学校编码：10384　　分类号_____密级____
学号：X2011230980　　UDC ____

厦门大学

工 程 硕 士 学 位 论 文

Android 智能手机隐私数据保护系统的设计与实现

Design and Implementation of Android Smartphone's Privacy Guarding System

曾剑凯

指 导 教 师： 廖 明 宏 教 授

专 业 名 称： 软 件 工 程

论文提交日期： 2013 年 9 月

论文答辩日期： 2013 年 11 月

学位授予日期： 2013 年 12 月

指 导 教 师：_____

答辩委员会主席：_____

2013 年 9 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为(　　)课题(组)的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（ √ ）2.不保密，适用上述授权。

（请在以上相应括号内打“ √ ”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘 要

随着云计算、物联网以及各种 Web2.0 技术的快速发展，人类社会所产生的数据种类和数据规模正以前所未有的速度增长，我们已经进入大数据时代。大数据在带来各种智能化和人性化服务的同时，也使得隐私保护问题愈发严重。智能手机以其强大的多媒体应用、实时网络浏览和个性化程序应用等功能，已成为承载个人核心隐私数据的终端设备。Android 作为使用量最大的智能手机操作系统，它的安全性直接影响海量智能手机用户的个人隐私安全，但是层出不穷的 Android 系统漏洞事件令其安全性堪忧。本文针对以上问题进行研究和分析，提出了隐私数据保护方案，设计了“隐私数据保护系统”，实现了“远程保护”子系统。

本文对大数据时代隐私保护问题和现有 Android 平台各种保护方案进行了综述，提出了隐私保护应从智能手机终端这个“源头”抓起，结合静态和动态防护手段，全方位地从“隐私数据生命周期”的各个环节进行保护的思想，设计了隐私数据保护方案和基于 Android 平台的隐私数据保护系统。在远程安全传输模块的设计上，课题采用了私有的通信协议和隧道协议，综合利用分层设计、身份验证和加密等手段，从“内容加密”和“通道加密”两方面保证了传输通道安全性。远程保护子系统主要功能是通过设计的 SMS 隧道，实现“安全手机”和“丢失手机”间的安全通信，有效对失去控制权的手机隐私数据进行管理和销毁。

本课题的独特之处在于将手机用户隐私数据泄漏控制在手机终端这个源头，实现手机用户的“信息自决权”；抽象出了“隐私数据生命周期”，使得对隐私数据的保护更全面、更有针对性；使用了隧道技术保证了“端到端”间的通信安全。

大数据时代带来了更多机遇和挑战，本课题对隐私保护问题的研究只是做了初步的探索，相信隐私保护问题会得到更多地研究和更好解决，让大数据技术充分发挥作用为我们服务。

关键词：智能手机；Android；隐私保护

Abstract

The big data era is approaching along with blooming technologies from cloud computing, thing of Internet and various Web2.0. The services provided by big data make human life more intelligence and meantime more security issues are exposed. Smartphone, which provides rich media, networking and personalized applications, are becoming core devices that carry private information. Android plays very important role in personal privacy since it is becoming most popular OS and target of hackers. This paper presents a proposal to protect individual privacy.

This paper firstly analyzes existing protecting solution on Android system and gets conclusion: it has to take smartphone itself as source point, incorporates with static and dynamic approaching to protect each cycle of privacy's life. A privacy protecting module based on Android is proposed: Adopts private communication and tunnel protocol together with authentication and encryption to provide security for transmission. The remote protecting module's primary function is to make lost phone communicate with safe phone and thus effectively control privacy from lost phone.

The specific features of the proposal are: terminate leaking from smartphone end and thus control the privacy information; abstract concept of "life of privacy" to keep integrity of private information; provide tunnel to ensure security of end-to-end communication.

Big data brings opportunities and challenges, this paper's research security field of big data, hope more concerns will be solved and big data serves human better.

Key words: Smart Phone; Android; Privacy Protection

目 录

Contents

第一章 绪论

1.1 引言

随着云计算、物联网以及各种 Web2.0 技术的快速发展，人类社会所产生的数据种类和数据规模正以前所未有的速度飞速增长，我们已经进入大数据时代。每天由各种传感器、监视器、信息发布机构和互联网用户产生的数据量已经大大超出我们所想象。基于对这些大数据的挖掘，政府机构、各大网络运营商提供了更智能的、更人性化的服务：亚马逊通过根据用户数据挖掘购物习惯以实现自动推荐“感兴趣”物品，提高销售额；谷歌通过分析用户搜索记录，挖掘用户搜索习惯，以更准确的、更个性化的展现搜索结果；各种 SNS 服务商则通过分析用户的兴趣爱好和人际关系，实现好友推荐、群组推荐等功能。但大数据技术也给我们带来了新的挑战，“棱镜门”事件[1]的曝光使得个人隐私保护问题令人堪忧。用户个人隐私数据被非法收集、“二次利用”[2]以及非授权的数据关联分析等，都是造成个人隐私泄漏的原因。

根据英国调查咨询公司 Wireless Expertise 的最新预计，到 2013 年时的智能手机年销售量将从 09 年的 1.65 亿增加到 4.23 亿，全球智能手机的用户人数也将达到 16 亿。智能手机以其功能性强、联网便捷、扩展性强以及便于携带等特点已成为日常生活的必需品，许多手机用户甚至全天候随身携带。智能手机已经成为用户核心隐私数据的载体，承载着通信录、银行账号、各种账号密码和多媒体信息等敏感数据。

而 IDC 发布的最新报告[3]显示，2013 第二季度全球智能手机出货总量为 2.364 亿部，同比增长 51.3%，环比增长 9.3%。其中，Android 市场份额由去年同期的 69.1%上升至 79.3%，是市面上使用最多的智能手机操作系统。由于 Android 平台的开放性和庞大的市场占有量，以及强大的开发技术支持、较低的开发门槛以及 AppMarket 的运作,使得 Android 平台上第三方移动应用数量高速增长。

但是层出不穷的 Android 系统漏洞事件令其安全性堪忧，其脆弱的安全性导致第三方应用程序可能非法使用、收集用户隐私数据。加之手机用户安全意识淡薄（如肆意的 root，刷第三方系统 ROM，安装未知软件等），造成了手机用户的

隐私数据泄露或被恶意定制付费服务的情况。特别是智能手机强大的存储功能和多媒体功能（如录音功能、摄像功能等），可能使得用户的核心隐私数据和私密多媒体文件泄漏，严重威胁了用户个人的信息安全。因此，对移动智能手机的隐私保护刻不容缓。

1.2 项目开发背景及意义

大数据时代中，数字技术已经让社会丧失了遗忘的能力，取而代之的则是完善的记忆。这是因为数字化技术、廉价存储器、归档提取技术和全球性覆盖这 4 个驱动力，使得遗忘变得昂贵而又困难，记忆反而便宜又容易[4]。作为个人隐私数据更是如此，一旦用户失去了对自身隐私数据的控制权，这些数据将很可能永久地被存储在某个存储中。基于大数据的数据挖掘、关联分析等技术，都有可能以这些数据为支点，充分挖掘出其他更丰富的隐藏价值。而目前对于隐私保护的立法、司法处于严重滞后的状态，商业公司全凭自我约束力来处理收集到的这些数据。因此，从源头抓起，保持用户对隐私数据的控制权，防止其失控流入非受控区域，是目前应对这一危机的有效手段。

智能手机作为现代化的移动智能终端，已经不仅仅是通信联络的工具，更多地是满足用户对多媒体应用、实时网络浏览和个性化程序应用等需求的生活必需品。由于智能手机已经渐渐地与人类活动形影不离（许多手机用户几乎全天候随身携带），它承载了大量的用户核心隐私数据，例如通信录、银行账号、各种账号密码和多媒体信息等。智能手机也成为商业公司、第三方应用程序开发者争夺用户资源的阵地，而为了提供更加智能化、人性化的服务，对用户个人数据的抓取、收集和分析成为必不可少的手段之一。部分恶意第三方应用程序开发者更是不折手段地进行非授权的系统操作，造成了用户隐私泄露或被恶意定制付费服务的情况。还有可能发生的情况是，手机用户失去对手机的控制权（例如手机丢失），这时候存储于手机上的隐私数据也会处于不可控的情况，极可能造成隐私泄漏。

Android 作为使用量最大的智能手机操作系统，占据了将近八层[3]的市场份额，它的安全性直接影响着智能手机用户的信息隐私安全。但是最近美国国土安全部和司法局近期发布了联合报告，作为美国几大主要移动平台之一的 Android，由于其开源开放的特性，是绝大多数恶意软件攻击的对象。据一份统计结果显示，

在 2012 年度 Android 平台的恶意软件数约占所有平台的 79%[5]。由此可见，Android 系统的安全性令人堪忧，若仅仅依靠 Android 自身的安全防护，远无法满足手机用户对隐私数据进行保护的需求。因此，急需在 Android 系统平台上，开发出一款能够捍卫手机用户隐私数据权的防护软件，让用户自己真正掌控隐私数据。

作为手机上存储的用户的核心隐私数据，如果因为系统漏洞、使用不当或者恶意软件攻击而泄露或丢失，那将给手机用户带来难以估量的损失和困扰。对于恶意攻击者或者其他有心人，这些数据可能变成手中的“武器”。例如攻击者可能利用通讯录中的联系人，冒充手机用户的身份对其进行诈骗、骚扰，套取更多敏感信息；攻击者还可能监听手机用户的敏感信息，如银行账户、支付密码等，直接获取经济上的利益；更恶劣的情况是，攻击者可能借助高速的网络环境（WIFI、3G 等），利用智能手机的录音或摄影、摄像等功能进行实时或离线的远程监控，手机用户将毫无隐私可言。由此可见，对于智能手机隐私数据的保护应该是全方位的：它包括了对静态数据的保护，如已经存储在手机上的通信录、通话记录、短信息和多媒体文件等；还应该包括对可以生成、获取或收集隐私数据的资源的保护：如话筒、摄像头、输入键盘和 GPS 模块等。

本课题充分考虑到大数据时代的背景环境，选取了使用量最大的主流移动智能手机操作系统 Android 作为研究平台，深入分析智能手机隐私数据的保护各个环节并提出了“隐私数据生命周期”的概念，设计了私有的通信协议和隧道协议，综合使用了静态和动态保护手段，提出了一个智能手机隐私保护方案，并以此为核心实现了 Android 智能手机隐私数据保护系统——PrivacyGuard 系统的远程保护子系统原型。这对于大数据时代中还未解决的“个人隐私数据保护”问题，是一个探索和尝试，具有积极的意义。

1.3 研究现状

隐私问题由来已久，计算机的出现使得越来越多的数据以数字化的形式存储在计算机中，互联网的发展则使得数据更加容易产生和传播，数据隐私问题越来越严重[6]。作为承载着用户核心隐私数据的智能手机，它的安全性直接关乎着手机用户的隐私数据安全。

为了在 Android 系统平台的基础上提高它的安全性，以增强手机用户对隐私数据的掌控能力，研究者从不同角度提出了许多保护方案。目前 Android 平台上针对隐私保护的研究方向，主要可以分为两大类：静态分析和动态控制。第一类是在应用程序安装之前，对其申请的执行权限进行静态分析。Kirin 设计了一套的权限策略，一旦应用拒绝违反该权限策略则拒绝安装程序包；Stowaway 则从满足程序功能所需的“最小权限集”的观点出发，比较程序申请的权限集是否超出了“最小权限集”的范围，从而可以判定该程序是否有越权的嫌疑。第二类是在应用程序安装后，在运行时对其进行动态控制。主要包括扩展标记追踪、行为分析、接口模拟、应用级的强制访问控制、远程复制分析和标签化的追踪[7][8][9][10]。

这两类方法各有优缺点，第一种方法是将安全防护的关口提前到程序安装阶段，一旦发现程序有超出其功能的权限申请就拒绝安装。这种做法好处在于可以将损失最大化减少。但是其不足之处也很明显：静态分析时间冗长，时间成本较高；精确度不高，容易造成漏报和误报的情况，用户往往面对“鱼和熊掌不可兼得”的尴尬，要在安全性和便利性之间做出选择；即使满足“最小权限集”的要求，静态分析也无法应对“程序组合权限提升”的攻击。

第二种方法则将保护的关口后移到程序执行“危险操作”时，才对应用程序作出限制。这种做法好处在于可以对应用程序作出“细粒度”的控制，让用户在安全性和便利性之间取得一个平衡点，保留应用程序有用的部分。其不足之处在于为了实现动态监控应用程序的功能，需要调用操作系统底层资源，可能会牺牲一定的效率和稳定性；存在“漏控”的情况，被恶意软件“绕过”监控；要求手机用户对 Android 系统有一定的了解，或具备一定的专业知识，这对于大部分普通用户比较难执行。

在商用软件方面，市面上的主流隐私监控类软件一般都具备这两种类型的功能，但是其具采用的方法和实现的功能各有不同。以使用量较大的“360 手机卫士”、“QQ 手机管家”、“LBE 隐私卫士”和“网秦安全”为例，它们大都以上述两类方法为基础，实现了隐私保护功能。主要包括了针对智能手机隐私数据的保护（如：短信、通信记录、联系人、GPS 信息、后台录音、联网权限、录音、手机识别码、摄像头等），对应用程序的访问权限进行控制和对私密数据的保护。这些软件的特点主要是“面对功能”的，即主要以实现对具体隐私数据的保护功能