一种栅格数据的敏感信息保护模型

张德胜[1],徐 震[1],冯登国[1],李鹏飞[2]
(1.中国科学院软件研究所信息安全国家重点实验室,北京 100190;
2.中国科学院软件研究所综合信息系统技术国家级重点实验室,北京 100190)

摘 要: 卫星测绘技术的进步使得地理信息系统能够提供精确的地图查询服务,同时也给国土安全带来潜在威胁.本文针对已有空间数据访问控制模型中存在的根据访问结果进行敏感信息推理的问题,提出PPR-RBAC(a Privacy-Preserved RBAC for Raster data).该模型在RBAC模型的基础上,提出伪装客体的概念,采用数据伪装技术,将敏感客体扩展为真实客体和伪装客体;定义客体激活的方法,建立用户对真实客体和伪装客体的访问控制机制.最后,形式化证明PPR-RBAC模型的基本安全定理,为模型在地理信息系统中的应用奠定基础.

关键词: 地理信息系统;栅格数据;敏感信息保护;数据伪装;客体激活
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2012)04-0647-07
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2012.04.005

A Privacy-Preserved Authorization Model for Raster Data

ZHANG De-sheng[1], XU Zhen[1], FENG Deng-guo[1], LI Peng-fei[2]
(1. *State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing* 100190, *China*;
2. *State Key Laboratory of Integrated Information System Technology, Institute of Software, Chinese Academy of Sciences, Beijing* 100190, *China*)

Abstract: Due to the fact that GIS(Geographic Information System) could provide high-resolution image with commercial observation satellites, this commercial availability of unprecedented and timely information and images of the earth poses significant threats to national security. Since existing access control models could not avoid the information inference according to the authorization results, a privacy-preserved RBAC for Raster Data is proposed, in PPR-RBAC, fake objects are made to protect sensitive raster objects, and authorization mechanisms are contributed for user to access sensitive raster objects by sensitive object activation. In conclusion, PPR-RBAC is formally proved to be safe and it lays the groundwork for the security deployment of PPR-RBAC in GIS.

Key words: GIS; raster data; sensitive information protection; data counterfeiting; sensitive object activation

1 引言

卫星测绘技术的发展使得测绘卫星能够获得高清晰的地表测绘图片,利用这些测绘图片构建的地理信息系统已能为用户提供精确地图查询服务.以GoogleEarth为例,目前能提供分辨率达0.5m的清晰图片(分辨率1m的卫星图片就可以清晰看到马路上的行人),堪比海湾战争时期世界主要军用间谍卫星的精度.然而,由于地表信息(如交通路况、军事基地、军事演习信息等)完全暴露于测绘卫星航拍之下,恶意用户能利用这些地理信息系统收集敏感空间信息.为此,印度政府的态度已经由"开始表示担心"转而"责令GoogleEarth模糊化印度的战略重地".这种模糊化的处理方法依然存在敏感信息泄漏的风险,栅格数据的敏感信息保护问题已成为地理信息系统急需解决的核心问题.

空间数据访问控制模型的研究起步较晚,研究的方法是在已有访问控制模型的基础上进行时空扩展,依据扩展方法划分为2类[1]:其一是针对模型的主体进行扩展,这类模型均在RBAC模型[2]的基础上进行时间和空间的扩展[3~8],适合于用户驱动的空间应用;其二是对模型的客体进行扩展,这类模型是在传统的DAC模型的基础上进行时空扩展的[9~12],适合于数据驱动的空间应用.然而这些模型在授权过程中,都存在同一个问题:授权结果为"允许访问"或是"拒绝访问".当授权结果为"拒绝访问"时,恶意用户能根据这一授权结果推测出请求访问的空间数据为敏感信息,从而造成敏感信息的泄漏.这些模型均无法对栅格数据的敏感信息进行保护.

收稿日期:2011-03-02;修回日期:2011-04-06
基金项目:国家863高技术研究发展计划重大项目(No.2007AA120404,No.2007AA120405);国家自然科学基金项目(No.61003228)

针对已有的空间数据访问控制模型不能解决敏感信息推理的不足,本文在 RBAC 的基础上,提出一种栅格数据的敏感信息保护模型 PPR-RBAC.本文的主要贡献体现在:

(1)提出伪装客体的概念.模型采用伪装技术,选取非敏感的伪装客体无缝填补敏感客体,防止恶意用户依据查询结果进行敏感信息推理.

(2)建立敏感客体激活机制.模型引入环境约束条件如时间、访问者 *ip*、访问者属性等,使其支持策略的动态性,保证合法用户访问敏感栅格数据.

(3)定义模型的基本安全定理,并形式化证明该模型的安全性,为模型在地理信息系统的安全应用建立理论依据.

2 相关工作

在空间应用安全需求的驱动下,近年来空间数据安全的研究得到快速发展,提出一系列的空间数据安全策略模型.这些模型均在传统的访问控制模型的基础上进行时空扩展.为解决以用户为驱动的空间应用的安全问题,在 RBAC 模型的基础上,对角色进行时空扩展,使角色支持环境上下文、时序上下文、空间上下文等,提出了 GRBAC[3]、GTRBAC[4]、X-GRBAC[5]、LoT-RBAC[6]和 GEO-RBAC[7,8].这些模型针对不同场景的空间应用,使策略具有更强的表达能力,并易于部署于特定的空间应用中.然而,在栅格数据的隐私保护上,这些模型存在 3 点不足:(1)时空上下文的复杂性增大了模型中角色管理的难度;(2)这类模型适合用户驱动的空间应用;(3)模型的访问机制带来了敏感信息推理的风险.为解决以空间数据为驱动的空间应用的安全问题,文献[9]首次提出授权窗口的概念,用于指定用户授权访问的区域.在此基础上,文献[10]将空间操作权限转化为对数据库表的操作权限,并且实现权限传播的控制.文献[11]将授权信息附加到空间索引信息中,以避免因授权判定而额外增加的一次空间查询;文献[12]进一步在授权模型中引入了时间约束,并在实现上解决空间索引中客体相互交叠的问题.这些空间数据授权模型依然没有考虑恶意用户依据模型的授权访问机制进行敏感信息推理的问题.

为解决栅格数据在空间应用的隐私保护问题,PPR-RBAC 模型在 RBAC 的基础上,对模型的客体进行扩展,提出伪装客体的概念,利用数据伪装技术来屏蔽敏感信息,使恶意用户无法依据查询结果进行敏感信息推理;同时建立敏感客体激活机制.以保证合法用户访问敏感栅格数据.最后,利用形式化方法对 PPR-RBAC 模型进行安全性分析.

3 敏感信息保护

3.1 敏感信息分类

栅格数据的敏感信息大致分为三类:

(1)敏感信息的内容.在地理信息系统中,这类敏感信息体现在空间区域内的敏感客体,如军事演习区域出现的新型舰艇;还体现在敏感客体的移动上,如军事演习区域的舰艇,直升机的配合作战暴露海战的战术.这一类型的敏感信息的保护在访问中进行.

(2)敏感信息的拥有关系.在地理信息系统中,体现在空间客体敏感信息与拥有者的关系,如军事演习中的新型潜艇,舰艇,战斗机的数量.这一类型的敏感信息保护主要也是在访问中进行的.

(3)隐私实践.隐私实践是指访问者在获取敏感信息之后,对获得的敏感信息的使用进行约束.如获得军事基地的地形图后,不能将该敏感信息存储到受到安全威胁的存储设备中.这一类型的敏感信息保护在访问后进行.

第 3 类敏感信息的保护方法主要依赖于协议条款和法律法规,本文将研究栅格数据的第 1、2 类敏感信息的保护问题.

3.2 数据伪装

数据伪装是指为空间区域内的敏感客体制造一个伪装客体,其目的在于防止恶意用户根据授权结果做出敏感信息推理.通过数据伪装技术,无权访问敏感客体的用户进行访问时,只能访问伪装客体;有权访问敏感信息的用户,当会话的环境属性满足环境约束时,通过敏感客体激活,用敏感客体替换伪装客体,使其访问真实的敏感客体.

数据伪装技术的效果取决于伪装客体的有效性.如果数据伪装的不好,让恶意用户能够猜出该敏感区域进行了数据伪装,这样就达不到数据伪装的目的.解决伪装数据的有效性问题必须考虑:(1)用户的预先知识;如军事演习中的岛屿,对于绝大部分人而言,都了解该岛屿大致的地理位置,因而将这整块军事演习海域的岛屿伪装成海浪就取不到预定的效果;(2)伪装客体与周围区域的和谐.使得伪装客体和周围环境融为一体,而不被恶意用户发现数据伪装的痕迹;(3)伪装客体不会误导用户.使得用户在进行正常数据访问的时候不会被伪装客体所影响和干扰.如何制作伪装客体已超出本文的范围,将不作进一步的介绍.

3.3 客体激活

PPR-RBAC 模型为会话引入环境条件,并增加环境约束用于敏感客体的激活.环境条件除了包括时间和访问者的空间属性,还包括访问者的其他属性、发起访问的 *ip*、访问相关的应用等.以军事演习为例,假设区

域 A 包含一个敏感客体 B,而 B 周围 10km 内的所有空间数据均为敏感信息,当区域 A 发生自然灾害时.救灾过程需要利用 B 周围的道路信息.访问控制策略能根据这一需求,限定在正常应用中用户不能访问客体 B 周围 10km 的空间信息,而在救灾的特殊时期,能对其空间信息进行激活,进而访问相关空间信息.

文献[3]把环境属性作为角色的一个属性,同样可以处理角色激活的问题,在本文的模型中,并没有采用将环境属性与角色绑定的原因在于:环境属性是作为访问控制策略的一个输入,是用来激活敏感客体的.如果进行绑定,一方面,为角色增加属性会增大角色管理的难度;另一方面,在敏感信息的访问条件发生变化的情况下,不利于敏感信息保护策略的管理,同时也不能很好的支持策略的动态性.

4　PPR-RBAC 模型

PPR-RBAC 模型如图 1 所示,该模型在 RBAC 的基础上,提出伪装客体的概念,依据栅格数据的特征,扩展模型的客体,引入区域、普通客体、敏感客体和伪装客体等组件,从不同粒度和层次描述栅格数据;建立客体激活机制,扩展会话属性,增加环境变量,利用环境约束实现对敏感客体的激活,从而在实现栅格数据授权的同时,满足敏感数据隐私保护的需求.模型的形式化描述如下:

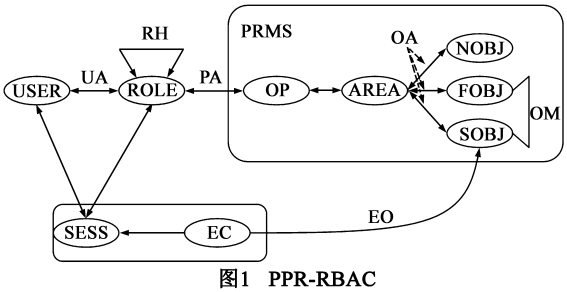


图1　PPR-RBAC

4.1　模型的形式化描述

定义 1　(PPR-RBAC 模型) PPR-RBAC 模型 = {*USER*(用户集), *ROLE*(角色集), *OP*(操作集), *AREA*(区域集), *OBJ*(客体集), *NOBJ*(普通客体集), *FOBJ*(伪装客体集), *SOBJ*(敏感客体集), *PRMS*(权限集), *SESS*(会话集), *EC*(环境条件集), *UA*(用户-角色集), *PA*(角色-权限集), *RH*(角色继承关系), *OA*(区域-客体集), *OM*(客体伪装), *EO*(客体激活)}

(1)用户集 *USER*,角色集 *ROLE*,会话集 *SESS*,用户角色集 *UA*,角色权限集 *PA*,角色继承关 *RH* 和 RBAC 的定义一致.

(2) *OP*:操作集.即对栅格客体的访问操作.

(3) *AREA*:空间客体所在区域.

(4) $OBJ \subseteq ID \times SUBOBJ \times OBJDATA \times LOC \times LAYER$ 空间客体集合. $OBJ = NOBJ \cup FOBJ \cup SOBJ$.

(5) *ID*:客体的标识集合.

(6) *SUBOBJ*:客体子集.对于一个客体 $o(id, subobj, objdata, loc, layer)$, $o.subobj$ 表示与客体 o 对应的位于栅格金字塔下层的客体集合(图 2(a)所示).

(7) *OBJDATA*:客体的空间数据.

(8) *LOC*:栅格客体的坐标数据.

(9) *LAYER*:空间客体在栅格金字塔的位置,用栅格的图层表示.

(10) $PRMS \subseteq 2^{(OP \times AREA)}$ 权限集合.权限的操作对象为区域,表示与区域相交空间客体执行操作的权利.

(11) *EC*:环境条件.包括访问者属性、访问的 *ip* 等.

(12) $OM \subseteq FOBJ \times SOBJ \times CONS$ 表示伪装客体与敏感客体之间的映射关系.其中, *CONS* 表示激活敏感客体的环境约束.

4.2　会话、用户、角色

模型中的会话、用户、角色的定义和 RBAC 模型一致.这里将简单给出会话-用户、会话-角色定义:

定义 2(会话-用户)　会话-用户的关系定义为函数 $session\_user: SESS \rightarrow USER$

定义 3(会话-角色)　会话-角色的关系定义为函数 $session\_roles: SESS \rightarrow ROLE$,对于给定会话 s, $session\_roles(s) = \{r \mid (session\_user(s), r) \in UA\}$

4.3　客体

PPR-RBAC 的客体为栅格数据.栅格数据通用的数据模型是栅格金字塔模型(图 2(a)所示),相同坐标的栅格数据在金字塔的下层要比上层的分辨率更高,精度也更高.对于金字塔的每一层,在数据生产阶段,为了得到更逼真的数据,采用多波段数据采集与合成的方式,并且被分成方形数据进行存储,每一个方形数据均为一个数据分块(图 2(b)).数据分块是栅格数据存储与访问的最小单元.PPR-RBAC 的客体定义为一系列的数据分块,而权限定义为操作与区域的笛卡尔积,表示对与区域相交的数据分块操作的权利.详细定义如下:

定义 4(空间区域 *AREA*)　$AREA \subseteq LOC \times LAYER$.一个空间区域包含多个空间客体,是授权与访问的单元.

定义 5(空间客体 *OBJ*)　一个空间客体为一个数据方块集合.

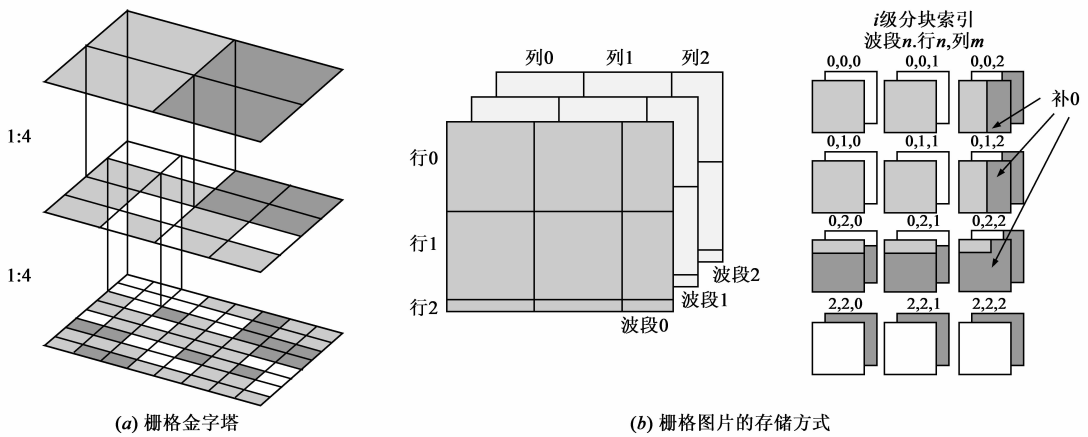
定义 6(客体伪装 *OM*)　定义敏感客体与伪装客体的映射关系,定义为 $OM \subseteq FOBJ \times SOBJ \times CONS$.其中, *FOBJ* 表示伪装客体, *SOBJ* 表示敏感客体, *CONS* 表示激活敏感客体的约束条件.

定义 7(空间区域-客体包含) 空间区域与客体的包含关系定义为 $area\_obj: AREA \rightarrow 2^{OBJ}$,是一对多的关系.给定 $area$, $area\_obj(area) = \{obj \mid obj \in OBJ \wedge obj.layer = area.layer \wedge intersect(obj, area) = 1\}$ *

定义 8(空间区域-伪装客体包含) 空间区域与伪装客体的包含关系定义为一个关系 $area\_fobj: AREA \rightarrow 2^{FOBJ}$,是一对多的关系.给定 $area$, $area\_fobj(area) = \{fobj \mid fobj \in FOBJ \wedge fobj.layer = area.layer \wedge intersect(fobj, area) = 1\}$

定义 9(空间区域-敏感客体包含) 空间区域与敏感客体的包含关系定义为一个关系 $area\_sobj: AREA \rightarrow 2^{SOBJ}$,是一对多的关系.给定 $area$, $area\_sobj(area) = \{sobj \mid sobj \in SOBJ \wedge sobj.layer = area.layer \wedge intersect(sobj, area) = 1\}$

定义 10(空间区域-普通客体包含) 空间客体与普通客体的关系定义为一个关系 $area\_nobj: AREA \rightarrow 2^{NOBJ}$,是一对多的关系.给定 $area$, $area\_nobj(area) = \{nobj \mid nobj \in NOBJ \wedge nobj.layer = area.layer \wedge intersect(nobj, area) = 1\}$



(*a*) 栅格金字塔 (*b*) 栅格图片的存储方式

图2 栅格数据模型与存储方式

4.4 权限

在地理信息系统中,对于大部分栅格数据,用户都可访问.仅仅是对敏感栅格客体,需要限制用户的访问.针对这一特点,在 PPR-RBAC 模型中,普通客体默认均可访问而敏感客体必须授权访问,即模型的授权策略均是敏感信息保护策略.如果授予角色对敏感区域的访问权限,且当前会话能的环境条件满足敏感客体的激活条件,则扮演该角色的用户能访问敏感客体;否则仅能访问敏感客体对应的伪装客体.

定义 11(权限分配) 权限分配定义为 $assigned\_prms: ROLE \rightarrow 2^{PRMS}$,表示分配给角色的权限集合.给定角色 r, $assigned\_prms(r) = \{p \mid (r, p) \in PA\}$

由于栅格数据采用金字塔模型,而金字塔下层的数据精度要比金字塔上层数据的精度高.换言之,如果金字塔上层客体是敏感客体,其包含的下层客体则是敏感程度更高客体.因而,对于栅格金字塔相邻的两层,下层敏感客体的权限(p),蕴含着对上层低敏感客体权限的权限(p').对于权限的隐含关系 $\vdash\!\!\rightarrow$,有:

定义 12(权限隐含) 权限隐含记为 $\vdash\!\!\rightarrow$,定义为:

$$\forall p = op \times area, p' = op' \times area',$$
$$(p \vdash\!\!\rightarrow p') \leftrightarrow op = op' \wedge$$
$$\{o'_{sub} \mid o' \in area\_object(area') \wedge o'_{sub} \in o'.subobj \wedge o'_{sub}.layer = area.layer\} \subseteq \{o \mid o \in area\_object(area)\}$$

4.5 客体使能与客体激活

定义 13(客体使能) 敏感客体的使能定义为一个关系 $enable\_sobj: AREA \times EC \rightarrow SOBJ$,表示在会话的特定环境条件和访问区域下对区域内的敏感客体使能.给定会话条件 ec 以及访问区域 $area$, $enable\_sobj(area, ec) = \{sobj \mid \exists om, om \in OM \wedge sobj = om.sobj \wedge sobj \in area\_sobj(area) \wedge ec \rightarrow om.cons\}$

定义 14(客体激活) 敏感客体激活定义为函数 $active\_sobj: ROLE \times OP \times AREA \times EC \rightarrow SOBJ$,表示一次用户访问能够激活的客体集.其激活条件为:该客体被使能,并且存在一条授权策略,授予用户访问敏感客体的权限.给定角色 r 在环境条件为 ec 下,对区域 $area$ 发起操作 op,角色激活的形式化描述如下:

$$active\_sobj(r, op, area, ec) = \{sobj \mid sobj \in enable\_sobj(area, ec) \wedge ((\exists p'(op', area'), op' = op \wedge intersect(area', sobj) = 1 \rightarrow p' \in assigned\_perms(r)) \vee (\exists p''(op'', area''), p''', op'' = op \wedge intersect(area'', sobj) = 1 \rightarrow p''' \vdash\!\!\rightarrow p'' \wedge p''' \in assigned\_perms(r)))\}$$

* $intersect(x_1, x_2) = 1$ 表示栅格客体 x_1 与 x_2 的坐标数据相交

定义 15(替换的伪装客体集)　替换的伪装客体集表示在一次用户访问中,激活的敏感客体集对应的伪装客体集.形式上定义为一个关系 $replace\_obj: ROLE \times OP \times AREA \times EC \rightarrow FOBJ$,给定角色 r 在环境条件 ec 下,对区域 $area$ 发起操作 op,替换的伪装客体集的形式化描述为:

$$replace\_fobj(r, op, area, ec) = \{fobj \mid \exists\, sobj, om, om \in OM \wedge sobj = om.sobj \wedge om.sobj \in active\_sobj(r, op, area, ec) \rightarrow fobj = om.fobj)\}$$

4.6　敏感信息访问控制机制

PPR-RBAC 的授权粒度为区域,表示访问者能对该区域的所有空间客体进行相应的访问操作.用户进行客体访问时,将会指定一个访问区域.默认情况下,仅能访问到该区域内的普通客体和伪装客体.只有当前环境条件满足敏感客体使能条件,且存在一条授权策略授予用户访问该敏感客体,该敏感客体才被激活,即访问者才能访问到敏感客体.访问控制机制定义如下:

定义 16(访问集)　访问集定义为 $AR \subseteq SESS \times OP \times AREA \times EC$,分别为会话、操作、空间区域和环境条件.

定义 17(访问控制机制)　访问控制机制定义为一个关系 $authorization: AR \rightarrow OP \times OBJ$.给定访问请求 $ar = (sess, op, area, ec)$ 其授权结果将表示为操作与客体的笛卡尔积,表示能对客体集进行相应的访问操作.给定一次用户访问 ar,访问控制的形式化描述为:

$$authorizaiton(ar) = \{(op, obj) \mid obj \in \bigcup_{r \in session\_roles(sess)} ((area\_nobj(area) \cup area\_fobj(area) \cup active\_sobj(r, op, area, ec) - replace\_fobj(r, op, area, ec))\}$$

4.7　应用

现以军事演习为例对 PPR-RBAC 模型的应用部署进行阐述.假定中国在东海的某海域进行抢滩登陆战的军事演习.演习过程仅能被参与本次军事演习的指战员所访问.因而,当对该片海域的分辨率小于 10m 时,海域内与演习相关的空间客体,如巡洋舰,护卫舰等,被定义为敏感空间客体,将被伪装成海浪.在演习过程中,只有从演习指挥中心的终端发起的查询才能对演习的过程进行访问(策略描述图 2 所示).现有两个会话 s_1 和 s_2,在会话 s_1 中,武器研发部门的李将军(ip = 192.168.1.11)对该演习海域进行访问时,他将不能访问演习过程的敏感客体,其返回的的结果将是敏感客体的伪装客体,即海浪;在会话 s_2 中,演习指挥部的张将军(ip = 192.168.100.56)对该区域进行访问时,可以看到敏感客体,了解演习过程.

5　安全性分析

为模型在地理信息系统中的安全应用提供理论依据,本章节对安全应用系统进行安全性分析.安全应用系统的形式化安全分析包含受限系统采用的安全模型的形式化分析和受限系统自身的安全性分析.安全模型形式化分析的目标在于确保对模型元素的操作是安全的,受限系统安全性分析的目标在于确保用户对受限系统的客体访问是安全的.PPR-RBAC 模型在角色管理和角色-用户的管理上与RBAC保持一致,尽管文献

Basic objects:

USER = { General_Li, General_Zhang}　　ROLE = {rw(weapon_dev), rc(commander)}

OP = {view}　　AREA = {ECS = East_China_Sea, SBA = Sham_Battle_Area}　　PRMS = { p_1(view, SBA)}

NOBJ = {island, wave}　　SOBJ = { cruiser, frigate}　　FOBJ = {c_wave, f_wave}

OM = {(c_wave, cruiser, {ip∈192.168.100.*, time = 2008-10-07, resolution < 10m})
(f_wave, frigate, {ip∈192.168.100.*, time = 2008-10-07, resolution < 10m})

OA = {(ECS, island), (ECS, wave), (ECS, cruiser), (ECS, frigate), (ECS, c_wave), (ECS, f_wave),
(SBA, island), (SBA, wave), (SBA, cruiser), (SBA, frigate), (SBA, c_wave), (SBA, f_wave)}

User and permission assignment:

UA = {(General_Li, rw), (General_Zhang, rc)}　　PA = {(rc, p_1)}

Session:

SESS = {s_1, s_2}

session_user(s_1) = General_Li, session_user(s_2) = General_Zhang, session_roles(s_1) = rw, session_roles(s_2) = rc

authorization(s_1, view, SBA, {ip = 192.168.1.11, time = 2008-10-07, resolution = 1m})
= {(view, island), (view, wave), (view, c_wave), (view, f_wave) }

authorization(s_2, view, SBA, {ip = 192.168.100.56, time = 2008-10-07, resolution = 1m})
= {(view, island), (view, wave), (view, cruiser), (view, frigate) }

图 3　应用举例

[13]详细分析了 RBAC 在模型管理上的安全性,但未对模型保护的受限系统做任何安全性分析.

安全应用系统安全性分析的步骤包括 3 步:(1)定义受限系统,包括系统状态、访问集、决策集、状态转换函数;(2)定义系统状态满足的安全约束,即系统的状态不变量;(3)形式化证明安全应用系统在状态转换过程中前后状态均满足安全约束.进行受限系统的形式化证明之前,预先做如下定义.

定义 18(决策集) 决策集定义为 $D=\{$"*yes*","*no*","*error*","?"$\}$,"*yes*"表示允许访问敏感栅格数据;"*no*"表示禁止访问敏感栅格数据,即仅能访问伪装数据;"*error*"表示出现未知错误;"?"表示系统无法处理.

定义 19(操作序列集) 操作系列集定义为 $B\subseteq USER\times OBJ\times OP$.分别是用户、操作对象和操作.操作对象包括模型元素和栅格客体.由于本文分析受限系统的安全,因而操作对象特指栅格客体.

定义 20(系统状态) PPR-RBAC 模型的系统状态定义为 V 定义为:$\{USER, ROLE, OP, AREA, OBJ, NOBJ, FOBJ, SOBJ, PRMS, SESS, EC, UA, PA, RH, OA, OM, EO, B\}$

文献[13]已对模型元素操作的安全性做详细分析,我们将着重讨论对栅格数据操作的安全性分析.由于系统包含许多基本元素,简化表示为 $V=\{B, OTHER\}$.

定义 21(状态转换函数) 状态转换函数定义为 $\delta: V\times AR\rightarrow D\times V^{*}$.分别表示转换前的状态、用户请求、决策和转换后的状态.

定义 22(受限系统) 系统定义为四元组 $\Sigma(V, AR, D, Z_0)$,分别表示受限系统的系统状态、用户请求、决策集、状态转换函数和系统初始状态.

受限系统安全性依赖于系统的安全约束,即系统的状态不变量.文献[13]给出模型的 20 个状态不变量,但没有考虑对栅格客体操作的状态不变量.在此,给出栅格操作的状态不变量.

Inv_raster. 操作系列中对栅格数据的任何一个操作 $b(u, o, op)\in B$ 必须满足下列 3 个安全条件之一:(1)o 为非敏感客体;(2)存在一条授权策略直接授予用户访问敏感客体 o;(3)存在一条策略隐含授予用户访问敏感客体 o.形式化表示如下:

$$\forall b(u,o,op), b\in B\rightarrow o\in FOBJ$$
$$\vee(\exists r, p(op, area), (u,r)\in UA\wedge o\in area\_sobj(area) \rightarrow p\in assigned\_perms(r))$$
$$\vee(\exists r, p'(op', area'), p'', op'=op\wedge o\in area\_sobj(area') \wedge(u,r)\in UA\rightarrow p''\in assigned\_perms(r)\wedge p''\mapsto p')$$

定义 23(安全状态) 把满足状态不变量 Inv_raster 的系统状态称为系统的安全状态.

如果一个系统是安全的,那么对于系统的任意一个状态转移系列 $Z_0, V_1, V_2, V_3, \cdots$,其每一个状态都是安全的.我们将通过归纳法证明定理的安全性,即先证明系统初始状态是安全的,而后假设系统的某一状态 V_{i-1}是安全的,进而证明其下一状态 V_i 也是安全的,通过这种归纳的方式证明系统是安全的.为此,将引入两个引理.

引理 1 系统的初始状态 Z_0 是安全的.

证明 对于初始状态 Z_0,由于不存在任何用户访问,即 $Z_0.B=\varnothing$,因而系统是安全的.证毕.

引理 2 在系统状态 $V_{i-1}(i=1,2,3,\cdots)$下,处理用户 u 请求 ar_i,系统进入下一状态 V_i,如果 V_{i-1}是安全的,则 V_i 也是安全的.

证明 设状态 V_{i-1}, V_i 的访问集合分别为 B_{i-1}和 B_i, ar_i 为 $(sess, op, area, ec)$,由前提可知 $B_i=B_{i-1}\cup\{(u,o_{i_1},op),\cdots,(u,o_{i_k},op)\}$,其中$(op, o_j)\in authorization(ar_i)(j=i_1,\cdots,i_k)$.

(1)由于 V_{i-1}是安全的,由安全状态的定义可知任意 $b\in V_{i-1}$,都是安全的访问.

(2)对于$(u, o_j, op)(j=i_1, i_2, \cdots, i_k)$,

(ⅰ)如果 o_j 为普通客体,则(u, o_j, op)为安全的访问.

(ⅱ)如果 o_j 为敏感客体,由访问控制机制可知:

$$(u,r)\in UA\wedge o_j\in active\_sobj(r, op, area, ec)$$
$$\Rightarrow(u,r)\in UA\wedge o_j\in enable\_sobj(area, ec)\wedge$$
$$((\exists p'(op', area'), op'=op\wedge intersect(area', o_j)=1 \rightarrow p'\in assigned\_perms(r))$$
$$\vee(\exists p''(op'', area''), p''', op=op''\wedge intersect(area'', o_j)=1 \rightarrow p'''\mapsto p''\wedge p'''\in assigned\_perms(r)))$$
$$\Rightarrow(u,r)\in UA$$
$$\wedge((\exists p'(op', area'), op'=op\wedge intersect(area', o_j)=1 \rightarrow p'\in assigned\_perms(r))$$
$$\vee(\exists p''(op'', area''), p''', op''=op\wedge intersect(area'', o_j)=1 \rightarrow p'''\mapsto p''\wedge p'''\in assigned\_perms(r)))$$

即:

$$(\exists r, p'(op', area'), (u,r)\in UA\wedge op' =op\wedge o_j\in area\_sobj(area') \rightarrow p'\in assigned\_perms(r))$$
$$\vee(\exists r, p''(op'', area''), p''', op'' =op\wedge o_j\in area\_sobj(area'')\wedge$$
$$(u,r)\in UA\rightarrow p'''\in assigned\_perms(r)\wedge p'''\mapsto p'')$$

由(ⅰ)和(ⅱ)可知(u, o_j, op)满足安全不变量 Inv_raster,是安全的访问.

由(1)和(2)可知 $b\in B_{i-1}\cup\{(u,o_{i_1},op),\cdots,(u,o_{i_k},op)\}$都是安全的,即 $b\in B_i$ 都是安全的.因而,状态

V_i 是安全的.证毕.

定理 1　PPR-RBAC 模型下的系统是安全的.

证明　由引理 1 和引理 2,利用归纳原理可知,任意一个状态转移序列 $Z_0, V_1, V_2, V_3, \cdots$ 是安全的.即该模型下的受限系统是安全的.证毕.

6　结论

本文根据地理信息系统在空间数据查询服务的特点和访问控制的需求,在 RBAC 的基础上提出了一种带敏感信息保护的访问控制模型,PPR – RBAC 模型在 RBAC 的基础上,对模型的客体进行扩展,提出伪装客体的概念,利用数据伪装技术来屏蔽敏感信息,利用非敏感的信息无缝填补敏感信息,使得恶意用户无法依据查询结果进行敏感信息推理.同时建立敏感客体激活机制.以保证合法用户访问敏感栅格数据.最后,利用形式化方法证明 PPR – RBAC 模型下的空间应用系统是安全的.

在该模型中,仍然有一些开放性的问题值得进一步研究.一方面,在敏感信息的管理上,伪装数据的有效性是对该模型而言是一个关键问题.如果伪装数据起到伪装的作用,将不能对敏感数据起到保护的作用;另一方面,空间数据的多样性和复杂性给敏感信息的组织上带来一定的困难,如果组织不好,将影响模型实施的性能.这两个问题是我们今后研究工作的重点.

参考文献

[1] M L Damiani, E Bertino. Spatial Data on the Web[M]. Berlin, Heidelberg: Springer, 2007. 189 – 214.

[2] R S Sandhu, E J Coyne, H L Feinstein, et al. Role-based access control models[J]. IEEE Computer, 1996, 29(2): 38 – 47.

[3] M J Covington, W Long, S Srinivasan, et al. Securing context-aware applications using environment roles[A]. Proc of 6th ACM Symp on Access Control Models and Technologies[C]. New York: ACM, 2001. 10 – 20.

[4] J Joshi, E Bertino, U Latif, et al. A generalized temporal role-based access control model[J]. IEEE Trans on Knowledge and Data Engineering, 2005, 17(1): 4 – 23.

[5] R Bhatti, A Ghafoor, E Bertino, et al. X-GTRBAC: an XML-based policy specification framework and architecture for enterprise-wide access control[J]. ACM Trans on Information and System Security, 2005, 8(2): 187 – 227.

[6] S M Chandran, James B D Joshi. A location and time-based RBAC model[A]. Proc of WISE 6th Intl Conf on Web Information Systems Engineering[C]. Berlin: Springer, 2005. 361 – 375.

[7] E Bertino, B Catania, M L Damiani, et al. GEO-RBAC: a spatially aware RBAC[A]. Proc of the 10th ACM Symp on Access Control Models and Technologies[C]. New York: ACM, 2005. 29 – 37.

[8] M L Damiani, E Bertino, B Catania, et al. GEO-RBAC: a spatially aware RBAC[J]. ACM Trans on Information and System Security, 2007, 10(1): 1 – 42.

[9] E Bertino, M L Damiani, D Momini. An access control system for a web map management service[A]. Proc of 14th Intl Workshop on Research Issues in Data Engineering[C]. Los Alamitos, CA: IEEE, 2004. 33 – 39.

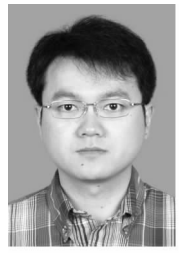
[10] A Belussi, E Bertino, E Catania, et al. An authorization model for geographical maps[A]. Proc of 12th ACM Intl Workshop on Geographic Information Systems[C]. New York: ACM, 2004. 82 – 91.

[11] V Atluri, P Mazzoleni. A uniform indexing scheme for geo-spatial data and authorizations[A]. Proc of 16th IFIPWG11.3 Working Conf on Database Security[C]. Dordrecht: Kluwer Academic Publishers, 2002. 207 – 218.

[12] V Atluri, Qi Guo. STAR-Tree: An index structure for efficient evaluation of spatiotemporal authorizations[A]. Proc of IFIP TC11/WG 11.3 18th Annual Conf on Data and Applications Security[C]. Dordrecht: Kluwer Academic Publishers, 2004. 31 – 47.

[13] S I Gavrila, J F Barkley. Formal specification for role based access control user/role and role/role relationship management [A]. Proc of the 3rd ACM Workshop on Role-Based Access Control[C]. New York: ACM, 1998. 81 – 90.

作者简介



张德胜　男,1981 年生于福建永定.中科院软件所信息安全实验室博士生,主要研究方向为系统安全与数据库安全.

徐　震　男,1976 年生于天津,中科院软件所信息安全国家重点实验室副研究员.主要从事系统安全方面的研究工作.
E-mail: xuzhen@is.iscas.ac.cn

冯登国　男,1965 年生于陕西靖边.研究员、博士生导师,中科院软件所信息安全国家重点实验室主任.主要从事信息与网络安全方面的研究工作.

李鹏飞　男,1974 年生于河北定州.博士,高级工程师.主要从事信息安全领域的研究工作.