**Report about researched media covert channels for mobile devices, known attacks with utilization of covert channels for mobiles**

**By Serhii Zakharash**

**Вступление**

В изолированной системе данные защищены от несанкционированного доступа или модификаций, а код от исполнения его паттернов или изменений этого кода. В среде с более чем 1 пользователем эти защитные меры просто необходимы для защиты процессов пользователей. Путей вмешательства в процессы пользователей множество. В этом исследовании будут описаны возможные пути воздействия на мобильные устройства на базе операционной системы Android путём атак с использованием скрытых каналов.

Стоит начать с того, какова функция скрытых каналов (Covert channels) для злоумышлеников. Скрытые каналы используются чтобы изъять необходимую информацию из защищенной/изолированной среды или системы таким образом, чтобы эту атаку было сложно обнаружить или предотвратить. Мобильные устройства являются крайне распространённым видом вычислительной платформы, которые имеют доступ или хранят важную для пользователя информацию. По данным самого Android состоянием на 2019 год (<https://twitter.com/Android/status/1125822326183014401?s=20>) количество активных девайсов привысило 2.5 миллиардов единиц (Учитывались устройства со встроенным Google Assistant). В следствии чего, эти устройства и стали основными целями атак злоумышленников.

**Разновидности вредоносного софта для атак на данные мобильных устройств**

Перечислять все виды атак будет слишком долго, поэтому можно выделить несколько распространённых и эффективных способов:

* Модель кражи данных через разрешения использования функций компонентов (Permissions: camera, Bluetooth, GPS, telephony, and network access) андроид устройств - Трояны. Путём получения доступа к функциям, связанных с этими элементами смартфона злоумышленники могут получить доступ к данным смартфона. Это может быть как отдельное вредоносное ПО, которое требует слишком много разрешений, вопреки своей функциональности (назначению для пользователя), или просто создаёт скрытую утечку.
* Еще один тип атак – Third party software. В отличии от троянов, такое ПО уже имеет несанкционированный доступ ко всем необходимым для злоумышленников функциям доступа к данным и их кражи.
* Стоит выделить еще один неочевидный для обычного пользователя тип атак. Атака осуществляется с помощью связки из нескольких приложений (чтобы избежать лишних подозрений со стороны пользователя). Рассмотрим более детально этот случай. На пример, первой вредоносной программой может выступать персональный помощник, который требует разрешения ко всему, кроме доступа в сеть, что даёт пользователю уверенность в том, что его конфиденциальные данные никак не извлечь, а второй программой будет наоборот приложение, которое не требует никаких разрешений, кроме доступа в сеть. Таким образом, если эти программы могут взаимодействовать между собой, то принцип получения данных очевиден. (1)
* Последний, рассмотренный мною тип атаки, является взаимодействие на датчики, доступ к которым имеет каждое приложение т.к. к нему не требуется разрешение со стороны пользователя. Эти атаки я буду рассматривать немного позже в своём отчёте, но, сперва, хочу описать несколько важных для дальнейшего исследования объектов и принципы их работы.

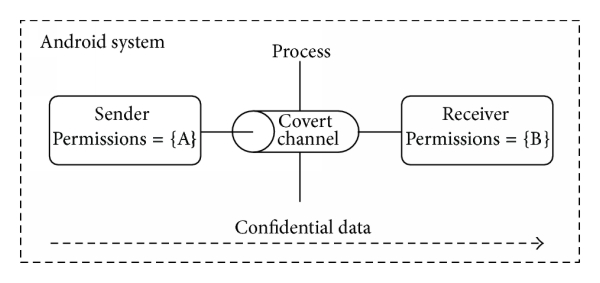
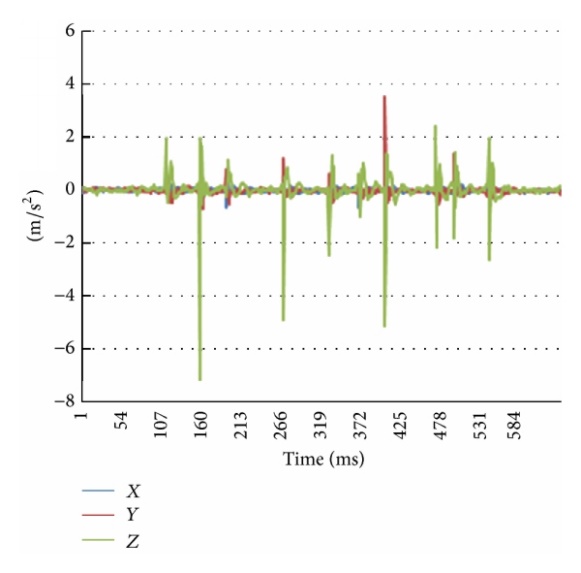
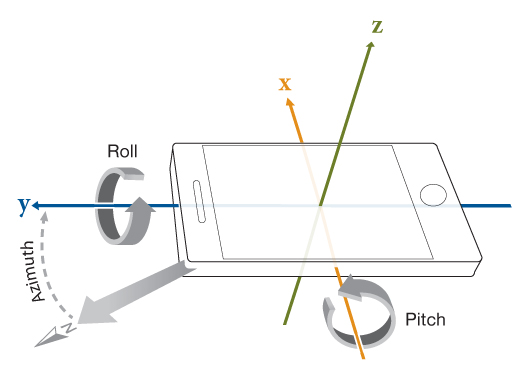
**Общая модель скрытых каналов Android** 

Иллюстрация выше показывает общий принцип работы скрытых каналов Android устройств. Если предположить, что для осуществления атаки вредоносному ПО нужен множество разрешений {{A}, {B}}, где {A} – это подмножество, имеющее доступ к конфиденциальной информации но не имеющее предпосылок как-либо эту информацию использовать , а {B} – подмножество с доступом в сеть, но отсутствием доступа к конфиденциальной информации, то при сценарии где злоумышленник смог использовать два синхронизированных приложения каждое приложение будет запрашивать безобидно выглядящее подмножество разрешений и работать незаметно. (1)

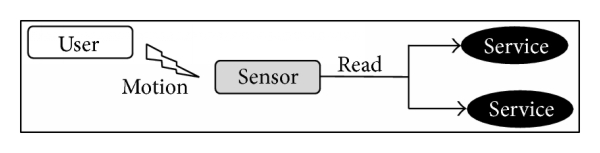
**Сенсоры Android**

Рассмотрим сначала акселерометр Android устройств. Данные, считываемые с этого модуля, имеет привязку к 3-х осевой системе координат. Так, на изображения ниже демонстрируют координатную систему акселерометра и показания, считываемые с акселерометра при наборе цифр «0123034880».



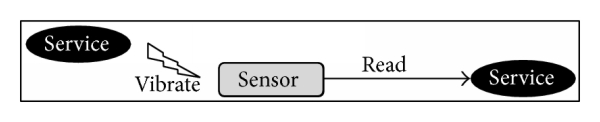
Также данные считываются и с гироскопа, который отвечает за считывания вращения смартфона по осям x, y. Таким образом считываемая информация с датчиков движения может быть считана и преобразована в текст, который пользователь набирал в момент работы вредоносной программы.

Датчики движения вряд ли воспринимается как канал для обмена информацией, кроме как, вызваной действиями пользователя. Такие вредоносные приложения перехватывали данные датчиков во время ввода данных пользователем на сенсорные экраны и выводили конфиденциальную информацию. Это односторонняя связь от датчика к приложению. Есть и обратный способ, а именно механизм для передачи личных данных от вредоносного приложения к датчику. Поскольку показания датчиков доступны для всех приложений Android без разрешений безопасности, любая информация, содержащаяся в данных датчиков, может быть получена другими приложениями, работающими в данный момент на телефоне. Хитрость заключается в том, что приложение использует встроенный двигатель вибратора для генерации моделей вибрации, которые кодируют конфиденциальные данные. Вибрации модулируют сигналы ускорения и перехватываются и декодируются другим мошенническим приложением.



На изображении сверху модель считывания сигналов датчиков, вызванных действиями пользователя. Нижнее изображение демонстрирует

Использование функции вибрации для модуляции сигналов датчиков и создания скрытого канала.



**Источники**:

Exploring Covert Channel in Android Platform. By Wade Gasior and Li Yang (2012)

[Link](https://ieeexplore.ieee.org/document/6542541)

A New Sensors-Based Covert Channel on Android. By Mahamod Ismail and Rosdiadee Nordin

[Link](https://www.hindawi.com/journals/tswj/2014/969628/)

An autonomic and permissionless Android covert channel. By Ken Block, Sashank Narain and Guevara Noubir.

[Link](https://www.researchgate.net/publication/318409055_An_autonomic_and_permissionless_Android_covert_channel)