Хакер - Самая дырявая ОС. Сравниваем безопасность iOS, Windows, Android, Sailfish и Tizen

nopaywall

https://t.me/nopaywall

Олег Афонин

Содержание статьи

Мы часто пишем о безопасности мобильных ОС, публикуем информацию о найденных уязвимостях, описываем слабые стороны защиты и способы взлома. Мы писали и о слежке за пользователями Android, и о зловредных приложениях, которые встраиваются прямо в прошивку, и о неконтролируемой утечке пользовательских данных в облако производителя. Какая же из современных мобильных платформ наиболее безопасна для пользователя — или хотя бы наименее небезопасна? Попробуем разобраться.

Что такое безопасность?

Нельзя говорить о безопасности устройства, не определив, что мы, собственно, имеем в виду. Физическую безопасность данных? Защиту от методов низкоуровневого анализа с извлечением микросхемы памяти или же просто защиту от любопытных, которые не знают пароля и не умеют обманывать сканер отпечатков пальцев? Передача данных в облако — плюс это или минус с точки зрения безопасности? А в какое облако, кому и куда, каких именно данных, знает ли об этом пользователь и может ли отключить? А насколько вероятно на той или иной платформе подхватить троянца и расстаться не только с паролями, но и с деньгами на счете?
Аспекты безопасности мобильных платформ невозможно рассматривать в отрыве друг от друга. Безопасность — это комплексное решение, охватывающее все грани использования устройства от коммуникаций и изоляции приложений до низкоуровневой защиты и шифрования данных.

Сегодня мы коротко опишем основные достоинства и проблемы во всех современных мобильных ОС, которые имеют хоть какое-то распространение. В список входят Google Android, Apple iOS и Windows 10 Mobile (увы, но Windows Phone 8.1 назвать современной уже нельзя). Бонусом пойдут BlackBerry 10, Sailfish и Samsung Tizen.

Старички: BlackBerry 10

Прежде чем приступать к описанию актуальных платформ, скажем пару слов о BlackBerry 10, которая уже сошла с дистанции. Почему BlackBerry 10? В свое время система активно продвигалась как «самая безопасная» мобильная ОС. В чем-то это было действительно так, что-то, как всегда, преувеличили, что-то было актуальным три года назад, но безнадежно устарело сегодня. В целом нам нравился подход компании BlackBerry к безопасности; впрочем, не обошлось и без провалов.
Плюсы:

- Микроядерная архитектура и система доверенной загрузки — это действительно безопасно. Прав суперпользователя за все время существования системы не получил никто (между прочим, пытались неоднократно, в том числе в серьезных конторах — BlackBerry далеко не всегда была аутсайдером).
- Также невозможно обойти пароль на разблокирование устройства: спустя десять неудачных попыток данные в устройстве полностью уничтожаются.
- Нет никаких встроенных облачных сервисов и нет целенаправленной слежки за пользователем. Данные не передаются на сторону, если только пользователь не

решит установить облачное приложение самостоятельно (опционально поддерживаются такие службы, как OneDrive, Box.com, Dropbox).
- Образцовая реализация корпоративных политик безопасности и удаленного контроля через BES (BlackBerry Enterprise Services).
- Надежное (но опциональное) шифрование как встроенного накопителя, так и карт памяти.
- Облачных резервных копий нет совсем, а локальные шифруются с помощью безопасного ключа, привязанного к BlackBerry ID.

Минусы:

- Данные по умолчанию не шифруются. Впрочем, компания может активировать шифрование на устройствах сотрудников.
- Шифрование данных блочное, одноранговое; отсутствует понятие классов защиты и что-либо, хотя бы отдаленно напоминающее Keychain в iOS. Например, данные приложения Wallet можно извлечь из резервной копии.
- В учетную запись BlackBerry ID можно зайти просто с логином и паролем; двухфакторная аутентификация не поддерживается. Сегодня такой подход совершенно неприемлем. Кстати, если известен пароль от BlackBerry ID, можно извлечь ключ, с помощью которого расшифруется созданный привязанным к данной учетке бэкап.
- Защита от сброса к заводским настройкам и защита от кражи очень слабая. Она обходится простой заменой приложения BlackBerry Protect при сборке автозагрузчика или (до BB 10.3.3) понижением версии прошивки.
- Отсутствует рандомизация MAC-адреса, что позволяет отслеживать конкретное устройство с помощью точек доступа Wi-Fi.

BlackBerry 10 умеет шифровать как внутреннюю память, так и SD-карту

Еще один звоночек: BlackBerry охотно сотрудничает с правоохранительными органами, оказывая максимально возможную помощь в поимке преступников, которые пользуются смартфонами BlackBerry.

В целом при грамотной настройке (а пользователи, выбравшие BlackBerry 10, как правило, настраивают свои устройства вполне грамотно) система способна обеспечить как приемлемый уровень безопасности, так и высокий уровень приватности. Впрочем, «опытные пользователи» могут свести все преимущества на нет, установив на смартфон взломанную версию Google Play Services и получив все прелести присмотра «Большого Брата».

Экзотика: Tizen и Sailfish

Tizen и Sailfish — явные аутсайдеры рынка. Аутсайдеры даже в большей степени, чем Windows 10 Mobile или BlackBerry 10, доля которой упала ниже отметки 0,1%. Их безопасность — это безопасность «неуловимого Джо»; о ней мало что известно лишь потому, что они мало кому интересны.
Насколько оправдан такой подход, можно судить по недавно опубликованному исследованию, в котором обнаружено порядка сорока критических уязвимостей в Tizen. Тут можно разве что подытожить давно известное.

- Если не проводились серьезные независимые исследования, то говорить о безопасности платформы нельзя. Критические уязвимости вскроются не раньше, чем платформа получит распространение. Но будет поздно.
- Зловредного ПО нет лишь из-за слабой распространенности платформы. Тоже в каком-то роде защита.
- Механизмы безопасности недостаточны, отсутствуют или описаны лишь на бумаге.
- Любые сертификации говорят лишь о том, что устройство прошло сертификацию, но ровным счетом ничего не говорят о фактическом уровне безопасности.

Jolla Sailfish

С Sailfish ситуация неоднозначная. С одной стороны, система как бы жива: на ее основе время от времени анонсируются какие-то устройства, и даже «Почта России» приобрела большую партию устройств с запредельно высоким ценником. С другой — пользователям предлагают заплатить стоимость крепкого середнячка на Android за модель под управлением Sailfish, обладающую характеристиками китайского дешевого смартфона трехлетней (!) давности. Такой подход сработает в единственном случае: если модели на Sailfish будут закупаться за бюджетные деньги, после чего раздаваться государственным служащим нижнего звена. Разумеется, о какой-то там безопасности при таком подходе думать участникам сделки совсем не интересно.
И даже наличие государственных сертификатов не дает никакой гарантии точно так же, как ее не дает открытый исходный код. К примеру, уязвимость Heartbeat была обнаружена в прошивках роутеров, исходный код для которых был в открытом доступе более десяти лет. В операционной системе Android, которая также обладает открытым исходным кодом, новые уязвимости обнаруживаются регулярно.
Экзотические ОС — это отсутствие инфраструктуры, крайне ограниченный набор устройств и приложений, недоразвитые средства управления корпоративными политиками безопасности и более чем сомнительная безопасность.

Sailfish OS

Samsung Tizen

Несколько особняком от остальных «экзотических» платформ стоит Samsung Tizen. В отличие от Ubuntu Touch и Sailfish, Tizen — вполне распространенная система. Под ее управлением работают десятки моделей умных телевизоров Samsung, а также умные часы и несколько бюджетных смартфонов (Samsung Z1–Z4).
Как только Tizen получила заметное распространение, за систему взялись независимые исследователи. Результат неутешителен: в первые же месяцы было найдено более сорока критических уязвимостей. Процитируем слова Амихая Нейдермана, который провел исследование безопасности Tizen:

> Возможно, это худший код из тех, что мне довелось видеть. Все ошибки, которые можно было допустить, были допущены. Очевидно, что код писал

> или проверял кто-то, кто ничего не понимает в безопасности. Это все равно что попросить школьника написать для вас программное обеспечение.

В целом вывод понятен: использовать экзотическую, малораспространенную систему в корпоративной среде — открытое приглашение для хакеров.

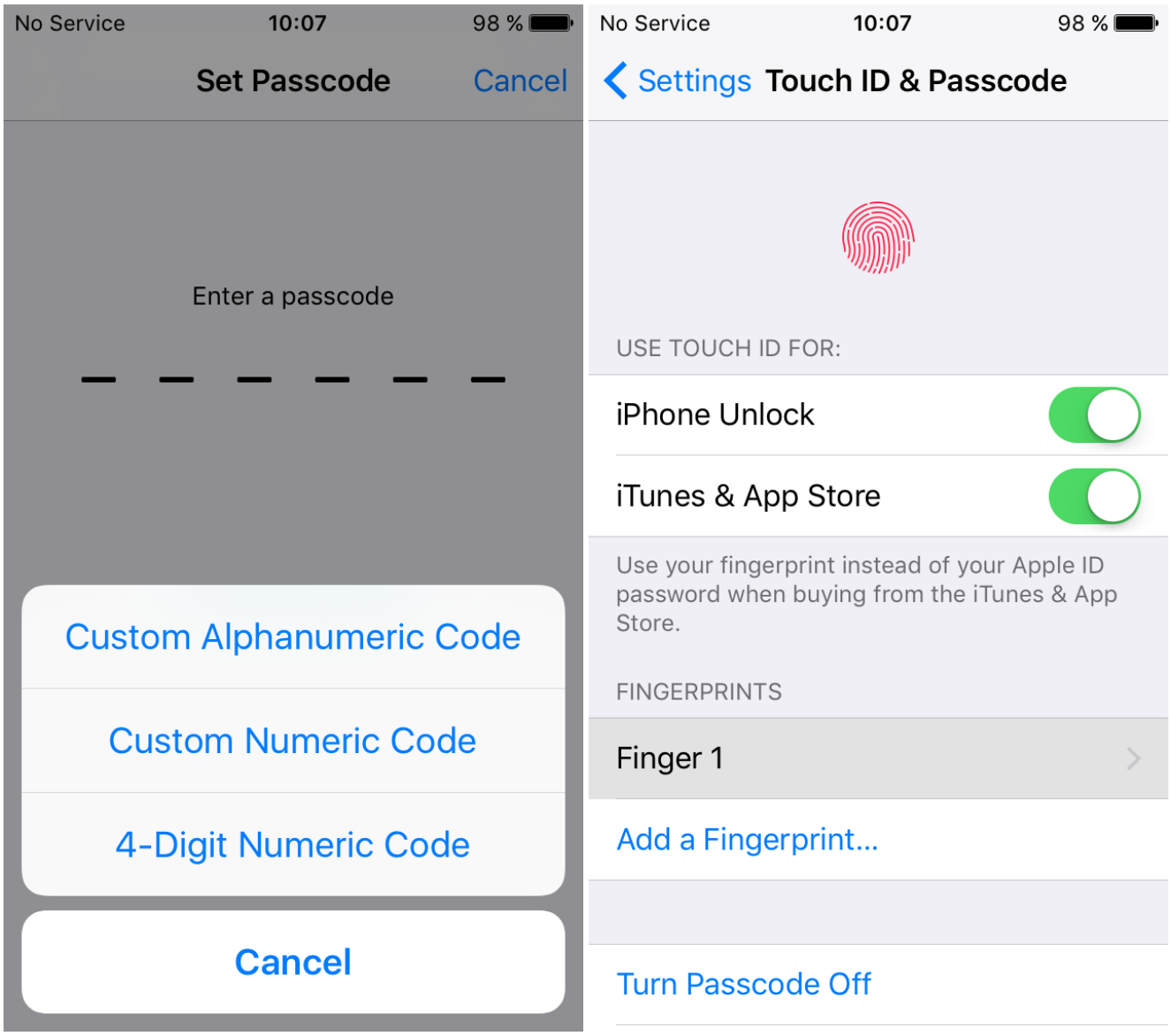
Телевизор Samsung под управлением Tizen

Apple iOS

Apple мы будем хвалить. Да, это закрытая экосистема, и да, ценник несопоставим с техническими возможностями, но тем не менее устройства под управлением iOS были и остаются самыми безопасными из распространенных коммерческих решений. В основном это касается текущих моделей поколений iPhone 6s и 7 (и, пожалуй, SE). Более старые устройства обладают меньшим запасом прочности. Для стареньких iPhone 5c, 5s и 6 уже есть способы разблокирования загрузчика и атаки на пароль устройства (за подробностями можно обратиться к разработчикам — компании Cellebrite). Но даже для этих устаревших устройств взлом загрузчика — дело трудоемкое и весьма недешевое (в Cellebrite просят за услугу несколько тысяч долларов). Думаю, мой или твой телефон никто таким способом ломать не станет.
Итак, что мы имеем на сегодняшний день. Начнем с физической безопасности.

1. Все iPhone и iPad iOS 8.0 и выше (а в настоящий момент актуальна iOS 10.3.2, которая еще более безопасна) применяют настолько стойкие методы защиты, что даже их производитель как официально, так и фактически отказывается извлекать информацию из заблокированных устройств. Независимые исследования (в том числе в лаборатории «Элкомсофт») подтверждают заявления Apple.
2. В iOS предусмотрена (и действительно работает) система защиты данных в случае кражи или потери устройства. Доступны механизмы удаленного стирания данных и блокировки устройства. Украденное устройство невозможно будет разблокировать и перепродать, если злоумышленнику неизвестны как пароль на устройство, так и отдельный пароль от учетной записи Apple ID владельца. (Впрочем, китайским умельцам доступно все, и вмешательство в аппаратную часть устройства способно обойти эту защиту… для iPhone 5s и более старых устройств.)
3. Многоуровневое шифрование данных «из коробки» идеально спроектировано и реализовано. Раздел данных шифруется всегда; используется блочный шифр с ключами, уникальными для каждого отдельного блока, при этом при удалении файла соответствующие ключи удаляются — а значит, восстановить удаленные данные в принципе невозможно. Ключи защищены выделенным сопроцессором, входящим в систему Secure Enclave, и вытащить их оттуда нельзя даже с jailbreak (мы пробовали). Данные при включении остаются зашифрованными, пока ты не введешь правильный пароль. Более того, некоторые данные (например, пароли к веб-сайтам, скачанная на устройство электронная почта) дополнительно шифруются в защищенном хранилище Keychain, причем часть из них невозможно извлечь даже с джейлбрейком.
4. Ты не можешь просто воткнуть в компьютер iPhone и скачать с него данные (кроме фотографий). В iOS предусмотрена возможность установления доверительных отношений с компьютерами. При этом создается пара криптографических ключей, позволяющих доверенному компьютеру делать с телефона резервные копии. Но даже эту возможность можно ограничить с помощью корпоративной политики безопасности или фирменным приложением Apple Configurator. Безопасность бэкапов обеспечивается возможностью установить сложный пароль (пароль требуется исключительно для восстановления данных из резервной копии, поэтому в режиме повседневного использования мешаться не будет).
5. Разблокировка iPhone сделана на достаточно безопасном уровне. Для разблокировки можно использовать как стандартный PIN-код из четырех цифр, так и более сложный пароль. Единственный дополнительный способ разблокирования устройства — отпечаток пальца. При этом реализация механизма такова, что у злоумышленника будет очень мало возможностей им воспользоваться. Данные отпечатка зашифрованы и будут удалены из оперативной памяти устройства после выключения или перезагрузки; через некоторое время, если устройство ни разу не

разблокировалось; после пяти неудачных попыток; через некоторое время, если пользователь ни разу не вводил пароль для разблокировки устройства.



PIN-код или датчик отпечатков — решать тебе

6. В iOS есть опция, позволяющая автоматически удалять данные после десяти неудачных попыток входа. В отличие от BlackBerry 10, эта опция контролируется на уровне операционной системы; для старых версий iOS (вплоть до iOS 8.2) существуют способы ее обойти.

В iOS можно ограничить запуск приложений отдельным паролем

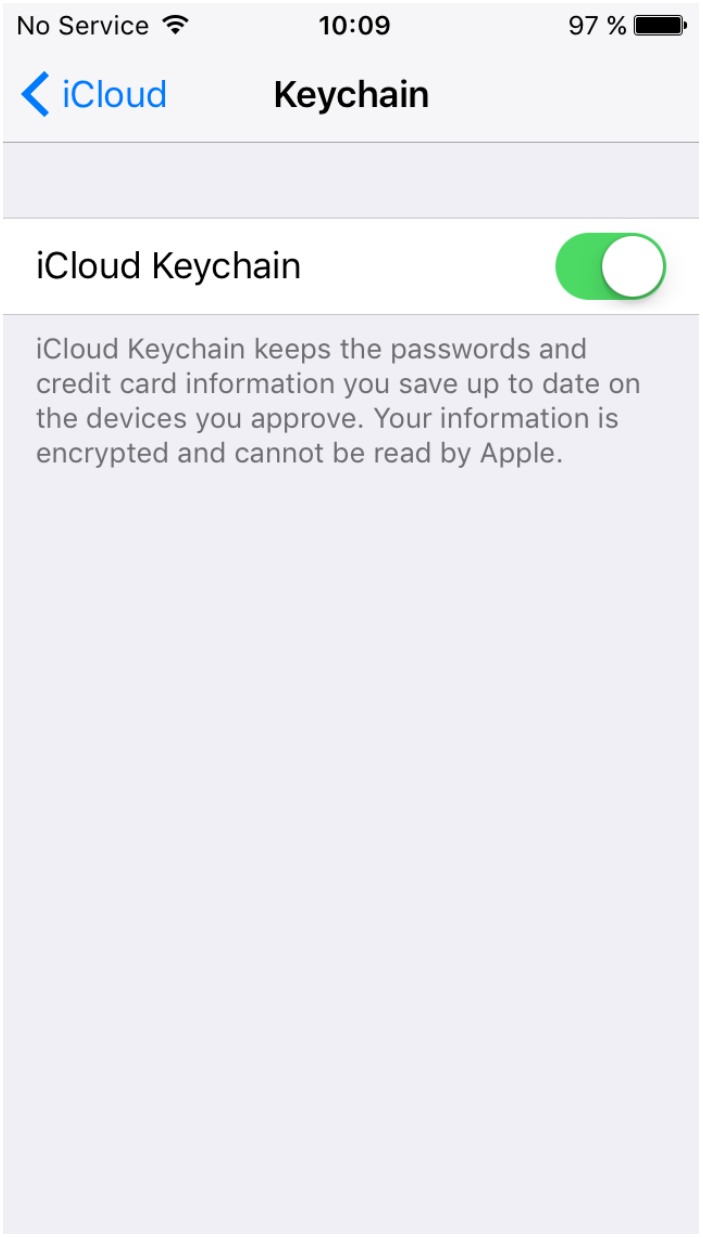
Что у нас со слежкой за пользователем и с утечками?

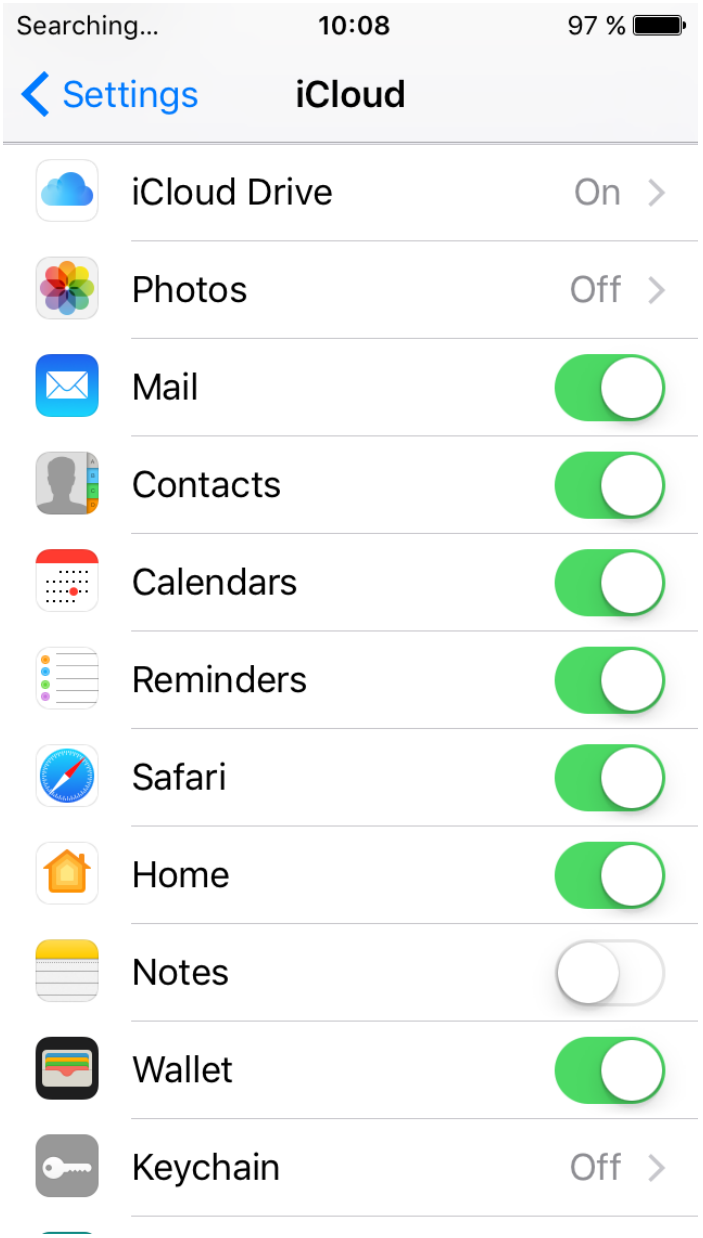
В iOS есть отключаемая синхронизация с облаком через собственный сервис Apple iCloud. В частности, в iCloud обычно сохраняются:

- резервные копии данных устройства;
- синхронизированные данные — журнал звонков, заметки, календари, пароли в iCloud Keychain;
- пароли и история посещения ресурсов в браузере Safari;
- фотографии и данные приложений.

Все виды облачной синхронизации в iOS можно отключить, просто выключив iCloud и деактивировав iCloud Drive. После этого никакие данные не будут передаваться на серверы Apple. Несмотря на то что некоторые механизмы работают не слишком

интуитивно (как пример — для выключения синхронизации звонков нужно отключать iCloud Drive, вообще-то предназначенный для синхронизации файлов и фотографий), полное выключение облачных сервисов синхронизацию полностью же отключает.





Любые виды синхронизации можно отключить

В iOS предусмотрен механизм для предотвращения слежки (система может представлять внешнему миру случайные идентификаторы модулей Wi-Fi и Bluetooth вместо фиксированных настоящих).

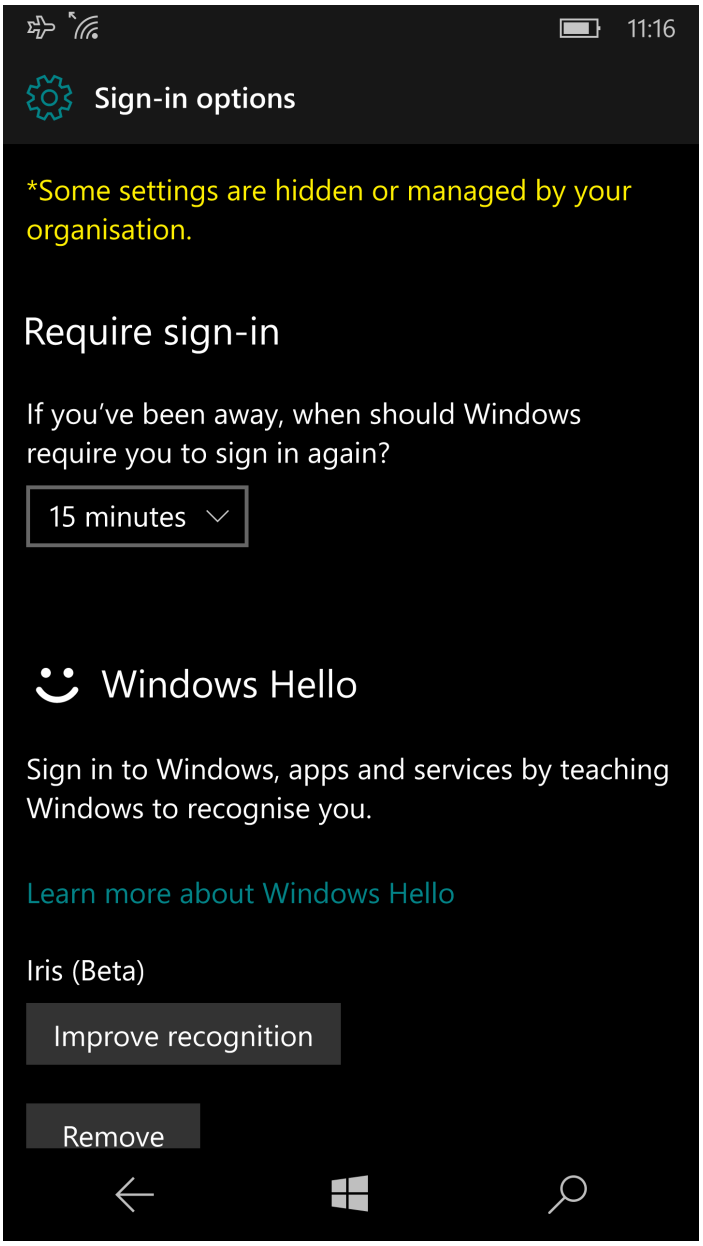
Хорошо, а как обстоят дела со зловредами? В iOS практически исключена возможность установки зловредного ПО. Единичные случаи были (через приложения, собранные с использованием взломанных инструментов для разработки), но они быстро локализовались и исправлялись. Даже тогда большого вреда причинить эти приложения не смогли: в iOS каждое приложение надежно изолировано как от самой системы, так и от других приложений с помощью песочницы.

Нужно отметить, что в iOS давным-давно был реализован гранулярный контроль за разрешениями приложений. Ты можешь по отдельности разрешить или запретить

каждому приложению такие вещи, как возможность работы в фоновом режиме (в «чистом» Android такой возможности нет!), доступ к местоположению, уведомлениям и тому подобное. Наличие этих настроек позволяет эффективно ограничивать слежку со стороны приложений, которые сделали такую слежку своим основным бизнесом (это касается как приложений класса Facebook, так и игр наподобие Angry Birds).
Наконец, Apple регулярно обновляет iOS даже на старых устройствах, практически моментально (в сравнении с Android) исправляя найденные уязвимости. При этом обновления прилетают одновременно всем пользователям (снова «в отличие от»).
Что интересно, iOS начиная с 9-й версии защищена и от атак класса man in the middle с перехватом и подменой сертификата. И если в лаборатории «Элкомсофт» удалось отреверсить протокол бэкапов iCloud в 8-й версии системы, то в более новых ОС этого сделать не вышло по техническим причинам. С одной стороны, получаем гарантию безопасности передаваемых данных; с другой — у нас нет возможности достоверно убедиться в том, что на серверы не будет отправлена «лишняя» информация.
Наконец, нельзя не сказать о мифических «закладках» в ОС, из-за возможного наличия которых чиновники предпочтут «сертифицированные» устройства с Sailfish вместо отлаженных iPhone. В «Элкомсофт» тщательно исследовали десятки моделей iPhone, начиная с самых ранних. В совсем старых моделях (до iPhone 4 включительно) были уязвимости, которые получилось успешно использовать. Начиная с iPhone 4s ни уязвимостей, ни «черных ходов» подобного уровня нам обнаружить не удалось. Логика подсказывает, что, если бы они были, ФБР не пришлось бы платить миллион долларов компании Cellebrite за взлом единственного iPhone 5c. Та же Cellebrite тщательно скрывает (в первую очередь — от Apple) информацию об уязвимостях, которые она использует для взлома загрузчика. «Мы потратили полтора года, чтобы обнаружить эту уязвимость. У Apple займет полторы недели, чтобы ее устранить» — дословная цитата представителя компании на конференции. На этом тему шапочек из фольги предлагаем закрыть.
В то же время Apple целиком и полностью контролирует собственную облачную инфраструктуру и готова выдавать данные из облака по запросу правоохранительных органов. А в облаке, между прочим, хранится довольно много интересного. Статистика о количестве удовлетворенных запросов полностью публична. С более подробной аналитикой можно ознакомиться на сайте «Элкомсофта».
В целом безопасность Apple iOS 10.3 на устройствах iPhone SE, 6s, 7 и их версиях Plus находится на высочайшем уровне. Придраться особо не к чему, а имеющиеся изъяны легко исправляются штатными средствами.

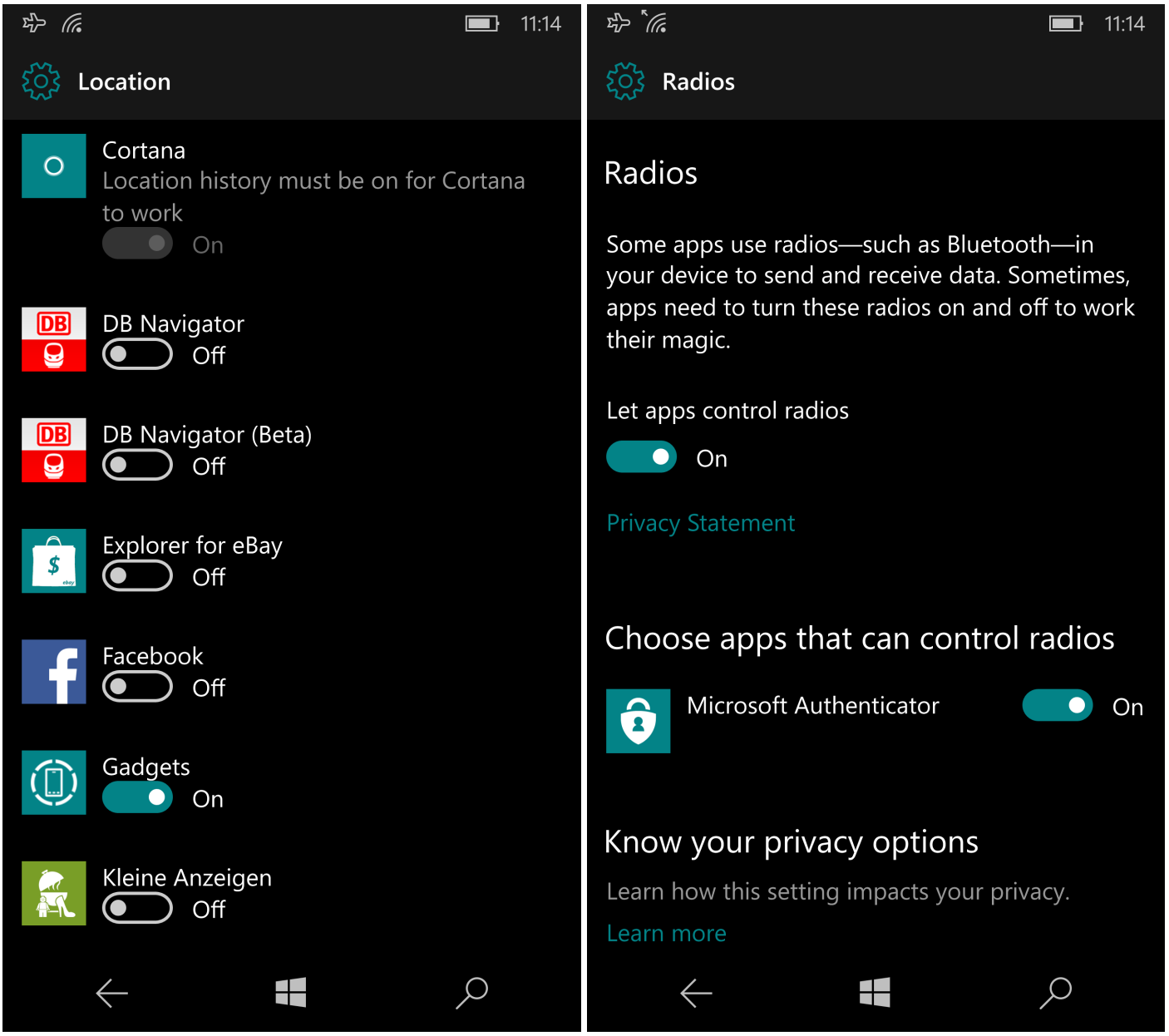
Windows 10 Mobile

Android мы оставим на закуску, а пока посмотрим на смартфоны под управлением Windows 10 Mobile. В первую очередь нам интересны, конечно же, флагманы производства самой Microsoft — это Lumia 950 и 950 XL. Дело в том, что эти устройства изначально разрабатывались именно для нужд корпоративных потребителей.
Интереснейшая особенность Windows 10 Mobile в том, что это единственная мобильная ОС, не основанная на той или иной версии UNIX. Собственный подход к проектированию ядра и самой системы, отличная оптимизация ОС и всего софта под ограниченный список поддерживаемых чипсетов помещают Windows 10 Mobile где-то посередине между полностью закрытой iOS и полностью открытым Android.
В ОС компании Microsoft есть возможность полнодискового шифрования (но, в отличие от Apple iOS, многоуровневая защита данных здесь отсутствует), которую, впрочем, можно включать и отключать по желанию пользователя (или сетевого администратора). Также можно настроить шифрование данных на внешних носителях (картах формата microSD, если они используются).
Разблокировка телефона возможна как с помощью традиционного PIN-кода, так и по биометрическому датчику — сканеру радужной оболочки глаза (только для моделей Lumia 950 и 950 XL). По скорости и удобству работы сканер радужки заметно уступает сканеру отпечатка пальца в устройствах iOS, да и в современных Android. Безопасность, впрочем, на уровне. В отличие от Android, в Windows 10 Mobile не предусмотрены и недопустимы небезопасные способы аутентификации.



Аутентификация по радужной оболочке включается в настройках

Гранулярный контроль за разрешениями приложений присутствует: есть возможность ограничивать доступ приложений к местоположению пользователя и возможность запретить работу в фоне.



Слева: приложения с доступом к геоданным, справа: переключатель доступа к телефонии

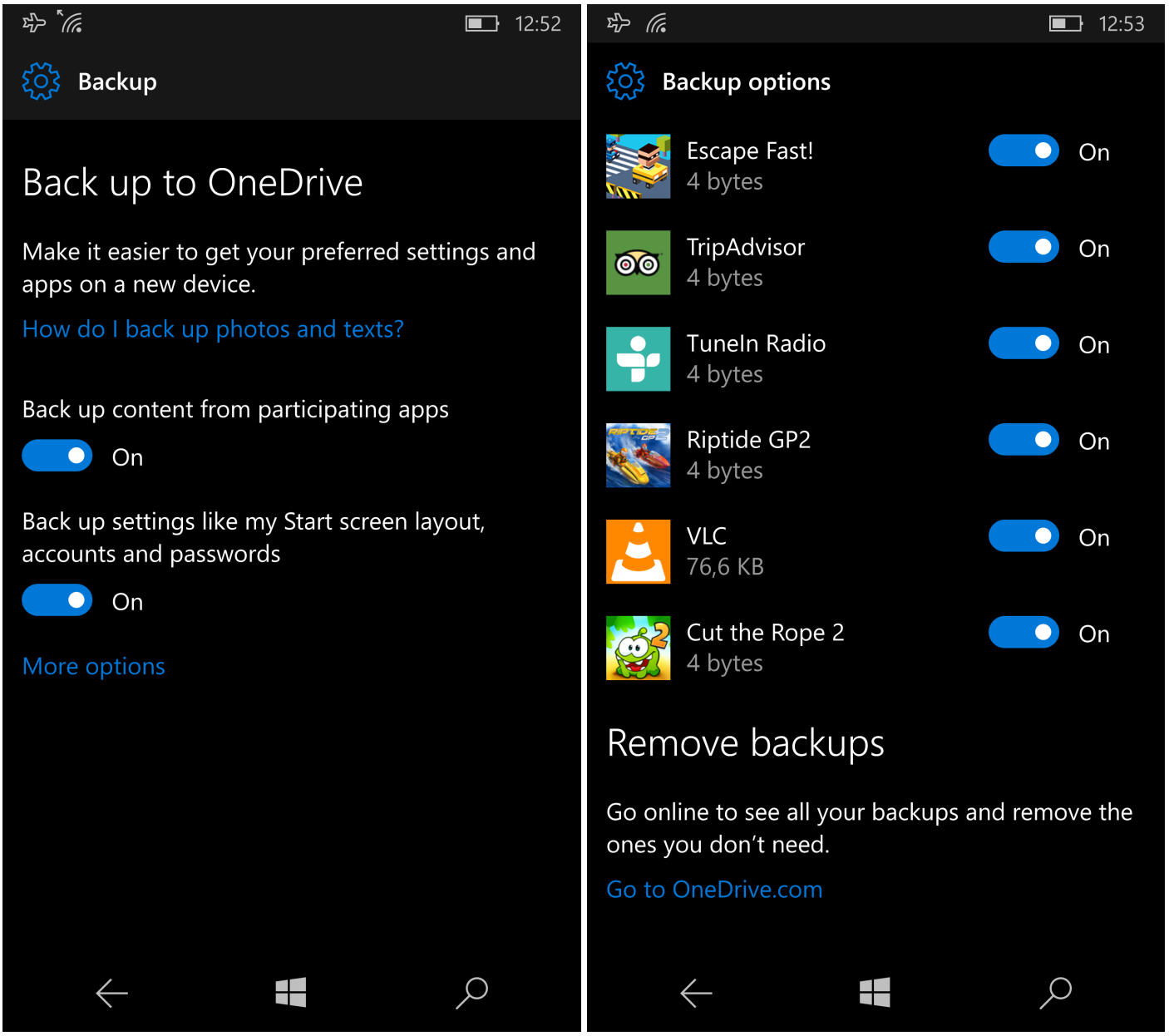
Изоляция приложений в песочнице присутствует. Возможность установки приложений из сторонних источников по умолчанию заблокирована и может быть дополнительно усилена с помощью корпоративной политики безопасности, запрещающей пользователю включать возможность установки неподписанных приложений.

Кстати, для Windows 10 Mobile существует аналог jailbreak, позволяющий получить эскалацию привилегий, доступ к редактированию реестра (он, к слову, практически не отличается от реестра «большой» Windows 10) и файловой системе. Устанавливать его не слишком просто, но все делается с помощью вполне штатных средств из режима для разработчиков: ни о какой эксплуатации уязвимостей речи не идет, способ давно известен и сохраняет работоспособность во всех версиях Windows 10 Mobile, включая обновление до Creators Update.

Плюс это или минус с точки зрения безопасности — сказать сложно; в конце концов, на разблокирование телефона или доступ к зашифрованным данным такой «взлом» никак

не влияет (в отличие от jailbreak в iOS, с помощью которого успешно обходятся встроенные в систему механизмы безопасности).

Так же как и Apple, Microsoft собирает информацию о пользователях своих устройств. По объему данных и масштабу «слежки» компания снова посерединке между Apple и Google. В облаке Microsoft OneDrive телефоны создают резервные копии (в том числе данные приложений), синхронизируют звонки и SMS (а вот iOS синхронизирует только звонки, но не сообщения). Также синхронизируются пароли и история браузера.



Функцию бэкапа можно отключить для отдельно взятых приложений

Сервис защиты от кражи и удаленного блокирования устройства Find My Phone есть, но вот сервис, аналогичный iCloud Lock (Apple) или Factory Reset Protection (Google), доступен исключительно в моделях, выпущенных для американского рынка.

Как и в случае с iOS, все эти возможности достаточно легко отключить как в настройках устройства, так и с помощью корпоративной политики безопасности.

Microsoft так же, как и Apple, регулярно обновляет свои устройства и оперативно исправляет найденные уязвимости. Ситуация с обновлениями здесь гораздо лучше, чем

в Android. Впрочем, малая распространенность системы и слабая заинтересованность самой Microsoft в будущем платформы нивелируют многие ее преимущества.

Google Android

Наконец-то мы дошли до Android. Про безопасность в Android написаны десятки тысяч статей и сотни книг. Разумеется, мы не будем пытаться объять необъятное; вместо этого попробуем окинуть взглядом экосистему в целом.
Скажем сразу: смартфоны на Android самые распространенные, но при этом наименее безопасные. Версии Android 4.4 и ниже можно назвать дырявым ведром, не слишком погрешив против истины. Критические уязвимости и зияющие бреши в безопасности были (и есть) в сборках 5.0–5.1.1. Минимально приемлемый уровень безопасности в Android был достигнут только с версией 6.0, причем только в тех устройствах, которые выходили с завода уже с Android 6.0 на борту. А вот в Android 7 (относительная доля которого до сих пор не перевалила за 8% устройств) физическая безопасность уже реализована вполне неплохо.
Называя Android дырявым ведром, нельзя не уточнить, что по абсолютному числу найденных уязвимостей iOS далеко впереди. Однако если Apple исправляет уязвимости и выпускает обновление в течение двух-трех недель, то уязвимости, найденные в Android, будут исправлены в «сферическом коне в вакууме», полумифическом AOSP. Обычные же пользователи могут получить их вместе с ежемесячным обновлением безопасности (только для актуальных флагманов у избранных производителей), получить через полгода-год или не получить никогда. Диаграмма распространенности разных версий Android намекает, что актуальные патчи безопасности своевременно поступят к от силы 7% пользователей.
В случае с Android значение имеет не только какая версия системы установлена, но и с какой версией устройство вышло с завода. Так, Android 6.0 «из коробки» по умолчанию шифрует раздел с пользовательскими данными, но смартфонов, обновившихся до Android 6 по воздуху, это не коснется.

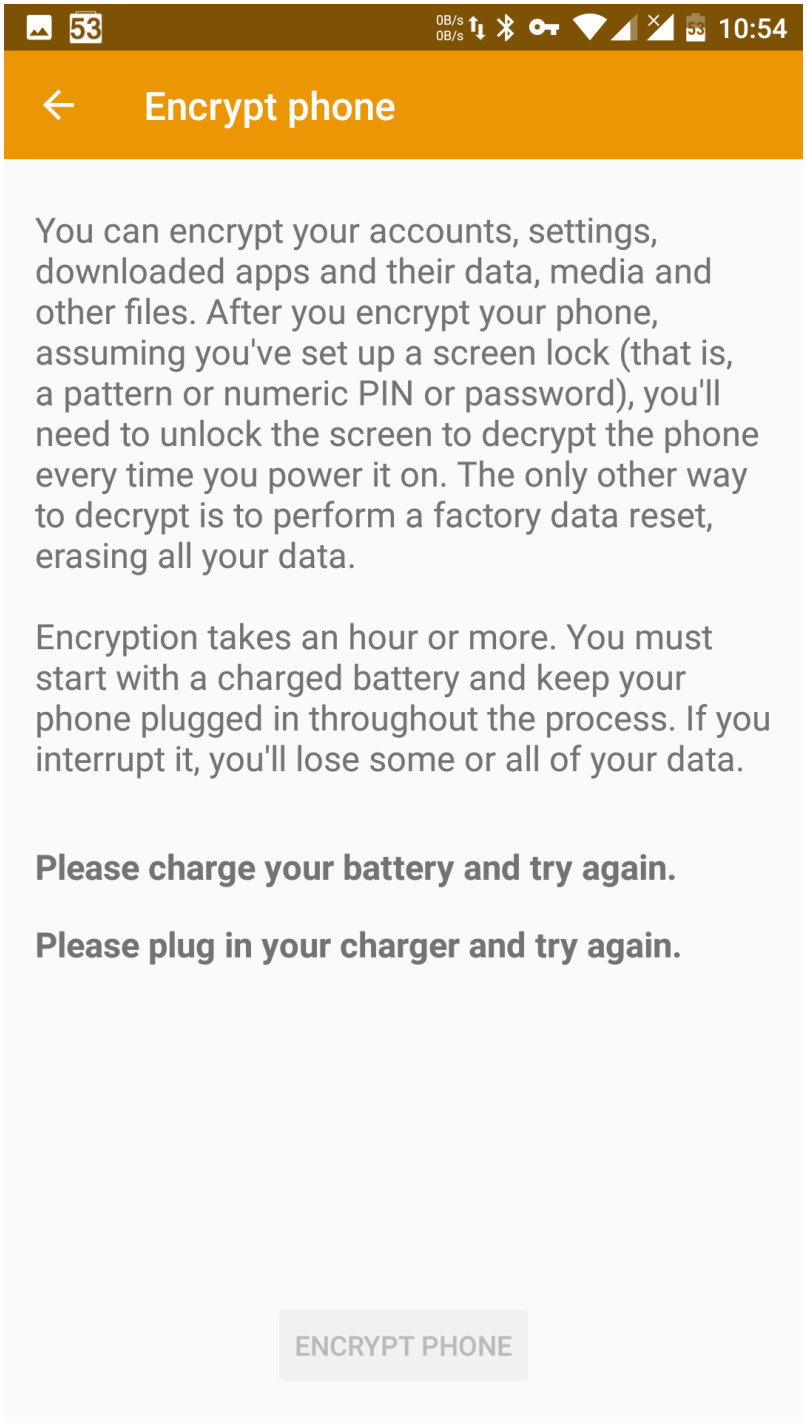
Сколько телефонов с Android зашифровано?

На Google I/O сообщили, что порядка 80% устройств под управлением Android 7 и порядка 25% под управлением Android 6 зашифрованы. Что это означает на практике? Сравним распространенность версий Android с данными о шифровании:

- Android 5.1.1 и более старые: ~62% рынка (данных о шифровании нет);

- Android 6: 0,31 (31% рынка) * 0,25 = 0,078;
- Android 7: 0,07 (7% рынка) * 0,80 = 0,056.

Итого получаем цифру в 13,4%. Это — число устройств на Android, которые точно зашифрованы. Основная заслуга здесь принадлежит Google, которая заставила производителей устройств, выходящих с Android 6 или 7 на борту, обязательно активировать шифрование. Данных о шифровании более старых версий нет, но можно предположить, что их пользователи не горят желанием замедлять работу устройства, включив опциональное шифрование. С учетом этого вряд ли конечная цифра зашифрованных «Андроидов» превысит 15%.



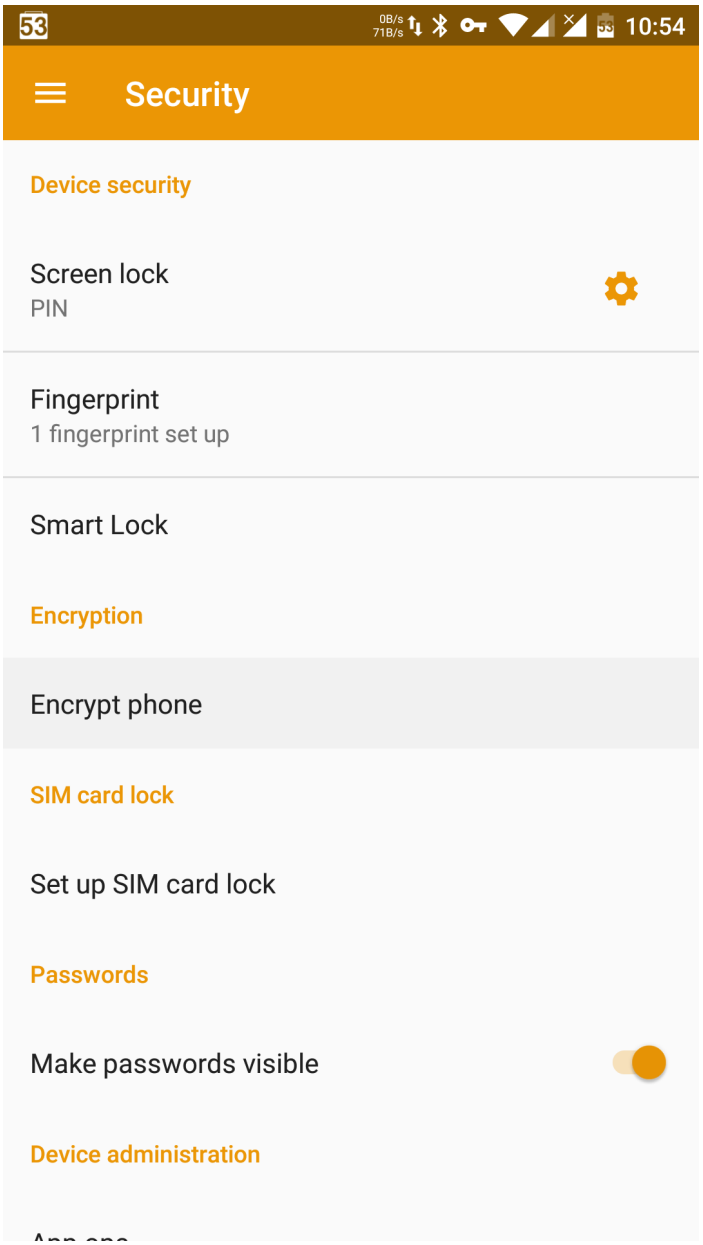
Несмотря на то что Android, как и iOS, запускает приложения в песочницах, тут гораздо больше свободы. Приложения могут вмешиваться в работу других приложений (в

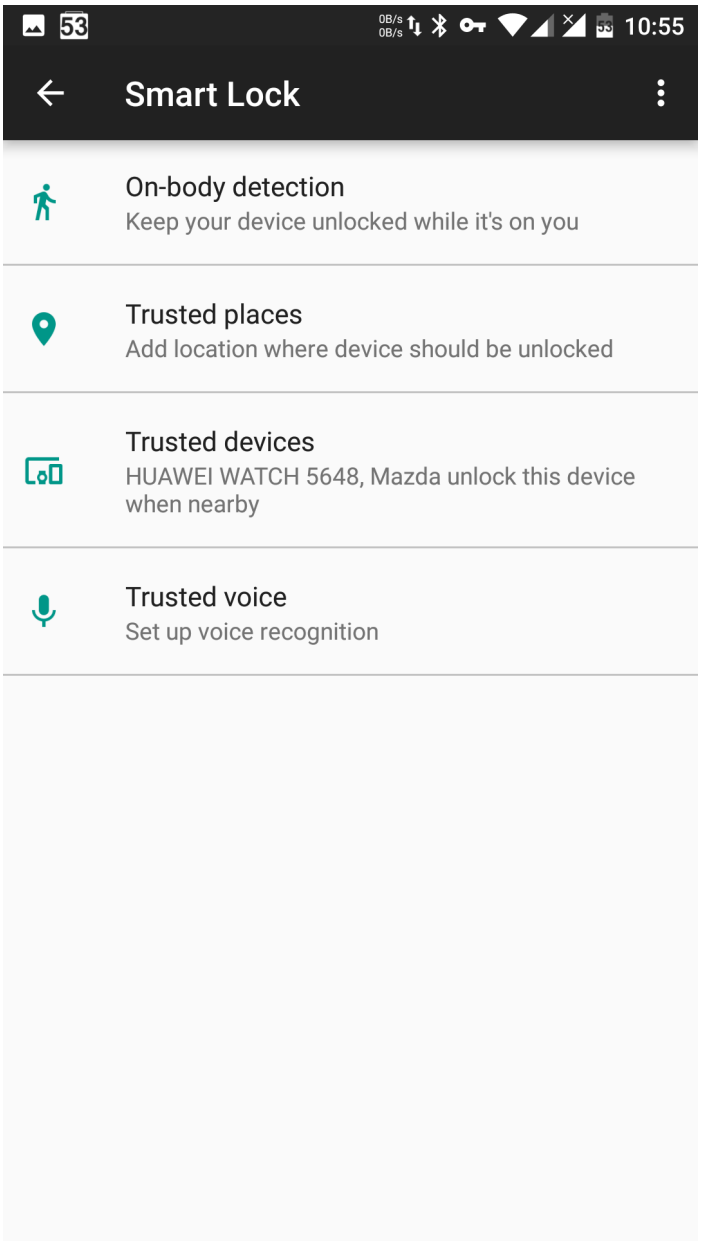
первую очередь это разнообразные службы Accessibility, которые могут даже нажимать кнопки, и сторонние клавиатуры, которые автоматически получают возможность шпионить за пользователем). Приложения могут собирать данные о приблизительном местоположении пользователя, даже если соответствующие права отсутствуют (механизм интересный, часто применяется на практике и заслуживает отдельной статьи). Многочисленные зловреды появляются еженедельно, а в некоторых телефонах (о таких мы писали) они сидят прямо в прошивках и избавиться от них возможно только с помощью перепрошивки.

Да, эта особенность, а точнее степень свободы заложена в систему (то есть это фича, а не баг), и те же сервисы Accessibility и сторонние клавиатуры требуют отдельного подтверждения для активации. Но поверь, твоему ребенку, теще или бабушке сильно легче от этого не станет, как бы ты ни пытался натаскать их на «сюда не тыкай никогда».

А разблокирование смартфона? Казалось бы, простейшее действие, которое невозможно испортить… Но нет, разработчики Android (именно Android AOSP) — смогли. В Android встречаются любые, самые небезопасные способы аутентификации. Например, Smart Lock — автоматическое разблокирование телефона по местоположению (представь ситуацию, в которой ФБР не приходится платить миллион долларов за взлом iPhone 5c — вместо этого агент просто дошел до дома подозреваемого). Или разблокирование при соединении с доверенным Bluetooth-устройством (агент включает трекер активности или магнитолу в машине подозреваемого).

Еще можно авторизоваться по лицу пользователя или его фотографии. Некоторые способы можно запретить с помощью корпоративной политики безопасности, но для запрета необходимо перечислить их в явном виде. Сисадмин забыл запретить разблокировку по Bluetooth-устройствам? Этой лазейкой непременно воспользуются. Ну и если появится новый небезопасный способ разблокировки — его придется запрещать дополнительно.

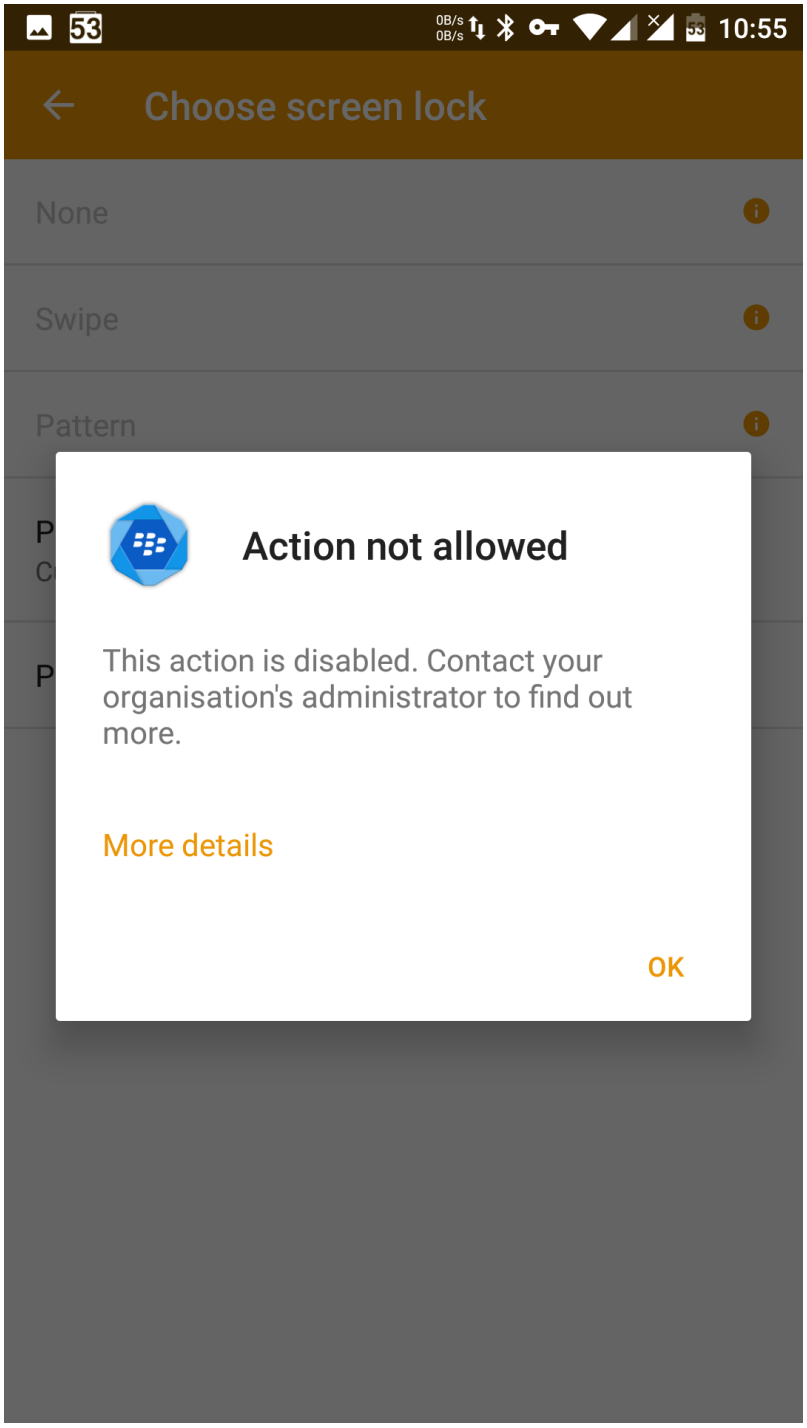




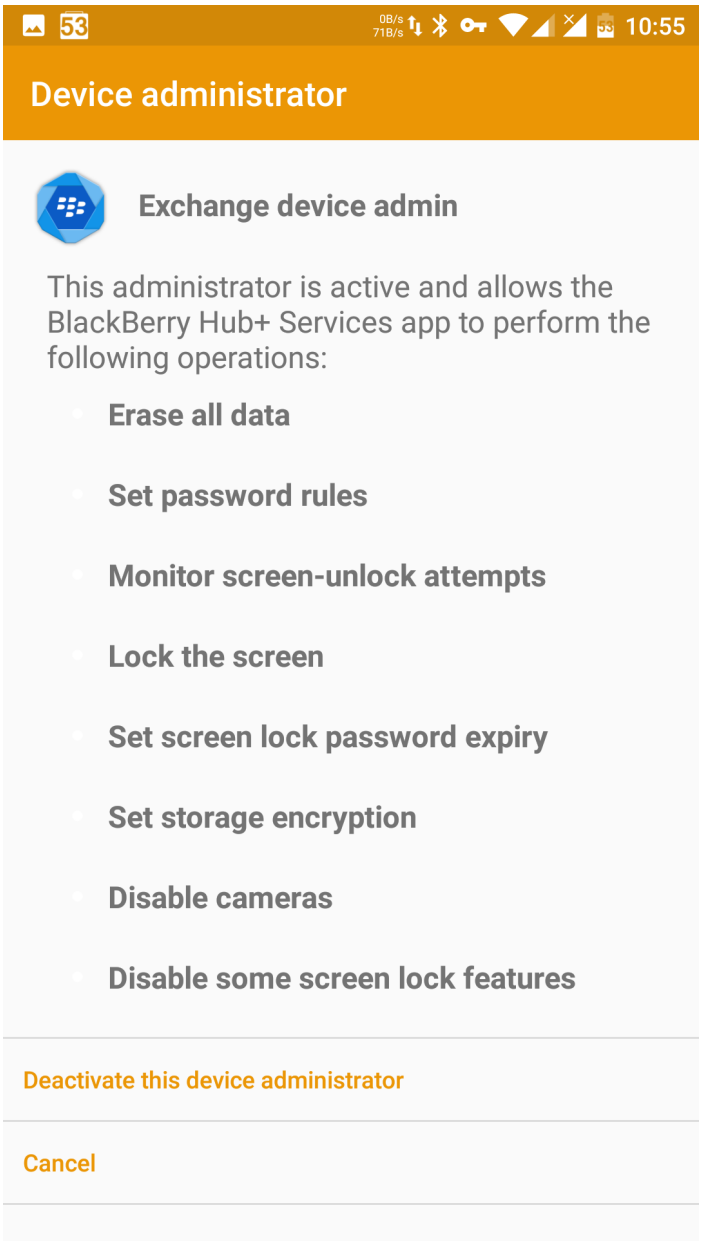
Любые виды разблокировки на твой вкус

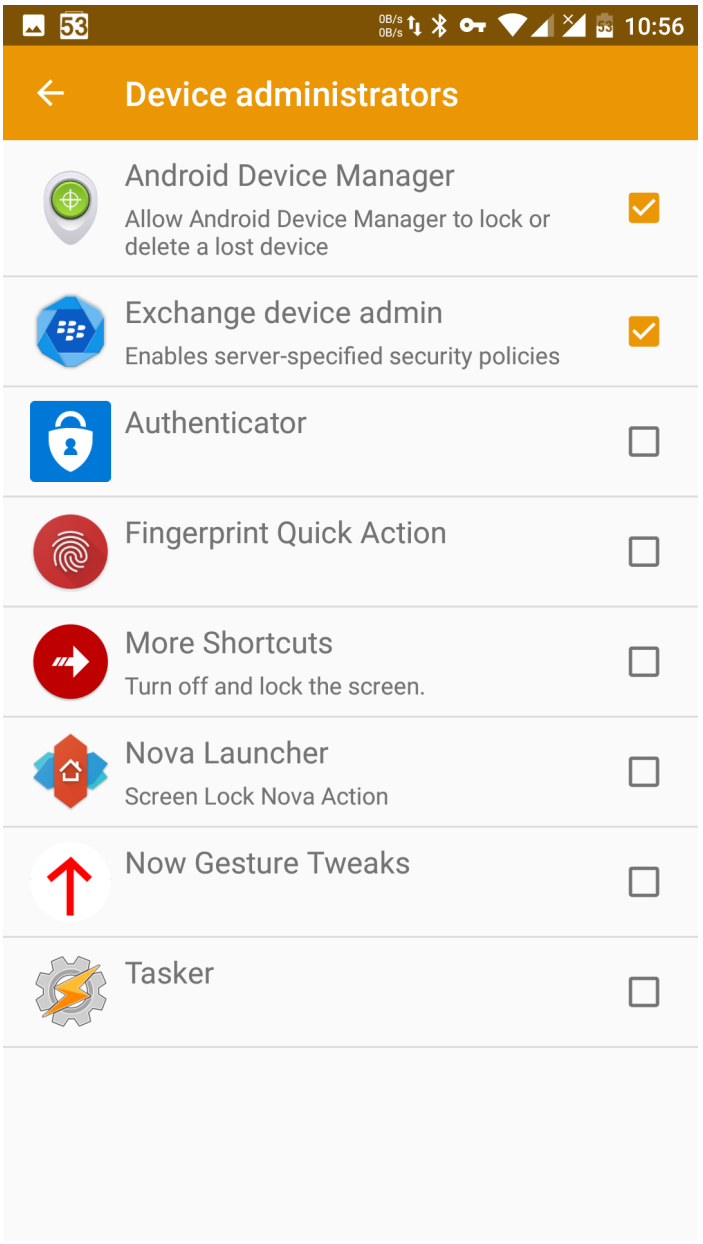
Да, намерения были благими: хоть как-то попробовать заставить пользователей устройств без датчика отпечатков пальцев устанавливать код блокировки. Вот только вред от таких способов просто катастрофический: пользователю внушается ложное чувство безопасности, на самом же деле «защитой» подобные способы можно назвать лишь в кавычках. Более того, Smart Lock остается доступным даже в последних сборках Android и даже в устройствах, уже оборудованных датчиком отпечатков пальцев. Нет, использовать Smart Lock тебя никто не заставит, но ведь это же так удобно…

К счастью, с помощью политики безопасности некоторые виды разблокировки можно ограничить административно:

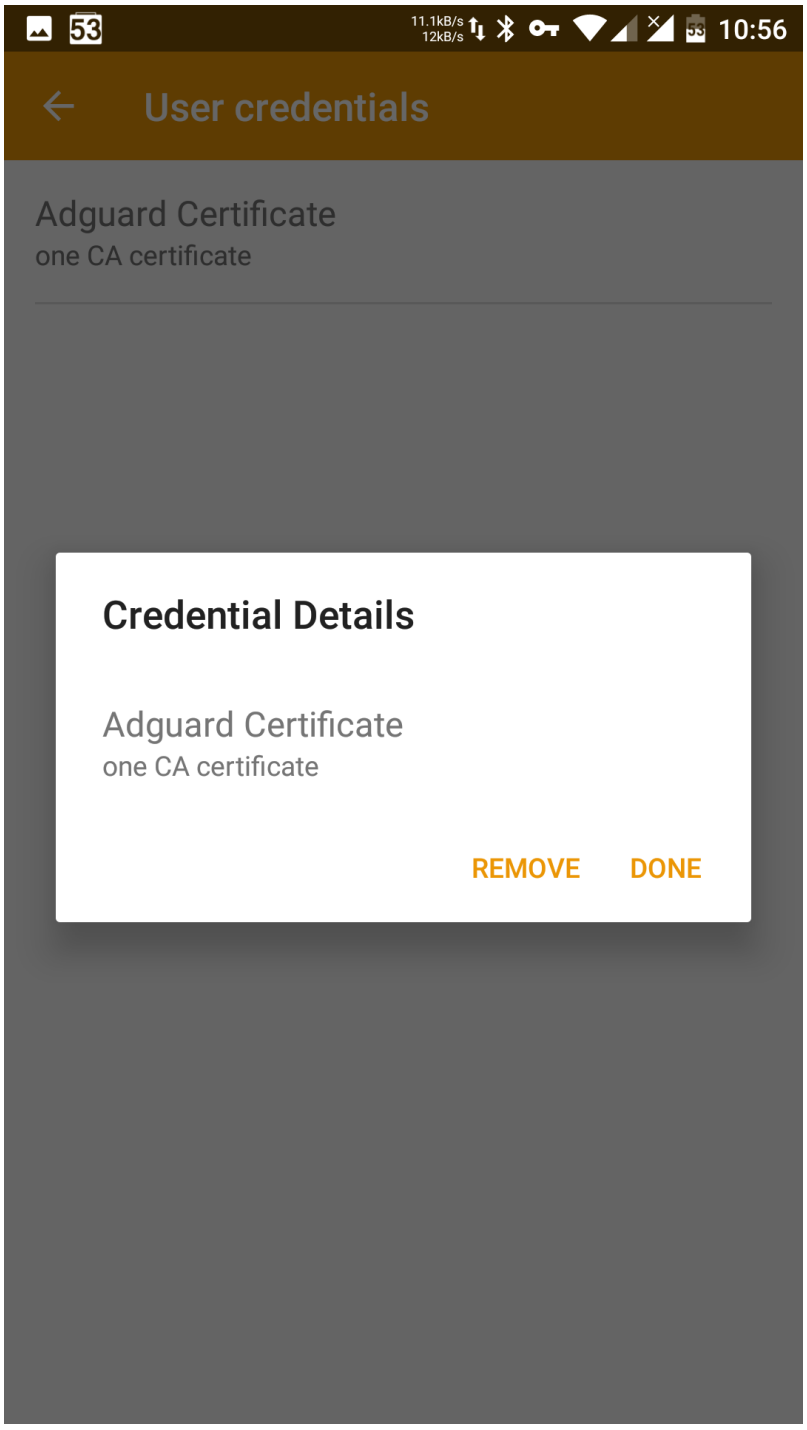


Впрочем, нет никакой возможности помешать пользователю деактивировать такую политику:


10:55
Device administrator
Exchange device admin
This administrator is active and allows the BlackBerry Hub+ Services app to perform the following operations:
Erase all data
Set password rules
Monitor screen-unlock attempts
Lock the screen
Set screen lock password expiry
Set storage encryption
Disable cameras
Disable some screen lock features
Deactivate this device administrator
Cancel


10:56
Device administrators
Android Device Manager
Allow Android Device Manager to lock or delete a lost device
Exchange device admin
Enables server-specified security policies
Authenticator
Fingerprint Quick Action
More Shortcuts
Turn off and lock the screen.
Nova Launcher
Screen Lock Nova Action
Now Gesture Tweaks
Tasker

В Android есть возможность установить свой сертификат для снифинга HTTPS-трафика:

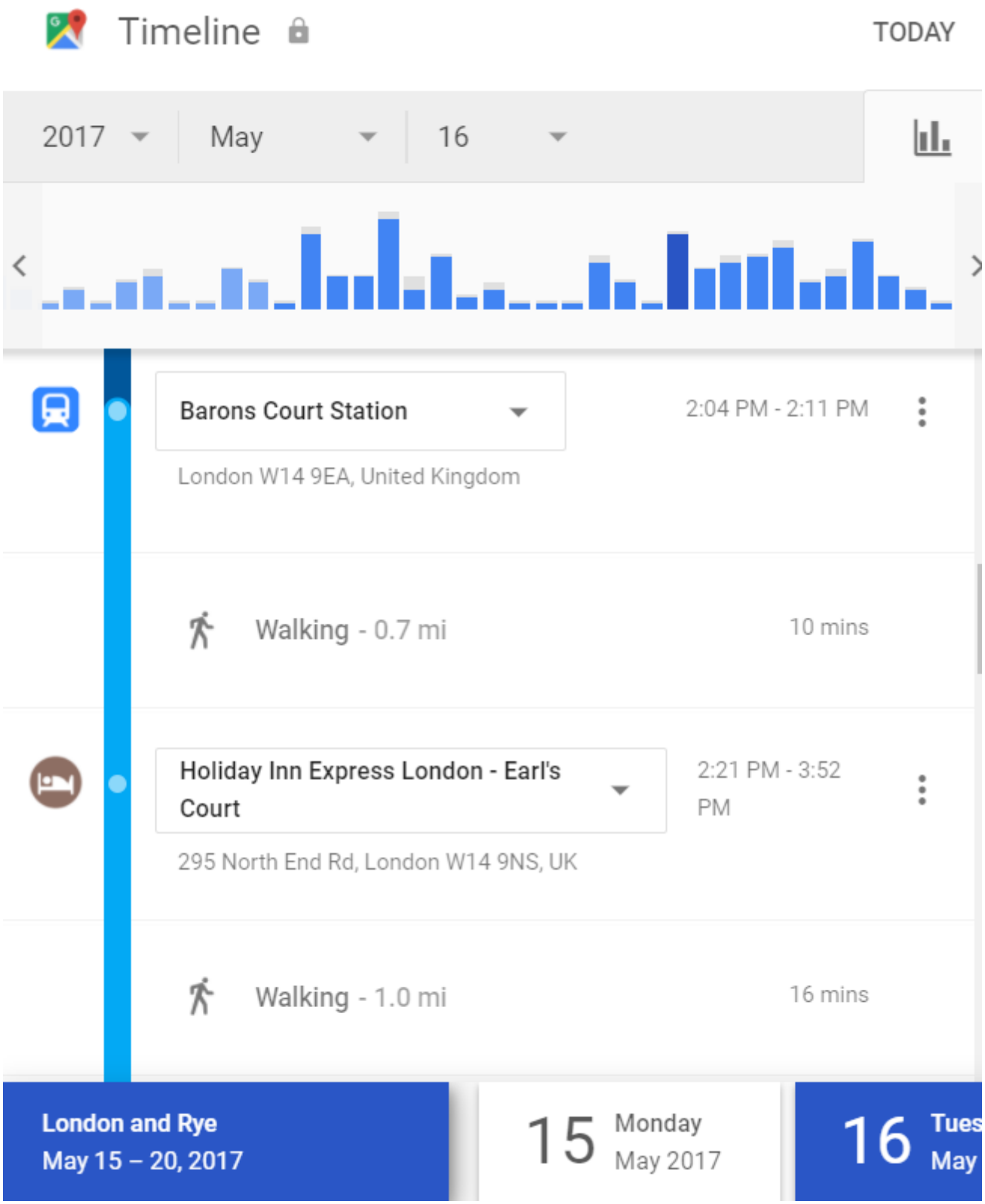


Теперь у приложения Adguard есть возможность вырезать рекламу из HTTPS-трафика. Но на его месте могло оказаться что угодно.

Большой Брат следит за тобой

Google собирает огромное количество информации о пользователях Android. Ее детальность и проработка просто фантастические: ты можешь подробно увидеть, где ты был и что делал в такое-то время такого-то числа за последние шесть лет. Что характерно, Google знает не только *где* ты был в терминах географических координат, но и *в каком месте* ты побывал. Гостиница, ресторан, боулинг, театр, парк — Google

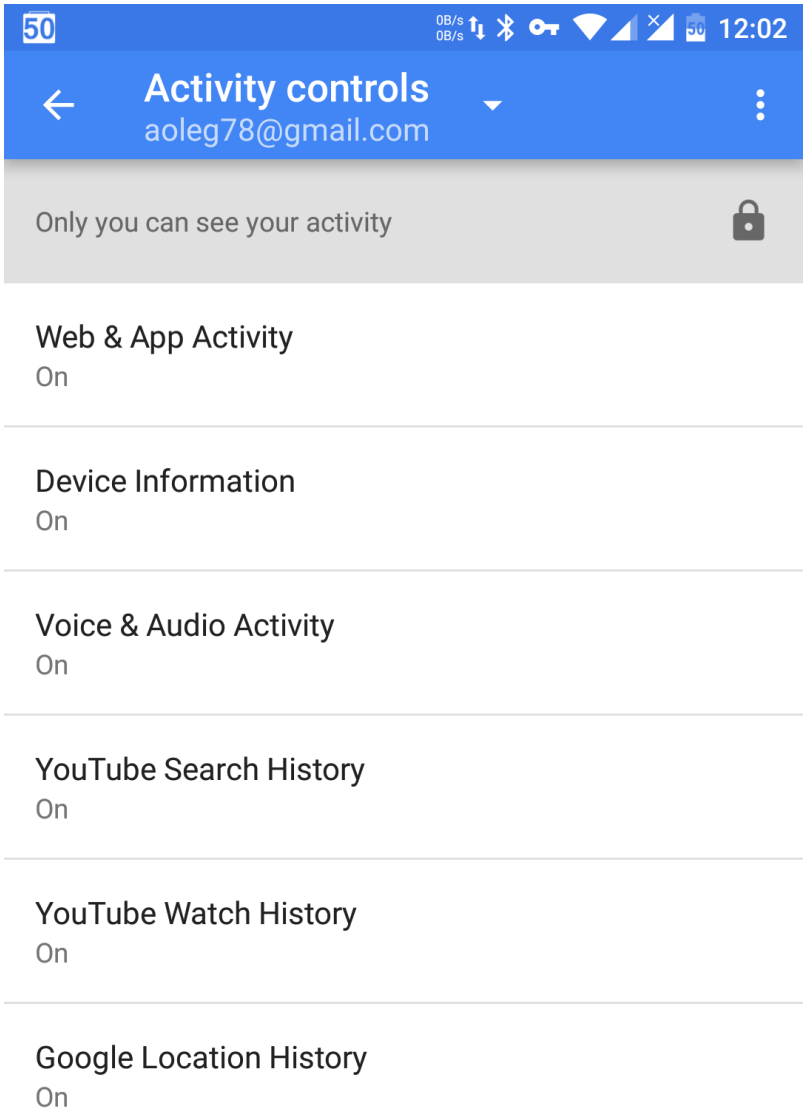
видит твои координаты и соотносит их с местоположением других пользователей (а их — миллиарды). Результат — компании известно все вплоть до того, сколько времени ты просидел за столиком в ресторане в ожидании первого блюда.
Скажешь, я сгущаю краски? Ничуточки. Мы уже писали о том, что собирает Google и как до этой информации добраться.



Google знает о тебе больше тебя
Само собой разумеется, в Google есть статистика запуска и использования приложений, история браузера и поисковых запросов, логины и пароли Chrome, слова, которые

вводились с клавиатуры Gboard, голосовые запросы, просмотренные на YouTube ролики и многое, многое другое.

Да, слежку и сбор информации ты можешь ограничить, а уже собранные данные — удалить, но разнообразие этих данных таково, что только их перечисление займет несколько страниц убористого текста. Более того, время от времени Google без предупреждения включает сбор новых типов данных (яркий пример — синхронизация информации о звонках и SMS на некоторых устройствах); как отключить их сбор и хранение, не всегда ясно даже специалистам. В двух словах: ограничить сбор данных можно, но гарантии того, что запрещен сбор всех твоих данных, — никакой.



Лишь часть того, что собирает Google

Большинство телефонов с Android поставляется с незакрытыми режимами сервисного доступа к памяти, которые изначально создавались для прошивки устройств в случае

неисправности. Эти же режимы можно использовать и для извлечения данных из устройства, даже если оно выключено или заблокировано. В частности, это присуще большинству процессоров Qualcomm (режимы 9006 и 9008), практически всем MediaTek, Rockchip, Allwinner, Spreadtrum, некоторым устройствам на основе Samsung Exynos. Собственный низкоуровневый сервисный протокол есть в телефонах LG, и воспользоваться им для извлечения данных — дело техники.

Использование сервисного режима для кражи данных не оставляет следов. Защититься от кражи информации через сервисный режим довольно просто: достаточно включить шифрование данных (при этом рекомендуется Android 6.0 или выше, но даже в Android 5 шифрование уже вполне надежно).

Гранулярный контроль за разрешениями приложений в Android — больная тема. В «чистом» Android (AOSP) контроль за использованием разрешений появился только с выходом версии 6.0. В сторонних прошивках он был и раньше, но работал чрезвычайно нестабильно. При этом контроль далек от совершенства: запретить приложению работать в фоне штатными средствами невозможно, а ограничение доступа к разрешению доступа к местоположению приводит только к тому, что приложение будет определять местоположение устройства другими способами с помощью использования разрешений, гранулярный контроль которых невозможен даже в свежих версиях Android. Наконец, многие приложения просто не поддерживают гранулярное управление разрешениями, и пользователь по-прежнему соглашается с запросом на предоставление целого пакета разрешений, часть из которых вовсе не безобидна.

С помощью корпоративных политик безопасности можно запретить пользователю некоторые (но, к сожалению, далеко не все) способы обойти встроенные в систему меры безопасности. Например, можно заставить его использовать PIN-код, отключить Smart Lock, заставить использовать встроенное шифрование. Еще можно купить Android-смартфон BlackBerry; на них, по крайней мере, своевременно приходят патчи безопасности и активен режим доверенной загрузки. Впрочем, от действий самого пользователя, слежки и утечки данных в облако фирменный софт BlackBerry не защищает никак.

В Android просто не существует какой-то общей модели безопасности, которая могла бы обезопасить устройство и данные пользователя на всех уровнях. Можно включить KNOX, можно выбрать телефон с доверенной загрузкой… но все это не помешает самому пользователю установить какое-нибудь приложение, которое воспользуется «особенностями» Android (например, Overlay и Accessibility) для автоматической установки опасных зловредов, и те, снова используя уязвимости системы, попытаются получить root-доступ и прописаться в системном разделе.

Слово редактора

Стоит отметить, что, хотя автор прав в том, смартфон на какой ОС более уязвим к взлому, следует иметь в виду, что речь именно о смартфонах, но не об Android как операционной системе. Да, Android заслужил славу дырявой операционки и рассадника вирусов, но если вдуматься: а что есть Android? Это то, что установлено на смартфонах LG или Samsung, те самые сильно модифицированные операционки, которые кажутся совсем не похожими на «голый» Android? Это прошивки менее распространенных брендов, которые устанавливаются на смартфоны, годами не получающие обновлений? Или, может быть, это что-то другое?

Технически ОС Android — это то, что Google в форме исходников выкладывает во всеобщий доступ в рамках проекта AOSP. Это тот самый чистый Android, который компания предустанавливает на смартфоны Nexus и, в слегка измененном виде, на смартфоны Pixel. Все остальные прошивки, сильно и не очень сильно модифицированные, в терминах open source называются форками. По сути это уже нечто другое, но все это тем не менее принято называть общим именем Android.

Безопаснее ли чистый Android прошивок от производителей? Да, множество багов было найдено именно в измененном Android от производителя. К тому же в чистом Android эти баги исправляются намного быстрее и обновления, с небольшой задержкой, получают сразу все юзеры Nexus и Pixel. Общий срок поддержки этих смартфонов составляет два года для крупных обновлений и еще год для обновлений безопасности.

Как правильно отметил Олег, по общему количеству найденных критических уязвимостей Android остается позади iOS, причем больше половины этих багов находят вовсе не в Android, а в закрытых драйверах железа. Перечисленные в статье проблемы смартфонов вроде того же сервисного режима к Android отношения не имеют, это проблема производителя устройства. Однако в том же Nexus сервисный режим доступен — логично, если учесть, что это смартфон для разработчиков.

Серьезная проблема Android — это вовсе не дырявость и не безграмотная архитектура ОС. В конце концов, даже версия Android 1.0 включала в себя такие вещи, как полноценные песочницы для приложений, система обмена данными между приложениями через типизированные каналы с проверкой полномочий, многоуровневая проверка легитимности тех или иных запросов к данным или функциям ОС и memory safe язык Java, нивелирующий 90% возможных уязвимостей. О более поздних версиях с интегрированной системой мандатного контроля доступа SELinux, песочницами на основе seccomp, ASLR, механизмом доверенной загрузки, шифрованием и целым букетом прочих технологий говорить вообще не стоит.

Серьезная проблема Android — это та самая фрагментация, благодаря которой Android’ом называется все, что было основано на AOSP, а по факту уже не являющееся Android’ом. Компания выпускает смартфон на Android, забивает на его обновление, чем ставит под угрозу пользователя, — виновным объявляют Android. Samsung

модифицирует Android, допуская ошибку в реализации локскрина, — виноват Android. Китайцы поставляют смартфоны с незалоченным загрузчиком — это Android дырявый. Также не стоит забывать о гораздо больших, в сравнении с iOS, возможностях системы. Все эти Accessibility, оверлеи и другие функции, которые автор преподносит как уязвимости, — это стандартная часть Android, которая доступна сторонним приложениям. Чем больше функциональности предлагает система, тем больше возможностей использовать ее в грязных целях.
Сравнивать iOS, систему с сильно обрезанной функциональностью, отсутствием возможности ставить приложения из сторонних источников и закрытой экосистемой, с открытым Android, который дает гораздо больше возможностей и доступен для свободного скачивания и модификации кому угодно, некорректно. Это все равно что сравнивать полноценную ОС типа Windows и какую-нибудь Chrome OS.

Можно ли сделать Android действительно безопасным?

Если телефоном пользуется ребенок, бабушка или человек, который увлекается чем угодно, только не вопросами безопасности мобильных операционных систем, — нет. В их руках телефон на Android никогда не будет безопасным, даже если это Samsung с активированным KNOX или BlackBerry с последним патчем безопасности. Причина? Слишком много зловредов и слишком большая для среднего пользователя степень свободы, позволяющая убрать «мешающие» средства безопасности, отключить шифрование на этапе загрузки, активировать установку приложений из сторонних источников и проделать массу других глупостей, которые тебе даже трудно вообразить. Если же устройство дать в руки специалисту и устройство это — актуальный флагман одного из избранных производителей, не пренебрегающих ежемесячными патчами безопасности, то при должной настройке (запрет Smart Lock, шифрование с обязательным запросом пароля для дальнейшей загрузки устройства, — не путать с PIN-кодом разблокировки! — использование административной политики, жестко запрещающей установку из сторонних источников, запрет оверлеев и сервисов Accessibility, постоянный контроль за тем, какую информацию мы разрешаем о себе собирать и кому именно) для обычного пользователя вполне сойдет. Впрочем, чиновники, президенты, террористы и преступники все равно не будут так рисковать; их выбор до сих пор — BlackBerry 10 или iOS.
Традиционно последний параграф — про обновления и патчи безопасности. Специфика Android такова, что производители могут обновлять, а могут и не обновлять свои устройства до актуальных версий Android и патчей безопасности. Найденные уязвимости могут исправляться, а могут не исправляться (в большинстве случаев — не исправляются). Более-менее регулярные обновления бывают у флагманов известных

производителей, но даже в этом случае сроки поддержки заметно короче, чем у устройств производства Apple или Microsoft. Телефоны с Android по уровню безопасности нельзя ставить на одну ступень с iOS или даже Windows 10 Mobile. Чем дешевле устройство, тем хуже у него будут обстоять дела с безопасностью уже через несколько месяцев после выпуска. Совсем дешевые устройства несут дополнительные риски, связанные с отсутствием обновлений (в том числе исправлений критических уязвимостей), физическими уязвимостями на уровне устройств и встроенными в прошивки зловредными «бонусами».

Заключение

Если расставить системы по уровню безопасности, то ряд будет выглядеть следующим образом: Apple iOS (iPhone SE, 6s/7), Windows 10 Mobile (Lumia 950 и 950 XL), Android (лучше всего дела обстоят у свежих флагманов Samsung, BlackBerry и других крупных производителей; хуже всего — у бюджетных моделей китайских производителей, с полным спектром решений между этими крайностями). Что из этого стоит брать? Все зависит от твоих приоритетов. Для большинства пользователей будет вполне достаточно того невысокого уровня безопасности, который предлагает Android, — разумеется, при условии, что у тебя установлен PIN-код и включен датчик отпечатков пальцев (но только если стоит Android 6.0 или выше и только если он сертифицирован Google); если нет root и заблокирован загрузчик; если активировано полнодисковое шифрование и выключены небезопасные способы аутентификации Smart Lock; если… Впрочем, это перечисление уже тянет на отдельную статью.

В случае с Apple все намного проще: свежие флагманы под управлением свежих версий iOS безопасны, но если ты озабочен приватностью своих данных — отключи облако. Больше ничего делать не нужно.

«Неуловимые Джо» (Sailfish, Tizen, Ubuntu Touch и прочая экзотика) небезопасны до тех пор, пока не будет доказано обратное. Про Tizen выводы уже сделаны, Sailfish — на очереди.