              Clarifications to BGP Origin Validation Based on
                Resource Public Key Infrastructure (RPKI)

Abstract

   Deployment of BGP origin validation based on Resource Public Key
   Infrastructure (RPKI) is hampered by, among other things, vendor
   misimplementations in two critical areas: which routes are validated
   and whether policy is applied when not specified by configuration.
   This document is meant to clarify possible misunderstandings causing
   those misimplementations; it thus updates RFC 6811 by clarifying that
   all prefixes should have their validation state set and that policy
   must not be applied without operator configuration.

Status of This Memo

Copyright Notice

   Copyright (c) 2018 IETF Trust and the persons identified as the
   document authors. All rights reserved.

Table of Contents

1. Introduction

   Deployment of RPKI-based BGP origin validation is hampered by, among
   other things, vendor misimplementations in two critical areas: which
   routes are validated and whether policy is applied when not specified
   by configuration. This document is meant to clarify possible
   misunderstandings causing those misimplementations.

   When a route is distributed into BGP, the origin validation state is
   set to NotFound, Valid, or Invalid per [RFC6811]. Operational
   testing has shown that the specifications of that RFC were not
   sufficient to avoid divergent implementations. This document
   attempts to clarify two areas which seem to cause confusion.

   The implementation issues seem not to be about how to validate, i.e.,
   how to decide if a route is NotFound, Valid, or Invalid. The issues
   seem to be which routes should be evaluated and have their evaluation
   state set, and whether to apply policy without operator
   configuration.

2. Requirements Language

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and
   "OPTIONAL" in this document are to be interpreted as described in
   BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all
   capitals, as shown here.

3. Suggested Reading

   It is assumed that the reader understands BGP [RFC4271], the RPKI
   [RFC6480], Route Origin Authorizations (ROAs) [RFC6482], and
   RPKI-based Prefix Validation [RFC6811].

4. Evaluate ALL Prefixes

   Significant Clarification: A router MUST evaluate and set the
   validation state of all routes in BGP coming from any source (e.g.,
   eBGP, iBGP, or redistribution from static or connected routes),
   unless specifically configured otherwise by the operator. Otherwise,
   the operator does not have the ability to drop Invalid routes coming
   from every potential source and is therefore liable to complaints
   from neighbors about propagation of Invalid routes. For this reason,
   [RFC6811] says:

      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.

   [RFC6811] goes on to say, "An implementation MAY provide
   configuration options to control which routes the lookup is applied
   to."

   When redistributing into BGP from any source (e.g., IGP, iBGP, or
   from static or connected routes), there is no AS_PATH in the input to
   allow RPKI validation of the originating Autonomous System (AS). In
   such cases, the router MUST use the AS of the router's BGP
   configuration. If that is ambiguous because of confederation, AS
   migration, or other multi-AS configuration, then the router
   configuration MUST provide a means of specifying the AS to be used on
   the redistribution, either per redistribution or globally.

5. Set State, Don't Act

   Significant Clarification: Once routes are evaluated and have their
   state set, the operator should be in complete control of any policy
   applied based on the evaluation state. Absent specific operator
   configuration, policy MUST NOT be applied.

   Automatic origin validation policy actions such as those described in
   "BGP Prefix Origin Validation State Extended Community" [RFC8097]
   MUST NOT be carried out or otherwise applied unless specifically
   configured by the operator.

6. Security Considerations

   This document does not create security considerations beyond those of
   [RFC6811].

7. IANA Considerations

   This document has no IANA actions.

8. Normative References

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119,
              DOI 10.17487/RFC2119, March 1997,
              <https://www.rfc-editor.org/info/rfc2119>.

   [RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A
              Border Gateway Protocol 4 (BGP-4)", RFC 4271,
              DOI 10.17487/RFC4271, January 2006,
              <https://www.rfc-editor.org/info/rfc4271>.

   [RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support
              Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480,
              February 2012, <https://www.rfc-editor.org/info/rfc6480>.

   [RFC6482] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route
              Origin Authorizations (ROAs)", RFC 6482,
              DOI 10.17487/RFC6482, February 2012,
              <https://www.rfc-editor.org/info/rfc6482>.

   [RFC6811] Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R.
              Austein, "BGP Prefix Origin Validation", RFC 6811,
              DOI 10.17487/RFC6811, January 2013,
              <https://www.rfc-editor.org/info/rfc6811>.

   [RFC8097] Mohapatra, P., Patel, K., Scudder, J., Ward, D., and R.
              Bush, "BGP Prefix Origin Validation State Extended
              Community", RFC 8097, DOI 10.17487/RFC8097, March 2017,
              <https://www.rfc-editor.org/info/rfc8097>.

   [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
              2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
              May 2017, <https://www.rfc-editor.org/info/rfc8174>.

Acknowledgments

Author's Address

   Randy Bush
   Internet Initiative Japan
   5147 Crystal Springs
   Bainbridge Island, Washington 98110
   United States of America

   Email: randy@psg.com