有 DAC, MAC 和基于角色的访问控制(RBAC)。下面就这三种不同的访问控制策略分别进行描述。

1.1 自主访问控制

自主型访问控制(DAC, Discretionary Access Control)最早出现在 20 世纪 70 年代初期的分时系统中,它是多用户环境下最常用的一种访问控制技术,在目前流行的 Unix 类操作系统中被普遍采用。DAC 基于这样的思想:客体的主人(即资源所有者)全权管理有关该客体的访问授权,有权泄露、修改该客体的有关信息。因此,有些学者把 DAC 称为“基于主人的访问控制”。为了提高效率,系统不保存整个访问控制矩阵,在具体实现时给予矩阵的行或列来实现访问控制。

自主访问控制的特点是,资源的属主将访问权限授予其他用户或用户组后,被授权的用户便可以自主地访问资源,或者将权限传递给其他的用户。

自主访问控制策略已经在流行操作系统(如 Unix, Window NT 等)和许多数据库系统中得到广泛使用。但自主访问控制策略的资源管理权比较分散,信息容易泄漏,难以抵御特洛伊木马的攻击。

1.2 强制访问控制

强制型访问控制(MAC, Mandatory Access Control)最早出现在 1965 年由 AT&T 和 MIT 联合开发的安全操作系统 Multics 系统中,在 1983 年美国国防部的可信计算机系统评估标准中被用作 B 级安全系统的主要评价标准之一。

常用的强制访问控制是指预先定义用户的可信任级别及资源的安全级别,当用户提出访问请求时,系统对两者进行比较以确定访问是否合法。

在强制访问控制系统中,所有主体(用户,进程)和客体(文件,数据)都被分配了安全标签,安全标签标识一个安全等级。

- (1)主体(用户,进程)被分配一个安全等级;
- (2)客体(文件,数据)也被分配一个安全等级;
- (3)访问控制执行时对主体和客体的安全级别进行比较。

在强制式策略中,资源访问授权根据资源和用户的相关属性确定,或者由特定用户(一般为安全管理员)指定。它的特征是强制规定访问用户必须或者不许访问资源或执行某种操作。资源特征是强制规定访问客体强制访问控制策略目前主要应用于军事系统或是安全级别要求较高的系统之中。强制访问控制策略对特洛伊木马攻击有一定的抵御作用,即使某用户进程被特洛伊木马非法控制,也不能随意扩散机密信息。

1.3 基于角色的访问控制

基于角色的访问控制技术(RBAC, Role - Based Access Control)出现于 90 年代,它是从传统的自主访问控制和强制访问控制发展起来的。“角色”概念的出现有效地克服了 DAC 和 MAC 的缺陷,有效减少了授权管理的复杂性,更加有利于安全策略的实施。

基于角色的访问控制策略的基本思想是在用户与权限之间引入角色的概念,利用角色来实现用户和权限的逻辑隔离,即用户与角色相关联,角色与权限相关联,通过给用户分配角色而使用户获得相应的权限。

目前对于 RBAC 的研究较为深入的有以 NIST (National Institute of Standards and Technology)研究会的 John F. Barkley 为首的 DAC 研究小组和美国 George Mason 大学 Ravi Sandhu 等人。

NIST 的 DAC 研究小组主要提出了 RBAC 在商业和政府中的应用架构,特别提出了 RBAC/Web 模型,将 RBAC 独立于 Web 服务器和浏览器,给 Intranet 提

供了一种方便灵活又安全可靠的访问控制策略。RBAC既可以嵌入到操作系统或者数据库系统中,也可以在应用级中实现。

以 Sandhu 为代表的学院派主要提出了 RBAC96 和 RBAC97 模型。Sandhu 在 1996 年提出的 RBAC96 模型是模型的基础, Sandhu 等人认为 RBAC 是个内容广泛的概念,难以用一个模型全面地描述,他将该模型划分为 4 个部分:RBAC0, RBAC1, RBAC2 和 RBAC3,如图 1 所示。

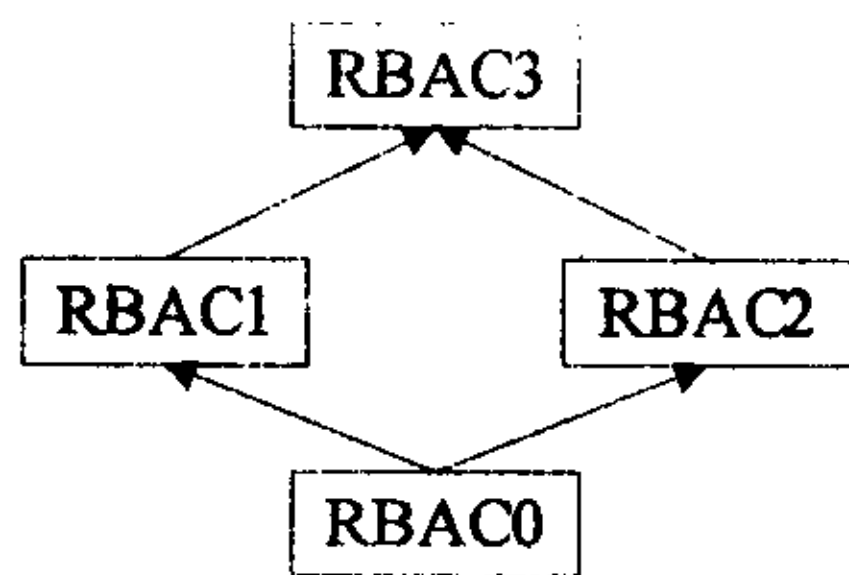


图 1 RBAC96 模型 4 部分的关系

RBAC96 模型 4 部分的关系是:

(1)RBAC0 是基本模型,定义了系统所需的最小需求;

(2)RBAC1 在 RBAC0 的基础上添加了角色层次的概念;

(3)RBAC2 在 RBAC0 的基础上添加了约束的概念;

(4)RBAC3 包含了 RBAC1 和 RBAC2,通过传递,也包含了 RBAC0。

为了更好地说明基于角色的访问控制策略,先简要说明与该策略相关的几个概念。

角色:角色与权限相联系,为权限的集合,是权限的分配对象。

用户:只有安全管理认可的有效用户才能够登录到系统中。不能直接给用户分配权限,权限是分配给角色的,当某个角色被分给用户以后,该用户就拥有了该角色的权限。

静态互斥(SSD, Static Separation of Duties):角色 A 与角色 B 为静态互斥关系,当且仅当角色 A、角色 B 不能同时授予同一个用户。

动态互斥(DSD, Dynamic Separation of Duties):角色 A 与角色 B 为 DSD 关系,当且仅当角色 A、角色 B 虽然可以同时授予同一个用户,但两角色中的权限不能同时执行。

权限与操作和资源相联系:不同的操作和资源的组合构成了不同的权限。

角色与权限相联系:角色和权限是多对多的关系^[2]。一个权限可以分配给一个或多个角色;一个角色也可以拥有一个或多个权限。

用户与角色相联系:用户和角色也是多对多的关

系。一个用户可以具有一个或多个角色;一个角色也可以分配给一个或多个用户。用户、角色、权限以及操作、资源的关系如图 2 所示。

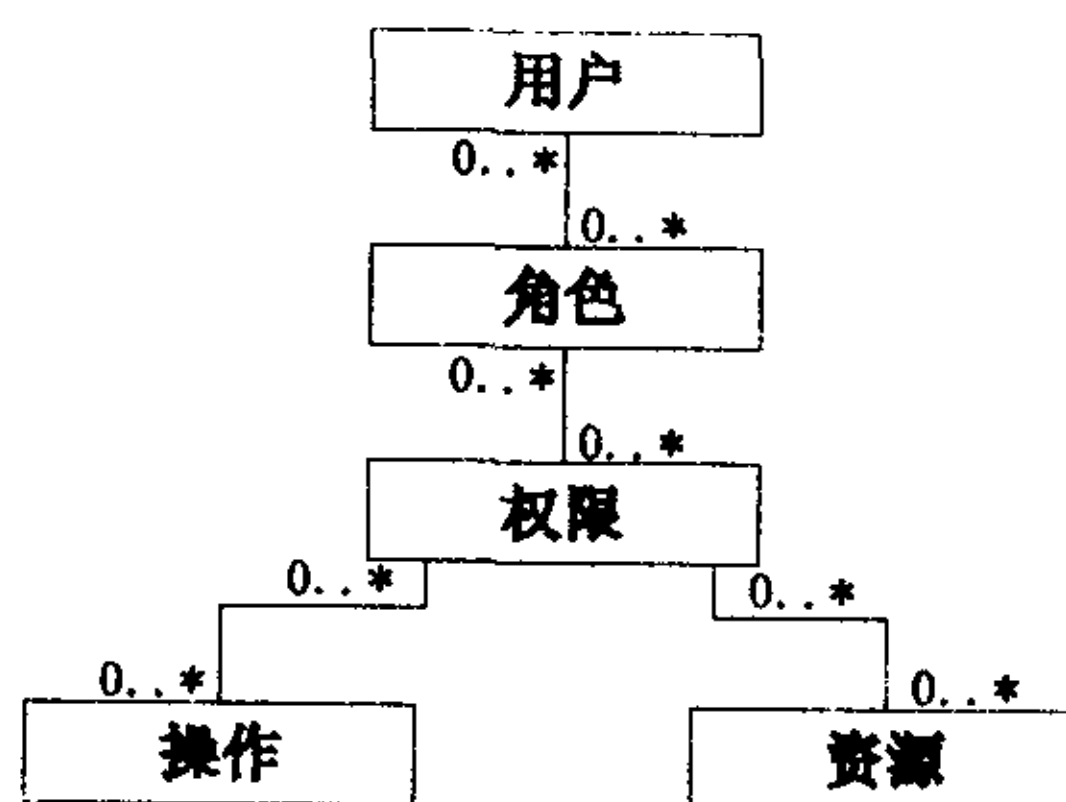


图 2 用户、角色、权限以及操作、资源的关系

由系统管理员根据需要定义角色,然后给角色设置适当的访问权限,再根据用户的不同身份将角色分配给不同的用户^[1]。这样可以减少授权的复杂性,为系统管理员提供一个比较好的实现安全管理的环境。

RBAC 并不是针对特定访问控制策略,角色之间、角色与权限、角色与用户的关系可以根据具体的应用环境和策略进行配置和指定^[3]。

RBAC 模型的两个安全原则:

1)责任分离原则。对于一个特定的事务集,可能一个用户并不能执行这个事务集中的每一个事务。例如,在银行信贷处理中,不存在一个职员既可以处理信贷事务,又能够处理审计事务。信贷和审计这两个相关的职责,不能由一个用户来承担。责任分离原则的实施有角色静态互斥和动态互斥两种,具体操作在角色约束中来完成^[4]。

2)最小特权原则。它保证某个角色在完成相应职责时,拥有所需的所有许可,并且这个许可集决不超过他实际所需的许可,即不给角色分配多余的权限许可,保证拥有这个角色的用户具有最小的特权。

另外,RBAC 还要遵循下面三条访问控制规则:

(1)如果一个主体不具有任何角色,那么该主体无权执行任何事务,这一规则保证任何主体只有通过角色才能完成其功能,而不能绕过角色直接访问客体;

(2)主体的活动角色必须经过授权,即确保用户只能扮演经过授权的角色;

(3)如果某个主体要执行某个事务,那么事务必须授权给该用户的当前角色。

2 DAC, MAC 与 RBAC 的比较

DAC 技术存在明显的不足,主要体现在以下几方面:

(1)既然主体可任意在系统中规定谁可以访问它们的资源,那么系统管理员就难以确定哪些用户对哪些资源有访问权限,不利于实现统一的全局访问控制。

(2)在许多组织中,用户对它们所能访问的资源并不具有所有权,组织本身才是系统中资源的真正拥有者。而且,各组织希望访问控制实现能与组织内部的安全策略相一致,并由管理部门统一实施访问控制,不允许用户自主地处理,而 DAC 却存在着用户滥用职权的问题。

(3)用户间的关系不能在系统中体现出来,不易管理。

(4)信息容易泄露,不能抵御特洛伊木马(Trojan Horse)的攻击。特洛伊木马是嵌入在合法程序中的一段以窃取或破坏信息为目的的恶意代码。在自主型访问控制下,一旦带有特洛伊木马的应用程序被激活,特洛伊木马便可以任意泄露和破坏接触到的信息,甚至改变这些信息的访问授权模式。

强制访问控制在主体访问级别和客体安全级别的划分上与现实要求往往无法一致,所以用这两种访问控制方法来处理日益复杂的数据资源安全问题就变得不合实际且非常困难^[5]。基于角色的访问控制通过引入角色而实现了用户与权限的逻辑分离。对于一个存在大量用户和权限分配的系统来说,从大量的权限管理转到管理、操纵少量的角色,这样简化了权限分配管理,提高了安全管理的效率和质量^[4]。通常情况下,角色和权限之间的变化比角色和用户关系之间的变化相对要慢得多,并且把用户注册到角色中不需要很多技术,而配置权限到角色的工作则比较复杂^[6],需要由技术人员来进行,但是不给他们委派用户的权限。这与现实中的情况正好一致。

RBAC模型的核心是角色(Role)。基于角色的访问控制策略具体有下列优点:

①减少权限管理:不用显式地将同一组权限授权给几个用户,只需将此组权限分配给特定角色,然后将该角色授权给相应用户。

②动态权限管理:如果一组权限需要改变,只需修

改分配给角色的权限,所有被授予该角色的全部用户的安全域将自动地反映对角色所做的修改。

③权限的选择可用性:授权给用户的角色可选择地使其使能(可用)或不使能(不可用)。

④应用可知性:当一个用户用某一用户名执行应用时,该应用可查询字典,将自动地选择使角色使能或不使能。

⑤专门的应用安全性:角色使能可由口令保护,应用可提供正确的口令使角色使能,达到专门的应用安全性,因用户不知其口令,不能使角色使能。

3 小 结

介绍并分析了当前流行的三种访问控制技术,并对三种访问控制技术的优缺点进行了比较。因为基于角色的访问控制策略所具备的诸多优点而成为主流的访问控制策略,像 Linux 等操作系统^[3]、Oracle、SQL Server 等主流的数据库软件在安全管理方面都不同程度地借鉴并实现了 RBAC 模型^[1],是公认的极具发展潜力的访问控制策略,正得到广大学者广泛的关注和深入的研究。

参考文献:

- [1] 结凤克,朱爱军,马桂杭,等. Oracle 系统中基于角色管理的访问控制模型[J]. 中原工学院学报,2003,14:33-35.
- [2] 耿 晖,王海波. 基于 XML 的角色访问控制(RBAC)[J]. 计算机应用研究,2002(12):14-15.
- [3] 曾小超,姚立红,曾庆凯,等. 操作系统安全增强技术研究进展[J]. 高技术通讯,2003(7):106-110.
- [4] 张志勇. 基于角色的工程数据库安全管理的设计与实现[J]. 计算机与现代化,2004(5):68-70.
- [5] 谭文芳,胡南军,陈贵海. 基于 CORBA 的分布式访问控制[J]. 小型微型计算机系统,2001,22(11):1359-1363.
- [6] 张振洋,顾学春,张曼平. 分布式数据库应用系统安全管理实现方法的研究[J]. 西安交通大学学报,1999,33(7):23-27.

(上接第95页)

的实现方式也是多种多样的。文中讨论的这种方式结构灵活、实用。

此动态报表实现方式的实用性已在实际的项目中进行了验证。

参考文献:

- [1] 沈 俊,王志坚. .Net 主流技术在 GIS 中的应用研究[J]. 计算机技术与发展,2006,16(S):197-200.

- [2] Eckel B. Java 编程思想[M]. 第2版. 北京:机械工业出版社,2002.
- [3] Pantham S. 深入学习:JFC 2D 图形图像编程[M]. 北京:电子工业出版社,2002.
- [4] Sun Microsystems Corp. The Java Tutorial[EB/OL]. 2005-04-15. <http://java.sun.com/docs/books/tutorial>.
- [5] 李 莉,郭忠文. 基于 Web 的报表打印方法[J]. 计算机工程与设计,2004,25:803-805.