访问控制模型研究综述

沈海波[1,2], 洪　帆[1]

(1. 华中科技大学 计算机学院, 湖北 武汉 430074; 2. 湖北教育学院 计算机科学系, 湖北 武汉 430205)

摘　要: 访问控制是一种重要的信息安全技术。为了提高效益和增强竞争力,许多现代企业采用了此技术来保障其信息管理系统的安全。对传统的访问控制模型、基于角色的访问控制模型、基于任务和工作流的访问控制模型、基于任务和角色的访问控制模型等几种主流模型进行了比较详尽地论述和比较,并简介了有望成为下一代访问控制模型的 UCON 模型。

关键词: 角色; 任务; 访问控制; 工作流

中图法分类号: TP309　　**文献标识码:** A　　**文章编号:** 1001-3695(2005)06-0009-03

Survey of Research on Access Control Model

SHEN Hai-bo[1,2], HONG Fan[1]

(1. *College of Computer, Huazhong University of Science & Technology, Wuhan Hubei* 430074, *China*; 2. *Dept. of Computer Science, Hubei College of Education, Wuhan Hubei* 430205, *China*)

Abstract: Access control is an important information security technology. To enhance benefits and increase competitive power, many modern enterprises have used this technology to secure their information manage systems. In this paper, several main access control models, such as traditional access control models, role-based access control models, task-based access control models, task-role-based access control models, and so on, are discussed and compared in detail. In addition, we introduce a new model called UCON, which may be a promising model for the next generation of access control.

Key words: Role; Task; Access Control; Workflow

访问控制是通过某种途径显式地准许或限制主体对客体访问能力及范围的一种方法。它是针对越权使用系统资源的防御措施,通过限制对关键资源的访问,防止非法用户的侵入或因为合法用户的不慎操作而造成的破坏,从而保证系统资源受控地、合法地使用。访问控制的目的在于限制系统内用户的行为和操作,包括用户能做什么和系统程序根据用户的行为应该做什么两个方面。

访问控制的核心是授权策略。授权策略是用于确定一个主体是否能对客体拥有访问能力的一套规则。在统一的授权策略下,得到授权的用户就是合法用户,否则就是非法用户。访问控制模型定义了主体、客体、访问是如何表示和操作的,它决定了授权策略的表达能力和灵活性。

若以授权策略来划分,访问控制模型可分为:传统的访问控制模型、基于角色的访问控制(RBAC)模型、基于任务和工作流的访问控制(TBAC)模型、基于任务和角色的访问控制(T-RBAC)模型等。

1　传统的访问控制模型

传统的访问控制一般被分为两类[1]:自主访问控制 DAC(Discretionary Access Control)和强制访问控制 MAC(Mandatory Access Control)。

自主访问控制 DAC 是在确认主体身份以及它们所属组的基础上对访问进行限制的一种方法。自主访问的含义是指访问许可的主体能够向其他主体转让访问权。在基于 DAC 的系统中,主体的拥有者负责设置访问权限。而作为许多操作系统的副作用,一个或多个特权用户也可以改变主体的控制权限。自主访问控制的一个最大问题是主体的权限太大,无意间就可能泄露信息,而且不能防备特洛伊木马的攻击。访问控制表(ACL)是 DAC 中常用的一种安全机制,系统安全管理员通过维护 ACL 来控制用户访问有关数据。ACL 的优点在于它的表述直观、易于理解,而且比较容易查出对某一特定资源拥有访问权限的所有用户,有效地实施授权管理。但当用户数量多、管理数据量大时,ACL 就会很庞大。当组织内的人员发生变化、工作职能发生变化时,ACL 的维护就变得非常困难。另外,对分布式网络系统,DAC 不利于实现统一的全局访问控制。

强制访问控制 MAC 是一种强加给访问主体(即系统强制主体服从访问控制策略)的一种访问方式,它利用上读/下写来保证数据的完整性,利用下读/上写来保证数据的保密性。MAC 主要用于多层次安全级别的军事系统中,它通过梯度安全标签实现信息的单向流通,可以有效地阻止特洛伊木马的泄露;其缺陷主要在于实现工作量较大,管理不便,不够灵活,而且它过重强调保密性,对系统连续工作能力、授权的可管理性方面考虑不足。

2　基于角色的访问控制模型 RBAC

为了克服标准矩阵模型中将访问权直接分配给主体,引起管理困难的缺陷,在访问控制中引进了聚合体(Aggregation)概念,如组、角色等。在 RBAC(Role-Based Access Control)模型[2]中,就引进了“角色”概念。所谓角色,就是一个或一群用户在组织内可执行的操作的集合。角色意味着用户在组织内的责

收稿日期: 2004-04-17; 修返日期: 2004-06-28

任和职能。在 RBAC 模型中,权限并不直接分配给用户,而是先分配给角色,然后用户分配给那些角色,从而获得角色的权限。RBAC 系统定义了各种角色,每种角色可以完成一定的职能,不同的用户根据其职能和责任被赋予相应的角色,一旦某个用户成为某角色的成员,则此用户可以完成该角色所具有的职能。在 RBAC 中,可以预先定义角色-权限之间的关系,将预先定义的角色赋予用户,明确责任和授权,从而加强安全策略。与把权限赋予用户的工作相比,把角色赋予用户要容易灵活得多,这简化了系统的管理。

2001 年,标准的 RBAC 参考模型 NIST RBAC 被提出,如图 1 所示。

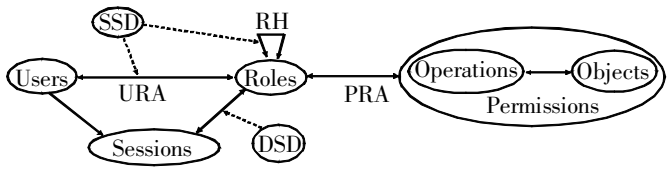

图 1 NIST RBAC 参考模型

NIST RBAC 参考模型分成基本 RBAC、等级 RBAC 和约束 RBAC 三个子模型。基本 RBAC 定义了角色的基本功能,它包括五个基本数据元素: Users(用户) 、Roles(角色) 、Sessions(会话集) 、Objects(客体) 、Operations(操作) ,以及角色权限分配(PRA) 、用户角色分配(URA) 。其基本思想是通过角色建立用户和访问权限之间的多对多关系,用户由此获得访问权限。

等级 RBAC 在基本 RBAC 的基础上增加了角色的等级,以对应功能的或组织的等级结构。角色等级又可分为通用角色等级和有限角色等级。在通用角色等级中,角色之间是一种代数的偏序关系,而有限角色等级是一种树结构。在角色等级中,高等级的角色继承低等级角色的全部权限,这是一种“全”继承关系。但这并不完全符合实际企业环境中的最小特权原则,因为企业中有些权限只需部分继承。

约束 RBAC 在基本 RBAC 的基础上增加了职责分离(SoD) 关系,而职责分离又分为静态职责分离(SSD) 和动态职责分离(DSD) 。静态职责分离用于解决角色系统中潜在的利益冲突,强化了对用户角色分配的限制,使得一个用户不能分配给两个互斥的角色。动态职责分离用于在用户会话中对可激活的当前角色进行限制,用户可被赋予多个角色,但它们不能在同一会话期中被激活。DSD 实际上是最小权限原则的扩展,它使得每个用户根据其执行的任务可以在不同的环境下拥有不同的访问权限。

NIST RBAC 参考模型中还包括功能规范,分为管理功能、系统支持功能和审查功能,这里不再详述。上述的 DAC, MAC 和 RBAC 都是基于主体-客体(Subject-Object) 观点的被动安全模型,它们都是从系统的角度(控制环境是静态的) 出发保护资源。在被动安全模型中,授权是静态的,在执行任务之前,主体就拥有权限,没有考虑到操作的上下文,不适合于工作流系统;并且主体一旦拥有某种权限,在任务执行过程中或任务执行完后,会继续拥有这种权限,这显然使系统面临极大的安全威胁。工作流是为完成某一目标而由多个相关的任务(活动) 构成的业务流程,它的特点是使处理过程自动化,对人和其他资源进行协调管理,从而完成某项工作。在工作流环境中,当数据在工作流中流动时,执行操作的用户在改变,用户的权限也在改变,这与数据处理的上下文环境相关,传统的访问控制技术 DAC 和 MAC 对此无能为力。若使用 RBAC,则不仅需频繁更换角色,而且也不适合工作流程的运转。为了解决此问题,人们提出了基于任务的访问控制模型 TBAC。

3 基于任务和工作流的访问控制模型 TBAC

在 TBAC 模型[4,5] 中,引进了另一个非常重要的概念——任务。所谓任务(或活动) ,就是要进行的一个个操作的统称。任务是一个动态的概念,每项任务包括其内容、状态(如静止态、活动态、等待态、完成态等) 、执行结果、生命周期等。任务与任务之间一般存在相互关联,如相互依赖或相互排斥。如任务 A 必须在任务 B 之后执行;任务 A 与任务 B 不能同时执行等。

TBAC 模型是一种基于任务、采用动态授权的主动安全模型。它从应用和企业的角度来解决安全问题。它采用面向任务的观点,从任务的角度来建立安全模型和实现安全机制,在任务处理的过程中提供实时的安全管理。其基本思想主要有:

(1) 将访问权限与任务相结合,每个任务的执行都被看作是主体使用相关访问权限访问客体的过程。在任务执行过程中,权限被消耗,当权限用完时,主体就不能再访问客体了。

(2) 系统授予给用户的访问权限,不仅仅与主体、客体有关,还与主体当前执行的任务、任务的状态有关。客体的访问控制权限并不是静止不变的,而是随着执行任务的上下文环境的变化而变化。TBAC 的主动、动态等特性,使其广泛应用于工作流、分布式处理、多点访问控制的信息处理和事务管理系统的决策制定等方面。

尽管 TBAC 具备许多特点,并已应用于实际中,但当应用于复杂的企业环境时,就会暴露出自身的缺陷。例如在实际的企业环境中,角色是一个非常重要的概念,但 TBAC 中并没有将角色与任务清楚地分离开来,也不支持角色的层次等级;另外,访问控制并非都是主动的,也有属于被动形式的,但 TBAC 并不支持被动访问控制,需要与 RBAC 结合使用[6] 。

4 基于任务和角色的访问控制模型 T-RBAC

4.1 T-RBAC 模型

为了能适应复杂企业的特定环境需求,通过在 RBAC96 模型中加入“任务”项,构造了基于企业环境的访问控制模型——T-RBAC(Task-Role-Based Access Control) 模型[7] ,如图 2 所示。

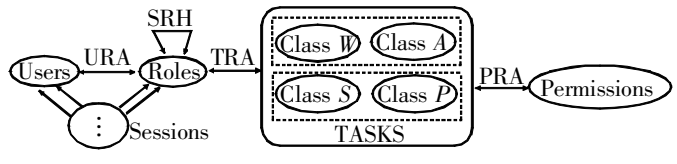

图 2 T-RBAC 模型

不像 RBAC 中没有将任务从角色中分离出来,也不像 TBAC 中没有明确地突出角色的作用,T-RBAC 模型把任务和角色置于同等重要的地位,它们是两个独立而又相互关联的重要概念。任务是 RBAC 和 TBAC 能结合的基础。

不像 RBAC 中将访问权限分配给角色,T-RBAC 模型中是先将访问权限分配给任务,再将任务分配给角色,角色通过任务与权限关联,任务是角色和权限交换信息的桥梁。

在 T-RBAC 模型中,任务具有权限,即根据具体的执行任务要求和权限约束,任务具有相应的权限,不同的任务拥有不同的权限,权限随着任务的执行而变动。这真正实现了权限的按需和动态分配,角色只有在执行任务时才具有权限,当角色不执行任务时不具有权限;权限的分配和回收是动态进行的,任务根据流程动态到达角色,权限随之赋予角色,当任务完成

时, 角色的权限也随之收回; 角色在工作流中不需要赋予权限。这样, 不仅使角色的操作、维护和任务的管理变得简单方便, 也使得系统变得更为安全。

4.2　模型中的两个重要问题

(1) 任务分类问题。企事业环境与需求不同, 访问控制的要求也就不同, 所要执行的任务也应具有不同的特点。任务应根据企事业的组织结构和访问控制要求进行分类, 从而模型可根据任务的分类实现不同的访问控制, 即实现任务级的访问控制。在企业组织中, 访问控制基于任务的特点是非常重要的, 因为访问权限是根据分配的任务赋给用户的。如可根据组织结构和业务流程、权限继承和主动/被动访问特性, 将任务分成了四类(表 1) : *W, S, A, P*, 从而可实现主动访问控制和被动访问控制的结合[7] 。

表 1　任务分类表

	权限不可继承	权限可继承
被动访问	Class *P*	Class *S*
主动访问	Class *W*	Class *A*

(2) 角色继承问题。不像 RBAC 模型中, 角色之间是一种偏序关系, 角色的继承是一种向上的“全”继承关系。在 T-RBAC 模型中, 引进了一种新的角色等级 S-RH, 即 Supervision Role Inheritance(管理角色等级) 。S-RH 定义为: 如果角色 R_1 的级别比角色 R_2 的级别高, 则 R_1 只继承 R_2 中属于类 *S* 或类 *A* 中的任务权限。在 S-RH 中, 高等级的角色并不全部继承低等级角色的权限, 这就解决了部分继承的问题。

通过引进新的角色等级 S-RH, 不仅解决了角色等级中的部分继承问题, 而且还解决了 RBAC 模型中“若角色 A 和角色 B 是互斥的, 则它们不能有相同上层高级角色。”的问题。

5　下一代访问控制模型 UCON

在研究访问控制的过程中, 为适应不同的应用场合, 人们提出了许多新的概念, 如信任管理(Trust Management) 、数字版权管理(Digital Rights Management) 、义务(Obligations) 、禁止(Prohibitions) 等。为了统一这些概念, J. Park 和 R. Sandhu 提出了一种新的访问控制模型, 称作使用控制(Usage Control: UCON) 模型[8] , 也称 ABC 模型[9] 。UCON 模型包含三个基本元素: 主体、客体、权限和另外三个与授权有关的元素: 授权规则、条件、义务, 如图 3 所示。

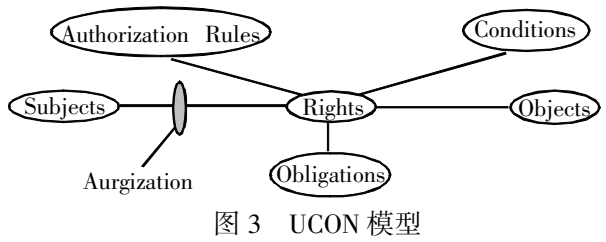

图 3　UCON 模型

UCON 模型中的主要元素如下:

主体(Subjects) 。它是具有某些属性和对客体(Objects) 操作权限的实体。主体的属性包括身份、角色、安全级别、成员资格等。这些属性用于授权过程。

客体(Objects) 。它是主体的操作对象, 它也有属性, 包括安全级别、所有者、等级等。这些属性也用于授权过程。

权限(Rights) 。它是主体拥有的对客体操作的一些特权。权限由一个主体对客体进行访问或使用的功能集组成。UCON 中的权限可分成许多功能类, 如审计类、修改类等。

授权规则(Authorization Rules) 。它是允许主体对客体进行访问或使用前必须满足的一个需求集。授权规则是用来检查主体是否有资格访问客体的决策因素。

条件(Conditions) 。它是在使用授权规则进行授权过程中, 允许主体对客体进行访问权限前必须检验的一个决策因素集。条件是环境的或面向系统的决策因素。条件可用来检查存在的限制, 使用权限是否有效, 哪些限制必须更新等。

义务(Obligations) 。它是一个主体在获得对客体的访问权限后必须履行的强制需求。分配了权限, 就应有执行这些权限的义务责任。

在 UCON 模型中, 授权规则、条件、义务与授权过程相关, 它们是决定一个主体是否有某种权限能对客体进行访问的决策因素。基于这些元素, UCON 有四种可能的授权过程[8] , 并由此可以证明: UCON 模型不仅包含了 DAC, MAC, RBAC, 而且还包含了数字版权管理(DRM) [10] 、信任管理[11] 等。UCON 模型涵盖了现代商务和信息系统需求中的安全和隐私这两个重要的问题。因此, UCON 模型为研究下一代访问控制提供了一种有希望的方法, 被称作下一代访问控制模型。

6　结束语

访问控制是一种重要的信息安全技术, 是现代商务企业保障其信息管理系统安全不可缺少的。网络技术的发展为访问控制技术提供了更为广阔的发展空间, 也使得对访问控制技术的研究显得尤其重要。因篇幅所限, 本文只对几种主要的访问控制模型作了概述。事实上, 仅 RBAC 模型就有多种。很多问题, 如权限表示方法等, 有待进一步研究。

参考文献:

[1] Snyder. Formal Models of Capability-based Protection Systems[J]. IEEE Transactions on Computers, 1981, 30(3): 172-181.

[2] R Sandhu, E Coyne, H Feinstein. Role-based Access Control Models [J]. IEEE Computer, 1996, 29(6): 38-47.

[3] D Ferraiolo, R Sandhu, *et al*. Proposed NIST Standard for Role-based Access Control[J]. ACM Transactions on Information and System Security(TISSEC) , 2001, 4(3): 224-274.

[4] R Thomas, R Sandhu. Task-Based Authorization Controls(TBAC) : A Family of Models for Active and Enterprise-Oriented Authorization Management[C]. Lake Tahoe, CA: Proceedings of the 11th IFIP WG11.3 Conference on Database Security, 1997.

[5] 邓集波, 洪帆. 基于任务的访问控制模型[J]. 软件学报, 2003, 14(1): 76-81.

[6] Gail-Joon Ahn, Myong Kang, *et al*. Injecting RBAC to Secure a Web-based Workflow System[C]. ACM RBAC, 2000.

[7] Sejong Oh, Seog Park. Task-role-based Access Control Model[J]. Information System, 2003, 28: 533-562.

[8] J Park, R Sandhu. Towards Usage Control Models: Beyond Traditional Access Control[C]. Proceedings of the 7th ACM Symposium on Access Control Models and Technologies, 2002.

[9] R Sandhu, J Park. Usage Control: A Vision for Next Generation Access Control, MMM-ACNS[EB/OL]. http://www.list.gmu.edu/conference_papers.htm, 2003.

[10] Sonera Plazza Ltd MediaLab. Digital Rights Management. White Paper[EB/OL]. http://www.medialab.sonera.fi/workspace/DRM-WhitePaper.pdf, 2002.

[11] 徐锋, 吕建. Web 安全中的信任管理研究与进展[J]. 软件学报, 2002, 13(11): 57-64.

作者简介:

沈海波(1963-) , 男, 副教授, 博士研究生, 主要研究领域为访问控制与网络安全; 洪帆(1942-) , 女, 教授, 博士生导师, 主要研究领域为密码学、计算机安全与保密。