Secure Inter-Domain Routing (SIDR) G. Huston
Internet-Draft G. Michaelson
Intended status: Informational APNIC
Expires: April 9, 2009 October 6, 2008

Validation of Route Origination in BGP using the Resource Certificate PKI
draft-ietf-sidr-roa-validation-01.txt

Status of this Memo

Abstract

This document defines an application of the Resource Public Key Infrastructure to validate the origination of routes advertised in the Border Gateway Protocol. The proposed application is intended to fit within the requirements for adding security to inter-domain routing, including the ability to support incremental and piecemeal deployment, and does not require any changes to the specification of BGP.

Table of Contents

1. Introduction

This document defines an application of the Resource Public Key Infrastructure (RPKI) to validate the origination of routes advertised in the Border Gateway Protocol (BGP) [RFC4271].

The RPKI is based on Resource Certificates. Resource Certificates are X.509 certificates that conform to the PKIX profile [RFC5280], and to the extensions for IP addresses and AS identifiers [RFC3779]. A Resource Certificate describes an action by an issuer that binds a list of IP address blocks and Autonomous System (AS) numbers to the Subject of a certificate, identified by the unique association of the Subject's private key with the public key contained in the Resource Certificate. The PKI is structured such that each current Resource Certificate matches a current resource allocation or assignment. This is described in [I-D.ietf-sidr-arch].

Route Origin Authorizations (ROAs) are digitally signed objects that bind an address to an AS number, signed by the address holder. A ROA provides a means of verifying that an IP address block holder has authorized an AS to originate route objects in the inter-domain routing environment for that address block. ROAs are described in [I-D.ietf-sidr-roa-format].

Bogon Origin Attestations (BOAs) are digitally signed objects that describe a collection of address prefixes and AS numbers that are not authorised by the right-of-use holder to be advertised in the inter-domain routing system [I-D.ietf-sidr-boa].

This document describes how ROA and BOA validation outcomes can be used in the BGP route selection process, and how the proposed application of ROAs and BOAs are intended to fit within the requirements for adding security to inter-domain routing [ID.ietf-rpsec-bgpsecrec], including the ability to support incremental and piecemeal deployment. This proposed application does not require any changes to the specification of BGP protocol elements. The application may be used as part of BGP's local route selection algorithm [RFC4271].

2. Validation Outcomes of a BGP Route Object

A BGP Route Object is an address prefix and a set of attributes. In terms of ROA and BOA validation the prefix value and the origin AS are used in the validation operation.

If the route object is an aggregate and the AS Path contains an AS Set, then the origin AS is considered to be the AS described as the

AGGREGATOR [RFC4271] of the route object.

ROA validation is described in [I-D.ietf-sidr-roa-format], and the outcome of the validation operation is that the ROA is valid in the context of the RPKI, or validation has failed.

BOA validation is described in [I-D.ietf-sidr-boa], and the outcome of the validation operation is that the BOA is valid in the context of the RPKI, or validation has failed.

There appears to be two means of matching a route object to a ROA: decoupled and linked.

2.1. Decoupled Validation

The decoupled approach is where the ROAs are managed and distributed independently of the operation of the routing protocol and a local BGP speaker has access to a local cache of the complete set of ROAs and the RPKI data set when performing a validation operation.

In this case the BGP route object does not refer to a specific ROA. The relying party to match a route object to one or more candidate valid ROAs and BOAs in order to determine the appropriate local actions to perform on the route object.

The relying party selects the set of ROAs where the address prefix in the route object either exactly matches an ROAIPAddress (matching both the address prefix value and the prefix length), or where the route object spans a block of addresses that is included in the span described by the ROA's address prefix value and length and where the route object's prefix length is less than the ROA's prefix length and greater then or equal to the ROA's corresponding maxLength attribute.

The following outcomes are possible using the defined ROA validation procedure for each ROA in this set:

Exact Match:
A valid ROA exists, where the address prefix in the route object exactly matches a prefix listed in the ROA, or the ROA contains a covering aggregate and the prefix length of the route object is smaller than or equal to the ROA's associated maxLength attribute, and the origin AS in the route object matches the origin AS listed in the ROA.

Covering Match:
A valid ROA exists, where an address prefix in the ROA is a covering aggregate of the prefix in the route object, and the prefix length of the route object is greater than the ROA's associated maxLength attribute, and the origin AS in the route object matches the AS listed in the ROA.

Exact Mismatch:
A valid ROA exists where the address prefix in the route object exactly matches a prefix listed in the ROA, or the ROA contains a covering aggregate and the prefix length of the route object is smaller than or equal to the ROA's associated maxLength attribute, and the origin AS of the route object does not match the AS listed in the ROA.

Covering Mismatch:
A valid ROA exists where an address prefix in the ROA is a covering aggregate of the prefix in the route object, the prefix length of the route object is greater than the ROA's associated maxLength attribute, and the origin AS of the route object does not match the AS listed in the ROA.

No ROA:
There are no Exact Matches, Covering Matches, no Exact Mismatches or Covering Mismatches in the RPKI repository.

The ROA to be used for the validation function is selected from the set of ROAs in the order given above. In other words an Exact Match is preferred over a Covering Match, which, in turn, is preferred over an Exact Mismatch which is preferred over a Covering Mismatch.

The set of BOAs that are used for the validation function are composed of the set of valid BOAs where the origin AS of the route object matches an AS described in a BOA, or where an address prefix in a valid BOA that is an exact match or a covering aggregate of the route object. In the case that the validation outcome using ROAs is one of Exact Mismatch, Covering Mismatch or No ROA, then the validation outcome of the BOA changes the overall validation result to "Bogon".

Bogon:
A valid BOA exists where an address prefix in the BOA is a an exact match for the prefix in the route object, or is a covering aggregate of the prefix in the route object, or an AS in the BOA matches the originating AS in the BOA. In addition, there is no valid ROA that is an Exact Match or a Covering Match with the route object.

2.2. Linked Validation

The linked approach requires the route object to reference a ROA either by inclusion of the ROA as an attribute of the route object, or inclusion of a identity field in an attribute of the route object as a means of identifying a particular ROA.

If the ROA can be located is valid within the context of the RPKI then the route object can be compared against the ROA, as per the previous section, giving one of five possible results: Exact Match, Covering Match, Exact Mismatch, Covering Mismatch, and No Match, which is defined as:

No Match:
The valid ROA does not comtain any address prefix that exactly matches the address prefix in the route object, or is a covering aggregate of the address prefix in the route object.

In the case of a Mismatch or a No Match condition, the relying party should check for the presence of valid BOAs where the origin AS of the route object matches an AS described in a BOA, or where an address prefix in a valid BOA that is an exact match or a covering aggregate of the route object. If a valid BOA can be found that matches either of these conditions that the overall route object validation of a route object with a linked ROA is changed to "Bogon".

3. Applying Validation Outcomes to BGP Route Selection

Within the framework of the abstract model of BGP operation, a received prefix announcement from a peer is compared to all announcements for this prefix received from other peers and a route selection procedure is used to select the "best" route object from this candidate set which is then used locally by placing it in the loc-RIB, and is announced to peers as the local "best" route.

It is proposed here that the validation outcome be used as part of the determination of the local degree of preference as defined in section 9.1.1 of the BGP specification [RFC4271].

In the case of partial deployment of ROAs there are a very limited set of circumstances where the outcome of ROA validation can be used as grounds to reject all consideration of the route object as an invalid advertisement. While the presence of a valid ROA that matches the advertisement is a strong indication that an advertisement matches the authority provided by the prefix holder to advertise the prefix into the routing system, the absence of a ROA or
the invalidity of a covering ROA does not provide a conclusive

indication that the advertisement has been undertaken without the address holder's permission, unless the object is described in a BOA.

In the case of a partial deployment scenario of RPKI route attestation objects, where some address prefixes and AS numbers are described in ROAs or BOAs and others are not, then the relative ranking of validation outcomes from the highest (most preferred) to the lowest (least preferred) degree of preference are proposed to be as specified int he following list. The exact values to apply to a Local Preference setting are left as a matter of local policy and local configuration.

1. Exact Match

   The prefix has been allocated and is routeable, and that the prefix right-of-use holder has authorized the originating AS to originate precisely this announcement.

2. Covering Match

   This is slightly less preferred because it is possible that the address holder of the aggregate has allocated the prefix in question to a different party. It is also possible that the originating AS is using more specific advertisements as part of a traffic engineering scenario.

3. No ROA

   In the case of partial deployment of ROAs, the absence of validation credentials is a neutral outcome, in that there is no grounds to increase or decrease the relative degree of preference for the route object.

4. Covering Mismatch

   A Covering Mismatch is considered to be less preferable than a neutral position in that the address holder of a covering aggregate has indicated an originating AS that is not the originating AS of this announcement. On the other hand it may be the case that this prefix has been validly allocated to another party who has not generated a ROA for this prefix even through the announcement is valid.

5. Exact Mismatch

   Here the exact match prefix holder has validly provided an authority for origination by an AS that is not the AS that is originating this announcement. This would appear to be a bogus

announcement by inference.

6. No Match

Here the route object has referenced a ROA that is not valid, or does not include an address prefix that matcehs the route object, or the referenced ROA could not be located. This could be an attempt to create a false route object and use an invalid ROA.

7. Bogon

Here the right-of-use holder of the AS or address prefix has explicitly tagged the address prefix or the AS as a "bogon". This implies that the announcement has been made without the appropriate authority, and the local preference of the route object should be ranked at a level commensurate with rejecting the route object.

In the case of comprehensive deployment of RPKI route attestion objects the absence of a specific ROA origination authority for the route object should render it as an unusable for routing. In this case the local preference setting for the route object is as follows:

1. Exact Match

The prefix has been allocated and is routeable, and that the prefix right-of-use holder has authorized the originating AS to originate precisely this announcement.

2. Covering Match, No ROA, Covering Mismatch, Exact Mismatch, No Match

The local preference of the route object should be ranked at a level of least preferred, due to the constraints noted in the following section.

3. Bogon

Here the right-of-use holder of the AS or address prefix has explicitly tagged the address prefix or the AS as a "bogon". This implies that the announcement has been made without the appropriate authority, and the local preference of the route object should be ranked at a level commensurate with rejecting the route object.

3.1. Validation Outcomes and Rejection of BGP Route Objects

In the case of comprehensive deployment of ROAs, the use of a validation outcome other than an Exact Match as sufficient grounds to reject a route object should be undertaken with care.

The consideration here is one of potential circularity of dependence. If the authoritative publication point of the repository of ROAs or any certificates used in relation to an address prefix is stored at a location that lies within the address prefix described in a ROA, then the repository can only be accessed once a route for the prefix has been accepted by the local routing domain. It is also noted that the propagation time of RPKI objects may be different to the propagation time of route objects in BGP, and that route objects may be received before the relying party's local repository cache picks up the associated ROAs and recognises them as valid within the RPKI.

For these reasons it is proposed that, even in the case of comprehensive deployment of ROAs, a missing ROA or a mismatch should not be considered as sufficient grounds to reject a route advertisement outright. Alternate approaches may involve the use of a local timer to accept the route for an interim period of time until there is an acceptable level of assurance that all reasonable efforts to local a valid ROA have been undertaken.

4. Further Considerations

This document provides a description of how ROAs and BOAs could be used by a BGP speaker.

It is noted that the proposed procedure requires no changes to the operation of BGP.

It is also noted that the decoupled and linked approach are not mutually exclusive, and the same procedure can be applied to route objects that contain an explicit pointer to the associated ROA and route objects where the local BGP speaker has to create a set of candidate ROAs that could be applied to a route object. However, there are a number of considerations about this approach to origination validation that are not specified here.

These considerations include:

- It is not specified when validation of an advertised prefix

should
      be performed by a BGP speaker. Is is considered to be a matter
of
      local policy whether it is considered to be strictly necessary to
      perform validation at a point prior to loading the object into
the

Adj-RIB-In structure, or once the object has been loaded into Adj-RIB-In, or at a later time that is determined by a local configuration setting. It is also not specified whether origination validation should be performed each time a route object is updated by a peer even when the origin AS has not altered.

- The lifetime of a validation outcome is not specified here. This specifically refers to the time period during which the original validation outcome can be still applied, and the time when the routing object be revalidated. It is a matter of local policy setting as to whether a validation outcome be regarded as valid until the route object is withdrawn or further updated, or whether validation of a route object should occur at more frequent intervals?

- It is a matter of local policy as to whther there are circumstances that would allow a route object to be removed from further consideration in route selection upon a validation failure, similar to the actions of Route Flap Damping.

- It is a matter of local configuration as to whther ROA validation is performed on a per-AS basis rather than a per-BGP speaker, and the appropriate BGP mechanisms to support such a per-AS iBGP route validation service are not considered here.

5. Security Considerations

This approach to orgination validation does not allow for 'deterministic' validation in terms of the ability of a BGP speker to accept or reject an advertised route object outright, given that there remains some issues of potential circularity of dependence and time lags between the propagation of information in the routing system and propagation of information in the RPKI.

There are also issues of the most appropirate interpretation of outcomes where validation of the authenticity of the route object has not been possible in the context of partial adoption of the RPKI, where the absense of validation information does not necessarily constitute sufficient grounds to interpret the route object as an invalidly originated object.

The consequence of these considerations is that while the use of ROAs can increase the confidence in the validity of origination of route

objects that match a valid ROA, ROAs cannot perform the opposite, namely the rejection of route objects that cannot be validated by

ROAs. To assist in the case of rejecting some forms of route objects that cannot be explicitly validated, the BOA has been used as a means of explicit rejection of certain classes route objects. The implication is that publishers in the RPKI should publish both ROAs and BOAs in order to provide the greatest level of information that will allow relying parties to make appropriate choices in terms of route preference selection.

6. IANA Considerations

[There are no IANA considerations in this document.]

7. Normative References

[I-D.ietf-sidr-arch] Lepinski, M., Kent, S., and R. Barnes, "An Infrastructure to Support Secure Internet Routing", draft-ietf-sidr-arch (work in progress), February 2008.

[I-D.ietf-sidr-boa] Huston, G., Manderson, T., and G. Michaelson, "Profile for Bogon Origin Attestations (BOAs)", draft-ietf-sidr-bogons (work in progress), August 2008.

[I-D.ietf-sidr-roa-format] Lepinski, M., Kent, S., and D. Kong, "An Infrastructure to Support Secure Internet Routing", draft-ietf-sidr-roa-format (work in progress), July 2008.

[ID.ietf-rpsec-bgpsecrec] Christian, B. and T. Tauber, "BGP Security Requirements", draft-ietf-sidr-roa-format (work in progress), November 2007.

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

[RFC4271] Rekhter, Y., Li, T., and S. Hares, "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.

Authors' Addresses

Geoff Huston
Asia Pacific Network Information Centre

Email: gih@apnic.net

George Michaelson
Asia Pacific Network Information Centre

Email: ggm@apnic.net

Full Copyright Statement

Intellectual Property