第 33 卷 第 2 期 计 算 机 工 程 2007 年 1 月
Vol.33 No.2 Computer Engineering January 2007
·安全技术· 文章编号：1000—3428(2007)02—0145—03 文献标识码：A 中图分类号：TP393.08

面向代理机制的角色访问控制

许 谦[1]，雷咏梅[1]，蔡红霞[2]
（1. 上海大学计算机科学与工程学院，上海 200072；2. 上海大学CIMS和机器人中心，上海 200072）

摘 要：基于角色的访问控制模型简化了访问控制授权，但是与代理机制相结合所带来的授权问题，制约了其在网格中的应用。该文介绍了 RBAC 与代理机制相结合所带来的授权问题，在定义了角色屏蔽概念的基础上，提出了面向代理机制的角色访问控制模型。引入了全局角色、本地角色等概念，用于描述 PRBAC 模型。PRBAC 模型对用户与角色的匹配是通过角色委派集和多种角色合并策略完成的。PRBAC 模型可以很好地解决在网格环境中使用代理机制的情况下引入 RBAC 所带来角色屏蔽问题，加强了服务节点的访问安全控制。
关键词：网格；角色；代理；安全

Proxy Mechanism Oriented Role-based Access Control

XU Qian[1], LEI Yongmei[1], CAI Hongxia[2]
(1. School of Computer Science and Engineering, Shanghai University, Shanghai 200072;
2. CIMS & Robot Center, Shanghai University, Shanghai 200072)

【Abstract】Although it makes the authorization easier, role-based access control (RBAC) model will cause authorization problem when combining with proxy mechanism. This paper discusses the authorization problem and defines the conception of covered role, presents a proxy mechanism oriented role-based access control (PRBAC) model. In the model, it introduces some notions to describe PRBAC model. In PRBAC model, user's role can be appointed by kinds of coalition policies and role appointed unit. This model can efficiently resolve the covered role and enhance authorization of service nodes.
【Key words】Grid; Role; Proxy; Security

网格通过提供服务实现了计算资源、存储资源、数据资源、信息资源、知识资源、专家资源的全面共享。由于网格提供了代理机制下的分布式资源共享，这就使得网格的信息安全，尤其是访问控制安全，变得十分重要。

目前在网格中将安全策略分为全局与本地两部分，采用了CAS、身份映射(Identity Mapping Service)[2]等中间件服务。然而随着网格在各行各业中的应用，人们需要在网格中引入各式各样的访问控制模型以满足应用的需要。其中包括基于角色的访问控制模型。基于角色的访问控制(RBAC)[3]模型的突出优点是简化了各种环境下的授权管理。为了保证用户只需单一登录就可以使用网格中的资源[4]，在网格中采用了基于X.509 证书的代理机制用于授权与委托，这使得RBAC的引入存在很大的安全隐患。

为解决在网格中使用代理机制的情况下引入基于角色的访问控制策略所产生的问题，本文提出了面向代理机制的角色访问控制模型。

1 网格中引入角色访问控制存在的问题

如果将 RBAC 引入网格中，那么作为访问控制策略，就必然要与网格中的授权机制——代理机制相结合。看下面一个例子，如图 1 所示。在网格中，有以下两种角色：(1)资源提供者角色：提供资源；(2)管理者角色：对网格中资源进行统筹管理。其中，文档是资源提供者的机密，不能被竞争对手(其他具有资源提供者角色的用户)所获得。用户 A 具有管理者角色。B 和 C 具有资源提供者角色。如果用户 A 将自己的代理证书授予用户 B，委托其调用 C 提供的查阅文档服务。那么这时，B 将以 A 的身份对 C 进行访问，从而可以获得 C 的文档，显然是与 C 设定的 RBAC 策略相冲突的。

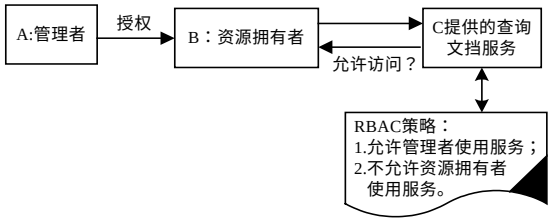

图 1 代理机制与 RBAC 结合实例

问题产生的原因是：当用户 A 将代理证书授予用户 B 后，屏蔽了 B 原本的角色。而代理机制本身就是对另一用户的授权，接受代理的用户的角色必然会被代理发放者的角色所屏蔽。为了更好地说明问题，本文提出了角色屏蔽的概念。角色屏蔽是指用户的当前角色屏蔽了用户具有的其他角色。这就使得在访问时仅仅依据用户的当前角色进行授权，而不考虑其它角色。如果这时用户拥有两个冲突的角色，则会产生安全问题。

2 面向代理机制的角色访问控制

为了解决上节中的问题，本文提出了面向代理机制的角色访问控制模型(Proxy Mechanism Oriented Role-based Access Control, PRBAC)。与网格中的安全策略相似，该模型的访问控制策略分为全局和本地两部分，其中以本地访问策

基金项目：上海市教委E研究院–上海高校资助网格项目
作者简介：许 谦(1983－)，男，硕士生，主研方向：网格技术，计算机信息安全； 雷咏梅，副教授；蔡红霞，硕士、讲师
收稿日期：2006-04-02 **E-mail：**pencil169@126.com

略为重。

2.1 PRBAC 定义

在介绍 PRBAC 模型之前，先给出以下几个定义。

定义 1 全局角色(Grid Role)是指用户在全局环境中所具有的角色，用于指定用户对网格中服务的访问权限。全局角色是在网格中统一设定的。用户 k 的全局角色记作 gr(k)。证书链中所有用户的全局角色集合记作 GR。

定义 2 本地角色(Local Role) 是由服务提供者在本地设定的角色，用于限定用户对本地服务的访问权限，记作 LR。

定义 3 威胁度(Threaten Degree)是衡量角色安全性的一个标准。一个角色的威胁度越高，对用户赋予该角色时就应越谨慎。系统中每个角色的威胁度可由用户自行设定，其取值范围是[1,…,10]之间的整数，值越大说明威胁度越高。角色 k 的威胁度，记作 TD(k)。

定义 4 全局角色委派(Grid-Role Appointed)是由全局角色服务对用户进行的角色委派，使得用户具有访问网格中服务的权限。

定义 5 本地角色委派(Local Role Appointed)是服务提供者对用户指定的本地角色，使得该用户访问本地服务时只能以指派的本地角色访问。

定义 6 用户-全局角色委派集(Grid Role Appointed Unit)是指记录了每个用户所具有的全局角色的集合。记作 GRAU。

定义 7 用户-本地角色委派集(Local-Role Appointed Unit)是指记录了服务提供者对某些用户所指定的本地角色的集合。记作 LRAU。

定义 8 全局角色-本地角色映射(Grid Role Local Role Mapping Rules)是由服务提供者制定的规则，它将用户的全局角色映射为本地角色。

定义 9 映射角色(Mapped Local Role)是本地角色的子集，特指由用户全局角色通过全局角色——本地角色映射规则生成的本地角色。用户 k 的映射角色记作 mlr(k)。证书链中用户的映射角色集合记作 MLR。

定义 10 委派角色(Appointed Local Role)是本地角色的子集，特指用户通过本地角色委派生成的本地角色。用户 k 的委派角色记作 alr(k)。证书链中用户的委派角色集合记作 ALR。

定义 11 证书链用户本地角色集(User Local Roles Unit in Certificate Chain)是由证书链中用户的所有本地角色生成的集合。记作 UC ，UC=ALR+MLR。

定义 12 临时角色(Temporary Role)是由证书链用户本地角色集中的本地角色通过角色合并策略生成的。临时角色具有时效性，其生命期就是服务执行的时间段。记作 TR。

2.2 PRBAC 模型

PRBAC 是面向代理机制的 RBAC 模型，其数学关系为 PRBAC＝(U, P, R, S)，其中 U 代表证书链中的用户；P 代表权限；R 代表角色，包括全局角色(GR)，本地角色(LR)；S 代表服务。定义以下关系：

(1)角色分配关系用户到角色是多对多的关系，记作 RA $\subseteq$ U x R，其中 R=GR$\cup$LR；

(2 权限分配关系是访问权限到角色的多对多的映射关系,记为 PA, PA $\subseteq$ R x P；

(3)角色关系是角色间的相互关系,如角色的继承和派生等关系。角色关系的集合称为角色关系集，记为 RR，RR $\subseteq$ R x R；

(4) 服务关系是服务间的关系，在业务系统中主要表现为服务间的相互依赖关系，记为 SR, SR $\subseteq$ S x S；

(5)全局角色-本地角色映射关系是指全局角色与本地角色之间的映射关系，通过该映射关系获得用户的映射角色。记作 GLM，其中 $m\ln(n) = GLM(gr(n)), n \in U$ ；

(6)用户-本地角色委派是服务提供者对用户所委派的本地角色策略，记作 LRA。其中 alr(n)=LRA(n)，n$\in$U。

在以上数学关系的基础上，建立了具体的 PRBAC 模型，如图 2 所示。该模型分为全局和本地两部分。

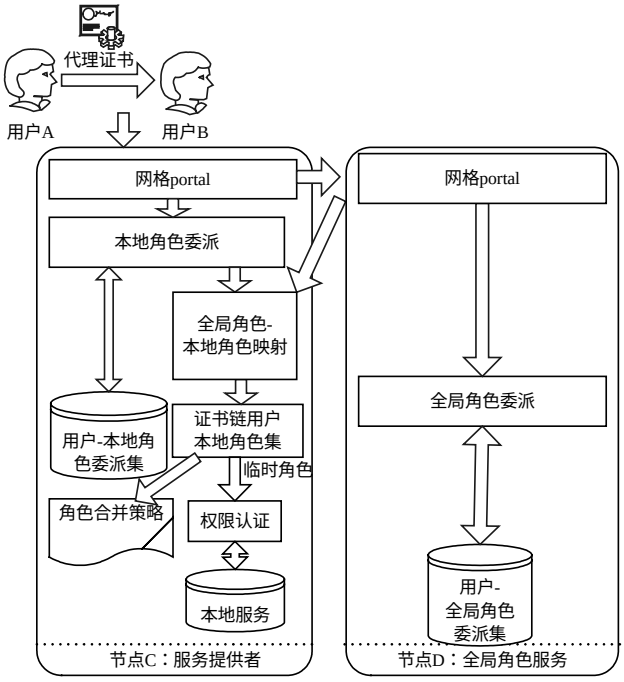

图 2 PRBAC模型

模型的本地部分由网格 portal，本地角色委派、全局角色-本地角色映射、证书链用户本地角色集、权限认证 5 部分组成。

(1)网格 portal：服务的接口，负责接收和发送消息。

(2)本地角色委派：按照用户——本地角色委派集取得用户的委派角色；同时对于用户——本地角色委派集中没有被委派的用户，通过申请全局角色服务获得用户所具有的全局角色。

(3)全局角色-本地角色映射：根据用户的全局角色生成用户的映射角色。

(4)证书链用户本地角色集：将所有本地角色依照角色合并策略生成临时角色。

(5)权限认证：验证临时角色是否有权访问服务，如果有权则执行服务并返回结果。

模型的全局部分由网格 portal 和全局角色委派两个部分组成：

(1)网格 portal：是服务的接口，负责接收和发送消息。

(2)全局角色委派：负责为用户分配全局角色，并记录在用户-全局角色委派集中；同时还提供用户全局角色的查询服务，依照提供的用户 ID 返回该用户的所有全局角色。

2.3 PRBAC 模型中的策略与机制

PRBAC 访问控制重点是取得证书链中所有用户的本地角色，并存储在证书链用户本地角色集中。然后对其中的本地角色按照角色合并策略进行合并，最终生成访问本地服务的临时角色。

下面将按照 PRBAC 访问流程对相应策略与机制作详细的介绍。

(1)本地模型需要先获取证书链中所有用户的本地角色，

生成证书链用户本地角色集。模型在该阶段提供了 3 种策略，对于证书链中的一个用户只可以使用一种策略：

1)在用户-本地角色委派集中没有对用户明确委派。即 LRA(k) 为空(k 为用户)。在这种情况下，需要通过全局角色服务获得用户的全局角色，并通过全局角色-本地角色映射转换为本地角色。这时，用户 k 的本地角色 LR(k)＝mlr(k)= GLM(gr(k))。

2)在用户-本地角色委派集中明确将本地角色委派给用户。在这种情况下,不需要考虑该用户的全局角色。用户 k 的本地角色 LR(k)= alr(k)=LRA(k)。

3)在用户-本地角色委派集中明确限定用户不可被委派某些本地角色。这种情况下，需要通过全局角色服务获得用户的全局角色，并通过全集角色-本地角色映射转换为本地角色，同时确保其中不包括被禁止委派的本地角色。用户 k 的本地角色

$$LR(k) = m\ln(k) \cap \neg alr(k) = GLM(gr(k)) \cap \neg LRA(k)$$

取得的所有本地角色存储在证书链用户本地角色集中，记为

$$UC = \sum_{i \in U} LR(i)$$

该阶段的 3 种策略可以满足多种访问控制要求。例如，如果要想为某个服务设定一个代理，所有要访问该服务的用户都必须通过代理访问。这时只需要创建一个唯一可访问该服务的角色 m，使得 m∈LRAU&&m∉GLM(i),其中 i∈GR。并将角色 m 按照策略二唯一的委派给一个用户，则可以实现设定代理的目的。此外，如果要永久禁止用户拥有某一本地角色只需将该用户按照第 3 种策略进行委派，这样不论该用户的全局角色如何变化都无法获得被禁止拥有的本地角色。

(2)对集合 UC 中的本地角色按照角色合并策略进行合并，生成临时角色。在该阶段模型提出 4 种角色合并策略，每种策略的侧重点不同,服务提供者可以按照需要任选其一。

1)强委派控制策略(Strong Appointed Control Policy):是一种加强委派角色作用的策略。记为 SACP。在这种策略下选择的临时角色 TR 为

$$TR = SACP(UC) = SACP(\{\sum_{i \in U} LR(i)\})$$
$$= (\sum_{l \in U} \cap m\ln(l)) \cup (\sum_{i \in U} \cup alr(i)),\ l \neq i$$

2)强信任控制策略(Strong Trust Control Policy)：该策略只考虑访问发起者的本地角色，而不考虑证书链中其他用户。这种访问策略是基于对访问发起者的绝对信任。记为 STCP。

TR=STCP(UC)=LR(start)，start∈U。

3)最强控制策略(Strongest Control Policy)：将所有本地角色所具有的权限取交集。这时生成的临时角色具有最严格的访问控制限制，记为 SCP。

$$TR = SCP(UC) = SCP(\{\sum_{i \in U} LR(i)\}) =$$
$$(\sum_{l \in U} \cap m\ln(l)) \cap (\sum_{i \in U} \cap alr(i)),\ l \neq i$$

4)威胁度控制策略(Threaten Degree Control Policy)：该策略是选取威胁度最低的本地角色作为临时角色，记为 TDCP。

$$TR = TDCP(UC) = TDCP(\{\sum_{i \in U} LR(i)\})$$
$$= LR(k),\ (TD(k) = MIN(TD(i)),\ i, k \in U)$$

2.4 PRBAC模型的应用

目前PRBAC模型已经应用于制造网格之中。制造网格是上海大学E研究院网格项目下的子项目，主要研究制造业在网格环境中的应用。在制造网格中加工器件时，往往需要将其细分为更小的加工单位。在这种情况下，为了能够更好地完成加工任务，用户会将自己的代理证书发放给其他用户，委托其代为完成一部分加工任务。通常这样的委托不仅仅是一级的，而是多级的，这就产生了一条证书链，同时产生了角色屏蔽。这就给资源节点的访问控制带来了很大的挑战。通过将PRBAC模型引入到制造网格当中，很好地解决了这一问题，从而加强了资源节点的访问控制安全。

3 总结

本文首先介绍了RBAC所具有的安全隐患,并指出RBAC与代理机制结合后出现的安全问题；然后在此基础上提出了面向代理机制的角色访问控制模型。该模型重点解决了RBAC与代理机制相结合后所产生的角色屏蔽问题。针对网格中复杂的环境，该模型提出了多种角色委派策略和角色合并策略，从而进一步加强了网格中的访问控制安全。

参考文献

1 Foster I, Kesselman C. The Grid: Blueprint for a New Computing Infrastructure[M]. San Fransisco: CA Morgan Kaufmann, 1999.

2 Welch V, Siebenlist F, Foster I. Security for Grid Services[C]. Proceedings of the 12th IEEE International Symposium on High Performance Distributed Computing, 2003-06-22: 48-57.

3 Bo Dengji, Fan Hong. Task Based Access Control Model[J]. Journal of Software, 2003, 14(1): 76-82.

4 Welch V, Foster I, Kesselman C. X.509 Proxy Certificates for Dynamic Delegation[C]. Proc. of the 3rd Annual PKI R&D Workshop, 2004.

~~~~~~

(上接第 141 页)

5 结束语

本文围绕补丁自动管理软件的开发，阐述了补丁自动管理系统从设计到实现所涉及的关键技术和要点，并成功地实现了对中文补丁的自动下载、检测及安装。此外在支持多系统补丁、制定详细的分发策略及补丁测试等方向上还值得我们作进一步的研究与开发。

参考文献

1 Benjurry. 居安思危——论补丁管理[Z]. 2004-05. http://www.xfocus.net/articles/200405/698.html.

2 Microsoft. 软件更新服务 SUS[Z]. 2004. http://www.microsoft.com/china/security/guidance/prodtech/SUS.mspx.

3 Yellow Dog Updater Modified[Z]. 2005-08. http://wiki.linux.duke.edu/Yum.

4 BigFix 公司. Patch Management[Z]. 2005. http://www.bigfix.com/products/patch.html.

5 Shavilik 公司. 2005-04. https://xml.shavlik.com/mssecure.xml.
~~~~~~