文章编号:1671-4598(2017)07-0012-04 DOI:10.16526/j.cnki.11—4762/tp.2017.07.003 中图分类号:TP309 文献标识码:A

基于 Android 网络恶意行为检测系统的应用研究

贺 强[1,2],王双喜[1],李剑勇[1],曲长征[1]
(1. 山西农业大学 信息学院,山西 晋中 030800;2. 太原市电子研究设计院,太原 030002)

摘要:目前,Android 系统是当今网络用户最对的应用系统之一,而随着科学技术的发展,对于 Android 系统的恶意行为软件也逐渐增多,给当前的应用用户的财产以及私人信息安全带来了很大的威胁,严重的迟缓了当前移动通信网络技术以及相关于应用客户端的推广;为此,根据 Android 系统的特有机构设计出一种基于 Binder 信息流的自动检测恶意行为系统,以此来解决对于当前网络安全对于 Android 系统用户带来的负面影响;根据目前网络中的应用通信信息,检测可能存在的泄露用户信息的应用软件为目标,建立信息矢量图以此来分析当前网络中的恶意行为;通过对软件进行检测,研究可实用性和检测效果,结果显示其识别率可以达到 100%,并且软件运行只占有内存的 7%,结果可以达到当前的 Android 用户的使用范围。

关键词:Android;网络恶意行为;Binder;检测

Application Research of Malicious Behavior Detection System Based on Android Network

He Qiang[1,2], Wang Shuangxi[1], Li Jianyong[1], Qu Changzheng[1]
(1. College of Information, Shanxi Agricutural University, Jinzhong 030800, China;
2. Taiyuan Electronic Research and Design Institute, Taiyuan 030002, China)

Abstract: The Android system is one of the most of the application system of the network users, and with the development of science and technology, the software for malicious behavior Android system has gradually increased, brought great threat to the application of the user's current property and personal information security, severe delay on the current mobile communication network technology and extension on application client. According to the specific mechanism of Android system to design a Binder based on the information flow of the automatic detection system of malicious behavior, in order to solve the negative impact of the current network security system for Android users. According to the application communication information in the current network, the application software of the possible leakage user information is detected, and the information vector is built to analyze the malicious behavior in the current network. Through testing the software of practicability and detect, the results showed that the recognition rate can reach 100%, software occupies only 7% memory. Results can reach the current Android user usage.

Keywords: Android; network malicious behavior; Binder; detection

0 引言

随着近些年网络技术和通信技术的不断发展以及结合,移动通信网络的建立,不断地推动着当今网络移动客户端的发展。而为满足当今的社会现象,以及当前网络环境中信息数据量的要求,Android 系统成为最为热门以及系统运算较为先进的代表,逐渐取代以往的 JAVA 系统成为移动通信端的主要操作系统。并开启了当今智能手机的新时代。而且在当今的市场应用现状来说,具有竞争力的两大系统则为 Android 系统以及苹果公司推出的 IOS 系统。但是由于 IOS 系统为苹果公司独有的移动手机应用系统,只在 Iphone 系列产品中使用,市场占有率毕竟有限,而 Android 系统为当今大多移动手机制造商所使用,是当前市场中占有率最高的操作系统而且应用程度也最为普遍。但是由于网络环境的复杂以及科学技术的不断进步,网络安全问题已经不再仅仅是威胁着主机 PC 端的问题,正在逐渐延伸至智能手机用户端,为此对于保护 Android 系统的用户私人信息安全以及应用软件的可靠性,急需建立一个完善的恶意行为检测系统[1]。

而在目前的开发现状当中,针对 Android 系统开发的检测方法以及系统设计已经有多种方案。例如应用 Indus 针对 Android 应用的源代码采用程序切分的方法分析存在的信息泄露问题分析,形成一种静态分析办法。但是这种办法存在着只有在软件处于休眠状态下才可以发现是否具有威胁性。而利用 TaintDroid 工具开发的动态污点分析法可以做到对于敏感对象实施标记并跟踪监控以及及时发现恶意行为。然而,此系统的操作流程复杂,占中的数据资源极高,实用性上欠佳。

为此本文提出利用 Binder 信息流设计出对于恶意行为检测的办法。在 Android 系统当中 Binder 是最为常用的通信方式,按类别上分属于动态分析法范畴之内,通过收集通信信息做到对于多种方面的安全需求分析。此系统的目的是为了分析由于恶意行为导致的信息泄露现象,通过拦截泄露的信息进行恶意行为分析,以达到检测的效果。

1 Binder 信息流

安卓系统所采用的应用内核是 Linux 内核,而在这中内核当中进行程序运行过程中,会存在许多种的通信机制。例如命名管道 (Named Pipe)、消息队列 (Message Queue)、信号 (Signal)、共享内存 (Share Memory) 以及 Socket。然而在

收稿日期:2016-12-28; **修回日期**:2017-02-06。

基金项目:山西省教育科学"十二五"规划 2015 年度规划课题(GH-15010);2016 年山西省高等学校教学改革创新项目(J2016146)。

作者简介:贺 强(1982-),男,山西太原人,高级工程师,主要从事软件工程方向的研究。

Android 系统运行终端中出现恶意行为的产生一般性的都是由于后行下载的应用软件所夹带的恶意软件。而这些软件所使用的通信机制为 Binder，为此本文所研究的这些恶意软件所产生的私人信息泄露问题检测则采用 Binder 信息流进行分析研究。Binder 是当前 Android 系统中一种较为新颖的 IPC（Inter Process Cimmunication）机制，较为一些原始通信机制相比较来看，此通信机制具备更加简洁的操作流程和更快的运算速度，并且对于系统整体的内存资源占有率较少，所产生的成本也相对可观。

Binder 作为最近科学技术的产物，在 Android 系统的应用也越来越深，逐渐成为了当前系统当中独有的通信 C/S 结构。在 Android 系统中包括了客户端、服务器端以及全局管理和服务器控制端。而 Binder 作为一种较为特殊的运算字符型设备，适应着 Linunx 设备所支持的驱动模型。在用户的使用空间当中包括了以上所提到的 3 个部分，而 Binder 的驱动程序则安装在内核空间之中。在相互关系中服务器控制端辅助 Binder 进行管理工作，客户端以及服务器端则是为 Binder 提供可操作界面以及相应的操作基础设施构造，实现两端口之间可以随时通信的功能。其结构图如图 1。

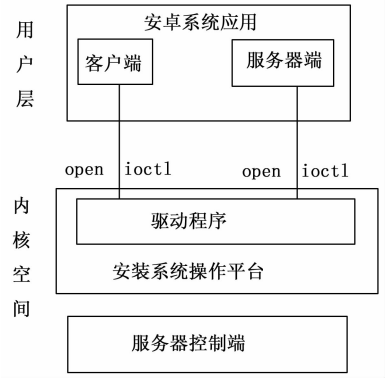

图 1　Binder 机制的结构图

2　利用 Binder 信息流设计安卓恶意行为检测系统

2.1　系统的设计分析

在实现恶意行为检测的基本原理上所利用的是 Binder 机制当中可以对于应用软件所获取的用户信息传递过程中进行拦截，并且对与拦截的到的信息进行全面分析一发现是否存在恶意行为。并且还对当前的应用软件与应用软件之间的通信和应用软件与操作系统之间的通信制成相关的日志文件，对通信过程中的信息进行标注，对可疑的信息传输进行跟踪调查，构建应用通信信息流图像，实现对于恶意信息的全面检测办法[2]。

在系统设立的架构中所采用的是服务器到客户端的模式，在整个系统的操作过程中分为 3 个重要的工作部分。为 Binder 日志收集、Binder 日志文件处理以及最后的恶意分析工作。而这些工作部分中日志收集工作处在客户端部分进行，而剩下两组任务在服务器端进行完成，并且对于之间的信息传输采用 Socket 进行通信，以协同完成恶意行为检测。

2.2　日志收集

在 Android 系统当中各个应用组件通信方式在进行通信过程中都应该经过 Binder 方式来实现。为此在进行日志收集的过程中所得到的信息来源基本上为应用间的信息流通信息流以及 Binder 在驱动运行中所拦截道德通信信息流。而为了将系统设计进行更加简约以及灵活性高和内耗较少，所采用日志的模式，将信息写入到日志当中，并且将日志文件存放在客户端当中，可以大大减少对于内存的占用。但是这种模式下需要对用户空间设置相应的守护进程，保证整个日志文件的安全以及共分析过程中可以方便提取以及不会受到损坏。而这个守护进程随 Android 智能手机开启时便随之启动并且随时与 Binder 驱动设备进行实时通信，为及时对日志进行处理和分析工作。

2.3　日志处理

在 Binder 通信日志的储存形式当中所采用的是二进制的储存格式，在进行分析和运算的过程中驱动程序无法单独对其运算和解析，需要将数据导入到数据库当中进行分析，为此对于收集到的隐私信息的查询或是通信记录的调取都从数据库端进行操作。

然而被写成的日志文件可视性极差，很难进行直接的分析和解读，并且不同数据文件的写入方式不同，对于分析工作有着跟大的阻碍。为此进行相应的分析和解读过程中需要对当前所收集到的日志文件进行预处理工作，将数据之间的字段符号意义重新规划并且设定成可以进行解读的模式。在当前的 Android 系统应用软件通信过程中所涉及的字段大致分为 3 种，通信数据编号 ID 用于发送 Binder；通信类 Type 以及 Type 四种通信请求，通信请求并且要求反馈的字段，对于所发送的请求接收并且给予反馈字段，对于发送的请求接收但不给予反馈的字段；在应用软件发送的进程号 from－id 以及进程名 from－name 字段；接收方所对于该进程接收号 to－id 和进程接收名 to－name 字段；通信内容大小和内容的 date－size 和 date。在预处理过程中需要将日志当中的复杂字符字段通过预处理重新编写成上述大致使用的基本字段，便于后期对于日志信息的处理工作。

在进行日志分析和处理过程中建立应用间信息通信流图可以更加快速的分析出应用信息之间的关联。建立方法将日志文件导入到数据库当中，并且对上述处理后的字段进行分析。而为保证识别的准确性以及对于危害用户私人数据的安全行，因采用的对比方法设置用户隐私数据样本，并且通过收集到的通信数据内容与样本匹配发现所可能存在的涉及到隐私数据外泄的数据源和通信记录。为找到泄露的通信信息流向，利用发送发的进程为开始出发点，将接收方作为终点，得出整体的数据流向数据。而目前的网络通信环境复杂，一般性为一点对多点的通信交流方式，为此采用不断迭代的方式来进行每一个数据流向进行矢量图构造。最后将所有的数据流向图汇总形成信息矢量图。而且要对矢量图当中存在信息泄露的信息流向线进行标记。矢量图的构建方式如图 2 所示。

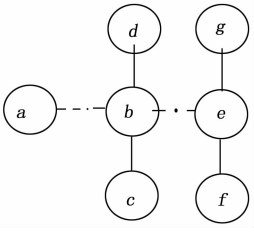

图 2　信息矢量图构建

图中各字母都代表着是一个应用。而 a－b－c 应用时间进

行通信过程中存在了匹配到的隐私数据信息。在矢量图当中可以显示出应用之间进行通信连接的路径。此图为举例图，在图中可以看出应用 b 与 a、c、d、e4 个应用都有着信息流通的情况，为此根据这些流通路径进行分析可以发现在这些应用当中是否存在着对用户信息造成泄露的现象以及是否存在恶意行为。

2.4 恶意行为分析

对与应用软件之间的信息流通不都代表着存在着信息泄露和具备恶意行为的现象。在进行恶意行为定责的过程中需要因实际情况具体分析。在整个分析的过程中需要假定在系统中运行的所有应用软件均为可靠的，并且这些软件不会受到不信任的第三方软件的干扰和控制。所以通过对于矢量图的方法运用以下代码运算[3]：

```
void Traverse(Graph G)
{//按照遍历图 G 广度优先,分析是否具备恶意行为
for( v=0; v(G.vexnum,++v)
//Malicious
Malicious[v]=FALSE;
//Visited
Visited[v]=FALSE;
InitQueue(Q)
for( v=0; v(G. vexnum,++v)
if(! visited[v])
{EnQueue(Q,v);
While(! QueueEmpty(Q))
{DeQueu(Q,u);
for(w=FirstAdjVex(Q,u);w(=0;
w=NextAdj Vex(Q,uw))
```

//如果此过程仍然无法确定 u 是否具备恶意行为继续进行分析。

```
if(! Visited[u],&&! Malicious[u])
```

{//如果检测到在 u 和 w 之间存在着标记的隐私数据传输行为,进行恶意分析

```
//对(u,w)这条矢量图边线进行恶意分析
BinderAnalysis (u,w);
//根据分析结果显示是否存在有恶意行为。
```

通过对以上的算法进行计算，可以通过对矢量图的信息流向线路计算结果可以看出检测的应用与应用之间的通信是否存在有用户私人信息的传递过程，对此过程在进行重点的算法分析后，可以看出其是否存在着恶意行为的现象。通过函数 BinderAnalysis（u，w）的表示可以将结果展示出来并做到检测的目的保证用户的个人隐私数据的安全。

3 设计系统的实现

本文所设计研究的对于安卓系统的恶意行为检测采用的是 Binder 采集信息，并且利用信息建立相应的矢量图，反映出应用软件之间的信息流向，通过这些流向和路径的分析得出是否存在恶意行为。通过改变 Binder 的底层代码以适应当前的安装系统版本，而且当前的安卓系统本更根性非常快，加之许多手机制造商均根据安卓系统为原型设计出符合自身特点的操作系统，需要根据不同的手机品牌的操作系统设定相应的代码才可以达到更有效的恶意行为检测。

在 Binder 的通信信息收集过程当中内核层中的驱动以及用户层所应用的守护进程分别保护一个结构体数组，每个数组中含有的数都为 32 个，并且这两个结构都代表着一个 Binder 的通信信息，变量则为字段。在通信过程中 Binder 系统每次拦截的一个应用的信息流就将这个信息数据赋值成这个数组的结构体当中。当数组当中的 32 个个体都被重新赋值之后系统的驱动将会告知守护进程。守护进程将会利用 Ioctl 协议访问 Binder 驱动系统，并且驱动系统将会对这些数组进行复制并且发送到守护进程当中的数组集当中。守护进程将会把这些复制过来的新数组形成日志的形式编写进数据库当中。当这些日志的数量被累积到一定的程度时，系统将会自动将这些日志文件上传到服务器当中，并且利用服务器的数据库对此进行分析识别工作。在 Binder 通信日志的储存过程中采用二进制的储存方式并且利用 Ultraedit 软件进行日志的开发。其日志的显示图如图 3。

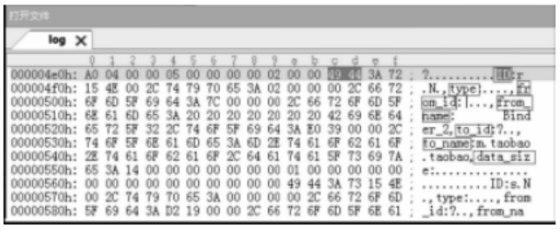

图 3 日志显示图

从图中可见其代码不宜进行解读为此需要进行上文所提到的预处理工作。将每一个字段重新解读并且组成为可以进行分析的上文所提到的字段形式中，并且将预处理之后的字段数据导入到 Binderlog 的数据表当中以供后期处理[4]。

而日志的处理工作大致位于服务器当中的数据库中来进行的。绘制的矢量图基于 Struts＋Spring＋H ibernate 架构，采用的绘制软件为 script，并且图形库选择为 Raphael。并且在矢量图的分析中得出存在的用户个人隐私信息的信息传递链条，将这些信息重新设定一个 Phonestate 的表格。通过对于新表格当中的发送发、接收方、节点和应用之间的信息流向进行研究，构建出单独的存在问题的矢量图。图 4 为信息矢量图的应用软件和构建结构过程图。

图 4 信息矢量图展示

在恶意分析过程中的实现则是应用了现今的安卓语言来进行。将分析后的数据函数输入到矢量图当中，分析当前的信息数据是否存在恶意行为，并且根据信息流向找出流出软件应用和接收方。例如，某一方在进行访问某特定数据的时并没有访问的权限，但是该应用在进行传递信息的过程中存在了其某特定数据，则定义此应用软件产生了恶意行为，并归为恶意软件[5]。

4 软件实际检测和结果

实际检测样本为选择了一款装有最新安卓系统的智能手机，并且应用其在网上下载 200 款网络应用 APP，而且为保

证对于系统检测的可能性保真，实验中所应用的到的检测对象分为 IMEI、Wifi MAC、蓝牙、安卓版本号、操作系统序列号、短信信息这六种类别，分别应用设计出的系统对其进行恶意行为检测[6-7]。并且将恶意应用软件的数量结果进行统计智能表 1。

表 1　恶意应用软件的数量结果

类别	IMEI	WIFI MAC	蓝牙	安卓版本号	操作系统序列号	短信信息
恶意应用数量	65	75	42	21	10	16
百分比	32.5%	37.5%	21%	10.5%	5%	8%

从表 1 中可以看出，该系统的检测结果显示，当前网络应用环境当中 IMEI 以及 WIFI MAC 的恶意软件应用数量最多。而系统性能分析中得出系统在进行运算这些软件是否存在恶意软件的进程所耗费时间为 6 秒左右，对于系统的运算能力有着杰出的表现，结果显示此系统对于当前的安卓系统当中的应用软件检测能力非常高，并且占有内存和耗时较少，运行程度较为流畅，有很高的应用性。

5　结论

在当前的网络环境中，网络安全成为最为重要的研究方向，而目前移动手机客户端的接入网络以及 Android 系统应用的智能手机开发，将智能手机网络时代的推向了高潮。为此防止网络中的恶意软件侵入，造成用户个人隐私数据泄露和财产安全等原因考虑，本文设计利用 Android 系统当中的 Binder 信息流模式构建出检测系统，对于用户中的应用软件信息流向进行检测以分析是否存在恶意行为，保证用户在使用过程中的安全性和当前网络复杂环境中的保靠。通过检测可以得出，此系统对于网络应用的检测成果较高，并且耗时时间段，运算所占用的 Android 系统内从较少，有很高的可行性和安全性。在众多的网络安全设计当中提出一种设计构想和参考基础。

参考文献：

[1] 贾同彬，蔡　阳，王跃武，等. 一种面向普通用户的 Android APP 安全性动态分析方法研究 [J]. 信息网络安全，2015，10 (9)：1-5.

[2] 杨　欢，张玉清，胡予濮，等，基于多类特征的 Android 应用恶意行为检测系统 [J]. 计算机学报，2014，37 (1)：1-13.

[3] 李桂芝，韩　臻，周启惠，等. 基于 Binder 信息流的 Android 恶意行为检测系统 [J]. 网络信息安全，2016，3 (2)：54-59.

[4] 王汝言，蒋子泉，刘乔寿. Android 下 Binder 进程间通信机制的分析与研究 [J]. 计算机技术与发展，2012，22 (9)：107-110.

[5] 邓平凡. 深入理解 Android [M]. 北京：机械工业出版社，2011.

[6] 马晋杨，徐　蕾. 基于 Android 系统的手机恶意软件检测模型 [J]. 计算机测量与控制，2016，24 (1)：156-158.

[7] 林　鑫. 基于沙盒的 Android 恶意软件检测技术研究 [J]. 电子设计工程，2016，24 (12)：48-50.

(上接第 7 页)

[57] Lin Z, Broucke M, Francis B. Local control strategies for groups of mobile autonomous agents [J]. IEEE Transactions on Automatic Control, 2004, 49 (4): 622-629.

[58] Ren W, Beard R W. Consensus seeking in multiagent systems under dynamically changing interaction topologies [J]. IEEE Transactions on automatic control, 2005, 50 (5): 655-661.

[59] Lin Z, Wang L, Han Z, et al. Distributed formation control of multi-agent systems using complex Laplacian [J]. IEEE Transactions on Automatic Control, 2014, 59 (7): 1765-1777.

[60] Wang L, Han Z, Lin Z. Formation control of directed multi-agent networks based on complex Laplacian [A]. Proceeding of the IEEE 51st Annual Conference on Decision and Control (CDC) [C]. 2012: 5292-5297.

[61] Wang L, Han Z, Lin Z, et al. A linear approach to formation control under directed and switching topologies [A]. Proceedings of the IEEE International Conference on Robotics and Automation (ICRA) [C]. 2014: 3595-3600.

[62] Han T, Lin Z, Xu W, et al. Three-dimensional formation merging control of second-order agents under directed and switching topologies [A]. Proceedings of the 11th IEEE International Conference on Control & Automation (ICCA) [C]. 2014: 225-230.

[63] Turnbull L, Samanta B. Cloud robotics: Formation control of a multi robot system utilizing cloud infrastructure [A]. Proceedings of IEEE Southeastcon [C]. 2013: 1-4.

[64] Cook J, Hu G. Vision-based triangular formation control of mobile robots [A]. Proceedings of the 31st Chinese Control Conference (CCC) [C]. 2012: 5146-5151.

[65] Scheggi S, Morbidi F, Prattichizzo D. Human-robot formation control via visual and vibrotactile haptic feedback [J]. IEEE Transactions on Haptics, 2014, 7 (4): 499-511.

[66] Wang Y, Cheng L, Hou Z G, et al. Optimal Formation of Multi-robot Systems Based on a Recurrent Neural Network [J]. IEEE Transactions on Neural Networks and Learning System, 2015, PP (99): 1.

[67] 张洪亮. 多机器人编队技术的研究与应用 [D]. 北京：北京工业大学，2009.

[68] Dalfior J S, Vassallo R F. Nonlinear formation control for a cooperative load pushing [A]. IEEE International Conference on Industrial Technology (ICIT) [C]. 2010: 1439-1444.

[69] Moon S, Kwak D, Kim H J. Cooperative control of differential wheeled mobile robots for box pushing problem [A]. Proceedings of the 12th International Conference on Control, Automation and Systems (ICCAS) [C]. 2012: 140-144.

[70] Bai H, Wen J T. Cooperative load transport: a formation-control perspective [J]. IEEE Transactions on Robotics, 2010, 26 (4): 742-750.

[71] Eoh G, Jeon J D, Choi J S, et al. Multi-robot cooperative formation for overweight object transportation [A]. IEEE/SICE International Symposium on System Integration (SII) [C]. 2011: 726-731.

[72] Zhaohui D, Min W, Xin C. Multi-robot cooperative transportation using formation control [A]. Proceedings of the 27th Chinese Control Conference (CCC) [C]. 2008: 346-350.

[73] N. Michael, J. Fink, and V. Kumar. Cooperative manipulation and transportation with aerial robots [J]. Autonomous Robots, 2011, 30 (1): 73-86.

[74] Lee, Taeyoung. Geometric control of multiple quadrotor UAVs transporting a cable-suspended rigid body [A]. Proceedings of the IEEE 53rd Annual Conference on Decision and Control (CDC) [C]. 2014.

[75] Farhad A. Goodarzi, Taeyoung Lee. Dynamics and Control of Quadrotor UAVs Transporting a Rigid Body Connected via Flexible Cables [A]. American Control Conference [C]. 2015: 4677-4682.