安卓手机系统的安全威胁及应对

■清华大学网络科学与网络空间研究院/诸葛建伟

斯诺登曝光美国“棱镜”秘密情报监视项目，引发各方媒体与专家热议。而作为一名纯粹的技术研究者，我只从斯诺登逃离香港时爆出的一个细节谈起，也就是斯诺登在香港期间要求来访者将手机放入冰箱之后才许可和他见面。相信斯诺登是担心来访者手机被NSA定位监听，从而危及他的生命安全。我也不去分析手机放入冰箱是否真的可以免遭监听，而是分析斯诺登所担心的事情是否可能真实发生，以及会以何种方式发生？

脆弱的安卓手机系统

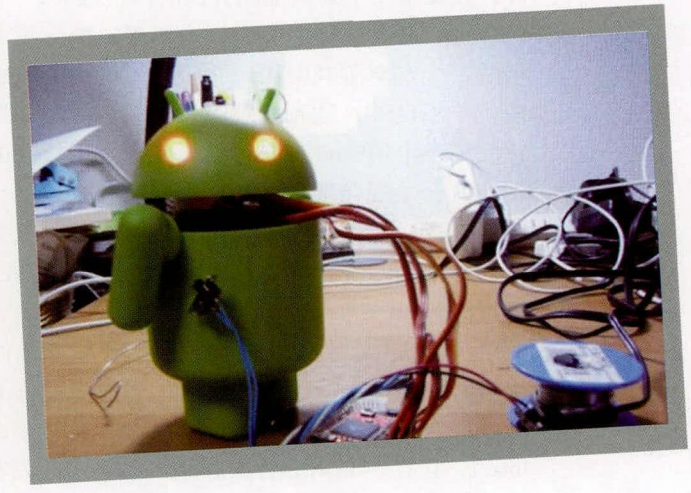
目前安卓手机占据了全球手机市场的主流地位，因此我们不妨相信来访者手机中肯定有安卓手机。那么安卓手机系统安全吗？我们可以从安卓手机系统已爆出的安全漏洞情况来做一个推断：根据我和一位学生发起的SCAP中文社区安卓平台漏洞库的统计数据，目前安卓平台已公开的漏洞就有374个，而且近年来的增长趋势非常迅速。这么多已公开的安全漏洞就能够说明安卓手机并不安全，更何况还有大量未被发现、甚至说已经被NSA掌握的未公开0day漏洞。

安卓平台上的这些安全漏洞会给安卓手机系统带来什么样的安全威胁呢？安卓手机系统的体系结构分层从底到上分别包括内核层、原生层、框架层和应用层。应用层和框架层的漏洞可以导致信息泄露或伪造，而一些接受远程输入的浏览器、Webview、短信等应用则可能被远程渗透攻击，从而让攻击者可以进入原生层获得远程访问权限，然后攻击者可以进一步利用原生层中具有Root权限进程或者内核层中的本地提权漏洞，提升权限获得对系统内核的访问，一旦获得内核访问权，攻击者可以进行后渗透攻击，从而控制整个安卓手机。

安卓手机系统的特点及带来的漏洞

那么，如何应对安卓手机系统的安全威胁，让安卓手机变得更加安全呢？因为安全漏洞是安卓手机安全风险的根源，所以最实际的一个技术途径就是检测安全漏洞并进行修补，然而当安全研究人员要向厂商验证漏洞时，往往需要提供漏洞验证和利用代码。

因此安卓手机系统安全漏洞检测与利用，就成了我们关注的一个重要研究方向，我们也非常幸运的得到了核高基项目的资助，来从事这方面的研究。接下来我就结合在这个项目中



的一些研究经验和初步成果，来分析前面斯诺登所担心的事情是否会发生，以及如何发生。

我们在进行安卓手机系统安全漏洞检测时，首先考虑了安卓平台的独特特性，这样才能够指导我们做一些具有原创性的研究，而不仅仅是应用现有技术。

安卓平台的第一个独特特性是，它是一个开源、闭源代码混合共生的环境。之前PC平台上的Windows是闭源环境，Linux是开源环境，而Android第一次能够将开源和闭源软件很好的结合在一起，在应用层、框架层、原生层和内核层每个层次上都有开闭源代码之间的交互。

这样的独特特性给安卓安全漏洞检测带来了异构性和多样性方面的挑战，但与此同时也带来了更多的机会。复杂性意味着安卓系统存在更多的漏洞，对于安全研究人员来讲也意味着更多的技术创新机会。而开闭源代码混合共生环境，使得研究人员可以从开源代码和交互接口中获得更多的高层类型信息，来指导安全漏洞的挖掘与分析，可以结合之前的源码白盒分析和二进制级的黑盒分析，从而构建智能的灰盒分析技术。下面我们就以安卓应用权限泄露漏洞作为实例，来分享我们利用这一独特特性，在安卓安全漏洞检测方面的研究经验。

我们考虑这样的一个攻击场景，植入了木马的一个安卓游戏应用，希望能够隐蔽的发送短信给不良SP，达到恶意吸费目的。但是如果它向用户申请Send_SMS权限，安全意识较高的用户就会发现异常，而选择不安装这个应用。然而如果没有申请到权限，那它就发不了吸费短信。而这时手机系统其实已经存在着一些已被授予Send_SMS权限的预装应用或是已安装的第三方应用，如果这些应用开放了发短信的接口，但未做安全保护，就会导致权限泄露漏洞。恶意应用就可以利用这类漏洞，通过发送Intent，让存在漏洞的合法应用帮助它发送吸费短信，从而成功进行攻击。

已有的研究工作主要使用静态分析方法来发现这类漏洞，但针对第三方应用缺少源代码的情况，在字节码粒度上构建的分析方法会引入误报，以及需要非常深入的静态程序分析技术支持。

而我们则是充分利用了安卓开闭源代码混合共生的环境优势，构建了动态的智能Fuzzing策略，并实现了权限泄露漏洞检测工具Intent Fuzzer。对于Fuzzer来说，最主要的是完成两个技术上的挑战，一个输入的构造，另外一个是程序行为的监控。在Intent输入的构造中，我们在开闭源代码交互接口Manifest文件中充分获取到了Intent输入的基本结构，然后利用对Android框架层开源代码中GetExtra API的监控，来获取Intent中的Extra域键值对信息的提取，从而逐步构建出全面准确的Intent输入，尽可能触发敏感权限申请和使用的代码路径。在程序行为监控点上，我们可以从外部观察直接转移到内部的精确监控点。对于开源Android代码，我们直接在源码上定位和Hook权限检查函数，而对于第三方手机的闭源ROM，我们则可以在开源代码指引下进行字节码上的插装监控。

我们以Intent Fuzzer测试了Google Play官方市场上各个分类最流行Top 200中的免费应用共2790个，以及两款国内主流手机厂商开发的第三方ROM。检测结果显示，有13%至30%的应用发现了权限泄露，其中涉及敏感权限也就是可以修改系统配置和数据的也有5%–7%。涉及到的权限占总权限的比例也高达20%至50%。我们也发现一些0day可利用的漏洞，也通过课题管理组提交给厂商确认。

而安卓平台第二个独特特性是版本碎片化的问题，这里面包括官方版本多样化和严重过时，以及第三方手机厂商推出定制版本进一步延长官方版本更新周期的问题。与此同时，安卓平台各

个层次上也大量复用了PC平台的代码。

这个独特特性给Android安全漏洞带来的挑战是需要检测大量的版本，造成研究成本和工作量更大。但同时也带来了更大的一个机会，安全漏洞生命周期在安卓平台上变得很长，使得刚刚公开1day漏洞的价值大幅提升。而普遍的代码重用也导致很多1 day漏洞在大量安卓手机上并未被修复，这使得研究人员可以利用1day漏洞补丁信息来辅助挖掘发现这类漏洞，由于这类漏洞在安卓手机上尚未修补，仍可以落入0day漏洞范畴，但是漏洞信息已被部分公开，因此我们也可以称这类漏洞为0.5 day漏洞。

我们这里举Webkit漏洞案例，我们新发现了安卓 4.2.2最新版本中未修补Webkit内存破坏漏洞导致浏览器崩溃的有8个，但是要成功利用必须绕过安卓4引入的安全防护机制，目前还在艰难的开发与测试过程中。另外一个实例是，我们以Linux Kernel最新发现的1day漏洞信息作为参考索引，在安卓中发现了一个未修补的0.5 day本地提权漏洞，并成功开发了本地提权的攻击代码，并在Google Nexus 4真机的最新ROM版本4.2.2（内核版本3.4）上进行了测试，能够成功对手机进行ROOT“越狱”。而这个漏洞的渗透代码是目前公开渠道上第一个针对安卓4.1以后版本的通用ROOT提权代码。

我们最后一个考虑的安卓平台特性是新型移动智能终端的通用特性、注重能耗、而且硬件性能较PC弱，需要保证用户体验。在漏洞检测方面的机会是，安卓平台为了保证用户体验，低能耗往往选择弱化安全性，这就为安全研究人员提供了更多机会来找到安全漏洞或弱点。

这里的一个案例是我们所发现的安卓应用签名验证流程中存在的安全风险。安卓系统在应用启动时的签名验证只根据最后修改时间戳和文件路径进行验证，而没有涉及任何密码学验证，这当然是为了低能耗和用户体验的考虑。然而这就会带来安全风险，绕过应用签名认证机制，但攻击需要ROOT权限，这在安卓的安全原则中是不成立的前提条件，然而我们之前已经演示了我们可以突破最新版本的安卓来获得ROOT权限，这就使得这种安全风险可以被利用。

应用签名绕过的具体步骤是：先常规的对目标APK进行重打包，制作木马化的版本；然后获得ROOT权限的手机将目标应用替换成木马化版本；第三个步骤是进行应用签名验证绕过的关键，也很简单，只需要更新时间戳保持和原先的一致，然后删除原先应用的odex优化代码文件，等待系统重启之后就可以达到绕过应用签名验证机制，将目标应用进行木马化的攻击目的。

现在，你能否理解斯诺登在担心什么了吧！事实上，利用我们前面发现或成功利用的几个漏洞，就可以实现从短信伪造，到Webkit远程代码执行，到本地ROOT提权，并对任意应用进行木马化，最终实现定位监听的目的。我当然相信NSA所掌握的资源和能力远在我们研究小组之上，难道不是吗？不过我们的研究目的不是像NSA那样对斯诺登进行监听，而希望能将我们研究的安卓漏洞检测技术用于安卓手机系统的安全测试，让安卓系统，特别是国产手机系统变得更加安全。