# 数据采集可行性分析

## 一、需求

通过加固业务尝试采集加固产品所安装设备的多方位信息。

初步分析为三个方向：

1. Android OS 信息
2. 加固APP信息
3. 其他APP信息

## 二、技术细节分析

### 2.1、Android OS 信息获取

获取一些基础的Android设备信息是不受任何限制的，当前已知的有：

1. 操作系统版本号
2. 当前系统发布状态（测试版本系统或者正式版系统，这一信息可作为判断设备是否已root的不充分条件）
3. 手机品牌
4. 手机型号
5. CPU个数和CPU指令集
6. 设备主机地址
7. ……

硬件调用（需要对应的权限）：

1. 网卡（WIFI/流量）
2. GPS
3. 陀螺仪(体传感器，可用于获取生物信息”心率”)
4. 摄像头
5. 麦克风
6. 红外线感应器
7. 听筒
8. SIM卡信息
9. 蓝牙
10. ……

系统级的用户信息（每一个动作都需要对应的权限），这一点和其他APP信息在理解上有交集，因为这些信息都是通过单独的应用进行管理的：

1. 电话信息（读、写、拨）
2. 短信信息（读、写、发）
3. 日历/日程信息（读、写）
4. 账户信息（邮箱）
5. 当前正在运行的APP列表
6. 当前正在与用户交互的APP
7. ……

### 2.2、 加固APP信息获取

1. 版本号
2. 崩溃信息
3. 启动（次数、频率、时间）
4. 渠道信息

### 2.3、 其他APP信息获取

获取其他app信息有两种情况

1. 在无ROOT权限的情况能获取的信息为：
   1. 目标APP暴露在SDCard的信息私有目录信息无法获取。
   2. 通信数据，需要网络监控
2. 在有ROOT权限的情况下获取的信息：目标APP所有的数据包括本地化数据和通信数据。

假设要获取的目标APP为testin.apk

在非Root 的情况下需要做两个步骤：

1. 首先针对目标testin.apk进行分析，看他对外暴露的信息有哪些（主要指存储在SDCard公共区域的信息，应用私有目录的信息不可操作）。
2. 在加固的过程中确保被加固app具有SDCard权限，从而可以获取目标程序信息。

在Root时访问Android系统上的任何信息都是不受任何限制的（其他APP的信息是Android系统所有信息的一个子集）。

#### 2.3.1、 ROOT

要ROOT一个Android设备通常：

1. 系统已经预留了接口（后门），利用这个系统预留接口完成ROOT。
2. 根据当前系统版本的特定漏洞开发ROOT程序完成ROOT。
3. 为硬件重新安装定制版系统（当前应用场景可行性差）

上述1/2两种思路的具体实现是（常见）：

1. 修改SU可执行文件源码并重新编译（SU源码位于AOSP）。
2. 将重新编译后的SU放入系统指定位置（/system/bin）。
3. 利用上述漏洞（接口）为SU设定恰当的权限。
4. 谁调用该SU谁即可获取ROOT权限（这里可限制为只有testin可调用）。

ROOT的难点在于

1. 操作系统开发商很多，漏洞或者接口不尽相同（也可能没有），需要逐个适配。
2. 旧版本系统的漏洞或接口新系统不一定适用，每次版本发布需要投入（无法预估的）生产力进行研究。

## 三、当前主流数据采集商（友盟）

友盟主要提供的主要统计功能如下：

|  |
| --- |
| APP启动次数[衍生出活跃用户] |
| 新增用户数 [默认基于设备(IMEI)，可以通过接口设置根据账号] |
| 版本分布 |
| 统计应用崩溃信息(如果开发者自行进行统计的话，需要开发者将崩溃信息自行上传到友盟服务器) |
| 经纬度(具体数据开发者自行获取，将获取到的数据交付给友盟API) |
| 渠道统计 |
| 终端属性 |
| [衍生数据]-留存分析 |
| [衍生数据]-用户参与度 |
| [无法统计]-功能使用 |

友盟所需要的权限：

|  |
| --- |
| <!-- 必须的权限 --> |
| <uses-permission android:name="android.permission.ACCESS\_NETWORK\_STATE" />  <uses-permission android:name="android.permission.ACCESS\_WIFI\_STATE" />  <uses-permission android:name="android.permission.READ\_PHONE\_STATE" />  <uses-permission android:name="android.permission.INTERNET" /> |
| <!-- 推荐的权限 -->  <!-- 添加如下权限，以便使用更多的第三方SDK和更精准的统计数据 --> |
| <uses-permission android:name="android.permission.ACCESS\_COARSE\_LOCATION" />  <uses-permission android:name="android.permission.ACCESS\_FINE\_LOCATION" />  <uses-permission android:name="android.permission.CHANGE\_WIFI\_STATE" />  <uses-permission android:name="android.permission.WRITE\_EXTERNAL\_STORAGE" /> |

上述功能列表中统计用户行为习惯（功能使用）一个点我们无法完成统计（需要开发者配合）其他均可实现。

## 四、例子

上文关于系统，硬件，其他app信息的获取在非ROOT情况下都是依赖一定的权限的，下文是部分权限列表：

|  |
| --- |
| android.permission.READ\_CALENDAR | 读取日程提醒 |
| android.permission.WRITE\_CALENDAR | 写入日程提醒 |
| android.permission.CAMERA | 拍照权限 |
| android.permission.READ\_CONTACTS | 读取联系人 |
| android.permission.WRITE\_CONTACTS | 写入联系人 |
| android.permission.GET\_ACCOUNTS | 访问账户Gmail列表 |
| android.permission.ACCESS\_FINE\_LOCATION | 获取精确位置 |
| android.permission.ACCESS\_COARSE\_LOCATION | 获取错略位置 |
| android.permission.RECORD\_AUDIO | 录音 |
| android.permission.READ\_PHONE\_STATE | 读取电话状态 |
| android.permission.CALL\_PHONE | 拨打电话 |
| android.permission.READ\_CALL\_LOG | 读取通话日志 |
| android.permission.USE\_SIP | 使用SIP视频 |
| android.permission.PROCESS\_OUTGOING\_CALLS | 处理拨出电话 |
| android.permission.SEND\_SMS | 发送短信 |
| android.permission.RECEIVE\_SMS | 接收短信 |
| android.permission.READ\_SMS | 读取短信内容 |
| android.permission.RECEIVE\_WAP\_PUSH | 接收Wap Push |
| android.permission.RECEIVE\_MMS | 接收彩信 |
| android.permission.READ\_EXTERNAL\_STORAGE | 读取外部存储 |
| android.permission.WRITE\_EXTERNAL\_STORAGE | 写入外部存储 |
| android.permission.WRITE\_CALL\_LOG | 写通话记录 |
| com.android.voicemail.permission.ADD\_VOICEMAIL | 添加语音邮箱 |
| android.permission.BODY\_SENSORS | 体传感器 |

上述每一条权限都有对应的数据或者硬件操作，这些操作AndroidSDK尽数提供了相关的API下面是几个权限对应API的不完全统计示例：

|  |  |
| --- | --- |
| 日程提醒权限 | android.permission.WRITE\_CALENDAR  android.permission.READ\_CALENDAR |
| API： | Landroid/content/ContentResolver;->query [对应READ权限]  Landroid/content/ContentResolver;->insert [对应WRITE权限]  Landroid/content/ContentResolver;->update [对应WRITE权限]  Landroid/content/ContentResolver;->delete [对应WRITE权限] |
| 拍照权限 | android.permission.CAMERA |
| API： | Landroid/hardware/Camera;->open()Landroid/hardware/Camera; Landroid/hardware/camera2;->openCamera() |
| 获取定位权限 | android.permission.ACCESS\_FINE\_LOCATION  android.permission.ACCESS\_COARSE\_LOCATION |
| API： | Landroid/location/LocationManager;->getLastKnownLocation(Ljava/lang/String;)Landroid/location/Location; |
| 录音权限 | android.permission.RECORD\_AUDIO |
|  | Landroid/media/AudioRecord;->startRecording(); |
| SIP视频权限 | android.permission.USE\_SIP |
| API： | Landroid/net/sip/SipManager;->newInstance(Landroid/content/Context;)Landroid/net/sip/SipManager; |
| 发送短信权限 | android.permission.SEND\_SMS |
| API： | Landroid/telephony/SmsManager;->sendTextMessage  Landroid/telephony/SmsManager;->sendDataMessage |

## 五、总结

综上，数据采集目标可行，但是受限于当前应用所具有的权限。