

网格环境下授权策略的研究

鲍美英^{1,2}, 马 礼¹, 高玉斌¹

(1 中北大学 信息与通信工程学院, 山西 太原 030051;

2 山西大同大学 计算机科学与技术系, 山西 大同 037009)

摘 要: 针对网格环境下授权的特性, 分析了现有网格授权机制和访问控制模型的缺陷, 提出了适用网格环境的 TSRBAC 授权模型. 该模型以虚拟组织为基础, 改进了 RBAC 策略, 实现了权限的分布式管理和动态授权. 通过将角色分离, 满足了资源动态性和策略自主性的要求, 适应了网格环境的特点. 给出了该模型中概念的定义和形式化描述, 并用该模型改进了 CAS 系统.

关键词: 网格; 授权; 角色; 任务; 社区团体授权

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2010)03-0043-04

Research on the Authorization Policy in Grid

BAO Mei-ying^{1,2}, MA li¹, GAO Yu-bin¹

(1 School of Information and Communication Engineering, North University of China, Taiyuan 030051, China;

2 Department of Computer Science and Technology, Shanxi Datong University, Datong 037009, China)

Abstract: In view of the characteristic of the grid environment, a TSRBAC authorization model which is suitable for the grid environment is proposed after analyzing the limitation of existing grid authorization mechanism and the access control models. The model improved the RBAC policy and realized the distributional management of permission and the dynamic authorization. It has satisfied the request that dynamic of the resources and independent of policy, and adapted the characteristic of the grid environment. This paper has given the concept definition and formal description of the model, and improved the CAS architecture with this model.

Key words: grid; authorization; role; task; CAS

1 引言

随着网格技术的逐渐成熟, 安全已经成为网格研究的热点问题. Globus 项目中的 GSI(Grid Security Infrastructure)是现今最成熟的网络安全解决方案. 它提供网格实体的认证和安全通信, 通过代理证书机制和单点登录等简化了用户与各种服务的交互. 然而, GSI 授权是通过对一个文件的操作实现的, 该文件提供全局用户到本地账号的映射关系, 每个资源提供者都需要维护一个庞大的全局/本地映射表, 因此难以扩展到拥有大量资源和用户的虚拟组织(Virtual Organization, VO)环境中, 不能很好

地适应网格动态和资源量大的情况. 为了克服大规模虚拟组织环境中的策略需求和 GSI 的不足, 人们又提出了基于策略的授权系统: 社区授权服务(Community Authorization Service, CAS)^[1]. CAS 本质上是一种基于角色的授权系统, 它解决了虚拟组织中资源和数据访问控制的灵活性、可扩展性等问题, 但也存在着一些缺陷.

文中在基于角色的访问控制模型的基础上, 对模型中的角色进行了重新划分, 并且借鉴 TBAC 中任务的概念, 引入任务, 提出了一种网格环境下的授权模型 TSRBAC(Task and Separation-Role Based Access Control).

收稿日期: 2009-03-06; 修回日期: 2009-05-08

基金项目: 国家自然科学基金项目(90412006, 60573110); 山西省自然科学基金项目(2008011009)

2 访问控制模型

2.1 传统的访问控制模型

传统的访问控制方式主要包括自主访问控制 (Discretionary Access Control, DAC) 和强制访问控制 (Mandatory Access Control, MAC). 传统的访问控制机制中, 授权主要是基于主体属性、对象属性和访问控制权. 传统的访问控制模型授权是建立在访问矩阵的基础上, 当主体和对象的数量增多时, 矩阵将变得非常巨大, 这样不利于系统的扩展, 而且管理和维护也会变得非常困难.

2.2 基于角色的访问控制模型

为了解决传统访问控制模型存在的扩展性问题, 提出了基于角色的访问控制模型 (Role-Based Access Control, RBAC)^[2] (如图 1 所示). RBAC 通过引入角色这个概念, 将用户与权限有效地联系起来, 其核心是定义多种角色并设定相应的访问权限, 用户被授予角色, 从而获得访问权限. RBAC 可以根据实际情况设定角色, 授权比较灵活, 可以实现细粒度的访问控制^[3].

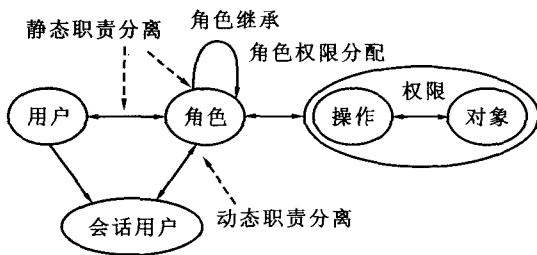


图1 NIST RBAC 参考模型

因为角色授权是基于主体属性和对象属性的静态授权方式, 所以存在以下的一些问题:

(1) RBAC 中授权是静态的, 在执行任务前, 主体就拥有了权限, 而且在任务执行中或执行后, 仍会拥有权限, 使得系统存在很大的安全隐患, 且不利于权限的管理.

(2) RBAC 授权过程只考虑了角色而没有考虑具体的任务, 这样对于不同的任务只要是角色相同就可以获得相同的权限, 显然这种授权方式不满足授权的“最小特权”的原则.

2.3 基于任务的访问控制模型

Thomas R K 和 Sandhu R 提出了一种基于任务的访问控制模型 (Task-Based Access Control, TBAC)^[4], 与以往的访问控制策略不同, TBAC 是一种主动访问控制策略. TBAC 模型是一种以任务为中心的, 并采用动态授权的主动安全模型. 其基本思

想: 授予给用户的权限, 不仅依赖主体和客体, 还依赖于当前执行的任务、任务的状态、任务活动时用户拥有的权限. 任务挂起时, 权限被冻结; 任务恢复执行, 权限恢复; 任务终止时, 权限撤消.

TBAC 拥有的主动控制、动态分配权限的优点, 使它适用于工作流、分布式处理、多点访问控制的信息处理^[5], 特别是应用于安全工作流管理中. 然而它目前还处于理论阶段, 未能得到广泛的应用.

3 网络环境下的授权模型

在网络环境下, 通常由网络用户向网络门户提交复杂的项目, 每个项目通常被划分为多个任务, 分发给不同的资源提供者来完成, 任务在网格中是一个很重要的概念. 基于角色的团体授权技术, 虽然克服了自主授权中的访问控制列表无限增大的缺点, 但是还没有很好地解决角色授权本身存在的问题. 文中提出的新模型 TSRBAC 就是借鉴 TBAC 中任务的概念, 在 RBAC 中引入任务, 将系统要实现的一系列功能细化为一个一个任务, 通过任务来实现对权限的动态管理. 并且对原 RBAC 模型中的角色重新划分, 将权限的集中式管理变为分布式管理, 模型如图 2 所示.

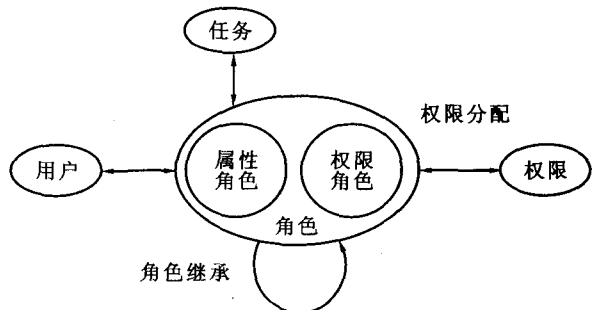


图2 TSRBAC 模型

在该模型中, 把角色分为属性角色和权限角色, 属性角色是用户的身份信息, 也即用户在虚拟组织中的角色. 权限不直接授予属性角色, 而是根据任务, 由资源提供者指派, 指派后称为权限角色. 最后由本地资源根据权限角色和本地安全策略激活所需的权限, 这样就实现了权限的动态管理.

3.1 模型中的基本概念定义

在 TSRBAC 模型中虚拟组织作为独立单元对授权和资源进行管理, 基本控件的构成以 NIST 标准的 RBAC 为基础, 主要包括: 用户 (U)、角色 (R)、对象 (O)、操作 (M)、许可 (P) 等, 为了实现权限的分布式管理, 引入了属性角色 (AR) 和权限角色 (PR) 的概念. 符号“ $\geq$ ”统一表示授权, 它是一种广义继

承关系.

用户(User):可以独立访问网格系统中数据或资源的主体.

角色(Role):一群用户在组织内可执行的操作集合,意味着用户在组织内的责任和职能.

属性角色(Attribute Role):描述用户和虚拟组织的关系,用户所属的角色和用户的某些特权.

权限角色(Permission Role):组或角色被允许在资源上执行的操作,这类信息由资源本地安全机制所维护.

角色继承(Role Hierarchy):为了避免相同操作的重复进行,角色除了具有自身的属性与权限之外,还可以继承其它角色,从而自动拥有被继承的角色的属性与权限.这里将 r' 继承 r ,记为 $r' \geq r$,并称 r' 是 r 的父角色, r 是 r' 的子角色.对于属性角色,角色继承主要是针对该角色的身份、特权信息.而对于权限角色,则主要继承该角色拥有的权限.

任务(Task):任务是系统执行过程中完成一定功能目标的最小工作单元,具有原子性.任务可按其功能分为管理任务、监督任务和数据操作任务.管理任务用来管理用户组内低级用户的活动任务,并进行任务分派.监督任务用来查看活动任务的活动状态.数据操作任务进行底层的数据存取操作.

权限(Permission)或称作许可:用户拥有的对于对象操作的一些特权.权限是一个用户对对象进行访问或使用的功能集组成.

3.2 模型的形式化描述

根据前面的定义和分析,TSRBAC 模型的形式化描述如下:

(1) 角色指派

$ARA \subseteq AR \times U$,为属性角色指派; $PRA \subseteq AR \times T$,为权限角色指派,表示权限角色由属性角色和任务共同决定.

$R(u) = \{r \mid \text{指派给主体 } u \text{ 的角色}, u \in U\}$

(2) 权限指派

$PRA \subseteq PR \times P$,表示权限角色与权限的关系, $PRA(pr, p)$ 表示权限角色 pr 拥有权限 p .

$TPA \subseteq T \times P$,表示任务与权限的关系,用 $TPA(p, t)$ 表示任务 t 要求操作权限 p .

(3) 角色关系

$AR \cap PR = \emptyset$,表示属性角色和权限角色相互独立;

$ARH \subseteq AR \times AR, PRH \subseteq PR \times PR$,表示了属性角色和权限角色各自内部的层次继承关系.

(4) 激活角色集

主体在一次任务开始时启用的角色集,用 $PR(t)$ 表示任务 t 开始时激活的角色集.

$\exists \forall t \in t(T)(PR(t)) \subseteq AR$

若角色 r_i 被激活,则 r_i 所包含的下层角色 r_j 也同样被激活.

(5) 约束规则

约束策略的制定以静态互斥角色集和动态互斥角色集为依据,其中:

静态互斥角色集是指在访问授权时不能同时指派给主体的两个或多个角色的集合.

$Sta_mutex(r_i) = \{r_j \mid r_j \text{ 和 } r_i \text{ 满足静态互斥}, i \neq j\}$

动态互斥角色集则是指主体开始任务时不能同时激活的两个或两个以上角色的集合.

$Dyn_mutex(r_i) = \{r_j \mid r_j \text{ 和 } r_i \text{ 满足动态互斥}, i \neq j\}$

约束规则:静态互斥角色集的两个角色不能同时指派给同一主体.动态互斥角色集的两个角色不能在任意一次任务执行中被同时启用.

$\forall (u, r_i, r_j)(r_i \in R(u) \wedge r_j \in R(u)) \Rightarrow r_j \notin Sta_mutex(r_i)$

$\forall (t, r_i, r_j)(r_i \in AR(t) \wedge r_j \in AR(t)) \Rightarrow r_j \notin Dyn_mutex(r_i)$

此外,VO 的管理者还可以根据具体的安全需求自定义约束规则,并随时进行调整.

3.3 安全分析

TSRBAC 是一种动态的授权模型,能解决传统 RBAC 模型中静态授权带来的权限脱离任务问题,可以实现基于任务的细粒度的授权,使用户所拥有的权限仅能满足这次任务的需要.体现了“最小特权”的安全原则.

4 基于 TSRBAC 的网格授权系统

在网格资源共享过程中,授权扮演了十分重要的角色^[6-7].从网格授权的角度看,网格授权是基于资源提供者和虚拟组织之间的契约,因此资源提供者和虚拟组织在资源管理上扮演了不同的角色,在 VO 中明确区分二者的职责是十分必要的.

4.1 社区授权服务

社区授权服务 CAS 是由 Globus 项目组开发的、建立在公钥认证和代理机制之上的基于角色的团体授权技术,用来补充现有资源服务器的授权语言和策略.CAS 的引入减少了用户与资源服务器之

间信任关系的数量,而且可以方便地改动策略,大大提高了系统的可扩展性.用户通过向 CAS 服务器发出请求来获得一组权限,然后利用这组权限向资源提供者提出请求.资源提供者在接收到请求后,先判断是否该虚拟组织拥有这样的权限,然后再判定该用户具有的权限是否允许这样的操作.图 3 给出了 CAS 模型的授权过程.

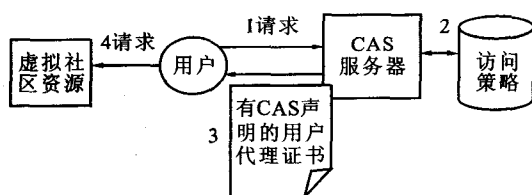


图 3 CAS 模型的授权过程

从授权过程可以看出,用户角色的分配和权限的授予都是在 CAS 服务器进行的,CAS 的策略声明直接给出了最终权限,不需要资源提供者来进一步对组或角色授权.这样的优点是控制高度集中,单点管理,并有灵活的策略标记语言;缺点是在负荷重的情况下会影响整个系统的性能,容易成为通信的瓶颈,并且这种授权方式是静态的,没有考虑具体的执行任务,不适合网格环境资源数量大,动态性和策略自主性的特点.

4.2 TSRBAC 网格授权模型的应用

下面就运用 TSRBAC 模型改进 CAS 系统,使得网格授权过程更加合理,安全有效,如图 4 所示.

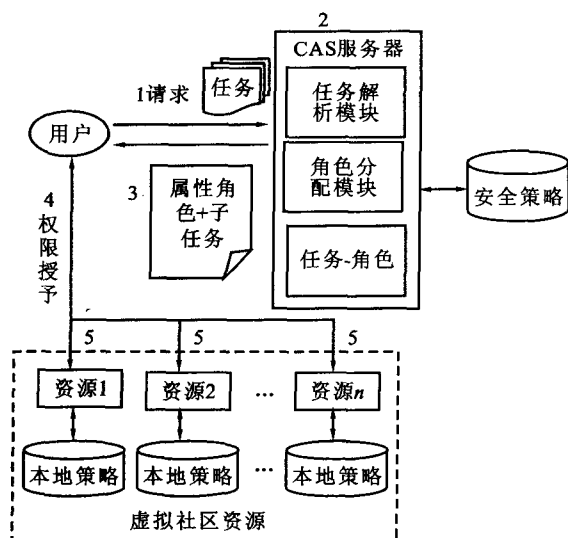


图 4 基于 TSRBAC 的网格授权系统

(1) 总体框架

任务解析模块:对用户发送过来的任务进行解析,根据任务的偏重把任务分成不同的子任务,分别

以 1 到 n 的序号命名,即任务 1,任务 2,...任务 n .

角色分配模块: CAS 服务器中的核心模块,根据一定的访问策略以及实际的任务请求来决定分配给用户什么样的角色.角色分配过程不仅仅考虑用户在虚拟组织中承担的角色,还要考虑实际的任务请求,角色的分配是以任务作为标准的,根据任务确定用户的角色.分配后称为属性角色.

角色任务配置模块:把子任务和不同属性角色进行分组标记.

(2) 工作流程

① 在网格环境下,用户使用 grid-proxy-init 生成代理证书,并向本地的 CAS 服务器提出角色请求,将代理证书和任务的具体信息传递给 CAS 服务器.

② CAS 服务器调用任务解析模块,对任务进行分块,然后调用角色分配模块根据不同的子任务,为用户分配不同的属性角色,最后把不同的属性角色和子任务分类.

③ CAS 服务器为用户生成新的包含有 CAS 声明的用户代理证书,以及属性角色+子任务发送给用户.

④ 用户使用新的代理证书向不同的资源提供者提出权限操作请求,然后根据实际的资源情况,把属性角色+子任务发送给不同的资源提供者.

⑤ 资源提供者根据用户发来的代理证书,判断用户的属性角色和子任务,根据本地的安全策略,进行授权,即权限角色,并执行任务.

4.3 系统分析

改进后的系统把 CAS 服务器的工作由 CAS 和不同的资源提供者共同分担,CAS 服务器只用来存放社区用户的身份声明信息,称为属性角色.并且考虑了网格中的任务,在 CAS 中增加任务解析模块.由资源提供者,也即本地站点的本地中心授权服务和本地信任映射服务根据具体的任务和本地的安全策略来进行授权.CAS 服务器的工作是进行角色定义与分配,以及任务解析,更加有利于管理员进行维护.

改进的模型是一种动态构造模型,结构灵活,扩展性强,实现了动态授权和按需授权,不会使用户分配了某个角色之后,只要激活该角色,用户就拥有了该角色的权限;某一资源节点权限分配不会影响其他节点,可以根据属性角色和任务,以及本地安全策略,进行细粒度授权,满足最小特权原则.

(下转第 50 页)

5 结束语

近年来,以 EZW 为基础的各种改进算法相继推出,它们主要是针对 EZW 算法本身实现效率或其他相关问题进行改进算法的研究,而大多都忽略人眼视觉特性对图像编码的影响.文中根据人眼视觉特性,在经典 EZW 算法的基础上提出一种新的改进算法,目的是对边缘和极平滑区小波系数分配更多的比特数,以使重构图像具有更好的主观视觉质量.实验结果表明文中算法对平滑图像和边缘丰富图像具有更好的重构效果,对于纹理丰富图像则在低比特率情况下具有更好的重构图像质量.

参考文献:

- [1] 余平,马小虎,李建国. 基于 LS9/7 小波的图像压缩算法研究[J]. 微电子学与计算机,2008,25(9): 109 - 111.
- [2] 刘丹,王湘海. 提升方案小波和位平面下的图像质量可分级编码研究[J]. 微电子学与计算机,2007,24(2): 150 - 153.
- [3] Shapiro J M. Embedded image coding using zero trees of wavelet coefficients[J]. IEEE Transactions on Signal Processing, 1993, 41(12): 3445 - 3463.
- [4] Said A, Pearlman W A. A new, fast and efficient image codec based on set partitioning in hierarchical trees[J].

IEEE Transactions on Circuits and Systems for Video Technology, 1996,6(3):243 - 250.

- [5] Patel S, Srinivasan S. Modified embedded zerotree wavelet algorithm for fast implementation of wavelet image codec [J]. Electronics Letters, 2000, 36(20):1713 - 1714.
- [6] Ouafi A, Ahmed A T, Baarir Z, et al. Color image coding by modified embedded zerotree wavelet (EZW) algorithm [C]// IEEE International Conference on Information & Communication Technologies. Damascus, Syria, 2006(1): 1451 - 1456.
- [7] 丁海涛. 一种 EZW 编码的改进算法[J]. 仪器仪表学报, 2005,26(8): 565 - 569.
- [8] Wang, Bovik A C, Sheikh H R, et al. Image quality assessment: from error measurement to structural similarity [J]. IEEE Transactions on image processing, 2004, 13(4):600 - 612.
- [9] Sheikh H R, Bovik A C. Image information and visual quality[J]. IEEE Transactions on image processing, 2006, 15(2): 430 - 444.

作者简介:

付伟男,(1984-),硕士研究生.研究方向为图像质量评价、图像压缩编码.

顾晓东男,(1970-),博士后,副教授.研究方向为人工神经网络、图像处理、模式识别等.

(上接第 46 页)

5 结束语

文中提出的 TSRBAC 模型结合网格环境中的角色和任务,实现了动态授权和按需授权以及权限的细粒度分配.在以后的工作中,将考虑用户属性角色的冗余和权限角色的矛盾等问题,进一步作深入的研究.

参考文献:

- [1] Pearlman L, Kesselman C, Welch V, et al. The community authorization service: status and future[C]//Proc. of Int'l Conference for Computing in High Energy and Nuclear Physics. USA: La Jolla, 2003.
- [2] Sandhu R, Coyne E, Feinstein H, et al. Role-based access control models[J]. IEEE Computer, 1996, 29(2): 38 - 47.
- [3] 毛碧波,孙玉芳.角色访问控制[J].计算机科学, 2003, 30(1):121 - 125.
- [4] Thomas R K, Sandhu R. Task-based authorization con-

trols: a family of models for active and enterprise-oriented authorization management[C]//Proceedings of the 11th I-FIP WG11. 3 on Database Security. Canada, Vancouver, 1997: 166 - 181.

- [5] 张亚红,王勇,陈辉.网格环境下基于角色和任务的访问控制模型设计与研究[J].微电子学与计算机, 2008,25(5):179 - 181.
- [6] 吴毓毅,贺也平.关于网格计算授权机制的研究[J].计算机应用研究,2005,22(8):81 - 83.
- [7] 孙翥,张毓毅,李军怀,等.基于角色的轻量级多粒度访问控制框架研究[J].微电子学与计算机,2008,25(7): 87 - 91.

作者简介:

鲍美英女,(1975-),博士研究生,讲师.研究方向为网络安全、符号矩阵.

马礼男,(1968-),博士,教授.研究方向为高性能计算、网络计算.

高玉斌男,(1962-),博士,教授.研究方向为组合矩阵、符号矩阵.