Methods for Detection and Mitigation of BGP Route Leaks

ietf-idr-route-leak-detection-mitigation-02
(Route leak definition: draft-ietf-grow-route-leak-problem-definition)

K. Sriram, D. Montgomery, B. Dickson, K. Patel, and A. Robachevsky

IDR Working Group Meeting, IETF-95
April 2016

Acknowledgements: The authors are grateful to many folks in various IETF WGs for commenting, critiquing, and offering very helpful suggestions (see acknowledgements section in the draft.)
Changes Since Last Presented

• Re-synced with the latest definition draft
• Simpler, clearer description of the route leak detection algorithm
• Section 5.1: discussion of upgrade and downgrade attack possibilities
  ➢ in the absence of BGPsec security protection for the RLP attribute
• Sections 5.1 through 5.4 offer updated design discussions and insights – based on WG comments, feedback
Route Leak Avoidance

• The proposal has built-in route-leak avoidance as well
• Will be explicitly described in the next revision
• Algorithm for route-leak avoidance:
  ➢ When incoming update has RLP field set to ‘01’ by any AS in the received AS path, then receiver SHOULD NOT propagate to a provider or peer

Note: For route-leak prevention marking, “SHOULD NOT propagate to a provider or peer” is better normative text than “CAN propagate only to customers”. Operator may choose to select and forward a marked update for reachability if there is no alternate route.
Why is per Prefix Marking Important

• Routes for prefixes with different business models are often sent over the same peering link

• Hence, sender-receiver relation does not always conform to P2C, C2P, P2P categories (estimate: about 35% of BGP peering links (see [Anwar]))

• But ISP has knowledge of its policy and hence knows the type of peering relationship on a per prefix basis

• If major ISPs mark routes for RLP, that would result in substantial success for RLP-based avoidance/detection/mitigation

[Anwar] "Investigating Interdomain Routing Policies in the Wild”
http://www.cs.usc.edu/assets/007/94928.pdf
Route Leak Protection (RLP) Attribute: Per Update

AS1

P1 originated by AS1

AS2

RLP=1

AS3

AS3 detects; prefers alternate path via AS5

AS5

Detected/Mitigated 😊

AS2 leaks it; leaves RLP intact
RLP Attribute: Per Update

P1 originated by AS1

AS1

RLP=1

AS2

AS3

AS5

RLP=0

Not Good 😞

AS2 leaks it and errs (faulty implementation/configuration)

AS3 accepts and propagates leaked route
Optional transitive RLP attribute structure - examples:
<AS4, RLP4> <AS3, RLP3> <AS2, RLP2> <AS1, RLP1> -- when all ASes upgraded
<AS4, RLP4> <AS3, RLP3> <AS1, RLP1> -- when AS2 is not upgraded
**RLP Attribute: Per Hop**

P1 originated by AS1

- **AS1**
  - Received from **AS2**
  - Sent to **AS3**

- **AS2**
  - Received from **P1**
  - Sent to **AS1**

- **AS3**
  - Detected/Mitigated 😊
  - Prefers alternate path

- **AS5**
  - Received from **AS3**
  - Sent to **P1**

**AS2 leaks it** and is not upgraded for RLP
Per Update vs. Per Hop -- Summary

- Partial deployment will exist for years ... having a per-hop RLP flag allows operator to evaluate better, e.g., if they would prefer well marked provider path over a questionable customer path.

- Per-hop RLP marking can be more easily secured in the future; E.g., by placing the marking bits in BGPsec Flags field which is per hop.