Д. А. Степаньян, В. Н. Конев, М. И. Фроимсон, А. С. Смирнов

АНАЛИЗ БЕЗОПАСНОСТИ ДАННЫХ О ПЕРЕМЕЩЕНИИ ПОЛЬЗОВАТЕЛЕЙ МОБИЛЬНЫХ УСТРОЙСТВ

Современный мобильный телефон хранит огромное количество информации о своем владельце: список контактов, журнал вызовов, историю SMS-сообщений, конфиденциальные документы. С развитием мобильных технологий и повышением технической сложности телефонных аппаратов пользователи получают возможность использовать различные приложения, оперирующие данными их банковских счетов, учетными записями, прочими персональными данными. Многие из этих программ собирают необходимую информацию автоматически, без ведома владельца, что при отсутствии должной защиты может позволить третьим лицам получить доступ к секретным данным, при этом пользователь может и не знать, что такая информация окажется доступна.

Мобильные телефоны на базе наиболее распространенных на сегодняшний день платформ Android и iOS обладают, наряду с широкими вычислительными возможностями, позволяющими запускать приложения практически любой сложности, также системой позиционирования GPS (или A-GPS), акселерометром, гироскопами и компасом. Таким образом, техническая оснащенность устройств позволяет отследить перемещения пользователя как в режиме реального времени с использованием троянских программ, так и при анализе журналов операционной системы.

Рассмотрим одну из наиболее популярных на сегодняшний день мобильных платформ, iOS, под управлением которой работают продукты фирмы Apple: мобильные телефоны iPhone, планшетные компьютеры iPad и мультимедиаплееры iPod Touch.

Одним из достоинств iOS является поддержание актуальности данных на мобильном устройстве и персональном компьютере пользователя с помощью автоматической синхронизации, выполняемой с использованием программы iTunes при каждом подключении телефона, плеера или планшета к ПК.

При синхронизации на компьютере сохраняются резервные копии настроек и данных с мобильного устройства. В числе прочих передается также информация о его перемещениях, полученная с помощью позиционирования по доступным базовым станциям сотовых операторов и точкам доступа Wi-Fi. Этот способ, хотя и не является настолько точным, как позиционирование на основе GPS, все же позволяет достаточно достоверно определить местонахождение мобильного устройства пользователя.

Рассмотрим механизм получения этой информации.

На компьютерах под управлением операционной системы Mac OS X данные с устройств сохраняются в папку

/Users/<имя пользователя>/Library/Application/Support/MobileSync/Backup/.

Каждый раз при синхронизации iPad, iPhone или iPod Touch файлы будут скопированы в новую папку в этом каталоге [1]. Имена папок и файлов, содержащихся в них, как правило, представляют собой случайно выработанные строки символов, но эти названия разрешаются в реальные имена с помощью присутствующих в каталоге индексных файлов, например Info.plist и Manifest.mbdb.

Каталог, в котором хранятся наиболее свежие данные, можно найти, просмотрев даты модификации папок, а затем, изучив файл Info.plist, можно узнать, к какому именно устройству они относятся.

Файл Manifest.mbdx содержит имена файлов в папке Backup в двоичном виде и имеет следующую структуру:

- заголовок файла — 6 байт;
- для каждой записи повторяются поля:
  — идентификатор файла в папке Backup — 20 байт;
  — смещение соответствующей строки в файле Manifest.mbdb — 4 байта;
  — уровень доступа к файлу — 2 байта.

Файл Manifest.mbdb представляет собой список реальных имен файлов и содержит следующие данные:

- заголовок — 6 байт;
- для каждой записи повторяются строковые поля:
  — категория данных, содержащихся в файле;
  — реальное имя файла;
  —служебная информация о файле (три строковых значения и 40 байт двоичных данных).

Строка имеет переменную длину, которая указывается с помощью 2 байт, помещаемых перед ней.

Используя извлеченные из этих двух файлов данные, можно найти файл consolidated.bd, который представляет собой базу данных SQLLite. Для его просмотра можно использовать любой клиент базы данных, поддерживающий формат SQLLite.

В числе прочих файл содержит следующие таблицы:

- WiFiLocation.

Содержит MAC-адреса, временные метки и географические координаты точек доступа к Wi-Fi, к которым подключалось устройство.

- CellLocation.

Содержит идентификаторы, временные метки и координаты базовых станций, которые были доступны устройству, а также силу сигнала.

- CdmaCellLocation.

Содержит ту же информацию, что и таблица CellLocation, наряду с некоторыми специфическими данными для 3G-вышек.

В системе, работающей под управлением операционной системы Windows, файлы синхронизации будут располагаться в каталоге

C:\Users\<имя пользователя>\AppData\Roaming\Apple Computer\MobileSync\Backup. Просмотреть таблицы можно с помощью клиента базы данных, предварительно проведя поиск необходимых файлов, выполнив в консоли следующую команду:

findstr /M <имя таблицы> C:\Users\Andykn\AppData\Roaming\Apple Computer\MobileSync\Backup\<каталог актуальной резервной копии>*.*

Используя полученные данные, злоумышленник может составить карту передвижений пользователя, привязанную ко времени, с точностью от 50 (по информации о Wi-Fi точках) до 500 метров (по данным о вышках сотовых операторов) [2, 3].

Как видно из рассмотренного выше случая, данные о перемещениях хранятся на продуктах компании Apple в легко читаемой форме, и любой пользователь, обладающий доступом к компьютеру, с которым синхронизируется мобильное устройство, имеет возможность просматривать их. Также существует опасность заражения вирусными программами, в частности троянскими приложениями, собирающими эту информацию и отправляющими ее третьим лицам.

Подобную информацию собирают и сотовые операторы, обеспечивая при этом высокий уровень защиты этих данных, гарантируя ее конфиденциальность. Рядовой же пользователь не всегда может обеспечить необходимый уровень безопасности.

Приведенный пример является лишь единичным случаем открытой журнализации частной информации, ставшим известным широкой общественности. Нет никаких оснований полагать, что

подобная ситуация в той или иной форме не повторяется для платформ других производителей – HTC, Nokia, Google, Samsung, Sony Ericsson, Siemens и т. д. Так, недавно компания Google признала факт сбора информации о пользователях своих телефонов на базе ОС Android, в частности, сохраняется информация о поисковых запросах, точках доступа в сеть Интернет и истории просмотра web-страниц.

Подобные механизмы предусмотрены производителями для удобства пользователей (хотя нет никаких достоверных данных, отрицающих факт передачи этой информации на сервера компаний), например, для восстановления устройства из резервной копии, оптимизации подключения к беспроводным точкам доступа, предложения таргетированной рекламы.

Тем не менее все эти данные хранятся в открытой форме, что делает их доступными для различных видов атак.

Возможности мобильного устройства могут быть использованы также вирусными программами.

Например, вместо данных о местоположении, собираемых мобильным устройством по информации о доступных базовых станциях сотового оператора и беспроводных точках доступа, приложение злоумышленника, устанавливаемое на телефон, может использовать модуль GPS-навигации, обладающий точностью до 2 метров, а также воспользоваться сетевыми возможностями устройства для передачи полученных данных злоумышленнику в режиме реального времени.

Таким образом, с повышением функциональности мобильных устройств увеличивается и диапазон угроз, которым подвержены их владельцы. Отключение дополнительных возможностей телефона не является решением проблемы, поскольку в некоторых случаях это не предусматривается производителем, а часть этих функций являются критичными для работы аппарата.

Единственным средством, сочетающим удобство пользователя с повышением уровня безопасности, остается использование дополнительных средств защиты, а именно:

- шифрование резервных копий на компьютере и оперативных данных на устройстве;
- антивирусное программное обеспечение на мобильном устройстве и персональном компьютере;
- сетевые экраны.

Использование перечисленных средств защиты как по отдельности, так и в сочетании с другими мерами безопасности позволит обеспечить конфиденциальность личных данных пользователя и предотвратить их использование в преступных целях.

СПИСОК ЛИТЕРАТУРЫ:

1. *Ali M.* Advanced iOS 4 Programming: Developing Mobile Applications for Apple iPhone, iPad, and iPod touch. Wiley, New-York. 2010.
2. IEEE 802.11 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE SA, New-York, 2007.
3. 3GPP TS 45.001 Physical layer on the radio path; General description, ETSI, Nice, 2009.