Trends in RPKI deployment

LACNIC 33
• Non-profit foundation: Open Source, Open Standards, Open Internet

• Specialised in DNS & Routing: Security, Stability, Privacy

• DNS: NSD, Unbound, OpenDNSSEC

• RPKI: Routinator, Krill, Analytics
RPKI is Coming of Age
A Longitudinal Study of RPKI Deployment and Invalid Route Origins

• Paper at Internet Measurement Conference 2019
• Using routing information from various sources:
  - RIPE RIS
  - Routeviews
  - Akamai
• Historic information on RPKI repositories:
  https://ftp.ripe.net/rpki/
• Read more: https://dl.acm.org/authorize?N695009
ROA Uptake and Accuracy Maps

- Routing information from Routeviews

- Historic information on RPKI repositories: https://ftp.ripe.net/rpki/

- Historic information RIR assignments to regions: https://www.nro.net/about/rirs/statistics/
Coverage April 2018
BORDER GATEWAY PROTOCOL ATTACK —

Suspicious event hijacks Amazon traffic for 2 hours, steals cryptocurrency

Almost 1,300 addresses for Amazon Route 53 rerouted for two hours.

DAN GOODIN  -  4/24/2018, 9:00 PM

Amazon lost control of a small number of its cloud services IP addresses for two hours on Tuesday morning when hackers exploited a known Internet-protocol weakness that let them to redirect traffic to rogue destinations. By subverting Amazon's domain-resolution service, the attackers masqueraded as cryptocurrency website MyEtherWallet.com and stole about $150,000 in digital coins from unwitting end users. They may have targeted other Amazon customers as well.

Traffic for Google, Apple, Facebook, Microsoft and other tech giants routed through Russia, experts believe it was an intentional BGP Hijacking.

Last week a suspicious event routed traffic for major tech companies (i.e. Google, Facebook, Apple, and Microsoft) through a previously unknown Russian Internet provider. The event occurred on Wednesday, researchers who investigated it believe the traffic was intentionally hijacked.

The incident involved the Internet's Border Gateway Protocol that is used to route traffic among Internet backbones, ISPs, and other large networks.

BGPmon.net
@bgpmon
Example of a @facebook prefix briefly routed towards AS9523 DL-LINK-ASbgpmon.net/popular-destin...

bgpstream@bgpstream
BGP Hijacked prefix AS32034 31.13.84.0/24, Facebook, Inc., By AS9523 DL-LINK-AS, bgpstream.com/event/119897

By Declan McCullagh
Updated: February 25, 2008 4:28 PM PST

How Pakistan knocked YouTube offline (and how to make sure it never happens again)

YouTube becoming unreachable isn't the first time that Internet addresses were hijacked. But if it spurs interest in better security, it may be the last.
Use of ROAs in routing decisions

• Before mid 2018 there were early adopters:
  • Colombia was very active, as were others in Latin America
  • Small networks in Europe, especially the Netherlands

• The route53 leak was a pivotal moment
  • enough is enough
ASNs dropping invalids

- Ben Cox did active probing measurements:
  - September 2018: 50 ASNs
  - September 2019: 616 ASNs

  https://www.youtube.com/watch?v=fn9xrCoRYLQ

- Many public announcements, including tier-1

Very cool, @ctestart regenerated the graph with the latest data. You can sort of recognise in the jumps what different networks at different times meant for the global routing system. Read as: "arrow points to deployment timestamp, and the graph's subsequent direction is impact."

https://twitter.com/JobSnijders/status/1256326712347881473
Accuracy April 2020

2020-04-28

[Map of the world showing accuracy]
Accuracy 90-100% Trend

Accuracy below 90% is shown as white!

https://nlnetlabs.nl/static/rpki_maps/accuracy-90-latam.mp4
https://nlnetlabs.nl/static/rpki_maps/accuracy-90-world.mp4
Coverage Trend

Coverage keeps increasing

https://nlnetlabs.nl/static/rpki_maps/coverage-latam.mp4
https://nlnetlabs.nl/static/rpki_maps/coverage-world.mp4
ASNs dropping invalids

• General advice: Monitor before dropping

• Train your help desk if you start dropping!
  ➔ Educate your customers and peers
  ➔ Put in temporary exceptions

• Very strong incentive to keep ROAs up to date!

• Coverage keeps rising
Delegated RPKI CAs under NIC.BR

- nic.br does not have a hosted service (yet), users run their own CA
- nic.br provides a publication service
Delegated RPKI CAs under RIRs

➡️ RIRs also have the option to run your delegated CAs
➡️ APNIC has a repository service, other RIRs not yet
• RPKID by Dragon Research Labs
• In use at several NIRs and some delegated CAs
Bienvenido a Krill

Empecemos por crear su Autoridad de Certificación (CA) RPKI. Esta se usará para configurar el RPKI Delegado con una o múltiples CA padre, generalmente su Registro Regional o Nacional de Internet.

El identificador que escoja identificará a su CA en sus interacciones con las CA padres e hijos. No se publicará en el RPKI. Escoja un identificador que ayude a los demás a reconocer a su organización. Una vez guardado, el identificador no se puede cambiar. Más información...

* CA Handle

Creo CA

This is not a valid CA name

NLnet Labs, funded by nic.br, ripe ncc & ncsc
Why Run a Delegated CA?

✓ Run a single CA under multiple RIRs
✓ Delegate space to others (customers, teams)
✓ Use API to integrate with routing work flow (ipam)
✓ Local control of who can access, rather than web portal

- Hardware requirements are low, but needs to be maintained
- Need to host an RPKI repository (unless under nic.br)
Running Krill

• Build it yourself:  

• Docker:  

• Looking at Krill packages (debian, FreeBSD, others)

• Use 'krillmanager'
  • Digital Ocean Marketplace: https://youtu.be/qunvH2t6rqU
  • AWS coming
  • Looking at generic (own infrastructure) support
Some Statistics

• NIC.BR
  - December 2019: Launch of service
  - May 1 2020:
    - 113 Delegations to members
    - 523 Prefixes in ROAs
    - Coverage 2.7%
    - Accuracy 99.1%

• RIRs
  - May 2020: ARIN 3, RIPE 3, APNIC 2
Issues Found

• Publishing to 'localhost'
  • Fixed in Krill 0.5.0 (February 2020)

• Some operators stop their CA
  • Their repository goes stale, then expires
  • NIC.BR is monitoring
Conclusions

• Delegated CAs are seeing uptake:
  • nic.br members do not have a portal
  • early adopters in other regions

• Some initial issues, getting fixed

• Good uptake and data quality

• Managed repositories needed!
Questions?

ℹ️  https://rpki.nl

✉️  tim@nlnetlabs.nl

✉️  rpki-team@nlnetlabs.nl

✉️  rpki@lists.nlnetlabs.nl

🔗  https://github.com/nlnetlabs/routinator

🔗  https://github.com/nlnetlabs/krill