Secure Inter-Domain Routing (SIDR)
Internet-Draft
Intended status: Informational
Expires: September 4, 2010

G. Huston
G. Michaelson
APNIC

March 3, 2010

Validation of Route Origination using the Resource Certificate PKI and ROAs

draft-ietf-sidr-roa-validation-04.txt

Abstract

This document defines the semantics of a Route Origin Authorization in terms of the context of an application of the Resource Public Key Infrastructure to validate the origination of routes advertised in the Border Gateway Protocol.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and 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/1id-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 September 4, 2010.

Copyright Notice

Table of Contents

1. Introduction

This document defines the semantics of a Route Origin Authorization (ROA) in terms of the context of 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].

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 a particular 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 ROA, with particular reference to application in inter-domain routing relating to the origination of route objects, and the intended scope of the authority that is conveyed in the ROA.

2. ROA Validation Outcomes for a Route Object

A "route object" is an address prefix and an associated set of routing attributes. In terms of validation of the route object in the context of BGP [RFC4271]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].

It is assumed here that a Relying Party (RP) has access to a local cache of the complete set of valid ROAs when performing validation of

a 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 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.

This approach to route object origination validation uses a model of "positive" attestations, where route objects that cannot be validated within the RPKI framework would conventionally be treated by a RP as "invalid". However, the considerations of accommodating environments of partial adoption of the use of ROAs, where only a subset of validly advertised address prefixes have associated published ROAs within the structure of the RPKI, imply some modification to this model of positive attestation. In the context of route object validation it is assumed that once an address prefix is described in a ROA, then this ROA speifically encompasses all address prefixes that are more specific than that described in the ROA. Thus, any route object for more specific address prefix than that described by any valid ROA that does not itself have a matching valid ROA is considered to be "invalid". However, routes objects for address prefixes that are not fully described by any single ROA, i.e., those route objects whose address prefixes may be an aggregate of address prefixes described in a valid ROA, or have address prefixes where there is 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. Such route objects have a validation outcome of "unknown".

The validation condition of a route object with a prefix and an origin AS when using single ROA for validation 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. It is considered to be "invalid" if one (or more) ROAs provide an "invalid" outcome and no ROAs provide a "valid" outcome. It is considered to be "unknown" when no ROA produces either a "valid" or an "invalid" outcome.

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 of the selected ROAs 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 Route Selection

Within the framework of the abstract model of the operation of inter-domain routing using BGP [RFC4271], a received prefix announcement from a routing peer is compared to all announcements for this prefix received from other routing peers and a route selection procedure is used to select the "best" route object from this candidate set.

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, in which case the local order of preference is as follows:

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

It is a matter of local routing policy as to the actions to be undertaken by a routing entity 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 routing policy as to whether "invalid" route objects are considered to be ineligible for further consideration in a route selection process. A possible 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 by the RP 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, 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.

4. 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 construct an authorization where no valid AS has been granted any such authority to originate a route object for an address prefix. This is acheived by using a ROA where the ROA's subject AS is one that must never be used in any 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 AS 0 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 AS 0 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.

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.

5. Route Object Validation Lifetime

The "lifetime" of a validation outcome refers to the time period during which the original validation outcome can be still applied. The implicit assumption here is that when the validation lifetime expires the routing object SHOULD be re-tested for validity.

The validation lifetime for a ROA is controlled by the Valid times specified in the End Entity (EE) Certificate used to sign the ROA, and the valid times of those certificates in the certification path used to validate the EE Certificate. A ROA validation "expires" at the Validity To field of the signing EE certificate, or at such a time when there is no certification path that can validate the ROA. A ROA issuer may prematurely invalidate a ROA by revoking the EE certificate that was used to sign the ROA.

6. Security Considerations

ROA issuers should be aware of the validation implication in issuing a ROA, in that a ROA implicitly invalidates all route objects that have 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 for this prefix.

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 holder authorises multiple AS's to originate route objects it is necessary for a ROA be generated for every such authorized AS.

7. IANA Considerations

[There are no IANA Considerations.]

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), October 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), October 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", March 2010.

Authors' Addresses

Geoff Huston
Asia Pacific Network Information Centre

Email: gih@apnic.net

George Michaelson
Asia Pacific Network Information Centre

Email: ggm@apnic.net