Individual Submission
Internet-Draft
Intended status: Informational
Expires: August 11, 2008

G. Huston
G. Michaelson
APNIC

February 8, 2008

Validation of Route Origin Authorizations in BGP using the Resource Certificate PKI

draft-huston-sidr-roa-validation-00.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 3
2. Validation Outcomes of a BGP Route Object using ROAs 3
3. Applying Validation Outcomes to BGP Route Selection 5
3.1. Using ROA Validation Outcomes to reject BGP advertisements 7
4. Open Issues 8
5. Security Considerations 8
6. IANA Considerations 9
7. Normative References 9
Authors' Addresses 9
Intellectual Property and Copyright Statements 11

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 on Resource Certificates. Resource Certificates are X.509 certificates that conform to the PKIX profile [RFC3280], 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 are intended to fit within the requirements for adding security to inter-domain routing [ID.ietf-rpsec-bgpsecrec], including the ability to support incremental and piecemeal deployment, and, furthermore, does not require any changes to the specification of BGP.

2. Validation Outcomes of a BGP Route Object using ROAs

A BGP Route Object is an address prefix and a set of attributes. In terms of ROA validation the prefix value and the origin AS are used

in the validation operation.

[Note: If the origination of the prefix is an AS Set then ??. The draft authors do not have a clear idea as to what to propose here!]

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.

The decoupled approach 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 route object does not refer to a ROA, a certificate validation path, CRLs nor Trust Anchors, and it is the role of the relying party to match a route object to one or more candidate ROAs and perform the validation operation on a selected ROA in order to determine the appropriate local actions to perform on the route object. The second approach is where the route object references a ROA, either by explicit inclusion of the ROA itself as an attribute of the route object that is carried in BGP or by reference where some identification of the ROA is carried as an attribute of the object.

The more general case here is the decoupled approach where a set of ROAs are selected where the address prefix in the ROA is an exact match, or the address prefix in the ROA is a covering aggregate of the address prefix in the route object and the ROA has the requireExactMatch set to FALSE.The following outcomes are possible using the defined ROA validation procedure for each ROA in this set:

- An "exact match" is a valid ROA where the address prefix in the route object exactly matches a prefix listed in the ROA and the origin AS in the route object matches the origin AS listed in the ROA.

- A "covering match" is a valid ROA where the address prefix in the ROA is a covering aggregate of the prefix in the route object, and the ROA has the requireExactMatch value of TRUE, and the origin AS

in the route object matches the AS listed in the ROA.

- An "exact failure" is a ROA where the address prefix in the route object exactly matches a prefix listed in the ROA, the origin AS matches the AS listed in the ROA, but the EE certificate of the ROA signature fails to validate within the context of the RPKI.

- A "covering failure" is a ROA where the address prefix in the ROA is a covering aggregate of the prefix in the update, and the ROA has the requireExactMatch value FALSE, and the origin AS in the update matches the origin AS listed in the ROA, but the EE certificate that is associated with the ROA's digital signature fails to validate within the context of the RPKI.

- An "exact mismatch" is a ROA where the address prefix in the route object exactly matches a prefix listed in the ROA and the origin AS of the route object does not match the AS listed in the ROA.

- A "covering mismatch" is a ROA where the address prefix in the ROA is a covering aggregate of the prefix in the route object, the ROA has the requireExactMatch value FALSE, and the origin AS of the route object does not match the AS listed in the ROA.

- "ROA missing" is where there are no exact or covering matches, no exact or covering mismatches and no exact of covering failures in the RPKI repository.

In this case the ROA that would be used for the validation function is selected from the set such that the most specific valid ROA that matches or covers the route object address prefix and where the route object origin AS matches the ROA AS. If there is no such ROA in the set, then the most specific valid ROA is selected. If there is no such ROA in the set then the most specific ROA is selected.

The linked approach requires the route object to reference a ROA either buy inclusion of the ROA as an attribute of the route object, or inclusion of a identity field as a means of identifying a particular ROA. In this case the set of outcomes of ROA validation is a subset of the decoupled approach, as follows:

- "exact match"
- "covering match"
- "exact failure"
- "covering failure"
- "ROA missing"

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 candiudate 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 that the validation outcome 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].

In the case of a partial deployment scenario, when some prefixes are described in ROAs and others are not, then the relative ranking of

validation outcomes from the highest (most preferred) to the lowest (least preferred) degree of preference are proposed as follows:

1. "exact match"

   An exact match indicates that the prefix has been allocated and is routeable, and that the prefix right-of-use holder has authorized the originating AS to originate precisely this announcement.

2. "covering match"

   A covering match is slightly less preferred becuase it is possible that the address holder of the aggregate has allocated the prefix in question to a different party, and both the

aggregate address holder and the prefix holder have signed ROAs and are advertising the prefix.

3. "ROA missing"

   In the case of partial deployment of ROAs the absence of validation credentials is neutral, in that there is no grounds to increase or decrease the relative degree of preference for the prefix.

4. "covering mismatch"

   A covering mismatch is considered to be less preferable than a neutral position in that the address holder of a covering aggregate has indicated an originating AS that is not the originating AS of this announcement. On the other hand it may be the case that this prefix has been validly allocated to another party who has not generated a ROA for this prefix even through the announcement is valid.

5. "covering failure"

   A convering failure indicates that the ROA is not valid in terms of the PKI, but this still admit the possibility that the prefix has been allocated to another party who has not generated a ROA.

6. An "exact mismatch"

   Here the exact match prefix holder has validly provided an authority for origination by an AS that is not the AS that is originating this announcement. This would appear to be a bogus announcement by inference.

7. "exact failure"

   Here the authority to originate is not valid, indicating t6hat either the authority has expired or that the authority infomation has been constructed by someone other than the prefix owner. This implies that the announcement is made without authority.

In the case of comprehensive deployment of ROAs the relative local

degree of preference can be adjusted such that cases 3 through 5 of the above list have an equal level of lesser preference, as in this case there is no "missing" ROA so that a validation failure need not be interpreted as a potentially valid route object that does not have an associated ROA.

3.1. Using ROA Validation Outcomes to reject BGP advertisements

In the case of partial deployment of ROAs there are a very limited set of circumstances where the outcome of ROA validation can be used as grounds to reject all consideration of the route object as an invalid advertisement. While the presence of a valid ROA that matches the advertisement is astrong indication that an advertisement matches the authority provided by the prefix holder to advertise the prefix into the routing system, the absence of a ROA or the invalidity of a covering ROA does not provide a conclusive indication that the advertisement has been undertaken without the address holder's permission.

In the case of comprehensive deployment of ROAs an invalid ROA could be considered grounds for rejection of the route object advertisement were it not for the issue of circular dependence. If the authoritative publication point of the repository of ROAs or any certificates used to related to an address prefix is stored at a location that lies within the address prefix, then the repository can only be accessed once a route for the prefix has been accepted. If the local BGP speaker is in a position to use some mechanism to check for circular dependencies then in the case of comprehensive deployment of ROAs an invalid ROA would be sufficient grounds to reject a route object.

It is noted that validation of a ROA infers two properties of the address, namely that the address prefix itself is "valid" and is not part of a "reserved" pool held by the IANA, an RIR or any LIR, and secondly that the origination of the address in the routing system has been undertaken with the explicit permission of the address holder. Accepting an advertisement of an address prefix that has failed ROA validation admits the possibility of accepting an advertisment for an invalid address that is drawn from a reserved pool. In the case of comprehensive deployment of ROAS the validation

outcome of "ROA missing" is a strong indication that the address

itself is invalid, as in the comprehensive deployment model all validly advertised address space is, by definition, covered by a ROA. The issue of circularity dependency between the address and the publication point of the ROA would still need to be addressed in this case.

4. Open Issues

This document provides a description of how ROA validation 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 ques5tions about this approach that are not resolved here.

Some open issues at this point are:

- When should validation of an advertised prefix be performed by a BGP speaker? Is it 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? Should validation be performed each time a route object is updated by a peer even when the origin AS has not altered?

- What is the lifetime of a validation outcome? When should the routing object be revalidated? Should the validation outcome be regarded as valid until the route object is withdrawn or further updated, or should validation occur at more frequent intervals?

- Are there 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?

- Can ROA validation be performed on a per-AS basis rather than a per-BGP speaker? What BGP mechanisms would be appropriate to support such a mode of operation?

5. Security Considerations

[to be completed]

6. IANA Considerations

[There are no IANA considerations in this document at this stage. Later iterations of this draft propose to add a ROA identifier into the BGP route attribute set]

7. 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), November 2007.

[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 2007.

[ID.ietf-rpsec-bgpsecrec]
Christian, B. and T. Tauber, "BGP Security Requirements", draft-ietf-sidr-roa-format (work in progress), November 2007.

[RFC3280] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[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.

Authors' Addresses

Geoff Huston
Asia Pacific Network Information Centre

Email: gih@apnic.net
URI: http://www.apnic.net

George Michaelson
Asia Pacific Network Information Centre

Email: ggm@apnic.net
URI: http://www.apnic.net

Full Copyright Statement

Intellectual Property

specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).