一种基于量化用户和服务的大规模网络访问控制方法

刘庆云[1),3),4),5)] 沙泓州[2),4)] 李世明[2),4)] 杨 嵘[3),4)]

[1)](中国科学院计算技术研究所 北京 100193)

[2)](北京邮电大学计算机学院 北京 100876)

[3)](中国科学院信息工程研究所 北京 100190)

[4)](信息内容安全技术国家工程实验室 北京 100190)

[5)](中国科学院大学 北京 100049)

摘 要 目前,传统的 RBAC(Role-Based Access Control)访问控制模型在支持细粒度服务和角色迁移的可控性上存在一定不足.针对这些不足,结合开放式网络环境的实际情况,文中提出了量化服务的概念,实现了一种基于细粒度角色和服务的访问控制机制,给出了一个形式化的基于量化服务和角色的访问控制模型 QSRBAC(Quantified Services and Roles Based Access Control).该模型提供了灵活的访问控制粒度,支持对角色和服务的多角度访问控制,支持权限动态调整和条件角色迁移,可以用于大规模开放式网络环境.经测试,在百万规模规则的情况下,基于该模型的访问控制系统内存占用 9.6GB 以下,平均规则执行时间 20μs 以内.实验结果证明,该模型可以满足访问控制的效果和时间要求,它的应用显著增强了访问控制过程的可管理性.

关键词 访问控制;量化角色;量化服务;细粒度;条件角色迁移;信息安全;网络安全

中图法分类号 TP309 **DOI 号** 10.3724/SP.J.1016.2014.01195

An Access Control Method Based on Quantified Services and Roles in Large Scale of Network Visits

LIU Qing-Yun[1),3),4),5)] SHA Hong-Zhou[2),4)] LI Shi-Ming[2),4)] YANG Rong[3),4)]

[1)](*Institute of Computing Technology, Chinese Academy of Sciences, Beijing* 100193)

[2)](*School of Computer Science and Technology, Beijing University of Posts and Telecommunications, Beijing* 100876)

[3)](*Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100190)

[4)](*National Engineering Laboratory for Information Security Technologies, Beijing* 100190)

[5)](*University of Chinese Academy of Sciences, Beijing* 100049)

Abstract Due to the shortage of existing RBAC (Role-Based Access Control) model in supporting the control of the role migration and fine-grained service, this paper proposes the concept of quantified service and realize a fine-grained access control mechanism based on the quantified roles and services. Combined with the actual situation of an open network environment, it puts forward the formal definition of QSRBAC (Quantified Services and Roles Based Access Control). The model provides a flexible access control granularity, supports the multi-angle access control for the roles as well as services, and supports the dynamic adjustment of rights and conditional role migration. Therefore, it can be used in the large-scale open network environment. Experiments show that when the scale of configuration is 1 million, the maximum amount of memory required by the access control system is below 9.6GB, while the average execution time is below

收稿日期:2013-04-15;最终修改稿收到日期:2013-12-30.本课题得到国家"八六三"高技术研究发展计划项目(2011AA010703)、中国科学院战略性先导科技专项(XDA06030200)和国家科技支撑计划(2012BAH46B02)资助.**刘庆云**,男,1980 年生,博士研究生,高级工程师,中国计算机学会(CCF)会员.主要研究兴趣为信息安全、网络安全.E-mail:liuqingyun@iie.ac.cn.**沙泓州**,男,1988 年生,博士研究生,主要研究方向为信息安全、网络内容安全等.**李世明**,男,1987 年生,硕士研究生,主要研究方向为信息安全、网络内容安全等.**杨 嵘**,男,1978 年生,硕士,工程师,主要研究方向为信息安全、网络安全.

20 microseconds. By this end, the model satisfies the effectiveness and delay requirements of access control. And this model significantly enhances the manageability of access control process.

Keywords access control; quantified role; quantified service; fine-grained; conditional role migration; information security; network security

1 引 言

近年来,随着互联网技术的迅猛发展,各种网络应用服务不断涌现,这些服务方便了人们的日常生活,提高了生产效率,但也带来了许多新的安全威胁,比如恶意软件入侵,网络带宽消耗,机密资料外泄等.而由于缺乏对网络应用的有效识别和控制能力,传统防火墙已远远不能满足用户对自身网络的安全管理需求.面对这一新的安全威胁和挑战,下一代防火墙技术应运而生.

2009 年,Gartner① 首先定义了下一代防火墙的概念.它将网络防火墙定义为在线安全控制措施,即可实时在各个受信网络间执行网络安全策略的部件.目前下一代防火墙的研究主要包括应用流量的识别和检测研究[1]、网络访问控制策略研究[2]和面向攻击的入侵防御技术研究[3].其中,访问控制策略的研究依然是防火墙领域最为核心的问题.

在下一代网络防火墙中,如何在用户和服务之间建立对应的访问控制机制并进行合理可靠的授权是安全的关键,国内外很多学者对这一问题进行了深入的研究[4-6].这些研究按照访问控制模型的不同分为两类:(1)基于信任度的访问控制模型[4].信任度是指一个实体对另一个实体的信任程度.此类模型往往通过描述不同实体间信任程度的差别进行访问控制;(2)基于用户-角色映射关系的访问控制机制[5].角色是特定访问权限的集合.此类模型往往通过将用户映射到角色从而进行访问控制.在这两类模型中,前者主要用于在自治域间协同结构松散的情况;而后者主要用于自治域间相互熟悉,存在依赖或信任关系的情况,并且因为实用性强而受到广泛关注.在基于映射的研究中,蔡伟鸿等人[6]综合前人的工作,引入了"可度量角色"的概念,提出了支持细粒度的委托授权模型.这一模型对基于角色的访问控制研究具有重要的理论价值.

然而,由于网络行为逐步呈现出规模大、高并发及"服务-角色"授权关系复杂等特点,传统的基于角色或权限映射的授权关系已经暴露出了可扩展性差,可复用性低等弱点.例如,在蔡伟鸿等人的研究中,只讨论了角色的授权问题,而忽视了角色所访问的服务属性和服务的优先级问题.举例来说,在一个网络防火墙内,角色 A、B 都可能通过 80 端口访问即时通信和网页邮箱两个服务.在访问控制和委托授权模型中,A 应当被禁止访问即时通信服务,而 B 的网页邮箱服务属于关键服务,应该优先保证.而根据现有授权模型,无法判断应该如何给 A、B 授权访问 80 端口.由此可见,忽视服务属性及服务的优先级可能导致实际应用时发生授权角色访问非法服务或者关键服务因带宽有限而被拒绝访问等问题,降低控制的有效性和灵活性.

本文在蔡伟鸿等人的研究基础上重点讨论了服务和用户的属性,从研究大规模网络行为的角度出发,提出了一个基于量化服务和角色的访问控制模型 QSRBAC(Quantified Services and Roles Based Access Control).该模型研究网络行为到"角色-服务"的映射关系,在分析服务和用户属性的基础上提出了可量化服务和角色的概念.通过对服务和角色的量化,使得访问控制具有足够的可扩展性和灵活性.同时,本文在 QSRBAC 模型的基础上,依据量化用户和服务的思想,提出了一种细粒度的大规模网络访问控制方法.该方法通过动态评估服务和用户的属性,进而调整用户的角色,使其访问权限发生变化,以支持权限的动态迁移.上述方法的特点在于对服务和用户提供了具体的量化方法,并能够保证其属性可以进行动态变更,从而使其能够适应开放式的网络环境.实验证明,该方法相比传统方法具有更高的鲁棒性和实用价值.

本文第 2 节介绍相关研究工作;第 3 节给出 QSRBAC 模型;第 4 节给出原型系统的实现和评价;第 5 节总结全文并讨论进一步的研究方向.

2 相关工作

在信息安全领域的研究中,访问控制技术作为

① http://www.gartner.com/

一种关键技术而受到研究人员的广泛关注[7]. 通过监控用户访问资源的过程，人们应用该技术以保证在合法时间内，合法用户可以获得足够和有效的系统访问权限[8]. 现有的访问控制模型包括但不限于强制访问控制模型，自主访问控制模型，基于任务、角色和信任度的访问控制模型.

早在 20 世纪 70 年代，访问控制技术就已经出现并获得重视. 那时，访问控制技术常常被用于保护大型计算机系统的数据集[9]. 基于这一安全需求，研究人员先后提出了自主访问控制模型(Discretionary Access Control，DAC)以及强制访问控制模型(Mandatory Access Control，MAC). 其中，DAC 模型曾被广泛应用于操作系统以及数据库中[10]. 然而，DAC 模型的缺陷也十分明显. 在这一模型中，用户的访问权限通常具有可传递性，而权限的传递过程往往是不可控的. 与此不同的是，MAC 模型有效提高了信息的机密性，但没有考虑对信息完整性的验证和控制问题.

随着网络信息系统的发展和进步，在访问过程中，信息完整性以及权限控制的问题日益严重. 此外，网络信息系统日益开放，导致用户数目不断增多且变动频繁，对授权管理的可扩展性提出了更高的要求. 在上述安全需求背景下，Ferraiolo 和 Kuhn 提出了 RBAC(Role Based Access Control)模型[11]. RBAC 模型的优势在于，它依据对工作职务的描述简化了授权管理过程，从而显著提高了这一访问控制模型的可扩展性. 在 RBAC 模型中，用户和角色间存在多对多的映射关系，用户通过角色可以获取访问特定系统资源的权限. 通过定义不同类型的角色，角色间的继承和包含关系以及限制条件，RBAC 模型可以更准确地规范用户行为. 基于该模型的思想，先后出现了 RBAC96[12]、ARBAC97[13]、ARBAC99[14]、ARBAC02[15] 和 NIST RBAC[16] 等. 这些模型从系统的角度出发，侧重于资源的保护，但不支持资源的动态授权.

随着分布式计算的发展，任务的组织进一步自动化，人们希望在任务的执行过程中可以动态授权，从而对访问控制技术提出了新的需求. Thomas 等人[17]从“面向任务”的角度出发，提出了基于任务的授权控制模型(Task-Based Authorization Control，TBAC)，并建立了相应的安全机制. TBAC 模型的最大特点是它可以对不同任务流以及同一任务流中的不同子任务提供不同的访问控制策略. 这一特点使它能够满足工作流及分布式网络环境的要求. 黄勤等人[18]提出了基于任务状态的转授权模型，邢光林等人[19]提出了基于角色和任务的工作流授权模型并给出了相应的约束条件.

此外，针对基于角色访问控制的动态性和监管性的不足，Chakraborty 等人[20]提出了基于信任的访问控制模型. 该模型符合开放式的网络环境特点，但是在信任度的计算上存在不足. 赵庆松等人[21]和孙波等人[22]等人从分布式转授权的角度提出了基于角色的转授权模型，较好地解决了权限传播的问题.

上述研究工作主要集中在对访问主体的层次结构，操作方式以及计算环境的异构性进行分析，而忽视了访问客体(包括资源和服务)的结构特点和动态特性. 随着大量新型应用和服务通过少数端口和采用少数网络协议进行通信，访问控制机制中客体的层次和特点发生了变化. 这种变化要求访问控制技术能够依据服务、角色及其相关环境的特点制定相应的访问控制策略. 为了满足上述要求，许峰等人[7]首次将服务的概念引入传统的访问控制方法，提出了一种基于服务依赖关系的访问控制技术，但没有考虑服务的细粒度访问控制和量化问题.

例如，在图 1 中，假设用户 John 当前获得的服务为 $S1$，$S2$. 那么当服务动态调整时，如新增服务 $S3$ 时，传统的 RBAC 系统需要增加服务 $S3$ 及与其相关的访问控制策略. 而 QSRBAC 系统可以以服务属性为基础进行细粒度的服务访问控制，并可以通过给不同属性赋予不同权值，达到量化服务的目的，并建立任务执行过程的安全控制机制.

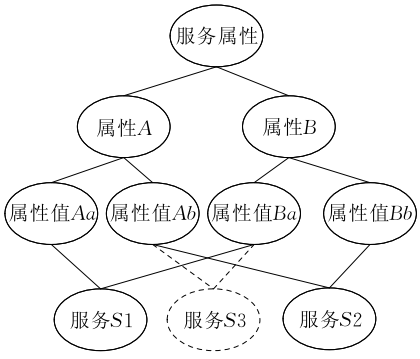


图 1　服务属性层次结构示例

在前人的工作基础上，我们对服务的概念进行了延伸和扩展，提出了基于量化服务和角色的访问控制模型 QSRBAC. 同传统的访问控制模型比较，它的优点在于：

(1)通过对用户和服务的量化，进一步简化了对访问控制对象的管理. 该模型能够依据量化结果

对服务进行动态授权，从而较好地适应动态变化的复杂网络环境.

(2)提出了一种基于映射机制的动态访问控制方法.该方法能够适应开放式的网络环境的要求，并支持细粒度的访问控制.

3 基于量化服务和角色的访问控制模型(QSRBAC)

在传统的 RBAC 模型中，系统提供的用户、角色、资源、服务以及它们间的映射关系相对固定.在开放式的网络环境中，随着用户、服务和资源不受限制地接入网络，映射关系动态变化，原有假设不再成立.为此，我们提出 QSRBAC 模型，以适应网络环境的开放性和“角色-服务”映射关系的动态变化.

3.1 QSRBAC 的基本概念

与传统 RBAC 模型不同，QSRBAC 模型提出了量化用户和服务的概念，以实现开放式环境中访问控制对象的动态管理.

在给出 QSRBAC 模型的定义之前，我们先给出如下定义.

定义 1. 可量化用户.系统中用户的集合 U.

$U=\{user_1, user_2, \cdots, user_n\}$. 其中，$user_i=\{uid_i, uattr_{i1}, uattr_{i2}, \cdots, uattr_{in}\}$用户 $user_i$ 指一个可以独立访问网络服务的主体，是由用户 uid 和一组用户属性 $uattr$ 构成.

定义 2. 角色.系统设置的角色集合 R.

$R=\{role_1, role_2, \cdots, role_n\}$，在本模型中，角色是指用户在一个系统中拥有的身份或所属组别.通常由用户的角色决定其对系统中部分资源进行操作的权力或者资格.

定义 3. 可量化服务.系统为用户提供的服务集合 S.

$S=\{service_1, service_2, \cdots, service_n\}$. 其中，$service_i=\{sid_i, sattr_{i1}, sattr_{i2}, \cdots, sattr_{in}\}$ 服务 service 是由服务 sid 和一组服务属性 $sattr$ 标识构成.

定义 4. 属性.属性 $Attr$ 是指实体在某一方面的特点，特征和特质.在本模型中，它包括用户属性 $uattr$ 和服务属性 $sattr$ 两类.

定义 5. 操作.用户对服务可以执行的操作集合 $OPT=\{opt_1, opt_2, \cdots, opt_n\}$.

定义 6. 条件.用户对服务可以执行操作时需要达到的要求 $Condition$.在本模型中，条件是指用户为了获得指定权限应当满足的要求.它包括时间触发条件、授权次数条件等.

定义 7. 权限.权限是对系统所提供的服务进行访问的许可.在本模型中，权限的形式化定义为 $Permission=(opt, service, condition)$，其中，服务 $service$ 是访问控制的客体，操作 opt 是访问服务采取的方式，$condition$ 是角色被允许执行该操作时应当满足的阈值要求.

定义 8. 会话.会话集合 $SESSION$.会话是指用户和他所激活的角色之间的映射关系.

3.2 用户量化模型

用户可量化是指可以通过用户属性 $uattr$ 的计算结果来衡量该用户所属的角色.用户属性(例如，“地域”、“年龄”和“性别”)从不同维度刻画了用户具有的特征.根据访问控制目的的不同，选择的用户属性也不完全相同.本文以“地域”、“年龄”和“性别”等属性为例，说明用户的角色量化过程.而其量化结果决定了该用户的角色分配情况，进而影响该用户的访问权限.图 2 所示为本文提出的用户量化模型的结构.

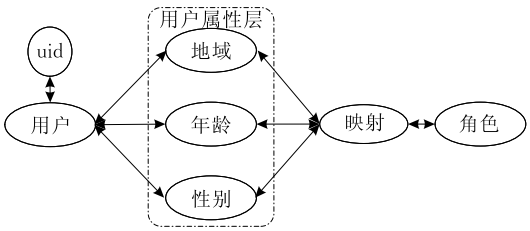


图 2 用户量化模型结构

3.3 服务量化模型

服务可量化是指可以通过服务属性 $sattr$ 的计算来衡量该服务的授权访问范围.服务的量化结果决定了服务的角色分配情况.这样用户对服务的访问不仅取决于用户所属角色，而且取决于该服务所具有的属性.本文提出的服务量化模型的结构如图 3.

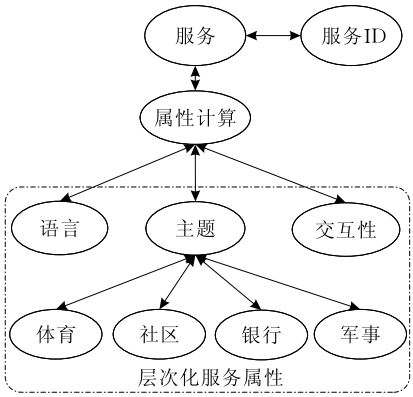


图 3 服务量化模型结构

该模型包括服务、服务 ID、属性计算及层次化服务属性. 其中层次化服务属性是由属性(例如，语言、主题、交互性等)和属性域(例如，体育、社区、银行、军事等)等构成.

定义 9.　量化服务的权限. $QSA=\{(s,k)\mid s\in S\wedge 0<k\leq total(sattr)\}$ 是全部量化服务的权限集合. 其中，$total(attr:Attr)\rightarrow N$ 是服务的属性总量函数，k 是该量化服务所包含的属性量值.

$kserv((s,k):QSA)\rightarrow 2^N$，该函数将 (s,k) 映射到其量值集.

$qrpsrc(qs:QSA)\rightarrow 2^{SA\cup PA}$，该函数将量化服务映射为其权限.

定义 10.　量化服务上的权限关系＝和≥.

$$(s,k)=(s',k')\Leftrightarrow\begin{cases}s=s',\\ kserv(s,k)=kserv(s',k')\end{cases}$$

$$(s,k)\geq(s',k')\Leftrightarrow\begin{cases}kserv(s,k)\supseteq kserv(s',k'),\ s=s'\\ \exists x:SERVICES\cdot(s,x)\in qrpsrc(s,k)\wedge x\geq s',\ s\neq s'\end{cases}$$

如果 $(s,k)\geq(s',k')$，一个被明确授权访问 (s,k) 的用户可以访问 (s',k').

定理 1.　量化服务上的≥关系是偏序关系.

证明.　由偏序关系的概念可知，只需证明≥是自反的、反对称的和传递的.

自反性：根据定义，$(s,k)\geq(s,k)$ 是显然的.

反对称性：

$$(s,k)\geq(s',k')\Leftrightarrow$$

$$\begin{cases}kserv(s,k)\supseteq kserv(s',k'),\ s=s' & (1)\\ \exists x:SERVICES\cdot(s,x)\in qrpsrc(s,k)\wedge\\ \quad x\geq s',\ s\neq s' & (2)\end{cases}$$

$$(s',k')\geq(s,k)\Leftrightarrow$$

$$\begin{cases}kserv(s',k')\supseteq kserv(s,k),\ s'=s & (3)\\ \exists x':SERVICES\cdot(s',x')\in qrpsrc(s',k')\wedge\\ \quad x'\geq s,\ s'\neq s & (4)\end{cases}$$

若式(1)、(3)成立，则有 $(s,k)=(s',k')$.

若式(2)、(4)成立，根据式(2)，$s\geq x\geq s'$ 并且 $s\neq s'$，则 $s>s'$.

根据式(4)，$s'\geq x\geq s$ 并且 $s\neq s'$，则 $s'>s$. 产生矛盾，所以式(2)和式(4)不可能同时成立. 显然式(1)、(4)不可能同时成立，式(2)、(3)不可能同时成立.

依据上述证明，

$$(s,k)\geq(s',k')\wedge(s',k')\geq(s,k)\Rightarrow(s,k)=(s',k').$$

传递性：

$$(s,k)\geq(s',k')\Leftrightarrow$$

$$\begin{cases}kserv(s,k)\supseteq kserv(s',k'),\ s=s' & (5)\\ \exists y:SERVICES\cdot(s,y)\in qrpsrc(s,k)\wedge\\ \quad y\geq s',\ s\neq s' & (6)\end{cases}$$

$$(s',k')\geq(s'',k'')\Leftrightarrow$$

$$\begin{cases}kserv(s',k')\supseteq kserv(s'',k''),\ s'=s'' & (7)\\ \exists y':SERVICES\cdot(s',y')\in qrpsrc(s'',k'')\wedge\\ \quad y'\geq s'',\ s'\neq s'' & (8)\end{cases}$$

根据式(5)、(7)，当 $s=s''$ 时，$kserv(s,k)\supseteq kserv(s'',k'')$.

根据式(6)、(8)，则有 $s>s'>s''$，

$\exists z:SERVICES\cdot(s,z)\in qrpsrc(s,k)\wedge z\geq s'',s\neq s''$.

综上可知，$(s,k)\geq(s'',k'')$. 从而证明该式是可传递的.　　证毕.

量化服务在服务关系＝和≥下形成了服务的层次结构. 该层次结构依赖于服务的属性关系和属性值. 量化服务是对 RBAC 模型中服务结构的扩展，可以表示其任意部分. 适用量化服务作为服务对象提供了灵活的访问控制粒度，同时避免引入过高的管理和维护代价.

3.4　QSRBAC 模型

QSRBAC 模型从服务和用户的量化出发，是传统 RBAC 模型的一种扩展形式. 它包括基于量化服务的访问控制视图和基于量化角色的访问控制视图两个部分. 本文提出的 QSRBAC 模型结构如图 4.

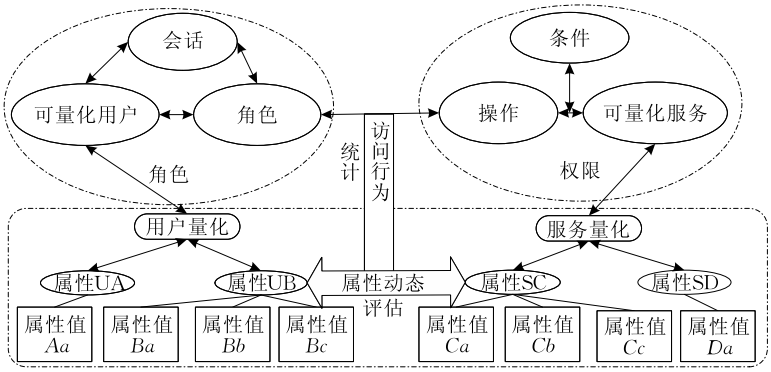


图 4　QSRBAC 模型结构

定义 11. QSRBAC 模型. QSRBAC=$\{U,R,S,Attr,OPT,Condition,Permission,SESSION\}$，其中，$U$ 是用户集，R 是角色集合，S 是服务集合，$Attr$ 是属性集合，OPT 是操作集合，$Condition$ 是条件集合，$SESSION$ 是会话集合，$Permission$ 是权限集合.

定义下列关系：

(1)用户分配关系(User Assignment)是一种从用户到角色的多对多映射关系，记为 UA，$UA\subseteq U\times R$.

(2)权限分配关系(Permission Assignment)是一种从访问权限到角色的多对多的映射关系，记为 PA，$PA\subseteq R\times P$；

$P_{assigned}(r:R)\rightarrow 2^P$，表示一个将角色映射到其分配的权限的函数，

$$P_{assigned}(r)=\{p\in P\mid (p,r)\in PA\}.$$

(3)用户-属性映射关系(User Attribute Map)是从属性到用户的多对多的映射关系，记为 UAM，$UAM\subseteq U\times Attr$；

$own_{uattr}(u:U)\rightarrow 2^{Attr}$ 表示一个将用户映射到其拥有的属性的函数，

$$own_{uattr}(u)=\{attr\in Attr\mid (u,attr)\in UAM\}.$$

(4)服务-属性映射关系(Service Attribute Map)是从属性到服务的多对多的映射关系，记为 SAM，$SAM\subseteq S\times Attr$；

$own_{sattr}(s:S)\rightarrow 2^{Attr}$ 表示一个将服务映射到其拥有的属性的函数，

$$own_{sattr}(s)=\{attr\in Attr\mid (s,attr)\in SAM\}.$$

(5)条件角色迁移(Conditional Role Transition)，是指用户在执行授权的过程中，根据触发条件而产生的用户属性变化，致使其所属角色发生变化的过程. 系统根据用户当前的状态统计和触发条件，动态调整用户所属的角色. 条件角色迁移是访问行为统计和属性动态评估的结果.

(6)动态授权关系(Dynamic Access)，是指在授权过程中依据授权迁移状态和角色拥有的访问权限，访问控制系统可以动态地决定角色的实际执行权限. 其中，判定角色的当前授权迁移状态 $state_{(r,t)}$ 采用以时间为自变量的决策函数 PD，$state_{(r,t)}=PD(t,state_{(r,t-1)})$.

定义 12. 量化用户信任度. 设 $\Gamma_u(uattr,t)$ 表示访问控制系统对量化用户 u 的信任评价，称为量化用户信任度. 令 $\Gamma_u(uattr,t)=\sum_{i=1}^{n}m_iY_i(uattr_i)$，其中 $uattr$ 是用户属性集合，$Y_i(uattr_i)$ 是第 i 个用户属性值，m_i 是第 i 个用户属性的重要程度，t 是时间戳. 为了提高信任度评估的准确性，把一段时间分为若干个时间戳，时间戳反映了某一个时刻量化用户 u 的信任度，信任度随时间的变化而变化. 量化用户的信任度是属性计算的结果，也是用户权限分配的依据. 一般情况下，信任度越高的用户，其获得的访问权限也越高.

定义 13. 量化服务信任度. 设 $\gamma_s(sattr,condition)$ 表示访问控制系统对量化服务 s 的信任评价，称为量化服务信任度，令 $\gamma_s(sattr,condition)=\sum_{i=1}^{n}m_iY_i(sattr_i)$，其中 $sattr$ 是服务属性集合，$Y_i(sattr_i)$ 是第 i 个服务属性值，m_i 是第 i 个服务属性的重要性程度，$condition$ 是触发条件. 服务的信任度是属性计算的结果，是权限分配的依据.

定义 14. 总体信任度. 设 $\varpi(uattr,sattr,t,condition)$ 表示用户和服务的总体信任评价，称为总体信任度. 令 $\varpi(uattr,sattr,t,condition)=\Gamma_u\otimes\gamma_s$，$\otimes$ 表示矩阵的乘积. 总体信任度的高低是此次访问是否会获得授权的重要判断标准.

定义 15. 用户服务授权. 设授权可分为 P 个决策 $S=\{s_1,s_2,\cdots,s_p\}$，信任空间记作 C，表示为 $C=\{c_1,c_2,\cdots,c_p\}$. 信任空间 C 具有如下性质：$c_i\cap c_j=\varnothing(i\neq j)$ 且 $c_1<c_2<\cdots<c_p$，即 c_{k+1} 比 c_k 大. 则 C 是一个有序分割类，S 和用户信任度及服务信任度之间的映射函数 Ψ，称为用户服务授权. 它可以表示为

$$\Psi(\Gamma_u\otimes\gamma_s)=\begin{cases}s_p, & c_p\leq\Gamma_u\otimes\gamma_s\leq 1\\ \cdots & \\ s_k, & c_{k-1}\leq\Gamma_u\otimes\gamma_s\leq c_k\\ \cdots & \\ s_1, & 0\leq\Gamma_u(uattr,t)\times\gamma_s(sattr,condition)\leq c_1\end{cases}.$$

当用户 u 向访问控制系统请求服务时，首先要根据量化用户 u 的信任度 $\Gamma_u(uattr,t)$ 决定它能得到的服务可信度区间. 这样既可以分级对不同用户提供不同信任度的服务，也有利于使用服务量化的结果对服务作细粒度访问控制.

综上所述，QSRBAC 模型的访问策略是由角色、服务、触发条件共同确定的. 而上述部件之间的

关系则由系统管理员统一配置决定.

3.5 访问控制策略分析

作为一种动态访问控制模型，QSRBAC 模型可以随时间和上下文的变化而变化. 在这一模型中，角色获得服务访问权限的过程也是动态交互的. 访问控制系统依据当前的限制条件和授权结构体的状态进行综合判断，从而确定是否允许角色对服务的这一访问.

在 QSRBAC 模型中，用户获得系统访问授权的途径有 3 种：权限分配、条件角色迁移以及动态权限调整.

(1) 权限分配

权限分配过程是指将角色和对应的访问权限分配给用户的过程. 这一过程包含角色分配和访问权限分配两个操作. 其中，角色分配用二元组〈u，r〉来表示，记作 $ua(u,r)$，角色 r 所包含用户的集合记为 $UA(r)$.

$$UA(r)=\{ua(u_i,r)\mid ua(u_i,r)\in UA, i=1,2,\cdots,n\}.$$

而系统中中角色的访问权限主要表现为访问服务的能力，进而权限的分配关系 PA(Permission Assignment)可以用二元组〈r，s〉来表示，记为 $pa(r,s)$. 类似地，如果角色被授予一组权限，则记为 $PA(r)$.

$$PA(r)=\{pa(u_i,r)\mid pa(u_i,r)\in PA, i=1,2,\cdots,n\}.$$

(2) 条件角色迁移

当用户被分配角色以后，系统依据权限分配结果给该用户分配权限. 当他的状态统计结果满足系统触发条件时，其用户属性发生改变，用户所属角色发生迁移. 条件角色迁移过程包括用户属性变更和角色迁移两个步骤. 当用户属性 $attr(u)$ 变更后，触发用户所属的角色 $Role(u)$ 的重新计算. 其中，$Role(u)=func(attr(u))$.

(3) 动态权限调整

在 QSRBAC 模型中，其基本的授权结构体 $AU=\{User,Role,LF\}$，其中 LF 表示该授权结构体的生命周期. 当授权结构体被触发时，它的生命周期开始进入倒计时，在 AU 的整个生命周期中授权始终有效. 但当授权超过生命周期时，系统则认为该授权结构体的授权无效.

3.6 QSRBAC 模型的访问控制算法

在 QSRBAC 模型的基础上，将量化服务的计算过程引入访问控制模型中. 在某一个应用系统内，用户 *user* 访问服务 *service* 的授权结果 *Auth*(*user*，*service*)是通过算法 1 获得. 在算法 1 中，用 *stream* 表示流量(流量中包含用户 *user*，服务 *service*)，*policy* 表示策略，*uid* 和 *sid* 分别表示用户和服务的身份信息，*uattr* 和 *sattr* 分别表示用户和服务的属性信息，*cache* 表示缓存信息，*server* 是服务器，用于保存用户和服务的信息库.

算法 1. 基于量化服务和角色的访问控制算法.

输入：*stream*，*policy*

输出：*Auth*

```
1.  function AccCon(stream,policy)
2.    Auth←∅;
3.    uid←f_extractu(stream);
4.    sid←f_extracts(stream);
5.    uattr=FINDATTR(cache,server_u,uid);
6.    sattr=FINDATTR(cache,server_s,sid);
7.    Auth=Inquire(uattr,sattr,policy);
8.    return Auth
9.  end function
10. function FINDATTR (cache,server,id)
11.   i←0;
12.   attr←∅;
13.   block←sizeof(AttrSet);
14.   while i<cache/block do
15.     if attr=∅ then
16.       attr=lookup(block[i],id);
17.       break;
18.     end if
19.     i++;
20.   end while
21.   if attr=NULL then
22.     attr=lookup(server,id);
23.   end if
24.   return attr
25. end function
```

函数 *AccCon* 通过对 *stream* 和 *policy* 进行分析，判断当前流是否需要采取何种控制措施. 在这个函数中，有 3 个子函数. 其中，$f_{extract}$ 是通过对 *stream* 的信息进行分析，解析出用户和服务的 *id* 信息. *FINDATTR* 函数根据用户和服务的 *id* 信息与 *cache* 和 *server* 中保存的信息进行比较，输出查询到的属性信息 *attr*. *Inquire* 函数，依据服务和用户的属性信息 *attr* 以及系统策略 *policy* 查询策略，判断应当采取的控制措施. 此外，*lookup* 函数通过对缓存指定块 *block* 或服务器 *server* 进行查询，返回用户或服务的属性值 *attr*.

3.7 QSRBAC 模型的优点

同传统的 RBAC 模型进行比较，QSRBAC 模型

具有下述优势：

(1)支持权限动态调整

传统的 RBAC 模型以静态分配为主，并不涉及权限的动态调整.通过引入授权结构体及它的生命周期，QSRBAC 模型支持权限的动态调整，符合连续变化的网络环境的要求.

在 QSRBAC 模型中，系统对用户的状态进行统计，结合触发条件将统计结果反映在用户的属性变更上.通过重新计算用户的属性，系统可以将新的角色及其访问权限分配给用户，从而达到用户的条件角色迁移.通过这样的设计，QSRBAC 模型能够更好地适应开放式的环境.特别地，当用户属性不明确时，系统无需为用户创建临时角色，通过访问结果的统计即能达到分配角色和访问控制的目的.

(2)支持服务动态扩展和更新

通过引入服务属性和可量化服务的概念，QSRBAC 模型可以方便地对服务的种类和数目进行扩展和更新.对比 RBAC 模型，引入属性的概念对角色和服务进行统一量化和封装，可以使开放式网络环境中服务的可扩展性更强，同时该模型提供了更加方便的安全管理方式.

(3)提供粒度可控的访问控制关系管理

对服务属性的多层次划分使得 QSRBAC 模型对服务和用户的细粒度访问权限控制成为现实.

此外，由于采用层次化的服务属性，服务的访问控制粒度的大小可以由安全人员自行控制，以应对不同的访问控制需求.

3.8 QSRBAC 模型的应用场景

随着网络环境的日益开放，一方面，各种网络应用和服务层出不穷；另一方面，大量用户动态地接入网络.因此，人们对访问控制的可扩展性和安全性提出了更高要求.这恰恰是传统的基于角色的访问控制技术所不能满足的.而 QSRBAC 模型适用于面向开放性网络服务的系统，尤其适合于复杂授权关系下的大规模访问控制系统.

3.9 访问控制性能分析

在传统的 DAC、MAC、RBAC 和 TBAC 模型中，某一类服务(资源)S_r往往作为一个整体参与访问权限控制，即一旦将 S_r的权限赋予某一角色，该角色将获得 S_r中所有服务的访问权限.在开放式的网络环境中，这种机制违背了“最小特权”原则.在表 1 中，给出了QSRBAC与传统模型在访问控制性能方面的对比.从表 1 中可知，相比于其他传统模型仅支持授权主体(即用户)的访问控制粒度，QSRBAC 还支持授权客体(即服务或资源)的访问控制粒度和层次性，因而能很好地满足用户在细粒度访问控制方面的需求.此外，通过在角色信任度的量化过程中引入时间戳的概念，模型的可管理性和可控性得到了进一步提升.

表 1 QSRBAC 与 DAC、MAC、RBAC 和 TBAC 的性能对比

模型	角色粒度		服务粒度		服务授权层次	临时性限制	
	整体	部分	整体	部分	层次化	次数	周期性
QSRBAC	√	√	√	√	√	√	√
DAC	√	×	√	×	×	×	×
MAC	√	×	√	×	×	×	×
RBAC	√	×	√	×	×	×	×
TBAC	√	√	√	×	×	√	√

4 模型的应用

4.1 原型系统的实现

目前，QSRBAC 模型已经在开发的一个基于用户和服务的网络防火墙系统中得到了应用.在该系统中主要类别的服务数如表 2.

表 2 预置的服务分类情况

类别总数/类	覆盖总数/条	主要类别			
		体育类	社区类	军事类	银行类
43	50286	567	41339	128	305

从表 2 可以看出，系统目前能够预设了 43 类服务，覆盖了超过 5 万个常用服务.

4.2 原型系统的评价

本文分别从系统的覆盖能力，准确性和系统的处理性能对这个原型系统进行测试和评价.

该访问控制系统对网址的识别覆盖率和划分准确率的测试.识别覆盖率是指系统识别的 URL 数目占输入 URL 的百分比，划分准确率是指系统正确识别的 URL 数目占所有识别 URL 数目的百分比.首先，本文采集了著名的导航网站 hao123 的网站分类结果(30 个类别，共 1776 个 URL)作为标注样本集.然后，取出其中四个典型类别，将服务分类结果同系统服务的量化结果作比较，其结果如表 3 所示.由表 3 可知，在最坏情况下，识别覆盖率能够达到 91.6%，划分准确率达到 84.6%，符合大多数系统的访问控制要求.

表 3　服务识别与划分

类别	识别覆盖率/%	划分准确率/%	测试 URL 数目
体育	100.0	85.7	21
社区	**91.6**	90.4	273
军事	100.0	93.7	32
银行	92.8	**84.6**	70

性能测试，实验环境为 8 核主频为 2.13GHz 内存大小为 16 GB 的服务器. 下列实验主要测试了在不同规模的访问控制规则和复杂规则占比不同的情况下执行规则的时间和内存使用情况. 这里的规则主要包括访问者、访问资源、条件和控制策略（例如通过、阻止）等 4 部分. 由于复杂规则在精细化控制过程中经常使用，具有很强的现实意义. 所以在实验过程中，引入复杂规则的概念. 在实验中假设访问控制系统中只有复杂规则和简单规则两种. 在实验中设计的复杂规则所涉及区域是简单规则的 6 倍，用 p 表示复杂规则数占规则总数的比例.

下面从时间和内存使用量两个角度来考察系统在不同规则规模情况下的性能，实验效果如图 5、图 6 所示. 图 5 表示了不同规模和复杂规则比例情况下执行规则所需的时间变化情况. 为了全面检查系统性能，对每种情况独立运行 10 000 次，以统计执行时间的分布情况. 由图 5 可知，当规则规模小于 300 万条的情况时，执行规则的时间一般在 20 μs 以下，且不随时间线性增长. 系统执行规则时间的分布随复杂规则比例的增加而变得稀疏，复杂规则比例越大，执行时间越长. 但系统的平均执行时间基本不变.

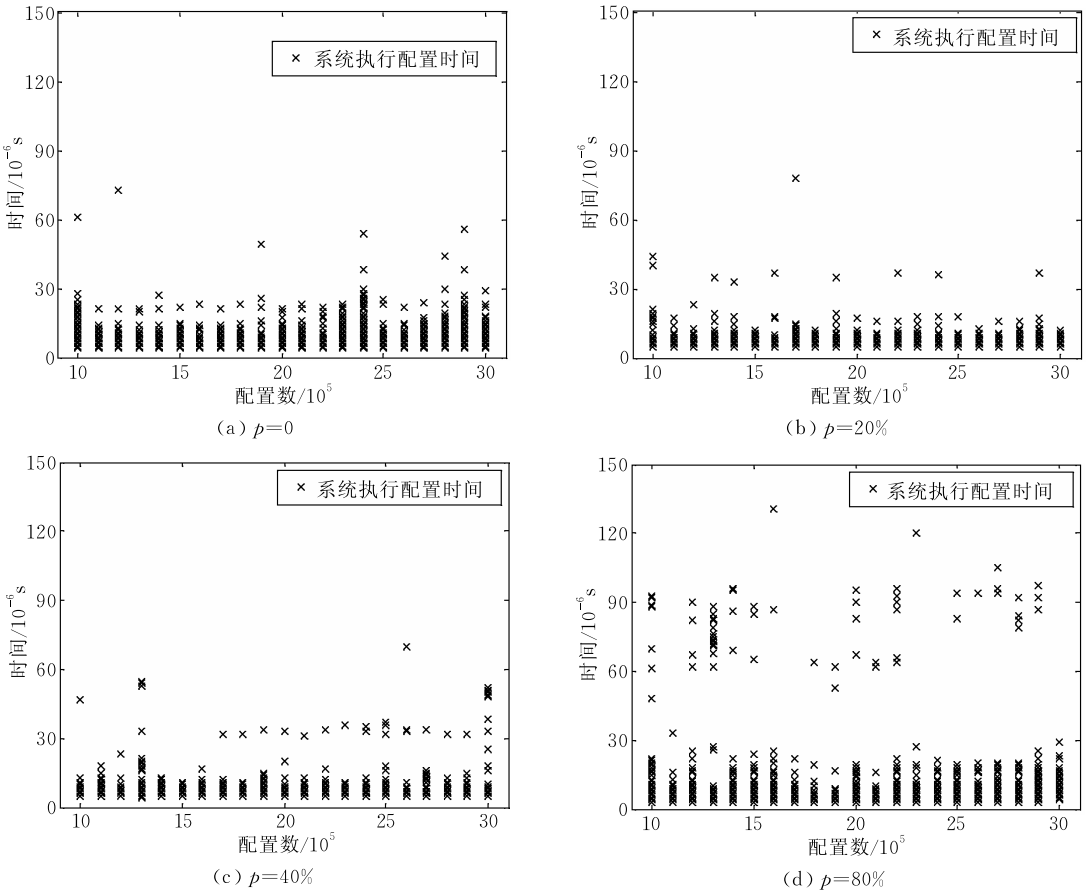
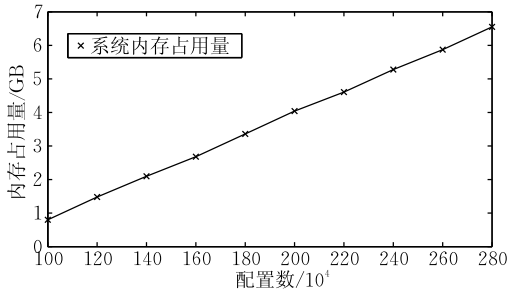


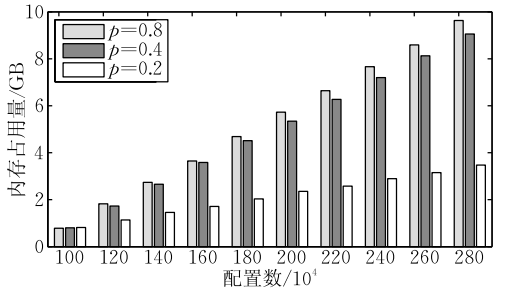
图 5　系统执行时间随规模和规则组成的变化趋势

图 6 表示了不同规则规模和复杂规模占比的情况下访问控制系统的内存占用情况. 图 6(a)显示，系统占用内存随着规则规模的扩大而扩大. 图 6(b)显示，当复杂规则占比为 0.8，规则规模达到 280 万条时，系统占用内存达到 9.6GB. 从内存的角度来看，内存与规则数目大致呈线性关系. 复杂规则占比越大，系统占用内存越多. 这是由于系统的首要需求是保证系统执行规则的时间尽可能短，访问控制的效果尽可能好，因而在内存中保存了规则的一部分信息. 因此，它满足真实应用场景下的实际需求.

从功能测试和性能测试的结果来看，该原型系统基本能够完成大规模网络行为的访问控制任务，在进一步扩大服务覆盖范围和优化服务量化准确度后，可以取得理想的效果.



(a) 不同规模配置占用内存



(b) 不同复杂配置占比情况下占用内存

图 6 系统占用内存随规则规模和组成的变化趋势

相比于传统的访问控制系统,该访问控制系统的优势如下:

(1)通过细粒度的访问控制机制,更好地支持了两个著名的安全控制原则,即最小特权原则及职责分离原则.

(2)提供了开放式的接口,可扩展性强.

(3)覆盖范围广,准确率高.

5 结 论

在开放式的网络环境中,网络资源和服务以及用户的随时动态接入一方面提高了生产效率,另一方面对下一代防火墙技术提出了很多新的安全挑战,而现有的诸多访问控制技术并不能满足开放式网络环境的要求.

针对现有 RBAC、TBAC 模型在支持服务细致授权粒度上的不足,本文引入了量化服务的概念并将其应用在访问控制系统中.量化服务是传统访问控制模型中服务的扩展形式,通过服务属性对服务进行划分,从而达到服务的扩展性要求.以很低的管理和维护代价实现了灵活的访问控制粒度.为了增强权限的动态可控性,该模型引入了条件角色迁移的概念,从而实现了细粒度的访问控制.本文形式化地定义了服务量化模型和角色量化模型,并在此基础上提出了基于量化角色和服务的访问控制模型(QSRBAC).

量化角色和服务是一种在 RBAC 系统中实施最小特权原则的有效机制,角色迁移是在开放式网络环境下运行访问控制系统的必然要求.研究量化角色和服务以及角色迁移是解决开放式网络场景中面临的访问控制要求的有效手段.

下一步的工作,将围绕分布式计算环境中的访问控制系统开展研究,以建立细粒度多级安全的访问控制模型.此外,将深入研究区域网络中策略的冲突和冗余的问题,并提出相应的检测及消解的方法.

参 考 文 献

[1] Jiang Jian-Chun, Ma Heng-Tai, Reng Dang-En, Qing Si-Han. A survey of intrusion detection research on network security. Journal of Software, 2000, 11(11): 1460-1466(in Chinese)
(蒋建春, 马恒太, 任党恩, 卿斯汉. 网络安全入侵检测:研究综述. 软件学报, 2000, 11(11): 1460-1466)

[2] Tian Li-Qin, Lin Chuang. A kind of game-theoretic control mechanism of user behavior trust based on prediction in trust worthy network. Chinese Journal of Computers, 2007, 30(11): 1930-1938(in Chinese)
(田立勤, 林闯. 可信网络中一种基于行为信任预测的博弈控制机制. 计算机学报, 2007, 30(11): 1930-1938)

[3] Jiang Jian, Zhuge Jian-Wei, Duan Hai-Xin, Wu Jian-Ping. Research on botnet mechanisms and defenses. Journal of Software, 2012, 23(1): 82-96(in Chinese)
(江健, 诸葛建伟, 段海新, 吴建平. 僵尸网络机理与防御技术. 软件学报, 2012, 23(1): 82-96)

[4] Liao Jun-Guo, Hong Fan, Zhu Geng-Ming, Yang Qiu-Wei. Trustworthiness-based authorization delegation model. Chinese Journal of Computers, 2006, 29(8): 1265-1270(in Chinese)
(廖俊国, 洪帆, 朱更明, 杨秋伟. 基于信任度的授权委托模型. 计算机学报, 2006, 29(8): 1265-1270)

[5] Yan Han, Zhang Hong, Xu Man-Wu. Object modeling and implementation of access control based on role. Chinese Journal of Computers, 2000, 23(10): 1064-1071(in Chinese)
(严悍, 张宏, 许满武. 基于角色访问控制对象建模及实现. 计算机学报, 2000, 23(10): 1064-1071)

[6] Cai Wei-Hong, Wei Gang, Xiao Shui. Fine-grained role delegation model based on mapping mechanism. Acta Electronic Sinica, 2010, 38(8): 1753-1758(in Chinese)
(蔡伟鸿, 韦岗, 肖水. 基于映射机制的细粒度 RBAC 委托授权模型. 电子学报, 2010, 38(8): 1753-1758)

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

[8] Li Feng-Hua, Su Mang, Shi Guo-Zhen, Ma Jian-Feng. Research status and development trends of access control model. Acta Electronic Sinica, 2012, 40(4): 805-813(in Chinese)

(李凤华，苏锦，史国振，马建峰. 访问控制模型研究进展及发展趋势. 电子学报，2012，40(4)：805-813)

[9] Gladney H M，Worley E L，Myers J J. An access control mechanism for computing resources. IBM Systems Journal，1975，14(3)：212-228

[10] Zhang Hong，He Ye-Ping，Shi Zhi-Guo. A delegation model for periodicity constraints-based DAC. Chinese Journal of Computers，2006，29(8)：1427-1437(in Chinese)
(张宏，贺也平，石志国. 基于周期时间限制的自主访问控制委托模型. 计算机学报，2006，29(8)：1427-1437)

[11] Sandhu R S. Role-based access control. Advances in Computers，1998，46：237-286

[12] Sandhu R S，Coyne E J，Feinstein H L，et al. Role-based access control models. Computer，1996，29(2)：38-47

[13] Sandhu R，Bhamidipati V，Munawer Q. The ARBAC97 model for role-based administration of roles. ACM Transactions on Information and System Security(TISSEC)，1999，2(1)：105-135

[14] Sandhu R，Munawer Q. The ARBAC99 model for administration of roles//Proceedings of the 15th Annual Computer Security Applications Conference(ACSAC' 99). Los Alamitos，USA，1999：229-238

[15] Oh S，Sandhu R. A model for role administration using organization structure//Proceedings of the 7th ACM Symposium on Access Control Models and Technologies. New York，USA，2002：155-162

[16] Ferraiolo D F，Sandhu R，Gavrila S，et al. Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security (TISSEC)，2001，4(3)：224-274

[17] Thomas R K，Sandhu R S. Task-based authorization controls (TBAC)：A family of models for active and enterprise-oriented authorization management//Proceedings of the IFIP WG11.3 Workshop on Database Security. California，USA，1997：166-181

[18] Huang Qin，Gao Dong-Qun，Liu Yi-Liang. Task-state-based delegation model in workflow system. Computer Technology and Development，2011，21(2)：34-38 (in Chinese)
(黄勤，高东群，刘益良. 工作流系统中基于任务状态的转授权模型. 计算机技术与发展，2011，21(2)：34-38)

[19] Xing Guang-Lin，Hong Fan. A workflow authorization model based on role and task and constraints specification. Journal of Computer Research and Development，2005，42(11)：1946-1953(in Chinese)
(邢光林，洪帆. 基于角色和任务的工作流授权模型及约束描述. 计算机研究与发展，2005，42(11)：1946-1953)

[20] Chakraborty S，Ray I. TrustBAC：Integrating trust relationships into the RBAC model for access control in open systems//Proceedings of the 11th ACM Symposium on Access Control Models and Technologies. New York，USA，2006：49-58

[21] Zhao Qing-Song，Sun Yu-Fang，Sun Bo. RPRDM：A repeated-and-part-role-based delegation model. Journal of Computer Research and Development，2003，40(2)：221-227 (in Chinese)
(赵庆松，孙玉芳，孙波. RPRDM：基于重复和部分角色的转授权模型. 计算机研究与发展，2003，40(2)：221-227)

[22] Sun Bo，Zhao Qing-Song，Sun Yu-Fang. TRDM-temporal role-based delegation model. Journal of Computer Research and Development，2004，41(7)：1104-1109(in Chinese)
(孙波，赵庆松，孙玉芳. TRDM-具有时限的基于角色的转授权模型. 计算机研究与发展，2004，41(7)：1104-1109)

LIU Qing-Yun，born in 1980，Ph.D. candidate，senior engineer. His research interests include information security，network security.

SHA Hong-Zhou，born in 1988，Ph. D. candidate. His research interests include information security，network content security.

LI Shi-Ming，born in 1987，M. S. candidate. His research interests include information security，network content security.

YANG Rong，born in 1978，M. S.，engineer. His research interests include information security，network security.

Background

This work is partially supported by the National High Technology Research and Development Program (863 Program) of China (Grant No. 2011AA010703) and the "Strategic Priority Research Program" of the Chinese Academy of Sciences (Grant No. XDA06030200) and the National Key Technology R&D Program (Grant No. 2012BAH46B02).

As the rapid development of network technology，network control is becoming more and more important. RBAC is suitable for the traditional network environment. In recent years，a great number of researchers have paid much attention to the area of RBAC，and focused on theoretical model and practical applications. However，a lot of issues still have not been addressed well. The author study the access control strategy based on qualified users and services and illustrates the mapping method from the behavior control strategy to executable rules in firewall. At the same time，starting from the possible relations between the users and service of firewall domain，this paper discusses the role migration and the dynamic changes of service and proposes a dynamic access control method.