



基于 iOS 系统的恶意行为检测研究

王玉良,陈晓东,吴吞

(中国电信股份有限公司上海研究院,上海 200122)

摘要:首先列举了多个 iOS 平台的恶意应用的案例,通过剖析作案手法以及造成的恶劣影响,分析了 iOS 平台下移动应用的主要恶意行为特征,研究了恶意行为检测过程中的各项关键技术,提出了 iOS 应用恶意行为检测的模型。最后,给出了 iOS 应用恶意行为检测的解决方案。

关键词: iOS;恶意行为;iOS 应用安全

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2017047

Research on malicious behavior detection based on iOS system

WANG Yuliang, CHEN Xiaodong, WU Tun

Shanghai Branch of China Telecom Co., Ltd., Shanghai 200122, China

Abstract: Firstly, the cases of malicious application of multiple iOS platforms were enumerated. The main malicious behavior of mobile application under iOS platform was analyzed by dissecting the misuse of crime and the bad influence. The key technologies of malicious behavior detection process were studied. The iOS application malicious behavior detection model was put forward. Finally, iOS application malicious behavior detection solution was given.

Key words: iOS, malicious behavior, iOS application safety

1 引言

iOS 操作系统在设计之初就拥有诸多优良的安全保护机制,并且历经苹果公司多年的不断升级以及改进,现在已经发展成为一款安全性能非常良好的移动操作系统。除了系统本身的安全机制外,苹果还引入了 App Store(应用商店)保护系统不受恶意软件入侵。但是尽管如此,iOS 各种漏洞和恶意应用还是频频出现。

本文以 iOS 应用的恶意行为为基点,首先从已经爆发的应用恶意行为开始,管中窥豹,对现在 iOS 应用安全的严峻形势做一个描述,然后对各种恶意行为做分析和归类,最后给出一套解决方案。

2 iOS 应用安全的严峻形势

从历年的案例着手,分析那些曾经猖獗目前已销声匿迹的应用或者依然猖獗在一线的应用。

2.1 海马苹果助手

海马苹果助手作为第三方应用商店,之所以受到用户的喜爱,是因为一些在苹果应用商店收费的软件通过它却可以免费获取,而且,海马苹果助手使用起来非常简单,可以让用户更容易安装应用程序和管理用户设备。

不幸的是,这个特别的辅助应用程序有着用户未知的恶意行为。首先它会收集用户的 Apple ID 和密码,具体如图 1 所示。



· Idfv:唯一区分某 union(设备和 App)的标记符。

此次受到影响的 App 程序众多,据称受感染的 App 多达 76 个,而记载着 App 名单的截图应该来自“360 安全播报平台”,其在 2016 年 9 月 19 日更新的消息中将受 XcodeGhost 感染的 App 数量上调为 344 款;而截至 9 月 20 日下午的通报,受感染的 App 数量为 1 078 款。

知名度较高的部分 App 为微信、网易云音乐、滴滴打车、高德地图、12306、同花顺、中信银行动卡空间、简书等,涉及即时通信软件、地图应用甚至金融服务产品。

对于用户来说,这是自从 iOS 诞生以来最大的一次威胁;对于苹果公司来说,这是自成立以来最大的一次安全挑战。

2.3 爱思助手

该木马通过 PC 感染未越狱的 iOS 设备,而无需利用企业证书。“爱思助手”利用了苹果数字版权管理(digital right management, DRM)上的 FairPlay 漏洞来感染 iOS 设备。苹果允许用户通过计算机上的 iTunes 客户端里的应用商店购买和下载 iOS 应用,然后将之安装到自己的 iOS 设备上。

每款安装到 iOS 设备上的应用都需要提供一个切实购买的授权码,而在 FairPlay 中间人攻击中,攻击者在应用商店上购买了一款应用,然后拦截并保存了该授权码。之后,他们用开发出来的 PC 软件来模拟 iTunes 客户端的行为,欺骗 iOS 设备相信应用是由受害人购买的。

用户因而可以安装他们实际未支付过的应用,但软件开发者也能够借此向不知情用户的设备偷偷安装恶意软件。

2.4 其他应用

YiSpecter 可以下载、安装和启动应用,替换已安装应用,显示非法应用的广告以及改变 Safari 默认搜索引擎,将用户信息上传至远程服务器。

InstaAgent 是一款可以与 Instagram 账户连接,并用来追踪来访用户的应用,但该应用擅自存储用户账户和密码,并以明文上传至 instagram.zunamedia.com 远程服务器。不仅如此,InstaAgent 在与用户的 Instagram 账户连接后,还会在未经用户允许的情况下擅自发布垃圾信息和图片。Instagram 本身尚未允许通过第三方应用发布状态,所以 InstaAgent 直接以用户的身份发布这些垃圾图片,对用户和用户的好友都会造成困扰。

由此可见,iOS 系统绝不是一个绝对安全的环境,对手机的依赖加深时,越来越多的信息会被存储在手机上,

破解手机的价值会越来越大,应用的恶意行为造成的伤害也会越大。从现在的趋势看,更多的不法分子看到了这一点,并打算从中牟利,所以,现在以及将来 iOS 应用安全的形势都是严峻的,应当积极与之对抗。

3 iOS 应用恶意行为检测解决方案

通过以上案例,发现应用的恶意行为分为以下方面:

- 下载、安装、启动应用;
- 窃取用户信息;
- 操作用户文件;
- 显示非法广告;
- 恶意传播信息。

这些恶意行为有一个共同点:完成这些恶意行为需要调用相应的 API(application programming interface,应用程序接口),如果能得到该应用调用的所有敏感 API,获取该行为的信息,就能判断该行为是否为恶意行为。

结合以上构思和反复的实践,提出以下解决方案。

3.1 方案技术原理

本方案的主要原理为:对应用的 API 进行 Hook 并记录,以一定时间为周期,将应用行为梳理为行为序列,以行为序列为单位,对比恶意行为序列库,判断该行为序列是否为恶意行为序列。

该系统分为两部分:行为追踪器和行为分析器。其中,行为追踪器安装在 iOS 终端中,通过 Hook 关键行为的 API 来获取指定软件的关键行为,这些 API 包括:文件系统、用户偏好设置、密钥链、通用加密、安全框架、HTTP、粘贴板、URL 方案、XML 等。最后记录这些函数调用的信息并永久保存在数据库中。行为分析器安装在 PC 设备中,将行为追踪器生成的数据库文件作为输入,进行分析处理后,在本地生成行为序列的结果报表,通过与恶意行为序列库进行对比,识别是否是恶意行为。

恶意行为序列库以行为序列为单位进行存储,记录非法的恶意行为,该库会在实践中不断完善,也会在其他合作机构中进行补充。

3.2 方案架构

该系统架构如图 3 所示,其主要由 iOS 终端层和 PC 设备层两部分组成:iOS 终端层用于监测和记录应用行为,PC 设备层用于提取和解析来自 iOS 终端层的数据。

Theos 框架是一套越狱开发环境,由 iOS 越狱界知名

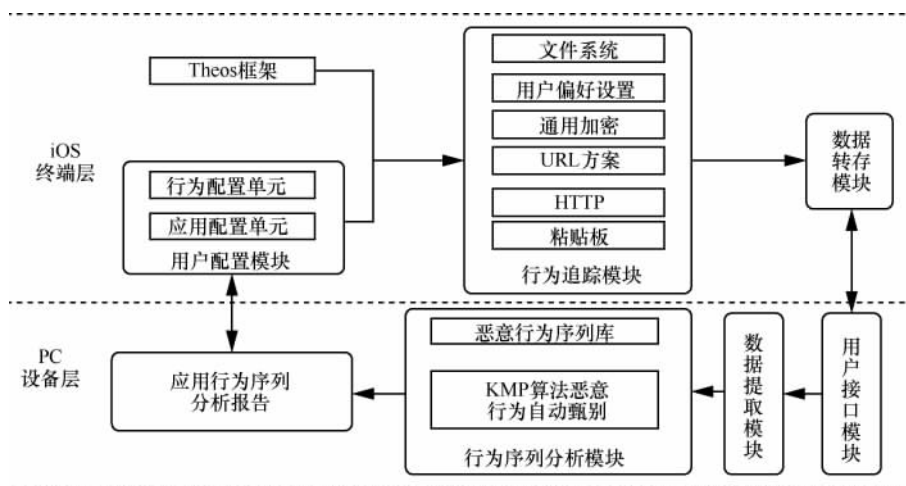


图3 方案架构

人士 DustinHowett 开发并分享到 GitHub 上。Theos 与其他越狱开发工具相比,最大的特点就是简单,可以让使用者把精力都放在开发工作上。本方案就是基于 Theos 框架进行开发的。

用户配置模块使用 Setting.bundle 在设置中添加配置项,配置项包括两部分:一部分对检测的应用开启检测,支持各个应用同时检测,该操作会将用户的配置存储到一个 plist 文件中,另一部分是应用行为的各个 API 检测的开启或关闭,列表中所有的检测默认都是开启的。

行为追踪模块、数据转存模块:如图4所示,行为追踪模块使用图3罗列的各种敏感 API 进行 Hook,将应用的行为存储在本地。但是 Hook API 对所有调用者都是有效的,记录的结果有些并不需要。需要对这些调用加以甄别,精确地找到需要检测应用的行为,所以在开始追踪应用行为之前,该模块会读取用户配置信息,从用户配置信息中获取需要检测的应用 ID,然后在 Hook 之前使用 %ctor 函

数对其进行选择性 %init,由于 iOS 设备中程序文档目录在 var/mobile/Containers/Data/Applocation 中,所以很容易找到对应程序的目录文件,并在该应用的文档里创建数据库,对该应用的行为进行保存。

在 PC 层布置服务器,首先将计算机与 iOS 设备置于同一网段下,服务器通过 SSH 使用户登录移动设备,服务器会通过用户配置模块获取应用的 ID,并得到应用的文档目录,将沙盒中的数据库文件分别提取到 PC 端,如图5所示。

从数据库中提取出来的是一条条的 API 和参数,会记录一个额外的参数:调用 API 的系统时间。数据库数据按照系统时间通过数组保存,即梳理成一个行为序列。

恶意行为序列库是一个特征库,里面会留存已知的恶意行为,特征库在运作的时候会不断完善,也会从合作的机构中获取新特征。当得到行为序列时,立刻与特征库进行比对,比对成功即可认为该行为序列为恶意行为序列。

在拥有大量数据时,人工的效率会变得很低,所以进行恶意行为序列匹配时,使用一个通用算法进行匹配——KMP (Knuth-Morris-Pratt, 字符串查找) 算法,常用于在一个文本串 S 内查找一个模式串 P 的出现位置,这个算法由 Knuth D、Pratt V、Morris J H 三人于 1977 年联合发表,故取这 3 人的姓氏命名此算法。

当本方案运行在 iOS 设备中时,会一直记录应用的行为(除非在用户设置模块中去掉该应用),因此鼓励使用周期性的检测方法,恶意行为会存在潜伏期,会使用一个星期甚至一个月作为一个周期去检测该应用。

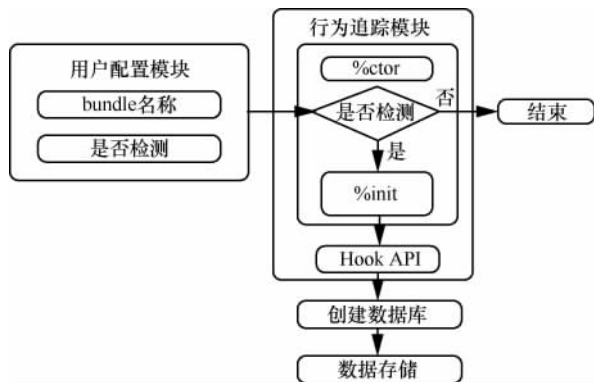


图4 用户配置



902:UIPasteboard valueForPasteboardType:
903:UIPasteboard generalPasteboard
904:UIPasteboard valueForPasteboardType:
905:UIPasteboard valueForPasteboardType:
参数:
<pre>{ "pasteboardType": "public.utfg-plain-text" }</pre>
返回值:
"MISAS"
906:UIPasteboard valueForPasteboardType:
907:UIPasteboard generalPasteboard
908:UIPasteboard valueForPasteboardType:
909:UIPasteboard valueForPasteboardType:
910:NSUserDefaults boolForKey:
911:NSUserDefaults boolForKey:
912:NSUserDefaults boolForKey:
913:NSUserDefaults boolForKey:
914:NSFileManager createFileAtPath:contents:attributes:
915:NSFileHandle fileHandleForWriting ToURL:error:
916:NSData dataWithContentsOfURL:
917:NSData dataWithContentsOfURL:

图5 数据库提取的行为

最后的报告中会显示该周期的具体时间,并判断该周期内的行为是否存在恶意行为,还会列出一些敏感性的行为以供人工二次审查。

3.3 系统实现流程

系统实现流程如图6所示。

该系统的实现流程分为两部分。

(1) iOS 设备上的流程

iOS 设备上的流程具体如下:

- 通过用户接口配置监测应用;
- 行为追踪模块基于 Theos 框架,对应用行为的 API 进行 Hook,截获应用行为 API 的系统时间、参数、返回值;
- 将 API、参数、返回值、系统时间存储到本地。

(2) PC 端数据的提取和解析流程

PC 端数据的提取和解析流程具体如下:

- 登录用户接口,使用数据提取模块提取数据到 PC 端;
- 数据处理模块将数据梳理成行为序列,使用 KMP 算法将之与恶意行为序列库进行对比,然后对该行为序列进行评分;
- 根据行为序列分析模块产生的分析结果,汇总并输出检测报告。

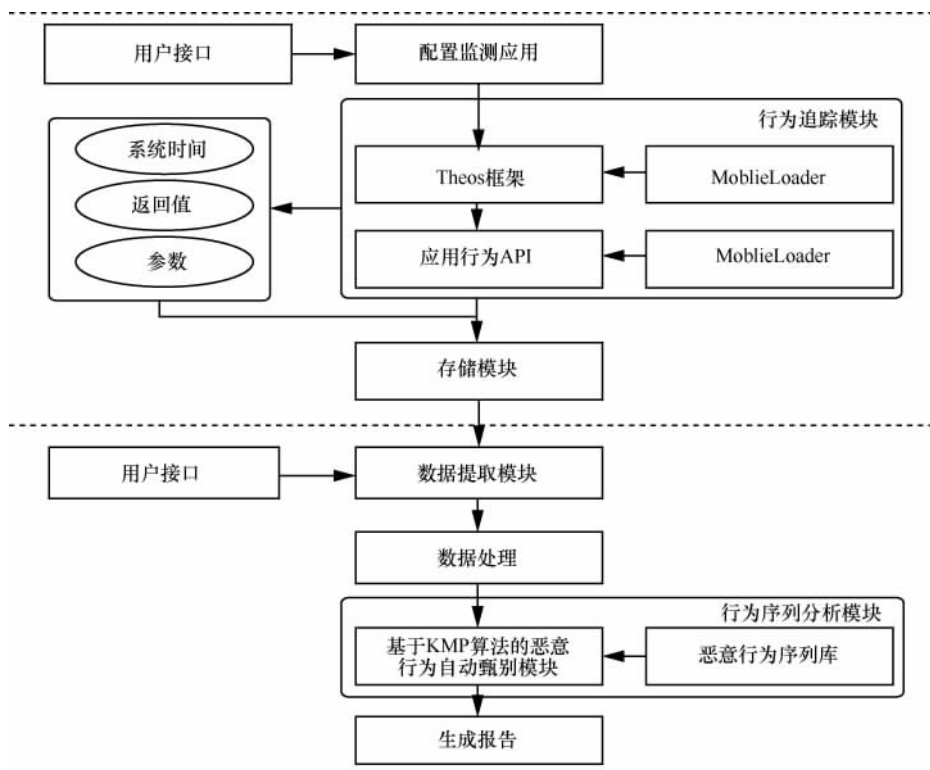


图6 系统实现流程

4 与现有方案对比

4.1 现有方案架构

如图 7 所示, 现有方案架构是一种基于 Hook 的 iOS 关键行为检测装置和方法, 该检测装置通过 Hook 关键行为的 API, 实时捕获 iOS 系统的关键行为, 用于监控 iOS 系统的关键行为, 获取与该关键行为相关的信息, 并在服务端实时展示给用户, 或者保存为结果报表, 以供用户进行审核与评估。该装置由分别设置在 iOS 终端层的行为追踪模块以及位于 PC 设备层、顺序连接的用户接口模块、安全风险报告模块和行为分析模块共 4 个部件组成。

4.2 方案对比

本文所提方案与现有方案对比有诸多优点, 具体如下。

- 现有的方案主要针对私有 API 进行检测, 不能完成对应用恶意行为的检测, 本文所提方案针对的是对移动应用恶意行为的检测。
- 现有方案的通信单元是即时通信, 针对单个 API 即单个行为进行检测, 本文所提方案采用本地存储策略, 针对的不是单个行为而是行为序列, 以一定周期(可能是一周或者更长, 这是即时通信无法完成的)的行为序列判断该行为是不是恶意行为, 对于恶意行为的检测更具有针对性、可行性。
- 现有方案由于采用即时通信策略, 只能短时对单个

应用进行检测, 本文所提方案采用本地存储策略, 可以长期对多个应用进行检测。

5 结束语

随着移动互联网技术的不断发展, 人们可以通过移动设备拍照、录制视频、玩游戏、炒股或者办公, 以手机为代表的智能终端逐渐成为人们日常生活中必不可少的工具。但值得注意的是, 移动设备里存储了大量的用户数据及隐私信息。手机一旦出现安全问题, 就会严重威胁到用户的数据和隐私安全。现在, 手机功能越来越强大, 上网越来越便利, 人们在手机上安装的应用也越来越多, 随之而来的安全问题也越来越突出。iOS 作为目前最流行的移动智能应用平台, 同时也是市场占有率极高的移动操作系统, 吸引了大量的恶意攻击者通过应用商店发布带有恶意行为的应用软件。对用户的信息和财产安全构成了严重的威胁, 这种现象亟待解决。

恶意代码的检测技术能够促进移动互联网产业健康和稳定的发展。建立移动应用软件的安全监测技术体系, 建设权威的第三方检测平台, 有利于移动应用软件产业链的形成和发展。与此同时, 应用软件的安全性 with 用户利益紧密相关, 只有科学的、权威的恶意代码检测系统, 才能构建一个用户可信赖的移动互联网应用使用环境, 安全要求高、经济附加值高的移动应用才值得推广和应用, 才能使移动互联网真正地繁荣发展。

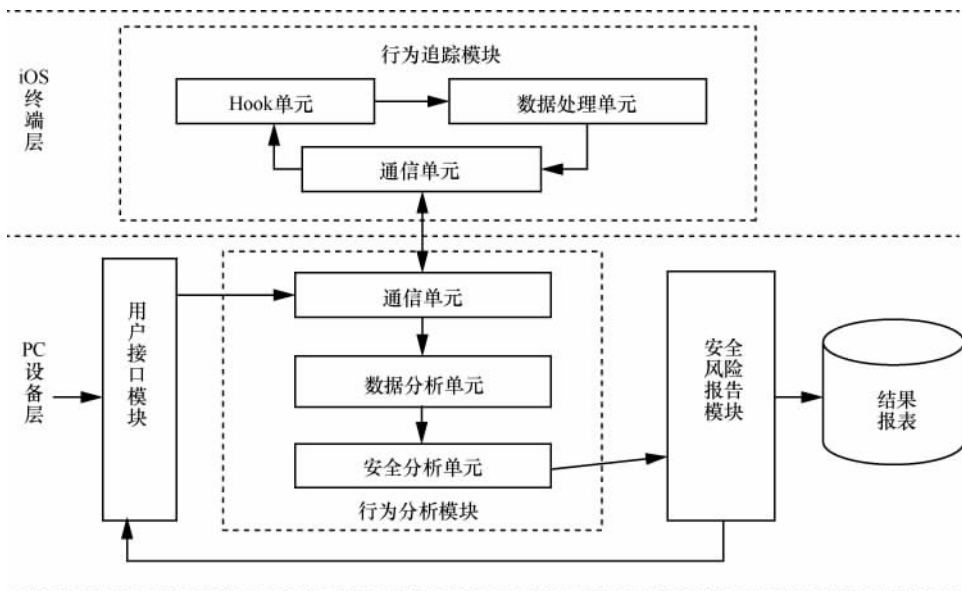


图 7 现有方案架构



参考文献:

- [1] 徐磊. iOS 应用安全无法销毁的文件 [J]. 计算机与网络, 2015, 41(20): 46-47.
XU L. iOS application security files cannot be destroyed [J]. Computer & Network, 2015, 41(20): 46-47.
- [2] 刘朋飞. iOS 应用程序的攻击手段分析及防护 [D]. 成都: 电子科技大学, 2014.
LIU P F. Analysis and protection of attack means of iOS App[D]. Chengdu: University of Electronic Science and Technology of China, 2014.
- [3] 罗喧, 梁柏青, 潘军彪, 等. 智能手机应用安全关键技术探讨 [J]. 电信科学, 2013, 29(5): 19-27.
LUO X, LIANG B Q, PAN J B, et al. Study on the key technologies of smartphone application security[J]. Telecommunications Science, 2013, 29(5): 19-27.
- [4] 李柏岚, 谷大武. iOS 平台的软件安全性分析[D]. 上海: 上海交通大学, 2011.
LI B L, GU D W. Software security analysis of iOS platform[D]. Shanghai: Shanghai Jiao Tong University, 2011.
- [5] 黄斐一, 武静雅, 孔繁盛. 移动互联网手机应用安全研讨[J]. 移动通信, 2014(17): 60-63.
HUANG F Y, WU J Y, KONG F S. Research on application security of mobile internet[J]. Mobile Communications, 2014(17): 60-63.

[作者简介]



王玉良(1992-),男,中国电信股份有限公司上海研究院研究员,主要研究方向为移动互联网安全、应用仿真测评等。



陈晓东(1984-),男,中国电信股份有限公司上海研究院研究员,主要研究方向为移动应用安全、漏洞挖掘技术等。



吴吞(1993-),男,中国电信股份有限公司上海研究院研究员,主要研究方向为移动互联网安全、应用仿真测评等。