ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.19, No.10, October 2008, pp.2754−2761
DOI: 10.3724/SP.J.1001.2008.02754

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于协商的跨社区访问的动态角色转换机制*

付长胜+, 肖 侬, 赵英杰, 陈 涛

(国防科学技术大学 计算机学院,湖南 长沙 410073)

Negotiation-Based Dynamic Role Transition in Data Access across Multi-VOs

FU Chang-Sheng+, XIAO Nong, ZHAO Ying-Jie, CHEN Tao

(School of Computer, National University of Defense Technology, Chang 410073, China)

+ Corresponding author: E-mail: csffcs@126.com

Fu CS, Xiao N, Zhao YJ, Chen T. Negotiation-Based dynamic role transition in data access across multi-VOs. *Journal of Software*, 2008,19(10):2754−2761. http://www.jos.org.cn/1000-9825/19/2754.htm

Abstract: This paper proposes an approach to data access across multi-Vos (virtual organizations), using dynamic role transition under role-based access control model in data grid. A negotiation mechanism is introduced to establish the data access based on the trust of both VOs, which also sets up the role transition relationship between them. Once the negotiation succeeds, the dynamic role transition is controlled by several local policies according to the role owned by the user.

Key words: dynamic role transition; negotiation; VO (virtual organization); data grid

摘 要: 在基于角色的访问控制模型下,将一个虚拟社区中的角色动态地转换成另一个虚拟社区的角色,从而获得跨虚拟社区的数据访问权限.引入协商机制,建立起两个社区之间的角色转换关系,将跨虚拟社区的数据访问建立在双方社区的信任关系之上,并通过一系列的本地控制策略,根据用户拥有的角色动态地进行角色转换.

关键词: 动态角色转换;协商;虚拟社区;数据网格

中图法分类号: TP393 **文献标识码**: A

在数据网格[1,2]中,用户想要访问某特定资源,必须获得该资源的资源提供者授予的访问权限.为了更好地管理和共享资源,基于一系列的规则和共同的目标,人们建立起虚拟社区[3].资源提供者将资源的访问权限授予虚拟社区.在基于角色的访问控制模型下,虚拟社区将获得的资源的访问权限分配给角色,当该虚拟社区的一个用户拥有了某个角色后,则意味着该用户取得了该角色相对应的资源访问权限.一个用户为了获得不同的资源访问权限,可以拥有多个不同的角色.此时,资源提供者只需确认该用户的角色,即可允许该用户进行相应的访问操作.

当多个虚拟社区之间达成协议,需要协同完成某项工程时,其中某社区的用户往往需要访问其他虚拟社区中的数据资源,但由于该用户不属于资源所属的虚拟社区,导致其无法获得合适的授权,从而不能访问该资源.

* Supported by the National Natural Science Foundation of China under Grant No.60573135 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant Nos.2006AA01A106, 2006AA01A118 (国家高技术研究发展计划(863))

Received 2007-07-30; Accepted 2008-02-25

本文引入了协商机制,在基于角色的访问控制模型[4−6]下,将本地需要进行跨社区访问的角色动态地转换为被访问社区中的角色.这样,访问其他虚拟社区中的数据资源的用户,可以根据其所属社区中的角色获得被访问社区中的相应角色,从而使得被访问资源的提供者可以识别该用户的角色,同时,该用户也能获得该资源的访问权限,最终实现了跨多个社区的数据访问.协商机制可以建立起虚拟社区之间的信任关系.协商的双方并不需要了解对方社区内部的全部角色,仅需要提供将来用于角色转换的角色及相应的资源.角色转换机制建立在协商的基础上,而不是采用集中控制的方法.

本文第 1 节介绍相关工作.第 2 节讨论虚拟社区间如何进行协商,以便建立起主动访问社区中的角色与被动访问社区中的角色之间的映射关系,这是本文提出的角色动态转换的基础.第 3 节研究主动访问社区将这些可以进行跨社区访问的角色授予本地用户使用的本地策略.第 4 节探讨被动访问社区如何进行角色转换,以使主动访问社区的用户能够对跨域资源进行访问.第 5 节进行实验,并分析结果.最后总结全文.

1 相关工作

Kapadia,Al-Muhtadi 等人提出了可互操作的基于角色的访问控制(interoperable role-based access control,简称 IRBAC)[7,8]机制,可以实现不同社区间的角色转换.它需要由一个共同的管理人员建立双方虚拟社区间的角色映射关系,且需要集中控制角色转换过程.与本文相比,IRBAC 要求双方管理员了解对方社区内部的所有角色,这比较苛刻,且很多角色实际上并不参与角色转换.另外,在网格这一特定的应用场景中,虚拟社区双方的管理员往往不是同一个人,在空间上也相隔较远.本文通过协商机制,允许双方管理人员利用网络建立双方虚拟社区间的角色映射关系.在角色转换过程中,本文采用了分布式控制的方法,由资源所属社区控制角色转换.

文献[9]中使用了用户的信誉值及换算因子来控制动态角色(dynamic-role)的转换.它需要资源提供者和用户对对方的行为进行打分,打分会最终影响用户的信誉值,从而限制用户的跨社区访问的行为.首先,它对于资源提供者和用户来说,打分增加了他们的管理负担,如果有大量的用户对某一资源进行访问,资源提供者的承受能力将受到极大的挑战.其次,换算因子在每次打分后,都需要重新计算,于是,每次访问也都需要按照新的换算因子重新进行动态角色的转换,这样,每次访问都将有角色转换带来的效率上的消耗.

文献[10]中提出了分布式基于角色的访问控制模型及机制(dynamic role-based access control,简称 dRBAC).它最吸引人的特点是第三方委托,即若允许已授权的实体授权给由其他人创建的角色,只需直接引用该角色的创建者的名空间即可.加上它其他的特点,这样,dRBAC 就使得每一项对保护资源的授权都可以定义自己的信任关系,进而构建出一个分布式的访问控制系统.与本文相比,它可能会产生很长的信任链,需要付出更多的代价完成访问控制.

随着越来越多的网格采用或兼容 GSI(grid security infrastructure)[11,12]标准,本文的协商过程可以建立在 GSI 的基础之上,从而保证其协商的安全性并具有一定的通用性.

2 虚拟社区间的协商

我们首先引入一些基本概念.

定义 1(**跨域资源**). 社区中的某一资源,若按照一定的共享规则,允许非本社区的用户对其进行访问,则称其为跨域资源.

定义 2(**跨社区访问**). 社区中某一用户,若按照一定的授权访问规则,对跨域资源进行访问,则称此次访问为跨社区访问.

定义 3(**主动访问社区**). 能够发起跨社区访问的用户所在的社区,称为主动访问社区.

定义 4(**被动访问社区**). 提供跨域资源的社区,称为被动访问社区.

例如,生物虚拟社区 BioVO 和化学虚拟社区 ChemVO 达成协议,想要进行某项生物化学研究工作,此时,BioVO 中的用户 Usr 需要访问 ChemVO 中的资源 Res,以获得研究需要的化学资料.BioVO 是主动访问社区,而 ChemVO 是被动访问社区,ChemVO 中的资源 Res 就是跨域资源.

在跨社区访问发生之前,主动访问社区与被动访问社区要进行协商,其协商的主要过程包括:

Step 1. 主动社区与被动社区建立信任关系,双方可以识别对方签名,进行安全会话;

Step 2. 主动访问社区与被动访问社区商定跨域资源;

Step 3. 被动访问社区建立可转换角色列表,该列表中的角色是被动访问社区中的本地角色,主动访问社区中的角色将可能被转换成其中的角色,从而拥有上面所商定的资源的访问权限;

Step 4. 主动访问社区从其内部选择可以进行跨社区访问的角色,建立各角色到被动访问社区中可转换角色的映射,被动访问社区对每个角色及其映射关系进行审核,对于审核通过的角色,双方对该角色可获得的资源的跨社区访问权限要达成共识.

2.1 可转换角色

经过协商过程的 Step 1 和 Step 2,主动访问社区与被动访问社区将能够进行跨社区访问的跨域资源协商确定下来.

记跨域资源的访问权限的集合为 $PRMS_c$,且 $PRMS_c \subseteq PRMS_n$,其中 $PRMS_m$ 是被动访问社区中的本地资源的访问权限的集合.设被动访问社区的本地角色集为 $ROLES_c$,其访问权限到角色的多对多映射关系为 $PA_n \subseteq ROLES_n \times PRMS_n$.

定义 5(可转换角色).拥有跨域资源的访问权限的角色,称为可转换角色.

现记可转换角色的集合为 $ROLES_{cn} = \{r \in ROLES_n \mid (p,r) \in PA_n, p \in PRMS_c\}$.显然, $ROLES_{cn} \subseteq ROLES_n$.

若记 $PA = \{(p,r) \in PA_n \mid p \in PRMS_c, r \in ROLES_{cn}\}$,显然 $PA \subseteq PA_n$,则 PA 描述了跨域资源的访问权限到可转换角色的多对多映射关系.

于是,对于每个可转换角色,它所代表的跨域资源的访问权限的集合为 $cross\_prms(r) = \{p \in PRMS_c \mid (p,r) \in PA, r \in ROLES_{cn}\}$.

在协商过程的 Step 3 中,被动访问社区将可转换角色集 $ROLES_{cm}$,所有跨域资源的访问权限集 $PRMS_c$,以及跨域资源的访问权限到可转换角色的多对多映射关系 PA,一并提交给主动访问社区,而主动访问社区将保留这些信息.

2.2 跨域角色

在协商过程的 Step 3 之后,主动访问社区从被动访问社区处获取了可转换角色集及每个可转换角色所代表的跨社区的访问权限.但此时,主动访问社区中的用户不能直接使用这些权限,并且被动访问社区中的资源提供者也不认可主动访问社区把跨域资源的访问权限授权给其本地用户.

主动访问社区根据自己的需要,选取本地角色集 $ROLES_m$ 中的部分角色作为将来可以进行跨社区访问操作的角色.同时,主动访问社区建立这些角色到可转换角色集 $ROLES_{cm}$ 的多对一映射 $RA_m \subseteq ROLES_m \times ROLES_{cn}$.主动访问社区再将这些角色及映射 RA_m 提交给被动访问社区,由被动访问社区决定这些映射关系是否成立;若被动访问社区不同意某些角色映射关系,则可能需要双方多次交换意见,最终确立一系列双方均认可的角色映射关系.因此,这种主动访问社区对跨域资源的授权实际上是对跨域资源的访问权限的申请,最终决定权仍然在被动访问社区手中.

被动访问社区同意主动访问社区的申请后,主动访问社区就可以将该角色授予本地用户使用了.

定义 6(跨域角色).经过双方社区协商,建立映射 $RA: ROLES_m \mapsto ROLES_{cn}$,对应于可转换角色 $r \in ROLES_{cn}$,若 $t \in ROLES_m$ 满足 $RA(t)=r$,则称 t 是 r 的跨域角色,简称跨域角色.

记这些跨域角色的集合为 $ROLES_{cm}$,显然有 $ROLES_{cm} \subseteq ROLES_m$.

对于每个跨域角色 $t \in ROLES_{cm}$,它所拥有的跨社区访问的权限为 $assigned\_cross\_prms(t) = cross\_prms(r) = \{p \in PRMS_c \mid (p,r) \in PA\}$,其中, $r \in ROLES_{cn}$ 且满足 $RA(t)=r$.

在协商的 Step 4 中,主动访问社区与被动访问社区对 RA 这一从本地角色集到可转换角色集的映射达成一致.主动访问社区根据 RA 可以获知某跨域角色所赋予的跨社区访问权限,而被动访问社区将根据 RA 把跨域角

色转换为可转换角色.显然,一个跨域角色可以同时拥有本地资源的访问权限和相应的跨域资源的访问权限.

2.3 BioVO与ChemVO协商的例子

如图 1 所示,为 BioVO 与 ChemVO 协商成功后的跨域角色与可转化角色之间的关系.图 1 左部分为 BioVO 中的部分角色,其中边框为虚线的角色是协商后的跨域角色;右部分为 ChemVO 中的部分角色,其中边框为粗实线的角色是协商后的可转换角色;虚尾箭头将跨域角色及其对应的可转换角色连接起来,表示其尾部的跨域角色 t 与其头部的可转换角色 r 之间存在映射关系,即满足 $RA(t)=r$.另外,用箭头连接起来的角色 t_1 和 t_2,若角色 t_1 在该箭头的尾部且角色 t_2 在该箭头的头部,则表示 r_1 继承了 r_2 的所有权限.本文在第 3 节中讨论权限继承问题.

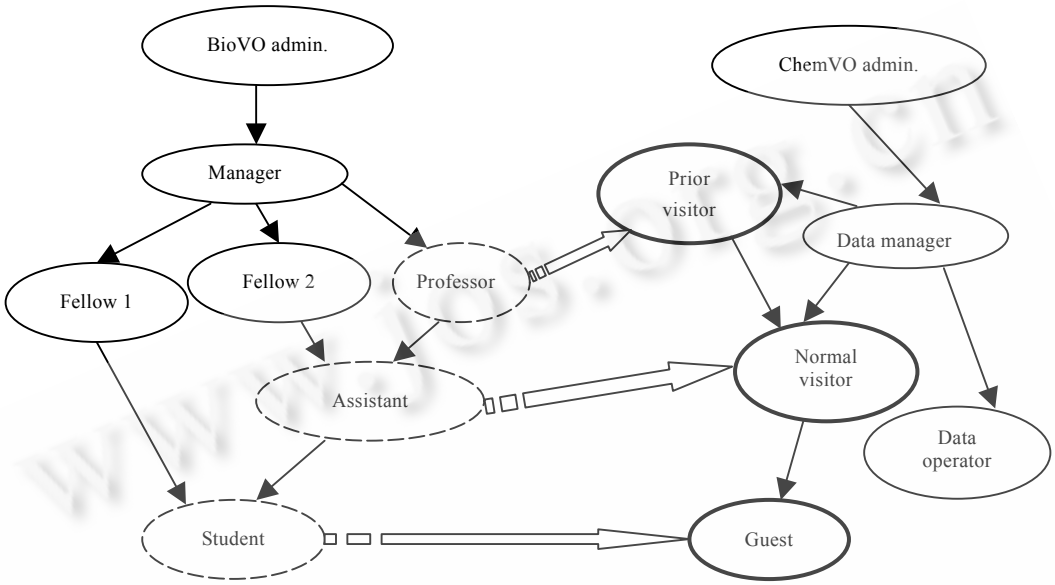

Fig.1 Negotiated relationship of role mapping between BioVO and ChemVO

图 1 BioVO 与 ChemVO 协商后的角色映射关系示意图

这里所列出的可转换角色的名称,暗示了该角色能够代表的跨域资源的访问权限.例如,“访客”,这个可转换角色,从其名称上可以知道它的跨社区访问权限最低,而“高级资源访问者”这个角色的跨社区访问权限最高.

2.4 多个虚拟社区协商的复杂度

现在,假设有 m 个虚拟社区达成协议,允许跨社区访问,共有 N 个用户明确地需要进行跨社区访问,每个用户都至少拥有一个跨域角色,而每个虚拟社区中跨域角色数为 C_i,其中 i=1,2,…,m.

注意,在实际应用中,一个角色总是对应多个用户的,并且一个社区中的角色数量一般都远少于其用户数量,因此,记 $C=\sum_{i=1}^{m}C_i$,可以有 $C \ll N$.

对于一个跨域角色,假定双方进行一次协商即可确定其相应的可转换角色,则确定它对 m 个社区的跨域资源的访问权限,最多需要 m 次协商.因此,现在所需要的总的协商次数最多为 $C_1 \cdot m + C_2 \cdot m + ... + C_m \cdot m = m \cdot \sum_{i=1}^{m} C_i = m \cdot C$,则协商的复杂度为 $O(C)$.如果考虑到虚拟社区中的跨域角色数量往往保持一个相对恒定的值,那么可以认为 C 是一个常数.

3 主动访问社区的跨域角色授予策略

在主动访问社区与被动访问社区协商成功后,主动访问社区便可以将商定的跨域角色授予社区内的用户,

使其获得跨社区访问资源的权限.

由于跨域角色集往往只是主动访问社区的本地角色集的一个非空子集,因此,并不是主动访问社区中的每个本地角色都与某个可转换角色建立了映射关系.这也意味着,主动访问社区中的那些非跨域角色将不能转换为可转换角色,也就不能获得跨域资源的访问权限.这显然使得社区间的角色转换仅限于跨域角色.但在实际应用中,主动访问社区中的某些非跨域角色也会产生对跨域资源的访问请求.如果将所有可能需要跨域资源的访问权限的本地角色都变成跨域角色,这无疑将增加社区(安全)管理员的工作量,社区间将进行大量的协商以建立这些跨域角色到可转换角色的映射关系.以图 1 为例,由于 BioVO 中的本地角色"项目管理员"没有与任何可转换角色建立映射关系,它将无法获得任何跨域资源的访问权限.但拥有"项目管理员"这个角色的用户可能需要对项目中所涉及到的跨域资源进行访问.

在有层次的 RBAC(role-based control access)机制的基础上,提出了继承策略和例外策略来解决上述问题.

在有层次的 RBAC 中,存在一个角色集 $ROLES$ 上的偏序关系 $RH \subseteq ROLES \times ROLES$, 记为 $\succeq$,若 $r_1, r_2 \in ROLES$ 且 $r_1 \succeq r_2$,当且仅当 r_1 的所有用户都是 r_2 的用户,并且 r_2 的所有权限都是 r_1 的权限.也就是说,r_1 继承了 r_2 的所有权限.特别地,$\succeq$ 具有传递性,即若 $r_1, r_2, r_3 \in ROLES$ 且 $r_1 \succeq r_2, r_2 \succeq r_3$,则有 $r_1 \succeq r_3$.

3.1 继承策略

为了方便主动访问社区对角色权限的管理,对角色授权时,不特意地区分本地访问权限和跨域资源的访问权限.这使得主动访问社区无需对角色之间原有的偏序关系 RH 进行修改.因此,本地角色可以通过对跨域角色的权限的继承获得跨域资源的访问权限.

于是,对于主动访问社区中的本地角色 $s \in ROLES_m$ 以及跨域角色 $t \in ROLES_{cm}$,可转换角色 $r \in ROLES_{cn}$,若 $s \succeq t$,且有 $RA(t)=r, (p,r) \in PA$,则角色 s 被赋予的跨社区访问权限为所有满足上述条件的 t 所代表的跨社区访问权限的并集,形式化地有, $assigned\_cross\_prms(s) = \{p \in PRMS_c \mid s \succeq t, RA(t) = r, (p,r) \in PA\}$.

在图 1 中,BioVO 中的角色"研究员 2"与"副研究员"满足"研究员 2 $\succeq$ 副研究员",因此,角色"研究员 2"可以继承"副研究员"对跨域资源的访问权限;同时,又由于"副研究员 $\succeq$ 学生",则由传递性可知,"研究员 2 $\succeq$ 学生",故角色"研究员 2"又可以继承"学生"对跨域资源的访问权限.

3.2 例外策略

对于主动访问社区中的某些本地角色,我们可能希望限制它所能获得的跨域资源的访问权限,例如,不允许它具有任何跨域资源的访问权限,或者不允许它继承某个跨域角色对跨域资源的访问权限.

为此,我们可以建立一个 BLOCK 列表 $LIST_{block}$,该列表的第 1 列为受限的本地角色,列表的第 2 列为跨域角色;这样,可以将 $LIST_{block}$ 看作是一个集合,它的元素为其每一行中本地角色 $s \in ROLES_m$ 与跨域角色 $t \in ROLES_{cm}$ 组成的序对(s,t),且有 $s \succeq t$.

BLOCK 列表 $LIST_{block}$ 将限制本地角色 s 对跨域角色 t 的跨域资源访问权限的继承.

现有本地角色 $s \in ROLES_m$ 以及跨域角色 $t \in ROLES_{cm}$, 若 $s \succeq t$,并且二者没有出现在 BLOCK 列表 $LIST_{block}$ 的同一行中,即 $(s,t) \notin LIST_{block}$,且有可转换角色 $r \in ROLES_{cn}$,则满足 $RA(t)=r, (p,r) \in PA$.

Table 1 BLOCK list in BioVO

表 1 BioVO 中的 BLOCK 列表示例

Local roles	Translated role
Manager	Professor
Fellow 2	Student

根据继承策略,本地角色 s 就可以继承跨域角色 t 对跨域资源的访问权限,形式化地有 $assigned\_cross\_prms(s) = \{p \in PRMS_c \mid s \succeq t, (s,t) \notin LIST_{block}, (t,r) \in RA, (p,r) \in PA\}$.

例如,在图 1 中,BioVO 中的本地角色"项目管理员"与跨域角色"教授"之间满足"项目管理员 $\succeq$ 教授".如果我们将(项目管理员,教授)加入表 1 所示的 BLOCK 列表中,那么,尽管存在"项目管理员 $\succeq$ 教授",但"项目管理员"将不能继承"教授"对跨域资源的访问权限,不过,"项目管理员"仍可以继承"副研究员"和"学生"对跨域资源的访问权限.

主动访问社区的本地继承策略使得某些用户可以利用层次 RBAC 的角色之间的关系,通过其原本拥有的角色继承某跨域角色的权限,从而获得对相应的跨域资源的访问权限.同时,主动访问社区还可以使用例外策

略,禁止某些用户通过继承策略获得某些跨域资源的访问权限.主动访问社区可以通过这些本地策略,灵活地解决非跨域角色对跨域资源的访问权限问题,并且没有增加社区间协商的工作量.

值得注意的是,主动访问社区并没有通过这些本地策略将跨域资源的访问权限直接授予用户原有的本地角色,而是将相应的跨域角色临时授予了用户,用户将使用这些临时获得的跨域角色对跨域资源进行访问.

4 被动访问社区的角色转换控制

4.1 角色转换过程

被动访问社区接到一个主动访问社区的用户对某跨域资源的访问请求后,首先,需要验证该用户所拥有的跨域角色的有效性.在一个社区授予用户某角色时,该社区要对它的这一授权进行签名;资源提供者验证社区的签名无误后,则承认该用户拥有这个角色对资源的访问权限.类似地,被动访问社区经过与主动访问社区的协商后,被动访问社区可以识别主动访问社区的签名,从而验证用户所拥有的跨域角色的有效性.

接下来,被动访问社区根据跨域角色与可转换角色之间的映射关系 RA 来确定跨域角色所对应的可转换角色.设主动访问社区的用户所拥有的跨域角色集为 $ROLES_{ucm}$,则经过被动访问社区的角色转换,该用户可以得到的可转换角色集为 $ROLES_{ucn}=\{r\in ROLES_{cn}\mid t\in ROLES_{ucm},RA(t)=r\}$.

仍然以 BioVO 和 ChemVO 的跨社区数据访问为例,BioVO 社区中的本地用户 Usr,他拥有“研究员 2”这样一个本地角色,如图 1 所示,根据 BioVO 社区中的本地继承策略,BioVO 可以授予用户 Usr 的跨域角色为“副研究员”和“学生”.ChemVO 社区根据跨域角色与可转换角色之间的映射关系 RA,可以知道 BioVO 社区的用户 Usr 此时可以获得的可转换角色为“普通资源访问者”(RA(副研究员) = 普通资源访问者)和“访客”(RA(学生)=访客).

不过,可能存在 ChemVO 中的资源 Res,“普通资源访问者”可以对其进行读写操作,而“访客”只能对其进行读操作(不能进行写操作).此时,用户 Usr 因拥有“普通资源访问者”和“访客”这两个角色,从而出现了对资源 Res 的访问权限冲突.关于这种访问权限冲突问题,我们将在第 4.2 节中进行详细讨论.

最后,被动访问社区对主动访问社区用户的请求进行安全检查.被动访问社区需检验该主动访问社区用户的请求是否安全,是否在该用户可拥有的可转换角色所允许的权限范围之内.在用户的请求通过安全检查之后,被动访问社区将可转换角色临时授予主动访问社区的用户使用,并将请求转发给该用户所请求的资源提供者.最终,被动访问社区内的资源提供者可以像对待本地用户那样,处理主动访问社区用户所发出的资源访问请求.

4.2 角色转换过程中的权限冲突解决策略

这里的权限冲突指的是,角色转换后,主动访问社区的用户可能获得多个可转换角色,但不同的角色对同一资源的访问可能存在权限的冲突.由于主动访问社区使用了继承策略,而被动访问社区并不能直接了解主动访问社区的角色层次关系,所以,被动访问社区只能按照自己社区内的角色层次关系来解决这种冲突.

设主动访问社区的用户所拥有的跨域角色集为 $ROLES_{ucm}$,经过角色转换,该用户得到的可转换角色集为 $ROLES_{ucn}=\{r_v\in ROLES_{cn}\mid r_u\in ROLES_{ucm},(r_u,r_v)\in RA\}$.若角色 $r_1,r_2\in ROLES_{ucn}$,且 $r_1\geq r_2$,则

1. 当角色 r_1 没有对资源 Res 进行访问操作 OP 的权限,而角色 r_2 有对资源 Res 进行访问操作 OP 的权限时,被动访问社区将拒绝用户对资源 Res 的访问操作 OP;
2. 当角色 r_1 有对资源 Res 进行访问操作 OP 的权限,而角色 r_2 没有对资源 Res 进行访问操作 OP 的权限时,被动访问社区将允许用户对资源 Res 的访问操作 OP.

这种解决策略充分尊重被动访问社区内部的角色层次关系,将资源访问权限的最终决定权完全交给被动访问社区,从而避免了权限冲突可能引起的安全漏洞.同时,该策略保持了双方社区的角色层次关系的透明性,既不会增加额外的协商内容,也不会增加过多的角色转换负担.该策略可以在被动访问社区对主动访问社区用户的请求进行安全检查时执行.

4.3 角色转换过程的复杂度

若设跨域角色集 $ROLES_{cm}$ 中的元素个数为 m,由本文第 3 节可知,对于一个主动访问社区中的用户,其拥有

的角色为 $r \in ROLES_m$ ($ROLES_m$ 为主动访问社区的本地角色集),则主动访问社区最多需要进行 m 次比较,即可知道 r 是否与跨域角色集中的某个跨域角色存在继承关系.再根据继承策略可确定该用户所能拥有的跨域角色集合.故确定某本地用户可拥有的跨域角色的复杂度为 $O(m)$.可设该跨域角色集合含有的元素个数为 a,显然 $a \le m$.

若设可转换角色集 $ROLES_{cn}$ 中的元素个数为 n,跨域角色到可转换角色的映射为 RA.根据 RA,对此用户获得的跨域角色集合中的每个元素最多做 n 次尝试转换,共需 $a \cdot n$ 次,即可获得可转换角色集合.因此,确定某主动访问社区用户可拥有的可转换角色的复杂度为 $O(mn)$.

综上,动态角色转换的复杂度为 $O(m)+O(mn)=O(mn)$.显然,这与双方社区所含有的角色个数并没有关系.

5 仿真实验与结果分析

在 Griden[13](原名 GridDaen)平台上,我们对本文的动态角色转换机制进行了仿真实验.

我们用两台部署在广域网上的主机来分别模拟主动访问社区和被动访问社区的数据请求代理服务器,其硬件配置为 1.7G Pentium4 CPU,512M RAM,Intel 100Mbps Ethernet Card,Apache Tomcat 5.0,MySQL 4.1;广域网上的另一台计算机作为主动访问社区中的一个终端用户,其硬件配置为 1.7G Pentium4 CPU,1G RAM,Intel 100Mbps Ethernet Card,Apache Tomcat 5.0,MySQL 4.1.

用来测试的主动访问社区和被动访问社区的本地角色数均为 1×2^{12} 个,而可转换角色集及跨域角色集的元素个数均为 1×2^{10} 个.我们为每个跨域角色集中的元素都选定了一个对应的可转换角色,因此角色转换需要处理的角色映射关系共 1×2^{10} 条.

首先,我们随机选取了主动访问社区的 1 000 个角色,模拟了用户访问其社区内部资源时的情况,计算其平均访问时间.

接下来,我们随机选取某个跨域角色,由被动访问社区将其转换为可转换角色,模拟主动访问社区用户进行跨域访问的情况.每次随机选取一个跨域角色,重复 1 000 次,计算其平均访问时间.

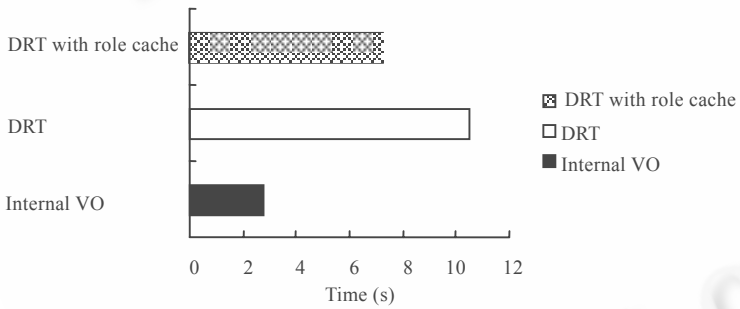

Fig.2 Simulations by different means

图 2 3 种情况下的模拟结果

最后,为了减少网络通信量,我们采用角色缓存的方法,将每个跨域角色的角色转换结果事先缓存在主动访问社区,这样,用户在取得跨域角色之后,即可获得对应的可转换角色,而不必等待被动访问社区完成角色转换.角色缓存后,每次随机选取一个跨域角色,重复 1 000 次,计算其平均访问时间.

如图 2 所示,分别为访问社区内部资源时、使用角色转换进行跨社区访问时及使用角色缓存再进行跨社区访问时,这 3 种情况下所花费的时间,其横轴代表时间,单位为秒.

从实验结果中可以看出:1) 由于社区内部的情形没有经过动态角色转换,主要花费社区内部权限检查等安全过程的时间,其耗费的时间最短;2) 在使用角色转换进行跨社区访问时,除在社区内部的时间开销外,还要考虑双方社区之间动态角色转换的交互时间,耗费的时间最长;3) 在使用角色缓存进行跨社区访问时,可以节省跨域角色与可转换角色之间动态转换的时间,但不能节省双方社区内部权限检查等安全过程所耗费的时间,所以其耗费的时间处于前两种情形之间.

这里,若考虑使用角色缓存进行跨社区访问时所消耗的只是双方社区内部的安全过程的时间,那么,可以大致认为双方社区动态角色转换的时间等于单纯使用角色转换与使用角色缓存技术进行跨社区访问的时间差.从图 2 中可以估算出这个时间差为 2~3 秒,约占整个双方跨社区访问过程(不包括数据传输过程)的时间的 20%~30%.也就是说,动态角色转换的额外开销相对还是较小的.

6 结 论

本文为跨社区的数据访问提供了一种基于协商的动态角色转换机制.该机制通过协商确立起社区间的角色映射关系,并保持了社区内部的角色层次关系对外是透明的,其协商过程及动态角色转化过程的复杂性都较低.在角色转换过程中,本文采用了分布式控制方法,由资源所属社区控制角色转换.同时,该机制对资源提供者和用户均相对透明,并没有增加他们额外的管理负担.

References:

[1] Foster I. The grid: A new infrastructure for 21st century science. Physics Today, 2002,55(2):42−47.

[2] Chervenak A, Foster I, Kesselman C, Salisbury C, Tuecke S. The data grid: Towards an architecture for the distributed management and analysis of large scientific datasets. Journal of Network and Computer Applications, 2001,23:187−200.

[3] Foster I, Kesselman C, Tuecke S. The anatomy of the grid: Enabling scalable virtual organizations. Int'l Journal of Supercomputer Applications, 2001,15(3):200−222.

[4] Ferraiolo DF, Sandhu R, Gavrila S, Kuhn DR, Chandramouli R. Proposed NIST standard for role-based ACCESS CONTROL. ACM Trans. on Information and System Security, 2001,4(3):224−274.

[5] Sandhu RS, Coyne EJ, Feinstein HL, Youman CE. Role-Based access control models. IEEE Computer, 1996,9(2):38−47.

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

[7] Kapadia A, Al-Muhtadi J, Campbell R, Mickunas D. IRBAC 2000: Secure interoperability using dynamic role translation. Technical Report, UIUCDCS-R-2000-2162, Urbana: University of Illinois, 2000.

[8] Al-Muhtadi J, Kapadia A, Campbell R, Mickunas D. The A-IRBAC 2000 model: Administrative interoperable role-based access control. Technical Report, UIUCDCS-R-2000-2163, Urbana: University of Illinois, 2000.

[9] Chen Y, Yang SB, Guo LT, Shen K. A dynamic access control scheme across multi-domains in grid environment. Journal of Computer Research and Development, 2006,43(11):1863−1869 (in Chinese with English abstract).

[10] Freudenthal E, Pesin T, Port L, Keenan E, Karamcheti V. dRBAC: Distributed role-based access control for dynamic coalition environments. In: Proc. of the 22nd Int'l Conf. on Distributed Computing Systems (ICDCS 2002). Vienna: IEEE, 2002. 411−420.

[11] Foster I, Kesselman C, Tsudik G, Tuecke S. A security architecture for computational grids. In: Proc. of the 5th ACM Conf. on Computer and Communications Security. New York: ACM Press, 1998. 83−92.

[12] Butler R, Engert D, Foster I, Kesselman C, Tuecke S, Volmer J, Welch V. A national-scale authentication infrastructure. IEEE Computer, 2000,33(12):60−66.

[13] Wu XN, Xiao N. Design and implementation of the data grid system GridDaen's security. Computer Engineering and Science, 2006, 28(2):14−16 (in Chinese with English abstract).

附中文参考文献:

[9] 陈颖,杨寿保,郭磊涛,申凯.网格环境下的一种动态跨域访问控制策略.计算机研究与发展,2006,43(11):1863−1869.

[13] 武小年,肖侬.数据网格系统 GridDaen 安全机制的设计与实现.计算机工程与科学,2006,28(2):14−16.

付长胜(1982−),男,黑龙江哈尔滨人,博士生,CCF 学生会员,主要研究领域为数据网格,网格安全.

赵英杰(1981−),男,博士生,主要研究领域为数据网格.

肖 侬(1969−),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为分布计算,网格计算.

陈涛(1982−),女,博士生,主要研究领域为网络存储,网格监控.