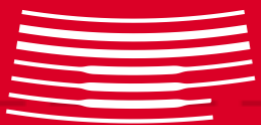
УЯЗВИМОСТИ СЕТЕЙ МОБИЛЬНОЙ СВЯЗИ НА ОСНОВЕ SS7

Дмитрий Курбатов, Сергей Пузанков

2014 г.



POSITIVE TECHNOLOGIES

Оглавление

1. Введение

В настоящее время сети мобильной связи являются самой активной частью критически важной информационной инфраструктуры и ключевым инструментом во многих сферах жизни общества, от управления персональными банковскими счетами до переговоров на уровне лидеров мировых держав. При этом, невзирая на заверения в защищенности мобильной связи, мы часто видим примеры обратного: в последние годы в Интернете не раз появлялись записи приватных телефонных разговоров министров, послов, военных, бизнесменов и других людей, чей статус обычно ассоциируется с повышенными мерами безопасности.

В качестве реакции на эти утечки часто выдвигается версия о сложных и дорогих технологиях прослушки, которые могут использоваться лишь могущественными спецслужбами. Такая точка зрения характерна для людей, которые представляют мобильную связь как набор самых современных и хорошо защищенных технологий (и неудивительно: ведь именно такую картину создает реклама новых устройств и услуг). Однако на практике телекоммуникационная сеть представляет собой сложную систему из множества подсистем различного технологического уровня. В подобных случаях уровень безопасности всей сети зачастую определяется уровнем самого слабого звена.

В частности, процесс установления голосовых вызовов в современных мобильных сетях до сих пор основан на технологии SS7, которая уходит корнями в 70-е годы прошлого столетия. В то время безопасность протоколов сводилась к физической защите узлов и каналов связи, а получение доступа в сеть SS7 с помощью отдельного несанкционированного узла было неосуществимо. В начале 2000-х годов была разработана спецификация SIGTRAN, позволяющая передавать сообщения SS7 по IP-сетям [1]. При этом была унаследована вся слабость безопасности верхних уровней протоколов SS7. В результате злоумышленники имеют возможность бесконтрольно посылать, перехватывать и изменять сообщения протоколов SS7, осуществляя различные атаки на мобильные сети и их абонентов.

Материалы, представленные в данном отчете, собраны экспертами компании Positive Technologies в 2013 и 2014 годах в ходе консалтинговых работ по анализу защищенности нескольких крупных мобильных операторов, а также подкреплены практическими исследованиями найденных уязвимостей и нюансов работы сети SS7.

2. Резюме

Уязвимости сетей сотовой связи на основе технологии SS7 позволяют внешнему злоумышленнику даже с невысокой квалификацией проводить серьезные атаки, результатом которых может быть потеря денежных средств абонентов, утечка конфиденциальных данных или нарушение доступности абонентов и элементов сети в интересах третьих лиц.

В процессе тестирования защиты сетей мобильной связи эксперты Positive Technologies смогли реализовать такие атаки, как раскрытие местоположения абонента, нарушение доступности абонента, перехват SMS-сообщений, подделка USSD-запросов и перевод средств с их помощью, перенаправление голосовых вызовов, подслушивание разговоров, нарушение доступности мобильного коммутатора.

При этом было продемонстрировано, что даже телеком-операторы, входящие в десятку мировых лидеров, не защищены от подобных атак. Кроме того, уже известны случаи практического применения подобных техник на международном уровне, включая раскрытие местоположения абонентов в других странах, а также прослушивание переговоров с территории другого государства.

Общие особенности этих атак:

Злоумышленнику не требуется сложное оборудование. В наших исследованиях использовался узел на базе обычного компьютера под управлением ОС семейства Linux, с установленным SDK для формирования пакетов SS7 — это средство разработки доступно для свободного скачивания в Интернете.

Злоумышленник, успешно осуществивший одну атаку с использованием команд сигнальной сети SS7, с легкостью может провести весь спектр означенных атак теми же средствами. Так, если он научился определять местоположение абонента, ему осталось сделать один шаг до перехвата SMS, перевода средств и т. п.

Атаки базируются на легитимных сообщениях SS7: нельзя просто отфильтровать сообщения, поскольку это может оказать негативное влияние на весь сервис. Альтернативный опыт решения проблемы предлагается в заключительной главе данной работы.

3. Методика исследования

Предпосылки для проведения атак

Большинство атак в сети SS7 базируются на главном принципе сетей сотовой связи — мобильности абонента. Во-первых, для того чтобы вызов дошел до абонента, в системе должна храниться и обновляться информация о местоположении абонента. Сама эта информация может быть объектом атаки. Во-вторых, мобильность абонента подразумевает доступность услуг не только в любой точке, где присутствует радиопокрытие домашней сети, но также в сетях роуминг-партнеров (например, за границей).

Взаимодействие сетевых элементов оператора происходит с помощью стандартизованных сообщений SS7. Сеть SS7 используется практически всеми операторами мобильной связи. Злоумышленник может находиться где угодно: сообщения могут приходить из любой страны мира и из любой сети. При этом фильтрация некоторых сообщений может привести к нарушению работы роуминга или международной связи.

Кроме того, системы телефонной связи все глубже интегрируются с IT-системами. Если ранее узлы телефонных сетей представляли собой некую «вещь в себе» или черный ящик, то сейчас все чаще и чаще их строят на базе широко распространенного аппаратного и программного обеспечения, например на операционных системах Linux, Solaris, VxWorks.

Профиль атакующего

Атакующим может быть человек или группа людей с квалификацией, достаточной для построения узла, эмулирующего работу оператора сотовой связи. Для доступа к сети SS7 атакующие могут приобрести на черном рынке подключение у существующего оператора, получить разрешение на деятельность в качестве оператора связи в странах с лояльным законодательством в сфере регулирования связи. Если участник хакерской группы работает техническим специалистом в компании — операторе связи, то у него также есть возможность обеспечить подключение своего оборудования к сети SS7. Техническому специалисту для осуществления некоторых атак достаточно воспользоваться легитимным набором функций существующего оборудования сети связи. Остается также и возможность проникнуть в сеть оператора через взломанное пограничное устройство, будь то GGSN или сота Femtocell.

Целями атакующего могут быть различные схемы мошенничества, получение конфиденциальных данных об абоненте, нарушение доступности отдельных абонентов или всей сети. Атаки могут выполняться на заказ, в интересах третьих лиц.

Необходимые ресурсы

Для построения узла, эмулирующего работу оператора сотовой связи или отдельного компонента сети, может быть использован персональный компьютер под управлением ОС семейства Linux. Формирование сообщений сигнализации SS7 и отправка их в сеть осуществляется средствами общедоступных стеков протоколов SS7.

4. Обзор исследований

Для всех описанных атак характерны следующие параметры: сложность реализации атаки, учитывая условия (3) — средняя; воспроизводимость атаки, то есть возможность ее успешного повторения другими злоумышленниками — высокая.

4.1. Раскрытие идентификатора IMSI

Цель: исследование сети оператора, получение данных об абонентах.

Описание. В сетях мобильной связи идентификация абонентов происходит не по телефонному номеру (MSISDN), а по международному идентификатору SIM-карты — IMSI. Идентификатор IMSI является частью конфиденциальных данных об абоненте.
Атака базируется на запросе адреса MSC/VLR, где находится абонент, и идентификатора IMSI абонента. Данный запрос является частью процедуры доставки сообщения SMS и выполняется для того, чтобы сеть-источник получила информацию о местонахождении абонента — для дальнейшей маршрутизации сообщения. Исходными данными для создания запроса является телефонный номер абонента.

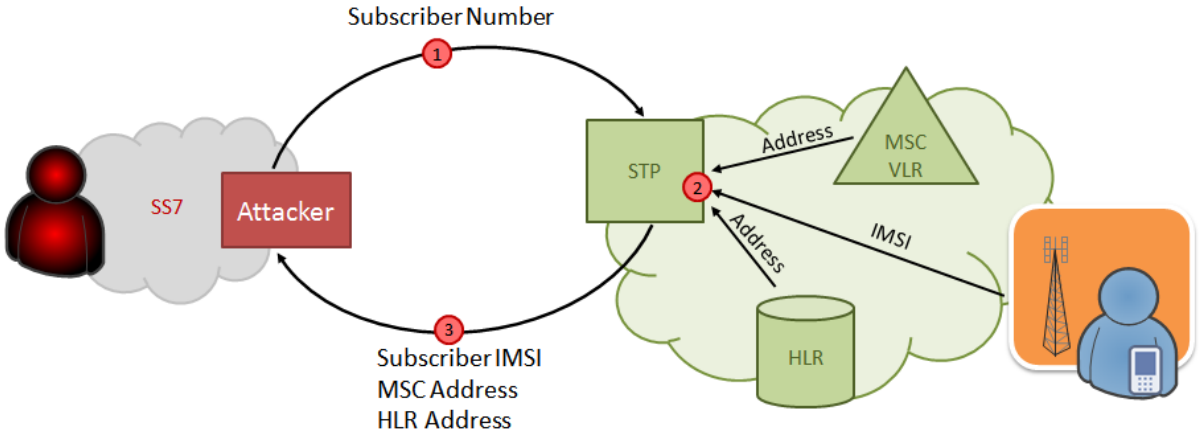


Рис. 1. Схема атаки на раскрытие идентификатора IMSI

Результат. В случае успешной атаки злоумышленник получает следующие данные:

- IMSI абонента,
- адрес MSC/VLR, обслуживающий абонента,
- адрес HLR (БД), в котором хранится подписка абонента.

По адресу MSC/VLR можно определить местоположение абонента, как правило с точностью до региона. Кроме того, все полученные данные злоумышленник может использовать в более сложных атаках, описание которых следует далее.

4.2. Раскрытие местоположения абонента

Цель: определение местоположения мобильного абонента.

Описание. Атака основана на легитимном запросе местоположения абонента, результат которого обычно используется для тарификации в реальном времени входящего вызова на абонента. Исходными данными являются IMSI абонента и адрес текущего MSC/VLR. Эти данные можно получить в результате успешно проведенной атаки 4.1.

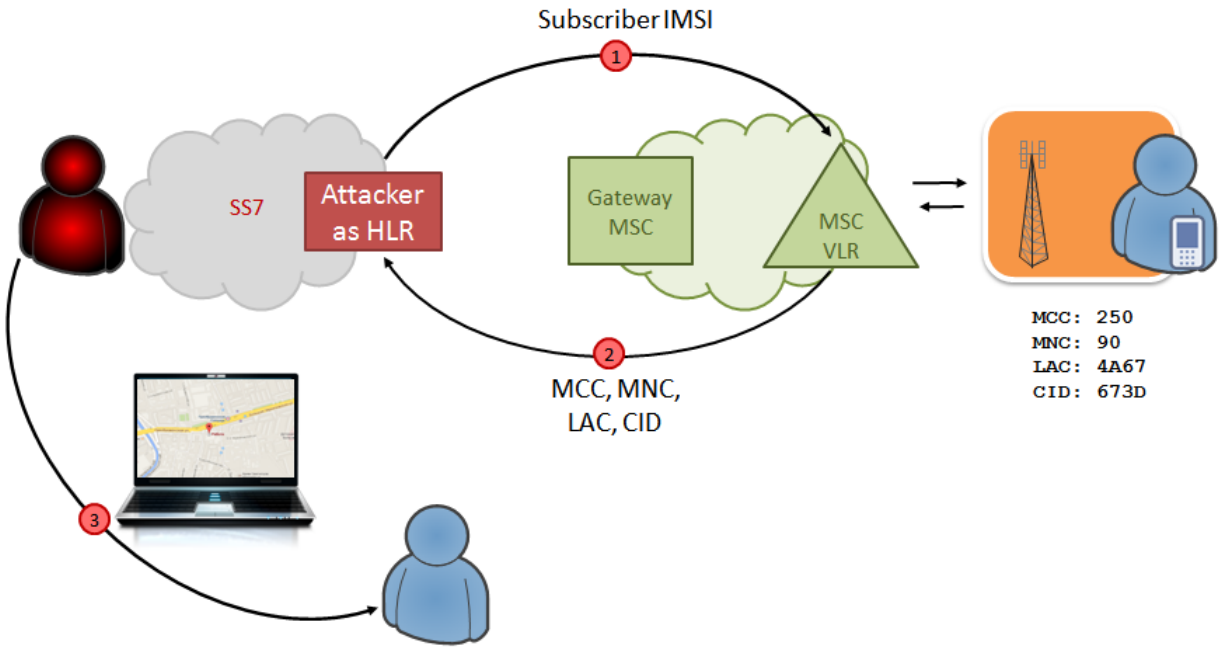


Рис. 2. Схема атаки по определению местоположения мобильного абонента

Результат. Злоумышленник получает глобальный идентификатор соты CGI, который состоит из четырех параметров:

- MCC (Mobile Country Code),
- MNC (Mobile Network Code),
- LAC (Location Area Code),
- CID (Cell Identity).

В сети Интернет есть ряд общедоступных сервисов, которые по указанным идентификаторам определяют местоположение базовой станции на карте местности. В условиях городской застройки точность определения положения абонента составит несколько сотен метров.

4.3. Нарушение доступности абонента

Цель: сделать для мобильного абонента невозможным прием входящих вызовов и SMS-сообщений.

Описание. Атака представляет собой процедуру регистрации абонента в зоне действия «фальшивого» MSC/VLR. Аналогичная процедура происходит при регистрации абонента в сети роуминг-партнера. Исходными данными являются IMSI абонента и адрес текущего MSC/VLR. Эти данные можно получить в результате атаки 4.1.

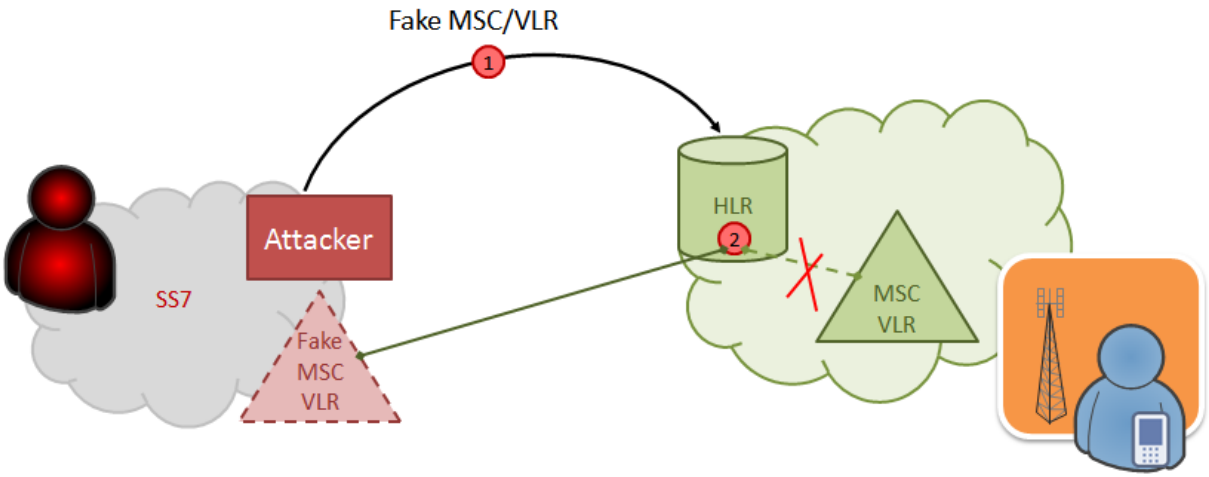


Рис. 3. Схема атаки на нарушение доступности абонента

Результат. Абонент перестанет получать входящие вызовы и SMS-сообщения, при этом телефон абонента будет показывать, что он находится в зоне действия сети. Абонент будет недоступен, пока он не переместится в зону действия другого MSC/VLR, не произведет перезагрузку телефона или не осуществит исходящий вызов.

4.4. Перехват входящих SMS-сообщений

Цель: перехват входящих SMS мобильного абонента.

Описание. Атака является продолжением атаки 4.3 и не требует дополнительных действий со стороны атакующего.

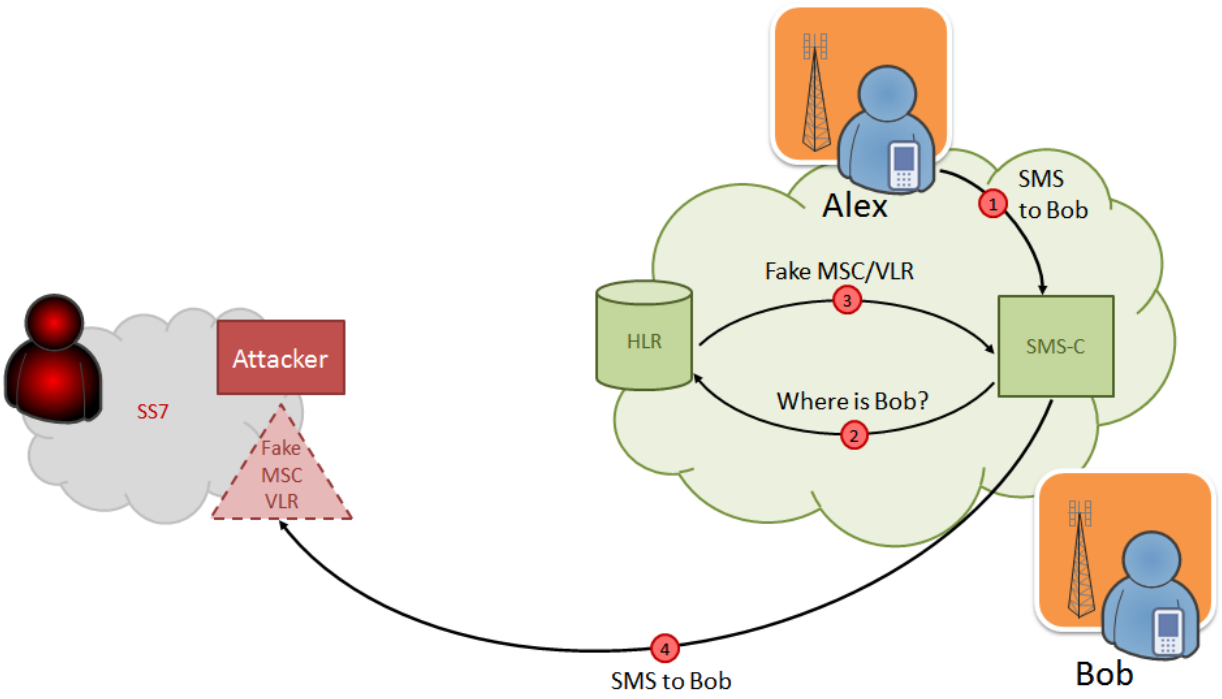


Рис. 4. Схема атаки с перехватом SMS-сообщения

Результат. После проведения регистрации абонента на «фальшивом» MSC/VLR (4.3) все SMS-сообщения, предназначенные абоненту, будут приходить на узел атакующего.

Атакующий может:

- отправить ответ о получении сообщения (у отправляющей стороны будет впечатление, что SMS доставлено получателю);
- не отправлять отчет о получении и перерегистрировать абонента на прежний коммутатор (в этом случае через несколько минут сообщение будет отправлено получателю вторично);
- отправить отчет о получении, перерегистрировать абонента на прежний коммутатор и отправить ему измененное сообщение.

Данная атака может быть использована для:

- перехвата одноразовых паролей мобильного банка,
- перехвата восстановленных паролей от интернет-сервисов (почты, социальных сетей и т. п.),
- получения паролей для личного кабинета на сайте мобильного оператора.

4.5. Манипуляции с USSD-запросами

Цель: отправка прямых USSD-запросов к HLR.

Описание. Атака является полной аналогией легитимного сообщения с USSD-запросом, пересылаемого от VLR к HLR. Исходными данными являются телефонный номер абонента, адрес HLR и строка самого USSD-запроса. Телефонный номер, как правило, известен с самого начала, адрес HLR можно получить в результате успешной атаки 4.1, описание USSD-запросов всегда есть на сайте оператора связи.

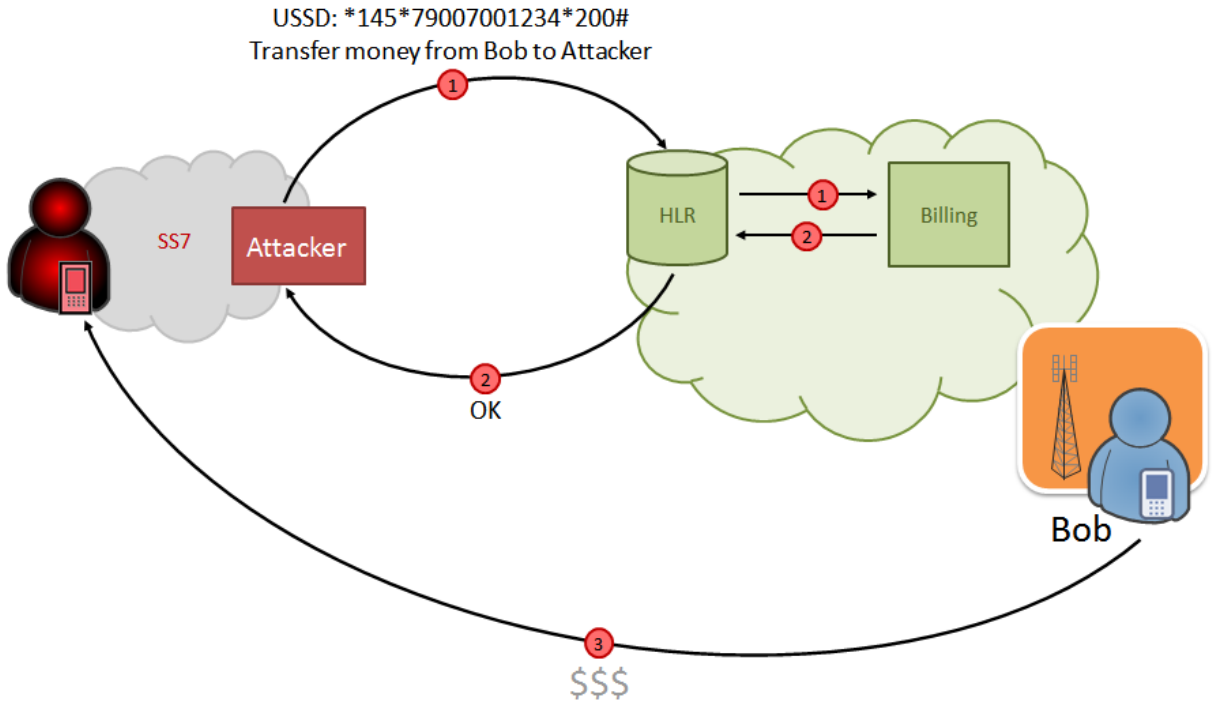


Рис. 5. Схема атаки с манипуляцией с USSD-запросами

Результат. Наиболее опасным вариантом реализации атаки можно считать проведение запроса на перевод средств между счетами абонентов. Такая атака может оставаться незамеченной в течении длительного времени, даже если при снятии средств со счета абонента оператор посылает оповещение с помощью SMS-сообщения. Проведение данной атаки совместно с атакой 4.4 дает злоумышленнику возможность остаться незамеченным.

4.6. Изменение профиля абонента в VLR

Цель: изменение профиля абонента в VLR может преследовать много целей, например обход системы тарификации.

Описание. В процессе регистрации абонента на коммутаторе его профиль копируется из БД HLR в БД VLR. В профиле содержится информация об активированных и деактивированных услугах абонента, параметры переадресаций, адрес платформы

онлайн-тарификации и прочее. Атакующий может произвести отправку в VLR фальшивого профиля абонента.

Исходные данные для атаки: телефонный номер абонента, IMSI абонента, адрес VLR, детали профиля абонента. Номер абонента, как правило, известен заранее. IMSI и адрес VLR злоумышленник может получить в результате атаки 4.1, детали профиля абонента можно получить, проведя атаку 4.3.

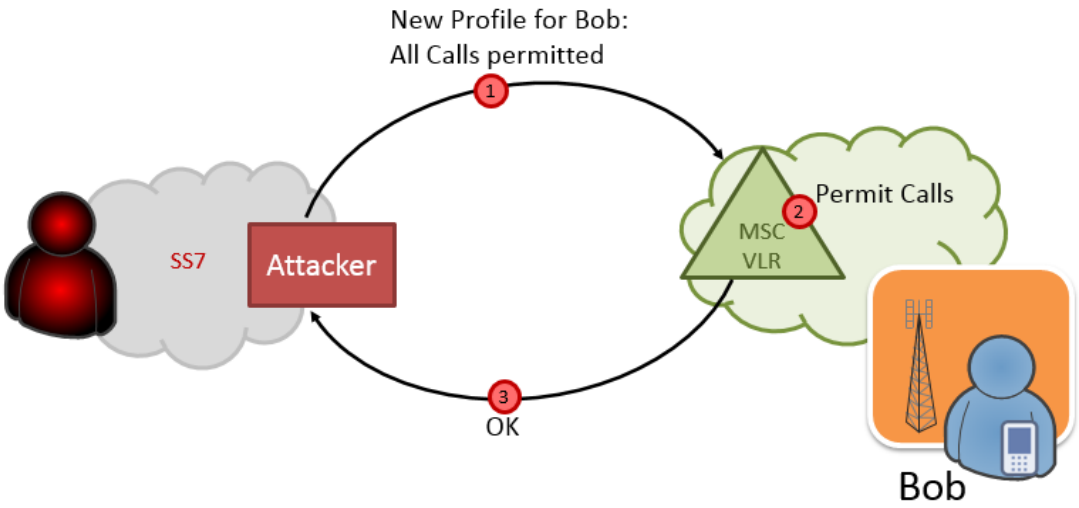


Рис. 6. Схема атаки с подменой профиля абонента

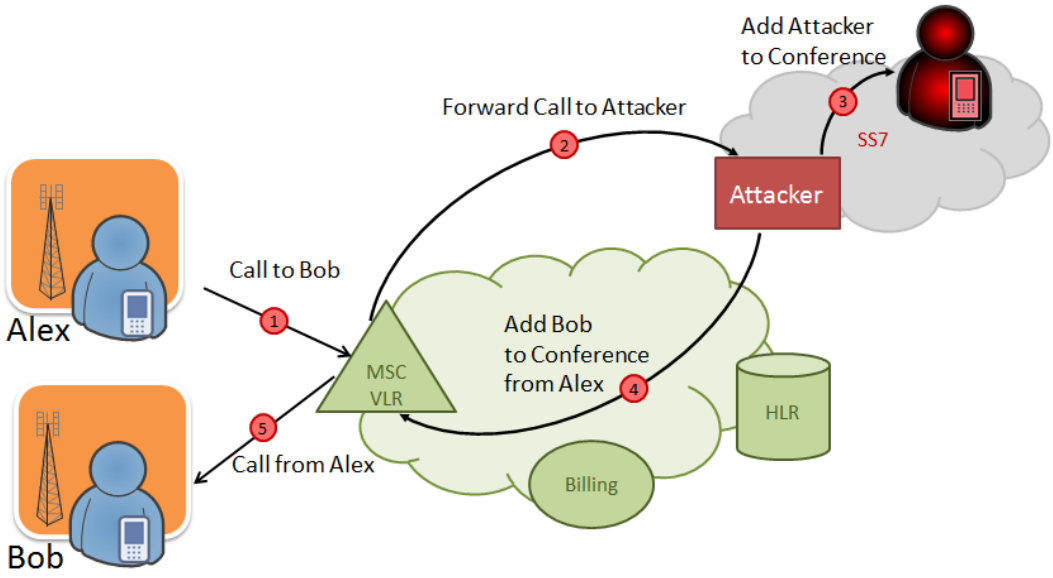
Результат. Фальшивый профиль заставит MSC/VLR обслуживать абонента в соответствии с заданными злоумышленником параметрами. Например, абонент сможет совершать голосовые вызовы в обход системы тарификации.

Вариации. Атака с подменой профиля может использоваться для прослушки разговоров абонента-жертвы.

4.7. Подслушивание исходящих вызовов

Цель: перенаправить голосовой трафик абонента-жертвы и служебную информацию на оборудование злоумышленника.

Описание. Атака является расширением атаки 4.6. В профиле абонента-жертвы злоумышленник меняет адрес платформы тарификации, указывая адрес подконтрольного ему оборудования. После этих действий в момент осуществления исходящего вызова абонента-жертвы, запрос на тарификацию уходит на оборудование злоумышленника. В этом запросе содержится номер вызываемого абонента. Зломушленник имеет возможность перенаправить голосовой вызов на своё оборудование и создать конференц вызов на три стороны: вызываемый абонент, вызывающий абонент, подслушивающий аппарат злоумышленника.



Результат. Раскодированный голосовой трафик пройдёт через оборудование злоумышленника и возвратится к вызываемому абоненту, разговор состоится, но в нём несанкционированно будет участвовать третья сторона.

4.8. Перенаправление входящих вызовов

Цель: повлиять на механизм маршрутизации голосовых вызовов, например для перенаправления входящих вызовов абонента-жертвы.

Описание. Атака базируется на сценарии входящего вызова и является продолжением атаки 4.3. При входящем вызове пограничный MSC (GMSC) отправляет запрос на HLR с целью определения, в зоне действия какого MSC/VLR находится абонент. Эта информация нужна для маршрутизации вызова на соответствующий коммутатор.
После успешной атаки 4.3. HLR, получив указанный запрос, переадресует его на «фальшивый» MSC/VLR, который, в свою очередь, отправляет номер для перенаправления вызова (MSRN). HLR транслирует этот номер на GMSC, который осуществляет перенаправление вызова на предоставленный MSRN.

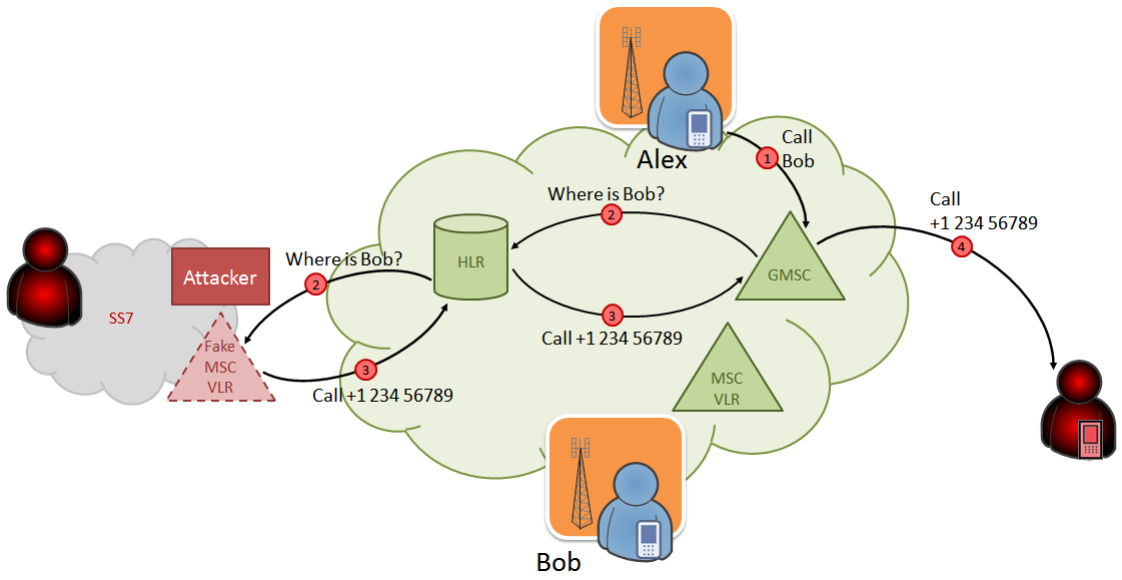


Рис. 7. Схема атаки с перенаправлением входящего вызова

Результат. Атакующий влияет на механизм маршрутизации голосовых вызовов, в данном случае перенаправляет входящих вызов адресованный абоненту-жертве на произвольный номер.

Вариации. Вариантом исполнения этой атаки может быть перенаправление вызова на дорогое международное направление. Злоумышленник, обладая некоторой предприимчивостью, может наладить схему мошенничества, продавая такой трафик. Убытки оператора от этой схемы будут определяться себестоимостью международного трафика.

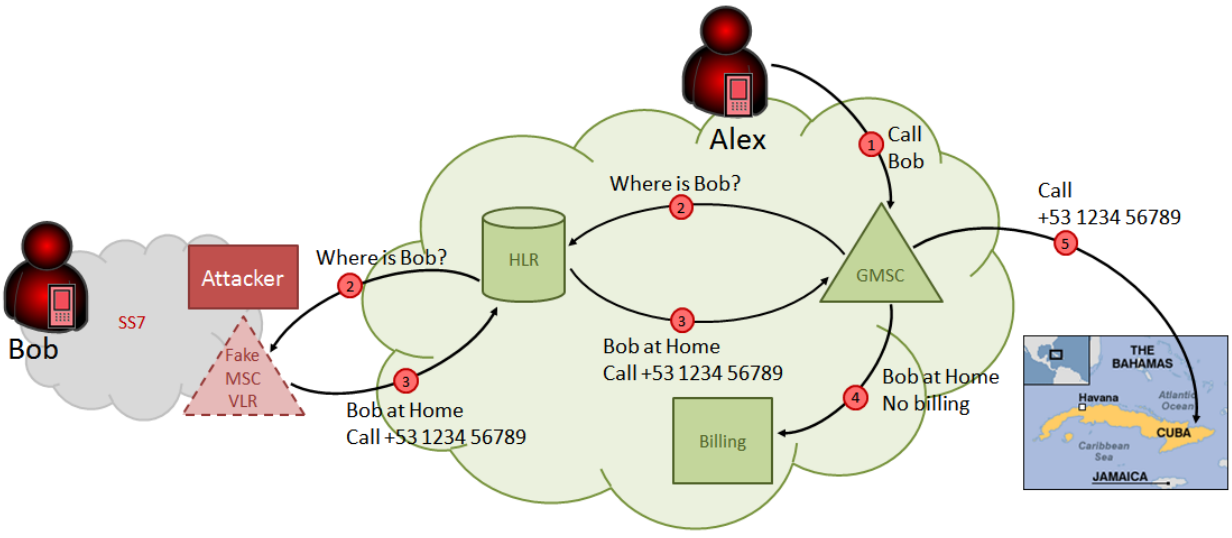


Рис. 8. Схема атаки с перенаправлением входящего вызова на дорогое направление

4.9. Отказ в обслуживании MSC для входящих голосовых вызовов

Цель: отказ в обслуживании входящих вызовов MSC.

Описание. В основе атаки лежит процедура выделения роумингового номера (MSRN) при установлении входящего голосового вызова. При вызове сначала происходит определение текущего MSC/VLR для абонента, затем создание голосового канала до этого коммутатора. Для этого используется временный роуминговый номер. В нормальной ситуации время жизни роумингового номера составляет доли секунды. Однако, значения таймеров для удержания роумингового номера, указанные в оборудовании по умолчанию, составляют 30—45 секунд. Если на коммутатор массово отправлять запросы на выделение роуминговых номеров, то можно довольно быстро израсходовать весь пул роуминговых номеров, и у коммутатора пропадет возможность осуществлять входящие мобильные вызовы.

Исходные данные для атаки: IMSI любого абонента, адрес коммутатора. Эти данные можно получить в результате успешно проведенной атаки 4.1.

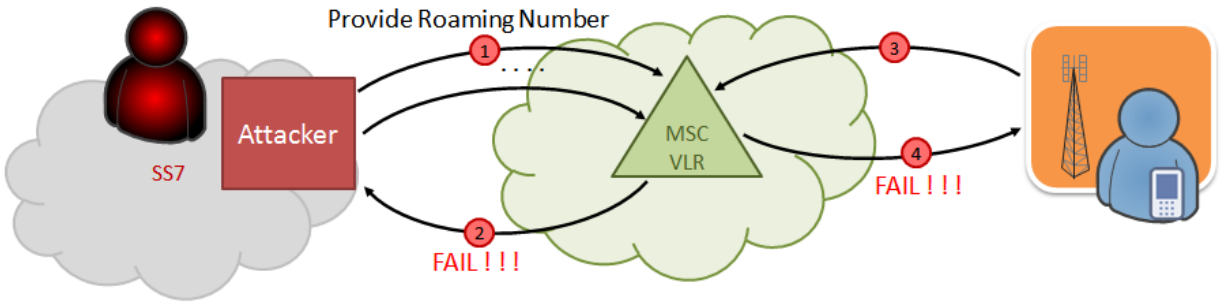


Рис. 9. Схема атаки отказ в обслуживании MSC

Результат. В результате атаки будут недоступны все мобильные абоненты, находящиеся в зоне обслуживания данного коммутатора.

5. История и практика атак через SS7

Один из первых публичных докладов об уязвимостях сигнальной сети SS7 прозвучал в 2008 году на хакерской конференции Chaos Computer Club, где немецкий исследователь Тобиас Энгель (Tobias Engel) показал технику слежки за абонентами мобильных сетей [6]. Однако в профессиональной среде эти уязвимости были известны гораздо раньше. Инженеры телекоммуникационных компаний предупреждали о возможности вычисления местоположения абонентов, а также о различных схемах мошенничества на основе SS7, начиная с 2001 года [2, 3, 4]. Уже тогда об этих возможностях знали и правительства некоторых стран. Так, в книге Томаса Портера и Майкла Гафа «Как обойти защиту VoIP» (How to Cheat at VoIP Security, 2007) приводится цитата из отчета одного из американских ведомств о потенциальных угрозах сетей GSM, где в частности говорится, что «администрация Президента США серьезно обеспокоена высоким уровнем угрозы атак на основе SS7», а ведущие мобильные операторы уже изучают эту угрозу [5].

По понятным причинам операторы не торопились рассказывать широкой публике об этих уязвимостях. Поэтому новый всплеск общественной озабоченности случился в 2013 году, когда бывший сотрудник ЦРУ Эдвард Сноуден раскрыл миру историю о тотальной слежке Агентства Национальной Безопасности США за гражданами своей страны (да и не только за ними). История Сноудена вызвала целую лавину разоблачений — среди которых снова всплыли уязвимости SS7 как одна из техник, использованных АНБ для слежки [10].

Вскоре стало известно о существовании частных компаний, которые предлагают весь описанных спектр атак любому желающему. Так работает, например, сервис SkyLock американской компании Verint:

SkyLock Overview

SkyLock is a real time and independent location finding solution for GSM and UMTS subscribers, which enables operational agencies to retrieve subscriber location information on a global basis, including the case of inbound/outbound roamers and foreign countries, all subject to license limitations.

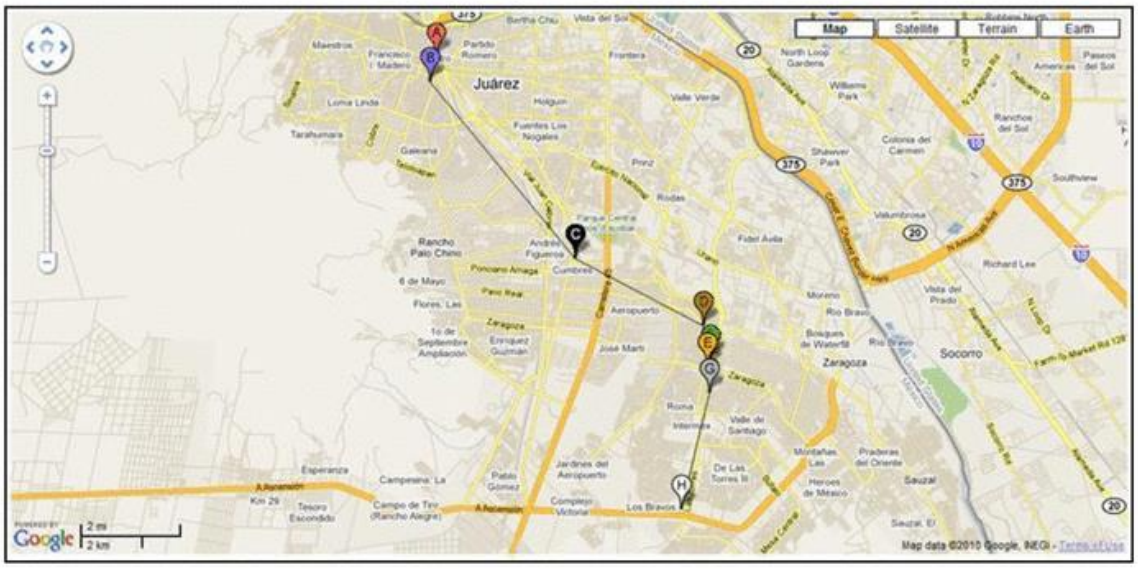
SkyLock presents subscriber information on a Country/Network/LAC/Cell level, and may constitute a platform for various agencies to locate and track people of interest, such as criminals or terrorists on the one hand or survivors of natural disasters on the other.

SkyLock's location finding capabilities are based on the ability to send and handle standard signaling messages (MAP messages) through the international SS7 network. This solution does not require any special hardware or software installation neither in the cellular network nor in the mobile phone. In spite of that, it can track virtually any subscriber in the world, in a covert way, even if the subscriber's mobile phone is not GPS enabled.

Компания Verint активно продает свои услуги в Израиле, но не исключено, что среди ее клиентов есть и спецслужбы других государств: именно для них была создана презентация,

кадры из которой приводятся здесь. Еще одна из возможностей SkyLock — не только одноразовое определение местоположения, но и запись маршрутов передвижения объекта:

> **Route -** Presents the route of a target, up to the last 8 queries, plotted in chronological order. This module enables tracking a target's movements over time.



При этом, как отмечает Washington Post, американская компания Verint не использует слежку против американских и израильских граждан, «однако ряд других аналогичных сервисов, работающих в Швейцарии и на Украине, не подчиняются подобным ограничениям» [11].

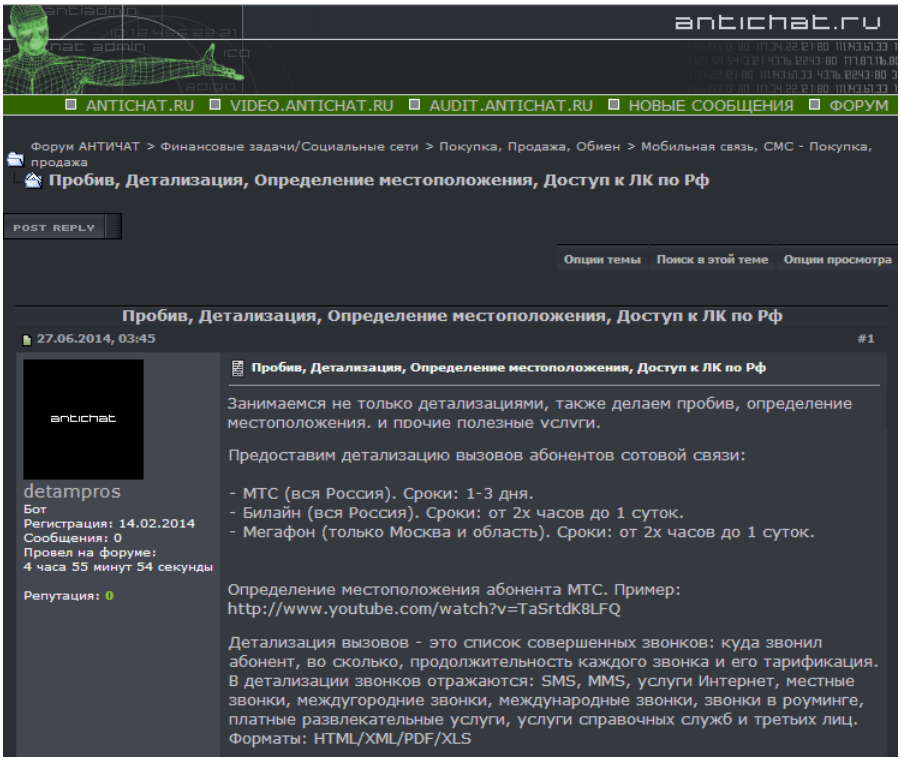
Приведенная цитата — одно из возможных объяснений целой волны скандалов, связанных с публикаций записей телефонных переговоров на Украине. Наиболее известные из них — слова бывшего премьера страны Юлии Тимошенко о необходимости применения ядерного оружия против России, а также оскорбительная фраза, брошенная в адрес Евросоюза представительницей Госдепертамента США Викторией Нуланд в разговоре с послом США на Украине. В свою очередь Служба безопасности Украины в публичных выступлениях не раз использовала записи переговоров представителей донецкого ополчения.

Невзирая на такое количество утечек, украинские операторы и их контролирующие органы тоже не спешат признавать уязвимости. Только в июне 2014 года Национальная комиссия регулирования связи и информатики Украины сообщила о случаях прослушки абонентов «МТС-Украина» через сервер, предположительно принадлежащий российской дочерней компании оператора Tele2 [12].

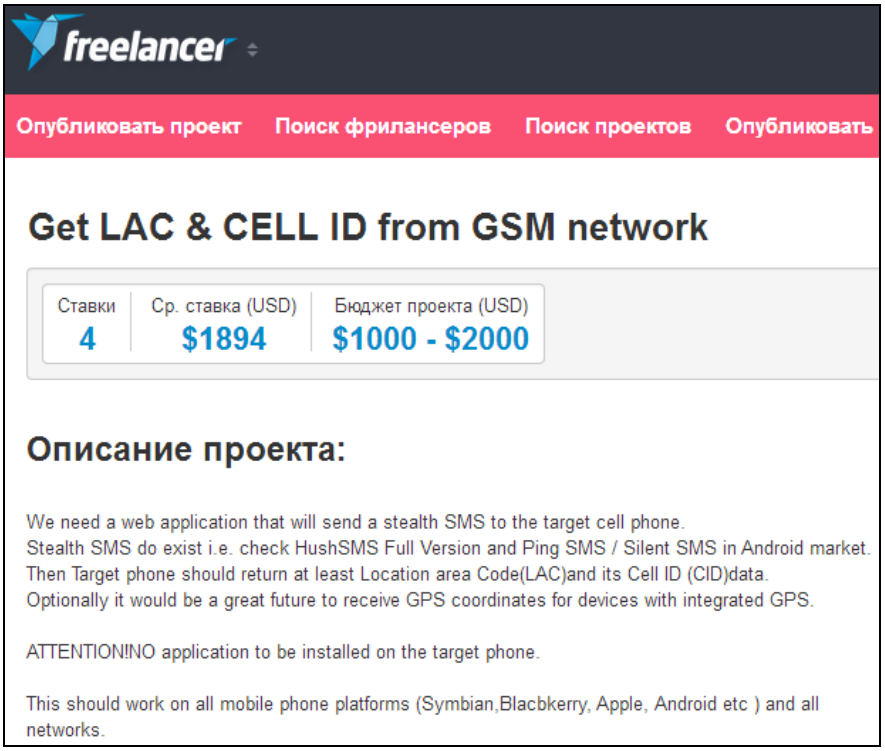
У письмовому зверненні Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України від 12.04.2014 №30/1/3-3955 (далі – лист СБУ) зазначено, що «у оператора зв'язку ПрАТ « МТС УКРАЇНА» є передумови для несанкціонованого втручання з боку іноземних компаній в роботу автоматизованих систем ПрАТ « МТС УКРАЇНА», а саме: 01 – 03 квітня поточного року було виявлено надходження нестандартних команд з боку мережних елементів з номерами GT 7904349006678, 7904349006685, 7952378398777, 7916896031349 на номери абонентів 380503110059, 380503101191, 380662142849, 380503470207, 380504967308, 380501657521, 380997535592, 380955191559, 380958278960, 380997568880. Команди, що використовувалися, дозволяють отримувати відомості про місцезнаходження українських абонентів , вхідні та вихідні номери телефонів з яким відбувається з'єднання, а також переадресовувати виклики через територію Російської Федерації, що дозволяє здійснювати повний контроль за розмовами окремих абонентів тощо. Виконання таких дій можливо при наявності доступу до загальної мережної сигналізації SS7 з мережі звичайного оператора зв'язку».

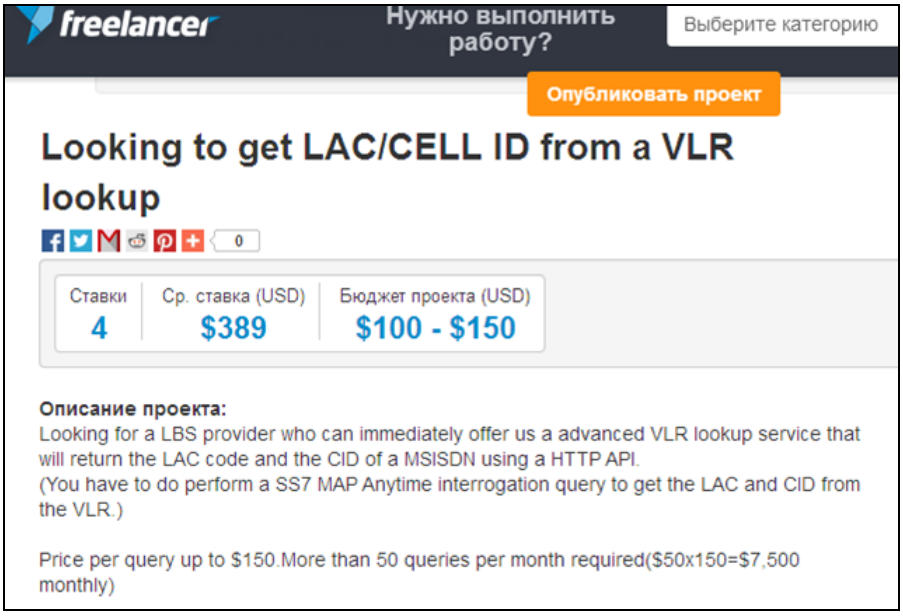
Однако даже в этом случае никаких деталей использованной уязвимости не раскрывалось. По мнению экспертов Positive Technologies, описанный алгоритм прослушки является комбинацией атак, представленных в данном исследовании, а также в наших предыдущих публикациях [9, 13]. Атака могла проводиться не только с территории соседнего государства, но и с любой другой точки земного шара.

В настоящее время в российском Интернете можно найти массу предложений по определению местоположения абонента. Очевидно, что во многих случаях это просто приманка для кражи персональных данных «заказчика» или для распространения вредоносного ПО. Тем не менее, часть таких предложений действительно основана на уязвимостях сетей мобильной связи.



Кроме того, в Интернете есть и предложения заказчиков атак. На основе этих объявлений можно оценить рынок и заметить, что цены снижаются и подобные услуги становятся доступны не только спецслужбам:


freelancer
Опубликовать проект
Поиск фрилансеров
Поиск проектов
Опубликовать
Get LAC & CELL ID from GSM network
Ставки
4
Ср. ставка (USD)
$1894
Бюджет проекта (USD)
$1000 - $2000
Описание проекта:
We need a web application that will send a stealth SMS to the target cell phone.
Stealth SMS do exist i.e. check HushSMS Full Version and Ping SMS / Silent SMS in Android market.
Then Target phone should return at least Location area Code(LAC)and its Cell ID (CID)data.
Optionally it would be a great future to receive GPS coordinates for devices with integrated GPS.
ATTENTION!NO application to be installed on the target phone.
This should work on all mobile phone platforms (Symbian,Blacbkerry, Apple, Android etc) and all networks.


freelancer
Нужно выполнить работу?
Выберите категорию
Опубликовать проект
Looking to get LAC/CELL ID from a VLR lookup
0
Ставки
4
Ср. ставка (USD)
$389
Бюджет проекта (USD)
$100 - $150
Описание проекта:
Looking for a LBS provider who can immediately offer us a advanced VLR lookup service that will return the LAC code and the CID of a MSISDN using a HTTP API.
(You have to do perform a SS7 MAP Anytime interrogation query to get the LAC and CID from the VLR.)
Price per query up to $150.More than 50 queries per month required($50x150=$7,500 monthly)

6. Прогнозы и решения

Кража денег, определение местоположения и прослушка абонентов — это лишь самые очевидные возможности, которые получают злоумышленники с помощью атак на основе уязвимостей SS7. Как показывает опыт Ирака, Сирии, Туниса, Украины и других конфликтных зон, манипуляции с мобильной связью могут сыграть серьезную роль в эскалации массовых беспорядков путем дезинформации.

С другой стороны, благодаря мобильному Интернету сотовая связь становится одним из способов проникновения в другие критически важные инфраструктуры, включая системы управления предприятием и жизненно-важными ресурсами.

Если операторы не начнут внедрять средства защиты от атак со стороны сети SS7, то в ближайшее время жертвами таких атак могут стать любые абоненты мобильной связи, организации или целое государство.

По опыту экспертов Positive Technologies, адекватная защита должна представлять собой комплекс мероприятий, который включает:

- инвентаризацию узлов оператора в сети SS7,
- проверку фильтрации сообщений,
- мониторинг трафика SS7,
- анализ возможности реализации атак и технологического фрода,
- поиск уязвимостей протоколов и ошибок конфигурации оборудования.

Для автоматизированного решения этих задач могут использоваться следующие решения Positive Technologies:

- **Сканер PT SS7 Scanner** размещается в сети оператора связи; результаты регулярного сканирования сверяются с базой данных уязвимостей Positive Technologies, которая постоянно обновляется на основе различных открытых и коммерческих баз данных, а также за счет собственных исследований компании.
- **Система выявления атак PT DPI-SS7** обеспечивает мониторинг трафика на стыках сети SS7, что позволяет своевременно выявлять попытки атак и технологического фрода.
- **Система контроля защищенности и соответствия стандартам MaxPatrol** осуществляет поиск известных уязвимостей, ошибок конфигурации оборудования, контроль соответствия политикам. Направлен на предотвращение технологического фрода, связанного с внесением изменений в конфигурации систем.

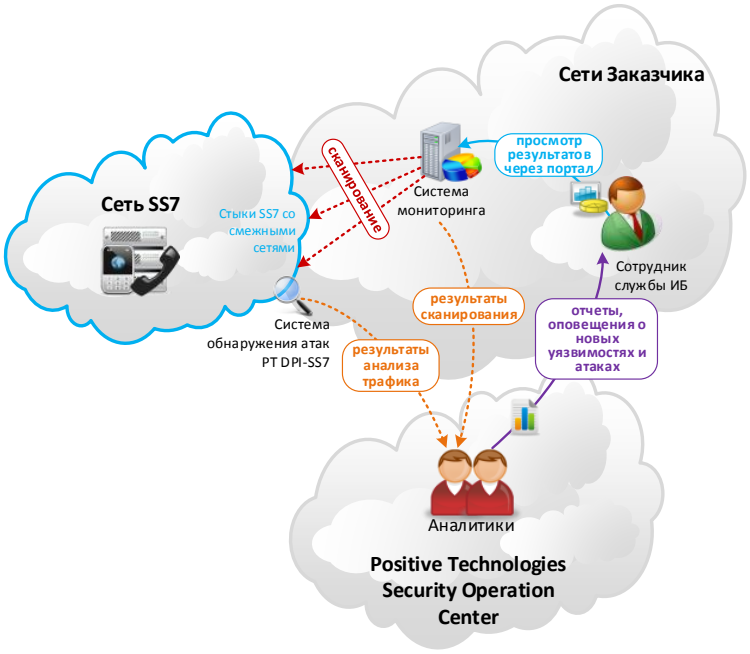


Схема мониторинга защищенности сети SS7

По результатам работы перечисленных сервисов эксперты Positive Technologies готовят отчеты о найденных уязвимостях и возможных атаках. На основе представленной аналитики специалисты оператора связи проводят оценку рисков, после чего принимается решение о внесении изменений в конфигурации систем, о принятии рисков либо о расширенном мониторинге потенциальных атак.

Данная схема обеспечения безопасности уже зарекомендовала себя как надежное средство защиты от атак со стороны сети SS7 в нескольких крупных телекоммуникационных компаниях — как российских, так и зарубежных.

Источники

1. Signaling Transport (sigtran). — The Internet Society, 1999-2007.
http://datatracker.ietf.org/wg/sigtran/documents/

2. A Study of Location-Based Services. — Lennart Ostman, CellPoint Systems, 2001.
http://epubl.ltu.se/1402-1617/2001/254/LTU-EX-01254-SE.pdf

3. SMS SS7 Fraud 3.1 — GSM Association, 2003-2005.
http://www.gsma.com/newsroom/wp-content/uploads/2012/12/IR7031.pdf

4. Can Active Tracking of Inroamer Location Optimise a Live GSM Network? — Katerina Dufková, Jirí Danihelka, Michal Ficek, Ivan Gregor, Jan Kouba, CTU-Ericsson-Vodafone R&D, 2007.
http://www.rdc.cz/en/publications/publications/dufkova07ss7tracker.pdf

5. How to Cheat at VoIP Security. — Thomas Porter, Michael Gough, 2007.
http://www.amazon.com/How-Cheat-at-VoIP-Security/dp/1597491691

6. Locating Mobile Phones Using Signalling System #7. — Tobias Engel, 2008.
http://berlin.ccc.de/~tobias/25c3-locating-mobile-phones.pdf

7. Getting in the SS7 Kingdom. — Philippe Langlois, P1 Security Inc, 2010.
http://www.hackitoergosum.org/2010/HES2010-planglois-Attacking-SS7.pdf

8. Dmitry Kurbatov. Five Nightmares for a Telecom. — Positive Hack Days, 2013.
http://www.slideshare.net/phdays/d-kurbatov-5-nightmaresfortelco

9. Как раскрыть местоположение мобильного абонента. — Сергей Пузанков, Positive Technologies, 2013.
http://habrahabr.ru/company/pt/blog/191384/

10. New documents show how the NSA infers relationships based on mobile location data. — Washington Post, 2013.
http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/new-documents-show-how-the-nsa-infers-relationships-based-on-mobile-location-data/

11. For sale: Systems that can secretly track where cellphone users go around the globe. — Washington Post, 2014.
http://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html

12. Абоненти МТС під ковпаком. — Независимое бюро новостей, 2014.
http://www.mobile-review.com/articles/2014/image/crimea-roam/doc.pdf

13. Прослушка украинских мобильников: как это сделано и как защититься. — Сергей Пузанков и Дмитрий Курбатов, Positive Technologies, 2014.
http://habrahabr.ru/company/pt/blog/226977/

Список аббревиатур и сокращений

CGI (Cell Global Identity) — глобальный идентификатор соты; является стандартным идентификатором сети GSM и используется для идентификации конкретной соты внутри зоны местоположения.
CID (Cell ID) — идентификатор соты.
GMSC (Gateway MSC) — граничный коммутатор.
HLR (Home Location Register) — база данных, которая содержит информацию об абоненте.
IMSI (International Mobile Subscriber Identity) — международный идентификатор мобильного абонента.
LAC (Local Area Code) — код локальной зоны.
MAP (Mobile Application Part) — прикладная подсистема мобильной связи.
MCC (Mobile Country Code) — код страны, в которой находится базовая станция.
MNC (Mobile Network Code) — код сотовой сети.
MSC (Mobile Switching Center) — специализированная автоматическая телефонная станция.
MSISDN (Mobile Subscriber Integrated Services Digital Number) — номер мобильного абонента цифровой сети с интеграцией служб.
MSRN (Mobile Station Roaming Number) — роуминговый номер мобильной станции.
SS7 (Signaling System 7) — общеканальная система сигнализации, используемая в международных и местных телефонных сетях по всему миру.
VLR (Visitor Location Register) — база данных, которая содержит информацию о нахождении и перемещении абонента.

ЗАО / ПОЗИТИВ ТЕКНОЛОДЖИЗ
107061 / МОСКВА / ПРЕОБРАЖЕНСКАЯ ПЛ., Д. 8
ТЕЛ.: +7 (495) 744 01 44 / ФАКС: +7 (495) 744 01 87 / PT@PTSECURITY.COM
WWW.PTSECURITY.RU / WWW.MAXPATROL.RU / WWW.SECURITYLAB.RU