智能手机面临的安全威胁

辛阳[1],韩紫东[1],徐勤[2]

1. 北京邮电大学计算机学院,北京 100876
2. 北京安码科技有限公司,北京 100876

智能手机的广泛普及给人们提供便利的同时也带来了来自移动安全的威胁,由于智能手机与用户的隐私信息紧密相关,导致任何对智能手机的攻击威胁都会被无限放大。智能手机所搭载的系统通用漏洞,包含恶意行为的应用以及无线攻击等新型攻击都是智能手机目前所面临的安全威胁。本文介绍智能手机面临的安全问题,提出相应的防御措施,并介绍移动安全研究的发展趋势。

1 智能手机与移动安全

近年来,随着移动互联网行业的崛起,智能手机在生活中扮演的角色也越来越多样化,手机从打电话、发短信的通信工具发展成为提供多媒体和网络互动娱乐的载体设备。当前,智能手机正以70%的速度高速发展。据统计,未来3年中国智能手机销量,将从现在的4700万部,增长到8000万部;而平均价格则从几年前近4000元,一路下降到2000元左右,而且仍下滑不止。这说明智能手机发展已进入成熟收获期。同时伴随着3G、4G及WiFi技术的成熟普及,智能手机与移动互联网完成了无缝对接。

在移动智能手机阵营中,以Google公司为首的Android系统智能设备和苹果公司的iOS系统智能设备占了移动市场的大部分市场份额,包括手机、平板、手环等智能设备。然而这些智能设备,尤其是智能手机在移动互联网的发展中像一把双刃剑,既扮演了推进移动互联网与人类生活发展趋势的载体角色,同时也给移动互联网中的信息安全问题带来了新的挑战和威胁。

移动安全,是移动互联网崛起背景下带来的新的信息安全问题。移动安全是指移动互联网领域技术发展中面临的移动设备安全、移动应用安全、移动支付安全等多类新型信息安全问题,与传统信息安全问题相比,由于借助移动互联网的相关特性,它明显具有传播速度更快、危害范围更广、主动防御更加困难等特点。由于人们普遍使用智能手机上网、通信、支付等多项功能,智能手机可以说是移动安全威胁的主要载体媒介,其安全从一定程度上决定了移动安全的发展态势。近年来由智能手机安全问题引发的用户信息大面积泄露,移动端病毒木马猖獗导致的用户经济受损、厂商信誉度受损等危害正逐步扩展,更为麻烦的是,即使针对相应类型的移动安全问题厂商进行相应的修补或者系统更新,绝大多数智能手机的使用者由于自身移动安全意识薄弱以及刷机等技术限制,仍使用较为不安全的系统版本或应用,这样便给了许多攻击者利用的可乘之机。

如今,Android和iOS系统走在了智能手机系统的技术前列,相比之下两种智能手机都存在相应的安全问题,但由于系统特性不同,其安全问题及防护方案也不相同。Google公司推出的Android系统是在Linux系统的基础上移植而成,适应兼容了Arm架构下的移动设备及相关驱动的移植特性,和Linux一样,由于Android系统的开源特点,以及Android源码公开、Android应用市场渠道监管不够、系统更新速度快等因素,使得Android智能手机遭受来自系统级,应用级等多方位的攻击威胁。而苹果公司推出的iOS系统是闭源的,并且提供相应的App Store作为应用下载渠道,对于未"越狱"的iPhone手机,用户遭受来自应用的安全威胁与Android相比要少得多,然而作为闭源系统的iOS智能手机同样面临着来自系统级的安全威胁,并且大量用户往往是在受到这类0day漏洞的攻击之后,该漏洞

收稿日期:2016-04-28

作者简介:辛阳,副教授,研究方向为网络信息安全、云计算大数据安全和灾备安全,电子信箱:yangxin@bupt.edu.cn;徐勤(通信作者),副总经理,研究方向为网络信息安全,电子信箱:xuqin@safe-code.com

引用格式:辛阳, 韩紫东, 徐勤. 智能手机面临的安全威胁[J]. 科技导报, 2016, 34(9): 63-68; doi:10.3981/j.issn.1000-7857.2016.09.009

信息才被曝光,随后升级系统进行修复。从某种意义上来说,闭源的iOS系统没有杜绝和预防iPhone智能手机遭受的系统安全问题,而是以通过升级系统的方式来应对。

智能手机和移动安全问题息息相关,对智能手机面临的安全问题加以了解以及采取相应的防护措施,会使移动安全的发展趋势更明朗。智能手机安全问题主要来自系统通用漏洞、恶意应用病毒、无线安全攻击等多个方面。

2 通用漏洞安全威胁

2.1 系统通用漏洞

系统通用漏洞是由于操作系统本身的设计不够完善而造成潜在的一系列安全隐患问题,这些问题一旦被攻击者发现并利用,将造成大批量的用户和厂商遭受损失,原因在于,其一存在问题的操作系统往往用户面广,如Windows,Linux/Unix,Android,iOS等,每种操作系统都有其固定用户,一旦系统本身存在漏洞并被恶意利用,攻击者就如同拿到万能钥匙般通杀几乎所有同类型版本的操作系统,造成大量用户被攻击;另一方面,由于操作系统实际上是特殊的系统软件,并且用户应用及部分系统应用都是安装在操作系统之上,因此一旦系统本身存在通用漏洞,便是能提取高权限的高危漏洞。

从安全防护的角度上来看,系统通用漏洞往往属于0day漏洞,即还没有打补丁的漏洞,攻击者在拿到0day漏洞之后,由于了解该漏洞的人相对较少,便利用其构造恶意攻击,提取系统最高权限后,实现恶意攻击或信息窃取等攻击行为,短期内即对用户造成极大损失。同时地下黑色产业链对0day漏洞的需求也使得很多攻击者将其卖给不法分子,从中牟利,在系统厂商发现漏洞并修补或白帽子提交通用漏洞到确认之前的这段时间内,可能已有数千万的用户遭受了损失,可谓防不胜防。

随着移动设备的普及,大量攻击者的目标由传统的PC系统(Windows,Linux/Unix)转为移动端操作系统(Android/iOS等),然而由于系统开放程度不同,Android与iOS系统面临来自系统通用漏洞的安全问题也并不相同。

2.2 iOS系统漏洞

iOS系统是苹果公司针对其智能设备设计的一款优秀的操作系统,从开放性上来说是闭源的,然而闭源的iOS系统并没有完全杜绝苹果设备的安全性问题,除了手机用户"越狱"后产生的安全问题以外,iOS系统本身也会受到攻击者的攻击研究(如Fuzzing攻击等方式),例如近期的iOS"1970"漏洞,该系统漏洞在搭载64位处理器的iOS8至iOS9.3beta3的系统设备上,通过设置系统时间为1970年5月及更早的日期,触发iOS手机重启变砖的漏洞,而在iOS9.3beta3版本后的系统上,苹果公司修复了这一漏洞,但之后的安全研究人员在iOS9.3正式版系统中又发现该漏洞的问题并没有完全根除,黑客仍可以利用iOS手机连接WiFi存在的一些弱点问题,构造虚假的attwifi无线网络热点,然后搭建一个NTP服务器(伪装成苹果服务器time.apple.com),这样就可以将iOS设备日期变成1970年1月1日。因此可以看出,即使采用了闭源特性的iOS系统也难以避免受到系统通用漏洞的影响。

2.3 Android系统漏洞

Android系统是Google公司推出的一种基于Linux的自由及开放源代码的操作系统(主要用于移动设备),不同于iOS系统,Android系统的推出以其开源性著称。开源的特性帮助Android系统在推出后受到了大量Android开发人员的共同开发与完善,与Google公司预期的一样,Android系统在后续的版本更新过程中完美适应了移动互联网的飞速发展要求,从Android1.x、Android2.x、Android3.x、Android 4.x等版本与2009年开始的多台Android智能手机井喷出现来看,Android系统的发展似乎正朝着一个良好又有利的方向发展。

然而,Android系统及相关智能设备在大量占领市场份额的时候,产生的移动安全问题也随之浮出水面,并且隐隐有随着Android占有率上升而扩大化的趋势。造成这一问题的原因之一,恰恰就是赋予Android系统生命力的开源特性。开源特性是一把双刃剑,由于Android源码的公开特点,对比与iOS系统,攻击者往往不再仅依赖Fuzzing之类的黑盒测试手段来研究系统中的漏洞,可以对不同版本的Android系统源码(包括内核源码)进行深入研究,一旦发现高危的通用提权漏洞或其他的系统漏洞,便可以设计构造相关攻击手段对市场上搭载含有该漏洞的Android版本智能设备进行攻击。可以想象,Google公司在对Android系统开源之初应当预见这一景象,然而大量的智能手机设备在抢占市场份额的同时,形成由Android系统带来的移动安全问题愈发难以控制,那么Android系统中的通用漏洞究竟是怎样产生和存在的?

Android系统的架构如图1所示,是由Android的应用层(Application)、应用框架层(Framework)、系统运行库层(libc,Runtime)及内核层(Kernel)自顶向下的组成。对于普通的Android开发者来说,应用框架层提供的组件、API等开发模块方便了开发者进行Android应用的开发,因此对于攻击者来说,挖掘该层中潜在的通用漏洞,可以针对手机中存在的系统漏洞及相关的应用漏洞进行攻击利用,例如Media Framework信息泄露漏洞(CVE-2015-6628)、通用型提权漏洞(CVE-2015-3636)及通用拒绝服务漏洞等。据统计在2015年Application Framework & Libraries漏洞中,占比最高的3类漏洞是代码执行、溢出和拒绝服务漏洞,分别占比26%、23%和20%。其中,由媒体库引发的代码执行漏洞数量最多,约占全部代码执行漏洞的40%。

通用漏洞危害大的一个主要原因就在于普通用户往往认为只要是从正规渠道下载的应用就不会受到安全威胁,但对于通用系统漏洞来说这种认知是过时的,以代码执行漏洞为例,其中一类攻击是攻击者利用Android某些版本中使用的多媒体框架核心组件Stagefright中存在的漏洞,在多媒体文件解析的过程中,获取到MediaServer进程的权限,再结合其他漏洞提权到

Root权限,从而对智能手机进行非法控制等攻击行为,该通用漏洞的存在使得搭载Android 5.1(5.1系统之后进行了修复)之前所有系统版本的手机设备均受到了威胁。如果说在Framework、libc等层面上存在的漏洞问题还不够直观,那么来自内核层的漏洞安全问题才是Android系统通用漏洞影响如此巨大的一个根本原因。说到Android内核系统漏洞,首先需要了解一下Root这一概念对于Android系统的意义。

使用过Linux/Unix系统的用户对Root这一概念一定不会陌生,如果你是忠实的Windows用户也没有关系,你一定知道Administrator系统管理员的意义,Android系统的Root其实就是获取Android的超级用户权限,换言之,一旦拿到了Root权限,即等于完全控制了整个操作系统。出于安全考虑,设备厂商在出产手机的时候都会关闭Root权限,对于闭源的iOS系统来说,获取设备系统权限的方法只有通过"越狱"的方法,而对于Android设备来说便是Root手机这一方法。虽然Root之后使得Android系统的可玩可操作性大大提升,但是产生的安全问题也随之而来。例如2010年的RageAgainstTheCage漏洞利用Android sdk中的adb工具相关原理及逻辑漏洞,便实现对设备的Root破解提权过程。在Root提权的这一背景下,Android内核的通用漏洞成为攻击者及白帽子重点关注的一个问题。

在Linux内核层面下除了内核通用代码漏洞以外,设备驱动也是产生内核通用漏洞的主要区域。Android内核是基于Liunx内核并面向ARM架构的移动设备进行兼容性移植,因此Linux系统中存在的一些通用漏洞问题在Android内核中同样存在,并且由于移动设备的特殊性,其安全威胁被放大了。例如缓冲区溢出漏洞在Linux系统中的高危害影响在Android 4.0之前的系统版本中仍然存在,Android内核中由于本身处于系统架构的底层,一旦攻击者通过其中存在的缓冲区溢出漏洞,构造shellcode进行提权等操作,便可以直接在内核中获取到Root权限,而对于Android 4.0之后的版本,Google在Android内核中引入了ASLR(Address Space Layout Randomization)技术来对堆、栈、共享库映射等线性区布局的随机化,增加攻击者预测目的地址的难度,防止攻击者直接定位攻击代码位置,达到阻止溢出攻击的目的。但这并不意味4.0之后的Android系统内核就十分安全。内核层的攻击往往来自于那些驱动文件中存在的问题,Android内核WiFi模块栈缓冲区溢出(CVE-2016-0801)可通过发送恶意的无线控制信息包进行利用。该包可能会使内核内存崩溃,并使Android设备暴露于内核级别的远程代码执行风险之中。除了缓冲区溢出漏洞之外,Android内核中的Futex漏洞(CVE-2014-3153)、本地提权漏洞(CVE-2015-3636)等利用内核代码存在的漏洞进行Root提权。从影响效果上来看内核层的通用漏洞效果最直接(提升Root权限),造成的漏洞危害较高。

通过对Android系统的通用漏洞进行介绍以及智能手机受到的相应安全威胁分析,可以看出系统通用漏洞对Android设备的影响很大,那么采取什么措施才能有效防范来自系统漏洞的安全威胁?很遗憾,不论是对于Android或是iOS设备来说,大多数设备使用者或是更高级一些的开发人员都没有办法主动对通用系统漏洞进行防范。

2.4 针对系统通用漏洞的被动防御与碎片化问题

由于闭源的特性,使用iOS系统智能手机的用户在面对系统通用漏洞造成的影响时往往显得手足无措,唯一能做的就是等待苹果公司官方在推送的新版本系统中对该问题漏洞进行补丁升级。而对于Android智能设备的使用者来说,虽然Google公司认为Android系统是开源的,产生相应的安全漏洞也可以由广泛的开源开发和研究人员加以发现并及时修补,但由于Android碎片化的问题过于严重,在市场上的Android系统升级上存在大量的问题版本遗留。即使Android系统的更新速度与安全问题的修复速度相对闭源的iOS系统快,但由于很多普通用户的自身安全意识和技术能力所限,仍然使用相对较落后的Android版本(Android 4.x版本)。造成了解决方案或措施应用上的局限性,从而使得面对系统通用漏洞安全威胁的时候,原本应当更胜一筹的Android系统在效果上反而不如iOS系统的处理。因此在针对系统通用漏洞的防御上,iOS及Android智能设备所

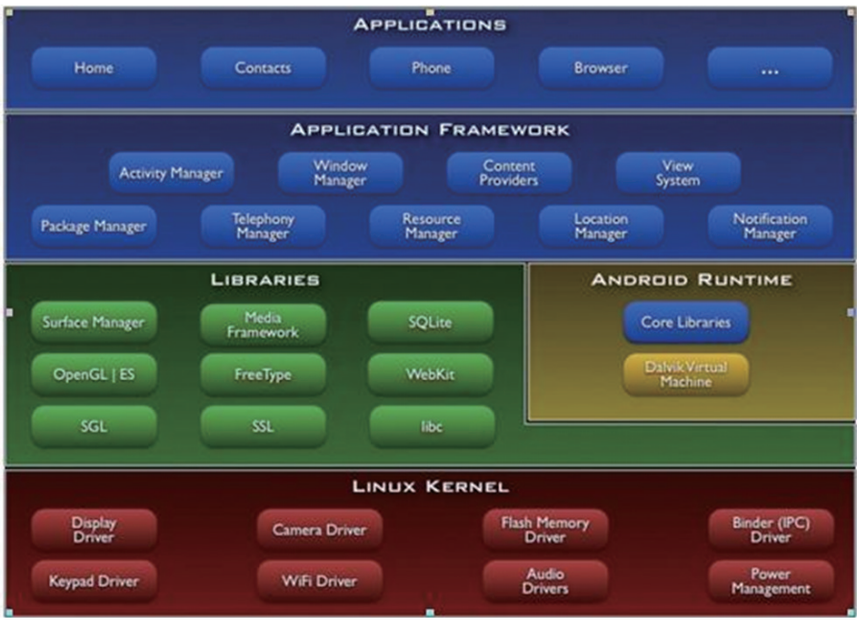

图1 Android系统架构

采用的方式都是一种被动防御的措施，即等待系统更新升级，对相应的漏洞做出修复。

从防御效果上来看，被动防御在面对系统通用漏洞时实在显得有些力不从心，对于iOS系统来说产生的影响和防御的方案尚能接受，而对于Android智能手机来说，无论是面对已经在CVE（Common Vulnerabilities & Exposures）上公布的通用漏洞，还是掌握在攻击者手上威胁更大的0day漏洞，Android系统对其防御效果都不尽如人意。前者的防御方案通过更新Android系统或Android SDK来修补相应的漏洞，解决相关问题，这看似是一种有效的主动防御措施，然而却因为Android市场碎片化（Rom以及设备类型）的问题使得防御效果大打折扣，多数Android智能手机仍遭受着相关的系统漏洞安全威胁（没有及时更新系统版本的能力和意识）；而对于后者来说，0day漏洞形成的APT（Advanced Persistent Threat）攻击本身就难以防范，从这个角度上，只能把希望寄托在致力于漏洞挖掘的那些白帽子身上，只有发现更多未公布的0day漏洞，才能使智能手机设备安全性得到更好的保障和技术支持，即使这仍然是一种被动防御的应对方案。

3 恶意应用安全威胁

3.1 移动恶意应用与Owasp移动恶意行为标准

智能手机受到的移动恶意应用安全威胁除了来自于系统通用漏洞以外还受到恶意应用的威胁。移动恶意应用不同于传统PC端的恶意应用病毒木马，除了破坏性、控制性等特点外，还有着隐蔽性、目的性等新型特点。简单来说原因主要有两点，其一是因为传统PC上的杀毒技术较为成熟，恶意应用需要通过强大的免杀技术来逃过杀毒软件的查杀；另一方面由于移动终端特别是手机的普及，人们将越来越多的个人隐私信息放置在手机上。虽然人们已经具有对PC端的一定安全保护意识，但对于移动端的安全意识还没有那么清晰，给攻击者可乘之机。如果此时相关设备厂商在这方面的防护做的不够的话，那么用户在心理不设防的情况下遭受攻击的可能性就大大提升。

Owasp移动应用恶意行为是SecApp Lab联合OWASP中国、百度、互联网安全研究中心、通付盾等应用安全联盟成员，在对上百万应用安全分析，并参考行业各类资源后，发布的十大移动应用恶意行为，如图2所示。

其中包含了恶意扣费、山寨应用、静默下载、隐私窃取等10类移动恶意行为，包含这些恶意行为的恶意应用在用户的使用过程中给用户造成了不可估量的损害，从这一角度上来说，恶意应用对智能手机安全的威胁也不容小觑，那么对于Android和iOS的智能手机来说，究竟来自恶意应用的安全威胁各自有多少呢？

3.2 三方ROM与电子市场的利弊

对于iOS系统来说，苹果公司对系统和应用的安全管控都十分严格，一方面通过对“越狱”用户的抵制措施，另一方面在App Store（苹果自己的应用电子市场）上加大应用的监管力度，在应用上线前经过严密的审核与检查，虽然使应用上线周期变长了，却在一定程度上杜绝了恶意应用的肆虐。

而开源的Android系统相对来说就差了许多。由于开源的特性，大量的Android开发者进驻Android开发平台，在Android系统发布的很多年里，Android应用市场对电子应用的安全性审核似乎一直都做得不够，这是由于一方面虽然Google有自己的Google Play应用中心来保证应用的安全性，然而却因为种种原因使国内的用户无法享受多数Google服务，这样一来，国内的Android应用便不得不依赖于大量的第三方电子市场，而在这些电子市场中应用的渠道难以保证，很多用户在论坛或者一些应用市场中下载后，就给恶意应用进入用户空间提供了机会；另一方面即使部分用户可以甄别一些应用的可靠性（实际上多数用户很难做到），仍然没法避免恶意应用的存在与攻击，这是因为第三方Rom的存在。

Rom，通俗来说就是刷机包中的只读内存镜像，是Android用户刷机（无论是线刷或是卡刷）都需要的镜像，从某种角度上来说，来自Google原生AOSP编译后的img文件便是最为纯净的Android Rom。那么为什么作为刷机包的Rom会成为恶意应用帮凶之一？这是因为很多厂商或者Rom制作者为了优化Android系统或是适配某些机型的硬件设备等原因，需要对原生的Rom进行修改定制，然后做成自己的第三方Rom放出来给众多Android刷机爱好者体验，例如赫赫有名的CM发行版Rom（CyanogenMod），它提供一些在官方Android系统或手机厂商没有提供的功能，例如：支持Free Lossless Audio Codec- FLAC（无损音频压缩编码）音频格式的音乐、多点触控、从SD外置存储器运行程序等功能。制作三方Rom的作者本意是帮助用户改进对Android系统的体验，然而有着不怀好意的一些人员通过在Rom中进行恶意应用的植入，或者利用有些三方Rom系统本身存在的Root后门进行提权操作，进而

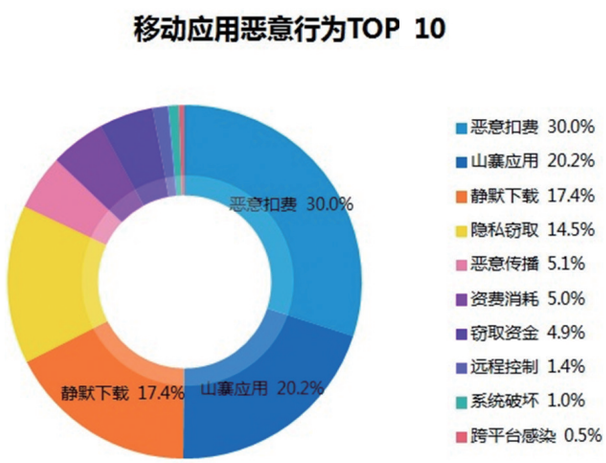

图2 移动应用恶意行为TOP 10

控制用户的手机设备等方式,来达到非法牟利或者破坏行为。这些恶意应用一旦被攻击者植入相应的Rom包中,往往有备份存放在相应的高权限目录下,用户如果下载安装了相应的Rom,在未Root的情况下无法卸载该Rom中植入的恶意应用(权限不够),即使将手机Root之后删除相应的应用,一旦重启手机,Rom包仍会将被删除的应用通过备份重新安装到手机上,形成难以根除的恶意顽固应用,用户只能找到相应的应用备份位置删除或者弃用该Rom。

从以上分析来看,Android的电子市场虽然符合了Android系统开源的特性和精神,给了开发者一个平台来分享应用的同时,也由于恶意应用和第三方Rom的存在给电子市场的安全性带来挑战,也给Android智能手机的安全带来了威胁。

3.3 深层次Rootkit攻击

如果说来自第三方Rom与恶意应用的攻击手段是攻击者侵害用户利益的直接手段的话,那么Rootkit下的内核攻击就是更为高级的攻击技术。Rootkit是一种特殊的恶意软件,其功能是在安装目标上隐藏自身及指定的文件、进程和网络链接等信息,比较多见的Rootkit一般与木马、后门等其他恶意程序结合使用。Rootkit通过加载特殊的驱动,修改系统内核,进而达到隐藏信息的目的。

在Android系统中,多数的设备厂商都会定制自己的内核系统来适配设备的硬件兼容性。从内核上来说,几乎不存在一种通用的内核可以兼容所有厂商的Android手机,但是对于内核的Rootkit攻击并不是完全没有可能。

攻击者通过某种机型的内核(公开内核)进行修改,使其在一定条件下加载可执行模块,如可以在内核中劫持相应的系统调用,使得使用该内核的用户在接到某个攻击号码的来电时,触发相应的恶意行为。由于Rootkit攻击者本身所处的攻击位置较深,权限较高,因此一旦诱骗用户刷了该内核和相应的Rom,便可以做很多事情.

然而虽然Rootkit攻击的效果和威力很明显,但是其带给智能手机的威胁要远小于恶意应用和恶意Rom的威胁,根本原因在于Rootkit攻击依赖的条件过于苛刻了,即要求用户刷入攻击者定制的内核,而定制非模拟器内核本身难度就很大,加之一般的Android用户既不会也没有必要重刷内核,导致攻击者很难锁定并诱导受害者来发出Rootkit攻击,这样一来其传播性和有效性便大打折扣。

那么对于这些恶意应用的威胁,智能手机的用户需要采取怎样的措施来防御?

3.4 对抗恶意应用攻击的主动防御

对于来自恶意应用攻击的威胁,这一次防御主动权掌握在了用户的手中。对于包含恶意行为的恶意应用,用户如果在没有甄别能力的情况下,可以通过来自可靠的电子市场下载渠道来下载应用,从而在一定程度上确保应用的安全可靠性;另一方面,对于热衷于刷机的爱好者来说,选择可靠的发行版Rom可以在一定程度上避免来自恶意应用的安全威胁,并且不要随意下载不明来源的第三方Rom及内核;用户也可以在手机上安装360手机卫士、腾讯手机管家等手机安全软件来对恶意应用进行查杀。与面对通用漏洞的威胁相比,在面对恶意应用时,用户完全可以通过以上主动防御手段尽可能使手机避免来自恶意应用的安全威胁。

4 无线攻击安全威胁

4.1 WiFi时代来临

WiFi是一种允许电子设备连接到一个无线局域网(WLAN)的技术。WiFi这种技术让网民摆脱了有限上网的限制。根据《2015中国移动互联发展指数数据报告》,中国移动智能终端用户规模达11.8亿台。移动智能终端的普及更是加速了WiFi的发展。

大多数人到一个地方,先用手机搜寻WiFi信号成为了一种习惯。打开手机,找出WLAN连接界面,手机就能搜索到各种WiFi信号,有密码的、无密码的、公共的、个人的、免费的、收费的。这些WiFi逐渐成为大部分“低头族”不可或缺的生活要素。WiFi逐渐融入了衣食住行的日常生活之中。吃饭时餐厅会提供免费的WiFi,公交车上只需下载一个软件就可以免费使用,在一些公共场所更有运营商提供的公共热点。为了让信息的流通更加便捷,政府也在主导公共免费WiFi的建设。据报道,贵州省贵阳市全域公共免费WiFi项目二期一阶段近日已建成进入验收阶段,中心城区主干道实现免费WiFi全覆盖。公共免费WiFi被有些人称之为水、电、气、路之后城市的第五公共设施。随着智能终端的普及、公共免费WiFi的发展,“WiFi时代”真正来临了。

4.2 WiFi攻击安全威胁

WiFi时代的来临,使得来自WiFi攻击的安全威胁显得越发恶劣。在2014年,Wifi威胁被第一次提上了台面。扬州某市民错连“钓鱼”WiFi导致了密码泄露,不到2天时间,就被盗取了69笔交易,多达6000多万元被转走。在这里先了解一下什么是WiFi“钓鱼”。俗话说,“姜太公钓鱼,愿者上钩”,WiFi“钓鱼”是指,攻击者通过伪装免费WiFi,引诱受害者连接,在受害者浏览网页的时候,将一些正常的网站替换成伪装的网站,这其中危害最大的就是网银站点了,受害者未察觉到伪装的网站与正常网站有何不同,从而输入个人密码,导致密码泄露。

别看WiFi“钓鱼”的原理这么复杂,其实设备非常简单,只需要一台可控的路由器用来发射无线信号即可。通过这台“特别的”路由器,攻击者就可以监控连接到该路由器的智能设备,分析智能设备与服务器通信的数据包,修改服务器返回的网页,甚至还可以伪装成受害者与服务器通信。

在使用公共WiFi、免费WiFi的时候,需要时刻注意保护自己的隐私。一般钓鱼WiFi会把WiFi名字起为“CMCC”、“KFC”等众所周知的热点名称,遇到没有密码的WiFi也要慎重,正规运营商或政府提供的WiFi一般都需

要手机等方式登录验证后才能使用,如果遇到没有密码、热点名称众所周知、连接即可上网这样的WiFi,需要提高警惕,多加注意。

4.3 如何应对Bluetooth攻击

Bluetooth(蓝牙)作为一种短距离的数据交换技术,为生活提供了诸多便利。蓝牙一方面可以建立与辅助设备的通信,如蓝牙耳机、蓝牙键盘等,另一方面还可以作为与对等设备数据交换的手段,如蓝牙传输数据。最早的蓝牙攻击出现在2005年,一种称为Lasco.A针对塞班系统的病毒开始出现,这种病毒通过蓝牙进行传播,它会不断尝试与可见蓝牙设备进行连接,一旦用户接收来自受害设备端通过蓝牙发送的文件,病毒就会自动下载并安装,此时病毒通过蓝牙复制到其他设备上。

蓝牙的攻击并不像WiFi攻击那么容易,蓝牙工作小组(Bluetooth Special Interest Group)指出,要攻击一个蓝牙设备,首先要强迫两个已配对的蓝牙装置中断连接,然后窃取重新连接所发送的PIN码封包,解开封包,伪装成蓝牙设备进行配对连接。由于蓝牙是一种近距离的通信协议,攻击与被攻击设备还要保持在近距离内(9 m左右),大大加剧了蓝牙攻击的难度。一旦攻击者成功与被攻击设备建立连接,就可以利用蓝牙设备提供的服务来拦截蓝牙发送的数据、窃取设备上的隐私数据等。

当然,由于蓝牙的诸多限制,蓝牙攻击需要透过高昂的设备和高超的技术,所以不必过于担心蓝牙攻击带来的危害。将蓝牙设为隐藏模式、不随意与其他设备配对、不随意接收来自蓝牙的文件,这些措施可以有效防范蓝牙攻击,保护好自己的隐私。

4.4 针对NFC技术的攻击

说到NFC(近场通信协议),大家都不会陌生,这也是最近被广泛应用到生活中的一种技术。生活中的NFC也无处不在,使用支持NFC的手机可以替代公交卡,两台NFC手机之间可以传数据,通过刷写特制的NFC标签可以提供一些数据。当然公交卡也是一种特殊的NFC标签。

NFC虽然不会直接造成危害,但是也能成为一个入口,为攻击者实施进一步攻击打开大门。2012年举行的黑帽技术大会上,展示了通过NFC作为入口如何对智能手机进行攻击。攻击者首先使用特制的NFC标签,用Android NFC手机进行识别,这会像手机发送一段恶意代码,这段恶意代码可以让手机打开一些指定的文件或网页,从而获取手机的控制权。通过两个NFC手机接触可以传送文件,这种方式不是由NFC实现的,而是通过NFC和蓝牙的协作完成的,NFC进行配对,蓝牙进行传输。攻击者可以利用这种方式间接进行蓝牙连接,使手机在没有提示的情况下接收一些文件。

NFC攻击非常难以测试,属于近场通信(需要接触才能进行),在通信距离上有着不易被窃听和不易被损害数据的优势,在日常生活中大可不必担心,随着技术的发展NFC的安全性会越来越有保障。

5 智能手机安全问题研究现状与发展趋势

无论是来自系统通用漏洞、恶意应用,还是无线攻击等新型攻击手段的威胁,智能手机的安全无时不刻不紧随时代潮流。在移动互联网飞速发展的今天,越来越多的安全人员开始对智能手机安全加大了关注力度,许多白帽子在移动App的漏洞挖掘和Android系统漏洞的研究上投入了大量精力,而国内的许多对安全有所涉猎研究的厂商,如360、腾讯、阿里巴巴等都对来自移动的安全问题投入了研究,并取得了相应的成果,同时也和乌云社区一起提供了相应的应急响应中心,接受并处理由白帽子挖掘寻找到的移动安全漏洞。在智能手机的安全问题上,正向着积极而又充满正义的方向前进。

另一方面,对移动安全的研究也不再仅仅拘泥于这些应用于系统的层面上,如对应用的研究不仅要面对漏洞与恶意行为的组合攻击,还要加固应用自身的安全特性,也就是防破解能力,借此来对抗山寨应用或恶意行为的植入攻击;在漏洞利用方面,诸如对摄像头等驱动进行攻击的案例研究分析也越来越多。

有理由相信,在移动互联网与移动安全共同发展的今天,智能手机的安全问题就像一把双刃剑,在存在本身安全威胁的同时,也激励着安全研究紧跟发展,在对抗的过程中更上一个台阶。

(责任编辑 刘志远)