移动僵尸网络中数据流的采集与分析

徐 建,吴烨虹,程晶晶
(南京邮电大学 计算机学院,江苏 南京 210023)

摘 要:近年来,移动僵尸网络已经成为移动通信和网络安全的最大威胁。随着移动设备功能的不断增强,给网络犯罪提供了更好的环境。因此,僵尸网络等各种新型的恶意软件在移动设备和网络中肆意传播。针对移动设备安全的研究还不充分,依然缺乏高效的安全解决方案。因此,提供有效的数据以了解和分析移动僵尸网络,对于移动设备的安全和隐私来说至关重要。为此,在对移动僵尸网络数据集的生成、正常数据流量数据集的区分以及对非正常数据的清理详细介绍的基础上,对数据进行了标注和聚合。通过对以往的数据集和样本优缺点的分析讨论,进一步研究与分析了适合移动僵尸网络的数据集与样本的建立方法、数据采集和清理方法以及数据聚合成合法数据并摆脱移动僵尸主控机控制的方法。

关键词:移动僵尸网络;检测;数据集;数据分析
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2016)11-0101-05
doi:10.3969/j.issn.1673-629X.2016.11.023

Collection and Analysis of Data Flow in Mobile Botnet

XU Jian, WU Ye-hong, CHENG Jing-jing
(College of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China)

Abstract: In recent years, mobile Botnet has become the biggest threat for mobile communications and network security. With the continuous enhancement of the function of mobile devices, it provides a better environment for network crimes. Therefore, Botnet and other new types of malicious software in mobile devices and networks have been spread. Investigation on mobile device security has not still been sufficient because of lack of efficient security solutions. Thus, it is most important and necessary for security and privacy of mobile devices to provide effective data to understand and analyze the mobile Botnet. So the data have been labeled and aggregated on the basis of a detailed introduction to the generation of mobile Botnet data sets, the distinction between normal data traffic data sets and the non-normal data cleaning. Based on the analysis of the previous data set and the advantages and disadvantages of samples, further investigations and analysis on establishment methods of data sets and samples suited to mobile botnet as well as those of data sampling and data cleaning and for the approaches of data aggregation into legitimate data and extrication from mobile zombie master machine control is carried out.

Key words: mobile Botnet; detection; data set; data analysis

0 引 言

现如今智能手机已成为人们随身携带的沟通工具,它已经不是单纯的移动电话,而是基本上包含了所有计算机的功能,可以看作是一台掌上计算机。因此针对计算机的威胁在不断地迁移到智能终端设备和智能手机上。起初攻击者利用各种短信来诈骗。随着技术的革新和网络浏览器的进步,手机上网成为一种潮流,手机上可以设计安装各种应用程序(这里主要指 Android 系统)。这也给攻击者提供了更多的机会,在移动设备上的攻击和威胁方式有多种形式,如病毒、木马、蠕虫和移动僵尸网络[1]。其中威胁最大的是移动僵尸网络,它是由一个称之为“移动僵尸主控机”的攻击者,通过复杂的连接和通信,在网络空间创建、执行恶意活动,并控制其子网络进行协调攻击,最终形成一个有组织的网络犯罪形式[2]。

近年来,移动恶意软件的攻击和威胁,以及移动僵尸网络一直处于上升的趋势。F-Secure[3] 的调查表明,移动恶意软件的威胁数量与 2013 年第三季度同期相比上升了 26%,2013 年第三季度相比 2012 年第三季度有 259 个新的威胁出现。在 2012 年,有一个值得

收稿日期:2015-06-30 **修回日期**:2015-10-28 **网络出版时间**:2016-10-24
基金项目:国家自然科学基金资助项目(61202353);南京邮电大学实验室工作研究课题(2015XSG05)
作者简介:徐 建(1980-),男,硕士,工程师,研究方向为信息安全、人工智能。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20161024.1105.002.html

关注的移动僵尸网络攻击,它是 Zitmo 僵尸网络的变体,专门攻击安卓、塞班、Windows 和黑莓智能手机,被称为 Eurograbber。它对受害者的银行账户进行欺诈,导致了超过 4 700 万美元的损失[4]。因此,移动僵尸网络给人们带来的损失是巨大的。而针对安卓平台上的数据流进行采集和分析,有助于今后对移动僵尸网络的检测和应用。

为此,从移动僵尸网络的特点出发,简述了检测移动僵尸网络的两种途径,对检测的数据流进行分析,共同探讨它的数据收集方式,为今后移动僵尸网络的进一步研究提供一些依据。通过对移动僵尸网络的数据进行采集、分析、清理,来分析数据的有效性。

1 移动僵尸网络的特点

与传统的计算机环境下的僵尸网络类似,移动僵尸网络也包含三个主要元素:僵尸主控机、僵尸机和 C&C 机制[5-6]。移动僵尸主控机通过 C&C 机制在移动僵尸机上设计和实现移动恶意应用,去感染其他的移动设备,并将其转化为移动僵尸机[7]。与其他类型的恶意软件的主要区别在于被感染的设备相互连接,形成了移动僵尸网络[1,8]。移动僵尸主控机主要通过 C&C 机制给移动僵尸机发送命令和设置更新[9]。据上所述,移动僵尸网络的生命周期可以分为三个阶段:传播和感染、信息的传递、接收指令和攻击[10]。

1.1 传播和感染

在移动僵尸网络中传播恶意代码的主要途径是使用者的传播和对漏洞的利用。首先,最流行的就是利用社会工程学,就如那些计算机的软件一样,目前的智能手机已超出了以前打电话和发送信息的范畴,有自己独立的操作系统,与计算机更加相似,可以频繁访问 INTERNET 网络,因此它也成为了恶意软件攻击的目标。在垃圾邮件和 MMS 消息中包含有恶意内容的附件,或在垃圾邮件和 MMS 消息中嵌入链接,指向包含有恶意代码的虚拟主机。在移动设备使用者不经意间就会执行附件或点击那些下载恶意程序的链接,从而受到移动僵尸主控机的控制,加入到移动僵尸网络中。常见的还有利用系统或软件的漏洞,在移动设备上传播恶意代码。例如由西班牙安全研究人员披露的 HTC 蓝牙漏洞[11],Mulliner 等[12]发现的一种不需要通过移动服务提供商的网络,就可以直接操纵不同移动平台的短信。还可以通过蓝牙技术进行传播,被感染的移动设备可以使用蓝牙搜索附近的设备,与之配对之后,主控机会将恶意软件注入到周边的移动手机中。总之,智能手机在使用方便的同时,也给攻击者开辟了更广阔的空间。

攻击者的攻击手段多种多样,主要是利用手机漏洞,被感染的 URL,SMS/MMS 和蓝牙等感染新的移动设备,使用户在不知情的情况下成为移动僵尸网络的成员[13-14]。一般来说,攻击者就是操纵僵尸主控机,利用高带宽无监控的智能手机设备去尽可能多地传播和感染僵尸机[1,9]。

1.2 信息的传递

这是每个移动僵尸网络的关键阶段,它由每个僵尸机通过控制命令(C&C)服务器获得僵尸主控机的新命令和更新,僵尸机在接收到命令后,将执行结果立即报告给僵尸主控机[5,15]。C&C 机制作为僵尸主控机发出命令到目标机器(僵尸机)和接收响应的接口[16]。目前一直在研究僵尸主控机与僵尸机之间的通信方式。起初在基于计算机的僵尸网络中,可以建立 IRC 服务器及相应的信道,接着发展到 P2P 和 HTTP 机制[17]。但是在移动僵尸网络中,由于不同的操作系统,缺乏公共的 IP 地址,不同方式的连接类型以及通信的成本,很难实现一个多种模式的 C&C 机制[18]。下面讨论几种技术创造的 C&C 机制。

1.2.1 短信息服务

短信息服务是移动设备最广泛的通信方式。在一些科研人员的研究中[19],评估了 Kademila 和 Gnutella 两种模型,建立了基于 SMS 的移动僵尸网络。但在现实世界中,短信是需要收费的,通信成本会通知移动用户,从而导致该模式能很快被检测出来[20]。因此基于 SMS 的移动僵尸网络的数量比较少。

1.2.2 互联网/网络

由于移动设备与因特网的融合,大量的移动僵尸网络是基于网络技术和协议的(例 HTTP 协议)。为了能与僵尸机(被感染的移动设备)进行通信,就需要僵尸主控机发布特定的命令[21]。僵尸主控机通过标准的网络协议和服务,将控制命令隐藏在正常的网络数据流中,这样更加隐蔽,很难检测出来。在今后的技术发展中,Web 服务和互联网会更加广泛地应用到移动设备中。基于 HTTP 的僵尸网络被认为是僵尸网络中最危险的类型之一,被移动僵尸网络广泛应用[9]。美国北卡罗莱纳州立大学的 Zhou Yajin 等[22]在与网秦的合作过程中,一年内成功识别和收集了 1 200 多种移动恶意软件,他们发现超过 97% 的移动僵尸机都是通过基于 HTTP 的 Web 数据流与 C&C 服务器进行通信的。表 1 为几种移动僵尸网络实例所使用的 C&C 机制[23]。

1.3 攻击行为

感染僵尸机和建立 C&C 机制的目的就是进行攻击,在攻击的前后,僵尸机与主控机之间都要进行信息的交互,僵尸机可以接收并执行多种类型的攻击命令。事实上,移动僵尸网络是一个攻击平台,每种类型的恶

意活动都可以在移动设备和网络中进行,例如:对固件的破坏、垃圾邮件、窃取敏感信息、点击欺诈和广告软件,以及下载更多内容等。除了上述所讨论的攻击外,移动僵尸网络还会利用自带智能设备(BYOD)攻击企业的机密信息、金融资产和知识产权。近年来,BYOD 已成为人们办公的一种流行趋势,它可以在任何时间、任何地点通过网络进行灵活的办公[24]。在超过 80% 的国家组织中都使用 BYOD,但是许多员工的安全意识较低。

表 1　移动僵尸网络 C&C 机制

移动僵尸机	SMS	互联网/网络
AnserverBot	-	√
Geinimi	-	√
DroidKungFu	-	√
GoldDream	-	√
NickyBot	√	-
Zitmo	-	√
GPSSMSSpy	√	-

尽管目前针对 BYOD 的移动安全也提出了一些解决方案,例如安装登录终端、增加安全控件等,但这些方案大都专注于管理设备(MDM)、应用程序(MAM)和一些策略信息(MIM)[25-26]。因此,随着移动设备和用户的不断增多,移动安全和移动僵尸网络的检测与分析就成为了全球性的关键问题。

2　移动僵尸网络的检测

以往研究的蜜罐和蜜网、攻击的行为分析、监测和 DNS 分析、基于签名的僵尸网络检测和行为分析技术,都是基于计算机和计算机网络行为特征的,不能直接应用于移动设备。因此需要先了解当前移动僵尸网络检测所面临的问题:

(1)资源的局限性和特殊性。移动设备的资源,如 CPU、内存和电池寿命都是有限的,而且移动设备的安全管理策略与计算机也有差异,因此不能将僵尸网络的检测直接部署到移动僵尸网络。La Polla M 等[13]对移动性、详细的个性特征、不同类型的连接、技术融合等多种功能进行了总结。

(2)感染和传播的多样性。移动设备的传播媒介多样,它可以通过 SMS/MMS、蓝牙、WiFi 以及互联网等不同方式进行传播。

(3)自我保护技术。正如其他类型的僵尸网络,移动僵尸机也有一些很难被检测到的特征,而且僵尸主控机也不断地从现有的检测方案中尝试不同的技术来保护自己的僵尸机。

(4)缺乏安全管理中心。移动设备相比计算机和计算机网络缺少更多的保护,主要是它们的用户不注意安全的更新。从上述问题来看,最主要的就是缺乏安全管理中心,因为它可以追踪和监控安全威胁,并在相应的移动设备上更新安全策略[2]。此外正如 Bailey 等[27]提出,目前广泛的僵尸网络检测方法的设计是在同一个僵尸网络内,基于形成合作行为的僵尸机。事实上,在移动设备中,对这些相似之处的分析没有集中的安全管理。

对于移动僵尸网络检测的这些问题,目前已有专家在技术上进行了尝试。尽管这些技术主要都是针对移动恶意软件的检测,但也促进了移动僵尸网络技术的开发。常见的检测方式有两种:静态分析和动态分析。也可以将两者结合,形成混合的方式[28]。

静态分析是指对没有执行的移动应用程序的检查和评估(如 apk 文件)。它的主要步骤是将 apk 文件逆向到源代码,从源代码本身分析寻找恶意行为。而动态分析是在应用程序执行期间评估它的行为和动作。除此之外,还可以根据移动僵尸网络的自身特点,分析僵尸机与 C&C 服务器的通信特性。

3　数据采集及分析

检测数据是否属于移动恶意软件,是否用来提供 C&C 通信,这需要有基准的数据集来判断。M. Eslahi 等指出[15]移动僵尸网络是最近才出现,还没有进行充分的研究。因此对于移动僵尸网络检测和分析的主要挑战是对这些新出现的网络犯罪形式的了解有限,缺乏足够的样品和基准数据集[22,29]。因此本节参照现有的恶意软件样本和数据集,分析和寻找有关移动僵尸网络活动的数据。

3.1　有效的恶意软件样本

在现有移动安全研究中,最主要的问题就是没有完整的移动恶意软件样本,只有部分研究团体公布了一些恶意软件实例,而且数据样本也并不完全可靠。

由北卡罗莱纳州立大学的 Zhou Yajin 和 Jiang Xuxian 两位研究人员发起的 Android Malware Genome Project(安卓恶意软件基因组计划),共享了安卓平台恶意程序样本和分析结果,这成为了安卓平台上最大规模的综合恶意软件数据样本之一。一年中,他们成功地从 49 种不同恶意软件家族中收集了 1 200 多个安卓恶意代码样本。在收集的这些恶意软件中,超过 93% 的转换成手机的僵尸机,通过 C&C 服务器与僵尸主控机通信。

由马来西亚博特拉大学进行的 M0Droid 项目,是通过模式识别技术来分析和检测安卓恶意软件。他们发布了两类实例,被称为恶意软件和 Goodware 数据集。M0Droid 项目的主要优势是恶意软件和可信应用

的采集,它有效地促进了对正常行为异常活动的异常检测分析[23]。

3.2 真实世界行为数据集

除了以上提到的恶意软件样本,智能手机有它自身的一些特点,例如系统信息、位置、运算以及手机使用等。目前可以从两个方面对数据进行分析。

(1)移动数据的挑战(MDC)。MDC 是最全面的移动行为数据集,是通过大规模的研究来收集的唯一一组数据,之后可以对此数据进行深入分析。表 2 就是由 N. Kiukkonen[30] 等收集的数据。MDC 是由 200 多人经过两年时间收集的,它是所有数据中最真实、完整的数据集之一。

表 2 收集的数据集

数据类型	数量	持续时间/小时
电话	132 109	3 907
短信息	88 225	
照片	28 054	
视频	2 163	
蓝牙扫描	15 362 182	
无线网扫描	12 568 788	
音频样本	218 021	1 817
应用程序事件	3 569 860	
电话本记录	34 053	

(2)数据开发(D4D)的挑战。N. Kiukkonen[30] 等于 2011 年 12 月到 2012 年 4 月,从 5 亿用户的信息中收集了 2.5 亿多条记录。这项研究已经从移动痕迹、集群通信和通信子图三个类别发布了几个数据集。而最后两个数据集可以作为移动恶意软件分析的依据,在被感染的移动网络中,区分僵尸机通信和正常的用户。

4 数据采集方法的探讨

由于目前没有足够的移动 HTTP 流量数据(良性和恶性),Meisam Eslahi 等[23] 提出了一种数据收集方法来除去恶意的和与僵尸机通信产生的流量,创建正常移动网络流量。在任何一个实验中,如何选择真正的移动恶意软件是非常重要的,因此为了确保恶意的 APK 肯定是僵尸机,样品必须来自于合法的来源[31]。然而,准确的网络流量可能不是简单地通过提交 APK 文件生成服务。图 1 所示为如何构建数据集。

4.1 生成移动僵尸网络数据集

要想生成恶意数据集,首先需要建立一个虚拟的移动僵尸网络。它主要包括三部分:安卓虚拟环境、移动僵尸机和虚拟的 C&C 服务器。

安卓的虚拟环境:可以在 Android x86 平台上创建一组移动设备,并构成移动网络测试平台实现虚拟的移动僵尸网络。

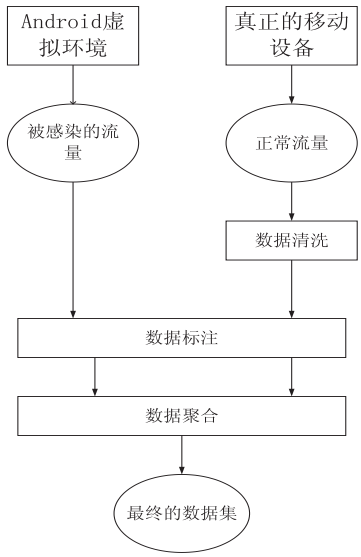

图 1 数据集构建过程

移动僵尸机:虚拟的移动设备被重新封装的真正移动僵尸机所感染,将它们原始 C&C 服务器的 IP 和 URLs 地址重新替换成新的虚拟 C&C 服务器的地址。相同的方法在文献[32]中也有研究,在一个实验环境中,Geinimi、DroidKungFu-B 和 DroidKungFu 僵尸机样本修改新设置执行网络连接。

虚拟的 C&C 服务器:M. Eslahi 等在文献[9]中指出,僵尸机的通信模式和特征可以用来区分僵尸网络和正常的网络活动。另一方面,移动僵尸机大部分最初的 C&C 服务已在安卓恶意软件基因组项目数据集中被发现并关闭。因此,为了能够在实验平台上模拟一个完整功能的移动僵尸网络,就必须植入虚拟的 C&C 服务器。

4.2 生成正常数据流量数据集

虽然在模拟环境中同样可以生成正常的流量,为了能生成更真实的数据,许多移动设备需要安装一个网络嗅探器模块来收集网络流量。文献[32]提到根据目前的研究,4 到 8 个移动设备收集真实数据需要持续两个星期到三个月。然而,有更多的设备就可以更可靠和准确地收集数据。

4.3 数据清理

数据清理是数据集预处理的主要部分,特别是涉及到人为因素。与控制环境(如实验平台)不同,现实世界的数据通常是不完整的(如缺乏感兴趣的某些属性),会包含有噪声、错误、异常数据等。因此数据清理主要应用于收集正常流量数据,平滑噪声数据,识别或删除错误数据,以及解决数据的不一致问题。

4.4 数据标注和聚合

将恶意和正常的数据进行标注可以促进和评价过程。此外,收集的流量数据也是基于原始应用程序的

标注。最后将这两个数据聚合,创造出最终的数据集。研究人员可以从最终的数据集中提取他们所需要的功能,去进行未来的分析研究。

5　结束语

针对目前移动僵尸网络的发展还不完善的现状,为杜绝其现存和未来的危害,在详细介绍其特点和检测方式的基础上,分析了当前移动僵尸网络的数据集和数据样本,并提出了对现有的数据集和数据样本进行改进的方法。在实际的现实世界中,大多数真实的移动僵尸网络是通过 HTTP 协议在互联网上进行通信的。大部分的研究都是针对基于 HTTP 的移动僵尸网络数据集的分析。因此,只有通过对移动僵尸网络的数据合理的采集、分析、清理,才能区分出什么是合法有效的数据。但目前对于移动僵尸网络的研究还处于起步阶段,需要进行更进一步的研究,给大家提供更方便、快捷的移动网络服务。

参考文献:

[1] Eslahi M, Salleh R, Anuar N B. Bots and botnets: an overview of characteristics, detection and challenges[C]//Proceedings of the IEEE international conference on control system, computing and engineering. [s. l.]: IEEE, 2012: 349–354.

[2] Flo A R, Josang A. Consequences of Botnets spreading to mobile devices[C]//Proceedings of the 14th Nordic conference on secure IT systems. [s. l.]: [s. n.], 2009: 37–43.

[3] F-Secure. F-Secure mobile threat[R]. [s. l.]: F-Secure, 2013.

[4] Kalige E, Burkey D, Director I P S. A case study of Eurograbber: how 36 million euros was stolen via malware[M]. [s. l.]: [s. n.], 2012.

[5] Balhare Z J, Gulhane V S. A study on security for mobile devices[J]. International Journal of Research in Advent Technology, 2014, 2(4): 196–203.

[6] Liao Q, Li Z. Portfolio optimization of computer and mobile botnets[J]. International Journal of Information Security, 2014, 13(1): 1–14.

[7] Leavitt N. Mobile security: finally a serious problem? [J]. Computer, 2011, 44(6): 11–14.

[8] Lee H, Kang T, Lee S, et al. Punobot: mobile botnet using push notification service in android[C]//International workshop on information security applications. [s. l.]: Springer International Publishing, 2013: 124–137.

[9] Eslahi M, Hashim H, Tahir N M. An efficient false alarm reduction approach in HTTP-based botnet detection[C]//Proceedings of the IEEE symposium on computers & informatics. [s. l.]: IEEE, 2013: 201–205.

[10] Rodríguez-Gómez R A, Maciá-Fernández G, García-Teodoro P. Survey and taxonomy of botnet research through life-cycle [J]. ACM Computing Surveys, 2013, 45(4): 45.

[11] HTC smartphones left vulnerable to bluetooth attack[EB/OL]. 2009-07-14. http://www.cio.com/article/497146/HTC_Smartphones_Left_Vulnerable_to_Bluetooth_Attack.

[12] Miller C, Mulliner C. Fuzzing the phone in your phone[C]//Black hat technical security conference. USA: [s. n.], 2009.

[13] LaPolla M, Martinelli F, Sgandurra D. A survey on security for mobile devices[J]. IEEE Communications Surveys & Tutorials, 2013, 15(1): 446–471.

[14] Mohite S, Sonar P R S. A survey on mobile malware: a war without end[J]. International Journal of Computer Science and Business Informatics, 2014, 9(1): 23–35.

[15] Eslahi M, Salleh R, Anuar N B. MoBots: a new generation of botnets on mobile devices and networks[C]//Proceedings of the IEEE symposium on computer applications and industrial electronics. [s. l.]: IEEE, 2012: 262–266.

[16] Hachem N, Ben Mustapha Y, Granadillo G G, et al. Botnets: lifecycle and taxonomy[C]//Proceedings of the conference on network and information systems security. [s. l.]: [s. n.], 2011: 1–8.

[17] Jae-Seo L, Hyun-Cheol J, Jun-Hyung P, et al. The activity analysis of malicious HTTP-based botnets using degree of periodic repeatability[C]//Proceedings of the international conference on security technology. [s. l.]: [s. n.], 2008: 83–86.

[18] Mulliner C, Seifert J P. Rise of the iBots: owning a telco network[C]//Proceedings of the 5th international conference on malicious and unwanted software. [s. l.]: [s. n.], 2010: 71–80.

[19] Zeng Y, Shin K G, Hu X. Design of SMS commanded-and-controlled and P2P-structured mobile botnets[C]//Proceedings of the fifth ACM conference on security and privacy in wireless and mobile networks. [s. l.]: ACM, 2012: 137–148.

[20] Hua J, Sakurai K. Botnet command and control based on short message service and human mobility[J]. Computer Networks, 2013, 57(2): 579–597.

[21] Silva S R S C, Silva R M P, Pinto R C G, et al. Botnets: a survey[J]. Computer Networks, 2013, 57(2): 378–403.

[22] Zhou Yajin, Jiang Xuxian. Dissecting Android malware: characterization and evolution[C]//Proceedings of the symposium on security and privacy. [s. l.]: IEEE, 2012: 95–109.

[23] Eslahi M, Rostami M R, Hashim H, et al. A data collection approach for mobile botnet analysis and detection[C]//IEEE symposium on wireless technology and applications. Kota Kinabalu, Malaysia: IEEE, 2014: 199–204.

[24] Morrow B. BYOD securitychallenges: control and protect your most sensitive data[J]. Network Security, 2012(12): 5–8.

[25] Armando A, Costa G, Merlo A. Bring your own device, securely[C]//28th annual ACM symposium on applied computing. Coimbra, Portugal: ACM, 2013.

(下转第 110 页)

5 实验结果分析

5.1 手机端生成公钥和私钥

使用 Base64 编码处理并转换为 String 类型的手机端公钥和私钥如下所示：

手机端生成的私钥：[redacted]BMGByqGSM49AgEGCCqGSM49AwEHBHkwdwIBAQQgxSZ
4d1F6oseBK8VJsxUq5Fduuom3kmnF8i+phWg4vkqgCgYIKoZIzj0DAQehRANCAATpN8GDypODC8af
2NBLyhiRzYKf0XuRcy3Mby5MEOrgeF/eitXWPZ3kJ/I5EJ9rxZrS3l1hBTYsCXJBZb99gH76
手机端生成的公钥：MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE6TfBg8qTgwvGn
9jQS8oYkc2Cn9F7kXMtzG8uTBDq4Hhf3orV1j2d5CfyORCfa8Wa0t5dYQU2LAIyQWW/fYB++g==

5.2 手机端敏感数据加密和数字签名

待加密的敏感数据如下所示：

敏感数据：{phone_num:"+86185153[redacted]",phone_imsi:"460015351[redacted]",sequence:"null",
receive_time:"null",mobile_current_score:0,phone_imei:"354273059996756",phone_version:"4.
3",phone_type:"GT-N7108",curr_version:"1.2.35",location:[],pics_lack:0,model_flag:5,screen_on
off:[],icons_url:[],app_flow:{"360 手机助手":0}}

使用 Base64 编码处理并转换为 String 类型的加密后敏感数据为：

BHEY0n6rWN4i2UXQPqzBaBSOpNT/CA6soMJFSVfHEpJQXc43tQdTjzQ7T4lY7pcPqjipnAbDlk1gok3
5OU+ugMCjIV6896OvkPIAuqcK4NH/PvQLL5QEcERQbrQmIcpLdPx0eeiAZt47sFwm8s8/hAedLHxV+
jRJdwWEJINIjHlQNmbM+xJI5+uZR8ml+6mALN49v/w2rmh4SHG1IbqyBFEMWbtXV55V6QIhiaeJA8
E0muHs+PUgYrMhNT63BMuE8sVXFeYZeydoHo22HoNZQkfFU1KI608bWU+3ViB+f/8LF+Xmhx0Qk
UVQrgWbOT+rdXMIzLA44KCldhGOMvuXtqN3qFInyIVXrD2gNlyZNzD/hDqZ8VxLJnE5x7PLZAdX282
Rh773rTK3stXog7n2IRGq5yoEXV282NBsYvGJD6fzV/ejvy1a1nEyxOY3lnTRYOcxAuHt/vmCu0hvTjkP
z52RNH5JTAPvQgRnQA4+yRKzrvVyB6U8coTPlXlwNjTkzuq1G8JtQ==

对加密后的敏感数据生成摘要信息并进行签名：

签名处理后的字符串:MEQCICA1y/9uyvwrRWK+mrnMqXZT51xDnr5iBFST57lgS7DZAiBKg8l8vf
+6yx5dpvpwPngL5nbUaU/b4rQXJLVkeQcQaA==

5.3 服务器端验证签名和解密

Server 签名验证成功。
还原为原始数据：{phone_num:"+8618515351[redacted]",phone_imsi:"460015351[redacted]",sequence:
"null",receive_time:"null",mobile_current_score:0,phone_imei:"354273059996756",phone_versi
on:"4.3",phone_type:"GT-N7108",curr_version:"1.2.35",location:[],pics_lack:0,model_flag:5,scre
en_onoff:[],icons_url:[],app_flow:{"360 手机助手":0}}

6 结束语

文中设计的方案在 Android 智能终端和 Web 服务器之间的数据交互使用了第三方 Bouncy Castle、SpongyCastle 中支持的 ECIES 实现椭圆曲线数据加密和解密，使用JDK8中的SHA1 withECDSA签名算法实现通信数据的签名和验证，保证了移动互联环境下智能终端和服务器端数据通信的安全性、完整性、一致性和不可抵赖性。通过综合采用椭圆曲线加密算法、消息摘要算法、数字签名使得移动互联网项目具有更高的安全性和实用性。

参考文献：

[1] 彭 丽，李光明. 移动办公业务在行业内的应用分析[J]. 办公自动化，2014(5)：57-59.

[2] 刘 军. 云计算应用模式下的移动互联网安全问题[J]. 硅谷，2013(16)：141.

[3] 班晓芳，佟 鑫. 移动互联网安全威胁分析[J]. 电信技术，2012(7)：77-78.

[4] 房秉毅，张云勇，徐 雷. 移动互联网环境下云计算安全浅析[J]. 移动通信，2011，35(9)：25-28.

[5] Stallings W. Cryptography and network security principles and practice[M]. 5th ed. Beijing：China Machine Press，2011.

[6] Davies J. Implementing SSL/TLS using cryptography and PKI[M]. USA：Wiley，2011.

[7] 白永祥. 基于 ECDSA 的智能卡软件设计与实现[J]. 电子设计工程，2015，23(14)：29-32.

[8] 麻胜海. 基于椭圆曲线的数字签名在移动办公中的应用[J]. 科技信息，2010(5)：85-86.

[9] 张凤元，武美娜. ECDSA 的算法改进及其标量乘法的选取[J]. 微计算机信息，2009，25(8-3)：168-169.

[10] 范云海. 集成加密方案 ECIES 的设计与验证[J]. 信息技术，2012(1)：115-117.

[11] 周卫宁，刘友刚. 移动互联网发展技术与安全问题[J]. 科技传播，2012(3)：210.

[12] 胡向东，魏琴芳，胡 蓉. 应用密码学[M]. 北京：电子工业出版社，2011.

[13] 石 莎. 移动互联网络安全认证及安全应用中若干关键技术研究[D]. 北京：北京邮电大学，2012.

[14] 程耕国，覃 科. 基于 Bouncy Castle 的 J2ME 网络安全[J]. 计算机与现代化，2006(1)：108-110.

[15] 陈尚义. 移动互联网安全技术研究[J]. 信息安全与通信保密，2010(8)：34-37.

(上接第 105 页)

[26] Eslahi M，Naseri M V，Hashim H，et al. BYOD：current state and security challenges[C]//IEEE symposium on computer applications & industrial electronics. Peneng，Malaysia：IEEE，2014.

[27] Bailey M，Cooke E，Jahanian F，et al. A survey of botnet technology and defenses[C]//Proceedings of the cybersecurity applications & technology conference for homeland security. [s. l.]：[s. n.]，2009：299-304.

[28] Abdullah Z，Saudi M M，Anuar N B. Mobile botnet detection：proof of concept[C]//2014 IEEE 5th control and system graduate research colloquium. [s. l.]：IEEE，2014：257-262.

[29] Jiang X，Zhou Y. A survey of Android malware[M]//Android malware. New York：Springer，2013：3-20.

[30] Kiukkonen N，Blom J，Dousse O，et al. Towards rich mobile phone datasets：lausanne data collection campaign[C]//Proc of ICPS. Berlin：[s. n.]，2010.

[31] Deshotels L，Notani V，Lakhotia A. DroidLegacy：automated familial classification of Android malware[C]//Proceedings of ACM SIGPLAN on program protection and reverse engineering workshop. San Diego，CA，USA：ACM，2014.

[32] Shabtai A，Tenenboim-Chekina L，Mimran D，et al. Mobile malware detection through analysis of deviations in application network behavior[J]. Computers & Security，2014，43：1-18.