网络安全学院学生创新资助计划

创新任务申请书

项目名称：针对安卓/iOS 应用权限滥用问题的检测方法研究

课题设置企业：蔚来

所属领域：数据安全

推荐高校（盖章）：上海交通大学

在本校所有推荐项目中的排名：

项目申请人：徐小洁

联系电话：13032822183

中国网络空间安全协会制

2022 年 **5** 月 **10** 日

承诺书

承诺人：徐小洁

身份证号：210282200009252126

本人就申请网络安全学院学生创新资助计划创新任务向本项目发起方中国网络空间安全协会、中国互联网发展基金会、所申请创新任务项目的资助企业以及所在高校作出如下承诺

1.保证和免责：

（1）本人确认并保证提交的任务申请文件以及获得资助企业立项资助后所产生的相关成果，包括但不限于文献、专利、程序、原型等的原创性，不违反法律法规或其他适用法律的限制，也不会侵犯任何第三方知识产权、商业秘密等权利或违反保密义务。如涉及开源项目或软件使用，本人将明确说明开源项目名称、遵循的开源协议等相关内容。

（2）本人所提交的任务申请文件及相关成果均由本人自主创作，如有抄袭、盗用等不符合任务规定的不法行为，本人将退还相关研究经费，所产生的所有责任由本人自行承担和赔偿。

2.知识产权：

（1）原有知识产权。本人及资助企业在资助任务履行之前各自拥有的原有知识产权仍归各自所有，如研究项目中不可避免必须要使用资助企业的原有知识产权，经资助企业书面同意，本人承诺仅能为执行研究项目在其内部于项目执行期间使用该原有知识产权。本人同意就研究项目所涉及的原有知识产权授予资助企业及其关联公司在

世界范围内不可撤销的、永久的、免费的制造、使用、修改、运行、演示、许诺销售、销售、进出口、发行、制作衍生作品或产品的权利以及对上述权利进行分许可的权利，上述知识产权使用费用已在资助金额中涵盖。若本人转让研究项目所涉及的原有知识产权，资助企业享有同等条件下的优先受让权。

（2）新产生知识产权。除法律另有规定，研究项目下新产生知识产权归本人以及资助企业共同共有，即将来若进行知识产权的申请、注册或登记的，权利人应为我本人及资助企业。我本人及资助企业均有权独自使用项目成果，但未经双方同意，任何一方不得将项目成果转让给第三人，否则违约的一方将向对方承担违约赔偿责任。双方根据研发项目的需要，建立定期例会机制，汇报研究项目的新产生知识产权和能够成为知识产权的创意、构思、技巧等，必要时经过双方商议，可临时组织交流会议。

（3）新产生知识产权的保护。新产生知识产权的获得、维护、保护等费用由资助企业承担。双方应积极鼓励、协助和配合获得、维护和保护新产生知识产权，包括设置激励机制，以鼓励研究项目的参与人员积极参与提交专利申请、软件著作权登记等，以全面保护研究成果，还包括配合签署权利获得、维护的相关文件。

（4）衍生知识产权及保护。本人独立创造的衍生知识产权归本人所有，资助企业享有被授予该等衍生知识产权的许可权利，若本人转让该等衍生知识产权，在同等条件下，资助企业享有优先受让权。就衍生知识产权的许可、转让的具体事宜，双方协商一致后，另行签署书面协议进行约定。

3.本人就所提供的或在创新任务中涉及的素材，包括但不限于照

片、视频、音频等，所涉本人肖像权授予资助企业及其关联方一项免费的、可再授权的、非排他的许可以实现本资助计划或资助企业品牌宣传活动在各渠道的推广。

4.隐私权：本人理解并同意，为了资助计划及任务的组织管理、对参赛者身份进行验证、评审、公示等与本任务相关之目的，本计划的组织实施方中国网络空间安全协会可收集、存储、分享并使用本人在任务报名和实施过程中提供的个人信息，包括但不限于姓名、地址和电子邮件地址等。并且本人知情并同意将个人信息及研究项目信息录入项目数据库。

5.保密义务：本人承诺将对各方提供的基础数据、资源支持、相关资料等保密，未经各方同意，不向任何第三方透露前述信息，否则愿意承担违约赔偿责任；

6.若本人的资助申请获得批准并收到资助款项，将愿意接受各方的监督，及时汇报资助款项的使用情况及项目研究进展；本人承诺将资助款项仅用于研究项目，否则将向各方承担违约责任；本人将依照法律、行政法规规定及税务机关相关要求及时纳税。

7.对外宣传：除非法律禁止，提交申报书或获奖即表示本人同意计划发起方为推广宣传或其他商业目的使用本人姓名、形象、照片、肖像、个人简历、参赛作品和声明以及与任务相关的任何录像片段，无需额外补偿。此外还同意将本人姓名放在获奖者名单上。

承诺人（签字）：徐小范

日期：2022 年 7 月 31 日

创新任务申请书

<table>
<tr><td colspan="8">一、基本信息</td></tr>
<tr><td>项目名称</td><td colspan="7">针对安卓/iOS 应用权限滥用问题的检测方法研究</td></tr>
<tr><td>资助企业</td><td colspan="7">蔚来</td></tr>
<tr><td rowspan="2">推荐高校</td><td>高校名称</td><td colspan="6">上海交通大学</td></tr>
<tr><td>所在地区</td><td colspan="6">上海市闵行区东川路 800 号</td></tr>
<tr><td rowspan="6">项目申请人</td><td>姓名</td><td colspan="2">徐小洁</td><td>学院</td><td colspan="2">网络空间安全学院</td></tr>
<tr><td>就读专业</td><td colspan="2">网络空间安全</td><td>在读学位</td><td colspan="2">□博士
√硕士
□学士
□其他</td></tr>
<tr><td>证件类型</td><td colspan="2">居民身份证</td><td>证件号码</td><td colspan="2">210282200009252126</td></tr>
<tr><td>移动电话</td><td colspan="2">13032822183</td><td>电子邮箱</td><td colspan="2">xu.xiaojie@sjtu.edu.cn</td></tr>
<tr><td>指导教师</td><td>√有指导教师
□无指导教师</td><td>指导教师姓名</td><td>邱卫东</td><td>指导教师专业</td><td>网络空间安全</td></tr>
<tr><td colspan="7"></td></tr>
<tr><td>个人学习和研究经历</td><td colspan="7">本人高中就读于大连海湾高级中学拔尖班，本科就读于四川大学网络空间安全学院，主要研究深度学习、隐私保护领域，期间获得过国家奖学金、综合一等奖学金、肆零肆网络空间安全奖学金；以第一作者发表一篇 CCF-C 类 SecureComm 会议论文；获得第四届“强网杯”全国网络安全挑战赛作品赛三等奖、2022 年 OPPO 安全隐私创意大赛优胜奖；参与两项大创省级优秀结题项目；参与指导教师杨进副教授的四川省科技厅创新创业科技人才项目等；自 2021 年 11 月至 2022 年 8 月，在中国平安加马人工智能研究院（Gamma Lab）NLP 组实习，担任助理算法工程师，从事 NLP 模型搭建及部署工作，协助撰写 3 篇发明专利。
今年 9 月即将开始的研究生阶段研究方向是网络安全和隐私保护，目前基于毕业设计“APP 隐私泄露行为的动态检测和测量技术研究”对 Android 应用动态分析和网络测量已有较深入的研究，结合前期参与隐私创意大赛时对静态分析方法的研究，正在将研究成果转化为论文待投稿。</td></tr>
<tr><td>相关附件</td><td colspan="7">请见附件。</td></tr>
<tr><td colspan="8">1. 各奖学金证明；
2. 论文录用证明及论文文本；
3. 各类竞赛、大创及项目参与证明；
4. 实习证明；
5. 毕业设计介绍材料；</td></tr>
</table>

二、研究目标和内容

1.课题拟解决的关键技术问题，拟采取的技术路线和主要创新点

待突破前沿技术：

1. 隐私政策解析过程中，如何排除与权限滥用问题不相关的语句对信息抽取结果的影响，以及如何精确获取隐私政策中声明的**权限和数据类型**、**数据接收方**信息；

2. 动态分析方法受到动态测试工具界面触发率的限制，尤其是现有动态测试工具很难自动化注册或登陆应用账号，导致遗漏进入登陆状态后的应用行为，应该如何**自动化触发应用登陆状态**；以及通过动态测试获取到的**交互流量数据、应用界面截图**，应该如何充分利用，来挖掘权限和数据的实际使用情况和滥用情况，包括泄露信息类别、泄露信息流向等；

3. 静态分析方法需要借助逆向工具得到中间代码和资源文件，拥有许多经典的分析方法，如何利用如 **UI 分析、数据流分析、API 分析**等方法对静态的代码和文件进行充分的分析和挖掘，来发现权限和数据的实际使用情况，进而挖掘权限滥用问题；

4. 动态分析方法会有界面触发率等限制、静态分析方法会有无法分析动态加载代码等限制，所以动静态分析方法都有实现的必要性，因此如何兼顾上述多种分析方法优势，同时又能按照权限和个人信息的敏感度和检出次数合理**整合**分析结果；最终如何清晰展示一致性匹配结果、权限和数据滥用情况也是一个重要的问题。

主要研究内容：

1. 数据获取及预处理

待获取数据主要包括**移动应用安装包**、**隐私政策**及其他**应用基本信息**。当下移动应用主要依托于各大应用商城，如应用宝、Google Play 等，因此可以从上述商城网站上爬取安装包和应用基本信息。前期工作已经实现了适用于国内应用宝、小米应用商店、华为应用市场和国外 Google Play 的爬虫工具，并拥有前期的爬取结果，因为应用发展迅速版本迭代快，前期爬取结果存在一定滞后性，需要补充完善。

而隐私政策的获取渠道具有不稳定性，例如隐私政策链接会指向主页或 404 错误页，因此有以下两种获取方法。

（1）按照法律要求，应用在应用市场上架时须提供隐私政策，并在应用详情页将隐私政策展示给用户，因此使用网站爬虫也可以获取隐私政策，该部分的爬虫工具和爬取结果前期工作也已实现，待补充完善。

（2）应用运行过程中会在用户注册或登陆时提醒用户阅读在线的隐私政策文档并选择‘同意’，因此可以借助 Uiautomator[1]工具编写动态运行脚本，定位隐私政策链接；也可以直接在应用的文字中搜索类似“隐私政策”的字段，获取字段指向的链接。

以网页形式呈现的隐私政策，需要 HtmlToPlaintext[2]工具将 HTML 转换为纯文本格式，在确保内容一致的前提下，实现删除部分 HTML 标记、页码等干扰数据，整合嵌套列表项等预处理方法，该部分预处理工作前期已实现。

2. 隐私政策文本分析

为探究权限或数据在声明和使用上的**一致性问题**，首先需要从隐私政策中获取应用声明的即将使用的权限和数据类型、数据接收方，该部分主要包括**权限相关语句定位**和**二元组信息抽取**两个子任务。

2.1 权限相关语句定位任务

法律对隐私政策有多方面约束，要求隐私政策充分介绍如信息收集类型、信息安全保护措施、用户个人权利等内容。如下图所示，不仅是介绍信息收集类型部分(左)会涉及到权限或数据类型，其他部分也会涉及(右)，如果将隐私政策全文直接用于信息抽取，识别结果的误报率会很高，因此需要对隐私政策进行处理，排除与权限滥用问题不相关的语句对信息抽取结果的影响。

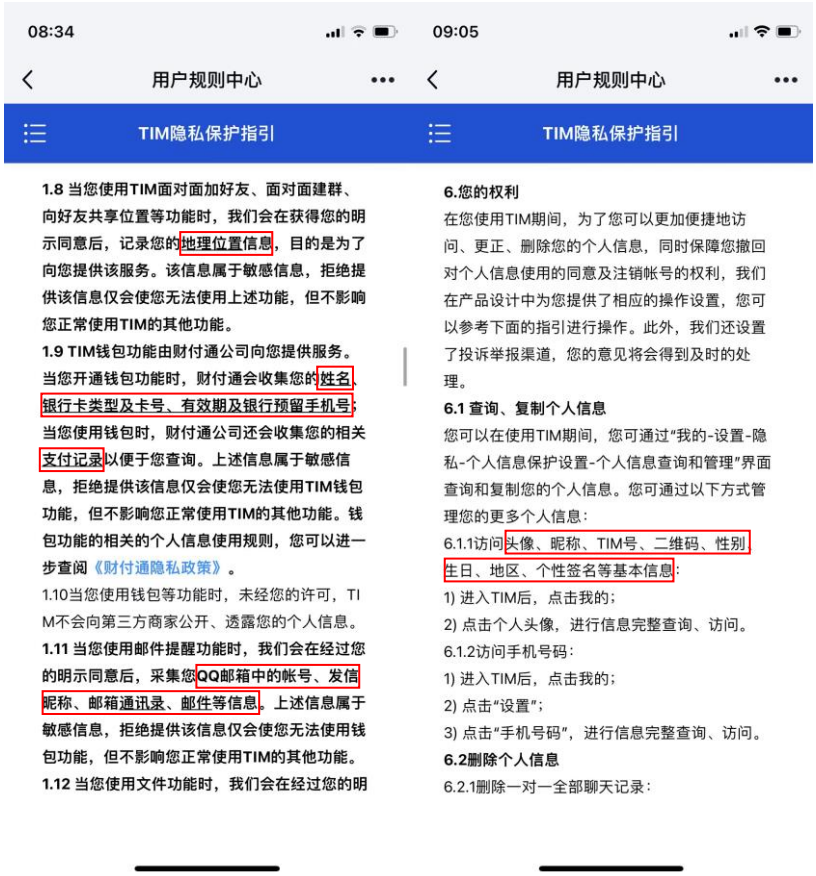

图 2.1 隐私政策截图

现有多种 NLP 预训练模型的下游分类任务均可实现对文本中逐句描述的内容进行分类，如 BERT 家族中的 RoBERTa，基于标注数据集对预训练模型进行微调，再通过对比实验选取效果最佳的模型，利用模型来定位权限和数据使用声明部分。该分类任务难点是需要标注数据集，现有数据集 OPP-115 针对的是英文场景且参考的规范是欧盟 GDPR，本任务还面向中文场景并且关注的是国内各项法律规范，因此人工标注数据集是必要的，前期工作已构建了一个基于个人信息保护法的隐私政策多分类数据集，包含 8,000+条隐私政策语句，但为适配本任务仍要进一步补充完善。

2.2 二元组信息抽取任务

PolicyLint[3]基于实体识别和包容关系提取的**本体生成方法**，构建了多个用于获取隐私政策中的关键信息的本体，包括①个人信息、财务信息等数据本体，②第三方、第一方等接收方本

体，下图所示是 PolicyLint 开源的个人信息本体树状图中的一小部分，该本体中共有 455 个节点，另外接收方本体包含 513 个节点。

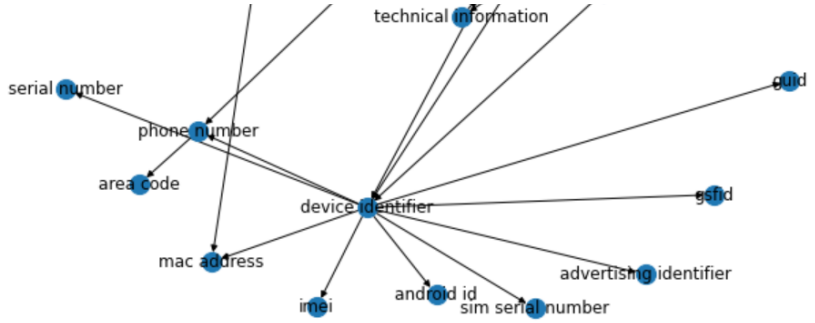

图 2.2 PolicyLint 开源数据本体示例

PolicyLint 的整体目标是挖掘英文隐私政策中的逻辑矛盾，但它的信息抽取方法对本任务有很大的参考价值，而且它的代码和数据完全开源，具体应用方法如下：首先使用上述定位任务得到的分类模型，定位到隐私政策中的权限相关语句，再使用中文命名实体识别(NER)方法识别语句中所有实体，实体识别的结果再与①②本体进行相似度匹配，即可实现二元组信息抽取。

基于深度学习的实体识别相较于基于关键字和基于统计的实体识别在处理模糊、多变和未知名词时效果更佳，考虑从头开始训练一个优秀的 NER 模型对数据量的要求非常大且十分耗时，参考 PolicyLint，合适的解决方案是在已有模型的基础上，新增本任务的训练样本对模型微调，该部分的标注数据无需太多，因为可以采用随机替换、拼接等方法增强语料。spaCy[4]是一个支持多语言的工业级自然语言处理工具，3.0 版本的 NER 工具基于 OntoNotes 规范已达到了 89.8%的准确率，最重要的是它支持用户使用自己的标注数据来更新模型，优化抽取结果。

3. 应用行为分析

为探究权限和数据在声明和使用上的**一致性问题**，还需要获取应用实际使用的权限和数据类型。按照是否需要在模拟器中运行应用可以分为**动态分析方法**和**静态分析方法**，两大类分析方法中各包含多个具体的方法。最后检出结果的整合步骤，还需要按照权限和个人信息的敏感度和检出次数进行后处理来提升可视化效果、减少误报。

为探究**权限和数据的滥用问题**，还需对相关数据进行追踪来分析潜在的数据安全风险，主要的方法是动态分析方法中的**流量数据分析**和静态分析方法中的**数据流分析**。

3.1 动态分析方法

动态分析方法是指需要在模拟器中运行应用，依赖动态测试工具模拟应用运行状态，收集运行时的行为数据进行分析，主要包括流量数据和界面截图数据。

1）动态测试工具改进

针对现有动态测试工具的界面触发率低、无法结合应用界面信息动态生成输入文本，进而难触发应用登陆状态等问题，拟采用 TextExerciser[5]反馈迭代式文本生成工具，结合应用界面提示信息动态生成输入文本，有效解决应用对输入文本如“长度大于 8 个字符”、“必须包含数字、大小写字母”等约束条件，实现账号自动注册登陆等功能，触发应用登陆后的行为。前期工作已实现了 TextExerciser 动态测试的全流程并实现了 416 个安卓应用的动态测试，但 TextExerciser 的初始处理语言是英文，需要基于 TextExerciser 源码进行语言调整即可实现中文文本生成功能，以适应中文应用。

2）流量数据分析

因为模拟器完全可控，使用中间人攻击方法可以获取多数应用动态运行时产生的明文流量数据(其中部分流量本身即采用明文传输，可以通过流量中的协议类型判断)，分析流量数据可以挖掘应用传输了哪些用户隐私信息。具体方法是在流量数据中检索动态测试时预定义的个人数据，同时基于关键字匹配的方法在流量数据中检索键名，如'long'、'Atv_Lon'，两种方法互为补充，以完整检出流量数据中的用户信息。前期工作已收集了 Google play 中应用的 390680 条交互流量数据，下图所示是前期工作挖掘到的 Google play 中下载量高达 10,000,000+的应用直接使用 HTTP 明文协议传输用户的 GPS 定位信息。

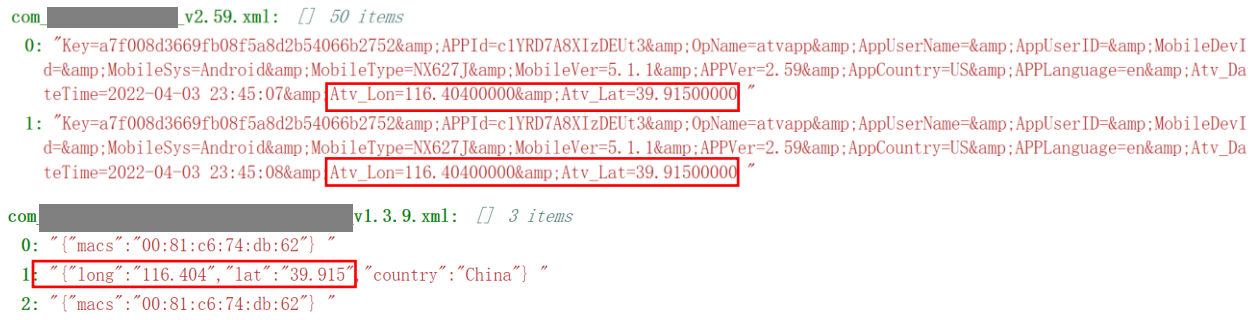

图 3.1 应用运行时截图示例

另外数据接收方也是一个重要的分析目标，数据传输至第一方应用提供商和第三方服务提供商是需要区别考虑的，因为第三方服务提供商多为广告推荐公司、数据分析公司、数据驱动的运营公司[6]等，应用会因利益驱动无视法律约束向第三方共享用户数据。现有研究区分第三方公司多依赖黑名单[7]的方式，而黑名单在当前互联网科技发展飞速的背景下很难满足完整性和时效性，会因为黑名单不全面导致漏报。因此提出了一个通用性交互方划分标准，针对流量中的域名信息，利用 Python 中的 Whois 工具查询域名的注册机构名称信息，即域名所属公司信息，与爬取到的 Google play 中的应用基本信息匹配，进而定位第一方应用提供商和第三方服务提供商。如下图所示，前期工作在分析了 390680 条流量数据后，发现 74%的流量均是与第三方交互，与应用提供商交互的流量只占 10%。

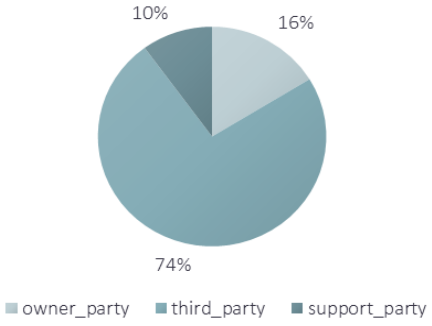

图 3.2 流量交互方分布

3）界面截图分析

如下图所示，应用运行过程中的界面截图包含了①应用请求用户手动输入的个人信息(左)，用户手动输入的信息难以通过检测权限调用检测到，而且如果该部分是动态加载的代码，使用静态分析方法难以检出，因此该部分信息不容忽视；②请求用户点击同意申请的权限类型(右)，该类权限多涉及到危险权限，因为 Android 要求应用申请危险权限需要在运行时弹出许

可对话框，用户手动同意之后才会获得授权，因此也是不容忽视的部分。

对界面截图的分析首先需要依赖如 paddleOCR 开源 OCR 工具识别界面文字，如“请输入您的邮箱”、“想访问您的相机”，再对文字进行实体识别定位到“邮箱”、“相机”。综上，可以确定应用在实际使用过程中，依赖用户输入收集的信息类型和依赖用户同意请求的权限类型。

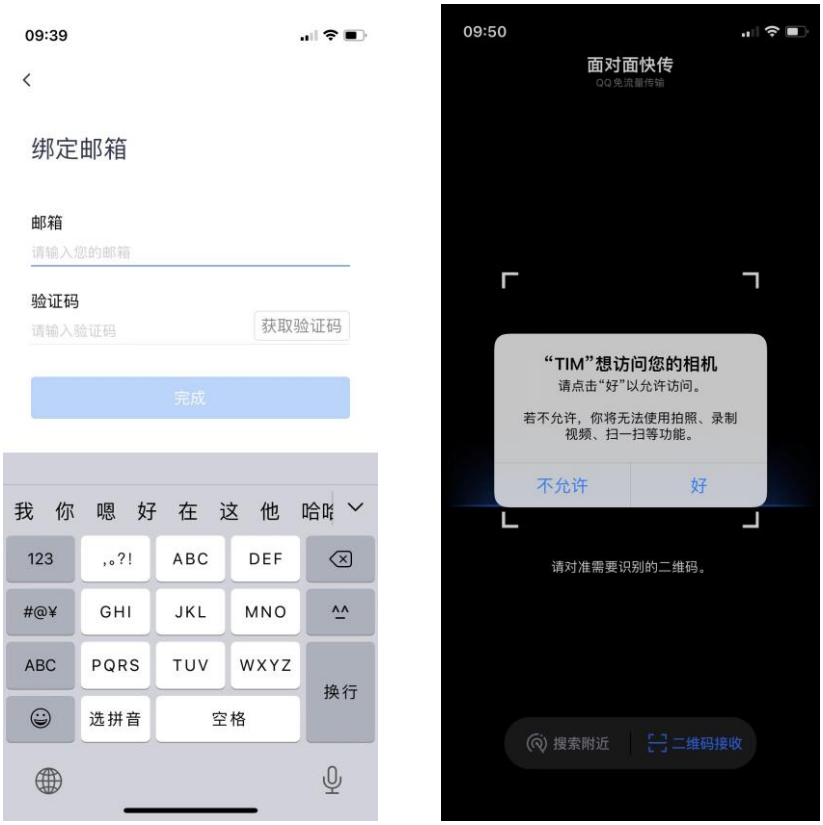

图 3.3 应用运行时截图示例

3.2 静态分析方法

静态分析方法是指使用如 Apktool 工具对程序进行逆向操作，通过扫描反编译代码或静态文件来了解潜在的执行行为，包括 UI 分析、数据流分析、API 分析，上述分析方法在解决具体问题时各有优势，因此都可以作为挖掘方法。前期三种方法均有实现，但是考虑任务的适配性和现有方法的局限性，仍需进一步完善。

1）UI 分析

应用的布局有两种定义方式：①XML，②运行时用代码创建，这两种方法通常被灵活地结合起来使用，其中运行时用代码创建的控件由上述动态分析方法中的界面截图分析方法检出，而 XML 的分析方法相对简单一些。应用 Apk 反编译后的 res/layout/目录下存放着 XML 格式的布局文件，通过检测控件属性可以判断其是否为输入控件或选择控件，如 TextView, EditText, Button 等，然后将 strings.xml 中控件的文本提示信息输入上述实体识别模型得到识别结果，进而得到文本输入控件收集的个人信息类型。

2）数据流分析

FlowDroid[8][9]是一款开源的静态数据流分析工具，本任务需要将 Android 系统收集用户隐私相关的敏感方法定义为 Source，将数据传输相关的敏感方法定义为 Sink，检测 Source 集合

中信息的数据流流向，追踪其是否流动到 Sink，即判定是否存在完整路径。能够全面且精准的定义 Source 和 Sink 是提升该方法有效性的一个关键，因此 Source 应包括调用从布局信息中获取的文本收集控件 id 的方法如 findViewById()等、常见的信息收集类 API 如 getSimSerialNumber()等，Sink 包括敏感操作或者将隐私数据传输到外界的方法，如 sendTextMessage()发送短信 API、跨进程发送数据 API、网络 API 等。

3）API 分析

Android 实现了一个基于权限的系统来规范应用程序对资源的访问，每个安卓应用程序均包含一个 AndroidManifest.xml 文件，它包含应用向系统申请了哪些受保护的 API；另外，反编译 dex 文件后可以得到字节码信息，从中也可以提取 API 的名称、参数、返回值等信息。最后将上述两种方法获取到的 API 与敏感权限对应起来，即可获取应用使用的敏感权限及数据类型，已有多个研究实现了该映射关系[10]可作为参考。

3.3 后处理

上述两种动态分析角度和三种静态分析方法得到的结果，理论上都可以作为应用实际使用用户权限和数据的依据，但是实际上会下述三种情况：

（1）Android 将权限分为普通权限和危险权限，危险权限是指可能会触及用户隐私或者对设备安全性造成影响的权限，使用者对各等级权限的关注程度是不同的；

（2）不同个人信息类型的敏感度不同；

（3）检测结果不完全可信，可能会有误报；

因此需要依赖**后处理**步骤对各个分析方法得出的结果进行整合，可以按照权限等级和信息敏感度来定义优先级，然后按照优先级对检出结果进行加权，结合加权后的结果设置阈值，低于阈值的即作为误报舍弃，例如使用了 android.permission.ACCESS_NETWORK_STATE 获取网络状态权限、收集了用户性别等只有一个方法检出，那么该权限或信息可以舍弃，反之例如使用了 android.permission.CAMERA 开启摄像头危险权限、收集了用户身份证号码等被多个方法检出，那么该权限或信息会被优先考虑。整个后处理过程会以可视化的方式呈现出来，供使用者参考。

4. 一致性匹配及可视化结果呈现

步骤 2 和步骤 3 获取到的信息需要进行匹配，来判断权限和隐私数据在声明和使用阶段的一致性，结果分为“声明且使用”、“声明但未使用”、“未声明但使用”。其中**“未声明但使用”**部分可以视为权限和数据的滥用情况，具体包括①隐私政策中未声明但却实际使用、②隐私政策中声明传输至第一方，但却违规传输至第三方。追溯到该部分权限的分析方法，即可获取权限的滥用细节。

为增强一致性判断结果的说服力，可视化界面需要呈现隐私政策文本分类和二元组信息抽取的结果、动态分析得到的流量数据和界面截图的挖掘结果、各静态分析方法的分析结果，以及最后一致性匹配的结果（注：前期已有相关的可视化网站，与本项目存在一定相似性可以借鉴），具体细节如下。

（1）在隐私政策分析结果展示部分，可以使用不同的高亮颜色清晰地展示权限相关语句定位结果和二元组信息抽取结果（权限和数据、接收方）。

图 4.1 隐私政策分析结果展示(示例)

（2）在动静态分析展示部分，可以首先按照分析方法逐个展示分析结果；再结合上述后处理逻辑，汇总所有分析方法获取到的应用实际使用权限和信息列表，该部分需要完整展示出后处理过程。

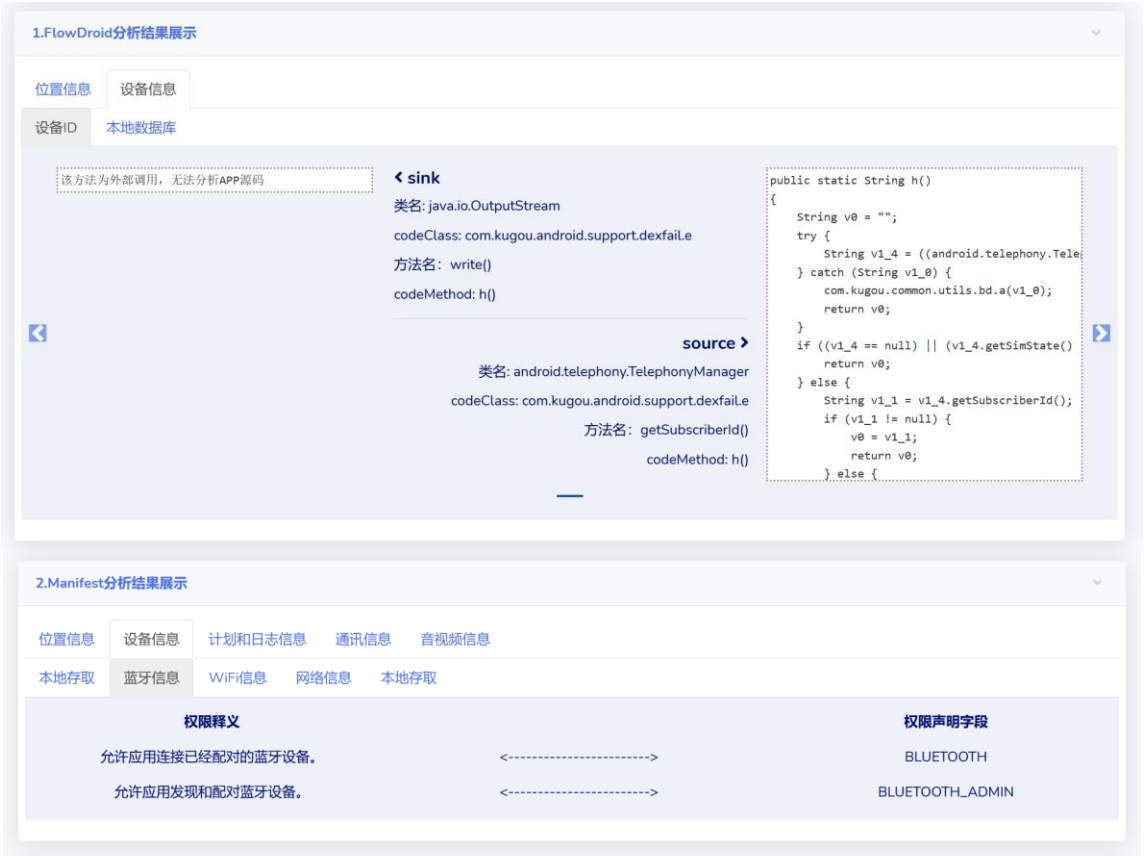

图 4.2 动静态分析展示(示例)

(3) 在一致性匹配结果展示部分，可以分类展示“声明且使用”、“声明但未使用”、“未声明但使用”的权限或信息类型，同时可以展示对应的统计性数据图表；“未声明但使用”部分即**数据滥用部分**，需要将具体的使用细节展示给用户，尤其要给出信息接收方的信息。

图 4.3 一致性匹配结果展示(示例)

(4) 另外，需要一个上传界面接收分析任务，考虑任务需求，需要提供应用的隐私政策文档和安装包。

图 4. 4 新建任务展示(示例)

创新点：

1. 隐私政策解析过程中，首先使用基于隐私政策标注数据微调的 NLP 分类模型，排除与权限滥用问题不相关的语句对信息抽取结果的影响;再使用基于微调的 spaCy NER 模型和本体匹配的**二元组信息抽取**方法，来精确获取隐私政策声明的权限和数据类型、数据接收方信息;

2. 动态分析方法中，利用了 TextExerciser 反馈式文本生成工具**自动化触发应用登陆状态**，提升动态测试工具的界面触发率；提出了基于交互方划分标准的**交互流量**分析方法、基于 OCR 和命名实体识别的**应用界面截图**分析方法，来挖掘权限和数据的实际使用情况和滥用情况；

3. 静态分析方法中，利用了基于布局信息实体识别的 **UI 分析方法**、基于完整且适配的预定义 Source 和 Sink 的**数据流分析方法**、基于 manifest 和字节码信息的 **API 分析方法**，对静态的代码和文件进行充分的分析和挖掘，来发现权限和数据的实际使用情况，进而挖掘权限滥用问题；

4. 提出了基于优先级、检出次数和阈值的**后处理方法**整合动静态分析结果，兼顾上述多种分析方法优势的同时又能提升可视化效果、减少误报；最终对整个分析过程、一致性匹配结果、权限和数据滥用情况进行可视化展示。

参考文献：

[1] Uiautomator 2.2.0, https://developer.android.google.cn/training/testing/ui-automator
[2] HtmlToPlainText, https://github.com/benandow/HtmlToPlaintext
[3] Benjamin Andow, Samin Yaseer Mahmud, Wenyu Wang, Justin Whitaker, William Enck, Bradley Reaves, Kapil Singh, and Tao Xie. PolicyLint: Investigating internal privacy policy contradictions on google play. In 28th USENIX Security Symposium (USENIX Security 19), pages 585–602, Santa Clara, CA, aug 2019. USENIX Association.
[4] spaCy 3.0, https://spacy.io/

[5] He Y, Zhang L, Yang Z, et al. TextExerciser: Feedback-driven text input exercising for Android applications. Proceedings - IEEE Symposium on Security and Privacy. 2020;2020-May:1071-1087. doi:10.1109/SP40000.2020.00071
[6] Bleier A, Goldfarb A, Tucker C. Consumer privacy and the future of data-based innovation and marketing. International Journal of Research in Marketing. 2020;37(3):466-480. doi:10.1016/j.ijresmar.2020.03.006
[7] Ad Server Block List. http://pgl.yoyo.org/adservers/
[8] Arzt S, Huber S, Rasthofer S, Bodden E. FlowDroid: Precise Context, Flow, Field, Object-sensitive and Lifecycle-aware Taint Analysis for Android Apps. Proceedings of the ACM Conference on Computer and Communications Security. 2014;2014-Novem(November):21-26. doi:10.1145/2666620.2666621
[9] FlowDroid 2.9, https://github.com/secure-software-engineering/FlowDroid/releases/tag/v2.9
[10] Kathy Wain Yee Au, Yi Fan Zhou, Zhen Huang, and David Lie. Pscout: analyzing the android permission specification. In Proceedings of the 2012 ACM conference on Computer and communications security, pages 217–228, 2012.

2.课题研究任务与其他课题相互间的逻辑关系（存在课题分解时需填写）

该部分主要介绍前期课题工作与本任务重叠的部分，以及待改进的问题：

(1) 前期工作已经实现了适用于国内应用宝、小米应用商店、华为应用市场和国外 Google Play 的爬虫工具，包括移动应用安装包、隐私政策及其他应用基本信息，并拥有前期的爬取结果，因为应用发展迅速版本迭代快，前期爬取结果存在一定滞后性，需要补充完善；

(2) 前期工作已构建了一个基于个人信息保护法的隐私政策多分类数据集，包含 8,000+条隐私政策语句，但为适配本任务仍要进一步补充完善；

(3) 前期工作已实现了 TextExerciser 动态测试的全流程并实现了 Google play 中 416 个 Android 应用的动态测试，但 TextExerciser 的初始处理语言是英文，需要基于 TextExerciser 源码进行语言调整即可实现中文文本生成功能，以适应中文应用；

(4) 前期工作已基于动态分析方法收集了 Google play 中 416 个 Android 应用共计 390680 条流量，提出了数据通用性交互方划分标准来区分流量交互方，并实验验证其有效性，本任务偏向中文应用，因此需要重新采集流量分析；

(5) 前期静态分析的三种方法均有实现，但是考虑任务的适配性和已有方法的局限性，仍需进一步完善；

(6) 前期工作已实现了与本任务相关的可视化网站，但大部分细节仍需改进和实现；

三、课题计划

（一）项目起止时间： 2022 年 8 月 18 日 —— 2023 年 7 月 18 日（不超过 1 年）

（二）项目实施进度及阶段主要目标（建议以 3 个月为一阶段）

开始日期--结束日期	主要工作内容	预期目标	绩效指标

2022 年 8 月 18 日--2022 年 10 月 18 日	• 应用安装包、隐私政策及相关数据获取； • 数据集构建； • 分类模型、命名实体识别模型微调，二元组模式匹配方法实现；	• 多渠道获取大量应用安装包和隐私政策，数据预处理以适配模型输入要求； • 构建隐私政策分类数据集、实体识别小批量补充数据集； • 基于构建数据集训练分类模型和命名实体识别模型，实现二元组信息抽取；	• 获取应用安装包及隐私政策 10000+； • 分类数据集达 15000 条，实体识别数据集达 500 条； • 分类模型准确率>98，实体识别方法准确率>89，二元组信息抽取效果优异；
2022 年 10 月 18 日--2023 年 12 月 18 日	• 动态分析任务实现：包括动态测试工具部署；流量数据获取及分析；界面截图获取及分析；	• 调整 TextExerciser 工具以兼容中文场景并部署运行应用； • 从流量数据挖掘到应用传输的信息类型和信息流向； • 从界面截图挖掘到应用通过请求用户输入和用户同意的方式获取的信息类型； • 多次实验调整方法的有效性；	• 界面触发率相较于传统工具如 monkey 有 40%的提升； • 两个渠道的信息挖掘脚本效果良好且尽可能通用；
2022 年 12 月 18 日--2023 年 2 月 18 日	• 静态分析任务实现：包括 UI 分析；数据流分析；API 分析；	• 反编译安装包获取可分析资源代码和资源文件； • 配置三种方法所需环境，挖掘到应用使用的权限及数据类型； • 多次实验调整方法的有效性；	• 三个渠道的信息挖掘脚本效果良好且尽可能通用；
2023 年 2 月 18 日--2023 年 4 月 18 日	• 分析结果整合； • 一致性匹配，追踪权限滥用问题； • 可视化平台搭建；	• 使用加权和阈值对动静态分析结果进行后处理； • 结合声明和使用的情况进行一致性匹配； • 针对“未声明但使用”部分追踪滥用权限和数据类型及信息流向； • 实现一个界面友好美观、内容丰富完整的可视化平台；	• 有效结合各分析结果得出一致性分析结果； • 有效追踪权限滥用问题； • 可视化平台功能及内容满足课题需求；
2023 年 4 月 18 日--2023 年 7 月 18 日	• 资料汇总； • 文档撰写；	• 完成课题交付物；	• 完整交付课题要求的原型系统、系统设计实现和使用说明文档；

（三）现有工作基础和工作条件

1. 相关研究工作基础

1） 本科毕业设计

毕业设计题目是“APP 隐私泄露行为的动态检测和测量技术研究”，研究依赖从 Google play 中爬取的 Android 应用安装包及详细信息，使用 Uiautomator 自动化工具模拟应用真实的运行状态，结合 TextExericer 反馈迭代式文本生成工具，按照应用界面提示信息动态生成输入文本，实

现了账号自动注册功能，即迭代式生成符合应用约束的账号和密码文本，有效触发了应用的登陆状态，提升了界面覆盖率和函数覆盖率；动态运行过程中，通过中间人代理抓包方法，获取了Google play 中 416 个 Android 应用动态运行时产生的共计 390680 条流量数据，然后基于提出的通用性交互方划分标准，将流量交互方划分为应用提供商、支持方和第三方，改进了以往基于黑名单的第三方检出方法时效性不足的问题；完成了应用程序隐私泄露行为的多维度动态分析和测量，测量包括隐私信息泄露至第三方的情况、隐私信息明文泄露情况等，并给出了详细的可视化结果。因此对于 Android 应用动态分析、流量数据获取和行为发现以及网络测量有一定的经验。

2） 参与 OPPO 安全隐私创意大赛

参与实现“安卓应用隐私政策合规性与行为一致性分析系统”。系统利用深度学习和实体对齐方法实现了隐私政策合规性分析，首先结合相关法律法规对隐私政策内容的约束，构造了一个隐私政策文本多分类数据集，然后基于 Bert 预训练模型微调，得到的模型用于判断隐私政策中逐句提及的隐私信息相关描述是否符合法律法规规范，进而实现应用程序隐私政策的合规性分析；系统还利用数据流分析等多种静态分析方法，挖掘了应用代码中对用户信息收集的情况，与隐私政策实体对齐的结果匹配，进而实现了隐私政策信息收集声明与移动应用信息收集行为的一致性分析。

系统的呈现效果是一个基于 Bootstrap 和 Flask 框架实现的 Web 可视化平台，不仅支持对单个应用的分析，还通过实时网络爬虫技术实现了各大应用市场的自动化检测，最后统一以报告的形式呈现检测结果；系统还对所有已分析的应用按照其不同的特征和条件进行分类和组合，再结合时间、地域等参数生成相应的态势感知情况与事态防控趋势。最终成果获得了 2022 年 OPPO 安全隐私创意大赛优胜奖。

3） 以第一作者发表 CCF-C 类会议论文

发表的论文题目是“A Sybil detection method in OSN based on DistilBERT and Double-SN-LSTM for text analysis”，发表会议是 SecureComm 2020。论文参考标准在线社交网络 bot 账号数据集构建方式，基于 Kaggle 平台多个公开数据集构建了一个时效性更强的 twitter 平台 Sybil 账号数据集，使用 DistilBERT 处理 tweet 的文本特征、Double-SN-LSTM 处理 tweet 发表的时序特征，来实现账号分类，解决在线社交网络中女巫账号检测问题，最终模型在准确率、召回率等指标上均有很好的表现。

4） 参与强网杯网络安全挑战赛

参与实现“XSS 智能检测和可解释平台”，期间负责深度学习模型训练和 web 系统前后端的开发工作。集成了 LSTM 深度学习模型、LIME 机器学习可解释性、可视化平台搭建等技术，实现

了一个检测结果准确率高并可解释、检测界面清晰的 XSS 攻击检测平台，有助于减少 XSS 攻击引发的危害，最终成果获得了第四届“强网杯”全国网络安全挑战赛作品赛三等奖。

5） 参与四川省科技厅项目

本人本科期间参与到指导老师杨进副教授的四川省科技厅创新创业科技人才项目“基于深度学习的加密恶意流量智能检测系统及关键技术研究”，项目提出了一种基于深度 Q 网络(DQN)和深度卷积生成对抗网络(DCGAN)的加密流量样本生成方法，从加密流量训练样本中学习新样本，解决原始训练样本不足、样本不平衡等问题；另外，基于 ResNet 构建加密流量学习分类模块，对加密的网络恶意流量进行自动特征提取以使模型具有自学习和自适应能力。

6） 中国平安 gamma 人工智能研究院实习

自 2021 年 11 月至 2022 年 8 月，一直在中国平安 gamma 人工智能研究院 NLP 组实习，担任助理算法工程师，从事 NLP 模型构建工作，协助撰写 3 篇发明专利，参与 CMRC 2022 阅读理解竞赛初赛阶段排名第一（决赛未结束）。实习过程中熟悉了深度学习模型构建、训练、调优的全过程，可以独立根据实际需求使用深度学习方法解决问题。

2. 工作条件

本人研究生阶段导师是邱卫东教授（副院长，中国中文信息学会大数据与隐私计算专委会副主任委员、入选教育部“新世纪优秀人才计划”、上海市优秀技术带头人，荣获中央网信办全国网络安全优秀教师）。所在实验室是密码分析与大数据安全实验室，实验室长期从事密码分析/密码工程、大数据安全分析和隐私保护，承担了包括国家重点研发计划、科技部 863 计划专项、科技部科技支撑计划、国家自然科学基金、国防预研等一系列国家级项目，研究成果荣获上海市科技进步一等奖。近年来在 IEEE Transaction on Industrial Electronics、Knowledge-Based Systems、JOC、FSE、Information Sciences、Computer&Security 等发表了 100 余篇学术论文。

推荐高校意见	（公章） 院长签字： 年　　月　　日
企业立项意见	（公章） 年　　月　　日
专家评议结果	签 字： 年　　月　　日