doi:10.3969/j.issn.1002-0802.2018.02.023

Android 平台细粒度权限管理系统的研究与实现 *

吕 博，李永忠

（江苏科技大学 计算机学院，江苏 镇江 212003）

摘 要：由于 Android 平台的开源性，它拥有庞大的用户数量，而其本身的提供的粗粒度安全机制，如沙盒、权限控制、应用签名等，已经不能满足用户日益增多的需求。所以，Android 粗粒度安全机制下存在安全问题急需解决。借鉴 Android 细粒度的权限管理机制，设计实现了对用户隐私数据的提取进行权限控制。该系统能够分析隐私权限，并且用户在授予权限时能够拥有选择的权利，从而增加 Android 系统权限控制的安全性，同时大大提高对隐私数据的安全性控制。

关键词：Android；细粒度的安全机制；权限控制；信息安全

中图分类号：TP302 **文献标志码：**A **文章编号：**1002-0802(2018)-02-0389-05

Exploration and Implementation of Fine-Grained Permission Management System for Android Platform

LV Bo, LI Yong-zhong

(College of Computer, Jiangsu University of Science and Technology, Zhenjiang Jiangsu 212003, China)

Abstract: Due to its open-source nature, Android platform has the vast number of users, and the coarse-grained security mechanisms provided by itself, such as sandbox, permission control, application signature, can no longer meet the increasing needs of users, so the security issue existed in Android coarse-grained security mechanism requires a prompt solution. So with reference on the fine-granularity management mechanism of Android, the permission control of the extraction for user privacy data is designed and implemented. The system can analyze the privacy authority, and the user can have the right to make selection when the authority is granted, thus increasing the permission-control security of Android system. And at the same time, the security control of private data is greatly improved.

Key words: Android; fine-grained security mechanism; permission control; information security

0 引 言

当今社会，人们在工作、生活和娱乐等各个方面都越来越依赖智能终端。在这个大背景下，Android 作为一个开源的系统平台，备受关注。截止到 2017 年第一季度，国外的市场数据调研公司 Kantar woroldpanel 公布，在中国、英国、德国、西班牙、法国等国家，安卓的市场占有率稳居第一，而且还有不断上升的趋势。然而，由于庞大的用户群体，安卓本身存在的安全隐患逐渐显现。

目前，Android 平台的安全形势变得越来越复杂，而对 Android 的安全研究，其中重要的一点就是对权限控制的研究。Android 粗粒度的安全机制，主要是“一次性的授权”，用户只有看到某个应用所要的权限，而不能自主进行选择；如果用户想要拒绝某个权限，只能放弃安装此软件 [1]。这样用户的隐私信息就不能得到周全保护。本文主要是针对 Android 安全机制本身存在的漏洞，借鉴 Android 细粒度的权限管理机制，不仅可以对隐私权限进行分析与检测，而且在进行授权时，用户可以有自主选择的权利，从而增加 Android 系统的安全性 [2]。

* 收稿日期：2017-10-11；修回日期：2018-01-07 Received date:2017-10-11;Revised date:2018-01-07

1 Android 系统架构

Android 是 Google 开发的基于 Linux 内核的开源手机操作系统。系统架构主要分为 4 层，从下而上分别为：Linux 内核层（Linux Kernel）、系统运行库层（Libraries）、应用框架层（Application Framework）和应用层（Application）[3]，如图 1 所示。Linux 内核是 Android 系统的运行平台，为其提供底层的驱动；系统运行库层是 Linux 内核和应用程序框架层之间的沟通渠道 [4]；应用框架层是 Android 开发的基础，并能提供编程接口（API），简化了组件重用，极大方便了应用程序的开发；应用层是 Android 中安装所有应用程序的所在层 [5]。

图 1 Android 系统架构

2 Android 安全机制

Android 本身建立在 Linux 内核的基础上，因此需在 Linux 系统的基础上建立了一套属于自己的安全机制 [6]。它不仅继承了 Linux 操作系统的安全机制，而且其系统架构的各个层次都有独特的安全特性。Android 的安全体系框架主要包括：内核级别的安全机制、系统级别的安全机制、基于应用程序级别的安全机制和用户级别的安全机制，本文将着重介绍权限控制机制 [7]。Android 的安全体系框架，如图 2 所示。

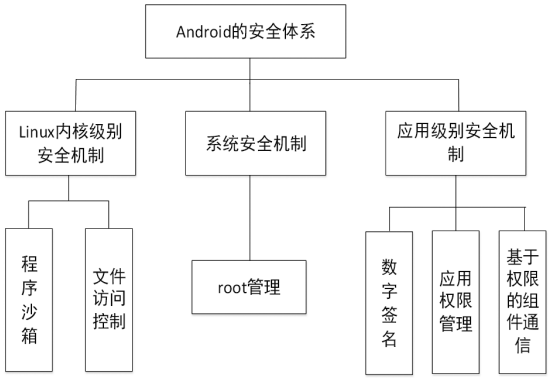


图 2 Android 系统安全框架

Android 本身的安全机制简单概括，即在默认情况下，应用程序不能对整个系统、其他应用或用户进行不利的操作 [8]。而 Android 系统的开源性，使得其对应用程序的安全设计上采取的是粗粒度的安全机制。它主要提供的功能是用户自己对自己负责的权限申请与授权机制 [9]。可以大致把 Android 的权限管理机制分为 3 个部分：权限定义与申请层、权限解析与验证层、权限访问实现层，如图 3 所示。

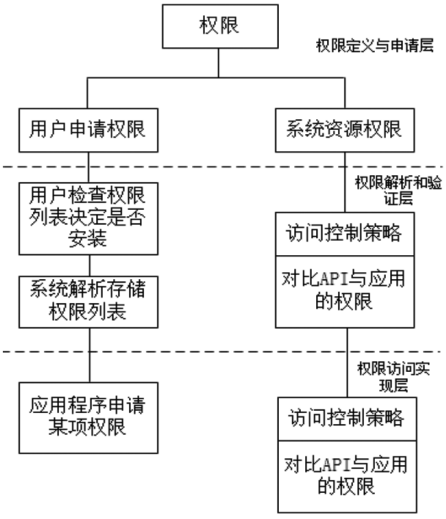


图 3 Android 权限访问框架

在用户安装 APK 时，Android 系统规定每个应用都要将自己所需要的权限告诉用户，即在安装的过程中，要详细显示其所要申请的权限。若用户认为应用程序所要申请的权限已经超过其本身所需要的，那么用户只有权利放弃安装，而不能对权限进行分析与拒绝。可见，Android 系统的粗粒度安全机制，并不能保证用户隐私信息的安全。此外，这种安全机制还存在其他缺陷。第一，权限一经授予应用程序，此权限在该应用程序生命期间都将有效，用户无法剥夺权限；第二，权限机制缺乏灵活性，要么全都批准应用程序所要求的所有权限，要么拒绝应用程序的安装；第三，权限机制安全性不够，不能阻止恶意软件通过 JNI 技术直接调用 C 库，从而获取系统服务。

对 Android 安全机制的介绍可以看出，尤其是 Android 的权限控制机制，在粗粒度的安全机制下，将无法有效保证 Android 系统的安全。所以，本文针对粗粒度安全机制的缺陷，提出了细粒度的权限管理机制。不仅能分析隐私数据本身的提取，而且实现了对权限的分析，同时用户可以根据应用程序属性，控制应用所要提取的权限，从而实现对隐私数据更加安全与全面的保护。

3　隐私保护技术的设计与实现

3.1　设计总体思想

本系统是一个基于 Android 平台的隐私保护技术系统，主要针对用户隐私数据保护，从而保证用户的信息安全。

本文提出的 Android 细粒度的权限控制，主要分为三大模块：权限数据库存储模块、隐私权限控制模块和权限设置管理模块。此系统首先解决 Android 粗粒度下的缺陷，用户可以通过权限设置管理模块，自定义地设置应用所需的有关权限。此外，当应用要申请某项权限时，隐私权限控制模块就会截获应用的请求，并查看是否具有此权限。若存在，则通过申请；若不存在，则对用户做出警告提示，从而加强 Android 系统安全机制本身存在的安全问题。整个系统的框架设计，如图 4 所示。

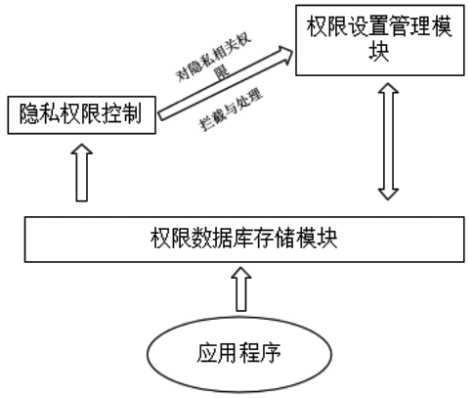


图 4　系统总体设计框架

3.2　权限设置管理模块

权限设置管理模块相当于用户对应用权限的总控制中心。该模块主要先从 Android 系统中已经安装的应用中提取权限列表，然后过滤所有和隐私相关的权限，并显示在相应的权限列表中。这样用户就可以根据自己的需要选择每个应用所需要的权限。简单来说，就是通过获取 PackageManager 对象，调用 getInstalledAoolications() 获取应用的 list 对象，最后通过获取的对象得到应用的权限列表。此外，此模块维护了一个存储着用户在权限设置管理模块手动设置的每个应用的隐私权限的数据库，这个数据库是隐私权限控制模块的基础。具体设计如图 5 所示。

3.3　隐私权限控制模块

隐私权限控制模块是此系统的核心模块。此流程中，如果某个应用程序要读取用户的隐私数据，隐私权限控制模块就会截获此信息，并与权限数据库存储模块中的数据进行对比，查看是否存在。若存在，隐私权限控制模块就会通过；若不存在，则会弹出警告窗口，建议用户阻止该处理。具体设计如图 6 所示。

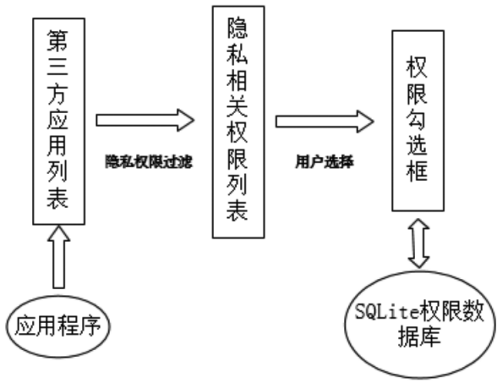


图 5　权限设置管理模块

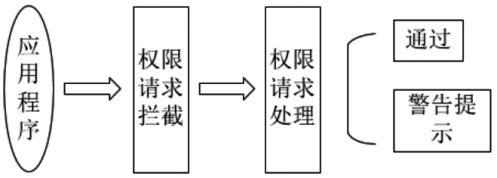


图 6　隐私权限控制模块

3.4　系统整体设计与实现

本系统主要设计了权限设置管理模块、隐私权限控制模块以及权限数据库存储模块。系统的整体设计流程图，如图 7 所示。

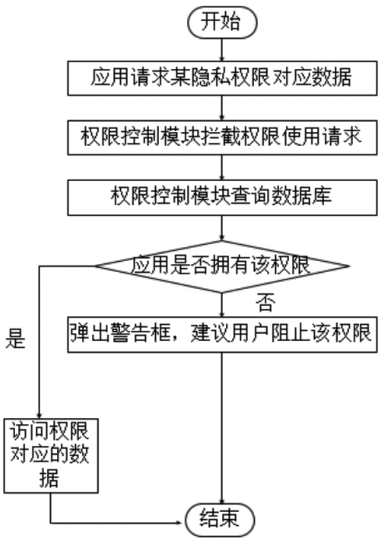


图 7　系统的整体设计流程

系统开始运行后，在第三方应用请求隐私数据权限时，隐私权限控制模块会拦截应用的请求信息，然后与权限设置管理模块中的数据库信息进行

比对，接着查询此应用是否拥有此权限。若拥有此权限，则访问权限对应的数据；若没有通过查询，则隐私权限控制模块则会弹出一个警告提示框，建议用户拒绝该权限。

4 系统测试

本系统主要实现权限设置管理模块和隐私权限控制模块的功能。其中，权限设置管理模块的功能主要是实现能够获取第三方应用的权限，用户能够选择要阻止的权限；隐私权限控制模块主要是实现当应用要提取用户的隐私信息时，分析应用所要提取的权限，并与权限数据库存储模块中的数据进行对比，对用户做出提醒，给出合理建议。这两个模块的结合，可实现对用户隐私数据更全面的保护。它的测试图如图 8、图 9 所示。

图 8 权限管理器

图 9 隐私权限控制模块与后台启动 service

5 结 语

根据上述测试结果，当用户需要安装某一应用程序时，权限数据库存储模块将执行提取第三方应用权限的功能，且用户可以根据自己的需要，选择某项不需要的权限进行阻止；其次，当第三方应用想要申请用户隐私数据的授权时，隐私权限控制模块也会给出相应提示信息，给予用户操作该申请的权利，从而改变以往用户只有查看权限的权利。即若用户出于隐私保护等方面考虑，要阻止某一权限时只能取消安装，而现在用户可以有权利阻止某项权限而不需要取消安装，更加全面地保护了用户隐私信息的安全。

参考文献：

[1] 符易阳，周丹平 .Android 安全机制分析 [J]. 信息网络安全 ,2011(09):23-25.
FU Yi-yang,ZHOU Dan-ping.Android Aecurity Mechanism Analysis[J].Information Network Security,2011(09):23-25.

[2] 陈璟，陈平华，李文亮 .Android 内核分析 [J]. 现代计算机 : 专业版 ,2009(11):112-115.
CHEN Jing,CHEN Ping-hua,LI Wen-liang.Android Kernel Analysis[J].Modern Computer(Professional Edition),2009(11):112-115.

[3] 公磊，周聪 . 基于 Android 的移动终端应用程序开发与研究 [J]. 计算机与现代化 ,2008(08):85-89.
GONG Lei,ZHOU Cong.Development and Research of Mobile Terminal Application Based on Android[J]. Computer and Modernization,2008(08):85-89.

[4] 赵楠，刘佳 . 移动 APP 隐私乱象 [J]. 中国中小企业 ,2013(10):56-57.
ZHAO Nan,LIU Jia.Mobile APP Privacy Chaos[J].China SME,2013(10):56-57.

[5] 林佳华，任伟，贾磊雷 .Android 手机隐私保护系统的设计与实现 [J]. 信息网络安全 ,2013(07):16-19.
LIN Jia-hua,REN Wei,JIA Lei-lei.Design and Implementation of Android Mobile Privacy Protection System[J].Information Network Security,2013(07):16-19.

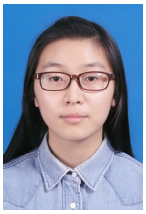
[6] 李中平，邱健峰，李璐等 .Android 手机远程控制关键技术分析 [J]. 计算机应用与软件 ,2013(04):113-115.
LI Zhong-ping,QIU Jian-feng,LI Lu,et al.Analysis of Key Technologies of Remote Control of Android Mobile Phone[J].Computer Applications and Software,2013(04):113-115.

[7] 姚一楠，于璐，何桂立 .Android 平台的安全挑战及应对措施 [J]. 现代电信科技 ,2012(09):16-21.
YAO Yi-nan,YU Lu,HE Gui-li.Security Challenges of Android Platform and Countermeasures[J].New Technology,2012(09):16-21.

[8] 吴剑华，莫兰芳，李湘 .Android 用户隐私保护系统 [J]. 信息网络安全 ,2012(09):50-53.
WU Jian-hua,MO Lan-fang,LI Xiang.Android User Privacy Protection System[J].Information Network Security,2012(09):50-53.

[9] 曾露 .MVP 模式在 Android 中的应用研究 [J]. 软件 ,2016(06):75-78.
ZENG Lu.Application Research of MVP Pattern in Android[J].Software,2016(06):75-78.

作者简介：



吕　博（1992—），女，硕士，主要研究方向为网络与信息安全；

李永忠（1961—），男，硕士，教授，主要研究方向为网络安全、藏文信息处理。