RIPE RPKI Open House

Routing Security, whats next?

Massimiliano Stucchi & Melchior Aelmans
20 January, 2021

Agenda

- RPKI Origin Validation
  - Current state of affairs
  - What RPKI ROV doesn’t help with
    - BGPsec
- What’s next on the plate?
  - AS-Cones
  - ASPA
  - RTA
- Call to action
  - Implement BCPs and ROV
  - MANRS

RPKI OV - Current State of affairs

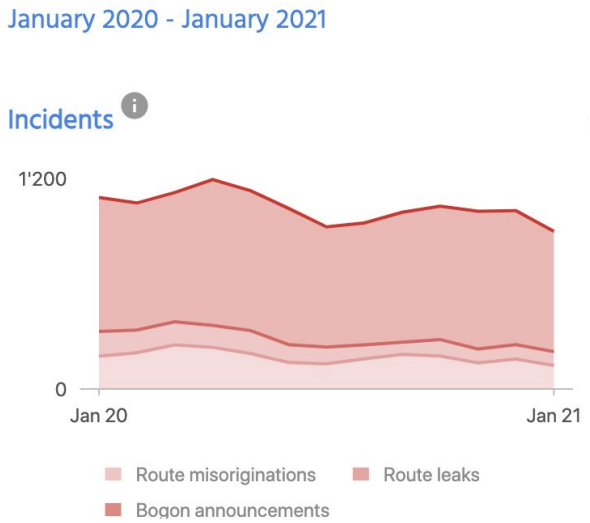
RPKI OV - Current State of affairs

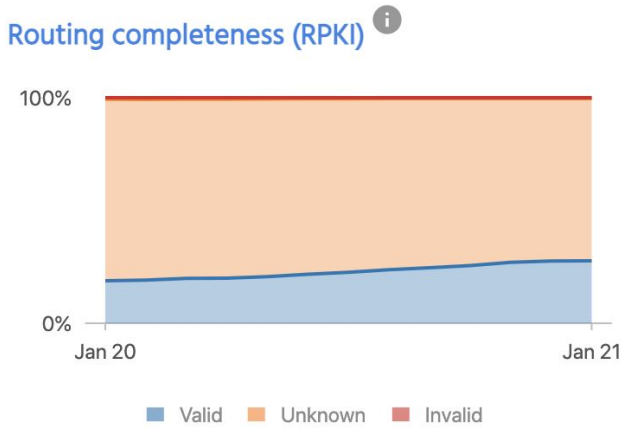
Adoption increasing. Large network operators are deploying;

- Google: https://cloud.google.com/blog/products/networking/how-google-is-working-to-improve-internet-routing-security
- Amazon: https://aws.amazon.com/blogs/networking-and-content-delivery/how-aws-is-helping-to-secure-internet-routing/
- Microsoft: https://azure.microsoft.com/en-us/blog/microsoft-introduces-steps-to-improve-internet-routing-security/

RPKI OV - Current State of affairs

Number of incidents slowly decreasing. Number of valid ROAs increasing.





Source: https://observatory.manrs.org/

What RPKI ROV doesn’t help with

What RPKI ROV doesn’t help with

- Path validation is still a problem **not** solved by RPKI OV.

- Work is ongoing in IETF

BGPSec

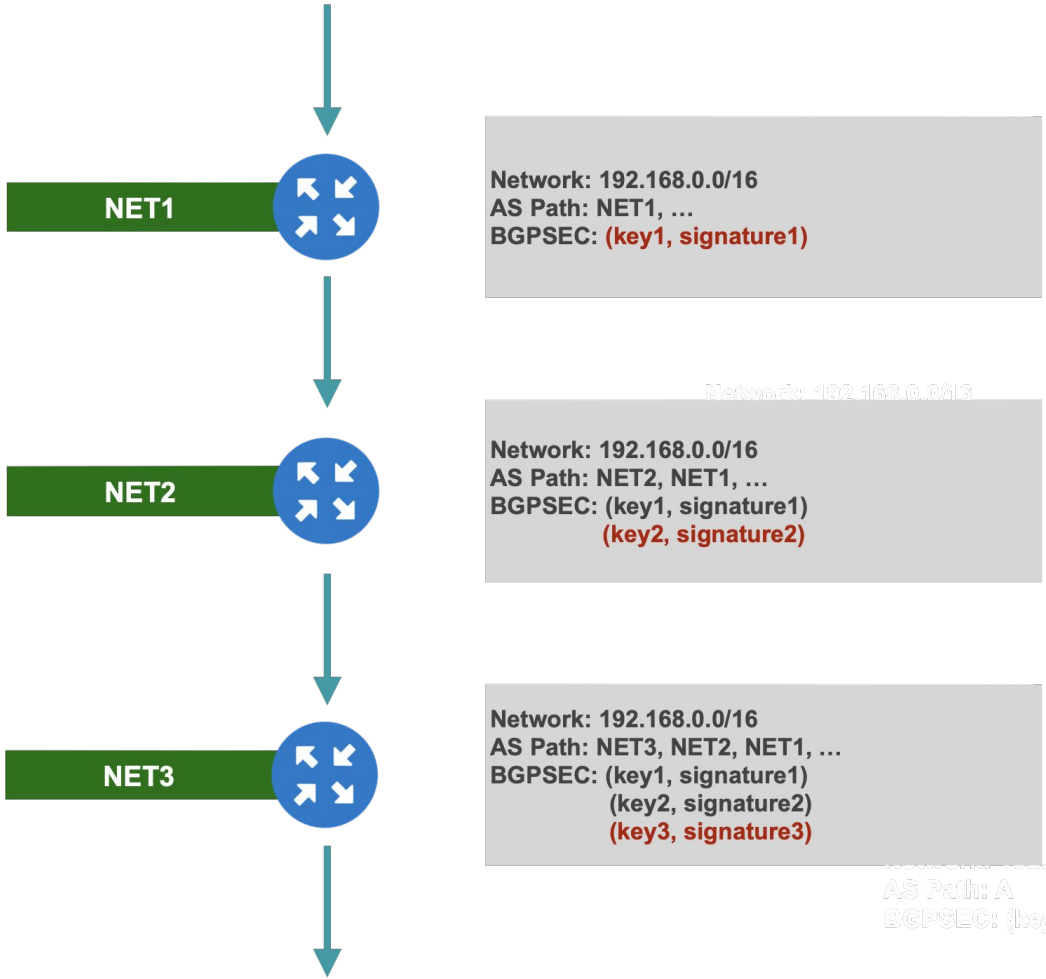
- RPKI does not protect against path redirection attacks

- We need a way to verify the AS-Path of a given BGP Announcement
  - And understand if anyone tampered with the data on the way to our routers

BGPSec Path Validation

- With BGPSec, the AS-Path attribute is cryptographically signed
  - Using the operator’s certificate from RPKI

- In order to validate an AS-Path, routers verify the chain of trust of all the signatures of the AS-Path


NET1
NET2
NET3
Network: 192.168.0.0/16
AS Path: NET1, …
BGPSEC: (key1, signature1)
Network: 192.168.0.0/16
AS Path: NET2, NET1, …
BGPSEC: (key1, signature1)
(key2, signature2)
Network: 192.168.0.0/16
AS Path: NET3, NET2, NET1, …
BGPSEC: (key1, signature1)
(key2, signature2)
(key3, signature3)

However BGPsec isn’t deployed?

- That is mainly due to the amount of computational power needed on the routers’ control plane

- Potentially (rough estimate) you could validate around 4k paths (depends on the length) so how to handle ‘the rest’?

- BGPsec isn’t the solution as it doesn’t scale.

What’s new and upcoming

AS-Cones, ASPA, RTA

AS-Cones

- IETF Draft
  - https://datatracker.ietf.org/doc/draft-ss-grow-rpki-as-cones/

- Goals
  - Create more feature parity between IRR and RPKI
  - Make provisioning operations easier
  - Go global, independent from IRR
  - In second instance, try to provide lightweight AS-Path verification

Features of AS-Cones

- Granularity of declarations
- Default namespace
- Simple validation process
- Stub networks don’t need to do anything

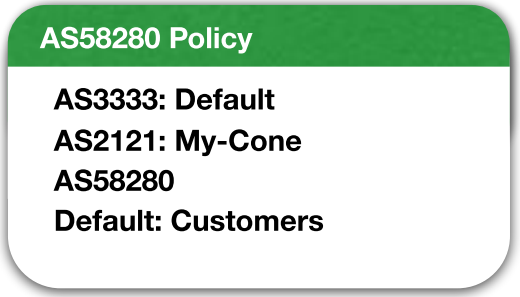
Two objects

A policy definition; and

The AS-Cone

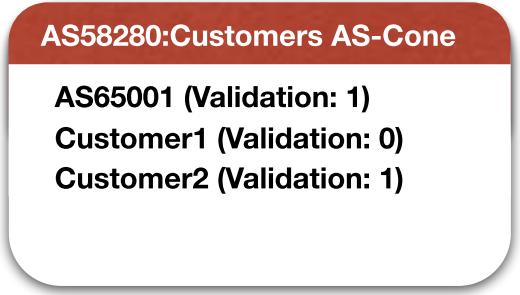
Policy Object

- Must contain a “Default” policy
  - Which, by default, contains only the ASN



- Every relationship can point to an AS-Cone or

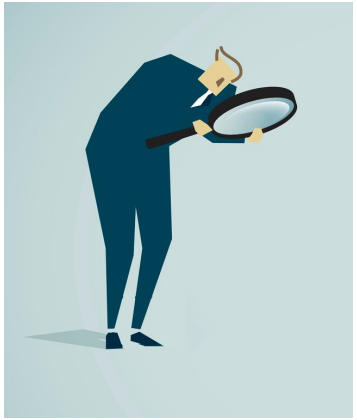
AS-Cone Object



- Contains a list of ASNs or AS-Cones from customer networks
- AS Cones referenced as ASXXXX:Cone_name
  - Name must be unique only per ASN
- The inclusion of an entry can be validated by the holder of the resource (ASN or AS-Cone)

Finding Policies and AS-Cones

- Policies and AS-Cones should be distributed by your favourite Validator
- To generate prefix filters, access the validated cache via an API



Generating Prefix Filters with AS-Cones

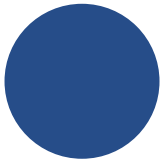
- As an upstream, read the policy definition for your customer network.
  - Check if it contains a specific policy declaration, otherwise Default
- Take the AS-Cone referenced
- Walk the AS-Cone, create a list of all the ASN included
  - If you find circular AS-Cones declaration, discard them
- Verify the status of the “validated” field
- For every ASN, pick all the ROAs where it’s listed as originator

Security model

- Adding an AS-Cone to another AS-Cone **requires** acknowledgement
  - Avoids anyone adding, for example, large networks in their customer cone
- Adding an ASN to an AS-Cone has an **optional** acknowledgement
- The acknowledgement is registered in the AS-Cone as a boolean value in the “Validated” field for each entry

Building prefix filters

Loose



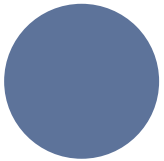
Get any ASN and any AS-Cone in the AS-Cone indicated by your downstream

Opportunistic

Get any ASN and any AS-Cone.

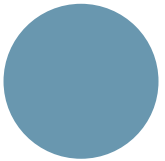
For the ASNs, only consider those where the “Validated” field is set to 1

Almost-strict



Remove any sub-trees where any one single entry is not validated

Strict



Only consider the AS-Cone if **every** entry has been validated

References

- Material on Github
  - https://github.com/bgp/draft-ss-grow-rpki-as-cones

- Discussion welcome in the Grow IETF WG

ASPA

- Additional object in RPKI to define upstreams for a defined ASN
- Provides infrastructure to do lightweight path validation
- Still in draft state
  - https://datatracker.ietf.org/doc/draft-ietf-sidrops-aspa-profile/

RTA

- Resource Tagged Attestations
- General-purpose system to sign objects in RPKI
- Allows more data and information to be put into RPKI
- https://datatracker.ietf.org/doc/draft-michaelson-rpki-rta/

What can you do ?

Call to Action

- **Implement routing BCPs, RPKI OV and MANRS**

- **See for tips and tricks:**
  http://bgpfilterguide.nlnog.net/
  https://rpki.readthedocs.io/

- **Support MANRS:**
  https://www.manrs.org/

MANRS For Network Operators

Filtering

Prevent propagation of incorrect routing information

Ensure the correctness of your own announcements and announcements from your customers to adjacent networks with prefix and AS-path granularity

Anti-spoofing

Prevent traffic with spoofed source IP addresses

Enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure

Coordination

Facilitate global operational communication and coordination between network operators

Maintain globally accessible, up-to-date contact information in common routing databases

Global Validation

Facilitate validation of routing information on a global scale

Publish your data so others can validate

MANRS for IXPs

Action 1
Prevent propagation of incorrect routing information

Implement filtering of route announcements at the Route Server based on routing information data (IRR and/or RPKI).

Action 2
Promote MANRS to the IXP membership

Provide encouragement or assistance for IXP members to implement MANRS actions.

Action 3
Protect the peering platform

Have a published policy of traffic not allowed on the peering fabric and perform filtering of such traffic.

Action 4
Facilitate global operational communication and coordination

Facilitate communication among members by providing necessary mailing lists and member directories.

Action 5
Provide monitoring and debugging tools to the members.

Provide a looking glass for IXP members.

MANRS for CDNs and Cloud Providers

Action 1
Prevent propagation of incorrect routing information

Ensure correctness of own announcements and of their peers (non-transit) by implementing explicit (whitelist) filtering with prefix granularity.

Action 2
Prevent traffic with illegitimate source IP addresses

Implement anti-spoofing controls to prevent packets with illegitimate source IP address from leaving the network (egress filters).

Action 3
Facilitate global operational communication and coordination

Maintain globally accessible, up-to-date contact information in PeeringDB and relevant RIR databases.

Action 4
Facilitate validation of routing information on a global scale

Publicly document ASNs and prefixes that are intended to be advertised to external parties (IRR and/or RPKI)

Action 5
Encourage MANRS adoption

Actively encourage MANRS adoption among the peers.

Action 6
Provide monitoring and debugging tools to the peering partners

Provide a mechanism to inform peering partners if announcements did not meet the requirements of the peering policy.

MANRS For Vendors ?

Increased MANRS support. Vendors next?

- Operators, IXPs and CDN/Cloud providers are on board
- Next up are vendors.
  - Initial brainstorm call last week
  - Juniper publicly voiced support https://blogs.juniper.net/en-us/industry-solutions-and-trends/building-a-better-and-safer-internet-with-manrs
  - Bring in more vendors (ask your favorite vendor about supporting MANRS)

Questions ?

max@stucchi.ch, melchior@juniper.net