移动互联环境下数据通信安全技术的应用研究

吴明礼,陈 斌
(北方工业大学 计算机学院,北京 100144)

摘 要:随着信息技术的迅速发展,移动智能终端已经越来越普及,各种各样的手机应用程序给人们的日常生活和工作带来了便利。然而,移动互联网环境下数据通信安全面临着非法篡改、信息窃取、数据丢失等各种威胁。对移动互联环境下智能终端与服务器之间的网络通信安全策略进行了研究,借鉴互联网环境下的相关技术,充分考虑移动互联网的特点,提出了一种综合使用 SHA、数字签名、椭圆曲线算法等技术的安全策略,保证智能终端和服务器在移动互联网环境下数据交互的安全性、完整性、一致性、不可抵赖性。该安全策略经过分析、编码实现与测试,具有较好的效果,在移动互联网项目中具有一定的实用和推广价值。

关键词:移动互联网;通信安全;完整性;数字签名;加密
中图分类号:TP39 **文献标识码**:A **文章编号**:1673-629X(2016)11-0106-05
doi:10.3969/j.issn.1673-629X.2016.11.024

Research on Application of Data Communication Security Technology in Mobile Internet Environment

WU Ming-li, CHEN Bin
(School of Computer Science, North China University of Technology, Beijing 100144, China)

Abstract: With the rapid development of information technology, mobile intelligent terminal has become more and more popular, and a variety of mobile phone applications make people's daily life and work more convenient. However, in the mobile Internet environment, data communication security is facing various threats such as illegal tampering, information theft, data loss and so on. The research on security policy of the network communication is carried out between the intelligent terminal and the server under the mobile Internet environment, and a comprehensive security strategy for the use of SHA, digital signature, elliptic curve algorithm and so on is proposed by reference of the related techniques and considering the characteristics of mobile Internet, ensuring the security, integrity, consistency and non repudiation of the data interaction between the mobile terminal and the server in the mobile Internet environment. This security strategy has good effect through analysis and encoding implementation and testing, and has a certain practical and promotional value in the mobile Internet project.

Key words: mobile Internet; communication security; integrity; digital signature; encryption

1 移动互联网通信安全现状分析

在移动互联网迅速发展和智能终端设备日益普及的今天,用户通过智能终端浏览网页、查看新闻资讯、查询和预约周边位置各种生活服务越来越普遍[1]。移动数据网络利用无线信道传递信息,由于无线信道的开放性,任何人都可以接收无线电波,从而为信息的截取、篡改、干扰等提供了可能性,给信息的安全带来诸多威胁[2]。

在移动互联网下,尤其是在移动电子商务中,网络通信数据安全面临的问题主要包括以下几个方面:

(1)安全性:在无线网络中传送的用户隐私数据可能被非法窃取。

(2)完整性:用户的敏感信息或者电子商务交易数据,在无线网络传输过程中,由于某些原因使信息在传输中遭到破坏,接收方收到的信息并非是发送方发送的完整数据[3]。

收稿日期:2016-01-14 **修回日期**:2016-04-13 **网络出版时间**:2016-10-24
基金项目:北京市属高等学校创新团队建设与教师职业发展计划项目(IDHT20130502);北京市教育委员会科技发展计划面上项目(KM201410009008);北方工业大学优势学科项目
作者简介:吴明礼(1978-),男,讲师,研究方向为电子商务、大数据处理等。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20161024.1105.016.html

(3)一致性:数据在网络传输过程中,遭到了非法篡改,使得接收方收到的数据与发送方发送的数据不一致。

(4)不可抵赖性:发送消息的一方对发送消息的行为予以否认,没有足够的信息来证明已经发生的消息发送行为。

2　移动互联网通信安全设计方案

文中借鉴互联网中比较成熟的相关技术,结合移动互联网的特点,探索基于移动互联网的数据通信安全策略。对移动互联网数据交换的隐私数据使用椭圆曲线密码算法进行加密处理,对一些非核心非隐私的数据采用明文传输,这样既充分保证数据处理和传输的效率,又保证了关键信息在移动互联网中交互过程的安全性[4]。文中设计方案综合采用 SHA、数字签名、椭圆曲线加密算法等技术保证智能终端 Android 应用程序和 Web 服务器在移动互联网中数据交互的安全性、完整性、一致性、不可抵赖性[5]。为了保证手机端 app 和服务器之间数据通信的安全,使用椭圆曲线加密算法对隐私数据进行加密,保证数据的安全性;使用 SHA 生成数据摘要信息,从而保证数据的完整性、一致性;使用数字签名技术保证数据的不可抵赖性[6]。

图 1 为手机端到服务器单向数据的处理流程,而服务器反馈给手机端的单向数据处理流程是类似的。文中将按照图 1 中的设计方案,重点讲解手机端向服务器端单向数据的处理流程。

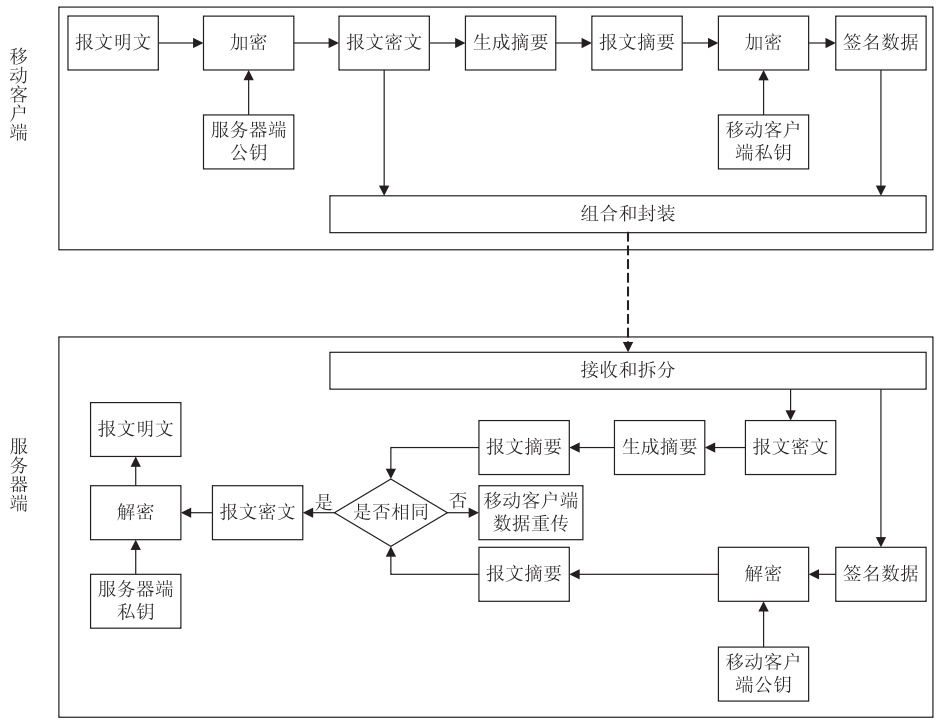

图 1　手机端访问服务器单向通信安全设计方案

3　采用的关键技术

3.1　椭圆曲线密码体制

椭圆曲线密码体制(Elliptic Curve Cryptography, ECC)利用有限域上椭圆曲线点集构成的群实现了离散对数密码算法,其安全性基于椭圆曲线上求离散对数问题的困难性[7]。椭圆曲线密码是密码学的重要分支之一,它可以用来加密数据,进行数字签名或者在安全通信的开始阶段进行密钥交换[8]。由于椭圆曲线密码体制具有计算量小、处理速度快、存储空间小、带宽要求低等优点,更加适合于在移动互联网中的智能终端使用[9]。RSA 和 ECC 同属于公开密钥密码体制,表 1 和表 2 对两种算法进行了比较。

表 1　RSA 与 ECC 理论基础比较

算法	数论基础	安全性基础	安全密钥长度
RSA	欧拉定理	大素数的因子分解	1 024 位
ECC	离散对数	椭圆曲线离散对数问题	160 位

表 2　RSA 与 ECC 等价安全强度的密钥长度比较

RSA 密码长度/位	ECC 密码长度/位	RSA/ECC 密码长度比率
512	106	5:1
1 024	160	7:1
2 048	210	10:1
21 000	600	35:1

从表 2 可以看出,在相同安全强度下,ECC 算法的密钥长度明显要小很多。此外,在密钥对的生成、签名

及认证方面,ECC 的实现速度相对于 RSA 要快很多[10]。文中方案的加密采用基于 ECC 的综合加密方案(Elliptic Curve Integrated Encryption Scheme,ECIES)。

3.2 消息摘要算法

使用消息摘要主要是为了确保信息传输完整一致,它可以为任何文件产生一个独一无二的“数字指纹”,一般用于数字签名[11]。如果文件发生任何改变,其生成的消息摘要将会发生变化。常用的消息摘要算法有 SHA 和 MD5,它们都是基于散列算法的单向加密算法。表 3 是对 SHA1 与 MD5 两种摘要算法的比较。

表 3 SHA1 与 MD5 比较

算法	生成摘要长度	执行速度	抗攻击强度
SHA1	160 位	慢	高
MD5	128 位	快	低

SHA1 是在 MD5 的基础上发展而来的,对于强行攻击具有更强的抗攻击强度[12]。文中使用 SHA1 来生成消息摘要。

3.3 数字签名

数字签名算法是非对称加密算法和消息摘要算法的结合体,用来验证数据的完整性,确保数据来源的可认证性和数据发送行为的不可否认性[13]。消息摘要算法是数字签名算法的必要组成部分,用来验证数据的完整性。数字签名包括签名和验证两个过程。在签名和验证方面,采用 ECDSA(Elliptic Curve Digital Signature Algorithm)。ECDSA 算法是椭圆曲线加密算法 ECC 与 DSA 算法的结合,具有速度快、强度高、签名短等优点。根据使用的摘要算法的不同,签名算法主要分为 MD5 和 SHA 两大系列,如 NONEwithECDSA、SHA1withECDSA、SHA256withECDSA、SHA512withECDSA 等。文中方案使用的是 JDK8 中签名抽象类 Signature 支持的签名算法 SHA1withECDSA,它使用的消息摘要算法是 SHA1。

3.4 Bouncy Castle 与 Spongy Castle

文中设计方案中涉及到椭圆曲线加密和解密时,使用的都是椭圆曲线集成加密方案 ECIES。在 JDK8 中支持的加密算法包括 ECIES,但是在安装的 JDK8 中并不存在支持该算法的 Provider,所以需要使用第三方支持该算法的 Provider。Provider 是实现部分或者全部 Java Security 相关方法的类。

Bouncy Castle 提供了一个轻量级的密码学 API,它是一个 Java 密码扩展(JCE)的提供者[14]。在 Web 服务器端代码中公私钥生成和加密、解密功能实现中使用 Bouncy Castle 这个 Provider。由于在 Android 平台已经内置了一个精简过的旧版本 Bouncy Castle,这就导致了使用一个新版本的该类库会出现类加载冲突。Spongy Castle 对 Bouncy Castle 做了一些修改,使它能在 Android 平台上更好的工作。因此,在 Android 端代码中的公私钥生成和加密、解密功能实现中使用的是 Spongy Castle。

4 设计方案实现

文中研究方案基于移动互联网下的一个综合性项目,包括 Web 服务器端、Android 端 app,实现广告图片推送和展示。在 Android 端 app 和服务器进行网络数据交互的过程中,会涉及一些敏感数据。对于非敏感数据直接采用明文传输,仅对敏感数据进行加密和签名处理。对于大量原始数据进行签名会耗费很多系统资源和时间,需要采用摘要算法将原始数据生成一串简单的摘要信息,然后再对摘要信息进行签名[15]。服务器端接收到手机端发送过来的信息后,对原始数据重新生成摘要信息,与传送过来经过解密得到的摘要信息进行比对。如果不匹配的话,则不再执行后续的相关操作,说明服务器端接收到的数据的可靠性和完整性存在问题,告知手机端需要重传信息。如果匹配的话,则对接收到的加密数据进行解密处理,得到 Android 端传送的真正明文信息。

目前,网络数据传输主要使用 xml 和 json 两种数据格式。文中方案采用 json 作为 Android 手机应用程序和 Web 服务器之间的数据交互格式。它能有效降低交互的数据量,并且具有较快的解析速度。

4.1 公私钥对的生成和分发

服务器端使用 Bouncy Castle 支持的 ECIES 算法来生成唯一的服务器端公钥和私钥。在创建 KeyPairGenerator 实例时,使用 Bouncy Castle 这个 Provider 提供的 ECIES 算法作为参数。服务器端私钥由服务器端自己保留,公钥嵌入到 Android 手机 app 程序中。用户安装该手机端应用程序,相当于就已经持有了指定服务器的公钥。

每一个 Android 手机端用户在和指定服务器进行真正的数据交互之前,需要首先生成一对公私钥。私钥由手机端应用程序自己保留,用来解密数据或者对数据签名。对于生成的公钥,则需要通过加密后提交给指定服务器。在创建 KeyPairGenerator 实例时,使用 Spongy Castle 这个 Provider 提供的 ECIES 算法作为参数。安装在手机中的该 app 第一次运行的时候,会使用 Spongy Castle 插件借助于椭圆曲线集成加密算法生成手机端公钥和私钥。

Android 手机 app 将生成的公钥提交给指定服务器的流程如下:

(1)借助于服务器端公钥对手机端生成的公钥、手机设备号使用椭圆曲线加密算法进行加密,传递给

服务器端。

(2)服务器端接收到手机端传送来的加密数据后,使用服务器端私钥借助椭圆曲线算法进行解密,获取传送过来的手机设备号和公钥。

(3)服务器端查询数据库表中是否已经存在该设备号的记录。如果设备号不存在,则表示是新的手机用户首次访问,将公钥信息直接保存;如果设备号存在,则表示是已经存在的用户,则对数据库中之前保存的该手机终端的公钥进行更新。

(4)如果保存操作成功,则返回给手机终端相应的 json 信息,确认服务器端成功保存了手机端的公钥信息。然后,移动终端和服务器端就可以正常进行后续的信息交互了。

4.2　Android 手机端对隐私数据加密和签名

文中移动互联网项目中手机端应用程序需要向服务器端传送的数据,包括敏感数据部分和非敏感数据部分。对于非敏感数据部分采用明文传输,提高数据的处理和传输效率。对于敏感数据使用椭圆曲线加密算法,借助于手机端应用程序内部自带的服务器端公钥和自身私钥,进行数据加密和数字签名处理。

对于敏感数据的加密和签名处理流程如下:

(1)手机智能终端使用椭圆密码算法 ECIES、服务器端公钥,对待传输的敏感数据进行加密处理。

(2)使用 SHA 算法对加密后的数据生成摘要信息。

(3)使用椭圆密码算法、智能终端的私钥对摘要信息生成数字签名。

(4)使用 ECIES 加密后的密文数据和生成的数字签名拼接为事先和服务器端协商好的 json 串的格式,通过移动互联网发送给指定服务器。

流程图如图 2 所示。

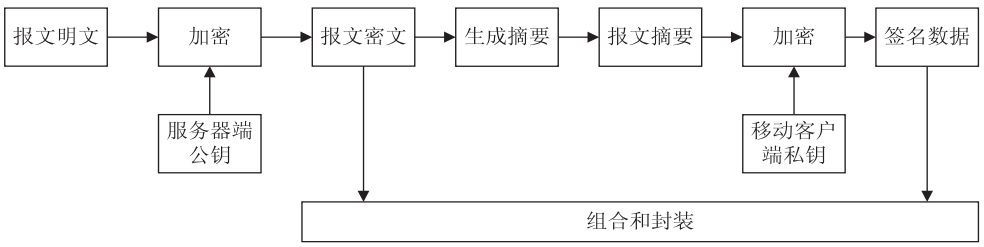

图 2　手机端对隐私数据加密和签名流程

4.3　服务器端接收数据进行签名验证和解密

文中移动互联网项目的服务器端接收到 Android 手机终端应用程序发送过来的数据,对该 json 格式数据进行分离和提取,得到数字签名和报文密文,进行签名验证和密文解密处理。

服务器端接收数据后进行签名验证和解密处理的流程如下:

(1)服务器对智能终端发送过来的数据,按照事先商定的协议对数据进行拆分,得到报文密文和数字签名。

(2)对报文密文使用 SHA 算法生成新的摘要信息。

(3)对接收到的数字签名使用智能终端的公钥进行解密,得到智能终端生成的报文摘要信息。

(4)比较新生成的摘要信息与解密后的智能终端摘要信息是否完全相同,如果不相同则说明数据在传输过程中出现了问题,不能保证数据的完整性和一致性。

(5)如果比较结果是一致的,则对接收到的报文密文使用服务器的私钥进行解密得到真正的明文信息。

(6)如果比较结果不一致,则返回给手机终端相应的 json 信息,让手机端进行数据重传。

流程图如图 3 所示。

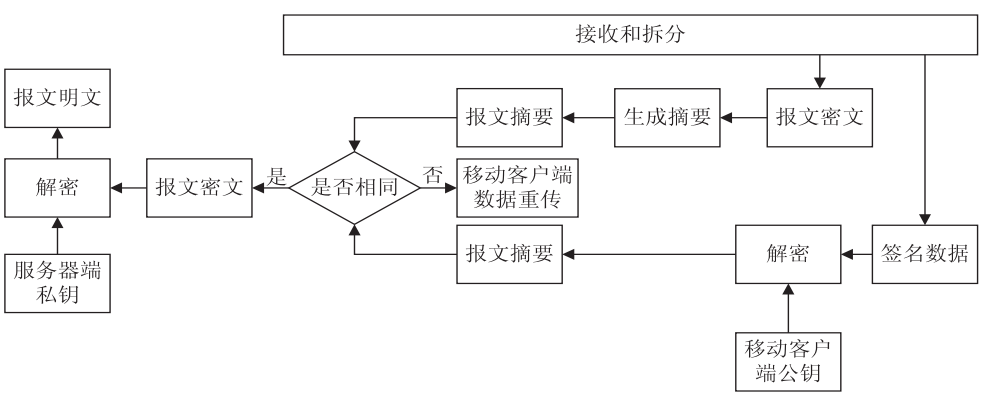

图 3　服务器端验证签名和解密数据流程

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.