               Validation of Route Origination Using
      the Resource Certificate Public Key Infrastructure (PKI) and
                  Route Origin Authorizations (ROAs)

Abstract

   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 to validate the origination of routes
   advertised in the Border Gateway Protocol.

Status of This Memo

   This document is not an Internet Standards Track specification; it is
   published for informational purposes.

   This document is a product of the Internet Engineering Task Force
   (IETF). It represents the consensus of the IETF community. It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG). Not all documents
   approved by the IESG are a candidate for any level of Internet
   Standard; see Section 2 of RFC 5741.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   http://www.rfc-editor.org/info/rfc6483.

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) [RFC6480] 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
   [RFC6480].

   ROAs are digitally signed objects that bind an address to an AS
   number, and are 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 routes in the inter-domain routing
   environment for that address block. ROAs are described in [RFC6482].
   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 routes, and the intended scope of the authority
   that is conveyed in the ROA.

2. ROA Validation Outcomes for a Route

   A "route" is unit of information that associates a set of
   destinations described by an IP address prefix with a set of
   attributes of a path to those destinations, as defined in Section 1.1
   of [RFC4271].

   A route's "origin AS" is defined as follows: If the final path
   segment of the AS_PATH is of type AS_SEQUENCE, the origin AS is the
   first element of the sequence (i.e., the AS in the rightmost position
   with respect to the position of octets in the protocol message). If
   the AS_PATH contains a path segment of type AS_SET, indicating that
   the route is an aggregate, then the origin AS cannot be determined.
   In terms of validation of a route in the context of a routing
   environment, the address prefix value and the origin AS are used in
   the ROA validation operation.

   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. (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 [RFC6482].) The RP needs to
   match a route to one or more valid candidate 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.

   This approach to route origination validation uses a generic model of
   "positive" attestation that has an associated inference that routes
   that cannot be validated within the RPKI framework would
   conventionally be interpreted by an 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 validation, it is assumed that once an
   address prefix is described in a ROA, then this ROA specifically
   encompasses all address prefixes that are more specific than that
   described in the ROA. Thus, any route for a more specific address
   prefix than that described by any valid ROA that does not itself have
   a matching valid ROA can be considered "invalid". However, routes
   for address prefixes that are not fully described by any single ROA
   (i.e., those routes 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 valid ROA), and are not
   matched by any valid ROA and do not have an address prefix that is a
   more specific address prefix described in any valid ROA, cannot be
   reliably classified as "invalid" in a partial deployment scenario.
   Such routes have a validation outcome of "unknown".

An abstract attribute of a route can be determined as the outcome of
this validation procedure, namely a "validity state" [BGP-PFX]. The
validity state of a route, with a prefix and an origin AS as defined
above, when using single ROA for determining this validity state, is
summarized in the following table:

```
        Route    matching  non-matching
   Prefix  AS->   AS           AS
    V            +---------+---------+
   Non-          | unknown | unknown |
   Intersecting  |         |         |
                 +---------+---------+
   Covering      | unknown | unknown |
   Aggregate     |         |         |
                 +---------+---------+
   match ROA     | valid   | invalid |
   prefix        |         |         |
                 +---------+---------+
   More          |         |         |
   Specific      | invalid | invalid |
   than ROA      |         |         |
                 +---------+---------+
```

                   Route's Validity State

In an environment of a collection of valid ROAs, a route's validity
state is considered to be "valid" if any ROA provides a "valid"
outcome. It's validity state is considered to be "invalid" if one
(or more) ROAs provide an "invalid" outcome and no ROAs provide a
"valid" outcome. Its validity state is considered to be "unknown"
(or, synonymously, "not found" [BGP-PFX]) when no valid ROA can
produce either a "valid" or an "invalid" validity state outcome.

A route validity state 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. This selection forms the set of
      "candidate ROAs".

   2. If the set of candidate ROAs is empty, then the procedure stops
      with an outcome of "unknown" (or, synonymously, "not found", as
      used in [BGP-PFX]).

   3. If the route's origin AS can be determined and any of the set
      of candidate ROAs has an asID value that matches the origin AS
      in the route, and the route's address prefix matches a
      ROAIPAddress in the ROA (where "match" is defined as where the

route's address precisely matches the ROAIPAddress, or where
the ROAIPAddress includes a maxLength element, and the route's
address prefix is a more specific prefix of the ROAIPAddress,
and the route's address prefix length value is less than or
equal to the ROAIPAddress maxLength value), then the procedure
halts with an outcome of "valid".

4. Otherwise, the procedure halts 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 from this candidate set.

The route's validity state, described in Section 2, of "valid",
"invalid", or "unknown" 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 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 those routes with
"unknown" validity states. 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" validity state outcomes being considered as sufficient
grounds to reject a route outright from further consideration as a
local best route.

It is a matter of local routing policy as to whether routes with an
"invalid" validity state are considered to be ineligible for further
consideration in a route selection process. Potential circular
dependence is a consideration here: 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 routes, and that routes may be learned by an RP's routing
system before the RP's local RPKI repository cache picks up the

associated ROAs and recognizes them as having a validity state of
"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 for an address prefix. This is achieved by
   using a ROA where the ROA's subject AS is one that must not be used
   in any routing context. Specifically, AS 0 is reserved by the IANA
   such that it may be used to identify non-routed networks [IANA-AS].

   A ROA with a subject of AS 0 (AS 0 ROA) 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 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
   relative preference than any other ROA that has a routable AS as its
   subject. This allows a prefix holder to use an AS 0 ROA to declare a
   default condition that any route that is equal to or more specific
   than the prefix to be considered "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 a maxlength value of 128 for IPv6 addresses;
   although, in terms of route 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 may coexist with ROAs that have different
   subject AS values; although in such cases, the presence or lack of
   presence of the AS 0 ROA does not alter the route's validity state in
   any way.

5. Route 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 route 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
notAfter 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 elect to 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 routes 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 ASes
   prior to the issuing of ROAs for larger encompassing address blocks,
   in order to avoid inadvertent invalidation of valid routes during ROA
   generation.

   ROA issuers should also be aware that if they generate a ROA for one
   origin AS, then if the address prefix holder authorizes multiple ASes
   to originate routes for a given address prefix, then is necessary for
   a ROA be generated for every such authorized AS.

7. Acknowledgements

   The authors would like to acknowledge the helpful contributions of
   John Scudder and Stephen Kent in preparing this document, and also
   the contributions of many members of the SIDR working group in
   response to presentations of this material in SIDR WG sessions. The
   authors also acknowledge prior work undertaken by Tony Bates, Randy
   Bush, Tony Li, and Yakov Rekhter as the validation outcomes described
   here reflect the authentication outcomes and semantics of origin AS
   verification described in [NLRI-ORIG]. A number of validation
   concepts relating to a route's validity state presented in [BGP-PFX],
   edited by Pradosh Mohapatra, et al., have be used in this document.

8. References

8.1. Normative References

   [RFC3779]   Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP
               Addresses and AS Identifiers", RFC 3779, June 2004.

   [RFC4271]   Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "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.

   [RFC6480]   Lepinski, M. and S. Kent, "An Infrastructure to Support
               Secure Internet Routing", RFC 6480, February 2012.

   [RFC6482]   Lepinski, M., Kent, S., and D. Kong, "A Profile for Route
               Origin Authorizations (ROAs)", RFC 6482, February 2012.

8.2. Informative References

   [BGP-PFX]   Mohapatra, P., Ed., Scudder, J., Ed., Ward, D., Ed.,
               Bush, R., Ed., and R. Austein, Ed., "BGP Prefix Origin
               Validation", Work in Progress, October 2011.

   [IANA-AS]   IANA, "Autonomous System (AS) Numbers",
               http://http://www.iana.org/assignments/as-numbers

   [NLRI-ORIG] Bates, T., Bush, R., Li, T., and Y. Rekhter, "DNS-based
               NLRI origin AS verification in BGP", Work in Progress,
               January 1998.

Authors' Addresses

   Geoff Huston
   APNIC

   EMail: gih@apnic.net

   George Michaelson
   APNIC

   EMail: ggm@apnic.net