企业门户中基于令牌的角色访问控制模型

朱晓洁 熊 璋 吴 晶

(北京航空航天大学 计算机学院, 北京 100083)

摘 要: 企业门户中用户和访问权限管理的研究是一项复杂且具挑战性的工作. 传统的基于角色的访问控制模型(RBAC, Role-Based Access Control)在实现上通常受单一系统和应用的约束,因此提出了一种基于令牌的角色访问控制模型(TRBAC, Token Role-Based Access Control). 该模型采用门户平台下的单点登录(SSO, Single Sign On)技术,将 RBAC 模型与令牌访问机制相结合,使角色能跨越门户平台下所有的 Web 应用. 该模型是一个动态激活的模型,根据用户实际的访问需求动态激活相应角色,为用户管理和访问控制管理提供了一个新的解决方案. TRBAC 模型具有统一的用户安全管理标准,支持集中审核和控制. 实践表明,采用 TRBAC 模型提高了系统的访问效率,保证了系统的安全性.

关 键 词: 企业门户; 访问控制模型; 基于角色的访问控制; 令牌

中图分类号: TP 309.2

文献标识码: A **文 章 编 号**: 1001-5965(2006)07-0873-04

New model for token role-based access control on enterprise portal

Zhu Xiaojie Xiong Zhang Wu Jing

(School of Computer Science and Technology, Beijing University of Aeronautics and Astronautics, Beijing 100083, China)

Abstract: Manage users and access rights are a complex and challengeable job in enterprise portal. Importing the role concept may simplify the access control, but its implementation is usually constrained by the single system and application. A new model, TRBAC (token role-based access control), was proposed for RBAC (role-based access control) on enterprise portal, which integrated the SSO (single sign on) technology and combined the RBAC model with token access mechanism. The role could span all web systems in portal. It was a token-based and dynamic-activated access control model, which could dynamically adjust the access rights according to user access requirement. It solved the problems on user management and access control management, and supported the corporate security standards, central auditing and control. The practice indicates that TRBAC improves the system efficiency and ensures the security.

Key words: enterprise portal; access control model; role-based access control; token

门户是 Web 应用程序简单统一的访问入口,提供了集成的内容和应用服务以及统一的工作协作环境[1]. 企业门户作为门户的应用分支,要求集成各种结构化和非结构化的信息资源,为用户提供统一的资源入口、整体的安全机制及统一的用户管理. 因此,在企业门户中,用户和访问控制管理成为研究和开发人员所关注的问题.

1992 年由 Ferraiolo 和 Kuhn 提出的基于角色的访问控制模型(RBAC, Role-Based Access Control)通过引入角色这一中介实现了用户与权限的逻辑分离[2],其主要思想是将访问权限分配给角色. 与用户相比角色是相对稳定的,角色所关联的权限和用户是动态的. 通过用户-角色、角色-权限的关联,RBAC 与直接的用户-权限关联访问控制模型相比,简化了授权的管理,减少了授权管理工作的复杂度[3],这一模型为用户和访问权限管理

收稿日期: 2005-07-25

基金项目: 国家高技术研究发展计划(863 计划)资助项目(2002AA113070)

作者简介: 朱晓洁(1982-), 女, 湖南湘潭人, 硕士生, zhu _ xiaojie@ hotmail. com.

提供了简单有效的方法. 然而,传统的基于角色的访问控制模型在实现上通常受单一系统和应用的约束,它将用户、角色、权限看成是静态的对象[4],而不考虑用户执行操作时所处的环境,这种机制在多应用系统中,尤其是在角色种类繁多、结构复杂的多应用集成环境下,系统安全不易保障. 因此,在集成了多个拥有大量数据信息的应用系统及要求系统能访问跨平台应用的企业门户体系架构中,必须加强对门户集成多应用系统的身份认证和访问控制,以适应大规模用户在企业门户平台上的访问以及对海量数据资源的管理.

1 企业门户结构中实体关系的建立

针对目前大型企业门户架构的特点,本文将门户系统的结构抽象为 3 层体系架构,即用户表示层、认证链接层以及目标应用层,如图 1 所示. ①用户表示层是基于 Web 的图形用户接口 GUI,提供集中式的管理;②认证链接层由门户验证服务器和门户目录服务器组成,构成门户服务器:验证服务器实现访问控制的业务逻辑,提供统一的用户身份验证入口;目录服务器用来存放用户属性基本信息;③目标应用层是门户集成的应用系统,本文称之为目标应用系统(TAS, Target Application System),在 TAS 上安装的代理提供了验证服务器和 TAS 之间的连接.

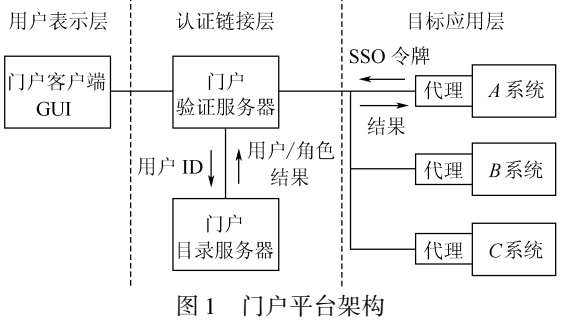


图 1 门户平台架构

根据以上门户平台架构,建立企业门户的实体关系图,见图 2. 关系图中门户实体部分包括用户、角色和门户管理单元,其中用户是门户实体的中心,也是门户管理单元的成员;角色用来分配权限;用户和角色之间为多对多的映射关系.

图 2 中 TAS 实体部分包括用户 ID、资源角色和组. 用户 ID 是用户在 TAS 实体中的具体表现形式,它可以是组成员,与资源角色之间建立多对多的映射关系,TAS 实体与门户实体之间通过用户 ID(即用户账户)来映射. 令牌中携带的用户 ID 信息则将多个 TAS 与门户服务器联系起来. 因此,在增加了令牌对 TAS 访问的同时,本文提出了一种与令牌机制相结合的角色访问控制模型(TRBAC, Token Role-Based Access Control).

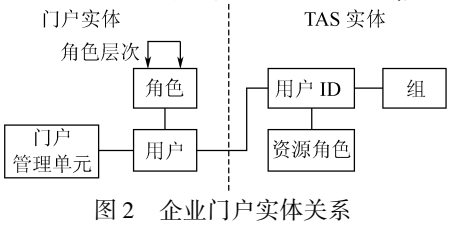


图 2 企业门户实体关系

2 TRBAC 模型

2.1 TRBAC 模型的设计

在传统的 RBAC 中,由于用户和操作对象都被作为静态对象来考虑,用户一旦被授予某个角色,就拥有了该角色对应的服务资源的访问权限,而没有考虑用户及操作对象的动态性[4]. 实际上用户的权限既受限于其所扮演的角色,又取决于用户当前操作的应用. 这些新的要求在 TRBAC 模型的设计中反映如下:①引入了 TAS 的概念. 门户中的角色能跨越多个不同的 TAS,它的权限由授予的所有应用的权限集合组成;②访问控制过程中引入令牌机制. 目标应用验证令牌中包含的权限信息,通过令牌动态激活用户的相应角色,实现用户对 TAS 的访问控制;③动态管理角色. 通过触发令牌,动态激活用户在访问过程中扮演的角色,加强对用户实际行使权限的控制能力,方便管理员的集中审核和控制.

在门户集成的多个应用系统中,用户访问不同的应用时需要为每个应用分别建立一个会话,每个会话包含各自的访问权限,由于没有统一的 RBAC 模型支持,这些权限由不同的系统管理,带来了操作的复杂性. 引入令牌机制方便对用户进行集中统一的管理,增加了用户与请求服务之间的透明度,简化了管理员的操作. 当用户登录成功获取令牌后,将此用户的角色信息添加到令牌中,用户访问 TAS 只需提交此令牌,由目标应用验证令牌中包含的权限信息,实现对用户的授权访问控制管理.

由此,建立基于令牌的角色访问控制模型 TRBAC 如图 3 所示. 对 TRBAC 模型做如下定义:

定义 1 TRBAC 模型. $M_{\mathrm{TRBAC}}=(U,R,P,U_{\mathrm{ID}},T,P_{\mathrm{TAS}})$. 其中,$U$ 是用户集;R 是角色集;P 是权限集合;T 是令牌;U_{ID}是用户 ID;P_{TAS}是指定的目标应用系统的权限集合. 在模型中定义下列关系:①用户分配关系(UA, User Assignment)是用户到角色的多对多的映射关系,用 U_{UA}表示,即 $U_{\mathrm{UA}}\subseteq U\times R$;②权限分配关系(PA, Permission Assign-

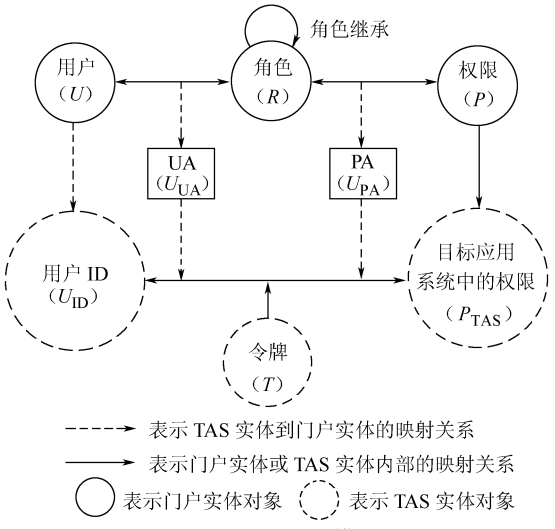


图 3　TRBAC 模型

ment)是访问权限到角色的多对多的映射关系,用 U_{PA} 表示,即 $U_{PA} \subseteq R \times P$;③用户角色限制关系(UC,User Constraint)是角色授予的用户最大数目限制关系,用 U_{UC} 表示,即 $U_{UC} \subseteq R \times \mathbf{N}$($\mathbf{N}$ 为自然数集合);④令牌分配关系(TU,Token User Assignment)是令牌与用户之间一对一的映射关系,用 U_{TU} 表示,即 $U_{TU} \subseteq T \times U$.

定义 2　令牌. 令牌简单地包含了用户 ID 及相应角色的权限信息,它提供了基本用户名/密码验证的方法. 令牌可以做如下操作:①令牌创建(token creation):当用户登录成功后,为当前用户创建一个令牌;②令牌激活(token activation):令牌与用户建立映射关系后,将激活此用户关联的角色,直至被撤销;③令牌生存(token lifetime):令牌创建后,将赋予一个生命周期,在此段时间内,令牌映射的用户所关联的权限是有效的;④令牌撤销(token revocation):令牌的生命周期中止时,自动撤销令牌,令牌与用户的映射关系也被取消,同时由令牌激活的所有角色都将被收回.

2.2　TRBAC 访问控制策略

TRBAC 模型是一个基于令牌的角色动态激活的访问控制模型,其访问控制实施过程分为以下 3 个阶段.

1) 目标应用系统-用户权限分配.

系统管理员根据不同的 TAS 对用户进行角色分配以及对角色的权限进行预定义. 在 TRBAC 模型中,用户被授予的角色集合用 $U_{RA}(u)$ 表示,用户 u_i 与角色 r_j 之间的关系表现为 $U_{RA}(u_i) \rightarrow 2^{r_j}$. 角色 r 授予的用户集合用 $U_{UA}(r)$ 表示,角色 r_i 与用户 u_j 之间的关系表现为 $U_{UA}(r_i) \rightarrow 2^{u_j}$. 角色 r 授予的最大用户数记为 $c(r)$,拥有角色 r_i 的最大用户数目表现为 $c(r_i) \leqslant \zeta$,其中 ζ 为常量. 同理,角色 r 被授予的一组权限集记为 $U_{PA}(r)$,角色 r_i 与权限 p_{tasj} 之间的关系表现为:$U_{PA}(r_i) \rightarrow 2^{p_{tasj}}$.

2) 令牌使能的角色动态激活.

用户要获得实际的角色授权,需要在静态角色分配的基础上在令牌中动态地激活角色,只有当角色授权给令牌关联的用户时,令牌才能激活此角色. 在 TRBAC 模型中,令牌与用户之间一对一的映射关系记为 U_{TU},$U_{TU} \subseteq T \times U$,$U_{TU}(t)$ 表示令牌 t 关联的用户,令牌 t_i 与用户 u_j 的关系表现为 $U_{TU}(t_i) = u_j$. 令牌与角色之间的映射关系记为 U_{AR},$U_{AR} \subseteq T \times R$,令牌 t 激活的角色集用 $U_{AR}(t)$ 表示,令牌 t_i 与角色 r_j 的关系表现为 $U_{AR}(t_i) \rightarrow 2^{r_j}$. 激活令牌的生成函数为 $A_r(r,t)$,表示用户在令牌 t 中被授予角色 r;相应地,撤销令牌的生成函数为 $R_r(r,t)$,表示用户被授予的角色 r 在令牌 t 中被撤销.

当用户提出对 TAS 的访问请求后,门户系统将对用户进行身份验证,根据令牌中的 U_{ID} 查找用户是否被分配了具有访问该应用系统的权限,如果成功则在令牌中激活该角色 $A_r(r,t)$ 的生成条件可以表示为

$$(\forall t \in T, u \in U, r \in R) u \in U_{UA}(r) \wedge U_{TU}(t) \in U_{UA}(r) \wedge r \in U_{AR}(t) \Rightarrow A_r(r,t)$$

3) 动态权限调整.

在 TRBAC 模型中,通过动态的职责分离(DSD,Dynamic Separation of Duty)以及令牌的生命周期 2 个方面来动态调整用户的访问权限. 在 DSD 中,互斥的角色用 E_r 表示,$E_r = \{(r_i, r_j) \mid r_i \in R, r_j \in R\}$. 在 TRBAC 模型的动态调整过程中,根据 DSD 原则,互斥的角色可以分配给同一用户,但不能被同时激活. r_i 和 r_j 互为互斥的角色,若 r_i 由令牌 t_1 激活,r_j 由令牌 t_2 激活,则 t_1 和 t_2 必定关联不同的用户,通过这种方式来实现动态的职责分离. 表现如下:

$$(\forall t_1, t_2 \in T)(\forall r_i, r_j \in R) (r_i, r_j) \in E_r \wedge r_i \in U_{AR}(t_1) \wedge r_j \in U_{AR}(t_2) \Rightarrow U_{TU}(t_1) \neq U_{TU}(t_2)$$

令牌的生命周期用来限制对用户的授权,当令牌没有被触发之前,用户相关联的角色并没有被激活,所授予的权限是无效的;一旦令牌被触发,立即激活角色,同时令牌的生命时钟开始计数,在此生命周期内角色的权限是有效的;当授权超过生命周期,权限就失效了,令牌生命周期终止时,将撤销所有激活角色.

一个用户 u 能否对目标应用系统 p_{tas} 进行访

问的条件是:存在一个角色 r 被分配给用户 u,u 在令牌中被激活,且 r 对 p_{tas} 有授权. 令函数 $A_u(u, p_{tas})$ 表示访问应用系统的方法,函数 $R_u(u, p_{tas})$ 表示访问应用系统的请求,即

$$A_u(u, p_{tas}) \rightarrow R_u(u, p_{tas}) \wedge$$
$$\exists r(u \in U_{UA}(r) \wedge p_{tas} \in U_{PA}(r) \wedge A_r(r, t))$$

因此,用户对目标应用系统的访问,取决于用户角色的分配、令牌使能的角色激活以及在实际访问过程中动态权限调整.

2.3 TRBAC 的安全性

TRBAC 支持 2 个经典的安全控制原则:

1) 最小特权原则[5]:在执行任务时只给用户分配所需的权限,未执行任务或任务终止后用户不再拥有所分配的权限;而且在执行任务过程中,当某一权限不再使用时,令牌自动将该权限回收;

2) 职责分离原则[6]:有时一些敏感的任务需要不同的用户执行,这可以通过在令牌中动态权限调整来实现.

3 TRBAC 模型的应用实现

本文提出的 TRBAC 模型适用于企业门户系统,尤其适用于基于单点登录令牌访问机制的门户集成应用系统.

TRBAC 模型的实现见图 4,客户端与 IS 认证服务之间采用门户服务专门的 Identity SDK 接口,策略管理与目录服务器之间采用标准的 LDAP(Lightweight Directory Access Protocol)访问方式即 JNDI 接口,单点登录令牌采用封装的 JAVA 包实现. 这个过程包括:

1) 验证用户的身份信息(用户名/密码是否匹配);

2) 联系策略管理,与 LDAP 通信,获取用户的角色信息,同时在令牌中激活该角色;

3) 用户策略管理,制定用户访问策略,将决策返回认证服务器;

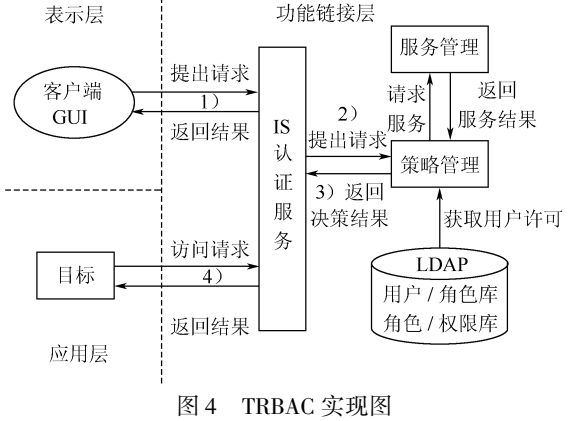


图 4 TRBAC 实现图

4) 服务允许反馈,认证服务器将结果(允许或拒绝访问)返回到客户端.

目前,TRBAC 模型已经在 863 虚拟软件专业孵化器门户系统中得到了应用. 该系统采用 Sun JES 平台及其门户体系架构,以门户组件方式部署,与专业门户整合技术相结合实现统一协同门户系统. 实践表明,采用 TRBAC 模型缩短了设计周期,提高了系统的访问效率,保证了系统的安全性.

4 结束语

大型企业采用门户技术已经成为一种必然的趋势,而用户管理和访问控制的高复杂性是其实现过程中的关键难点. 本文针对企业门户平台架构的特点,提出了一种新的基于令牌的角色访问控制模型——TRBAC,它结合 RBAC 模型,增加令牌机制,将传统 RBAC 的角色扩展到多系统和多应用中,使之能够适应集成多个应用的企业门户环境. 与传统 RBAC 模型比较,TRBAC 通过令牌来激活角色的授权,在权限分配上支持动态职责分离和最小权限原则,能够使系统灵活授权,且权限集中管理,同时考虑了安全管理问题,适合大型企业门户平台下访问控制的实施.

参考文献 (References)

[1] 徐家俊,贾文玉. 企业信息门户 EIP[M]. 北京:机械工业出版社,2004
Xu Jiajun, Jia Wenyu. Enterprise information portal[M]. Beijing: China Machine Press, 2004(in Chinese)

[2] Ferraiolo David, Kuhn Richard. Role-based access controls[C]// Proceedings of the 15th NIST-NCSC National Computer Security Conference. Baltimore: NIST-NCSC, 1992: 554-563

[3] Ferraiolo David, Barkley John, Kuhn Richard. A role-based access control model and reference implementation within a corporate intranet[J]. ACM Transaction on Information and System Security, 1999, 2(1): 34-64

[4] 许峰,赖海光,黄皓,等. 面向服务的角色访问控制技术研究[J]. 计算机学报,2005,28(4):686-693
Xu Feng, Lai Haiguang, Huang Hao, et al. Service-oriented role-based access control[J]. Chinese Journal of Computers, 2005, 28(4): 686-693(in Chinese)

[5] Saltzer J H, Schroeder M D. The protection of information in computer systems[J]. Proceedings of the IEEE, 1975, 63(9): 1278-1308

[6] Wood C, Fernandez E B. Authorization in a decentralized database system[C]//Proceedings of the 5th International Conference on Very Large Databases. Brazil: IEEE Computer Society, 1979: 352-359

(责任编辑:文丽芳)