

Пять препятствий на пути к безопасности глобальной системы маршрутизации

Протокол маршрутизации BGP по-существу является нервной системой Интернета. Этот протокол обеспечивает распространение информации о связности и доступности сетей среди всех узловых точек Интернета. С помощью BGP каждая сеть сообщает своим соседям, или пирам, информацию о собственной связности - подключенных к ней других сетях, а также том, что сеть узнала от других соседей.

Эта информация пополняется, формируя для каждого узла так называемую глобальную таблицу маршрутизации, и распространяется по всему Интернету. В результате каждая сеть знает, с той или иной степенью детализации, как достичь любую другую сеть глобального Интернета.

Несмотря на свою фундаментальную значимость, протокол BGP основан на доверии между соединенными сетями, принимая полученную от них информацию за чистую монету. Более того, доверие это обладает транзитивным свойством - пиры доверяют своим соседям, те, в свою очередь, - своим, и в итоге все доверяют всем.

Другими словами, BGP позволяет лгать и ложь эта, если не поставить дополнительных заслонов, будет распространяться по всему Интернету. Эта ложь может быть следствием ошибок конфигурации или умышленным подлогом. Последствия ее могут быть невинны и незаметны, а могут представлять собой атаку, затрагивающую все системы и сервисы.

Разумеется, сеть вольна не доверять полученной информации и осуществить дополнительную проверку, но, к сожалению, сам протокол BGP в его настоящем виде здесь вряд ли поможет и при этом необходимо прибегать к дополнительным средствам, о которых мы поговорим в этой статье.

Несмотря на наличие широкого арсенала средств и кажущуюся срочность и необходимость принятия мер, сервис-провайдеры не спешат внедрять технологии, повышающие безопасность маршрутизации. В чем же причина?

В этой статье я попробую рассмотреть некоторые противодействующие факторы, а также обсудить пути их преодоления.

Препятствие 1: Необозначенные риски

Даже если уязвимые места и угрозы достаточно понятны, риски большей частью недооцениваются. Отсутствие данных о реальном состоянии дел делает этот аспект еще более туманным.

В информационном документе IETF RFC4593 (<http://datatracker.ietf.org/doc/rfc4593/>) обсуждаются потенциальные угрозы системы маршрутизации, а RFC4272 (<http://datatracker.ietf.org/doc/rfc4272/>) подробно обсуждает уязвимые места протокола BGP. Суть их сводится к следующему:

- Отсутствие внутреннего механизма, обеспечивающего сильную защиту целостности, свежести и аутентичности сообщений BGP, которыми обмениваются сети-пиры друг с другом
- Отсутствие механизма для проверки прав автономной системы, или сети, анонсировать префикс
- Отсутствие механизма для проверки подлинности атрибутов пути, анонсированных сетью-пиром

Векторы атаки на систему маршрутизации представлены на рисунке 1.

Первая проблема имеет отношение к защите канала между пирами и часто решается локальными средствами. Рабочая группа IETF KARP (<http://datatracker.ietf.org/wg/karp/>) занимается разработкой продвинутых решений в этой области. Две остальные уязвимости имеют более существенное значение в глобальном масштабе.



Рисунок 1 Атаки на систему маршрутизации

Отсутствие механизмов проверки подлинности полученной информации позволяет атакующему повлиять на маршрутизацию трафика, относящегося к той или иной сети, в глобальном масштабе. Наиболее распространенными являются захват префикса, или маршрута (prefix hijacking, route hijacking), когда префикс какой-либо сети анонсируется атакующим и трафик, предназначенный этой сети, перенаправляется в сторону атакующего, см. рис. 2.

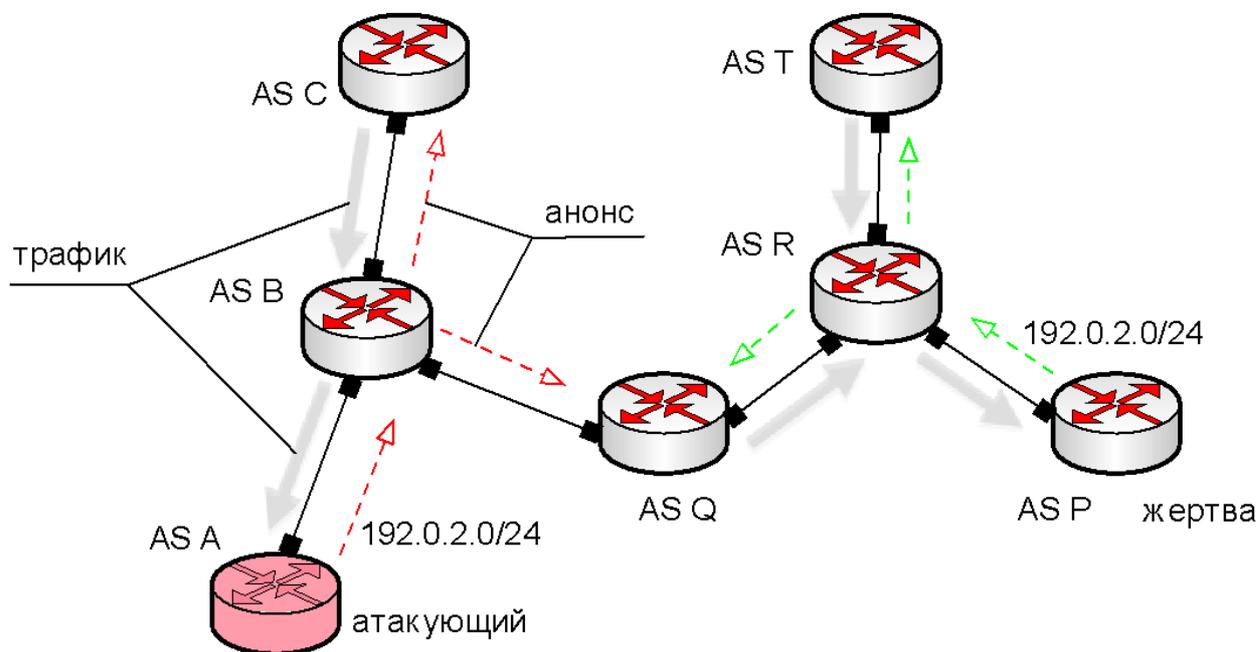


Рисунок 2 Захват префикса. Атакующая сеть AS A анонсирует префикс, принадлежащий сети AS P. В результате конкуренции трафик в части Интернета перенаправляется к атакующей сети.

Эта атака имеет несколько вариантов:

- Захват маршрута, когда сеть анонсирует не принадлежащее ей адресное пространство в качестве сети-источника. При выборе маршрута BGP предпочтет более короткий, измеряемый числом сетей между источником и получателем, маршрут. Таким образом захваченный маршрут будет конкурировать с истинным.
- Захват подсетей, когда анонсируются более специфичные префиксы. При выборе маршрута BGP

предпочитает тот, который указывается более специфичным префиксом, и таким образом атакующий выигрывает несмотря на топологическую удаленность. В отсутствие конкурирующих префиксов такого же размера, захват имеет глобальный эффект.

- Захват нераспределенного или неиспользуемого адресного пространства. В этом случае анонсируемый префикс не встречает конкуренции и имеет высокие шансы распространения по всему Интернету. В то же время очевидные недопустимые префиксы, так называемые bogons, как правило, фильтруются провайдерами.

- Перенаправление трафика. В этом случае трафик доставляется получателю, но передается по пути, отличному от нормального выбора BGP. Теоретическую возможность такой атаки и ее маскировку показали А.Пилосов и А. Капелла (см. статью "Безопасность системы маршрутизации Интернета", http://www.ripn.net/articles/secure_routing/, а также <http://www.wired.com/threatlevel/2008/08/revealed-the-in/>). Реальный пример масштабного перенаправления трафика произошел в апреле 2010 года, когда одна из китайских сетей, скорее всего случайно, анонсировала 40000 не принадлежащих китайским сетям маршрутов (см. <http://www.renesys.com/blog/2010/11/chinas-18-minute-mystery.shtml>, а также <http://ddos.arbornetworks.com/2010/11/china-hijacks-15-of-internet-traffic/>).

Последствия этих атак могут быть различными. Захват маршрута приводит к перетягиванию трафика, предназначенного «захваченной» сети, который, как правило, затем отбрасывается. То есть происходит DoS-атака на все сервисы сети. В эту категорию попадает большинство ошибок конфигурации. Такая атака может также быть использована для краткосрочной генерации трафика, например для рассылки спама. В более изощренном виде захват маршрута может быть направлен на захват некоторого информационного ресурса, например вэб-сайта, с предоставлением пользователям подложного сайта. В этом случае даже защита DNSSEC будет бессильна, а учитывая относительную простоту получения сертификата TLS, такая атака может иметь серьезные последствия для пользователей – например, кражу данных по кредитным картам.

Очевидно, что глобальная система маршрутизации уязвима для всех перечисленных атак, тем не менее связанные с ними риски зачастую считаются незначительными и "принимаются" без дополнительных мер защиты. Опытные операторы рассматривают эту проблему более серьезно, правда в большинстве случаев учитываются только риски, связанные с непосредственным окружением – сетями-клиентами и пирами. Это отражается в наиболее распространенной практике фильтрацией маршрутов собственных сетей-клиентов и установкой максимального числа принимаемых маршрутов от пириров и сетей, предоставляющих транзит. Реже производится фильтрация маршрутов, полученных от пириров. Принятая практика безопасной политики показана на рис. 3.

Бездействие по отношению к угрозам, источником которых являются топологически удаленные сети, или глобальный Интернет в целом, может быть объяснено несколькими причинами.

Во-первых, отсутствием эффективных средств уменьшения таких рисков, как удобного инструментария, так и надежных данных о легитимности маршрутов и сетей.

Во-вторых, недостатком достоверной статистики о реальном положении дел. Операторам достаточно хорошо известны такие происшествия как «захват» сайта YouTube в феврале 2008 года (см. <http://www.ripe.net/news/study-youtube-hijacking.html>), «захват» Интернета оператором TNet в декабре 2004 (см. http://www.renesys.com/blog/2005/12/internetwide_nearcatastrophela.shtml), де-агрегация префиксов AS7007 в апреле 1997 (см. <http://lists.ucc.gu.uwa.edu.au/pipermail/lore/2006-August/000040.html>). Эффект от этих атак был колоссальным, для многих сетей Интернет на несколько часов просто перестал существовать. Но эти происшествия случаются нечасто, они почти моментально детектируются и благодаря координации между операторами довольно быстро ликвидируются. В то же время, информация о более «скромных» и, возможно, более умышленных инцидентах, происходящих на периферии Интернета, практически отсутствует. Исследование, проведенное в группе NIST, показывает, что подозрительная активность не прекращается, особенно в темных закоулках нераспределенного адресного пространства. Тепловая карта, построенная на базе этих данных приведена на рис. 4. Заметим, что такого пространства остается все меньше и меньше.

Наконец, в-третьих, оператор вряд ли может быть признан ответственным за события, происходящие где-то там в Интернете, а засим не очень склонен вкладывать усилия в борьбу за всеобщую безопасность.

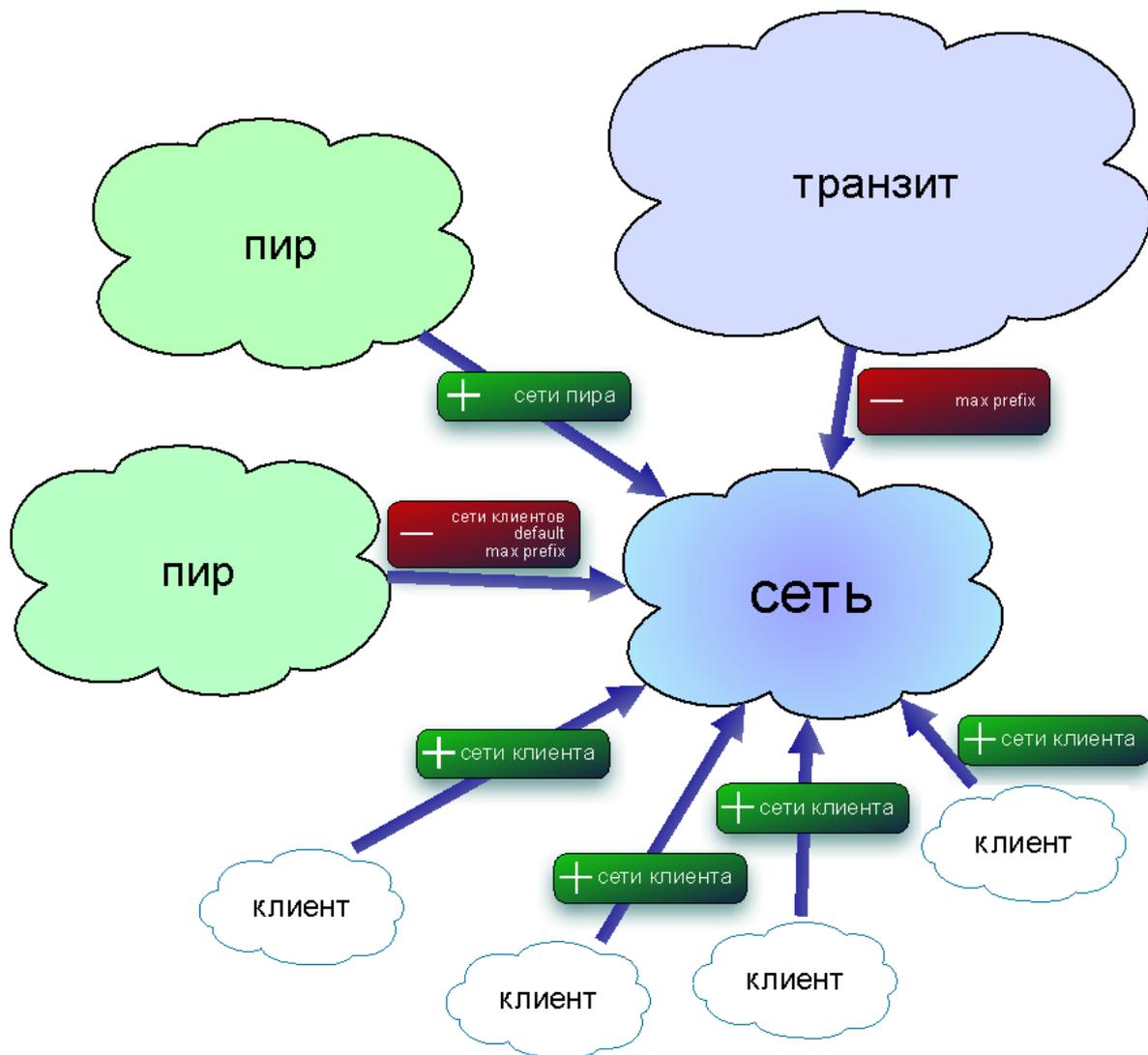


Рисунок 3. Принятая практика безопасной политики маршрутизации

Препятствие 2: Безопасность и стабильность

Стабильность является основным приоритетом, а меры безопасности в некоторых случаях могут оказывать как положительное, так и отрицательное воздействие.

Для большинства операторов стабильность сети и ее устойчивость к внешним факторам – атаки, выход из строя оборудования и кабельной системы, являются первоочередными требованиями. Хотя уязвимость системы маршрутизации и представляет угрозу стабильности, безопасность глобальной системы маршрутизации для многих не является приоритетом.

Во-первых, в качестве вектора атаки другие методы являются более простыми, эффективными и употребительными. Хотя по своему эффекту захват маршрута во многом превосходит традиционные распределенные DoS-атаки, обнаружение и координация действий по борьбе с ним являются относительно более простыми.

Во-вторых, стабильность с точки зрения маршрутизации означает устойчивость политики маршрутизации. Если ошибки со стороны ближайшего окружения – клиентов и пиров – не вызывают существенного искажения этой политики – сеть считается стабильной. Типичная политика довольно проста (см. рисунок 3), и существующая практика фильтрации считается достаточной для поддержания стабильной политики.

В-третьих, дополнительные меры безопасности означают возможность дополнительных ошибок, которые могут иметь негативное влияние на стабильность сети. Например, ошибки в построении фильтров или использование неправильных данных. Вопрос в том, хотите ли вы зависеть от своих или чужих ошибок. В первом случае, для положительного результата всего лишь необходимо, чтобы собственные ошибки случались реже внешних.



Рисунок 4. Тепловая карта анонсируемого адресного пространства. Зеленым цветом показано legitimately анонсируемое адресное пространство, красным – подозрительные анонсы, белым – адреса не анонсируемые в Интернете (источник: Kotikaludi Sriram, et.al. “A Comparative Analysis of BGP Anomaly Detection and Robustness Algorithms”, http://www.antd.nist.gov/bgp_security/publications/NIST_BGP_Robustness.pdf)

Препятствие 3: Неготовность решения, нехватка инструментария

На сегодня отсутствует стандартный подход, набор методов, целостно решающих проблему. Даже наиболее продвинутые провайдеры решают проблему локально.

В начале этого года рабочая группа IETF SIDR (<http://datatracker.ietf.org/wg/sidr/>) завершила стандартизацию системы RPKI, опубликовав 17 RFC, описывающих ее работу и определяющих ее элементы. На сегодняшний день это одно из наиболее полных и проработанных решений в области безопасности глобальной системы маршрутизации. Фундаментом системы является система открытых ключей (Public Key Infrastructure, PKI), элементами которой являются сертификаты Интернет-ресурсов. На основе этих сертификатов держатели ресурсов могут создавать криптографически заверенные объекты, например ROA (Route Origin Authorization), указывающие на список автономных систем, которые могут являться источником определенного маршрута. Более подробно о системе RPKI я писал в своей статье «Сертификация Адресных Интернет-Ресурсов» (<http://www.ripn.net/articles/certification/>).

Хотя RPKI на первом этапе не решает проблему перенаправления трафика, она позволяет частично защитить сети против захвата маршрутов. Почему частично? Дело в том, что на данной фазе путь прохождения анонса по-прежнему невозможно достоверно проверить. В результате атакующий может захватить маршрут, представив, что авторизованная автономная система находится за ним. Цена этой лжи – увеличение длины атрибута AS_PATH, регистрирующего автономные системы, через которые прошел анонс. Как следствие – маршрут становится менее конкурентоспособным и риск атаки снижается в среднем на 60% (см. https://labs.ripe.net/Members/David_Murray/content-bgp-route-origin-validation).

В то же время RPKI является эффективным средством борьбы с захватом подсетей – наиболее разрушительным средством атакующих.

Текущий этап работы SIDR – разработка расширений BGPSEC, призван решить задачу защиты атрибута AS_PATH, и, тем самым, закрыть наиболее уязвимые места BGP. Об этом этапе разработки я писал в статье “Путевые _заметки: IETF80” (<http://www.ripn.net/articles/ietf80.pdf>).

Хотя модель RPKI/BGPSEC является наиболее полной, она имеет ряд недостатков. Во-первых, полное внедрение этой технологии требует нового программного и аппаратного обеспечения, другими словами, замены маршрутизаторов. Само по себе это не является невозможным, так как замена так или иначе происходит естественным путем, но отодвигает возможность внедрения на средний цикл обновления оборудования, то есть на 5-8 лет. Другим недостатком является то, что BGPSEC существенно усложняет и без того перегруженный протокол BGP, что может негативно сказаться на его глобальной производительности, в частности – сходимости. Наконец, некоторых смущает тот факт, что технология построена на модели PKI с единым центром контроля (или, по крайней мере, с ограниченным числом таких центров), что может негативно сказаться на устойчивости системы.

В отсутствие BGPSEC, RPKI является своего рода строительным блоком, который может быть использован операторами в создании собственной системы безопасности. Проблема заключается в том, что набор методов, целостно решающих проблему конфигурации, которая стоит шире просто безопасности, отсутствует. Наиболее продвинутые провайдеры решают проблему с использованием собственных разработок.

Препятствие 4: Отсутствие данных

Фундаментальным аспектом глобальной безопасности системы маршрутизации является наличие достоверных текущих данных о политике маршрутизации отдельных сетей, в частности, о префиксах, легитимным источником которых сеть является.

Авторизованным источником данных о распределенных номерных ресурсах – адресном пространстве и номерах автономных систем, – являются Региональные Интернет-Регистратуры (РИР). К сожалению, доступная информация, обычно предоставляемая в виде ответов на запросы whois, не очень пригодна к использованию в контексте безопасности маршрутизации. Формат объектов whois различается от РИРа к РИРу, а большая часть информации предусматривает человеческую, а не машинную интерпретацию. За редким исключением в этих базах отсутствует информация, связывающая адресное пространство с автономными системами, которые авторизованы его анонсировать (объекты базы данных ARIN содержат такую информацию).

С другой стороны, существуют многочисленные Интернет-Регистратуры Маршрутизации (Internet Routing Registry, IRR), которые собственно и созданы для предоставления требуемой информации. Беда в том, что в большинстве случаев достоверность данных IRR не поддается проверке. Во многих случаях IRR содержит устаревшую информацию, а сама система может представить «слабое звено» в общей безопасности. Например, в большинстве IRR не производится проверок легитимности создаваемого объекта route, связывающего префикс с сетью-источником.

Система, построенная на основе RPKI призвана решить эти проблемы. Во-первых, данные о распределенных номерных ресурсах предоставляются в стандартной форме цифровых сертификатов со стандартными расширениями (расширения X.509 собственно и содержат список ресурсов, привязанных к открытому ключу сертификата). Во-вторых, достоверность и свежесть данных может быть проверена с использованием криптографических средств третьими лицами. Как и в стандартном PKI, для проверки необходима конфигурация доверия только к одному сертификату – т.н. «точке доверия» (Trust Anchor, TA). В-третьих, сертификаты ресурсов могут использоваться их владельцами (держателями адресного пространства) для, например, электронной авторизации определенных автономных систем для анонсирования этого адресного пространства, выполняя, таким образом, функцию объектов route традиционных IRR.

Проблема в том, что, как и в случае с IRR, данные неполны. Позитивным фактором является то, что все РИРы за исключением североамериканской ARIN (они вот-вот ее запустят) предоставляют возможность операторам-членам соответствующего РИРа получить сертификат и создать необходимые ROA. Однако система эта используется операторами в полутестовом режиме и пока мало кто воспринимает ее всерьез. Дополнительной проблемой является то, что тестовые объекты неотличимы от нормальных, то есть использовать RPKI сегодня приходится с большой осторожностью.

Препятствие 5: Зависимость от других игроков

Реальный потенциал заложен в глобальной системе безопасности, когда значительное число игроков принимают соответствующие меры. Усилия отдельного провайдера вносят несущественный вклад в улучшение глобальной системы и, как ни парадоксально, еще менее существенный - в улучшение собственной безопасности

При рассмотрении проблематики безопасности глобальной системы маршрутизации мы сталкиваемся с обратным феноменом трагедии общин (http://ru.wikipedia.org/wiki/Трагедия_общин). Первопроходцы несут затраты, все преимущества от которых получают их последователи. Осуществляя фильтрацию анонсов или ограничивая распространение ошибок и умышленных захватов, оператор фактически защищает чужие сети, на безопасность же собственной его действия не влияют. В то же время, если все будут действовать в собственных краткосрочных интересах – улучшения в этой области не произойдет.

С разрабатываемыми в настоящее время криптографическими технологиями, основанными на инфраструктуре открытых ключей RPKI и BGPSEC, связан новый аспект, вызывающий некоторую озабоченность технического сообщества. Как и в любой системе PKI, организации, стоящие выше в иерархической системе контролируют дочерние сертификаты и все сертификаты, выданные на более низких уровнях. В рамках классической модели RPKI, полностью соответствующей системе распределения глобальных номерных ресурсов (адресного пространства и номеров автономных систем), в «корне» иерархии находится IANA, которая выдает сертификаты РИРа, которые, в свою очередь, сертифицируют ресурсы, распределенные между своими членами – локальными регистратурами и сервис-провайдерами. Иерархия может быть продолжена и дальше, в случае если сервис провайдер сертифицирует пользовательские сети.

Это означает, что теоретически IANA может влиять на действительность сертификатов любой цепочки иерархии. Ошибка в сертификате IANA приведет к недействительности всех данных системы RPKI, а удаление из корневого сертификата адресного блока сделает сертификаты этих сетей недействительными. Те же опасения, хотя и в меньшей степени, относятся и к сертификатам, выданными РИРа.

Хотя обсуждаемые сценарии сложно воплотить на практике по техническим и политическим причинам, следует признать, что в данной ситуации регистратуры начинают играть более важную роль в области маршрутизации. Как следствие, возрастают требования к их операционным и техническим возможностям, а также их нейтральности по отношению к государственным и правоохранительным структурам – требование труднодостижимое, поскольку каждая из регистратур действует в определенной национальной юридической системе и подчиняется ее законам.

На начальном этапе использования технологии RPKI эти проблемы носят чисто теоретический характер. Параллельно ведется обсуждение способов внедрения этой технологии в более «эластичном» режиме.

Взгляд в будущее

Создание глобальной системы безопасности требует значительной консолидации усилий операторов и не может быть решена исключительно на основе бизнес-мотивации. Однако для активирования других побудительных мотивов, например, мотива следования за лидером, поддержки репутации или соответствия требованиям регулятора необходимо создание некоторой критической массы операторов, успешно использующих эти технологии.

В этом плане можно выделить несколько этапов, причем на начальных этапах доминируют мотивы собственной выгоды, в то время как на заключительных этапах они существенно дополняются другими побуждениями.

Защита границ

Наиболее явной угрозой со стороны системы маршрутизации является существенное нарушение политики маршрутизации сети за счет ошибок ближайшего окружения – клиентов и пиров. Например, анонсирование клиентом маршрутов, о которых он, возможно, узнал от другого провайдера, включая и полную таблицу маршрутизации, может превратить этого клиента в провайдера транзита и, учитывая неадекватную для этого инфраструктуру, фактически заблокировать услуги сети. Уже упоминавшийся «захват» Интернета оператором TNet в декабре 2004 (см. http://www.renysys.com/blog/2005/12/internetwide_nearcatastrophela.shtml) является одним из примеров данной ситуации.

Реализация политики (см. рис. 3) в соответствии с текущей практикой в значительной степени уменьшает

риски и тем самым улучшает стабильность сети. Эта политика означает прием от клиентов только их собственных маршрутов, от сетей-пиров – собственных маршрутов и маршрутов их клиентов, и ограничение числа принимаемых маршрутов от провайдеров транзита.

Одной из обозначенных проблем является отсутствие надежных источников данных для построения такой политики. Сегодня в отношении клиентов используются либо собственные регистрационные базы данных провайдера, либо базы IRR. При этом, добросовестность требует проверки легитимности использования клиентом анонсируемого адресного пространства.

Переход к использованию RPKI в качестве исходных данных принятия решений позволит решить обе задачи. Во-первых, клиенты смогут независимо регистрировать собственные ресурсы (ROA), которые сразу же становятся доступными в защищенной форме их провайдеру, а во-вторых, положительная проверка достоверности такой регистрации удостоверяет легитимность анонса.

Почти 80% всех активных автономных систем Интернета являются конечными клиентами, предоставляющими услуги только конечным пользователям, а не другим сетям (т.н. stub AS). Это означает, что выполнение требования клиентами регистрации своих ресурсов (адресного пространства и анонсов – ROA) в системе RPKI приведет к 80-процентной полноте данных! Это, в свою очередь, откроет дополнительные возможности использования системы.

Защита выбора

В многосвязной системе, каковой в большинстве своем является Интернет, у сети появляется необходимость выбора. Действительно, маршрут может быть получен от более чем одного провайдера. Сегодня выбор во многом определяется задачами инжиниринга трафика – выбор более дешевого провайдера, запасной путь и т.п. Внедрение системы безопасности позволяет добавить еще одну переменную в задачу выбора. Какой маршрут будет предпочтительнее – достоверный или тот, который не выдержал проверки и, возможно, ведущий в никуда? Ответ непосредственно влияет на качество услуг сети.

Заметим, что ответ на вопрос не так прост, особенно на начальном этапе внедрения системы. Например, выбрать ли достоверный маршрут более дорогого провайдера или недостоверный от недорогого?

Защита пути

RPKI в изначальном варианте в значительной степени защищает источник маршрута, но все же, как мы обсуждали, позволяет лгать. Закрывать эту лазейку можно лишь защитив путь по которому был передан анонс маршрута. Это задача более отдаленного будущего, решаемая расширением протокола BGP – BGPSEC.

Внедрение этой технологии позволит достоверно осуществлять политики, предписывающие использование определенного пути между сетями. Или же, запрещающие определенные сети для прохождения трафика.

Острова в океане

Наивно предполагать, что система глобальной безопасности возникнет сразу во всем Интернете. Скорее всего она продолжит развиваться вокруг наиболее продвинутых в этой области провайдеров. При этом, внедрение технологий RPKI и BGPSEC возможно в рамках «федераций» - нескольких взаимодействующих провайдеров. Отмечу, что включение в игру крупных провайдеров, т.н. tier1, позволит существенно ускорить прогресс в этой области.

Андрей Робачевский, Менеджер по программам ISOC

Мнения, представленные в статье, не обязательно отражают официальную позицию ISOC