Secure Inter-Domain Routing (SIDR)
Internet-Draft
Intended status: Informational
Expires: February 5, 2010

G. Huston
G. Michaelson
APNIC

August 4, 2009

Validation of Route Origination in BGP using the Resource Certificate PKI

draft-ietf-sidr-roa-validation-02.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]. ROAs are intended to fit within the requirements for adding security to inter-domain routing, including the ability to support incremental and piecemeal deployment.

This document describes the semantic interpretation of a valid ROA, with particular reference to application in BGP relating to the origination of route objects. The document does not describe any application of a ROA to validation of the AS Path.

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 validation of the Route Object the prefix value and the origin AS attribute 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.

It is assumed here that ROAs are managed and distributed independently of the operation of BGP itself, 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.

A BGP route object does not refer to a specific ROA that should be used by a Relying Party (RP) to validate the origination information contained in the route object, nor does it refer to the set of certificates that the RP should use to validate the ROA's digital signature. The RP 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.

To validate a route object the RP would undertake the following steps:

1. Select all valid ROAs that include a ROAIPAddress value that either matches, or is a covering aggregate of, the address prefix in the route object.
2. If the set of candidate ROAs is empty the validation process stops with an outcome of "unknown".
3. If any ROA has an asID value that matches the originating AS in the route object, and either the route object's address prefix precisely matches an address in the ROA, or the route object's address prefix is a more specific prefix of the address in the ROA and the prefix length value is less than or equal to the ROAIPAddress's maxLength value, then the validation process stops

with an outcome of "valid".
4. Otherwise, the validation outcome is "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 installing it in the loc-RIB [RFC4271], and is announced to peers as the local "best" route.

It is proposed here that the ROA validation outcome of "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".

It is a matter of local BGP selection policy in 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 local policy settings should not result in "unknown" validation outcomes being considered as sufficient grounds to reject a route object outright from

consideration as a local "best" route.

A local policy setting may be considered such that "invalid" validation outcomes would be sufficient grounds to reject the route object. However, due to the considerations of circular dependence and differing propagation times as noted above, a local policy setting may be considered that would involve the use of a local timer to accept the route as feasible for an interim period of time until there is an acceptable level of assurance that all reasonable efforts to obtain a valid ROA for the object 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. However, there are a number of considerations about this approach to origination validation that are relevant to the operation of a BGP speaker 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. It is considered to be a matter of local policy whether it is strictly required to perform validation at a point prior to loading the object into the Adj-RIB-In structure [RFC4271], 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, at the expiration of which the routing object should be re-tested for validity. 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.

- o 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 mechanisms to support a de-coupled framework of validation of ROAs and the loading of outcomes into BGP speakers are not considered here.

5. Security Considerations

This approach to origination validation uses a model of positive security, where information that cannot be validated within the RPKI framework is intended to interpreted by a RP as invalid.

However, the considerations of accommodating environments of partial adoption, where only a subset of valid route objects have associated ROAs within the structure of the RPKI imply some modification to the model of positive security. Here it is assumed that once an address prefix is described in a ROA, then this ROA "protects" all address prefixes that are more specific than that described in the ROA. Thus, any more specific address prefix and originating AS combination of a valid ROA, that does not have a matching valid ROA is considered to be "invalid".

The match condition of a route object against a single ROA is summarized in the following table:

Prefix	match AS	mismatch AS
Covering Aggregate	unknown	unknown
match ROA prefix	valid	invalid

More Specific than ROA	invalid	invalid

In an environment of a collection of ROAs, a route object is considered "valid" if any ROA provides a "valid" outcome, and "invalid" if one or more ROAs provide an "invalid" outcome and no ROAs provide a "valid" outcome. The "unknown" outcome occurs when no ROA produces a "valid" or an "invalid" outcome.

6. IANA Considerations

[There are no IANA considerations in this document.]

7. Changes -01 to -02

Following WG review of the means of specification of denial in routing authorizations in the context of the RPKI at IETF 74 and IETF 75, it appears that there is no general WG support for the use of an explicit denial object (termed a 'BOA'). The alternative approach, explored in previous iterations of this draft, used a more restricted interpretation of a ROA that yielded only "valid" or "unknown" outcomes (by using "unknown" where "invalid" is used in this revision of the document). To allow for "invalid" outcomes the draft used the BOA to undertake the role of a 'disavow' constraint, where a route object was considered to be "invalid" if it was the subject of a valid BOA and was not considered to be "valid" by any valid ROA. The reasons advanced to support the dropping of the BOA was the increased complexity of RP systems through the use of a second object in route validation, a potentially confusing mismatch in the interpretation scope between the ROA and the BOA, where the ROA's scope was limited to set of prefixes described in the ROA, while the BOA's scope included all possible more specifics of the prefixes listed in the BOA, and the ability to reconstruct the semantic equivalent of a BOA through the use of a ROA that used a restricted-use AS as its asID. Accordingly, this draft has been revised to remove all references to the use of an explicit denial object and uses the implicit semantics of denial in a ROA object.

There appears to be no WG interest in consideration of validation in

a "linked" model, where a ROA is bound to the route object that it is intended to validate. Accordingly this section of the text has also been dropped from this version.

8. Normative References

[I-D.ietf-sidr-arch]
Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", draft-ietf-sidr-arch (work in progress), July 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), July 2009.

[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