doi: 10.3969/j.issn.1671-1122.2012.01.016

移动智能终端安全威胁分析与防护研究

彭国军，邵玉如，郑祎

（武汉大学计算机学院，湖北武汉 430072）

摘 要： 文章调查分析了移动智能终端的发展趋势，论述了当前移动智能终端的安全现状及远程木马控制、话费吸取、隐私窃取等典型安全威胁，重点探讨了恶意软件植入、固件植入、手工植入、捆绑植入、诱骗下载等手机恶意软件的危害和常见植入方式。文章研究了目前移动智能终端的安全防护技术、安全产品及其缺陷，并对未来移动智能终端及移动互联网安全攻防的发展趋势做出了分析与展望。

关键词： 智能终端；安全威胁；信息安全；隐私防护

中图分类号： TP393.08 **文献标识码：** A **文章编号：** 1671-1122（2012）01-0058-06

Mobile Intelligent Terminal Security Threat Analysis and Protection Research

PENG Guo-jun, SHAO Yu-ru, ZHENG Yi

(*Wuhan University Institute of Computer, Wuhan Hubei* 430072, *China*)

Abstract: This article investigates and analyzes the development trend of mobile intelligent terminals, discusses the current security situation and typical security threats, such as remote controlling Trojan, illegal charges, privacy theft, on mobile intelligent terminals. It focuses on a variety of the common implanting methods of malware, including firmware implanting, manual implanting, integrated implanting, misleading downloads, and so on. Besides, this article researches the technology of privacy protection on mobile intelligent terminals and security protection tools and their defects. Finally, for the future of attack and defense on intelligent terminals and mobile Internet, this article puts forward some novel opinions.

Key words: intelligent terminals; security threats; information security; privacy protection

0 前言

随着信息技术的不断发展，移动终端已成为生活工作中与人们关系最密切的电子设备。从最初的手机，到PDA，再到如今3G时代的智能手机、平板电脑、电子书和车载导航设备等，移动智能终端越来越普及，在形式上和功能上发生了巨大的变化：形式上越来越多样化，功能上越来越丰富，越来越智能化。工业和信息化部的数据显示，2010年全球移动终端出货量达16亿部，同比增长52%[1]。

手机作为人们必不可少的通信工具，是目前移动终端市场最重要的组成部分，销售数量呈现不断增长的趋势。虽然普通的功能型手机仍然占据着大部分低端市场，但是不可忽视的是，移动互联网时代已经到来，性能更强劲、娱乐性更好、上网速度更快、用户体验更友好的智能手机越来越受到用户的青睐。

根据市场调研机构Gartner发布的最新统计报告显示[2]，2011年一季度全球手机销售量共4.278亿部，与去年同期相比增长了19%，其中智能手机销量超过1亿部，同比增长了85%。而智能手机也因此在整体终端销售比例上达到了20%至25%。到2011年底，全球移动连接数将达到56亿，较2010年的50亿增长11%。而2011年移动数据业务收入将达到3147亿美元，较2010年的2570亿美元增长22.5%。

收稿时间： 2011-12-15

基金项目： 国家自然科学基金[61103220]、中央高校基本科研业务费专项资金[6082013]、湖北省自然科学基金[2011CDB456]

作者简介： 彭国军（1979-），男，湖北，副教授，博士，主要研究方向：恶意代码、网络及信息系统安全等；邵玉如（1990-），男，山东，本科，主要研究方向：移动智能终端安全；郑祎（1989-），男，湖北，硕士研究生，主要研究方向：移动智能终端安全。

在如此广阔的市场前景下，国内外的众多IT企业纷纷发布了自己的软件或者硬件产品，移动智能终端领域竞争激烈。苹果公司发布了搭载IOS系统的iPhone和iPad等系列的终端设备，谷歌领衔开发的开源Android系统被大多数知名终端制造厂商所采用，微软的Windows Phone、RIM公司的Blackberry、老牌手机厂商诺基亚的Symbain平台等都得到了广泛应用；国内企业也不甘落后，阿里巴巴公司2011年推出了阿里云手机，小米公司的MIUI和小米手机销售情况异常火爆，备受用户追捧。

1 移动智能终端安全现状及典型安全威胁

1.1 安全现状

移动智能终端与人们关系密切，在生活和工作中使用频率非常高，并且有别于传统PC平台的是，大部分移动智能终端是实时在线、用户随身携带使用的，因此涉及到用户大量的隐私数据。另外，智能手机的许多功能和服务是涉及用户资费的，与用户的经济利益直接相关。还有，根据瞻博网络全球威胁监控中心（Juniper Global Threat Centre）最新发布的数据显示[3]，目前移动智能终端已经被大量应用于商务领域，76%的用户使用智能手机和平板电脑获取敏感的商业情报。

许多不法分子已经将视线由传统的PC平台转移到了移动智能终端上。一方面，受经济利益的驱使，不法分子大量制造并传播恶意扣费软件，给用户造成了极大的经济损失；另一方面，出于不可告人的目的，不法分子诱骗用户安装手机木马或间谍软件，在用户不知情的情况下收集用户的隐私数据，包括联系人、短信、通话录音甚至背景声音录音，地理位置信息等，严重侵犯了用户的个人隐私，甚至有可能从中窃取商业机密或政府情报。

针对移动智能终端的恶意软件增长速度是非常惊人的。瞻博网络全球威胁监控中心的数据还显示，2009-2011年，针对智能手机的恶意软件数量增长了250%。Android平台作为当前市场占有率最高的智能终端操作系统（截止2011年11月已达到43%），恶意软件增长更是达到了惊人的472%。近日，移动安全服务企业－北京网秦天下科技有限公司发布的《2011年第三季度全球Android手机安全报告》数据也显示，2011年第三季度查杀到的Android手机恶意软件及其变种达到2703款，其中新增恶意软件1492款，直接感染手机216万部。受影响的区域方面，中国大陆以超过47.3%的感染比例位居首位（国内北京市位居首位），北美加利福尼亚州安全形势严峻，欧洲监测数据显示，英国Android恶意软件呈泛滥趋势。在感染对象方面，部分移动智能终端恶意软件已经具备了同时感染用户的智能手机及平板电脑的能力。例如，2011年8月18日，名为“Ginger Master”的Android恶意软件被发现，该款软件可以同时感染用户手机及平板电脑。

可见，目前移动智能终端领域的安全问题日益严重，用户的隐私和财产安全、企业商业机密和政府情报等受到了严重的威胁。

1.2 移动智能终端的典型恶意软件及其安全威胁

恶意软件是目前移动智能终端上被不法分子利用最多、对用户造成危害和损失最大的安全威胁类型。智能终端操作系统的多任务特性，为恶意软件在后台运行提供了条件，而用户对恶意软件的运行毫不知情。数据显示[4]，目前Android平台恶意软件主要有四种类型：远程控制木马、话费吸取类、隐私窃取类和系统破坏类，其具体比例如图1所示。

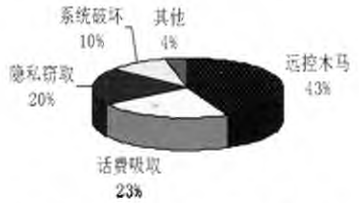

图1 Android平台各类恶意软件比例

1.2.1 远程控制木马

远程控制木马可以接收攻击者远程发送的各种指令，进而触发恶意行为。与其他恶意软件在威胁方式上有较大不同，其威胁是动态的、可变的，恶意行为的类型根据攻击者下达的具体指令的不同而改变，因此使用户层面临着多个层次的安全威胁。远程控制木马的控制方式和工作原理如图2所示。

图2 远程控制木马工作原理

1）隐私窃取。根据攻击者的指令，木马可以搜集用户的短信内容、联系人、通话记录、手机IMEI码、当前位置坐标等数据上传到指定的服务器上。有些木马接收到指令后，甚至可以进行通话录音和背景声音录音，从而达到通话监听和背景声音监听的目的。2）吸费扣费。很多远程控制木马同样具有话费吸取的功能，攻击者在指令中给出增值业务号码，控制手机发送短信进行定制。与一般话费吸取软件不同的是，增值业务号码是可以根据攻击者指令更换的。3）恶意推广。远程控制木马能够接收攻击者的指令，连接到指定的下载服务器，下载恶意推广的软件、广告图片等，还能自动启动浏览

器访问特定的恶意推广网站。4）更新和下载其他恶意软件。为了避免安全防护软件的查杀，攻击者可以控制木马连接到更新服务器进行更新。还可以下载更多种类和数量的其他恶意软件，进而对用户造成更加严重的危害。

攻击者对木马的远程控制主要有两种方式：基于短信的控制和基于网络的控制。基于短信的控制是攻击者向安装有远程控制木马的手机发送含有特殊指令的短信，木马接收后进行解析并执行。基于网络的控制是木马通过与控制服务器进行网络通信获取指令并解析执行。基于网络可以进行批量监控和指令下达，因此被绝大多数的远程控制木马所采用，另外也有少数木马采用了两种方式结合的方法。

“Geinimi”是一款功能全面的典型的Android远程控制木马。根据国外权威移动安全公司Lookout发布的分析报告[6]，“Geinimi”能够根据指令，实现读取手机短信发送到远程服务器，发送删除短信，后台拨打电话，后台下载文件，打开系统浏览器访问指定URL等恶意功能。而且，命令和数据在传输过程中使用DES算法和指定密钥进行了加密。

1.2.2 话费吸取软件

话费吸取软件定时在系统后台发送短信到增值业务服务提供商，大量定制增值业务，或自动拨打指定增值业务号码，并且能自动拦截相关业务定制后的确认短信和运营商的资费提醒短信，暗地里“吸取”用户的资费。

“安卓老虎机”是一款疯狂吸费的Android恶意软件，分析表明[5]，该恶意软件以10秒一次的高频率触发恶意扣费行为，自动删除短信发送记录及运营商的确认短信，完全剥夺了用户对手机资费的知情权，用户几乎不可能在第一时间得知自己已被扣费。

1.2.3隐私窃取

有一些恶意软件能实现窃听功能，监听用户的通话录音和背景环境声音，并给攻击者留下后门，使手机沦为黑客的“肉鸡”。

“金雕”（Android.Hack.GoldenEge）是一款功能全面，设计精巧的Android后门病毒[7]。“金雕”后门安装到Android手机之后，不会留下任何图标。后门会实现自动启动，受窃听者短信指挥实现监听短信内容和通话记录的功能。当监听到手机通话时，病毒会启动录音服务进行录音，通话结束后停止录音。然后“金雕”病毒自带的邮件引擎再将录音文件发送到窃听者邮箱。

还有一些移动智能终端上的远程监控软件，虽然开发的最初目的和设计用途并不一定是恶意的，但是一旦被不法分子作为间谍软件非法利用，也将会对用户隐私、企业和政府机密带来严重威胁。

“Kidlogger”[8]是国外一款用于家长控制孩子上网的产品，并推出了Android平台的版本，能够记录几乎所有的手机操作。除了短信、电话和联系人等常规信息，甚至可以记录剪贴板数据、Wi-Fi和USB连接记录、键盘按键记录等，根据监控者的设置，定时上传到服务器上，监控者可以登录到服务器上进行查看。

1.2.4 系统破坏

绝大多数系统破坏类恶意软件都会非法获取系统的最高权限，即Root权限。获取最高权限后，恶意软件可以强行结束安全防护软件的进程，将自身程序移动到系统程序目录以伪装成系统应用，使自己无法被卸载，破坏了用户的手机系统。

1.2.5 其他

此外，还有许多其他种类的恶意软件，比如仿冒正规软件的诱骗欺诈类程序，制作者不以牟利为目的的资源消耗类程序等，也严重影响了用户的正常使用和手机系统的安全。而且，随着设计和编写技术的不断提高，许多恶意软件的恶意行为趋于多样化，同时具有多种恶意行为特征，给用户造成了多种威胁。

2 手机恶意软件植入手段及其背景分析

2.1 “越狱”及其安全隐患

2.1.1 “越狱”的背景

出于安全的考虑，许多智能终端操作系统对用户和应用程序的权限进行了限制。正常情况下，用户和非系统应用程序仅在系统中拥有较低的权限。对于IOS设备和Windows Phone等设备来说，没有经过官方授权的应用程序是无法运行的，所以用户只能安装和使用在官方的应用商店（如苹果的App Store）中下载的软件；对于Android终端设备，用户只能安装设备生产商提供的系统固件。许多优秀的应用软件为了更大发挥手机的性能，会涉及系统底层的操作，必须要“越狱”后才能正常使用。

对于种种权限限制，许多用户在使用中感到非常不方便，因此就有黑客利用系统漏洞，开发了可以破解权限限制的工具提供给用户使用，用户通过这些工具可以获得并使用系统最高权限——Root（管理员）权限，这就是所谓的“越狱”（在Android系统中，也称“越狱”为Root）。下面以Android系统为例，说明“越狱”的原理和过程。

2.1.2 “越狱”原理分析

Android系统是建立在Linux内核的基础上的，继承了Linux基于用户和属组的权限控制方式。每个应用程序都是一个用户，在系统中都有自己唯一的ID（Root的ID为0）。对于涉及系统底层的操作，普通用户权限不够，不能直接执行，而是切换成Root以Root的身份才能执行。完成用户切换是由系统/system/xbin目录下的su程序完成的。

通过对 Android 2.2 系统 su 源代码的分析（su 程序的源码在源代码的 /system/extras/su 目录下），我们发现如下关键代码，如表 1 中所示。

表1 Android系统su程序关键代码

```
64  if (myuid != AID_ROOT && myuid != AID_SHELL)
    {  // 非 root 并且非 shell 用户
65  fprintf(stderr,"su: uid %d not allowed to su\n", myuid);
66  return 1;   // 程序结束
67  }
68
69  if(setgid(gid) || setuid(uid)) {  // 切换为 root，uid 和 gid 之前已被赋值为 0
70   fprintf(stderr,"su: permission denied\n");
71   return 1;
72  }
```

由表 1 中代码可以看出，在切换成 Root（69 行）之前，对执行 su 的用户进行了判断（64 行），如果当前用户的 ID，即 myuid 不等于 AID_ROOT 也不等于 AID_SHELL，也就是当前用户不是 Root 用户也不是 Shell 用户，则程序直接退出。这样就达到了过滤请求的目的，对用普通用户切换到 Root 的请求给予拒绝。

“越狱”时，使用修改后的不过滤切换请求的 su 程序替换系统原有 su，使所有程序都能够切换成 Root，执行所有涉及底层的操作。而执行这些的操作的前提，也是要获得 Root 权限，这时只能利用某个系统漏洞，通过运行针对这个漏洞的 exploit 程序来获得。“越狱”的整个流程可以用图 3 来表示。

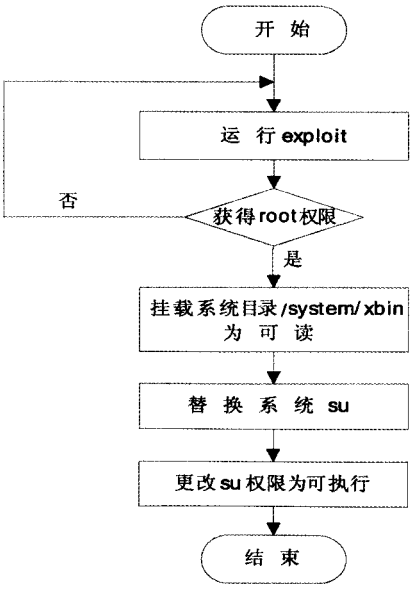

图3 Android系统“越狱”过程

“越狱”之后，所有的应用程序均能通过新的 su 程序来切换成 Root，执行之前不能进行的操作。

2.1.3 “越狱”的安全隐患

用户可以安装没有经过官方审查和授权的软件到“越狱”后的 IOS 和 Windows Phone 中，也可以为 Root 后的 Android 手机更换第三方开发者开发的 Android 固件（称为“刷机”）。

“越狱”后的权限提升虽然能让用户和应用程序进行更多的操作，但是与此同时，由于打破了系统原有的安全机制，用户无法保证未授权的软件中是否含有恶意代码，也无法保证第三方开发者开发的系统固件中是否被植入恶意软件，而且第三方开发者发布的系统固件往往比官方发布的版本有更多的安全漏洞。Lookout 2011 年 6 月发现了木马“jSMSHider”[6]，它能利用第三方 Android 系统中的签名漏洞执行恶意行为，主要影响的就是那些安装了第三方 Android 系统或者被“越狱”过的 Android 手机。

更为严重的是，如前文中关于对系统破坏类恶意软件的说明，一旦恶意软件非法获得了 Root 权限，其破坏力和威胁性大大增强。

2.2 恶意软件植入方式分析

2.2.1 恶意软件伪装成正常软件通过软件分发网站植入

对于目前受恶意软件侵害最为严重的 Android 平台，恶意软件的泛滥不仅与其较高的市场占有率有关，也与 Android 应用程序安装包的特性有关。Android 系统的软件安装包非常容易被反编译而直接得到源代码，所以不法分子可以轻易将恶意代码插入到正常的应用软件中去，然后重新编译发布。许多恶意代码嵌入在时下非常热门和流行的应用软件中，通过论坛和非官方的应用商店进行大范围传播。

以国内为例，随着 Android 用户的迅速增长，出现了许多相关的 Android 论坛，很多国内开发者在坛上发布自己开发或者汉化、破解的应用，免费提供给用户下载安装。另一方面，由于国内访问谷歌官方的 Android 应用商店 Android Market 速度较慢，且应用商店的设计并不符合大多数中国用户的使用习惯，出现了许多“本土”的第三方应用商店。

因为缺少严格、专业的审核机制，难以保证在论坛和第三方应用商店上发布的软件的安全性。报告数据显示[4]，手机论坛的危险指数在不断上升，以 37% 的比例成为传播恶意软件的重灾区，29% 的用户通过第三方应用商店下载而感染恶意软件。

2.2.2 固件植入

“越狱”后的 Android 手机由于没有了权限限制，用户可以进行“刷机”操作。大多数用户“刷”的是经过修改、美化的第三方 Android 系统固件，恶意软件就可能随着这些第三方 Android 系统固件植入到用户的手机中。通过固件植入的恶意软件伪装成系统程序，隐蔽性更好，更不容易被用户察觉。而且，卸载随固件安装的程序是需要系统的最高权限的，但是绝大多数的安防软件不会主动获取手机的最高权限，即使发现也无法清除这种恶意软件。虽然目前已发现的通过固件植入的恶意软件较少，但如“白卡吸费王”[9]，其对用户的危害性却更大。

2.2.3 系统漏洞植入

近日，苹果产品安全问题专家、Accuvant Labs 的研究员查理米勒(Charlie Miller)发现苹果 IOS 平台存在一个安全漏洞[10]。攻击者可能会利用这个漏洞通过一些恶意软件在用户的苹果产品上悄悄安装恶意程序，进而窃取用户隐私或破坏用户数据。他还开发了一款恶意软件原型“Instastock”来测试该漏洞，上传到了苹果 App Store 应用商店，且通过了苹果的安全审批。

2.2.4 手工植入

对于具有间谍软件性质的监控类软件，多是通过社会工程学等手段，手工植入到用户手机中的，如前文提到的家长控制工具“Kidlogger”。还有臭名昭著的“X 卧底”[11]，早期版本也是手工植入的方式。这种植入方法非常有针对性，也往往更关注的是被监控用户的隐私，用来做婚外恋调查、商业和政府机密窃取等不可告人行为。

2.2.5 捆绑植入

Android 应用软件安装包中可以包含原始的、不会被压缩的资源文件(存放在安装包 /res/raw 目录中)，这就给了攻击者可乘之机，他们将恶意软件直接捆绑到普通软件中，普通软件安装后，恶意软件安装包被释放，然后安装到用户手机中。正常的软件安装包和被捆绑恶意软件的安装包对比如图 4 所示。

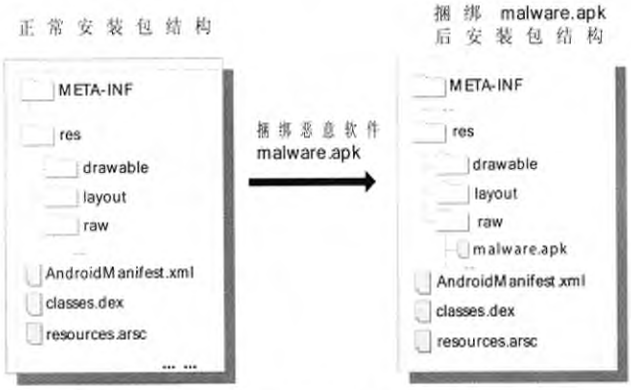

图4 正常软件安装包和捆绑恶意软件后的安装包结构对比

最近发现了一款隐藏在“绿色家园”等应用软件安装包中的木马[12]，正常应用程序安装后，会释放出一个名为 Testnew.Apk 的木马子包，这个子包会自动安装到用户手机上，实施恶意行为。

2.2.6 诱骗下载

诱骗用户主动下载恶意软件的方式比较多，有的是通过发送给用户带有恶意软件下载连接的短信、彩信，并附上诱惑性的说明文字，诱导用户去点击下载；或者打着热门应用软件的名号，欺骗用户，导致用户下载的其实是恶意软件；还有的则是利用二维码，用户使用手机中的二维码识别软件扫描后得到恶意软件下载地址。

2.2.7 已安装恶意软件后台下载

有些恶意软件内部含有“下载器”，安装后还能在后台源源不断地下载其他恶意软件到用户的手机中，如前文提到的恶意软件“Geinimi”。

3 移动智能终端主要安全产品及其缺陷

借鉴传统 PC 平台的安全防护思路，结合移动智能终端的特点，许多安全厂商推出了自己的安全防护产品，在 Android 平台和 Symbain 平台上，已有多款安全防护类软件，譬如 360 手机卫士、金山手机卫士、网秦手机卫士和 QQ 手机管家(原 QQ 安全助手)等。

目前面向智能手机的安全防护技术手段主要可以分为以下种类：病毒木马查杀、骚扰拦截、网络防火墙、软件管理、系统优化、隐私保护、手机防盗。

1) 病毒木马扫描。同 PC 平台类似，手机上的病毒木马扫描也是基于病毒库和特征值匹配技术的。也有些厂商推出了联网“云查杀”来确认可疑软件。如网秦手机卫士就采用了“云+端”的双引擎查杀方式。

2) 骚扰拦截。允许用户将垃圾短信和骚扰电话加入到黑名单中，短信接收或电话呼入时，若号码与黑名单中的号码匹配，则进行拦截。如金山手机卫士，能够拦截广告、诈骗、扣费短信、响一声电话等，防止恶意骚扰。

3) 网络防火墙。同 PC 上的防火墙意义不同，智能手机上的防火墙大多仅仅具有流量统计和限制应用程序进行网络连接的功能，当每月累积流量超出用户设置的限额时，提示用户停止网络连接以节省资费，如 QQ 手机管家的上网管理。

4) 软件管理。严格意义上说这并不是一种安防手段，只是安防软件为用户提供的一个更方便安装卸载应用程序的工具。如 QQ 手机管家，不仅能管理已安装程序和安装包，还具有一站式下载安全绿色的装机必备等软件的功能。

5) 系统优化。查看系统的运行状态，包括内存、CPU 使用率等信息，优化用户的系统速度，清理缓存和垃圾文件，关闭后台运行的进程，如 360 优化大师。

6) 隐私保护。将涉及隐私的短信、联系人、通话记录等内容加密存储到手机特定的位置，防止隐私数据泄露。如金山手机卫士提供的私密空间，能加密保护个人信息，防止他人偷看，保护隐私安全。

7) 手机防盗。一旦用户的手机丢失，可以定位手机的位置，若 SIM 卡被更换，则会发送短信到指定的手机号码。如 360 手机卫士，检测到更换 SIM 卡后自动锁机，远程控制保护隐私。

除此之外，Android 平台上也出现了以“主动防御”而知名的安全防护软件，比如 LBE 小组开发的 LBE 隐私卫士和 LBE 安全大师[13]。采用类似 PC 上进程 Hook 的 API 拦截技术，

LBE 隐私卫士和 LBE 安全大师能够实时监控和动态拦截系统中的敏感操作。

虽然目前安全防护软件众多，在一定程度上能起到保护用户隐私和财产安全的作用。但是，大多安防软件思路类似，功能雷同，并且还有诸多问题和缺陷。

安全防护软件的病毒木马查杀和“云查杀”功能，是基于特征值扫描技术的。一方面，智能手机的物理资源和电池续航能力有限，病毒查杀会占用较多物理资源，加速电量消耗，给用户的正常使用带来较大影响；另一方面，频繁更新病毒库或者“云查杀”需要连接互联网，可能会给用户带来额外的流量费用。

而且，基于特征值的扫描技术依赖病毒库的，对于病毒库中不存在的病毒，便无能为力了。面对每天都会产生的各种新型恶意程序及其变种，这种方法具有不可避免的滞后性。这也使得利用该技术的安全产品的安全防护性能打了大大的折扣。

LBE 安全大师和 LBE 隐私卫士这类“主动防御”安全防护软件，虽然做到了动态拦截敏感操作，但是对于每个敏感操作的放行或者阻止留给了用户去选择。普通用户难以判断敏感操作是否是应用程序的正常行为，也难以判断是否会带来安全风险。这种基于单个 API 的拦截无法自主判断软件的恶意性，这和主动防御基于行为自主分析判断恶意软件是有非常大的区别的。

至于手机防火墙、手机防盗功能也往往没有想象中的有效。由于只能监控流量和限制应用程序对外的网络连接，没有真正做到手机系统与外部网络的隔离，因此手机防火墙根本无法阻止攻击者从外部入侵用户的手机。并且安全防护软件也只是运行在手机中的普通应用程序，一旦系统恢复出厂设置，那么安全防护软件同其他非系统软件一样，也是会被清除的，无法达到手机防盗的目的。

4 移动智能终端及移动互联网安全攻防的发展趋势分析与展望

随着移动互联网的高速发展，“人人时时处处在线”、“人人都是信息源”成为现实，移动智能终端和移动互联网安全将会面临更加严峻的挑战。

从目前的数据和发展趋势可以预测，未来的移动互联网安全攻防仍将围绕移动智能终端展开。移动智能终端将会越来越开放和智能，越来越贴近个人，承载的用户信息会更有价值。同时，移动智能终端不断扩展的办公、支付等业务功能，也会承载更巨大的商业价值。

攻防形式方面，巨大的经济利益将会刺激恶意软件继续增长，在攻击者与安全厂商的博弈过程中，安全厂商将会继续处于被动地位。安全厂商与移动智能终端制造商，系统提供商和移动互联网服务提供商的合作，也许能成为降低移动智能终端及移动互联网安全威胁的有效措施。

相信在未来很长一段时间内，如何做好用户隐私和财产安全的防护，仍将是一个非常重要的课题。移动智能终端用户也应提升自身的安全防护意识，减少各类安全威胁造成的损失。● （责编 杨晨）

参考文献：

[1] 工信部通信信息研究所. 2010-2011 年全球移动终端市场发展研究报告 [EB/OL]. http://www.doc88.com/p-979478996571.html, 2011-09-19/2011-11-10.

[2] Gartner. Gartner Top Predictions for 2011: IT's Growing Transparency and Consumerizatio[EB/OL]. http://www.gartner.com/it/content/1462300/1462334/december_15_top_predictions_for_2011_dplummer.pdf, 2011-12-10

[3] Juniper Global Threat Centre. Malicious Mobile Threats report 2010/2011[EB/OL]. http://www.juniper.net/us/en/local/pdf/whitepapers/2000415-en.pdf, 2011-12-10.

[4] 网秦安全中心. 2011 年第三季度全球 Android 手机安全报告 [EB/OL]. http://www.netqin.com/upLoad/File/baogao/2011Android.pdf, 2011-12-10.

[5]360 安全中心. 360 手机卫士安全播报 - 第二十七期 [EB/OL]. http://shouji.360.cn/securityReportlist/securityReport_27.html, 2011-12-10.

[6] lookout 官方博客. Geinimi Trojan Technical Analysis[EB/OL]. http://blog.mylookout.com/2011/01/geinimi-trojan-technical-analysis/, 2011-12-11.

[7] 金山安全中心. Android.Hack.GoldenEge 分析报告 [EB/OL]. http://m.ijinshan.com/news/20110826.shtml, 2011-12-10.

[8]Kidlogger 官方网站 [EB/OL]. http://www.kidlogger.net/, 2011-12-10.

[9]360 安全中心. 360 手机卫士安全播报 - 第三十一期 [EB/OL]. http://shouji.360.cn/securityReportlist/securityReport_31.html, 2011-12-11.

[10] 360 安全中心. 360 手机卫士安全播报 - 第三十六期 [EB/OL]. http://shouji.360.cn/securityReportlist/securityReport_36.html, 2011-12-09.

[11] 网秦安全中心. 揭秘 X 卧底的前世今生 [EB/OL]. http://www.netqin.com/security/topicinfo.jsp?id=3821, 2011-12-09.

[12] 360 安全中心. 360 手机卫士安全播报 - 第二十六期 [EB/OL]. http://shouji.360.cn/securityReportlist/securityReport_26.html, 2011-12-09.

[13] 隐私卫士 . LBE 官方网站 [EB/OL]. http://www.lbesec.com,2011-11-20/2011-12-10.

资讯

第二届云安全联盟高峰论坛在北京召开

2011 年 11 月，由国际云安全联盟中国分会主办，绿盟科技和启明星辰共同承办的第二届云安全联盟（CSA）高峰论坛在北京隆重召开。本次大会以“融合、协同、探索、创新”为主题，旨在推动国内的云安全交流，分享云安全平台建设和应用经验，探索合理高效的云计算运营方式。来自 CSA、云提供商、运营商、云计算用户等领域的专家就云计算面临的威胁和云安全最佳实践等话题和与会者进行了深入的交流和探讨。（记者 杨晨）