Манипуляции с маршрутными объявлениями. Защита BGP

Поскольку маршрутное объявление протокола BGP формируется шаг за шагом многими провайдерами, при этом достоверность информации каждого шага проверить невозможно, у провайдера имеется полная свобода действий при обработке маршрутного объявления и передаче его соседним провайдерам. Например, вместо простого добавления номера своей автономной системы к уже имеющейся последовательности AS-номеров, он может выполнить ряд следующих манипуляций с полученным маршрутом:

- Поместить адрес чужой сети с номером своей автономной системы в качестве исходной, чтобы направить трафик в свою автономную систему. Такая атака называется захватом префикса и именно она произошла в инцидентах с AS7007 и Pakistan Telecom. Для того чтобы объявление адреса выглядело предпочтительнее, адрес должен быть более специфическим, чем у объявлений «настоящей» исходной автономной системы.
- Выбросить из последовательности какую-то определенную автономную систему, чтобы обойти политику некоторой третьей автономной системы, которая по финансовым или иным соображениям блокирует все маршруты, проходящие через удаленную автономную систему.
- Добавить номер соседней автономной системы перед передачей ее объявления, чтобы соседняя автономная система, получив объявление и увидев в нем свой номер, отбросила его, решив, что объявление зациклилось.
- Добавить номер своей автономной системы несколько раз, чтобы объявление стало непривлекательным для других провайдеров (из-за размера последовательности AS).
- Составить ложную последовательность автономных систем, но поместить в качестве исходного правильный (но не свой) номер AS, чтобы вызвать доверие к маршруту.

Как видим, незащищенность маршрутного объявления дает большой простор для злонамеренных искажений и просто ошибок при его обработке. Вероятность ошибки усугубляется тем, что в отличие от внутренних протоколов маршрутизации, которые обрабатывают сообщения с минимальным вмешательством администратора, работа протокола BGP обычно регулируется большим количеством правил фильтрации, которые задаются вручную администратором AS. Эти фильтры определяют политику маршрутизации той или иной автономной системы, отражающую взаимоотношения данного провайдера с каждым из провайдеров, с которым у него есть пиринговые соглашения о передаче трафика. Вместе с тем, фильтры политики BGP представляют собой мощный и популярный способ защиты BGP-маршрутизации от ошибок и атак. Но для этого их нужно правильно применять.

Защита BGP

Первым заслоном на пути ошибок и атак типа «злоумышленник посередине» должна быть *защита BGP-сеанса между соседними маршрутизаторами*, особенно защита сеанса внешнего протокола BGP, так как маршрутизаторы в этом случае принадлежат разным провайдерам и между ними могут находиться промежуточные коммутаторы и другие маршрутизаторы, работающие не по протоколу BGP.

По умолчанию BGP-сеанс использует протокол TCP, поэтому описанные ранее атаки на TCP подвергают риску и работу BGP. Результатом атаки на TCP может стать удаление всех BGP-маршрутов из таблицы маршрутизации, так как все они могли быть получены в результате одного и того же длительного TCP-сеанса между BGP-маршрутизаторами. Подделка TCP-сегмента может привести к появлению ложного маршрута в таблице маршрутизации или удаления из нее корректного маршрута.

Для защиты TCP-сеанса между BGP-маршрутизаторами рекомендуется использовать режим работы TCP с аутентификацией сегментов посредством цифровой подписи.

Защита BGP-маршрутизации на основе базы данных маршрутов

С середины 90-х годов региональные информационные центры Интернета, которые распределяют IP-адреса и номера автономных систем среди провайдеров своих регионов (то есть RIPE NCC, ARIN, APNIC, LACNIC и AfriNIC), начали вести базу данных маршрутов Интернета.

В **базе данных маршрутов Интернета** (Internet Routing Registry, **IRR**) для каждого *зарегистрированного* провайдера указываются номера администрируемых им автономных систем и политика маршрутизации, проводимую этим провайдером в пределах каждой из своих автономных систем по отношению ко всем ее

соседним автономным системам, с которыми у него установлены пиринговые отношения.

Например, пусть провайдер ISP1 администрирует автономную систему AS1 и у него имеются пиринговые соглашения с AS2, AS3 и AS4. Тогда в базе IRR будет существовать объект типа `aut-num` с параметрами такого вида:

```
aut-num:AS1
aut-name:ISP1
import:from AS2 action pref=50; accept AS2
export: to AS2 announce AS1
import:from AS3 action pref=50: accept any
export:to AS3 announce AS1
import:from AS4 action pref=50: accept AS3
export:to AS4 announce AS1
address:XX XXXXX XXXX
phone:YY-YYYYY-YYYYY
```

Из приведенного списка видно, что политика маршрутизации системы AS1 состоит в том, что ее маршрутизаторы объявляют каждой из пиринговых автономных систем только о тех маршрутах, которые ведут к адресам ее собственных сетей (об этом говорит атрибут `announce AS1`). В свою очередь, автономная система AS1 также готова принимать от AS2 и AS4 только те маршруты, которые исходят от адресов их собственных сетей, а от AS3 она готова принимать любые маршруты. Скорее всего, AS2 и AS4 являются клиентами AS1, а AS3 — это магистральный провайдер, через которого происходит связь AS1 с остальными автономными системами Интернета. В параметрах атрибутов `export` и `import` можно использовать не только номера автономных систем, но и префиксы IP-адресов.

Кроме объектов `aut-num` в базе IRR существуют объекты типа `route`, которые говорят о том, какие адреса будет объявлять та или иная автономная система в своих маршрутных объявлениях. Адреса, указанные в объектах `route`, являются подмножеством адресов, выделенных провайдеру, поскольку некоторые из них могут быть еще не назначены реальным сетям, другие могут быть предназначены для внутренней маршрутизации.

Регистрация в базе IRR не является обязательной для провайдеров, но она желательна, а иногда и необходима, так как некоторые провайдеры отказываются устанавливать пиринговые отношения с провайдерами, не зарегистрированными в базе IRR. Базы IRR всех пяти региональных центров RIR идентичны. База IRR является открытой, любой пользователь Интернета может запросить сведения о любой автономной системе с помощью команды `whois`. Обычной практикой провайдера является построение фильтров политики протокола BGP на своих маршрутизаторах на основании данных о политике соседей, полученных из базы IRR. Существует также утилита IRRToolSet, которая автоматизирует этот процесс и транслируют правила политики, описанные в базе IRR, в язык BGP-фильтров определенного типа маршрутизаторов.

Обращаясь снова к инциденту с автономной системой AS7007, заметим, что ее администратор мог бы легко предотвратить распространение специфических префиксов из маршрутизатора своего клиента, если бы установил простой фильтр, принимающий от маршрутизатора клиента только префиксы адресов, которые были назначены данному клиенту провайдером AS7007. Пострадавшие провайдеры соседних с AS7007 автономных систем также могли бы построить свои фильтры соответствующим образом, если бы провайдер AS7007 зарегистрировал свои объекты в базе IRR.

Несмотря на то, что база IRR существует уже много лет и большинство провайдеров регистрируют в ней свои правила политики маршрутизации, инциденты с захватом префиксов по-прежнему регулярно случаются. Это стало поводом к началу работ по созданию новой безопасной масштабируемой версии протокола BGP, координируемых рабочей группой IETF SIDR (Secure Inter-Domain Routing).

Сертификаты ресурсов и их использование для защиты BGP

В качестве средства защиты BGP группа SIDR решила использовать публичную систему сертификатов[1].

Главным назначением **системы сертификатов ресурсов** (Resource Public Key Infrustructure, **RPKI**) является удостоверение того факта, что некоторый провайдер владеет определенными номерами

[1] См. раздел «Системы аутентификации и управления доступом операционных систем Unix и Windows».

автономных систем и префиксами IP-адресов.

Например, если провайдер ISP1 имеет сертификат RPKI, то этот сертификат показывает, что провайдеру *в установленном порядке* выделены номера автономных систем AS1, AS2, …, ASn и префиксы IP1, IP2, IP3, …, IPm. Установленный порядок означает, что номера и адреса были выданы либо IANA (корневая организация, выделяющая номера и адреса в Интернете), либо пятью региональными Интернет-центрами, либо провайдерами, получившими эти адреса от региональных центров. Провайдеров в этой иерархии обычно называют **локальными Интернет-центрами** (Local Internet Register, **LIR**).

Система RPKI состоит, как и любая система PKI, из **центров сертификации** (Certificate Authority, **CA**), при этом каждая организация из иерархии IANA→RIRs→LIRs имеет свой центр сертификации, который выдает сертификаты по запросу нижестоящей организации. RPKI-сертификаты имеют дополнительные поля для номеров автономных систем и префиксов адресов, в остальном же это обычный сертификат, в котором содержится открытый ключ владельца сертификата и имя владельца.

Сертификат называется *сертификатом ресурса*, потому что он предназначен не для аутентификации владельца сертификата, а для его *авторизации* (то есть наделения правами) — сертификат свидетельствует, что владелец имеет законное право распоряжаться номерами автономных систем и префиксов адресов, например, передавать или продавать префиксы, указывать их в маршрутных объявлениях как исходные, и т. п. Сертификаты здесь представляют собой масштабируемое решение, не требующее хранения множества паролей для проверки законности владения номером или номерами автономных систем и префиксов адресов некоторой организацией, вместо этого производится проверка предъявленного сертификата вдоль не очень длинной иерархии сертификационных центров.

Однако, сам по себе RPKI-сертификат не может свидетельствовать о достоверности номера исходной автономной системы в маршрутном объявлении протокола BGP, так как обладатель некоторого префикса может делегировать право на объявление этого префикса в качестве маршрута автономной системе вышестоящего провайдера или клиента; наконец, некоторые адреса провайдер может не объявлять вовсе, зарезервировав их для внутреннего использования.

Поэтому для проверки законности объявления некоторой автономной системы как исходной для определенного префикса в маршрутном объявлении рабочая группа SIDR предложила использовать новый тип объекта, название которого можно перевести как объект **авторизации источника маршрута** (Route Origination Authorisation, ROA). ROA содержит номер автономной системы и несколько префиксов IP-адресов, которые эта автономная система имеет право объявлять в BGP-маршрутах. Объект ROA создается и подписывается владельцем префиксов, указанных в этом объекте.

Провайдеры могут использовать базу данных объектов ROA двумя способами. Во-первых, они могут задействовать данные этих объектов так же, как данные объектов `aut-num` и `route` из базы IRR для построения фильтров маршрутизаторов. Отличие состоит в том, что объекты ROA снабжены цифровой подписью, которую можно проверить, а объекты базы IRR — нет. Во-вторых, провайдеры могут автоматизировать процесс проверки достоверности источника маршрута. Для этого каждому провайдеру необходимо создать свой локальный кэш базы RPKI, к которому могут обращаться маршрутизаторы при проверке каждого маршрутного объявления протокола BGP.

Возможность проверки достоверности номера исходной автономной системы для префикса сети является важным шагом в повышении защищенности протокола BGP от ошибок и атак. Однако это только первый шаг в нужном направлении, так как он не исключает манипуляций с маршрутными объявлениями при передаче их от провайдера к провайдеру. Даже тот факт, что указанная в маршруте исходная автономная система имела право объявить маршрут к тому или иному префиксу (факт, проверенный с помощью ROA), не гарантирует того, что маршрут был сгенерирован данной автономной системой — его вполне мог скомпоновать и провайдер-злоумышленник.

Поэтому следующим этапом должно стать появление средств, которые позволят маршрутизаторам «на лету» проверять достоверность всех звеньев маршрута. Таким протоколом является, по мнению специалистов из группы SIDR, протокол **BGPSEC**, который основан на цифровых подписях каждого провайдера, участвующего в пошаговом формировании маршрутного объявления протокола BGP. Получив объявление, маршрутизатор провайдера проверяет цифровые подписи предыдущих провайдеров, чьи автономные системы указанны в объявлении, а затем добавляет свою подпись, которая подписывает предыдущую версию объявления с добавленными номером автономной системы данного провайдера и номером автономной системы следующего шага. Добавление номера автономной системы следующего шага препятствует перехвату и незаконной передаче маршрутного объявления не по назначению, то есть срывает атаку «злоумышленник посередине». Пошаговое удостоверение маршрута гарантирует также, что объявление прошло именно тот путь через последовательность автономных

систем, который указан в данном объявлении. Для проверок цифровой подписи используются сертификаты, выпущенные в рамках системы RPKI.

Этот способ защиты BGP является наиболее радикальным, так как он требует полной замены текущей версии BGP в маршрутизаторах провайдеров.