文章编号:1001-2486(2011)05-0123-05

一种面向公共服务的跨域授权模型的研究及实现*

申巍葳[1],王宝生[2],贺建忠[3]
(1. 北京科技大学 信息工程学院,北京 100083; 2. 国防科技大学 计算机学院,湖南 长沙 410073;
3. 华北计算技术研究所,北京 100083)

摘 要:文章提出一种基于策略的RBAC的跨域统一授权模型,在基于策略的RBAC单域授权模型的研究基础上,扩展单域模型为多域模型,通过授权控制中心之间建立跨域级联机制,构成广域授权网络,实现面向多应用系统、大型公共服务域的跨域统一自动授权机制。

关键词:跨域授权;模型;访问控制;安全
中图分类号:TP311 **文献标识码**:A

Study and Realization on an Authorization Model Oriented Public Service of Over Domain and Application

SHEN Wei-wei[1], *WANG Bao-sheng*[2], *HE Jian-zhong*[3]
(1. School of Information Engineering, University of Science and Technology Beijing, Beijing 100083, China;
2. College of Computer, National Univ. of Defense Technology, Changsha 410073, China;
3. North China Institute of Computer Technology, Beijing 100083, China)

Abstract: An authorization model of over domains based on RBAC is presented. The study described an RBAC authorization model based on policies for a single domain firstly, and then it built a network model by extending it to an authorization model for crossing the domains. So it resolved the problem of authorization integrating facing to many applications crossing the domains.

Key words: authorization; over domain; model; security

面向公共服务的多应用系统的整合是软件业发展的趋势,而目前系统整合面临着授权方式不统一、资源难以有效共享的问题。在任何一个大型公共服务领域,作为每个应用系统保护系统资源必备部分的授权管理,由于授权实现思路不统一、用户种类和数量的急剧攀升,造成了系统集成的极大困难。为了解决这一问题,出现了多种访问控制模型,如强制访问控制(Mandatory Access Control,MAC)模型、自主访问控制(Discretionary Access Control,DAC)模型、基于角色的访问控制(Role Based Access Control,RBAC)模型、基于任务的访问控制(Task Based Access Control,TBAC)模型[1-2]等。其中RBAC能够降低安全管理成本和管理复杂性,是解决大型、复杂系统访问控制问题的首选方案[3-4],至今仍然在授权管理领域得到广泛使用,但RBAC模型仍然不能解决多应用系统高效统一授权问题。

解决大型系统高效授权的问题,基于策略的自动授权是一种好方法,这方面已开展了大量研究[5]。我们在以往基于策略方法的基础上,提出一种基于策略的RBAC统一授权模型[6],通过规范权限表示和引入授权代理的方式,有效降低策略表示的复杂性,提高系统的访问效率。但是,当服务域面临的地域广阔,网络通讯与管理上要求分为不同的多个服务域(广域子网)时,需要跨域授权和访问控制,目前的模型还难以适应。为解决这一问题,本文在前期单域模型的研究基础上,将单域模型扩展为一种面向大型公共服务域的跨域授权模型。该模型仍以基于策略的RBAC模型为基础,在逻辑设计上将每个域授权机制分为授权中心和应用代理两部分,利用授权中心建立的目录体系,构成多域授权与访问控制机制,从而解决面向多应用、多子域及大量用户的跨域自动授权问题。

* 收稿日期:2011-01-17
基金项目:国家自然科学基金资助项目(60803153)
作者简介:申巍葳(1970—),男,博士生。

1 数据模型

1.1 单域概念模型

每个域 yu 是一个三元组 (P, Pt, App)，其中 P 是一个人员子集，Pt 是 P 对应的人员属性集，App 是一个应用子集。域的概念模型如图 1 所示。

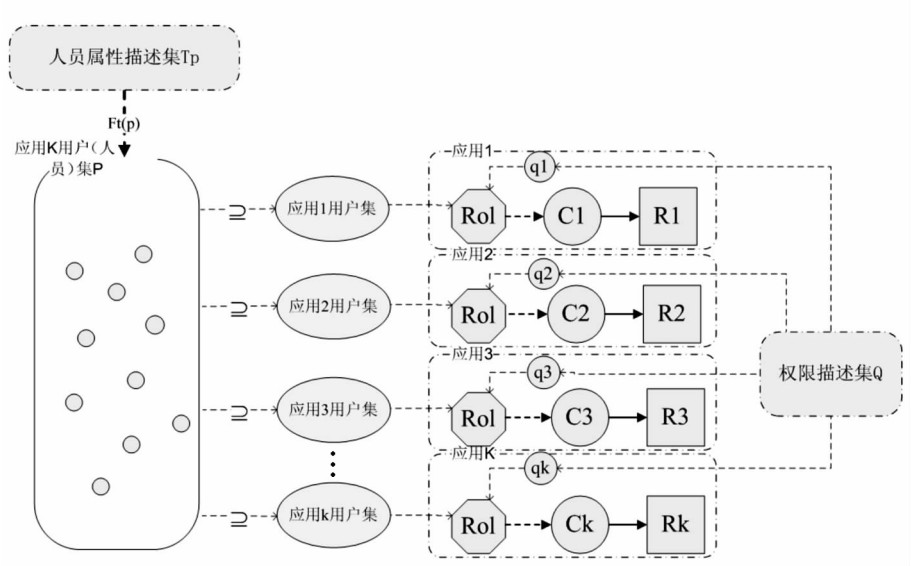

图 1 域概念模型

Fig. 1 Concept model of domain

从图中可以看出，一个域可有多个应用，一个应用可对应多个用户。假设一个域 yu 中有 k 个应用，域中每个应用 j 对应一个用户集 P_j，则该域中所有应用的用户集 $P = \bigcup_{j=1,\cdots,k} P_j$。

图 1 中，人员属性描述集 Tp、用户集 P 和映射集 $Ft(p)$ 构成该域中的人员及对应属性集 Pt，即 $Pt = (P, Tp, Ft(p))$。Tp 是该域中的人员属性集，该集合是有限集合，由独立属性 u 组成，即 $Tp = \bigcup_{j=1,\cdots,k} u_j$。其中，每个属性 u 都有自己的值域，比如性别属性的值域 $\mathrm{Domain}(u_{sex}) = \{male, female\}$。$Ft(p)$ 是一个映射，每个人员对应一组确定的属性表述值 $Ft(p) = (u_1: t_1, \cdots, u_n: t_n)$，其中，$u_i \in Tp$，$t_i$ 为 u_i 对应的值，$t_i \in \mathrm{Domain}(u_i)$。

假设一个域 yu 中有 k 个应用，每个应用记作 app_j，则该域的所有应用 $App_{yu} = \bigcup_{j=1,\cdots,k} app_j$。其中，每个应用 app_j 是一个 6 元组 (P'', R, C, Q, Rol, Fpr)。其中：

P''：人员子集，$P'' \subseteq P$；

R：资源集；

C：操作集，每个元素是对资源的一个操作；其中每个 $c \in C$，都存在一个资源集 $Rc \subseteq R$，是 c 可操作的最大资源范围，成为 c 的操作约束集；

Q 的每个元素为一个权限 q，权限 q 为一个二元组 (c, R')，其中 $c \subseteq C$，$R' \subseteq Rc$，表示每个操作子集 c 约束在一个可操作的资源子集 R' 上。一个权限可属于多个角色，一个角色可包括多个权限。

Rol：为角色集，其中每个元素是一个角色，每个角色为一个三元组 (C, R, Q)，C 为该应用的操作集，R 为该应用的资源集，Q 为该应用的权限集，每个权限 $q = (c, R') \in Q$，其中 $c \subseteq C$，$R' \subseteq Rc$；

Fpr：是一个映射，每个 $p \in P''$，存在至少一个 $rol \in Rol'$，$Rol' \subseteq Rol$，$Fpr(p) = Rol'$，即为一个人员分配一个或多个角色，使该人员具有一组权限。

1.2 单域数据模型

在一个域中，用户权限是在统一授权中心授予的。统一授权中心利用每个应用制定的规则集给对应应用的用户授予角色。用户访问应用系统时，通过访问控制节点验证用户拥有的角色是否有权限访问对应资源。单域的数据模型如图 2 所示。

图中，每个应用的用户集 P_j 是该域用户集 P 的一个子集，具有人员属性描述集 Tp 中的部分属性。每个应用利用用户属性等要素撰写授权规则，为用户授予具体角色。

用户访问某个特定应用的资源时，应用将通过其对应的应用代理检验用户是否有此权限。具体数据流为用户带着自己的角色向应用申请资源访问，应用代理解析用户角色是否拥有所申请的权限，若有，通过申请，否则拒绝申请。

1.3　多域模型

单个域构成的域集合称为 Yu,即 $Yu = \bigcup_{i=1,\cdots,k} yu_i$,其中 yu 表示一个域。多个单域连接起来,构成多域模型,即一个多域模型 PSOACS 是四元组 (P, Pt, App, Yu)。如图 3 所示。

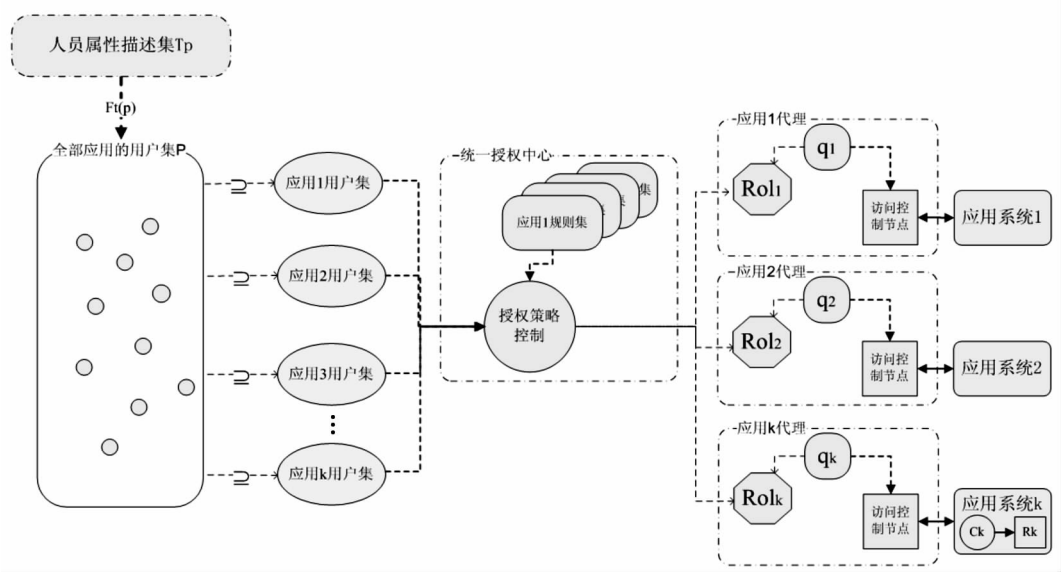

图 2　域数据模型

Fig. 2　Model of domain data

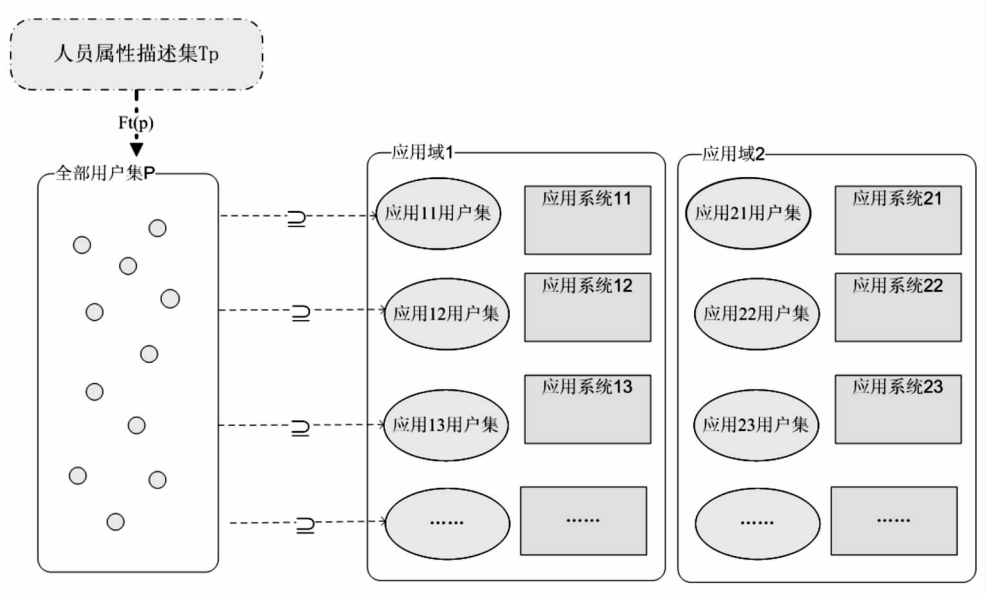

图 3　多域模型

Fig. 3　Model of multi-domian

假设一个多域模型 PSOACS 有 n 个域,每个域的用户集记作 P'_j,则 PSOACS 用户集 $P_{Yu} = \bigcup_{j=1,\cdots,n} P_j$,即,$Yu$ 中所有单域的人员集 P'_j 形成域集合的人员集 P 的一个划分;将每个域的应用集记作 App'_j,则 PSOACS 应用集 $App_{Yu} = \bigcup_{j=1,\cdots,n} App'_j$,即,$Yu$ 中所有单域的应用集 App'_j 形成应用集 App 的一个划分。

多域时通过单域的授权中心记录其他可信域,从而实现多域连接。多域授权机制是在单域基于规则的基础上实现的,其授权规则及其策略的表示请参看文献[6],在此不再赘述。

2　系统设计与实现

2.1　基本框架

根据单域数据模型,在一个域中需要建立一个授权管理中心,形成单一的访问入口,针对每个

应用建立一个对应的应用代理,形成如图 4 所示的单一访问控制中心面向多应用系统的统一授权与访问控制框架。授权中心收到用户请求后根据授权策略(规则)授予其用户相应的角色,通过属性证书方式传递给相应应用代理,该应用代理验证其操作是否允许所赋予的角色执行。

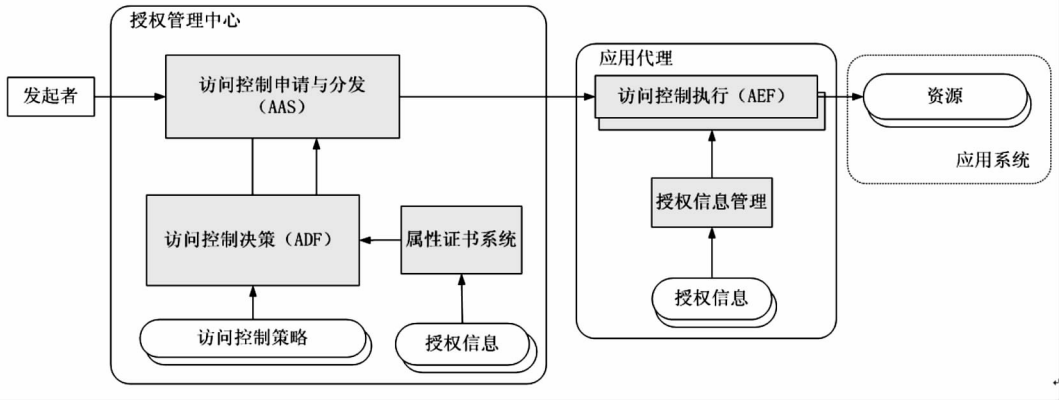

图 4 单域的授权与访问控制框架

Fig. 4 Framework of authorization and access control for single domain

2.2 跨域结构

实现跨域的核心,是在每个域的授权管理中心建立一个应用系统注册的目录体系,通过级联机制实现多域的连接,其结构如图 5 所示。

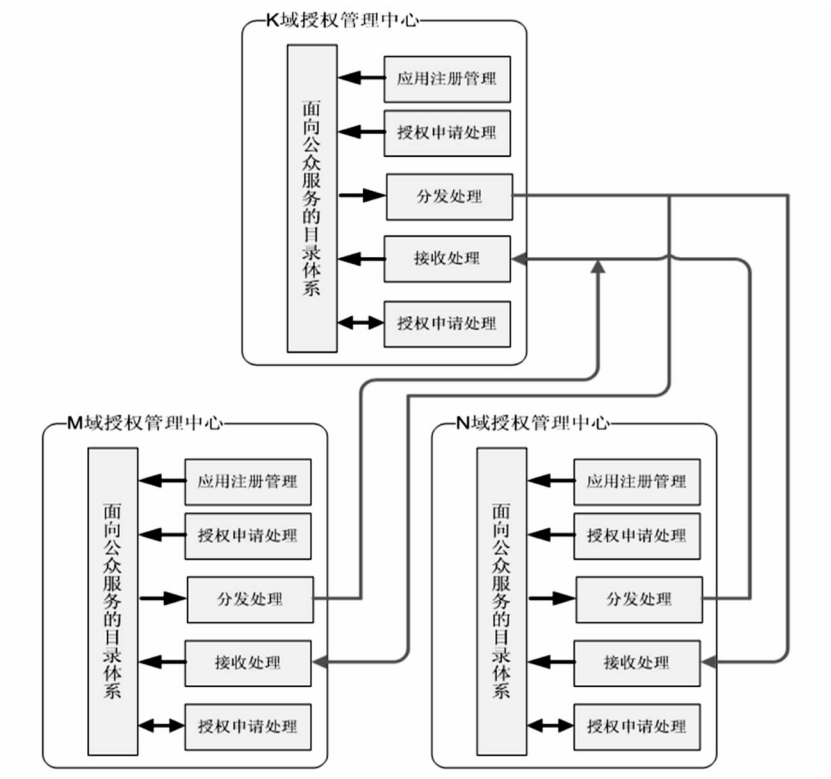

图 5 多域级联机制

Fig. 5 Mechanism of multi-domain cascade mechanism

当一个应用系统注册在其所在域的授权管理中心时,该授权管理中心通过级联机制自动分发给其它域的授权管理中心,记录在其目录体系中。当用户访问外域的应用系统时,用户所在域的授权管理中心通过其目录体系自动寻址到应用系统所在域的授权管理中心,实现其自动授权。

2.3 逻辑设计

根据多域的级联机制,每个域的授权管理中心和应用代理的逻辑设计结构如图 6 所示。

授权管理中心主要包括访问请求处理、访问控制决策与规则管理、授权信息管理、安全管理、信息转发与级联控制等功能。应用代理主要包括

权限验证与访问控制、安全管理等功能。其中,安全管理由各种保密机、加/解密/签名/验证算法、日志与审计等具体功能组成。

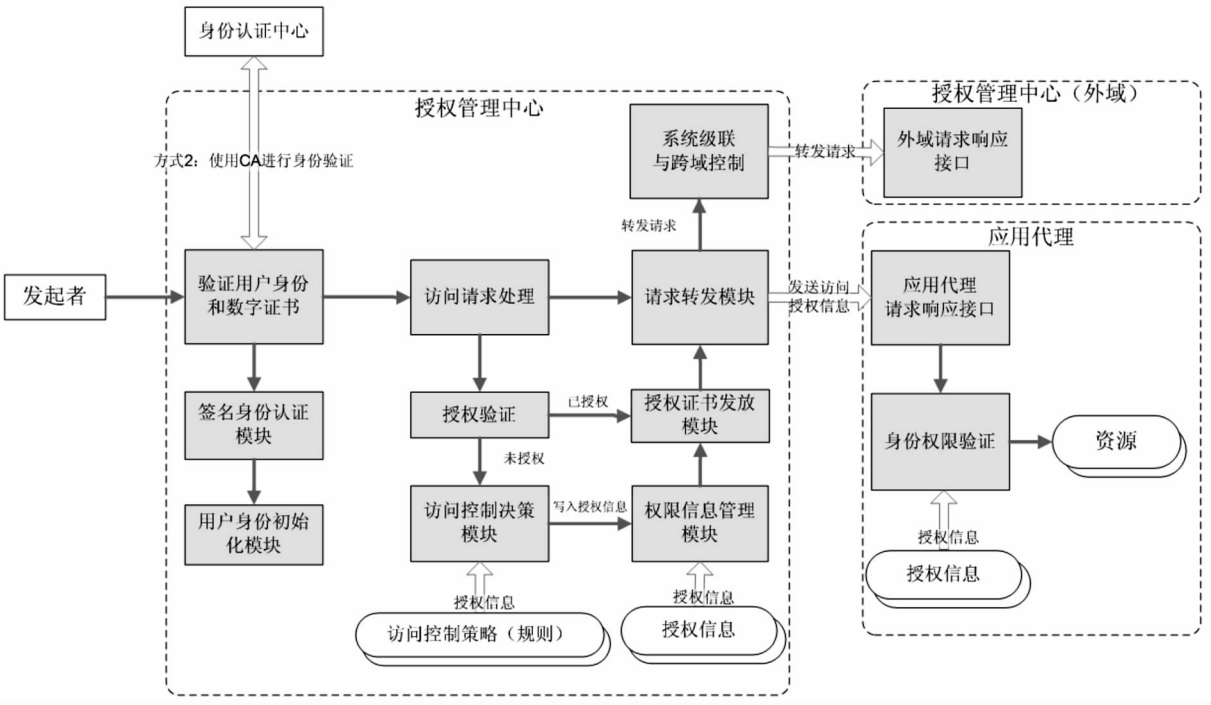

图 6　系统逻辑设计结构

Fig. 6　Architecture of logical system design

系统的处理流程为:用户通过授权管理中心统一登陆点登陆后,提交访问请求,系统验证身份后,首先检验用户是访问本域的应用系统还是外域应用系统,如是外域系统,则转发给指定外域的授权管理中心进行处理,如是本域,则检查其访问的应用系统是否已给其授权,如已授权,则提出授权信息,申请调用授权属性证书打包,发给应用系统代理,应用代理解析证书和授权信息,提交给应用系统资源控制,如未经授权,则调用访问控制决策模块,通过规则推理给其授权,并将授权信存入授权信息管理模块中。

3　结 论

本文在单域模型的基础上,针对面向多应用的大型服务域(地域广阔、多子域)软件服务集成需要,重点研究适应多域级联的跨域统一授权模型。该模型以单域自动授权为基础,利用授权中心建立跨域级联,构成授权网络,解决了多系统在授权部分的整合问题。本文同时介绍了基于这种模型的统一授权系统的实现。着重介绍了系统多级级联和跨域授权的机制和系统逻辑设计。该系统在实际中得到很好运用,证明了模型的合理性及系统实现的有效性。

参 考 文 献:

[1] Thomas R K, Sandhu R. Task-based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management [C]//Proceedings of the 11th IFIP WG11.3 on Database Security, Vancouver, Canada, 1997: 166 - 181.

[2] Oh S, Park S. Task-role-based Access Control Models [J]. Information Systems, 2003, 28(6): 533 - 562.

[3] Ferraiolo D, Sandhu R. Proposed NIST Standard for Role-based Access Control [J]. ACM Transactions on Information and System Security, 2001, 4(3): 224 - 274.

[4] 刘婷婷,汪惠芬,张优良. 支持授权的基于角色的访问控制模型及实现[J]. 计算机辅助设计与图形学学报, 2004, 16(4):414 - 419.

[5] 黄刚,王汝传. 基于 XACML 的网格访问控制研究[J]. 计算机系统应用,2007,16(8):48 - 51.

[6] 何长龙,李伟平,贺建忠,等. 基于策略的 RBAC 统一授权模型研究[J]. 信息安全与通信保密,2010,32(6).:221 - 227.