УЯЗВИМОСТИ МОБИЛЬНОГО ИНТЕРНЕТА (GPRS)

Дмитрий Курбатов
Сергей Пузанков
Павел Новиков

POSITIVE TECHNOLOGIES

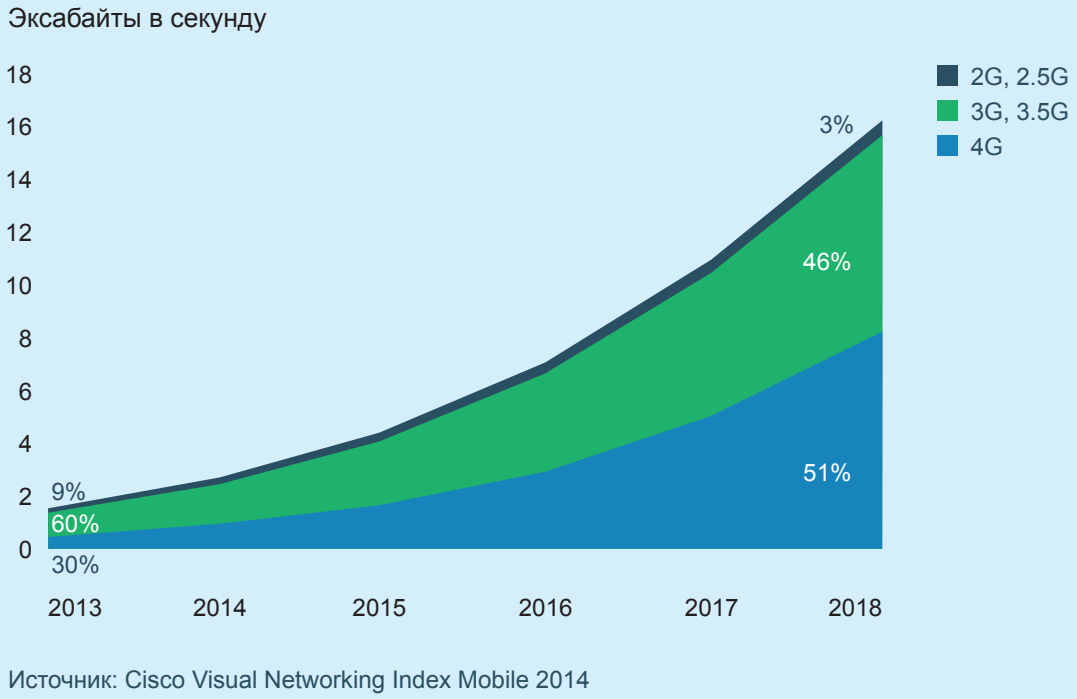
2014

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ

Современные сети мобильной связи позволяют своим абонентам использовать Интернет максимально удобным способом, без привязки к определенным помещениям и статичным инфраструктурам. Почтой, мессенджерами, социальными сетями и электронными магазинами человек может теперь пользоваться в любое время и практически в любом месте, где он окажется. Крупный бизнес использует мобильный Интернет для удаленного администрирования, финансовых операций, электронной торговли, M2M и других целей. Государственные организации предоставляют гражданам все больше услуг через Интернет. Все это ведет к значительному увеличению мобильного трафика в мире.

Многие уже научились с осторожностью пользоваться классическим кабельным Интернетом, тем более что для этой сферы предложено множество защитных решений — антивирусы, межсетевые экраны и др. Но что касается мобильного Интернета, уровень сознательности пользователей очень низок. Большинство абонентов считают, что работа через сотовую сеть достаточно безопасна, ведь крупный оператор связи наверняка позаботился о защите. Увы, на практике в мобильном Интернете есть множество возможностей для злоумышленников. В данном отчете мы предлагаем анализ этих угроз, а также рекомендации по обеспечению безопасности мобильных интернет-услуг.



Источник: Cisco Visual Networking Index Mobile 2014

Рис. 1. Ожидаемый рост объемов мобильного трафика [1]

2. РЕЗЮМЕ

В результате наших исследований выяснилось, что значительное количество устройств, принадлежащих 2G/3G-сетям мобильных операторов, доступны через Интернет благодаря открытым GTP-портам, а также другим открытым протоколам передачи данных (FTP, Telnet, HTTP). Используя уязвимости в этих интерфейсах (например, стандартные пароли), злоумышленник может подключиться к узлу оператора мобильной связи.

При этом всякий, кто получил доступ к сети любого оператора, автоматически получает доступ к сети GRX, которая объединяет всех сотовых операторов и используется для предоставления доступа к Интернету абонентам в роуминге. Таким образом злоумышленник получает возможность проводить различные атаки на абонентов любого оператора:

- поиск валидных идентификаторов абонентов (IMSI);
- получение данных об абоненте по заданному IMSI (включая его местоположение);
- отключение абонентов от Интернета или блокировка их доступа к нему;
- подключение к Интернету под видом другого абонента и за чужой счет;
- подслушивание трафика жертвы, фишинг.

Необходимые для защиты от таких атак меры безопасности включают правильную настройку оборудования, использование межсетевых экранов и периодический мониторинг защищенности. Рекомендуемый комплекс защитных мероприятий более подробно описан в заключительной части данного обзора.

3. СХЕМА МОБИЛЬНОЙ СЕТИ

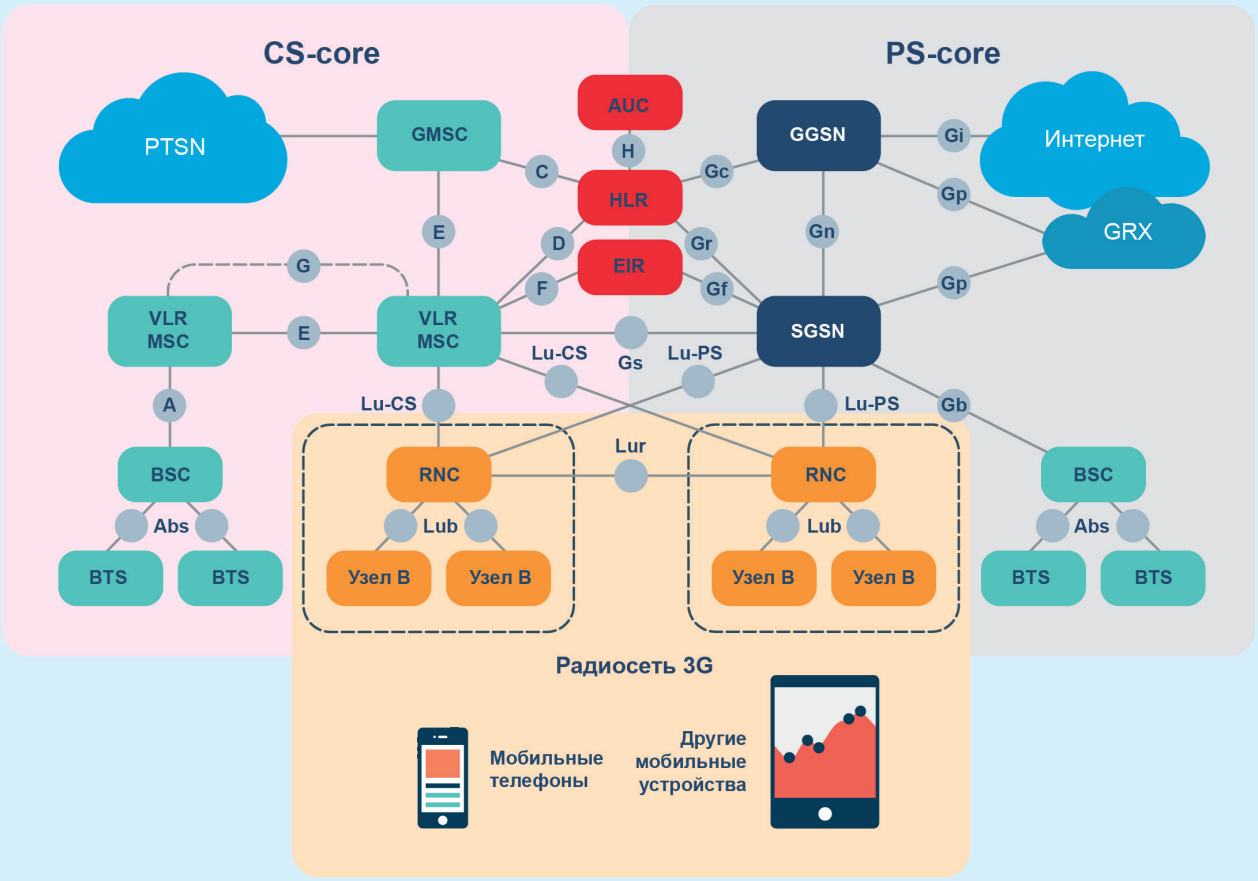


Рис. 2. Сеть оператора сотовой связи

Сеть оператора сотовой связи состоит из опорной сети с коммутацией каналов Circuit Switched Core Network (CS-core), опорной сети передачи пакетных данных Packet Switched Core Network (PS-core), сети базовых станций и их контроллеров 2G (BSC и BTS на схеме), сети базовых станций и их контроллеров 3G (Node B и RNC). На схеме видно, что сеть 3G является надстройкой над сетью 2G на уровне радиосети, остальная часть сети оператора не претерпела значительных изменений при эволюции в третье поколение.

Нас интересует подсистема передачи пакетных данных (PS-core, рис. 3).

Основными элементами для передачи данных являются Service GPRS Support Node (SGSN) и Gateway GPRS Support Node (GGSN). Первый служит для предоставления абонентам услуг передачи данных и взаимодействует с остальными элементами сотовой сети, второй же является своеобразным шлюзом из внутренней сети оператора в сеть Интернет.

Кроме соединения с Интернетом, есть подключение к сети GRX, или Global Roaming eXchange, которая объединяет всех сотовых операторов и используется для предоставления доступа к интернету абонентам в роуминге.

Данная схема отражает архитектуру системы передачи данных в сети второго поколения (2G). В третьем поколении (UMTS) имеются отличия в цепочке между мобильной станцией (MS) и узлом SGSN. На схеме видно, что проникнуть в сеть оператора можно:

- со стороны мобильной станции абонента,
- со стороны Интернета,
- через сеть GRX, то есть через другого оператора.

Таким образом, если злоумышленник проникнет в сеть любого оператора в мире, то сможет воздействовать и на работу других операторов.

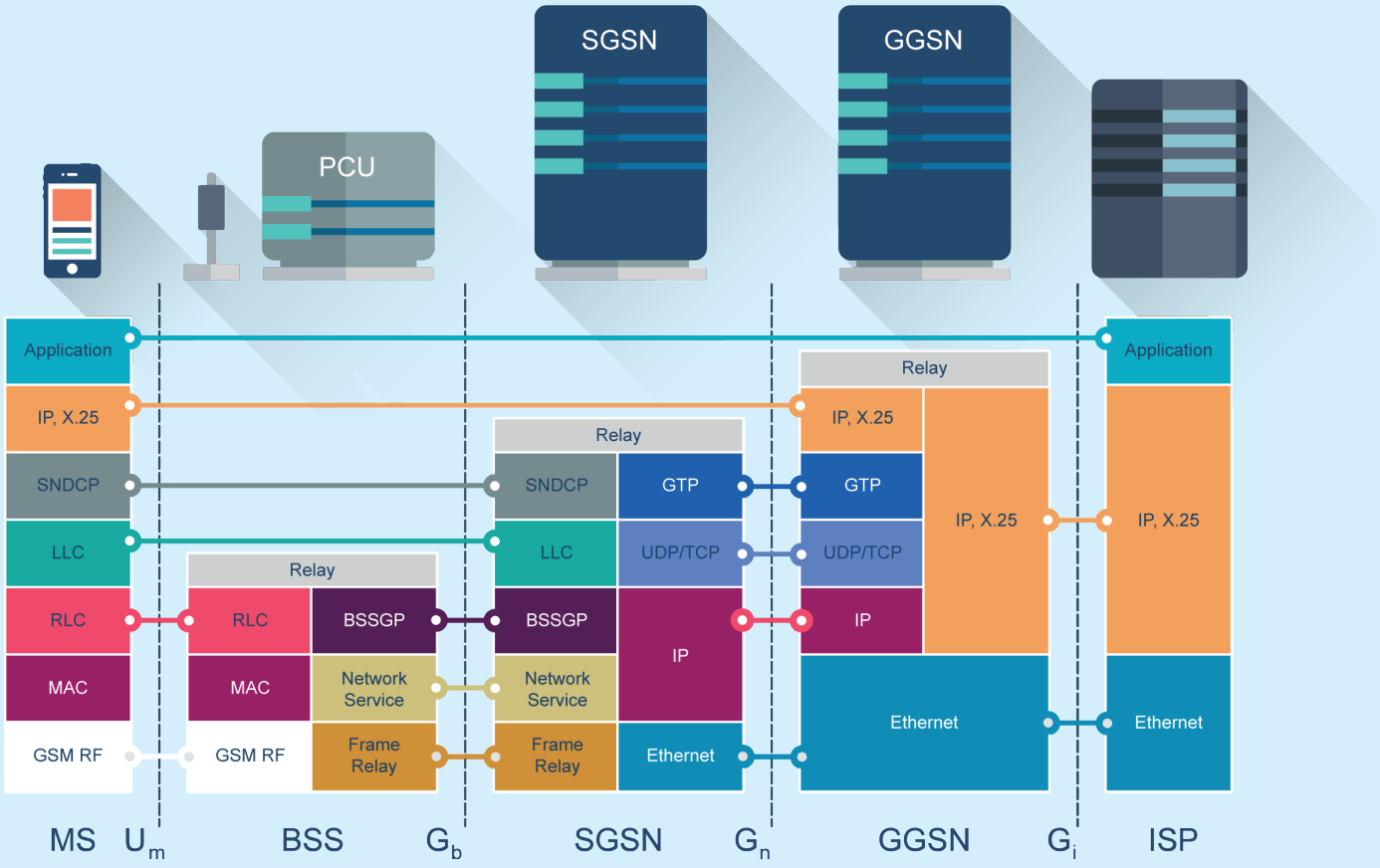


Рис. 3. Схема передачи пакетных данных в мобильных сетях (с указанием протоколов)

4. ПРОТОКОЛ GTP

Для передачи трафика внутри PS-core и GRX используется протокол GTP (см. рис. 4). Это протокол туннелирования, работает поверх протокола UDP и использует порты 2123 (для управления, GTP-C), 2152 (для передачи пользовательских данных, GTP-U), 3386 (для биллинга, GTP').

Поле Message Type преимущественно используется для управления в GTP-C, в GTP-U обычно Message Type = 0xFF (T-PDU).

TEID — идентификатор туннеля, который не сопоставляется с IP-адресом, т.е. отправителем пакетов с одним TEID в разное время могут быть разные адреса (в случае если абонент перемещается и переключается на другие SGSN).

При подключении абонента к Интернету выполняется процедура PDP Context Activation.

В упрощенном виде эта процедура выглядит следующим образом (см. рис. 5). Телефон отправляет на SGSN запрос активации контекста, в котором, в числе прочего, присутствуют логин, пароль и APN (адрес точки доступа). Узел SGSN, получив APN, пытается разрешить его на внутреннем DNS-сервере. Сервер разрешает предоставленный APN и возвращает адрес GGSN, отвечающего за данный APN. По этому адресу SGSN отсылает запрос на создание PDP-контекста. GGSN проверяет на RADIUS-сервере предоставленные логин и пароль. Затем получает IP-адрес для телефона и всю необходимую для активации PDP-контекста информацию передает обратно на SGSN. Узел SGSN завершает процедуру активации, отсылая на телефон данные, необходимые для установления соединения.

По сути процедура PDP Context Activation — это создание GTP-туннеля между телефоном и шлюзом в операторской сети.

Октеты	8	7	6	5	4	3	2	1
1	Version			PT	(*)	E	S	PN
2	Message Type							
3	Length (первый октет)							
4	Length (второй октет)							
5	Tunnel Endpoint Identifier (первый октет)							
6	Tunnel Endpoint Identifier (второй октет)							
7	Tunnel Endpoint Identifier (третий октет)							
8	Tunnel Endpoint Identifier (четвертый октет)							
9	Sequence Number (первый октет)[1) 4)]							
10	Sequence Number (второй октет)[1) 4)]							
11	N-PDU Number[2) 4)]							
12	Next Extension Header Type[3) 4)]							

(*) Данный бит зарезервирован как запасной. Он всегда равен 0, анализировать его значение не имеет смысла.
1) Значение поля релевантно, только если флаг S равен 1.
2) Значение поля релевантно, только если флаг PN равен 1.
3) Значение поля релевантно, только если флаг E равен 1.
4) Данное поле добавляется к заголовку, только если установлен хотя бы один из флагов S, PN или E.

Рис. 4. Структура заголовка GTP

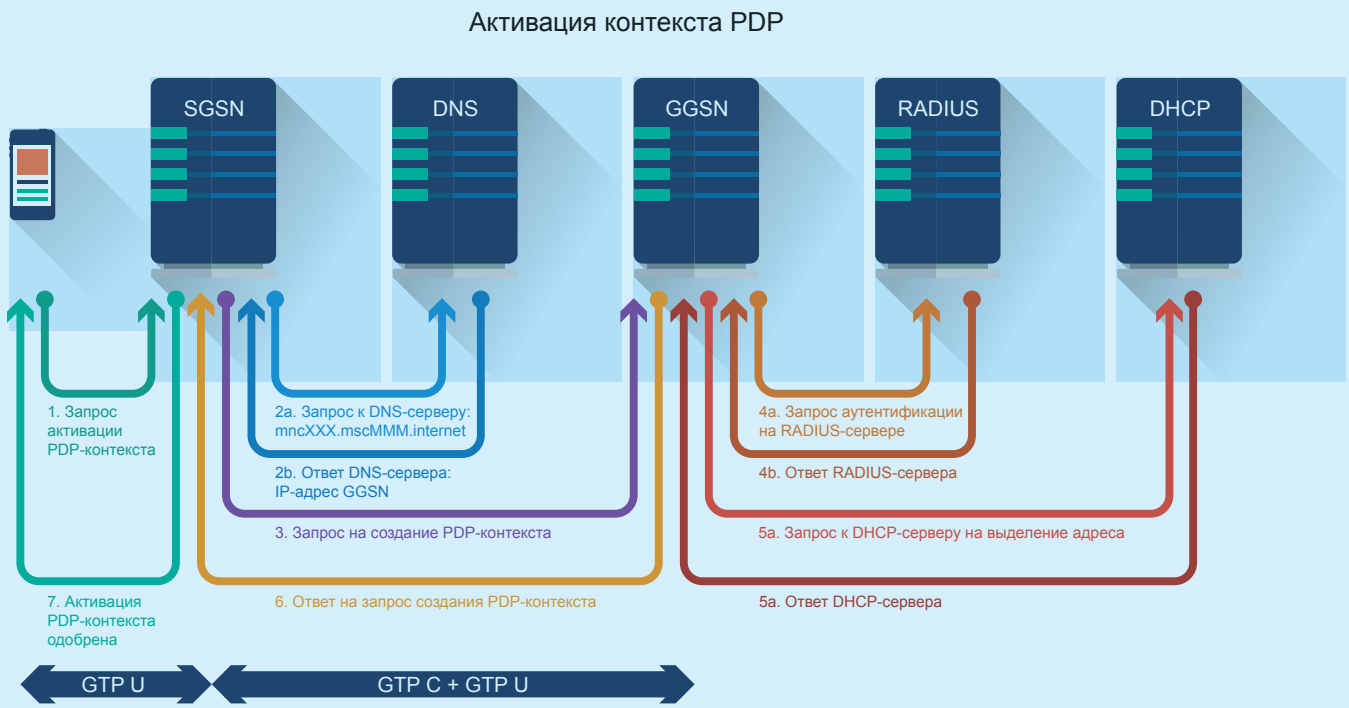


Рис. 5. Процедура установления соединения

5. ПОИСК ОБОРУДОВАНИЯ МОБИЛЬНЫХ ОПЕРАТОРОВ В ИНТЕРНЕТЕ

Мы уже знаем, что граничным устройством в сети должен быть GGSN. Воспользовавшись сервисом Shodan.io, который предназначен для поиска промышленных систем управления с интернет-доступом, мы можем найти нужные нам устройства по баннерам.

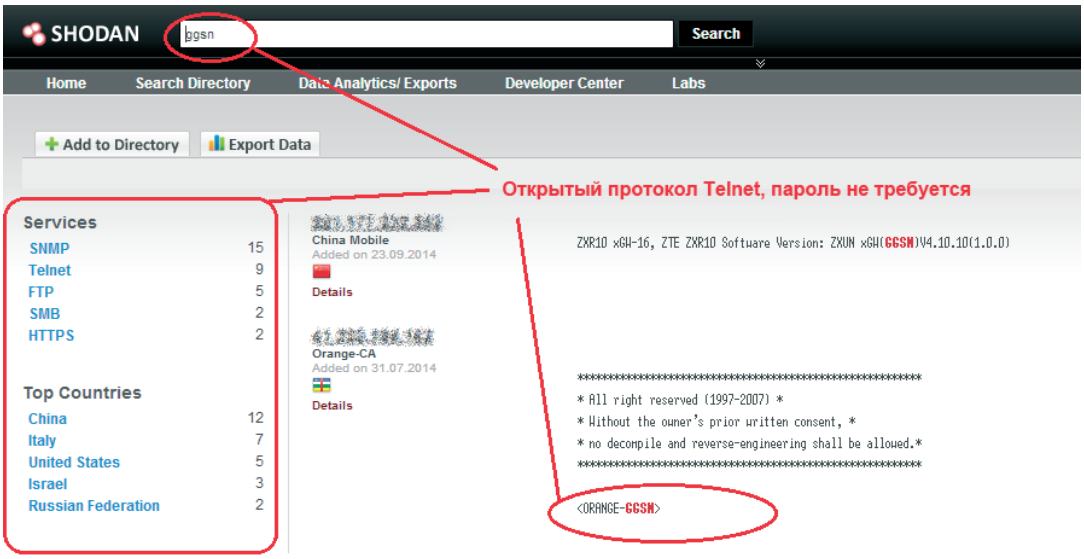


Рис. 6. Результаты поиска в Shodan

Результат поиска — около 40 устройств, содержащих данную аббревиатуру в баннерах. На рисунке приведены несколько таких устройств, в том числе с открытым Telnet и отключенным паролем. Злоумышленнику достаточно подключиться к данному устройству и произвести в нем необходимые настройки для того, чтобы оказаться внутри сети оператора в Центральноафриканской Республике.

Имея доступ к сети любого оператора, злоумышленник автоматически получает доступ к сети GRX и к другим операторам. Единичная ошибка в конфигурации на одном устройстве у единственного оператора в мире представляет опасность для многих других сотовых сетей. Есть множество вариантов использования скомпрометированного пограничного узла, например подмена DNS (подробнее об атаках см. ниже).

Узлы GGSN и SGSN можно найти и другими способами. Протокол GTP, описанный выше, должен использоваться только внутри сети PS-core и GRX и никаким образом не должен быть «виден» со стороны Интернета. Но на практике это часто не так: в Интернете имеется более 207 тысяч устройств по всему земному шару с открытыми GTP-портами.

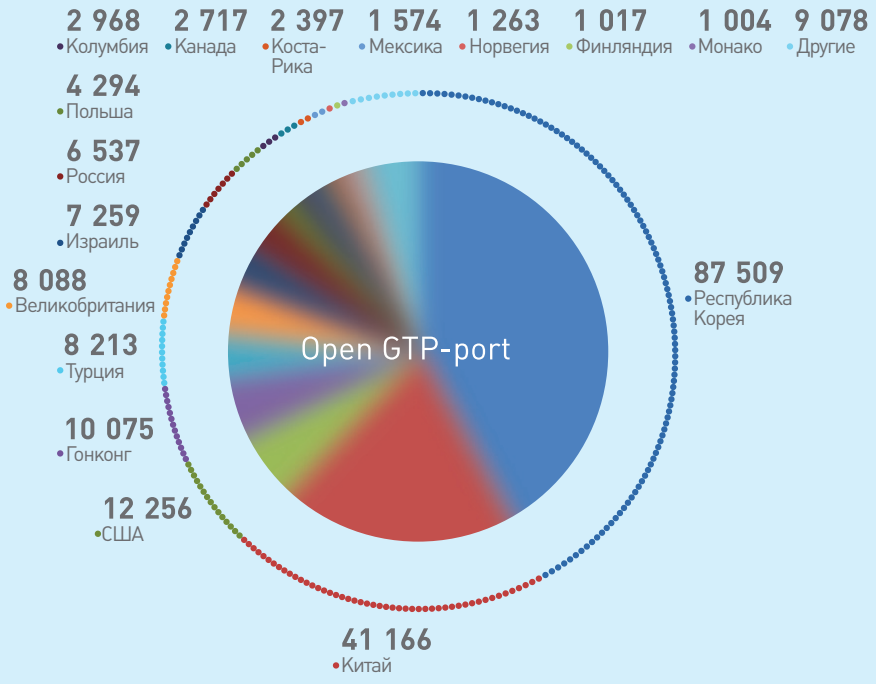


Рис. 7. Страны с наибольшим количеством узлов, имеющих открытые GTP-порты (более 1000)

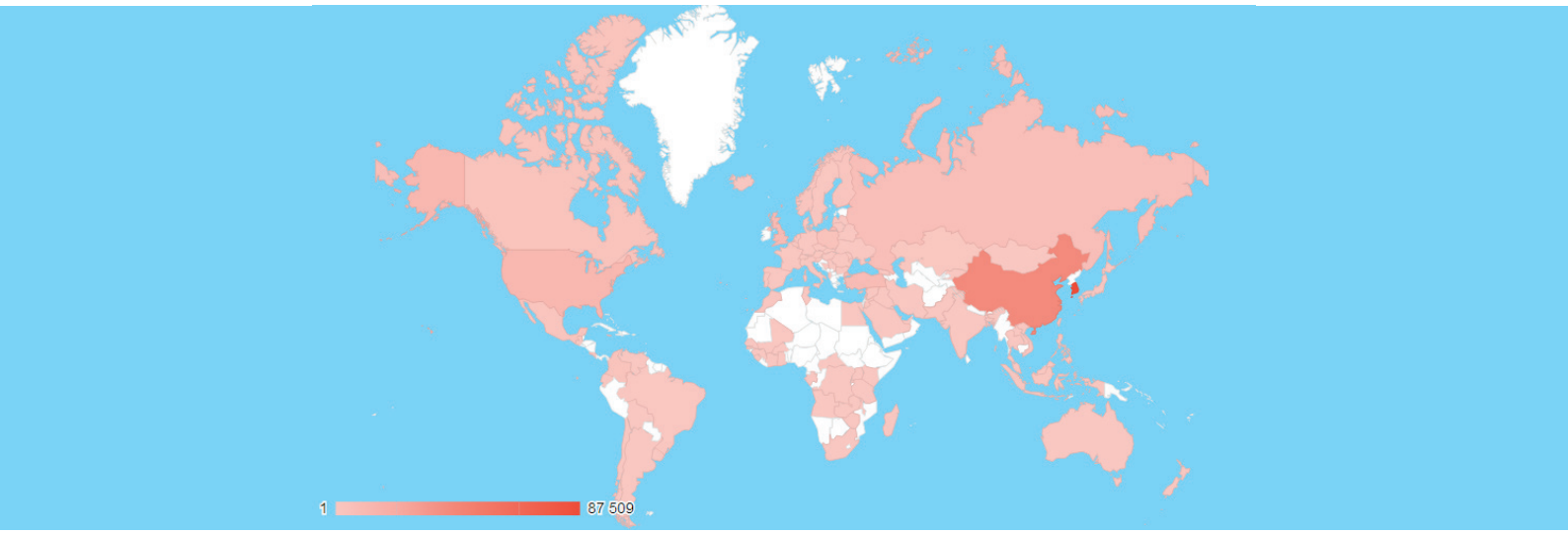


Рис. 8. Распределение узлов с открытыми GTP-портами по миру

Что представляют собой найденные 207 тысяч устройств? 7255 из них не имеют никакого отношения к GTP и отвечают HTTP-ответами (см. рис. 9).

Остальные адреса (около 200 тысяч) отвечают корректными GTP-сообщениями. Однако более глубокий анализ показал, что зачастую отдельно взятое устройство не является компонентом сотовой сети: это универсальные устройства, используемые для иных целей, но администраторы конкретных сетей попросту не выключили на них данную функцию. Часто среди таких устройств попадаются Alcatel-Lucent 7750 и ZTE ZXUN xGW, причем у второго обычно открыты порты FTP и Telnet.

548 устройств отвечают на запрос об установлении соединения: 4 из них позволяют создать туннель, другие отвечают различными ошибками (рис. 10).

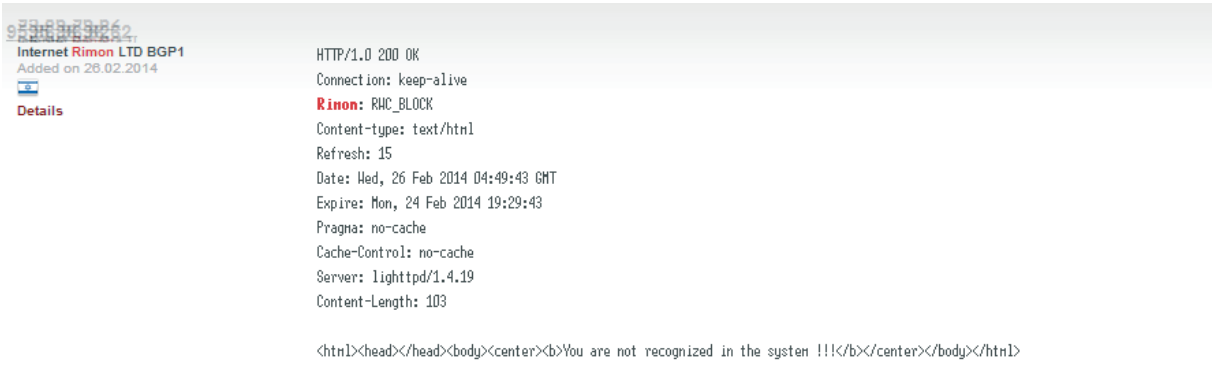


Рис. 9. Ответ на GTP-запрос от оборудования компании Internet Rimon LTD

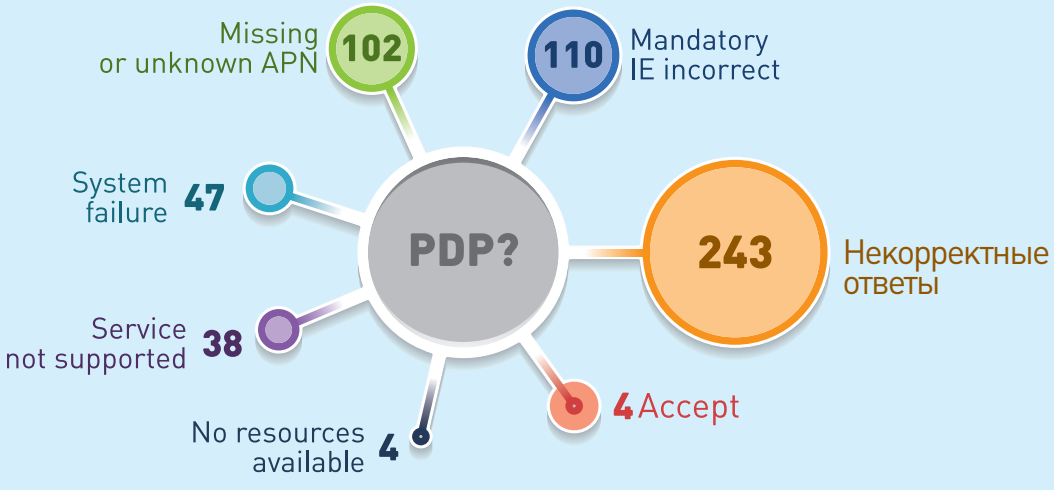


Рис. 10. Ответы на попытку установления PDP-соединения

Попробуем разобраться в ответах.

Ответы System failure и Mandatory IE incorrect означают, что в запросе не были заполнены необходимые для данного узла поля GTP-пакета.

Ответ No resources available означает, что у узла закончился DHCP-пул, либо PDP-пул.

Ответы Missing or unknown APN и Service not supported означают, что используемый APN не попадает в список разрешенных (найти подходящие APN достаточно просто на сайтах самих операторов в настройках Internet, WAP, MMS).

Ответ Accept означает, что устройство выдает IP-адрес и другие атрибуты соединения, т.е. создается туннель.

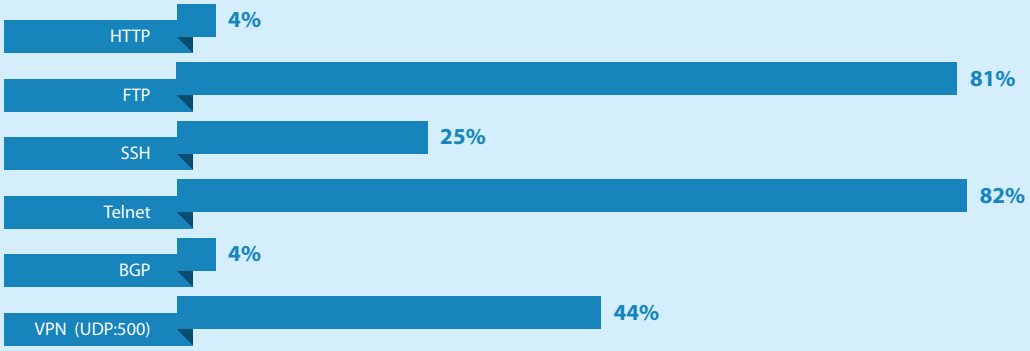


Рис. 11. Количество узлов с различными сервисами

Итак, злоумышленник из сети Интернет может найти подходящий GGSN, установить GTP-соединение, а затем инкапсулировать в созданный туннель управляющие пакеты GTP. При правильном подборе параметров GGSN воспримет их как пакеты от легитимных устройств сети оператора.

Еще одна возможность для атак связана с тем, что GTP — далеко не единственный протокол управления на найденных узлах. Также встречаются Telnet, FTP, SSH, Web и др. Выше приведены данные о том, сколько найдено открытых портов для каждого протокола.

Согласно статистике Positive Technologies по результатам тестов на проникновение [2], использование открытых протоколов передачи данных (FTP, Telnet, HTTP) и доступность интерфейсов управления из сети Интернет — входят в список наиболее частых уязвимостей на сетевом периметре информационных систем крупных компаний. Причем в 2013 году распространение этих уязвимостей выросло в два раза по сравнению с 2011—2012 годами.

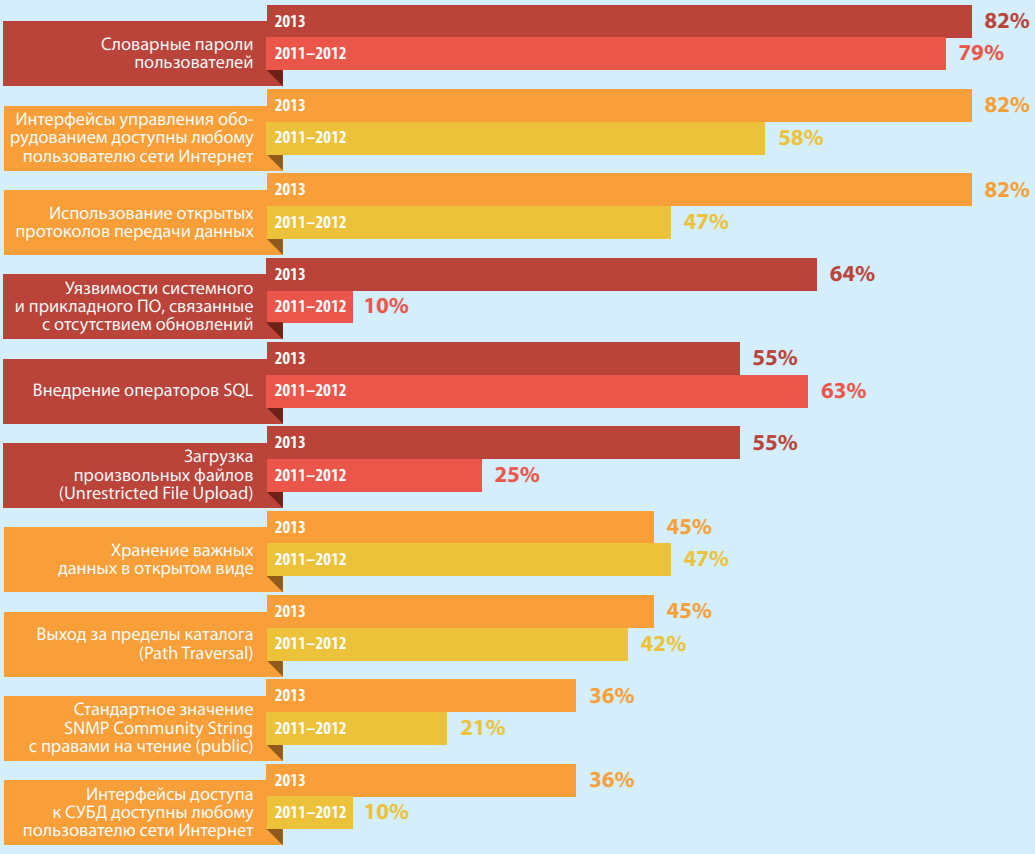


Рис. 12. Наиболее распространенные уязвимости на сетевом периметре

6. УГРОЗЫ

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

6.1. ПЕРЕБОР IMSI

Цель: поиск валидных IMSI.

Вектор атаки: злоумышленник действует через сеть GRX или из сети оператора.

Описание. IMSI — это номер абонента, запрограммированный в SIM-карте. Состоит из 15 цифр, первые 3 цифры это MCC (Mobile Country Code) — мобильный код страны. Еще две цифры это MNC (Mobile Network Code) — код мобильной сети. На сайте mcc-mnc.com можно выбрать интересующего нас оператора, подставить нужные MCC и MNC, а затем прямым перебором подобрать остальные 10 цифр путем посылки сообщения «Send Routeing Information for GPRS Request» через сеть GRX. Данное сообщение можно передавать на любое GSN-устройство, а оно преобразует данный запрос в формат сети SS7 (компонент сети CS-core), отправляет на HLR, и далее такой запрос обрабатывается сетью SS7. В случае если абонент с данным IMSI пользуется Интернетом — получим IP-адрес SGSN, обслуживающий данного абонента. Иначе ответ будет следующим: «Mobile station Not Reachable for GPRS».

Результат. Получение списка валидных IMSI для осуществления дальнейших атак.

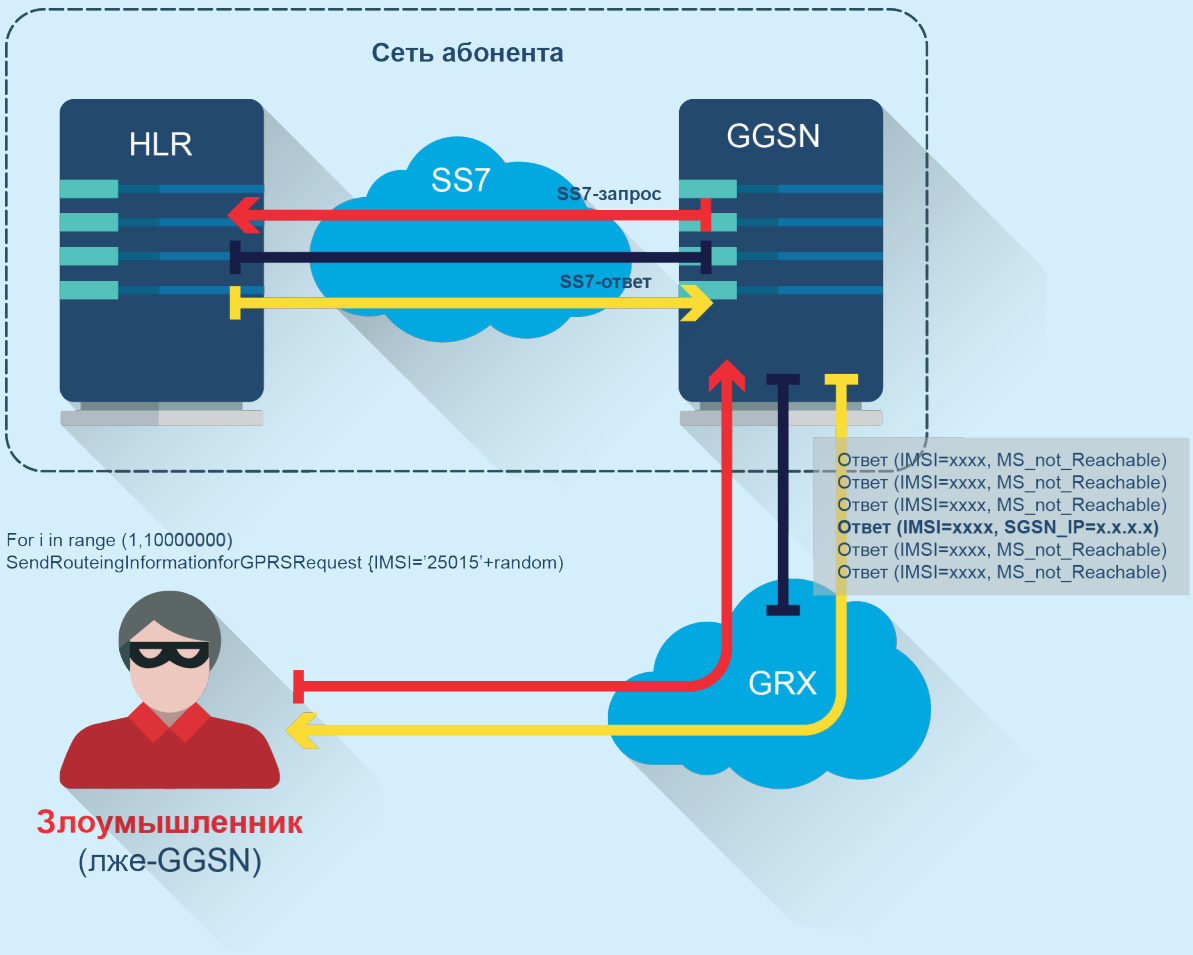


Рис. 13. Схема атаки

6.2. РАСКРЫТИЕ ДАННЫХ АБОНЕНТА ПО IMSI

Цель: получение номера телефона, данных о местоположении, модели мобильного устройства абонента по IMSI.

Вектор атаки: злоумышленник действует через сеть GRX или из сети оператора.

Описание. Можно использовать после успешного завершения предыдущей атаки либо заранее зная IMSI абонента, например через вирусное приложение для смартфона абонента. Сначала требуется узнать IP-адрес обслуживающего SGSN с помощью все той же предыдущей атаки. Затем на IP-адрес обслуживающего SGSN отправляется запрос «Update PDP Context Request» с запросом о местоположении абонента и подмененным на свой IP-адрес «GSN Control Plane», в ответе будет содержаться MSISDN (номер телефона абонента), IMEI — идентификационный номер мобильного устройства (по нему можно узнать модель телефона абонента), а также местоположение с точностью до базовой вышки (MCC, MNC, LAC, CI). Затем с помощью сайта xinit.ru/bs/ можно узнать местоположение абонента с точностью до нескольких сотен метров.

Результат. Получение конфиденциальных данных об абоненте.

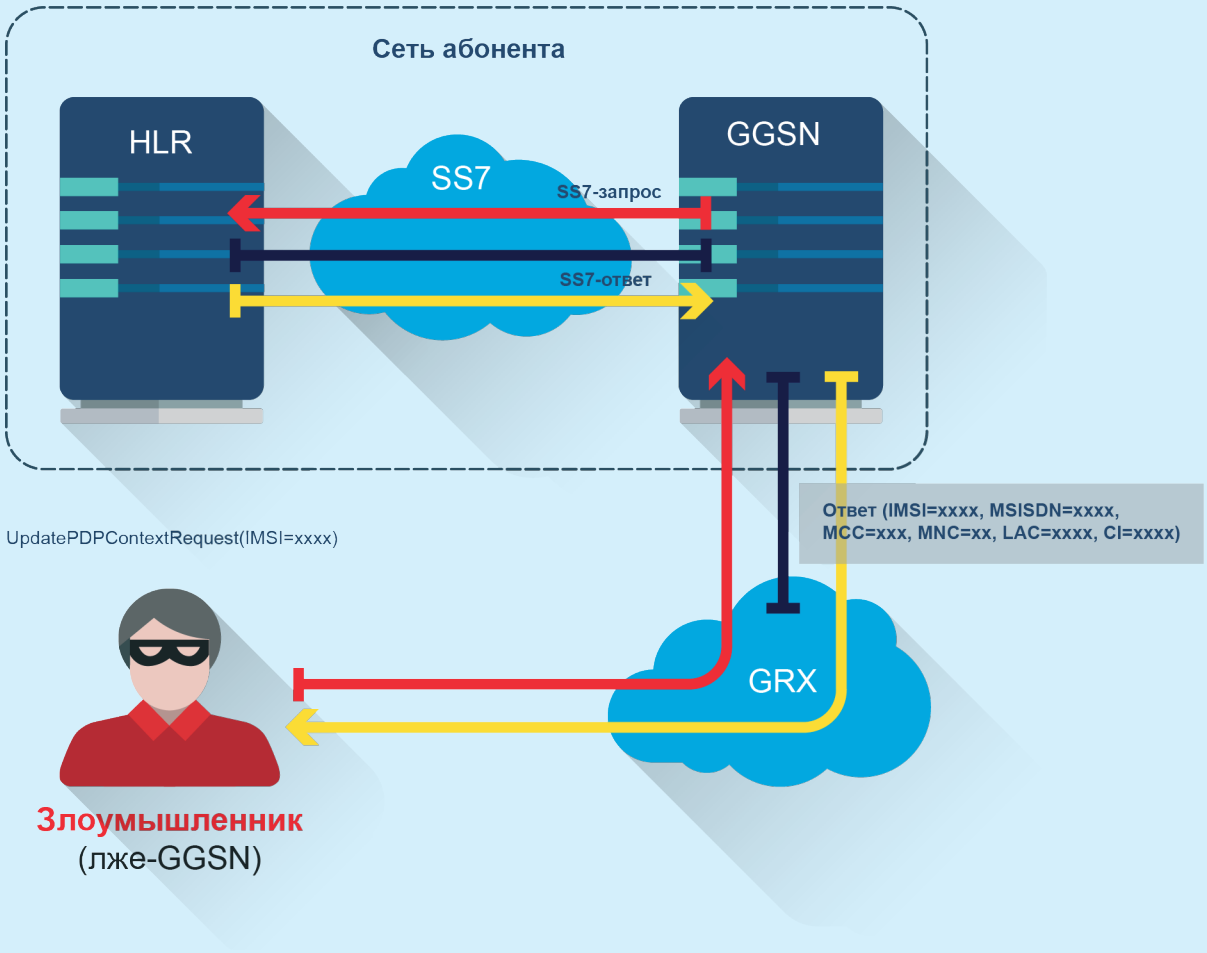


Рис. 14. Схема атаки

6.3. ОТКЛЮЧЕНИЕ ЛЕГИТИМНЫХ АБОНЕНТОВ ОТ СЕТИ ИНТЕРНЕТ

Цель: отключение от сети уже подключенных абонентов.

Вектор атаки: злоумышленник действует через сеть GRX или из сети оператора.

Описание. Атака основывается на отправке пакетов «PDP context delete request» на целевой GGSN с перечислением всех TEID, в результате все PDP Context удаляются и валидные абоненты отключаются от сети Интернет.

При этом GGSN в одностороннем порядке закрывает туннели, а ответы по этому событию отправляет злоумышленнику. А валидный SGSN, через который подключался абонент, ничего «не знает» о закрытии соединений, и туннели продолжают занимать ресурсы оборудования. У абонента просто перестает работать Интернет, но соединение отображается как активное.

Результат. Все подключенные к данному GGSN абоненты будут отключены. К одному GGSN подключаются все пользователи макрорегиона.

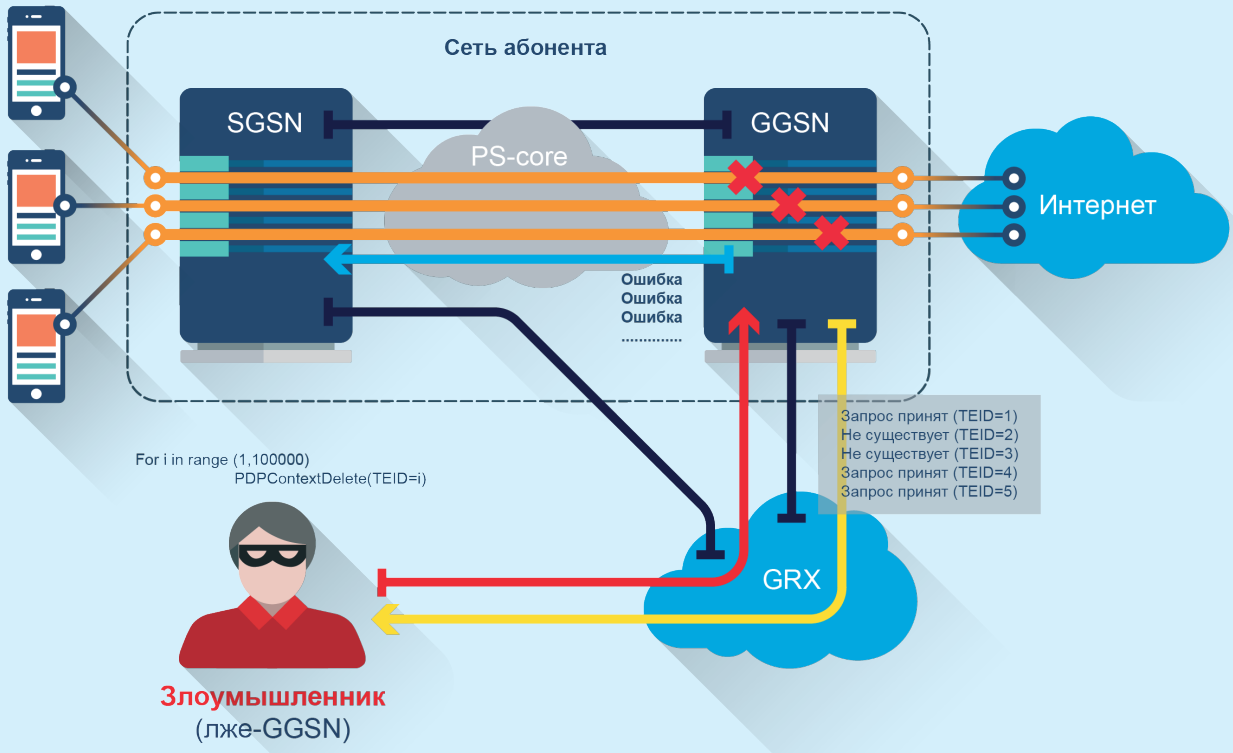


Рис. 15. Схема атаки

6.4. БЛОКИРОВКА ПОДКЛЮЧЕНИЯ К СЕТИ ИНТЕРНЕТ

Цель: невозможность установления новых соединений с сетью Интернет.

Вектор атаки: злоумышленник действует через сеть GRX или из сети оператора.

Описание. Атака основывается на отправке пакетов «Create PDP context request» с перечислением IMSI, таким образом происходит исчерпание доступного пула PDP туннелей. Например, максимальное количество PDP Context Cisco 7200 с 256 МБ памяти — 80 000, с 512 МБ — 135 000: перебрать все не так сложно. Кроме того, выдаются все новые и новые IP-адреса из DHCP-пул, и они также могут закончиться. Неважно, что быстрее закончится — DHCP-пул или PDP-пул, в конечном итоге GGSN на все валидные запросы по созданию новых подключений будет отвечать «No resource available». Более того, GGSN не может закрыть туннели, так как при попытке закрыть туннель GGSN посылает злоумышленнику «Delete PDP context request» с номером закрываемого туннеля, и если ответа нет (а его нет, поскольку злоумышленник этого не хочет), GGSN посылает такие запросы снова и снова. А ресурсы остаются занятыми.

В случае удачного осуществления данной атаки валидные абоненты не смогут подключиться к сети Интернет, а те, которые были подключены, — отключатся, так как GGSN передаст эти туннели на адрес злоумышленника.

Атака является аналогом атаки DHCP Starvation на уровне протокола GTP.

Результат. Абоненты атакуемого GGSN не смогут подключиться к сети Интернет. К одному GGSN подключаются все пользователи макрорегиона.

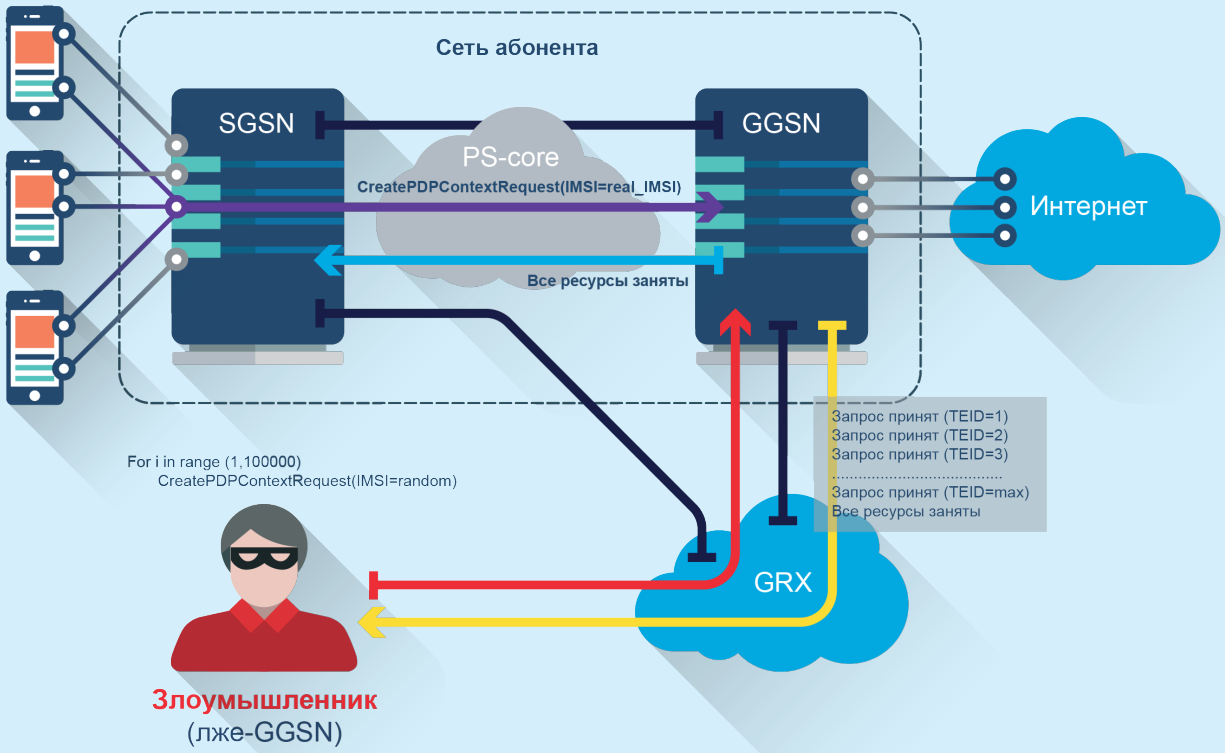


Рис. 16. Схема атаки

6.5. ИНТЕРНЕТ ЗА ЧУЖОЙ СЧЕТ

Цель: исчерпание счета абонента, использование подключения в противозаконных целях.

Вектор атаки: злоумышленник действует через сеть GRX или из сети оператора.

Описание. Атака заключается в отправке пакетов «Create PDP context request» с IMSI известного заранее абонента, таким образом происходит подключение к сети с его учетными данным. Ничего не подозревающий абонент получит огромные счета.

Возможно подключение с IMSI несуществующего абонента, так как авторизация абонента происходит на этапе подключения к SGSN, а к GGSN доходят уже «проверенные» соединения. Поскольку SGSN в данном случае скомпрометирован, никакой проверки не проводилось.

Результат. Подключение к сети Интернет под видом легитимного абонента.

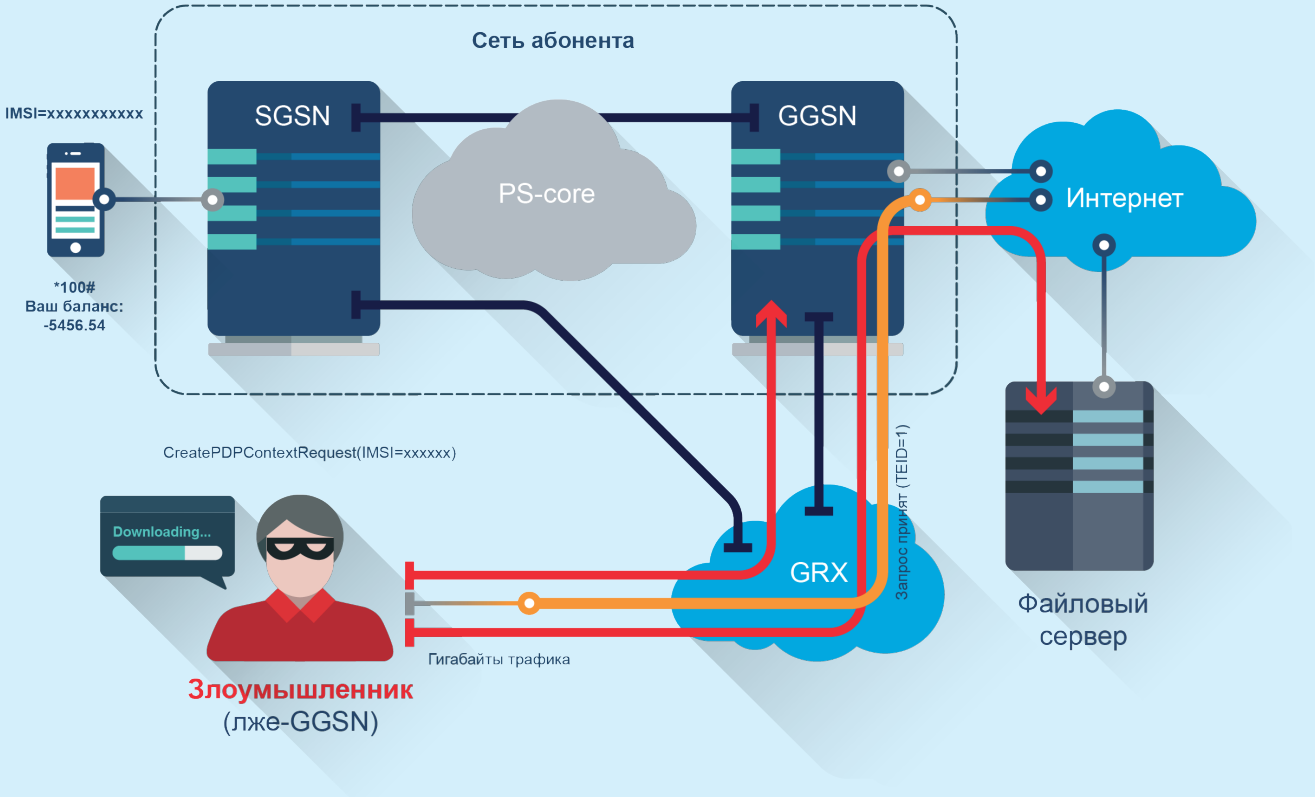


Рис. 17. Схема атаки

6.6. ПЕРЕХВАТ ДАННЫХ

Цель: подслушивание трафика жертвы, фишинг.

Вектор атаки: злоумышленник действует через сеть GRX или из сети оператора.

Описание. Злоумышленник может перехватить данные, передающиеся между абонентским устройством и сетью Интернет, путем отправки на обслуживающий SGSN и GGSN сообщения «Update PDP Context Request» с подмененными адресами GSN. Данная атака представляет собой аналог атаки ARP Spoofing на уровне протокола GTP.

Результат. Подслушивание или подмена трафика жертвы, раскрытие конфиденциальной информации.

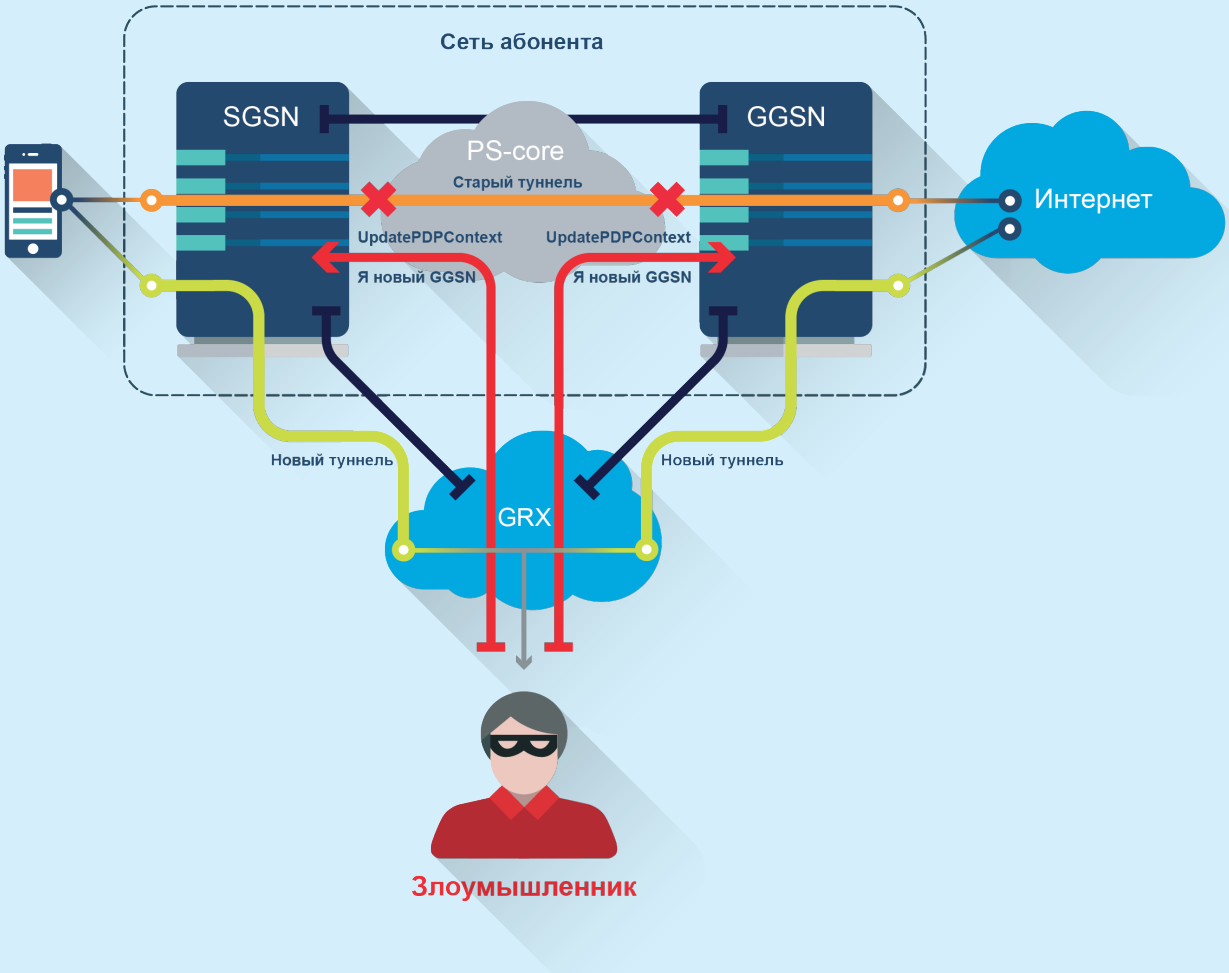


Рис. 18. Схема атаки

6.7. DNS-ТУННЕЛИРОВАНИЕ

Цель: получить нетарифицируемый доступ к Интернету со стороны мобильной станции абонента.

Вектор атаки: злоумышленник — абонент сотовой сети, действует через мобильный телефон.

Описание. Давно известная атака, уходящая корнями во времена dial-up, потерявшая смысл при появлении дешевого и быстрого выделенного Интернета. Однако в мобильных сетях находит применение, например, в роуминге, когда цены за мобильный Интернет неоправданно высоки, а скорость передачи данных не так важна (например, для проверки почты).

Суть атаки в том, что некоторые операторы не тарифицируют DNS-трафик, обычно для того, чтобы переадресовать абонента на страницу оператора для пополнения счета. Этим можно воспользоваться — путем отправления специализированных запросов на DNS-сервер; также для этого необходим специализированный узел в Интернете, через который будет осуществляться доступ.

Результат. Получение нетарифицируемого доступа к сети Интернет за счет оператора сотовой связи.

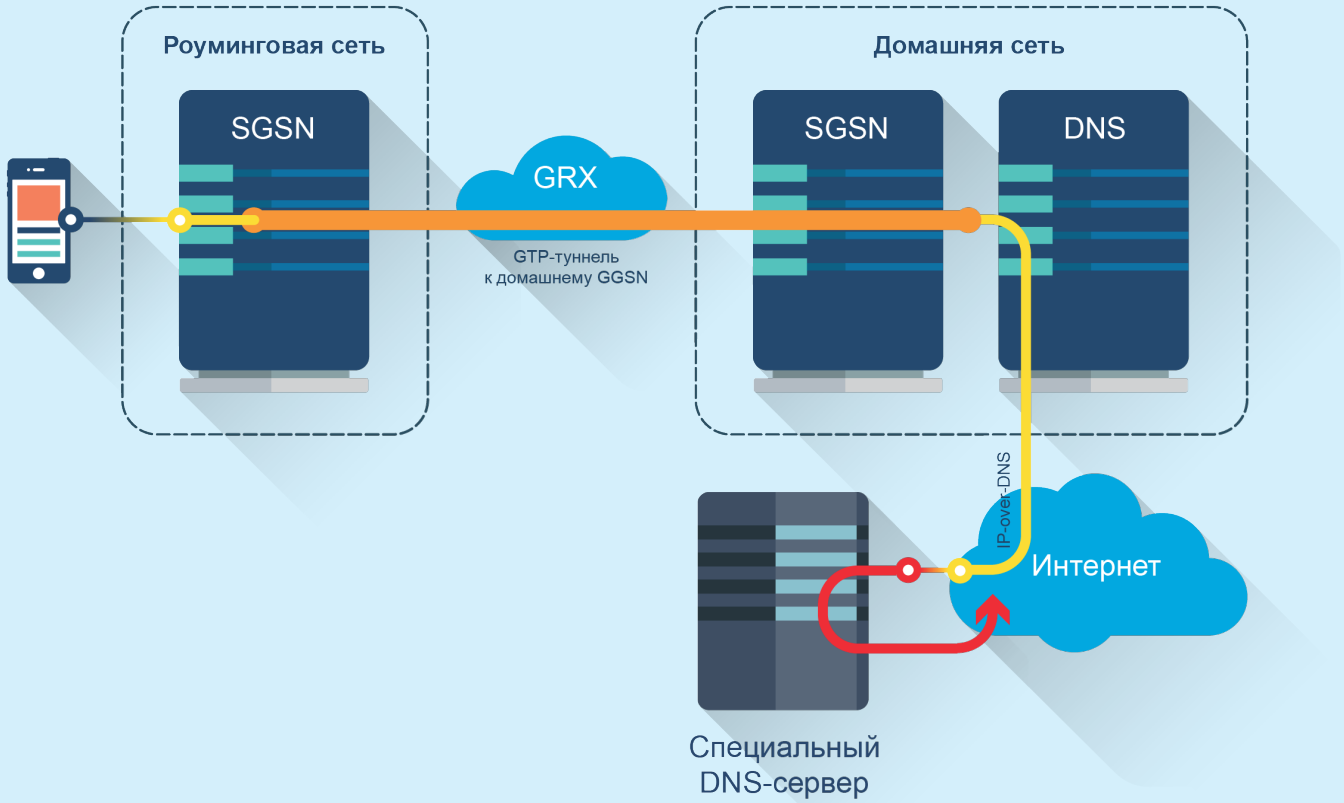


Рис. 19. Схема атаки

6.8. ПОДМЕНА DNS НА GGSN

Цель: подслушивание трафика жертвы, фишинг.

Вектор атаки: злоумышленник действует через Интернет.

Описание. В случае получения доступа к GGSN (что, как мы уже заметили, вполне возможно) можно подменить адрес DNS на свой, перенаправить весь абонентский трафик через свой узел и таким образом осуществить «подслушивание» всего мобильного трафика.

Результат. Подслушивание или подмена трафика всех абонентов, сбор конфиденциальных данных, фишинг.

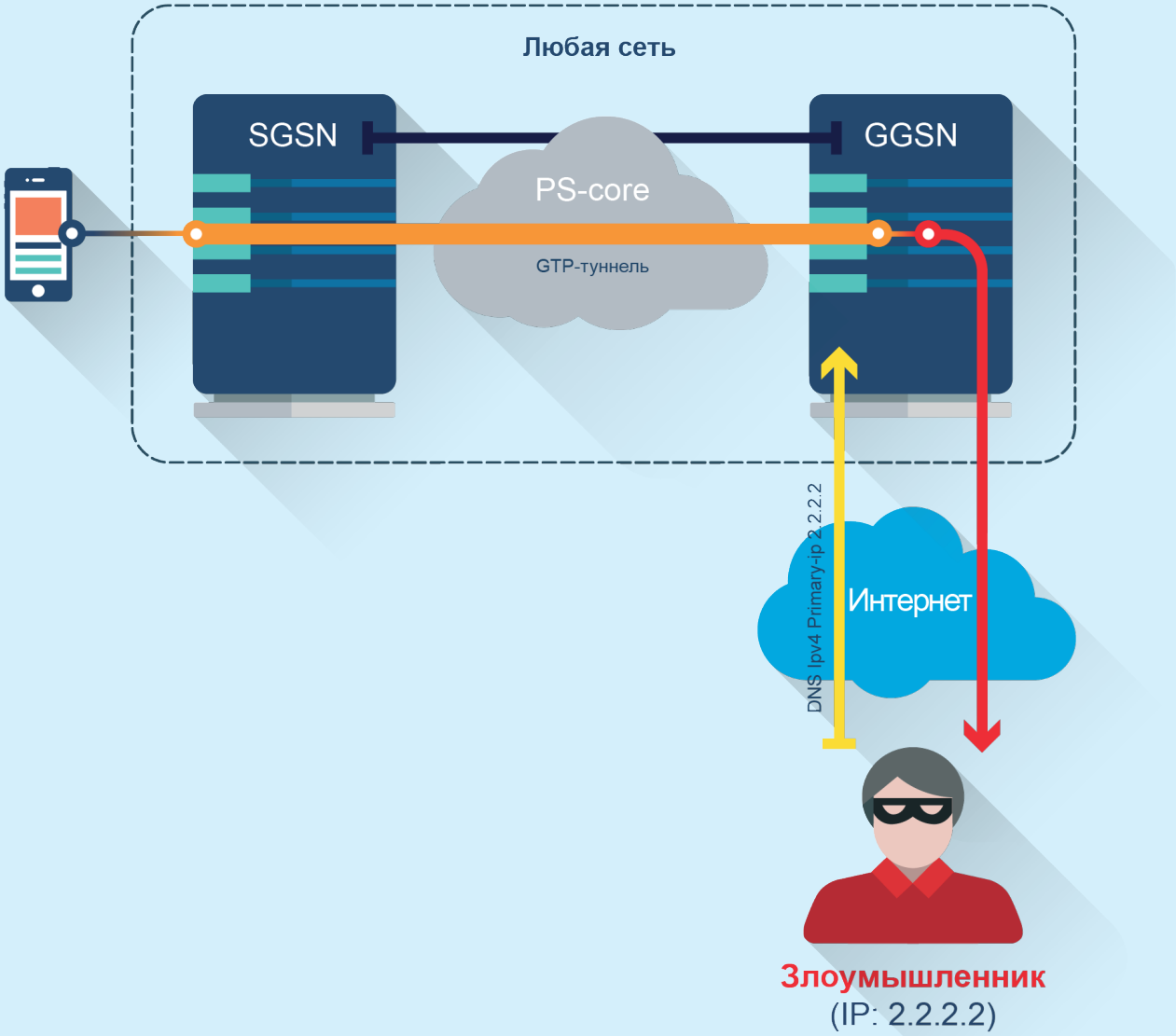


Рис. 20. Схема атаки

7. ВЫВОДЫ И РЕКОМЕНДАЦИИ

Современные сети мобильной связи содержат множество уязвимостей, которые дают злоумышленникам возможность при помощи недорогого оборудования совершать разнообразные атаки как на отдельных пользователей мобильного Интернета, так и на целые инфраструктуры — например, для промышленного шпионажа или устранения конкурентов на рынке. Кроме того, каждый раз при ухудшении международной обстановки мы видим, как активизируется прослушка мобильной связи, с последующей скандальной публикацией переговоров политиков или военных [3].

Некоторые из описанных атак было бы невозможно провести при правильной настройке оборудования. Но результаты нашего исследования говорят о том, что некорректная настройка — отнюдь не редкость в мире телекомов, которые экономят на безопасности. Зачастую и производители оставляют включенными некоторые сервисы, которые должны быть отключены на данном оборудовании, что дает нарушителям дополнительные возможности.

Многие возлагают надежды на новые стандарты связи, которые включают и новые технологии безопасности. Однако, несмотря на появление таких стандартов (3G, 4G), совсем отказаться от сетей старого поколения (2G) не удастся. Причиной этого являются особенности реализации мобильных сетей, в частности то, что у базовых станций 2G лучше покрытие, а также то, что на их инфраструктуре работают и сети 3G. Также на данный момент (конец 2014 года) большинство операторов в мире не предоставляют возможности передачи голоса через сети 4G: при осуществлении вызова мобильный телефон принудительно переключается в сеть 3G или даже 2G, а после окончания вызова переключается обратно, если это возможно. Возможность таких «невидимых» переключений активно используется для мобильной слежки [4].

С другой стороны, ключевое отличие сетей 4G — передача голоса через IP-сети — само по себе может стать уязвимостью: воздействовать можно будет не только на пользовательские данные, но и на сами телефонные разговоры. Так что от сетей 4G стоит ожидать еще больших сюрпризов [5].

Что же касается ныне используемых сетей (2G и 3G), эксперты Positive Technologies рекомендуют следующие меры безопасности на стороне операторов связи (рис. 21):

1. Использовать межсетевые экраны на границе сети GRX, блокирующие службы, которые не имеют отношения к предоставлению доступа абонентам в роуминге (GTP, DNS, и т. п.).
2. Использовать межсетевые экраны на границе сети Интернет, блокирующие доступ к сервисам, которые не должны быть доступны из Интернета.
3. Использовать рекомендации 3GPP TS 33.210 для настройки безопасности внутри сети PS-Core. Сеть должна быть защищенной, в частности за счет использования IPsec для передачи трафика GTP-C внутри сети PS-core.

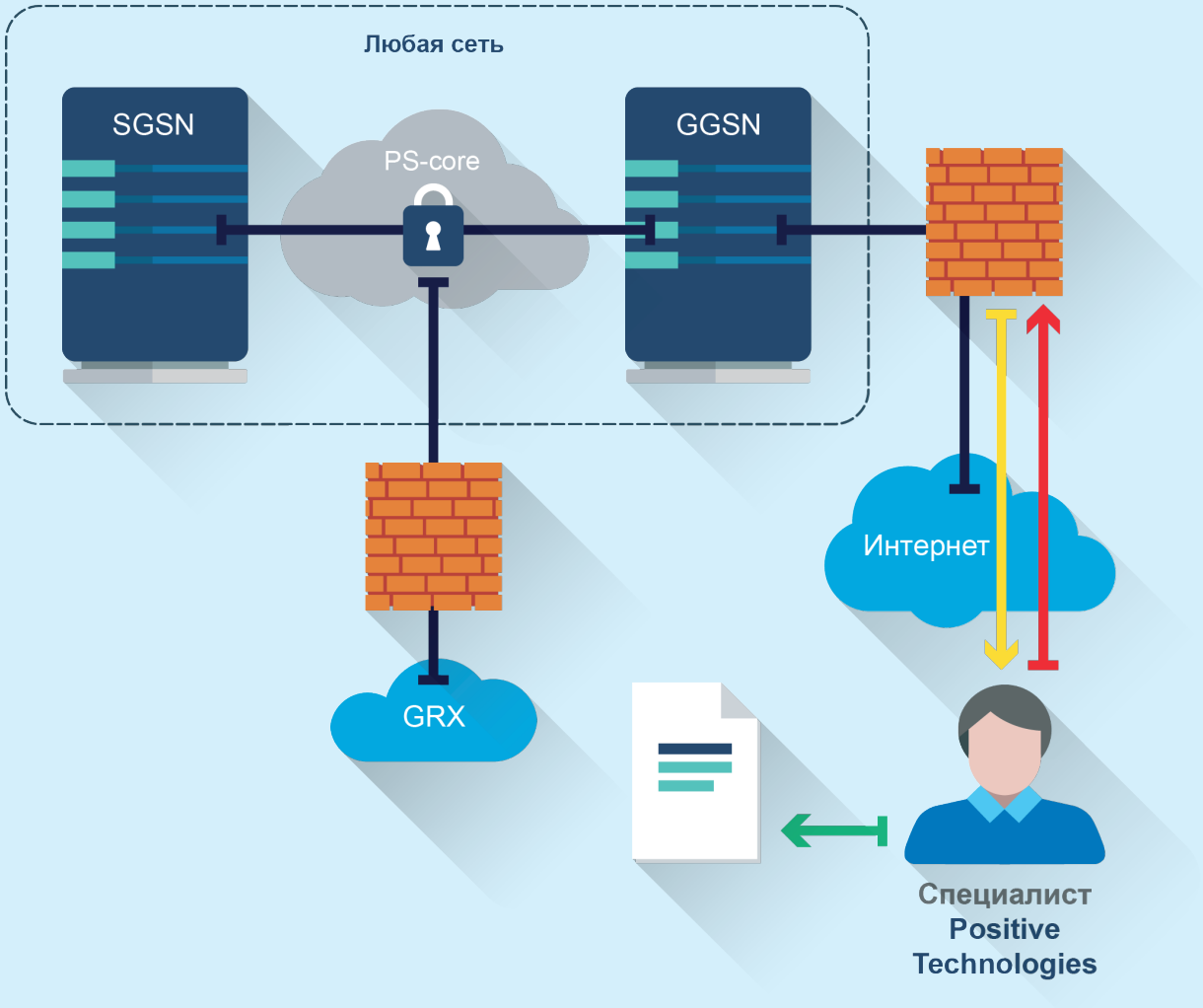


Рис. 21. Рекомендуемый комплекс мер безопасности

4. Проводить периодический контроль периметра (сервис ABC). Это комплекс мероприятий, направленных на мониторинг защищенности сети клиента от угроз, исходящих из Интернета. В процессе мониторинга осуществляется регулярное сканирование всех доступных из Интернета сетей и узлов оператора. В результате сканирования выявляется информация о доступных сервисах, их версиях, типах операционных систем. Полученная информация сверяется с содержимым базы данных уязвимостей и эксплойтов. Таким образом, у оператора появляется возможность контролировать, как выглядит периметр со стороны злоумышленника, прогнозировать возможные атаки и предотвращать их.
5. Выработать безопасные стандарты конфигурации оборудования и проводить периодический контроль соответствия этим стандартам (см. пример на рис. 22).

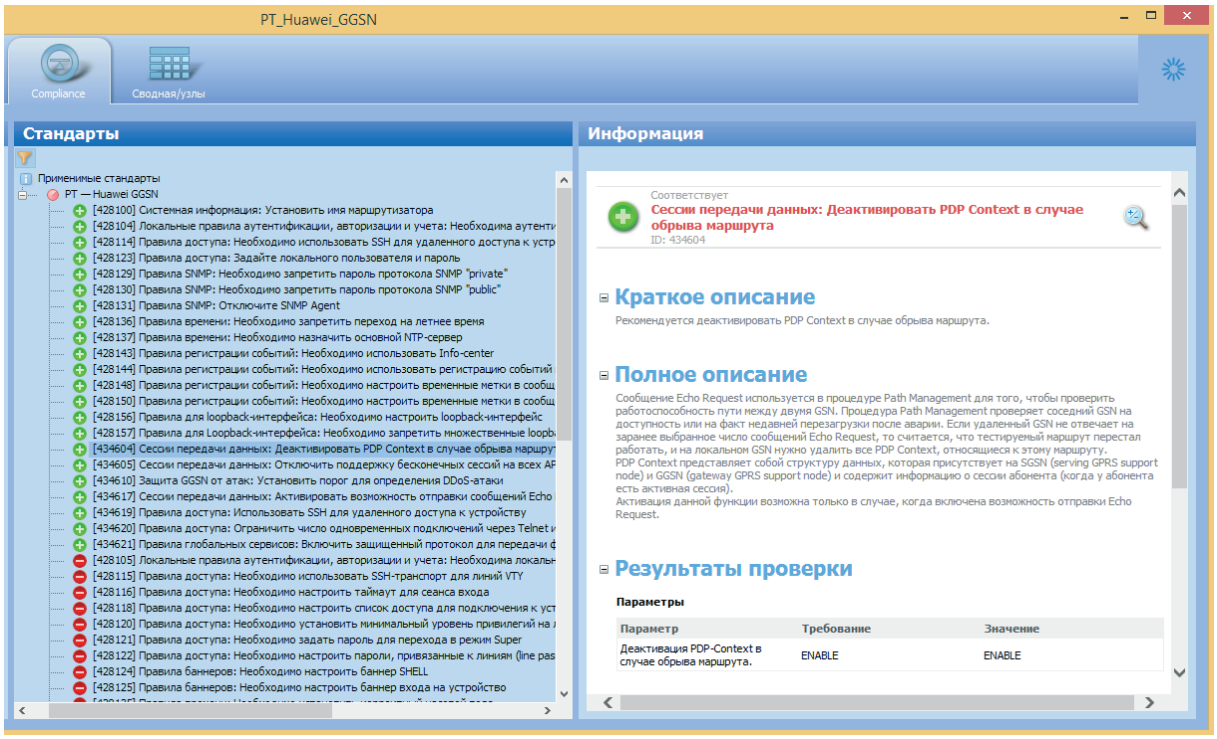


Рис. 22. Контроль соответствия в системе MaxPatrol

ИСТОЧНИКИ

1. Cisco Global Mobile Data Traffic Forecast Update, 2013–2018. Cisco VNI Mobile, 2014
http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf

2. Статистика уязвимостей корпоративный информационных систем в 2013 г. Positive Technologies, 2014
http://www.ptsecurity.ru/download/PT_Corporate_vulnerability_2014_rus.pdf

3. Уязвимости сетей мобильной связи на основе SS7. Positive Technologies, 2014
http://www.ptsecurity.ru/download/PT_SS7_security_2014_rus.pdf

4. Мобильные телефоны и тотальная слежка АНБ: как это работает. Positive Technologies, 2014
http://habrahabr.ru/company/pt/blog/245113/

5. 4G 'inherently less secure' than 3G. The Telegraph, 2014
http://www.telegraph.co.uk/technology/internet-security/10951812/4G-inherently-less-secure-than-3G.html

6. Безопасность мобильного интернета изнутри и снаружи. Positive Technologies, 2013
http://habrahabr.ru/company/pt/blog/188574/

7. GRX and a Spy Agency
http://www.slideshare.net/StephenKho/on-her-majestys-secret-service-grx-and-a-spy-agency

8. 3GPP TS 29.060
http://www.3gpp.org/DynaReport/29060.htm

СПИСОК АББРЕВИАТУР И СОКРАЩЕНИЙ

APN (Access Point Name) — символическое название точки доступа, через которую пользователь может иметь доступ к запрошенному типу услуги (WAP, Internet, MMS)

BSC (Base Station Controller) — контроллер базовых станций

BTS (Base Transceiver Station) — комплекс радиопередающей аппаратуры (ретрансляторы, приемо-передатчики), осуществляющий связь с конечным абонентским устройством

CI (Cell ID) — идентификатор соты

CS (Circuit Switched) — передача данных с коммутацией каналов

DHCP (Dynamic Host Configuration Protocol) — протокол динамической настройки узла

DNS (Domain Name System) — система доменных имен

FTP (File Transfer Protocol) — протокол передачи файлов

GGSN (Gateway GPRS Support Node) — узел, входящий в состав PS Core Network и обеспечивающий маршрутизацию данных между GPRS Core network и внешними IP-сетями

GPRS (General Packet Radio Service) — пакетная радиосвязь общего пользования

GRX (Global Roaming eXchange) — сеть для предоставления услуг пакетной передачи в роуминге

GTP (GPRS Tunneling Protocol) — протокол, который описывает и осуществляет передачу данных между узлами GSN в пакетной сети

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

HTTP (HyperText Transfer Protocol) — протокол передачи гипертекста

IMEI (International Mobile Equipment Identity) — уникальный международный номер телефонного терминала

IMSI (International Mobile Subscriber Identity) — международный идентификатор мобильного абонента

LAC (Local Area Code) — код локальной зоны

MCC (Mobile Country Code) — код страны, в которой находится базовая станция

MMS (Multimedia Message System) — это система передачи мультимедийных сообщений (изображений, мелодий, видео) в сетях сотовой связи

MNC (Mobile Network Code) — код сотовой сети

MS (Mobile Station) — общепринятое обозначение для мобильной станции абонента

MSISDN (Mobile Subscriber Integrated Services Digital Number) — номер мобильного абонента цифровой сети с интеграцией служб

PS (Packet Switched) — передача данных с коммутацией пакетов

SGSN (Service GPRS Support Node) — основной компонент GPRS-системы по реализации всех функций обработки пакетной информации

SS7 (Signaling System 7) — общеканальная система сигнализации, используемая в международных и местных телефонных сетях по всему миру

SSH (Secure Shell) — безопасная оболочка

TEID (Tunnel Endpoint IDentifier) — идентификатор туннеля

UDP (User Datagram Protocol) — протокол пользовательских датаграмм

UMTS (Universal Mobile Telecommunications System) — технология сотовой связи, разработана Европейским институтом стандартов телекоммуникаций (ETSI) для внедрения 3G в Европе

WAP (Wireless Application Protocol) — беспроводной протокол передачи данных