RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Recent developments in RPKI

Mikhail Puzanov | 30 March 2023 | INEX

What is RPKI

- Public key infrastructure for route origin validation (ROV)
- Certification Authority hierarchy with
  - 5 RIR trust anchors
  - 2 AS0 trust anchors from APNIC and LACNIC
- Signed objects with different payloads
  - ROA with VRP (used for ROV)
  - ASPA with VAP (in development)
- Currently only ROAs are of active practical use

Statistics

- RPKI covers about 37% of IPv4 and 32% of IPv6
  - https://ftp.ripe.net/pub/stats/ripencc/nro-adoption/latest
- About 2800 installations of RPKI validators in the world
- About 2300 unique /24 or /48 running RPKI validators
- Still steady growth of adoption and number of ROAs
  - https://certification-stats.ripe.net/

Statistics

20,000
15,000
10,000
5,000
0
Certificates
Apr 01, 2011
Apr 01, 2012
Apr 01, 2013
Apr 01, 2014
Apr 01, 2015
Apr 01, 2016
Apr 01, 2017
Apr 01, 2018
Apr 01, 2019
Apr 01, 2020
Apr 01, 2021
Apr 01, 2022
Date
Trust Anchor
APNIC
ARIN
AfriNIC
LACNIC
RIPE NCC

RPKI validators are mature

- Much better than 5 years ago
- Installation, configuration, documentation is way better
- Big research work on vulnerabilities in 2021
  - https://arxiv.org/pdf/2203.00993.pdf
  - Multiple fixes in all validators
  - Mostly addressing potential DoS attacks

RPKI validators are mature

- Risk of monoculture, so run different ones
  - https://rov-measurements.nlnetlabs.net/stats/
  - Routinator - 80%
  - rpki-client - 8%
  - OctoRPKI - 6%
  - Fort - 3%
  - RIPE NCC RPKI Validator 3 - 3% **[STOP USING IT IF YOU STILL DO]**

Trendy: Publication as a service

- There are two flavours of RPKI
  - **Hosted**: RIR maintains key pairs and objects and publishes them for you
  - **Delegated**: you maintains key pairs objects and publish them in your repository
- Publication as a service is an in-between flavour
  - You maintain key pairs and objects and send them to RIR
  - RIR publishes your objects in its repository
- Supported by APNIC, ARIN, RIPE NCC, NIRs
  - AKA “Publication in parent” or “Hybrid RPKI”

Trendy: Publication as a service

- Win-Win for smaller delegated CAs
- Availability numbers are way better for RIR repositories
- RIRs have vast experience with maintaining consistency
  - Well documented and easy to set up
- Fun fact: even then you don’t need 100% availability
  - ARIN did a test with simulated outage of ~60 minutes
  - Validators cache everything anyway
  - RFC 9286 aligns validators’ behaviour in such cases
  - Objects do not expire for hours

What’s coming: ASPA

- Autonomous System Provider Authorisation
  - a draft, about to become an RFC
- Validation of AS_PATH
- Already supported in a couple of validators out there
- Supported by RIPE NCC’s API in pilot environment
  - Planned support in portal UI
- RPKI-to-Router support — RFC 8210bis, final draft
- Support in OpenBGPD and NIST BGP-SRx

What’s coming: One ROA per prefix

- RFC (draft) prescribing to generate one ROA per prefix
  - Mainly for preventing issues for delegated CAs when resources change
- Will likely result in changes in some CA software
- No changes in validators necessary
- Performance impact up to ~3 times more ROAs overall
  - More CPU, more storage, probably more memory
  - Some validator installations might start running out of resources

Others features

- BGPSec certificates are usable
  - Usable in PaaS or self-hosted
- RSC (RPKI Signed Checklists)
  - Usable in PaaS or self-hosted

Conclusion

- RPKI has become a mature ecosystem
- ROV + ASPA prevents large fraction of hijacks and route leaks
- RPKI deployment effort is not that big
- Go for it if you still did not

Questions ?

rpki@ripe.net
mpuzanov@ripe.net