Detection and Mitigation of BGP Route Leaks

ietf-idr-route-leak-detection-mitigation-08
(Route leak definition: RFC 7908)

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

IDR Working Group Meeting, IETF-101
March 2018

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 in -08 compared to the -07 version

• The draft now focuses on the RLP solution which is inter-AS (multi-hop)
  ➢ Note: The intra-AS (local AS) solution with iOTC Attribute is provided in ietf-idr-bgp-open-policy draft
• The main body is now concise since several sections have moved into the Appendices
Changes in -08 compared to the -07 version

- The Appendices now contain:
  - Related prior-work review
  - Design rationale and discussion
    - Questions raised in IDR/GROW and the discussions captured here
  - Stopgap solution
  - Intra-AS route leak prevention with Community (includes inputs from NANOG list)
Route Leak: The Tale of Two Culprits

- Intra-AS and Inter-AS solutions are necessary.
Hathway / Airtel Route Leaks of Google Prefixes
March 12, 2015

Incident analysis: http://research.dyn.com/2015/03/routing-leak-briefly-takes-google/
Route Leak Protection (RLP) Field Encoding by Sending Router

- RLP is a 2-bit field set by each AS along the path
- Can be carried as a transitive per hop attribute in BGP or in the existing Flags field in BGPsec
- The RLP field value MUST be set to one of two values as follows:
  - 00: Default value (i.e. "nothing specified")
  - 01: 'Do not Propagate Up or Lateral' indication
    - Sender indicates that the route SHOULD NOT be subsequently forwarded Up towards a transit-provider or to a lateral (non-transit) peer
Inter-AS Solution – RLP Attribute

RLP = <AS1, 1>
AS2 leaks it

P1 originated by AS1

RLP = <AS1, 1>
AS3 detects leak; prefers alternate path

Route Leak Detected/
Mitigated 😊
Format of RLP Attribute

Optional Transitive Attribute

<table>
<thead>
<tr>
<th>ASN: 2</th>
<th>RLP: 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASN: 1</td>
<td>RLP: 1</td>
</tr>
</tbody>
</table>

Most Recently Added

Least Recently Added
Effectiveness of the Proposed Solution

Percentage of Route Leaks NOT DETECTED

- **99% accidental**
- **0% Not Detected** (i.e. All Route Leaks Detected)
- **1% malicious**

**Current BGP**

**BGP with Proposed RLP**

**BGPSEC with Proposed RLP**

- **Accidental**
- **Malicious**
## Building Blocks

<table>
<thead>
<tr>
<th>Security: Include RLP in BGPsec Flags field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intra-AS route leak prevention (iBGP messaging)</td>
</tr>
<tr>
<td>• iOTC Attribute</td>
</tr>
<tr>
<td>Inter-AS route leak detection/mitigation</td>
</tr>
<tr>
<td>• Optional transitive RLP attribute</td>
</tr>
</tbody>
</table>

### Set peering relation for each peer (per prefix)

- BGP OPEN / BGP Role Capability negotiations – re-confirming the role stated in OOB communication
- OOB communication between operators: Peering relation, ASN, interface IP

---

*idr-bgp-open-policy*
No Single Point of Failure & Large ISPs’ Ring of Security

More robust in partial deployment (AS7, AS8, AS9 not upgraded)

Major ISP
Small ISP or Customer
Not upgraded

RLP(AS5) = 1
RLP(AS1) = 1

AS1
AS2
AS3
AS4
AS5
AS7
AS8
AS9
AS15

Leak
Leak
Leak
Customer cone
Customer cone
Customer cone

More robust in partial deployment
(AS7, AS8, AS9 not upgraded)