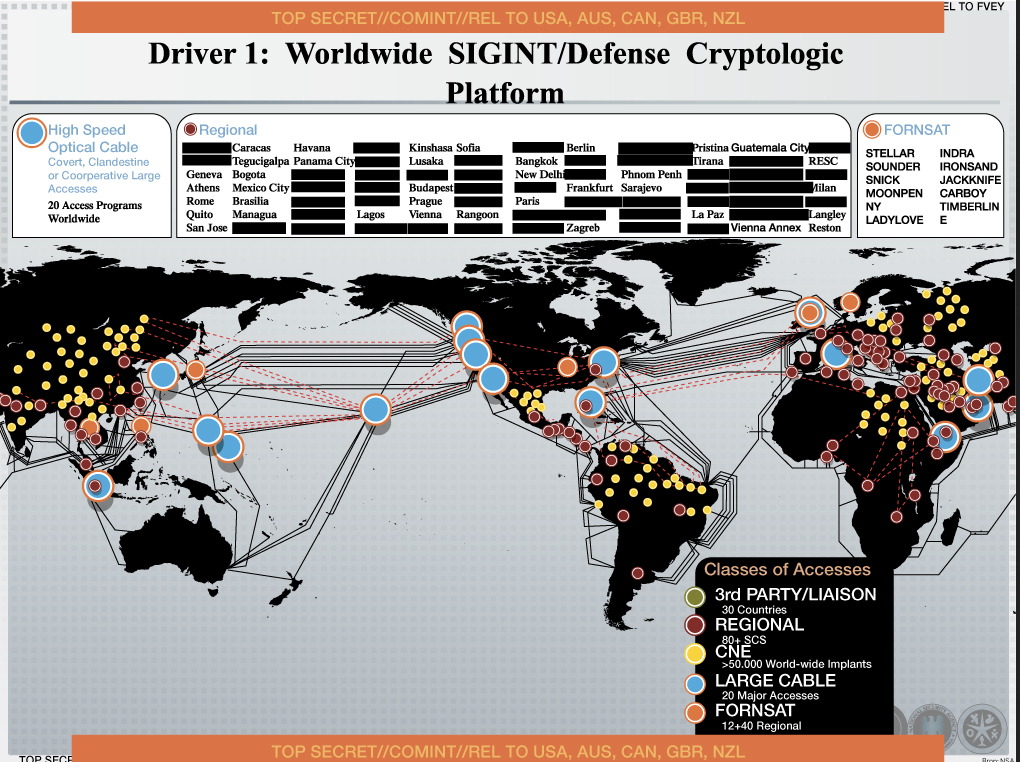
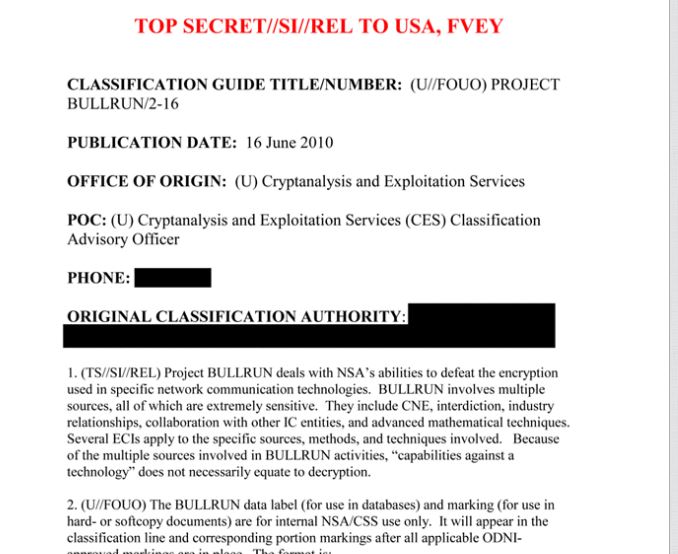
Мобильные телефоны и тотальная слежка АНБ: как это работает



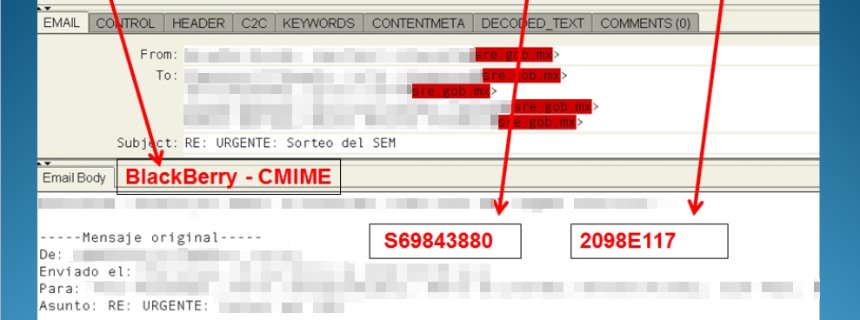
Имя Эдварда Сноудена последние два года регулярно мелькает в новостях по теме информационной безопасности. Благодаря разоблачениям этого бывшего сотрудника американских спецслужб все уже слышали, что Агентство национальной безопасности (АНБ, NSA) обладает возможностями тотальной мобильной слежки за гражданами. Но как именно устроена эта слежка, мало кто знает. В данном обзоре мы собрали некоторые подробности о технологиях, которыми пользуется NSA - и не только оно.

Одна из первых неприятных новостей от Сноудена касалась подрыва доверия **к технологиям криптозащиты**. В рамках секретного проекта АНБ под названием [Bullrun](http://www.theguardian.com/world/interactive/2013/sep/05/nsa-project-bullrun-classification-guide) была получена возможность обхода многих систем шифрования – но не за счёт взлома, а за счёт эксплуатации закладок, специально оставленных производителями по требованию АНБ. А в некоторых случаях вендоров просто обязали сдавать агентству шифровальные ключи. Таким образом, [были дискредитированы](http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html) многие стандарты безопасности, считавшиеся надёжными и применявшиеся в крупном бизнесе и государственных организациях.



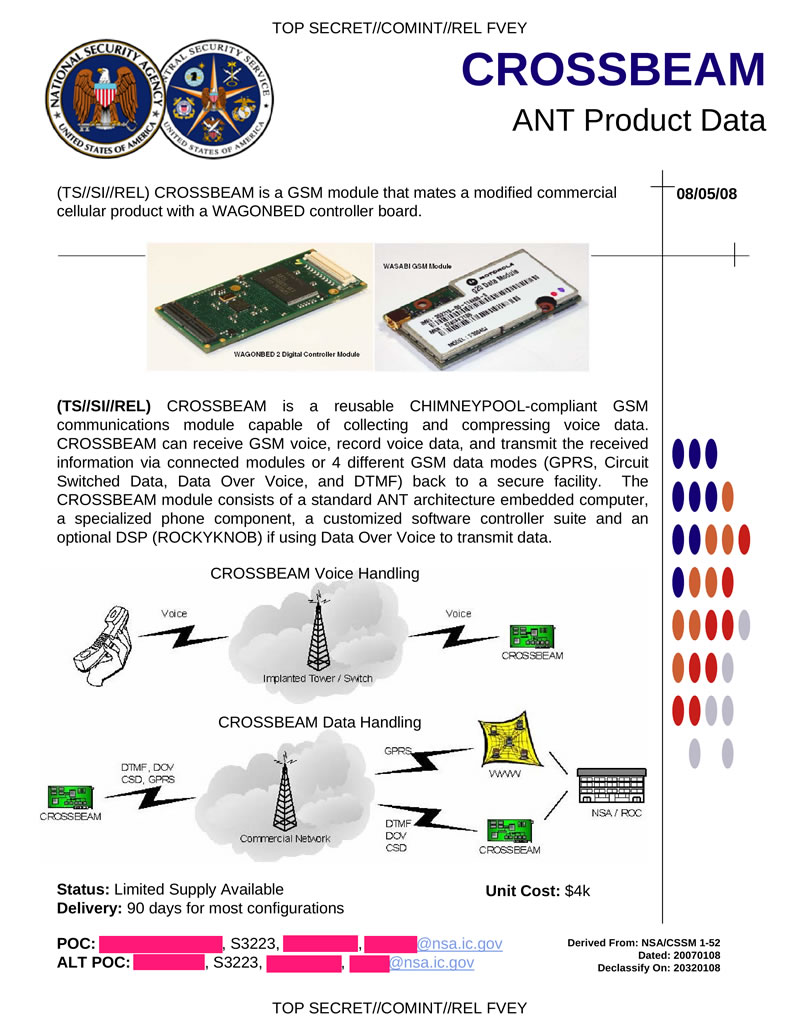
Буквально на днях в СМИ появилось развитие этой истории – некоторые детали операции [AuroraGold](https://firstlook.org/theintercept/2014/12/04/nsa-auroragold-hack-cellphones/), в рамках которой АНБ следило за сотрудниками телекомов, читая их электронную переписку и внутренние документы. Уже в мае 2012 года АНБ собрало таким образом технические данные о 70% мобильных сетей всего мира. Под прослушку попала и GSM Association – международная организация телекомов, где разрабатываются рекомендации по новым стандартам связи. Цель операции AuroraGold – та же, что и у проекта Bullrun: внедрить закладки либо узнать об уязвимостях, которые помогут обойти алгоритм шифрования A5/3 и другие новые технологии защиты. Судя по документам из архива Сноудена, первые попытки [взломать G4](https://firstlook.org/theintercept/document/2014/12/04/first-ever-collect-high-interest-4g-cellular-signal) удавались агентству АНБ ещё в 2010 году – то есть ещё до того, как этот «безопасный» стандарт получил широкое распространение.

Другой вектор атак АНБ – это **мобильные ОS и приложения**. Как выяснилось, спецслужба имеет доступ ко множеству данных на смартфонах: списки контактов и звонков абонентов, а также их SMS и GPS-данные. Для этого в АНБ были собраны команды хакеров, каждая из которых занималась взломом одной из популярных OS. В публикации немецкого журнала [Spiegel](http://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html) подчёркивается, что одной из первых была взломана операционка Blackberry, хотя традиционно она считалась более защищенной, чем iOS и Android.

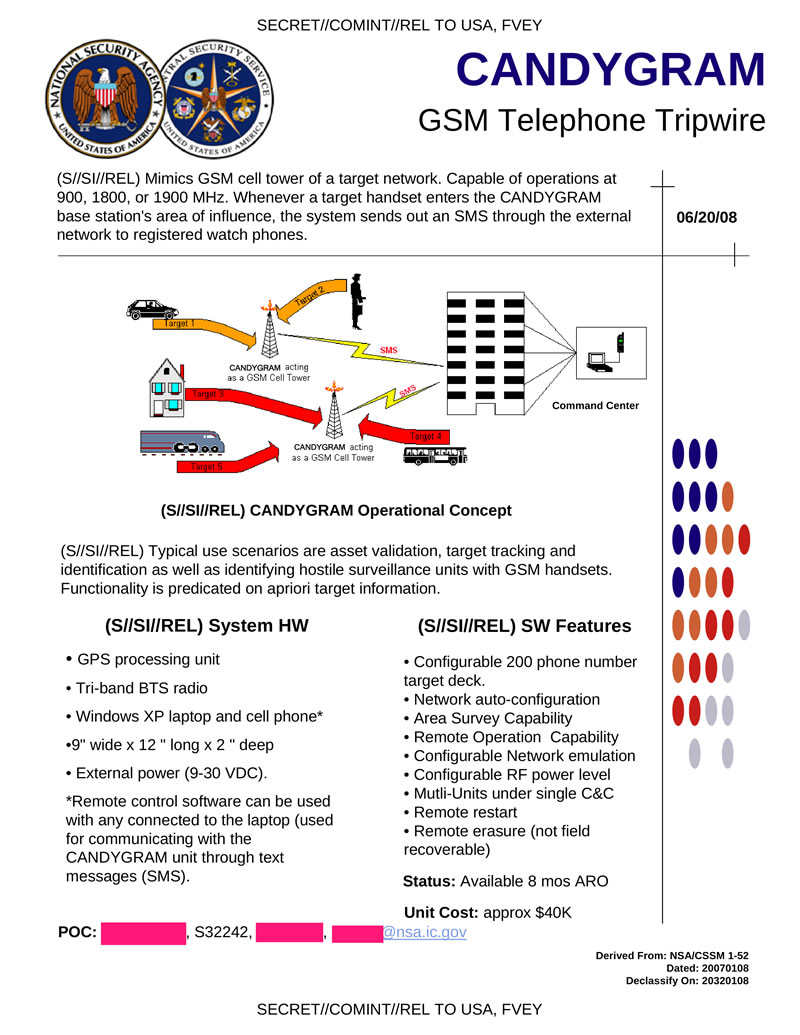


И конечно же, возможности прослушки значительно расширились благодаря развитию рынка **мобильных приложений**. Многие из них регулярно передают значительное количество пользовательских данных третьим сторонам. Таким образом, для подслушивания необязательно взламывать OS – достаточно убедить пользователя поставить себе «полезное» мобильное приложение.

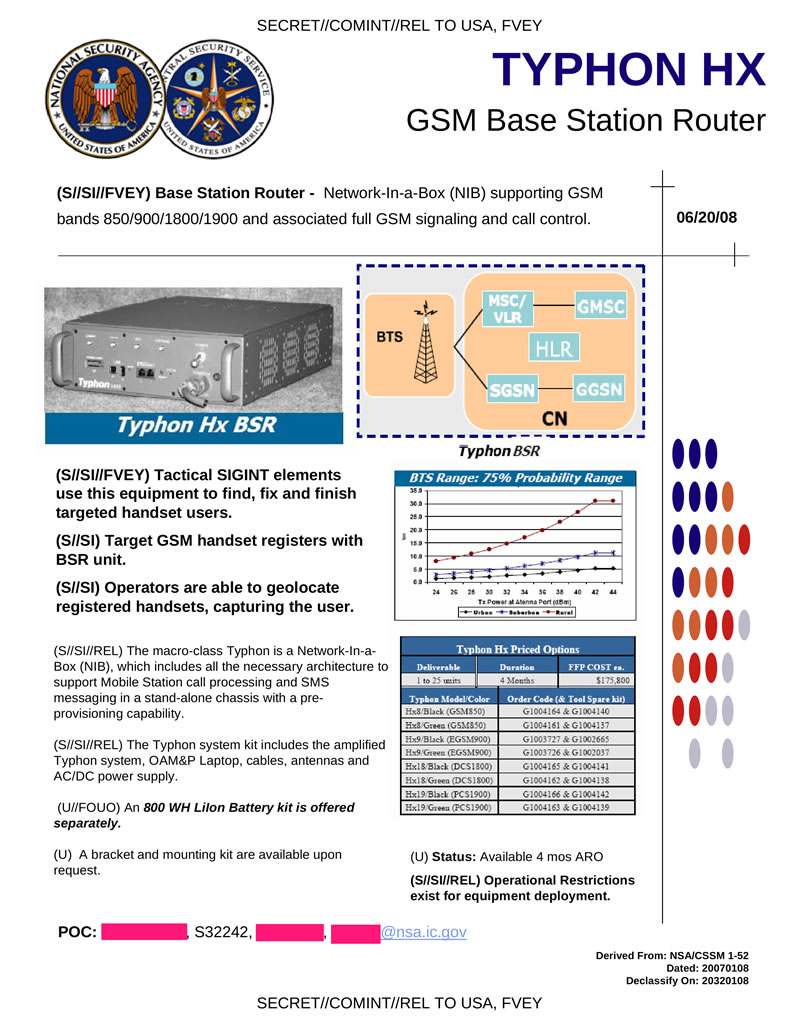
Но ещё больше возможностей для слежки обнаружилось в самих **сетях мобильной связи**. В документах Сноудена нашлось описание шпионского каталога АНБ - [проекта Ant](http://www.spiegel.de/international/world/a-941262.html), в котором есть решения для манипуляции мобильными сетями на все случаи жизни. Необязательно перехватывать данные через уязвимое ПО - можно установить закладки на стадии изготовления устройств связи. Вот, например, скомпрометированный радио-модуль для телефона:



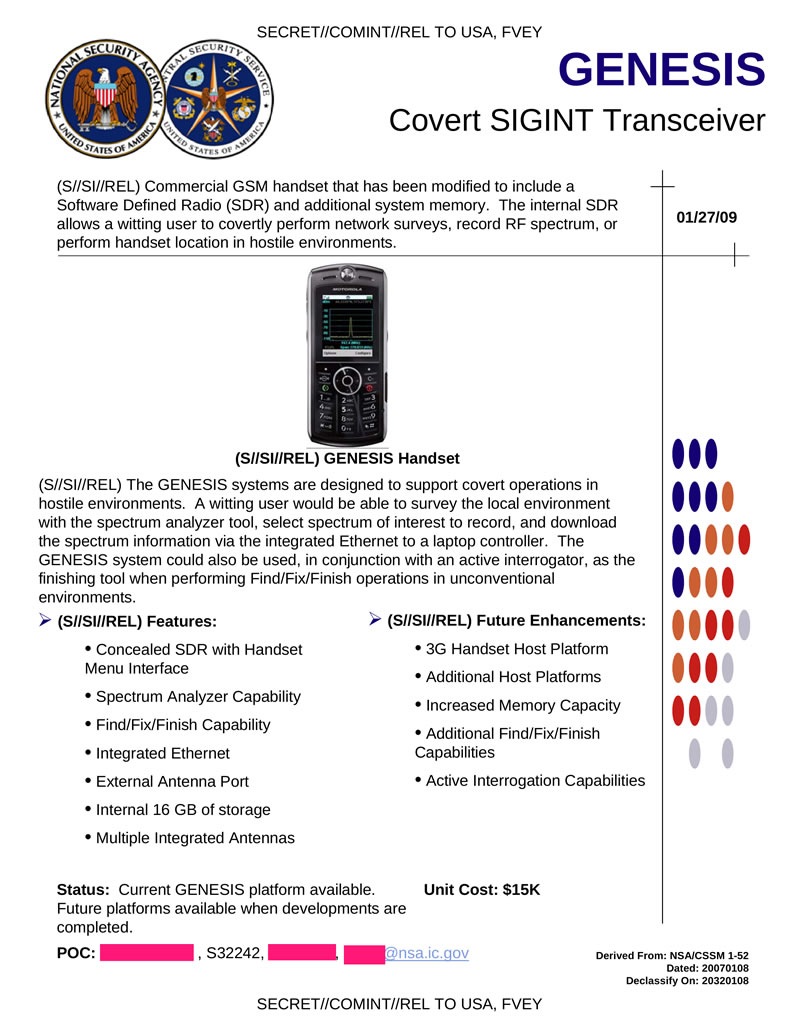
Другой вариант - поддельные базовые станции, с помощью которых можно перехватывать трафик абонента и манипулировать данными на его телефоне:



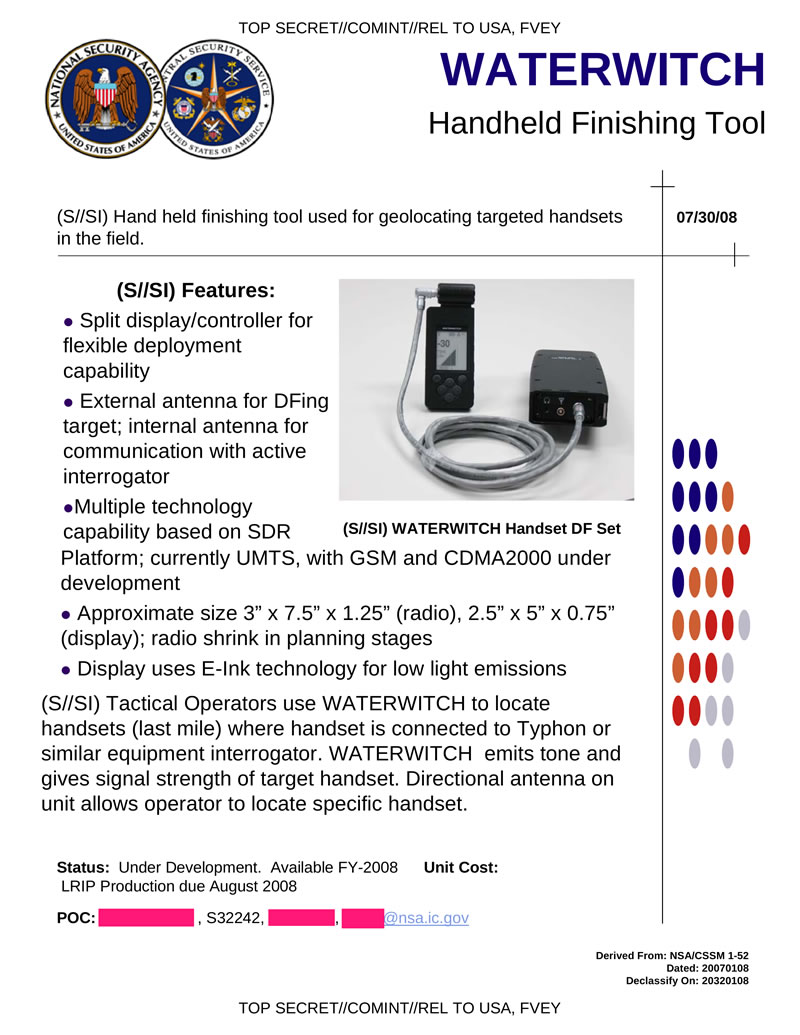
Или целая сотовая сеть в одной коробке:



Есть и спектральный анализатор на базе мобильного телефона Motorola L9, который позволяет записать радио-спектр для дальнейшего анализа:



Определение местоположения с помощью сотовой сети - достаточно приблизительное. Для точного поиска жертвы на месте есть отдельный портативный инструмент:



Конечно, само по себе существование такого каталога устройств не означает, что кто-то уже использует их для тотальной слежки. Однако вслед за публикацией каталога стали появляться и свидетельства практического применения.

В сентябре 2014 года [была обнаружена](http://securityaffairs.co/wordpress/28666/intelligence/nsa-spying-un-vienna.html) подозрительная будка на крыше IZD-Tower, напротив комплекса UNO-city (Венский международный центр). Будка огорожена прочным металлическим забором, под наблюдением 10 камер. Вероятнее всего, это поддельная базовая станция мобильной сети.



Вена является третьим городом-резиденцией ООН (после Нью-Йорка и Женевы), там же расположены штаб-квартиры ОПЕК и ОБСЕ. Вполне понятен интерес АНБ к месту, где собираются высокопоставленные лица большинства стран. А вот предположительная зона покрытия данной станции:

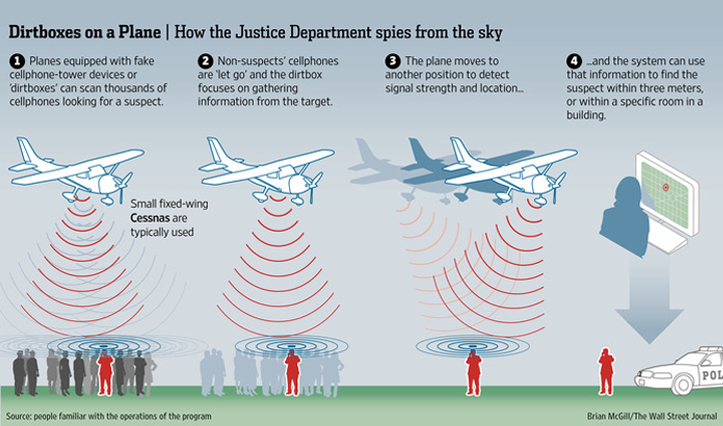


Такие базовые станции могут перехватить IMSI (так называемые IMSI-catcher), а затем через сеть SS7 отслеживать местоположение жертвы. Однажды отследив IMSI жертвы, можно отслеживать ее перемещение по всему миру до тех пор, пока пользователь не сменит SIM-карту. Подробнее о таких атаках мы уже рассказывали [здесь](http://habrahabr.ru/company/pt/blog/226977/).

Документы Сноудена говорят о том, что станция в Вене (Vienna-Annex) является лишь частью глобальной сети слежения [SIGINT](http://securityaffairs.co/wordpress/wp-content/uploads/2014/09/NSA-surveillance-Vienna-annex.png). Дальше уже можно искать по списку стран и городов, упомянутых в этих документах. Вот фото похожей структуры, найденной на крыше в Риме:



Кстати, американские спецслужбы не ограничиваются стационарными системами слежения. Они уже давно используют станции-перехватчики [StingRay](http://resources.infosecinstitute.com/stingray-technology-government-tracks-cellular-devices/) на специальных автомобилях, которые могут подъехать к заданной цели. А в ноябре журнал Wall Street Journal [сообщил](http://securityaffairs.co/wordpress/30175/intelligence/cell-phone-data-spied-airplane.html), что Министерство юстиции США использует самолеты Cessna с поддельными базовыми станциями для перехвата данных пользователей:



**Кто виноват и что делать?**

Прежде всего нужно отметить, что невзирая на громкие заголовки газет, описанные технологии сейчас доступны не только спецслужбам. По сути, прослушка мобильных сетей и защита от неё стали новым высокотехнологичным рынком. И как на всяком рынке, здесь постоянно появляются новые, более дешевые решения.

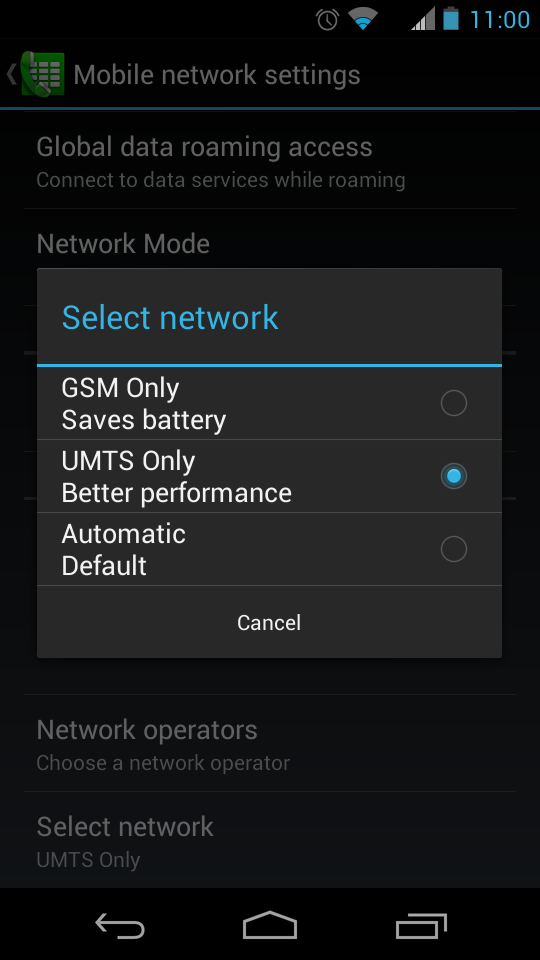
В августе 2014 года журнал Popular Science [рассказал](http://www.popsci.com/article/technology/mysterious-phony-cell-towers-could-be-intercepting-your-calls) о том, как группа специалистов по безопасности ESD America продвигает собственную разработку – «особо защищенный» смартфон CryptoPhone 500 на базе Android. Поскольку подобных продуктов на рынке уже несколько, разработчики использовали небанальный рекламный ход. С помощью своего продвинутого смартфона они обнаружили на территории США 17 поддельных базовых станций, которые в принудительном порядке отключают шифрование данных:



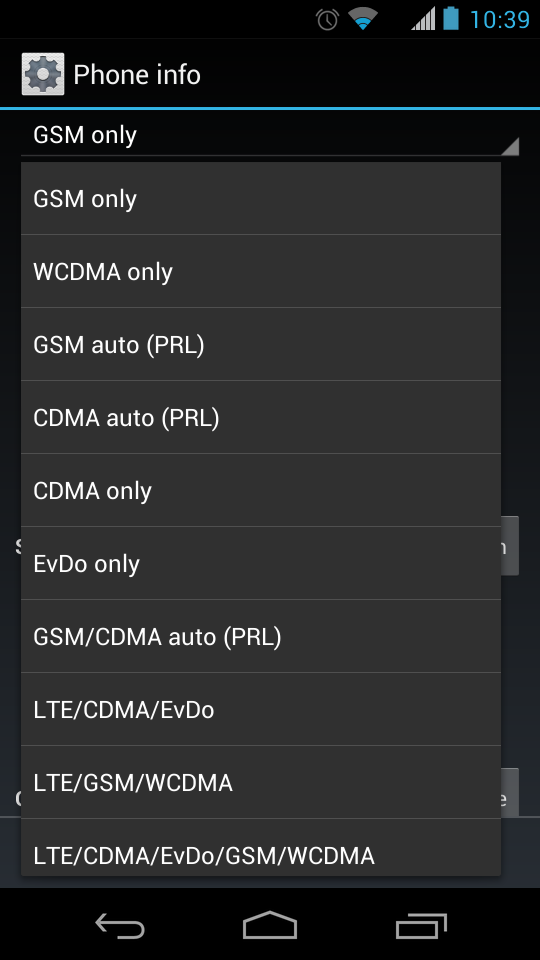
Одну такую станцию прослушки обнаружили около крупного казино в Лас-Вегасе, ещё несколько - вблизи военных баз США. Кто, кроме АНБ, может использовать такую технику? Да кто угодно. Правда, коммерческие комплексы [дороговаты](http://www.meganet.com/meganet-products-cellphoneinterceptors.html) - более $100 тыс. Однако можно значительно удешевить решение, если воспользоваться [бесплатным ПО](http://openbsc.osmocom.org/trac/) для создания своей собственной базовой станции.

Как от этого спастись? Один из вариантов уже упомянут выше – «защищенный» смартфон. Однако удовольствие недешёвое: CryptoPhone стоит $3.500. За эти деньги клиент получает «закрытие» ряда векторов атаки, которые фигурировали выше в нашем списке. В частности, здесь есть контроль известных уязвимостей Android OS, контроль подозрительной деятельности мобильных приложений, и даже мониторинг baseband-процессора: именно эта фича позволяет определить подключение фальшивой базовой станции-перехватчика, чего не замечают обычные смартфоны.

Защититься от поддельных базовых станций с обычным телефоном сложнее, но кое-что сделать всё-таки можно. В сетях UMTS (G3) используется взаимная аутентификация мобильной станции в сотовой сети, и сотовой сети - в мобильной станции. Поэтому одним из признаков прослушки является принудительное переключение из режимов G4 и G3 в менее безопасный режим G2. Если пользователь заранее отключит у себя 2G-режим, это усложнит злоумышленнику задачу перехвата радио-эфира. Некоторые модели мобильных телефонов позволяют переключать используемый тип сети:



Также во многих телефонах на базе Android есть сервисное меню, вызываемое командой \*#\*#4636#\*#\*, где можно выбрать тип сети. Правда, такое решение чревато повышенным потреблением батареи, а также потерей связи в случае отсутствия покрытия сети 3G.



Поддельные базовые станции позволяют перехватывать любые данные, передаваемые через сотовую сеть – однако для этого требуется физическое нахождение абонента в зоне действия базовой станции. Поэтому более продвинутым методом слежки можно считать **атаки на сеть SS7**, позволяющие перехватывать данные абонента, а также его местоположение, из любой точки земного шара. Здесь тоже есть свои коммерческие решения: в одном из прошлых постов мы рассказывали о системе [SkyLock](http://habrahabr.ru/company/pt/blog/237981/) американской компании Verint, которая позволяет отслеживать любых абонентов по всему миру.

Как можно помешать прослушке в этом случае? Поскольку атаки базируются на легитимных сообщениях сигнальной сети SS7, грубая фильтрация этих сообщений может оказать негативное влияние на весь сервис. По опыту экспертов Positive Technologies, адекватная защита от атак на SS7 должна представлять собой комплекс мероприятий на стороне оператора, включая мониторинг трафика SS7 и «умный» контроль фильтрации, который позволяет блокировать только попытки атак и фрода. Подробнее о том, как это реализуется на основе наших продуктов, можно прочитать в статье «[Безопасность сетей мобильной связи на основе SS7](http://www.ptsecurity.ru/download/PT_SS7_security_2014_rus.pdf)».