

УГРОЗЫ БЕЗОПАСНОСТИ ЯДРА ПАКЕТНОЙ СЕТИ 4G

2017

POSITIVE TECHNOLOGIES



СОДЕРЖАНИЕ

Основные компоненты и протоколы Evolved Packet Core	3
Сценарии атак	4
Что необходимо для успешной атаки	5
Угрозы безопасности EPC.....	6
1. Мошенничество.....	6
2. Перехват интернет-соединения	8
3. DoS-атака на абонента	9
4. DoS-атака на оборудование оператора	9
5. Управляющие пакеты внутри пользовательского туннеля: GTP-in-GTP	10
Заключение.....	11
Термины и сокращения.....	12

Широкое распространение мобильных сетей связи четвертого поколения упростило доступ к быстрому интернету для миллиардов пользователей. Однако не только смартфоны, планшеты и компьютеры массово подключаются к 4G. Высокая скорость передачи данных и минимальные задержки в LTE-сетях позволяют использовать их для построения инфраструктуры интернета вещей. По прогнозам аналитиков, к 2022 году число IoT-устройств, подключенных к сотовым сетям, увеличится с 400 млн до 1,5 млрд¹. Таким образом, защищенность систем «умного города», самоуправляемых «подключенных автомобилей» и других IoT-технологий будет тесно связана с вопросами безопасности современных (4G) и перспективных (5G и LTE-M) сетей мобильной связи.

В 2016 году специалисты Positive Technologies проводили работы по анализу защищенности сигнальных сетей 4G. Во всех исследованных сетях телеком-операторов были выявлены уязвимости, обусловленные фундаментальными недостатками ядра пакетной сети Evolved Packet Core. Обнаруженные проблемы позволяют отключать одного или множество абонентов, перехватывать интернет-трафик и SMS-сообщения, выводить из строя оборудование оператора и осуществлять другие нелегитимные действия. Процесс эксплуатации уязвимостей в сетях 4G не требует от злоумышленника труднодоступных инструментов или высокого уровня квалификации.

В настоящем отчете подробно рассмотрены возможные сценарии атак и перечислены необходимые меры по повышению защищенности.

ОСНОВНЫЕ КОМПОНЕНТЫ И ПРОТОКОЛЫ EVOLVED PACKED CORE

Для сетей четвертого поколения консорциум 3GPP разработал новую архитектуру ядра сети — System Architecture Evolution (SAE). Базовым элементом новой архитектуры является ядро пакетной сети Evolved Packet Core (EPC)². По сравнению с сетями предыдущих поколений структура ядра EPC стала проще (рис. 1), что увеличило пропускную способность и снизило задержки сигнала при передаче пользовательских данных и служебной информации. В частности, исчез важный компонент — сеть с коммутацией каналов. Сети 4G построены по принципу All IP Network, что позволяет передавать в пакетной среде не только данные, но и голосовые вызовы. Однако до сих пор не все операторы реализовали

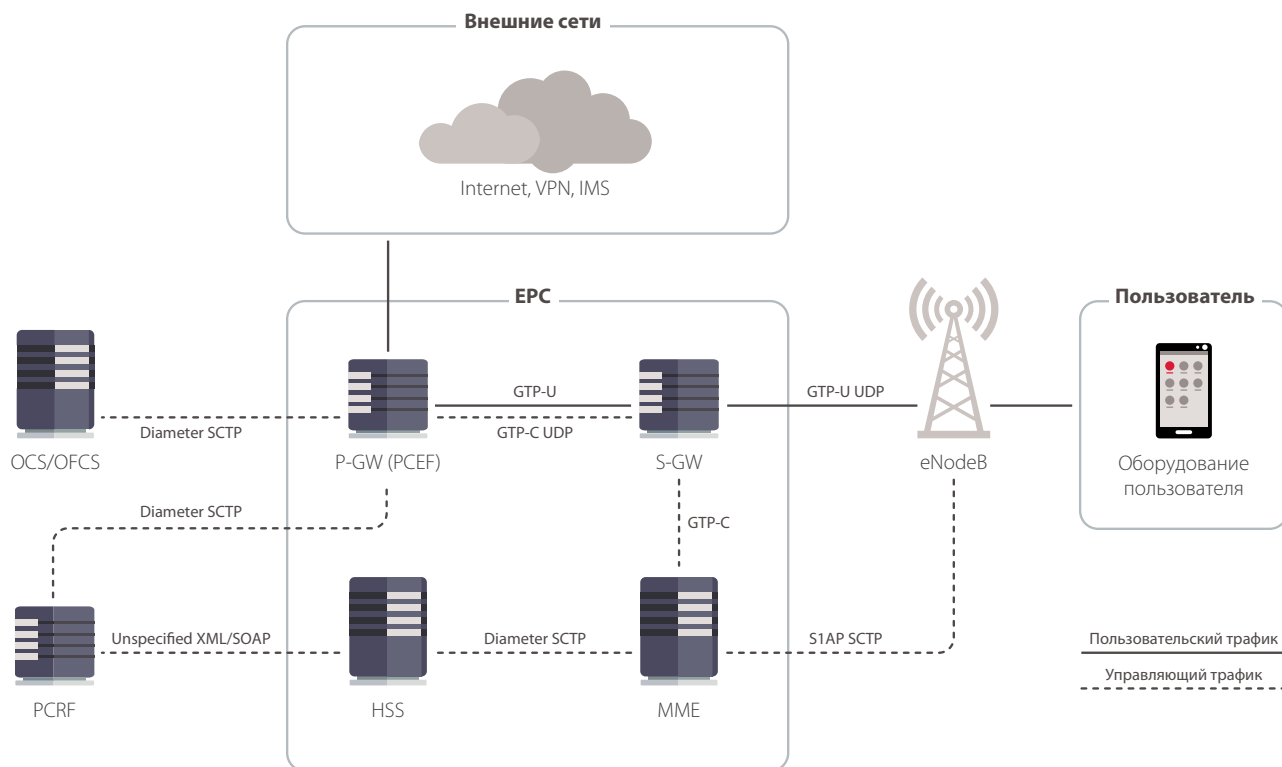


Рис. 1. Структура ядра пакетной сети Evolved Packet Core (EPC)

¹ Согласно исследованию Ericsson Mobility Report 2016:

www.ericsson.com/assets/local/mobility-report/documents/2016/ericsson-mobility-report-november-2016.pdf

² EPC называют также «улучшенным пакетным ядром».

необходимые технологии (например, IMS для VoIP) для передачи голоса средствами 4G. В таких случаях при осуществлении вызова аппарат абонента принудительно переключается в 2G/3G и может столкнуться с уязвимостями, о которых мы неоднократно рассказывали в наших исследованиях³.

Основными компонентами ядра пакетной сети являются следующие элементы:

Сервер абонентских данных (HSS) представляет собой большую базу данных и предназначен для хранения информации об абонентах. Фактически HSS заменяет собой базы VLR, HLR, AUC и EIR, которые использовались в сетях 2G/3G.

Обслуживающий шлюз (S-GW) обеспечивает передачу и обработку пользовательских данных между пользовательскими устройствами (UE) и подсистемой базовых станций сети LTE (eNodeB) оператора.

Пакетный шлюз (P-GW) управляет потоками данных, передаваемых во внешние пакетные сети, по сути являясь в сети оператора точкой входа и выхода пользовательского трафика. При совмещении с PCEF — элементом сети, отвечающим за применение правил тарификации, — обеспечивает корректную работу расчетных систем и применение тарифных правил.

Узел управления мобильностью (MME) обеспечивает возможность переключения между базовыми станциями и работу в роуминге. Кроме того, MME отвечает за аутентификацию пользовательских устройств (UE), взаимодействуя с HSS, а также за выбор шлюза S-GW.

Каждый узел EPC может обеспечивать не только функции проверки и фильтрации сетевых пакетов по их содержимому (DPI), но и различные функции законного перехвата, используемого правоохранительными органами.

Для взаимодействия между собой узлы EPC используют GPRS Tunneling Protocol (GTP), S1 Application Protocol (S1AP), Diameter и другие протоколы. Основные угрозы протокола Diameter подробно описаны в предыдущем отчете⁴. Рассмотренные в настоящем отчете атаки направлены на узлы, взаимодействующие по протоколу GTP.

СЦЕНАРИИ АТАК

Большой интерес для злоумышленника представляют специальные интерфейсы, через которые осуществляется обмен информацией между компонентами EPC. По этим каналам могут передаваться пользовательская информация и служебные данные, так называемый сигнальный трафик. Поскольку все интерфейсы не имеют встроенных механизмов шифрования данных, злоумышленник может проводить следующие атаки:

- + перехват персональных идентификаторов пользователя MSISDN, IMSI;
- + определение местоположения абонента;
- + атаки типа «человек посередине» для незашифрованного трафика (перехват доступа к незащищенной почте, посещаемым сайтам и т. п.);
- + перехват SMS-сообщений;
- + прослушивание звонков VoLTE путем перехвата пакетов;
- + создание сессии от имени абонента с целью мошенничества;
- + атаки типа «отказ в обслуживании» на абонента, которые вызывают потери в передаче пользовательских данных, а для сетей с VoLTE — прерывание вызовов;
- + атаки типа «отказ в обслуживании» на оборудование, которые приводят к перебоям в работе сети.

Сценарии большинства возможных атак базируются на особенностях предоставления услуг роуминга и недостатках межоператорского взаимодействия через сеть GRX (GPRS Roaming Exchange, или роуминговый обмен в среде GPRS). Сигнальный и пользовательский трафик выходит за границы сети одного оператора и передается как по транзитной сети пакетной передачи данных GRX, так и по сети гостевого оператора. С целью обеспечения аутентификации пользователей и применения к ним тарифных правил участники межоператорского обмена взаимодействуют друг с другом через открытые интерфейсы.

³ Статистика основных угроз безопасности в сетях SS7 мобильной связи (2016): www.ptsecurity.com/upload/ptru/analytics/SS7-Vulnerability-2016-rus.pdf

⁴ www.ptsecurity.com/upload/corporate/ru-ru/analytics/Diameter-rus.pdf

Злоумышленник может воспользоваться доступностью этих интерфейсов для проведения атак на абонентов или на оборудование телеком-оператора⁵.

ЧТО НЕОБХОДИМО ДЛЯ УСПЕШНОЙ АТАКИ

Реализовать подобные атаки через сеть глобального роумингового обмена GRX могут как сотрудники практически любого телеком-оператора, так и внешние злоумышленники, получившие доступ к инфраструктуре оператора, что осуществимо в том числе с помощью подбора словарных паролей или использования простейших уязвимостей на сетевом периметре.

До появления LTE для перехвата голосовых вызовов нарушителю необходимо было обладать глубокими знаниями о работе специфичных протоколов, обеспечивающих голосовые звонки между абонентами, и иметь в своем распоряжении специальные технические средства. Но поскольку сети 4G построены по принципу All IP Network, нарушитель может использовать весь наработанный до сегодняшнего дня хакерский инструментарий, существенно автоматизированный и не требующий глубокого понимания природы атаки. Злоумышленнику достаточно располагать ноутбуком, свободно распространяемым дистрибутивом для проведения тестов на проникновение и базовыми навыками программирования. Зачастую в интернет выставлены реальные операторские GGSN, с настоящими APN и абонентами, что сокращает время на подготовку самой простой атаки — DoS-атаки на абонентов оператора — всего до несколько часов, с учетом подготовки инструментария.

Входные параметры, необходимые для проведения атак, будут зависеть от задействованных протоколов и требуемых параметров сообщений. Изначально злоумышленнику необходимо располагать временным идентификатором абонента мобильной сети (TMSI), международным идентификатором абонента мобильной сети (IMSI) и идентификатором конечной точки туннеля (TEID).

Атакующий может найти корректный идентификатор TEID с помощью перебора, направляя на шлюз P-GW сообщения GTP-U с произвольными значениями TEID. Если TEID некорректный, то P-GW отвечает сообщением GTP-C, содержащим ошибку «Error Indication», а если сообщение об ошибке не пришло, то TEID — корректный (рис. 2). Хотя на полный перебор значений TEID может уйти несколько часов, диапазон значений TEID у большинства устройств можно предсказать, что позволяет сократить время перебора до нескольких минут.

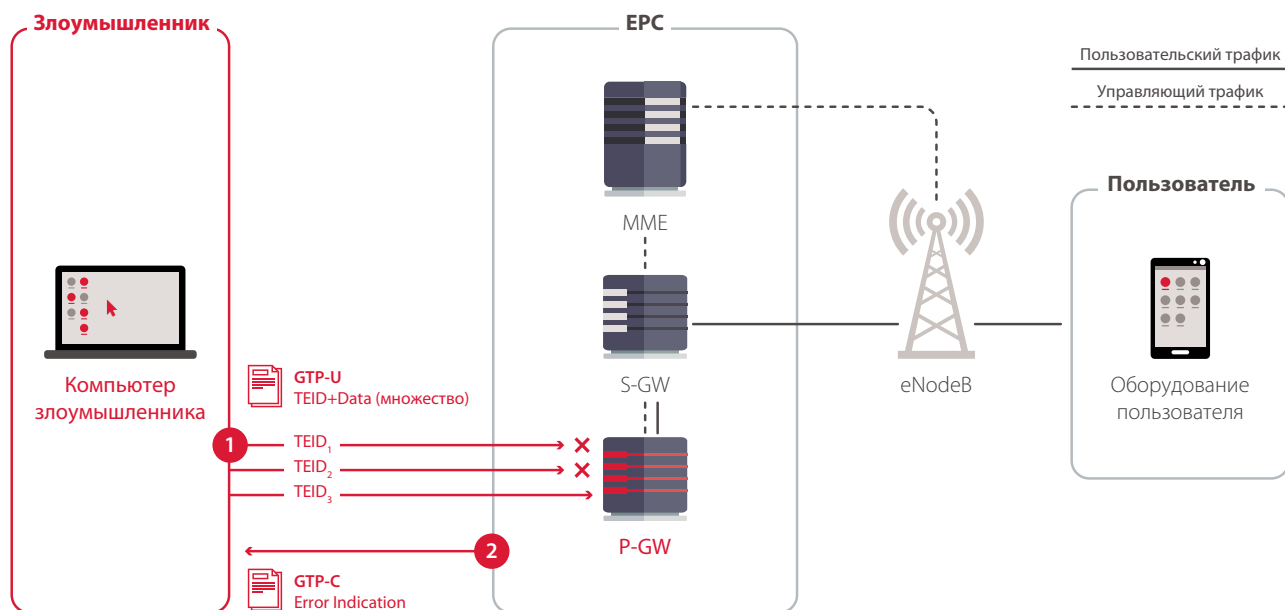


Рис. 2. Подбор идентификатора конечной точки туннеля (TEID)

Для успешной реализации некоторых описанных атак в формируемых запросах необходимо указывать TMSI жертвы. Этот идентификатор злоумышленник может получить разными способами: прямым перебором, пассивным сканированием радиоэфира, используя поддельную базовую станцию (FakeBTS) или IMSI-catcher.

⁵ www.ptsecurity.com/upload/corporate/ru-ru/analytics/GPRS-security-rus.pdf

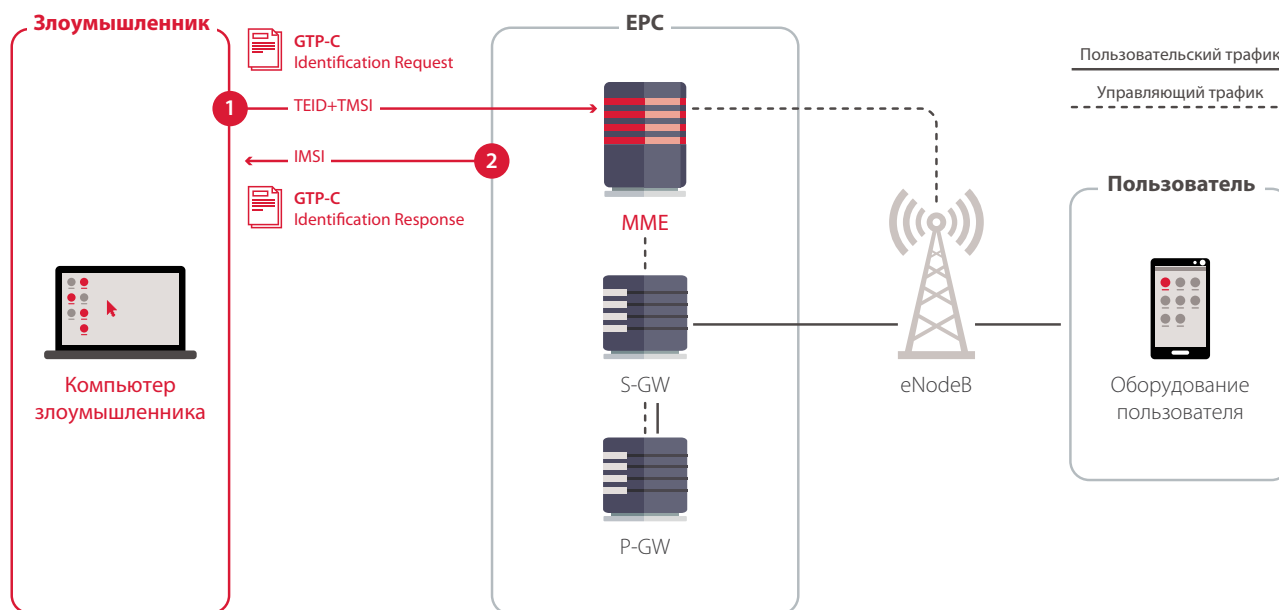


Рис. 3. Определение IMSI абонента

Располагая идентификаторами TEID и TMSI, можно определить IMSI абонента (рис. 3). Для этого злоумышленнику необходимо отправить сообщение GTP-C «Identification requests» на MME. В случае успешного прохождения запроса в ответ будет получено сообщение «Identification Response», содержащее IMSI атакуемого абонента.

IMSI является основным идентификатором для осуществления атак на SS7 и Diameter. Кроме того, данная атака позволяет злоумышленнику обойти защиту радиointерфейса по маскированию реальных идентификаторов IMSI подменой их временными TMSI и отслеживать перемещение абонента с использованием пассивного сканирования радиоэффира.

УГРОЗЫ БЕЗОПАСНОСТИ EPC

Ядро пакетной сети EPC является основой сетей четвертого поколения, но в нем заложены протоколы и механизмы, обеспечивающие обратную совместимость с сетями прошлых поколений (2G/3G). Например, обслуживающему шлюзу (S-GW) и пакетному шлюзу (P-GW) необходимо поддерживать протокол предыдущей версии GTPv1 для нормального перехода из 4G в 2G/3G, когда сигнал LTE становится недоступным.

В некоторых случаях, даже если на устройстве обеспечивается корректная обработка пакетов GTPv2, производители оборудования могут упустить проверку корректности пакетов GTPv1, так как работа над устаревшими технологиями обычно сворачивается при появлении новых, а просто отключить поддержку старого протокола зачастую невозможно. В результате злоумышленник может проводить атаки на абонентов и оборудование телеком-оператора по протоколу GTPv1, что проще и быстрее. Так, например, для проведения атаки с перехватом интернет-сессии абонента в параметрах GTPv2-сообщения «Context Request» необходимо заполнить причину отправки данного сообщения (location update), параметры переключения, поддерживаемые мобильным устройством типы шифрования и т. д. А для аналога этого сообщения «SGSN Context Request» в протоколе GTPv1 нужно указать только TMSI.

Рассмотренные далее сценарии атак предполагают применение сообщений протокола GTPv2.

1. Мошенничество

Недостаточная защита компонентов ядра EPC позволяет атакующему получить доступ к услугам и ресурсам оператора в обход системы тарификации либо за счет других абонентов. В результате таких действий оператор может понести прямые финансовые потери, а абоненты — получить гигантские счета за услуги, которыми не пользовались. К подобным ситуациям может привести отсутствие проверки IP-адресов устройств, направляющих запросы на оборудование.

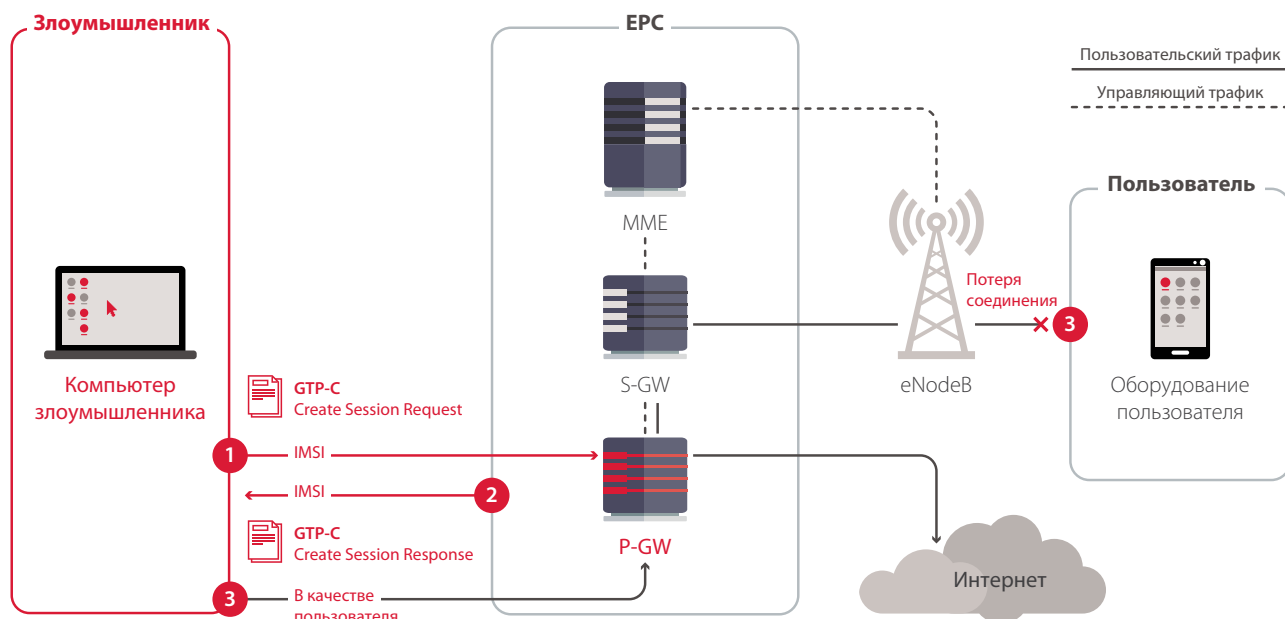


Рис. 4. Использование услуг за счет оператора или другого абонента с помощью запроса GTP-C

Злоумышленник может создать новую сессию от имени другого абонента для того, чтобы неправомерно воспользоваться услугой по доступу в сеть Интернет, направив сформированный специальным образом служебный запрос GTP-C «Create Session Request» на шлюз P-GW (рис. 4). Если в запросе будет указан IMSI, соответствующий реальному абоненту, то система тарификации включит в счет этого абонента оплату за весь трафик, использованный злоумышленником. В противном случае, когда IMSI не назначен реальному абоненту, расходы по передаче данных сразу понесет оператор связи (рис. 4).

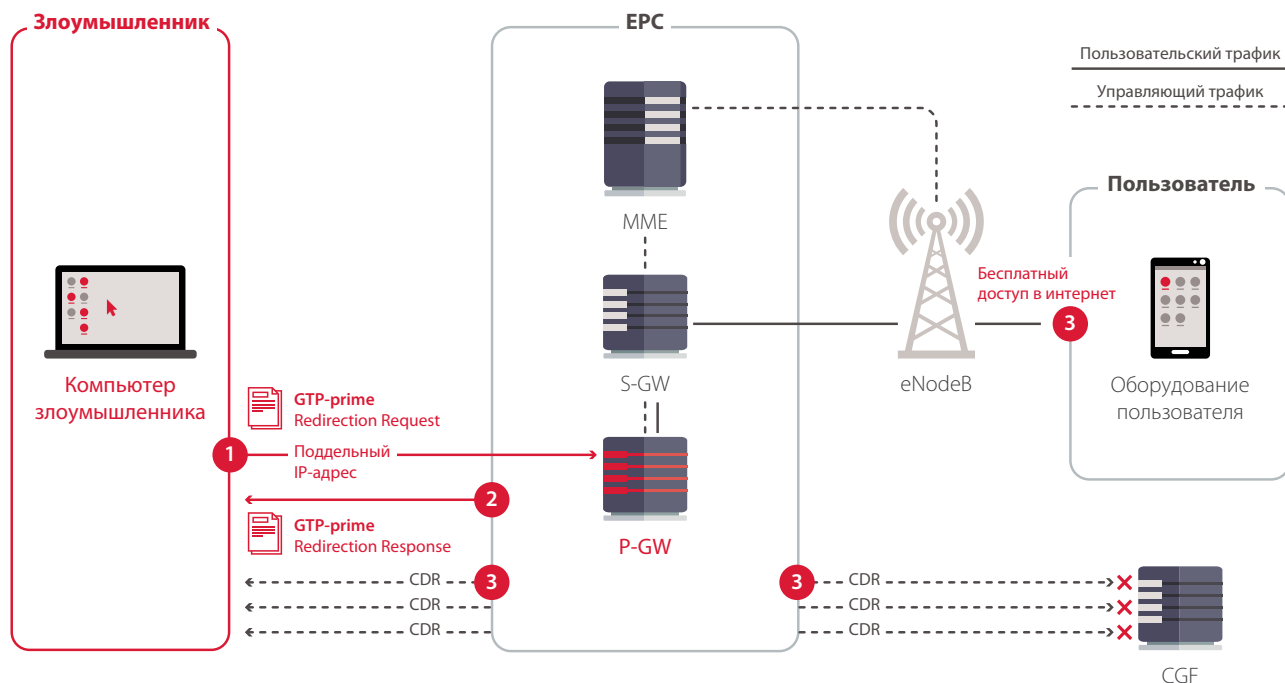


Рис. 5. Обход системы учета использованных услуг с помощью буфера шлюза CGF

Другой вариант данной атаки (рис. 5) использует механизм организации отказоустойчивости шлюза CGF (Charging Gateway Function). Этот компонент отвечает за прием и проверку детализации данных об оказанной услуге CDR (Charging Data Record) в расчетной системе. При переполнении или перегрузке буфера шлюза CGF информация о предоставленной услуге может быть отклонена сообщением «Redirection Request» с указанием IP-адреса резервного шлюза. Эксплуатируя эту особенность, злоумышленник может направлять такие запросы на пакетный шлюз P-GW, указывая свой IP-адрес в качестве адреса свободного CGF, что позволит обойти систему учета использованных услуг.

Описанные сценарии атаки потенциально дают злоумышленнику возможность получить неограниченный доступ к ресурсам, которые ему не предоставляются, например к услугам, которые не предусмотрены его тарифным планом, что приведет к прямой потере денег телеком-оператором.

2. Перехват интернет-соединения

Атака грозит утечкой конфиденциальных данных абонента и компрометацией важных ресурсов. Злоумышленник может продолжать сессию от имени абонента, причем в момент передачи управления соединением самому абоненту будет отказано в дальнейшем обслуживании.

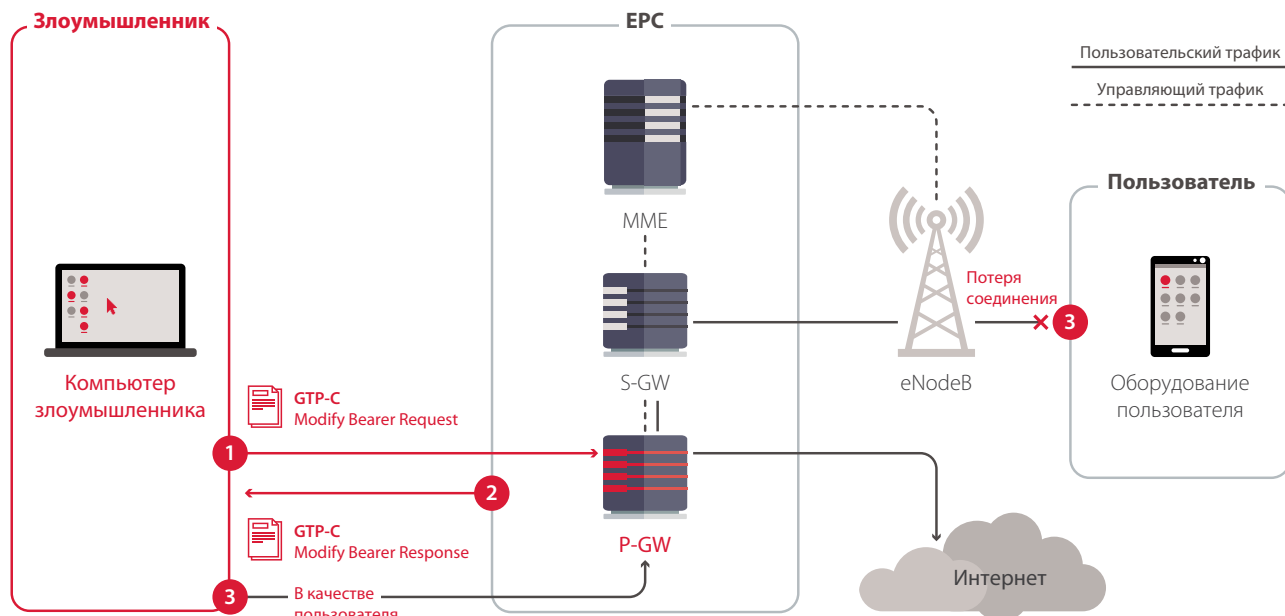


Рис. 6. Перехват интернет-соединения с помощью запроса «Modify Bearer Request»

Для проведения атаки злоумышленнику необходимо направить от лица S-GW сформированный специальным образом запрос GTP-C «Modify Bearer Request» на P-GW. В результате атакующий будет подключен к текущему соединению абонента и продолжит сеанс вместо него. P-GW будет пересылать данные злоумышленнику, а соединение абонента будет разорвано (рис. 6).

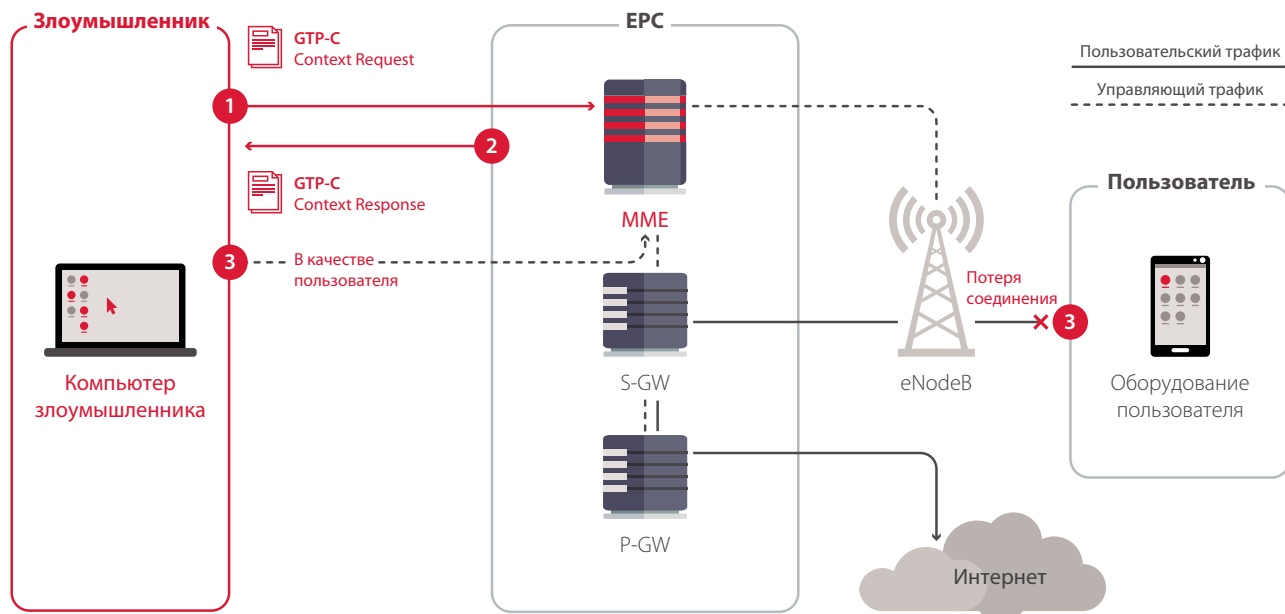


Рис. 7. Перехват интернет-соединения с помощью запроса «Context Request»

Такую же атаку можно провести и на узел управления мобильностью MME, используя сформированное специальным образом сообщение GTP-C «Context Request» и указав в числе прочих параметров TEID и TMSI атакуемого абонента (рис. 7).

Описанный сценарий, возможный из-за уязвимости в протоколе GTP и отсутствия проверки IP-адресов отправителя сообщений, позволяет злоумышленнику получить доступ к сети Интернет от имени абонента. Эта особенность может быть использована для обхода систем законного перехвата — например, лицами, скрывающимися от правоохранительных органов.

3. DoS-атака на абонента

В ядре EPS осуществимы несколько сценариев проведения атаки типа «отказ в обслуживании», блокирующей интернет-соединение абонента. При однократном разрыве соединения пользователь может перезагрузить смартфон, чтобы восстановить связь. Но если злоумышленник будет проводить подобную атаку непрерывно, то абонент окажется полностью заблокированным. Перебирая разные значения TEID, можно разрывать соединения сразу множества пользователей. Подобные действия существенно отражаются на общем качестве предоставляемых услуг и на лояльности абонентов к оператору связи.

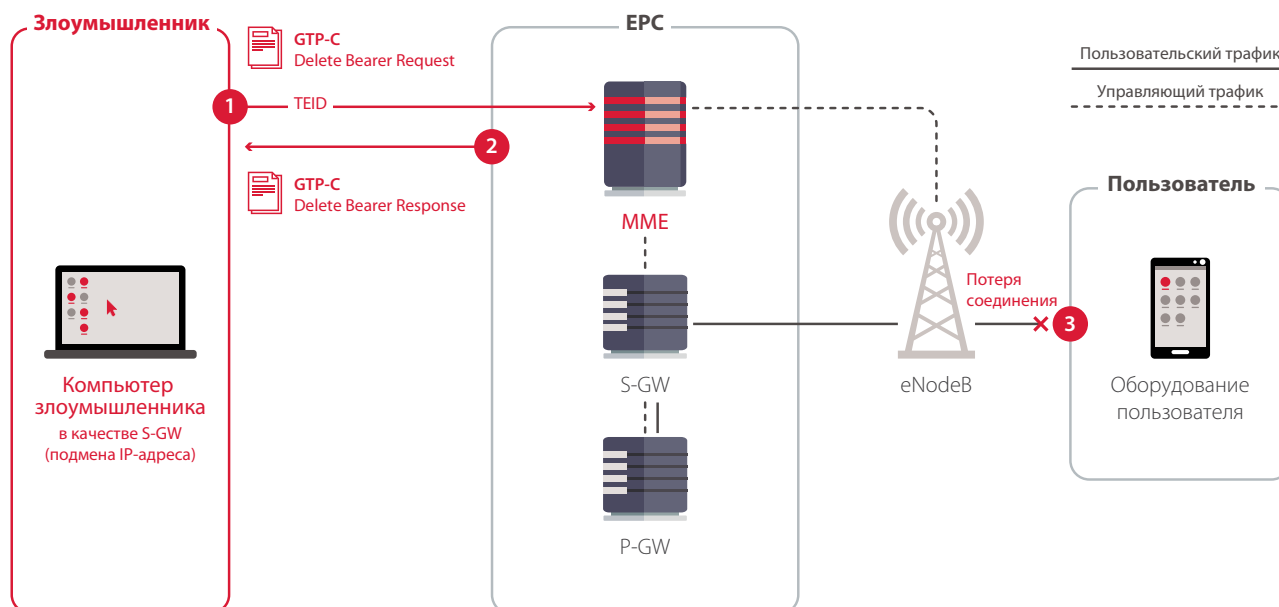


Рис. 8. DoS-атака на абонента с помощью запроса «Delete Bearer Request»

Данная атака (рис. 8) реализуется злоумышленником при отсутствии проверки адреса отправителя на оборудовании, когда он от имени шлюза S-GW направляет на MME запрос GTP-C «Delete Bearer Request» с указанием идентификатора TEID абонента, подменив IP-адрес отправителя на IP-адрес S-GW. После этого соединение с конечным устройством абонента прерывается до его повторного подключения к сети или следующей перезагрузки устройства.

Злоумышленник также может отключить абонента от сети Интернет, выяснив TEID текущей сессии абонента и направив запрос GTP-C «Delete Session Request» на шлюз P-GW (рис. 9).

4. DoS-атака на оборудование оператора

Производители телекоммуникационного оборудования не всегда тщательно проверяют так называемые негативные сценарии использования интерфейсов и протоколов, полагая, что все элементы сети работают в соответствии с требованиями стандартов. Наш опыт показывает, что вывести из строя элементы сигнальной сети телеком-оператора могут несколько специально сформированных неправильных пакетов (рис. 10).

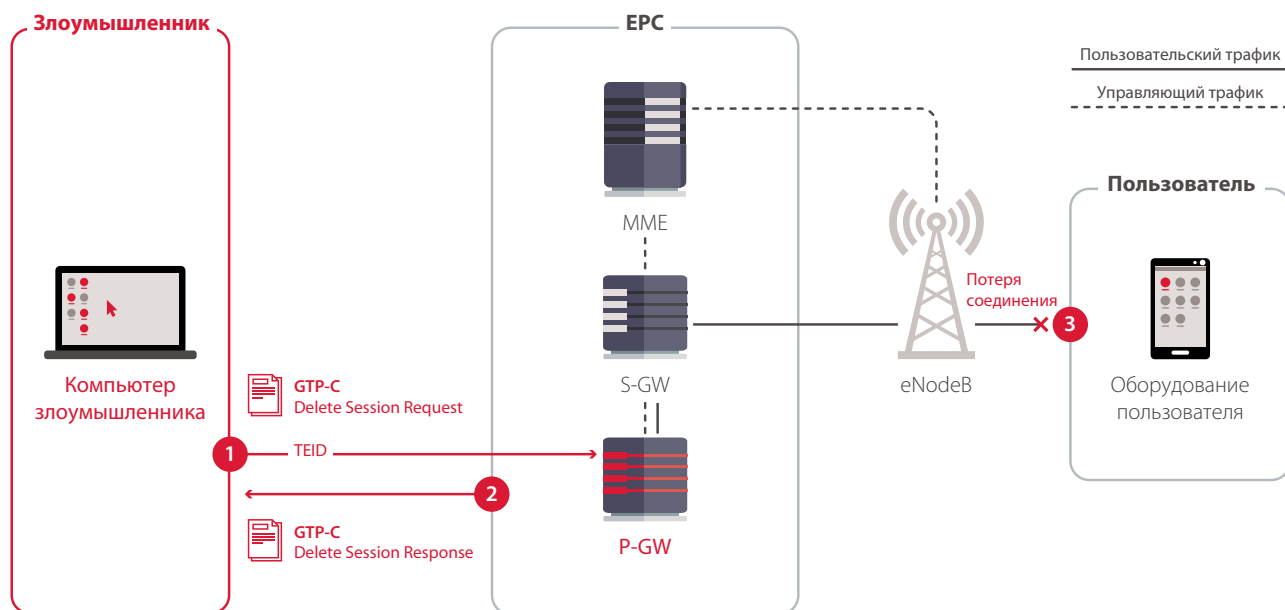


Рис. 9. DoS-атака на абонента с помощью запроса «Delete Session Request»

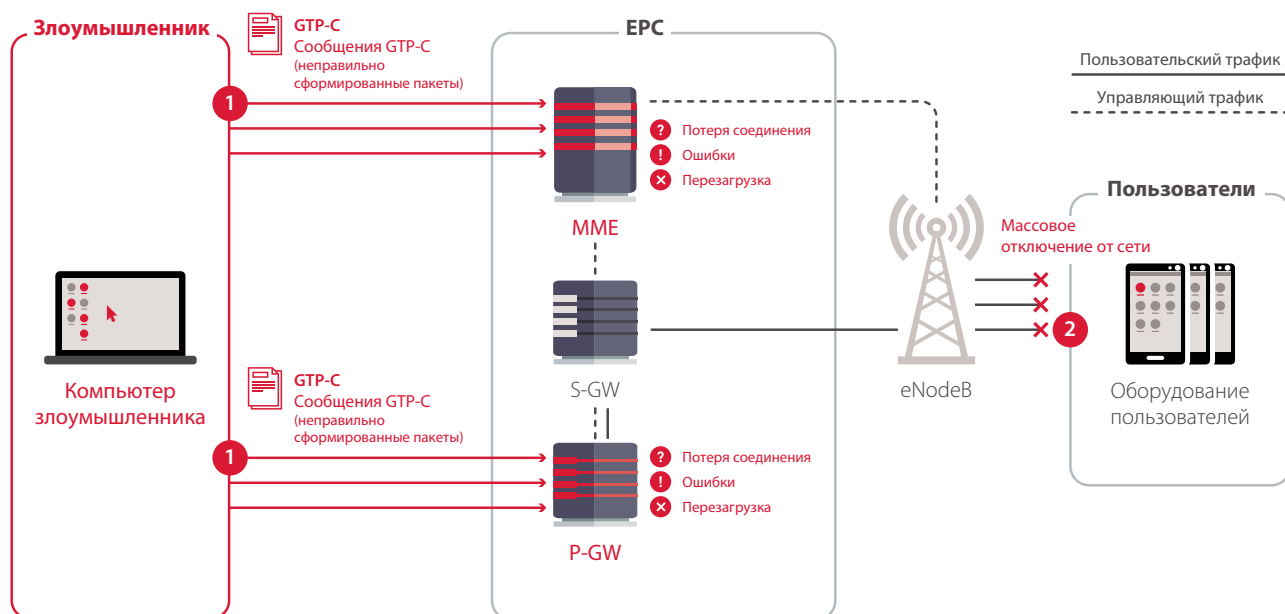


Рис. 10. DoS-атака на оператора при помощи неправильных пакетов

Подобные уязвимости должны оперативно устраняться согласно выработанным рекомендациям (об этом в разделе «Заключение»). Ошибки оборудования при обработке сообщений могут повлечь за собой сбои в работе сети, ухудшение качества или отказ в обслуживании множества абонентов.

5. Управляющие пакеты внутри пользовательского туннеля: GTP-in-GTP

Еще одна крупная проблема безопасности возникает в связи с тем, что туннели с пользовательскими данными GTP-U заканчиваются на пакетном шлюзе P-GW, а во внешние сети передается только полезная нагрузка (payload). Если легальный пользователь мобильного интернета инкапсулирует в качестве полезной нагрузки в пакет с данными пользователя (GTP-U) пакет со служебной информацией (GTP-C), то шлюз P-GW может не отправить этот тандем дальше по сети, а обработать как управляющий сигнальный пакет. Таким образом, если в сети не заблокирована атака GTP-in-GTP, то все описанные в отчете атаки возможны не только изнутри сети, но и с LTE-модема или мобильного телефона абонента (рис. 11).

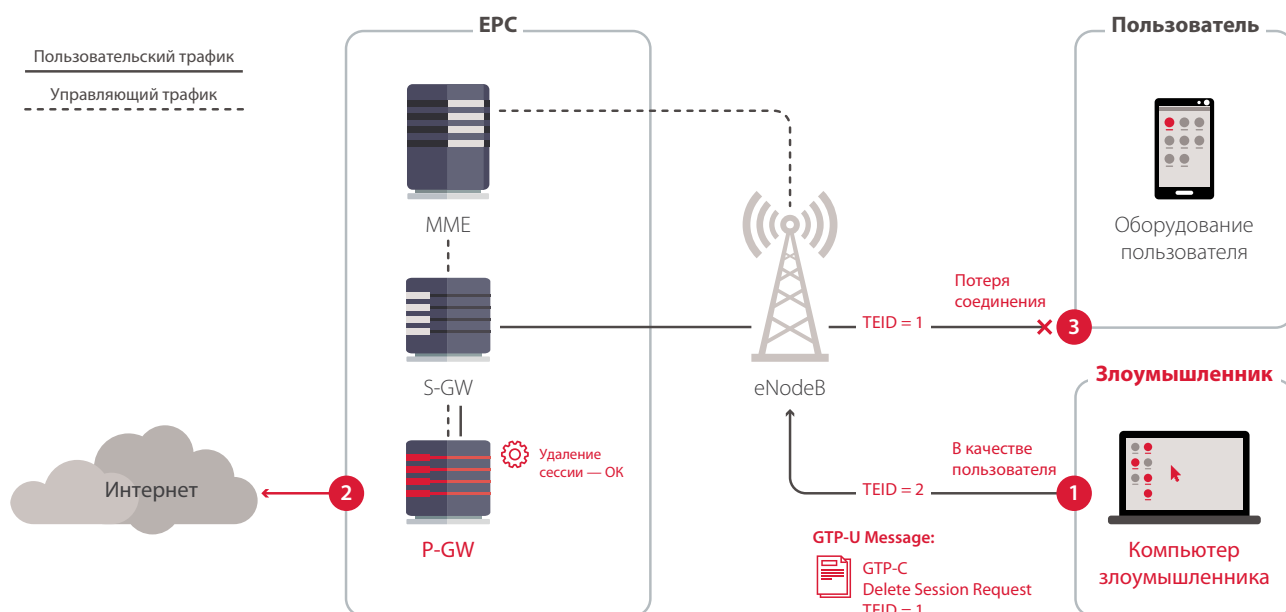


Рис. 11. Атаки возможны не только изнутри сети, но и с мобильного телефона абонента

Например, для проведения DoS-атаки в отношении определенного пользователя достаточно отправить на шлюз P-GW служебные запросы GTP-C на отключение абонента «Delete Session Request» от имени другого пользователя по пользовательскому туннелю GTP-U.

ЗАКЛЮЧЕНИЕ

В отчете продемонстрированы основные угрозы безопасности, связанные с особенностями основного компонента мобильных сетей 4G (LTE) — ядра пакетной сети EPC. В условиях доступности интерфейсов для потенциальных злоумышленников из внешних сетей и недостаточного внимания производителей телекоммуникационного оборудования к вопросам защищенности, телеком-операторы оказались не готовы противостоять атакам.

Упрощенная структура ядра пакетной сети и переход к модели All IP Network дают потенциальным злоумышленникам возможность использовать широкий спектр готовых инструментов для осуществления таких атак, как подделка сессий абонентов с целью мошенничества, перехват SMS-сообщений и электронной почты, прослушивание звонков VoLTE, блокирование связи.

Некоторые угрозы вызваны недостатками в конфигурации оборудования — например, отсутствием проверки IP-адреса и порта отправителя на устройстве. Такие факторы позволяют атакующему подменять адрес отправителя или создавать, перехватывать и завершать сессии от имени абонента. Другие проблемы являются следствием отсутствием шифрования на интерфейсах устройств, которое дает злоумышленнику возможность эксплуатировать служебную информацию телеком-оператора в своих целях.

Надо понимать, что упрощение защитных механизмов или полное их отсутствие — это осознанный выбор, сделанный разработчиками оборудования в пользу сокращения задержек на сети и повышения скорости обработки данных. Сегодня конкуренция в сфере телекоммуникаций вынуждает операторов сотовой связи молниеносно абсорбировать новые технологии, не учитывая защищенность абонентов. Также очевидно, что любой дополнительный элемент, например Security Gateway, будет вносить соответствующую задержку.

Однако в ближайшие годы с развитием интернета вещей (IoT) и промышленного интернета вещей (IIoT) вопросы безопасности сетей 4G обретут значительно большую актуальность. Например, согласно прогнозам Международного совета по повестке в области будущего ПО и общества, озвученным в рамках Всемирного экономического форума, к 2026 году 10% всех автомобилей в мире будут беспилотными⁶. К этому моменту ожидается появление первого умного города, автоматически управляющего энергетикой, логистикой и трафиком, а также компьютерного разума, участвующего в принятии бизнес-решений на

⁶ www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

уровне совета директоров. Эксплуатация слабозащищенных каналов коммуникации и злонамеренные нарушения в работе таких систем могут приводить к серьезным последствиям для жизнеобеспечения городов, техногенным авариям на промышленных объектах, транспортным коллапсам. Поэтому операторы сотовой связи, которые первыми построят безопасную экосистему для подключения инфраструктуры IoT, приобретут мощное конкурентное преимущество.

Операторы сотовой связи должны обеспечивать защиту коммуникаций и своего оборудования от несанкционированного доступа и регулярно исследовать защищенность инфраструктуры, особенно на стыках с сетями межоператорского взаимодействия (GRX в случае EPC). Для выработки адекватных мер необходимо в первую очередь провести анализ защищенности оборудования ядра пакетной и сигнальной сети. Требуется проанализировать потенциальные векторы атак, доступные для злоумышленника, и оценить связанные с ними риски. Рекомендации по результатам анализа могут включать как меры по предотвращению физического доступа к оборудованию и коммуникациям, так и меры по логической защите данных от несанкционированного доступа, например с помощью IPSec.

Надо помнить, что изменение численного или качественного состава оборудования меняет конфигурацию сети и может снизить уровень ее безопасности. В таком случае специальные средства мониторинга, анализа и фильтрации сообщений, пересекающих границы сети, позволят поддерживать настройки безопасности в актуальном состоянии.

Реализация этих мер в их необходимой полноте всецело лежит на конкретном операторе связи или организации, обслуживающей сеть в интересах одного или нескольких операторов.

ТЕРМИНЫ И СОКРАЩЕНИЯ

3GPP (The 3rd Generation Partnership Project) — консорциум, разрабатывающий спецификации для мобильной телефонии.

AUC (Authentication Center) — центр аутентификации.

CDR (Charging Data Record) — запись данных о списании.

CGF (Charging Gateway Function) — шлюз между 3GPP-сетью и системами биллинга, передает CDR в биллинговую систему.

Diameter — протокол AAA (авторизация, аутентификация, аккаунтинг) для компьютерных сетей.

DPI (Deep Packet Inspection) — система глубокого анализа сетевых пакетов.

EIR (Equipment Identification Register) — реестр идентификации оборудования, содержит перечень идентификаторов (IMEI) телефонов, которым разрешен доступ в сеть оператора.

eNodeB (Evolved Node B) — базовая станция в сетях LTE.

GRX (GPRS Roaming Exchange) — сеть обмена роуминговым трафиком между операторами.

GTP-C — протокол управления туннелями стандарта GTP.

GTP-U — протокол передачи пользовательского трафика через туннели стандарта GTP.

HLR (Home Location Register) — база данных, содержащая информацию об абонентах сети.

HSS (Home Subscriber Server) — сервер домашних абонентов, аналог HLR в сетях LTE.

IMS (IP Multimedia Core Network Subsystem) — система передачи мультимедийного содержимого на основе IP-протокола.

IMSI (International Mobile Subscriber Identity) — международный идентификатор мобильного абонента, уникальный идентификатор записанный в SIM-карту.

LTE (Long Term Evolution) — стандарт беспроводной высокоскоростной передачи данных в сетях мобильных операторов.

MME (Mobility Management Entity) — узел управления мобильностью, обеспечивает безразрывную связь при перемещениях абонента между базовыми станциями.

OCS (Online Charging System) — система онлайн-биллинга.

OFCS (Offline Charging System) — система офлайн-биллинга (постфактум).

MSISDN (Mobile Station ISDN Number) — номер телефона мобильного абонента.

PCEF (Policy and Charging Enforcement Function) — функциональный элемент, осуществляющий применение PCC-правил, полученных от PCRF.

PCRF (Policy and Charging Rules Function) — функциональный элемент, осуществляющий решения по применению PCC-правил.

PCC (Policy and Charging Control) — контроль качества обслуживания, разрешение (запрещение) сервисов для абонента.

P-GW (Packet Data Network Gateway) — шлюз к сетям передачи данных.

S1AP (S1 Application Protocol) — сигнальный протокол между EPC и радиоподсистемой.

SCTP (Stream Control Transmission Protocol) — протокол транспортного уровня в сетях IP.

S-GW (Serving Gateway) — обслуживающий шлюз, предназначен для обработки пакетов на границе EPC и радиоподсистемы.

SS7 (Signaling System No. 7) — система сигнализации № 7.

TEID (Tunnel Endpoint Identifier) — идентификатор GTP-туннеля.

TMSI (Temporary Mobile Subscriber Identity) — временный идентификатор абонента, служит для сокрытия IMSI в радиозфере.

UDP (User Datagram Protocol) — транспортный протокол в IP-сетях.

UE (User Equipment) — пользовательское оборудование.

VLR (Visitor Location Register) — временная база данных абонентов, которые находятся в зоне действия определенного центра мобильной коммутации.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована ФСТЭК России и в системе добровольной сертификации «Газпромсерт». Организации во многих странах 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 телеком-операторов.