СТАТИСТИКА ОСНОВНЫХ УГРОЗ БЕЗОПАСНОСТИ В СЕТЯХ SS7 МОБИЛЬНОЙ СВЯЗИ

2016

POSITIVE TECHNOLOGIES

Оглавление

Введение

С помощью уязвимостей SS7 злоумышленник из любой точки планеты может превратить чужой телефон в открытую книгу — перехватить SMS-сообщения, обнаружить местоположение и выполнить другие нелегитимные действия. Эта техника доступна не только спецслужбам, но и хакерам средней квалификации. В 2014 году мы подробно рассказывали о проблемах безопасности сигнальных сетей [1]. В настоящем отчете проанализирована защищенность от подобных атак сетей SS7 операторов разных стран, обслуживающих от 10 до 70 миллионов абонентов.

Наследие 70-х

Систему сигнализации SS7 иногда называют нервной системой телефонной сети. До появления SS7 служебные команды для соединения абонентов и доставки информационных пакетов передавались по разговорному каналу. Такой подход был признан неэффективным, поэтому более 30 лет назад появилась физически отделенная глобальная система сигнализации. Сегодня стандарт Signaling System 7 (называемый в России общим каналом сигнализации № 7 — ОКС-7) определяет процедуры и протоколы обмена информацией между сетевыми устройствами телекоммуникационных компаний. На базе SS7 построена сигнальная инфраструктура операторов местной, междугородной, международной и беспроводной связи.

Разработанная в 70-х годах прошлого века система содержит определенные недостатки в плане защищенности: отсутствуют, к примеру, шифрование и проверка подлинности служебных сообщений. Долгое время это не представляло опасности ни для абонентов, ни для оператора, — сеть SS7 была замкнутой системой, в которую подключались только операторы фиксированной связи. Однако время идет, сеть эволюционировала для поддержки нужд мобильной связи и предоставления дополнительных услуг. В начале 2000-х была предложена спецификация SIGTRAN, позволившая передавать служебную информацию SS7 по IP-сетям. Сигнальная сеть перестала быть изолированной.

Первые публичные демонстрации уязвимостей SS7 состоялись в 2008 году: немецкий исследователь Тобиас Энгель показал технику слежки за абонентами мобильных сетей [10]. В 2015 году специалисты SR Labs в эфире австралийской программы «60 минут», будучи в Германии, перехватывали SMS-переписку австралийского сенатора Ника Ксенофонта и британского журналиста, а потом наблюдали за передвижениями сенатора в командировке в Токио с точностью до базовой станции [7].

Специалисты знали об этих уязвимостях задолго до того: Леннарт Остман писал о проблемах SS7 еще в 2001 году [4], а в администрации Президента США выражали обеспокоенность ими в 2000 году [5]. В 2013 году Сноуден отметил SS7 в числе техник, использованных АНБ [9]. По данным Bloomberg, услуги по выслеживанию абонентов с помощью SS7 предлагают Defentek и Verint Systems [2], [6]. Об аналогичных предложениях со стороны израильской CleverSig и болгарской Circles говорилось и в утекшей переписке Hacking Team [11]. По сведениям Брюса Шнайера, британская компания Cobham продает госструктурам более 10 стран систему, позволяющую определить местоположение любого сотового телефона с точностью до метра [8]. Рынок слежки через SS7 растет, и соответствующие предложения все чаще можно увидеть на хакерских форумах.

Возможности злоумышленника

Имея доступ к SS7 и зная номер телефона жертвы, можно подслушать разговор, определить местоположение человека, перехватить SMS для доступа к мобильному банку, отправить USSD-команду на платный номер и осуществить другие атаки [1].

Конечно, напрямую попасть в сигнальную сеть не получится. Для подключения потребуется найти SS7-шлюз. Однако на черном рынке есть немало предложений приобрести полноценный доступ к сети действующего оператора за сумму в несколько тысяч долларов. В некоторых странах с либеральным законодательством в области связи можно и вовсе оформить лицензию оператора вполне официально. Кроме того, технический специалист компании-оператора может выполнять ряд атак с помощью легитимного набора команд или подключить к SS7 свое оборудование. Существуют также способы попасть в сеть через взломанное операторское оборудование, GGSN [3] или фемтосоту.

Атаки через SS7 могут выполняться из любого места на планете, что делает этот метод наиболее перспективным для нарушителя. Злоумышленнику не надо физически находиться рядом с абонентом, как в случае с поддельной базовой станцией, поэтому вычислить его практически невозможно. Высокая квалификация также не требуется — в сети достаточно готовых приложений для работы с SS7. При этом операторы не могут блокировать команды с отдельных узлов, поскольку это оказывает негативное влияние на весь сервис и нарушает принципы функционирования роуминга.

Уязвимости сигнальных сетей позволяют осуществлять самые разнообразные атаки. К примеру, с помощью команд SS7 MAP можно удаленно разблокировать сотовые телефоны [12]. Незащищенность SS7 угрожает при этом не только пользователям мобильных телефонов, но и растущей экосистеме промышленных и IoT-устройств, от банкоматов до GSM-систем контроля за работой газовых станций.

В подобных условиях обеспечение безопасности сетей SS7 — одна из первоочередных задач при построении комплексной защиты мобильной связи.

В исследовании приведены статистические данные, собранные специалистами Positive Technologies при проведении работ по анализу защищенности сетей SS7 различных операторов мобильной связи в 2015 году. Мы проанализировали актуальные угрозы информационной безопасности и оценили текущий уровень защищенности сигнальных сетей от атак со стороны внешнего нарушителя.

Список сокращений

GwSTP (Gateway Signaling Transfer Point) — пограничный узел для маршрутизации сигнальных сообщений.

HLR (Home Location Register) — база данных, которая содержит информацию об абоненте.

MSC (Mobile Switching Center) — мобильный телефонный коммутатор.

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.

1. Методика исследования

Эксперты отдела безопасности телекоммуникационных систем компании Positive Technologies в 2015 году осуществили 16 проектов по анализу защищенности сетей SS7 мобильной связи. Такие работы проводились в отношении сетей ведущих мобильных операторов регионов EMEA и APAC. Для подробного сравнительного анализа были выбраны результаты 8 наиболее информативных с точки зрения статистики проектов с максимально полным перечнем проверок.

В ходе работ по анализу защищенности сетей моделировались действия внешнего нарушителя, атакующего из международной или национальной сигнальной сети. Посредством специального программного обеспечения производилось инструментальное сканирование сети SS7 для проверки:

+ фильтрации сигнальных сообщений и связанных с ними уязвимостей,
+ возможности атаковать узлы сети сигнализации,
+ возможности атаковать абонентов мобильного оператора.

Эксперты рассматривали модель нарушителя, который действует из внешней по отношению к тестируемой сигнальной сети и осуществляет атаки, основанные на возможном прохождении запросов различных протоколов уровня приложений (MAP, CAP) в сеть оператора.

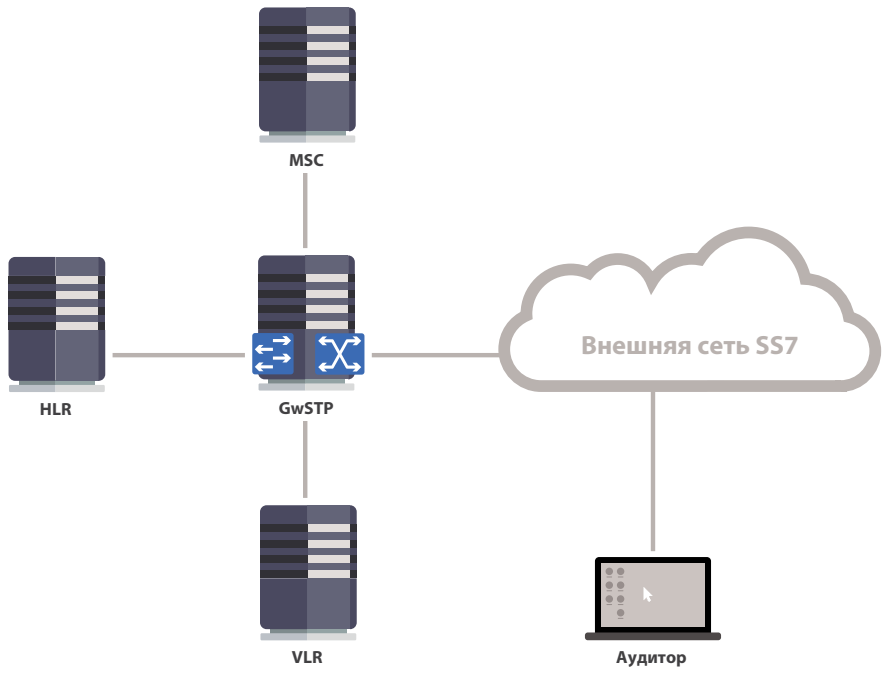

Рис. 1. Схема проведения работ по анализу защищенности сети SS7

Полученная в ходе анализа защищенности информация предназначена для повышения уровня защищенности мобильных сервисов и снижения рисков нарушения доступности сети и фрода.

2. Резюме

Результаты проведенного исследования позволяют сделать следующие основные выводы:

Каждая сеть SS7 уязвима

Все исследованные операторские сети SS7 подвержены тем или иным уязвимостям, которые может успешно проэксплуатировать внешний нарушитель. Например, отказ в обслуживании отдельного абонента был осуществлен в 80% случаев. Угрозы, связанные с мошенничеством, включая хищение денежных средств со счетов пользователей, могли быть реализованы в 67% случаев.

Данные абонентов под угрозой

Во всех сетях SS7, вошедших в выборку, возможны были кража информации об абоненте и перехват SMS. Определить местоположение абонента не удалось лишь в одной из сетей.

Сети региона EMEA менее защищены

Хуже обстоят дела в сетях операторов стран Европы, Ближнего Востока и Африки. Они позволяли потенциальному злоумышленнику провести весь спектр злонамеренных действий — вызвать сбой в работе, осуществить мошенничество и кражу чувствительной информации. Впрочем, выборка недостаточна велика, чтобы сделать общий вывод об уровне защищенности сетей SS7 всех операторов мобильной связи данного региона.

Крупные операторы не могут гарантировать защиту

Как и следовало ожидать, небольшие операторы мобильной связи оказались хуже защищены от атак со стороны внешнего нарушителя. Однако даже крупнейшие в своих регионах операторы не обеспечивают безопасность своих абонентов: доля успешных атак была велика во всех случаях.

3. Портрет участников

25% исследованных нами сетей SS7 принадлежат крупнейшим мобильным операторам. Число абонентов у таких компаний — свыше 70 млн человек. Каждый четвертый участник обслуживает от 40 до 70 млн клиентов. Относительно небольшие компании (до 10 млн абонентов) также фигурируют в отчете, их доля составляет 25%.

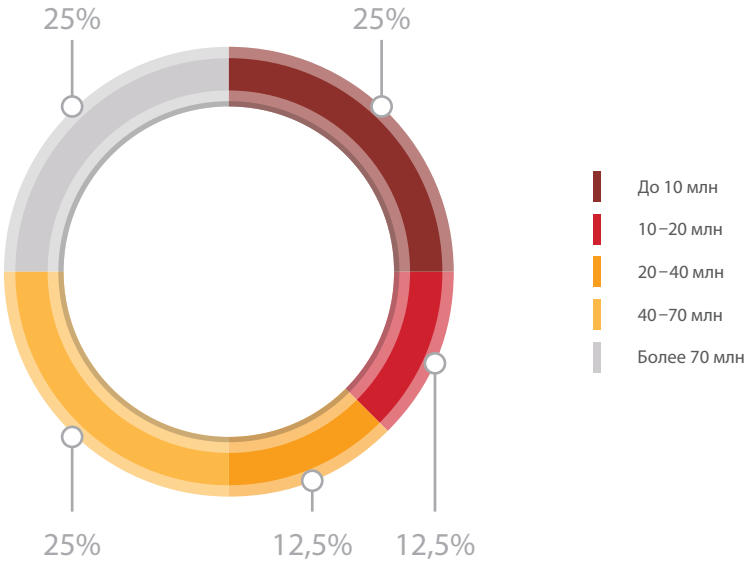

Рис. 2. Объем абонентской базы операторов

Большинство сетей SS7 принадлежат операторам стран Азиатско-Тихоокеанского региона (APAC), и лишь одна четверть — странам EMEA, региону, включающему в себя Европу (в том числе Россию), Ближний Восток и Африку.

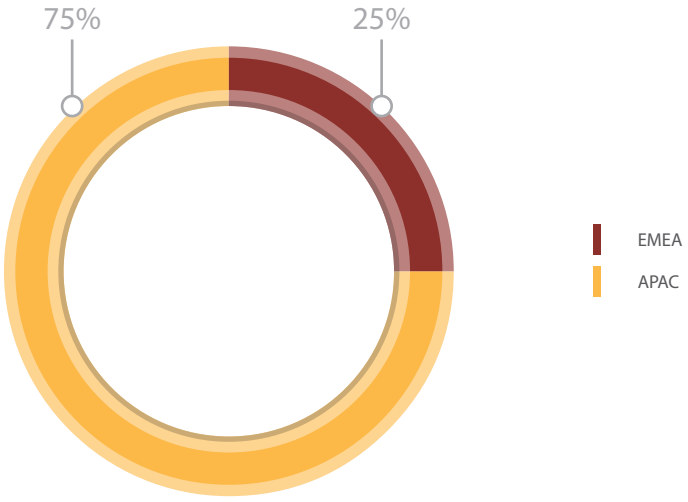

Рис. 3. Исследованные системы по регионам

В соответствии с политикой ответственного разглашения подробная информация об уязвимостях и названия компаний-операторов не указываются.

4. Статистика реализации основных угроз

Угрозы со стороны потенциального нарушителя в отношении сетей SS7 и абонентов мобильных операторов мы разделили на три класса:

+ мошенничество,
+ утечка чувствительной информации,
+ сбои в работе.

Все они чреваты для оператора репутационными и финансовыми потерями.

Мошенничеством в данном случае считались любые неправомерные действия нарушителя при использовании сервисов оператора. Это, например, несанкционированный перевод денежных средств со счетов пользователей, переадресация вызовов или внесение изменений в профили абонентов.

Под утечкой информации понимались разглашение, перехват или хищение данных об абонентах операторов или информации о конфигурации сети SS7. Сюда относятся определение местоположения абонентов, прослушивание переговоров, чтение SMS.

Сбои в работе — атаки, направленные на отказ в обслуживании самой сети SS7 или отдельных ее сервисов.

4.1. Наиболее распространенные угрозы

Все исследованные в 2015 году сети SS7 мобильных операторов были подвержены тем или иным угрозам. В ходе работ по анализу защищенности эксперты смогли успешно провести 80% атак, направленных на сбои в работе, 77% атак с целью вызвать утечку информации и 67% мошеннических атак.

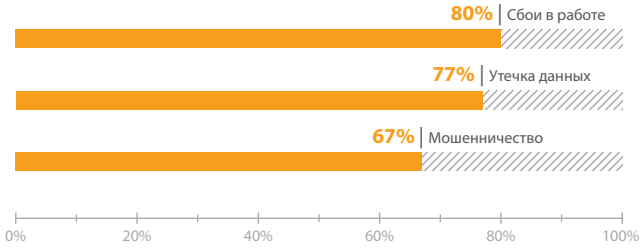

Рис. 4. Угрозы (доли успешных атак)

Реализовать перечисленные угрозы позволяют уязвимости и ошибки конфигурации сетевого оборудования и используемого на нем ПО. Все выявленные недостатки можно разделить на четыре типа:

+ отсутствие проверки реального местоположения абонента;
+ отсутствие фильтрации неиспользуемых сигнальных сообщений;
+ невозможность проверки принадлежности абонента сети;
+ недостатки конфигурации Home Routing.

SMS Home Routing — это аппаратно-программный комплекс, который обеспечивает функции проксирования конфиденциальных абонентских идентификаторов и адресов оборудования во время приема SMS-сообщений со стороны внешних подключений.

Эксплуатация названных уязвимостей может приводить к реализации различных классов угроз. Например, в случае успешных атак с использованием недостатков, связанных с невозможностью проверки принадлежности абонента сети, нарушитель может как определять текущее местоположение абонента (утечка информации), так и перенаправлять его исходящие вызовы на платный номер (мошенничество).

В среднем на одну исследованную сеть SS7 приходилось более 9 успешных атак, связанных с эксплуатацией уязвимостей типа «Отсутствие проверки реального местоположения абонента». Более трех успешных попыток эксплуатации уязвимостей были вызваны невозможностью проверки принадлежности абонента сети. Эти недостатки были оценены в большинстве случаев как критически опасные.

Цвет на диаграмме (см. рис. 5) обозначает уровень риска: красный — высокий, желтый — средний. Степень опасности уязвимости определялась специалистами Positive Technologies с учетом возможного воздействия на систему и сложности эксплуатации. По оценке экспертов, злоумышленнику для проведения атак на рассмотренные системы не требуется сложное оборудование. В нашем исследовании использовался узел на базе обычного компьютера под управлением ОС семейства Linux, с установленным SDK для формирования пакетов SS7 (это ПО доступно бесплатно в сети Интернет).

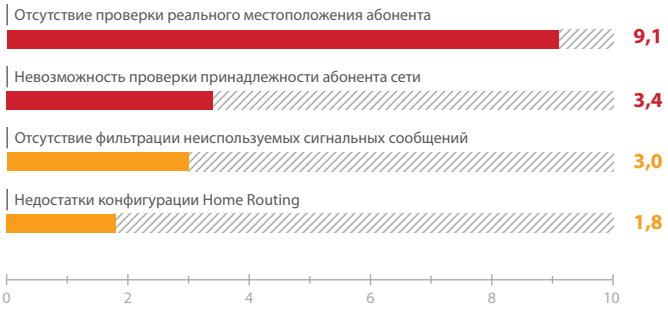

Рис. 5. Уязвимости (среднее количество успешных атак на одну сеть SS7)

Перечисленные уязвимости в общем случае могут классифицироваться как недостатки конфигурации (отсутствие фильтрации неиспользуемых сигнальных сообщений и недостатки конфигурации Home Routing), архитектурные проблемы протоколов и систем (невозможность проверки принадлежности абонента сети и отсутствие проверки реального местоположения абонента) либо как ошибки в используемом ПО (к таким ошибкам был отнесен недостаток, связанный с отсутствием проверки реального местоположения абонента в одном из проектов).

Как видно на рис. 6, большинство реализованных угроз связаны именно с использованием архитектурных недостатков (61%) и лишь 1% успешных атак был основан на эксплуатации уязвимостей в ПО.

Для устранения уязвимостей каждой из категорий необходим соответствующий подход. Это может быть как применение дополнительных технических и программных средств защиты, так и внесение изменений в настройки систем. Более подробно методы защиты от атак описаны в разделе 4.4.

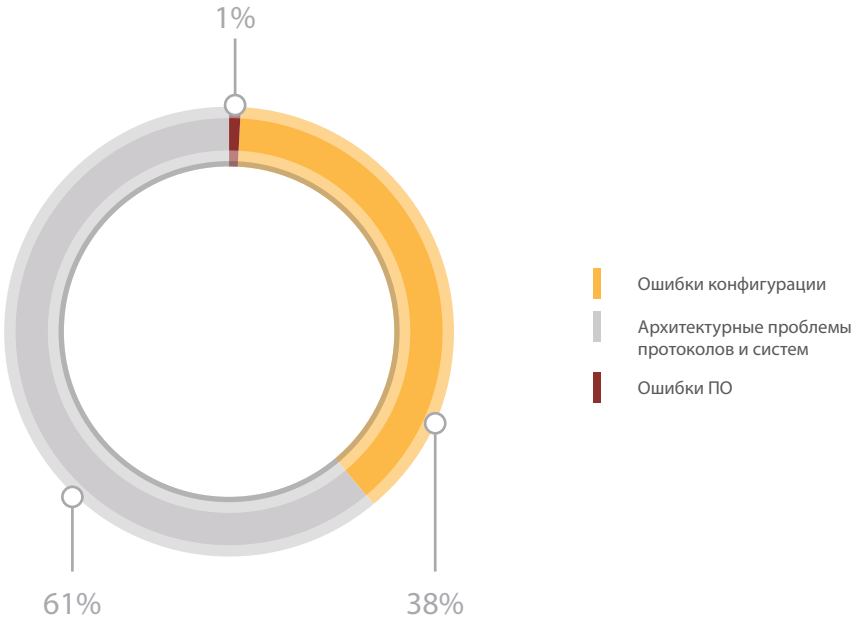

Рис. 6. Категории уязвимостей (доли успешных атак)

4.1.1. Утечка информации

Как отмечалось выше, угроза утечки информации связана с получением нарушителем каких-либо данных об абонентах операторов или информации о конфигурации сети SS7. В общем случае реализация подобных угроз не несет прямого ущерба операторам связи. Однако в случае выявления и публичного разглашения информации о подобных инцидентах ИБ в конкретной сети компания-оператор может потерять репутацию надежного провайдера.

Среди угроз ИБ, относящихся к данному классу, можно выделить основные пять:

+ прослушивание звонков;
+ получение информации о балансе абонента;
+ перехват SMS-сообщений;
+ определение текущего местоположения абонента;
+ кража информации об абоненте.

Рис. 7. Доля успешных атак с целью получения чувствительной информации

Во всех сетях SS7, вошедших в выборку, были возможны кража информации об абоненте и перехват SMS, а определить местоположение абонента не удалось лишь в одной из сетей. Проведение атак в каждом случае возможно несколькими методами, и не каждый из них оказался эффективен. Например, практически все атаки с целью получения баланса абонента или кражи информации о нем оказались успешными (более 90%), но в случае прослушивания звонков лишь половина попыток дали результат.

Для получения данных о пользователях мобильных сетей используются, среди прочего, специально сформированные сообщения следующих типов:

+ SendRoutingInfo;
+ SendRoutingInfoForSM;
+ SendRoutingInfoForLCS;
+ SendIMSI.

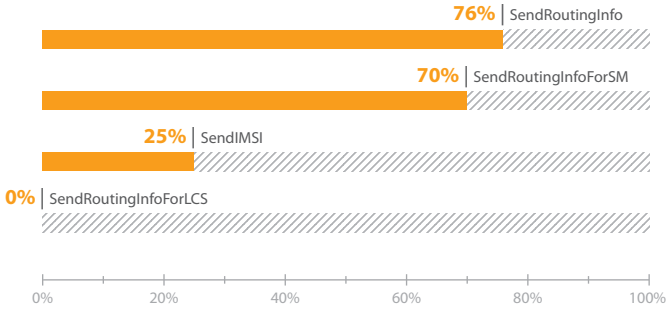

Рис. 8. Методы атак с целью кражи информации об абоненте (доля успешных атак)

Как показывает диаграмма, успешная реализация атаки в 76% случаев возможна с помощью метода **SendRoutingInfo**. Он основан на использовании недостатка, связанного с отсутствием фильтрации неиспользуемых сигнальных сообщений. SendRoutingInfo — сообщение протокола MAP, которое используется при входящем голосовом вызове и служит для запроса маршрутной информации для локализации вызываемого абонента. При нормальном режиме функционирования это сообщение должно передаваться только между элементами своей сети. Специалисты Positive Technologies оценивают уровень риска данной уязвимости в рамках метода SendRoutingInfo как средний. Используя данный метод, нарушитель может не только получить информацию об абоненте, но и определить его текущее местоположение.

SendRoutingInfoForSM — сообщение протокола MAP, которое используется при входящем SMS-сообщении и служит для запроса маршрутной информации для локализации абонента-получателя. Это сообщение должно маршрутизироваться на оборудование SMS Home Routing, если оно установлено в сети оператора. Соответствующий метод оказался эффективен в 70% случаев.

SendIMSI — сообщение протокола MAP, которое используется для запроса идентификатора IMSI абонента по его телефонному номеру. В настоящее время данное сообщение практически не используется операторами мобильной связи, однако оборудование часто все же обрабатывает его, согласно стандарту 3GPP. Каждая четвертая атака с использованием этого метода оказалась успешной.

SendRoutungInfoForLCS — сообщение протокола MAP, которое используется в сервисах, задействующих местоположение абонента, и служит для запроса маршрутной информации. При нормальном режиме функционирования это сообщение должно передаваться только между элементами своей сети. Ни одна из атак, основанных на методе SendRoutingInfoForLCS, не привела к получению данных об абоненте.

Нарушитель может использовать и другие методы атак с целью получения информации о местоположении абонента, например представленные на диаграмме ниже.

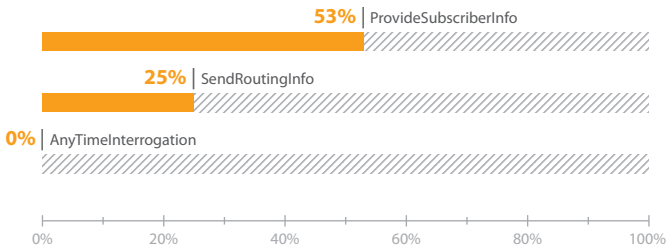

Рис. 9. Методы атак с целью получения информации о местонахождении абонента (доля успешных атак)

AnyTimeInterrogation — сообщение протокола MAP, которое используется узлами, реализующими логику интеллектуальных услуг, для запроса местоположения абонента. Данное сообщение используется исключительно внутри своей сети.

ProvideSubscriberInfo — сообщение протокола MAP, которое используется для получения информации о местоположении абонента в интересах различных сервисов. Не допускается прохождение запросов со стороны внешних подключений на абонентов своей сети.

Ни одна из атак методом AnyTimeInterrogation не оказалась успешной в осуществленных в 2015 году проектах. При этом в рамках каждой второй атаки (53%) было возможно получение информации о текущем местоположении абонента методом ProvideSubscriberInfo. Реализовать такую угрозу получилось практически в каждой сети SS7, лишь в двух сетях защита была эффективной.

Как было отмечено выше, половина атак с целью прослушивания входящих и исходящих звонков оказались успешными. В случае прослушивания входящих вызовов осуществлялась атака, основанная на применении метода подмены роумингового номера с переводом трафика на другой коммутатор. Прослушивание же исходящих вызовов осуществлялось методом InsertSubscriberData с переводом трафика на другой коммутатор.

InsertSubscriberData — сообщение протокола MAP, которое используется для изменения профиля абонента в базе данных VLR. Атакующий может заменить в профиле значение платформы для тарификации вызовов на адрес своего оборудования. В момент исходящего вызова мобильный коммутатор отправит запрос на продолжение вызова на указанный злоумышленником адрес. Злоумышленник должен отправить директиву на перенаправление вызова на подконтрольную ему АТС, затем перекоммутировать трафик на вызываемого абонента. Таким образом, разговор между двумя абонентами пойдет в открытом виде через АТС, полностью подконтрольную атакующему.

Для перехвата входящих SMS-сообщений был применен метод **UpdateLocation**. В 89% случаев атака оказалась успешной. UpdateLocation — сообщение, которое используется для запроса регистрации в зоне действия нового мобильного коммутатора (это сообщение приходит, в частности, из сети роуминг-партнера, когда абонент пытается произвести там регистрацию). Злоумышленник может зарегистрировать абонента в фальшивой сети, после чего все входящие SMS будут приходить на указанный им адрес.

4.1.2. Мошенничество

В каждой из систем были выявлены недостатки, позволяющие реализовывать мошеннические действия со стороны внешнего нарушителя. Примерами таких действий могут служить перенаправление вызовов, перевод денежных средств со счета абонента или изменение профиля абонента.

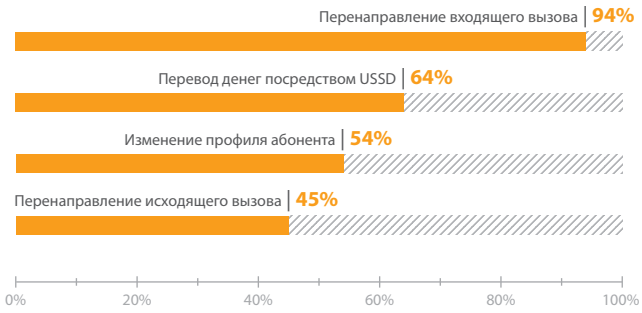

Рис. 10. Виды мошеннических действий (доля успешных атак)

Большинство атак (94%) с целью перенаправления входящих вызовов оказались успешны. При этом перенаправить исходящий вызов удалось лишь в 45% случаев. Столь высокий процент успешных атак свидетельствует о существенных проблемах, связанных с архитектурой протоколов и систем в уязвимых сетях SS7.

Для перенаправления исходящих вызовов применялся метод InsertSubscriberData. А атаки с целью перенаправления входящих вызовов осуществлялись с использованием двух методов — подмены роумингового номера и манипуляции с переадресацией.

Подмена роумингового номера осуществляется в момент входящего вызова на атакуемого абонента. Предварительно атакуемый абонент должен быть зарегистрирован в фальшивой сети. В ответ на запрос роумингового номера атакующий должен отправить номер для перенаправления вызова. Плата за установленное соединение ляжет на оператора.

Манипуляция с переадресацией — несанкционированная установка безусловной переадресации. Все входящие вызовы будут перенаправляться на указанный номер, а плата за них ляжет на абонента.

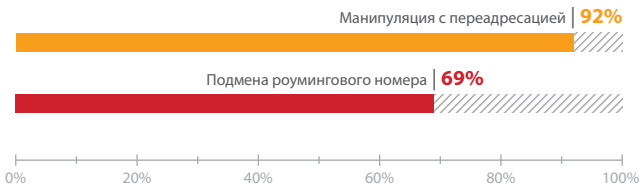

Рис. 11. Методы перенаправления входящего вызова (доля успешных атак)

Каждый из приведенных методов оказался эффективен; например, манипуляция с переадресацией для перенаправления вызова была проведена в 92% случаев. Реализация угрозы возможна вследствие уязвимостей, связанных с отсутствием проверки реального местоположения абонента. Данный недостаток безопасности оценивается специалистами Positive Technologies как критически опасный (в случае подмены роумингового номера) или как недостаток среднего уровня риска (в случае манипуляции с переадресацией).

Изменение профиля абонента возможно в каждой второй атаке, осуществленной методом InsertSubscriberData (54%).

4.1.3. Сбои в работе

Результаты исследования показали, что большинство исследованных сетей SS7 в той или иной мере подвержены недостаткам, позволяющим проводить атаки, направленные на отказ в обслуживании отдельных абонентов. В рамках всех проектов был использован метод UpdateLocation, в 80% случаев атаку удалось реализовать.

В результате осуществления атак на отказ в обслуживании нарушитель может вызвать сбои в работе сети для отдельных абонентов мобильного оператора, при этом не происходит нарушения доступности или ухудшения качества предоставления услуг для всех других абонентов. Таким образом нарушитель может проводить целенаправленные атаки.

4.2. Угрозы по регионам

Мы не приводим здесь подробную статистику по результатам оценки эффективности отдельных методов атак для каждого из регионов (EMEA и APAC), так как эти данные малоинформативны и могут нанести ущерб репутации отдельных операторов мобильной связи. В настоящем разделе приведены общие результаты, позволяющие показать, какие из классов угроз могут в той или иной мере быть реализованы в отношении сетей в каждом из регионов.

Например, абсолютно все методы атак с целью отказа в обслуживании абонента оказались успешны в сетях региона EMEA, и лишь в 71% случаев эти методы принесли результат в странах APAC.

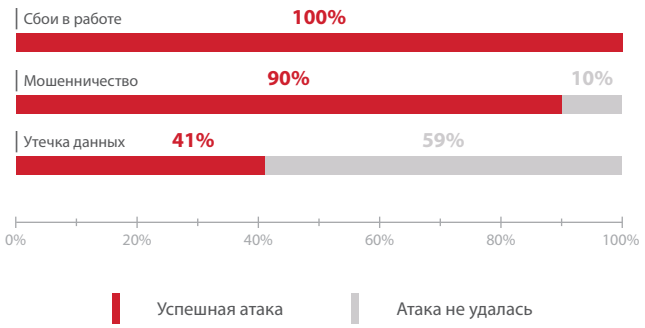

Рис. 12. Успех атак в регионе EMEA

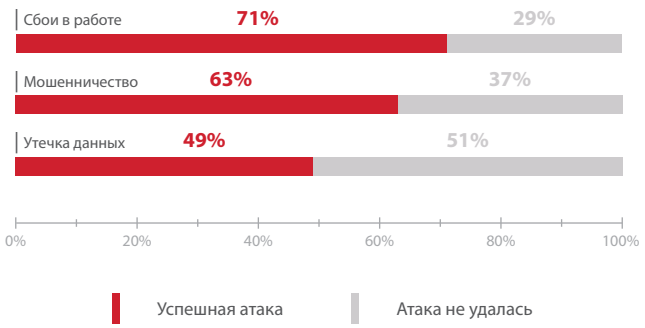

Рис. 13. Успех атак в регионе APAC

В целом данная угроза оказалась наиболее актуальной для обоих регионов. Предположительно это вызвано тем, что операторы мобильной связи уделяют большее внимание защите от атак, направленных на отказ в обслуживании сетей SS7 и сетевого оборудования, при этом не всегда обеспечивая на должном уровне защиту абонентов.

Наиболее опасной угрозой, рассматриваемой в рамках данного исследования, можно назвать мошенничество. Успешная ее реализация может напрямую привести к финансовым потерям, например в случае перевода денежных средств со счетов абонентов, а также к потере репутации надежного провайдера услуг. В регионе EMEA практически все методы атаки с целью совершения мошеннических действий оказались успешны (90%). Этот факт подтверждает сделанный ранее вывод о недостаточном внимании операторов мобильной связи к архитектурным проблемам используемых протоколов и систем.

На рис. 14 показано соотношение успешно реализованных атак — в случае если в рамках атаки по крайней мере один из использованных методов оказался эффективен. Так как некоторые атаки могут быть реализованы разными методами, атака считалась успешной, если сработал по крайней мере один из них.

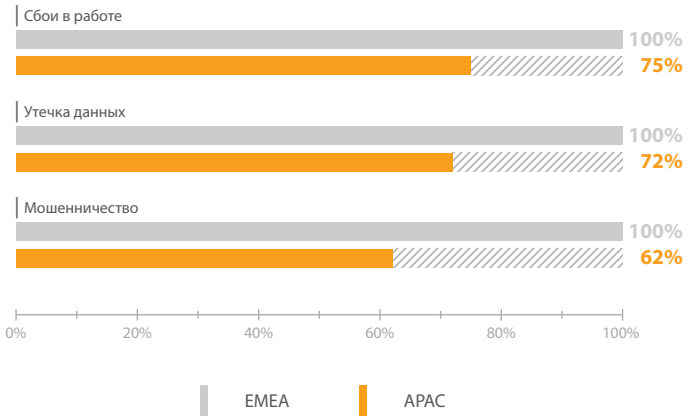

Рис. 14. Доли успешно реализованных угроз для каждого региона

К примеру, атака с целью реализации угрозы утечки данных (с использованием тех или иных методов) оказалась успешна во всех сетях региона EMEA в отношении всех участвовавших в тестах абонентов, и лишь в 75% случаев такие атаки принесли результат в сетях SS7 стран APAC.

Выборка невелика, и эти данные не позволяют, возможно, делать общие выводы относительно всех операторов мобильной связи стран EMEA. Тем не менее результаты исследования подтверждают, что только комплексный подход к защите сетей SS7 может минимизировать существующие риски. Если реализовать защиту только от определенного типа атак, нарушитель может использовать комбинацию других методов — и с высокой долей вероятности добиться поставленной цели.

4.3. Угрозы по объему абонентской базы оператора

При рассмотрении проблем сетей SS7 в зависимости от количества абонентов были сделаны следующие выводы:

+ крупные операторы уделяют больше внимания защите сетей от всех рассмотренных классов угроз;
+ чем меньше объем абонентской базы оператора, тем менее защищены его абоненты от атак с целью мошеннических действий;
+ ни один из операторов — вне зависимости от величины его абонентской базы — не обеспечивает должный уровень защиты своих абонентов от атак со стороны внешнего нарушителя.

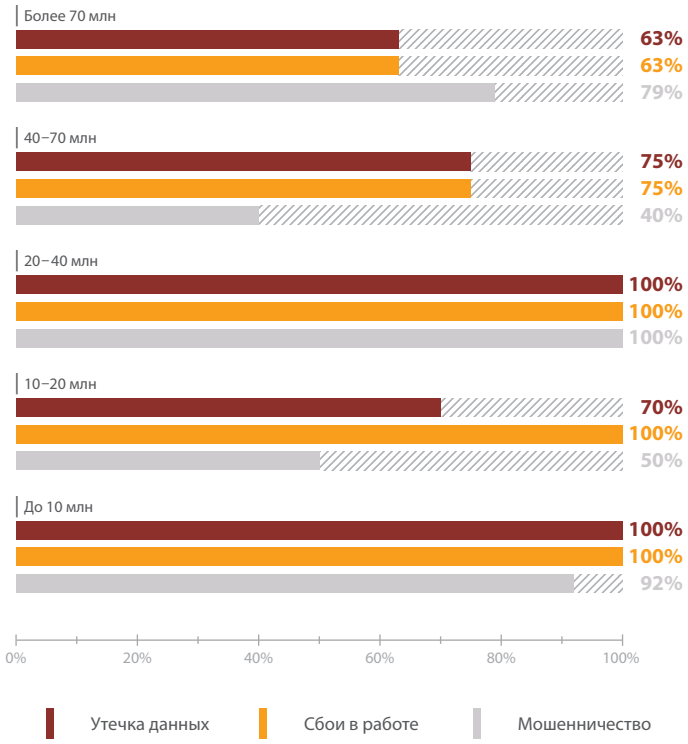

Рис. 15. Доля успешных атак в зависимости от реализуемой угрозы для различных категорий операторов

Полученные результаты можно объяснить тем, что более крупные операторы мобильной связи, как правило, обладают достаточным бюджетом для внедрения различных механизмов и систем для обеспечения защиты сети SS7 от атак. Стоимость подобных средств защиты часто слишком велика для небольших операторов, поэтому уровень защищенности их сетей существенно ниже. Однако доля успешных атак, реализующих каждый из классов угроз, столь велика для всех типов сетей, что говорить о достаточном уровне защиты не приходится даже в случае крупных операторов, которые являются лидерами рынка в своем регионе.

4.4. Рекомендуемые меры для защиты

Согласно с основными тремя категориями уязвимостей сетей SS7 можно выделить три основных механизма защиты:

- настройки конфигурации,
- внедрение дополнительных средств защиты,
- комбинацию этих двух методов.

Большинство недостатков, позволяющих определить местоположение абонента, а также реализовать кражу данных, могут быть устранены в результате изменения конфигурации сетевого оборудования. Например, если установить запрет на обработку сообщений AnyTimeInterrogation и SendIMSI на HLR.

Архитектурные проблемы протоколов и систем, позволяющие осуществлять отказ в обслуживании, перехват SMS-сообщений, перенаправление вызовов и прослушивание звонков, а также изменение профиля абонента, могут быть решены путем фильтрации нежелательных сообщений (таких как SendIMSI, SendRoutungInfoForLCS, SendRoutingInfo). Однако не все подобные сообщения бывают опасны; при фильтрации абсолютно всех таких сообщений или при некорректных настройках фильтрации с высокой долей вероятности может быть нарушена работа легальных сервисов сотового оператора. Необходимо реализовать фильтрацию таким образом, чтобы отсекались только нежелательные сообщения, используемые в рамках атак. Для этого рекомендуется внедрять дополнительные средства защиты, например программно-аппаратные комплексы класса IDS SS7. Подобные системы не влияют на трафик сети, однако при этом позволяют выявлять действия нарушителя и определять настройки фильтрации сообщений, необходимые для предотвращения атак.

Наиболее эффективный способ противостояния всем перечисленным в исследовании типам атак — это комбинация названных методов (в том числе в тех случаях, когда причиной возникновения уязвимости являются ошибки в используемом ПО).

Описанные варианты защиты наиболее эффективны в том случае, когда в компании — операторе мобильной связи налажен эффективный процесс внутреннего аудита безопасности сетей SS7. Однако не каждый оператор связи, особенно обладающий сравнительно небольшой абонентской базой, может обеспечить такой аудит на должном уровне. В таких случаях необходимо регулярно проводить аудит сетей мобильной связи с привлечением сторонних специализированных организаций. Это позволит объективно определить текущий уровень защищенности, выявить существующие угрозы безопасности и минимизировать существующие риски, приняв своевременные меры по устранению уязвимостей.

Заключение

Уровень защищенности сетей SS7 всех исследованных операторов мобильной связи оказался крайне низок. В отношении каждой сети SS7 могли быть успешно реализованы атаки, связанные с утечкой данных, нарушениями в работе сети и мошенническими действиями.

Как показало исследование, телекоммуникационные компании используют различные меры защиты, но их явно недостаточно, чтобы компенсировать весь спектр методов, которые могут применять потенциальные нарушители. Абоненты даже крупных операторов связи не защищены от несанкционированного прослушивания звонков, перехвата SMS-сообщений, перенаправления вызовов и хищения денежных средств со счета. Кроме того, нарушители могут в любой момент определить текущее местонахождение абонента.

Для снижения рисков необходим комплексный подход к защите инфраструктуры SS7. Рекомендуется регулярно (дважды в год) проводить аудит безопасности сигнальной сети. На основании информации о недостатках и уязвимостях, выявленных в рамках аудита, следует разрабатывать меры по минимизации соответствующих рисков. Для выявления и своевременного предотвращения атак, основанных на эксплуатации уязвимостей архитектуры протоколов и систем, важно также использовать дополнительные средства защиты. К примеру, система выявления атак класса IDS SS7 может обеспечить мониторинг трафика на стыках сигнальных сетей, обнаружение и блокирование попыток технологического фрода. Подобная стратегия успешно себя зарекомендовала в сетях ряда крупнейших операторов мобильной связи.

Источники

1. Уязвимости сетей мобильной связи на основе SS7
www.ptsecurity.ru/download/PT_SS7_security_2014_rus.pdf

2. Атаки на SS7: вчера для спецслужб, сегодня для всех
habrahabr.ru/company/pt/blog/237981

3. Уязвимости мобильного интернета (GPRS)
www.ptsecurity.ru/download/GPRS%20security.pdf

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

5. How to Cheat at VoIP Security — Thomas Porter, Michael Gough
goo.gl/dxQfgs

6. What Happens When the Surveillance State Becomes an Affordable Gadget? — Роберт Колкер, Bloomberg Businessweek
goo.gl/weqptW

7. Special Investigation: Bugged, Tracked, Hacked
www.9jumpin.com.au/show/60minutes/stories/2015/august/phone-hacking

8. SS7 Phone-Switch Flaw Enabled Surveillance
schneier.com/blog/archives/2015/08/ss7_phone-switc.html

9. New documents show how the NSA infers relationships based on mobile location data — Ashkan Soltani and Barton Gellman, The Washington Post
goo.gl/cCmlzn

10. Locating Mobile Phones using Signalling System #7 — Tobias Engel
events.ccc.de/congress/2008/Fahrplan/attachments/1262_25c3-locating-mobile-phones.pdf

11. Can they hear you now? Hacking Team & SS7
adaptivemobile.com/blog/can-they-hear-you-now-hacking-team-ss7

12. Unblocking Stolen Mobile Devices Using SS7-MAP Vulnerabilities
goo.gl/dveK7Y

О компании

Positive Technologies — лидер европейского рынка систем анализа защищенности и соответствия стандартам. Деятельность компании лицензирована Минобороны РФ, ФСБ и ФСТЭК, продукция сертифицирована «Газпромом» и ФСТЭК. Более 3000 организаций из 30 стран мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телекомов. В 2013 году компания заняла третье место на российском рынке ПО для безопасности и стала лидером по темпам роста на международном рынке систем управления уязвимостями. В 2015 году Gartner назвал Positive Technologies «визионером» в своем рейтинге Magic Quadrant for Web Application Firewalls.

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.ru