一种扩展的委托授权模型及其面向对象的建模

张志勇 普杰信
(河南科技大学电信学院 河南 洛阳 471003)

摘 要 基于角色的委托授权模型旨在解决传统授权管理的集中性和复杂性问题,从而满足分布式计算环境的需求。本文在RBAC96模型的基础上,给出了一种扩展的基于访问许可和角色的两级委托授权模型——PRBDM及其面向对象的建模过程。该模型降低了委托授权的粒度,解决了分布式环境下多 Agent授权管理的复杂性问题。

关键词 访问控制 角色 许可 委托 建模

AN EXTENDED DELEGATION MODEL AND OBJECT-ORIENTED MODELING

Zhang Zhiyong Pu Jiexin
(School of Electronic and Information Engineering, HAUST, Luoyang Henan 471003, China)

Abstract Role-Based Delegation Model mainly solves the centralization and complexity questions of traditional authorization management, and satisfies the requirement of distributed computing environment. The paper gives a Permission and Role-Based Delegation Model and Object-Oriented Modeling in the basis of RBAC96 Model. The model reduces granularity of Delegation, and solves the complexity question of multi-agents authorization management in the distributed environment.

Keywords Access control Role Permission Delegation Modeling

1 引 言

传统的集中式授权管理不再适应于分布式计算环境下的安全访问控制问题,基于角色的委托模型是在 RBAC策略基础上提出的一种旨在解决分布式计算环境下访问授权管理复杂性问题的思想和安全机制。

在 RBDM研究中,目前具有代表意义的主要有 RBDM0和 RBDM2000等。它们都不支持许可级粒度的委托授权,而是把角色作为委托授权的基本单位,即只能委托角色及其所具有的全部许可,这违背了 RBAC策略中“最小特权原则”,使得用户可能获得超出自身所需的权限许可,从而造成信息安全的隐患[1,2];上述 RBDM也未考虑委托的时效性问题,而这又是实现企业级安全访问控制策略通常所必须的[3,4]。同时它们和 RPRDM都未曾采用统一建模语言——UML实现对模型静态和动态特性的建模过程,这也不利于该模型在实际安全系统中的设计与实现[5]。

2 基于角色的委托授权模型(RBDM)

在分布式计算环境下,传统的集中式授权管理加重了安全管理员的负担。这种繁重的授权工作已经不再适应新的环境,为此提出了角色委托的概念,它是安全的分布式计算环境的一个重要因素。基于角色委托的基本思想是在分布式环境下,用户可以不经过安全管理人员,将自身具有角色(显式角色)或所继承的角色(隐式角色)委托给其他用户,使他能够代表自己的职责(角色)行使一定的权限。这样便分散了授权管理,增加了分布式系统的灵活性,其中委托授权后产生的安全性问题可由系统审计来处理。

2.1 委托的重要特征

委托就是用户将自己所具有的权限或者角色转授给其他用户,使其可以代表自己的利益行使一定的职责,完成某些任务。例如,在企事业组织中具有某种角色的职员可能因为某种原因暂时离开岗位,或者是为了和其他职员协同工作,都可以将自身所具备的一些角色或者权限委托给其他职员,达到权利共享的目的。在必要的时刻,他还可以撤销该委托,收回所共享的权利。和委托相关的三个实体是:委托者;委托的角色;受托者。

委托具有以下一些主要特征:

1) 角色委托或部分角色委托 角色委托是指用户可以将自身的角色整体委托给其他用户,从而使其获得该角色所具有的全部权限,而不能只委托该角色的部分权限。这种情况不能满足基本安全策略所要求的“最小特权原则”。部分角色委托可以允许用户将角色中的部分权限委托给另一用户,这样降低了可委托的粒度,遵循了最小特权原则,但是会产生大量逻辑意义上不完整的角色,从而又增加了管理的复杂性。

2) 单步委托或多步委托 单步委托是受托者不可以进一步地将委托角色或权限再委托给其他用户;多步委托则允许受托者进一步对委托角色或权限实施委托,这种情况在撤销委托时将会带来一定的复杂性。

委托的逆操作是撤销,它是收回委托的角色或许可。撤销

收稿日期:2004 - 05 - 09。河南省自然科学基础研究资助项目(0311012600),河南科技大学青年基金资助项目(2003QN06)。张志勇,讲师,主研领域:信息安全,智能决策支持系统。

的主要特征有级联撤销、非级联撤销,独立于授权的撤销,非独立于授权的撤销,系统自动撤销和用户撤销等[5]。

3　PRBDM 及其特性

3.1　PRBDM 构建与形式化描述

PRBDM是在 RBAC96模型的基础上增加了临时委托角色 TDR而扩展出来的。系统为用户的一次委托授权自动创建 TDR,用户可以将需要委托的普通角色和许可指派给 TDR,然后再将其委托给其他用户,从而完成一次委托授权过程。由于 TDR具有时效性,因此在 PRBDM中描述了"TDR生命周期",进而丰富了 PRBDM的语义。PRBDM主要由用户、普通角色、委托角色、许可、约束和会话等六部分构成,如图 1所示:

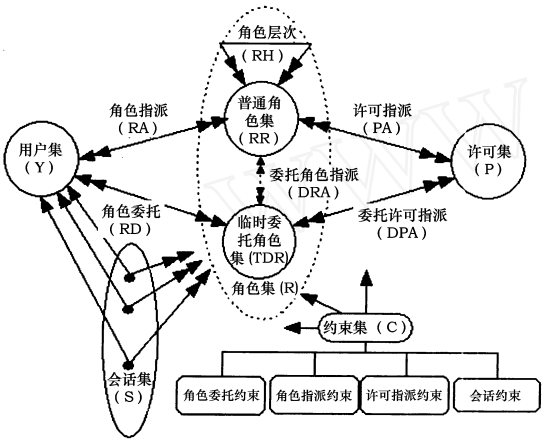

图 1　PRBDM

用集合论和谓词逻辑形式化描述 PRBDM如下:

定义用户集 U,角色集 R,普通角色集 RR,临时委托角色集 TDR及其状态集 S,许可集 P,约束集 C,角色委托约束集 DC,会话集 S。

定义 1(临时委托角色)　TDR是普通角色和许可的并集,$TDR = \{r_1, r_2, \cdots, r_m, p_1, p_2, \cdots, p_n \mid r \in RR, p \in P\}$,即 TDR = RR Up。

定义 2(委托授权)　委托授权关系是一个五元组 (U_1, U_2, TDR, TL, DC),其中 U_1 为委托者,U_2 为受托者,TL (Limit of Time)为委托时限,DC是委托约束。该五元组的语义解释为用户 U_1 在满足 DC的前提下可以将 TDR委托授权给用户 U_2,使得 U_2 在 TL内享有 TDR所有的显式或隐式许可。

定义 3(状态集)　TDR的状态集 S = { init, invoke, sleep, expire},其中 init为初始态,invoke为激活态,sleep为睡眠态,expire为终止态。

定义 4(委托时限)　TDR具有时效性,委托时限 $TL = \{x \mid x = [\tau_{bi}, \tau_{ei}]\ (i = 1, 2, \cdots, n)\}$,其中 τ_{bi} 为该时段的起始时间,τ_{ei} 为终止时间。

定义 5(状态迁移)　TDR在其生命周期内会发生以下状态转换:假定 ST为系统时间,$\forall i (i \in N)\ ST \notin [\tau_{bi}, \tau_{ei}] \wedge ST < \tau_{b1} \rightarrow S = init$; $\exists i (i \in N)\ ST \in [\tau_{bi}, \tau_{ei}] \rightarrow S = invoke$; $\forall i (i \in N)\ ST \notin [\tau_{bi}, \tau_{ei}] \wedge (ST > \tau_{b1}) \wedge (ST < \tau_{en}) \rightarrow S = sleep$; $\forall i (i \in N)\ ST \notin [\tau_{bi}, \tau_{ei}] \wedge ST > \tau_{en} \rightarrow S = expire$。

3.2　PRBDM中的委托约束及相关性质

普通基于角色或许可授权的实施者为若干个系统管理员,授权管理相对集中;而在分布式环境下委托授权的实施者是系统中的所有用户,授权操作比较分散。因此实施委托约束有利于加强委托管理,以防止某些用户有意或无意地进行非法授权委托,提高系统的保密性、完整性和可控性。委托约束主要包括非委托角色和许可、委托冲突角色和许可、委托步和委托基数约束等。

定义 6(非委托角色和许可集)　非委托角色和许可集 $NDRP = \{r_1, r_2, \cdots, r_i, p_1, p_2, \cdots, p_j\}$。

约束规则 1　非委托角色和许可集中的元素不能进行委托。

$\forall x (x \in NDRP) \rightarrow (x \notin TDR)$

定义 7(委托冲突)　如果角色 r_i 和 r_j 不能同时委托给其他用户,则称两者为委托冲突角色,记为 $collr(r_i, r_j)$;如果许可 p_m 和 p_n 不能同时委托给其他用户,则称两者为委托冲突许可,记为 $collp(p_m, p_n)$。

约束规则 2　临时委托角色集中任意两个角色或许可都不能存在委托冲突。

$\forall r_i, r_j, p_m, p_n\ (r_i \in TDR, r_j \in TDR, p_m \in TDR, p_n \in TDR)\ collr(r_i, r_j) \vee collp(p_m, p_n) = F$

定义 8(委托步和委托基数)　委托步 d为自然数,表示角色 r_i 或许可 p_j 可以级联委托的次数,当 d = 1时,称为单步委托;当 d > 1时,称为多步委托。委托基数 n为自然数,表示角色 r_i 或许可 p_j 可以委托的用户数。

约束规则 3　TDR的委托步和委托基数取决于 TDR集中所有角色和许可的委托步或委托基数的最小值。

$\forall r_i, p_m\ (r_i \in TDR, p_m \in TDR)\ d_{TDR} < d_{ri} \wedge d_{TDR} < d_{pm}$

$\forall r_i, p_m\ (r_i \in TDR, p_m \in TDR)\ n_{TDR} < n_{ri} \wedge n_{TDR} < n_{pm}$

性质 1(多步委托)　用户间 TDR的多步委托关系是一种偏序关系,满足自反性、反对称性和传递性。

性质 2(级联委托撤消)　当原始用户强制收回委托授权或 TL结束时,经用户多步委托出去的 TDR被级联收回。

性质 3(依赖委托撤销)　只有原始委托者可以撤销委托授权,具有相同角色的其他用户都无权收回委托。

最小特权原则、责任分离原则和数据抽象原则是实现企业级访问控制的基本安全策略,也是提供安全服务的首要原则。约束规则 1增强了应用系统中对委托授权的控制,满足了"最小特权原则";约束规则 2解决了企业级委托授权的冲突问题,实现了"责任分离原则"。许可集中的任意许可既可以为读、写、执行等,也可以是企业级抽象的许可,如现金出纳、账目审计等,从而达到"数据抽象原则"。

4　PRBDM 面向对象的建模

4.1　面向对象与统一建模语言

面向对象的方法是一种运用对象、类、继承、封装、聚合、消息传递、多态性等概念来构造系统的软件开发方法。面向对象方法的基本思想是:从现实世界中客观存在的事物(即对象)出发来构造软件系统,并在系统构造中尽可能运用人类自然的思维方式。面向对象方法的主要特性是:封装性、继承性和多态性。

1997年 1月 Rational软件公司的三位学者正式提出了面向对象系统的建模语言 UML (Unified Modeling Language,简称 UML) 1.0版,这是 00行业中具有里程碑性质的新进展。UML语言的出现也建立了统一的面向对象开发方法,可视化描述模型元素是面向对象建模方法的显著特点。UML符号表示法定

义了可视化元素,并为开发者或开发工具使用这些图形符号和文本语法进行系统建模提供了标准。这些图形符号和文字所表达的是应用级的模型,在语义上它是 UML 元模型的实例。UML 表示法主要由五类图组成,分别为用例图、静态图、行为图、交互图和实现图等[6]。

4.2 PRBDM 的建模

在分布式计算环境中,PRBDM 能够较好地实现委托授权,从而满足分布式、分散性的需求,解决了由于集中授权带来的复杂性问题。为了便于设计和开发基于 PRBDM 的应用系统,缩短理论安全模型形式化、抽象性和实际应用系统开发之间的差距,支持系统面向对象的分析与设计,因此采用面向对象的思想利用 UML 对其进行系统建模是非常必要的[7]。

关于 PRBDM 的静态建模,主要描述 PRBDM 应用系统的用例图、实体类和类关系图。在 PRBDM 系统用例图中,主要从用户角度描述系统的对外功能。对于这些功能的实施者可以分为以下四类:系统管理员、系统安全员、系统审计员和普通用户。这四类用户分别完成不同的工作:系统管理员完成用户和普通角色的管理;系统安全员负责管理约束规则库,实施角色、许可和会话约束规则;系统审计员主要完成对系统管理员授权管理操作的跟踪监视,以及对普通用户委托授权和应用系统数据访问的审计等;对于普通用户主要是在系统中创建与撤销会话、进行角色委托等等,系统用例图如图 2所示。

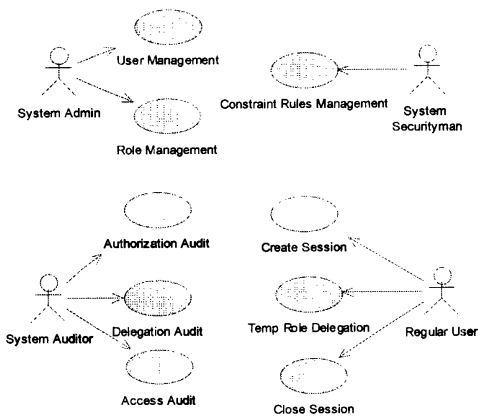

图 2 PRBDM 系统用例图

对于 PRBDM 系统主要设计六个实体类,并包括了主要的属性与方法(操作),以及各类之间的关系等,如图 3所示。类关系描述了 PRBDM 的静态特征,其中主要为泛化和关联关系,以及关联关系的基数特征。这里约束类被泛化为角色委托约束、角色指派约束、许可指派约束和会话约束等若干个子类,分别完成对角色委托和角色、许可指派以及用户会话创建等约束规则的监控工作。泛化后的子类除了继承父类公用的属性和方法外,还可以具有自身的属性和方法。在图 3关联关系中描述了各个类之间的基数特征,如用户、TDR 和许可三个类之间是多对多的关系,用户和会话之间是一对多的关系等等。

PRBDM 的动态建模主要是描述 PRBDM 应用系统的交互图和对象行为图。对于它的动态建模,这里由于篇幅问题不可能完全描述系统中所有的动态行为特征,因此选择具有代表性的角色委托时序图(交互图中的一种)加以描述和解释。普通用户间委托授权的时序图如图 4所示,它描述了委托授权过程的动态特性,以及各步骤之间的时序关系。用户的委托过程要受到委托约束机制的监控,这是 PRBDM 系统的重要特性。

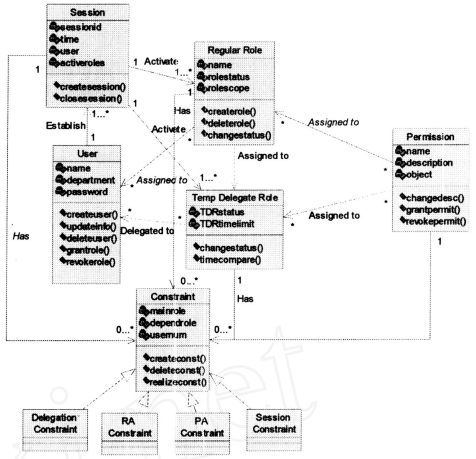

图 3 实体类关系图

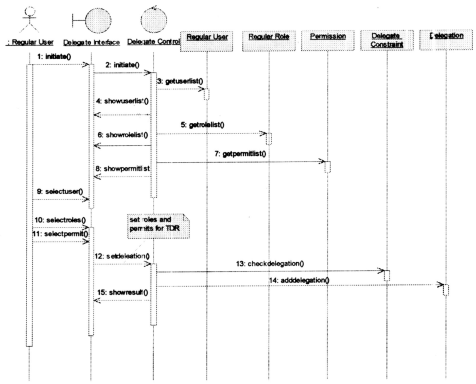

图 4 委托授权时序图

5 结束语

本文所给出的 PRBDM 既弥补了其它模型不支持许可级委托授权的缺陷,又保持了角色级委托授权管理中高效、灵活的特点,是一种在分布式计算环境下解决委托授权问题较完备的模型。同时 PRBDM 面向对象的建模也有利于分布式环境下多 Agent访问控制的设计与实现。PRBDM 关于上下文中的委托约束特性将会进一步增强该模型的语义表达能力,对此需做进一步的研究工作。

参 考 文 献

[1] Ezedin Barka, Ravi Sandhu, A Role-Based Delegation Model and Some Extensions[C], The 16th Annual Computer, Sheraton New Orleans, 2000.

[2] SangYeob Na, SuhHyun Cheon, Role Delegation in Role-Based Access Control[C], ACM BRAC2000.

[3] Longhua Zhang, Gail-Joon Ahn, Bei-Tseng Chu, A Rule-Based Framework for Role-Based Delegation[C]. SACMAT2001.

[4] Ravi Sandhu. Role-Based Access control[J], Internet Computer, 1996, 29(2): pp. 38～47.

[5] 赵庆松、孙玉芳等,"RPRDM:基于重复和部分角色的转授权模型[J]",《计算机研究与发展》,2003, Vol 40, No. 2: pp. 221～227.

[6] 鲁博、柴跃廷,"关于统一建模语言—UML[J]",《计算机工程与科学》,2000, Vol 22, No. 4: pp. 57～60, 70.

[7] Michael E. Shin, Gail - Joon Ahn, UML - Based Representation of Role - Based Access Control[C], In Proceeding of 5th IEEE Internation Workshop on Enterprise Security, NIST, MD, 2000.