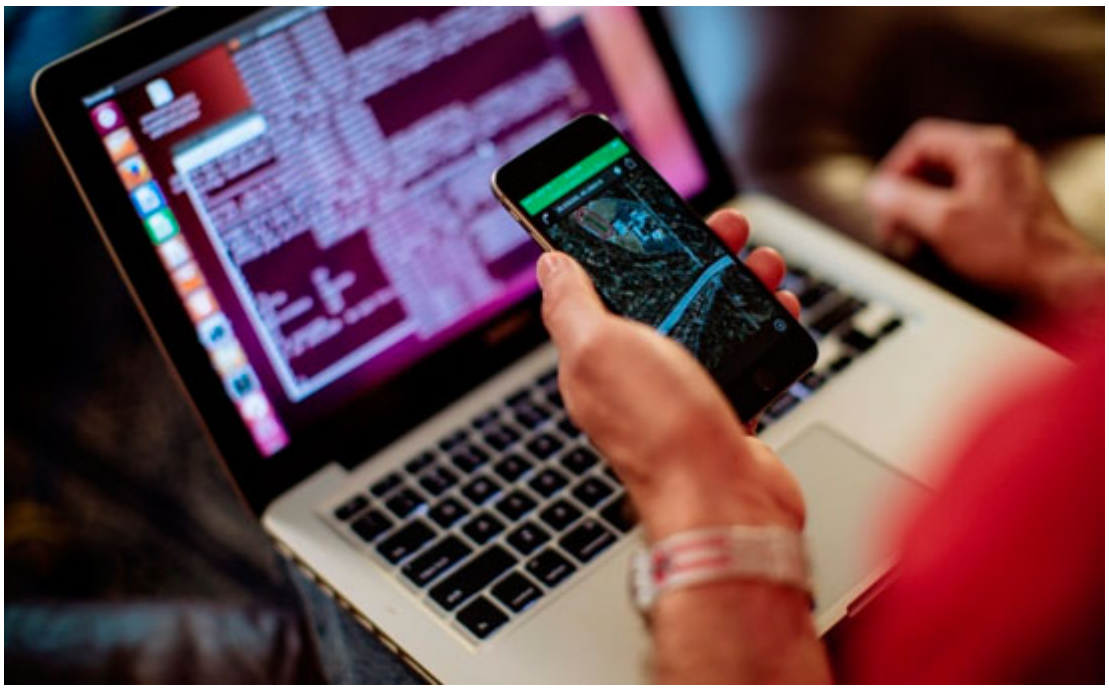
Взлом сотовых сетей - как и зачем

23.11.2015 | Александр Б.

Как оказалось, взломать сотовую сеть, прослушать разговоры абонентов, почитать их SMS, узнать местоположение или украсть с баланса деньги достаточно просто путем даже обычных USSD-запросов.



Сначала теория

Любые сети подключены к СОРМ (системе технических средств для обеспечения функций

оперативно-розыскных мероприятий). В результате, все наши звонки и сообщения могут быть прослушаны или просмотрены органами правопорядка. Также данные спецслужбы могут узнать и наше местоположения в случае осуществления розыска преступников.

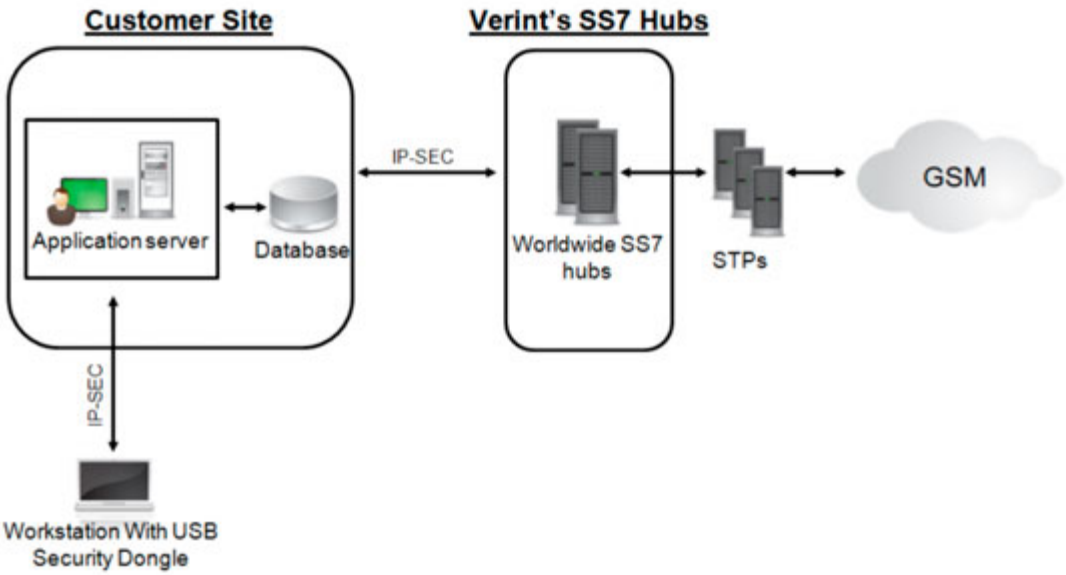
Однако это спецслужбы. Что касается лиц противоположной деятельности - хакеров и/или злоумышленников, то им наша персональная мобильная информация тоже оказалась достаточно легко доступной.

Основная уязвимость заключается в протоколах сигнализации ОКС-7 (или SS7), которые были созданы еще в 1970 гг. и утверждены в 81-м. Благодаря ним для передачи служебных команд (самой сигнализации) стал применяться выделенный канал, закрытый от абонента и изначально придуманный для междугородних звонков. С его помощью выставлялись счета за межгород. Но злоумышленники нашли в данном канале лазейку - и стали общаться с другими городами за чужой счет путем «спуфинга запросов номера».

Это стало возможным благодаря изобретенной в начале XXI столетия спецификации, позволяющей передавать по IP-сетям команды ОКС-7. Поэтому незащищенные протоколы попали в открытые IP-сети, и хакерам осталось лишь войти в интернет и вооружиться несложной программой под Linux с установленным SDK.

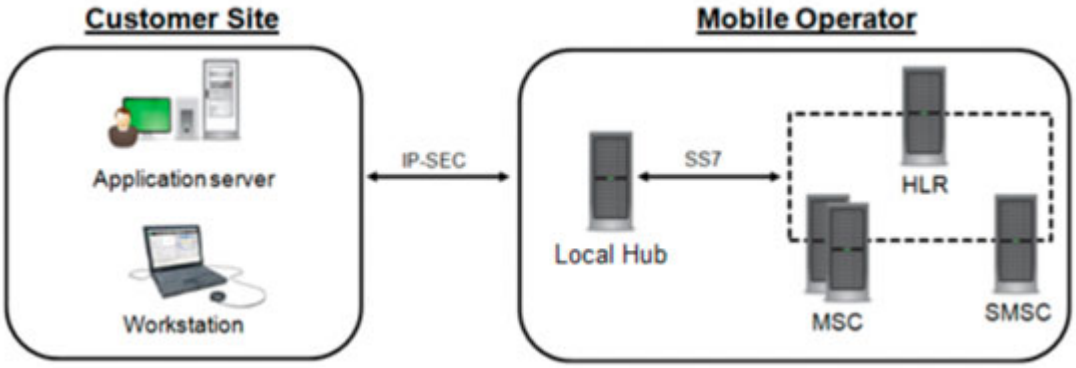
В итоге, система не выполняет проверку источника пакетов SS7 и производит обработку команд хакеров таким же образом, как и легитимных. Тем самым злоумышленники влазят куда им нужно и осуществляют атаку по принципу man-in-the-middle. Отфильтровать данные пакеты никак нельзя.

Подключение ч/з ОКС-7 с целью атаки:



Правда, для осуществления подобной атаки вам понадобится еще и подключение в роли мобильного оператора. Купить подобный доступ к шлюзу можно на черном рынке, получив «открытую дверь» к номерам абонентов операторов разных стран. Другой способ несанкционированного доступа - взлом фемтосоты. Можно поступить и еще проще: открыто заказать услугу подключения напрямую к оператору через IP-SEC у компании Verint в рамках сервиса SkyLock.

Прямое подключение к оператору через IP-SEC путем сервиса SkyLock:

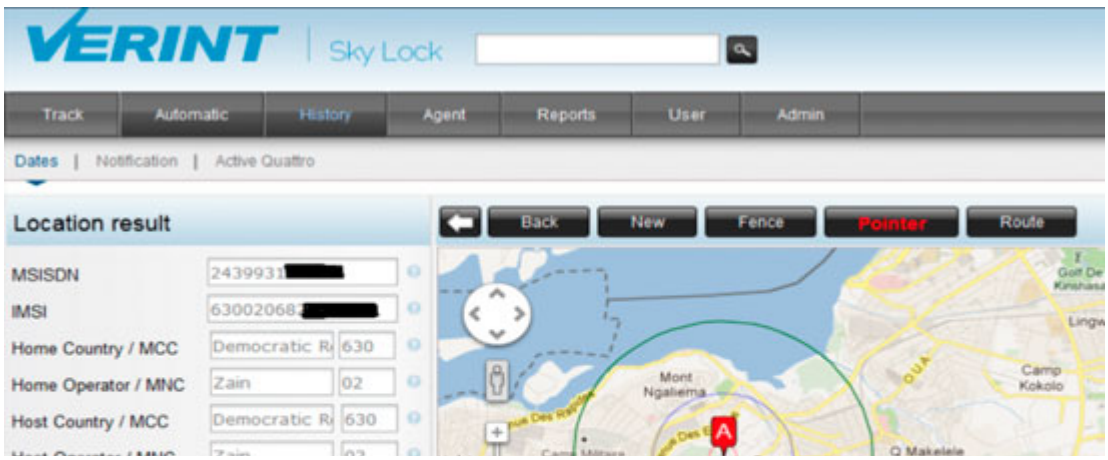


Немного об устройстве сетей сотовой связи

Скажем, у вас номер +79161112233. Им является Mobile Subscriber Integrated Services Digital Number (сокращенно - MSISDN), который не хранится на сим-карте. С нее передается в сеть IMSI (International Mobile Subscriber Identity), что происходит в момент регистрации в ней абонента. Им является число типа 250113336665559 в размере 15 цифр, где 250 - код страны, 11 - код оператора, далее идут 10 знаков - внутренний номер конкретной сим-карты, являющийся уникальным значением (MSIN - Mobile Subscriber Identification Number). Он и используется с целью опознания абонента мобильной сети для получения возможности пользоваться услугами сотовой связи.

Данные об IMSI и MSISDN абонентов находятся в базе данных под названием HLR (Home Location Register), которых может быть несколько. Поэтому вам иногда не могут заменить в салоне SIM-карту, т.к. у сотрудника может банально не быть карточки под ваш номер, т.к. IMSI имеющихся уже прикреплен к другому HLR. В то же время для всех коммутаторов сети применяется схожая база данных VLR (Visitor Location Register). Разница здесь состоит в том, что информация в ней хранится лишь определенный срок, поступая из HLR в случае регистрации SIM-карты в конкретном сегменте сети. Помимо этого, в VLR имеются данные и о настоящем месте положения клиентов для управления их звонками и прочими услугами через определенную базовую станцию. Такую информацию использует для своих функций коммутатор - MSC (Mobile Switching Center).

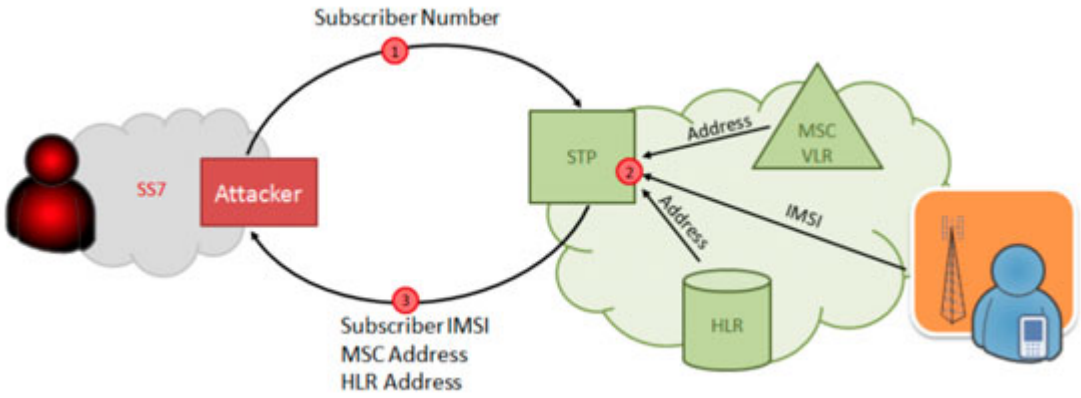
Местоположение абонентов на карте в сервисе SkyLock:



Как осуществляется взлом?

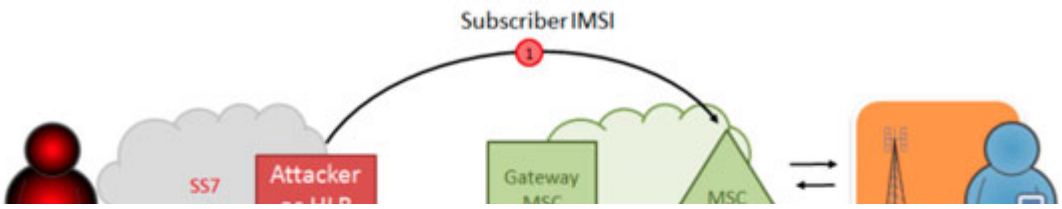
Хакер знает, прежде всего, лишь телефонный номер жертвы (MSISDN). Для своей цели ему необходимо выяснить еще и IMSI. Для его получения нужно сформировать запрос на SMS из своей внешней сети, которая эмулируется на ПК. При этом «домашняя» сеть дает в ответ адрес MSC/VLR, коим сейчас обслуживается пользователь номера. Такие данные нужны для информации - в «домашней» сети находится абонент или в роуминге. Если же он в роуминге, то где именно - чтобы отправить смс непосредственно из «гостевой» сети *(с обычными звонками такой способ не пройдет, т.к. они всегда идут ч/з MSC «домашней» сети, который и принимает решение о дальнейшем маршруте вызова)*. В этот момент осуществляется и передача IMSI, т.к. последний обязателен для маршрутизации. В итоге, мы получаем IMSI для доступа к функциям учетной записи абонента, HLR-адрес, где данные функции имеются, плюс узнаем, в какой стране он сейчас находится.

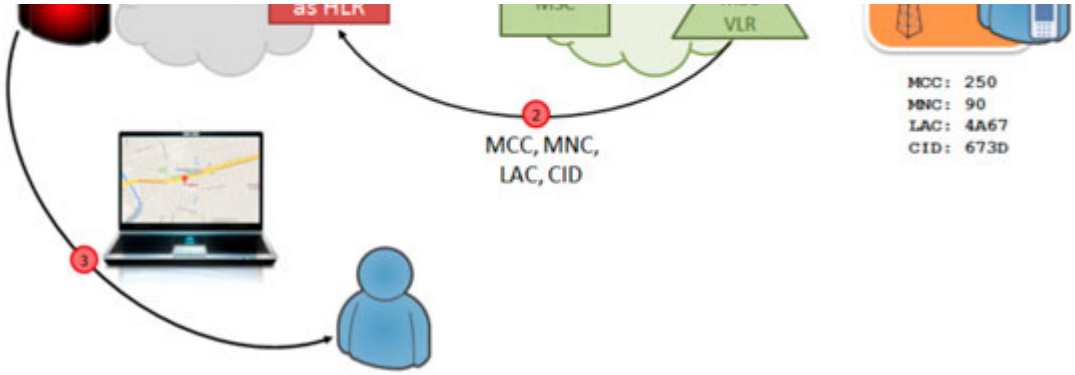
Получение IMSI:



Следующий шаг - уточнение местоположения пользователя. Злоумышленник, владея информацией об MSC/VLR, делает туда запрос с целью уточнения - в зоне действия какой БС сейчас находится абонент с определенным IMSI. На него он получает ответ в виде уникального идентификатора базовой станции. Информацию о ее местонахождении можно потом уточнить без труда. После этого, аналогично GPS, уже понятно, где находится абонент с точностью до нескольких сот метров в диаметре.

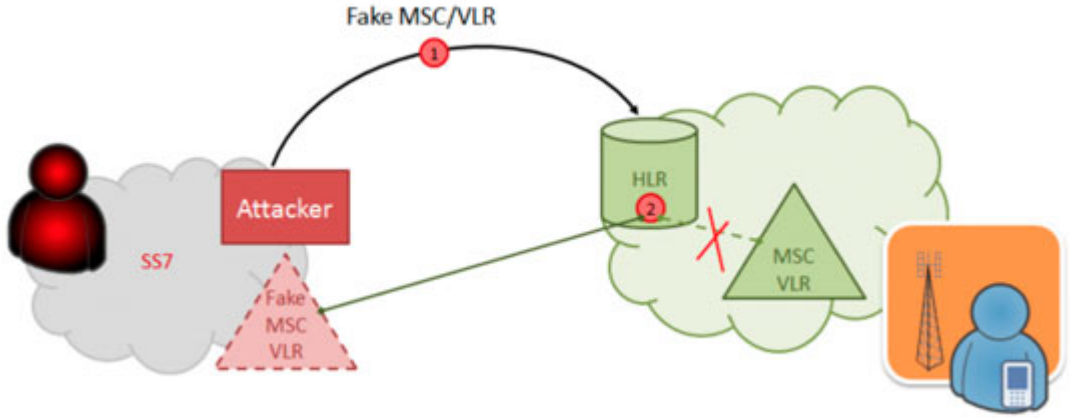
Определение местоположения абонента:



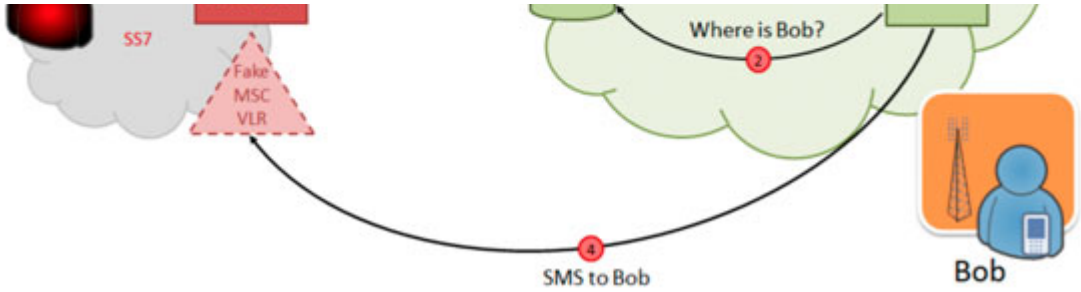


Теперь можно сообщить в HLR, что абонент находится в роуминге - передать IMSI с адресом нового MSC/VLR. Результат: жертве больше никто не дозвонится и не сможет отправить текстовое сообщение, т.к. «домашняя» сеть станет пересылать запросы «в пустоту». Пользователь же при этом будет также зарегистрирован в сети и останется в неведении о происходящем.

Блокировка доступности абонента:

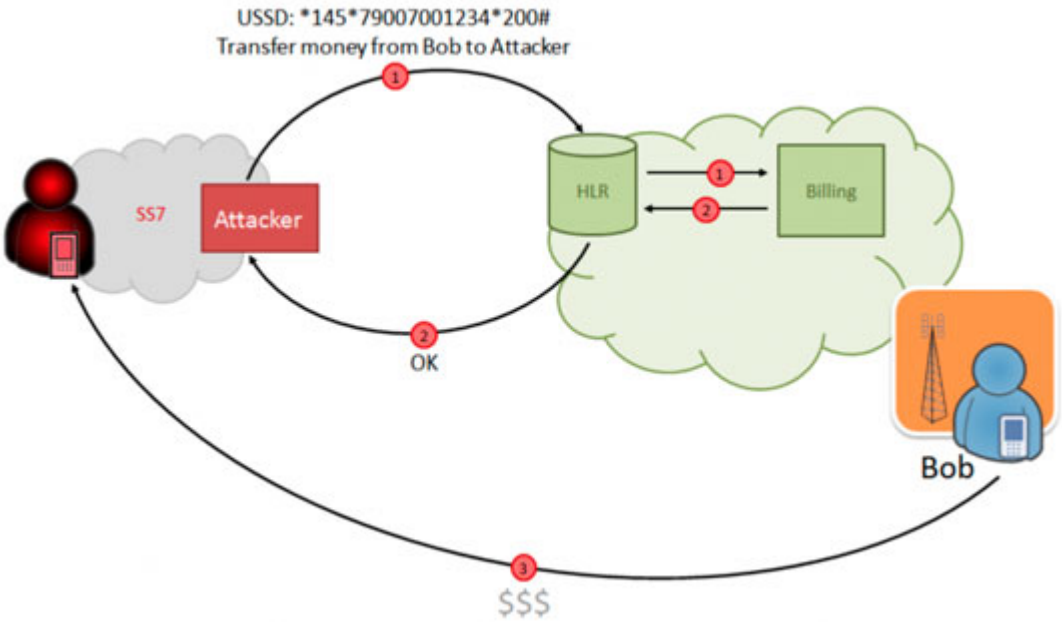


Но какой смысл перенаправлять «в пустоту» столь ценные голосовые вызовы и SMS-сообщения? Можно ведь прописать собственный MSC/VLR и получить себе данный трафик. Подобным способом можно перехватить, скажем, одноразовые пароли по SMS, чтобы иметь возможность кражи денег со счетов и прочей информации. Также подобным образом можно читать чужую смс-переписку. При этом ее авторы об этом даже не догадаются. Ведь от MSC/VLR требуется еще SMS-подтверждение о доставке. Если последнее не отсылать, перерегистрируя абонента на «правильный» MSC, то спустя время осуществится следующая попытка оператора доставить нужное SMS, и оно придет прямо по адресу. Тем самым одно сообщение будет отослано дважды - как хакеру, так и адресату.



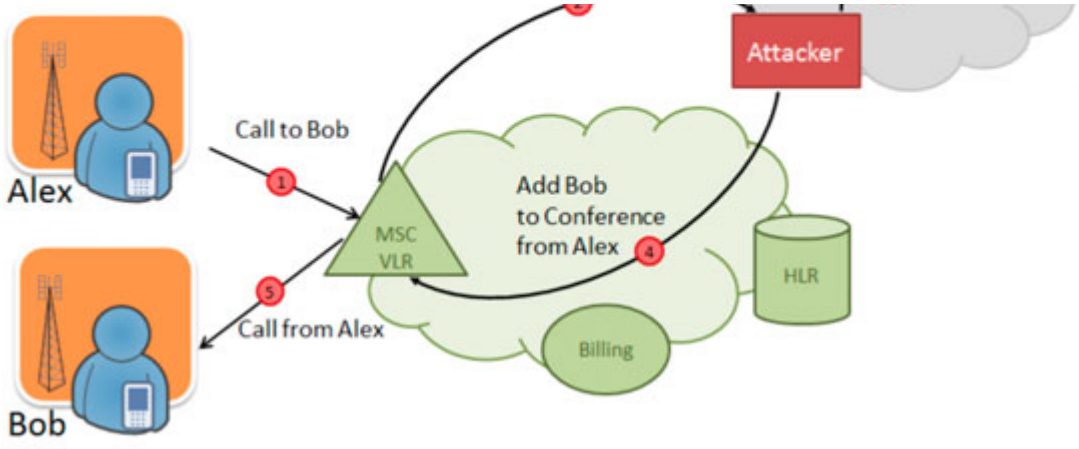
USSD-запросы в роуминге работают без проблем, отдавая информацию о балансе, активируя различные услуги и сервисы. Создав эмуляцию запроса по USSD от VLR к HLR, можно, скажем, осуществить перевод денежных средств между счетами. Часто для этого необходимо SMS-подтверждение, однако как его сделать - уже говорилось выше.

Отправка запросов по USSD от имени жертвы:



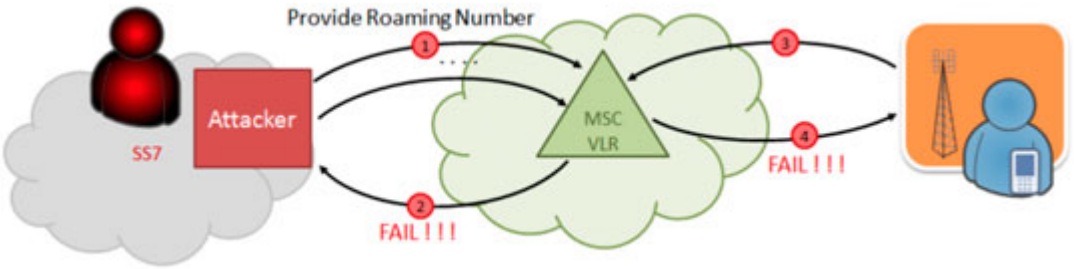
Сменив настройки личной учетки абонента в VLR, в том числе адрес биллинговой системы, хакер сумеет перехватить запрос тарификации исходящего звонка. Он увидит телефонный номер абонента, которому хочет позвонить его жертва. После этого данного вызываемого абонента также можно превратить в жертву. Здесь используется метод, аналогичный SMS-перехвату: переадресация звонка на номер преступника, который установит конференц-связь с реальным абонентом и сможет подслушать беседу. Для входящих звонков эмуляция биллинга уже не требуется. Такие манипуляции выполняются за считанные мгновения, потому никто из абонентов не заметит, что на линии есть еще «третья сторона». Таким образом можно перенаправлять трафик на сторонний платный сервис и хорошо на нем заработать за счет оплаты соединения звонящими жертвами.

Прослушка разговоров:



Но и это еще не все! Благодаря ОКС-7 реально осуществить даже DoS-атаку прямо на коммутатор, в результате чего все абоненты, которых он в данный момент обрабатывает, не смогут принимать входящие звонки. При регистрации в VLR на время дается роуминговых номер. Он требуется, чтобы MSC понимал, куда следует направить звонок. Сам роуминговый номер к непосредственно роумингу имеет минимальное отношение. Дается он и в «домашней» сети. Хотя MSC и VLR, в основном, объединяют, согласно принципам GSM ими являются 2 отдельных сетевых звена, между которыми осуществляется обмен сигнальными сообщениями. Если же отправлять очень много запросов на выделение роуминговых номеров, они просто-напросто кончатся. В результате, реальным пользователям не смогут поступать обычные звонки, т.к. коммутатор будет перегружен.

DoS-атаки на коммутатор:



Выход?

Ситуация очень сложная и угроза действительно существует. Прямо сейчас. Для контроля над ней, как правило, операторы лишь занимаются мониторингом сетевой активности, чтобы вовремя заметить атаки по описанным здесь схемам. Такая статистика дает возможность хотя бы выборочно пресекать ряд запросов. Однако операторы мобильной связи предпочитают о своих уязвимостях молчать. Ведь на их работу факт реальности взлома особо не влияет, абонентам же рекомендуется просто свести к минимуму особо щекотливые беседы по телефону или отправку конфиденциальных SMS. Авторизация по SMS тоже не всегда 100%-но надежна. Для последнего лучше иметь отдельный номер (SIM-карту), который никто не будет знать, кроме вас самих.

Также о технологиях:

Принцип работы сетей GSM >>

Обсудить на форуме

Подписаться на RSS

Подписаться на рассылку

Рейтинг: 0 / 5 (0)

Популярное на сайте

Новые статьи

- Авиакомпания S7: это и есть мародерство?
- Как я избавился от WhatsApp-зависимости
- Наши разговоры прослушивают
- Билайн: двойной развод на контент
- BQ Испания: после 2 лет эксплуатации

Случайные статьи

- Tele2 в Москве в работе: покрытие
- Зачем нужны «умные часы»?
- Мобильники все еще взрываются
- МегаФон по-русски плохо понимать!
- BQ Испания: после 2 лет эксплуатации

Разделы форума

- МТС
- Tele2
- Билайн
- МегаФон
- Другие операторы
- Общие вопросы связи
- Телефоны и смартфоны

Послать смс на МТС, Билайн, МегаФон, Теле2 с компьютера через интернет

комментарии

- **Dmytryi Petrov**
  1 час просмотра видео в hd качестве примерно 0,8 Гб. Соответственно на 1 - 2 дня 15 Гб должно...

  Сколько интернет-трафика нужно? · 3 months ago

- **Ryslan**
  пробиваем номера устанавливаем владельцев по номеру телефона по ФИО можем так же найти актуальный...

  Коды телефонов городов России · 4 months ago

- 
  Дарья Филина
  Знать регион — это, конечно, здорово… Но мало что дает. Нужно знать информацию о владельце. В...

  Коды телефонов городов России · 8 months ago

- **Давид**
  Что-то вы перепутали. Чем старше поколение интернет технологий, тем

Читайте также

МГТС «Smart для своих» дорожает

МТС вновь отменяет роуминг

Яровая будет драть с нас и дальше

МТС: новые пакеты дополнительных минут

МТС: снова скидка за автоплатеж

Капитализация МТС растет

В Tele2 умышленно лгут абонентам

ФАС: дело МТС рассмотрено

Билайн: не было денег? Заплатите!

У Ростелекома почти 1 млн абонентов

Новое на форуме

Смарт для своих, 900₽

Не публичные тарифы от МТС и

Билайн

коды СДС, Супер МТС ДС, Ультра по СУПЕР ценам, торопитесь

Интернет для разных устройств и разных операторов

Безлимитные звонки и интернет Ростелеком,Билайн,Мегафон,МТС

менее оно энергозатратно для...

Автопереключение Wi-Fi на Android · 9 months ago

- **Александр**
Тема и содержание статьи весьма полезна. Неужели Вы думаете, что тема Вашего комментария...

Как МТС абонента не отпускает (+ бардак) · 9 months ago

- **pride4**
А как вы в результате попали в Турцию, когда всё было закрыто? И что в конце концов с деньгами за...

Авиакомпания S7: это и есть мародерство? · 11 months ago

- **Светлана Абанасьян**
У меня модем //www.ozon.ru/context/detail/... с поддержкой LTE и безлимитным...

Тест модема ZTE MF823 (+Keenetic 4G) · 1 year ago

-  **Светлана Абанасьян**
  Я пользуюсь оператором билайн в компании Простономер, мне сразу установили запреты на подключение...

  Билайн: двойной развод на контент · 1 year ago

-  **Kirill Blinov**
  У меня вообще смени тариф. Был тариф "Говорит Москва", а поменяли на тариф "Мой онлайн+ 3000...

  Tele2 сменил тариф без спроса · 1 year ago

-  **admin**
  Мёртвый билайн
  сколько не звони на номер 0611 толку нет

  На сотового оператора можно жаловаться · 1 year ago