普适环境下的动态模糊访问控制模型研究

窦文阳 王小明 张立臣

(陕西师范大学计算机科学学院 西安 710062)

摘 要 普适计算环境下用于授权决策的上下文条件满足程度、用户的信任程度以及授予用户权限后产生的安全风险程度都具有模糊性,现有的访问控制模型大都不支持对模糊信息的授权推理。提出了一个基于角色的模糊访问控制模型(FRBAC模型),它把对用户到角色的指派(UA)和角色到权限的指派(PA)分为独立的两部分。在UA指派中,用户可以激活的角色是通过对上下文条件的满足程度、用户的信任程度以及激活角色可能产生的安全风险进行模糊推理自动生成的。FRBAC模型实现了普适环境下的动态模糊授权和用户角色的自动分配,简化了模型的安全管理工作。最后给出了FRBAC模型实现的体系结构,还给出了模糊授权推理器的设计以及模糊授权规则库、模糊授权推理算法的实现。FRBAC模型实现了普适计算环境下的动态模糊授权,为智能访问控制授权系统的研究提供了新思路。

关键词 普适计算,访问控制,模糊推理,授权控制

中图法分类号 TP309 **文献标识码** A

New Fuzzy Role-based Access Control Model for Ubiquitous Computing

DOU Wen-yang WANG Xiao-ming ZHANG Li-chen

(College of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

Abstract In the Ubiquitous Computing Environment the user's contextual conditions of satisfaction, the user's level of trust and the permission's level of security risk are fuzziness. Many of the existing access control model do not support for the inference of fuzzy information. This paper presented a fuzzy role-based access control model(FRBAC), the roles assigned to users(UA) and role to the permissions assigned(PA) are divided into two parts in the FRABC model, the user can activate the role by contextual conditions of satisfaction, the user's level of trust, as well as the possible security risks of activating the role. This authorization process is completed through the fuzzy reasoning. FRBAC model achieves dynamic fuzzy authorization and automatic distribution of user roles, it simplifies the security management of the RBAC model. Finally, the paper gave the architecture of the model to achieve and the related fuzzy authorized reasoning algorithm.

Keywords Ubiquitous computing, Access control, Fuzzy reasoning, Authorization control

1 引言

国内外学术界和工业界公认普适计算[1]是未来计算的主流模式,它将透明地给人们提供随时随地的数字信息服务。可以预计,普适计算将对计算机技术的发展和应用带来深刻的影响。

在普适计算的应用中,信息的安全保障是一个基础性问题[2]。由于普适计算环境的开放性的特点,用户可以随时随地通过任意方式访问信息资源,因此所面临的安全问题也将不同于以往的信息系统。信息的安全保护和用户隐私信息的保密已经成为阻碍普适计算技术进一步应用的关键问题[3]。

在普适计算环境下对用户的访问控制授权需要综合考虑多种因素,例如用户对上下文条件的满足程度、用户的可信程度以及授予用户权限可能造成的安全风险等。但是这些决定授权结果的因素是具有模糊性的。首先,用户对上下文条件的满足程度是具有模糊性的。由于普适计算环境的开放性及普适设备多样性的特点,普适环境下对资源的权限控制需要制定各种约束条件,如时间约束、空间约束、资源使用状态约束等,授予用户权限需要验证这些约束条件。在传统的访问控制模型中,如果用户满足全部约束条件,则授予权限;但是,如果用户有一个条件不能满足,则认为用户不满足约束条件,不予以授权。实际上这种处理方式忽略了用户满足部分约束条件的事实。而在人们的实际生活中,这样的处理方式也是不恰当的。在实际生活中人们做类似判断时往往会划分"非常满足"、"基本满足"、"基本不满足"等不同等级的满足程度来进行评价。例如,有10个约束,用户满足了其中的9个条件,人们往往给出的评价是"基本满足"约束条件。并且,这种不同等级的满足程度之间的关系不是非此即彼的,而是亦此

到稿日期:2009-10-10 返修日期:2009-12-14 本文受国家自然科学基金项目(60773224),教育部科学研究重点项目(107106)资助。

窦文阳(1979—),男,博士,主要研究方向为网络与信息系统安全、访问控制等,E-mail:douwenyang@snnu.edu.cn;王小明(1964—),男,博士生导师,主要研究方向为网络与信息系统安全、工作流系统安全等;张立臣(1979—),男,博士,主要研究方向为信息系统安全、工作流系统安全等。

亦彼的，具有典型的模糊性。

与此类似，普适环境下用户的信任程度也是具有模糊性的。信任关系本质上是基于信念的，具有主观性、不确定性和模糊性，无法精确地加以描述和验证[4]。主观信任的模糊性表现为信任不是二值的，即不是"非此即彼"的，而是亦此亦彼的。例如，人们在现实中常常会划分"完全信任"、"非常信任"、"很信任"等不同等级的信任，并且通常不会简单地断定是否应该"非常信任"某主体，而是认为应当在多大程度上"非常信任"该主体。在许多情况下，人们甚至会认为既可以在一定程度上"非常信任"某主体，也可以在另一程度上"很信任"该主体。

普适环境下用户激活权限后对系统产生的安全风险也是具有模糊性的[5]。一般情况下，用户激活的权限越多，给系统可能带来的安全风险就越高。但是，对于这种可能造成安全风险的描述，我们很难用精确的数学语言去描述，而需要用一些不同等级程度的模糊集合来描述。

基于角色的访问控制模型[6]（RBAC模型）是一个策略中立安全的模型，被认为是一种铰接策略的工具，而不是用来具体体现某种特定的策略。许多学者对RBAC模型进行了深入的研究，并且在系统的安全控制中得到了广泛的应用。但是，传统的基于RBAC模型都是基于精确数学模型建立的，无法支持对模糊信息的授权推理决策。此外，传统的RBAC模型都是基于封闭环境的静态授权模型，根据预先定义好的用户-角色-权限的关系进行授权，无法满足普适计算环境下根据环境上下文变化而动态授权的要求。

本文在RBAC模型的基础上提出了一个模糊访问控制模型：FRBAC模型。FRBAC模型把传统的RBAC模型分为两部分：用户-角色指派（UA）以及角色-权限指派（PA）。对于UA的指派，是通过用户对上下文条件的满足程度、用户的可信程度以及授予用户权限后产生的安全风险进行模糊推理，系统自动分配完成的，实现了普适环境下的动态模糊授权，简化了模型的安全管理工作。最后给出了实现模型的体系结构，以及授权模糊推理器和授权算法的实现。

本文第2节是相关研究；第3节提出了一个模糊的访问控制模型FRBAC模型；第4节给出了FRBAC模型实现的体系结构及模糊推理器的实现；第5节通过一个实例分析了FRBAC模型的授权能力；最后总结全文。

2 相关研究

有关安全的模糊性，1993年Hosmer在文献[7]中就进行了相关的论述。文献[8,9]也试图把模糊技术引入安全授权控制中。著名的访问控制专家R. Sandhu也认为模糊访问控制研究将是未来智能访问控制研究的有效切入点，模糊访问控制理论与方法研究必将成为一个重要的研究方向[9]。

关于模糊访问控制模型的研究，人们已做了很多工作：文献[10]提出了一个模糊BLP模型，但模型的适用范围有很大的局限性；文献[11]提出了一个基于信任度的访问控制模型，信任度的计算是通过模糊推理来完成的，但是在文中作者没有考虑到对模糊上下文信息的处理，不适用于普适计算环境；文献[12]提出了一个适用于数据库系统的模糊RBAC模型，该模型实现了对不同安全级别数据的安全控制，但也难以扩展在普适计算环境中的使用；文献[13]提出了一个基于模糊关系的增强RBAC模型，该模型实现了模糊授权，但其模糊推理算法比较简单，难以适用于复杂普适计算环境下的模糊授权控制；文献[14]通过模糊关系扩充了RBAC模型的职责分离约束，给出的模型也难以用于普适计算环境。

在已有的很多文献中，对RBAC模型进行了广泛深入的研究并取得了许多成果。RBAC模型作为一个策略中性的模型可以支持多种安全策略，所以非常适用于普适计算环境。本文在RBAC模型基础上，基于模糊逻辑进行扩展，引入了模糊上下文条件满足程度、模糊信任程度、模糊安全风险程度等概念，用于描述普适环境下的模糊授权信息，实现了一个适用于普适计算环境的动态模糊访问控制授权模型：FRBAC模型。最后对FRBAC模型实现的体系结构以及模糊推理器的设计也做了详细介绍。

3 FRBAC模型

3.1 模型概述

在RBAC模型中，角色分配与授权关系都是由管理员预先设定好的，这种限制造成了基于RBAC的访问控制模型都是静态集中式模型。为了实现普适环境下的动态授权，本文把传统RBAC模型中的用户-角色-权限的指派过程分为两部分：用户-角色指派（UA）和角色-权限指派（PA），如图1所示。UA分配一般由系统管理员完成，管理员根据系统实际应用背景设定相应的角色权限关系，建立一个角色到权限的多对多的映射。但是并不决定用户实际权限的使用，这样就保障了系统安全和用户权限使用信息的隐私，而且角色到权限的关系一旦制定好，一般不需要变动。PA分配不再是事先定义好的，而是需要根据系统上下文动态变化的。用户可以获得的角色将由用户对上下文条件的满足程度、用户信任度、角色的安全风险程度来确定，系统将通过模糊推理计算做出授权决策，授予用户可以使用的角色，从而获得相应的权限。如果用户对系统要求的条件不能够满足，系统可以收回用户使用的角色。

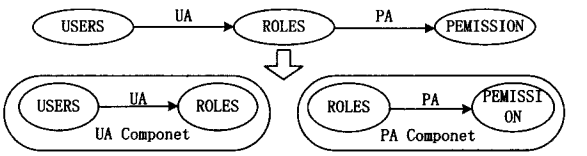

图1 动态授权的RBAC模型

3.2 基本元素定义

FRBAC模型是基于RBAC模型扩展得到的，图2给出了FRBAC模型关系图。在FRBAC模型中，授权要考虑3个方面的因素：上下文条件满足程度、用户可信程度、授予角色产生的安全风险程度。在模型中，角色-权限的分配不需要管理员完成，而是由系统通过模糊推理器根据授权模糊推理规则自动推理，完成分配。用户获得角色后，还需要满足系统约束才能激活角色，使用相应的权限。若用户不能满足上下文条件约束，或者用户不可信，或者用户权限的使用可能给系统带来较高的安全风险，系统将拒绝授权或者中止用户权限的使用。

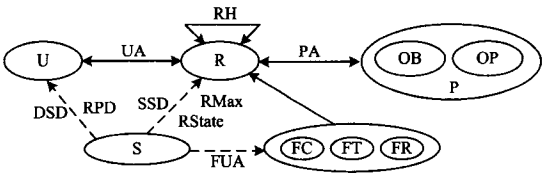

图2 FRBAC模型

FRBAC 模型基本组成元素定义如下：

定义 1 用户表示普适环境下的人或智能 Agent。用户集合记为 U，其元素用 u 表示。

定义 2 角色是实现某种功能所需权限集合的描述，与用户是多对多的关系。角色集合记为 R，其元素用 r 表示。

定义 3 客体是系统接收访问控制的所有对象。客体集合记为 OB，其元素用 ob 表示。

定义 4 操作表示能进行某项功能的最小动作序列。操作集合记为 OP，其元素用 op 表示。

定义 5 权限表示系统中对象的访问模式，可以表示为一个客体与操作的二元关系 $OP=OB\times OP$，权限的集合记为 P，其元素用 p 表示。

在权限集 OP 基础上，可以定义增强权限集 EP。EP 中的元素可以表示为一个三元组 (ob,op,t)，其中 t 表示时间段，例如 $t=$[8：00AM－12：00AM]，表示上午 8 点到 12 点这一时间段。EP 表示权限在时间 t 内可以有效使用。通过 EP 概念的引入可以大大增强系统的安全性。例如，在智能教室中，教师只有在上课的时间内才具有使用投影机的权限 r，可以表示为

(project,r,[8：00AM－12：00AM,14：30PM－18：30PM])

定义 6 会话是将用户与激活角色对应的映射。一个用户可以有多个会话，但一个会话只能从属于一个用户，一个会话可以对应多个角色。会话集合记为 S，其元素用 s 表示。

在会话中还包括一些约束(Constraints)，这些约束决定着用户最终权限激活的结果。FRBAC 模型中的约束包括静态职责分离约束(SSD)、动态职责分离约束(DSD)、激活角色最大数约束(RMax)、角色状态约束(RState)，角色依赖约束(RPD)。

定义 7 上下文条件满足程度(FC)描述了用户提出资源访问请求时对普适环境下所有授权条件的满足程度。FC 可以用一个二元组 $(User,Cf)$ 表示。其中 $User$ 是用户；Cf 是一个模糊集合，表示 $User$ 对上下文条件的满足程度。

定义 8 用户可信程度(FT)表示进入普适环境用户可以信任的程度，其含义包括用户身份是否可信、用户使用权限行为是否可信、用户的访问历史是否可信等。对信任度越高表示用户越可信，对其的授权控制就越宽松；信任度越低，对其的控制策略就需要越严格。FT 可以用一个二元组 $(User,Tf)$ 表示。其中 $User$ 是用户，Tf 是一个模糊集合，表示 $User$ 在环境下的可信程度。例如，(u1,一般信任)表示 u 当前的可信程度为“一般信任”。

定义 9 角色激活的安全风险(FR)表示当某一权限被用户激活使用后可能对环境产生的安全风险的大小程度。在 FRABC 模型中，不同角色具有不同的使用权限，因此角色可以表示权限的集合。在激活不同角色时，具有更多权限的角色可能造成的安全风险就越大。FR 可以用一个二元组 $(Role,Rf)$ 表示。其中 $Role$ 是角色，代表了一组权限集合，Rf 是一个模糊集合，表示 $Role$ 被激活后可能产生的安全风险。

定义 10 角色状态表示角色当前可以使用的状态，用 RS 表示。$RS=\{Disabled,Enable,Active\}$，其中 $Disable$ 表示角色当前不可用，$Enable$ 表示角色当前启用，$Active$ 表示角色当前激活，即用户可以使用角色的相关权限。例如，$r1.rs=Active$ 表示 $r1$ 的角色状态为 $Active$。

3.3 模型形式化描述

下面给出 FRBAC 模型的形式化描述：

(1)U,R,OP,OB,P,S 分别表示用户集合、角色集合、操作集合、客体集合、权限集合、会话集合；

(2)$UA\subseteq U\times R$，从 U 到 R 的多对多关系表示 u 被分配的 r。UA 表示 u 可以分配 r，但是 r 的激活要取决于 u 的 FC,FT 及 FR 经过模糊推理的结果；

(3)$PA\subseteq P\times R$，从 P 到 R 的多对多关系，表示 r 被赋予的 p；

(4)$ar:(u:U)\rightarrow 2^R$ 返回指定 u 在当前 s 中激活的 r 集合；

(5)$au:(r:R)\rightarrow 2^U$ 返回指定 r 的 u 集合；

(6)$ap:(r:R)\rightarrow 2^P$ 返回指定 r 的 p 集合；

(7)$uc(u:U)\rightarrow FC$，返回指定 u 的 FC；

(8)$ut(u:U)\rightarrow FT$，返回指定 u 的 FT；

(9)$ur(r:R)\rightarrow FR$，返回指定 r 的 FR；

(10)$frm(u,r,uc(u),ut(u),ur(r))$，当 frm 值为真时，表示根据 FC,FT,FR 经过模糊推理后 u 可以激活 r，即 $frm(u,r,uc(u),ut(u),ur(r))=\text{true}\Rightarrow r.rs=Active$；

(11)$FUA\subseteq U\times R\times RS$ 表示 U,R 和 RS 之间的关系，例如 $(u,r,Active)$ 表示 u 对 r 当前的使用状态为 $Active$；

(12)$active(s,u)\rightarrow 2^R$ 返回 u 在 s 中激活的 r 集合；

(13)$enable(s,u)\rightarrow 2^R$，返回 u 在 s 中启用的 r 集合；

(14)$disable(s,u)\rightarrow 2^R$ 返回 u 在 s 中禁用的 r 集合。

3.4 模型约束

在 RBAC 模型中，约束(Constraints)是很重要的部分，通过约束进一步限制用户对角色的使用，提高模型的安全性。用户只有满足系统定义的约束条件，才能够激活角色，使用相应权限；如果不满足约束，则不能够激活角色。本文在 RBAC 模型的基础上提出了 4 种约束。

定义 11 静态职责分离约束(SSD)指在系统中用户不能被指定给一个冲突角色集合中的两个或多个角色：

$$\forall r_1\in R,\forall r_2\in R,(r_1,r_2)\in SSD\Rightarrow au(r_1)\cap au(r_2)=\varnothing$$

定义 12 动态职责分离约束(DSD)指在系统中具有互斥关系的角色不能同时激活：

$$\exists s\in S,\exists u\in U,\forall r_1\in R,\forall r_2\in R,(r_1,r_2)\in DSD\Rightarrow$$
$$r_1\in ar(u)\rightarrow r_2\notin ar(u)\ \text{or}\ r_2\in ar(u)\rightarrow r_1\notin ar(u)$$

定义 13 激活角色最大数约束(RMax)指系统中可以激活某一角色的最大数目。RMax是一个三元组 $(r,number,r\text{Max})$，其中 r 表示激活的角色，$number$ 表示当前 r 激活的数目，rMax表示系统允许激活 r 的最大数目。$\exists s\in S,\exists u\in U,\forall r\in R$，则$R$Max约束可以表示为：

$$r.number\leqslant r.r\text{Max}\wedge(u,r)\subseteq UR\Rightarrow r.rs=Active$$

定义 14 角色依赖约束(RPD)表示一个角色的激活必须以另一个角色激活为前提。RPD 可以表示为一个三元组 (r_1,r_2,RPD)。$\exists s\in S,\exists u\in U,r_1\in R,r_2\in R$，则 RPD 约束可以表示为：

$$(r_1,r_2)\in RPD\wedge(r_1.rs=Active)\Rightarrow r_2.rs=Active$$

用 C 表示 FRBAC 模型中的约束，则：

$$C=SSD\cup DSD\cup R\text{Max}\cup RPD$$

3.5 模型授权

FRBAC模型的授权可以表示为一个七元组(u,r,p,FC,FT,FR,C)，其中u表示用户，r表示角色，p表示权限，FC表示用户对上下文条件的模糊满足程度，FT表示用户的信任程度，FR表示用户请求激活的角色可能产生的安全风险。模型首先对3个模糊变量进行模糊推理，验证用户是否能够分配角色。其次检查用户是否满足约束条件，最后根据验证结果给出用户授权结果。授权算法如下：

授权算法

```
输入:用户 u,客体 o,权限 p,会话 s
输出:true 表示授权成功;false 表示授权失败
    Grant(u,o,p,s)
      {
        foreach r∈R do
          {
            if(u,r) ∈UA
            then RR←r //获得 u 的 r 集合
          }
        foreach r∈RR do
          {
            if frm(u,r,o)=true
            then AR←r //获得 u 激活的 r 集合
          }
            if AR= null;
            then return false ;
            else if
                 {
                 foreach r∈rr do
                     {
                          if r 同时满足 SSD,DSD,RMax,RPD
                 约束;
                          then return true ;
                          else return false ;
                     }
                 }
```

4 FRBAC模型实现的体系结构

在普适环境下，用户是通过个人智能Agent完成对系统中资源的使用。在系统体系结构设计中，我们把用户Agent分为6个模块：①角色服务模块(RBAC server list module)；②上下文计算模块(Context computing module)；③信任度计算模块(Trust Computing module)；④角色风险模块(Role risk module)；⑤模糊推理模块(Fuzzy Reasoning Module)；⑥访问控制模块(Access control module)。FRBAC模型实现的系统体系结构如图3所示。

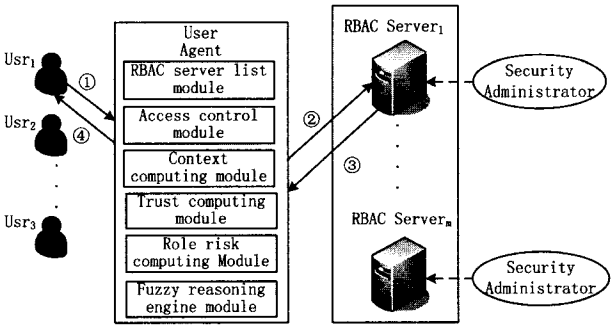

图3 实现FRBAC模型体系结构

在图3中，角色服务模块的功能是与角色服务器通讯，完成角色分配的相关工作；上下文计算模块的功能是获取系统授权的上下文条件，验证用户对上下文条件的满足程度；橘色风险模块的功能是获取角色的风险程度；模糊推理模块的功能是通过对用户的上下文信息、用户的信任度、角色使用风险的模糊综合推理决策用户可以激活的角色；访问控制模块的功能是完成用户的授权工作，此外当用户的个人属性发生变化时，需要重新判断用户的授权关系。

在体系结构中，用户进入普适计算环境，用户的个人智能Agent会自动与系统服务器交互。首先，用户Agent自动完成系统的登录认证，系统将为用户分配一个信任度。若用户提出对空间资源的访问请求，用户Agent的访问控制模块就开始工作，模糊推理模块根据用户的信任度、上下文信息及用户使用角色的风险进行模糊综合推理，最后授予用户可用的角色。系统授权流程如下：

(1)用户进入空间，用户Agent自动登录系统，信任度计算模块根据用户和系统上下文信息计算用户的信任度；

(2)用户提出访问请求，用户Agent根据上下文信息、信任度及角色的风险值通过模糊推理模块进行模糊综合推理，得到的结果发送给系统的角色服务器；

(3)角色服务器为用户分配角色，并返回给用户；

(4)用户根据可以激活的角色的权限访问资源。

下面分别给出上下文满足程度、信任度以及角色风险的计算方法，最后给出用于最终授权的模糊推理器的设计。

4.1 模糊推理器的实现

在对用户的角色指派中，我们通过模糊推理器(Fuzzy Reasoning Evaluator)组件完成角色授予的模糊推理过程。FRE的结构如图4所示。

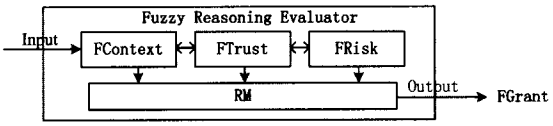

图4 模糊推理器

在FRE中输入的3个模糊量是模糊上下文条件满足程度FContext、模糊信任值Ftrust、模糊风险值Frisk；输出1个变量：模糊授权程度FGrant。因为FGrant是一个模糊值，所以系统还需要定义一个阈值r，用于判断最终的授权结果。如果$FGrant \geqslant r$，则授权；如果$FGrant < r$，则拒绝授权。阈值r可以根据应用环境取值，r取值越高，则安全控制强度越高；r取值越低，则安全控制强度越低。

在FRE中，核心部分是模糊推理机RM。下面我们给出RM的实现。在此之前，首先给出FContext，FTrust，FRisk，FGrant的模糊语言及其隶属度的定义，有关模糊数学的相关知识请参见文献[15]。

在系统设计时，为了减少模糊推理规则的数量，对FContext，FTrust，FRisk，FGrant分别取不同的语言值，如表1—表4所列。

表1 FContext模糊变量

	FC1	FC2	FC3
含义	非常满足	基本满足	基本不满足
记号	AC	BC	CC

表2 FTrust模糊变量

	FT1	FT2	FT3	FT4

含义	完全信任	很信任	一般信任	不信任
记号	AT	BT	CT	DT

表 3 FRisk 模糊变量

	FR1	FR2	FR3
含义	高风险	一般风险	低风险
记号	AR	BR	CR

表 4 FGrant 模糊变量

	FG1	FG2	FG3
含义	强授权	基本授权	基本不授权
记号	AG	BG	CG

根据实际情况中的授权原则可以制定模糊授权规则，多条模糊授权规则可以组成模糊授权库，如表 5 所列。

表 5 授权规则

FContext	FTrust	FRisk	FGrant
AC	AT	AR	BG
AC	AT	BR	AG
AC	AT	CR	AG
AC	BT	AR	CG
AC	BT	BR	BG
AC	BT	CR	BG
AC	CT	AR	DG
AC	CT	BR	DG
AC	CT	CR	CG
AC	DT	AR	DG
AC	DT	BR	DG
AC	DT	CR	CG
BC	AT	AR	CG
BC	AT	BR	BG
BC	AT	CR	BG
BC	BT	AR	DG
BC	BT	BR	CG
BC	BT	CR	BG
BC	CT	AR	CG
BC	CT	BR	BG
BC	CT	CR	BG
BC	DT	AR	CG
BC	DT	BR	CG
BC	DT	CR	BG
CC	AT	AR	DG
CC	AT	BR	CG
CC	AT	CR	BG
CC	BT	AR	DG
CC	BT	BR	CG
CC	BT	CR	CG
CC	CT	AR	DG
CC	CT	BR	DG
CC	CT	CR	CG
CC	DT	AR	DG
CC	DT	BR	DG
CC	DT	CR	DG

在表 5 中，每一行可以表示一条模糊授权规则。例如，第一行表示的模糊授权规则是

IF FContext = AC and FTrust = AT and FRisk = FR THEN FGrant = AG

该授权规则表示的含义为：如果用户对约束条件的满足程度(FContext)为完全满足，并且该用户信任程度(FTrust)为非常信任，用户激活角色的风险程度(FRisk)为低风险，则授予用户访问权限的可能性(FGrant)就非常高。

类似地，我们可以得到 3 * 4 * 3 = 36 条模糊授权规则。根据不同的 FContext，Ftrust，Frisk 输入，总是可以根据一条模糊授权规则进行推理，获得授权推理结果，所以表 5 给出的模糊推理规则库是完备的。

基于模糊推理规则库可以构造模糊推理机 RM。根据模糊数学的相关知识，模糊推理机 RM 表示 FContext，FTrust，FRisk，FGrant 上的一个模糊关系。

设 l 表示所有的规则数，FContext，FTrust，FRisk，FGrant 分别表示模糊上下文条件满足程度、模糊信任度、模糊风险程度、模糊授权，则：

$$RM=\bigcup_{l}(FContext_l\times FTrust_l\times FRisk_l\times FGrant_l)$$

在具体的计算中，我们采用模糊推理系统中常用的最小推理机[16]。最小推理机的特点是运算简便，而且对许多现实问题更为直观。有关最小推理机的内容可以详见文献[16]。因此，给定一组具体的输入 $FContext_i$，$FTrust_j$，$FRisk_m$，可以计算得到模糊授权程度 $FGrant_n$ 的值，即：

$$FGrant_n=(FContext_i,FTrust_j,FRisk_m)\circ RM$$

根据最小推理机的定义，令

$$u_x=FContext_i\times FTrust_j\times FRisk_m$$

$$rm_l=FContext_l\times FTrust_l\times FRisk_l\times FGrant_l$$

可得

$$FGrant_n=\max_{l}[\min(u_x,rm_l)]$$

最后，根据得到的 $FGrant_n$ 与预先定义的授权阈值 r 的比较结果，确定对用户的授权决策结果。

模糊授权推理过程分为以下 4 步：

(1)输入模糊变量 FContext，FTrust，FRisk；

(2)构造模糊推理机 RM；

(3)计算输出 FGrant；

(3)通过阈值比较，得到授权结果。

5 应用实例

在 RBAC 模型中，用户获得角色，就可以使用该角色具有的权限。这种用户-角色-权限的关系是确定的，无论在什么时间、什么地点都有相同的授权结果。但是在 FRBAC 模型中，用户具有的角色可能是变化的。本节通过智能教室中的一个实例来验证 FRBAC 模型的授权能力。智能教室的角色、上下文及权限设定如表 6－表 8 所列。

表 6 角色设定

角色名称	表示	可用权限	角色风险
管理员	User1	Read; Write; Copy; Using Computer; Using Print; Using P Machine; Using Internet	0.8
教师	User2	Read; Write; Copy; Using Computer; Using Print; Using P Machine; Get Name List	0.6
学生	User3	Read; Write; Using Internet;	0.3
工作人员	User4	Using Computer; Using Print; Using P Machine;	0.5
旁听者	User5	Read	0.1

表 7 权限设定

权限名称	表示
读文件	Read
写文件	Write
拷贝文件	Copy
使用计算机	Using Computer
使用打印机	Using Print
使用投影仪	Using P Machine
获得名册	Get Name List

(下转第 120 页)

结束语 以 IMS 为核心的下一代网络是未来融合网络发展的方向。本文分析了 IMS 网络中的注册过程和重注册过程，在前人研究的基础上，提出了一种改进的快速用户重注册过程。通过在 REGISTER 消息中增加 Route 消息头，携带 S-CSCF 的路由信息，将重注册过程中的 REGISTER 消息直接从拜访网络的 P-CSCF 转发到归属网络的 S-CSCF。数值分析结果表明，本文改进的快速重注册过程要优于标准重注册过程和已有的一些改进过程。同时，它没有对原网络进行大规模的改变，只是对 REGISTER 消息进行了稍许改动，对网络的影响并不大，容易实现。

参 考 文 献

[1] 3GPP TS 23.228, V. 8.2.0. IP Multimedia Subsystem(IMS)[S]. Sep. 2007

[2] Rosenberg J, Schulzrinne H, Camarillo G, et al. SIP: Session Initiation Protocol, IETF RFC 3261[S]. Internet Engineering Task Force, 2002

[3] Lin Y B, Tsai M H. Caching in I-CSCF of UMTS IP Multimedia Subsystem[J]. IEEE Transaction on Wireless Network, 2006, 5(1): 186-192

[4] 吕新荣，廖建新，杨波，等. IMS 域的位置管理策略研究[J]. 电子信息学报，2007，29(10)：2471-2476

[5] Larsen K L, Matthiesen E V, Schwefel H-P, et al. Optimized Macro Mobility within the 3GPP IP Multimedia Subsystem[C]// International Conference on Wireless and Mobile Communications. Bucharest, 2006: 82-88

[6] Farahbakhsh R, Varposhti M, Movahhedinia N. Transmission Delay Reduction in IMS by Re-registration Procedure Modification[C]// The Second International Conference on Next Generation Mobile Application, Services and Technologies. Cardiff, 2008: 142-146

[7] 3GPP TS 24.228, V. 5.15.0. Signalling flows for the IP multimedia call control based on Session Initiation Protocol(SIP) and Session Description Protocol(SDP)[S]. Sep. 2006

(上接第 67 页)

表 8 上下文信息设定

上下文名称	表示	举例
时间上下文	Time()	Time(User)=8：00 AM
位置上下文	Location()	Location(User)=Room 8302
环境上下文	Env()	Env(System)=Busy

假设 Pro Zhang 是一名上课的教师，根据课程安排他在 7:50AM 来到 Room 8201 教室上课。Pro Zhang 提出请求，要求激活其教师(User1)角色，以使用 User1 的权限。Pro Zhang 的信任度假设为 Trust=0.8，User1 的角色风险为 rs=0.8。Pro Zhang 的上下文有两个：Time=7:50AM，Location=Room 8201，根据上下文满足程度的计算式(2)可以得到 Pro Zhang 的上下文满足程度 con=0.9。

对于 Pro Zhang 授权请求 Request(Pro Zhang, User1, tu=0.8, rs=0.8, con=0.9)，根据模糊推理算法(3)计算可得 FResult. Request=0.6；如果当前系统的授权阈值为 0.5，由于 0.6 大于授权阈值，因此经过模糊综合推理，Pro Zhang 可以激活教师角色，进行上课。

结束语 FRBAC 模型是在传统 RBAC 模型的基础上通过引入模糊推理扩展得到的，具有更加灵活、智能的授权能力。FRBAC 模型引入了上下文条件满足程度、信任程度、角色风险程度等模糊概念，解决了普适环境下的复杂、模糊、动态授权问题。最后对模型实现以及模糊授权推理算法进行了详细说明。普适环境下的模糊安全强度自适应访问控制模型将是我们下一步的研究目标。

参 考 文 献

[1] Weiser M. The computer of the 21'st Century[J]. Scientific American, 1991, 265(3): 66-75

[2] Satyanarayanan M. Pervasive computing: vision and challenge [J]. IEEE Personal Communications, 2001, 8(8): 10-17

[3] Wang J, Yang Y, Yurcik W. Secure smart environments: security requirements, challenges and experiences in pervasive computing [C]// Proceedings of NSF Pervasive Computing Infrastructure and Experience Workshop. November, December 2005: 36-48

[4] 唐文，胡建斌，陈钟. 基于模糊逻辑的主观信任管理模型研究[J]. 计算机研究与发展，2005，42(10)：1654-1659

[5] Li Hetian, Liu Yun, He Dequan. A fuzzy set-based approach for model-based internet-banking system security risk assessment [J]. Wuhan University Journal of Natural Sciences, 2006, 11(6): 1869-1872

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

[7] Hosmer H H. Security is fuzzy: applying the fuzzy logic paradigm to the mutipolicy paradigm[C]// Proceedings of the ACM Workshop on New Security Paradigms. 1993: 175-18

[8] Richard A, Berrached A. Using fuzzy relation equations for adaptive access control in distributed system[C]// Proceedings of the IFIP International Conference on Distributed Computing and Security. IFIP Press, 2000: 81-86

[9] Ovchinnikov S. Fuzzy sets and secure computer systems[C]// Proceedings of the IEEE Workshop on Computer and System Security. IEEE Press, 2002: 626-75

[10] Wang H-F, Huang Zhi-hao. Top-down fuzzy decision making with partial preference information[J]. Fuzzy Optimization and Decision Making, 2002, 1(2): 161-176

[11] Zhang Shibin, He Dake. Fuzzy model for trust evaluation[J]. Journal of Southwest Jiaotong University, 2006, 14(1): 23-28

[12] Nawarathna U H G R D, Kodithuwakku S R. A Fuzzy Role Based Access Control Model for Database Security[C]// Proceedings of the International Conference on Information and Automation. Colombo, December 2005: 15-18

[13] Takabi H, Amini M, Jalili R. Enhancing role-based access control model through fuzzy Relations[J]. Information Assurance and Security, 2007: 131-136

[14] Takabi H, Amini M, Jalili R. Separation of duty in role-based access control model through fuzzy relations[C]// Proceedings of the 3rd International Symposium on Information Assurance and Security. 2007: 125-130

[15] 陈启浩. 模糊值及其在模糊推理中的应用[M]. 北京：北京师范大学出版社，2000：31-55

[16] 王立新. 模糊系统与模糊控制教程[M]. 北京：清华大学出版社，2003：73-80