Secure Inter-Domain Routing (SIDR)
Internet-Draft
Intended status: Informational
Expires: November 27, 2009

G. Huston
G. Michaelson
APNIC

May 26, 2009

Validation of Route Origination in BGP using the Resource Certificate PKI

draft-huston-sidr-roa-validation-01.txt

Status of this Memo

Copyright Notice

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].

This document describes how ROA validation outcomes can be used in the BGP route selection process, and how the proposed application of ROAs is intended to fit within the requirements for adding security to inter-domain routing, 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.

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 needs to match a route object to one or more candidate valid ROAs in order to determine the appropriate local actions to perform on the route object.

The relying party selects a set of valid 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.

If the set of ROAs is empty then the validation outcome can be classified as "unknown".

Otherwise the route object should be tested against the set of valid ROAS. 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.

More Specific:
: 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.

AS 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.

More Specific AS 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.

If any of the ROAs in the set provide an "Exact Match" outcome then the BGP route object can be interpreted by the Relying Party as "valid", otherwise the route object can be regarded as "invalid".

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, and can be validated if there is an "Exact Match" and otherwise be regarded as invalid.

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 (or "unknown", "valid" or "invalid") 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].

The proposed addition to the local degree of preference is "valid" is

to be preferred over "unknown" over "invalid".

3.1. Validation Outcomes and Rejection of BGP Route Objects

It is a matter of local preference setting whether "invalid" route objects are discarded from further consideration in the route selection process, however the following consideration should be taken into account in such a situation.

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 advised that, even in the case of comprehensive deployment of ROAs, "unknown" and "invalid" validations 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 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 whether 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 whether 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 origination validation does not allow for 'deterministic' validation in terms of the ability of a BGP speaker 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 appropriate 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 absence of validation information does not necessarily constitute sufficient grounds to interpret the route object as an invalidly originated object.

6. IANA Considerations

[There are no IANA considerations in this document.]

7. Changes from draft-ietf-sidr-roa-validation-01

Following WG discussion at IETF 74 on the appropriate means of specification of denial in routing authorizations in the context of the RPKI, it appears to the authors that there is no general WG support for the inclusion of an explicit denial capability. Instead, the authors are of the view there was visible WG support, to the level of some form of rough consensus, for the approach where a valid ROA acts as an implicit "denial" for those route objects that have address prefixes that are more specific than the set of prefixes specified in the ROA, and for those route objects which have originating AS numbers other than those listed in valid ROAs that span the address prefix listed in the route object. This draft has been revised to remove all references to the use of an explicit denial object in ROA validation, and uses only the semantics of a ROA to define an "invalid" route object in this context. The remainder of the WG internet draft has been left largely intact.

8. 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), March 2009.

[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), nOVEMBER 2008.

[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