ЛЕКЦИЯ 4. УЯЗВИМОСТИ МОБИЛЬНОЙ СВЯЗИ. СКАНЕРЫ ЧАСТОТ

4.1. УЯЗВИМОСТИ МОБИЛЬНОЙ СВЯЗИ

Один из самых старых и простых способов взлома мобильных сетей – это перехват ключей из эфира, их раскодирование и впоследствии создания временных «клонов» SIM-карт. Современные мощные компьютеры могут сделать это за считанные минуты, в отличие от своих предшественников в 1991 году, — именно тогда создавался стандарт GSM, и именно на те вычислительные мощности была рассчитана стойкость ключей.

Используя подобный взлом, злоумышленники могут получать несанкционированный доступ к мобильным телефонам случайных людей и использовать это для перевода средств на свои счета. Операторы предпочитают не афишировать эту проблему.

Между тем был обнаружен способ атаки на сотовые сети, не требующий ни специальных дорогостоящих радиосканеров, ни мощных компьютеров и доступный любому желающему. При этом операторы, увы, не могут защититься от подобного взлома практически никак.

Метод называется «атака через SS7». SS7, или, по-русски, ОКС-7, — это система сигнализации, используемая в сотовых сетях и разработанная еще в 1970-е годы для первых электронных АТС.

На самом деле никакой защиты в ОКС-7 нет: сигнальный трафик никак не шифруется, а отличить легитимные команды от поддельных невозможно — оборудование исправно выполняет все команды, которые получает, неважно, из какого источника.

Причина такого безобразия очень проста: при использовании SS7 сигнальный канал физически отделен от голосового, и поэтому, как справедливо полагали разработчики протокола 40 лет назад, никто чужой к нему доступа получить не может, кроме персонала телефонной станции. Да и смысла в этом никакого не было: тогда, кроме команды на установление соединения с таким-то абонентом, ничего интересного и не передавалось. Так что нелегитимных пакетов можно было не опасаться.

Однако в 2000 году была придумана система передачи команд SS7 по IP-каналам, и теперь получилось так, что доступ к сигнальному каналу стал возможен извне. Для этого нужен шлюз, он же SS7-хаб.

Плохая новость состоит в том, что законодательство в ряде стран позволяет довольно легко получить лицензию оператора связи и вполне легитимно установить этот самый хаб с подключением к какому-нибудь узлу обмена трафиком. Поэтому на черном рынке широко распространены предложения по подключению к таким хабам для всех желающих.

Где расположен хаб — совершенно не имеет значения, через него можно отправлять и принимать команды в сеть любого оператора в мире. А блокировка команд с определенных узлов с большой долей вероятности нарушит работу роуминга и международной связи, поэтому от подобных атак и сложно защититься.

Что же можно сделать, узнав номер телефона жертвы? Для начала нужно получить IMSI (International Mobile Subscriber Identity) — это условный внутренний идентификатор SIM-карты в сети, с помощью которого впоследствии и происходит взлом. Для этого используется SMS. Стоит напомнить, что сервис SMS изначально появился как недокументированная «фича» протокола. Так что сообщения передаются как раз по сигнальному каналу.

Если сформировать запрос на отправку SMS абоненту по его номеру, то сеть оператора, в которой он обслуживается (а именно HLR — основная база данных, где хранятся параметры учетной записи), пришлет в ответ идентификатор SIM-карты (IMSI) и адрес текущего коммутатора (MSC) и временной базы данных (VLR), в которой хранятся параметры на время пребывания абонента в конкретном месте.

Мол, вот тебе IMSI и адрес сегмента сети, где сейчас наш абонент: отправляй сообщение для этого IMSI на тот MSC/VLR. Адрес основной базы данных HLR при этом тоже становится доступным. Зная все эти адреса и идентификаторы, можно отправлять разные интересные команды.

Например, можно запросить идентификатор базовой станции, которая в данный момент обслуживает абонента. Используя этот идентификатор (а он уникален) и открытую для всех желающих базу данных в Интернете, можно получить местоположение абонента с точностью до нескольких сотен метров. При этом есть специальные программы, которые делают всю процедуру автоматически: вы вводите номер, а через пару секунд получаете точку на карте.

Можно послать в HLR команду на смену VLR и «подставить» несуществующий, заблокировав таким образом прохождение входящих звонков и сообщений.

Есть и еще более интересный вариант: можно указать адрес «своего» MSC/VLR, который вы эмулируете на компьютере, благо пакет SS7 для Linux доступен для свободного скачивания. В этом случае можно перехватывать сообщения и звонки, причем делать это незаметно.

Для этого достаточно получить SMS на подставной компьютер и не передать в ответ подтверждение доставки, а переключить VLR обратно на легитимный. Тогда сервер отправителя через пару минут снова его отправит, и оно дойдет-таки до адресата.

Перехват SMS-сообщений удобно использовать, например, для получения доступа к сервисам с двухфакторной авторизацией. Со звонками еще проще: в HLR можно установить безусловную переадресацию на наш промежуточный номер, а с него потом инициировать конференц-связь с жертвой.

Можно прослушать и исходящие звонки подобным способом, только чуть сложнее: переадресацию нужно будет установить на номере того, кому звонит жертва. Узнать его можно в момент, когда при исходящем вызове запрос, содержащий номер, передается на биллинг-платформу для тарификации вызова.

Подменив адрес биллинг-платформы на свой, а потом вернув его обратно, мы получим нужный номер. Жертва, соответственно, сможет совершить звонок только со второго раза, но вряд ли что-то заподозрит (кстати, регулярное прохождение исходящих звонков только со второго раза — верный признак того, что вас прослушивают).

Как видите, выложенные в Интернете телефонные разговоры политиков в наше непростое время уже не требуют ни подсовывания им специальных телефонов с «жучками», ни участия спецслужб: за относительно небольшие деньги такое может провернуть любой оппонент по предвыборной гонке.

У обычного пользователя можно утащить пару сотен тенге со счета, отправляя от его имени USSD-команды услуги «Мобильный перевод» либо переадресовывая его звонки на платные номера и продавая такой трафик.

Как уже было сказано выше, полностью защититься от таких атак невозможно — проблема заложена на уровне протокола, и от нее можно избавиться только после глубокой модернизации всей системы связи.

Альтернативный вариант — сложный анализ активности всех абонентов с целью выявления потенциально вредоносных действий. Некоторые ИТ-компании предлагают автоматизированные решения, по принципу работы напоминающие антифродовые системы банков.

Однако операторы не торопятся оповещать публику о внедрении подобных решений. Поэтому рядовой абонент не имеет возможности узнать, защищен он от описанных неприятностей или нет.

Так что остается напомнить, что все более-менее конфиденциальные переговоры стоит проводить не по телефону, а при личной встрече. А для двухфакторной аутентификации лучше приобрести отдельную SIM-карту, номер которой не будет знать никто, кроме вас.

4.1.1. Шпионские устройства для мобильной связи

CYCLONE Hx9 — эмулятор базовой станций GSM, предназначенный для проведения атак на мобильные телефоны стандарт GSM 900. Позволяет осуществлять прослушивание и перехват передаваемых данных. Дальность до 32 километров.

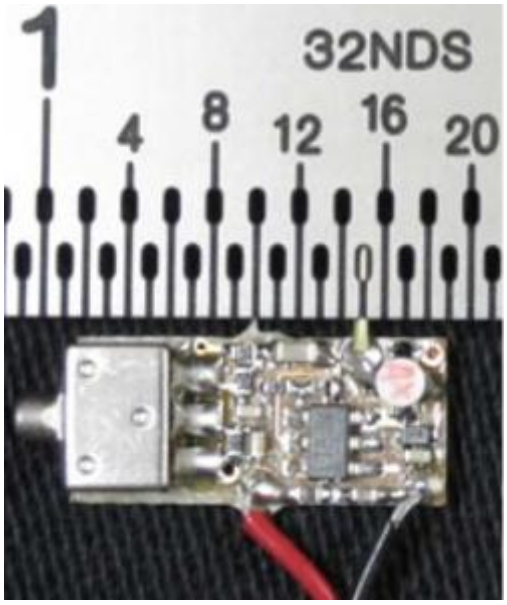
GENESIS — устройство для радиоэлектронной разведки на основе модифицированного сотового телефона стандарта GSM. Предназначено для поиска и анализа сотовых сетей, а также определения расположения телефонов целей. Имеет возможность записи радиочастотного спектра во внутреннюю память, объем которой составляет 16GB.

TYPHON HX — портативная базовая станция для сетей GSM (850/900/1800/1900). Имеет полную поддержку протокола GSM и управления вызовами. Тактический элемент радиоэлектронной разведки.

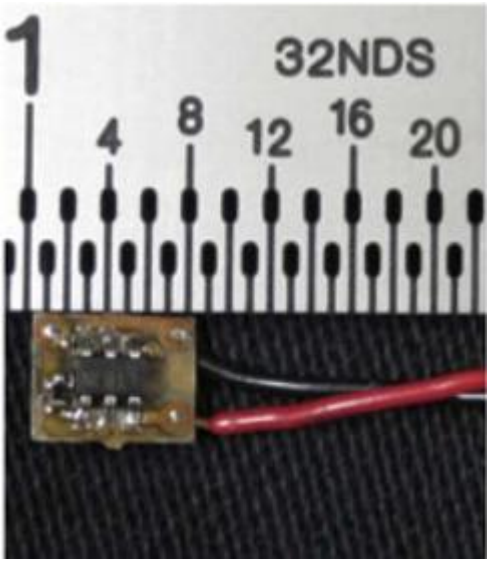
WATERWITCH — портативный прибор для определения координат целевых телефонов в радиусе действия.

GOPHERSET — программная закладка для SIM-карт GSM. Позволяет отправить телефонную книгу, SMS и информацию о вызовах телефона цели на предопределенный номер SMS. Загрузка на карту возможна либо через USB, либо по воздуху. В обоих случаях для установки могут потребоваться ключи для доступа к SIM-карте используемые оператором сотовой связи.

LOUDAUTO — аппаратная закладка. Срабатывает «жучок» при облучении специальным сигналом, передавая в отраженном радиосигнале звук из помещения, в котором он установлен.



TAWDRYYARD — миниатюрный радиомаяк, срабатывает при получении радиосигнала от специализированного излучателя. Используется для поиска мест установки других закладок, таких как, например, RAGEMASTER.



CTX4000 представляет собой портативный излучатель непрерывного действия, предназначен для подсвета целевых систем для получения данных от установленных там закладок.

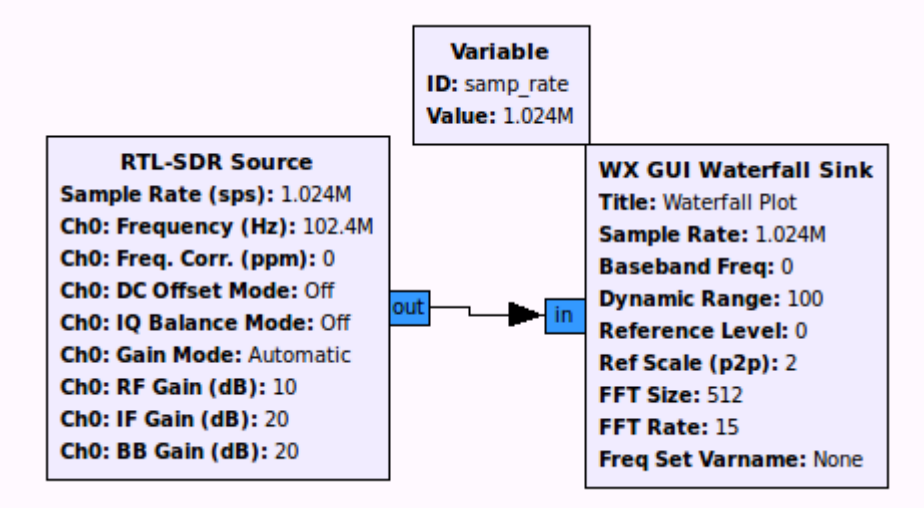
4.2. СКАНЕРЫ ЧАСТОТ ДЛЯ АНАЛИЗА РАДИО И ЦИФРОВОЙ СВЯЗИ

Люди используют радиоволны для самых разных целей. Радиолюбители общаются друг с другом, диспетчерская служба отдает указания пилотам самолетов, таксисты берут заказы, о которых узнают по радио, брелок автосигнализации переговаривается с автомобилем, чтобы подтвердить свою подлинность и открыть двери. Поэтому прослушивание эфира всегда было интересно многим.

Раньше построение приемника, способного принимать в широком диапазоне частот и декодировать разные виды модуляций сигнала, было сложной задачей, поэтому готовые приемники стоили дорого, а самостоятельно собрать такой мог далеко не каждый. С появлением производительных процессоров появилась возможность заменить значительную часть электронных узлов программной обработкой — точная настройка частоты приема, демодуляция, фильтрация шумов и помех — все это отлично реализуется программно, да еще и получает возможности по тонкой настройке без необходимости переделки.

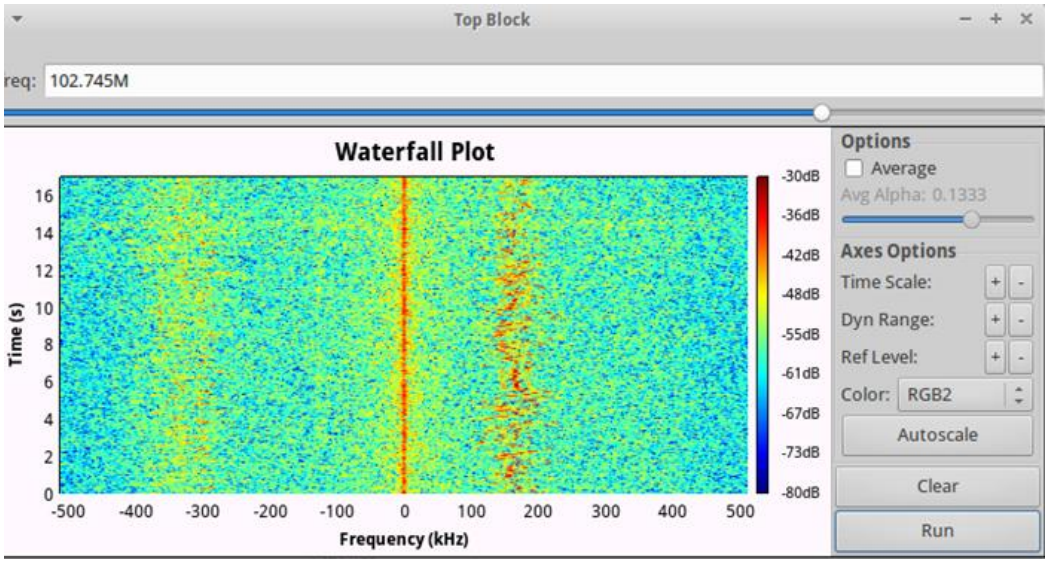
Аппаратной части остаются лишь задачи предварительного выделения желаемого участка радиодиапазона и его оцифровка. Такая концепция получила название SDR — Software-defined Radio.

GNU Radio — программный инструментарий, обеспечивающий основные функции цифровой обработки сигналов в SDR. Программы, создаваемые средствами GNU Radio, представлены как графы потока управления и могут использоваться с внешними устройствами или для создания программных симуляторов. Для программирования можно использовать визуальную среду GNU Radio Companion или библиотеки на C++ и Python.



GnuRadio:

- Позволяет создавать программные радиоприемники и радиопередатчики;
- Позволяет создавать схемы обработки сигналов в графическом режиме;
- Со схемой обработки сигналов можно связать графический интерфейс, и управлять параметрами интерактивно;
- В наличии богатая база готовых блоков для цифровой обработки сигналов;
- Можно писать свой софт для ЦОС, используя библиотеки GnuRadio;
- В качестве источников сигнала можно разнообразное оборудование;
- Благодаря открытым исходникам имеется возможность безгранично расширять функционал;
- Процесс ЦОС при помощи GnuRadio очень нагляден, что позволяет использовать его в учебном процессе.



4.2.1. RTL2832U based TV-stick

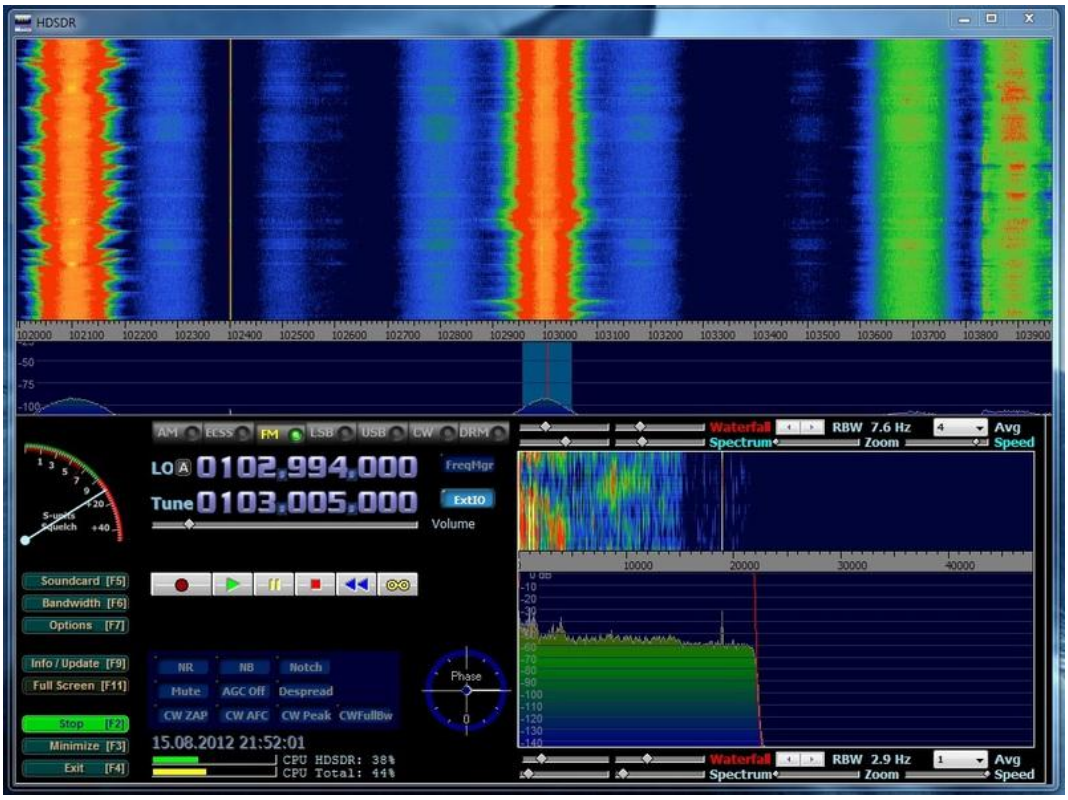
Теперь познакомиться с технологией SDR может любой желающий. Этим мы обязаны компании Realtek, выпустившей чип RTL2832. Его исходное предназначение — USB декодер DVB-T для приема цифровых телеканалов. Аналоговую часть (настройку на частоту телеканала) реализует твердотельный тюнер Elonics E4000, для управления которым у RTL2832 предусмотрены выходы. Таким образом, на основе этих двух микросхем и небольшого числа других деталей производители могут собирать USB DVB-T тюнеры.

Рассмотрим DVB-тюнер на чипе RTL2832, работающий в специальном режиме, который можно приобрести за $20 или даже дешевле. Он может принимать что угодно в диапазоне 60-1700 МГц (радиостанции, звуковое сопровождение ТВ, радиолюбителей, карманные радиостанции, радионяни, радиометки и многое другое).

У этого чипа был обнаружен режим, который отключает все встроенные функции декодирования и переводит его в режим быстрого АЦП, оцифровывающего все, что выдает E4000 с частотой до 3 млн. восьмибитных выборок в секунду. В свою очередь, E4000 может быть настроен на частоту от 60 до 1700 МГц, выдавая на вход RTL2832 выбранный «кусок» радиодиапазона шириной в 3 МГц для оцифровки. Добавив к этому программу обработки на ПК, мы получаем вполне рабочий SDR-приемник.

Как это все работает?

- антенна, подключенная к тюнеру, принимает сигналы с эфира;
- чип E4000 выделяет участок радиодиапазона, начинающийся там, где мы ему указали и шириной 3 МГц, усиливает его;
- чип RTL2832 оцифровывает этот участок и передает по USB на компьютер;
- программа (GnuRadio, HDSDR или другая) «настраивается» на выбранную частоту в пределах выбранных ранее 3 МГц, выполняет демодуляцию указанным способом и отправляет получившийся звук на звуковую карту. Также она может отправлять команды чипу E4000 на перестройку на другой участок диапазона.



Особенности модели:

- Малые размеры;
- Достаточно широкий диапазон (60 — 1700 МГц);
- Обзорная полоса 3,2 МГц;
- Дешевизна;
- Высокая шумность;
- Слабая чувствительность;
- Работа только на прием.

Существует большое количество гораздо более чувствительных и функциональных SDR-приставок. Некоторые из них обеспечивают полосу оцифровки и обзора до 100 МГц, некоторые — умеют работать на передачу, почти все более дорогие приставки

оцифровывают сигнал с дискретностью в 16 или 24 бита вместо 8. Обратите внимание на проект USRP.

Более сложные программные средства позволяют декодировать цифровые радиостанции, принимать сигналы от разнообразных беспроводных датчиков и даже декодировать сигналы аналогового и цифрового телевидения. Обратите внимание на проекты PowerSDR и GnuRadio.

4.2.2. HackRF One

- Малые размеры;
- Широкий диапазон (10 — 6000 МГц);
- Полоса пропускания в 10 МГц;
- Относительная дешевизна;
- Слабая чувствительность;
- Прием и передача только в режиме полудуплекса.

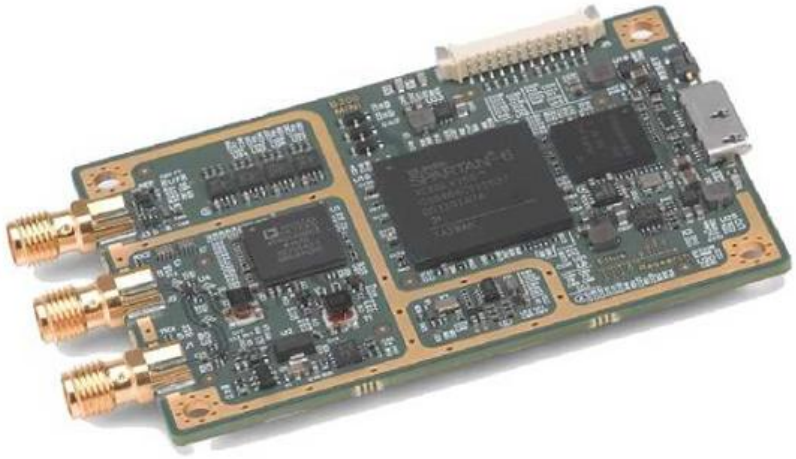
При помощи идущей в комплекте с HackRF утилиты, можно записать, а затем транслировать заново копию всего того, что передавалось в эфире.

Кроме этого, HackRF позволяет подменять GPS сигнал, подслушивать домашние радиотелефоны DECT, делать пеленгацию и др.

4.2.3. bladeRF

- Малые размеры;
- Полоса пропускания в 28 МГц;
- Полный дуплекс;
- Высокая чувствительность;
- UHV-SHF диапазон 300Mhz —3.8 GHz;
- Относительно высокая цена.

4.2.4. Ettus Research USRP



- Разнообразные варианты сменных плат расширения;
- Полоса пропускания в 56 МГц;
- Полный дуплекс;
- Отличная поддержка;
- Высокая цена.