

Безопасность системы маршрутизации Интернета

Андрей Робачевский
Технический директор RIPE NCC

Один из основных принципов Интернета – сеть прозрачна и функционально проста, все возможности Интернета обеспечиваются приложениями, сложность и разнообразие которых не знает предела. Новые приложения приносят дополнительные услуги, а их внедрение возможно с минимальными затратами, поскольку не требует изменений самой Сети и связанными с этим новыми технологиями, координацией и так далее. Совсем не так, как в телефонной сети, где приложения, собственно телефоны, являются пользовательским интерфейсом к функциям сети.

Без сомнения, этот принцип обеспечил бурное развитие и многообразие Интернета, превратив его из научно-исследовательского проекта в телекоммуникационную инфраструктуру, в корне изменившую представление об информации и доступе к ней.

Но не следует забывать о самой Сети. Список функций, на которые рассчитывают приложения, невелик и по существу включает передачу пакетов, надежное разрешение имен (трансляцию имени ресурса в IP-адрес сервера) и выбор правильного эффективного пути от отправителя к получателю. Что, в свою очередь, подразумевает каналы связи и маршрутизаторы, системы DNS (Domain Name System, <http://ru.wikipedia.org/wiki/DNS>) и систему маршрутизации. От надежности и безопасности этих фундаментальных систем Интернета в конечном итоге зависит работа всего многообразия «умных» приложений, без которых наша сегодняшняя жизнь уже немыслима.

Сегодня речь пойдет об одной из этих систем – системе маршрутизации.

Архитектура и эволюция системы маршрутизации

Маршрутизация между сетями в Интернете осуществляется с помощью протокола BGP (Border Gateway Protocol, http://ru.wikipedia.org/wiki/Border_Gateway_Protocol). Суть его заключается в том, что каждая сеть получает от своих соседей – пиров – информацию о связности, а именно через какую цепочку сетей доступен каждый конкретный префикс. Каждая сеть обрабатывает эту информацию в соответствии с собственной политикой, выбирая для каждого доступного префикса наилучший путь. Выбор этот основан на нескольких параметрах, основным из которых является "длина пути" – цепочка сетей, через которые пройдет трафик, чтобы достичь данного префикса. Сформированное таким образом видение Интернета сеть, в свою очередь, также сообщает своим пирам.

Здесь следует отметить, что маршрутизация осуществляется не между отдельными компьютерами или маршрутизаторами, а сетями, точнее доменами маршрутизации. Эти домены (отсюда термин междоменная маршрутизация – Inter-Domain Routing, IDR), также называемые Автономными Системами (Autonomous System, AS), представляют собой совокупность узлов, находящихся под единым административным контролем и имеющих согласованную политику маршрутизации. Этот аспект является одним из фундаментальных архитектурных принципов Интернета, позволяющий эффективно разделить глобальную систему маршрутизации на области с четким внутренним контролем, относительно высокой степенью безопасности и т.д. и "межобластное" пространство, основанное на кооперации и взаимодоволии.

Протокол BGP пришел на смену раннего протокола маршрутизации EGP (Exterior Gateway Protocol), использовавшегося в одной из сетей-родоначальников сегодняшнего Интернета – NSFnet. Сеть NSFnet, соединившая в 1986 году шесть суперкомпьютерных центров в США, являлась единым административным доменом и имела иерархическую архитектуру с единой опорной сетью (backbone), представлявшей логическую точку обмена трафиком и по-прежнему являвшейся в начале 1990-х опорной сетью Интернета. Протокол EGP предусматривал, что каждый узел знает всю топологию сети (а именно информацию обо всех остальных узлах и их связности) и может вычислить точный путь следования пакетов от источника к получателю. Плохая масштабируемость такого подхода привела к необходимости разработки нового протокола, когда в конце 1980-х началось значительное расширение сети.

BGP был разработан как для работы в иерархических сетях, таких как NSFnet, так и в сетях с неиерархической топологией, когда сети одного уровня иерархии – пиры – могут быть непосредственно соединены друг с другом, хотя первые версии протокола различали линки по их характеру – вверх, вниз или вбок. Благодаря этому фундаментальному изменению BGP в дальнейшем позволил развитие Интернета как коллекцию независимых, различным образом соединенных друг с другом сетей.

Первая версия протокола была стандартизована в 1989 году, хотя к тому времени он уже использовался в некоторых сетях. Согласно BGP каждый узел обменивается со своими

соседями информацией о доступных путях к другим сетям (последовательности узлов через которые должен быть передан трафик, чтобы достигнуть получателя). Таким образом, каждый узел имеет представление о различных путях, но не о топологии Интернета в целом. Поскольку сети уже не могут рассматриваться как иерархические, информация о суммарной "стоимости" пути, как это применялось в ранних протоколах маршрутизации, недостаточно, так как это может приводить к возникновению циклов. Чтобы решить эту проблему, каждый анонсируемый маршрут имеет специальный атрибут – AS_PATH, который содержит последовательность всех сетей, через которые он был передан. Если сеть обнаружит себя в списке AS_PATH полученного маршрута, это свидетельствует о цикле и такой маршрут должен быть отброшен.

Также, предполагая, что отдельные сети, находящиеся под единым административным контролем и имеющие согласованную политику маршрутизации, обеспечивают отсутствие внутренних циклов, межсетевую и внутрисетевую маршрутизацию можно рассматривать независимо. Соответственно, в контексте межсетевой маршрутизации такие сети, или автономные системы, могут рассматриваться как мета-узлы.

Выбор маршрута в BGP принимаются на основе пути и политики маршрутизации, принятой данной автономной системой. Другими словами, администратор сети может явно определить принципы выбора маршрута в определенных условиях (например, изначально политика маршрутизации в NSFnet разделяла коммерческий и некоммерческий трафик), но выбор этот основан на информации, полученной сетью от ее соседей, или пиров. При этом не существует единой эталонной топологии Интернета – каждая автономная системы вырабатывает свою собственную картину мира, которую она, в свою очередь, транслирует своим пирам.

С одной стороны данный подход позволяет значительно упростить глобальную систему маршрутизации и обеспечить масштабируемость Интернета, с другой – он основан на транзитивном доверии между взаимодействующими сетями.

Доверие – интересная вещь. Оно радикально упрощает взаимодействие между, в данном случае, сетевыми операторами и, как следствие, систему маршрутизации в целом. Это, безусловно, является одним из факторов, обеспечивших бурное развитие Интернета. С другой стороны, оно открывает существенные возможности для игроков не по правилам. Действительно, уязвимость системы, на которой основана колоссальная индустрия, поражает. Но также удивительна и сила сотрудничества между операторами, так как до сих пор нам известны только отдельные случаи злоупотребления этими возможностями.

Как можно атаковать систему маршрутизации

Говоря о системе маршрутизации можно выделить несколько общих типов атаки. Несмотря на различие целей и конечного эффекта, механизм атаки принципиально строится на возможности создания искаженной картины топологии Интернета атакуемой сетью, которая затем транзитивно распространяется по всей Сети.

Создание "Черных дыр". Целью этой атаки является недоступность сети или нескольких сетей для всего или части Интернета. Весь трафик, имеющий отношение к этим сетям, перенаправляется и затем отбрасывается. В результате все сервисы, предлагаемые данными сетями, становятся недоступными для пользователей. Основной задачей этого типа атак является Отказ в Обслуживании (Denial of Service, DoS).

Перенаправление. В этом случае трафик, предназначенный одной сети, перенаправляется в другую сеть. Часто эта сеть находится в руках атакующего и маскируется под атакуемую сеть с целью, например, получение секретной информации. Также перенаправление может быть использовано для проведения злоумышленниками определенных краткосрочных акций, например рассылки спама. После этого такая сеть, или ее фантом, разумеется, исчезает. Часто злоумышленниками используется нераспределенное или давно неиспользуемое адресное пространство.

Перехват. Эта атака похожа на предыдущую, только после прохождения по сети-перехватчику трафик возвращается в нормальное русло и попадает к получателю. Из-за этого такую атаку труднее обнаружить. Целью обычно является "подслушивание" или модификация передаваемых данных.

Нестабильность. Нестабильность в глобальной системе маршрутизации может быть вызвана частыми изменениями в анонсировании конкретной сети (попеременное анонсирование и аннулирование), с целью "демпфирования" маршрутов данной сети провайдерами и, как следствие, блокирования связности.

Фабрикация адреса источника трафика. Хотя в этом случае система маршрутизации как таковая не подвергается атаке, данный метод широко используется в так называемых атаках на отражение. В этом случае обратный трафик, например ответы на изначальные запросы, направляется не к истинному источнику, а к получателю, чей адрес был сфабрикован. Как правило, такие атаки используют протокол без установления соединения UDP (User Datagram Protocol, <http://ru.wikipedia.org/wiki/Udp>) и основаны на эффекте усиления, когда небольшие запросы от многих источников порождают ответы значительно большего размера.

Одна из критических систем, в основном использующая UDP и подверженная атакам такого рода, является DNS.

Давайте рассмотрим несколько примеров атак на систему маршрутизации.

YouTube

В воскресенье, 24 февраля 2008, Pakistan Telecom (AS17557) начал несанкционированное анонсирование части адресного пространства, используемого YouTube (AS36561), а именно более конкретного (more specific) префикса 208.65.153.0/24. Один из транзитных провайдеров Pakistan Telecom, PCCW Global (AS3491) проанонсировал данный маршрут далее, в глобальный Интернет, что привело к перенаправлению трафика YouTube в глобальном масштабе.

Топология связности YouTube уже спустя 2 минуты, выглядела следующим образом:

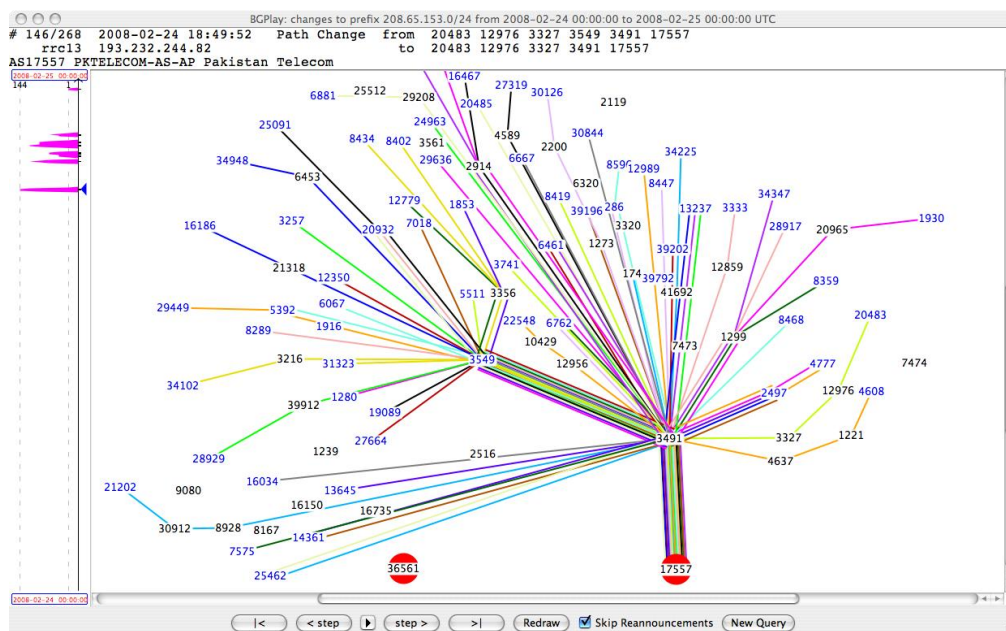


Рисунок 1 Топология связности YouTube (AS36561) после начала анонсирования префикса Pakistan Telecom (AS17557)

Как видно, весь трафик, предназначенный YouTube был перенаправлен в сеть Pakistan Telecom. Трафик этот представлял обрывки сеансов TCP, начатых с реальным сайтом YouTube, и попросту отбрасывался сетью Pakistan Telecom. Для пользователей YouTube это выглядело как недоступность ресурса.

Причиной явилось требование правительство Пакистана заблокировать доступ к враждебному сайту внутри страны. Однако результатом явилось создание типичной "черной дыры", которое привело к глобальному перебою служб YouTube.

Атака Пилосова (Pilosov)

Атака на YouTube имела значительные видимые последствия и получила широкую огласку и резонанс в сетевом сообществе. Однако ряд атак могут проходить почти незамеченными, но даже с более серьезными последствиями.

Речь идет о перехвате трафика, незаметном как для отправителя и получателя трафика, так и для большинства других участников. Целью может быть, например, перлюстрация данных, которыми обмениваются определенные сети, пользователи и т.д. Целью может также являться модификация этих данных.

Возможность и простота организации такой атаки была представлена на конференции DEFCON в августе 2008 Алексом Пилосовым (Alex Pilosov) и Антоном Капелла (Tony Karella). Они продемонстрировали, что

- практически любой префикс может быть захвачен без нарушения сквозной связности;

- это можно сделать очень незаметно, замаскировав присутствие атакующего на пути следования трафика (невидим для утилит типа traceroute, позволяющих получить список узлов, через которые передается трафик к получателю).

Суть атаки сводится к перехвату трафика стандартными методами (например, путем анонсирования атакующим более длинного префикса атакуемой сети, что делает анонс данной подсети более привлекательным с точки зрения BGP, как это произошло в случае с Pakistan Telecom). Далее трафик возвращается в прежнее русло, путем конфигурации статического маршрута атакующим. В результате трафик передается сети, являющейся частью изначального пути передачи трафика. Далее передача трафика происходит абсолютно законным путем.

Для маскировки движения трафика атакующая сеть производит манипуляцию с параметром TTL (Time To Live) пакетов перехваченного трафика. Согласно протоколу, при передаче пакета от одного маршрутизатора к другому, каждый узел сети уменьшает этот параметр на единицу. Не изменяя этот параметр при прохождении по атакующей сети, злоумышленники могут «замаскировать» этот участок, исключив, таким образом, атакующего из видимого пути передачи трафика. Для утилит типа traceroute участки пути в сети атакующего просто не попадают в список.

Атака Pílosov проиллюстрирована на рисунках 2 и 3. Первый рисунок показывает состояние системы маршрутизации перед началом атаки, когда трафик от пользователя сети AS70 доставляется через AS60 получателю сети AS200. На втором рисунке изображена связность сетей в процессе атаки. Хотя трафик перехватывается атакующей сетью AS100, этот путь не

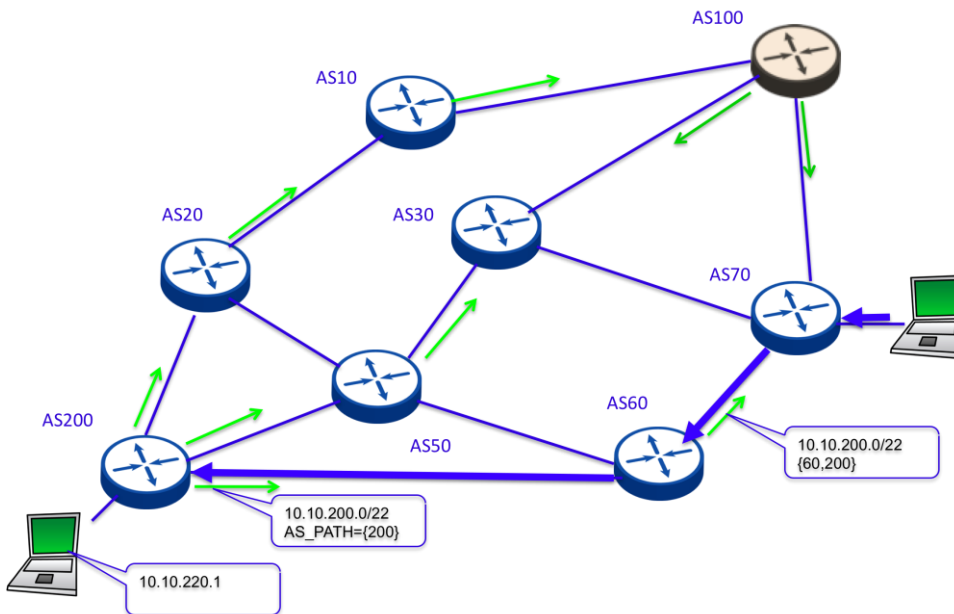


Рисунок 2 Состояние системы маршрутизации перед началом атаки Пилосова отражается программой traceroute.

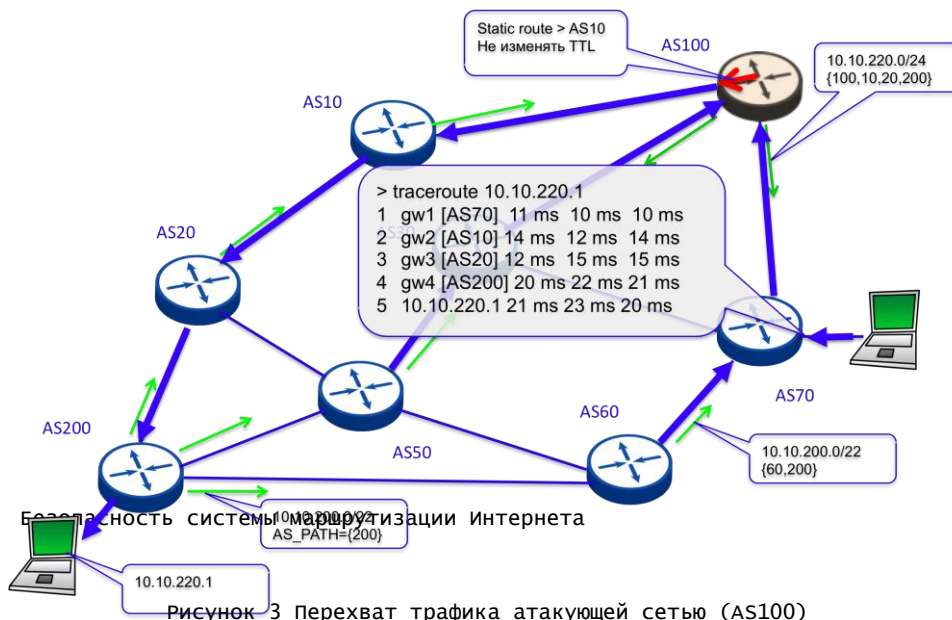


Рисунок 3 Перехват трафика атакующей сетью (AS100)

Существующая практика безопасности маршрутизации

Итак, просто доверия во многих случаях недостаточно. Даже если вы доверяете своим непосредственным пирам, где гарантия, что среди перепутья связности Интернета не найдется слабое звено? Сеть должна иметь возможность отличить правду от лжи, которая в большинстве рассмотренных случаев выражается в неправомерном присвоении какой-либо сетью чужого префикса (prefix hijacking). В этом случае политика маршрутизации сети может включать фильтрацию неправомерных анонсов, и, соответственно, препятствовать дальнейшему проникновению ложной информации в Интернете.

Безопасность и надежность системы маршрутизации во многом зависит от возможности правильного ответа на вопросы:

1. является ли префикс, полученный в сообщении BGP, правомерным (т.е. представляющим законно распределенное адресное пространство и право на его использования)?
2. является ли автономная система-отправитель сообщения BGP, правомочным источником (origin) префикса?
3. соответствует ли атрибут AS_PATH, полученный в сообщении BGP, действительному пути, который прошло данное сообщение в сети Интернет?

К сожалению, дать правильные ответы на поставленные вопросы очень трудно ввиду отсутствия надежного источника информации. Итак, что же имеется в арсенале сервис-провайдера?

Интернет-Регистратуры Маршрутизации (IRR)

Частичную помощь в решении данной проблемы оказывают Интернет-регистратуры Маршрутизации (Internet Routing Registry, IRR). Суть их заключается в следующем: сетевые операторы регистрируют в базе данных свою политику маршрутизации, а именно с кем и как сеть взаимодействует, и префиксы, которые сеть использует и анансирует в Интернет. В рамках IETF (www.ietf.org) был разработан специальный язык - RPSL (Routing Policy Specification Language), позволяющий описывать политику маршрутизации. Был также разработан инструментарий, наиболее известный - IRRToolset (<http://irrtoolset.isc.org/>), который позволяет автоматизировать конфигурацию маршрутизации провайдера по данным IRR.

Но IRR отображают весьма неполную картину, так как регистрация данных в этих базах данных сугубо добровольная. Многие операторы не хотят себе морочить голову какими-то IRR, часть операторов не регистрирует по причине нежелания разглашать свою политику. Те же, кто все же зарегистрировал свою политику, не всегда поддерживают актуальность данных. Проблема в том, что хотя эта деятельность служит на благо общего дела - безопасной системы маршрутизации, польза для самого провайдера не всегда ощутима.

Неполнота и ненадежное качество данных, а также плохая масштабируемость подхода - попробуйте-ка создать фильтры для всех префиксов, зарегистрированных в IRR! - существенно ограничивают их применение для решения проблем безопасности глобальной маршрутизации.

В результате IRR имеют весьма ограниченное распространение и в основном используются для администрирования провайдером подключенных клиентов.

whois

Можно воспользоваться более надежными данными - базами данных распределения адресного пространства на уровне Региональных Интернет-Регистратур (Regional Internet Registry, RIR). Хотя эту информацию можно получить через соответствующий whois-сервер Регистратуры, иногда более практичными способом является использование так называемых файлов статистики, доступных на сайте ftp (<ftp://ftp.ripe.net/pub/stats>). например, интернет ресурсы, распределенные RIPE NCC, представлены в файле: <ftp://ftp.ripe.net/pub/stats/ripenncc/delegated-ripenncc-latest>.

Как вы можете заметить, число записей весьма внушительно, также внушительным будет список префиксов в конфигурации ваших граничных маршрутизаторов.

База данных IANA (Internet Assigned Number Authority, www.iana.org), например <http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml> для ресурсов IPv4, является более компактной, хотя и не содержит деталей - каждая запись имеет размер /8 в случае IPv4, а детализация для адресного пространства IPv6 и того меньше. Однако данный подход позволяет по крайней мере блокировать сети, использующие нераспределенные адресные ресурсы.

Надежность границ

Глобальная безопасность маршрутизации является желаемой целью, но вряд ли легко достижимой. Между тем, если каждый оператор будет следить за «гигиеной» своих сетей-клиентов, ситуация может заметно улучшиться.

Наибольшие шансы такая стратегия имеет в сетях, с только одним уровнем подключенных клиентов. Для провайдеров более верхнего уровня (например, tier-2 или tier-1) задача учета клиентов своих клиентов является непреодолимо сложной.

Задача надежности границ двояка:

- на уровне маршрутизации не принимать анонсирование незарегистрированных сетей своих клиентов, и
- на уровне передачи трафика не принимать трафик, источником которого является незарегистрированные сети (например, с использованием сфабрикованных адресов источника)

Как мы уже обсуждали, для решения первой части проблемы может быть использована публичная IRR, или, если оператор не желает публиковать всех своих клиентов явно, собственная база данных клиентов.

Для противодействия трафику от источника с сфабрикованным адресом необходима фильтрация входного трафика (ingress filtering). Пакеты, в которых адрес отправителя не соответствует адресному пространству подключенного клиента, отбрасываются. Данный подход описан в документе IETF VSR38 (<http://www.ietf.org/rfc/rfc2827.txt>).

Одним из механизмов реализации такой фильтрации является использование так называемого метода "направления обратного пути" (reverse path forwarding, RPF). Суть его заключается в использовании имеющейся в распоряжении маршрутизатора информации о топологии сети, а именно таблиц маршрутизации. Только те пакеты, которые получены с направления лучшего пути к отправителю, передаются маршрутизатором. Логика здесь проста – если пакет пришел по тому же пути, по которому отправляются ответы, шансы велики, что отправитель истинный. Однако это предусматривает симметричность передачи прямого и обратного трафика, что в целом неверно. Решение части этих проблем описано в другом документе IETF – VSR84 (<http://www.ietf.org/rfc/rfc3704.txt>). В то же время, в случае непосредственно подключенных оконечных сетей-клиентов, такой механизм работает достаточно хорошо.

Сертификация ИНР и безопасность маршрутизации

Я подробно рассказывал о сертификации интернет-ресурсов в моей статье "Сертификация Адресных Интернет-Ресурсов". Система RPKI (Resource PKI), как более достоверная и технологичная система проверки достоверности информации о правах использования адресных интернет-ресурсов, может существенно упростить и позволить автоматизировать сегодняшние методы взаимодействия между сетевыми операторами, а также способствовать практике надежной и безопасной маршрутизации.

Текущая работа в рамках рабочей группы IETF SIDR (<http://www.ietf.org/dyn/wg/charter/sidr-charter.html>) направлена на разработку стандартов для базовой инфраструктуры RPKI и проверку подлинности отправителя. Другими словами, будучи воплощенной, система позволит определить является ли префикс, полученный в сообщении BGP, правомерным и является ли автономная система-отправитель сообщения BGP, правомочным источником (origin) префикса. То есть, ответить на два первых вопроса безопасной маршрутизации!

Ключевыми элементами этой фазы являются собственно Сертификаты Интернет-Ресурсов а также специальные объекты – ROA (Route Origin Authorisation, Разрешение на создание маршрута). В соответствии со спецификацией ROA содержит номер авторизованной автономной системы и список IP префиксов, которые эта автономная система имеет разрешение анонсировать. К этому «заявлению» прилагается сертификат, описывающий соответствующие интернет-ресурсы, и весь объект заверен цифровой подписью владельца сертификата.

Использование ROA возможно как для построения фильтров, так и в качестве дополнительного правила в процессе выбора пути BGP. Логично предположить, что интеграция информации, полученной от системы RPKI, в процесс BGP является более масштабируемым решением.

Архитектура такого решения схематично представлена на рисунке 4. Предполагается, что сервис провайдер хранит собственную копию всех объектов глобальной системы RPKI, проверяет их достоверность и периодически обновляет. Результирующая база данных содержит только достоверную информацию (достоверный кэш, validated cache) и может быть непосредственно использована процессом BGP маршрутизатора.

При получении очередного сообщения BGP, маршрутизатор запрашивает базу данных на предмет наличия префиксов, указанных в сообщении BGP. Если база данных не содержит указанных префиксов, это означает, что система RPKI не содержит ни одного правомерного объекта ROA для этих префиксов. Причин этому может быть несколько. Например, просроченный сертификат, в цепочке проверки подлинности ROA, или просто отсутствие ROA как такового. Учитывая, что внедрение данной системы будет происходить постепенно, данная ситуация

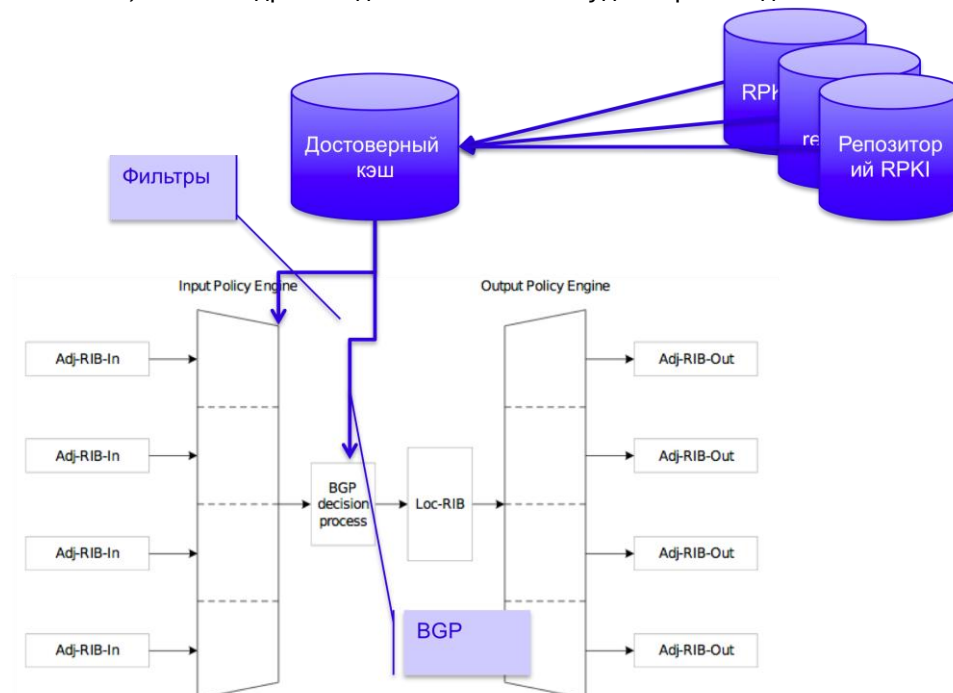


Рисунок 4 Интеграция RPKI в процесс принятия решения BGP

скорее свидетельствует, что сеть еще не использует преимущества RPKI, и такой маршрут может быть принят при отсутствии более надежного.

Напротив, если база данных содержит правомерные ROA, описывающие префиксы, указанные в анонсе BGP, но не соответствующие автономным системам-отправителям, возможно, это является свидетельством захвата префикса (prefix hijacking), и такой маршрут следует использовать с большой осторожностью. Скорее всего, его следует отбросить, даже если он единственный.

В принципе, как предлагается в Интернет-драфте draft-pmohapat-sidr-pfx-validate, результат удостоверения маршрут с использованием RPKI, является одним из критериев выбора маршрута в BGP, наряду с другими атрибутами BGP: длиной пути (AS_PATH), origin, MED (Multi-exit discriminator). В конечном счете, интерпретация этого параметра является частью политики маршрутизации данной сети.

На сегодняшний день RPKI является наиболее технологичным способом обеспечения безопасности маршрутизации, хотя и он, на данной фазе развития, не обеспечивает ее полностью. В действительности, его применимость ограничена непосредственно подключенными оконечными сетями-клиентами, также как и в большинстве других случаев. Дело в том, что пока не будет поддержана возможность установления подлинности пути передачи сообщения BGP – AS_PATH, остается возможность обмана.

Например, злоумышленник может утверждать, что автономная система, указанная в ROA, является его клиентом, путем присоединения номера этой AS в атрибут AS_PATH своих анонсов BGP. Другими словами, пока что RPKI не сможет надежно защитить глобальный Интернет от фабрикация адреса отправителя, атак типа Pilosov и YouTube.

Трудности

Основной трудностью решения задачи безопасной маршрутизации является распределенный и кооперативный характер самой системы. Польза от усилий и инвестиций отдельной сети в этой области распределяется на всех участников глобального Интернета, и в то же время лишь в незначительной степени решают проблемы данной сети.

Например, предупреждение рассмотренных атак, которые действительно могут негативно отразиться на услугах сети, зависит от действий других участников Интернета. Действия YouTube по защите собственных границ не имеют существенного влияния на возможность атаки этого ресурса, пока другие участники (PCCW Global, обеспечивающий транзит для Pakistan Telecom) готовы принять подозрительный анонс.

Ситуация похожа на обратный вариант так называемой дилеммы обедающих (http://en.wikipedia.org/wiki/Diner's_dilemma) или Трагедии Общин (http://ru.wikipedia.org/wiki/Трагедия_общин). Каждый сервис-провайдер минимизирует отношение затрат к выгоде путем ничегонеделания, рассчитывая, что в то же время другие игроки инвестируют в безопасность маршрутизации. Разумеется, если все операторы используют данную стратегию, безопасность не улучшается и в результате все проигрывают.

По своему характеру проблема мало отличается от других глобальных проблем – от глобального потепления, до внедрения IPv6. Решение таких проблем плохо укладывается в бизнес-логику коммерческих организаций ввиду отсутствия «business case» и неопределенно низкого коэффициента отдачи. До момента, пока критическая масса участников не перейдет на новые правила игры (например, полностью внедрит IPv6 или обеспечит защиту границ маршрутизации), проблема остается нерешенной, соответственно с точки зрения коммерческой выгоды единственно правильной стратегией является позиция выжидания достижения данной критической массы другими участниками.

Свет в конце тоннеля?

Однако не все так безысходно, как кажется.

Например, с точки зрения сервис провайдера, отсутствие доступа собственных клиентов к ресурсу YouTube также является серьезной проблемой. Другими словами, сервис провайдер также заинтересован в противодействии атакам на систему маршрутизации. Локальные меры по усилению безопасности, рассмотренные выше, безусловно, позволяют уменьшить вероятность таких атак.

Внимание к проблемам безопасности и меры, предпринимаемые сервис провайдером, являются косвенным свидетельством надежности и качества предоставляемых услуг в целом. По мере все большей информированности общественности о проблемах безопасности Интернета, соответствие сервис провайдером нормам защиты системы маршрутизации может явиться решающим в конкурентной борьбе за клиента.

Мониторинг состояния системы маршрутизации является еще одним из направлений, позволяющий если и не предотвратить атаку, то быстро обнаружить и уведомить соответствующих игроков. Конечно, в этом случае критичным является возможность глобального мониторинга, поскольку атака может носить весьма локальный характер и не быть видима даже вблизи атакуемой сети. Также необходимо иметь надежный источник данных о "правильной" топологии и политике отдельной сети.

Примером такой услуги является система MyASN (<http://www.ripe.net/projects/ris/index.html>), бесплатно предоставляемая RIPE NCC. Участвующая сеть имеет возможность задать набор событий, при наступлении которых данная сеть будет уведомлена. Например, в случае, если префикс, используемый сетью, анонсируется другой автономной системой в качестве источника.

Вместо заключения

Уязвимость системы маршрутизации – не единственная проблема этой системы, и, возможно не самая критичная. В конце концов, мы слышим только об отдельных случаях атак и захвата адресного пространства. Однако есть основания полагать, что по мере опустошения пула свободных адресов IPv4 вероятность таких атак будет возрастать. И учитывая, что внедрение новых технологий в Сети является долгосрочным и трудоемким процессом, готовиться к этому надо уже сегодня.

Технический директор RIPE NCC Андрей Робачевский

Мнения, представленные в статье, не обязательно отражают официальную позицию RIPE NCC