# 研究智能手机轻量级访问控制的探讨

周 健[1],马志媛[2],杨 宸[1]
(1. 陕西师范大学 计算机科学学院,陕西 西安 710062;
2. 西安电子科技大学 计算机科学学院,陕西 西安 710062)

**摘 要**:随着智能手机市场占有率的不断上升,智能手机已变得越来越普及。作为一种新型的掌上小型电脑,手机安全性的意义不言而喻。文中引入访问控制来对手机信息安全进行保护,但是由于手机自身电池电量和存储空间的有限性,使得现有的访问控制不能够直接移植到手机中。因此文中将根据智能手机的实际应用需求,对现有的访问控制进行轻量化,设计一种轻量级基于角色的访问控制系统来保证手机信息的安全访问,并对该访问控制模型和系统总体结构进行系统的论述。

**关键词**:角色;基于角色访问控制;智能手机
**中图分类号**:TP309 **文献标识码**:A **文章编号**:1673-629X(2011)11-0227-04

# Research on Access Control of Smart Phone

ZHOU Jian[1], MA Zhi-yuan[2], YANG Chen[1]
(1. School of Computer Science, Shaanxi Normal University, Xi'an 710062, China;
2. School of Computer Science, Xidian University, Xi'an 710062, China)

**Abstract**: As more and more phones are sold, smart phones are becoming increasingly popular. The significance of security about phone is self-evidence as a new kind of palmtop minicomputer. It introduces the access control to protect the information security for smart phone. Because of the limitation of battery and storage of smart phone, the existing access control program cannot be directly installed on the phone. Therefore according to the practical application requirements, it proposes a lightweight method for the existing access control program on smart phone, it designs a kind of lightweight role-based access control program to ensure the information security in smart phone, and discusses the access control model and system overall structure systematically.

**Key words**: role; role-based access control; smart phone

## 0 引 言

随着网络与通信技术的不断发展,手机功能正在向智能化迈进,智能手机正在成为人们的日常消费品。由于智能手机具有独立操作系统,用户可以自行下载、安装第三方服务商提供的程序,使得手机功能得到不断扩充;由于具备个人信息管理和无线网络连接功能,智能手机已经成为互联网中新型的终端节点。用户在使用智能手机的同时,会将许多敏感信息存放在手机中,这些信息一旦泄露或损坏,将对用户造成无法估量的损失。在智能手机系统中,引入访问控制,能很好的保护敏感信息。

访问控制系统可以对敏感资源的操作访问进行限制,防止非法用户的侵入以及对合法用户操作进行实时监控,防止不慎操作而造成的破坏,它在安全体系结构中具有不可代替的作用。传统的访问控制技术主要有三种形式:自主访问控制 DAC、强制访问控制 MAC 和基于角色的访问控制 RBAC。与 DAC 和 MAC 两种访问控制相比,基于角色的访问控制(Role Based Access Control, RBAC)技术[1],能有效地改进传统访问控制的不足,降低管理开销,提供了一个较好的安全环境。基于角色访问控制引入了角色概念,使得角色作为一个用户与权限的接口,解耦了权限和用户的关系。管理员根据实际情况定义所需角色,并给角色赋予相应的访问权限,而用户则根据实际情况再被赋予相应角色,这将访问控制过程分为2个部分,所有的授权给予了角色而不是直接给予用户,实现了用户和权限的分离,极大地方便了权限的管理。然而对于智能手机而言,由于电池电量和存储空间的局限性,无法长时间运算大型复杂程序,而目前的角色访问控制程序,在运算量和占用硬盘空间上都大大超过了手机的要求,因此对现有的程序进行轻量化将成为较好的选择。

**收稿日期**:2011-04-11;**修回日期**:2011-07-20
**基金项目**:陕西省科技攻关项目(2008K01-58)
**作者简介**:周 健(1988-),男,云南昆明人,硕士研究生,研究方向为信息安全与密码。

文中将根据智能手机的实际应用设计一种改进的轻量级基于角色访问控制系统，有效解决上述问题。

## 1 基于智能手机系统的轻量级 RBAC 模型描述

### 1.1 模型结构设计

智能手机的访问控制系统，作为一种轻量级的应用，它具有如下特点[2,3]：

(1)系统具有严格的用户操作验证，保证较高的安全性。

(2)系统只在智能手机上运行，用户数量有限。

(3)在系统中具有较为简单的权限操作，主要是对资源对象的增添、删除、修改、查询操作。

根据上述轻量级系统特点，在智能手机实际应用中，将手机用户角色分为手机拥有者和手机借用者，手机拥有者授予访问控制最高权限，拥有对访问控制权限的增添、修改、查询、删除功能。因此手机拥有者根据实际情况，为手机借用者授予指定权限，如手机借用者将无法拥有对手机短信内容、电话本、图片、文档等存有敏感信息的程序进行操作查询，而只能对一些普通程序进行操作，如通话、上网、玩游戏等。手机的界面显示也根据角色所具有的权限不同而不同，界面将在两种角色之间相互切换，并只显示指定程序。该访问控制规定除手机拥有者外的其他用户均为手机借用者，并且两种角色之间切换，只由手机拥有者执行，通过密码确认完成。综上所述，对经典 RBAC 模型进行轻量化，得到轻量级 RBAC 模型结构如图 1 所示[4,5]。

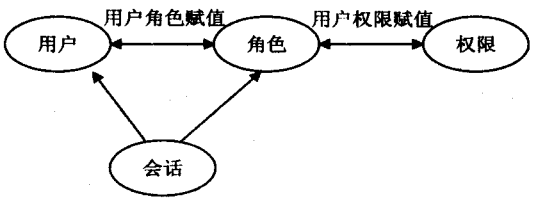


图 1 一种适用于智能手机的轻量级 RBAC 模型

图 1 中用户、角色、权限为基本核心要素，会话层只为单个元素。在实际应用中，仅有手机拥有者在手机开机或者角色切换时进行密码确认，而不存在在系统运行过程中同时有多个用户进行角色确认，因此会话层仅需要一个元素即可。当有其他用户借用手机时，手机拥有者运行访问控制程序，将角色改为手机借用者，手机界面也随之改变。当其他用户归还手机后，手机拥有者运行访问控制程序，将角色改为手机拥有者，并通过密码确认，完成操作。为了安全保密，该访问控制程序设置为快捷键，而不是直接显示在手机屏幕上。

### 1.2 基本要素关系定义

●对图 1 中的各要素定义为：

(1)用户(user)集合 $U = \{u_1, u_2, \cdots, u_m\}$ 是访问控制模型中的主体，是智能手机实际应用中所有用户的总和。

(2)角色(role)集合 $R = \{r_1, r_2\}$ 代表具有共同属性的一类主体，角色与用户的应用环境和上下文不相关，主要是由用户自身属性决定，并通过建立静态授权关系获得角色。在轻量级 RBAC 模型中的角色仅为手机拥有者、手机借用者，大幅度简化了角色的管理。

(3)权限(permission)集合 $P = \{p_1, p_2, \cdots, p_k\}$ 表示实际进行动作时，用户具体的智能表达，在智能手机实际应用中角色的相应权限被静态赋予。

●各要素间的关联关系为：

(1) $UA \in U * R$ 是一个多对多的从用户到角色的权限关系集。

(2) $PA \in P * R$ 是一个多对多的从角色到权限的授权关系集。

同时，设 $S$ 是用户和角色之间的二元关系。$T$ 为角色和权限之间的二元关系。所以，对应于 $S$ 有关系矩阵 $\boldsymbol{M}_S = [S_{ij}]_{m*n}$，对应于 $T$ 有关系矩阵 $\boldsymbol{M}_T = [T_{ij}]_{n*k}$。其中：

$$r_{ij} = \begin{cases} 1, & < u_i, r_j > \in S \\ 0, & < u_i, r_j > \notin S \end{cases}$$

$$t_{ij} = \begin{cases} 1, & < r_i, p_j > \in T \\ 0, & < r_i, p_j > \notin T \end{cases}$$

因此，得到复合函数关系：$S \cdot T = \{ < u, p > \mid u \in U \cap p \in P\}$，这样复合关系就将两个没有关系的 $U$ 和 $P$ 集合联系起来，形成了用户到权限的对应。由此就得到用户和权限的关系矩阵 $\boldsymbol{M}_{S \cdot T} = [st_{ij}]_{m*n}$。

## 2 轻量级 RBAC 系统总体结构设计

根据轻量级 RBAC 模型结构定义，对其访问控制系统总体结构进行设计[6,7]，如图 2 所示。

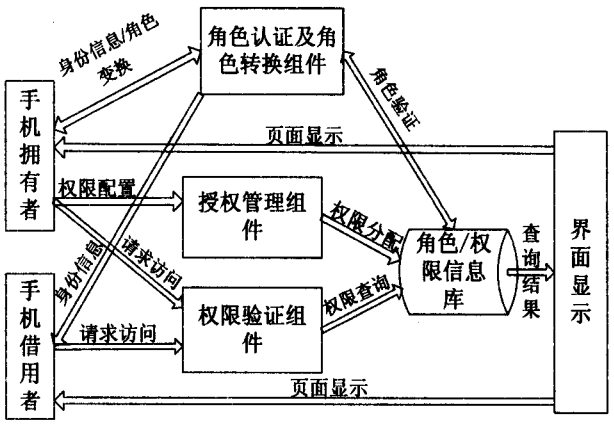


图 2 轻量级 RBAC 模型的访问控制系统总体结构

系统由以下几个部分组成：角色认证及角色转换组件、授权管理组件、权限验证组件、角色/权限信息库

以及界面显示五个部件。此设计使得系统各模块之间相互独立;使得系统组件轻量化;使得系统授权认证及访问控制更加高效。

系统各部分功能如下:

(1)手机拥有者在开机或者角色转换时,首先需要通过密码进行角色认证获得自己的角色信息。当有他人要借用手机时,手机拥有者通过角色转换组件修改角色属性,手机借用者则不需要进行密码确认,直接得到角色信息。

(2)在用户得到角色信息之后,就可以凭借当前的角色提出访问请求通过访问控制系统,之后权限验证的组件就会收到该访问的请求,并得到相应的用户角色信息。

(3)权限验证组件将所获得的用户信息在角色/权限信息中进行权限查询,在角色/权限信息库中得到相应的角色权限。

(4)角色/权限信息库将角色权限查询结果发送给界面显示,界面显示根据用户所具有的权限,在手机上显示出相应程序界面。

(5)授权管理组件提供给手机拥有者一个图形化管理界面,授权管理组件将显示出手机中所有的安装程序,让手机拥有者能很方便地选择手机借用者所能使用的程序权限,并将结果存入角色/权限信息库中,实现对手机权限的配置与管理。

根据上述描述,对五大部件进行如下设计:

(1)权限验证组件:它将会得到用户对手机资源提出所有的访问请求,并通过查询角色/权限信息库来检索用户对应角色的权限信息,从而验证用户对手机资源操作的合法性。因此说权限验证组件是整个访问控制系统的核心。

在手机的实际应用中,权限验证组件根据控制策略,首先依据用户角色信息以及相应的角色权限来验证用户对手机访问操作的合法性[8],并通过界面显示组件对手机界面的实时改变,显示出该用户所具有的访问操作图标。

(2)授权管理组件:它是以图形化管理界面来给手机拥有者提供操作的。从而手机拥有者可以通过管理界面对手机访问控制系统中的角色及权限信息配置与管理进行操作。它将以树形结构显示出角色、资源以及操作等权限信息,这样手机拥有者将无需了解角色/权限信息库中访问权限表的具体结构,它将由系统自行生成,记录相应数据。

根据手机的实际应用,授权管理组件提供以下管理操作:

角色管理:定义与创建系统中的角色并对角色信息进行配置[9]。根据该访问控制模型定义,本系统中的角色仅为手机拥有者和手机借用者两种。手机拥有者将通过授权管理组件提供的操作界面为角色添加和删除权限,灵活进行角色权限分配。

权限管理:对系统中的权限进行合法定义与管理。手机访问控制系统中将权限 Permission 定义为对资源 Source 和操作 Operation 的动态绑定[10,11]。手机拥有者可以通过授权管理组件来实现手机资源与用户操作的动态绑定,这一动作的实现是基于授权管理组件可提供图形化界面。根据上述方法对系统中的权限进行定义,并继而实现对该权限信息的修改与删除,达到动态授权管理的目的。

(3) 角色/权限信息库:它记录了访问控制系统中用户和权限信息,根据智能手机轻量级访问控制的实际应用,因为只存在两个角色信息和尽可能地节省存储空间,文中采用 Access 数据库来记录系统中的用户和权限信息。Access 数据库结构清晰,具有良好的扩展性,易于创建、存储与处理,有利于方便快速地提供数据库查询服务。数据库设计如图 3 所示。

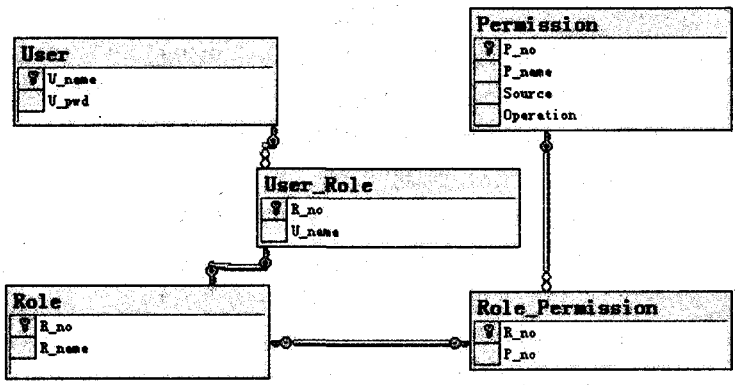


图 3　角色/权限信息库组件中数据库关系图

该关系数据库由 5 个表组成:

User 用户表:记录用户的基本信息,包括用户名和密码。

Role 角色表:记录角色信息,包括角色识别码、角色名。

Permission 权限访问表:记录访问权限信息,实现对资源和操作的动态绑定,包括权限识别码、权限名称、该权限的资源名称以及对该资源的操作名称[12]。

User_Role 用户角色表:记录用户和角色的匹配关系,其中只有机主自身为手机拥有者该角色,其他用户均为手机借用者。

Role_Permission 角色权限表:记录角色和权限的匹配关系,每一个角色信息都有多个权限和它匹配,所有的权限都由手机拥有者根据实际情况设定所得。

(4)角色认证和角色转换组件:它是手机轻量级访问控制系统中,最常用的图形图像界面组件,手机拥有者每次登陆和变更角色都是通过其进行。

角色认证和角色转换组件负责向用户提供角色信息。手机拥有者在手机开机之后就会向角色认证组件提供身份信息验证,包括:用户名和口令验证。角色认证组件将对该信息进行有效验证,角色认证组件从角色/权限信息库中检索出手机拥有者的角色信息,并返回该信息给手机拥有者。当手机进行角色转换时,手机拥有者通过角色认证和角色转换组件,设置角色为手机借用者,此时不再需要进行身份验证。该组件将直接从角色/权限信息库组件中检索出手机借用者的信息,并返回。直到手机归还后,手机拥有者再次通过角色认证和角色转换组件,设置角色为手机拥有者,提供身份信息(用户名和口令),进行确认。

(5)界面显示组件:它根据从角色/权限信息组件中得到的查询结果,改变手机显示界面,只该角色所拥有的资源和程序图标,动态化地对敏感资源做到实时保护。

## 3 结束语

文中介绍了一种适用于智能手机的轻量级基于角色访问控制模型系统,并对系统模型和总体结果进行了形式化描述。与一般的访问控制系统相比,该系统的特点为:运算复杂度较低,用户范围不大。所以该轻量级访问控制模型系统符合智能手机的轻量级应用特点,使得授权管理操作变得简捷,使得系统工作效率更高,且能保障用户敏感信息,降低电池能耗。随着无线网络的迅速发展和全部的覆盖,智能手机已经成为互联网中新型的终端节点。在未来的应用中,手机用户将更多地融入网络系统,共享和访问信息,收发邮件、与电脑协同操作,进行实时办公。

文中所设计的模型可以有效地保障信息安全,防止用户对资源的非法访问。相信随着智能手机的大力推广,会有很好的前景。

**参考文献:**


[1] Ferraiolo D, Cugini J, Kuhn R. Role Based Access Control: Features and Motivations[C]//Computer Security Applications Conference. [s. l.]:[s. n.],1995:81-85.

[2] 曹 磊,吕良双. 基于角色访问控制的轻量级访问控制系统的研究[J]. 计算机应用,2006,26(2):357-360.

[3] 张海峰,赵 凯,陆 徜. 轻量级认证与授权研究综述[J]. 计算机工程,2003,29(1):168-170.

[4] Sandhu R, Coyne E, Feinstein H, et al. Role-based Access Control Models[J]. Computer IEEE,1996,29 (2):38-47.

[5] Zou D Q, He L G, Jin H, et al. CRBAC: Imposing multi-grained constraints on the RBAC model in the multi-application environment[J]. Journal of Network and Computer Applications,2009,32(2):402-411.

[6] 张晓群,董丽丽. 角色访问控制模型的研究及应用[J]. 计算机技术与发展,2007,17(2):42-45.

[7] 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.

[8] 刘昌平,范明钰,王光卫,等. Android 手机的轻量级访问控制[J]. 计算机应用研究,2010,27(7):2611-2613.

[9] 王 立,万世昌,张 珍. 基于互信属性调配机制的访问控制模型[J]. 计算机技术与发展,2009,19(12):127-130.

[10] 朱益霞,孙道清,沈 展. 一种普适计算下的访问控制策略[J]. 计算机技术与发展,2010,20(8):90-93.

[11] 赵 洁,沈苏彬. Web 服务访问控制的设计和实现[J]. 计算机技术与发展,2010,20(10):159-162.

[12] 路 川,胡欣杰,纪 锋. 基于角色访问控制的协同办公系统设计与实现[J]. 计算机技术与发展,2010,20(3):230-233.


(上接第 226 页)


[3] 阮奇桢. 我和 LabVIEW [M]. 北京:北京航空航天大学出版社,2009.

[4] 谭 营,许化龙,吴 琳. 基于 LabVIEW 的舵机测试系统设计[J]. 微计算机信息,2007(31):133-134.

[5] 戴 鹏,刘 剑,符 晓. 基于 TMS320F2812 与 LabVIEW 的串口通信[J]. 计算机工程,2009(2):94-96.

[6] 吕向锋,高洪林. 基于 LabVIEW 串口通信的研究[J]. 理论与方法,2009,28(12):27-30.

[7] 戴鹏飞, 王胜开, 王格芳,等. 测试工程与 LabVIEW 应用[M]. 北京:电子工业出版社,2006:158-161.

[8] 郑祥波. 基于 LabVIEW 与 DSP 串口数据采集系统[J]. 微计算机信息,2004,20(2):45-46.

[9] Topal T, Polat H. Software Development for the Analysis of Heart Sounds of LabVIEW in Diagnosis of Cardiovascular Disease[J]. Springer Science & Business Media,2008,32:409-421.

[10] 杨乐平,李海涛,杨 磊. LabVIEW 程序设计与应用[M]. 北京:电子工业出版社,2005:431-439.

[11] 陈真诚,陈晓俐. 基于虚拟仪器和远程心电监护系统的研制[J]. 医疗卫生装备,2009(4):45-46.

[12] Gao Jingge, Wang Shuqiang. Research on Monitoring System for Granary Based on LabVIEW[C]//Proceedings of the 8th International Symposium on Test and Measurement. [s. l.]:[s. n.],2008:1683-1686.

[13] 张会香,成谢锋. LabVIEW 平台上的心音分析虚拟仪器设计[J]. 计算机技术与发展,2010,20(11):217-220.

[14] Barabiuk R G. Compressive Sensing[J]. IEEE Signal Processing Magazine,2007,24(4):118-121.