基于角色的访问控制研究

汪厚祥, 李　卉
(海军工程大学 信息与电气学院, 湖北 武汉 430033)

摘　要: 基于角色的访问控制 RBAC是一种方便、安全、高效的访问控制机制。分析了 RBAC 的总体思想和模型,介绍了 RBAC 的特点及应用优势,最后研究了 RBAC 机制的实现。

关键词: 自主访问控制; 强制访问控制; 基于角色的访问控制; 角色等级; 权限; 限制
中图法分类号: TP309. 2　　**文献标识码**: A　　**文章编号**: 1001-3695(2005)04-0125-03

Research of Role-based Access Control

WANG Hou-xiang, LI Hui
(School of Information & Electrical, Naval University of Engineering, Wuhan Hubei 430033, *China)*

Abstract: Role-Based Access Control(RBAC) is a kind of access control mechanism which is convenient, secure and of high-performance. Analyses the general principle and model of RBAC, introduces the characteristic and application advantages of RBAC. Finally studies how to implement RBAC.

Key words: DAC(Discretionary Access Control) ; MAC(Mandatory Access Control) ; RBAC; Role Hierarchies; Permission; Constraints

1　引言

随着计算机应用的日益普及,特别是网络和数据库的迅速发展,如何在发展和推广网络应用的同时进一步提高访问控制的安全与效率,已经成为目前网络界所必须研究和解决的课题。依据美国国防部制定的可信计算机系统评估准则(TCSEC) 的主要目标,即阻止非授权用户对敏感信息的访问,访问控制被分为两类: 自主访问控制(Discretionary Access Control, DAC) 和强制访问控制(Mandatory Access Control, MAC) 。DAC 是计算机系统中实现最多的访问控制机制,其主要特征表现在: 主体可以自主地把自己所拥有客体的访问控制权限授予其他主体或从其他主体收回所授予的权限; 而 MAC 则根据客体的敏感级和主体的许可级来限制主体对客体的访问,多用于多级军用系统。

近年来,随着计算机在商业和民事部门的广泛应用,尤其是 Intranet 的兴起,对访问控制也提出了更高的要求。例如 DAC 将赋予或取消访问权限的一部分权利留给用户个人,管理员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。在许多组织中,用户对他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所有者。各组织一般希望访问控制与授权机制的实现结果能与组织内部的规章制度相一致,并且由管理部门统一实施访问控制,不允许用户自主地处理。显然传统的 DAC, MAC 已经不能适应这些需求。

20 世纪 90 年代初,美国国家标准和技术研究院(National Institute of Standards and Technology) 着手组织对一种新的访问控制技术——基于角色的访问控制(RBAC) 进行研究。这种技术能够减少授权管理的复杂性,降低管理开销,而且还能为管理员提供一个比较好的实现复杂安全政策的环境。

收稿日期: 2004-01-18; 修返日期: 2004-06-03

2　RBAC 概述

2.1　RBAC 的总体描述

RBAC 的核心思想就是将访问权限与角色相联系,通过给用户分配合适的角色,让用户与访问权限相联系。角色是根据企业内为完成各种不同的任务需要而设置的,根据用户在企业中的职权和责任来设定他们的角色。用户可以在角色间进行转换,系统可以添加、删除角色,还可以对角色的权限进行添加、删除。这样通过应用 RBAC 将安全性放在一个接近组织的自然层面上进行管理。

2.2　角色的概念

在现实生活中经常提到某人扮演了什么角色,比如是局长还是副局长。不过在 RBAC 中角色与实际的角色概念有所不同。在 RBAC 中角色可以看作是一组操作的集合,不同的角色具有不同的操作集,这些操作集由系统管理员分配给角色。

同一个用户可以是多个角色的成员,即同一个用户可以扮演多种角色; 同样,一个角色可以拥有多个用户成员。这与现实是一致的,因为一个人可以在同一个部门中担任多种职务,而且担任相同职务的可能不止一人。因此, RBAC 提供了一种描述用户和权限之间的多 - 多关系。

3　RBAC 模型构件分析

从 1996 年发展到现在,专家们已经提出了一些 RBAC 模型,这里主要对 RBAC 研究较为深入的美国 George Mason 大学 RBAC96 模型进行探讨。该模型为开发实际的应用系统提供了一个总方针,并为 RBAC 用户提供了评判系统的标准,其基本结构如图 1 所示。其中:

RBAC0——基本模型,规定了任何 RBAC 系统所必须的最

小需求。

RBAC1——在 RBAC0 的基础上增加了角色等级(Role Hierarchies) 的概念。

RBAC2——在 RBAC0 的基础上增加了限制(Constraints) 的概念。

RBAC3——包含了 RBAC1 和 RBAC2, 依传递性也间接包含了 RBAC0。

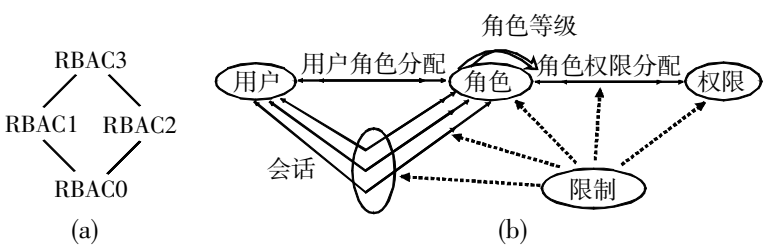

图 1 RBAC 模型

(1) RBAC0(基本模型) 。我们对 RBAC0 模型定义如下:

- U, R, P, S: 用户, 角色, 权限, 会话;
- PA⊆P ×R: 权限分配, 多对多的关系;
- UA ⊆U ×R: 用户分配, 多对多的关系;
- User: S→U, 每一个会话 s_i 对应单一用户 user(s_i) 的映射;
- Roles: $S \rightarrow 2^R$ (会话 s_i 到角色集合 role(s_i) $\subseteq \{ r \mid (user(s_i), r) \in UA \}$ 的映射, 并且 s_i 具有权限 $U_{r \le role(s_i)} \{ p \mid (p, r) \in PA \}$

易见, RBAC0 模型由三个实体组成, 分别是: 用户(U) 、角色(R) 、权限(P) 。其中用户是指自然人; 角色就是组织内部一件工作的功能或者工作的头衔, 表示该角色成员所授予的职权和责任; 权限是对系统中一个或多个客体以特定方式进行存取的许可, 系统中拥有权限的用户可以执行相应的操作。

用户与角色之间以及角色与权限之间用双箭头相连表示用户角色分配 UA 和角色权限分配 PA 关系都是多对多的关系, 即一个用户可以拥有多个角色, 一个角色也可被多个用户所拥有。同样地, 一个角色拥有多个权限, 一个权限能被多个角色所拥有。

用户建立会话从而对资源进行存取, 每个会话 S 将一个用户与他所对应的角色集中的一部分建立映射关系, 这个角色会话子集称为被会话激活的角色集。于是, 在这次会话中, 用户可以执行的操作就是该会话激活的角色集对应的权限所允许的操作。

(2) RBAC1(在 RBAC0 上引入角色等级) 。角色等级 RH 可以反映一个组织或部门的责任权力关系, 形成一种偏序关系。

对 RBAC1 模型定义如下:

- U, R, P, S, PA, UA 与 RBAC0 相同;
- RH⊆ R ×R 是关于 R 的偏序关系;
- Roles: $S \rightarrow 2^R$ (其中 $role(s_i) \subseteq \{ r \mid (\exists r' \ge r) [(user(s_i), r') \in UA] \}$ 以及会话 s_i 具有权限 $U_{r \le role(s_i)} \{ p \mid (\exists r' \ge r) [(p, r') \in PA \}$ 。有时由于某些原因, 不希望继承者享有被继承的全部权力, 此时就可以构造一些新的角色称为私有角色, 而将用户分配给这些私有角色。

(3) RBAC2 (在 RBAC0 上引入限制) 。RBAC2 除继承 RBAC0 已有的特征外, 引入了限制集合, 规定了 RBAC0 各种部件的操作是否可被接受, 只有可接受的操作才被允许。限制有许多种, 例如:

- 互斥角色(Mutually Exclusive Roles) 。同一用户仅可分配到一互斥角色集合中至多一个角色, 这样支持了职责分离的原则; 而在权限分配时也有互斥限制, 同样的权限在一个互斥集合中至多分配给一个角色, 这样尤其有利于对比较重要的权限进行分配。
- 基数限制(Cardinality Constraints) 。一个用户可拥有的角色数目受限; 同样, 一个角色对应的权限数目也受限。
- 先决条件角色。可以分配角色给用户仅当该用户已经是另一角色的成员; 对应地, 可以分配权限给角色, 仅当该角色已经拥有另一种操作权限。比如, 当用户拥有了角色 A 时才可以分配角色 B 给用户, 而且在其他任何情况下角色 B 都不能分配给用户, 那么角色 A 即为角色 B 的先决条件角色, 有的时候我们也称为必备角色。同理类推必备权限。
- 时间频度限制。规定特定角色权限的使用时间及频度。
- 运行时互斥。例如允许一个用户具有两个角色的成员资格, 但是在运行中不能同时地激活这两个角色。

(4) RBAC3 是 RBAC1 和 RBAC2 两者的结合, 其模型如图 1(b) 所示。

RBAC96 模型提供了一个分析现存系统能力, 评价其对 RBAC 支持程度的框架, 也提供了软件开发者在未来系统中实现基于角色访问控制的准则。但随着研究的深入, 原有模型将得到进一步的完善。

4 RBAC 的特点及应用优势

4.1 RBAC 的几大特点

(1) 访问权限与角色相关联, 不同的角色有不同权限。用户以什么样的角色对资源进行访问, 决定了用户拥有的权限以及可执行何种操作。

(2) 角色继承。角色之间可能有互相重叠的职责和权力, 属于不同角色的用户可能需要执行一些相同的操作。RBAC 采用角色继承的概念, 如角色 2 继承角色 1, 那么管理员在定义角色 2 时就可以只设定不同于角色 1 的属性及访问权限, 避免了重复定义。

(3) 最小权限原则, 即指用户所拥有的权力不能超过他执行工作时所需的权限。实现最小特权原则, 需要分清用户的工作职责, 确定完成该工作的最小权限集, 然后把用户限制在这个权限结合的范围之内。一定的角色就确定了其工作职责, 而角色所能完成的事物蕴涵了其完成工作所需的最小权限。用户要访问信息首先必须具有相应的角色, 用户无法绕过角色直接访问信息。

(4) 职责分离。例如在银行业务中, 授权付款与实施付款应该是分开的职能操作, 否则可能发生欺骗行为。一般职责分离有两种方式: 静态和动态。

(5) 角色容量。在一个特定的时间段内, 有一些角色只能由一定人数的用户占用。在创建新的角色时应该指定角色的容量。

4.2 RBAC 的应用优势

RBAC 最突出的优点就在于系统管理员能够按照部门、企业的安全政策划分不同的角色, 执行特定的任务。一个 RBAC 系统建立起来后主要的管理工作即为授权或取消用户的角色。用户的职责变化时只需要改变角色即可改变其权限; 当组织的功能变化或演进时, 则只需删除角色的旧功能, 增加新功能, 或定义新角色, 而不必更新每一个用户的权限设置。这极大地简

化了授权管理,使对信息资源的访问控制能更好地适应特定单位的安全策略。

RBAC 另一优势体现在为系统管理员提供了一种比较抽象的、与企业通常的业务管理相类似的访问控制层次。通过定义、建立不同的角色、角色的继承关系、角色之间的联系以及相应的限制,管理员可动态或静态地规范用户的行为。

5　RBAC 实现

由于 RBAC 的实现是在异构环境中,所以对 RBAC 的内部观点是多样的,与其实现平台有关。例如,若使用 IBM 的 AIX 4.0 操作系统,使用 IBM 的 DB2 数据库系统,则 RBAC 在网络上的实现可如图 2 来表示。

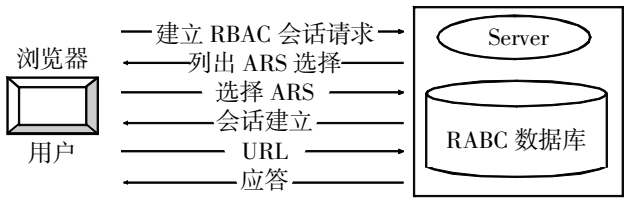

图 2 RBAC 在网络上的实现

在网络系统中使用 RBAC,其实是对网络服务器而言的,对于用户浏览器没有选择。而且在浏览器与服务器之间的通信方式有很多种,如 RBAC/Web CGI 或 RBAC/Web API。当然使用 RBAC 的前提是有效而正确的身份验证和保密地传输数据,这些包括使用用户号/口令字识别法、字段加密、安全 Socket 库(SSL) 和安全 HTTP(HTTPS) 以及私有信息技术协议(PCT) 等。

RBAC/Web 的整个通信过程如下: 当终端用户想要对数据库进行某一操作时,他首先向 RBAC Server 提出建立 RBAC 对话的请求, Server 显示该终端用户可以激活哪些角色(ARS) 。这些角色的选择满足限制条件和角色等级限制以及最小权限原则。用户进行选择后,将 ARS 选择传递给 Server, Server 根据用户的要求建立会话,这时用户就可以对 RBAC 数据库提出操作请求,由 Server 进行相应的处理。最后用户工作完毕, Logout 系统,结束这次会话。在整个过程中, ARS 保持被激活的状态,这些 ARS 构成了 RBAC 会话的基本特征。

6　结束语

一个安全的网络需要可靠的访问控制作保障。在网络规模变大、用户增多、需求更复杂的情况下,传统的 DAC 和 MAC 已经不能满足许多企业或组织的安全需求,基于角色的访问控制 RBAC 便明显地显示出其优越性。

RBAC 为内部网络环境提供了使用基于角色访问控制机制的优势,甚至在改善系统的过程中,可以不改动原有代码而只需加入新的 RBAC 机制来完善现有系统。RBAC 机制的引入,不仅为系统开发提供了一套有力的工具,还为用户评估系统提供了标准。

参考文献:

[1]　avi S Sandhu,　David Ferraiolo, Richard Kuhn. The NIST Model for Role-based Access Control: Towards an Unified Standard[J/OL] . ACM, 2000, 47-63.

[2]　David F Feraiolo, Ravi Sandhu, Serban Gavrila, *et al*. Proposed NIST Standard for Role-based Access Control[J] . ACM Transactions on Information and System Security, 2001, (3) : 224-274.

[3]　Ravi Sandhu, Edward J Coyne. Role-based Access Control Models [J] . Computer, l996, (2) : 38-47.

[4]　Sandhu R, Bhamidipati V, Munawer Q. The ARBAC97 Model for Role-based Administration of Roles[J] . ACM Trans. on Information and Systems Security, 1999, (1) : 105-135.

[5]　Sylvia Osborn, Yuxia Guo. Modeling Users in Role-based Access Control[C] . Berlin: Proceedings of the 5th ACM Workshop on Role-based Access Control(RBAC-00) , 2000. 26-27.

[6]　Ahn GJ, Arvisandhu. Role-based Authorization Constrains Specification[J] . ACM Transcations on Information and System Security, 2002, (3) : 207-226.

[7]　曹天杰,张永平. 管理信息系统中基于角色的访问控制[J] . 计算机应用, 2001, 21(8) : 21-23.

[8]　施景超,孙维详,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.

[9]　李孟珂,余祥宣. 基于角色的访问控制技术及应用[J] . 计算机应用研究, 2000, 17(10) : 44-47.

[10]　马建平,余祥宣,洪帆,等. 基于角色的安全策略[J] . 计算机研究与发展, 1998, 35(5) : 447-450.

作者简介:

汪厚祥(1960-) ,男,教授,博士研究生,主要从事网络应用技术、分布式系统等研究; 李卉(1981-) ,女,硕士研究生,主要从事网络应用技术、分布式系统等研究。

(上接第 77 页)

```
    < OperationName > 车 < / OperationName >
    < OperationDec >
    车端面,钻中心孔,车端面倒角
    < / OperationDec >
    < Equipment > CA6140 < / Equipment >
      < / ProcessDec >
  < / Process >
  < Process > < ! --描述第二道工序-- >
  < ProcessNo > 2 < / ProcessNo >
  < ProcessDec >
  < OperationName > 铣 < / OperationName >
  < OperationDec > 铣六方 < / OperationDec >
  < Equipment > X51 < / Equipment >
  < / ProcessDec >
  < / Process >
  . . .
< / Processes >
```

4　总结

通常对 CAPP 的软件设计都带有局限性,没有考虑工艺卡片和工艺规程变更的可能性以及与其他 CAX 系统集成的趋势,导致 CAPP 的工艺卡片不灵活,工艺设计数据和工艺卡片形式数据绑定在一起,不利于数据的检索和挖掘,使得 CAPP 成为封闭体。这些都源于 CAPP 在数据描述方式上的不规范性。本文提出以 XML 来描述 CAPP 的元数据和工艺数据,使得 CAPP 软件系统具有良好的可扩展性、通用性和集成能力,从而增强了 CAPP 软件系统的生命力,降低了重复开发及维护的成本。

参考文献:

[1]　苏海洋, 刘成颖, 翟昕, 等. 企业集成环境下 CAPP 系统的研究[J] . 现代制造工程, 2002, (5) : 24-26.

[2]　Bertrand Braunschweig, Rafiqul Gani. Software Architectures and Tools for Computer Aided Process Engineering[EB/OL] . http: //www. global-cape-open. org/ pub/ mtGCO. pdf, 2002-02 /2004-01.

[3]　苟凌怡,熊光楞,谢金崇,等. 基于 XML 的产品信息集成关键技术研究[J] . 计算机辅助设计与图形学学报, 2002, 2(14) : 1-6.

作者简介:

刘晨(1980-) ,女,辽宁沈阳人,硕士研究生,主要从事网络化制造技术、CAPP 等方面的研究; 蔡长韬(1963-) ,女,重庆人,教授,博士,研究方向为网络化制造、STEP 标准等。