SIDR Working Group
Internet-Drafts
Intended status: Standards Track
Expires: Oct 1, 2019

J. Beck
A. Gray
Charter
Mar 2019

# BGP Security Tracking
# draft-beck-bgp-security-tracking-00

Abstract

This document describes the BGP Path Security Tracking attribute, an extension to BGP-4. This attribute provides a transitive means for networks to indicate BGP security checks in place to upstream networks. Upstream networks can optionally use that information to modify the path selection algorithm giving preference to paths reporting better security where the prefix length is the same and as-path length is similar. Effectively reporting no security would be treated the same as prepending the announcement once and reporting strong security would be treated the same as not prepending. The net result of using the information to influence path selection is that more secured paths would be preferred over less secured paths.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on Oct 1, 2019.

Table of Contents



## 1. Introduction

Securing BGP from unauthorized prefix leaks is important. There are multiple measures available to validate inbound route announcements but most are only locally significant within an autonomous system (AS).The BGP Security tracking attribute allows a BGP speaking router to optionally mark the validation steps that were performed on a prefix with an attribute after accepting the prefix as valid for the purpose of transparency and allowing that information to influence the BGP path selection process. A router that learns of a prefix equal in length from multiple sources may optionally choose a path with better advertised security practices over a less secured one.

The intent is to encourage better security practices and partially limit the radius and impact of unauthorized route announcements.

Functionally the path selection is modified by assigning a cost based security practices implemented. A network with no ingress security would have a cost of 1 and a network with good ingress security would have a cost of 0. The BGP path selection algorithm would then be modified to evaluate the sum of ASN's in AS_PATH combined with the security measures for each network. A prefix with an AS_PATH length of 3 with no security would have a "cost" of 6 and prefix with an AS_PATH length of 3 with "good" security would have a "cost" of 3 allowing preference to the theoretically more secure path. Because the "cost" of security is less than or equal to an additional ASN in AS_PATH a bad actor is discouraged from spoofing false ASN's for the purpose of forging the security of that relationship.

## 2. Requirements Language

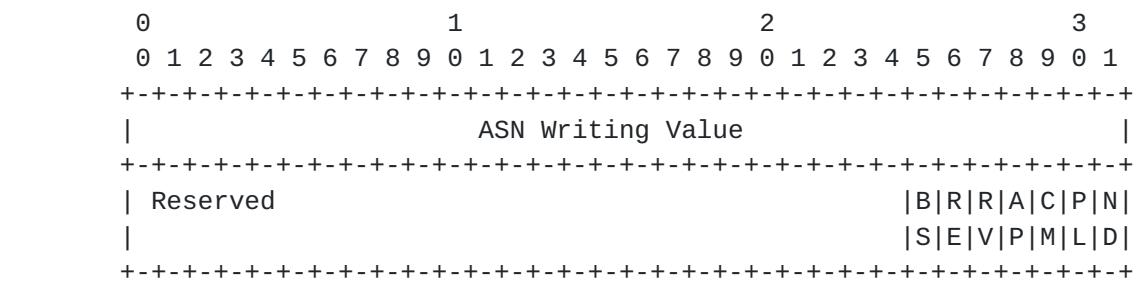
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

## 3. BGP Security Tracking Attribute

This document defines the BGP Security Tracking attribute as an optional transitive path attribute of variable length. The values are written to the prefix being accepted by the border router typically over an eBGP session before being announced upstream to other iBGP or eBGP peers. Networks opting not to disclose the information or not running supporting software do not push a value to the accepted prefix.

(Attribute type code for Security Tracking is to be assigned by IANA)

The format of the field is a concatenated list of 32-bit pairs of values, with each pair having the following definition:




All bits in the bitfield must start set to zero, and then set as below:

| Abbr | Name | Set to 1 if and only if |
|---|---|---|
| BS | BGPSec | Evaluated against BGPSec and returned VALID |
| RE | RPKI Eval | Evaluated against RPKI and was not INVALID |
| RV | RPKI Valid | Evaluated against RPKI and was VALID |
| AP | AS-Path | Validated against a per-customer AS-Path filter |
| CM | Community | Validated against a community tag value |
| PL | Prefix List | Validated against a per-customer prefix list |
| ND | Blocked | Data Not Disclosed |

The order of the attribute SHOULD reflect the order of ASN's in the AS_PATH. An ASN that is in the AS_PATH that lacks a corresponding BGP Security Tracking Attribute is assumed to be not participating or not

supported.

Setting a value is OPTIONAL but a network router MUST NOT modify values written by other downstream ASN's in the AS_PATH.

A value SHOULD be determined by the ingress router over an eBGP boundary. The originating ASN MUST NOT set a value for itself.

## 4. Canonical Representation

The canonical representation of the BGP Security Tracking attribute is 2 separate unsigned integers in decimal notation in the following order: Autonomous System Number, Security Methods Used. Numbers MUST NOT contain leading zeros; a zero value MUST be represented with a single zero. Each number is separated from the next by a single colon. For example: 64496:50 (RPKI Valid, validated against prefix list) or 64496:1 (data administratively suppressed).

## 5. Cost Value of Security Methods Used

84% of ASN's are stubs. Average AS-PATH length is 4-5 hops or 3.8 hops after accounting for prepends. Research by Sharon Goldberg and Boston University reflects that security against invalid announcements requires a combination of methods to be successful.
(Ref: http://www.cs.bu.edu/~goldbe/papers/BGPsecurityGoldbe.pdf)

As such, it is the intent of the cost values to reward use of multiple approaches and best practices. The use of the BGP Security Tracking attribute to modify the Path Selection Algorithm of BGP is OPTIONAL.

Methodology: By default networks with no security or no available data have a cost metric of 1. That value is reduced by 0.5 or 0.25 for validation methods used until the cost reaches 0 with 0 being the lowest possible and 1 being the highest possible value.

The cost reduction amounts are as follows:

1. Not Disclosed -0

2. Filtered against prefix list -0.5

3. RPKI Valid -0.5

4. RPKI Invalid +1

5. BGPsec -0.5

6. Validated against community -0.25

7. Validated against AS_PATH -0.25

## 6. Modifying BGP Best Path Selection Algorithm

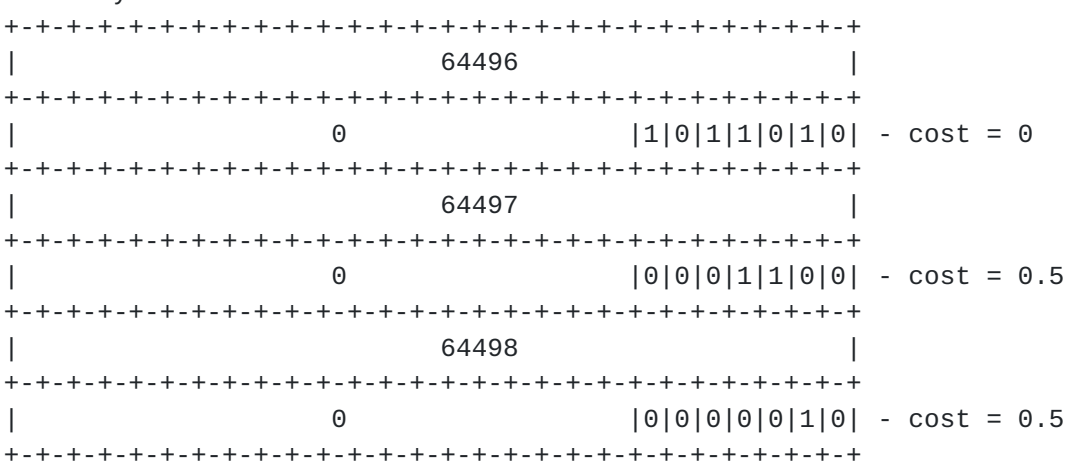
The use of the BGP Security Tracking attribute to modify the BGP Best Path Selection Algorithm of BGP is OPTIONAL.

In the path selection algorithm where a prefix is normally selected based on shortest AS_PATH this process is modified to take the sum of the AS_PATH plus the security tracking cost of the path. Functionally less secured paths have a higher cost of AS_PATH + Security and more secured paths have a lower cost of AS_PATH + Security.

Example 6.1

View from within ASN 64496:

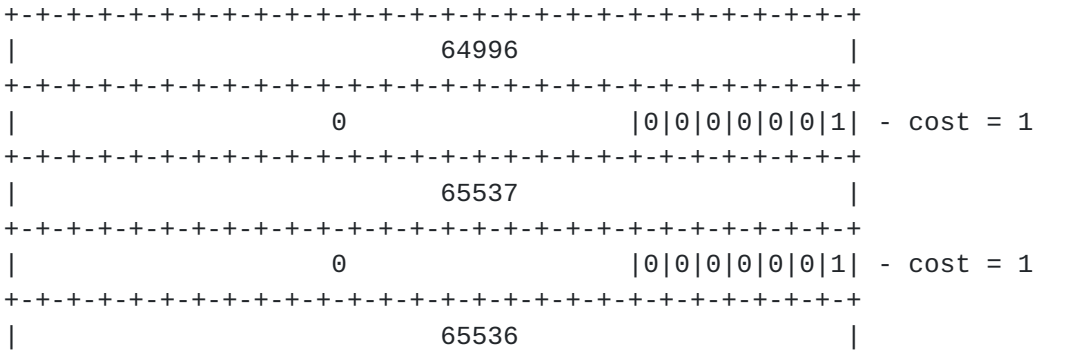
Security Attribute:

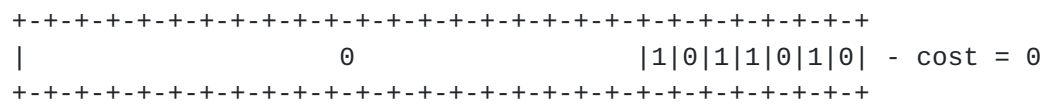



In example 6.1 even though the AS_PATH length is 3 the combined "cost" to reach the prefix is 4. There is no security value for ASN 64499 because it is the originating ASN and doesn't perform ingress validation of its own routes. There are 3 security tracking values because 64496:90 was written by the local ASN.

Example 6.2

View from within ASN 64496:
Security Attribute:






In example 6.2 even the AS_PATH length is 3 and the security "cost" is 2 for a total cost to reach the prefix of 5. A network evaluating a prefix with equal length received from both the example 6.1 and 6.2 path will see example 6.1 as having a shorter [AS_PATH + Security] preferring it.

In the event of a tie in combined AS_PATH + Security length the path with the lower security cost should be preferred breaking the tie. In the event they are both tied the router should continue through normal path selection or ECMP behavior.

## 7. Error Handling

The error handling of BGP Path Security Tracking is as follows:

- A BGP Security Tracking attribute SHALL be considered malformed if the length of the BGP Security Tracking Attribute value, expressed in octets, is not a non-zero multiple of 8.

- A BGP Security Tracking attribute SHALL be considered malformed due to presence of duplicate ASNs.

- A BGP Security Tracking attribute exceeding the number of ASNs in AS_PATH SHALL pair entries with corresponding ASN's in AS_PATH ignoring invalid entries (to handle potential repercussions of remove-private)

- A BGP UPDATE message with a malformed BGP Security Tracking attribute SHALL be handled using the approach of "treat-as-withdraw" as described in Section 2 of [RFC7606].

- If bits in the Reserved section are set, they MUST be preserved and MUST NOT be used for evaluation of the security "cost".

The BGP Security Tracking ASN field may contain any value, and a BGP Security Tracking attribute MUST NOT be considered malformed if the ASN field contains an unallocated, unassigned, or reserved ASN.

## 8. Security Considerations

As this document describes a security protocol, many aspects of security interest are described in relevant sections. This section points out issues that may not be obvious in other sections.

Spoofing of invalid path attribute values:
The most obvious means to defeat this measure is to falsify data about security checks that were not actually performed such as reporting that a prefix has been thoroughly validated when it has not. This is addressed by being lower to equal in value in the BGP Best Path Algorithm. If a bad actor is able to forge data it would generally be more beneficial to do so by shorting the AS_PATH rather than falsifying data about prefix validation or spoofing downstream ASN's for the purpose of reporting those borders as secure.

The exception to this is that it is possible to defeat RPKI validation by spoofing the valid origin ASN as being downstream artificially extending the AS_PATH length for the purpose of validating RPKI. In that case it would be more beneficial to forge the path security attribute data rather than shorten the AS_PATH.

More Specific Prefix Announcement:
The purpose of the path security tracking is to be able to select more secure paths over less secure paths where prefix length is equal. It does not override the preference for more specific routes over less specific routes and as such doesn't directly address the problem of invalid more specific announcements into the BGP table. It does indirectly help by encouraging adoption of better input validation and potential increased adoption of recommended best practices.

Network administrators should note the recommendations in [RFC7454] "BGP Operations and Security".

## 9. IANA Considerations

It is requested that IANA assign a value for SECURITY_TRACKING for an optional transitive attribute under the "BGP Path Attributes" subregistry under the Border Gateway Protocol (BGP) Parameters registry.

## 10. References

### 10.1. 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, <http://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, <http://www.rfc-editor.org/info/rfc4271>.

[RFC7606] Chen, E., Ed., Scudder, J., Ed., Mohapatra, P., and K. Patel, "Revised Error Handling for BGP UPDATE Messages", RFC 7606, DOI 10.17487/RFC7606, August 2015, <http://www.rfc-editor.org/info/rfc7606>.

### 10.2. Informative References

[RFC1997] Chandra, R., Traina, P., and T. Li, "BGP Communities Attribute", RFC 1997, DOI 10.17487/RFC1997, August 1996, <http://www.rfc-editor.org/info/rfc1997>.

[RFC4360] Sangli, S., Tappan, D., and Y. Rekhter, "BGP Extended Communities Attribute", RFC 4360, DOI 10.17487/RFC4360, February 2006, <http://www.rfc-editor.org/info/rfc4360>.

[RFC6793] Vohra, Q. and E. Chen, "BGP Support for Four-Octet Autonomous System (AS) Number Space", RFC 6793, DOI 10.17487/RFC6793, December 2012, <http://www.rfc-editor.org/info/rfc6793>.

[RFC7300] Haas, J. and J. Mitchell, "Reservation of Last Autonomous System (AS) Numbers", BCP 6, RFC 7300, DOI 10.17487/RFC7300, July 2014, <http://www.rfc-editor.org/info/rfc7300>.

[RFC7454] Durand, J., Pepelnjak, I., and G. Doering, "BGP Operations and Security", BCP 194, RFC 7454, DOI 10.17487/RFC7454,

February 2015, <http://www.rfc-editor.org/info/rfc7454>.

[RFC7607] Kumari, W., Bush, R., Schiller, H., and K. Patel, "Codification of AS 0 Processing", RFC 7607, DOI 10.17487/RFC7607, August 2015, <http://www.rfc-editor.org/info/rfc7607>.

## Acknowledgments

The authors would like to thank Jon Doe

## Contributors

The following people contributed significantly to the content of the document:

Jon Doe
Company Name
Email: email@domain.com

Authors' Addresses

Jody Beck
Charter Communications
14810 Grasslands Drive
Englewood, CO 80112
United States of America
Email: jody.beck@charter.com

Andrew Gray
Charter Communications
14810 Grasslands Drive
Englewood, CO 80112
United States of America
Email: andrew.gray@charter.com