ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.18, No.8, August 2007, pp.1958−1967
DOI: 10.1360/jos181958

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

一种基于信任度的自组安全互操作方法*

刘 伟[1,2+], 蔡嘉勇[1,2], 贺也平[1]

[1](中国科学院 软件研究所 基础软件国家工程研究中心,北京 100080)

[2](中国科学院 研究生院,北京 100049)

A Trustworthiness Based Ad-Hoc Secure Interoperation Method

LIU Wei[1,2+], CAI Jia-Yong[1,2], HE Ye-Ping[1]

[1](National Engineering Research Center for Fundamental Software, Institute of Software, The Chinese Academy of Sciences, Beijing 100080, China)

[2](Graduate University, The Chinese Academy of Sciences, Beijing 100049, China)

+ Corresponding author: Phn: +86-10-62661900, E-mail: liuwei04@ios.cn, http://www.iscas.ac.cn

Liu W, Cai JY, He YP. A trustworthiness based ad-hoc secure interoperation method. *Journal of Software*, 2007,18(8):1958−1967. http://www.jos.org.cn/1000-9825/18/1958.htm

Abstract: A trustworthiness-based ad-hoc secure interoperation method is proposed, in which the concept of trustworthiness is introduced to describe the probability of proper collaboration. The trustworthiness of an autonomic domain on a user is decided jointly by direct experiences of interactions and other domains' assessments on the user. Only the users who satisfy the requirements of target domains' trust policies have the privileges to access entry roles. Records of a user's malicious actions will decrease his trustworthiness and then accordingly reduce his privileges. Target domain uses weighted majority algorithm to update recommender's trustworthiness, which is reduced by unfair ratings. Experimental results show that this method can effectively resist cheating and malicious actions.

Key words: authorization; ad-hoc collaboration; secure interoperation; trustworthiness; weighted majority algorithm

摘 要: 提出了基于信任度的自组安全互操作方法,引入信任度描述自治域和用户正确参与协作的概率.自治域对用户的信任度由二者的直接交互经验以及其他域对用户的评价共同决定,满足信任策略要求的用户允许执行角色.用户的恶意历史行为将会降低其信任度,从而影响执行角色的范围.自治域对其他域的信任度由对用户的评价与直接经验的偏差根据加权主要算法反馈更新.自治域的恶意评价影响其推荐信息的可信程度.实验结果表明,该方法能够有效地抵御欺骗和恶意行为.

关键词: 授权;自组协同;安全互操作;信任度;加权主要算法

中图法分类号: TP393 **文献标识码**: A

随着Internet的发展,有越来越多的组织自发地联合起来协同工作.这种协同趋势不但影响到军事领域,例如

* Supported by the Science-Technology Project of the National "Tenth Five-Year-Plan" of China under Grant No.2005BA113A02 (国家"十五"攻关计划); the Graduate Innovation Grant of the Chinese Academy of Sciences (中国科学院研究生创新资金)

Received 2007-03-01; Accepted 2007-05-31

联合演习,也涉及商业领域,例如合作医疗.在协同环境中,组织内部独立管理,也称为自治域;通过共享资源和服务及组织之间的相互操作实现协同.在商业环境中,基于角色的访问控制(role-based access control,简称RBAC)[1]成为授权管理的主要方式.在RBAC中,角色与权限相关联,用户被授予角色从而获得相应权限.由于角色和权限的关系相对固定,管理员根据组织结构定义角色,减轻管理负担.近年来,实施RBAC策略的自治域之间安全互操作成为授权管理领域的研究热点之一.

协同关系按照互操作级别由高到低分为 3 类[2]:联合型、松散型和自组型.在前两类协同中,自治域之间相互熟悉,存在依赖或信任关系,适合长期稳定的协作;自组型协同结构松散,允许自治域动态加入或退出协同.

虽然传统的安全机制能够在单域范围内实施有效授权,但在自组协同环境中,各自治域采用安全机制不尽相同,实施安全策略存在差异,很难形成公认的可信第三方,共享导致非授权访问的可能性大为增加,授权管理面临更多的安全威胁.

自组协同环境中,自治域对用户授权必须基于本地安全策略.参考中国墙[3]安全策略的基本思想,Shehab等人[4,5]根据用户的访问历史和本地安全策略独立实施授权决策,具有可扩展、支持职责隔离等优点,其安全性基于以下假设:(1) 用户的访问历史是真实的,不存在伪造和篡改的可能;(2) 用户的行为符合安全策略要求,不会执行恶意操作.在实际协同中,自治域之间并不相互了解,不能排除存在恶意协作域和恶意用户的可能性,该方案中互操作的安全性无法保证.

本文提出了基于信任度的自组安全互操作方法,自治域对用户的授权不仅根据用户的访问历史,还依赖于对用户的信任程度.用户提出的访问请求中包含访问历史和推荐信息,前者反映用户执行角色的操作记录,后者反映其他域对用户行为的评价.自治域利用与用户的直接交互经验和推荐信息综合计算用户的信任度,满足本地安全策略要求的用户才能执行角色.用户的信任度与推荐信息紧密相关,可能受到恶意评价的影响.推荐信息与直接交互经验之间存在差异.我们使用基于加权主要算法的推荐评估方法更新自治域的信任度,减少恶意评价对用户信任度的影响.

本文第 1 节介绍相关工作.第 2 节描述用户和自治域的信任度计算方式及基于信任度的安全互操作方法.第 3 节进行仿真实验,并与其他方案对比.最后总结全文.

1 相关工作

研究人员提出通过访问映射实现异构系统之间的互操作,最初应用于数据库领域.Gong等人[6,7]通过安全级别交互映射实现多级安全数据库之间的互操作,解决存在的冲突,提供最大安全互操作方案,但该方案属于NP完全的集中式算法,存在公平性问题.Dawson等人[8]讨论在实施基于格的访问控制策略的异构系统间建立安全互操作的框架,存在策略中介,具有全局视角以实现策略比较、映射等操作.上述工作的主要缺点是可扩展性较差,成员之间要求保持长期、稳定的协同关系,不适合动态变化的自组协同.另外,基于格的访问控制策略多用于军事环境中,在商业环境中应用较少.

Bonatti等人[9]提出了基于代数的访问控制策略融合框架,在保持各部分策略独立性的前提下,实施对不同策略的融合.该方案同样使用集中式算法实施策略描述、转换等操作.Shafiq等人[10]研究实施RBAC策略的多个自治域之间的安全互操作问题,通过整合多个RBAC策略形成全局策略,关键是解决策略冲突,使用基于整数规划的冲突评价方法,提出最大跨域角色访问的优化标准.文献[11]中提出了基于角色的分布式信任管理解决方案,重点解决动态联合授权以及基于属性的委托授权,定义访问控制协议及执行体系,包括安全策略的协商、信任凭证的颁发、一致性验证等内容.基于信任管理的解决方案要求协同环境中存在可信第三方.上述研究适用于联合型及松散型协同,因为参与协同的自治域熟悉其他域的安全策略,同时全局的算法实现策略融合、冲突解决和协同管理.

Shehab等人[4,5]提出了自组协同的安全互操作方法,并应用于协同工作流系统[12].该方法采用类似于中国墙安全策略的思想,主体的访问请求包含访问历史,其他域根据访问历史确定是否实施授权.该方案根据本地安全策略独立实施授权决策,具有可扩展性好、支持职责隔离等优点.当存在恶意域或恶意主体时,互操作的安全性

被破坏.访问历史只能记录主体的执行历史,没有反映对主体的评价,无法抵御主体的恶意行为.恶意域也可以通过伪造访问历史欺骗协作域,影响互操作的有效性.

在未知环境中,信任代替主体标识成为授权的主要依据.TrustBAC[13]实现基于信任级别的访问控制,模型根据用户的凭证、历史记录和推荐信息等内容将用户映射到某个信任级别,信任级别与角色关联,用户从而担任相应角色并执行对应权限.通过监控用户信任级别的变化,模型无须调整用户的角色及访问权限,适用于开放系统(例如数字图书馆).与本文相比,TrustBAC没有判断推荐信息的可信程度,无法抵御恶意推荐的影响,也不涉及多域间的互操作.

根据不同的研究背景,研究人员提出若干信任评估模型.Beth等人[14]提出一个基于经验和概率统计的信任模型,给出经验推荐所引出的信任度推导和综合计算公式,应用于开放网络的安全认证.Abdul-Rahman等人[15]认为信任是非理性的,包括具体内容和程度划分两方面,提出分布式信任评估模型,将信任关系分为直接信任和推荐信任,采用离散数值度量信任关系.Jøsang等人[16]提出了事实空间和观念空间描述和度量信任关系,提供了主观逻辑算子用于信任度的推导和综合计算.信任评估模型研究信任的描述、度量、传递和综合等内容,对信任关系的动态变化,尤其是信任关系的反馈更新等方面研究存在不足,无法有效抵御恶意推荐信息.IFA[17]通过递归过滤的方法减少恶意推荐的影响,评价者的信息超出合理范围被视为恶意推荐,将不参与信誉值的计算.通过对合理范围的调节,IFA能够抵御恶意推荐.与本文的方案相比,IFA对恶意推荐的过滤导致信誉值振荡幅度较大,当推荐者数量较多时计算开销过大.

2 基于信任度的自组安全互操作

通过要求实施非RBAC策略的自治域在加入协同时提供对应的RBAC策略[18],我们假定自组协同环境中所有域实施RBAC策略.域i的RBAC策略表示为有向图[5]$G_i=(V_i,A_i)$,其中,顶点集合V_i代表角色,有向边集合A_i反映角色之间的支配关系,支配关系用符号 f 表示.例如,$r_1,r_2\in V_i$且 r_1 f r_2,则$(r_1,r_2)\in A_i$.具有n个域$G_i=(V_i,A_i)$ $(i=1,\ldots,n)$的自组协同环境通过允许访问集合F实现互操作,表示为有向图之间的有向边集合.角色映射$(u_1,v_1)\in F,u_1\in V_i,v_1\in V_j,i\neq j$,表示允许担任$V_i$中角色$u_1$的用户执行$V_j$中角色$v_1$.此外,限制访问集合$R$定义禁止执行的互操作,例如,$(u_2,v_2)\in R,u_2\in V_i,v_2\in V_j,i\neq j$,表示禁止担任$V_i$中角色$u_2$的用户执行$V_j$中角色$v_2$.$F$和$R$由自治域根据协同需要独立设置,限制访问优先级高于允许访问.

给定$G_i=(V_i,A_i),i=1,\ldots,n$,允许访问集合$F$和限制访问集合$R$.当满足下列条件时,我们称互操作$Q=(\cup_{i=1}^{n}V_i,A_Q),A_Q\subseteq(\cup_{i=1}^{n}A_i\cup F)$是安全的.

(1) $A_Q\cap R=\varnothing$;

(2) $\forall m,n\in V_i,(m,n)$在A_i中是合法的,当且仅当(m,n)在A_Q中是合法的.

上述条件称为安全互操作的两个原则[7]:安全性原则和自治性原则.前者要求任何单个自治域中被禁止的操作在安全互操作中必须被禁止;后者要求任何在单个自治域中被许可的操作在安全互操作中必须被许可,其中,合法性是指不违反相关规则,例如角色间支配关系的偏序性.

2.1 访问路径

自组协同具有松散的组织结构,自治域可能动态加入或退出协同,只了解与本域相关的互操作,并不了解全局的访问控制要求及目标.文献[5]提出了自组安全互操作方案,根据用户的访问请求及本地策略独立实施授权决策,访问请求包含用户执行角色的历史信息.用户所属域为初始域,当前正在访问的域为当前域,希望访问的域为目标域.我们首先定义访问路径描述用户访问角色的历史记录.

定义 1(访问路径)[5]. 使用r_{Status}^{Domain}表示角色,其中,$Status\in\{(E)ntry,e(X)it\}$表示域$Domain$的入口和出口角色,访问路径$P$是用户$u$从起始域$Home$到当前域$Current$的角色执行序列$P=\{r_{start},\ldots,r_{X_1}^{Home},\ldots,r_{E_1}^{Current},\ldots,r_{X_1}^{Current}\}$,其中,$r_{start}$是用户会话的起始角色.

如图 1 所示,访问路径$P_u=\{r_{h2},r_{h3},r_{c1},r_{c3}\}$表示在会话中$u$依次执行起始角色$r_{h2}$,$Home$出口角色$r_{h3}$和$Current$

入口、出口角色r_{c1}和r_{c3}.访问路径记录用户执行角色的历史信息,不恰当的访问路径可能破坏安全性原则.例如,u继续访问r_{t1},r_{t2},r_{h1},形成 $P'_u=\{r_{h2},r_{h3},r_{c1},r_{c3},r_{t1},r_{t2},r_{h1}\}$.由于在$Home$中$r_{h1}$支配$r_{h2}$,通过$F=\{(r_{h3},r_{c1}),(r_{c3},r_{t1}),(r_{t2},r_{h1})\}$实现互操作,担任$r_{h2}$的用户通过 P'_u 可以执行r_{h1},即 r_{h2} f r_{h1},违反自治性原则.为了防止访问路径导致互操作安全性的破坏,我们给出访问路径一致性的定义.

定义 2(访问路径的一致性). 访问路径$P=(r_1,r_2,r_n)$,其中,$1\le i<j\le n$表示r_i先于r_j执行.用$Domain(r)$表示角色r所属的自治域.当满足以下条件时,称P是一致性的:

(1) $\forall(i<j)\wedge(r_i,r_j\in P)\wedge(Domain(r_i)=Domain(r_j))\rightarrow(r_i\ \mathrm{f}\ r_j)$;

(2) $\forall(r_i,r_{i+1}\in P)\wedge(Domain(r_i)\neq Domain(r_{i+1}))\rightarrow(r_i,r_{i+1})\in F$;

(3) $\forall(i<j)\wedge(r_i,r_j\in P)\rightarrow(r_i,r_j)\notin R$.

条件(1)限定访问路径上属于同一自治域的角色之间满足支配关系,防止互操作引起的策略冲突;条件(2)和条件(3)分别满足允许访问集合 F 和限制访集合 R 的要求.

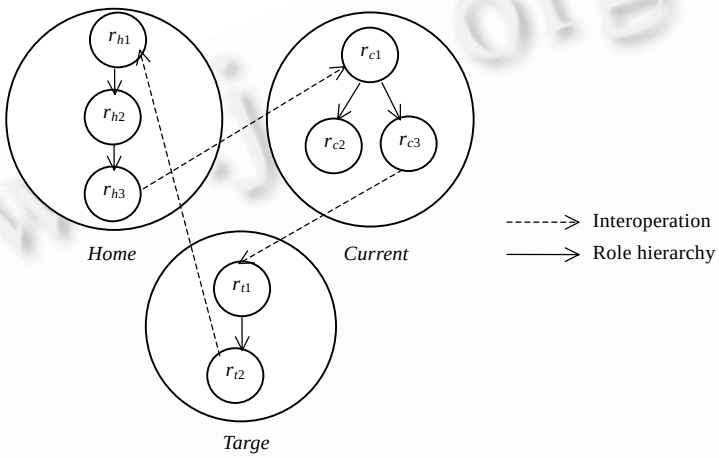


Fig.1 Access path example

图 1 访问路径示例

定理 1. 满足一致性的访问路径 P 构成的互操作 Q 是安全的.

证明:给定互操作 $Q=(\cup_{i=1}^{n}V_i,A_Q)$,其中,$A_Q\subseteq(\cup_{i=1}^{n}A_i\cup F)$,存在访问路径集合$PSET=\{P_1,\ldots,P_t\}$描述$A_Q$的传递闭包,对于$(m,n),(n,q)\in A_Q$,有$P_1=(m,n),P_2=(n,q),P_3=(m,n,q)$与其对应.证明$PSET$的所有元素是一致的则$Q$是安全的即可.对于任意$(r_i,r_j)\in A_Q,i<j$,至少有 1 条存在访问路径$P$包含$r_i,r_j\in P$.由条件(3)可知$(r_i,r_j)\notin R$,即$A_Q\cap R=\varnothing$满足安全性原则.下面证明自治性原则的充分性.用反证法,如果$m,n\in V_i,(m,n)$在A_i中是合法的,而(n,m)在A_Q中是合法的,必定存在$P=\{n,\ldots,m\}\in PSET,n$到$m$的访问路径经过其他域$V_j(i\neq j)$.由条件(1)可知,$P$是不一致的,即$P\notin PSET$,存在矛盾.必要性:$\forall m,n\in V_i,(m,n)$在$A_Q$中是合法的,存在$P=\{n,\ldots,m\}\in PSET$.如果该路径上所有角色属于同一自治域$V_i$,则$(m,n)$在$A_i$中显然合法;如果属于不同自治域,则$P$经过其他域$V_j(i\neq j)$.由条件(2)和条件(3)可知,$(m,n)$在$A_i$中是合法的. □

在文献[5]提出的自组安全互操作方案中,当用户需要执行目标域角色时,当前域连接已有的访问路径和本域内的执行序列,形成访问请求提交给目标域.根据访问路径,目标域独立实施授权决策.在此过程中,访问路径的真实性至关重要.该方案假设所有自治域都是可信的,从而保证访问路径的真实性.在实际协作中,上述假设的存在并不合理,因为恶意域可能伪造或篡改访问路径而影响授权.另外,访问路径仅仅描述执行角色的事件,并不包含是否正确执行角色的结论.恶意用户可能执行破坏性操作,而相关域则无法将该信息传递给其他自治域.在未知环境中,信任成为授权的主要依据.我们引入信任度描述自治域及用户正确参与协同的程度.

2.2 用户的信任度

自治域对用户的信任度依赖以下信息:(1) 自治域与用户的直接交互经验,用户正常访问本地资源的次数越多,则执行破坏性操作的可能性越小,相应的信任度也就越高;(2) 用户在其他域中执行角色的评价,用户正常参与其他域中协作的次数越多,则在本域中正确协作的可能性越高,信任度也就越高.

2.2.1 直接信任

用户与自治域的正常交互越多,表明其正确参与协同的可能性越大,后继的恶意行为概率越小.我们对一次交互时间段$[t_0,t_n]$内用户u担任自治域T中角色r执行的m个事件建模来描述T对u的直接信任,即对u正确访问资源的概率判断.将$[t_0,t_n]$分为n个间隔,每个间隔单独定义权重w_i,反映间隔对直接信任的影响程度,例如工作时间的权重较大.T 通过本地信任策略将系统事件分为正事件集Π和负事件集N,对应事件的信任度分别为正、负值,以表示信任度的增加与减少.假设用 e_k^i 表示在第 i 个间隔内的第 k 个事件,$v_k^i \in [-1,1]$ 表示该事件的信任值.如果 $e_k^i \in \mathrm{P}$,则 $v_k^i \in (0,1]$;反之,$e_k^i \in \mathrm{N}$,则 $v_k^i \in [-1,0)$,$|v_k^i|$ 表示对信任度的影响程度.例如,*guest* 角色直接访问密码文件的事件e_{pass}意味着非正常行为,管理员在本地信任策略中设置其信任值$v_{pass}=-1$.自治域与用户之间没有直接交互经验,则直接信任用符号$\perp$表示.

间隔 i 中,信任度 $I_i=\begin{cases}\sum_{k=1}^{m} v_k^i \Big/ \sum_{k=1}^{m} |v_k^i|, & \text{if } \exists e_k^i \in [t_{i-1},t_i] \\ \perp, & \text{otherwise}\end{cases}$,$T$ 对 u 的直接信任 $E_u^T=\begin{cases}\sum_{i=1}^{n} w_i \times I_i \Big/ \sum_{i=1}^{n} w_i, & \text{if } \exists I_i \neq \perp \\ \perp, & \text{otherwise}\end{cases}$.

2.2.2 推荐信任

用户完成操作后,当前域将与用户的直接交互经验作为推荐信息传递给目标域,表示用户在当前域的信任参考.用户行为可能随时间发生变化,当前越近的推荐信息的权重应该越高,这种方式与日常生活中的推荐行为相一致.我们定义持续因子$\lambda \in [0,1]$控制推荐信息随时间的衰减程度.$\lambda=0$ 表示只有最近的推荐信息有效;$\lambda=1$ 表示不随时间衰减.假设域 i 在时间周期 t 内的直接信任为 $E_{u,(t)}^T$,则周期 $t+1$ 的推荐信息为 $\lambda \times E_{u,(t)}^T + E_{u,(t+1)}^T$.目标域对用户的推荐信任由推荐信息和推荐域的可信度共同决定.给定用户u的访问路径$P_u=\{r_1,r_2,\ldots,r_n\}$,经过域$D_u=\{D_1,D_2,\ldots,D_m\}$,$m \le n$,对应的可信度分别为$t_1,t_2,\ldots,t_m$,提供推荐信息分别为$re_1,re_2,\ldots,re_m$.自治域对用户的评价标准可能存在差异,在加入协同时要求采用统一描述方式,例如,定义推荐信息$re=\{excellent,good,average,bad,mediocre\}$,目标域通过本地信任策略定义推荐信息的影响值$v \in [-1,1]$,例如,当$re_i=excellent$时,设置$v_i=0.8$;当$re_j=bad$时,设置$v_j=-0.4$.根据推荐信息,目标域$T$计算$u$的推荐信任为

$$R_u^T=\sum_{k=1}^{m} v_k \times t_k \Big/ \sum_{k=1}^{m} t_k .$$

2.2.3 信任度

我们使用 $Trust_u^T$ 描述目标域 T 对用户 u 正确执行角色的行为判断,包括直接信任 E_u^T 和推荐信任 R_u^T.其中,E_u^T 是由 T 与 u 的直接交互经验计算获得的,R_u^T 是由访问路径上的自治域向 T 提交关于 u 的评价综合计算获得的.T 对 u 的信任度表示为

$$Trust_u^T=\begin{cases} w_E \times E_u^T + w_R \times R_u^T, & \text{if } E_u^T, R_u^T \neq \perp \\ \perp, & \text{otherwise}\end{cases}, \quad w_E, w_R \in [0,1] \text{且} w_E+w_R=1.$$

其中,w_E,w_R反映直接信任与推荐信任的权重,由自治域通过本地信任策略定义.可知 $Trust_u^T \in [-1,1] \cup \{\perp\}$,信任度值越大,则表示 T 认为 u 正确担任角色的可能性越高.

用户的推荐信任由推荐信息以及推荐域的信任度共同决定,自组协同环境可能存在恶意协作域,提供不公正的推荐信息评价用户.目标域通过修改推荐域的信任度来减少恶意推荐的影响.此外,用户的信任度也对所属域的信任度产生影响.所属同一起始域的多个用户的恶意行为意味着该域其他用户正确参与协作的可能性较小.因此,自治域信任度的设置、调整及演化成为我们的重要研究内容.

2.3 自治域的信任度

在自组协同过程中,每个自治域需要维护信任度列表,保存其他协作域的信任度计算推荐信任.每次与用户直接交互后,自治域根据推荐信息的准确性反馈更新协作域的信任度,尽可能真实地反映其他域的协作意愿.加权主要算法(weighted majority algorithm,简称WMA)[19]是机器学习领域的重要算法之一,实现基于专家建议的预测.主算法(也称为学习算法)根据多个专家算法的预测对某事件进行判断,期望出现错误的机率最小.该算法维护专家算法的权重列表,通过专家算法加权输出进行预测,并根据预测值和实际值的差异更新权重.本文使用该算法实现域信任度的调整及更新.自组协同中对应于WMA中的事件判断用户执行角色的正确性,每个推荐域作为WMA中的一种专家算法,其输出为推荐信息,域的信任度则等价于专家算法的权重.目标域作为WMA中的主算法,推荐信任是加权后的专家算法输出,并作为事件的预测值.根据推荐信任与用户直接信任之间存在的差异,目标域使用WMA调整推荐域的信任度.

访问请求包含访问路径上其他域对用户的推荐信息,也包含对执行角色事件的评价.这些独立评价X是离散型随机变量,具有$r(r\geq 2)$个可能状态$x_1,\ldots,x_r$,对X的多重采样服从Dirichlet分布[20].这里,定义变量Θ的取值$\theta_1,\ldots,\theta_r$对应状态出现的概率,则$p(\theta|\xi)$表示给定背景知识ξ下X的概率密度函数.我们使用X_i表示第i次观察值,其集合为$D=\{X_1=x_1,\ldots,X_n=x_n\}$.因此,目标域对用户执行本域角色事件的判断转化为通过$p(\theta|\xi)$计算$p(X_{n+1}|D,\xi)$.X的先验分布密度函数为

$$p(\theta\mid\xi)=Dir(\theta\mid\alpha_1,\ldots,\alpha_r)=\frac{\Gamma(\sum_{k=1}^{r}\alpha_k)}{\prod_{k=1}^{r}\Gamma(\alpha_k)}\prod_{k=1}^{r}\theta_k^{\alpha_k-1},$$

其中$\alpha_k>0,k=1,\ldots,r$表示相应统计数量.根据贝叶斯理论可知,$p(\theta|D,\xi)=Dir(\theta|\alpha_1+n_1,\ldots,\alpha_r+n_r)$,其中,$n_k(k=1,\ldots,r)$是$D$的充分统计量$N=\{n_1,\ldots,n_r\}$中的对应元素,记录$D$中$X=x_k$出现的次数.给定历史经验集合$D$和背景知识$\xi$,下次评价观察值为

$$p(X_{n+1}=x_k\mid D,\xi)=\int\theta_k Dir(\theta\mid\alpha_1+n_1,\ldots,\alpha_r+n_r)\mathrm{d}\theta=(\alpha_k+n_k)/(\alpha+n).$$

我们使用WMA更新推荐域的信任度,分为两个步骤:(1) 根据历史交互经验和推荐信息(专家算法的输出),目标域对用户执行角色进行判断,给出事件的预测值;(2) 用户访问目标域后,目标域获得与用户的直接交互经验并计算事件的真实值.目标域根据二者之间存在的差异调整推荐域的信任度.假定访问路径经过m个域,推荐信息分别为$R_i=\{\alpha_{i,1}+n_{i,1},\ldots,\alpha_{i,r}+n_{i,r}\},i=(1,\ldots,m)$,这里,目标域无法区分观察值$\{\alpha_{i,1},\ldots,\alpha_{i,r}\}$和充分统计量$N_i=\{n_{i,1},\ldots,n_{i,r}\}$.推荐信息并非完全可信,目标域根据维护的信任度列表$t_1,\ldots,t_m$加权,将推荐信息R_i转换为等价采样,其充分统计量为$N_i'=R_i\times t_i/s$,其中,$s=\sum_{i=1}^{m}t_i$.历史交互经验和推荐信息的充分统计量为$N_f=N+\sum N_i'$,可知预测观察值的后验分布的概率密度函数为

$$p(\theta_f\mid D_f,\xi)=Dir(\theta_f\mid\alpha_1+n_1+\sum(\alpha_{i,1}+n_{i,1})\times t_i/s,\ldots,\alpha_r+n_r+\sum(\alpha_{i,r}+n_{i,r})\times t_i/s).$$

在用户执行角色后,目标域获得与用户的真实交互经验,在先验分布的基础上增加观测值$\alpha'=(\alpha_1',\ldots,\alpha_r')$,其中,$\alpha_k'\in\{0,1\},k=1,\ldots,r$且$\sum\alpha_k'=1$,表示此次交互中目标域对用户行为的评价.真实经验和根据推荐信息得到的期望值之间存在差异,我们使用WMA根据差异分别更新推荐域的信任度.每个域D_i使用推荐算法$E(\theta_i)$,即推荐信息R_i中关于分布$p(\theta_i|D_i,\xi_i)$的θ_i期望.目标域使用主算法$E(\theta_m)$,即关于分布$p(\theta_m|D_m,\xi)$的θ_m期望.在WMA的更新步骤中,目标域根据直接交互经验的关于$p(\theta|D,\xi)$的θ期望获得正确预测值ρ.更新后,推荐域D_i的信任度$t_i'=F\times t_i$,其中,F满足以下条件:$\beta^{|E(\theta_i)-\rho|}\leq F\leq 1-(1-\beta)|E(\theta_i)-\rho|,\beta\in[0,1]$表示域信任度的更新幅度.关于$F$的定义超出了本文的讨论范围,为了计算方便,我们将其定义为[21]

$$F=1-(1-\beta)\frac{|E(\theta_i)-E(\theta)|}{\sqrt{2}},$$

其中,$E(\theta_i)=(x_1,\ldots,x_r)$和$E(\theta)=(y_1,\ldots,y_r)$是$r$维向量,$|E(\theta_i)-E(\theta)|=\sqrt{\sum_{i=1}^{r}(x_i-y_i)^2}$.

2.4 基于信任度的自组安全互操作

自组安全互操作的基本思想是,当用户完成当前域的操作后提出访问请求,由当前域授予访问凭证,其中包含用户的访问路径及相关评价.用户将访问凭证提交给目标域,后者首先验证访问路径的一致性,不满足一致性要求的访问请求被拒绝.除了访问路径以外,授权依赖用户的信任度,由目标域根据访问凭证计算而获得.用户的信任度不满足访问目标域入口角色的信任度要求,则目标域拒绝授权;反之则允许,并在用户完成该域的操作后由目标域根据基于 WMA 的推荐评估方法更新推荐域的信任度.

访问凭证是授权决策的重要依据,需要加以保护,防止伪造和篡改.我们假定自治域D_i拥有公钥d_i和私钥e_i,在加入自组协同时提供.假设D_i从访问路径中前一个域D_{i-1}获得的访问凭证 $RC_{i-1}=(r_E^i,P_{i-1},E_{i-1},PS_{i-1},PE_{i-1})$,其中,$r_E^i$ 是域D_i的入口角色; $P_{i-1}=\{r_{start},...,r_X^1,...,r_E^{i-1},...,r_X^{i-1}\}$ 是D_{i-1}之前的访问路径,$r_E^k,r_X^k,k=1,...,i-1$,分别是域D_k的入口和出口角色;E_{i-1}是访问路径经过域的推荐信息,即对u执行本域角色的评价,PS_{i-1}是D_{i-1}使用e_{i-1}对访问路径的签名,PE_{i-1}是使用e_{i-1}对推荐信息的签名,表示为

$$PS_i=\begin{cases}seed, & \text{if } i=0\\ sign_{e_i}(PS_{i-1}\oplus hash(r_E^i \text{ o} r_X^i \text{ o} i+1)), & \text{if } i\ge 1\end{cases},\quad PE_i=\begin{cases}seed, & \text{if } i=0\\ sign_{e_i}(PE_{i-1}\oplus E_u^i), & \text{if } i\ge 1\end{cases},$$

其中,$sign$是签名函数,符号⊕表示按位与操作,符号 o 表示连接操作,$hash$是散列函数.用户u完成域D_i中的操作后提出访问请求.D_i根据RC_{i-1}、访问路径 $P=\{r_E^i,...,r_X^i\}$ 和与u的交互经验 E_u^i 产生新的访问凭证:

$$RC_i=(r_E^{i+1},P_i,E_i,PS_i,PE_i),$$

其中,r_E^{i+1} 是D_{i+1}中用户请求的入口角色, $P_i=P_{i-1}\text{ o}P$, $E_i=E_{i-1}\text{ o}E_u^i$.

当接收到RC_i后,域D_{i+1}根据算法 1 进行授权决策.

算法 1. 用户向域D_{i+1}提交访问凭证 $RC_i=(r_E^{i+1},P_i,E_i,PS_i,PE_i)$,域$D_{i+1}$根据本地信任策略作出授权决策.

输入:访问凭证RC_i.

输出:是否允许访问.

函数:$order(r)$返回角色 r 在访问路径中的序号;

$need_trust(r)$返回本地信任策略T,定义执行角色 r 所需信任度.

1. $k=i+1$; $t_1=PS_{k-1}$; $t_2=PE_{k-1}$;
2. while $k>1$ do
3. $k=k-1$;
4. $t_1=sign_{d_k}(t_1)\oplus hash(r_E^k \text{ o} r_X^k \text{ o}(k+1))$;
5. $t_2=sign_{d_{k-1}}(t_2)\oplus E_u^{k-1}$;
6. done
7. if $t_1\ne t_2$ or $t_2\ne seed$ return FALSE;
8. if $(r_X^i,r_E^{i+1})\notin F$ return FALSE;
9. for r in P_i do
10. if $(r,r_E^{i+1})\in R_{i+1}$ return FALSE;
11. if ($Domain(r)=i+1$) and (r_E^{i+1} o r) return FALSE;
12. done
13. $Trust_u^{i+1}=(w_E^{i+1}\times E_u^{i+1}+w_R^{i+1}\times R_u^{i+1})/(w_E^{i+1}+w_R^{i+1})$
14. if $Trust_u^{i+1}<need\_trust(r_E^{i+1})$ return FALSE;
15. return TRUE.

算法的正确性由以下定理决定:

引理 1. 单个域内部的访问路径是一致的.

证明:给定访问路径$P=\{r_1,r_2,\ldots,r_n\}$且$r_1,r_2,\ldots,r_n\in V_i$,由访问路径的定义可知,$\forall(i<j)\wedge(r_i,r_j\in P)\rightarrow r_i\ \mathrm{f}\ r_j$,满足一致性条件(1),而条件(2)讨论不同域间的角色关系,显然满足.任意限制访问关系$(u,v)\in R$,由$Domain(u)\neq Domain(v)$可得u,v不属于同一域,$(u,v)\notin A_i,i=1,\ldots,n$,即$A_i\cap R=\varnothing$满足条件(3). □

定理 2. 算法 1 输出的授权决策是安全的.

证明:由公钥加密的基本理论可知,签名函数满足性质$sign_{d_k}(sign_{e_k}(M))=M,k=0,\ldots,i$,$D_{i+1}$使用算法根据访问凭证$RC_i$递归验证签名的有效性.如果$RC_i$中$PS_i$和$PE_i$是有效的,则保证访问路径和推荐信息的有效性.根据定理 1,下面证明算法授权的访问路径满足一致性要求.对访问路径经过自治域的数量n使用归纳法.显然,$n=1$时,即访问路径$P_1=\{r_{start},r',...,r'',r_X^1\}$表示在单个范围内.由引理 1 可知,$P_1$是一致的.假设$n=i$时访问路径$P_i$是一致的,下面证明当$n=i+1$时,算法 1 构成的访问路径$P_{i+1}$同样满足一致性要求.$P_i=\{r_{start},r',...,r_E^i,...,r_i',r_X^i\}$经过的域为$D=\{D_1,\ldots,D_i\}$.由算法第 8 行可知,$(r_X^i,r_E^{i+1})\in F$满足条件(2).由算法第 10 行可知,$\forall r\in P_i,(r,r_E^{i+1})\notin R$,满足条件(3).分两种情况加以讨论:(1) $D_{i+1}\in D$,由算法第 11 行可知,$\forall r\in P_i,(Domain(r)=Domain(r_E^{i+1}))\rightarrow(r_E^{i+1}\circ\ r)$,则$r\ \mathrm{f}\ r_E^{i+1}$或二者不可比较,后者根据访问路径定义可得$r\ \mathrm{f}\ r_E^{i+1}$,满足条件(1);(2) $D_{i+1}\notin D$,显然满足条件(1).因此,算法输出的授权决策是安全的. □

自组协同环境中的恶意行为的主体包括用户和协作域.用户的恶意行为记录导致其信任度下降,从而影响能够执行的入口角色.目标域管理员通过安全策略设置不同的入口角色的信任度要求,实现灵活控制.例如,入口角色访问教授对用户的信任度高于访问学生的相应要求.本文主要讨论协作域与目标域的推荐关系交互,协作域可能提交不符合用户实际交互行为的评价信息,目标域通过调整相应的信任度减少恶意推荐对用户信任度的影响,同时,协作域的信任度也同样影响该域后续用户的信任度,增加其恶意行为的成本.

在计算协作域和用户的信任度时,目标域需要维护两个列表.在加入自组协同环境时,要求协作域的名称唯一,用户名采用与信任管理[11]类似的方法表示为"域名.用户名",例如,目标域将域D的用户*tester*记作*D.tester*,确保命名空间的一致性.当协作域和用户数量较多时,目标域定义当信任度衰减小于缺省值时,将该域或用户的条目从列表中删除,以减少存储消耗.

3 实验结果及分析

我们通过实验来初步验证基于信任度的自组安全互操作方法的有效性及合理性,并比较在存在恶意协作域的前提下,使用不同算法处理时用户信任度估计的演化情况.

实验场景模拟 50 个自治域参与的自组协同环境.协作域M具有随机选择的 6 个推荐域$D_1,...,D_6$,共进行 20 次会话,每次会话包含 10 次协作事务.推荐信息是推荐域与用户的直接交互信息,各域的评价标准存在差异.我们将推荐域对用户的评价统一为 5 种,见表 1.例如,推荐信息$re=(1,3,2,0,0)$表示用户执行 6 次协作事务,评价为 1 次优秀、3 次较好和 2 次一般.我们假定用户在一次会话中协作意愿保持不变,用户行为随时间变化,不同会话中用户的真实信任度发生变化.在会话s中,用户执行的真实信任度为t_s.在$s+1$会话中,真实信任度随机选择以下 3 种:t_s+c,t_s和t_s-c,其中,c反映信任度的波动程度.这种变化也可以模拟自治域的信任度评价存在的差异,恶意协作域可能对用户进行不公正评价.假设用户在当前会话中的信任度为x,推荐域对其评价分为 3 种类型:(1) 正确评价,即评价$y=x$与实际经验相符;(2) 提高评价,即评价$y=x+u\times(1-|x|)$高于实际值;(3) 降低评价,即评价$y=\begin{cases}(1-u)\times x, & \text{if } x\geq 0\\ -1-(1-u)\times x, & \text{if } x<0\end{cases}$低于实际值.后两种评价都属于不公正评价,其中,$u(0<u<1)$反映不公正评价的程度.

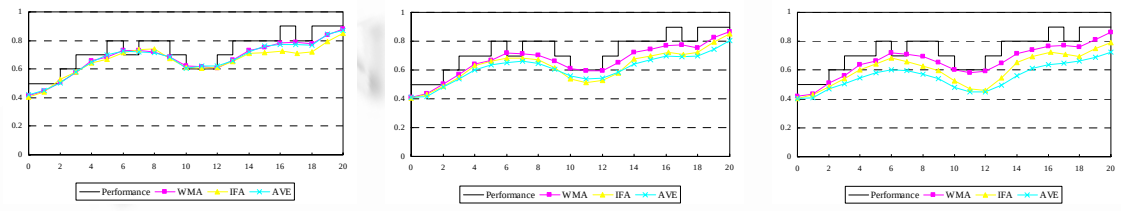
我们对比使用 3 种不同推荐评估算法时用户信任度估计的演变情况,包括简单求平均值的算法AVE,IFA[19]和WMA.我们设置IFA中$quantile=0.01$,WMA中域的初始信任度$t_i=1,i=1,...,6$.控制信任度更新幅度的$\beta=0.5$保持不变.用户执行角色的初始真实信任度$t_0=0.5$,波动程度$c=0.1$.推荐域不公正评价程度$u=0.8$.推荐信息的持续因子$\lambda=0.7$.用户的信任度估计取 10 次协作事务结果的平均值.

Table 1 User's trustworthiness and evaluation in recommendation

表 1 用户信任度与推荐信息评价

Level	Trustworthiness	Evaluation	Value
L_1	$-1\le t<-0.6$	Mediocre	−0.8
L_2	$-0.6\le t<-0.2$	Bad	−0.4
L_3	$-0.2\le t<0.2$	Average	0
L_4	$0.2\le t<0.6$	Good	0.4
L_5	$0.6\le t\le 1$	Excellent	0.8

图 2(a)是所有域都提交公平推荐信息的理想情况,目标域根据用户的实际执行与推荐信任的差异更新推荐域的信任度.此时,IFA 和 WMA 均不会改善可信度,反而 IFA 在协作事务最后出现偏差,表明算法错误地过滤了公正推荐.图 2(b)是存在 20%降低评价的情况,IFA 和 WMA 处理的信任度更接近用户的真实值.在前 40 次协作事务中,推荐域的信任度更新变化不大,因此,3 种算法获得用户的信任度估计差别较小.与 IFA 相比,WMA 在协作事务次数超过 40 以后效果明显.图 2(c)是存在 40%降低评价的情况,此时,WMA 比 IFA 的优势更加明显.后两种情况表明,IFA 和 WMA 都在一定程度上检测和避免不公正推荐,但 IFA 为了尽量过滤恶意评价导致用户的信任度评估的振荡幅度较大,而 WMA 相对更接近真实值.



(a) Fair recommendation

(a) 公正评价

(b) 20% unfair low recommendation

(b) 20%降低评价

(c) 40% unfair low recommendation

(c) 40%降低评价

Fig.2 Experimental results with different rate unfair recommendation

图 2 不同比例非公正推荐的实验结果

4 结 论

组织之间通过共享资源和服务及相互操作实现共同的目标,也导致非授权访问的可能性大为增加,自组协同下的授权管理面临更多的安全威胁.研究人员根据中国墙策略提出自组安全互操作的方案,但无法有效抵御自治域和用户的恶意行为.本文提出基于信任度的自组安全互操作方法,自治域根据用户的访问凭证和本地安全策略独立实施授权决策,依赖用户的访问历史和自治域对用户的信任度.用户恶意执行角色导致其推荐信任降低,从而降低其信任度,影响授权结果.根据推荐信息以及与用户的直接交互经验之间的偏差,自治域使用基于 WMA 的推荐评估办法更新推荐域的信任度.恶意评价导致自治域的信任度降低,影响其推荐信息的可信度.系统仿真实验表明,我们的方法与其他相关算法相比,安全性及有效性更好.

References:

[1] Sandhu R, Coyne E, Feinstein H, Youman C. Role-Based access control models. IEEE Computer, 1996,29(2):38−47.

[2] Shafiq B. Access control management and security in multi-domain collaborative environments [Ph.D. Thesis]. West Lafayette: Purdue University, 2006.

[3] Brewer D, Nash M. The Chinese wall security policy. In: Proc. of the IEEE Symp. on Security and Privacy. Oakland: IEEE Computer Society Press, 1989. 206−214.

[4] Shehab M, Bertino E, Ghafoor A. Secure collaboration in mediator-free environments. In: Meadows C, Syverson P, eds. Proc. of the 12th ACM Conf. on Computer and Communications Security. Alexandria: ACM Press, 2005. 58−67.

[5] Shehab M, Bertino E, Ghafoor A. SERAT: Secure role mapping technique for decentralized secure interoperability. In: Ferrari E, Ahn GJ, eds. Proc. of the ACM Symp. on Access Control Models and Technologies. Stockholm: ACM Press, 2005. 159−167.

[6] Gong L, Qian X. The complexity and composability of secure interoperation. In: Proc. of the IEEE Symp. on Security and Privacy. Washington: IEEE Computer Society, 1994. 190−200.

[7] Gong L, Qian X. Computational issues in secure interoperation. IEEE Trans. on Software and Engineering, 1996,22(1):43−52.

[8] Dawson S, Qian S, Samarati P. Providing security and interoperation of heterogeneous systems. Distributed Parallel Databases, 2000,8(1):119−145.

[9] Bonatti P, di Vimercati SDC, Samarati P. An algebra for composing access control policies. ACM Trans. on Information and System Security, 2002,5(1):1−35.

[10] Shafiq B, Joshi JB, Bertino E, Ghafoor A. Secure interoperation in a multi-domain environment employing RBAC policies. IEEE Trans. on Knowledge and Data Engineering, 2005,17(11):1557−1577.

[11] Zhang Y, Zhang WY, Li XX, Huai JP. Secure access control for group communication on multi-autonomous domains collaborative environment. Journal of Computer Research and Development, 2005,42(9):1558−1563 (in Chinese with English abstract).

[12] Shehab M, Bertino E, Ghafoor A. Workflow authorization in mediator-free environments. Int'l Journal of Security and Networks, 2006,1(1/2):2−12.

[13] Chakraborty S, Ray I. TrustBAC—Integrating trust relationships into the RBAC model for access control in open systems. In: Ferraiolo DF, Ray I, eds. Proc. of the ACM Symp. on Access Control Models and Technologies. Lake Tahoe: ACM Press, 2006. 49−58.

[14] Beth T, Borcherding M, Klein B. Valuation of trust in open network. In: Gollmann D, ed. Proc. of the European Symp. on Research in Security (ESORICS). Brighton: Springer-Verlag, 1994. 3−18.

[15] Abdul-Rahman A, Hailes S. A distributed trust model. In: Proc. of the 1997 New Security Paradigms Workshop. Langdale: ACM Press, 1997. 48−60.

[16] Jøsang A. An algebra for assessing trust in certification chains. In: Kochmar J, ed. Proc. of the Network and Distributed Systems Security Symposium (NDSS'99). San Diego: Internet Society, 1999.

[17] Whitby A, Jøsang A, Indulska J. Filtering out unfair ratings in Bayesian reputation systems. The Icfain Journal of Management Research, 2005,4(2):48−64.

[18] Osborn SL, Sandhu R, Munawer Q. Configuring role-based access control to enforce mandatory and discretionary access control policies. ACM Trans. on Information and System Security, 2000,3(2):85−106.

[19] Littlestone N, Warmuth M. The weighted majority algorithm. Information and Computation, 1994,108(2):212−261.

[20] Jøsang A, Haller J. Dirichlet reputation systems. In: Tjoa AM, Xhafa F, eds. Proc. of the 2nd Int'l Conf. on Availability, Reliability and Security (ARES 2007). Barcelona: IEEE Computer Society, 2007. 112−119.

[21] Shi JQ. A trust model with statistical foundation [MS. Thesis]. Ottawa: University of Ottawa, 2005.

附中文参考文献:

[11] 张煜,张文燚,李先贤,怀进鹏.多自治域协同环境中群组通信的安全访问控制.计算机研究与发展,2005,42(9):1558−1563.

刘伟(1979－),男,河南信阳人,博士生,主要研究领域为系统软件,安全操作系统.

贺也平(1962－),男,博士,研究员,博士生导师,主要研究领域为可信计算技术,安全操作系统形式化模型,安全协议的形式化分析.

蔡嘉勇(1978－),男,博士生,主要研究领域为信息安全,大型网络.