中国科学 E 辑: 信息科学
2007 年 第 37 卷 第 2 期: 254~271
http://www.scichina.com
《中国科学》杂志社
SCIENCE IN CHINA PRESS

一个支持空间上下文的访问控制形式模型

张 宏* 贺也平 石志国

(中国科学院软件研究所, 北京 100080; 中国科学院研究生院, 北京 100039)

摘要 利用上下文信息对授权决策进行控制已越来越受到重视. 在无线和移动网络领域中控制资源的访问要求定义支持空间上下文的访问控制形式模型. 然而, 传统的 RBAC 模型并不能满足这些空间上的需求. 文中对现有的 RBAC 模型进行扩充, 提出了 SC-RBAC 模型, 使其在定义安全策略时能结合用户的当前物理位置信息. 提出了空间角色的概念, 为角色赋予逻辑位置域以指定角色可以活动的空间范围. 角色激活依赖于用户从移动终端获得的当前物理位置. 紧接着, 给 SC-RBAC 引入层次来表达权限、激活继承等关系. 证明用层次化的空间角色在数学上可构建格模型以实施多级安全策略, 使其更适合安全关键的位置感知信息系统对信息流的安全控制要求. 随后, 受限的 SC-RBAC 描述了 3 类限制: 空间的职责隔离限制、基于位置的基数限制和基于位置的时序限制, 这些限制允许表达位置感知系统中细粒度的空间语义. 最后, 为受限的 SC-RBAC 模型设置了 9 个不变量, 证明了其基本安全定理, 为模型在实际环境中的应用奠定了基础.

关键词 信息安全 **RBAC** 空间上下文格 多级安全 限制 形式模型

访问控制是计算机安全中非常重要的一个方面, 它通过限制主体(或用户)对客体(或资源)的访问来提供保护系统资源的框架. 传统的访问控制模型(如强制访问控制、自主访问控制、基于角色的访问控制RBAC[1,2])都是典型的非上下文敏感的, 它们需要复杂而又静态的认证基础设施. 在某些情形下, 与用户标识相比, 访问控制更加依赖于用户的上下文. 此外, 当前的访问控制机制常常让终端用户背负不必要的安全相关的负担. 例如, 期望用户从会话一开始就担任某一角色, 从而导致不必要的多次登录. 而另一种选择是, 用户可自动地执行其拥有的级别最高的角色以获得该角色的权限, 且被认为能可信地执行安全策略, 不会滥用授予的特权. 目前, 人们越来越认识到在授权决策中利用上下文信息的重要性, 专门引入的上下文敏感的访问控制原则就用来解决这些问题 [3—12]. 若访问控制时能结合用户的或组的上下文信息, 则安全服务可变得更为用户友好、更为灵活.

无线和移动网络领域的迅猛发展培育出了新一代的设备, 它们适合于用作位置技术的传

收稿日期: 2006-07-12; 接受日期: 2006-10-13
* 联系人, E-mail: hong@ercist.iscas.ac.cn

感器、可计算工作环境中的相对位置和用户移动. 基于位置的服务和基于位置的移动应用程序的广泛部署迫切要求位置感知访问控制系统的支持, 这些应用程序需要基于位置的访问控制模型. 空间信息在这些模型中看成是一个关键的上下文参数.

空间感知的访问控制系统会存在这样几种需求: (1)个别用户只允许在他家和办公室的人们访问房间内的设备. (2)某个公司只允许在公司大楼某些特定区域内的用户访问给定的资源. (3)一个位置感知机构为了实现机密性只允许存在从低到高的信息流. (4)两个冲突位置区域的资源不能被同一用户访问. (5)当前处于某个空间区域的用户数量不能超过规定的上限. (6)只能在给定的时间间隔内访问某些位置区域.

为了满足上述列出的要求, 需要提出一种支持空间能力的访问控制模型 [13−15]. 在位置感知的应用程序中, 用户经常被分组为不同类别, 因此RBAC模型是个合理的选择. 情形(1)和(2)意味着空间数据的多粒度. 情形(3)表达了执行多级安全(Multi-Level Security)[16]的需求. 情形(4)表述了空间职责隔离和最小特权的要求. 从情形(5)可以看出基于位置的基数限制的要求. 情形(6)表达了空间信息的时间依赖性. 虽然目前出现了许多支持空间和基于位置的访问控制能力或限制的上下文感知的访问控制模型 [3,4,10,12,14], 但它们并不能满足上述的所有需求, 并且没有形式化关键组件给出系统清晰而又精确的定义.

本文将提出一个形式化的访问控制模型 SC-RBAC 来保证位置感知应用程序的安全. 为表达地理绑定的组织功能, 提出了空间角色的概念. 为说明角色的空间边界, 引入了逻辑位置域的概念. 紧接着, 对 SC-RBAC 进行扩充以处理空间角色层次结构, 证明层次化的空间角色可构成数学上的格序. 空间角色的格模型允许信息在格中从低往高向上流动, 并可通过使用这个格模型来控制信息流的安全. 此外, 还考虑了空间的职责隔离限制、基于位置的基数限制和基于位置的时序限制. 总之, 本文的主要贡献体现在 3 个方面: 提出了一个支持空间上下文的访问控制系统的形式化模型; 详细分析了空间角色的格模型, 允许表达多级安全策略; 扩充了 RBAC 的限制: 提出了空间职责隔离限制来处理冲突位置域, 提出了基于位置的基数限制和基于位置的时序限制, 并证明了其基本安全定理.

本文的其他部分将组织如下: 第 1 节简要介绍位置探测的各种技术, 研究怎样描述位置, 然后给出作为本文研究工作基础的相关定义. 第 2 节形式化描述 SC-RBAC 模型. 第 3 节讨论 SC-RBAC 模型的空间角色层次, 证明空间角色集可形成格. 格模型是表达多级安全策略的一种方法. 第 4 节给出受限的 SC-RBAC 模型和它的 9 个不变量, 然后解释怎样通过状态转换来保持 SC-RBAC 的安全属性. 第 5 节给出了模型的一个简单应用实例. 第 6 节介绍研究的相关工作. 第 7 节对文章进行总结, 并指出进一步研究的方向.

1　预备知识

为了能让 RBAC 支持空间感知, 我们需要研究怎样获取物理位置和怎样描述位置. 本节首先对位置检测技术进行分类, 介绍位置描述的方法, 然后引出相关的定义, 如逻辑位置域和位置映射函数.

1.1　位置探测

为了能让系统基于用户所在的空间维作出授权决策, 仲裁者必须获取提出访问请求的移动终端的位置信息. 目前存在几种评估移动终端位置的检测技术. 如使用 GPS(全球定位系统)

接收器可得到地理空间坐标. GPS 只能用来确定移动终端在室外的物理位置. 至于移动终端的室内位置追踪, 我们可以把居住地址信息或房间的位置属性储存在蓝牙设备中或配有 Wi-Fi 卡的手提电脑中. 当用户持有带蓝牙支持的设备进入房间时, 通过蓝牙的基站就可获得房间的位置信息. 此外, 电子标签(RFID)可嵌入到许多日常生活的物体中, 当物体接近电子标签阅读器时就可提供局部化的位置评估. 决定采用什么类型的位置评估技术依赖于对移动终端位置精确性方面的要求, 这也是系统在执行授权过程时所要求的. 例如, 某用户请求访问大楼内某一给定房间内的某安全设备时, 就需要较细粒度的支持以保证用户不会访问到来自隔壁房间的服务.

虽然详细比较这些探测技术已超出了本文的研究范围, 但值得注意的是它们在许多方面都存在差别, 其中包括: 所覆盖的地理面积的范围、工作在室内还是室外、清晰度、精确度、受干扰的可能性、花费、位置是由中央服务器确定还是由设备本身确定.

有了这些位置检测技术的支持, 可很容易地获取用户的当前物理位置, 因此, 我们假设 *GetLoc*(*u*)表示用户的当前物理位置.

1.2 位置描述

上下文感知的应用程序需要描述位置,需要用位置来为物理环境建模. 在不同领域中提出的各种位置模型可分为两类 [17]:

- 层次式的 (拓扑的、描述的或符号的, 比如房间).
- 笛卡尔的 (坐标的、公制的或几何的, 比如 GPS).

由于层次式的位置模型可很好地表达空间关系(比如包含和接近), 且具有良好的用户可读性, 所以我们决定采用它来表达位置. 层次式的位置模型有自描述的位置表示特性, 可把物理环境分解成不同级别的空间. 例如, 中国科学院软件研究所可分解为几个不同的子空间: 1 号楼, 2 号楼, 3 号楼, 4 号楼等. 每栋楼又可以分为更小的组成子空间, 直到我们达到足够的精度. 这样的层次称作空间树, 空间树的每个节点对应于物理环境中的一个实际空间. 树中的父子连接意味着两个空间之间的超级空间/子空间的关系. 图 1 给出了软件研究所的部分空间树. 由位置服务设计者来决定怎样划分物理环境.

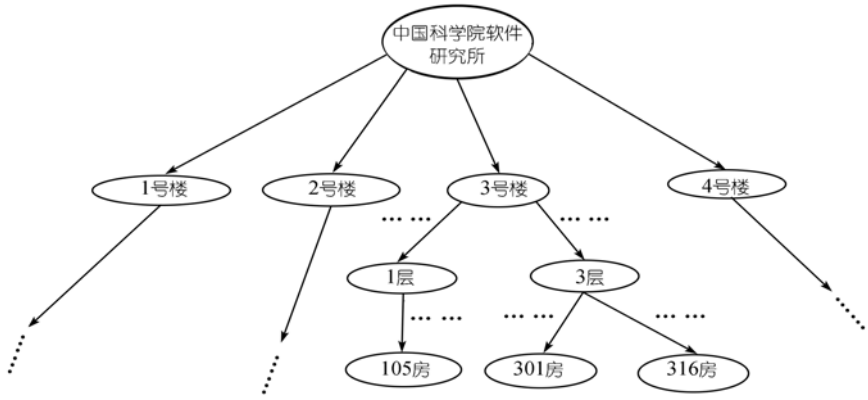

图 1 层次式的空间树

在 SC-RBAC 中用 *RLOC* 来表示实际位置的集合. 我们假设 *RLOC* 定义的区域覆盖了 SC-RBAC 的整个职责区域. *RLOC* 可划分为子域, 称为物理位置域, 表示为 π_i (i=1, …, k), 它

反映了基层结构可把用户位置唯一映射到特定房间的能力, 如 1025 号房间. 我们假设基础结构不能区分 π_i 里的不同位置. 然而, 在 SC-RBAC 中使用物理位置域并不实际, 因为物理位置域代表了位置检测系统的基础结构, 我们需要结构化的位置域来反映组织机构的基础结构. 因而, 我们引入逻辑位置域来表达组织机构的位置基础结构和组织机构的安全策略. 例如, 在某个公司内部可定义逻辑位置域表示部门、公共区域、单个办公室等位置.

定义 1 (逻辑位置域)　逻辑位置域定义了用户所承担的角色的逻辑空间边界. 由所有逻辑位置域组成的集合表示为 *LDOM*.

通常, 物理位置域和逻辑位置域之间存在紧密关联, 逻辑位置域可由物理位置域构成. 例如, 公司内某部门的部署可用位置表达式 $DepDom = [\pi_1, \pi_2]$来表示, 它指的是物理位置域 π_1 和 π_2 覆盖的区域. 逻辑位置域还可使用给定的位置映射函数从实际位置计算而出, 位置映射函数是与应用相关的.

定义 2(位置映射函数)　假设 *RLOC* 表示实际位置的集合, *LDOM* 表示逻辑位置域的集合, 则位置映射函数为 $MapLoc: RLOC \rightarrow LDOM$, 表示给定一个真实位置 *rp*, 返回相应的逻辑位置域.

假设 *SADom*, *SMDom*, *PMDom*, *OtherDom* 4 个逻辑位置域分别表示放置商业合同的安全区域、销售经理的办公室、工资经理的办公室和公司的其他区域, 则我们可把公司覆盖的空间区域定义为 $CompDom = SADom + SMDom + PMDom + OtherDom$. 这个例子说明了用位置表达式定义新的逻辑位置域的思想. 值得指出的是, 同一物理位置可属于不同的逻辑位置域. 由于逻辑位置域可看成集合, 我们可用与集合论中的各操作相类似的域操作(如并、交、差、补等)来定义新的逻辑位置域. 我们还可用集合间的包含关系来判断一个位置域是否包含在另一个位置域中.

逻辑位置域之间或者物理位置与逻辑位置域之间的空间拓扑关系包括相切、交叉、重叠、分离、相等、包含等 [13]. 这些都为二元互斥关系, 包含了所有可能的拓扑情形, 它们是对Clementini等人在文献 [18]中提出的空间拓扑关系的求精. 例如, 只有当逻辑位置域*y*的所有位置也是逻辑位置域*x*的位置时, 逻辑位置域*x*与*y*之间的*Contains*(*x*, *y*)关系才成立.

2　SC-RBAC 模型

我们将对现有的 RBAC 模型进行扩展, 使其能够在定义安全策略时利用位置信息. 本节将给出 SC-RBAC 的形式化定义, 讨论空间角色和有效角色的概念.

2.1　SC-RBAC 的形式化描述

基于文献 [1]和 [2]对RBAC模型的形式化描述, 我们给出一个包含空间角色的访问控制模型的精确描述. SC-RBAC的主要概念是空间角色, 它把角色与逻辑位置域连接起来, 表示空间绑定角色的含义.

定义 3 (空间角色)　空间角色 $sr = (r, ldom) \in R \times LDOM$, 其中 *r* 表示角色名称, *ldom* 表示角色的逻辑位置域. 由空间角色组成的集合称为空间角色集, 记为 *SR*.

空间角色用来指定用户行使某角色时可能占据的位置粒度. 用户会被指派空间角色. 比如(*Sales Manager*, *SMDom*)为一个空间角色, 它表示承担 *Sales Manager* 角色的用户只能工作在 *SMDom* 域中. 通过使用位置映射函数我们总能判断用户的当前逻辑位置域是否包含在给定

的逻辑位置域中, 因而决定会话中的哪些角色是有效的. 下面的定义给出了 SC-RBAC 的形式化语义:

定义 4 SC-RBAC 的一般模型具有如下的组件:

• $U, R, SR, OP, O, S, RLOC, LDOM$ 分别表示用户、角色、空间角色、操作、客体、会话、物理位置和逻辑位置域.

• $PRMS = 2^{OP \times O}$, 表示权限集合.

• PA: $PRMS \times SR$, 表示一个多对多的权限和空间角色之间的关系.

• $AssignedPrms$: $SR \rightarrow 2^{PRMS}$, 表示一个空间角色到权限集的映射关系. 若给定空间角色 sr, 则 $AssignedPrms(sr) = \{p \in PRMS | (p, sr) \in PA\}$.

• $UA \subseteq U \times SR$, 表示一个多对多的用户和空间角色之间的指派关系.

• $AssignedSession$: $U \rightarrow 2^S$, 表示把用户分配到会话集的函数.

• $AssignedUser$: $SR \rightarrow 2^U$, 表示将空间角色映射到用户集的函数. 若给定一个空间角色 $(r,ldom) \in SR$, 则 $AssignedUser((r, ldom)) = \{u \in U | (u,(r,ldom)) \in UA\}$.

• $SessionUser$: $S \rightarrow U$, 表示把每个会话 s_i 映射到单个用户的函数, 其中用户 $SessionUser(s_i)$在整个会话的生命周期内是不变的.

• $SessionRoles$: $S \rightarrow 2^{SR}$, 表示把每个会话 s_i 映射到空间角色集的函数, 其中 $SessionRoles(s_i) \subseteq \{(r,ldom) \in SR | (SessionUser(s_i),(r,ldom)) \in UA\}$.

2.2 会话和角色

$SessionRoles(s)$表示在会话 s 中能潜在激活的角色. 一般地, 如果用户分配了几个角色, 则由他来授权决定激活哪个 $SessionRoles(s)$. 在本文中, 集成了空间信息的空间角色在本质上是动态的, 用户可不必直接选择将要被激活的角色. 依赖于用户在会话中所处的位置, 只有一部分角色才是有效的且能被授予权限. 角色将自动地由环境激活或非激活. 为了决定有效的会话角色, 系统将评估给定位置域与当前逻辑位置域之间的包含关系, 因此引入有效角色的概念来决定用户的最终权限.

定义 5 (有效会话角色) 有效会话角色定义为函数

$$EffectiveSessionRoles: S \times RLOC \rightarrow 2^{SR},$$

使得

$$EffectiveSessionRoles(ses,rloc)$$
$$=\{(r, lext) \in SR | (r,lext) \in SessionRoles(ses) \wedge ldom = MapLoc(rloc) \wedge Contains(lext, ldom)=True\}.$$

系统根据用户的当前物理位置自动地选择将要生效的空间角色.图 2 描述了选取有效会话角色的过程. 有效角色是决定授权或拒绝访问请求的基础, 也就是说用它来定义授权机制. 访问请求 ar 是四元组 $(ses,rloc,op,o)$, 表示会话 ses 中的用户在物理位置 $rloc$ 试图对客体 o 执行操作 op, 因此$(s,rloc,op,o) \in S \times RLOC \times OP \times O$. 授权机制截获这个访问请求, 只有会话用户处在物理位置 $rloc$ 授权机制, 分配给有效角色的权限集中包含权限 (op, o)时才会允许此访问请求.

定义 6 (授权函数) 给定某一访问请求 $ar = (ses,rloc,op,o) \in S \times RLOC \times OP \times O$, 如果满足如下要求, 则允许在实际位置 $rloc$ 提出的访问请求 ar:

$$(op,o) \in \bigcup_{sr \in EffectiveSessionRoles(ses,rloc)} AssignedPrms(sr).$$

当访问控制系统接收到访问请求, 它通过使用位置映射函数和用户当前的实际位置获取

用户的当前逻辑位置域, 从而判断当前逻辑位置域是否包含在角色的逻辑位置域中来决定有效角色集合. 只要权限(*op,o*)属于分配给会话 *ses* 的有效角色 *sr* 的权限集中, 访问控制系统才允许此访问请求.

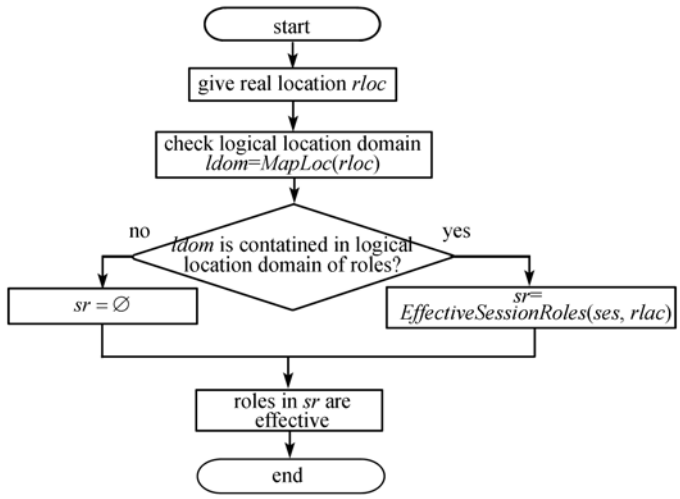

图 2　有效会话角色

3　SC-RBAC 中的层次

本节将扩展 SC-RBAC, 使其能处理空间角色层次, 为权限、用户和激活继承建模. 给出层次化的 SC-RBAC 模型(即为 SC-HRBAC)的形式化语义, 并且介绍多级安全(MLS)的概念. 然后, 证明针对多级安全的空间角色集合可形成数学上的格序, 不仅用它可以表达空间感知机构中敏感性的级别关系, 而且它也是用来表达多级安全策略的一种手段. 空间角色的格模型允许信息流在格中从低往高向上单向流动, 使得格模型更适合于控制某些安全关键的位置感知信息系统的信息流安全.

3.1　层次化的 SC-RBAC 模型

与层次化的RBAC模型给扁平RBAC模型添加角色层次关系的支持相类似 [1,2], 层次化的SC-RBAC模型也给SC-RBAC模型提供空间角色层次建模的支持. 根据文献 [1, 2]可知, RBAC中的角色层次定义了角色间的继承关系, 使得如果$r_i \leqslant \delta r_j$则意味着: (i) r_j 继承指派给r_i的所有权限; (ii) 指派了角色r_j的用户同时也被指派了角色r_i. 此外, 由于SC-RBAC引入了有效角色的概念, 因而假设下面的事实成立: (iii) 如果角色 r_j是有效的, 则用户可在会话s中承担该角色, 因而角色r_i在会话s中也是有效的.

在讨论空间角色间的继承关系时要考虑两种情形. 首先, 基本角色不同而逻辑位置域相同, 比如(r_1, $ldom_1$)和(r_2, $ldom_1$), 其中 $r_1 \leqslant r_2$, 则带有逻辑位置域 $ldom_1$ 的角色 r_2 继承具有相同逻辑位置域的低级角色 r_1 的所有权限.

另一种需要考虑的情形是基本角色相同而角色的逻辑位置域不同. 假设有两个空间角色(r, $ldom_1$)和(r, $ldom_2$), 其中逻辑位置域 $ldom_2$ 包含在逻辑位置域 $ldom_1$ 中, 则带有逻辑位置域 $ldom_2$ 的角色 r 必然继承带有较大逻辑位置域 $ldom_1$ 的角色 r 的所有权限. 在这种情形下, 我们

认为此处隐式地定义了逻辑位置域之间的层次关系.

总的来说, SC-HRBAC 模型形式化地定义如下:

定义 7 (SC-HRBAC 模型) SC-HRBAC 模型给 SC-RBAC 模型引入了空间角色间的偏序关系. 定义的层次如下:

• $SRH \subseteq SR \times SR$, 表示定义在空间角色集 SR 上的偏序关系, 即为空间角色层次关系. 只有满足 $r_1 \leqslant r_2$ 和 $ldom_2 \subseteq ldom_1$, $(r_1, ldom_1) \leqslant (r_2, ldom_2)$才会成立.

• $AssignedPrms$: $SR \to 2^{PRMS}$, 表示一个空间角色到权限集的映射关系. 若给定空间角色 sr, 则 $AssignedPrms(sr)$返回指派给 sr 和 sr 祖先的所有权限, 即为 $AssignedPrms(sr) = \{p \in PRMS | sr' \leqslant sr \wedge p \in AssignedPrms(sr')\}$.

• $AuthorizedUser$: $SR \to 2^U$, 表示一个空间角色到用户的映射关系. 若给定空间角色 sr, 则 $AuthorizedUser(sr)$返回被指派了 sr 和 sr 后代的所有用户, 即为 $AuthorizedUser(sr) = \{u \in U | sr \leqslant sr' \wedge (u, sr') \in UA\}$.

从上述的定义可很容易地得出下面的定理:

定理 1 令 $sr_i \in SR$, $sr_j \in SR$, 假设 $sr_j \leqslant sr_i$ 成立, 则具有下面的属性:

• $AssignedPrms(sr_j) \subseteq AssignedPrms(sr_i)$;

• $AuthorizedUser(sr_i) \subseteq AuthorizedUser(sr_j)$.

从上面的定义中可以看出空间角色间的次序关系对应于位置粒度的次序关系: 当逻辑位置域变得更为狭小时, 角色也会跟着变得更为具体, 即越高级的角色工作在越狭小的空间区域内.

3.2 多级安全(MLS)

多级安全策略通常用于控制信息系统的信息流, 它用安全级别的格来定义 [16]. 格定义了级别间的偏序关系, 称之为支配关系. 在许多情形下, 级别由两部分组成: 一个表示敏感度的有序序列元素(也就是不保密的、机密的、秘密的、绝密的)和一个范畴集合. 在这种情形下, 如果级别a的敏感度, 不小于级别b的敏感度并且级别b的范畴集合是级别a的范畴集合的子集, 则称级别a支配级别b. 然而, 级别并不一定要求都为这种结构. 分配给主体的级别代表它受信任的程度, 分配给客体的级别表示客体所含信息的敏感程度. 访问操作可分类为读和(或) 写. 在Bell-LaPadula版本的多级安全中规定 [19], 如果主体的级别支配客体的级别, 则允许主体执行读操作; 如果主体的级别由客体的级别来支配, 则主体可执行写操作. 多级安全主要应用在需要实施机密性的环境中.

3.3 格结构的推导

本小节将得出空间角色的格模型. 这个格在分析空间角色具有支持多级安全策略的能力时非常有帮助, 即 SC-HRBAC 是表述多级安全策略的工具.

关于偏序集合和格的理论大家都比较熟悉且有大量文献对其进行了详细描述, 在此我们仅给出它们的定义, 更多的信息可参考文献 [20].

定义 8(偏序集) 偏序集为结构 $\boldsymbol{P} = (P, \leqslant)$, 其中 P 表示一个集合, $\leqslant$表示集合 P 上的二元关系, 使得对于所有的 $x, y, z \in P$ 都满足这 3 个条件: (i) $x \leqslant x$ (自反性), (ii) $x \leqslant y \wedge y \leqslant x \Rightarrow x = y$ (反对称性), (iii) $x \leqslant y \wedge y \leqslant z \Rightarrow x \leqslant z$ (传递性).

如果没有引入空间上下文, 则可用上述定义来为基于角色的访问控制指定角色层次, 即$(R, \leqslant)$为偏序集. 现在我们说明怎样把空间上下文建模为一个偏序集.

在 3.1 节中提到了不同的逻辑位置域提供不同的保护级别, 因此, 在空间感知的访问控制系统中根据不同的逻辑位置域应提供不同级别的权限. 逻辑位置域的层次对应于位置粒度的排序: 当逻辑位置域变得更小时角色就会变得更为明确, 即更高级的角色活动在更小的空间区域中. 因此, 逻辑位置域的层次$(LDOM, \supseteq)$ 是一个偏序集.

根据定义 3, 我们得出空间角色集$SR = \{(r, ldom)| r\in R \wedge ldom\in LDOM\}$, 即$SR$是$R$和$LDOM$的乘积. 在表示空间角色的格结构之前我们首先给出格的定义 [20].

定义 9 (格)　如果偏序集$(P, \leqslant)$的任意两个元素同时拥有最大下界和最小上界, 则把偏序集 $(P, \leqslant)$称作格.

下面证明层次化的空间角色在数学上可构成格模型:

定理 2　假设$\leqslant$是 SR 上的定义 7 给出的二元关系, $(R_1, LDOM_1) \leqslant (R_2, LDOM_2)$当且仅当$R_1\leqslant R_2$, $LDOM_1 \supseteq LDOM_2$, $R_1, R_2\in R$ 且 $LDOM_1, LDOM_2\in LDOM$. 如果集合 R 和 $LDOM$ 关于交、并运算是封闭的, 则$(SR, \leqslant)$是一个格.

证明　首先证明$(SR, \leqslant)$是一个偏序集. $\forall(R_1, LDOM_1)\in SR$, 因为 $R_1\leqslant R_1$, $LDOM_1\supseteq LDOM_1$, 意味着$(R_1, LDOM_1)\leqslant(R_1, LDOM_1)$, 所以$\leqslant$关系具有自反性. $\forall(R_1, LDOM_1), (R_2, LDOM_2)\in SR$, 如果$(R_1, LDOM_1) \leqslant (R_2, LDOM_2)$, $(R_2, LDOM_2) \leqslant (R_1, LDOM_1)$, 则有 $R_1 \leqslant R_2$, $R_2 \leqslant R_1$ 和 $LDOM_1 \supseteq LDOM_2$, $LDOM_2 \supseteq LDOM_1$, 因而得到 $R_1 = R_2$ 和 $LDOM_1 = LDOM_2$, 即有$(R_1, LDOM_1) = (R_2, LDOM_2)$, 所以$\leqslant$关系具有反对称性. $\forall(R_1, LDOM_1), (R_2, LDOM_2), (R_3, LDOM_3)\in SR$, 如果有$(R_1, LDOM_1) \leqslant (R_2, LDOM_2)$和$(R_2, LDOM_2) \leqslant (R_3, LDOM_3)$, 则有 $R_1 \leqslant R_2$, $R_2 \leqslant R_3$, $LDOM_1 \supseteq LDOM_2$, $LDOM_2 \supseteq LDOM_3$, 因而得到 $R_1 \leqslant R_3$, $LDOM_1 \supseteq LDOM_3$, 即为$(R_1, LDOM_1) \leqslant (R_3, LDOM_3)$. 所以$\leqslant$关系具有传递性. 由定义 8 得出$(SR, \leqslant)$是一个偏序集.

下面证明$(SR, \leqslant)$中的任意两个元素存在最大下界, 对任意的$(R_1, LDOM_1)$, $(R_2, LDOM_2)\in SR$, 分两种情形来讨论:

(i) $(R_1, LDOM_1)$和$(R_2, LDOM_2)$可以比较. 结论显然成立.

(ii) 如果$(R_1, LDOM_1)$和$(R_2, LDOM_2)$不可比, 即 $R_1 \not\leqslant R_2$, $R_2 \not\leqslant R_1$或$LDOM_1 \not\supseteq LDOM_2$, $LDOM_2 \not\supseteq LDOM_1$, 则构造出另一元素$(R_3, LDOM_3)$, 使得 $R_3= R_1\cap R_2$, $LDOM_3= LDOM_1\cup LDOM_2$.

首先证明构造出的$(R_3, LDOM_3)$是$(R_1, LDOM_1)$和$(R_2, LDOM_2)$的下界.

由于 $R_3= R_1\cap R_2$, 故

$$R_3 \leqslant R_1, \quad R_3 \leqslant R_2, \tag{1}$$

并且 $LDOM_3= LDOM_1\cup LDOM_2$, 故

$$LDOM_3\supseteq LDOM_1 \text{ 且 } LDOM_3\supseteq LDOM_2. \tag{2}$$

根据(1)和(2)式及定义可知$(R_3, LDOM_3) \leqslant(R_1, LDOM_1)$且$(R_3, LDOM_3) \leqslant(R_2, LDOM_2)$. 所以$(R_3, LDOM_3)$是$(R_1, LDOM_1)$和$(R_2, LDOM_2)$的下界.

下面证明$(R_3, LDOM_3)$是$(R_1, LDOM_1)$和$(R_2, LDOM_2)$的最大下界. 假设$(R_4, LDOM_4)$是$(R_1, LDOM_1)$和$(R_2, LDOM_2)$的任意一个下界, 则有 $R_4 \leqslant R_1$ 且 $R_4 \leqslant R_2$, $LDOM_4 \supseteq LDOM_1$ 且 $LDOM_4\supseteq LDOM_2$. 而 R_3 的取值是 $R_1\cap R_2$, 因而有

$$R_4 \leqslant R_3. \tag{3}$$

此外，由于 $LDOM_4 \supseteq LDOM_1 \cup LDOM_2$，而 $LDOM_3$ 的取值是 $LDOM_1 \cup LDOM_2$，故

$$LDOM_4 \supseteq LDOM_3. \tag{4}$$

根据(3)和(4)式可知

$$(R_4, LDOM_4) \leqslant (R_3, LDOM_3). \tag{5}$$

从上面的证明可知$(R_3, LDOM_3)$是$(R_1, LDOM_1)$和$(R_2, LDOM_2)$的下界，而对于$(R_1, LDOM_1)$和$(R_2, LDOM_2)$的任意一个下界$(R_4, LDOM_4)$都有(5)式成立. 所以$(R_3, LDOM_3)$是$(R_1, LDOM_1)$和$(R_2, LDOM_2)$的最大下界.

综合情形(i)和(ii)可知，$(SR, \leqslant)$中的任意两个元素的最大下界是存在的.

类似地，我们也可证明$(SR, \leqslant)$中的任意两个元素存在最小上界. 限于篇幅，证明过程略.

综合上述的讨论和定义 9，可知$(SR,\leqslant)$是一个格.

为了最后总结空间角色的格模型所具有的特性，我们将举一个实例进行说明. 考虑一个提供多级安全支持的位置感知系统. 假设存在角色R_1和R_2，R_2是R_1的高级角色，并且假设用来绑定角色的所有逻辑位置域为dm_1，dm_2和dm_3，则总共会存在 $2\times2^3=16$ 个空间角色. 这些空间角色代表了不同的权限和用户继承关系，越高级的角色活动在越小的空间区域内，拥有更多权限，只可指派给更少的用户. 逻辑位置域说明了位置的不同粒度. 图 3 给出了这些空间角色的格模型. 在此，安全标签的概念与空间角色的概念之间有很大的相似性. 空间角色间的支配关系定义为：只要满足$R_1 \geqslant R_2$和$LDOM_1 \subseteq LDOM_2$，则$(R_1, LDOM_1) \geqslant (R_2, LDOM_2)$. 绑定了整个逻辑位置域的角色，如$(R_1, \{dm_1, dm_2, dm_3\})$对应于公共信息和不保密的信息. 越高级的角色绑定的逻辑位置域就越小，如$(R_2, \{dm_1\})$对应于更加机密的信息. 值得注意的是，空间角色$(R_2, \{\})$和$(R_1, \{\})$为两个不会自然出现的角色，它们不会真实存在于SC-HRBAC模型中，也不会指派给系统中的任何一个主体. 事实上，引入这些特殊空间角色的目的是为了构成一个完整的格. 由定义可知，空间角色$(R_2, \{\})$是这个格的最小上界，它支配所有其他的空间角色. 这个空间角色的格模型允许信息流在格中从低到高向上流动，不允许信息流从高到低向下流动，也不允许信息流在不可比较的空间角色之间流动. 因此，使用这样的格模型能执行多级安全策略. 当然，格中的这种单向信息流不仅可用于机密性，还可用于完整性以及同时满足机密性和完整性的情形，或用于聚合策略，如中国墙 [21].

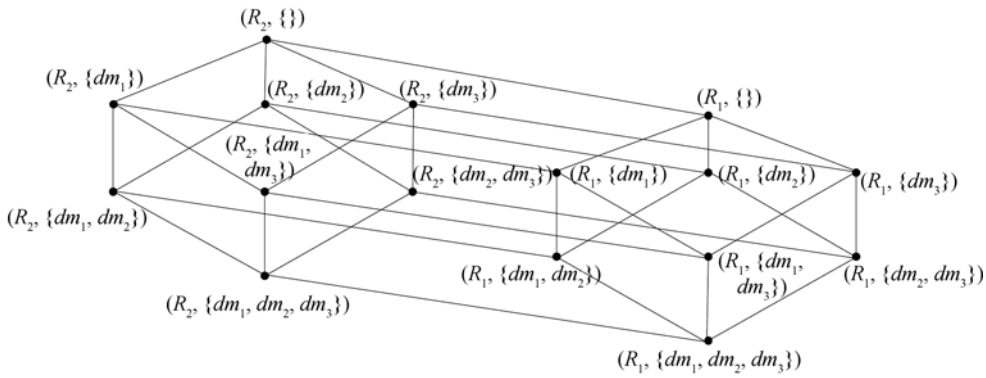

图 3 多级安全系统中空间角色的格模型

此外，值得说明的一点就是，当存在很多角色和逻辑位置域时，按照这种方式有可能生成

过于庞大的格模型. 而在实际应用中, 往往只会用到整个格模型的一小部分 1), 因此, 我们可根据真实的位置感知系统实例化这些空间角色.

4　受限的 SC-RBAC 模型

基数限制和职责隔离(SoD)限制对于保证应用程序的安全显得尤为重要. 不少研究者强调了在RBAC模型中使用基数限制和职责隔离限制的重要性 [1,22]. 然而, 据我们所知, 迄今为止并没有研究者提出基于位置的基数限制和基于位置的职责隔离限制. 此外, 基于位置的信息的一个重要特性就是时间依赖性, 也就是基于位置的信息只有在指定的时间区间内才是有效的. 我们应该提出基于位置的时序限制来解决这个问题, 因此, 受限的SC-RBAC模型给RBAC模型增加了空间职责隔离限制、基于位置的基数限制和基于位置的时序限制.

事实上, 为了表达当今大型系统中位置上的动态变化的访问控制需求, 还有可能需要更多的且必要的空间限制, 如对用户运动性方面的限制: 用户的速度、加速度、距离和前进方向等. 但本节仅关注这 3 种不同类型的限制. 我们首先给出它们的一些基本的形式化定义, 接着提出了受限 SC-RBAC 模型必须支持的一些不变量. 最后, 证明了受限 SC-RBAC 模型的基本安全定理.

4.1　空间职责隔离限制

我们在空间维上扩充了职责隔离的概念: 如果冲突角色不能用在同一位置域或同一角色不能用在冲突的位置域上时, 就给用户指派互斥的空间角色. 这种思想类似于静态职责隔离(SSoD)和动态职责隔离(DSoD), 它们主要用来限制用户可实施的权限. 不同于 SSoD 和 DSoD 的是, 互斥的空间角色依赖于用户所承担的基本角色和用户所处的逻辑位置域. 也就是说, 对于某一个给定的位置域, 指派给两个角色的权限可能会互斥. 而对于另一个位置域, 用户则有可能可以激活这两个角色. 因为指派给空间角色的权限集对于不同的位置会有所不同. 另一种情形是: 如果禁止角色处于某些给定的位置域, 则该角色就不能用于这些冲突的位置域.

(ⅰ) 空间静态职责隔离关系(SSSoD)实施某些限制以防止用户们在同一时刻获取用户和空间角色指派时发生利益冲突. 下面我们给出空间静态职责隔离一般化的形式定义:

定义 10 (空间静态职责隔离 SSSoD)　SSSoD $\subseteq (2^{SR}\times N)$是二元组$(rs, n)$的集合, 其中 rs 表示空间角色集, n 表示不小于 2 的自然数. 它具有的属性是: 不存在授权了多于 n 个空间角色的用户. 形式化地表示为

$$\forall (rs, n)\in \mathrm{SSSoD}, \forall t\subseteq rs : |t| \geqslant n \Rightarrow \bigcap_{r\in t} AuthorizedUser(r) = \varnothing .$$

空间静态职责隔离具有更强的表达能力, 它可以表达更加细粒度的隔离问题: 假设有两个角色在同一逻辑位置域中会发生冲突, 如果用户被指派了处于该逻辑位置域的角色, 则该用户就不能再指派给处于此逻辑位置域中的另一角色. 与此同时, 空间静态职责隔离还可以表示多边冲突问题: 假设存在两个冲突的逻辑位置域, 如果用户被指派了处于其中一个冲突逻辑位置域的角色, 则该用户就不能再指派给处于另一冲突逻辑位置域中的同一角色. 这仅仅是空间静态职责隔离关系的两种常见情形. 我们用图 4 来说明这两种常见情形. 如图 4(a)所

1) Smith G W. The modeling and representation of security semantics for database applications. Dissertation for the Doctoral Degree. Fairfax: George Mason University, 1990

示: 用户可在除了 $ldom_2$ 以外的任何位置域激活角色 R_1 和 R_2, 即$((R_1, ldom_2), (R_2, ldom_2))\in$SSSoD. 在经典的职责隔离中, 对$R_1$和$R_2$实施限制会导致任何用户都不能在整个位置空间(即位置域 $ldom_1$, $ldom_2$, $ldom_3$ 和 $ldom_4$)上指派这两个角色. 接着考虑如图 4(b)所示的情形: 任何用户都不会指派角色R_3给冲突的角色逻辑位置域, 即$((R_3, ldom_1), (R_3, ldom_3))\in$SSSoD. 这就允许我们表达更强的职责隔离限制.

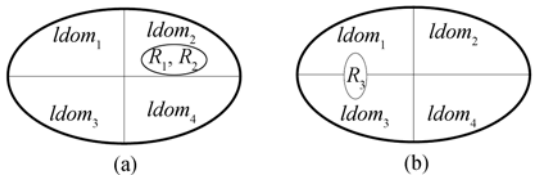

图 4 空间职责隔离的两种常见情形

(ii) 空间动态职责隔离关系(SDSoD)是为了限制用户权限以避免潜在的冲突, 它实施在激活的会话空间角色所分配的权限上. 下面先给出空间动态职责隔离一般化的形式定义:

定义 11 (空间动态职责隔离 SDSoD) SDSoD $\subseteq (2^{SR}\times N)$是二元组$(rs, n)$的集合, 其中 rs 表示空间角色集, n 表示不小于 2 的自然数. 它具有的属性是: 不存在可授权激活多于 n 个空间角色的用户. 形式化地表示为

$$\forall(rs, n)\in \text{SDSoD}, \forall s\in S, \forall t\subseteq SessionRoles(s)\cap rs : |t| \geqslant n \Rightarrow \bigcap_{r\in t} AuthorizedUser(r)=\varnothing .$$

在此仅仅讨论空间动态职责隔离关系的两种常见情形: 只有当在给定的逻辑位置域中激活会话角色不会发生冲突时, 空间动态职责隔离关系才允许给用户指派这些角色; 空间动态职责隔离关系也允许用户激活非冲突逻辑位置域上的角色. 如图 4(a)所示, 用户不能在位置域 $ldom_2$ 上同时激活单个会话中的角色 R_1 和 R_2, 即$((R_1, ldom_2), (R_2, ldom_2))\in$SDSoD. 如图 4(b)所示, 禁止用户在位置域 $ldom_1$ 和 $ldom_3$ 上同时激活单个会话中的角色 R_3, 即$((R_3, ldom_1), (R_3, ldom_3))\in$SDSoD. 这与传统的动态职责隔离相比有很多优点: 它可让限制只在给定的位置才能保持其合法性, 而传统的职责隔离把角色限制在整个组织空间.

为了很好地执行职责隔离的控制, 我们首先引入互斥逻辑位置域和互斥角色的概念, 然后基于文献 [23]提出空间互斥角色的概念.

定义 12 (互斥逻辑位置域) 称两个逻辑位置域互斥, 如果用户不能属于这两个逻辑位置域. 用 $ELDOM$ 表示互斥的逻辑位置域.

作为一个例子, 图 4(b)反映了这样的事实: $ldom_1$ 和 $ldom_3$ 为互斥逻辑位置域. 形式化地表示为: $(ldom_1, ldom_3)\in ELDOM$.

Kuhn描述了授权时互斥角色和运行时互斥角色 [23], 它们分别表示为ER_a和ER_r. 值得注意的是, 这里所指的互斥角色是相对于常规角色而言的, 与空间角色无关.

定义 13 (空间互斥角色) 称两个空间角色是授权时互斥的, 如果其中一个空间角色的成员集合与另一个空间角色的成员集合不相交. 授权时空间互斥角色用 SER_a 表示. 称两个空间角色是运行时互斥的, 如果系统中不允许存在这样的进程, 它能同时激活这两个空间角色. 运行时空间互斥角色用 SER_r 表示. 如果两个空间角色是授权时互斥的或运行时互斥的, 则简称它们是互斥的. 对于互斥的两个空间角色 i 和 j, 称它们的权限是完全互斥的, 如果对系统中任何与 i 不同的空间角色 k, i 的权限集合与 k 的权限集合不相交. 称空间角色 i 的权限与空间角色 j 的权限是部分互斥的, 如果至少存在一个权限 p, 使得 p 包含在 i 的权限集合中而不包含在 j 的权限集合中.

显然, 授权时空间角色互斥能实现空间静态职责隔离, 而运行时空间角色互斥能实施空

间动态职责隔离. 互斥的空间角色是实现空间职责隔离的一种有效方法.

4.2　基于位置的基数限制

文献中一般提到两种主要的基数限制——角色基数和用户基数 [2,24,25]. 然而, 本文所采取的使用空间信息来定义基数限制的方法可以让人们细粒度地表达访问控制策略. 作为进一步的考虑, 我们注意到在实际应用中也会存在非空间的基数限制. 非空间的基数限制相当于基于位置的基数限制的特殊情形, 即它们可用于任何位置.

定义 14 (基于位置的角色基数限制)　令 SR 表示空间角色集合, $\mathbb{N}$ 表示自然数集合, 则基于位置的角色基数限制定义为 LRC: $SR \rightarrow \mathbb{N}$, 即一个从空间角色到自然数的映射. 它描述了至多有多少个用户可被指派给这个空间角色.

值得注意的是, 空间角色本身包含空间信息, 即逻辑位置域, 因此不需要额外的空间参数来定义基于位置的角色基数限制.

定义 15 (基于位置的用户基数限制)　令 $LDOM$ 和 $\mathbb{N}$ 分别表示逻辑位置域的集合和自然数的集合, 则基于位置的用户基数限制定义为 LUC: $LDOM \rightarrow \mathbb{N}$, 即一个从逻辑位置域到自然数的映射. 它的语义是要求当前处在某个逻辑位置域中的用户数不会超过给定的数值.

4.3　基于位置的时序限制

当考虑位置感知的限制时, 需要解决基于位置的信息的时间依赖性问题, 即授权需要定义逻辑位置域的可允许的访问时间间隔. 如果没有这些限制则有可能造成空间信息的误用. 比如, 给普通的位置域分配工作日时间作为用户所允许的访问时间. 我们采用类似于文献 [26] 中的方法来描述时间限制. 时间单元表示一个时间子或固定数目的时间子, 时间子指的是最小的、不可见的时间单元. 用T表示时间集合, 时间间隔记为$tsp = [t_s, t_e]$, 它表示所有满足$t_s \leqslant tu \leqslant t_e$条件的时间单元$tu$, 其中$tu \in T$. 时间间隔的集合用$TSP$表示.

定义 16 (基于位置的时序限制)　基于位置的时序限制为一个二元组(tsp, $ldom$), 其中 $tsp \in TSP$ 表示用户可进入逻辑位置域 $ldom$ 的时间间隔$[t_s, t_e]$, $ldom \in LDOM$. 基于位置的时序限制集合记为 LTC. 假设给定一个时序限制 $ltc \in LTC$, 则 ltc_{tsp} 和 ltc_{ldom} 分别表示 ltc 在元组分量 tsp 和 $ldom$ 上的投影.

4.4　不变量

尽管Gavrila等人 [27]列出了RBAC的 20 个不变量, 但这些不变量没有考虑空间信息, 没有区分激活角色和有效角色, 没有考虑基于位置的各种限制, 特别是没有指出冲突的角色逻辑位置域, 因此仍然有一些不变量没有被考虑到. 在此, 我们给出受限SC-RBAC模型所支持的 9 个不变量.

Inv_1. 授权使用某个空间角色的用户数目不超过空间角色的基数, 形式化地表示为

$$\forall sr \in SR \bullet |AuthorizedUser(sr)| \leqslant LRC(sr).$$

Inv_2. 授权可处于某逻辑位置域的用户数目不能超过逻辑位置域的用户基数, 形式化地表示为

$$\forall u \in U, s \in S, \forall r \in R, \forall ldom \in LDOM \bullet | u \in SessionUser(s) \wedge (r, ldom) \in SessionRoles(s) \wedge u \in AuthorizedUser(sr) \wedge Contains(ldom, GetLoc(u)) | \leqslant LUC(ldom).$$

Inv_3. 如果用户可授权成为某空间角色的成员, 则此空间角色与用户原有的空间角色必

须兼容. 即, 如果两个空间角色在授权时互斥, 则它们不能授权给同一用户. 形式化地表示为

$$\forall u \in U, sr_i, sr_j \in SR \bullet sr_i \neq sr_j \wedge u \in AuthorizedUser(sr_i) \wedge u \in AuthorizedUser(sr_j) \Rightarrow (sr_i, sr_j) \notin SER_a .$$

Inv_4. 如果两个空间角色在同一会话中是有效的, 则这两个空间角色在运行时不互斥. 形式化地表示为

$$\forall sr_i, sr_j \in SR, \forall s \in S \bullet sr_i \neq sr_j \wedge (\exists rloc_1, rloc_2 \in RLOC \bullet sr_i \in EffectiveSessionRoles(s, rloc_1) \wedge sr_j \in EffectiveSessionRoles(s, rloc_2)) \Rightarrow (sr_i, sr_j) \notin SER_r.$$

Inv_5. 只有空间角色的常规角色授权时互斥或空间角色的逻辑位置域互斥, 空间角色才会发生授权时互斥; 只有空间角色的常规角色运行时互斥或空间角色的逻辑位置域互斥, 空间角色才会发生运行时互斥. 形式化地表示为

$$\forall r_i, r_j \in R, \forall ldom_1, ldom_2 \in LDOM \bullet ((r_i, ldom_1), (r_j, ldom_2)) \in SER_a \Rightarrow (r_i, r_j) \in ER_a \vee (ldom_1, ldom_2) \in ELDOM,$$

$$\forall r_i, r_j \in R, \forall ldom_1, ldom_2 \in LDOM \bullet ((r_i, ldom_1), (r_j, ldom_2)) \in SER_r \Rightarrow (r_i, r_j) \in ER_r \vee (ldom_1, ldom_2) \in ELDOM.$$

Inv_6. 用户的访问请求时间必须落入基于位置的时序限制对某逻辑位置域规定的时间间隔内. 形式化地表示为

$$\forall s \in S, \forall rloc \in RLOC, \forall requestingtime \in T, \forall ltc \in LTC \bullet (\exists r \in R, \exists ldom \in LDOM \bullet ldom = ltc_{ldom} \wedge (r, ldom) \in EffectiveSessionRoles(s, rloc) \wedge requestingtime \in ltc_{tsp}).$$

Inv_7. 如果用户授权为某空间角色的高级角色的成员, 则用户也可授权为此空间角色的成员. 形式化地表示为

$$\forall sr_i, sr_j \in SR,\ \forall u \in U \bullet sr_i \neq sr_j \wedge sr_i \leqslant sr_j \wedge u \in AuthorizedUser(sr_j) \Rightarrow u \in AuthorizedUser(sr_i).$$

Inv_8. 会话的有效角色也是可应用于此会话用户的空间角色. 形式化地表示为

$$\forall s \in S, \forall rloc \in RLOC \bullet EffectiveSessionRoles(s, rloc) \subseteq SessionRoles(s).$$

Inv_9. 能否让某一低级空间角色有效依赖于它的高级空间角色是否有效. 形式化地表示为:

$$\forall s \in S, \forall rloc \in RLOC, \forall sr_1 \in SR,\ \forall sr_2 \in SR \bullet sr_1 \leqslant sr_2 \wedge sr_2 \in EffectiveSessionRoles(s, rloc) \Rightarrow sr_1 \in EffectiveSessionRoles(s, rloc).$$

前两个不变量关注的是基于位置的角色基数和用户基数. 从不变量 3 到不变量 5 可以看出互斥的空间角色是实现空间职责隔离的一种手段. 不变量 6 说明用户的访问请求时间必须遵守基于位置的时序限制. 根据不变量 7 可以看出, 空间角色可继承它的祖先角色的权限. 不变量 8 和 9 关心的是有效会话角色的特性: 有效角色与会话角色间的包含关系和有效角色间的依赖关系.

4.5 基本安全定理

如果可以保证模型中的每个系统状态都是安全状态, 就可证明受限的 SC-RBAC 模型关于状态转换是保持安全的. 首先, 定义受限 SC-RBAC 模型中的系统状态和安全状态, 然后给出一些基本定义. 在完成基本安全定理的证明过程之后, 我们将简要讨论受限 SC-RBAC 模型的安全目标.

定义 17 (当前访问集) 当前访问集 $CAS \subseteq S \times RLOC \times T \times OP \times O$ 包含当前会话的用户在当前时间和当前物理位置对客体执行操作的记录.

定义 18 (系统状态) 受限 SC-RBAC 模型的系统状态 v 定义为: (CAS, U, SR, OP, O, S,

RLOC, *LDOM*, *PRMS*, *PA*, *UA*, *SRH*, *AssignedPrms*, *AssignedSession*, *AssignedUser*, *AuthorizedUser*, *SessionUser*, *SessionRoles*, *EffectiveSessionRoles*, *ELDOM*, ER_a, ER_r, SER_a, SER_r, ≤, *LRC*, *LUC*, *LTC*).

由于系统状态包含了模型的许多基本元素, 故用 $v=(CAS,OTHER)$来简化系统状态的表示, 其中 *OTHER* 代表系统状态 v 中的其他元素.

定义 19 (决策集)　决策集 D={"yes", "no", "error", "?"}, 其中"yes"表示访问请求被执行, "no"表示拒绝访问请求, "error"表示出现了某些未知的错误, "?"表示不能处理此访问请求.

定义 20 (请求序列集、决策序列集、状态序列集)　X 定义为所有请求序列 R 的集合; Y 定义为所有决策序列 D 的集合; Z 定义为所有状态序列 V 的集合. 每个 X, Y 和 Z 分别代表了请求、决策和状态的连续数值的序列集合.

定义 21 (状态转换关系)　假设 $\omega = \{\rho_1,\cdots, \rho_s\}$是一组规则集合, 则对于任何请求 $r_k\in R$、决策 $d_m\in D$、状态集 V、后续状态集 V'来说, 状态转换关系 $W(\omega)\subset R\times D\times V\times V'$定义为

(ⅰ) $(r_k,d_m,V', V)\in W(\omega)$, 当且仅当 $d_m\neq$"?"且 $d_m\neq$"error";

(ⅱ) 存在唯一的 i $(1\leqslant i\leqslant s)$, 使得$(d_m, V')= \rho_i(r_k,V)$.

定义 22(安全状态)　把满足以上 9 个不变量 Inv_i (i=1, …, 9)的系统状态 $v\in V$ 称为系统的安全状态.

定义23 (受限系统)　由状态转换关系 W 及初始状态 z_0 决定的受限系统$\sum(R, D, W, z_0)\subset X\times Y\times Z$, 是指集合$\sum(R, D, W, z_0)=\{(x, y, z)\in X\times Y\times Z|\ \forall t\in T, (x_t, y_t, z_t, z_{t-1})\in W\}$.

从上述定义可知, 从初始状态 z_0 出发, 输入 x 产生了决策 y 和状态 z 的后续状态. 系统$\sum(R, D, W, z_0)$包含了从状态 V_0 开始所有可能的执行序列.

为了定义安全的受限系统, 我们首先引入安全状态序列、外观(appearance)、安全外观的概念.

定义 24(安全状态序列、外观、安全外观、安全的受限系统)　如果对任意的 $i\in T$, z_i 是安全状态, 则状态序列 $Z=\{z_1, z_2, \cdots, z_i, \cdots\}$称为安全状态序列. 受限系统$\sum(R, D, W, z_0)$中的每个元素$(x, y, z)$称为系统的一个外观. 如果 z 是安全状态序列, 则受限系统$\sum(R, D, W, z_0)$中的某个外观(x, y, z)称为安全外观. 如果初始状态 z_0 是安全的, 且每个外观$(x, y, z)\in\sum(R, D, W, z_0)$都是安全外观, 则受限系统$\sum(R, D, W, z_0)$称为安全受限系统.

定理 3　如果任何初始状态 z_0 都是安全的, 则受限系统$\sum(R, D, W, z_0)$是安全的受限系统, 当且仅当对每个$(R_i, D_j, (CAS', OTHER'),(CAS, OTHER))$来说状态转换关系 W 满足下面两个条件:

(ⅰ) 如果 $(ses, rloc, t, op, o)\in CAS'-CAS$, 则它满足 4.4 节中所描述的 9 个不变量;

(ⅱ) 对每一个不满足 9 个不变量的$(ses, rloc, t, op, o)\in CAS$, 有$(ses, rloc, t, op, o)\notin CAS'$.

证明　(⇐). 任选$(x, y, z)\in\sum(R, D, W, z_0)$, 对每个 t 有 $z_t=(CAS_t, OTHER_t)$.

假设$(x_1, y_1, z_1, z_0)\in W$, 需要证明如果 z_0 是安全的, 则 z_1 也是安全的. 最终通过归纳得出这个受限系统是安全的.

我们有: $CAS_1=(CAS_1-CAS_0)\cup(CAS_1\cap CAS_0)$和$(CAS_1-CAS_0)\cap(CAS_1\cap CAS_0)=\varnothing$.

假设$(ses, rloc, t, op, o)\in CAS_1$, 则$(ses, rloc, t, op, o)$要么属于$(CAS_1-CAS_0)$, 要么属于$(CAS_1\cap CAS_0)$.

假设$(ses, rloc, t, op, o)$属于(CAS_1-CAS_0), 则根据(i)可知$(ses, rloc, t, op, o)$满足 9 个不变量.

假设 $CAS^*=\{(ses, rloc, t, op, o)|(ses, rloc, t, op, o)$不满足 9 个不变量$\}$. 根据(ⅱ)可知$(CAS^*\cap CAS_1)=\varnothing$. 但如果 CAS^*同时属于 CAS_0 和 CAS_1, 即 CAS^*属于 $CAS_1\cap CAS_0$, 则$CAS^*\cap(CAS_1\cap CAS_0)= (CAS^*\cap CAS_1)\cap CAS_0=\varnothing$.

因此, 如果$(ses, rloc, t, op, o)\in(CAS_1-CAS_0)$, 则$(ses, rloc, t, op, o)\notin CAS^*$.

根据上述两种情形, 可知$(ses, rloc, t, op, o)$必须满足这 9 个不变量, 从而证明了 z_1 是一个安全状态.

对 N_t 进行归纳可知 z_t 是安全的, 因而, 外观(x, y, z)是一个安全外观. 由于(x, y, z)是任选的, 所以受限系统$\sum(R, D, W, z_0)$是安全的受限系统.

($\Rightarrow$). 若用反证法, 则要证明的命题为: 存在一个状态转换(x_t,y_t,z_t,z_{t-1})以至于要么(ⅲ)有一些不满足 9 个不变量的$(ses, rloc, t, op, o)\in(CAS_t-CAS_{t-1})$, 要么(ⅳ)有一些不满足 9 个不变量的$(ses, rloc, t, op, o)\in CAS_{t-1}$属于 CAS_t.

假设(ⅲ)成立, 则存在一些不满足这 9 个不变量的$(ses, rloc, t, op, o)\in CAS_t$ 因为$(CAS_t-CAS_{t-1})\subseteq CAS_t$.

假设(ⅳ)成立, 则存在一些不满足这 9 个不变量的$(ses, rloc, t, op, o)\in CAS_t$.

因此, z_t 不满足这 9 个不变量, (x, y, z)不满足这 9 个不变量. 所以$\sum(R, D, W, z_0)$不满足这 9 个不变量, 而这与初始的假设矛盾, 因而得出受限系统$\sum(R, D, W, z_0)$是安全的受限系统.

下面分析受限 SC-RBAC 模型需达到的主要安全目标:

- 为了给支持空间能力的访问控制系统提供安全控制. 例如: 位置感知的应用程序可能有不同的信任级别, 或许也有不同的管理域以至于处于某个位置上的用户可使用的资源不同于另一位置上用户可使用的资源.
- 为了实现系统管理的职责隔离, 特别是可以用来定义冲突的角色位置域和用户位置.
- 为了实施最小特权的管理和基于位置的信息的安全管理.
- 为了完全解决基于位置的信息的时间依赖性问题.

上述描述的第一个目标可用模型中的空间角色来维护系统, 空间角色代表的是地理位置绑定的组织功能. 第二个目标可通过空间的互斥角色来实现. 特别是, 互斥的逻辑位置域能处理冲突的角色位置域. 利用基于角色的基数限制可达到第三个目标. 使用基于位置的时序限制则可以实现第四个目标.

5 应用

考虑一个商业公司, 公司里有: 公司总经理, 他可以签署商业合同; 销售经理负责公司的盈利, 可以在档案室里查看原来已签署的商业合同; 技术部经理考虑技术的可行性, 可在其办公室阅览机密的技术资料; 普通员工可以访问公共资源(如电子书籍, 花名册等)、使用打印机. 为了规避技术风险, 公司规定: 在签署商业合同之前, 销售经理和技术部经理将就合同问题在会议室进行商议. 只有双方达成一致, 公司总经理才允许签署最终合同.

从上述的应用场景中可知 $R=\{GM, SM, TM, EM\}$, 其中 GM 表示总经理, SM 表示销售经理, TM 表示技术部经理, EM 代表普通员工. $LDOM=\{DR, TO, MR, OR\}$, 其中 DR 代表档案室, TO 代表技术部经理的办公室, MR 代表会议室, OR 代表公司的其他位置域, 则公司覆盖的整个空间区域就为 $CR=DR+TO+MR+OR$. 从中可构造如下的空间角色: (SM, DR), (SM, MR), (TM, TO), (TM, MR), (EM, CR), ….

假设用户 A 是技术部经理. 用户 A 在实际位置 $rloc_1$ 创建了会话 s_1. 如果 $rloc_1$ 对应的逻辑位置域包含在 TO 中, 则空间角色(TM, TO)在会话 s_1 中是有效的; 如果 $rloc_1$ 对应的逻辑位置域包含在 MR 中, 则空间角色(TM, MR)在会话 s_1 中是有效的; 如果用户 A 在公司的其他位置创建了会话 s_1, 则用户 A 唯一的有效会话角色就为(TM, CR), 该角色所具有的权限与普通职员所具有的权限相同.

由于签订合同之前需要销售经理和技术部经理的同意, 并且为了防止共谋, 系统要求销售经理和技术部经理这两个角色不能由同一用户承担, 因此需要实施空间静态职责隔离限制, 即((SM,MR), (TM,MR))∈SSSoD. 为了实现商业保密, 防止泄密. 要求销售经理在和技术部经理就合同问题进行商议时, 销售经理不能同时再到档案室查阅商业合同, 避免技术部经理获取不必要的商业机密. 换句话说, 即在同一个会话中用户不能在位置域 DR 和 MR 上同时激活销售经理这一角色, 因此我们需要实施空间动态职责隔离限制: ((SM, DR), (SM, MR))∈SDSoD. 此外, 为了保证公司相关信息的机密性, 控制信息的单向流动, 系统安全管理员可以方便地根据空间角色层次关系(EM, CR)≤(SM, DR), (EM, CR)≤(SM, MR), (EM, CR)≤(TM, TO), (EM, CR)≤(TM, MR)制定多级安全策略. 比如, 销售经理和技术部经理把商议好的合同提交给总经理后就不能再进行修改.

为了简化系统的初始化配置和管理, 可以把空间上下文当成一个动态参数, 即低级别的空间角色可以不用空间上下文信息. 相反地, 较高级别的空间角色则还需参考空间信息. 如上面例子中的空间角色(EM, CR)等同于传统的不带空间上下文的角色 EM, 它只具有系统中最基本的权限, 因此, 授权机制在处理承担空间角色(EM, CR)的用户提出的访问请求时, 可不用考虑空间上下文.

6　相关工作

目前有许多研究工作提出了处理访问控制决策中上下文信息的不同解决方法, 这些研究工作包括抽象的高层模型, 也包括案例分析和具体的、已实现了的软件系统.

用作访问控制的上下文信息的类型依赖于具体情形. 针对于工作流和协同任务而言, 上下文是指工作流或任务的状态 [7,11]. Wolf等人在文献 [8]中建议把鉴别某特定主体的认证方法(如基于口令的和基于证书的认证)看作上下文信息来指派或激活特定的角色. 在文献 [6]中, Georgiadia等人引入了基于上下文的组访问控制模型C-TMAC是对Thomas提出的TMAC模型 [7]的扩充. 在C-TMAC模型中, 组的概念用来关联用户和上下文. Wiliekens等人 [5]提出了卫生保健领域中上下文相关的访问控制的解决方案, 并给出实例说明用时间限制、医生的物理位置、组成医护人员的成员作为上下文信息来控制对病历的访问操作. Kumar等人 [9]提出的CS-RBAC模型, 扩展了RBAC， 使其对用户和目标客体的上下文敏感. Cuppens等人 [4]提出了不同类型的上下文分类, 其中包括时序的上下文、空间的上下文、用户宣称的上下文、预先要求的上下文和临时的上下文, 同时研究了: 为了处理这些不同的上下文, 信息系统应该管理哪些数据. Covington等人 [3,10]提出了GRBAC(一般化的RBAC), GRBAC结合了环境角色来从环境中捕获与访问控制相关的信息用于访问仲裁, 比如星期或气候条件. 与普通使用的基于角色的访问控制方案相比, GRBAC提供了更强的表达能力, 更易于使用, 使其能适合于上下文感知的授权方案. 然而, GRBAC在实际中并不可行, 因为潜在的大量环境角色使得系统很难手工维护.

目前, 已经提出了一些支持空间和非空间的上下文感知扩展的访问控制系统 [3,10,12], 即使这些方案提出了添加上下文信息(如空间信息和时间信息)到访问控制机制的初步建议, 它们也都过于简单且没有给出形式化的定义. 这些模型多数都没有提供任何方法来描述空间感知系统中的复杂的限制集合. 据我们所知, 文献 [28]提出了第一个针对地理数据的访问控制模型, 但它只能处理卫星图像地图. 文献 [14]提出了RBAC的扩展模型: 当用户处于某特定位置时能自动激活角色, 但位置本身没有任何语义, 仅仅代表几何数值. 该模型面向于无线网络的应用程序且不能处理地理绑定的角色. Bertino等人最近在文献 [13]中提出了空间感知的RBAC模型——GEO-RBAC. GEO-RBAC依赖于OGC(Open GeoSpatial Consortium)空间模型 [29]为空间客体、用户位置和地理绑定的角色建模, 即用几何方式来定义位置. 此外, GEO-RBAC引入了角色模式的概念来定义一系列具有相同意义的空间感知机构组织功能的共有属性. 文献 [15]提出了一个将基于位置的条件与一般的访问控制模型相结合的方法, 考虑用来确定请求者位置的技术限制, 引入confidence和timeout参数来表述几个基于位置的谓词的形式化定义和它们的管理、评估和实施.

虽然上述研究工作解决了空间上下文感知的访问控制系统中的各种重要的问题, 但它们没有考虑把空间上下文集成到角色中. 空间上下文被看成为访问控制决策时的一个额外步骤, 并且, 这些工作缺乏表达位置空间上复杂限制的手段. 本文中的角色结合了逻辑位置域, 即提出了空间角色的概念, 证明了空间角色集合可构造成格. 我们可以用它来表达多级安全策略, 而多级安全策略是安全关键的位置感知机构所要求的. 本文给出了用来处理冲突逻辑位置域的空间职责隔离限制、基于位置的基数限制和基于位置的时序限制. 此外, 我们为受限的 SC-RBAC 模型引入了 9 个不变量, 证明了其基本安全定理, 为需要受限空间上下文感知的访问控制系统的具体应用奠定了基础.

7 结论

本文提出了 SC-RBAC 模型, 即用来处理空间信息和位置信息的 RBAC 扩展模型. SC-RBAC 依赖于层次式位置模型给空间客体建模, 使用该方法易于表达空间关系并能提供良好的用户可读性. 本模型的另一个重要特性在于能够处理从移动终端处获得的物理位置和逻辑位置. 逻辑位置可以表达不同粒度的位置, 具有特定的语义. 通过引入空间角色的概念来定制角色的空间边界, 引入有效会话角色, 则系统可根据用户的当前位置来判断会话中哪些角色是有效的. 此外, 对 SC-RBAC 模型进行了层次上的扩充, 证明空间角色的集合可形成格, 而格模型是用来描述多级安全策略的一种有效方法. 最后, 我们为受限的 SC-RBAC 模型确定了各种空间职责隔离限制、基于位置的基数限制和基于位置的时序限制.

在将来的工作中, 我们计划为本模型提供其他的上下文信息, 使其能适用于普适计算环境. 此外, 本模型还有些问题没有解决. 首先是没有考虑对位置信息实施安全隐私限制, 其次, 本文假设位置服务总能返回位置信息. 我们将对模型进行扩展, 考虑限制谁能提供位置信息和怎样提供位置信息, 这些策略具体来源于用户的隐私偏好或法规.

参 考 文 献

1 Sandhu R, Coyne E, Feinstein H, et al. Role base access control models. IEEE Comp, 1996, 29(2): 38—47

2 Ferraolo D, Sandhu R, Gavrila S, et al. Proposed NIST standard for role-based access control. ACM Trans Inf Syst Sec, 2001, 4(3): 224—274 [DOI]

3 Covington M, Long W, Srinivasan S, et al. Securing context-aware applications using environment roles. In: Proceedings of the 6th ACM Symposium on Access Control Models and Technologies. New York: ACM Press, 2001. 10—20

4 Cuppens F, Miège A. Modelling contexts in the Or-BAC model. In: Proceedings of the 19th Annual Computer Security Applications Conference. Washington: IEEE Computer Society Press, 2003. 416—427

5 Wilikens M, Feriti S, Sanna A, et al. A context-related authorization and access control method based on RBAC: A case study from the health care domain. In: Proceedings of the 7th ACM Symposium on Access Control Models and Technologies. New York: ACM Press, 2002. 117—124

6 Georgiadis C, Mavridis I, Pangalos G, et al. Flexible team-based access control using contexts. In: Proceedings of 6th ACM symposium on Access Control Models and Technologies. New York: ACM Press, 2001. 21—27

7 Thomas R. Team-based access control (TMAC): A primitive for applying role-based access controls in collaborative environments. In: Proceedings of 2nd ACM Workshop on Role-based Access Control. New York: ACM Press, 1997. 13—19

8 Wolf R, Keinz T, Schenider M. A model for context-dependent access control for web-based services with role-based approach. In: Proceedings of 14th International Workshop on Database and Expert Systems Applications. Washington: IEEE Computer Society Press, 2003. 209—214

9 Kumar A, Karnik N, Chafle G. Context sensitivity in role-based access control. ACM SIGPOS Op Syst Rev, 2002, 36(3): 53—66 [DOI]

10 Covington M, Moyer M, Ahamad M. Generalized role-based access control for securing future applications. In: Proceedings of 23rd National Information Systems Security Conference. Washington: IEEE Computer Society Press, 2003. 416—427

11 Cholewka D G, Botha R H, Eloff J H P. A context sensitive access control model and prototype implementation. In: Proceedings of the IFIP TC11 15th International Conference on Information Security. Reventer: Kluwer, 2000. 341—350

12 Hulsebosch R J, Salden A H, Bargh MS, et al. Context-sensitive access control. In: Proceedings of the 10th ACM Symposium on Access Control Models and Technologies. New York: ACM Press, 2005. 111—119

13 Bertino E, Catania B, Damiani M L, et al. GEO-RBAC: A spatially aware RBAC. In: Proceedings of the 10th ACM Symposium on Access Control Models and Technologies. New York: ACM Press, 2005. 29—37

14 Hansen F, Oleshchuk V. Spatial role-based access control model for wireless networks. In: Proceedings of IEEE Vehicular Technology Conference (VTC). Washington: IEEE Computer Society Press, 2003. 2093—2097

15 Ardagna C A, Cremonini M, Damiani E, et al. Supporting location-based conditions in access control policies. In: Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security. New York: ACM Press, 2006. 212—222

16 Denning D E. A lattice model of secure information flow. Comm ACM, 1976, 19(5): 236—243

17 Jiang C, Steenkiste P. A hybrid location model with a computable location identifier for ubiquitous computing. In: Proceedings of the 4th International Conference on Ubiquitous Computing. London: Springer-Verlag, 2002. 246—263

18 Clementini E, Felice P di, van Oosterom P. A small set of formal topological relationships suitable for end-user interaction. In: Proceedings of the 3rd International Symposium on Advances in Spatial Databases SSD'93. Londong: Springer-Verlag, 1993. 277—295

19 Bell D E, Lapadula L J. Secure computer systems: unified exposition and MULTICS interpretation. In: Technical Report MTR-2997. 1976

20 Davey B, Priestley H. Introduction to Lattices and Order. Cambridge: Cambridge University Press, 2002

21 Sandhu R S. Lattice-based access control models. IEEE Comp, 1993, 26(11): 9—19

22 Gligor V D, Gavrila S I, Ferraiolo D. On the formal definition of separation-of-duty policies and their composition. In: Proceedings of 1998 IEEE Computer Security Symposium on Research in Security and Privacy. Washington: IEEE Computer Society Press, 1998. 172—183

23 Richard K D. Mutual exclusion of roles as a means of implementing separation of duty in role-based access control systems. In: Proceedings of the 2nd ACM Workshop on Role-based Access Control. New York: ACM Press, 1997, 23—30

24 Osborn S, Sandhu R, Munawer Q. Configuring role-based access control to enforce mandatory and discretionary access control policies. ACM Trans Inf Syst Sec, 2000, 3(2): 85—106 [DOI]

25 Jaeger T, Tidswell J E. Practical safety in flexible access control models. ACM Trans Inf Syst Sec, 2001, 4(2): 158—190 [DOI]

26 Bertino E, Bettini C, Samarati P. A temporal authorization model. In: Proceedings of the 2nd ACM Conference on Computer and Communication Security. New York: ACM Press, 1994. 126—135

27 Gavrila S I, Barkley J F. Formal specification for role based access control user/role and role/role relationship management. In: Proceedings of the 3rd ACM Workshop on Role-Based Access Control. New York: ACM Press, 1998. 81—90

28 Atluri V, Mazzoleni P. A uniform indexing scheme for geo-spatial data and authorizations. In: Proceedings of the 16th IFIP WG11.3 Working Conference on Data and Applications Security. London: Springer-Verlag. 2002. 207—218

29 OpenGIS Consortium. OpenGIS simple features specification for SQL. In: Technical Report OGC 99-049. 1999