

# 带空间特性的访问控制在汽车终端上的应用

杨 宸,薛 丹,周 健

(陕西师范大学 计算机科学学院,陕西 西安 710062)

**摘 要:**文中主要研究具有位置特性的访问控制技术在汽车智能终端上的使用。介绍了基于位置的访问控制的相关定义以及运用到汽车智能终端上的一些约束,并定义了一些相关的角色,以期能将此运用在现实生活中。汽车行驶到不同的位置,其对于某个数据库扮演的角色也会相应发生改变。基于位置的服务作为IT信息服务的重要内容,它根据汽车所处空间位置向其提供在当前环境下所需的数据信息。为了保护隐私,保证数据资源不被非法利用,参考SRBAC访问控制模型,从空间环境下的约束、角色授予、约束违反的解决方式等方面,来描述它将来在汽车终端上的应用。

**关键词:**位置信息;访问控制;隐私保护

**中图分类号:**TP309

**文献标识码:**A

**文章编号:**1673-629X(2012)01-0225-03

## Application of Role-Based Access Control with Spatial Character in Automobile Terminal

YANG Chen, XUE Dan, ZHOU Jian

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

**Abstract:** Its major research is the use of role-based access control with spatial character in automobile terminal. Introduce the relate definitions about the location-based access control and give some restraints which can be used on the automobile terminal, hoping that can be used in the real life. The playing role of each car will change for one database when the automobile went to another place. Hope that the location-based service can provide the requisite data to the user who is authorized by the local database. In order to protect users' privacy and prevent the illegal use of private data, referred the spatial role-based access control model, described its application in automobile terminal on the restraints in spatial environment, the grant of roles, the solution of constraint violates, etc.

**Key words:** location information; access control; privacy-preserving

### 0 引言

目前移动通信<sup>[1]</sup>发展十分迅速,蓝牙、Wifi等无线通信技术的逐渐成熟为其发展提供了条件。这些技术的发展可以为用户提供更多的服务,用户可以使用移动终端在任何时候完成信息交互。汽车逐渐地进入普通人的家庭,以及物联网在未来的发展和应用,汽车将会成为未来物联网的一个智能终端,在普适计算的条件下参与运算。这就不可避免地要将访问控制运用到汽车终端上。而且用户的访问请求和权限会随着空间位置的不同而变化,所以在汽车终端的使用过程中给数据库加以空间特性约束<sup>[2]</sup>,以此来保护用户隐私,保证数据资源不被非法利用<sup>[3,4]</sup>显得十分重要。

目前基于位置空间的服务<sup>[5]</sup>已经成为IT服务的重要内容,它向用户提供经过搜集、整理、过滤过的信

息。提供的服务主要依据用户当前所处的位置、信息所存储的位置以及系统访问控制策略等因素,做出是否向特定用户提供信息服务的决策,并进行相关的后续操作。

随着物联网<sup>[6]</sup>的概念逐渐深入人心和移动终端的迅速发展,许多事物都将成为未来物联网的一个节点。在这里考虑将汽车作为一个终端,如果每辆车都有一个设备来发送和接收消息,将会为我们带来许多方便:在这里假设有一个统一的信息服务器,负责存储车辆的各种信息和每个终端上传的信息。当用户购买车辆的同时将车辆信息和用户个人信息同时写入数据库,并且规定只有当信息存入数据库之后汽车才能正常使用。用户可以在终端随时查看和修改自己的信息,这就涉及到一个访问控制策略,来规定哪种信息是可以修改的,哪种信息是不可以被修改的,以及用户可以读取的信息和其他用户通过登录数据库可以读取的信息有哪些不同。这种访问控制模型用RBAC模型<sup>[7,8]</sup>就可以得到较好的实现,但是由于车辆属于一种移动终

收稿日期:2011-06-14;修回日期:2011-09-23

基金项目:陕西省科技攻关项目(2008K01-58)

作者简介:杨 宸(1987-),女,河南漯河人,硕士研究生,研究方向为密码学与信息安全。

端,并且为了方便用户快捷的访问,每个省市对数据库访问权限开放给外省市的权限有所不同。根据上述内容,选择 SRBAC 模型<sup>[9]</sup>来描述未来访问控制在汽车终端上的应用。

## 1 相关技术

### 1.1 相关定义

在文献[1]中,作者给出了带空间特性的角色访问控制(SRBAC)的定义,在这个模型中,作者给位于不同位置同一角色赋予不同的权限,因为汽车终端的访问控制空间是很重要的一个约束条件,文中将参考这个模型并将其运用到汽车终端上。

$U = \{u_1, u_2, \dots, u_n\}$ ,表示所有用户的集合,所有有权限操作数据库的人,包括数据库管理员、车辆的使用者等;

$R = \{r_1, r_2, \dots, r_n\}$ ,表示所有角色的集合,在这里主要是在空间条件下通过空间位置的不同而分配的角色;

$Ob = \{ob_1, ob_2, \dots, ob_k\}$ ,表示所有对象的集合,对于整个数据库来说,每辆车都是一个对象;

$Op = \{op_1, op_2, \dots, op_k\}$ ,表示所有操作的集合,用户对数据库的操作,包括用户信息的登入,以及在使用过程中的发布、查询等;

$S = \{s_1, s_2, \dots, s_p\}$ ,表示所有会话的集合,即用户接收别的终端的信息产生的回话以及请求发送信息产生的回话;

$p = 2Op \times Ob$ ,表示所有权限的集合,对数据库操作权利的分配;

$POS = \{POS_1, POS_2, \dots, POS_n\}$ ,表示空间位置的集合,在这里,主要是国内的各个行政区;

$UAAU \times LOC \times R$ ,表示用户在空间位置发出请求后被授予的角色,在这里它是从用户集合到角色集合的多对多的映射,用户在不同的空间位置会被授予不同的角色;

$PAAP \times POS \times R$ ,表示用户空间位置发出请求并被授予相应角色之后所拥有的权限。在这里它是从许可集合到角色集合的多对多映射。

$RAAR \times R \times POS$ ,表示角色集合和权限集合的相互关系,可以称之为层次关系。如果  $(r_i, r_j) \in RH$ ,则定义为  $r_i \xrightarrow{(POS)} r_j$ ,表示在空间位置  $POS$ ,  $r_i$  继承  $r_j$  的权限;

$s = \langle U, R, UA, C, \text{ChangePosition}, op \rangle$ ,表示用户与系统的会话。用这个七元组来表示这个会话,并以此来定义该会话应该满足的约束规则、空间位置以及操作指令等内容。文中用到的操作有:

1)  $\text{authorized}(r, POS)$ :在空间位置  $POS$  给角色  $r$  授予权限。

2)  $\text{assign-user}(u, r, POS)$ :在车辆行驶到位置  $POS$  时,给该车的用户  $u$  分配角色  $r$ 。

3)  $\text{assign}(r, p, POS)$ :当车辆行驶到空间位置  $POS$ ,并且被分配了角色  $r$  之后,给该角色授予权限。

4)  $\text{get-role}(u, r, POS)$ :当车辆行驶到空间位置  $POS$  时,用户  $u$  可以激活角色  $r$ 。

5)  $\text{get-perm}(u, p, POS)$ :当车辆行驶到空间位置  $POS$  时,可以给角色  $r$  授予权限  $p$ 。

6)  $\text{get-perm-role}(p, r, POS)$ :当车辆行驶到空间位置  $POS$  时,在用户请求通过之后角色  $r$  获得权限  $p$ 。

7)  $\text{session-role}(u, s, POS)$ :当车辆行驶到空间位置  $POS$  时,返回在空间对象  $POS$  范围内用户  $u$  的会话  $s$  的相关角色。

8)  $\text{session-perm}(u, s, POS)$ :当车辆行驶到空间位置  $POS$  并发出会话请求后,授予用户  $u$  会话  $s$  的权限。

文中所讨论问题是汽车终端的访问控制,在这里将空间位置划分按照目前的地理区划来分,所以文中所述的空间位置就指各个省、自治区、直辖市等。而每辆汽车通常只在归属地使用,当车辆行驶到别的省市时,才需要访问别的省市的相关数据库。故而对车辆的位置进行监测,在车辆进入相应的地域的时候才赋予它相关的权限,以减小各省市数据库的访问压力。暂时不将位置划分细化到各市,是为了便于描述和说明。

### 1.2 相关角色与约束的描述及分析

$PS = \{P_i | P_i \in POS\}$  当车辆行驶到空间位置  $POS$  时,用  $P_i$  来表示该空间区域。在这里某个空间区域通常是行政区划中的一个省或者是一个市,所以行政区划就是这里区域分割的唯一依据。在这里,空间区域的集合是一个有限集,文中只讨论各省、直辖市等省级行政区划。也就是说该  $POS$  集合中的元素是各个省、直辖市、自治区等。讨论汽车终端上的应用时,空间位置的约束用来控制车辆用户在该地域是否能够建立会话,所建立的会话具有什么样的角色和权限。例如,当汽车行驶到别的省市,假设是从陕西省境内到河南省境内,当它在河南省时,河南省对应的实时路况信息的数据库就赋予它读和提交修改的权利,而对陕西省的数据库它就只有读的权利。还有一种情况是引言中所提到的不同用户的使用权限的设置问题。

首先进行角色设置:

管理员角色:具有对数据库操作的所有权限,可以分配给用户各种角色以及进行角色定义。

角色  $r_1$ :具有对所在地数据库的访问权限,可以查询、修改个人信息以及发布消息,比如对路况的描述以及求助信息的发布。

角色  $r_2$ :具有对所在地数据库的访问权限,可以查询、发布消息,但是不可修改数据库内相关信息。

角色  $r_3$ :只可对数据库进行查询,但不可以修改和发布消息。

角色  $r_4$ :具有使用该车的权限,可以访问所在地数据库,发布消息,但是不能修改个人信息。

角色  $r_5$ :具有对数据库进行查询,修改个人信息,但是不可以发布消息。

这就需要建立一些约束,如表 1 所列:假设汽车的所属地是陕西,约束  $a$ ,  $b$  是空间区域范围约束,  $a$  表示甲车的车主在陕西省被授权访问陕西省所建立的交通数据库,也就是说对车辆所在地的数据库授予角色  $r_1$ ,而不具有访问其他省市的数据库的权限,可以理解为对其他省市的数据库授予角色  $r_3$ ;  $b$  表示当甲车行驶到河南省时他具有访问河南交通数据库的权限,即对河南省交通数据库授予角色  $r_2$ ,而对陕西省交通数据库授予权限  $E$ 。约束  $c$  是使用者的约束,也就是说当使用者是非车主的时候,此人会被授予角色  $r_4$ 。约束  $d$  是角色激活基数约束,表示无论任何情况下,每辆车只有一个用户并且只可以激活一个角色。

表 1  相关约束

约束类型	约束内容
a	在归属地,对本地数据库属于角色 $r_1$ ,外地数据库属于角色 $r_3$
b	在外地,对外地数据库属于角色 $r_2$ ,归属地数据库属于角色 $r_5$
c	使用者非车主本人时,只能获得角色 $r_5$
d	对使用者人数的限制,只能为 1

2  汽车终端访问控制的实现

在实现汽车终端的访问控制时,发现当汽车所处的位置不同,该终端所获得的权限也不同。因为需要在不同的域中申请权限,这就出现了一系列安全违反的问题。基于角色的访问控制 RBAC 作为一种灵活的授权体系在科研领域和工业界逐渐兴起,而 SRBAC 模型是对 RBAC 模型的扩展,其自身具有良好的层次性划分,可以提供职责分离 (SoD) 约束、基于势 (cardinality) 的约束和依赖 (dependency) 约束等细粒度授权控制。要将其应用在汽车的终端上,必须实现域间的互授权<sup>[10]</sup>并建立互操作模型。以下给出了在车辆终端进行访问控制时基于 RBAC 进行域间互操作策略整合需要考虑的安全违反类型<sup>[11]</sup>,分别是:

1)角色分配约束违反。当车辆行驶到空间位置

POS 时,禁止数据库给用户  $U$  分配角色  $r$ ,但由于互操作策略的使用,用户  $u$  可以间接从数据库中获得角色  $r$  的一些相关权限,这就违反了角色分配的约束。

2)面向角色的职责分离约束违反。在汽车行驶到两个相邻的空间位置时,在进行域间互授权时,由于互操作策略的使用,在同一会话中,用户  $u$  可能会同时激活两个互斥的角色  $r_i$  和  $r_j$ ,这种情况便违反了针对角色的职责分离约束。

3)面向用户的职责分离约束违反。可以用  $UP$ , 来表示当汽车行驶到空间位置 POS 时所不能激活的角色集合。但是由于在域间互授权过程中使用了互操作策略,使得用户在该空间位置激活了它本不能激活的角色。这种情况违反了针对用户的职责分离约束。

访问控制技术自身的发展是随着应用的增加和技术的进步而不断进行扩展演变的。利用以上所述的安全违反类型,可以将汽车终端的交互情况进行定义。

在这里,假设现在存在的各个收费站是总数据库的一个节点。当汽车行至收费站时,收费站工作人员将车辆的行驶信息录入。以此来确认这辆车行驶到某个空间位置,当然,离开某地也以经过某个收费站而录入的信息进行判定。这样可让数据库根据车辆的信息以及行驶信息将相应的角色分配给该终端。在信息被数据库录入的同时,就确定了汽车终端所在的地域,使得在给该终端分配角色的时候有了一定的依据和参考<sup>[12]</sup>。为了消解以上安全违反,在给用户关联角色时必须检测所添加的新的关联是否与先前已有的角色发生冲突。如果发生冲突,那么就拒绝将该角色分配给当前用户。

3  结束语

文中介绍 SRBAC 模型在未来汽车终端上的应用,重点描述了位置空间访问控制模型的原理以及具体的使用方法。当汽车在行驶的过程中遇到道路拥塞或者道路检修无法使用的情况时,可以向服务器发送道路信息,由服务器判断发送消息节点位置并向距该节点一定距离的车辆发送道路路况信息,以便他们判断如何选择行驶方向。通过对各地数据库的使用约束可以实现数据库的最大限度使用并且不造成拥塞,使数据库的使用更加合理和方便。

参考文献:

[1]  张一衡,张  昊,邹  杰.下一代移动通信系统中无线协同定位技术[J].北京邮电大学学报,2011,34(1):126-129.

[2]  张光伟,王小明,罗  琴,等.基于角色的时空访问控制模型[J].计算机工程与应用,2008,44(4):46-49.

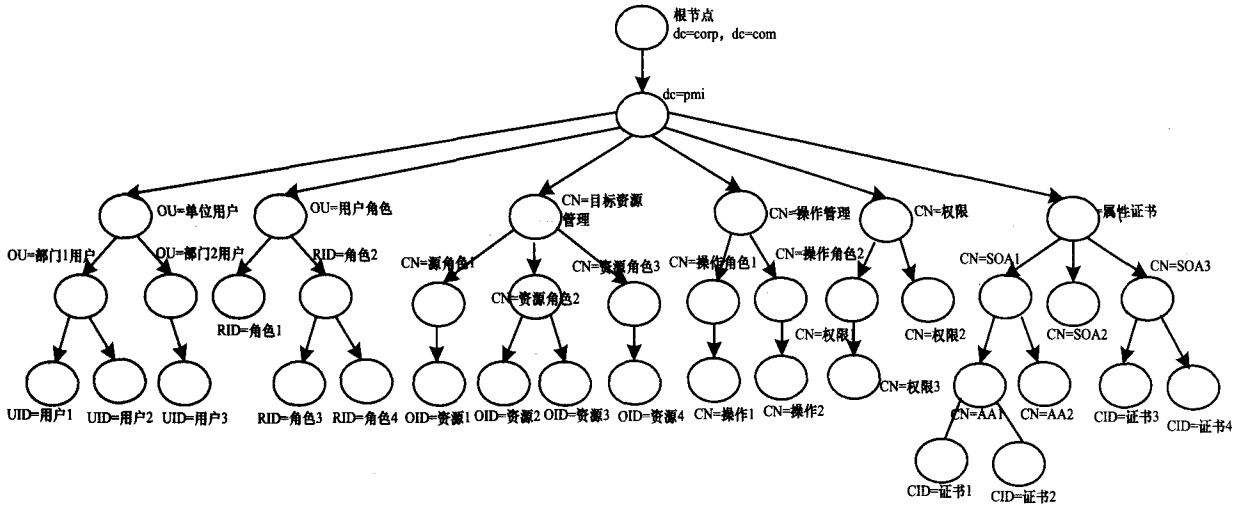


图 6 RBAC 访问策略在 LDAP 中的存储结构

了一个可行的访问控制方案,解决了跨组织边界的用户和服务资源的动态调整及安全属性种类繁多、权限决策辅助因素的多变等问题。该系统已在笔者单位开发的网络安全及安全办公平台等项目中得到应用,很好地解决了项目面临的安全问题。系统通过将访问控制机制从具体应用的开发和管理中分离出来,不仅屏蔽了安全技术的复杂性,也拥有很强的灵活性、适应性和可扩展性。

参考文献:

[1] ITU-T Rec. X509 (2000) | ISO/IEC 9594-8:2000, The Directory: Public-key and attribute certificate framework [S/OL]. 2000. <http://www.iso.org/iso/store.htm>.

[2] ITU-T Rec. X509 (2005) | ISO/IEC 9594-8:2005, The Directory: Public-key and attribute certificate framework [S/OL]. 2005. [http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=43793](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43793).

[3] 中华人民共和国信息产业部. GB/T 16264. 8-2005, 信息技术开放系统互连目录第 8 部分: 公钥和属性证书框架

[S]. 中国标准出版社, 2005.

[4] 刘宏月, 范久伦, 马建峰, 等. 访问控制技术研究进展[J]. 小型微型计算机系统, 2004, 25(1): 56-59.

[5] 李辉, 王芳. 一切皆角色的访问控制策略[J]. 计算机科学, 2006(9A): 121-125.

[6] 周彦萍. PMI 授权管理系统的接口设计[J]. 计算机技术与发展, 2010, 20(3): 167-171.

[7] Adame C, Lloyd S. 公钥基础设施—概念、标准和实施[M]. 冯登国, 译. 北京: 人民邮电出版社, 2001.

[8] 关振胜. 公钥基础设施 PKI 与认证机构 CA[M]. 北京: 电子工业出版社, 2002.

[9] Yeong W, Howes T, Kille S. RFC 2251, Lightweight Directory Access Protocol (v3) [S]. 1997.

[10] 曹晟, 杨洁, 孟庆春. 基于 PMI 的系统访问安全管理研究与设计[J]. 计算机工程, 2001(24): 141-143.

[11] 周彦萍, 张志业, 崔芸. 基于客体管理的增强型 RBAC 模型的研究[J]. 河北科技大学学报, 2010(3): 227-231.

[12] 孟凡滋, 谢琦. 基于 LDAP 的框架及其实现[J]. 计算机技术与发展, 2006, 16(10): 42-44.

(上接第 227 页)

[3] 余永红, 柏文阳. 安全数据库隐私保护和访问控制[J]. 计算机应用研究, 2010, 27(10): 3876-3879.

[4] Eugster P T, Felber P A, Guerraoui R, et al. The Many Faces of Publish/Subscribe[J]. ACM Computing Surveys, 2003, 35(2): 114-131.

[5] 高博, 万方杰, 宋国民, 等. 基于位置服务的空间信息传输模型[J]. 测绘科学技术学报, 2009, 26(1): 12-14.

[6] 张捍东, 朱林. 物联网中的 RFID 技术及物联网的构建[J]. 计算机技术与发展, 2011, 21(5): 56-59.

[7] Sandhu R S, Coney E J, Feinstein H L. Role-Based Access Control Models[J]. IEEE Computer, 1996, 29(2): 38-47.

[8] Ferraiolo D F, Sandhu R, Gavrila S, et al. Proposed NIST Standard for Role Based Access Control[J]. ACM Transac-

tions on Information and System Security, 2001, 4(3): 224-274.

[9] 邹志文, 陈昌乾, 鞠时光. 带空间特性的角色访问控制研究[J]. 计算机科学, 2010, 37(1): 189-196.

[10] 王雅哲, 冯登国. 域间授权互操作研究综述[J]. 计算机研究与发展, 2010, 47(10): 1673-1689.

[11] Shafiq B, Joshi J B D, Bertino E, et al. Secure interoperation in a multidomain environment employing RBAC policies[J]. IEEE Trans on Knowledge and Data Engineering, 2005, 17(11): 1557-1577.

[12] 蒋东兴, 刘启新, 郑叔亮. 基于角色和活动的数字校园访问控制模型[J]. 大连海事大学学报, 2010, 36(1): 132-134.