一种改进的基于角色的授权委托模型

孙翠翠,张永胜
(山东师范大学 信息科学与工程学院,山东 济南 250014)

摘 要:委托是访问控制模型中非常重要的组成部分,已成为分布式计算环境下重要的访问控制管理机制。提出了一种改进的基于角色的授权委托模型,此模型对用户的角色划分不仅仅基于用户的身份,还要考虑用户的信任度、能力等属性,通过综合多种因素对用户进行属性级别划分,不同的属性级别对应不同的角色从而对应不同的访问权限,以达到对用户进行访问控制的目的,是一种基于属性的角色授权委托模型。与传统基于身份划分的角色委托模型相比,此模型具有更细的访问控制粒度和更高的安全性。

关键词:委托;授权;用户属性级别;角色
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2010)11-0154-04

An Authorization Delegation Model Based on User Security Levels

SUN Cui-cui, ZHANG Yong-sheng
(School of Information Science and Engineering, Shandong Normal University, Jinan 250014, China)

Abstract: Delegation is a very important part of access control model and has become an important access control management mechanism under the distributed computing environment. An improved authorization delegation model based on user attribute is presented. Delegating role to users not only consider the user's position, but also the user's trustworthiness and ability and then make a user attribute levels, the different attribute levels correspond to different roles and thus correspond to different access permissions to control users' access. This model is an attribute-based role delegation model. Compared with the traditional authorization delegation model, this model has a fine-grained access control and higher security.

Key words: delegation; authorization; user attribute levels; role

0 引 言

在分布式环境中,系统的管理工作异常繁重,系统安全完全依赖于某个或者某些管理者的集中式管理方式,需要管理者参与系统中所有的授权行为,加重了系统管理员的负担。一些系统的高级用户希望自主地把自己拥有的一些权限在符合系统安全规定的前提下委托给其他用户。

授权委托是解决上述问题的一种有效方式,它允许将分布式环境下的集中式管理工作进行分散实施,提高了分布式系统的伸缩性和灵活性,有效地减轻了系统的授权管理负担。

收稿日期:2010-03-28;**修回日期**:2010-06-24
基金项目:山东省自然科学基金(Y2008G22)
作者简介:孙翠翠(1984-),女,山东临沂人,硕士研究生,研究方向为Web服务安全、面向服务计算;张永胜,教授,研究方向为软件工程环境、Internet/Intranet工程、网络信息安全。

1 几种授权模型

基于角色的访问控制[1](Role-Based Access Control,RBAC)通过引入角色的概念实现了用户和权限的逻辑分离,权限被授予角色,用户通过管理员为其分配的角色获得相应的权限,显著地降低了授权管理的代价。因此RBAC被认为是大型组织的一种有效的访问控制模型。大部分组织存在一些与访问控制策略相关的规则,如职责划分等,授权委托就是其中重要的一个。

委托[2](delegation)是指在不需要资源所有者干预的情况下把权限从一个主体传递给另一个主体。用证书表示委托,并且证书的发布者用自己的私钥对证书进行数字签名。目前,委托的研究工作更多的关注在用户与用户之间。RBDM0[3](Role-Based Delegation Model 0)模型是E. Barka和R. Sandhu在对基于角色的用户-用户权限委托代理特征进行定性研究的基础上,提出的仅支持扁平角色结构和单步委托代理的简

单角色委托代理模型。RDM2000[4]模型是 RBDM0 的一个扩展,支持角色继承关系下的多步委托和角色委托,并用一种基于规则的描述语言来实现委托策略。上述委托模型的基本单元都是角色。

针对一些委托单元是权限或权限与角色的混合的需求,Xinwen Zhang 等人提出了一种基于权限的委托模型 PBDM[5](Permission - Based Delegation Model),是一种灵活的委托模型。PBDM 支持用户 - 用户和角色 - 角色委托、多步转授权、多步撤销,也支持角色和权限级别委托。PBDM 由三个子模型组成,分别为 PBDM0、PBDM1 和 PBDM2 模型。PBDM0 提供单步转授权和多步转授权,通过将用户的部分权限或角色指派给临时委托角色以实现权限或角色的委托。PBDM1 是 PBDM0 的扩展,它通过增加可委托角色来限制可委托的权限,避免委托者将一些高级权限委托给低级用户,实现了管理员的安全管理监控功能。PBDM2 实现的是角色到角色之间的委托,主要通过临时可委托角色来接受其他角色委托的权限。

PBDM 模型很好地解决了委托单元问题,并且能对授权者的授权权限进行控制。但是 PBDM 无法确定用户的可信程度,不能够确定哪些用户是可信的,哪些是不可信的。它也可能对一些不可信的用户授予一些重要权限。因此文献[6]将信任管理引入委托授权模型中,依靠可信任第三方提供附加的安全信息对用户进行信任描述,增加了授权的可靠性。但是信任管理存在以下问题:一是权限委托时没有考虑两个实体之间的信任程度;二是没有很好地解决委托的深度控制问题。文献[2,7]引入信任度的概念,表示两个实体之间的信任程度,提出一种新的适合开放式环境的授权委托模型,即基于信任度的授权委托(TBAD)模型。既解决了实体间的信任度问题,又对委托深度进行了有效的控制。

但是基于信任度的授权委托模型将信任度作为授权委托的唯一依据,它不能对主体进行一个较全面的描述,主体的一些影响授权的重要因素未被考虑到。文中给出一种改进的基于角色的授权委托[8]模型,该模型对请求者的授权不仅要考虑请求者的信任度还要考虑请求者的能力和身份,因此能够对用户进行更有效控制,具有较高的安全性。

2　改进的角色授权委托模型

2.1　模型的组成元素和语义

改进的基于角色的授权委托模型将用户的信任度、能力和身份的因素进行综合考虑,利用选定的评估函数对用户进行属性评估,根据评估值对用户进行一个属性级别划分,不同的属性级别授予不同的角色从而授予不同的权限。达到对用户根据其属性进行授权委托的目的,具有较细的访问控制粒度[6]。

在该模型中沿用了 RBAC 中定义的用户(U)、角色(R)、权限(P)等几个概念。模型如图 1 所示。

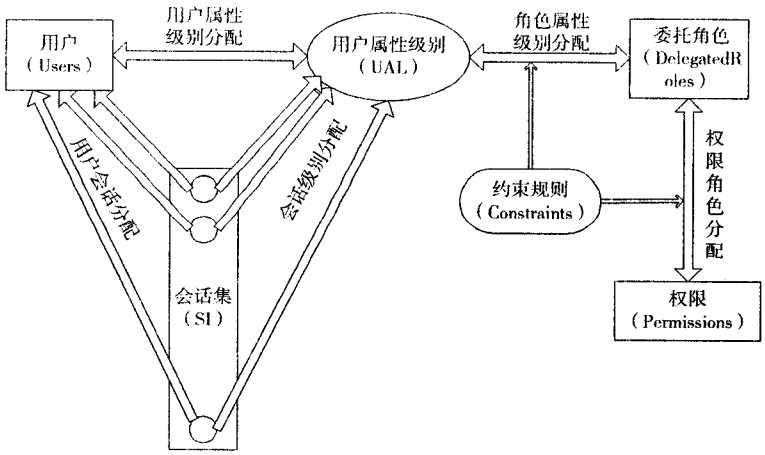

图 1　改进的模型图

模型的主要组成元素及其语义为:

(1)委托者(Delegator)发起委托动作的用户,即向其他用户进行授权的用户,记作 dor,用 Dor 表示委托者的集合,Dor⊆U。

(2)被授权用户(Delegatee)接受委托内容的用户,记作 dee,用 Dee 表示被授权用户的集合,Dee⊆U。

(3)委托角色[9](Delegated Role)授权者向被授权者委托授权时产生的具有时间限制的角色,记为 dr,用 DR 表示委托角色集,DR⊆R。

(4)会话实例集(Session Instances)表示用户的操作实例,会话实例体现了用户与用户所属角色集的当前活动子集间的映射关系。用户在一次访问中只要其操作不超出为其分配的最大权限即可进行多次会话,用 si 来表示一次会话,用 SI 代表用户在本次访问中操作的集合。

(5)用户属性评估(User Attribute Assessment)对用户的信任度、能力和身份等属性进行评估,以验证是否满足授权委托的要求。

用户的三种属性信任度(trustworthines)、能力(ability)和身份(position)分别用 Attr(t)、Attr(a)和 Attr(p)来表示,属性评估策略用函数 F(Attr(t),Attr(a),Attr(p))[10]来描述,F 函数是根据实体的规则来制定的,它描述了主体访问资源时必须满足的条件。F 值的不同将会对用户授予不同的角色。

(6)用户属性级(User Attribute Levels)根据函数 F

的值为用户定义一个属性级,不同的属性级别授予用户不同的角色,从而授予不同的权限。

2.2 模型授权规则

以下为模型授权规则[11]:

规则 1:用户会话分配(US):USA⊆U× SI。定义了用户会话分配之间的关系,其中,si∈SI 表示一次具体会话。在用户与会话分配关系上,模型允许一个用户可以同时激活多个会话,但每一时刻只有一个会话在执行。

规则 2:用户属性级分配(UAL):ULA⊆U×SL。用户属性级别分配定义了用户与属性级的分配关系,用户和用户属性级是多对多的映射关系,用户可以在同一时间激活多个会话,且每个会话可以具备不同的级别。同样,同一级别的会话也可以赋给多个用户。

规则 3:会话属性级分配(SAL):SLA⊆S×SL。会话属性级别分配定义了会话与用户属性级的分配关系,会话与属性级是一对多的映射关系,即一个会话只能属于一个明确固定的等级。而一个等级则可对应于多个会话。

规则 4:角色属性级别分配(RAL):RLA⊆R×SL。角色属性级分配定义了角色与属性级的分配关系。角色与属性级是多对多的映射关系,一个等级可与多个角色相关联,同样,一个角色可关联多个等级。

规则 5:用户角色分配(UR):URA⊆U×R。用户角色分配定义了用户与角色之间的多对多对应关系,一个用户可对应多个角色,一个角色也可赋予多个用户。

规则 6:角色权限分配(RP):RPA⊆R×P,角色权限分配定义了角色和权限之间的多对多映射关系。

2.3 模型的授权过程

当要对一个请求者进行授权委托时,需要对他的信任度、能力和身份进行验证。对于第一次访问的用户,系统要求其提供必要的用户信任度、能力、身份等各种信息,然后利用函数 F(Attr(t),Attr(a),Attr(p))来对用户进行评估。根据 F 的值对用户进行属性级划分,委托者根据属性级对用户生成一个临时委托角色,临时委托角色被赋予相应的访问权限,然后将此角色分配给该用户,同时系统会对此角色赋予一个有效时限,在此时限内该用户可多次访问所需的资源。

对于已经访问过的用户,系统维护一个用户信息列表,当用户临时委托角色在有效期内时,用户可不经过属性验证即可对资源进行访问。当时限过期或用户申请更高权限时,系统会将用户的信息如信任度、能力等参数传递给评估函数 F(Attr(t),Attr(a),Attr(p))进行重新评估,并为用户重新生成属性级,如果此属性级和用户申请的权限相对应则委托者可为用户分配所需的权限。如果用户申请的权限高于用户的属性级,将会被拒绝授权。

模型的授权过程如图 2 所示。

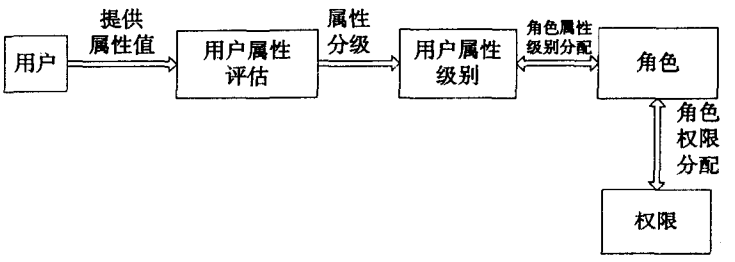

图 2 授权委托过程

一个具有委托权限的用户对其他用户进行转授权的过程为:

(1)被授权用户向系统提供自己的信任度、能力和身份等属性信息,系统对用户进行登记。

(2)系统利用评估函数 F(Attr(t),Attr(a),Attr(p))对用户的属性进行评估,以确定用户的属性级别。

(3)根据用户的属性级别利用用户属性级别分配关系将相应的委托角色赋予用户,根据角色权限分配关系将相应的权限赋予委托角色。

(4)被授权用户使用被赋予的委托角色对资源进行访问。

(5)用户访问完成后,角色即被收回但不会立即撤销。当用户在一定时间内再次执行相同访问时,可直接将此委托角色赋予用户,而不必重新生成委托角色。

3 模型应用

下面用一个具体实例来说明模型的授权过程。

3.1 应用描述

对于高校的教学资源管理系统必须进行实时的更新等工作。某高校的教学资源管理系统有三种角色可以对资源进行更新,分别为管理员、管理员助手、教学老师。假设此系统由管理员 A 来负责,由于工作量较大,A 需要一个助手来帮他完成一些工作,为了方便快速地完成工作就需要 A 对助手进行一些教学资源访问的授权。这就需要进行授权委托工作。

3.2 过程和结果

管理员 A 如果想对助手授权一些所需要的权限,就需要验证此助手是否满足访问此资源的要求,不同的资源对用户的属性要求是不同的。某个申请者 B 想要申请助手的职位,需要对 B 的信任度、能力和身份进行验证。假设 B 的信任度为 9,能力为较强,身份为老师。

教学资源管理系统由教师模块、学生模块、课程设置模块、课程内容模块等组成。不同的模块对用户的属性要求不同。

各模块要求如表 1 所示,其中属性要求的值分别对应为(信任度,能力,身份)。

表 1　模块 - 属性表

模块名称	属性要求
教师模块	(9,较强,管理员)
学生模块	(9,较强,老师)
课程设置模块	(8.5,较强,老师)
课程内容模块	(8,强,老师)

由表可知课程内容模块所要求的访问用户的属性为信任度为 8,能力强,身份为老师;课程设置模块要求用户的属性为信任度 8.5,能力为较强,身份为老师;学生模块访问用户的属性为信任度为 9,能力为较强,身份为老师;教师模块访问用户的属性为信任度为 9,能力为较强,身份为管理员。那么管理员 A 只能对 B 授予访问学生模块、课程设置模块和课程内容模块的权限,而不能对教师模块进行授权访问,因为教师模块要求的身份是管理员。

3.3　应用分析

从以上实例可看出,授权用户对被授权用户的委托授权不能仅考虑用户的一个属性因素,还要考虑用户的信任度和能力等各种因素,只有用户的属性都满足系统的要求时才能对用户进行授权委托。而且不同的资源对用户属性的要求不同,必须对不同的资源进行不同的访问控制。

该模型通过考虑多种因素对用户进行授权委托,使系统具有更细的访问控制粒度,同时也增加了模型的安全性,从而对系统资源的敏感信息进行了有效地访问控制。

4　结束语

授权委托已成为近年来访问控制授权研究的一个重点和热点课题。文中通过对基于角色授权委托模型的深入研究,综合现有授权委托模型的优点和不足,提出了一种改进的基于用户角色的授权委托模型,通过考虑用户的多种属性因素对进行用户属性级划分,并据此对用户授予相应权限,有效控制了授权委托的滥用,是一种安全性更高的访问控制模型。

参考文献:

[1] 杨秋伟,洪　帆,杨木祥,等.基于角色访问控制管理模型的安全性分析[J].软件学报,2006,17(8):1804 - 1810.

[2] 廖俊国,洪　帆,朱更明,等.基于信任度的授权委托模型[J].计算机学报,2006,29(8):1265 - 1270.

[3] Barka E, Sandhu R. Framework for Role - based delegation models[C]//In: Proceedings of the 16th Annual Computer Security Application Conference. Washington, DC, USA: IEEE Computer Society, 2000:168 - 176.

[4] Zhang Longhua, Ahn Gail - Joon, Chu Bei - Tseng. A Rule - Based Framework for Role - Based Delegation[C]//In: Proceedings of the 6th ACM Symposium on Access Control Models and Technologies Chantilly. Virginia, USA: ACM, 2001: 153 - 162.

[5] Zhang Xinwen, Oh S, Sandhu R. PBDM: A Flexible Delegation Model in RBAC[C]//In: Proceedings of the 8th ACM Symposium on Access Control Models and Technologies. VillaGallia, Como, Italy: ACM, 2003:147 - 157.

[6] 张志勇,黄　涛.信任管理中基于角色的委托授权研究进展[J].计算机应用研究,2008,25(6):1601 - 1605.

[7] 翟征德,冯登国,徐　震.细粒度的基于信任度的可控委托授权模型[J].软件学报,2007,18(8):2002 - 2015.

[8] 肖　钥.委托授权模型的研究[D].郑州:信息工程大学,2005.

[9] Lee HyungHyo, Lee YoungRok, Noh BongHam. A New Role - Based Delegation Model Using Sub - role Hierarchies[C]//In: Proceedings of the 18th International Symposium on Computer and Information Sciences. Antalya, Turkey: Computer and Information Sciences ISCIS, 2003:811 - 818.

[10] 傅鹤岗,李　竞.基于属性的 Web 服务访问控制模型[J].计算机科学,2007,34(5):111 - 114.

[11] 翟征德.基于量化角色的可控委托模型[J].计算机学报,2006,29(8):1401 - 1407.

(上接第 153 页)

[8] 岑贤道,安常青.网络管理协议及应用开发[M].北京:人民邮电出版社,1995:15 - 18.

[9] Dongmo S, Vautrot P, Bonne N, et al. Correction of surface roughness measurements in SPM imaging[J]. Appl. Phys. A, 1998, 66:819 - 823.

[10] Binning G, Quate C F, Gerder C H. Atom icforce m ic roscope [J]. Rhys. Rev. Lett., 1986, 56(9):930 - 933.

[11] 戴宗坤.信息系统安全[M].北京:金城出版社,2000:156 - 159.

[12] Whitehouse D J. Comparison between stylus and optical methods for measuring surfaces[J]. Annals of the CIRP, 1988, 37 (2):649 - 653.