浅析安卓平台下 VPN 应用程序存在的安全隐患

党李成 朱国辉 许 璐

（河南省疾病预防控制中心疫情信息管理中心 郑州 450000）

〔摘要〕 阐述安卓（Android）平台下建立虚拟专用网络（Virtual Private Network，VPN）连接的原理和特点，采用一种静态分析和动态验证相结合的方式，分析 Android 平台下 VPN 应用程序是否存在安全隐患并介绍安全隐患检测结果。

〔关键词〕 安卓；虚拟专用网络；安全隐患

〔中图分类号〕R－056 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2017.11.010

Analysis on the Potential Security Risks of the VPN Application under Android Platform *DANG Li－cheng, ZHU Guo－hui, XU Lu, Epidemic Information Management Center of Henan Center for Disease Control and Prevention, Zhengzhou 450000, China*

〔**Abstract**〕 The paper states the principles and characteristics of the Virtual Private Network (VPN) connection built under Android platform, analyzes whether VPN application has potential security risks by combining static analysis with dynamic verification, and introduces the detection result.

〔**Keywords**〕 Android; Virtual Private Network (VPN); Security risks

1 引言

在移动互联网时代虚拟专用网络（Virtual Private Network，VPN）应用程序在移动网络信息安全领域的作用显得非常重要。近期谷歌公司公开的安卓（Android）的官方文档突出显示 VPN 权限引发的严重安全问题：允许应用拦截并完全控制用户的业务，甚至允许访问敏感内容等[1]。这也就意味着恶意 VPN 应用程序开发者可能会滥用来收获用户的个人信息，同时带来严重的安全隐患[2]。本文将展开对常用 VPN 应用程序可能存在的安全隐患的研究。

〔修回日期〕 2017－05－19

〔作者简介〕 党李成，助理工程师，硕士，发表论文 9 篇。

2 安卓平台下建立的 VPN 连接

2.1 原理

安卓从 4.0 开始提供一个在安卓智能设备上建立 VPN 连接的解决方案，且不需要 Root 权限[3]。安卓平台下数据包通过 VPN 连接和数据传输过程，见图 1。具体过程如下：（1）应用程序使用 Socket 将相应的数据包通过智能移动设备上的网络接口发送到网络上[4]。（2）安卓系统通过 IP 地址表使用 NAT，将所有的数据包转发到 TUN 虚拟网络设备上去[5]，端口是 tun0。（3）VPN 程序通过打开/dev/tun 设备，读取该设备上的数据[6]，可以获得所有转发到 TUN 虚拟网络设备上的 IP 包[7]。（4）VPN 数据按照一定的规则做一些封装和拆包处理，然后

将处理过后的数据包，通过真实的网络设备发送出去。同时为防止发送的数据包被再次转到 TUN 虚拟网络设备上，VPN 程序所使用的 Socket 将被明确绑定到真实的网络设备上去[8]。

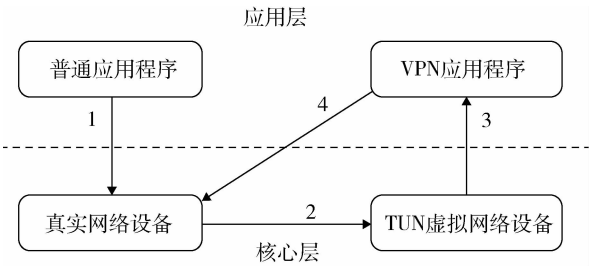

图 1 安卓平台下 VPN 连接实现原理

2.2 特点

从上文分析安卓框架下的 VPN 连接的实现过程，可以发现这种 VPN 连接方式有以下几个特点：（1）VPN 连接对于应用程序来说是完全透明的[9]，应用程序完全感知不到 VPN 应用程序的存在，也不需要为支持 VPN 应用程序做任何更改。（2）从编程的角度讲，VPN 程序并不需要获得设备的 Root 权限就可以建立 VPN 连接，所需要的只是在应用程序内的 AndroidManifest. xml 文件中申明需要一个叫做“android. permission. BIND_ VPN_ SERVICE”的特殊权限[10]。（3）在正式建立 VPN 链接之前，Android 系统会弹出一个对话框，需要用户明确同意该权限操作才能往下执行，而且一旦第一次申请通过，安卓平台就默认不再提示用户需要审核该权限操作[11]。（4）一旦在安卓设备上建立起了 VPN 连接，安卓设备上所有发送出去的 IP 包，都会被转发到虚拟网卡的网络接口上去。（5）VPN 应用程序可以通过读取这个接口上的数据，来获得所有设备上发送出去的 IP 包；同时可以通过写入数据到这个接口上[12]，将任何 IP 数据包插入系统的 TCP/IP 协议栈，最终送给接收的应用程序。（6）因为设备上的所有 IP 包都会被 NAT 转成原地址是 tun0 端口发送的，VPN 程序可以获得进出该设备的几乎所有的数据[13]。通过上面的分析可以看出 VPN 程序可以被用来做很多其他事情，比如可以用来抓设备上的所有 IP 包，而这就带来了诸多安全隐患。

3 安卓平台下 VPN 应用程序安全隐患检测方法

3.1 静态分析

采取一种静态分析和动态验证相结合的方式，测试分析 VPN 应用程序样本库（Google Paly 应用商店中的前 100 名的 VPN 应用程序）是否存在安全隐患以及都有哪些安全隐患。先使用静态分析方法来分析每个 VPN 应用程序的源代码。具体方法如下：（1）通过 Google Play 应用商店下载 VPN 应用程序。（2）借助反编译工具编译 VPN 程序。（3）详细核查反编译之后生成的源代码，重点关注诸如 AndroidManifest. xml 等类型文件，分析在其应用清单文件中直接申请的 Android VPN 权限[14]，或者在源代码中使用 < activity > 和 < service > 标签变相申请的 Android VPN 权限。（4）根据源代码中对 VPN 应用程序操作权限的实际使用情况，结合 VirusTotal 提供的辅助分析功能，最终标记出其中敏感操作或者导致信息泄露等行为[15]。（5）将所有可疑的代码行与其对应可能采取的操作对比记录在案，制作成可疑行为库以备下一步动态分析最终核对。

3.2 动态验证

将采用专门的拦截测试平台来拦截 VPN 应用程序的所有流量，分析这些流量的各种信息来核对上节静态分析中形成的可疑行为库。拦截测试平台运行原理，见图 2。

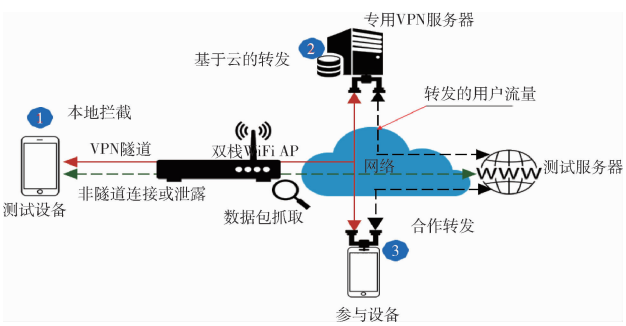

图 2 拦截测试平台运行原理

在这种拦截机制中包含 3 种流量拦截模式[16]：

（1）本地拦截作为透明代理。（2）通过 VPN 服务器进行基于云的转发。（3）通过参与节点（对等体）或其他参与节点的流量转发。专用测试平台中智能手机通过配置具有双栈支持的 WiFi AP 的计算机连接到互联网[18]。而 WiFi AP 通过运行网络数据采集分析工具 tcpdump 来拦截在智能手机和互联网之间传输的所有数据包流量。同时根据具体情况采取以下 3 种操作来帮助分析：（1）运行专用脚本，该专用脚本同时运行在测试设备和测试服务器之间，同时借助 ICSI Netalyzr 工具来生成流量并分析不同的网络和流量的各种信息[19]。（2）利用网络故障排除工具 Netalyzr for Android 来识别 TCP 级别的路径流终止代理，在 HTTP 代理的情况下，它们如何干扰用户的流量[20]，识别沿路径的不透明代理的方式制作数据包和 HTTP 请求。（3）检查 WiFi AP 捕获的数据包，以确定是否存在可能由 VPN 引擎为其他参与用户以对等方式通过我们的设备转发的外部流。

4 安卓平台下 VPN 应用程序安全隐患检测结果（图 3）

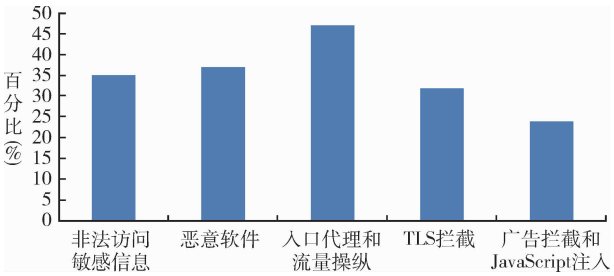

图 3 安全隐患分类占比

4.1 非法访问敏感信息

测试目标库中有 35% VPN 应用软件存在第 3 方应用跟踪和访问敏感的安卓权限的行为。虽然这些 VPN 应用程序使用第 3 方跟踪库和请求访问敏感资源的权限，而这些操作通常都涉及用户帐户、交易和文本等敏感消息[21]。

4.2 恶意软件

测试目标库中有 37% 的 VPN 应用程序存在恶意行为，如恶意广告不断弹出、色情网站自动链接、强制修改设备某些设置、自动安装特定应用等等。其中自动安装特定的应用程序最为普遍。

4.3 入口代理和流量操纵

测试样本库中有 47% 的 VPN 应用程序存在入口代理和流量操纵行为。这些软件大都部署不透明的代理，通过注入和删除头文件或执行图像转码等技术来修改用户的 HTTP 流量。入口代理允许 VPN 应用程序获取对用户流量的控制并且即时操纵流量[22]。此外许多代理功能可以为 ISP 和网络提供商提供经济利益，如 HTTP 报头注入或流量重定向的广告目的。VPN 应用程序 Hotspot – Shield 将电子商务流量重定向到合作域。当客户端通过 VPN 连接到访问特定的 Web 域时，该应用程序利用一个代理来拦截并将 HTTP 请求重定向到合作伙伴网站，具有以下语法：http://anchorfree.us/rdr.php? q = http://www.dpbolvw.net/click – 7772790 – 12173149 – 1427959067000。这样用户的流量在到达淘宝网站之前就通过两个组织进行中继：AnchorFree 和 dpbolvw.net，而这两个网站都是购物平台 valueclick.com 旗下的网站。

4.4 TLS 拦截

测试样本库中有 32% 的 VPN 应用程序存在 TLS 拦截行为。以 Packet Capture、DashVPN、DashNet 和 Neopard 4 个应用程序为例，它们都存在改变用户的 Root 存储，在应用执行过程中主动执行 TLS 插入的非法行为。这当中 3 个应用程序选择性地截取特定的在线服务（如社交网络，银行，电子商务网站，电子邮件和 IM 服务以及分析服务等）的流量。同时通过发出自签名证书来主动拦截 TLS 流量，见表 1。

表 1 部分 VPN 应用拦截常用网站情况汇总

测试网站 \ 测试软件	Neopard	DashVPN	DashNet	Packet Capture
Mail. google. com	√	√	√	√
Mail. yahoo. com	√	√	√	√
Maps. google. com	√	√	√	√
Play. google. com	√	√	√	√
www. akamai. com	×	√	×	√
www. ebay. com	×	√	×	√
www. facebook. com	√	√	√	√
www. gmail. com	√	√	√	√
www. google. com	√	√	√	√
www. hotwire. com	×	√	×	√
www. ibm. com	×	√	×	√
www. simple. com	×	√	×	√
www. skype. com	×	√	√	√
www. twitter. com	√	√	√	√
www. yahoo. com	√	√	√	√
www. qq. com	√	×	×	√
www. taobao. com	×	√	×	√
www. tripadvisor. com	×	√	×	√
www. viber. com	×	√	√	√
www. youtube. com	√	√	×	√

注：√代表不拦截，╳代表拦截。

4.5 广告拦截和 JavaScript 注入

测试样本库中有 24% 的 VPN 应用程序存在广告拦截和 JavaScript 注入行为。广告拦截，默认情况下 VPN 应用程序在测试的网站上主动阻止广告和分析流量例如 F－Secure Freedome VPN。这些应用没有在权限申明文件中提及 Google Play 商店列表中的广告拦截功能[23]。但是其源代码，却显示 F－Secure Freedome VPN 阻止来自与 Web 和移动跟踪相关联的预定义域列表的任何流量，包括 Google Ads，DoubleClick 等流行的标签/分析服务，如 Google Tag 和 comScore。JavaScript 注入。以 HotspotShield 和 WiFi Protector VPN 这两个 VPN 应用程序为例，通过使用 iframe 的 JavaScript 代码进行广告和跟踪。对其应用程序源代码的静态分析显示这两个程序都使用了 5 个以上不同的第 3 方跟踪库[24]。结果证实 WiFi Protector VPN 免费版本的应用程序注入 JavaScript 代码，用于跟踪和显示自己的广告给用户。

5 结语

本文提出一种静态分析和动态验证相结合的方法来检测 Google Paly 应用商店中部分 VPN 应用程序是否存在的安全隐患以及都有哪些安全隐患。依靠建立的分析模式，发现部分 VPN 应用程序存在非法访问敏感信息、流量操纵、广告拦截和跟踪拦截等非法行为。这些都无不说明在安卓平台下，由于其 VPN 应用程序存在不为用户所知的安全隐患，虽然只是发现部分软件存在问题，但是这已经足以引起注意。考虑到本文只是针对 100 款 VPN 应用程序进行了安全隐患测试和评估，测试样本库数量偏少，具体测试工作繁琐和适用面窄，未来将继续改进测试方法使之能够适应更高强度测试和更广的测试范围，加强对安卓平台下 VPN 应用程序存在的安全隐患的研究。

参考文献

1 蒋绍林，王金双，张涛，等，Android 安全研究综述［J］. 计算机应用与软件，2012，29（10）：206－210.

2 李凡. Android 系统安全机制的分析与增强［D］. 武汉：

华中科技大学，2012.
3 寇晓晖. Android 平台移动安全接入系统［D］. 武汉：华中科技大学，2013.
4 黄怡皓. 基于 android 系统的 IPSec VPN 的研究与改进［D］. 杭州：浙江工商大学，2012.
5 H Banuri, M Alam, S Khan, et al. An Andriod Runtime Secrity Policy Enforcement Framework, Personal & Ubiquitous Computing, 2012,（16）: 631 – 641..
6 Google Inc. Manifest. permission［EB/OL］.［2017 – 01 – 10］. http://developer. android. com/reference/android/Manifest. permission. html.
7 A Shabtai, Y Fledel, U Kanonov Y Elovici, et al. Google Android: a comptehensive security assessment［J］. IEEE Security and Privacy, 2010, 8（2）: 35 – 44.
8 Burns J. Developing Secure Mobile Aoolications for Android, Technical Report［J］. iSEC, 2008,（10）: 1 – 28.
9 Enck W, Ongtang M, McDaniel P. Un – derstanding Android Security［J］. IEEE Security&Privacy, 2009,（7）: 50 – 57.
10 郭宏志. Android 应用开发详解［M］. 北京：电子工业出版社，2010：35 – 78.
11 沈才樑，唐科萍，俞立峰，等. Android 权限提升漏洞攻击的检测［J］. 电信科学，2012，28（5）：115 – 119.
12 张一 . 基于 Android 平台的智能手机权限安全研究［D］. 上海：上海交通大学，2014.
13 杨广亮，龚晓锐，姚刚，等. 一个面向 Android 的隐私泄露检测系统［J］. 计算机工程，2012，38（23）：1 – 6.
14 李佳. Android 平台恶意软件检测评估技术研究［D］. 北京：北京邮电大学，2012.
15 王世发，高贤强，韩路. Android 安全机制分析及解决对策［J］. 电子测试，2013,（22）：59 – 60.
16 王斌，王娜. Android 平台强制访问控制系统研究［J］. 滁州职业技术学院学报，2014，13（1）：68 – 70.
17 佟得天. 基于行为分析的 Android 手机木马检测技术研究［D］. 广州：中山大学，2012.
18 刘泽衡. 基于 Android 智能手机的安全检测系统的研究与实现［D］. 哈尔滨：哈尔滨工业大学，2011.
19 戴威，郑滔. 基于 Android 权限机制的动态隐私保护模型［J］. 计算机应用研究，2012，29（9）：3478 – 3482.
20 蔡罗成. Android 后台监听实现机制浅析［J］. 信息安全与通信保密，2010，11（6）：39 – 41.
21 华鹏. 基于 Android 平台增强权限管理研究与实现［D］. 南京：南京理工大学，2012.
22 M Ongtang, S Mclaughlin, W Enck, et al. Semantiacally Rich Application – Centric Security in Andriod［J］. Securtity & Communication Networks, 2012, 56（5）: 658 – 673.
23 Hammad Banuri, Masoom Alam, Shahryar Khan, et al. An Android Runtime Security Policy Enforcement Framework［J］. Personal and Ubiquitous Computing, 2012,（6）: 631 – 641.
24 刘敏. 基于 Android 平台的软件行为分析系统的设计与实现［D］. 北京：北京邮电大学，2014.

（上接第 22 页）

参考文献

1 田丰，刘长军，李钒，等. 基于生理参数的急救背囊人体工效学评价［J］. 医疗卫生装备，2016，37（11）：1 – 6.
2 李英春，尤磊，贺靖康，等. 基于生理信号的情绪识别腕戴设备［J］. 电子技术应用，2017，（2）：69 – 72.
3 Ge J I, Orosz G. Optimal Control of Connected Vehicle Systems With Communication Delay and Driver Reaction Time［J］. IEEE Transactions on Intelligent Transportation Systems, 2016, 18（8）: 2056 – 2070.
4 Pourtaherian A, Scholten H, Kusters L, et al. Medical Instrument Detection in 3 – Dimensional Ultrasound Data Volumes［J］. IEEE Transactions on Medical Imaging, 2017, 36（8）: 1664 – 1675.
5 车国卫，刘伦旭，石应康. 加速康复外科临床应用现状与思考［J］. 中国胸心血管外科临床杂志，2016，（3）：211 – 215.
6 Mestais C S, Charvet G, Sauterstarace F, et al. WIMAGINE: wireless 64 – channel ECoG recording implant for long term clinical applications［J］. IEEE Transactions on Neural Systems & Rehabilitation Engineering A Publication of the IEEE Engineering in Medicine & Biology Society, 2015, 23（1）: 10 – 21.
7 Chien Y R, Mehta D D, Guenason J, et al. Evaluation of Glottal Inverse Filtering Algorithms Using a Physiologically Based Articulatory Speech Synthesizer［J］. IEEE/ACM Transactions on Audio Speech & Language Processing, 2017, 25（8）: 1718 – 1730.