Methods for Detection and Mitigation of BGP Route Leaks
draft-ietf-idr-route-leak-detection-mitigation-11

Abstract

   Problem definition for route leaks and enumeration of types of route
   leaks are provided in RFC 7908. This document describes a solution
   for detection and mitigation route leaks which is based on conveying
   route-leak protection (RLP) information in a Border Gateway Protocol
   (BGP) community. The RLP information is carried in a new well-known
   transitive BGP community, called the RLP community. The RLP
   community helps with detection and mitigation of route leaks at ASes
   downstream from the leaking AS (in the path of the BGP update). This
   is an inter-AS (multi-hop) solution mechanism. This solution
   complements the intra-AS (local AS) route-leak avoidance solution
   that is described in ietf-idr-bgp-open-policy draft.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

   RFC 7908 [RFC7908] provides a definition of the route leak problem,
   and enumerates several types of route leaks. For this document, the
   definition that is applied is that a route leak occurs when a route
   received from a transit provider or a lateral peer is forwarded
   (against commonly used policy) to another transit provider or a
   lateral peer. The commonly used policy is that a route received from
   a transit provider or a lateral peer may be forwarded "down only" to
   customers.

   This document describes a solution for detection and mitigation route
   leaks which is based on conveying route-leak protection (RLP)
   information in a Border Gateway Protocol (BGP) community. The RLP
   information is carried in a new well-known transitive BGP community,
   called the RLP community. The RLP community helps with detection and
   mitigation of route leaks at ASes downstream from the leaking AS (in
   the path of the BGP update). This is an inter-AS (multi-hop)
   solution mechanism. This solution complements the intra-AS (local

AS) route-leak avoidance solution that is described in
[I-D.ietf-idr-bgp-open-policy].

Previously, an optional transitive BGP RLP Attribute was proposed to
carry the RLP information (in earlier versions of this document).
However, this updated document proposes a well-known transitive BGP
community to carry the RLP information, with the intention of
promoting faster adoption.

The inter-AS RLP mechanism described here can be incrementally
deployed. Early adopters would see significant benefits. If a group
of big ISPs deploy RLP, then they would be helping each other by
blocking route leaks originated within one's customer cone from
propagating into a peer's AS or their customer cone.

2. Mechanisms for Detection and Mitigation of Route Leaks

There are two considerations for route leaks: (1) Prevention of route
leaks from a local AS [I-D.ietf-idr-bgp-open-policy], and (2)
Detection and mitigation of route leaks in ASes that are downstream
from the leaking AS (in the path of BGP update). This document
specifies the latter.

2.1. Ascertaining Peering Relationship

There are four possible peering relationships (i.e., roles) an AS can
have with a neighbor AS: (1) Provider: transit-provider for all
prefixes exchanged, (2) Customer: customer for all prefixes
exchanged, (3) Lateral Peer: lateral peer (i.e., non-transit) for all
prefixes exchanged, and (4) Complex: different relationships for
different sets of prefixes [Luckie]. For the complex case, the
peering role types provider, customer, or lateral peer apply for
different non-overlapping sets of prefixes.

Operators rely on some form of out-of-band (OOB) (i.e., external to
BGP) communication to exchange information about their peering
relationship, AS number, interface IP address, etc. If the
relationship is complex, the OOB communication also includes the sets
of prefixes for which they have different roles.
[I-D.ietf-idr-bgp-open-policy] introduces a method of re-confirming
the BGP Role during BGP OPEN messaging (except when the role is
complex). It defines a new BGP Role capability, which helps in re-
confirming the relationship when it is provider, customer, or lateral
peer. BGP Role does not replace the OOB communication since it
relies on the OOB communication to set the role type in the BGP OPEN
message. However, BGP Role provides a means to double check, and if
there is a contradiction detected via the BGP Role messages, then a
Role Mismatch Notification is sent [I-D.ietf-idr-bgp-open-policy].

When the BGP relationship information has been correctly exchanged
including the sets of prefixes with different roles (if complex),
then this information SHOULD be used to automatically set the role
per-prefix with each peer. For example, if the local AS's role is
Provider with a neighbor AS, then the per-prefix role is set to
'Provider' for all prefixes sent to the neighbor, and set to
'Customer' for all prefixes received from the neighbor.

Once the per-prefix roles are set, this information is used in the
RLP solution mechanism that is described in this document.

2.2. Route-Leak Protection (RLP) Semantics

The key principle is that, in the event of a route leak, a receiving
router in a transit-provider AS (e.g., referring to Figure 1, ISP2
(AS2) router) should be able to detect from the RLP community in the
update message that its customer AS (e.g., AS3 in Figure 1) should
not have forwarded the update (towards the transit-provider AS).
Likewise when the update is received from a lateral peer. This means
that at least one of the ASes in the AS path of the update put RLP
information in RLP community to indicate that it sent the update to
its customer or lateral peer, but forbade any subsequent 'Up'
(customer to provider) or 'Lateral' (peer to peer) forwarding.

```
                                    /\              /\
                                     \ route-leak(P)/
                                      \ propagated /
                                       \          /
            +-----------+    peer     +-----------+
    _____| ISP1 (AS1) |----------->| ISP2 (AS2)|---------->
   /        -----------+  prefix(P)  +-----------+ route-leak(P)
  | prefix |            \   update        /\         \ propagated
  \  (P)  /              \              /    \         \
   -------    prefix(P)   \            /       \        \
              update  \    \          /          \       \
                       \    \        /route-leak(P)  \/
                        \/  /
              +---------------+
              | customer(AS3) |
              +---------------+
```
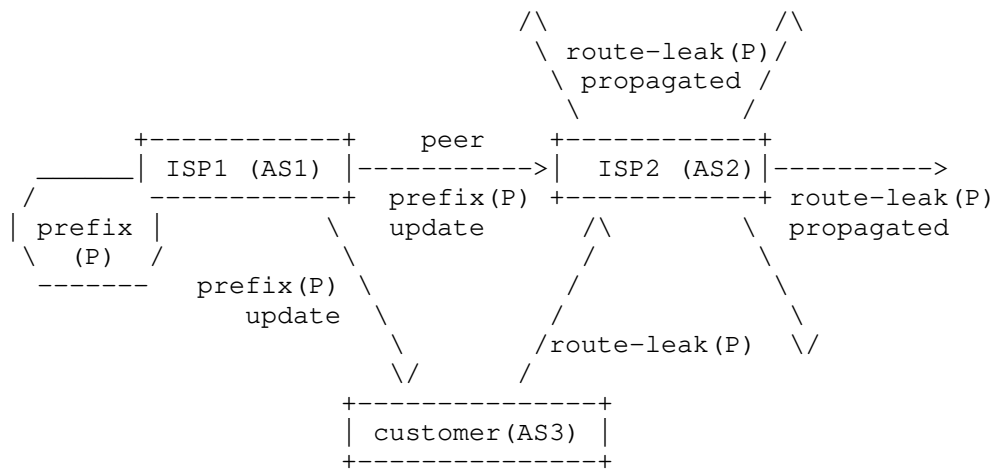
Figure 1: Illustration of the basic notion of a route leak.

The RLP information contained in the RLP community consists of one or
two AS numbers (ASNs) and has the following semantics:

1. Down Only (DO) indication: ASN of the most recent RLP-aware AS in
    the path to assert that it sent the update to a customer or
    lateral peer;

2. Leak detected (L) indication: ASN of the first RLP-aware AS in
    the path to assert that it forwarded the route from a customer or
    lateral peer despite detecting a leak (to avoid unreachability).

If the RLP community is present in an update, it will always contain
a single DO. However, L need not be always present. (Note: The bits
designated to carry L may be always present along with a DO, except
that a default value (all zeros) is carried in L when no AS in the
current AS path needed to assert L.) Once an AS asserts L (Leak
detected) by inserting its ASN value, it MUST not be changed
subsequently as the update propagates. But the ASN value in DO (Down
Only) is changeable along the AS path per its definition above.

Design assumption 1: Operators desire to avoid unreachability. So, a
design assumption here is that in the absence of an alternative
route, an AS may select and forward a route that is detected to be a
leak. (Note: This is the reason Leak detected (L) indication is part
of the design.)

Design assumption 2: An AS that is RLP-aware (i.e., implements the
RLP solution in this document) MUST also implement an intra-AS
solution for route leak avoidance in the local AS. The latter
solution uses an intra-AS signaling mechanism (see
[I-D.ietf-idr-bgp-open-policy], Section 3.7 of [RLP-Discussion]). By
doing this, the AS locally prevents the leaking of routes learned
from a transit provider or lateral peer to another transit provider
or lateral peer. Why this is critical to the overall solution is
made clear in slides 7 and 8 of [sriram2].

2.2.1. Format of the RLP Community

The format of the RLP community using a single Large Community is
shown in Figure 2.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Global Administrator  (IANA assigned for RLP)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             Local Data Part 1 = DO (ASN value)                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             Local Data Part 2 = L (ASN value)                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
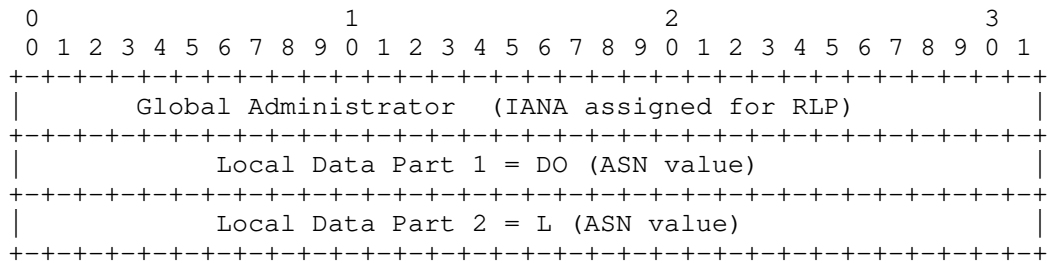
        Figure 2: Format of the RLP Community using a Large Community
                              [RFC8092].

2.3. Route Leak Detection Rules and the Ingress Router (Receiver)
      Actions

   A received BGP update is determined to be a route leak if:

   1. if L is present in the update;

   2. else (L is absent), the update is received from a customer and DO
       is present;

   3. else (L is absent), the update is received from a lateral peer
       and DO is present that is not the lateral peer's ASN.

   Note: Here by "L is present" we mean that its value is not the
   default value (all zeros) but is a proper ASN. Effectively "L is
   absent" if its value is the default value.

   In steps 2 and 3 above, the ingress router (receiver) MUST add L =
   local ANS. Doing this prior to the best path selection process is
   necessary. Also, if the route is selected as best path, then L is
   already set correctly before the egress router (sender) acts on it.

2.4. Route Selection Policy

   Minimum Default Policy: Whenever there is a choice between a customer
   route and a provider route that are both detected to be leaks (L is
   present), then lower the LocalPref to X (TBD by operator) for each of
   them. Then shortest path criterion would typically make the customer
   route preferred. (Note: This would help mitigate any possibility of
   persistent oscillation; see slide #7 in [sriram1].)

   Generalized Minimum Default Policy: Whenever there is a choice
   between multiple routes (customer/peer/provider) and each is detected
   to be a leak (L is present), then lower the LocalPref to X TBD by

operator) for each of them. Then apply shortest path criterion.
(Note: Some network operators may find this inadequate; see scenarios
#3 and #6 in slides #14 and #16, respectively, in [sriram2]. But
they may locally modify their policy while respecting the basic
principle.)

2.5. Egress Router (Sender) Actions

   After best path selection has been performed, a sender MUST perform
   the following RLP-related actions on the update to be propagated:

   1. When propagating a route originated by the local AS to a customer
       or lateral peer, add DO = local ASN;

   2. Else, when propagating a route that already includes a DO (i.e.,
       was received with a DO) to a customer or lateral peer, replace
       the DO value with the local ASN.

3. Pseudo Code

   [Begin: receiver action for route leak detection]

   {Comment: This precedes route selection policy.}

      if received route includes L, then save the route in RIB-in as is;

      else (L is absent), if route is received from a customer and DO is
      preset, then add L = local ASN;

      else (L is absent), if route is received from a lateral peer and
      DO is present that is not the lateral peer's ASN, then add L =
      local ASN

   {Comment: "Route does not include L" or "L is absent" only if L is
   either literally absent or has the default (all zeros) value.}

   [End: receiver action for route leak detection]

   [Begin: route selection policy]

      for each route that includes L, lower the LocalPref to X (TBD);
      apply best path selection policy*

   {*Comment: E.g., best path selection based on LocalPref first and
   then shortest path.}

   [End: route selection policy]

   [Begin: sender action]

   {Comment: RLP (includes DO and L or just DO) is a *transitive* BGP
   community and should propagate globally.}

      when propagating a route originated by local AS to a customer or
      lateral peer, add DO = local ASN;

      when propagating a route that includes a DO (i.e., was received
      with a DO) to a customer or lateral peer, replace the DO value
      with the local ASN;

   [End: sender action]

4. Security Considerations

   With the use of BGP community, there is often a concern that the
   community propagates beyond its intended perimeter and causes harm
   [streibelt]. However, that concern does not apply to the RLP
   community because it is a transitive community that must propagate as
   far as the update goes.

   The proposed Route-Leak Protection (RLP) information carried in the
   RLP community can benefit from cryptographic protection to prevent
   abuse by malicious actors in the AS path. In the future, if there is
   BGPsec deployment, the RLP information can be encoded in the Flags
   field in the Secure_Path Segment in BGPsec updates [RFC8205]. So,
   the cryptographic security mechanisms in BGPsec can also secure the
   RLP information. The reader is directed to the security
   considerations provided in [RFC8205].

5. IANA Considerations

   IANA is requested to register RLP in the well-known Large Community
   [RFC8092] registry (need help to clarify this). IANA is requested to
   allocate a new Global Administrator ID for the RLP community (Large
   Community) (see Figure 2 in this document). Note that BGP Path
   Attribute value for Large Community is 32 (IANA allocated) [RFC8092].

6. References

6.1. Normative References

   [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>.

6.2. Informative References

   [draft-dickson-sidr-route-leak-solns]
              Dickson, B., "Route Leaks -- Proposed Solutions", IETF
              Internet Draft (expired), March 2012,
              <https://tools.ietf.org/html/
              draft-dickson-sidr-route-leak-solns-01>.

   [I-D.ietf-idr-bgp-open-policy]
              Azimov, A., Bogomazov, E., Bush, R., Patel, K., and K.
              Sriram, "Route Leak Prevention using Roles in Update and
              Open messages", draft-ietf-idr-bgp-open-policy-05 (work in
              progress), February 2019.

   [Luckie]   Luckie, M., Huffaker, B., Dhamdhere, A., Giotsas, V., and
              kc. claffy, "AS Relationships, Customer Cones, and
              Validation", IMC 2013, October 2013,
              <http://www.caida.org/~amogh/papers/asrank-IMC13.pdf>.

   [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>.

   [RFC7454] Durand, J., Pepelnjak, I., and G. Doering, "BGP Operations
              and Security", BCP 194, RFC 7454, DOI 10.17487/RFC7454,
              February 2015, <https://www.rfc-editor.org/info/rfc7454>.

   [RFC7908] Sriram, K., Montgomery, D., McPherson, D., Osterweil, E.,
              and B. Dickson, "Problem Definition and Classification of
              BGP Route Leaks", RFC 7908, DOI 10.17487/RFC7908, June
              2016, <https://www.rfc-editor.org/info/rfc7908>.

   [RFC8092] Heitz, J., Ed., Snijders, J., Ed., Patel, K., Bagdonas,
              I., and N. Hilliard, "BGP Large Communities Attribute",
              RFC 8092, DOI 10.17487/RFC8092, February 2017,
              <https://www.rfc-editor.org/info/rfc8092>.

   [RFC8205] Lepinski, M., Ed. and K. Sriram, Ed., "BGPsec Protocol
              Specification", RFC 8205, DOI 10.17487/RFC8205, September
              2017, <https://www.rfc-editor.org/info/rfc8205>.

   [RLP-Discussion]
             Sriram (Ed.), K., "Design Discussion of Route Leaks
             Solution Methods", Work in Progress, draft-sriram-idr-
             route-leak-solution-discussion-00, July 2018,
             <https://tools.ietf.org/html/
             draft-sriram-idr-route-leak-solution-discussion-00>.

   [sriram1]   Sriram et al., K., "Route Leaks Solution Merger of RLP and
             eOTC Drafts", Presented at the IDR Working Group Meeting,
             IETF-102, Montreal, July 2018,
             <https://datatracker.ietf.org/meeting/102/materials/
             slides-102-idr-sessb-route-leaks-merged-solution-00>.

   [sriram2]   Sriram et al., K., "Solution for Route Leaks Using BGP
             Communities", Authors Team Discussion Slides, October
             2018, <https://www.nist.gov/sites/default/files/
             documents/2018/10/22/rlp_using_bgp_community-v4.pdf>.

   [streibelt]
             Streibelt et al., F., "BGP Communities: Even more Worms in
             the Routing Can", ACM IMC, October 2018,
             <https://archive.psg.com//181101.imc-communities.pdf>.

Acknowledgements

Contributors

   The following people made significant contributions to this document
   and should be considered co-authors:

Brian Dickson
Independent
Email: brian.peter.dickson@gmail.com

Doug Montgomery
USA National Institute of Standards and Technology
Email: dougm@nist.gov

Keyur Patel
Arrcus
Email: keyur@arrcus.com

Andrei Robachevsky
Internet Society
Email: robachevsky@isoc.org

Eugene Bogomazov
Qrator Labs
Email: eb@qrator.net

Randy Bush
Internet Initiative Japan
Email: randy@psg.com

Authors' Addresses

Kotikalapudi Sriram (editor)
USA National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899
United States of America

Email: ksriram@nist.gov

Alexander Azimov (editor)
Yandex
Moscow
Russia

Email: a.e.azimov@gmail.com