iOS 备份机制中隐私威胁问题的分析

李柏岚，　谷大武，　李卷孺，　孙　明
（上海交通大学 计算机科学与工程系，上海 200240）

【摘　要】目前，iOS 安全研究主要在应用程序安全性检测、安全模型剖析、漏洞和数据保护机制分析等方面，对于 iOS 备份机制的安全性缺乏深入系统地研究。备份是 iOS 系统中惟一合法获得设备内部数据的渠道，但是备份数据缺少必要防护措施，用户数据安全和隐私受到潜在威胁。通过描述备份分析的方法，进而对备份存储数据进行深入理解，发现其存在严重隐私威胁，忽视对第三方应用程序数据信息的保护，最后评估了备份机制潜在的安全影响并给出提高备份安全性的建议。

【关键词】备份机制；隐私泄漏；第三方应用
【中图分类号】TP309　　【文献标识码】A　　【文章编号】1002-0802(2012)02-0025-04

Analysis on Privacy Threats in iOS Backup Mechanism

LI Bai-lan，　GU Da-wu，　LI Juan-ru，　SUN Ming
(Department of Computer Science, Shanghai Jiaotong University, Shanghai 200240, China)

【Abstract】The security research of iOS mainly focuses on detection application security, privacy vulnerabilities, analysis of security model, and data protection mechanism, etc., while less in-depth study on backup mechanism security. Backup is the only certificated channel for acquisition of the data inside iOS devices. However, the transmitted data is short of necessary protective measures, thus leading to security and privacy threats. The method for backup analysis is described, and in-depth understanding of the backup data reveals that the serious privacy threats exist in iOS backup the protections of the third-party application data neglected. Finally, potential security vulnerabilities of the back-up mechanism are evaluated, and the security suggestions for protection of backup data proposed.

【Key words】backup; privacy leakage; third-party application

0 引言

随着移动智能终端的日渐普及，人们开始对它的功能需求有了进一步的提高。新一代的智能移动终端除了语音通信之外，还能播放影音、浏览网页、游戏娱乐等。更重要的是，用户可以从电子市场上下载并安装第三方开发的应用程序。在所有的智能移动设备中，苹果的 iPhone 和 iPad 深受用户和安全研究人员关注。这些设备的核心是其中的操作系统——iOS。

收稿日期：2011-10-31。
基金项目：国家自然科学基金（批准号：61100209）、上海市高新技术产业化重点项目资助。
作者简介：李柏岚（1987-），男，硕士研究生，主要研究方向为软件安全；谷大武（1970-），男，教授，博士生导师，主要研究方向为密码分析与设计、信息分析与密码工程、计算机安全体系结构；李卷孺（1983-），男，博士研究生，主要研究方向为软件安全；孙　明（1986-），男，硕士研究生，主要研究方向为软件安全。

由于苹果对 iOS 采取闭源不公开的政策，开发人员和用户对其安全机制了解甚少。目前安全研究人员给出了一些安全模型[1]和数据保护机制[2]的细节，但仍较难获取 iOS 内部的信息。黑客社区工作者挖掘系统漏洞[3]、分析沙箱模型和数据加密[4]。电子取证专家通常需要通过越狱来获得他们需要的信息，但越狱会改变系统原有的状态，所以他们更倾向于非入侵的方式。

虽然苹果有着严格的安全保护措施以避免数据泄漏，但它留下了一条供用户进行数据读写的通道。这就是 iTunes 的同步、备份与恢复机制，其中最值得关注的就是备份。iTunes 会自动为 iOS 设备创建备份，日后如需恢复到以前备份的状态则可使

用此备份。备份可以进行任意的复制，用于在其他机器上进行恢复。iTunes 的备份恢复机制为用户带来了便利也产生了安全问题。通过备份，大量的数据保存到用户电脑中，对用户隐私造成威胁。然而学术界的研究集中在检测在 iOS 应用程序中的隐私泄漏[5]，备份机制的研究仅局限于取证分析[6-7]。文献[8-9]从 iOS 备份机制着手，分析备份机制中存在的隐私泄露威胁。

1 备份分析方法

这里主要描述分析备份中隐私数据的方法。分析过程分成 3 个步骤：①生成备份；②解析备份；③分析备份。过程如图 1 所示。

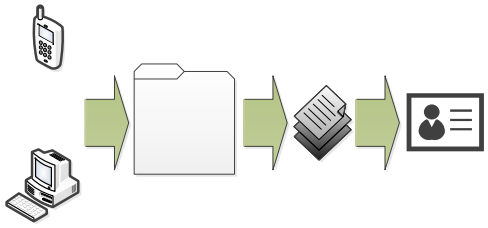

图 1 iOS 备份解析过程

1.1 生成备份

iPhone 或 iPad 连接到电脑的时候，iTunes 将自动同步电脑与设备之中的数据，创建一个备份。也就是说，如果 iOS 设备曾经与装有 iTunes 的电脑连接过，那么备份文件已经保存在电脑中备份目录。

如果没有备份，则通过如下两种不同的方法来创建备份。第一种是使用 iTunes 或者 iTunes 提供的 AppleMobileBackup.exe 来进行备份。iTunes 与 iOS 设备之间通过苹果文件通信（AFC，Apple File Communication）协议来进行通信。另一种创建备份的方法是使用 Libimobiledevice，它是一个支持 AFC 数据交互协议的 C 语言库。它支持 iOS 的备份功能，还支持同步，获取系统信息等功能。所以这也是一种创建备份的方法，这种方式的好处是它并不依赖于 Windows，在 Linux 下同样可以运行，开发者可以更自由地控制它的通信。

1.2 解析备份

iOS 备份目录名是被备份设备的惟一设备标识符（UDID，Unique Device Identification）。它由 40 位 16 进制字符组成，如：2b6f0cc904d137be2e1730235f5664094b831186。备份目录下的文件名都通过 SHA-1 哈希编码，所以无法辨别文件信息。利用备份中的 Manifest.mbdb 和 Manifest.mbdx 文件可以解析出备份的结构。

Manifest.mbdb 是备份的索引文件。它由一个定长的头部和若干定长的记录构成。

Manifest.mbdx 记录着文件信息，如：文件所在域、路径，哈希值，文件大小等。

1.3 分析备份

遍历经过解析后的备份目录，分析检查可疑文件。备份中大量的数据都是用 iOS 原生支持的 Sqlite 数据库格式保存，文中使用 Sqlite Database Browser 来分析这些文件中的内容。Property List（Plist）也是 iOS 支持的文件格式，它用来保存配置信息，使用 Plist Editor 来读取其中的信息。

2 备份中的隐私信息

这里主要总结分析的结果，重点关注与用户隐私相关的信息。这些信息分成两大类，系统内置信息和第三方应用程序信息。

2.1 系统内置信息

表1列举了iOS系统的内置信息。

表 1 iOS 备份中的系统内置信息

信息	路径	格式	备注
通讯录	Library/AddressBook/AddressBook.sqlitedb	sqlite	通讯录
通话记录	Library/CallHistory/call_history.db	sqlite	通话记录
短信	Library/SMS/sms.db	sqlite	短信
Email 账户	Library/Preferences/com.apple.accountsettings.plist	plist	同步 email 账户
位置	Library/Caches/locationd/consolidated.db	sqlite	基站和无线位置数据
照片	Media/DCIM	jpg	照片
	Media/PhotoData/Photos.sqlite	sqlite	照片基本信息
	Media/PhotoData/PhotosAux.sqlite	sqlite	照片辅助信息
日历	Library/Calendar/Calendar.sqlitedb	sqlite	日历中的事件
备忘录	Library/Notes/notes.sqlite	sqlite	备忘录
键盘	Library/Keyboard/Dynamic-text.dat	文本	键盘缓存
Safari	Library/Safari/Bookmarks.plist	plist	书签
	Library/Safari/History.plist	plist	浏览记录

通讯录。通讯录是iOS中包含信息最多也是被其他程序调用最多的一个数据库，它储存在AddressBook.sqlitedb文件中，记录着用户所有联系人的信息，包括电话号码、邮箱地址和住址等。AddressBookImages.sqlitedb记录着联系人的照片。

通话记录。通话记录保存在call_history.db。记录着所有历史电话记录。每一条电话记录它包含通话的日期、通话时长和对应的电话号码。

短消息。短消息存在sms.db中，记录着手机中所有能读取的短消息。每条记录包括日期、时间、电话号码、消息内容以及状态（发送或者接收）。

邮件账户。iPhone的同步账户保存在com.apple.accountsettings.plist中，这个账户主要用来同步通讯录和日历。账户的密码和具体的邮件内容并没有保存。

位置信息。consolidated.db记录着大量的经纬度坐标和获取该经纬度的时间戳。这些数据通过基站的三角定位获得保存于CellLocation表格中。WifiLocation表格中还记录着无线路由器的位置和MAC地址。

照片。照片保存在MediaDomain下，DCIM.Photos.sqlite中记录着照片的基本信息如拍摄时间、分辨率等。PhotoAux.sqlite包含照片的拍摄地点的坐标位置信息。

其他。除了之前所列之外，系统内部信息还包括日历、备忘录、键盘缓存、浏览记录、书签等。

2.2 第三方应用程序

备份中还包含着用户安装的第三方应用程序的信息。据统计，每个iOS用户平均安装大约37个应用，而这些应用由全世界各地的开发者提供。他们处理数据的方式各不相同，不局限于Sqlite数据库或是Plist文件。实验统计App Store上最流行的3类程序，下面对每一类进行分析。

（1）即时通讯类应用

即时通讯类应用中，实验选取了Skype、腾讯QQ、飞信、Yahoo Messenger、WhatsApp和Windows Live Messenger，基本上涵盖所有常用的即时通讯软件，如表2所示，发现所有的应用都会记录着用户的账号。实验发现所有的应用都会记录着用户的账号。更为严重的是67%的应用保存聊天记录和好友信息。以WhatsApp为例，备份目录下net.whatsapp.WhatsApp.plist文件中包含手机号码构成的账户名。在ChatStorage.sqlite的ZWAMESSAGE表格中保存着聊天记录的内容、时间、发送者，接收者。在ZWAFAVORITE表格中，记录了好友的姓名以及他们的电话号码。移动官方开发的最新飞信应用，账号和密码都保存在同一文件中。

（2）社交网络类应用

社交网络类应用中，实验选取了新浪微博、Facebook、LinkedIn、人人等应用程序，如表3所示，所有的应用都记录着用户名称或者昵称。新浪微博会将最近的微博内容缓存在数据库中。Facebook记录用户的姓名，同时在名为Friends.db的数据库中记录着好友姓名、地址、电话号码、邮件地址。对于LinkedIn应用，只保存用户的姓名。人人应用没有保存任何关于用户状态、朋友、聊天记录的信息。但是，登陆的用户名和密码以明文形式一起出现。攻击者用这个信息登陆人人就能获得更多用户的隐私信息。

表 2 即时通讯类应用

应用	账号	聊天记录	好友信息
Skype	Library/Preferences/com.skype.tomskype.plist		
腾讯 QQ	Documents/contennts/QQAccountsManager	Documents/contents/#/QQ.db	Documents/contents/#/QQ.db
飞信	Library/Preferences/com.aspire-info.fetion.plist	Documents/#/conversation/sip:#	
Windows Live Messenger	Documents/CurrentUserName.tmp		
Yahoo Messenger	Library/Preferences/com.yahoo.messenger.plist	Documents/yahoo-#.db	Documents/yahoo-#.db
WhatsApp	Library/Preferences/net.whatsapp.WhatsApp.plist	Documents/ChatStorage.sqlite	Documents/ChatStorage.sqlite

表 3 社交网络类应用

应用	用户名	其他
新浪微博	Library/Preferences/com.sina.weibo.plist	最近的微博
Facebook	Library/Preferences/com.facebook.Facebook.plist	好友
LinkedIn	Library/Preferences/com.linkedin.LinkedIn.plist	称谓，姓名
人人	Document/rr_persistence_[id]_object_kRRUserKey	密码（明文）、学校

（3）位置技术类应用

位置技术类应用中，实验选取了大众点评、街旁、丁丁生活、豆瓣活动、陌陌，它们是目前最流行的应用。如表4所示，在大众点评和丁丁地图找不到任何关于位置的信息。而这两个应用在实际使用中提供了大量的基于位置的信息。豆瓣活动应用保存着最后登陆时的位置。街旁将用户账号和访问过的评论缓存在Cache.sqlite中。在表格ZJPLOCATION中记录着坐标，时间和地址。陌陌则会保存附近朋友的详细信息。

表 4 位置技术类应用

应用	位置信息	其他
大众点评 街旁 丁丁生活	Documents/Cache.sqlite	地名、消息
豆瓣活动	Document/CONFIG_Douban.plist	
陌陌	Document/[id].sqlite	账号、附近好友

3 讨论

3.1 影响

从前一节可以看出备份中包含了几乎所有的个人信息，并且获取这些信息的方法非常简单。下面对隐私威胁模型中的每一类信息的影响进行分析。

用户活动相关信息：主要包括短信息、聊天记录、通话记录，不论是系统还是第三方应用程序都直接记录这些数据。通讯录泄漏大量设备使用者朋友的信息，社交类应用程序也会将好友信息保存下来。这些数据对用户隐私形成威胁，造成了直接的损害。

账户相关信息：所有第三方应用程序都会将用户和一个账户关联，实验表明账户信息会随着备份的泄露而泄漏。这些账户的行为等价于用户的行为，账户的匿名性不复存在。

地理位置信息：定位是新一代智能手机特有的重要功能，它被用在导航或者基于位置的应用中。但是，它可以悄悄的记录用户的空间活动信息。iOS系统和第三方应用都会记录用户的位置信息，它们通常与时间一起保存。这样，攻击者通过结合这两部分信息就可以分析出用户何时出现在何地，推断用户过去的行踪。

多媒体信息：照片、视频文件在网络中传播速度极快，有大量因为私人的照片，视频造成的负面新闻，这些数据未经保护散播出去后果难以想象。

3.2 局限

并不是在什么场景下都能成功对备份进行分析。下面两种情况就会对分析造成困难。

用户可以设置密码来锁住iOS设备，这个密码是一个4位的数字。当iOS设备连接到一个新的电脑时，只有密码输入正确后iTunes才会进行备份。但是，对于进行过备份的电脑会保存一份证书文件。攻击者可以利用其他机器上保存的证书文件来绕过密码进行备份。

用户还可以选择加密备份来保护他们的隐私。默认情况下备份是不加密的，用户可以从iTunes中开启加密选项，此后，备份文件全部都经过加密。据苹果官方描述，加密是使用AES-256 CBC来完成。这就意味着直接解密和破解AES难度一样。

3.3 应对措施

对于那些需要对用户数据进行保护的用户，这里建议加锁来保护系统，同时开启备份加密功能。这样可以完全防止隐私泄漏。文中发现第三方应用的程序泄漏了更多的隐私信息，部分原因是开发者没有意识到他们不合理的软件设计会带来隐私威胁。所以，需要提醒开发者不要将用户相关的数据保存在应用程序目录，或者至少对这些数据进行加密。对于那些将用户密码也保存在配置文件中的应用，建议苹果加以更加严格的审查，杜绝这类应用出现在电子市场之上。

4 结语

文中揭示了备份机制带来的潜在威胁，并深入的分析备份中的数据，给出应对措施。通过描述获取备份的和进行数据分析的方法，列举出备份中包含的各类信息。传统方法主要分析系统内置的信息，如：联系人、通话记录等。着重分析了备份数据中第三方应用存在的问题，这些应用程序受到大家的忽视，但他们存在更严重的隐私泄漏的威胁。最后，讨论隐私泄露的影响以及预防的对策。

参考文献

[1] CEDRIC H, JEAN S. iPhone Security Model & Vulnerabilities[R]. United States: HITB SecConf, 2010.

[2] JEAN-BAPTISTE B, JEAN S. iPhone Data Protection in Depth[R].United States: HITB SecConf，2011.

[3] STEFAN E. Exploiting the iOS Kernel[R].United States: Black Hat，2011.

[4] DINO A, DAI Z. Apple iOS Security Evaluation: Vulnerability Analysis and Data Encryption[R]. United States: Black Hat，2011.

[5] EGELE M, KERUEGEL C, KIRDA E, et al. PiOS: Detecting Privacy Leaks in iOS Applications[R]. United States: NDSS，2011.

[6] JONATHAN Z. iPhone Forensics[S].United States: O’Reilly，2008:144.

[7] SEAN M. iOS Forensic Analysis[S].United States: Apress，2010:317.

[8] 王军选.未来移动通信系统及其关键技术[J].通信技术，2009，42(09):142-144.

[9] 孙利.移动终端定制研究与分析[J].通信技术，2010，43(06):49-52.

（上接第 12 页）

[3] CHAKERES I D, KLEIN-BERNDT L.AODVjr, AODV Simplified[J]. Mobile Computing and Communications Review, 2002,6(03): 100-101.

[4] 蔡雨楠，王福豹，严国强.基于数服务和能量控制的ZigBee 路由策略研究[J].微型电脑应用，2008，24(06): 4-7.

[5] Texas Incorporate. CC2420 Datasheet SWRS041B[Z]. USA:Texas Instrum entsIncorporated, 2007.

[6] 林瑶瑶.基于 ZigBee 的现场参数无线检测装置的研究与设计[D].大连：大连理工大学，2009：43-45.

[7] 黄双华，赵志宏，郭志. ZigBee无线传感器网络路由研究与实现[J]. 电子测量技术，2007,30(02):59-61.

[8] 张毅刚，乔立岩.虚拟仪器软件开发环境 LabWindows/CVI 6.0 编程指南[S].北京:机械工业出版社，2002:185-207.