基于承诺2担保的访问控制模型

王小明[1], 赵宗涛[2], 马建峰[3]
(1. 陕西师范大学计算机科学学院, 陕西西安 710062; 2. 第二炮兵工程学院计算机系, 陕西西安 710025;
3. 西安电子科技大学计算机学院, 陕西西安 710071)

摘 要: 访问控制模型是信息安全领域研究的重点之一. 现有文献中可以见到许多访问控制模型, 但其只能依据已有的事实由授权系统单方面对授权请求进行判定处理, 不适合电子商务环境下根据用户对未来可满足条件的承诺进行交互式访问授权的需要. 提出了新的基于承诺2担保的访问控制模型(PABAC)以满足上述访问控制需要. 讨论了模型体系结构, 承诺担保机制, 授权职责分离以及访问控制. 模拟实验结果表明了模型的有效性.

关键词: 访问控制; 交互式授权; 承诺; 担保; 职责分离
中图分类号: TP309 文献标识码: A 文章编号: 0372-2112 (2003) 08-1150-05

A Promise2Assurance2Based Access Control Model

WANG Xiao2ming[1], ZHAO Zong2tao[2], MA Jian2feng[3]
(1. College of Computer Science, Shaanxi Normal University, Xi. an, Shaanxi 710062, China;
2. Department of Computer, The Second Artillery Engineering College, Xi. an, Shaanxi 710025, China;
3. College of Computer Science, Xidian University, Xi. an, Shaanxi 710071, China)

Abstract: The research of access control model is a topic of information security area. There are many access control models in existing literatures, but they process the access requests only depending on existing conditions by themselves. Therefore they are not able to meet the need that authorization process must interact with users and that user. s promises of the future actions are authorization conditions under electronic commerce environment. A promise2assurance2based access control model (PABAC) is presented to achieve the above access control need. Its architecture, promise & assurance mechanism, separation of duties of authorization and access control are discussed. The experimental results express its validity.

Key words: access control; interacting authorization; promise; assurance; separation of duty

1 引言

访问控制模型研究是信息安全领域研究的重要内容. 传统的访问控制模型(如 DAC, RBAC 等)均建立在授权系统必须对用户的访问授权请求/以当前事实为条件作出授权与否处理0的假设基础上, 是静态的[1,2]. 但是越来越多的现代信息系统(如电子商务, 电子政务)要求访问控制模型支持更加复杂的动态访问控制策略, 授权的前提条件不仅仅是已有的事实, 还可能要求用户或系统在授权系统进行授权与否的抉择过程中动态地创造一些必要的授权条件, 使授权过程由传统的授权系统单方面行为变为授权系统与用户之间的交互行为, 从而增强授权系统的灵活性. 对同一权限不同的用户创造的授权条件可能不同, 相应的权限管理措施也可能因人而异, 以便在某种程度上实现个性化授权管理. 用户动态创造的授权条件往往是对授权系统未来可满足条件的承诺, 其真正成为事实是未来的事件. 如果用户成功地作出了承诺, 则权限被授予, 否则给予否决处理. 基于用户承诺的访问授权是近年来受电子商务应用驱动提出的一种新型访问控制模型, 是新一代访问控制研究的重要方向, 具有广阔的应用前景[2,3]. 但是, 现有的基于承诺的访问控制模型还相当简单, 并且存在两个严重的不足: ¹ 授权安全性完全建立在承诺人信用基础上. 如果承诺人不按期履行其承诺, 则授权系统唯一能够采取的补救措施是降低承诺人信用度(reliability), 而信用度仅仅在用户申请新的权限时才对用户起作用. 例如, 系统限制信用度高于某数值的用户才有资格申请某权限; 信用度越高的用户, 系统优先受理其授权请求. º 一旦承诺人未履行其承诺, 并且不再申请新的授权或不再发出访问请求, 可能造成的系统损失无法挽回. 问题产生的根本原因是用户的承诺履行缺少第三方监督与责任担保. 为了克服上述基于承诺的授权系统缺陷, 本文引入承诺担保新概念, 提出基于承诺2担保的访问控制新模型(Promise2Assurance2Based Access Control, PABAC). 用户向授权系统作出承诺时必须向系统提供担保人为其承诺履行承

收稿日期: 2002-12-22; 修回日期: 2003-04-08
基金项目: 国家自然科学基金(No. 90204012); 国家 863 计划(No. 2002AA143021)

担担保责任. 一旦承诺人未按期履行其承诺时, 系统责令相应的担保人承担担保责任, 从而挽回可能造成的系统损失以保证承诺授权的安全性. 其次, 承诺2担保机制使原来单一的授权系统与承诺人信用安全风险关系分解为授权系统与承诺人、授权系统与担保人和承诺人与担保人三元风险关系, 在承诺人, 授权人和担保人之间形成一定的责任监督机制, 能够有效降低授权安全风险, 增强授权系统灵活性. 本文主要讨论 PABAC 模型的构成要素, 承诺担保机制, 授权职责分离和访问控制, 并通过模拟实验验证它的有效性.

2　PABAC 模型

2.1　体系结构

PABAC 模型的基本构成要素是授权人(授权服务器), 承诺人, 担保人, 权限, 承诺担保授权约束, 认证服务器, 承诺2担保监控器和访问控制算法. 承诺担保授权约束对承诺2担保关系, 承诺2授权关系和授权2担保关系的有效性进行约束. 认证服务器对用户登录系统和承诺担保协议的有效性进行验证. 承诺2担保监控器用于监控承诺和担保责任履行进展情况. 当监控器发现某承诺得不到履行时, 系统立即执行相应的担保函数, 责令担保人履行担保责任, 从而在一定程度上挽回造成的系统损失. 访问控制算法对承诺人的访问请求进行控制. 假设系统有多个授权人(如分布式环境下), 承诺人, 担保人和权限, 其两两之间可以是多对多关系, 用实体2关系(E2R)图表示如图 1.

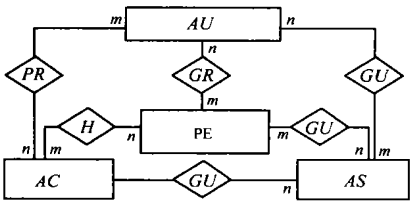

图 1　PABAC 构成要素之间的关系

其中 AU, AC, AS 和 PE 分别是所有授权人集合, 承诺人集合, 担保人集合和权限集合, 其中权限是被访问对象和对象上实施的操作的序偶(obj, op). PR, GR, GU 和H 分别表示承诺关系, 授权关系, 担保关系和拥有权限关系, n: m 表示多对多关系. PABAC 模型的体系结构如图 2.

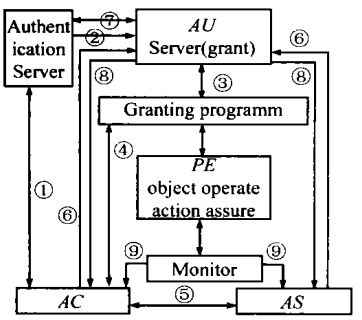

图 2　模型 PABAC 体系结构

在 PABAC 模型中, 每个权限需要何种承诺, 需要几个担保人, 采用何种担保结构, 以及需要担保的责任等均在权限定义中予以说明. 设映射 8: PE y 1 是权限担保责任函数, 其中 1 为非负整数集合. 对每一个权限 pe I PE, 8(pe) 表示 pe 所需要的全部担保责任.

PABAC 模型的授权过程描述如下:

Step1　认证服务器对权限请求人进行身份验证. 若权限请求人是系统合法用户, 则转 2, 否则给予否决处理.

Step2　认证服务器把权限请求人的访问请求转移给授权服务器以便进行访问控制.

Step3　授权服务器执行授权管理程序, 计算当前被请求权限所需要的最小承诺集合和候选担保人集合, 所求候选担保人必须满足担保人责任约束和职责分离约束(见第 2.2 和 2.3 节).

Step4　权限请求人与授权系统交互以动态创造某些授权必要条件, 授权系统给权限请求人返回最小承诺集合和候选担保人集合中的信息.

Step5　权限请求人按照所请求的权限担保要求与一个或多个候选担保人协商, 以便达成担保协议.

Step6　达成担保协议的权限请求人和担保人向授权服务器发送担保协议书.

Step7　授权服务器请求认证服务器对协议真伪进行验证.

Step8　若担保协议合法, 授权服务器批准承诺担保关系, 授予请求人权限并创建相应的担保人责任函数.

Step9　监控器(程序)对承诺担保责任履行事件进行监控.

2.2　承诺担保机制

根据不同的授权安全需要, PABAC 模型提供下列不同的担保机制. 为简单起见, 假设对于一个承诺授权一个担保人最多担保一次.

(1)无担保机制. 在这种情况下, PABAC 模型与现有的基于承诺的访问控制模型完全类似[1~3];

(2)简单担保机制($PABAC_0$). 一个授权仅需一个担保人为其担保. 模型简单, 但如果承诺得不到履行, 唯一的担保人也无法履行担保责任时, 授权安全性得不到保证. 因此, 适合安全性要求不高的领域;

(3)多方担保机制($PABAC_1$). 一个授权由多个担保人为其担保, 每一个担保人独立承担各自的担保责任, 但总的担保责任不小于权限定义中要求的担保责任. 当承诺得不到履行时, 系统责令每个担保人承担各自的担保责任. 它是一种扁平型担保结构. 如果承诺得不到履行, 而且某些担保人也无法履行担保责任时, 系统将无法挽回相应担保部分的损失. 它的优点是使担保风险分散化. 显然, 它比 $PABAC_0$ 安全;

(4)多级担保机制($PABAC_2$). 一个授权由一个担保人作首席担保, 由另外一个担保人为首席担保人的担保进行二级担保, 依此类推, 使多个担保人之间形成担保链(chain)式关系. 当承诺得不到履行时, 系统责令首席担保人承担全部担保责任. 如果首席担保人无法履行担保责任, 则由第二担保人承担全部担保责任, 依此类推, 它是一种线性多级担保结构, 担保责任沿担保链式关系传递. 因此, 它比 $PABAC_0$ 具有更高的

安全性. 但它使担保风险集中化了;

(5)混合担保机制(PABAC$_3$). 一个授权由多个担保人共同作首席担保,称这些担保人为首席担保人. 每一个首席担保人只承担权限的一部分担保责任. 一个或多个担保人可以为某一个担保人再承担担保责任,从而形成网络型担保关系. 它是 PABAC$_1$ 和 PABAC$_2$ 型担保的有机结合,是最复杂也是最安全的一种担保机制.

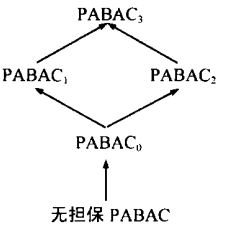

图3 担保机制安全级关系

上述担保结构的安全级别关系构成了一个格(lattice),如图3所示,沿有向边自底向上安全程度增加. 而 PABAC$_1$ 和 PABAC$_2$ 型担保的安全级别是不可比较的.

图4给出了承诺2担保机制的图形表示,其中 ac, pe, au 和 as 分别表示承诺人,权限,授权人和担保人. 设 AUR A AC@PE@AU 是承诺授权关系,三元组(ac, pe, au)表示授权人 au 授予承诺人 ac 权限 pe. 设 G(V, E)是承诺授权与担保关系标识有向图, V= AUR G AS 是顶点集合, E= {(x, [(ac, pe, au)], as$_i$)| x, as$_i$ I V, (ac, pe, au) I AUR, as$_i$ 为 x(授权或担保人)关于授权(ac, pe, au)的担保人}是标识有向边集合,其中[(ac, pe, au)]是有向边(x, as$_i$)的标识. 映射 K: E y l 是担保人责任函数, K((x, [z], as))表示担保人 as 为 x I AUR G AS 关于授权 z I AUR 所承担的担保责任. 对任意 x I AUR G AS, x 关于授权 z 的直接担保人集合为(x, [z])* = {as$_i$| x, as$_i$ I V, (x, [z], as$_i$) I E}, 被担保人 as 关于授权 z 直接担保的授权和担保人集合为*([z], as)= {as$_i$| as, as$_i$ I V, (as$_i$, [z], as) I E}. 授权(ac, pe, au)的所有担保人集合记作(ac, pe, au)**. 在不同担保模式下,承诺担保责任分别满足下列约束关系:

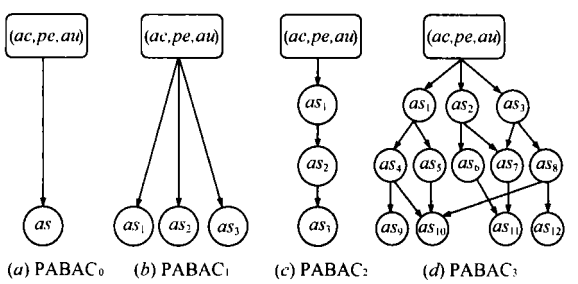

图4 承诺2担保机制图形表示

在担保模式 PABAC$_0$ 下,授权(ac, pe, au) I AUR 有唯一的担保人 as I AS, 下列公式成立:

$$K((ac, pe, au), [(ac, pe, au)], as) = 8(pe) \quad (1)$$

设|(ac, pe, au)**| = n. 在担保模式 PABAC$_1$ 下,下列公式成立:

$$\sum_{i=1}^{n} K((ac, pe, au), [(ac, pe, au)], as_i) = 8(pe) \quad (2)$$

在担保模式 PABAC$_2$ 下,下列公式成立,其中 1[i[n-1,并且 1[j[n.

$$\begin{cases} K(((ac, pe, au), [(ac, pe, au)], as_1)) = 8(pe) \\ K(as_i, [(ac, pe, au)], as_{i+1}) = 8(pe) \\ |(as_j, [(ac, pe, au)])^*| = 1 \end{cases} \quad (3)$$

在担保模式 PABAC$_3$ 下,对 P(ac, pe, au) I AUR, P as. I (ac, pe, au)**,下列公式成立:

$$\begin{cases} \sum_{as \in ((ac, pe, au), [(ac, pe, au)])^*} K((ac, pe, au), [(ac, pe, au)], as) = 8(pe) \\ \sum_{as \in (asc, [(ac, pe, au)])^*} K(asc, [(ac, pe, au)], as) = \\ \qquad \sum_{as \in (as, [(ac, pe, au)], asc)^*} K(as, [(ac, pe, au)], asc) \end{cases} \quad (4)$$

对 P as I AS, as 的担保能力用函数 D(as, val, t) I l 定义,其中 val 是 as 的信用度(值), t 是时间,它表示在时刻 t 担保人 as 的最大担保能力. 在任意时间 t, as 能够承担的全部担保责任必须小于或等于 D(as, val, t). 即

$$\sum_{x \in (ac, pe, au) I AUR} K(x, [(ac, pe, au)], as) [D(as, val, t) \quad (5)$$

2.3 承诺担保授权职责分离

设 APAA A AC@PE@AS@AUT 是承诺担保授权关系,承诺担保授权模式(简称授权模式)定义为 m= (x_{ac}, x_{pe}, x_{as}, x_{au}),其中 x_{ac}, x_{pe}, x_{as}, x_{au} 分别是承诺人,权限,担保人和授权人变量,也称为模式的属性,其取值范围是 dom(x_{ac}) I AC G {* }, dom(x_{pe}) I PE G {* }, dom(x_{as}) I AS G {* }, dom(x_{au}) I AUG {* },符号/ * 0的语义为任意承诺人,权限,担保人或授权人. 四元组(ac, pe, as, au) I APAA 表示授权人 au 在担保人 as 的担保之下授予承诺人 ac 权限 pe; (* , pe, as, au)表示授权人 au 在担保人 as 的担保之下授予任意承诺人权限 pe. 符号/ * 0在四元组其他位置上的语义与此相似. 所有承诺担保授权模式的实例构成承诺担保授权关系.

承诺担保授权职责分离约束是指禁止承诺人,担保人和授权人利用其固有的某些特殊关系(如亲戚关系等)获取某些授权,从而可能制造访问欺诈行为的机制,把这种特殊关系称作授权模式属性值互斥关系. 例如,通常情况下不允许妻子给其丈夫担保,父亲不可给自己的儿子授予某权限,等等. 除存在授权模式属性值互斥关系之外,不同的授权模式实例之间也可能存在互斥关系. 例如,假设已经存在授权关系实例(ac_q, pe_j, as_k, au_l),表示 au_l 在 as_k 担保下授予 ac_q/ 会计0权限 pe_j,如果再创建关系(ac_q, pe_o, as_k, au_l),表示 au_l 在 as_k 担保下授予 ac_q/ 出纳0权限 pe_o,则违反财务安全准则(同一人不允许同时拥有会计和出纳权限). 把这种互斥关系称为授权模式实例互斥关系. 显然,授权模式属性值互斥关系和实例互斥关系都具有自反性,对称性和传递性. 互斥关系使模型 PABAC 具有表达授权、承诺和担保职责分离约束的能力. 所有存在互斥关系的授权模式实例和实例偶对的集合记作 EX. 设 ac I AC, as I AS, pe I PE, au I AU,同一授权模式的实例属性值之间的互斥约束规则定义如下:

$$\forall ac \forall pe \forall as \forall au: (ac, pe, as, au) I EX] (ac, pe, as, au)| APAA \quad (6)$$

$$\forall ac \forall pe \forall as \forall au: (ac, pe, as, au) I APAA] (ac, pe, as, au)| EX \quad (7)$$

$$P au \forall ac \forall pe \forall as: (ac, pe, as, *) I EX] (ac, pe, as, au)| APAA \quad (8)$$

$$Pasv\,acv\,pev\,au:(ac,pe,*,au)\ I\ EX]\ (ac,pe,as,au)\ |\ APAA \quad (9)$$

$$Ppev\,acv\,asv\,au:(ac,*,as,au)\ I\ EX]\ (ac,pe,as,au)\ |\ APAA \quad (10)$$

$$Pacv\,pev\,asv\,au:(*,pe,as,au)\ I\ EX]\ (ac,pe,as,au)\ |\ APAA \quad (11)$$

$$PacPpev\,asv\,au:(*,*,as,au)\ I\ EX]\ (ac,pe,as,au)\ |\ APAA \quad (12)$$

$$PacPasv\,pev\,au:(*,pe,*,au)\ I\ EX]\ (ac,pe,as,au)\ |\ APAA \quad (13)$$

$$PacPauv\,pev\,as:(*,pe,as,*)\ I\ EX]\ (ac,pe,as,au)\ |\ APAA \quad (14)$$

$$PpePasv\,acv\,au:(ac,*,*,au)\ I\ EX]\ (ac,pe,as,au)\ |\ APAA \quad (15)$$

$$PpePauv\,acv\,as:(ac,*,as,*)\ I\ EX]\ (ac,pe,as,au)\ |\ APAA \quad (16)$$

$$PasPauv\,pev\,ac:(ac,pe,*,*)\ I\ EX]\ (ac,pe,as,au)\ |\ APAA \quad (17)$$

对于同一个授权模式实例中出现三个/ * 0符号的情况, 被认为该授权实例是毫无意义的, 因此不予讨论. 例如, (ac, * , * , *) 解释为承诺人 ac 永远不能获得任何授权, 因此应该将其从 AC 集合中删除.

不同的授权模式实例之间的互斥约束规则定义为:

$$(ac_q,pe_j,as_k,au_l)\ I\ APAAC(ac_n,pe_o,as_r,au_s)\ I\ APAA]$$
$$((ac_q,pe_j,as_k,au_l),(ac_n,pe_o,as_r,au_s))\ |\ EX \quad (18)$$
$$((ac_q,pe_j,as_k,au_l),(ac_n,pe_o,as_r,au_s))\ I\ EX]$$
$$å((ac_q,pe_j,as_k,au_l)\ I\ APAAC(ac_n,pe_o,as_r,au_s))\ I\ APAA) \quad (19)$$

使用符号/ * 0很容易从规则(18) 和(19) 演变出大量实例互斥的* 规则, 限于篇幅, 本文不再一一列举.

如果存在实例 (ac_q,pe_j,as_k,au_l), 必须存在实例 (ac_n,pe_o,as_r,au_s), 才能完整表达授权策略的语义, 则这两个授权实例协同[5]. 协同关系使 PABAC 模型具有表达授权、承诺和担保职责协同的良好机制. 例如, 在会计审计系统中, 会计权限和审计权限(角色) 必须授予两个不同的权限请求人, 并且必须先授予审计权限之后才允许授予会计权限(撤消权限顺序相反), 在这种情况下, 才能保证会计审计的安全性[5]. 所有协同的授权实例对偶构成的集合记作 COOP. 协同授权实例约束规则定义如下:

$$((ac_q,pe_j,as_k,au_l),(ac_q,pe_o,as_r,au_s))\ I\ COOP]$$
$$(ac_q,pe_j,as_k,au_l)\ I\ APAAC(ac_n,pe_o,as_r,au_s)\ I\ APAA \quad (20)$$

如果两个协同的承诺担保授权之间存在序约束, 则

$$((ac_q,pe_j,as_k,au_l),(ac_n,pe_o,as_r,au_s))\ I\ COOP]$$
$$(ac_q,pe_j,as_k,au_l)\ I\ APAAy(ac_n,pe_o,as_r,au_s)\ I\ APAA \quad (21)$$

根据系统需要, 还可以定义授权实例协同的* 规则. 在任意时刻, 集合 EX 和 COOP 的交集是空集, 以保证承诺担保授权的一致性. 即

$$COOP\ H\ EX=\ 5 \quad (22)$$

214　承诺担保监控与访问控制

承诺2担保监控实现可以采用主动数据库触发器技术[6], 其中承诺人访问请求为事件, 承诺是否履行为条件, 授权系统执行担保函数是行为, 即事件2条件2行为规则, 简称 ECA 规则. 限于篇幅, 有关 ECA 规则形式定义请参阅主动数据库有关文献[6]. 设承诺人(权限请求人) 访问请求为 (ac, pe, au), PABAC 模型的访问控制过程描述如下:

Step1　在授权日志中查找当前被请求权限 pe 是否已授予请求人 ac, 若未授予, 则系统执行授权过程, 转 4. 否则, 转 2.

Step2　在承诺日志中检查截止当前时刻请求访问的承诺人应该履行的承诺是否已全部履行. 若否, 则否决当前访问请求, 降低承诺人信用度, 撤消承诺人 ac 的权限 pe, 转 3. 否则, 允许承诺人执行访问, 转 4.

Step3　授权系统按 ac 未履行承诺的权限担保类型执行担保人责任函数, 责令相应的担保人承担担保责任.

Step4　结束.

设 z I AUR 是任意授权, x I AURGAS, x 关于z 的直接担保人集合为 $(x,[z])^*$, K((x, [z], as)) 表示担保人 as 为x 关于授权z 所承担的担保责任. 担保人 as 的担保能力用函数 D(as, val, t) I 1 定义, 其中 val 是as 的信用度(值), t 是时间, 它表示在时刻 t 担保人as 的最大担保能力, F (as, t) 表示担保人 as 的当前系统权益(如银行帐户存款额等), W(ac, pe, au, t) I No 表示系统当前应有的权益. 为描述简短, 担保人责任函数使用类 Pascal 语言递归定义如下:

```
Function assure( x, z): integer;
  Var y: integer
  Begin
    If (x, [z])* = 5 then return(0) /* 若无担保人, 则返回* /
      else for any as I (x, [z])*
/* 使 x 关于z 的每个直接担保人as 履行担保责任. 若 as 能够承担其担保责任, 则履行担保责任, 并给其信用度一个增加值 B, 作为激励. 否则使其信用度值减少 A, 作为惩罚, 并责令 as 关于z 的直接担保人履行担保责任* /
  if F ( as, t) \ ((x, [z], as)) /* as 能够承担担保责任* /
  then begin
         as. val z as. val+ B /* as 的信用度增加B * /
         F ( as, t) z F (as, t)- K((x, [z], as))
         W( ac, pe, au, t) z W( ac, pe, au, t)+ K((x, [z], as))
       end
    else begin
      If D( as, val, t) < A thenD( as, val, t) z 0
        else D( as, val, t) z D(as, val, t)- A;
        y= assure( as, z)
    end;
  End.
```

3　模拟实验结果

抽象的信贷消费贷款过程是一种典型的基于承诺的访问控制案例, 正得到访问控制领域深入地研究[3]. 以某银行信贷消费贷款业务为背景设计的 PABAC 模型原形进行实验. 假设用户已通过身份认证并成功提交了一个贷款申请, 则系统根据申请内容给用户提出一个或多个未来分期归还贷款的计划供其选择. 如果用户向系统承诺未来按某一计划归还贷款, 并且提供合法的承诺履行责任担保人, 则系统批准其贷款申请, 用户身份变为承诺人并获得贷款使用权限. 其中担保人是银行储蓄客户, 担保规则是当承诺人未按期履行其承诺时, 系统自动按担保协议从担保人帐户划拨担保资金入银行帐户以补偿银行损失. 随机选取一组使用贷款的承诺人, 假设每个承诺人或担保人按期履行承诺或担保责任的概率是 0. 5. 随不履行承诺人数增加, 在不同担保模式下银行损失变化情况如图

5. 可以看出, 无担保模式下损失上升最快, 多方多级担保模式下损失上升最慢, 简单担保模式下损失上升慢于无担保模式下的损失上升而远快于其他三种担保模式下的损失上升. 实验结果与本文的理论结果是一致的. 随机选择某承诺人使用特定贷款的权限进行实验, 随担保人数(包括担保层次数)增加, 在不同担保模式下银行损失下降情况如图 6. 可以看出, 在模式 $PABAC_3$ 下银行损失下降最快, 在模式 $PABAC_1$ 或 $PABAC_2$ 下银行损失下降慢于模式 $PABAC_3$ 下的损失下降, 而模式 $PABAC_0$ 下损失下降不变. 实验结果与本文的理论结果也是一致的.

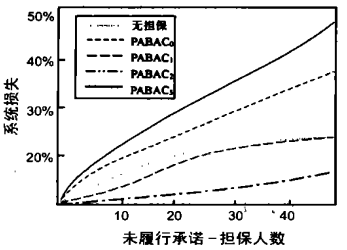

图 5 银行损失上升

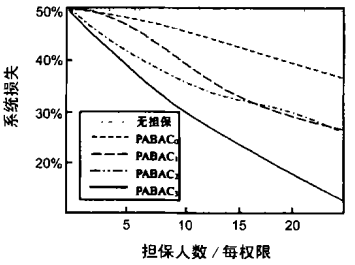

图 6 银行损失下降

4 结论

本文提出的基于承诺2担保的访问控制模型(PABAC)克服了传统访问控制系统封闭式处理访问请求和无法处理未来可满足授权条件的缺陷. 授权系统与授权请求人交互, 授权请求人对作为授权必要条件的未来行为作出承诺, 担保人为授权请求人履行承诺承担担保责任. 模型 PABAC 具有良好的授权灵活性和安全性, 它能够满足电子商务, 电子政务等新型应用对基于承诺的访问授权安全需要. 原型实验结果表明, 模型 PABAC 能够有效降低基于承诺的访问控制安全风险. PABAC 模型与传统的访问控制模型集成方法和高效的承诺担保授权约束实施算法将另文介绍.

参考文献:

[1] C Bettini, S Jajodia. Provisions and obligations in policy management and security applications[A]. In the proceedings of the 28th VLDB conference[C]. USA: VLDB press, 2002.

[2] S Jajodia, V Subrahmanian. Provisionalauthorizations[M]. USA: Kluv2erAcademic Press, 2001. 133- 159.

[3] C Bettini, S Jajodia. Obligation monitor in policy management[A]. In the proceedings of the IEEE 3rd internal conference on policies for dis2tributed systems and network[C]. USA: IEEE Press, 2002. 158- 178.

[4] R T Simon, M E Zurko. Separation of duty in role2based environments[A]. Proceedings of ACM on Computer Foundations Workshop[C]. USA: ACM Press, 1997. 43- 55.

[5] 王小明, 赵宗涛, 马建峰. 一种新的 RBAC 角色协同关系及其 Petri 网模型[J]. 电子学报, 2003, 31(2): 225- 227.

[6] N W Paton, O Diaz. Active database system[J]. ACM Computing Sur2veys, 1999, 31(1): 63- 103.

作者简介:

王小明 男, 1964 年 12 月生于甘肃省天水市, 博士, 副教授, 主要研究方向是信息系统安全, 访问控制与数据库. Email: wangxm@snnu. edu. cn.

赵宗涛 男, 1945 年出生于江苏省徐州市, 教受, 博士生导师, 主要研究方向是信息系统安全, 数据库与知识库.

马建峰 男, 1964 年出生于陕西省西安市, 教授, 博士生导师, 主要研究领域为信息安全与计算机网络, 密码学.