

Individual Submission
Internet-Draft
Intended status: Informational
Expires: February 8, 2009

G. Huston
G. Michaelson
APNIC
August 7, 2008

Validation of Route Origination in BGP using the Resource Certificate
PKI
draft-ietf-sidr-roa-validation-00.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on February 8, 2009.

Copyright Notice

Copyright (C) The IETF Trust (2008).

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.

Internet-Draft

Route Validation

August 2008

Table of Contents

1.	Introduction	3
2.	Validation Outcomes of a BGP Route Object	3
2.1.	Decoupled Validation	4
2.2.	Linked Validation	5
3.	Applying Validation Outcomes to BGP Route Selection	6
3.1.	Using Validation Outcomes to reject BGP advertisements . .	7
4.	Open Issues	8
5.	Security Considerations	9
6.	IANA Considerations	9
7.	Normative References	9
	Authors' Addresses	10
	Intellectual Property and Copyright Statements	11

Internet-Draft

Route Validation

August 2008

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-bgpsec](#)], 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 than 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:

- o An "exact match" is a valid ROA where the address prefix in the route object exactly matches a prefix listed in the ROA and the origin AS in the route object matches the origin AS listed in the ROA.
- o A "covering match" is a valid ROA where the 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 or equal to the ROA's maxLength attribute, and the origin AS in the route object matches the AS listed in the ROA.

- o An "exact mismatch" is a ROA where the address prefix in the route object exactly matches a prefix listed in the ROA and the origin AS of the route object does not match the AS listed in the ROA.
- o A "covering mismatch" is a ROA where the 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 or equal to the ROA's maxLength attribute, and the origin AS of the route object does not match the AS listed in the ROA.
- o "ROA missing" is where there are no exact or covering matches, no exact or covering mismatches and no exact or covering failures in the RPKI repository.

In this case the ROA that would be used for the validation function is selected from the set such that the most specific valid ROA that matches or covers the route object address prefix and where the route object origin AS matches the ROA AS. If there is no such ROA in the set, then the most specific valid ROA is selected. If there is no such ROA in the set then the most specific ROA is selected.

The set of BOAs that are used in validation are composed of the set

of valid BOAs where the origin AS matches an AS described in a BOA, or where the BOA's address prefix 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 "ROA missing"), then the validation outcome of the BOA changes the overall validation result to "bogon match".

[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. The relying party will still need check for BOAs that refer to this route object in the case that an exact match or a covering match is not present. The set of possible outcomes of linked validation is as follows:

- o "exact match"
- o "covering match"
- o "exact mismatch"
- o "covering mismatch"

- o "bogon match"
- o "ROA missing"

[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 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 or RPKI route attestation objects, when some prefixes 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 as follows:

1. "exact match"

An exact match indicates that 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"

A covering match 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, and both the aggregate address holder and the prefix holder have signed ROAs

and are advertising the prefix.

3. "ROA missing"

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

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 though the announcement is valid.

5. An "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. "bogon match"

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 prefix should be ranked at a level commensurate with rejecting the route object.

In the case of comprehensive deployment of ROAs the absence of a specific origination authority for the route object should render it as unusable for routing. In this case the relative degree of preference the relative local degree of preference can be adjusted such that cases 3 through 5 of the above list have an equal level of lesser preference.

[3.1.](#) Using Validation Outcomes to reject BGP advertisements

The use of a validation outcome of a missing ROA, or a covering or exact mismatch 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 to related 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. 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.

4. Open Issues

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 questions about this approach that are not resolved here.

Some open issues at this point are:

- o When should validation of an advertised prefix be performed by a BGP speaker? Is it 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? Should validation be performed each time a route object is updated by a peer even when the origin AS has not altered?
- o What is the lifetime of a validation outcome? When should the routing object be revalidated? Should the validation outcome be regarded as valid until the route object is withdrawn or further updated, or should validation occur at more frequent intervals?
- o Are there 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?

- o Can ROA validation be performed on a per-AS basis rather than a per-BGP speaker? What BGP mechanisms would be appropriate to support such a mode of operation?
- o If a relying party had access to RPKI signed objects with comparable semantics to a Route Registry's Route Object (RRRO), namely the acknowledgement by an AS holder that it intends to originate an advertisement for a specified address prefix, how would this validation procedure be altered. Presumably these signed RRROs would need to describe the complete set of address prefixes that may be announced by this originating AS in order to be of use in this context. Failure to match a valid RPKI RRRO would then be commensurate with a "bogon match", namely rejection of the route object, in a manner similar to the operation of a filter list constructed from a Route Registry.

5. Security Considerations

[To be Completed - the intent of this validation approach is to improve the level of confidence in route objects in the IDR domain. It is noted that this approach does not allow for 'comprehensive' validation 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, and issues of treatment of unauthorised route objects in the scenario of partial use of the RPKI. The consequence is that ROAs can increase the confidence in the validity of route objects that match a valid ROA, but cannot perform the opposite of explicitly rejecting invalid route objects. To assist in the case of rejecting invalid route objects the BOA has been used as a means of explicit rejection of certain classes route objects. The implication is that RRs should issue 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 at this stage. Later iterations of this draft may propose to add a ROA identifier into the BGP attribute set]

7. Normative References

[I-D.ietf-sidr-arch]

Lepinski, M., Kent, S., and R. Barnes, "An Infrastructure

Huston & Michaelson

Expires February 8, 2009

[Page 9]

Internet-Draft

Route Validation

August 2008

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
URI: <http://www.apnic.net>

George Michaelson
Asia Pacific Network Information Centre

Email: ggm@apnic.net
URI: <http://www.apnic.net>

Huston & Michaelson

Expires February 8, 2009

[Page 10]

Internet-Draft

Route Validation

August 2008

Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this

specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).