



专题:终端与智能卡技术

# 智能终端操作系统安全问题及解决方案

侯玉华,周晓龙

(中国联合网络通信有限公司研究院 北京 100032)

**摘要:**阐述了智能终端操作系统安全的现状,剖析现有操作系统存在的安全问题。分析了国内自主操作系统的研发现状,探讨了在国内自主 TIOS 的基础上进行全方位安全加固的解决方案,分别对内核、系统支撑库、GUI、应用框架层进行加固,介绍了九大基础安全应用规划。最后,提出了不同类型用户和不同安全等级操作系统的安全需求,为各类安全手机开发提供参考。

**关键词:**智能终端操作系统;Android;iOS;TIOS;安全加固

**doi:** 10.11959/j.issn.1000-0801.2015077

## Security Problems and Solutions of Smart Terminal Mobile Operating System

Hou Yuhua, Zhou Xiaolong

(China Unicom Research Institute, Beijing 100032, China)

**Abstract:** The present situation of the smart terminal operating system security was described. The security problem of the existing operating system and the present status of research and development of domestic independent operating system were analyzed. Solution of the security reinforcement based on domestic TIOS, which reinforces kernel, system support library, GUI, application framework of TIOS, was discussed. The nine basic safety application programming were introduced. Finally, security requirements of different users and different security level of operating system were proposed. It provides reference for the development of all types of secure mobile phone.

**Key words:** smart terminal mobile operating system, Android, iOS, TIOS, security reinforcement

### 1 智能终端操作系统安全现状

#### 1.1 智能终端市场现状

近几年智能终端产业迅猛发展,市场规模不断扩大。2013 年全球智能手机出货量为 10.042 亿部,根据 IDC 的预测,2014 年这一数据将达到 13 亿部,全球智能手机出货量将比 2013 年增长 26.3%。在上述终端中,82%为 Android 手机,13.8%为 iOS 手机。

我国智能终端市场需求不断增长,2014 年 5 月,据研究机构 Strategy Analytics 发布的研究报告称,2014 年我国首次超越美国成为全球营收最高的手机市场。从手机销量来看,我国 2014 年的手机销量增长 15%,达到 4.3 亿部,主要市场份额被三星公司和苹果公司占领,我国手机厂商的出货量也有巨大的发展,但是我国手机厂商终端一直持续低利润,主要原因在于其产品同质化现象严重,缺乏针对细分市场需求的产品,导致大众消费市场竞争激烈,利润低薄。

收稿日期:2015-02-05;修回日期:2015-03-03

论文引用格式:侯玉华,周晓龙. 智能终端操作系统安全问题及解决方案. 电信科学,2015077

Hou Y H, Zhou X L. Security Problems and Solutions of Smart Terminal Mobile Operating System. Telecommunications Science, 2015077



智能终端的市场不断发展壮大,其形态也不局限于智能手机、平板电脑、智能电视,应用领域也不再局限于大众消费市场。智能手表、智能眼镜等可穿戴产品也在逐渐走入大众市场,可穿戴设备不断催生出围绕个人运动、健康等主题的消费热点和消费模式。在三网融合及大众需求的大背景下,个人终端、家庭电视、PC之间的设备互联、融合互动将又会成为新的消费热点,多种设备的互动还会催生新型的应用体验模式。在智能终端时代,其在物联网领域又产生了新的应用模式,例如在线医疗监控和诊断、在线智能电表、智能水文监测等。据市场预测,未来3年智能眼镜、智能手表等可穿戴智能终端的市场规模将达到100亿美元,便携式家庭医疗设备也将迎来爆发式增长的良机。

## 1.2 主流操作系统发展现状

### 1.2.1 Android 系统

2007年11月5日,谷歌公司正式宣布开发一款新的手机操作系统——Android,其基于2005年收购的同名手机软件公司产品。Android系统以开源免费方式来吸引产业链的参与,形成巨大的产业链号召力,取得了非凡的市场成就。但在开源的背后有许多问题使业界对这种模式产生了质疑。

首先是碎片化问题,目前生产Android系统智能手机的有三星、联想、华为等众多厂商,各厂商的Android系统产品硬件设计方案不同,导致Android系统在各终端产品上的性能表现不同,直接导致系统开发难度的增加。另外,其版本众多,Android系统曾在18个月里发布了4个大版本,同时还存在多个版本分支,各个终端厂商对Android系统的代码进行修改,由此形成了众多的分化版本。据数据统计公司Opensignal 2014年Android设备碎片化的报告显示,Android系统的碎片化与去年相比增加了60%,碎片化问题更加严重。2014年10月15日,谷歌公司发布了Android 5.0版本。在这个版本中,谷歌公司将着力扭转碎片化问题,可能会禁止厂商基于新版的Android系统进行深度定制,碎片化的问题将有所改善,但还会在一段时期内长期存在。

其次是安全隐患问题,Android系统版本演进过快,版本管理比较混乱,其系统软件存在大量的bug和不完善的功能设计,如沙箱模型机制、权限授予机制、root权限获取等。同时,应用软件下载渠道众多,但缺乏有效的审查制度,应用签名机制脆弱,即使证书过期了也不会影响应用的使用。Android系统的应用安装包(APK)很容易被反编译,使得恶意程序将正版应用反编译成携带恶意代码的应用,并伪装成原来的应用,构成安全威胁。

### 1.2.2 iOS

iOS是苹果公司终端体系的基础,围绕iOS苹果公司构建了一个封闭的生态系统,即封闭的终端、封闭的应用、封闭的网络、收费的内容。iOS历经8个版本,不断进行着创新,iOS卓越的人性化设计成为智能、极致体验的代表,苹果公司的大量特色服务和应用都是在iOS的支持下,为用户提供了优秀的体验,加上苹果公司优秀的硬件设计,使苹果公司成为智能手机和智能平板市场的引领者,推动苹果公司取得优异的市场成绩。苹果公司将App Store作为移动互联网领域的标志性服务,App Store具有相对严格的审核机制,但苹果公司的审核机制不是完美的,虽然很难通过iOS漏洞开发恶意软件,但可以将恶意软件注入到合法软件的源代码中,伪装成合法软件供用户下载,也有数据表明iOS大量的应用程序都带有位置跟踪和读取用户地址簿功能,给用户的个人数据安全构成威胁。

### 1.3 智能终端的安全威胁

智能终端开放了原本封闭的终端操作系统,终端与互联网的交互越来越便捷,终端操作系统作为其中重要的一环,其安全性至关重要。终端操作系统的安全威胁主要体现在操作系统后门程序、操作系统漏洞以及API(application programming interface,应用程序编程接口)的滥用。

操作系统的后门是指开发过程中创建的可以控制或获取对程序或系统访问权的方法,后门程序在设计时有两种考虑,首先是可以方便地进入系统修复程序设计中的缺陷,另外就是程序设计者故意设置的控制操作系统的方法。这些后门程序大多不为用户所熟知,但是一旦被滥用,将给用户带来巨大的安全风险。操作系统的后门程序有很多种类型,简单的后门可以在系统中创建新账号,方便黑客进入。复杂的后门可以绕过系统的安全认证而取得系统读写权限等。Android系统中有一款名为kill switch的远程控制软件,可以远程入侵系统,删除用户设备中的应用程序和数据。2014年7月,iOS研发人员乔那森披露了多个后门,其可以从iPhone中提取大量数据,如用户的地理位置信息,这些是在用户毫不知情的情况下运行的,而且也无法被禁止。美国“棱镜门”揭秘者爱德华·斯诺登也曾表示,美国国家安全局可以在iPhone关机的情况下通过麦克风监听用户。

操作系统的漏洞主要是指系统本身在设计上存在的问题或技术缺陷,漏洞可以被黑客利用,通过植入木马、病毒等恶意软件攻击或控制整个系统。Android系统的开源和开放性特点使得恶意软件问题愈发严重,2013年

Android系统的恶意软件有804种, 占所有移动终端恶意软件的97%。中国软件测评中心对国内各种渠道的425万余个应用软件进行测评发现, Android平台的移动互联网应用软件恶意扣费、远程控制、隐私窃取、恶意传播、资费消耗等恶意行为非常普遍, 80%的手机恶意软件至少存在两种或两种以上恶意行为。

Android系统向开发者提供了大量的API和开发工具包, 但是对于API的使用缺乏完善和有效的授权机制和代码签名机制, 这就给各种恶意代码滥用系统API进行违法活动创造了机会。有很多的应用程序滥用前台服务接口(Service.startForeground() API)使应用程序常驻后台, 不能被杀死, 又通过制造一个异常的通知对象, 躲过操作系统的通知管理器(notification manager), 不被用户察觉, 威胁着用户的隐私安全。虽然在Android 4.3以后提供了正在运行的应用程序的知情权和处置权, 但只是治标未治本。

## 2 自主的智能终端操作系统

2013年曝光的棱镜门事件暴露了国外情报机构利用智能终端操作系统不断搜集大量用户的通讯录、短信、邮件、照片、位置等信息, 对用户隐私及国家信息安全造成很大的危险。要实现智能终端操作系统的安全, 必须对操作系统的自主访问控制、强制访问控制、身份鉴权、数据完整性、可信路径等方面提出安全技术要求。2009年国家“核高基”重大专项首次将智能终端操作系统基础软件的研发列入专项, 从国家高度思考移动互联网的关键环节如何保证国家信息的安全。发展自主的智能终端操作系统, 才能避免国外机构利用操作系统的后门程序危害我国信息安全和个人信息安全, 并可以掌控系统软件的发展路标, 为我所用。同时, 基于自主操作系统构建生态体系, 建立完善的应用签名机制和API授权机制, 尤其在特殊行业和特殊领域, 需要构建更为严格的应用管控机制, 最大限度地避免各种安全问题发生。

### 2.1 国内智能终端操作系统的现状

国内厂商在智能终端操作系统研发方面起步较晚, 受限于市场现状和技术能力, 开发的形式主要是基于Android系统进行二次开发, 在操作系统的浅层进行修改定制, 围绕应用层进行创新, 融入了个性的用户界面(UI), 提供了一些应用接口标准, 内置特色的移动互联网业务, 百度、阿里巴巴、小米等互联网巨头都推出了基于Android系统的个性化手机操作系统。这种方式虽然可以兼容

Android的生态系统, 顺应Android的潮流, 但是直接受制于Android系统的演进策略, 而且用户界面只是Android生态中的一环, 不是操作系统, 因而不能解决操作系统的安全问题。同时, 二次开发后的Android系统新的分支同样具有原生Android系统的设计缺点和安全隐患等问题, 手机产品严重同质化, 手机功能设计缺乏创新, 在应用研发方面很难做到与操作系统进行深度集成创新。从长远来看, 谷歌将逐步收权, 推出统一的UI设计标准, 这将造成定制化Android系统的发展越来越窄, UI和操控模式也将趋同。

### 2.2 TIOS

TIOS (trust internet operating system, 可信互联网操作系统)是在国家十一五、十二五“核高基”重大专项支持下进行的研发, 以Linux内核为基础, 具备清晰的分层体系架构, 支持多任务和多应用运行, 系统易于终端产品适配开发, 可扩展性好, 支持多种网络制式, 具有自主、开放、安全、高效的特点。

TIOS包括内核(kernel)、BSP(board support package, 板级支持分组)层、GUI(图形用户界面)图形交互系统、系统支撑库、framework应用开发框架和应用软件。

- kernel: TIOS内核采用开源的标准Linux kernel V2.6或以上版本, 主要功能包括进程管理、定时器、中断管理、内存管理、模块管理、文件系统、设备驱动程序、进程间通信、网络管理、系统启动等操作系统功能的实现。
- BSP: BSP是介于硬件物理设备和TIOS framework框架之间的中间层软件, 其主要目的是为了屏蔽底层硬件的多样性, 完成初始化底层硬件、检测系统硬件是否正常、加载TIOS并启动系统运行等操作。
- GUI图形交互系统: 包括窗口控件、消息机制、图形图像、语言文字、资源处理、输入法等。
- 系统支撑库: TIOS系统支撑库提供各种功能库, 这些功能库在系统中被各种功能组件使用。它们通过应用程序框架为开发者提供服务。实现基础的系统支撑功能, 主要包括libc、多媒体编解码库、OpenGL ES、SQLite、webkit、字体库等。
- framework应用开发框架: TIOS framework应用开发框架采用了通用的应用——视图模式, 基于事件驱动的消息循环实现。framework支持应用所需消息循环和消息分派机制, 并通过窗口向用户呈现相关信息及响应用户交互。framework还为开发者提供各类应用组件, 这些组件是介于上层应用软件、系统支撑库以及GUI之间的系统软件, 它可以屏蔽底



层系统并为上层应用程序提供多种功能接口和服务支持,具有跨平台的特性。常见的 TIOS 应用组件包括电话服务、数据服务、多媒体服务等,TIOS 还支持第三方功能组件的移植和管理。

- 应用软件:包括基础应用软件集、运营商定制软件集和第三方应用软件 3 类。TIOS 通过提供开放的应用开发工具,指引开发者参与应用开发。

### 2.3 安全加固的 TIOS

相比国外操作系统,TIOS 在安全性上具有天然的优势,可以满足大部分普通用户的移动安全需求。针对重要的政企行业客户的特殊安全需求,以自主可控 TIOS 为核心,采用国密级硬件安全技术,增强六大类安全功能、九大安全应用,并在云端采用可信移动应用软件下载平台、安全云服务平台、移动终端管理平台,配合打造覆盖硬件、系统、应用、云端服务的端到端整体移动安全解决方案,如图 1 所示。

智能终端系统安全是一个系统工程,需要从硬件底层就考虑必备的安全硬件芯片和安全手机设计架构。在 TIOS 的系统架构逐层进行安全加固,主要包括在内核层采用安全内核和安全启动技术,防止非法提权和非法刷机;在通用功能库增加安全访问控制和安全算法库;在 GUI 层增加安全输入输出控制;在应用框架层采用安全 API,提供安全应用运行环境等。

TIOS 加固后可确保系统自身安全,提供以下六大类安全功能。

- 系统完整性保护:提供安全启动、刷机管控、系统升级管控,终端启动时利用安全硬件检测操作系统的合法性,非法系统刷机、升级后,系统将无法启动。
- 应用软件可信管控:TIOS 应用开发采用了 C/C++ 语言,反编译困难,对应用程序安装进行管控,并配合可信应用商店机制,从应用开发、应用签名和审核、应用分发到应用安装进行全流程控制,避免过程中引入病毒,确保应用安全。
- 用户数据保护:提供个人信息保护机制,防止个人敏感信息的泄露,支持个人私密空间设置,对通讯录、短信、邮件、照片等提供密码保护。
- 系统安全调用控制:从底层对敏感的无线网络功能(Wi-Fi/移动通信网络/蓝牙/GPS)和数据采集功能(拍照和录音功能)进行控制,防止应用后台打开摄像头、麦克风、GPS 等设备进行非法监听和非法定位。
- 终端丢失管控:对终端开机登录进行高安全级加密增强,防止他人非法解锁手机获取隐私机密信息。通过远程锁机、远程销毁、手机定位机制,协助找寻丢失的手机,在必要时可远程锁定手机或销毁手机数据以避免数据泄露。

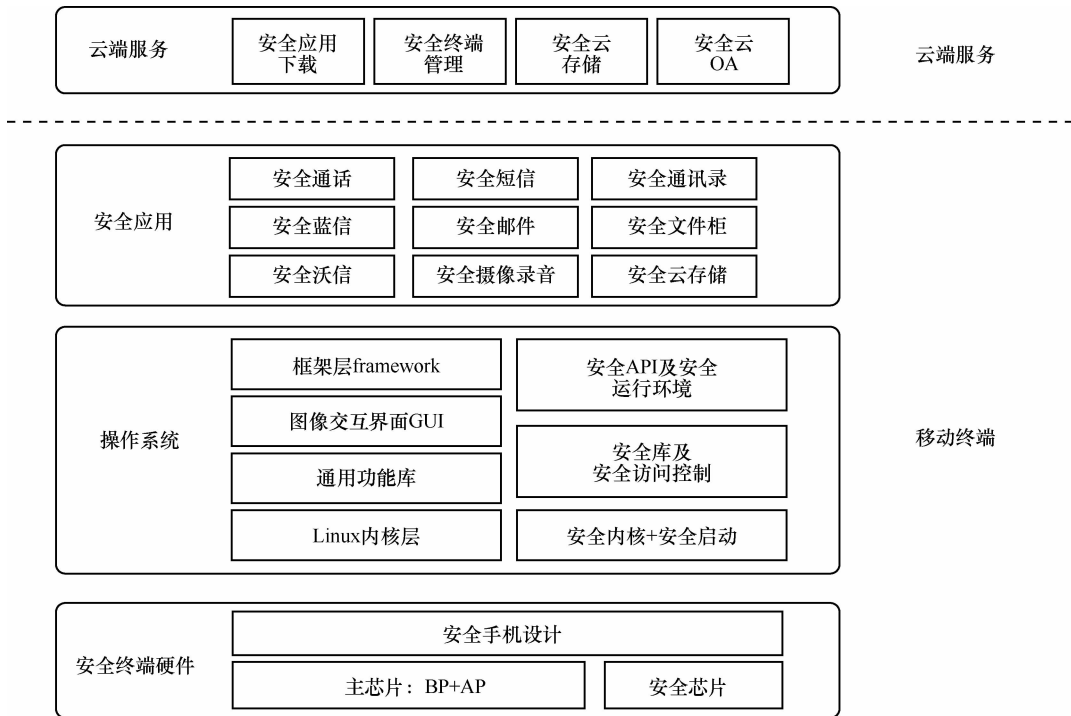


图 1 TIOS 的系统安全加固架构

- 防范网络攻击:通过建立网站白名单等机制,控制由访问不安全网站引起的木马网络攻击。

TIOS 针对最常用的基础应用,提供九大安全应用:安全通话、安全短信、安全通讯录、安全邮件、安全文件柜、安全云存储、安全摄像录音、安全蓝信、安全沃信。九大安全应用均采用国密级硬件安全技术,采用国密级对称、非对称算法对通信内容和本地存储的文件内容进行加密,从而进一步增强用户移动安全。

智能终端的安全同样还需要安全可信的网络云端服务配合,主要包括:可信应用商店提供的安全应用下载;安全终端管理提供安全策略、安全升级、丢失管理等服务;安全云存储提供可靠的网络备份与恢复机制;安全云 OA 提供安全便捷的移动办公服务等。

### 3 终端操作系统的多层次安全需求

随着用户对智能终端的需求越来越多,用户对操作系统的安全越来越重视。但是安全本身是个相对的概念,而且不同用户的安全需求也是不同的,针对用户的多层次安全需求,可以按照需求进行细分,为各类用户群体提供不同安全级别的解决方案。对于普通大众用户来说,首先关注操作系统是否具有良好的应用生态环境、是否操作便捷、是否能够带来良好的体验等方面,其安全需求主要围绕防隐私泄露、防恶意扣费、防病毒等,针对这种需求可以为用户提供应用安全管控措施提升安全性;对于移动商务用户来说,更关注防账号和密码泄露、防仿冒应用、防商业机密泄露、是否能够方便地提供安全的移动办公和数据管理等;对于涉及国家安全的政府和机构的敏感用户来说,关注防政务、命脉行业等机密的泄露,这种高级别安全需求要求提供安全可信的操作系统、可信的应用软件及云服务,甚至涵盖安全芯片和其他硬件设备在内的安全方案,全面保护国家重要机构和行业的信息安全。通过对用户的安全需求进行分级,提供不同的安全方案,既能够满足用户的安全需求,又能够满足用户的业务体验要求。

### 4 结束语

本文介绍了智能终端市场和主流操作系统发展现状,分析了现有操作系统存在的安全威胁。基于国内自主操作系统,提出了安全加固的 TIOS 解决方案,安全加固的 TIOS 能提供六大类安全功能、九大安全应用。最后,分析了终端操作系统的多层次安全需求,为各类安全手机开发提供参考。

### 参考文献

- 1 严斌峰,侯玉华,吴静.中国联通自主产权 TIOS 智能终端操作系统.信息通信技术,2012(4): 52~57  
Yan B F, Hou Y H, Wu J. TIOS intelligent terminal operating system of China Unicom's independent property rights. Information and Communications Technologies, 2012(4): 52~57
- 2 崔伟男,闵栋.移动智能终端操作系统发展趋势分析.电信网络技术,2013(5): 1~4  
Cui W N, Min D. Analysis of the development trend of mobile intelligent terminal operating system. Telecommunications Network Technology, 2013(5): 1~4
- 3 侯玉华,韩玲.3G 终端软件平台发展现状和趋势.移动通信,2010(17): 51~55  
Hou Y H, Han L. Present situation and development trend of the 3G terminal software platform. Mobile Communications, 2010(17): 51~55
- 4 符易阳,周丹平.Android 安全机制分析.信息网络安全,2011(9): 23~25  
Fu Y Y, Zhou D P. Analysis of the security mechanism of Android. Netinfo Security, 2011(9): 23~25
- 5 张玉清,王凯,杨欢等.Android 安全综述.计算机研究与发展,2014, 51(7): 1385~1396  
Zhang Y Q, Wang K, Yang H, et al. Survey of Android OS security. Journal of Computer Research and Development, 2014, 51(7): 1385~1396
- 6 孙奕.Android 安全保护机制及解密方法研究.信息网络安全,2013(1): 71~74  
Sun Y. Android security protection mechanism and decryption. Netinfo Security, 2013(1): 71~74
- 7 陈佳霖,王轶骏,薛质.iOS 系统数据安全研究.信息安全与通信保密,2012(8): 100~102  
Chen J L, Wang Y J, Xue Z. Study on iOS data security. Information Security and Communications Privacy, 2012(8): 100~102
- 8 李柏岚,谷大武,李卷儒等.iOS 备份机制中隐私威胁问题的分析.通信技术,2012, 45(2): 25~28  
Li B L, Gu D W, Li J R, et al. Analysis on privacy threats in iOS backup mechanism. Communications Technology, 2012, 45 (2): 25~28
- 9 赵金龙,王莉娟,惠合意.iOS 手机安全漏洞防范研究.电脑知识与技术,2013(34): 7725~7726  
Zhao J L, Wang L J, Hui H Y. Research on security vulnerability prevention of iOS mobile phone. Computer Knowledge and Technology, 2013(34): 7725~7726
- 10 逯全芳,唐杰,文红.Android 移动智能终端操作系统安全机制的安全性评估.信息安全与技术,2013(8): 54~58  
Lu Q F, Tang J, Wen H. The evaluation of security mechanism based on Android mobile intelligent terminal operating system. Information Security and Technology, 2013(8): 54~58

(2015077-6 接排在 2015074-9 后)