BGP security at internet exchanges

A practical experiment

Marco d'Itri
<md@linux.it>
@rfc1036

End Summer Camp 2K15 - Sep 5, 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.
- 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?

IX	total peers	vulnerable
MIX	109	59
NAMEX	18	6
AMS-IX	449	(...)

This is inexcusable

We announce 31 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?

`http://www.linux.it/~md/text/bgp-experiment-esc2k15.pdf`

(Google . . . Marco d'Itri . . . I feel lucky)