Internet Engineering Task Force (IETF) G. Huston
Request for Comments: 6483 G. Michaelson
Category: Informational APNIC
ISSN: 2070-1721 February 2012

Проверка пригодности источника маршрута с использованием RPKI и ROA

Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs)

Тезисы

Этот документ определяет семантику полномочий создания маршрутов (ROA[1]) в контексте использования инфраструктуры открытых ключей ресурсов (RPKI[2]) для проверки пригодности маршрутных анонсов протокола BGP[3].

Статус документа

Этот документ является проектом стандарта (Internet Standards Track).

Документ является результатом работы IETF[4] и представляет собой согласованное мнение сообщества IETF. Документ был вынесен на публичное рассмотрение и одобрен для публикации IESG[5]. Дополнительная информация о документах BCP представлена в разделе 2 документа RFC 5741.

Информация о текущем статусе этого документа, обнаруженных ошибках и способах обратной связи может быть найдена по ссылке http://www.rfc-editor.org/info/rfc6483.

Оглавление

1. Введение

Этот документ определяет семантику полномочий создания маршрутов (ROA) в контексте использования инфраструктуры открытых ключей ресурсов (RPKI) [RFC6480] для проверки пригодности маршрутных анонсов протокола BGP. [RFC4271].

RPKI основана на иерархии сертификатов ресурсов, которые согласованы со структурой выделения INR[6]. Сертификаты ресурсов являются сертификатами X.509, которые соответствуют профилю PKIX [RFC5280] и расширениями для адресов IP и идентификаторов AS [RFC3779]. Сертификат ресурса описывает действие эмитента, который привязывает список адресных блоков IP и номеров автономных систем (AS[7]) к субъекту сертификата, идентифицируемому уникальной связью секретного ключа субъекта с открытым ключом в сертификате ресурса. RPKI структурирована так, что каждый текущий сертификат ресурса соответствует текущему выделению или назначению ресурса. Это подробно описано в [RFC6480].

ROA являются объектами с цифровой подписью, которые связывают адреса с номером AS и подписываются владельцем адресов. ROA обеспечивают способ проверки того, что держатель блока адресов IP предоставил конкретной AS полномочия на создание в среде междоменной маршрутизации маршрута к этому блоку адресов. ROA описаны в [RFC6482] и служат для выполнения требований повышения уровня защиты междоменной маршрутизации.

[1]Route Origin Authorization.
[2]Resource Public Key Infrastructure.
[3]Border Gateway Protocol — протокол граничного шлюза.
[4]Internet Engineering Task Force.
[5]Internet Engineering Steering Group.
[6]Internet Number Resource — числовые ресурсы Internet.
[7]Autonomous System.

В этом документе описана семантическая интерпретация ROA с упором на применение для создания маршрутов в междоменной маршрутизации и объем полномочий, передаваемых в ROA.

2. Результаты проверки ROA для маршрута

«Маршрут» (route) представляет собой блок информации, который связывает множество адресатов, описываемых префиксом IP, с набором атрибутов пути к этим адресатам, как определено в параграфе 1.1 [RFC4271].

«AS-источник» (origin AS) для маршрута определяется следующим образом. Если финальный сегмент пути в AS_PATH имеет тип AS_SEQUENCE, источником является первый элемент этой последовательности (т. е. AS в самой правой позиции протокольного сообщения). Если AS_PATH содержит сегмент пути типа AS_SET, показывающий агрегатный характер маршрута, AS-источник определить невозможно. Применительно к проверке пригодности маршрута в контексте среды маршрутизации значение адресного префикса и исходная AS используются при проверке пригодности ROA.

Здесь предполагается, что зависимые от инфраструктуры стороны (RP[1]) имеют доступ к локальному кэшу полного набора пригодных ROA в процессе проверки пригодности маршрута (пригодными считаются ROA, которые корректны синтаксически и содержат подпись, проверяемую средствами RPKI, как описано в [RFC6482]). Для RP требуется соответствие маршрута одному или множеству пригодных полномочий ROA для получения результата проверки, который, в свою очередь, может применяться для определения подходящих локальных действий по отношению к этому маршруту.

Такой подход к проверке пригодности источника маршрута использует общую модель «положительного» подтверждения, где маршруты, которые невозможно проверить в RPKI, считаются RP «непригодными». Однако с учетом наличия сред с неполным использованием ROA, где лишь часть корректно анонсируемых адресных префиксов имеет связанные с ними и опубликованные ROA в структуре RPKI, эта модель положительного подтверждения несколько изменяется. В контексте проверки пригодности маршрутов предполагается, что наличие адресного префикса в ROA означает действие данного полномочия ROA для всех более конкретных префиксов, которые также охватываются этим ROA. Таким образом, маршрут с более конкретным, чем описано в любом пригодном ROA, адресным префиксом, но не имеющий сам по себе пригодного ROA, может считаться «непригодным». Однако маршруты для адресных префиксов, которые не описаны полностью каким-либо отдельным ROA (т. е. маршруты, чьи префиксы могут быть агрегатами адресных префиксов, описанных в пригодных ROA, или имеют адресные префиксы, которые не пересекаются ни с одним пригодным ROA) и не соответствуют какому-либо пригодному ROA, а также не имеют префикса, который является более конкретным по сравнению с описанным в каком-либо пригодном ROA, не могут быть надежно сочтены «непригодными» при частичном развертывании системы. Для таких маршрутов проверка пригодности дает неопределенный результат (unknown).

Можно определить абстрактный атрибут маршрута, являющийся результатом проверки пригодности, «состояние пригодности» (validity state) [BGP-PFX]. Состояния пригодности маршрутов с определенными выше префиксом и AS-источником при использовании для проверки пригодности одного ROA показаны в таблице.

Маршрут Prefix AS-> V	соответст. AS	не соотв. AS
Нет пересеч.	неизвест.	неизвест.
Покрывающий агрегат	неизвест.	неизвест.
Соответствует префиксу ROA	пригоден	непригод.
Конкретней чем ROA	непригод.	непригод.

Состояние пригодности маршрута.

В среде с набором действующих ROA маршрут считается «пригодным», если для любой ROA проверка дает результат «пригоден». Маршрут считается «непригодным», если результат проверки для одного (или нескольких) ROA дает значение «не пригоден» и нет результата «пригоден» для каких-либо ROA. Состояние считается «не определенным» (unknown или not found [BGP-PFX]), если нет пригодных ROA, дающих после проверки состояние «пригоден» или «не пригоден».

Процедура определения состояния пригодности маршрута приведена ниже.

1. Выбираются все пригодные ROA, включающие значение ROAIPAddress, которое соответствует или является включающим агрегатом для адресного префикса в маршруте. Результатом является набор ROA-кандидатов.
2. Если множество кандидатов пусто, процедура завершается с возвратом значения unknown (или not found, как принято в [BGP-PFX]).
3. Если создавшую маршрут AS можно определить и любой элемент множества ROA-кандидатов имеет значение asID, которое соответствует AS в маршруте, а префикс адреса соответствует ROAIPAddress в ROA (соответствие означает точное совпадение с ROAIPAddress или наличие в ROAIPAddress элемента maxLength, значение которого не меньше размера адресного префикса в маршруте а сам префикс является более конкретным, нежели ROAIPAddress), процедура завершается с возвратом значения valid.
4. В остальных случаях процедура завершается с возвратом значения invalid.

[1]Relying party.

3. Применение результатов проверки при выборе маршрутов

В рамках абстрактной модели работы междоменной маршрутизации с использованием BGP [RFC4271] полученный от партнера по маршрутизации анонс префикса сравнивается со всеми анонсами этого же префикса, полученными от других партнеров, и применяется процедура выбора маршрута для определения «лучшего» маршрута из числа кандидатов.

Состояния пригодности маршрута, описанные в разделе 2 («пригоден», «не определен» или «не пригоден») могут служить частью локальной процедуры определения предпочтений в показанном ниже порядке.

```
"пригоден" предпочтительней чем
"не определен", что предпочтительней чем
"не пригоден".
```

Выбор действий для маршрутов с неопределенным состоянием пригодности определяется локальной политикой маршрутизации. С учетом частичного применения ROA в гетерогенных средах (типа сети общего пользования Internet) предлагается в локальной политике не считать состояние unknown достаточным основанием для исключения данного маршрута из числа рассматриваемых в процессе выбора лучшего.

Вопрос использования маршрутов с состоянием пригодности invalid или отказа от их рассмотрения в процессе выбора маршрута решается на основе локальной политики. Здесь возможно возникновение циклической зависимости — если полномочная точка публикации репозитория ROA или каких-то иных сертификатов, относящихся к адресному префиксу, размещается по адресу, относящемуся к описанному в ROA префиксу, этот репозиторий будет доступен для RP лишь после того, как маршрут к этому префиксу будет воспринят локальным доменом маршрутизации RP. Отмечено также, что время распространения объектов RPKI может отличаться от времени распространения маршрутов и система маршрутизации RP может узнать о маршрутах до того, как локальный кэш репозитория RPKI в данной RP получит соответствующие ROA и сочтет их пригодными (valid) d hfvrf[RPKI.

4. Отказ от создания маршрутов

ROA служат подтверждением того, что владелец префикса предоставил AS полномочия на создание маршрута к этому префиксу в системе междоменной маршрутизации. Владелец префикса может создать полномочия, в соответствии с которыми ни одной пригодной AS не будет предоставлено право создания маршрута для этого префикса. Этот анонсируется с помощью ROA, где в качестве номера AS указывается значение, которое недопустимо использовать в каком-либо контексте маршрутизации. В частности, AS 0 зарезервировано IANA так, что может использоваться для обозначения немаршрутизируемых сетей [IANA-AS].

ROA с AS 0 (AS 0 ROA) является подтверждением от владельца префикса того, что описанный в ROA и все более конкретные префиксы не следует использовать в контексте маршрутизации.

Процедура проверки пригодности маршрута, описанная в разделе 2, будет давать на выходе valid (пригоден), если какое-либо любое полномочие ROA соответствует адресному префиксу и AS, даже если другие действующие ROA будут указывать на непригодность (invalid) в случае их «изолированного» использования. Следовательно, AS 0 ROA имеет наиболее низкий уровень предпочтения по сравнению с любыми другими ROA, в которых указана маршрутизируемая AS. Это позволяет держателям префиксов использовать AS 0 ROA задать по умолчанию, что любой маршрут с таким же или более конкретным префиксом будет считаться «непригодным» (invalid), позволяя в то же время другим ROA описывать действующие полномочия для более конкретных префиксов.

По соглашению в AS 0 ROA следует указывать maxLength = 32 для IPv4 и maxlength = 128 для IPv6, хотя при проверке пригодности маршрутов результат будет неизменным для любого значения maxLength и даже при отсутствии maxLength в ROA.

По соглашению AS 0 ROA должно быть единственным полномочием ROA для данного адресного префикса, но и это требование не является строгим. AS 0 ROA может существовать одновременно с ROA, указывающими другие AS, и в таких случаях наличие или отсутствие AS 0 ROA не меняет состояния пригодности маршрута.

5. Срок пригодности маршрута

«Срок действия» результата проверки пригодности указывает интервал времени, в течение которого результат процесса проверки остается применимым. Здесь присутствует неявное допущение о том, что по завершении срока действия маршрут следует заново проверить на пригодность.

Срок действия ROA определяется значениями Valid в сертификате конечного элемента (EE[1]), использованном для подписи ROA, и времени действия сертификатов на пути сертификации, используемом для проверки пригодности сертификата EE. Срок действия ROA завершается в момент наступления времени notAfter в сертификате EE или в момент «исчезновения» пути сертификации, позволяющего проверить пригодность ROA. Эмитент ROA может заранее прервать действие ROA путем отзыва сертификата EE, который был использован для подписи ROA.

6. Вопросы безопасности

Эмитентам ROA следует принимать во внимание воздействие проверки пригодности на выпуск ROA в том смысле, что ROA неявно объявляет непригодными все маршруты, которые имеют более конкретные префиксы с размером префикса больше maxLength, а AS-источник отличается от AS указанных в наборе ROA для этого префикса.

Консервативное практикой работы с полномочиями будет гарантия выпуска ROA для всех более конкретных префиксов с отличающимися AS-источниками до выпуска ROA для более крупных (охватывающих) адресных блоков во избежание нежелательного объявления непригодными действующих маршрутов в процессе создания ROA.

Эмитентам ROA следует также принимать во внимание что при создании ROA для одной AS-источника последующее предоставление держателем префикса полномочий на создание маршрутов для этого же префикса другим AS влечет необходимость создания ROA для каждой из этих уполномоченных AS.

[1] End-entity.

7. Благодарности

Авторы хотели бы отметить вклад в подготовку этого документа John Scudder и Stephen Kent, а также отклики многочисленных участников рабочей группы SIDR в ответ на представление материалов на сессиях SIDR WG. Авторы также отмечают предварительную работу Tony Bates, Randy Bush, Tony Li и Yakov Rekhter в части описанной здесь проверки пригодности и семантики проверки AS-источников, описанную в [NLRI-ORIG]. Многие концепции проверки пригодности маршрутов, представленные в [BGP-PFX] под редакцией Pradosh Mohapatra и др., были использованы в этом документе.

8. Литература

8.1. Нормативные документы

[RFC3779] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers", RFC 3779, June 2004.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, February 2012.

[RFC6482] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", RFC 6482, February 2012.

8.2. Дополнительная литература

[BGP-PFX] Mohapatra, P., Ed., Scudder, J., Ed., Ward, D., Ed., Bush, R., Ed., and R. Austein, Ed., "BGP Prefix Origin Validation", Work in Progress[1], October 2011.

[IANA-AS] IANA, "Autonomous System (AS) Numbers", http://http://www.iana.org/assignments/as-numbers

[NLRI-ORIG] Bates, T., Bush, R., Li, T., and Y. Rekhter, "DNS-based NLRI origin AS verification in BGP", Work in Progress, January 1998.

Адреса авторов

Geoff Huston

APNIC

EMail: gih@apnic.net

George Michaelson

APNIC

EMail: ggm@apnic.net

Перевод на русский язык

Николай Малых

nmalykh@gmail.com

[1]Работа опубликована в RFC 6811. *Прим. перев.*