文章编号:1001 - 9081(2007)09 - 2200 - 02

RBAC 模型中用户代理机制的研究

陈岳阳,马学森,韩江洪,魏振春
(合肥工业大学 计算机与信息学院, 合肥 230009)
(chen_chenyueyang@163.com)

摘 要:针对 ASP 服务平台用户和服务之间权限分配日趋复杂的问题,提出了一种新的角色访问控制(A_RBAC)模型,利用代理层将平台服务与企业级用户关联,采用分级授权的用户角色访问控制运行机制,实现了用户代理机制下权限访问的区域自治性,并应用轻量级目录访问协议(LDAP)和 J2EE 技术将其设计实现于合肥市中小企业信息化托管平台。实践证明,该模型有效地降低了权限分配的复杂性。

关键词:应用服务提供商;用户代理;基于角色的访问控制;权限;轻量级目录访问协议
中图分类号: TP311.5 **文献标志码**:A

Research of user Agent mechanism in RBAC model

CHEN Yue-yang, MA Xue-sen, HAN Jiang-hong, WEI Zhen-chun
(*School of Computer and Information, Hefei University of Technology, Hefei Anhui* 230009, *China*)

Abstract: In order to solve the more and more complicated problem of permission assignment between users and services on ASP service platform, A new Role-Based Access Control (A_RBAC) model was proposed. A_RBAC model made platform services associated with enterprise level user by making use of Agent layer, adopted mechanism of user role access control of classification authorization, implemented regional autonomy of permission access in user Agent mechanism and was applied to the platform of information trusteeship of small medium enterprises with Lightweight Directory Access Protocol (LDAP) and Java 2 Platform Enterprise Edition (J2EE) in Hefei city. The results show that the complexity of permission assignment is effectively reduced.

Key words: ASP; user Agent; Role-Based Access Control (RBAC); permission; Lightweight Directory Access Protocol (LDAP)

ASP 是指通过网络提供应用的部署、供应、管理以及对应用出租访问服务的一种集中管理的组织[1]。随着 ASP 服务平台的发展,平台提供的服务日趋增多,用户(以企业用户为主)规模日趋庞大,用户和服务之间权限分配日趋复杂。目前,用户管理主要采用主动和被动管理两种模式。主动管理是完全由用户进行自主定制服务并个性化的管理,有着 ASP 平台管理员不参与管理的缺点。而被动管理中,用户只能被动地接受 ASP 平台管理员的管理,又存在着不能自主地定制服务,缺少灵活性等缺点[2]。

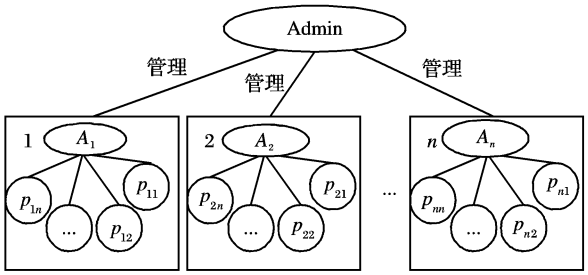
鉴于此,在向用户提供可定制的、个性化服务的同时,又能对服务的灵活性进行有效地监督、管理,保证 ASP 平台提供的应用服务被合法、安全地使用,本文提出了一种分级授权形式的基于用户代理机制的角色访问控制(A_RBAC)模型,通过 LDAP 目录信息树的设计与实现,最终部署应用于合肥市 J2EE 架构的中小型企业信息化应用服务托管平台中[3-6],有效降低了企业用户和服务间权限分配的复杂度,从而为企业用户提供安全、灵活的个性化服务。

1 用户代理管理和 A_RBAC 模型

1.1 用户代理管理与 A_RBAC 模型的关系

用户代理管理是指在企业个体中引入代理管理层,由其直接负责企业内部事务的具体管理,改变 ASP 平台的直接或垂直管理为间接管理。该管理方式既增强了用户的自主管理性,减轻平台管理的负担,同时又符合管理的现实性与可操作性。在此基础之上,建立分级授权的 A_RBAC 模型,它是指代理管理层以企业为单位,指派或取消平台提供服务的角色,达到对平台提供服务的权限灵活分配与控制管理。

1.2 用户代理管理



注: Admin:ASP平台管理员 1–*n*:企业
A_1–A_n:代理管理员 p_{11}–p_{1n},…, p_{n1}–p_{nn}:企业用户

图 1 代理管理层次图

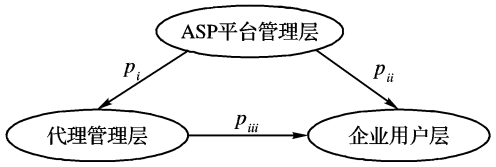
用户代理管理的具体实施采用 ASP 平台管理层集中授权企业超级用户管理组为该企业的代理管理层的方式,转变单个员工的终端服务对象为企业单位,实现间接、直接管理的

收稿日期:2007 - 03 - 30;**修回日期**:2007 - 06 - 07。 **基金项目**:合肥市制造业信息化专项基金资助项目(合科[2005]11 号);安徽省高等学校青年教师科研计划项目(2006JQ1013);合肥工业大学科学研究发展基金资助项目(060503F)。

作者简介:陈岳阳(1983 -),男,浙江绍兴人,硕士研究生,主要研究方向:企业信息化; 马学森(1976 -),男,安徽庐江人,讲师,博士研究生,主要研究方向:企业信息化、嵌入式系统; 韩江洪(1954 -),男,安徽泾县人,教授,博士生导师,主要研究方向:分布式控制、嵌入式系统; 魏振春(1978 -),男,宁夏青铜峡人,讲师,博士研究生,主要研究方向:离散事件控制系统、网络与分布式计算。

合理衔接,达到企业资源配置的最优化。该模式分为三层:最上层是 ASP 服务平台管理层,对 ASP 平台的所有用户进行授权和约束管理;中间层是面向企业内部用户的代理管理层,向上可根据企业自身需求,灵活定制 ASP 平台的服务,向下可根据企业组织结构,为不同的用户授予不同的权限;最底层是企业用户层,是 ASP 平台的基础用户(如图 1 所示)。

为了能使三层之间合理的管理,其授权关系必须满足以下约束条件:$P_i > P_{ii} \geqslant P_{iii}$,其中 > 表示高于,≥表示高于或等于(如图 2 所示)。



p_i —ASP平台管理层授予代理管理层的权限
p_{ii} —ASP平台管理层授予企业用户层的权限
p_{iii} —代理管理层授予企业用户层的权限

图 2　代理管理的授权模型

1.3　A_RBAC 模型

为了能高效、安全地访问 ASP 平台提供的各种应用服务,基于角色的访问控制不可或缺,ASP 平台视其为实现访问控制的基本语义实体,通过平台管理层将各个服务中的权限控制进行分组、归类,建立层次化映射关系,并抽象为对应的角色,再依据代理管理层所定制的服务,指派或取消该终端服务对象的角色,建立用户与服务权限集合间的灵活对应关系(一对一、一对多或多对多)。

该 A_RBAC 模型可描述为:若 $pr \in privilege_u(s)$ 表示企业 c 的用户 u 在服务 s 中具有某项权限 pr,若 $pr \in privilege_u(s)$,当且仅当下式成立:

$$(\exists r)(\exists c)(\exists s)((r \in Role_u(s)) \wedge (pr \in privilege_r(s)) \wedge (u \in Company(c)) \wedge (s \in Service(c)))$$

其中:

$Role_u(s)$—企业用户 u 在 ASP 平台上服务 s 角色的集合;

$privilege_r(s)$—角色 r 在 ASP 平台上服务 s 中被分配的权限的集合;

$privilege_u(s)$—用户 u 在服务 s 中拥有的权限的集合;

$Service(c)$—企业 c 在 ASP 平台上定制的服务集合;

$Company(c)$—企业 c 的员工集合;

u—企业用户;

r—ASP 平台中的角色;

pr—ASP 平台服务中的使用权限;

c—企业;

s—ASP 平台上的服务。

2　A_RBAC 模型的设计与实现

2.1　A_RBAC 模型的 LDAP 设计

由于 LDAP 是一种能提供方便、快捷查询的服务,所以将 A_RBAC 模型设计到 LDAP 提供的目录查询中。LDAP 是由目录信息树(DIT)的树型结构来组织数据的,它的根没有实际意义,它的叶子称作条目,是存储数据的入口,一个条目由唯一的“Distinguished Name”(DN)和任意多的(属性,值)对组成,一个属性可以包含一个或多个值。

假定 ASP 服务平台网址是 www. hfinfoasp. com,则“dc = hfinfoasp,dc = com”作为根节点。根据 A_RBAC 模型要求,每个企业对应根节点中的一个分支节点。而企业内部的员工则位于下面的子树。图 3 虚线框内显示了 ASP 平台的用户目录信息树。对于每一个特定用户,自顶而下的路径 DN 则唯一对应了该用户的辨识名。企业 Y 的代理管理员由“cn = 管理员 Y,ou = 企业 Y,dc = $hfinfoasp$,dc = com”来表示(其中 $Y \in \{1,2,\cdots,n\}$)。

由于各个企业的代理管理员定制的服务各不相同,所以在代理管理员的条目中存储着各自定制服务信息的 Java 对象;而各个企业用户的条目中存储着所在企业的代理管理员为其分配角色信息的 Java 对象(如图 3 实线框所示)。

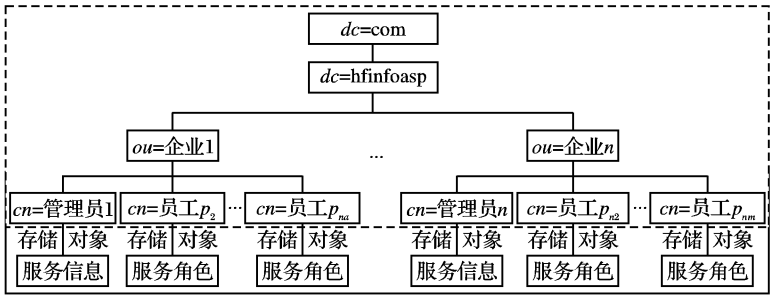


图 3　LDAP 目录信息树的设计

2.2　基于 J2EE 架构的 A_RBAC 模型实现

ASP 平台采用当前流行的 J2EE 架构,LDAP 的 A_RBAC 模型访问控制可概括为:通过提交条目信息,访问在 LDAP 服务器中存储的条目,获取对应的 Java 对象,根据 A_RBAC 模型的内在业务逻辑,判断返回结果,实现代理机制下权限控制。

基于 J2EE 的具体软件实现如图 4 所示:客户端通过浏览器或 Java Applet 输入用户信息并发送请求到 J2EE 服务器端;服务器端通过 Web 容器中的 JSP 或 Servlet 接收请求后,调用 EJB 容器中的 EJB 类;EJB 类通过 JNDI 的应用程序接口(API),调用 JNDI 的服务提供者接口(SPI),提交相关参数(LDAP 目录信息树的条目等信息),查询存储介质层的 LDAP 服务器(openldap等)中该用户的属性和Java对象;EJB类得

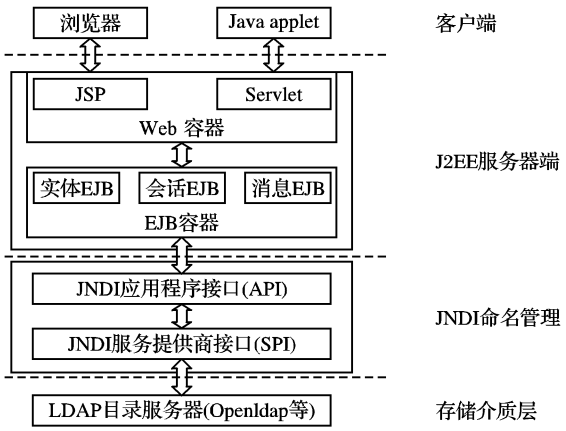


图 4　J2EE 软件架构的实现

(下转第 2205 页)

网络中激励机制研究的一个重要方向。

4　结语

随着对等计算技术的广泛应用,P2P 网络中普遍存在的搭便车问题也日益受到关注,而激励机制正是在这样的背景下产生和迅速发展起来。目前的各种激励机制虽然都还存在着一些问题,但对解决搭便车问题都起到了一定的效果,其中一些成果也已经在实际系统中得到应用。

作为对等计算领域的一个重要方向,激励机制仍存在着不少问题.我们认为未来的激励机制研究有如下 3 个方向:1)量化比较激励机制的代价与效用,衡量激励机制的引入对系统性能产生的正面和负面影响;2)结合不同激励机制的优点建立一种通用的激励框架,使之适应不同的应用环境等;3)进一步根据 P2P 网络节点行为与社会中人的行为的相似性,将经济学和社会学的有关理论引入到 P2P 网络中,改善激励机制的效率。

参考文献:

[1] 张维迎. 博弈论与信息经济学[M]. 上海: 上海人民出版社, 2004.

[2] 宿建宗, 李秉智. P2P 文件共享框架中激励机制的研究[J]. 重庆邮电学院学报: 自然科学版, 2006, 18(1): 123 - 125.

[3] 肖波. 基于遗传算法的 P2P 激励机制[J]. 西南交通大学学报, 2005, 40(3): 417 - 421.

[4] 田慧蓉. 激励一致的自适应 P2P 拓扑构造. 软件学报, 2006, 17(4): 840 - 852.

[5] FELDMAN M, CHUANG C. Overcoming free-riding behavior in peer-to-peer systems [J]. ACM SIGecom Exchanges, 2005, 5(4): 41 - 50.

[6] ADAR E, HUBERMAN B. Free riding on gnutella [J]. First Monday, 2000, 5(10): 42 - 68.

[7] GOLLE P, LEYTON-BROWN K, MIRONOV I. Incentives for sharing in peer-to-peer networks[C]// Proceedings of the 2001 ACM Conference on Electronic Commerce. [S. l.]: ACM Press, 2001: 264 - 267.

[8] YANG A, GARCIA-MOLINA H. PPay: micropayments for peer-to-peer systems [C]// Proceedings of the 10th ACM conference on Computer and communications security. [S. l.]: ACM Press, 2003: 300 - 310.

[9] WEI K, CHEN Y. WhoPay: a scalable and anonymous payment system for peer-to-peer environments[C]// 26th IEEE International Conference on Distributed Computing Systems. [S. l.]: IEEE Press, 2006: 13 - 23.

[10] COHEN B. Incentives build robustness in bittorrent [EB/OL]. [2007 - 02 - 01]. http://bitconjurer. org/BitTorrent/bittorrentecon. pdf.

[11] KOSTAS G, GREENWALD M. Exchange-based incentive mechanisms for peer-to-peer file sharing [C]// Proceedings 24th International Conference on Distributed Computing Systems. San Francisco: IEEE Computer Society, 2004: 524 - 533.

[12] KaZaA[EB/OL]. [2007 - 02 - 01]. http://www. kazaa. com.

[13] BURAGOHAIN C. A game theoretic framework for incentives in p2p systems [EB/OL]. [2007 - 02 - 01]. http://www. cs. ucsb. edu/ ~ suri/psdir/incentives. pdf.

[14] FELDMAN A. Robust incentive techniques for peer-to-peer networks [C]// Proceedings of the 5th ACM conference on Electronic commerce. San Diego: ACM Press, 2004: 102 - 111.

[15] FELDMAN M, PAPADIMITRIOU C. Free-riding and whitewashing in peer-to-peer systems [J]. IEEE Journal on Selected Areas in Communications, 2006, 24(5): 228 - 236.

[16] O'HEARN B. Experiences deploying a large-scale emergent network [C]// First International Workshop on Peer-to-Peer Systems. Cambridge: [s. n.], 2002: 116 - 123.

[17] VARIAN HR. Economic mechanism design for computerized agents [C]// Proceedings of the First USENIX Workshop on Electronic Commerce. New York: [s. n.], 2005: 241 - 251.

[18] FELDMAN A. Hidden-action in multi-hop routing [C]// Proceedings of the 6th ACM conference on Electronic commerce. [S. l.]: ACM Press, 2005: 12 - 22.

[19] NGAN T, WALLACH D, DRUSCHEL P. Incentive - compatible peer-to-peer multicast [C]// Proceedings of First Workshop on Economics of P2P Systems. Berkely: [s. n.], 2003: 56 - 63.

[20] XIONG L, LIU L. A reputation-based trust model for peer-to-peer ecommerce communities [C]// Proceedings of the 4th ACM conference on Electronic commerce. [S. l.]: ACM Press, 2003: 228 - 229.

[21] KAMVAR S D, SCHLOSSER M T, GARCIA - MOLINA H. The eigentrust algorithm for reputation management in P2P networks [C]// Proceedings of the 12th International Conference on World Wide Web. San Diego: ACM Press, 2003: 640 - 651.

(上接第 2201 页)

到查询的结果后,按照 A_RBAC 模型的内在业务逻辑判断返回结果;用户得到授权可访问的服务页面。

3　结语

本文在用户代理管理基础上,提出了一种基于用户代理机制的角色访问控制模型,以企业为单位的管理单元替代原先的单个用户,变直接管理单个用户为分层的间接管理,分层、分角色授权所管对象,同时将该模型设计、实现于 LDAP 服务中,有效地降低了用户和服务之间权限分配的复杂性,保证了 ASP 服务平台灵活安全地运行。目前,该模型已成功应用于合肥市中小型企业信息化应用服务托管平台中,较好地解决了 ASP 服务平台的用户和服务之间权限分配复杂性与实际操作的可行性问题。

参考文献:

[1] 易大勇, 邢桂芬, 赵曦滨. 基于应用服务商模式的轻量级企业 OA 的研究与应用[J]. 计算机应用研究, 2003, 20(7): 158 - 160.

[2] 戴建华, 蔡铭, 林兰芬, 等. 面向网络化制造的 ASP 服务平台若干关键技术研究[J]. 计算机集成制造系, 2005, 11(1): 48 - 52.

[3] 刘明, 蒋朝惠, 李燕华, 等. 基于 J2EE 标准 ASP 服务平台的实现[J]. 计算机应用与软件, 2006, 23(4): 142 - 144.

[4] 赵保翠, 刘岗. 基于 LDAP 的统一用户管理系统的设计和实现[J]. 微电子学和计算机, 2005, 22(11): 59 - 62.

[5] 韩煜玮, 梁意文, 李涛. 使用 LDAP 在 Web 环境中实现 RBAC 的方法[J]. 计算机工程, 2004, 30(8): 130 - 132.

[6] 金信苗. 基于角色的访问控制模型在 LDAP 服务中的研究与设计[J]. 微电子学与计算机, 2005, 22(6): 141 - 144.