Прослушка мобильного телефона

Кто шпионит за мобильными телефонами и зачем. Какие методы и оборудование используются для прослушивания телефонов и как защитить мобильный от «жучков».
Прослушивание мобильного телефона — один из методов несанкционированного доступа к личным данным. Включает в себя перехват и расшифровку GSM-пакетов (стандарта цифровой связи, используемого в мобильных), SMS- и MMS-сообщений.

Риск вторжения в частную жизнь владельцев телефонов, смартфонов и планшетов, а точнее в их переговоры и переписку растёт день ото дня. Девайсы, которые сканируют и анализируют поток радиосигналов, специальное ПО для дешифровки GSM и прочие технические и программные хитрости сегодня стали доступными как никогда раннее. При желании их можно купить, а то и вовсе заполучить бесплатно (утилиты). Прослушка мобильного теперь уже прерогатива не только спецслужб.

Кто прослушивает телефоны

Контингент жаждущих узнать содержание частных бесед и SMS-посланий достаточно велик, он включает в себя как шпионов-любителей, так и искушённых профессионалов. Цели и намерения соответственно у этих людей разные.

Прослушкой телефонов занимаются:

- **Правоохранительные органы** — для предупреждения терактов, провокаций, сбора доказательств во время оперативно-следственного процесса, поиска правонарушителей. При наличии письменного разрешения прокурора или суда могут перехватывать и записывать телефонные беседы во всех беспроводных (в том числе GSM) и проводных коммутационных линиях.
- **Конкуренты по бизнесу** — обращаются к профи для ведения промышленного шпионажа: сбор компромата на руководство компании-соперника, выведывание коммерческих планов, секретов производства, информации о партнёрах. Не жалеют денег и сил для достижения своей цели, задействуют новейшую аппаратуру и специалистов высокого класса.
- **Близкое окружение (члены семьи, друзья, знакомые)** — в зависимости от финансовой состоятельности отслеживание телефонного общения осуществляют самостоятельно (после краткого ознакомления с технологией). Либо обращаются за помощью к «умельцам», предоставляющим услугу по приемлемым ценам. Мотивы шпионажа носят преимущественно бытовой характер: ревность, делёж наследства, интриги, чрезмерные проявления заботы, банальное любопытство.
- **Аферисты и шантажисты** — орудуют исключительно своими силами. Выбирают жертв (абонентов мобильной связи) целенаправленно. В ходе перехвата разговоров выведывают всю интересующую информацию (бизнес-деятельность, встречи, ближайшие планы, круг знакомств). А затем используют её в совокупности с методами социальной инженерии для воздействия на владельца телефона, чтобы выманить у него финансовые средства.
- **Хакеры** — выполняют перехват разговоров преимущественно программными средствами — вирусами. Но иногда задействуют и девайсы, сканирующие GSM. Жертв для атаки выбирают случайным образом, по принципу «кто попадётся». Их интересы — добыча информационных «трофеев». Записанные из частного телефонного эфира каламбуры, забавные недоразумения, выяснения отношений выкладываются цифровыми хулиганами в различных интернет-изданиях на потеху посетителям.

- **Шутники** — как правило, знакомые жертвы. Организовывают «единоразовый» шпионаж ради «забавы», розыгрыша или чтобы сделать какой-нибудь сюрприз. Хотя иногда поддаются подлому соблазну, услышав из уст прослушиваемых собеседников какой-нибудь секрет из личной или деловой жизни.

Методы прослушивания мобильных

1. Установка «жучка»

Традиционный метод слежки, но, тем не менее, действенный и доступный в плане финансового вопроса. Крошечный девайс размером с булавочною головку (а то и меньше) устанавливается в телефон жертвы не более чем за 10 минут. При этом его присутствие тщательно маскируется, визуально и аппаратно.

Как выглядит "жучок"

«Жучок» запитывается от батареи, поэтому функционирует даже, если переговоры по телефону не ведутся, то есть постоянно «слушает» окружающее его пространство в радиусе чувствительности микрофона. Звук транслирует по GSM-связи либо по заданному радиоканалу, в зависимости от технической модификации устройства.

2. Перехват GSM-сигнала

С технической точки зрения один из самых сложных методов. Но наряду с этим, и один из самых результативных, мощных. Его принцип действия основан на получении несанкционированного доступа к приватному каналу GSM и последующему дешифрованию его пакетов. Перехватчик сигнала устанавливает сканирующую аппаратуру с интегрированным ПО, предназначенным для «чтения» сигналов, между вышкой-ретранслятором и абонентом. А затем, дождавшись установки связи (если охота идёт за конкретным номером), начинает прослушку.

GSM snifer

Алгоритмы шифрования мобильной связи

Все операторы мобильной связи для кодировки сигналов используют засекреченные алгоритмы шифрования данных. Каждый из них служит для выполнения конкретных задач:

- A3 — предотвращает клонирование телефона (защищает процедуру авторизации);
- A5 — кодирует оцифрованную речь абонентов (обеспечивает конфиденциальность переговоров);
- A8 — сервисный генератор криптоключей, использующий данные, полученные алгоритмами A3 и A5.

Перехватчики фокусируют своё внимание на алгоритме A5 (который маскирует речь), именно его они перехватывают и подвергают дешифрированию. В силу особенностей экспортирования криптосистемы A5, были разработаны две её версии:

- A5/1 — для стран Западной Европы;
- A5/2 (урезанная, слабая версия) для других стран (в том числе и для государств СНГ).

Какое-то время сущность алгоритма A5 являлась тайной за семью печатями, технологическим секретом на уровне государственной тайны. Однако к началу 1994 года ситуация коренным образом изменилась — появились источники, раскрывающие в подробностях его основные принципы шифрования.

На сегодняшний день об A5 интересующейся общественности известно практически всё. Если кратко: A5 создаёт 64-битный ключ путём неравномерного сдвига трёх линейных регистров, длина которых соответственно 23, 22 и 19 бит. Несмотря на высокую стойкость ключа к взлому, хакеры научились его «вскрывать» на оборудовании средней мощности — и в сильной (/1), и в слабой версиях (/2). Они используют специальный софт (ими же и разработанный), который распутывает «клубок» A5, используя разнообразные методы криптоанализа.

Оборудование для перехвата и мониторинга

Первые девайсы для прослушки мобильных появились сразу же после принятия стандарта GSM. Насчитывается порядка 20-ти топовых решений, которые активно используются для прослушки частными и юридическими лицами. Их стоимость колеблется в пределах 2-12000 долл. Среди авторов, создавших (и создающих) оборудование для перехвата GSM, числится и Военная академия связи им. С.М. Будённого — инженеры-конструкторы оснащали прослушивающими устройствами отделы МВД.

Любая модель GSM-перехватчика (снифера), в независимости от технических характеристик (конструкции, быстродействия, стоимости), выполняет следующие функции:

- сканирование каналов, детектирование активных;
- контроль управляющего и голосового канала ретранслятора/мобильного телефона;
- запись сигнала на внешний носитель (винчестер, USB-флешку);
- определение телефонных номеров абонентов (вызываемого и вызывающего).

Для мониторинга мобильных каналов активно применяются следующие девайсы:

- GSM Interceptor Pro — охватывает зону покрытия 0,8-25 км, поддерживает работу с A1/1 и /2;
- PostWin — комплекс на базе ПК класса P-III. Кроме GSM-900, перехватывает стандарты AMPS/DAMPS и NMT-450;
- SCL-5020 — аппарат индийского производства. Определяет расстояние до ретранслятора, может одновременно прослушивать до 16 GSM-каналов.

3. Подмена «прошивки» телефона

После технической модификации телефон жертвы все переговоры копирует и отправляет взломщику по GSM, Wi-Fi, 3G и другим актуальным стандартам связи (на выбор).

4. Внедрение вирусов

Особый вирус-шпион после инфицирования ОС смартфона, начинает скрытно выполнять «функции самописца» — то есть фиксирует все переговоры и перенаправляет злоумышленникам. Как правило, он распространяется в виде заражённых MMS , SMS и сообщений по электронной почте.

Меры защиты мобильного телефона от прослушивания

1. Установка в ОС телефона защитного приложения, которое предотвращает подключение к ложным ретрансляторам, сверяет идентификаторы и сигнатуры баз мобильного оператора, детектирует подозрительные каналы и вирусы-шпионы, блокирует доступ другим программам к микрофону и видеокамере. Топовые решения: Android IMSI-Catcher Detector, EAGLE Security, Darshak, CatcherCatcher

Android IMSI Catcher Detector

2. Проведение технической диагностики батареи: при прослушке она быстро разряжается, греется, когда телефон не используется.
3. Немедленное реагирование на подозрительную активность телефона (произвольно загорается подсветка, инсталлируются неизвестные приложения, во время переговоров появляются помехи, эхо и пульсирующий шум). Необходимо обратиться в ремонтную мастерскую для того, чтобы специалисты осмотрели телефон на наличие «жучков» и вирусов.
4. Отключение телефона с извлечением батареи на ночь, в идеале — вставлять батарею в телефон только для совершения исходящего звонка.

Как бы там ни было, если кто-то захочет прослушать ваш телефон, рано или поздно он это сможет сделать, самостоятельно или с чужой помощью. Никогда не теряйте бдительности и при малейшем проявлении симптомов перехвата сигнала, принимайте соответствующие меры.

https://sfztn.com/security/proslushka-mobilnogo-telefona