**北 京 邮 电 大 学**

**本科毕业设计（论文）开题报告**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 学院 | 计算机学院 | 专业 | | 计算机科学与技术 | | 班级 | 2015211308 |
| 学生姓名 | 周紫惠 | 学号 | | 2015211369 | | 班内序号 | 29 |
| 指导教师姓名 | 杨旭东 | 所在单位 | | 计算机学院 | | 职称 | 副教授 |
| 设计（论文）题目 | （中文）基于VirtualApp的安卓应用访问控制系统的设计与实现 | | | | | | |
| （英文）Design and Implementation of Android Application Access Control System Based on VirtualApp | | | | | | |
| 毕业设计（论文）开题报告内容：（主要包含选题的背景和意义；研究的基本内容和拟解决的主要问题；研究方法及措施；研究工作的步骤与进度；主要参考文献等项目） 1.选题的背景和意义 VirtualApp，是一个开源的Android应用虚拟化引擎，允许在其中创建虚拟空间，并在这个虚拟空间中任意安装，启动和卸载其他应用，并且与外部环境完全隔离，实现应用多开。VirtualApp可以被视为一个在应用层及服务层上的Android虚拟机，所有被VirtualApp打开的应用，和VirtualApp共享UID。VirtualApp在运行时，会通过反射调用的方法，Hook其中对系统服务的调用。利用应用层的ContentProvider模型，模拟系统服务向APP提供所需信息，例如位置、联系人、网络状态等。  Android是一种基于Linux的自由及开放源代码的操作系统，目前Android系统已成为移动计算终端中应用最广泛的操作系统，用户的隐私数据也呈现爆炸式增长，隐私泄露的风险也越来越大。Android应用隐私访问控制，是采用以应用为基准的授权方式，即：用户授予或禁止某应用访问某隐私信息的权限。Android应用的隐私访问，很多时候不仅来自于应用本身，还可能来自于应用所捆绑的插件，在以上模式下，若用户选择允许，则将允许应用的所有部件访问同样的隐私信息，由于第三方插件的不可控性，会带来隐私泄露风险。  为了控制隐私风险，针对部分应用，基于VirtualApp的安卓应用访问控制系统可以通过模糊化或屏蔽的方式，阻止其获取部分敏感的隐私信息。针对不同类别的应用和隐私信息提供多种控制策略供用户选择，增强了应用的安全性控制。 2.研究的基本内容和拟解决的主要问题2.1研究的基本内容  1. 研究应用在VirtualApp沙盒内部运行，通过ContentProvider对系统服务进行模拟，对APP要获取的敏感信息进行处理，在完全不改变APP自身行为，及Android既有授权模型的情况下，实现敏感信息的访问控制 2. 研究现有Android系统访问控制机制的原理。研究VirtualApp在应用层、服务层的虚拟化实现，以及如何在该框架下，针对应用，在其运行时，以虚拟化的方式，细粒度控制其对隐私信息的访问，作为对Android已有访问控制系统的补充。 3. 针对不同应用的功能特点，对不同类型的隐私信息，分别设计多种控制策略供用户选择。例如对于位置信息，用户可以选择不提供，直接提供精确位置，提供加偏处理后的精确位置等。  2.2 拟解决的主要问题 为了深入理解基于开源的Android应用虚拟框架VirtualApp，完成基于VirtualApp的安卓应用访问控制系统的设计与实现，需要解决以下问题：   1. 理解Android系统架构和VirtualApp在应用层、服务层的虚拟化实现，VirtualApp如何模拟Android系统服务向应用提供资源，实现系统服务的虚拟化和相关路径的虚拟化。 2. Android系统的安全性需求包括机密性保护需求、完整性保护需求、特权访控需求、最小权限原则需求和应用分域管控需求。针对不同类别应用和不同类型隐私数据设置安全等级，细化访问控制策略规则，约束应用程序的访问行为。 3. 现有Android系统自带的访问控制机制存在粗粒度的授权机制、粗粒度的权限、不充分的权限文档和权限提升攻击等问题。  3.研究方法及措施 根据本课题的研究内容和拟解决的主要问题，主要采用以下方法进行研究：   1. 文献阅读：研究Android系统架构和Android现有访问控制机制，分析不同类别应用的功能特点和不同类型隐私信息，设置不同的安全等级，制定细粒度的访问控制策略。 2. VirtualApp源码和Android系统访问控制机制源码阅读：通过阅读源码及动态调试，基本了解VirtualApp如何模拟Android系统服务，实现敏感信息的访问控制，制定细粒度的访问控制策略。 3. UML建模：依据Android系统中应用功能分类的特点以及Android系统安全防护需求，设计基于VirtualApp的Android系统的细粒度访问控制模型。 4. 计算机编程：在VirtualApp的基础上，对现有的Android访问控制机制改进，强化访问控制模块，解决Android系统安全机制存在的不足，实现基于VirtualApp的Android系统的细粒度访问控制。  4.研究工作的步骤与进度  1. 2月12日 - 2月25日：确定论文研究领域及范围，了解Android服务虚拟化相关技术及框架的研究现状，形成初步的开题报告。 2. 2月25日 - 4月21日：研究VirtualApp用作Android应用沙盒及服务层虚拟化框架的工作原理，研究APP获取隐私信息的途径，及通过修改虚拟化框架的实现，对隐私信息的获取进行控制的方法 3. 4月22日 - 5月20日：实现简单的访问控制原型演示，并在主流APP上进行验证 4. 5月21日 - 6月15日：完成论文撰写，准备最终答辩  5.主要参考文献 [1] Ryan Stevens, Clint Gibler, Jon Crussell 等. Investigating user privacy in Android ad libraries[C]. Workshop on Mobile Security Technologies (MoST). 2012  [2] Bin Liu, Hongxia Jin, Ramesh Govindan. Efficient Privilege De-Escalation for Ad Libraries in Mobile Apps. MobiSys’15, May 19–22, 2015, Florence, Italy.  [3] VirtualApp框架官网：https://github.com/asLody/VirtualApp  [4] ContentProvider |Android Developers,  <https://developer.android.com/reference/android/content/ContentProvider.html>  [5] Application security | Android Open Source Project,  <https://source.android.com/security/overview/app-security>  [6] Alexandra Burlacu. Android 6.0 Marshmallow: A Closer Look At App Permissions. Tech Times. 2015.11. http://www.techtimes.com/articles/102049/20151103/android-6-0-marshmallow-a-closer-look-atapp-permissions.htm | | | | | | | |
| 指导教师签字 |  | | 日期 | | 年 月 日 | | |

注：可根据开题报告的长度加页。