IRR for DNS Anycast ops

Rubens Kühl, TC IRR

What is a routing presentation doing in a DNS Forum ?

Answer: Anycast DNS

Same IP addresses at multiple locations

BGP announcements of the same IP block across multiple regions

DFZ (Default Free Zone) routing used to be done on trust, but malicious and non-malicious incidents changed that

And then…

Internet Society

27 April 2018

What Happened? The Amazon Route 53 BGP Hijack to Take Over Ethereum Cryptocurrency Wallets

By Aftab Siddiqui

Senior Manager, Internet Technology - Asia-Pacific

“I thought RPKI solved all that”

RPKI is decades away from network operators being able to deny all unknown routes

Current RPKI deployment is focused on origin hijack, but path hijack can also be used (ASPA plus BGPsec might come to the rescue)

NIST RPKI stats: 53% valid, 1% invalid, 46% unknown

APNIC RPKI stats: 21% worldwide filtering, 72% in USA

And to complicate things further…

RPKI TALs require DNS

`https://rrdp.lacnic.net/ta/rta-lacnic-rpki.cer`

`rsync://repository.lacnic.net/rpki/lacnic/rta-lacnic-rpki.cer`

RPKI repositories of ROAs and manifests require DNS

https://rpki-repo.registro.br/

`rsync://rpki-repo.registro.br/`

Preventing hijack is not all there is

DNS Anycast operators frequently suffer from asymmetric routing in the DFZ

For instance, if an anycast node at an IX gets a packet from an address source it has no route to send answers back to

So increasing acceptance of announced prefixes has both operational and security benefits

Route Registries

IRR has been used since circa 2000 to declare routing policies

While it started with non-authoritative registries, like RADB, the RIR system started providing authoritative registries (eventually phasing out their non-auth databases)

Using IRR

(at least to show off your acronym skills)

First option: RIR IRR configuration

Pros:

Already included in your RIR membership

Trusted by more network operators

Cons:

If you have number resources from multiple regions, you have multiple sources of truth to configure

Second option: Non-auth registry

Pros:

Single point of configuration for global resources

Specialized support (in case of paid options)

Merit's RADB is the most known option (https://www.radb.net)

Cons:

Cost (if paying)

Best effort support (if not paying)

Less trusted than RIR IRR's

Latin America

LACNIC provides hosted-RPKI support for number resources from the region, except for Brazil

LACNIC's hosted-RPKI includes a feature-capped IRR solution

TC IRR provides IRR services for the Brazilian IP address space

Free, but comes with best-effort support

Originally thought to also provide services for LAC region, but phased out support when LACNIC made it available

TC IRR x RADB

TC

Not operated by an IP address authority

Ties control to WHOIS/RDAP contacts

Free, voluntary support

Custom scripts to restrict resources to its specific owners (sign-up wizard, mirrorkill and daily clean)

Trusted by some tools as authoritative

RADB

Not operated by an IP address authority

Does not restrict who can add or manage resources

Paid with support

Routing survivability cookbok

IRR, RPKI, Peering DB: use them all

Sign your IP address blocks with RPKI

Consider if you are able to have ASPA in your RPKI configuration

May be a challenge for multi-region operations due to mix of hosted and delegated RPKI across the globe

Create your route, route6, aut-num route set and as-set objects in your chosen IRR (https://irr.net)

Create your PeeringDB entry, if you don’t have one

Update your PeeringDB listing with IRR as-set

One ring to rule them all

https://manrs.org

MANRS

Show of hands… or humming

( ) My IP resources are listed in IRR

( ) My IRR AS-SET or RS-SET is listed in PeeringDB

( ) My IP resources are signed with RPKI

( ) My IP resources are signed with RPKI and also feature ASPA

For the “not’s”: why not ? What could change that to yes ?

Thanks!

Contact us:

TC IRR
https://bgp.net.br

db-admin@bgp.net.br