Internet Engineering Task Force (IETF)
Request for Comments: 6811
Category: Standards Track
ISSN: 2070-1721

P. Mohapatra
Cisco Systems
J. Scudder
Juniper Networks
D. Ward
Cisco Systems
R. Bush
Internet Initiative Japan
R. Austein
Dragon Research Labs

January 2013

BGP Prefix Origin Validation

Abstract

To help reduce well-known threats against BGP including prefix mis-announcing and monkey-in-the-middle attacks, one of the security requirements is the ability to validate the origination Autonomous System (AS) of BGP routes. More specifically, one needs to validate that the AS number claiming to originate an address prefix (as derived from the AS_PATH attribute of the BGP route) is in fact authorized by the prefix holder to do so. This document describes a simple validation mechanism to partially satisfy this requirement.

Status of This Memo

This is an Internet Standards Track document.

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). Further information on Internet Standards is available in 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/rfc6811.

Table of Contents

1. Introduction

A BGP route associates an address prefix with a set of Autonomous Systems (ASes) that identify the interdomain path the prefix has traversed in the form of BGP announcements. This set is represented as the AS_PATH attribute in BGP [RFC4271] and starts with the AS that originated the prefix. To help reduce well-known threats against BGP including prefix mis-announcing and monkey-in-the-middle attacks, one of the security requirements is the ability to validate the origination AS of BGP routes. More specifically, one needs to validate that the AS number claiming to originate an address prefix (as derived from the AS_PATH attribute of the BGP route) is in fact authorized by the prefix holder to do so. This document describes a simple validation mechanism to partially satisfy this requirement.

The Resource Public Key Infrastructure (RPKI) describes an approach to build a formally verifiable database of IP addresses and AS numbers as resources. The overall architecture of RPKI as defined in [RFC6480] consists of three main components:

- a public key infrastructure (PKI) with the necessary certificate objects,
- digitally signed routing objects, and
- a distributed repository system to hold the objects that would also support periodic retrieval.

The RPKI system is based on resource certificates that define extensions to X.509 to represent IP addresses and AS identifiers [RFC3779], thus the name RPKI. Route Origin Authorizations (ROAs) [RFC6482] are separate digitally signed objects that define associations between ASes and IP address blocks. Finally, the repository system is operated in a distributed fashion through the IANA, Regional Internet Registry (RIR) hierarchy, and ISPs.

In order to benefit from the RPKI system, it is envisioned that relying parties at either the AS or organization level obtain a local copy of the signed object collection, verify the signatures, and process them. The cache must also be refreshed periodically. The exact access mechanism used to retrieve the local cache is beyond the scope of this document.

Individual BGP speakers can utilize the processed data contained in the local cache to validate BGP announcements. The protocol details to retrieve the processed data from the local cache to the BGP speakers is beyond the scope of this document (refer to [RFC6810] for such a mechanism). This document proposes a means by which a BGP speaker can make use of the processed data in order to assign a "validation state" to each prefix in a received BGP UPDATE message.

Note that the complete path attestation against the AS_PATH attribute of a route is outside the scope of this document.

Like the DNS, the global RPKI presents only a loosely consistent view, depending on timing, updating, fetching, etc. Thus, one cache or router may have different data about a particular prefix than another cache or router. There is no ’fix’ for this; it is the nature of distributed data with distributed caches.

Although RPKI provides the context for this document, it is equally possible to use any other database that is able to map prefixes to their authorized origin ASes. Each distinct database will have its

own particular operational and security characteristics; such characteristics are beyond the scope of this document.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119 [RFC2119] only when they appear in all upper case. They may also appear in lower or mixed case as English words, without special meaning.

2. Prefix-to-AS Mapping Database

The BGP speaker loads validated objects from the cache into local storage. The objects loaded have the content (IP address, prefix length, maximum length, origin AS number). We refer to such a locally stored object as a "Validated ROA Payload" or "VRP".

We define several terms in addition to "VRP". Where these terms are used, they are capitalized:

- Prefix: (IP address, prefix length), interpreted as is customary (see [RFC4632]).
- Route: Data derived from a received BGP UPDATE, as defined in [RFC4271], Section 1.1. The Route includes one Prefix and an AS_PATH; it may include other attributes to characterize the prefix.
- VRP Prefix: The Prefix from a VRP.
- VRP ASN: The origin AS number from a VRP.
- Route Prefix: The Prefix derived from a route.
- Route Origin ASN: The origin AS number derived from a Route as follows:
  - the rightmost AS in the final segment of the AS_PATH attribute in the Route if that segment is of type AS_SEQUENCE, or
  - the BGP speaker’s own AS number if that segment is of type AS_CONFED_SEQUENCE or AS_CONFED_SET or if the AS_PATH is empty, or
  - the distinguished value "NONE" if the final segment of the AS_PATH attribute is of any other type.

- Covered: A Route Prefix is said to be Covered by a VRP when the VRP prefix length is less than or equal to the Route prefix length, and the VRP prefix address and the Route prefix address are identical for all bits specified by the VRP prefix length. (That is, the Route prefix is either identical to the VRP prefix or more specific than the VRP prefix.)

- Matched: A Route Prefix is said to be Matched by a VRP when the Route Prefix is Covered by that VRP, the Route prefix length is less than or equal to the VRP maximum length, and the Route Origin ASN is equal to the VRP ASN.

Given these definitions, any given BGP Route will be found to have one of the following validation states:

- NotFound: No VRP Covers the Route Prefix.

- Valid: At least one VRP Matches the Route Prefix.

- Invalid: At least one VRP Covers the Route Prefix, but no VRP Matches it.

We observe that no VRP can have the value "NONE" as its VRP ASN. Thus, a Route whose Origin ASN is "NONE" cannot be Matched by any VRP. Similarly, no valid Route can have an Origin ASN of zero [AS0]. Thus, no Route can be Matched by a VRP whose ASN is zero.

When a BGP speaker receives an UPDATE from a neighbor, it SHOULD perform a lookup as described above for each of the Routes in the UPDATE message. The lookup SHOULD also be applied to routes that are redistributed into BGP from another source, such as another protocol or a locally defined static route. An implementation MAY provide configuration options to control which routes the lookup is applied to. The validation state of the Route MUST be set to reflect the result of the lookup. The implementation should consider the validation state as described in the document as a local property or attribute of the Route. If validation is not performed on a Route, the implementation SHOULD initialize the validation state of such a route to "NotFound".

Use of the validation state is discussed in Sections 3 and 5. An implementation MUST NOT exclude a route from the Adj-RIB-In or from consideration in the decision process as a side effect of its validation state, unless explicitly configured to do so.

We observe that a Route can be Matched or Covered by more than one VRP. This procedure does not mandate an order in which VRPs must be visited; however, the validation state output is fully determined.

2.1. Pseudo-Code

The following pseudo-code illustrates the procedure above. In case of ambiguity, the procedure above, rather than the pseudo-code, should be taken as authoritative.

```
result = BGP_PFXV_STATE_NOT_FOUND;

//Iterate through all the Covering entries in the local VRP
//database, pfx_validate_table.
entry = next_lookup_result(pfx_validate_table, route_prefix);

while (entry != NULL) {
  prefix_exists = TRUE;

  if (route_prefix_length <= entry->max_length) {
    if (route_origin_as != NONE
        && entry->origin_as != 0
        && route_origin_as == entry->origin_as) {
      result = BGP_PFXV_STATE_VALID;
      return (result);
    }
  }
  entry = next_lookup_result(pfx_validate_table, input.prefix);
}

//If one or more VRP entries Covered the route prefix, but
//none Matched, return "Invalid" validation state.
if (prefix_exists == TRUE) {
  result = BGP_PFXV_STATE_INVALID;
}

return (result);
```

3. Policy Control

An implementation MUST provide the ability to match and set the validation state of routes as part of its route policy filtering function. Use of validation state in route policy is elaborated in Section 5. For more details on operational policy considerations, see [ORIGIN-OPS].

An implementation MUST also support four-octet AS numbers [RFC6793].

4. Interaction with Local Cache

Each BGP speaker supporting prefix validation as described in this document is expected to communicate with one or more RPKI caches, each of which stores a local copy of the global RPKI database. The protocol mechanisms used to gather and validate these data and present them to BGP speakers are described in [RFC6810].

The prefix-to-AS mappings used by the BGP speaker are expected to be updated over time. When a mapping is added or deleted, the implementation MUST re-validate any affected prefixes and run the BGP decision process if needed. An "affected prefix" is any prefix that was matched by a deleted or updated mapping, or could be matched by an added or updated mapping.

5. Deployment Considerations

Once a Route is selected for validation, it is categorized according the procedure given in Section 2. Subsequently, routing policy as discussed in Section 3 can be used to take action based on the validation state.

Policies that could be implemented include filtering routes based on validation state (for example, rejecting all "invalid" routes) or adjusting a route’s degree of preference in the selection algorithm based on its validation state. The latter could be accomplished by adjusting the value of such attributes as LOCAL_PREF. Considering invalid routes for BGP decision process is a purely local policy matter and should be done with utmost care.

In some cases (particularly when the selection algorithm is influenced by the adjustment of a route property that is not propagated into Internal BGP (IBGP)) it could be necessary for routing correctness to propagate the validation state to the IBGP peer. This can be accomplished on the sending side by setting a community or extended community based on the validation state, and on the receiving side by matching the (extended) community and setting the validation state.

6. Security Considerations

Although this specification discusses one portion of a system to validate BGP routes, it should be noted that it relies on a database (RPKI or other) to provide validation information. As such, the security properties of that database must be considered in order to determine the security provided by the overall solution. If "invalid" routes are blocked as this specification suggests, the overall system provides a possible denial-of-service vector; for

example, if an attacker is able to inject (or remove) one or more records into (or from) the validation database, it could lead an otherwise valid route to be marked as invalid.

In addition, this system is only able to provide limited protection against a determined attacker -- the attacker need only prepend the "valid" source AS to a forged BGP route announcement in order to defeat the protection provided by this system.

This mechanism does not protect against "AS-in-the-middle attacks" or provide any path validation. It only attempts to verify the origin. In general, this system should be thought of more as a protection against misconfiguration than as true "security" in the strong sense.

7. Acknowledgments

The authors wish to thank Rex Fernando, Hannes Gredler, Mouhcine Guennoun, Russ Housley, Junaid Israr, Miya Kohno, Shin Miyakawa, Taka Mizuguchi, Hussein Mouftah, Keyur Patel, Tomoya Yoshida, Kannan Varadhan, Wes George, Jay Borkenhagen, and Sandra Murphy. The authors are grateful for the feedback from the members of the SIDR working group.

Junaid Israr’s contribution to this specification was part of his PhD research work and thesis at University of Ottawa.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[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.

[RFC4632] Fuller, V. and T. Li, "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan", BCP 122, RFC 4632, August 2006.

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

[RFC6793] Vohra, Q. and E. Chen, "BGP Support for Four-Octet Autonomous System (AS) Number Space", RFC 6793, December 2012.

8.2. Informational References

[AS0] Kumari, W., Bush, R., Schiller, H., and K. Patel, "Codification of AS 0 processing.", Work in Progress, August 2012.

[ORIGIN-OPS] Bush, R., "RPKI-Based Origin Validation Operation", Work in Progress, August 2012.

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

[RFC6810] Bush, R. and R. Austein, "The RPKI/Router Protocol", RFC 6810, January 2013.

Authors' Addresses

Pradosh Mohapatra
Cisco Systems
170 W. Tasman Drive
San Jose, CA 95134
USA

EMail: pmohapat@cisco.com

John Scudder
Juniper Networks
1194 N. Mathilda Ave
Sunnyvale, CA 94089
USA

EMail: jgs@juniper.net

David Ward
Cisco Systems
170 W. Tasman Drive
San Jose, CA 95134
USA

EMail: dward@cisco.com

Randy Bush
Internet Initiative Japan
5147 Crystal Springs
Bainbridge Island, WA 98110
USA

EMail: randy@psg.com

Rob Austein
Dragon Research Labs

EMail: sra@hactrn.net