

СЦЕНАРИИ АТАК НА СИГНАЛЬНУЮ ИНФРАСТРУКТУРУ МОБИЛЬНЫХ СЕТЕЙ ЧЕТВЕРТОГО ПОКОЛЕНИЯ



2017

POSITIVE TECHNOLOGIES

Содержание

Введение.....	3
Сценарии атак в сети на базе Diameter.....	3
Подготовка к атакам на абонентов и оборудование мобильной сети 4G.....	3
1. Раскрытие местоположения абонента.....	5
2. Перехват SMS-сообщений.....	7
3. DoS-атака на абонента.....	8
4. DoS-атака на оборудование оператора.....	9
5. Мошенничество.....	10
Заключение.....	11
Термины и сокращения.....	12

Введение

Мобильные сети четвертого поколения (4G) с каждым годом становятся все более распространенными. На сегодняшний день почти все крупные мобильные операторы в мире предлагают своим абонентам воспользоваться преимуществами, которые обеспечивают сети 4G. Разумеется, при этом пользователи ожидают от оператора, которому они доверяют, высокого уровня качества связи и защиты данных.

Практически все абоненты сетей четвертого поколения так или иначе являются и абонентами сетей предыдущего поколения. Например, если мобильный оператор сети LTE может обеспечивать только передачу данных, то для совершения звонка и передачи SMS используется технология временного переключения на сети предыдущего поколения — Circuit-Switched FallBack. Этот процесс можно заметить на большинстве смартфонов по изменению значка сети — как правило, с «4G» он меняется на «3G», «H», «E» и даже «G», если до этого передавались какие-либо данные. Поэтому абоненты сетей 4G остаются подвержены угрозам, характерным для сетей предыдущего поколения¹.

В настоящем исследовании показано, что на один из основных сигнальных протоколов в сетях четвертого поколения — Diameter — возможно реализовать те же атаки, что и ранее опубликованные нами в отчете по уязвимостям сетей мобильной связи на основе сигнального протокола SS7². В 2016 году каждая исследованная экспертами Positive Technologies сеть 4G на базе сигнального протокола Diameter обладала уязвимостями, позволяющими реализовывать атаки, связанные с определением местоположения абонента, перехватом SMS-сообщений, отказом в обслуживании и другими нелегитимными действиями.

Сценарии атак в сети на базе Diameter

Само название протокола Diameter является игрой слов: диаметр — удвоенный радиус. A RADIUS это протокол-предшественник, и Diameter должен превосходить его возможности. В стандарт протокола изначально заложены возможности защиты данных как на сетевом, так и на транспортном уровне, однако в реальности операторы далеко не всегда их используют. При этом применение этих возможностей не всегда защищает от действий недобросовестных сотрудников, несанкционированного доступа местных и иностранных разведывательных органов, а также легально действующих фирм и групп, которые используют свои знания и возможности эксплуатации уязвимостей сигнальных сетей для осуществления деятельности по негласному наблюдению и кибершпионажу.

Подготовка к атакам на абонентов и оборудование мобильной сети 4G

Для проведения практически любой атаки перед злоумышленником стоит задача первичного сбора информации об атакуемой сети и атакуемом абоненте. Поскольку в типичном сценарии атаки злоумышленник выдает себя за роуминг-партнера, то перед началом атаки необходимо располагать следующими данными:

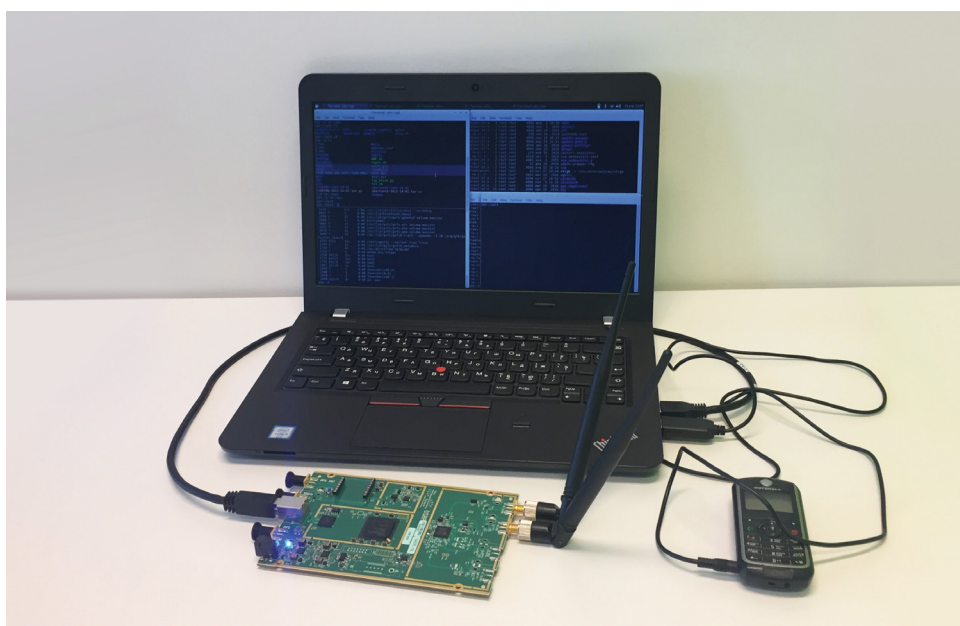
- + IP-адреса атакуемых пограничных узлов сети Diameter, к которым относятся пограничные агенты (DEA) и агенты маршрутизации (DRA), вместе и их идентификаторами;
- + идентификаторы узлов сети других операторов, с которыми может взаимодействовать атакуемый оператор для того, чтобы выдавать себя за легального роуминг-партнера.

¹ www.ptsecurity.com/upload/ptru/analytics/SS7-Vulnerability-2016-rus.pdf

² www.ptsecurity.com/upload/corporate/ru-ru/download/PT_SS7_security_2014_rus.pdf

Для атаки, направленной на конкретного абонента, как правило, необходимо знать его международный идентификатор абонента мобильной сети (IMSI). IMSI служит для уникальной идентификации абонента сотовой связи по всему миру. По IMSI можно определить, в какой стране и у какого оператора зарегистрирован абонент.

Существует несколько техник, позволяющих узнать IMSI абонента. Пожалуй, наиболее распространенной техникой является проведение атаки на раскрытие IMSI через уязвимости сигнального протокола SS7. Как было сказано выше, это возможно из-за того, что по тем или иным причинам практически все абоненты сетей четвертого поколения также являются абонентами сетей предыдущего поколения.



Возможна кража идентификатора IMSI с применением технических средств, так называемых IMSI-catchers. Это устройство способно полностью подменить собой базовую станцию сотовой сети и позволить злоумышленнику перехватывать информацию о пользователях мобильных телефонов, подключившихся к нему, в том числе и идентификаторы IMSI.

Некоторые операторы предоставляют возможность осуществлять звонки через сеть Wi-Fi³, в таком случае любой владелец точки Wi-Fi может использовать ее как дешевый IMSI-catcher.

Кроме того, в Интернете существуют как бесплатные⁴, так и платные⁵ сервисы, позволяющие по номеру абонента узнать его IMSI.

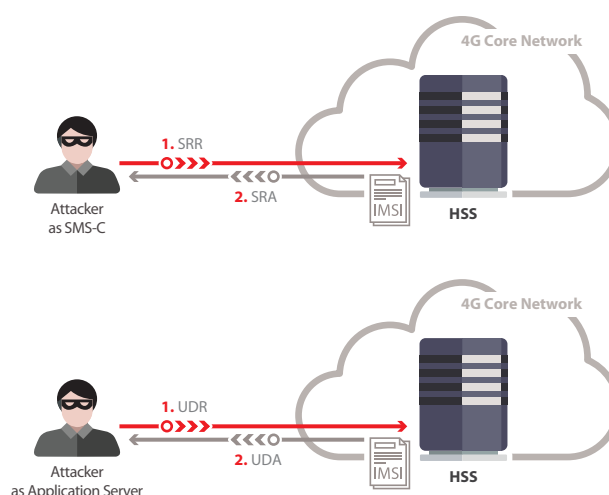
Также существуют способы получить IMSI абонента через сеть на базе Diameter. Для проведения атаки злоумышленнику необходимо знать номер мобильного абонента (MSISDN) и адрес пограничного узла сигнальной сети на базе Diameter.

Сценарий атаки может выглядеть следующим образом. Злоумышленник, выступая в роли SMS-центра (SMS-C), посылает серверу абонентских данных (HSS) специально сформированное сообщение SRR (Send-Routing-Info-for-SM-Request). В случае успеха атакующий в ответ получит IMSI атакуемого абонента.

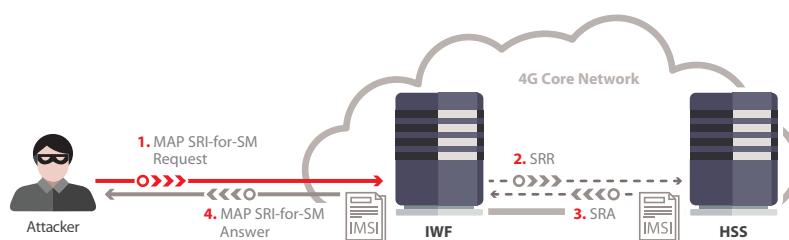
³ WiFi-Based IMSI Catcher // blackhat.com/docs/eu-16/materials/eu-16-OHanlon-WiFi-IMSI-Catcher.pdf

⁴ Проверка номера HLR-запросом: smc.ru/testhlr

⁵ HLR Number Lookup: txtnation.com/mobile-messaging/hlr-number-lookup



В другой ситуации атакующий может представиться сервером приложений и посылать HSS специально сформированное сообщение UDR (User-Data-Request). Полученные от HSS данные также будут содержать IMSI атакуемого абонента.



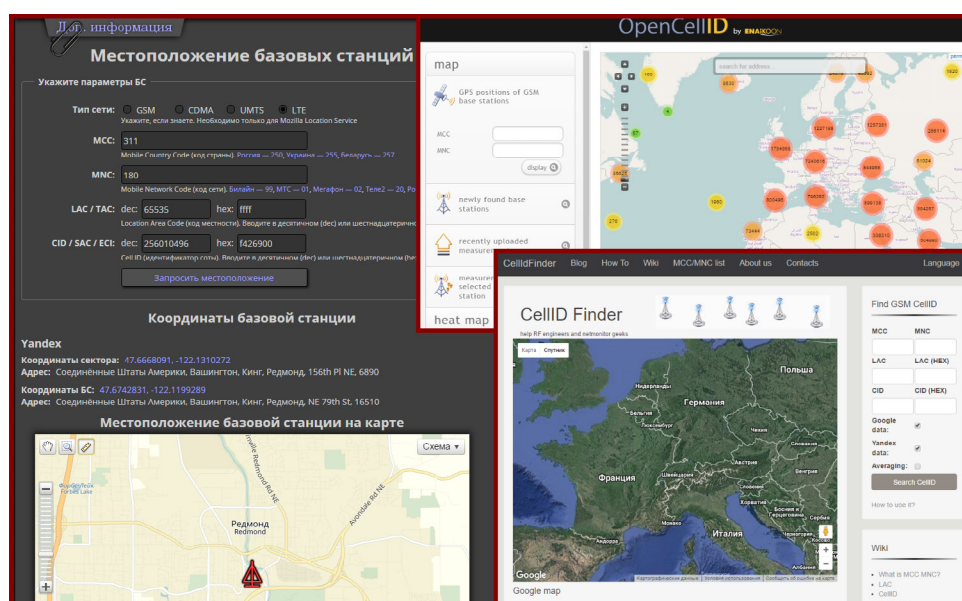
Еще один возможный вариант раскрытия идентификатора IMSI — атака на узел, обеспечивающий совместимость сети на базе Diameter с сетями предыдущих поколений посредством трансляции протокола MAP SS7 в Diameter и наоборот (IWF). В данном случае запрос SRI4SM из MAP SS7 транслируется в аналогичный Diameter-запрос SRR. В ответе злоумышленник опять получит IMSI запрашиваемого абонента.

После того, как злоумышленник тем или иным способом получит IMSI абонента и адреса узлов мобильной сети, которые его обслуживают, он сможет не только организовать слежку за абонентом, в любой момент определяя его местоположение, читать его личную переписку или даже перехватывать одноразовые пароли для интернет-банкинга, но и вообще препятствовать работе пользователя, постоянно отключая его от сети 4G или блокируя доступ к определенным услугам связи.

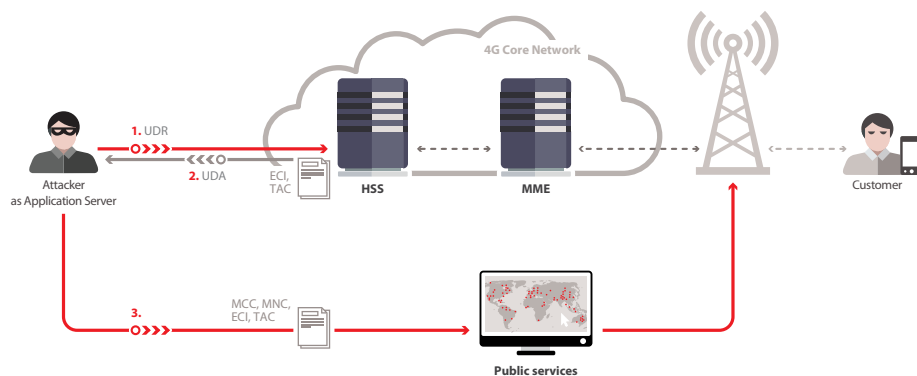
1. Раскрытие местоположения абонента

Пожалуй, одной из самых распространенных атак в сети Diameter является атака, позволяющая определить текущее местоположение абонента. Полученная информация может использоваться как при поиске человека, так и при негласной слежке за ним.

Например, злоумышленники могут применить подобную технику для компрометации политика или бизнесмена, опубликовав сведения о том, где, когда и с кем тот или иной абонент проводил встречи. В подобных случаях расследование покажет, что имела место утечка информации на стороне телеком-оператора.



Главная задача атакующего это получение идентификатора соты (CID или ECI) и кода зоны отслеживания (TAC или LAC). Google, Яндекс, Mozilla Location Services, OpenCellId предоставляют сервисы определения примерного местоположения пользователя по этим данным. Любой ресурс в сети Интернет, используя API этих сервисов, может не только запрашивать координаты расположения пользователя или базовой станции, которая его обслуживает, но и показывать результат на карте^{6,7,8}.

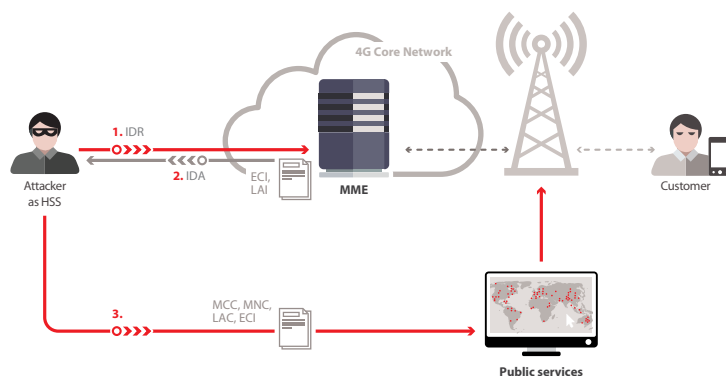


Существует несколько подходов к получению информации о местоположении абонента, и атака может проходить по следующим сценариям. В одном случае атакующий, выступая в роли сервера приложений, посылает HSS сообщение UDR, сформированное специальным образом. Если запрос проходит, то в полученном ответе будут содержаться идентификатор соты ECI и код зоны отслеживания TAC. Этой информации достаточно для того, чтобы определить местоположение пользователя с точностью до нескольких сотен метров, воспользовавшись одним из публичных онлайн-сервисов, о которых говорилось ранее. Далее, используя любой картографический сервис (к примеру, Google Maps или Яндекс.Карты), можно определить место, соответствующее точке с заданными координатами.

⁶ Местоположение базовых станций: xinit.ru/bs/

⁷ Find GSM base station cell id coordinates: cellidfinder.com

⁸ CellTower Locator: cell2gps.com



В другом случае атакующий, выдавая себя за HSS и направляя сообщение IDR (Insert-Subscriber-Data-Request) узлу управления мобильностью (MME), получает данные, по которым восстанавливаются идентификатор соты и код зоны отслеживания. Затем, как уже говорилось, через публичные сервисы в Интернете он устанавливает местоположение пользователя.

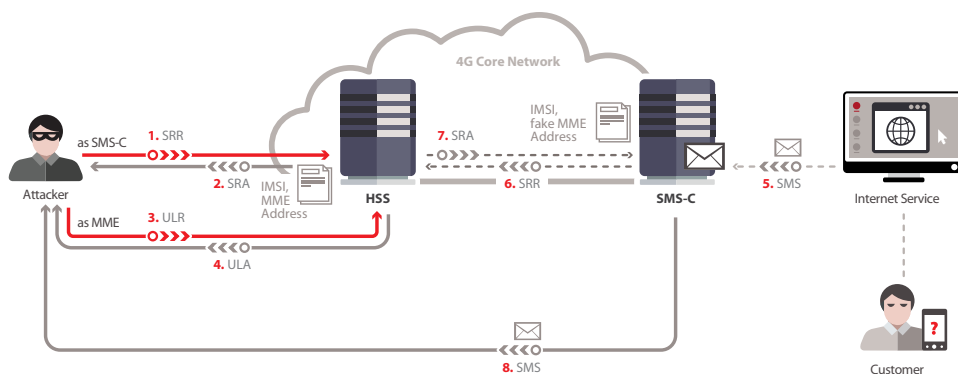
Таким образом, задача определения расположения пользователя и, следовательно, негласной слежки за ним, является тривиальной для любого, кто обладает доступом к сигнальной сети на основе Diameter. Более того, абонент никаким образом не может узнать о том, что кто-то получает информацию о его расположении и перемещении.

2. Перехват SMS-сообщений

Данная атака очень опасна для абонентов в контексте двухфакторной аутентификации, в основе которой лежит подтверждение операций через SMS, в том числе при работе с интернет-банкингом. Воспользовавшись данной уязвимостью, злоумышленник сможет украсть деньги пользователя со счета, при этом для банка это будет выглядеть как легитимное действие клиента с использованием двухфакторной авторизации. Пользователю в таком случае практически невозможно оспорить транзакцию.

В основе атаки по перехвату SMS-сообщений в сети на основе Diameter лежит идея аналогичной атаки, проводимой в сетях на базе SS7.

Злоумышленник, заранее зная номер абонента MSISDN и действуя как SMS-центр, посылает запрос SRR на HSS, в ответ на который получит информацию, в которой содержатся IMSI абонента и сведения об MME, который в данный момент обслуживает атакуемого пользователя.



Затем, выступая в роли MME, атакующий посылает запрос ULR (Update-Location-Request) на HSS и в случае успеха получает соответствующий ответ ULA (Update-Location-Answer). Тогда в HSS будет храниться обновленная информация, что атакуемый пользователь обслуживается на подставном MME и связан с SMS-центром злоумышленника.

Стоит отметить одну важную особенность протокола Diameter, среди прочего способствующую реализации этой атаки. Ответ на запрос всегда возвращается тому узлу, который его послал, вне зависимости от того, какая информация была указана в паре Origin-Host.

Далее атакующий может спровоцировать отправку SMS для восстановления пароля в каком-либо сервисе (социальная сеть, мессенджер и т. п.) или для подтверждения денежного перевода через систему ДБО.

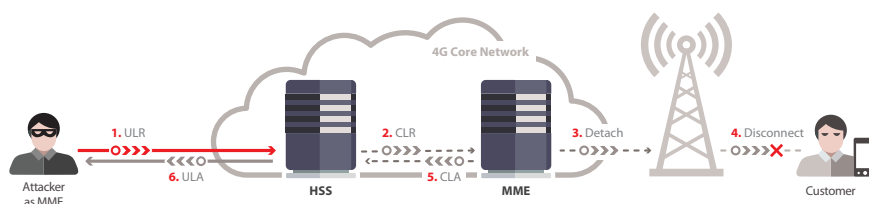
SMS-центр оператора запрашивает у HSS информацию об MME, который обслуживает атакуемого пользователя. HSS отвечает информацией о том, что пользователя обслуживают подставные MME и SMS-центр. Затем SMS-сообщение с конфиденциальными данными пользователя отправляется на подставной SMS-центр, подконтрольный злоумышленнику.

Используя код подтверждения из полученного SMS-сообщения, атакующий в одном случае может получить полный доступ к данным профиля пользователя в социальной сети и личной переписке, произвести смену пароля для входа, а также разместить от имени пользователя информацию, которая может нанести вред его репутации. В другом случае злоумышленник через систему ДБО может получить доступ к управлению банковским счетом пользователя и произвести хищение имеющихся на нем денежных средств.

Факт перехвата SMS-сообщений абонент может определить только по косвенным признакам. В частности, если на него производится подобная атака, он не будет получать никаких входящих SMS-сообщений.

3. DoS-атака на абонента

Ряд фундаментальных особенностей реализации протокола Diameter дает возможность провести простейшую, но вместе с этим довольно эффективную атаку типа «отказ в обслуживании» (DoS) на одного или многих абонентов. Несмотря на простоту и относительно небольшой ущерб, такие DoS-атаки на самом деле подрывают доверие абонента к оператору и в долгосрочной перспективе приводят к финансовым потерям.



При реализации этой атаки злоумышленнику необходимо заставить HSS «думать», что теперь он как MME обслуживает абонента с заданным IMSI. Тогда HSS инициирует процедуру отключения абонента от старого MME, после чего пользователь потеряет связь с сетью 4G.

Для этого злоумышленник, выступая в роли MME, посылает поддельное сообщение ULR к HSS с запросом на обновление соответствующей идентификационной информации и сообщает от своего имени, что в данный момент именно он как MME обслуживает это абонентское устройство. Когда HSS обновит базу, он отправит сообщение CLR (Cancel-Location-Request) на настоящий узел MME, ранее обслуживавший абонента, после чего

этот MME инициирует процедуру отключения абонента от сети передачи данных. Кроме того, если в сети оператора протокол Diameter применяется при осуществлении звонков (VoLTE) и пересылке SMS-сообщений, то для пользователя эти услуги окажутся также недоступны.

Конечно пользователь может попытаться исправить ситуацию, переподключившись к сети: для этого необходимо вновь зарегистрироваться в сети, например, перезагрузив устройство, подключенное к сети 4G. Однако злоумышленник может отправлять множество поддельных запросов, тем самым полностью блокируя подключение абонента и перегружая HSS паразитным сигнальным трафиком.

4. DoS-атака на оборудование оператора

Помимо DoS-атаки, направленной на абонента, злоумышленник потенциально может проводить аналогичные атаки и против оборудования оператора, нарушая его работу и вызывая прерывание предоставления услуг связи уже не одному, а множеству абонентов атакуемого оператора. Сейчас и в ближайшем будущем с широким развитием Интернета вещей (с использованием технологий LTE-M и 5G) и, в частности, систем «умного города» и самоуправляемых connected cars, атаки данного рода могут полностью парализовать город, а телекоммуникационные сети здесь будут лишь каналом, с помощью которого такие атаки стали возможными.

Протокол Diameter, так же, как и любой IP-протокол, может быть подвержен атакам типа «отказ в обслуживании» (DoS и DDoS) и другим атакам, применимым к IP-сетям. Поскольку телекоммуникационное оборудование производится и используется достаточно узким кругом компаний, то зачастую оно не проходит должного всестороннего тестирования и содержит большое число уязвимостей, эксплуатация которых может приводить к негативным последствиям, начиная с нарушения доступности оборудования и заканчивая удаленным выполнением произвольного кода.

Как свидетельствуют результаты работ по анализу защищенности сигнальных сетей на базе Diameter, проведенные экспертами Positive Technologies в 2016 году, каждый второй элемент исследованных сетей можно было вывести из строя направляемым ему пакетом со всего лишь одним неправильным битом.

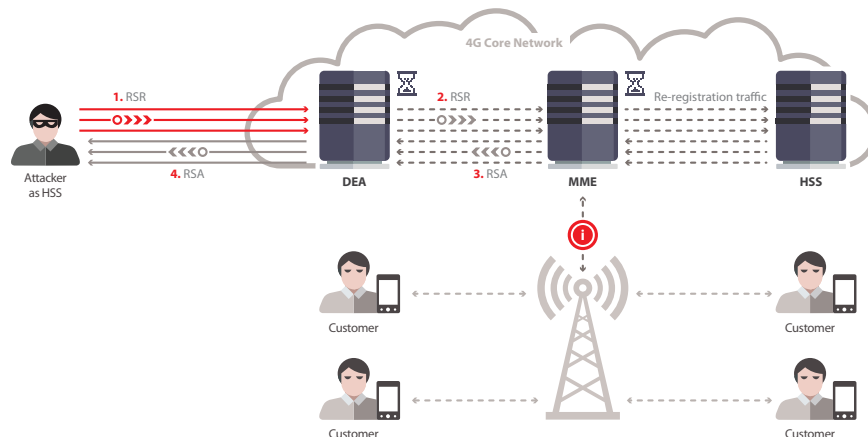
Перегрузка и выход из строя серверов Diameter могут повлечь за собой ряд серьезных последствий:

- + из-за перебоев в работе узлов сети недовольные качеством связи абоненты будут переходить к конкурентам;
- + злоумышленники получают возможность совершать противоправные действия и скрывать свое местоположение от правоохранительных органов, использующих системы законного перехвата;
- + возникающие случайно или по воле злоумышленников ошибки в биллинге и правилах применения тарифных планов к заданным пользователям будут приводить к фроду и недовольству пострадавших абонентов.

Все перечисленные последствия, несомненно, приведут не только к потере репутации надежного оператора связи, но и к прямым финансовым потерям.

Исходя из сказанного, надо учитывать, что протокол Diameter не имеет адекватной защиты от любого вида перегрузок. Более того, причиной спонтанного увеличения сигнального трафика может быть, например, сконструированное с ошибками или специальным образом измененное пользовательское приложение.

Существует несколько приемов и техник проведения DoS-атак в сети на основе Diameter. Простейшей является атака на истощение ресурсов узла сети путем отправки множества запросов CER (Capabilities-Exchange-Request) на установление соединения.

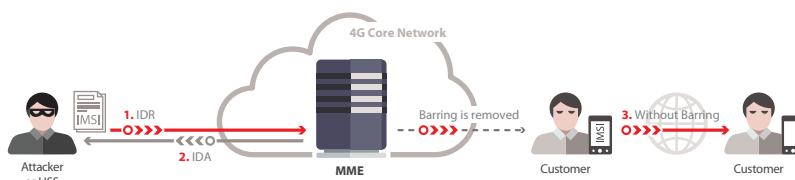


Кроме того, на истощение ресурсов может быть направлена посылка от лица HSS множества сообщений RSR (Reset-Request) на MME, обслуживающий абонентов из известного диапазона IMSI абонентов. Большой поток такого рода сообщений может вызвать лавинообразный всплеск объемов сигнального трафика между MME и реальным HSS, что впоследствии может нарушить его работоспособность, а значит — работоспособность сети в целом.

5. Мошенничество

В сетях на основе протокола Diameter существуют реализации атак, при которых злоумышленнику становятся доступны бесплатные услуги связи, такие как звонки, SMS, передача данных за счет оператора либо других абонентов, что приводит к прямой потере денег оператором.

Подобного рода атаки требуют исключительной информированности атакующего о внутренних процессах и устройствах сети оператора, особенно если речь идет о попытках изменить правила, применяемые к абоненту. Однако часть атак можно провести и обладая менее значительной начальной информацией — IMSI абонента и адресами некоторых узлов сети на базе Diameter. К таким атакам можно отнести попытки перенаправления потоков биллинга на несуществующий или подконтрольный расчетный сервер, а также снятия запрета на обслуживание или предоставление определенных услуг (barring).



Последний способ реализуется путем посылки специально сформированного сообщения IDR на MME. Атакующий выступает в роли HSS. В сообщении IDR удаляются сведения о запрете на обслуживание и предоставление услуг, что позволяет абоненту с указанным IMSI или MSISDN получить потенциально неограниченный доступ к ресурсам, которые обычно ему не предоставляются (например, к услугам, которые не предусмотрены его тарифным планом).

Заключение

В отчете рассмотрены угрозы безопасности абонентов в сети на основе Diameter, связанные с тем, что любой подготовленный злоумышленник, специальная группа или иностранные разведывательные органы могут с легкостью заполучить информацию о текущем месторасположении абонента, а затем использовать ее при негласной слежке, шпионаже или для публичного разглашения сведений о перемещениях абонента. Проблемы с конфигурацией оборудования и сервисов могут приводить к реализации угрозы перехвата пользовательских данных, в том числе SMS-сообщений. Эту возможность злоумышленник может использовать для получения доступа к системе ДБО, в которой для подтверждения входа пользователя используются временные пароли, пересылаемые по SMS. Перехватив временный пароль, атакующий получит полный доступ к системе ДБО пользователя и может похитить все денежные средства, которыми тот располагает. При этом пользователю во время кражи средств с банковского счета может быть заблокирован доступ к сети связи, таким образом он не будет получать уведомления ни через SMS-сообщения, ни по электронной почте — в связи с блокировкой услуг, предоставляющих доступ к мобильному Интернету. Более того, пользователь не сможет связаться с банком, чтобы произвести блокировку счета, поскольку оборудование оператора будет «считать», что он находится в другом регионе, и постоянно отключать его от сети.

Подобный сценарий описывает лишь некоторые возможности, которые получают злоумышленники в сигнальной сети оператора связи, оборудование и сервисы которого имеют ошибки в конфигурации. Для того чтобы минимизировать риски, связанные с рассмотренными угрозами, рекомендуется регулярно проводить анализ защищенности сигнальной сети. Надо понимать, что внедрение нового оборудования или внесение изменений в конфигурацию существующих устройств может повлиять на безопасность сети, поэтому такой анализ следует проводить периодически.

Для устранения угроз и поддержания настроек безопасности сети в актуальном состоянии необходимо осуществлять постоянный мониторинг, анализ и фильтрацию сообщений, пересекающих границы сети. С подобными задачами позволяют справиться специализированные системы обнаружения атак и оборудование, поддерживающее функциональность межсетевого экранирования сигнальных сообщений.

Термины и сокращения

DEA (Diameter Edge Agent) — пограничный агент. Обычно он функционирует на границе сигнальной сети оператора и служит в качестве прокси-агента для сигнального трафика из сетей других операторов.

DRA (Diameter Routing Agent) — агент маршрутизации. Осуществляет маршрутизацию Diameter-трафика.

HSS (Home Subscriber Server) — сервер абонентских данных. Один из важнейших элементов в инфраструктуре сетей четвертого поколения стандарта LTE, служит для хранения важной пользовательской информации и информации о действиях абонентов.

IMSI (International Mobile Subscriber Identity) — международный идентификатор абонента мобильной сети. Служит для уникальной идентификации абонента сотовой связи в пределах всего мира.

IWF (Interworking Function) — агент, осуществляющий трансляцию протокола MAP SS7 в Diameter для обеспечения стыковки с сетями предыдущих поколений.

MME (Mobility Management Entity) — узел управления мобильностью. Обеспечивает возможность переключения между базовыми станциями, работу в роуминге, аутентификацию пользовательских устройств, взаимодействуя с HSS, а также отвечает за выбор обслуживающего шлюза S-GW.

MSISDN (Mobile Station ISDN) — номер мобильного абонента цифровой сети с интеграцией служб.

S-GW (Serving Gateway) — обслуживающий шлюз. Обеспечивает передачу и обработку пользовательских данных, поступающих от пользовательских устройств из или в подсистему базовых станций оператора.

SMS-C (SMS-Service Centre) — SMS-центр. Отвечает за работу службы коротких сообщений сети мобильной связи.

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

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.