Secure Inter-Domain Routing (SIDR)
Internet-Draft
Intended status: Informational
Expires: February 7, 2010

G. Huston
G. Michaelson
APNIC

August 6, 2009

Validation of Route Origination in BGP using the Resource Certificate PKI and ROAs

draft-ietf-sidr-roa-validation-03.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 requirement 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) [I-D.ietf-sidr-arch] to validate the origination of routes advertised in the Border Gateway Protocol (BGP) [RFC4271].

The RPKI is based on a hierarchy of Resource Certificates that are aligned to the Internet number resource allocation structure. 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 RPKI is structured such that each current Resource Certificate matches a current resource allocation or assignment. This is further 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.

This document describes the semantic interpretation of a valid ROA, with particular reference to application in BGP relating to the origination of route objects.

This proposed application of validation of ROAs does not require any changes to the specification of BGP protocol elements. The outcomes of ROA validation may be used as part of BGP's local route selection procedure [RFC4271].

2. Validation Outcomes of a BGP Route Object

A BGP "route object" is an address prefix and an associated set of attributes. In terms of validation of the route object the address prefix value and the "origin AS" are used in the ROA validation operation. The route object's origin AS is the final element of the route object's AS_PATH attribute. If the final AS_PATH element is an AS Set, indicating that the route object is an aggregate, then the origin AS is taken as the AS component of the AGGREGATOR attribute [RFC4271].

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. The RP needs to match a route object to one or more candidate valid ROAs in order to determine a validation outcome, which, in turn, can be used to determine the appropriate local actions to perform on the route object. Valid ROAs are defined as ROAs that are determined to be syntactically correct and are signed using a signature that can be verified using the RPKI, as described in [I-D.ietf-sidr-roa-format]. The outcome of this ROA validation function is that either the RP has determined that the ROA is valid in the context of the RPKI, or the ROA is invalid, in which case the ROA is not to be used by the RP.

It is assumed here that ROAs are managed and distributed independently of the operation of BGP itself, and that a local BGP speaker has access to a local cache of the complete set of valid ROAs when performing a route object validation operation.

Route object validation is defined by the following procedure:

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 then the validation procedure stops with an outcome of "unknown".

3. If any ROA has an asID value that matches the origin AS in the

route object, and either the route object's address prefix precisely matches a ROAIPAddress in the ROA, or the route object's address prefix is a more specific prefix of a ROAIPAddress and the route object's prefix length value is less than or equal to the ROAIPAddress' maxLength value, then the validation procedure stops with an outcome of "valid".

4. Otherwise, the validation procedure stops with an outcome of "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 BGP speaking peer is compared to all announcements for this prefix received from other BGP peers and a route selection procedure is used to select the "best" route object from this candidate set. This route object is then used locally by installing it in the loc-RIB [RFC4271], and is announced to peers as

the local "best" route.

The route object validation outcome, described in Section 2, of "unknown", "valid" or "invalid" may 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 local degree of preference is as follows:

"valid" is to be preferred over
"unknown", which itself is to be preferred over
"invalid".

This preference ranking is performed prior to the steps described in section 9.1.1 of [RFC4271].

It is a matter of local BGP selection policy as to the actions to be undertaken by a BGP instance in processing route objects with "unknown" validation outcomes. Due to considerations of partial use of ROAs in heterogeneous environments, such as in the public Internet, 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 further consideration as a local "best" route.

It is a matter of local BGP selection policy as to whether "invalid" route objects are considered to be ineligible for further consideration in the route selection process. The consideration here is one of potential circularity of dependence. If the authoritative publication point of the repository of ROAs, or that of any certificate used in relation to an address prefix, is located at an address 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 RP's 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 RP's local repository cache picks up the associated ROAs and recognises them as valid within the RPKI.

A local policy setting may be considered such that "invalid" validation outcomes would be sufficient grounds to reject the route object. However, due to these considerations of circular dependence and differing propagation times of ROAs and route objects, an alternate local policy setting may be considered that would involve the use of a local timer to accept the route object 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 route object have been undertaken.

4. Further Considerations

4.1. Partial Deployment Considerations

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

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 this model of positive security. Here it is assumed that once an address prefix is described in a ROA, then this ROA encompasses 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".

Routes objects that describe address prefixes that are not fully described by any single ROA, i.e., those address prefixes that may be an aggregate of a ROA, or have no intersection with any ROA, and are not matched by any ROA and are not a more specific of any ROA cannot be reliably classified as "invalid" in a partial deployment scenario, and are therefore described as "unknown".

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

Prefix	matching AS	non-matching 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 to be "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 either a "valid" or an "invalid" outcome.

4.2. Disavowal of Routing Origination

A ROA is a positive attestation that a prefix holder has authorized an AS to originate a route for this prefix into the inter-domain routing system. It is possible for a prefix holder to attest that no AS has been granted any such authority by using a ROA where the ROA'S

subject AS is one that will not be used in a routing context. Specifically, AS 0 is reserved by the IANA such that it "may be use [sic] to identify non-routed networks" [IANA.AS-Registry].

A ROA with a subject of AS 0 is an attestation by the holder of a prefix that the prefix described in the ROA, and any more specific prefix, should not be used in a routing context.

The route object validation procedure, described in Section 2, will provide a "valid" outcome if any ROA matches the address prefix and origin AS, even if other valid ROAs would provide an "invalid" validation outcome if used in isolation. Consequently, an AS0 ROA has a lower preference than any other ROA that has a routeable AS as its subject. This allows a prefix holder to use an AS0 ROA to declare a default condition that any route object that is equal to, or more specific than the prefix to be considered to be invalid, while also allowing other concurrently issued ROAs to describe valid origination authorizations for more specific prefixes.

For example, the holder of prefix 203.0.113.0/24 may wish to authorise the origination of a route object of 203.0.113.196/26 by 64496, and explicitly declare that all other use of prefixes from this block should be considered invalid. This could be achieved through the issuing of a ROA for Address=203.0.113.0/24, maxLength=32, AS = 0 and a second ROA for Address=203.0.113.196/26, maxLength=26, AS=64496.

By convention, an AS 0 ROA should have a maxLength value of 32 for IPv4 addresses and 128 for IPv6 addresses, although in terms of route object validation the same outcome would be achieved with any valid maxLength value, or even if the maxLength element were to be omitted from the ROA. Also by convention, an AS 0 ROA should be the only ROA issued for a given address prefix, although again this is not a strict requirement. An AS 0 ROA can coexist with ROAs that have different subject AS values, although in such cases the presence of the AS 0 ROA does not alter the route object validation outcome in any way.

4.3. BGP 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.

* 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

ROA issuers should be aware of the validation implication in issuing a ROA, in that a ROA will implicitly invalidate all route objects for more specific prefixes with a prefix length greater than maxLength, and all originating AS's other than the AS listed in the collection of ROAs.

A conservative operational practice would be to ensure the issuing of ROAs for all more specific prefixes with distinct origination AS's prior to the issuing of ROAs for larger encompassing address blocks, in order to avoid inadvertent invalidation of valid route objects during ROA generation.

ROA issuers should also be aware that if they generate a ROA for one origin AS, then if the prefix is authorised by multiple AS's then ROAs should be generated for all such authorized AS's.

6. IANA Considerations

Dear IANA,

The AS number registry [IANA.AS-Registry] contains the following annotation against AS 0: "may be use to identify non-routed networks." Could you please add a 'd' as appropriate to this text?

Thank you,

the authors.

7. Change Log

Note: This section is NOT to be included in final version of this document.

7.1. Changes -02 to -03

Further Considerations section now has a subsection describing the assumptions that ROA validation is making about the precise nature of partial deployment, noting that a ROA has an implicit scope of application for all prefixes that are equal to or more specific than the prefix listed in the ROA

Moved the table of validation outcomes from the Security Considerations section to the section on Further Considerations.

Added consideration about disavowal and the use of an AS 0 ROA and its interpretation in the context of validation of route objects, and proposed conventions of use of an AS 0 ROA.

Noted hierarchical dependence of ROA issuance in the Security Considerations section.

7.2. 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 ROAs 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. References

8.1. 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.

8.2. Informative References

[IANA.AS-Registry]
IANA, "IANA Autonomous System Number Registry", August 2009.

Authors' Addresses

Geoff Huston
Asia Pacific Network Information Centre

Email: gih@apnic.net

George Michaelson
Asia Pacific Network Information Centre

Email: ggm@apnic.net