BGP security at internet exchanges
A practical experiment

Marco d’Itri
<md@seeweb.it>
@rfc1036

Seeweb s.r.l.

RIPE71 - Nov 16, 2015
Goal

Find out which networks accept anything that a peer will announce to them.

In a better world this would never happen, but reality is different...
Methodology

- Borrow from an accomplice an unused /24 part of one of their networks.
- Get from a BGP dump a list of the networks announced by your peers at multiple IXes.
- Scan each neighbor AS for a pingable IP, one random /29 at a time (this is the hard part!).
- Announce the hijacked borrowed network.
- Ping again the test IPs, this time from an IP from the borrowed network.
- See which ones are still reachable.
Technical details

- Configure quagga with an iBGP session to your routers and make it receive the relevant prefixes.
- Dump all the routes (`dump bgp routes-mrt ...`).
- Extract the relevant ones with my `zebra-dump-parser.pl`.
- Find a pingable IP in each AS with nmap and some Perl.
  (Also, exclude dynamically-assigned addresses which could go away at any time.)
- Configure on the system an IP from the /24 and announce it (only to neighbors, one IX at a time).
- More Perl to ping the target IPs and analyze the results.
Results

How many neighbors will happily accept an hijacked route?

<table>
<thead>
<tr>
<th>IX</th>
<th>total peers</th>
<th>vulnerable</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIX</td>
<td>109</td>
<td>59</td>
</tr>
<tr>
<td>NAMEX</td>
<td>18</td>
<td>6</td>
</tr>
<tr>
<td>TOP-IX</td>
<td>18</td>
<td>13</td>
</tr>
<tr>
<td>AMS-IX</td>
<td>462</td>
<td>441</td>
</tr>
<tr>
<td>DE-CIX</td>
<td>328</td>
<td>72</td>
</tr>
<tr>
<td>LINX</td>
<td>324</td>
<td>239</td>
</tr>
<tr>
<td>France-IX</td>
<td>110</td>
<td>101</td>
</tr>
</tbody>
</table>

This is inexcusable

We announce less than 50 routes, all of them properly registered in the RIPE IRR: our session can be easily validated automatically.

This confirms the need to raise awareness about routing security and the Routing Resilience Manifesto.
Questions?


(Google ... Marco d’Itri ... I feel lucky)
Thanks to...

- Paolo Agazzone at Intercom AS8224 for the /24.
- Gianfranco Delli Carri at ITGate AS12637 for the LINX, DE-CIX and France-IX testbed.