文章编号：1004-4353(2016)01-0069-06

基于访问控制的隐私保护方法的研究

苏晴， 李永珍*
（延边大学工学院 计算机科学与技术学科 网络与信息安全室，吉林 延吉 133002）

摘要：为保护移动终端中实时上传的位置信息，提出了一种基于分级角色的访问控制方法. 该方法对访问者进行二级角色定义，并根据访问者的不同角色定义不同的访问权限来保护位置信息. 对该访问控制方法进行了模型构建，同时在移动终端内进行了可行性测试. 实验结果表明，该访问控制方法能较好地保护实时上传的位置信息，且具有应用可行性.

关键词：移动终端；角色分级；访问控制；位置信息；可行性
中图分类号：TP309.2 **文献标识码**：A

Research of privacy protection method based on access control

SU Qing， LI Yongzhen*
（*Network and Information Security Lab.*, *Dept. of Computer Application Technology*, *College of Engineering*, *Yanbian University*, *Yanji* 133002, *China*）

Abstract: According to protect the position information of mobile terminal in real time to upload, this paper proposes a multi-level access control method based on role. We define the secondary role for the visitor and different access rights to protect the position information of mobile terminal in real time to upload according to the different role of visitors. A new model based on hierarchical role access control method is builded, at the same time a feasibility test in the mobile terminal is carry out. Results of experiments indicated that the new multilevel access control method based on role can protect upload real-time location information better and make application feasible.

Keywords: mobile terminal; role classfication; access control; location information; feasibility

随着互联网技术的迅猛发展，智能手机的普遍使用，使得用户很容易将自己的位置信息暴露出来，导致用户的个人位置信息安全受到威胁，因此对于移动终端中的位置隐私的保护引起了人们极大的重视. 目前，国内外学者多数以通过采用假地址技术[1]等方法来降低位置信息数据的准确度，达到保护移动终端中用户位置信息的目的. 这些方法虽然能在某种程度上保护用户的位置信息，但也降低了位置信息服务的质量[2]. 为了能更好地保护移动终端中实时上传的位置信息，本文提出了一种基于分级角色的访问控制方法，通过对访问者的身份进行二级角色定义，使不同的访问者拥有不同的访问权限. 本文对所提出的分级角色的访问控制方法进行了模型构建，并对其进行了可行性测试，结果表明该访问控制方法能较好地保护实时上传的位置信息，且具有应用可行性.

1 基于角色的访问控制(RBAC)

1.1 RBAC 的基本原理

RBAC 的基本思想是通过角色的形式来表示

收稿日期：2016-03-01

* **通信作者**：李永珍(1971—)，男，博士，副教授，研究方向为网络安全、无线网络协议.

用户的关系,角色是描述访问者与请求者之间的用户关系定义[3].访问者被用户加入不同的群组,从而依据加入的不同分组而获得不一样的角色,同时可获得相应的访问控制权限,使用户能有效地进行权限管理.角色是根据用户不同的需求而设定的,角色可依据新需求和系统合并赋予新权限,而权限也可根据需要从某角色中收回.用户可以在角色间进行转换,这样能够减少授权管理的复杂性,降低管理开销,提高系统安全策略的灵活性.

通常 RBAC 模型中主要存在 3 个实体:用户、角色和权限.RBAC 访问控制模型如图 1 所示.

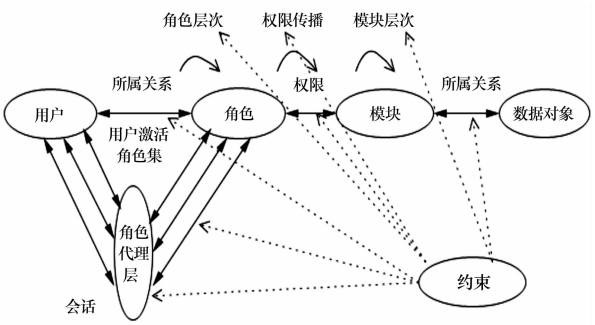

图 1 RBAC 访问控制模型

在 RBAC 中存在 3 个安全原则,分别是最小权限原则、责任分离原则和数据抽象原则[4].最小权限原则是 RBAC 可以将其角色配置成其完成任务所需要的最小的权限集;责任分离原则是 RBAC 可以通过调用相互独立互斥的角色来共同完成某项任务;数据抽象原则是 RBAC 可以通过权限的抽象来体现.上述这些原则必须通过 RBAC 各部件的详细配置才能得以体现.

1.2 RBAC 的形式化描述

对 RBAC 进行形式化的分析有助于验证 RBAC 的说明是否能够满足系统的安全需求,还可以比较不同的访问控制模型和预测不同安全策略下的系统行为[5].目前,对于 RBAC 的研究比较成熟,但对于 RBAC 的形式化的表示仍很缺乏.为了给出 RBAC 的形式化方法,有的学者提出了 RBAC 的描述逻辑 DLRBAC[6].

下面介绍角色分级模型 RBAC1.RBAC1 由以下内容确定:

U,R,P,S 分别表示用户集合、角色集合、许可权集合和会话集合[7].

PA $P\times R$ 表示许可权与角色之间多对多的指派关系[8].

UA $U\times R$ 表示用户与角色之间多对多的指派关系[9].

RH $R\times R$ 表示对 R 的偏序关系,称为角色等级或角色支配关系,也可用"$\geqslant$"符号表示.

用户:$S\rightarrow U$ 是每个会话 si 到单个用户 user(si) 的映射函数(常量代表会话的声明周期).

角色:$S\rightarrow 2$ 是每个会话 si 到角色子集 roles(si) $\{r\mid (r'\geqslant r)[\text{user}(si,r')\in UA]\}$(能随时间改变)的映射函数,会话 si 有许可权 $Ur\in \text{roles}(si)$ $\{p\mid (r''\leqslant r)[(p,r'')\in PA]\}$.

RBAC 模型具有广泛的应用前景,它支持最小权限原则、责任分离原则、数据抽象原则和继承概念[10].RBAC 模型中的概念都是实际系统中实际存在的实体,便于设计者建立 RBAC 模型.RBAC 模型的本质是对访问矩阵模型的扩充,能够解决系统中主体对客体的访问控制访问权力的分配与控制问题,但 RBAC96 模型仍存在一些问题,比如是否允许一个正在会话的用户再创建一个新会话,管理模型不支持用户和许可权的增加与删除等管理工作[11],这些问题都仍需要进一步进行研究.

2 基于分级角色访问控制方法的设计

2.1 系统基本模型

本文提出的基于分级角色访问控制的基础模型能够实现对位置信息数据以及访问权限进行划分,一对一映射,从上到下逐级授权,形成树状结构.该模型可针对手机中实时上传的位置信息进行保护,阻止访问客体的非法收集和利用.基于角色的多级访问控制模型如图 2 所示.

本文中的访问控制方法区别于传统的角色访问控制方法,主要区别在于:本文方法针对访问用户多的系统,根据用户角色进行二级划分并赋予角色不同的访问权限来保护用户的位置信息,同时根据系统操作者意愿设置权限.根据互斥原则,一个用户至多只能分到互斥角色中的一个,用户

一般只属于以上分级中唯一的一个.

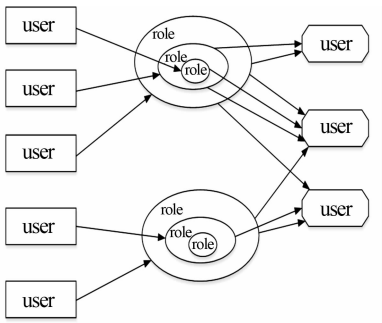

图 2　基于角色的多级访问控制模型

2.2　多级权限访问控制模型的说明

1)角色权限集 GETP(role)，是取得角色 role 的权限集合.

2)用户角色映射 ROLE(user)，取得用户 user 的所有直接授予角色.

3)角色用户映射 USER(role)，取得角色 role 的所有直接授予人.

4)父角色集 PARR(role)，是由角色 role 及其所有父角色组成的角色集合，父角色是 role 所继承的角色，$role' \in PARR(role) \rightarrow (role, role') \in RH$;

5)子角色集 CHIR(role)，是由角色 role 及其所有子角色组成的角色集合，子角色是继承自 role 的角色，$role' \in CHIR(role) \rightarrow (role, role') \in RH$;

6)用户角色集 ROLES(user)，是用户 user 所有可用角色的集合. 集合包括 user 被直接赋予的角色和间接赋予的角色. 间接赋予的角色指的是一个直接赋予的角色的父角色.

7)角色用户集 USERS(role)，是角色 role 的所有拥有用户的集合. 角色用户集中将包括相应角色的直接赋予人和间接赋予人，间接赋予人是相应角色子角色的拥有人，这样在角色用户集 USERS(role)中将包括所有可以行使 role 权限的用户全体.

8)用户级别集合 G(grade)，限制用户操作客体的权限.

9)功能模块集 M(module)，是用户所能操作的功能模块.

10)数据对象 D(data)，是文档 / 数据集合，是每一个任务完成过程中各实体所流转的文档或者是数据.

上述的模型功能说明，在访问控制中通过对角色的权限进行分级，根据不同的用户和权限可形成新的数据库并区分不同角色级别的访问权限，可有效保护移动终端中实时上传的用户位置信息.

3　访问控制方法的应用与分析

本文提出的访问控制方法其功能如下：

1)访问操作. 根据访问者的不同角色给予其相应的访问权限，并判断访问者对用户进行访问操作是否合法.

2)权限. 总结整理并可操作所有的数据资源，辨别操作者的身份，检索其角色.

3)角色. 定义角色并进行二次划分，保证角色与权限之间所存在的映射关系.

4)用户. 建立并判断用户与角色之间的绑定关系.

3.1　应用案例分析

本文的访问控制方法能够实现对表、数据、记录的访问控制，数据操作命令主要有查询、更改、删除等. 数据库信息表包括角色信息表、权限信息表、用户信息表、安全策略表. 各数据表之间的关系如图 3、表 1 和表 2 所示.

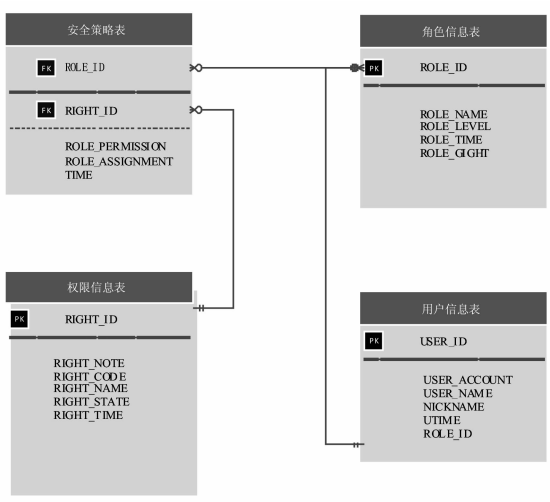

图 3　数据表之间的关系图

表 1 群组数据表

id	title	share	longitude	latitude	sharetime	pid	uid
86	亲密家人	1	1	1	1	1	50
87	一般家人	0	0	0	1	1	50
88	同事	0	0	1	0	2	50
89	同学	0	0	1	0	2	50
90	老师	1	1	1	1	2	50
91	闺蜜	1	1	1	1	0	50
92	同学 1	0	0	0	1	3	50
93	同学 2	0	1	1	0	3	50

注:数字 0 表示对该部分位置信息没有访问权限,数字 1 表示对该部分位置信息可以进行访问.

表 2 关系数据表

uid	fuid	ugroup	fgroup
50	53	88	0
50	54	94	0
50	55	90	0
50	56	91	0
50	57	92	0
50	58	93	0

注:数字 0 表示陌生人.

3.2 安全性分析

完整性是本文提出方法中的一个重要的安全需求.完整性有很多定义,其中一个重要的共同点就是数据和程序只能由授权的用户以被授权的方式进行修改[5];因此,所使用方法中首先要确保由管理者授权使用用户及其角色,其次要保证用户在进行各种操作处理数据时也同样是被授权的.

鉴于集中式管理具有数据实时共享、管理成本低等优点,本文采用集中式安全管理.在数据库中设置了角色并给予其相应的功能.首先,管理员可以根据实际情况对这些角色进行管理,例如:在我的朋友一级角色中设置我的同学这一二级角色,当其中成员角色全部发生变化时,由管理员进行删除或者重新设置该角色.其次,可实现角色嵌套,一级角色由二级角色构成,例如:角色中我的朋友和我的同事都可以查看用户所在位置的经度值,但我的朋友却不能获取用户本人具体的地理位置信息,而我的同事则可以获取.数据库系统的用户多角色关系如图 4 所示.

最小特权原则要求用户在进行操作时应当使用的特权要小于其完成任务所必须的权限,要保证信息的完整性.依据以上原则,在本方法中当访问者对用户的位置信息进行访问时或者终止访问时,访问者不再拥有所分配的权限,而且在访问位置信息的过程中,授权组会自动回收不再使用的权限.同时,对于不同的角色实行权限分离原则,在二级角色划分后进行权限划分.对于不同的角色赋予不同的访问权限,能更有效地起到对位置信息的保护作用.

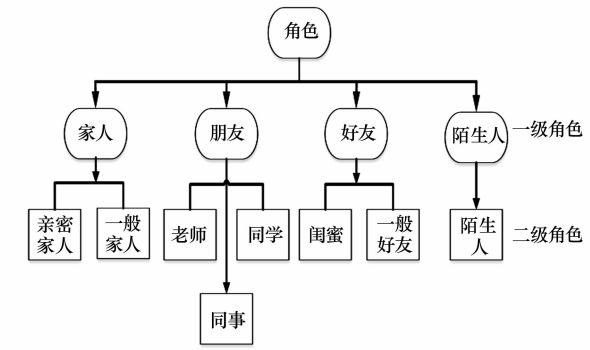

图 4 多角色关系 *P*

3.3 可行性测试

在智能手机的 APP 操作下,对本文访问控制方法的性能进行了检测.测试所用的手机操作系统为 Android 5.0,数据库为 MySQL 5.6.24,同时采用 Https 协议进行传输.具体测试内容如表 3 所示.

表 3 测试内容

序号	功能模块	具体测试事项
1	用户模块	用户的增加、查询、授权等
2	角色组模块	包括对访问角色的二级分组设定以及对访问角色的增加、修改、删除、查询、授予
3	权限模块	针对用户对访问用户赋予的角色权限进行测试,测试是否与设定的角色权限一致

在手机应用程序中添加二级角色并根据表 4 设置角色权限,如图 5 所示.添加二级角色并设定角色权限后,发布一条动态信息,然后登录其他访问用户账号查看是否最终测试结果与所设计的数据库表相一致.根据用户对访问者设定的角色以及角色授予的位置信息访问的权限来测试是否达

到设计目标的要求.

表 4　测试角色权限设置

用户	角色	权限
爸 X	亲密家人	全部可见
姑 X	一般家人	部分可见:时间
周 XX	同事	部分可见:纬度
王 XX	同学	全部可见
李 XX	老师	全部可见
王 XX	闺蜜	全部可见
李 X	陌生人	全部不可见

图 5　添加二级角色以及设置角色权限

对应用程序中的访问用户进行应用测试,权限为全部可见的测试结果如图 6 所示,测试结果与设置相一致,如表 5 所示.

图 6　权限为全部可见的测试图

表 5　权限为全部可见的测试结果

用户名	定义的角色	访问权限	测试结果
爸 X	亲密家人	全部可见	时间:2015-12-25 09:10:14
王 XX	同学	全部可见	发布内容:节日快乐!亲们
李 XX	老师	全部可见	发布地点:中国吉林省延边朝鲜族自治州延吉市龙新街
王 XX	闺蜜	全部可见	经度:129.459 967 纬度:42.892 405

权限为全部不可见的测试结果如图 7 所示,测试结果与设置相一致,如表 6 所示.

图 7　权限为全部不可见的测试图

表 6　权限为全部不可见的测试结果

用户名	定义的角色	访问权限	测试结果
李 X	陌生人	全部不可见	发布内容:节日快乐!亲们 发布地点:未知

权限为部分可见的测试结果如图 8 所示,测试结果与设置相一致,如表 7 所示.

图 8　权限为部分可见的测试图

表 7 权限为部分可见的测试结果

用户名	定义的角色	访问权限	测试结果
姑 X	一般家人	部分可见	时 间：2015-12-25 09:10:14 发布内容：节日快乐！亲们
周 XX	同事	部分可见	发布内容：节日快乐！亲们 纬度：42.892405

4 结论

本文对传统的角色访问控制方法的基本模型进行了改进，提出了二级角色定义，并根据用户对不同访问者设置的角色来设置相应的访问位置信息的权限. 手机应用程序的可行性测试结果表明，此方法有利于保护实时上传的位置信息，能有效防止非法攻击者对用户位置信息的收集和利用. 本文在可行性测试中，会出现访问用户同时可以被设置几个角色的问题，造成角色冲突，因此，如何解决在 APP 运行过程中角色冲突的问题需要得到进一步研究.

参考文献：

[1] 张丞. 移动互联网隐私泄露研究[D]. 北京：北京邮电大学，2012：4-26.

[2] Li J S, Chang G R. HARBAC model for the administration of role-based access control[J]. Journal of Chinese Computer System, 2009, 30(7): 1321-1325.

[3] 康丽珠，黄青松，刘利军. 一种改进的基于角色的分级授权访问控制模型[J]. 昆明理工大学学报，2009，34(1)：40-42.

[4] 李立新，陈伟民，黄尚廉. 强制访问控制在基于角色的安全系统中的实现[J]. 软件学报，2000，10(28)：56-59.

[5] Sandhu R, Bhamidipati V, Munawer Q. The ARBAC97 model for role-based administration of roles [J]. ACM Tran on Information and System Security, 1999, 2(1): 105-135.

[6] Li J S, Chang G R. HARBAC model for the administration of role-based access control[J]. Journal of Chinese Computer System, 2009, 30(7): 1321-1325.

[7] 李世宇. 基于访问控制的应用研究[D]. 济南：山东大学，2009：34-52.

[8] 王建飞. 基于角色访问控制策略的研究[D]. 西安：西北工业大学，2006：5-18.

[9] 肖宝亮，顾春华，高小伍，等. 基于分级角色的访问控制[J]. 华东理工大学学报，2006，32(11)：1327-1330.

[10] 马丽，马世龙，眭跃飞，等. 一种 RBAC 的描述逻辑表示方法[J]. 计算机网络与信息安全，2010，28(3)：908-945.

[11] 洪帆，胡龙斌. 基于角色的访问控制在分布式资源互访中的应用[J]. 计算机工程与应用，2002，54(18)：1567-1575.