- 敏感路径:该路径是以触发敏感行为为目标的执行路径,该路径的生成需要对安卓应用的 APK 文件进行静态分析,构建函数调用关系图 CG 并扩充为组件间调用关系图 ICCG(inter-component communication graph),进而通过 Intent 过滤,最终识别出敏感路径.具体处理过程见第 3.1 节;
- 标签敏感触发(labeled sensitive activation,简称 LSeA):由于 ICCG 只包含应用内的组件间调用关系,并不包含应用与系统乃至与其他应用间的交互,因此引入标签敏感触发,用于标识安卓系统与应用内组件的交互关系.标签敏感触发完善了对应敏感行为的触发信息,在系统事件与敏感行为之间建立了联系,包含系统事件的敏感路径能够更直观地反应敏感行为在何种情况下被触发.

3 安全性分析

我们设计的基于敏感路径识别的安卓恶意应用安全性分析方法可分为静态分析过程和机器学习过程两部分.其中,静态分析过程即对应用进行敏感路径分析的过程;机器学习过程则是对敏感路径信息进行处理抽象以及使用机器学习算法进行安全性判断的过程.

3.1 敏感路径分析

安卓系统使用了 Intent 机制来进行组件间、应用间、系统与应用间的通讯,因此需要分析应用所使用的 Intent,得出组件间调用关系 ICC,并需要将 CG 扩充为 ICCG,才能完整表达应用的函数调用关系.

安卓系统提供了 Intent 机制来协助组件的通信,它是一种运行时绑定(run-time binding)的机制.使用 Intent 机制完成组件间的通讯过程如下:组件 *A* 向安卓系统发送了 Intent 参数 *i*,安卓系统会根据 *i* 的属性内容选择合适的、能处理 *i* 的组件 *B*,*C*,…来完成 *A* 的请求.例如,某个 *Activity* 组件需要拨打电话,该活动组件会向系统发送 ACTION_VIEW,安卓系统会根据该 Intent 的需求找到拨号应用的对应组件来完成拨打电话的操作.

Intent 包含 ACTION,DATA,CATEGORY,COMPONENT 等几种属性,具体用途和释义如下.

(1) ACTION,表示 Intent 需要完成的动作.安卓系统提供了一些标准的 ACTION 常量,如 ACTION_VIEW 动作表示显示数据,会根据数据的具体类型,调用相应的组件进行后续操作;
(2) DATA,表示执行动作的数据对象,由一个 URI 变量表示;
(3) CATEGORY,表示能处理该 Intent 的组件所属的种类,一个组件可处于多个 CATEGORY 下,例如,CATEGORY_HOME 表示能够回到 HOME 界面的 *Activity* 组件;
(4) COMPONENT,表示该 Intent 的目标组件.有两种方式来寻找 Intent 参数的目标组件:一种是显式方式,Intent 参数的 COMPONENT 属性不为空,可以直接与目标组件建立联系;一种为隐式方式,Intent 参数的 COMPONENT 属性为空.

一个应用的所有组件能够处理的 Intent 参数的属性均注册在应用的 Manifest 文件中,系统需要在其中寻找与 Intent 参数的 ACTION,CATEGORY,DATA 属性相匹配的目标组件.各组件注册在 Manifest 文件中能够处理的 Intent 参数的列表被称为 Intent 过滤,包含了各组件的 ACTION,DATA,CATEGORY,COMPONENT 信息.

在此基础上,生成 ICC 的方法流程图如图 3 所示.

首先,需要分析函数中所定义的 Intent 参数,查看该 Intent 参数的 Component 属性是否为空.

- 如果不为空,Component 的属性值即是目标组件名,则在该函数与目标组件间建立调用关系;
- 如果为空,则进行 Action 属性的适配,分析在 Intent 过滤中组件注册的 Intent 参数的 Action 属性值.
  - ➢ 若完全适配,则建立调用关系;
  - ➢ 如果不适配,则筛选出 Intent 过滤中所有 Action 属性为空的组件,进行 Category 属性的适配:
    - ✧ 若完全适配,则建立调用关系;
    - ✧ 如果不适配,则在上一轮选出的组件中过滤出所有 Category 属性为空的组件,进行 Data.scheme 属性的适配:若完全适配则建立调用关系;如果还是不存在完全适配的目标组件,则该 Intent 参数无法被传向任何组件.

在得到应用的 ICC 调用关系后,可以将函数调用关系图 CG 扩充成组件间调用关系图 ICCG.过程如下:由

FlowDroid工具生成的CG包含一个虚拟的*main*函数节点*DummyMainMethod*(),由于该函数会影响之后的分析,将其删除;将ICC中包含的组件间调用关系作为有向边,添加至删除虚拟节点的CG中即可.

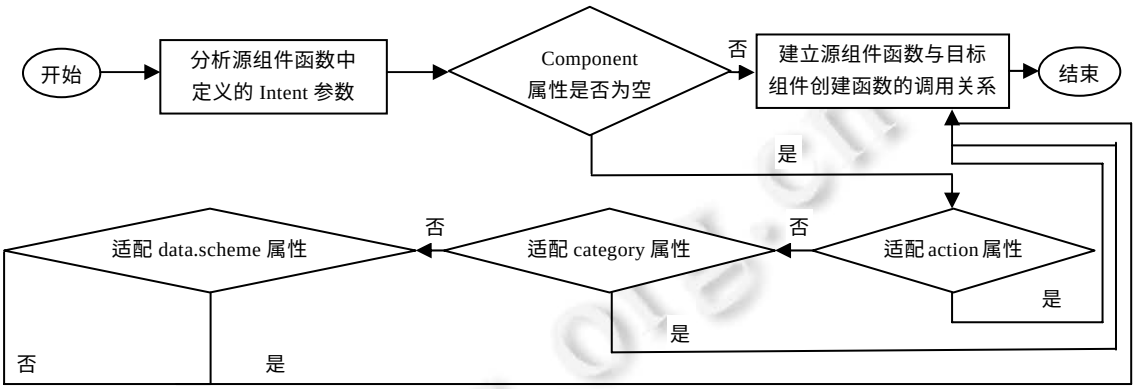


Fig.3 Process graph of generating ICC

图 3 ICC 生成流程图

得到ICCG后,进行敏感路径识别的过程见算法1.具体解释如下.

- 第1行、第2行,根据敏感行为的定义,在ICCG的节点中寻找代表敏感行为的函数节点.本文中,敏感行为是需要允许请求的API函数和与动态加载相关的函数;
- 第3行、第4行,针对每个敏感行为遍历ICCG,找到每条包含该敏感行为的执行路径.由于代表敏感行为的节点不会再调用其他函数,所以这些执行路径中不会再包含其他敏感行为;
- 第5行~第11行,分析每条包含敏感行为的执行路径,如果其包含与用户交互相关的函数,找到执行路径距离敏感行为节点最近的代表用户交互函数的节点,将该节点与敏感行为节点组成的敏感路径加入敏感路径的集合;
- 第12行、第13行,如果当前分析的执行路径中不包含与用户交互相关的函数,则将该条路径的进入点与敏感行为节点组成的敏感路径计入敏感路径的集合;
- 第14行~第18行,得到该应用包含的所有路径后,针对该应用的每个敏感触发,在Intent过滤中寻找敏感触发所属组件能够处理Intent参数的ACTION属性,将ACTION属性与敏感触发组成的标签敏感触发加入集合;
- 第19行、第20行,输出该应用所包含的敏感路径集合以及标签敏感触发集合.

算法 **1**. 敏感路径识别算法.

Inputs: ICCG: Inter Component Call Graph;

IF: A set of intent filters;

OutPuts: SeP: A set of sensitive paths;

LSeA: A set of labeled sensitive activations.

```
1  SeP←∅
2  SeB←getSensitiveBehavior(ICCG)
3  for each b in SeB
4     P←findExcutivePath(b,ICCG)
5     for each path∈P
6        a←findCaller(b)
7        while isNotEntryPoint(a)
8           a←findCaller(a)
```

```
9            if isUserIntractionFunction(a) then
10               SeP.add(a,b)
11               break
12           if isEntryPoint(a) then
13               SeP.add(a,b)
14 LSeA←∅
15 SeA←getSensitiveActivation(SeP)
16 for each a∈SeA
17     l←getAction(a,IF)
18     LSEA.add(l,a)
19 return LSeA
20 return SeP
```

3.2 特征抽象

一个安卓应用中包含了数量巨大的敏感行为和敏感触发,若将每一个敏感行为和敏感触发均视做特征,则特征种类数量过多,会造成特征矩阵过于稀疏,分析时间过长,影响准确率.因此,我们需要对敏感触发和敏感行为进行特征抽象,即:约减特征数量,使得特征的读写更加便捷.

敏感触发事件可分为硬件触发、用户触发以及系统触发这 3 大类.

- 硬件触发是指由手机或便携设备的硬件所产生的事件,诸如手机的锁屏键、音量键、内置的陀螺仪等硬件设备;
- 用户触发是指需要用户与触摸屏交互才会发生的事件,如单击、双击、长按等操作;
- 系统触发则是指系统自发产生的事件,包括两大类:一类是组件生命周期中各个阶段的常规事件;还有一类是 BroadCast Receiver 组件所监听的系统事件.

表 1 列出了本文处理的部分敏感触发函数,并对这些敏感触发函数进行了抽象表达.

Table 1 Abstraction of sensitive activation

表 1 敏感触发的抽象

所属种类	原始表达	抽象表达	详细
硬件触发	*boolean onKey*( )	KEY	按键事件
	boolean onKeyLongPress( )		
	boolean dispatchKeyShortcutEvent( )		
	boolean dispatchTrackballEvent( )	OTHERHARDWARE	轨迹球事件
	…		
用户触发	*void onClick*( )	CLICK	用户单击
	void onClickCancel( )		
	void StartbuttonClicked( )		
	boolean onLongClick( )	LONGCLICK	用户长按
	boolean onDoubleTap( )	DOUBLECLICK	用户双击
	boolean onDoubleTapEvent( )		
	void btZoomInClick( )	ZOOMIN	用户缩小
	void btZoomOutClick( )	ZOOMOUT	用户放大
	…		
系统触发	*void onCreate*( )	CREATE	组件创建
	void onPause( )	PAUSE	组件暂停
	void onStop( )	STOP	组件停止
	void onDestroy( )	DESTROY	组件销毁
	void onRestart( )	RESTART	组件重启
	void onResume( )	RESUME	组件复位
	void onReceive( )	详见表 2	
	…		

(1) 硬件触发.其中比较常见的是按键事件,在用户实际使用的过程中,诸如锁屏键之类的按钮使用频率相当高,很有可能被选为恶意功能的触发事件.还有诸如轨迹球等一类硬件设施,由于目前的手机使用到这些功能,将其作为 OTHERHARDWARE 抽象表达;

(2) 用户触发.同样发送信息的敏感行为,一个是不通知用户、直接通过后台监听系统事件触发,另一个是告知用户并由用户点击发送按钮来发送.显而易见,前者是恶意行为,后者是良性行为.是否由用户触发,是将良性行为与恶意行为区分开的主要判断依据.因为现实中存在用 UI 文字迷惑用户、诱骗用户进行操作但实际上却是激活恶意功能的情况,所以需要进一步将用户不同的操作手势区分开来;

(3) 系统触发.组件生命周期的各阶段可能会触发各种敏感行为,考虑到恶意应用的家族性(恶意应用被划分为多个种类,每个种类内的恶意应用从恶意功能的激活到恶意功能的执行都是类似的),将每个阶段的函数分别抽象.另外,根据标签敏感触发中的标签,针对基于监听系统事件的触发事件进行抽象,具体见表 2.

Table 2 System activation and abstraction based on monitoring system events

表 **2** 基于监听系统事件的系统触发及抽象

所属类别	抽象描述	原始描述	所属类别	抽象描述	原始描述
系统启动	BOOT	BOOT_COMPLETED	短信	SMS	SMS_RECEIVED
电话	CALL	PHONE_STATE NEW_OUTGOING_CALL ...	网络链接	NET	CONNECTIVITY_CHANGE DATA_STATE PICK_WIFI_WORK ...
电池电源	POWER	BATTERY_LOW BATTERT_OKAY ...	其他事件	OTHER	SIG_STR SIM_FULL USER_PRESENT ...

本文所提到的敏感行为可分为两大类:一类是动态加载相关的函数,一类为需要 Permission 权限才可以使用 API 函数.在本文中,前者被描述为 DynamicLoad,后者根据其所需的 Permission 对应至 Permission 描述.

表 3 列出本文对 Permission 的种类划分,大类里再按照功能以及敏感程度给予了进一步的划分.

(1) ReadInfo.与读取信息相关的 API 函数,根据其读取信息的不同,还可以细分为以下 3 种:AccountInfo,读取账户信息的行为,包括手机账户、Gmail 账户等信息;SystemInfo,读取系统信息的行为,不仅包括系统本身的配置信息,还包含系统内正在运行的进程列表等信息,例如 GET_TASK 所对应的函数;UserInfo,读取用户信息的行为,包括浏览器书签、历史记录等,也包含信息文本这种敏感程度较高的信息;

(2) Call.与拨打电话相关的 API 函数,CALL_PHONE,PROCESS_OUTGOING_CALLS 下所对应的敏感行为被划分至此类.如今已鲜有恶意应用执行拨打电话的恶意行为,但由于其敏感级别较高,特将其单列为一类;

(3) UseHardware.使用硬件设备(不包含触摸屏)的 API 函数,使用硬件设备很容易被用户察觉,但也是可能的安全隐患.根据设备所执行功能的不同,可以分为 4 类:BlueTooth,蓝牙设备;Camera,摄像头;NFC,较少手机配备的硬件设备,但是考虑到 NFC 可以读取交通卡等,将其单独列出;OtherHardware 包括震动马达、闪光灯等,考虑其对电池的损耗,将其列为一类;

(4) AccessLocation.能够获取手机所在位置的 API 函数,手机的位置也代表了用户的位置,用户在实际使用应用时,也相当关注自己的位置信息是否暴露;

(5) ChangeNetConfiguration.能够改变手机网络配置的 API 函数,其中既包括与 wifi 配置相关的函数,也包括与手机所使用的蜂窝网络相关的函数.连接网络是恶意应用执行多种恶意功能的必要条件,大部分恶意应用在执行恶意功能时,会使用到与网络相关的函数;

(6) SendMessage.与发送短信相关的 API 函数,私自发送短信也是常见的恶意功能之一,在进行安全性检测时,该类行为是需要着重监测的敏感行为;

(7) SystemOperation.对系统进行操作的函数,可分为 5 类:Data,更改数据的行为,如清除应用的缓存数据

CLEAR_APP_CACHE;DeviceConfiguration,更改设备配置的行为;ProcessOperation,操作进程的敏感行为;UserConfiguration,更改用户个性化配置的行为;OtherSystemConfiguration,无法划分至其他类的函数;

(8) WriteUserInfo.修改用户信息的函数.

Table 3 Abstraction of sensitive behaviors

表 3 敏感行为的抽象

Permission 权限/抽象描述 (敏感级别:低)	功能/抽象描述 (敏感级别:中)	类别/抽象描述 (敏感级别:高)
GET_ACCOUNTS, ...	AccountInfo	ReadInfo
GET_TASKS, READ_PHONE_STATE, ...	SystemInfo	
READ_HISTORY_BOOKMARKS, READ_SMS, ...	UserInfo	
CALL_PHONE, PROCESS_OUTGOING_CALLS	Call	
BLUETOOTH, BLUETOOTH_ADMIN	BlueTooth	UseHardware
CAMERA, RECORD_AUDIO, ...	Camera	
NFC	NFC	
VIBRATE, ...	OtherHardware	
ACCESS_COARSE_LOCATION, ACCESS_FINE_LOCATION, ...	AccessLocation	
CHANGE_NETWORK_STATE, CHANGE_WIFI_STATE, ...	ChangeNetConfiguration	
SEND_SMS, ...	SendMessage	
CLEAR_APP_CACHE, ...	Data	SystemOperation
CHANGE_CONFIGURATION, ...	DeviceConfiguration	
RESTART_PACKAGES, BROADCAST_STICKY, KILL_BACKGROUND_PROCESSES, ...	ProcessOperation	
SET_TIME_ZONE, ...	UserConfiguration	
SERIAL_PORT, ...	OtherSystemOperation	
WRITE_CALENDAR, ...	WriteUserInfo	
DynamicLoad		

3.3 使用决策树进行安全性分析

经过上述静态分析和特征抽象过程,我们得到了应用所包含的敏感路径信息.为了体现应用特征选取的全面性,我们引入应用 Manifest 文件中所申请的 Permission 请求作为特征的补充.首先,我们构建应用特征矩阵.

应用特征的矩阵构成如图 4 所示.

- *PID* 为应用的唯一标识符,用于区别其他应用;
- *M* 为代表应用是否为恶意应用的标签,“是”标为 1,“否”标为 0,安全性分析所要做的就是根据特征来计算该标签值;
- RF_i 为敏感路径特征,应用包含 RF_i,“包含”标为 1,“不包含”标为 0;
- 允许请求特征 PF_j 类似于 RF_i.

在此基础上,我们采用 Weka 工具中的决策树算法 C4.5 来完成对应用安全性的分析,即:给定一个数据集,其中每个元组都能用一组属性值来描述(对应图 4 中的一条特征向量),每一个元组属于一个互斥的类别中的某一类,通过有监督的学习,找到一个从属性值到类别的映射关系(为 0 或为 1),并且这个映射能用于对新的类别未知的实体进行分类(判断一个应用为恶意或良性).实际操作流程包括:

- 输入应用特征矩阵 *M*:如果 *M* 不可被划分(*M* 内各个应用的特征取值无区别)或达到算法停止的条件(如决策树达到一定深度),即完成了决策树的构造;
- 如果 *M* 可被划分,计算 *M* 内每个特征 *F* 的信息增益率,选取信息增益率最大的特征 *f*;根据特征 *f* 的取

值不同,将 M 划分为不同的子矩阵;针对每个子矩阵,重复以上流程.

	应用 ID	是否恶意	敏感路径特征				允许请求特征			
	PID	*M*	RF_1	RF_2	…	RF_k	PF_{k+1}	PF_{k+2}	…	PF_n
	001	0	0	0	…	0	0	0	…	0
	002	0	0	0	…	1	0	0	…	0
	003	0	0	0	…	0	0	0	…	0
	004	0	1	0	…	0	0	0	…	0
	005	0	0	0	…	0	0	0	…	0
	006	0	0	0	…	0	0	0	…	0
	007	1	0	1	…	1	0	0	…	1
	008	0	0	0	…	0	0	0	…	0
	009	0	0	0	…	0	0	0	…	0
	010	0	0	0	…	0	0	0	…	0
	…	…	…	…	…	…	…	…	…	…
一条应用数据 ←	*m*	0	0	0	…	0	0	1	…	0
	…	…	…	…	…	…	…	…	…	…
	p−1	0	0	0	…	0	1	1	…	0
	p	0	0	0	…	0	0	0	…	0

Fig.4 Constitutions of Android Apps feature matrix

图 4 应用特征矩阵的构成

4 实验分析

4.1 实验环境

本文进行的所有实验均是使用处理器为 Intel Core i5-3470 3.20GHz、内存为 8G、操作系统为 Windows 7 专业版的计算机所完成.实验由 Java 语言所实现,使用的开发环境为 JDK7.0,使用的 IDE 为 Eclipse Kepler.静态分析部分的功能使用了基于污点分析的工具 FlowDroid 所得的部分结果,同时借助了安卓开发工具 APKTOOL 获取 APK 文件内的 Manifest 文件,机器学习部分使用了工具 Weka 中的 C4.5 决策树算法.

4.2 评价指标

本文的最终目的是判定一个安卓应用是否为恶意应用.M 为分析时输入的应用特征矩阵,应用的实际情况与本实验的判定结果会产生 4 种情况,如下所示.

(1) True Positive,良性应用被判定为良性应用,该类应用被记为 $TP(M)$;

(2) True Negative,恶意应用被判定为恶意应用,该类应用被记为 $TN(M)$;

(3) False Positive,恶意应用被判定为良性应用,该类应用被记为 $FP(M)$;

(4) False Negative,良性应用被判定为恶意应用,该类应用被记为 $FN(M)$.

根据以上 4 种判定结果,分别针对良性应用和恶意应用使用精度、召回率、F 度量来对实验效果进行评价,同时考察整体分析的准确率.

4.3 数据集

本文实验所使用的数据集共包含 493 个现实世界中存在的安卓应用,其中包含良性应用 342 个,绝大部分下载自 Google Play 应用商店,小部分来自于国内的第三方市场“豌豆荚”;恶意应用 151 个,来自于数据集 Drebin, Contagio,VirusShare 中的恶意应用.

因为时间、设备以及所使用工具 FlowDroid 的限制(使用 FlowDroid 分析过大的 APK 文件,会造成分析时长无法估计、内存溢出等问题),我们从 Google Play 上下载了约 400 个大小在 8MB 以下的 APK 文件用于分析.在后续的分析中,剔除了分析时间过长的 APK 文件,共留下 303 个 APK 文件.同时,我们选取了同样来自于 Google Play、大小在 8MB 与 15MB 之间的 14 个 APK 文件以及来自于“豌豆荚”的、大小在 10MB 以下的 25 个 APK 文件作为补充,以保证数据集大小以及来源的多样性.

恶意应用主要收集自数据集 Drebin、网站 Contagio Mini Dump 和网站 VirusShare.其中,Drebin 是由德国哥廷根大学的 Daniel Arp 等人所提供的数据集,共包含 5 560 个来自于 179 个不同恶意应用家族的恶意应用,这些应用是在 2010 年 8 月~2012 年 10 月之间由 the MobileSandbox 工程所收集.我们从中随机选择了 100 个恶意应用,其中 3 个应用由于文件太小无法生成函数调用关系图等信息被剔除.因为 Drebin 中包含的恶意应用产生时间较早且隐去了应用名、描述等信息,我们又从 Contagio Mini Dump 与 VirusShare 网站中选取了共 54 个恶意应用作为补充.

4.4 实验结果及分析

我们提出 3 个研究问题并通过实验寻求这些问题的答案.

- RQ1:使用本文所提出的方法进行安全性分析的准确率如何?相对于其他方法,准确度是不是更高?
- RQ2:我们提出了敏感级别的概念,不同敏感级别下的安全性分析准确率如何?
- RQ3:数据集中 APK 文件的大小会对实验结果造成影响吗?

表 4 选取了数据集中的 15 种应用(其中良性应用 10 种,恶意应用 5 种),记录了它们所包含的信息.表头内容分别为应用的名称、该应用是否为恶意应用、APK 文件的来源、APK 文件的大小、分析所花时间、包含的敏感行为数量(因为表格大小限制,只列出原始表达与低敏感级别表达的数量)、包含的敏感触发数量(只列出原始表达)和包含的敏感路径数量.其中,RR 代表敏感触发和敏感行为均为原始描述,RL 代表敏感触发为原始描述、敏感行为为低敏感级别描述,AL 代表敏感触发为抽象描述、敏感行为为低敏感级别描述.因为 Drebin 中的恶意应用均已抹去应用本身的名称信息,所以所有恶意应用均选择了从 Contagio 网站获取到的恶意应用.

Table 4 Statistics of Android Apps in our data set

表 **4** 数据集中部分应用所包含的信息

Name	Is Mal	DL	Size (KB)	Time (s)	SeB		SeA	Sensitive path		
					Raw	SeLL		RR	RL	AL
power battery	Yes	Contagio	548	40	19	3	3	24	7	2
GlamorousSmoke	Yes	Contagio	1 014	86	23	17	17	264	174	23
3dtimeclockticks	Yes	Contagio	1 294	7	9	3	3	22	5	4
fdhgkihrtjkibx	Yes	Contagio	2 456	1	5	1	1	5	1	1
assassins creed	Yes	Contagio	3 332	6	5	3	10	10	6	4
科学计算器	No	Wandoujia	589	13	0	0	0	0	0	0
Apps2SD Move	No	Google	823	27	15	6	9	61	28	26
Word2PDF	No	Google	2 929	359	19	7	18	97	92	78
Manga Browser	No	Google	3 470	1 522	53	32	77	3 572	1 305	121
Auto Comment	No	Google	3 827	1 362	34	24	89	2 660	872	241
Saida Loans	No	Google	4 289	2 283	45	33	104	2 919	859	316
SuperBeam	No	Google	5 212	1 626	44	17	85	2 899	1 108	273
Google Voice	No	Google	5 965	722	26	13	141	1 008	470	434
OpenVPN	No	Google	7 857	77	5	3	15	52	31	17
Speedtest	No	Wandoujia	15 609	912	65	39	91	2 841	1 716	218

(1) RQ1

基于敏感路径识别的安全性检测方法所得检测结果见表 5.

本表中所列出的实验中使用的敏感路径描述的构成为 Raw(SeA)与 Raw(SeB),同时我们列出了仅使用 PSCout 所提供的敏感 API[30]作为特征(即,在使用时需要对 Permission 权限进行检查的 API 函数)进行数据挖掘的检测结果.

由表 5 可知:本文所提供的安卓应用安全性检测方法的准确率为 97.97%,高于基于 API-Feature 的检测方法(90.47%);此外,本文方法在恶意应用和良性应用检测的精度、召回率、F 度量等方面均优于 API-Feature 方法.这表明考察敏感行为的触发行为(即敏感触发)能够帮助分辨敏感行为是否可能存在恶意,能够用于判断包含此类敏感行为的安卓应用是否是恶意应用.因此,我们的结论是:本文所提出的基于敏感路径识别的恶意应用检测方法相对于 API-Feature 方法具有较好的检测效果.

Table 5 Comparison of our method and API-Feature method

表 5 本文方法与 API-Feature 的比较

	API-Feature	Raw(SeA)&Raw(SeB)
TP	316	335
TN	130	148
FP	21	3
FN	26	7
Accuracy (%)	90.47	97.97
B_Precision (%)	93.77	99.11
B_Recall (%)	92.40	97.95
B_F-measure (%)	93.08	98.52
M_Precision (%)	83.33	95.48
M_Recall (%)	86.09	98.01
M_F-measure (%)	84.69	91.03

(2) RQ2

在本节中,我们进行了不同敏感级别描述下的敏感路径作为特征的实验,实验结果见表 6.

Table 6 Experiment results of considering sensitive paths as features under different sensitive levels

表 6 不同敏感级别描述下的敏感路径作为特征的实验结果

	RR	RL	RM	AR
TP	335	330	297	332
TN	148	137	121	148
FP	3	14	30	3
FN	7	12	45	10
Accuracy (%)	97.97	94.72	84.78	97.36
B_Precision (%)	99.11	95.93	90.83	99.10
B_Recall (%)	97.95	96.49	86.84	97.08
B_F-measure (%)	98.52	96.21	88.79	98.08
M_Precision (%)	95.48	91.95	72.89	93.67
M_Recall (%)	98.01	90.73	80.13	98.01
M_F-measure (%)	96.73	91.33	76.34	95.79

敏感触发固定使用原始描述,我们分别使用原始描述 RR、低敏感级别描述 RL、中敏感级别描述 RM 的敏感行为作为特征进行实验.可以看到:原始描述和低敏感级别描述的结果相差不大,但是由于在抽象过程省略了一些信息,导致低敏感级别描述的准确率(94.72%)略低于原始描述的准确率(97.97%);而使用中敏感级别描述的准确率(84.78%)远低于前两者,但仍在可以接受的范围.

敏感行为固定使用原始描述,分别使用原始描述 RR、抽象描述的敏感触发 AR 作为特征.由于敏感触发的数量较少,抽象过程造成的信息损失也较少,相对于原始描述,抽象描述的实验结果 AR 多了 3 个 *FN* 的结果.

因此,通过对比不同敏感级别描述的特征进行安全性分析,实验结果表明:特征描述的抽象虽然赋予了敏感路径易读性,但是带来了部分信息的缺失.例如,同样在实际使用时需要申请 Permission 权限 SEND_SMS 的 API 可以是 *sendDataMessage*(),*sendMultipartTextMessage*()和 *sendTextMessage*().观察数据集中良性应用和恶意应用使用这 3 种 API 的状况可以发现:恶意应用使用的均是 *sendTextMessage*(),而良性应用后两者皆有,而 *sendDataMessage*()则没有被使用.若未进行特征抽象,则部分良性应用可在由这些敏感行为构成的敏感路径特征下与恶意应用形成差别;若统一抽象为 SEND_SMS,则这些差别就消失了,无法区分出良性应用和恶意应用,造成误报或漏报.

(3) RQ3

实验中我们发现,数据集中应用的平均大小会影响实验的结果.将数据集中的应用按照 APK 文件的大小分为两个子数据集:一个子数据集中包含大小为 0~4MB 的应用,共 374 个应用;另外一个子数据集中包含大小为 4MB~15MB 的应用,共 119 个应用.分别对这两个子数据集进行实验,所使用的敏感路径描述均为原始描述,实验结果见表 7.

Table 7 Experiment results with sub-data set

表 7 在子数据集上进行实验的结果

	0~4MB	4~15MB	0~15MB
TP	239	96	335
TN	133	15	148
FP	0	3	3
FN	2	5	7
Accuracy (%)	99.46	93.28	97.97
B_Precision (%)	100.00	96.97	99.11
B_Recall (%)	99.17	95.05	97.95
B_F-measure (%)	99.58	96.00	98.52
M_Precision (%)	98.52	75.00	95.48
M_Recall (%)	100.00	83.33	98.01
M_F-measure (%)	99.25	78.95	96.73

我们发现:在 0~4MB 的子数据集上,本文方法取得了更好的效果;而对于 4MB~15MB 的子数据集,其准确率略低于在 0~4MB 的子数据集和整个数据集上进行实验的效果.由于 4MB~15MB 的子数据集中的应用数量较少,不足以全面地展现本文方法的效果,但是仍然可以看出数据集中应用的大小对实验结果有着一定的影响.

另外,实验中对数据集内的每个 APK 文件进行敏感路径分析平均用时 170s.针对不同大小的 APK 文件,其分析用时如下:0~4MB 大小的 APK 分析,平均分析用时 89s;4MB~8MB 大小的 APK 分析,平均用时 918s;8MB~15MB 大小的 APK 分析,平均用时 2 579s.考虑到数据集内大部分 APK 文件大小要小于现实中的 APK 文件,在实际应用中,需要进一步降低我们方法的分析时间.

5 总 结

本文提出了一种结合了静态分析与机器学习的基于敏感路径识别的安卓应用安全性分析方法.使用静态分析的方法获取应用的组件间函数调用关系图,并由此获取敏感路径信息,再将这些信息特征进行不同敏感级别的抽象化,并根据这些信息赋予应用特征,使用决策树完成安卓应用安全性的分析.通过多角度的分析和对比,本文所提出的方法在数据集上的表现优于其他方法,尤其是在使用较高敏感级别描述下敏感路径作为特征的实验中具备较高的准确率.本实验数据集中的应用大小主要集中在 8MB 以内,而现实世界中常用的应用大部分都在 10MB 甚至 20MB 以上.由于受限于所使用的 FlowDroid 工具,在本文的实验环境中,一旦需要分析较大 APK 文件时,会出卡死、内存溢出等问题.后期我们会逐步改善实验条件和工具,引入规模更大的安卓应用.

本文主要工作是对安卓应用进行了安全性分析.如今,越来越多新兴的恶意应用使用了动态加载等技术来规避检测工具的排查.通过添加对这些新恶意应用的关注,静态分析方法能从一定程度上解决问题,但是不能完全根除,因为静态方法无法获得动态运行时信息.因此,需要考虑使用动态分析方法.但由于安卓系统的事件触发机制(单个安卓应用可能会有上千个事件及其回调函数)和框架模型的复杂性,动态方法实施起来的难度非常大;另外,动态方法一次运行只能覆盖部分事件,存在覆盖率较低的问题.与此同时,现有安卓应用的规模越来越大,如何结合静态、动态分析方法有效地改进安全性分析的效率、提高检测的准确率,是未来工作的主要内容.

References:

[1] Qing SH. Research progress on Android security. Ruan Jian Xue Bao/Journal of Software, 2016,27(1):45−71 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4914.htm [doi: 10.13328/j.cnki.jos.004914]

[2] Felt AP, Chin E, Hanna S, Song D, Wagner D. Android permissions demystified. In: Proc. of the ACM Conf. on Computer and Communications Security (CCS 2011). 2011. 627−638. [doi: 10.1145/2046707.2046779]

[3] Yang W, Xiao XS, Andow B, Li S, Xie T, Enck W. AppContext: Differentiating malicious and benign mobile App behaviors using context. In: Proc. of the 37th Int'l Conf. on Software Engineering (ICSE 2015). 2015. 303−313. [doi: 10.1109/ICSE.2015.50]

[4] Li L, Bartel A, Bissyand´e TF, Klein J, Traon YL, Arzt S, Rasthofer S, Bodden E, Octeau D, McDaniel P. IccTA: Detecting inter-component privacy leaks in Android Apps. In: Proc. of the 37th Int'l Conf. on Software Engineering (ICSE 2015). 2015. 280−291. [doi: 10.1109/ICSE.2015.48]

[5] Li GZ, Han Z, Zhou QH, Wang YZ. A detecting system for Android malicious behavior based on binder information flow. NetInfo Security, 2016,(2):54−59 (in Chinese with English abstract). [doi: 10.3969/j.issn.1671-1122.2016.02.009]

[6] Avdiienko V, Kuznetsov K, Gorla A, Zelle A, Arzt S, Rasthofer S, Bodden E. Mining apps for abnormal usage of sensitive data. In: Proc. of the 37th Int'l Conf. on Software Engineering (ICSE 2015). 2015. 426−436. [doi: 10.1109/ICSE.2015.61]

[7] Seo SH, Gupta A, Sallam AM, Bertino E, Yim K. Detecting mobile malware threats to homeland security through static analysis. Journal of Network and Computer Applications, 2014,38:43−53. [doi: 10.1016/j.jnca.2013.05.008]

[8] Huang JJ, Zhang XY, Tan L, Wang P, Liang B. AsDroid: Detecting stealthy behaviors in Android applications by user interface and program behavior contradiction. In: Proc. of the 36th Int'l Conf. on Software Engineering (ICSE 2014). 2014. 1036−1046. [doi: 10.1145/2568225.2568301]

[9] Elish K, Yao DD, Ryder BG. User-Centric dependence analysis for identifying malicious mobile Apps. In: Proc. of the IEEE Mobile Security Technologies (MoST 2012). 2012.

[10] Yang Y, Su PR, Ying LY, Feng DG. Dependency-Based malware similarity comparison method. Ruan Jian Xue Bao/Journal of Software, 2011,22(10):2438−2453 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3888.htm [doi: 10.3724/SP.J.1001.2011.03888]

[11] Enck W, Octeau D, McDaniel P, Chaudhuri S. A study of Android application security. In: Proc. of the USENIX Security Symp. (SEC 2011). 2011. 21−37.

[12] Grace M, Zhou YJ, Zhang Q, Zou SH, Jiang XX. Riskranker: Scalable and accurate zero-day Android malware detection. In: Proc. of the Int'l Conf. on Mobile Systems, Applications, and Services (MOBISYS). 2012. 281−294. [doi: 10.1145/2307636.2307663]

[13] Burguera I, Zurutuza U, Nadjm-Tehrani S, Crowdroid: Behavior-Based malware detection system for Android. In: Proc. of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices. 2011. 15−26. [doi: 10.1145/2046614.2046619]

[14] Blsing T, Batyuk L, Schmidt AD, Camtepe S, Albayrak S. An Android application sandbox system for suspicious software detection. In: Proc. of the 5th Int'l Conf. on Malicious and Unwanted Software (MALWARE). 2010. 55−62. [doi: 10.1109/MALWARE.2010.5665792]

[15] Zhou Y, Wang Z, Zhou W, Jiang X. Hey, you, get off of my market: Detecting malicious apps in official and alternative Android markets. In: Proc. of the 19th Annual Symp. on Network and Distributed System Security (NDSS 2012). 2012.

[16] Spreitzenbarth M, Schreck T, Echtler F, Arp D, Hoffmann J. Mobile-Sandbox: Combining static and dynamic analysis with machine-learning techniques. Int'l Journal of Information Security, 2014, 1−13. [doi: 10.1007/s10207-014-0250-0]

[17] Luo Y, Zhang QX, Shen QN, Liu HZ, Wu ZH. Android multi-level system permission management approach. Ruan Jian Xue Bao/Journal of Software, 2015,26(Suppl.(2)):263−271 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/15037.htm

[18] Britton W, Elish KO, Yao DF. Comprehensive behavior profiling for proactive Android malware detection. In: Proc. of the Information Security. 2014. 328−344. [doi: 10.1007/978-3-319-13257-0_19]

[19] Wu DJ, Mao CH, Wei TE, Lee HM, Wu KP. Droidmat: Android malware detection through manifest and API calls tracing. In: Proc. of the Asia Joint Conf. on Information Security (Asia JCIS). 2012. 62−69. [doi: 10.1109/AsiaJCIS.2012.18]

[20] Gascon H, Yamaguchi F, Arp D, Rieck K. Structural detection of Android malware using embedded call graphs. In: Proc. of the ACM Workshop on Artificial Intelligence and Security (AISEC). 2013. 45−54. [doi: 10.1145/2517312.2517315]

[21] Chakradeo S, Reaves B, Traynor P, Enck W. Mast: Triage for market-scale mobile malware analysis. In: Proc. of the ACM Conf. on Security and Privacy in Wireless and Mobile Networks (WISEC). 2013. 13−24. [doi: 10.1145/2462096.2462100]

[22] Aafer Y, Du W, Yin H. DroidAPIMiner: Mining API-level features for robust malware detection in Android. In: Proc. of the Int'l Conf. on Security and Privacy in Communication Networks (SecureComm). 2013. 86−103. [doi: 10.1007/978-3-319-04283-1_6]

[23] Arp D, Spreitzenbarth M, Hübner M, Gascon H, Rieck K. Drebin: Effective and explainable detection of Android malware in your pocket. In: Proc. of the 21th Annual Symp. on Network and Distributed System Security (NDSS 2014). 2014. [doi: 10.14722/ndss.2014.23247]

[24] Zhang XY, Zhang G, Shen LW, Peng X, Zhao WY. Similarity analysis of multi-dimension features of Android application. Computer Sceinece, 2016,43(3):199−205, 219 (in Chinese with English abstract). [doi: 10.11896/j.issn.1002-137X.2016.3.037]

[25] Kong DG, Cen L, Jin HX. AUTOREB: Automatically understanding the review-to-behavior fidelity in Android applications. In: Proc. of the 22nd ACM Conf. on Computer and Communications Security (CCS 2015). 2015. 530−541. [doi: 10.1145/2810103.2813689]

[26] Zhang M, Duan Y, Feng Q, Yin H. Towards automatic generation of security-centric descriptions for Android apps. In: Proc. of the 22nd ACM Conf. on Computer and Communications Security (CCS 2015). 2015. 518−529. [doi: 10.1145/2810103.2813669]

[27] Wang R, Feng DG, Yang Y, Su PR. Semantics-Based malware behavior signature extraction and detection method. Ruan Jian Xue Bao/Journal of Software, 2012,23(2):378−393 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3953.htm [doi: 10.3724/SP.J.1001.2012.03953]

[28] Yang H, Zhang YQ, Hu YP, Liu QX. A malware behavior detection system of Android applications based on multi-class features. Chinese Journal of Computers, 2014,37(1):15−27 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2014.00015]

[29] Zhou Y, Jiang X. Dissecting android malware: Characterization and evolution. In: Proc. of the IEEE Symp. on Security and Privacy. 2012. 95−109. [doi: 10.1109/SP.2012.16]

[30] Au KWY, Zhou YF, Huang Z, Lie D. Pscout: Analyzing the Android permission specification. In: Proc. of the 2012 ACM Conf. on Computer and Communications Security. 2012. 217−228. [doi: 10.1145/2382196.2382222]

附中文参考文献:

[1] 卿斯汉.Android 安全研究进展.软件学报,2016,27(1):45−71. http://www.jos.org.cn/1000-9825/4914.htm [doi: 10.13328/j.cnki.jos.004914]

[5] 李桂芝,韩臻,周启惠,王雅哲.基于 Binder 信息流的 Android 恶意行为检测系统.信息网络安全,2016,(2):54−59. [doi: 10.3969/j.issn.1671-1122.2016.02.009]

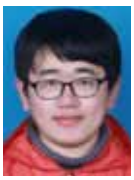
[10] 杨轶,苏璞睿,应凌云,冯登国.基于行为依赖特征的恶意代码相似性比较方法.软件学报,2011,22(10):2438−2453. http://www.jos.org.cn/1000-9825/3888.htm [doi: 10.3724/SP.J.1001.2011.03888]

[17] 罗杨,张齐勋,沈晴霓,刘宏志,吴中海.多层次的 Android 系统权限控制方法.软件学报,2015,26(Suppl.(2)):263−271. http://www.jos.org.cn/1000-9825/15037.htm

[24] 张希远,张刚,沈立炜,彭鑫,赵文耘.多维度的安卓应用相似度分析.计算机科学,2016,43(3):199−205,219. [doi: 10.11896/j.issn.1002-137X.2016.3.037]

[27] 王蕊,冯登国,杨轶,苏璞睿.基于语义的恶意代码行为特征提取及检测方法.软件学报,2012,23(2):378−393. http://www.jos.org.cn/1000-9825/3953.htm [doi: 10.3724/SP.J.1001.2012.03953]

[28] 杨欢,张玉清,胡予濮,刘奇旭.基于多类特征的 Android 应用恶意行为检测系统.计算机学报,2014,37(1):15−27. [doi: 10.3724/SP.J.1016.2014.00015]



缪小川(1990－),男,江苏南通人,硕士,主要研究领域为 Android 应用安全漏洞分析检测.

汪睿(1993－),男,学士,CCF 学生会员,主要研究领域为 Web 应用安全缺陷检测.

许蕾(1978－),女,博士,副教授,CCF 专业会员,主要研究领域为 Web 应用分析测试,Web 服务选择组合,并发缺陷检测.

张卫丰(1974－),男,博士,教授,CCF 专业会员,主要研究领域为软件分析测试,大数据处理.

徐宝文(1961－),男,博士,教授,博士生导师,CCF 会士,主要研究领域为程序设计语言,软件工程,并行与网络软件.