Secure Extension of BGP by Decoupling Path Propagation and Adoption

draft-zhang-idr-decoupling-01
draft-zhang-idr-decoupling-02

Mingui Zhang
mingui@huawei.com
False Routing Announcements

• Interrupt the Internet service

• Source
  – Malicious attack
  – Mis-configuration

• Attacker can do
  – Black holing
  – Interception
Solutions

• Prevention
  – based on RPKI (used by SIDR), act before attacks
  – however, not widely deployed

• Detection
  – monitoring & reaction, act after attacks

• Mitigation
  – filtering on routers’ own knowledge, act during attacks
DBGP: Decoupling path propagation and adoption in BGP

- (B X) is suspected and propagated in DAS_PATH attribute.
  - A DAS_PATH will only used for informational purpose rather than real data delivery!

- If (B X) is actually legitimate, the propagation in fact enable parallel validation.
  - When B propagate it to A as legitimate path later, A MAY have already finished the validation (e.g., checked by operators) in advance and can accept it directly without suspicion.
Optional & Transit DAS_PATH

```
+-----------------+
<table>
<thead>
<tr>
<th>Attribute Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2 bytes)</td>
</tr>
</tbody>
</table>
+-----------------+
| Attribute Length|
| (1 or 2 bytes)  |
+-----------------+
| Attribute Value  |
| (variable length)|
+-----------------+
```

<table>
<thead>
<tr>
<th>Value</th>
<th>Segment</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DAS_SET</td>
<td>unordered set of ASs a route in the UPDATE message has traversed</td>
</tr>
<tr>
<td>2</td>
<td>DAS_SEQUENCE</td>
<td>ordered set of ASs a route in the UPDATE message has traversed</td>
</tr>
</tbody>
</table>

• Similar with AS_PATH attribute
Comments

- Cooperate with prevention schemes
- Operational complexity
- Add multiple DAS_PATHs option
- Detection facilitation
- Maintain separate trust-info history database
1. Cooperate with Prevention

- If we have SIDR solutions deployed on BGP routers, there are no false routing announcements at all.
  - ISP has no strong incentive to deploy RPKI
  - We need a multiple-line defense against attack
    - prevention, detection, mitigation

- Not chartered by SIDR
  - Work together with IDR
  - For the ultimate goal: to Secure IDR
  - Things can change, re-charter to include?
2. Operational Complexity

• The additional complexity of the BGP implementations in the regular production routers is something that is really unwanted from operators.
  – An optional attribute, ignored when received
  – Complexity similar to the “add-paths” solution
    • draft-ietf-idr-add-paths-04.txt
3. Separate History Database

- Mitigation solutions need additional memory for a separate historical database. For example, PGBGP routers store trusted origins in their databases.
  - By default, DBGP only uses Adj-RIBs-In
    - Save memory & maintenance effort
4. Detection Facilitation

• What do the detection systems do when they receive DAS_PATHs.
  – DBGP doesn’t block the view of monitors of detection systems (the traditional mitigation does).
  – Detection systems had already been deployed. They can examine DAS_PATHs and send notifications to the victim AS (e.g., send email).
5. Multiple DAS_PATHs Export

• How about including multiple DAS_PATHs in one UPDATE message?
  – Multiple DAS_PATHs export is enabled now.

• Different from add-path WG draft
  – All the paths in “add-path” are available
  – All the paths in DAS_PATHs are unavailable
Thanks!