4 months in...

RPKI Origin Validation In Real Life

Ben Maddison - SAFNOG-5 - 28 Aug 2019 - Johannesburg ZA
benm@workonline.co.za

workonline communications

Background

Resource Public Key Infrastructure

- Special purpose RPKI for Internet number resources
- Follows the RIR-system hierarchy
- Allows resource holders to make verifiable assertions
- Many possible use cases in number management and routing security

Ben Maddison - SAFNOG-5 - 28 Aug 2019 - Johannesburg ZA
benm@workonline.co.za

workonline communications

RPKI-based Route Origin Validation

- Allows receiving BGP speakers to validate that the origin AS is authorised to originate a route for that prefix
- Example:

2001:db8:f00::/48 AS_PATH=65000_65001_**65002**

- Uses an RPKI signed object: Route Origin Authorisation (ROA)

Ben Maddison - SAFNOG-5 - 28 Aug 2019 - Johannesburg ZA
benm@workonline.co.za

workonline communications

ROA Creation & Publication

- Resource Holders sign ROAs using the private key corresponding to their **EE certificate**.
- ROAs are placed in the RPKI repository, and listed in the repo's **manifest**
- ROAs are not certificates, just signed blobs of **ASN.1**:

```
(
    originASN,
    [ (prefix1, maxLength1), …, (prefixN, maxLengthN)]
)
```

Validating Routes

- Set of validated ROAs (VRPs) transmitted to BGP speakers via **RPKI-RTR** protocol
- Routers compare routes received from BGP neighbors to the VRPs, and set a **Validation State** (internally) on the route:

  NotFound - No VRP with a prefix covering the route

  Valid - A covering VRP, with matching origin ASN and maxLength was found

  Invalid - A covering VRP was found, but none matched *both* origin ASN and maxLength

Route Origin Validation at AS37271

Ben Maddison - SAFNOG-5 - 28 Aug 2019 - Johannesburg ZA
benm@workonline.co.za

workonline communications

Plan

- Initial plan is to implement by **end-October 2018**
- Mid-October routers are **connected to the RP-caches**. No policy to act on validation state - just a test to ensure that the VRPs get to the routers.

Network explodes... more on that later

The Plan 2.0

- November 2019, Workonline and two other regional transit operators commit to turning on ROV and **dropping Invalids on 1 April 2019**
- Initial deployment of a pair of RP caches - both running RIPE RPKI Validator v3
- Do not use the ARIN TAL, because of legal problems
- Routers connected to the caches during Feb 2019

Analysis

Q. Are we learning Invalids from customers?

A. *Most Invalids already being filtered. Only 1 bestpath :-)*

Q. How much discard traffic will we see?

A. *Statistically insignificant*

Q. How much egress traffic will move to competitors?

A. *Solved out of band!*

Deployment

Routing policy was deployed on AS37271 on 1 April 2019 to drop Invalids:

- All eBGP sessions (customer, transit, peering)
- Filters applied at the cache to ignore our own ROAs
- No ARIN TAL. Will re-evaluate if the legal issues change

Dropped approx. 3.5k IPv4 and 500 IPv6 prefixes.

No measurable drop in traffic in aggregate.

Post Deployment Experience

AKA “do as I say, not as I do”...

The ARIN TAL

- Workonline elected is not using the ARIN TAL because of the indemnification clause in the RPA
- Read carefully and make up your own mind
- Beware - some RP software now bundling the TAL with “click-through” acceptance
- Substantial pressure in the ARIN community to resolve the issues
- In the meantime, trade-off between OV coverage and legal risks - e.g. AS13335/AS701 incident

RP Software

RIPE Validator version 3.0 - Initial deployment

- + Nice API
- - Rebuilding DB loses local policy overrides
- - Suuuuper flakey

RIPE Validator version 3.1 - Running for ~3 weeks

- + **Far** more stable
- + Fixes local override issue
- - Broken SLURM syntax (GH issue #94)

RP Software - cont.

Routinator (NLnetLabs)

- + Very fast
- + Responsive and active dev team
- +/- New codebase, rapid development, interface stability
- - Not yet feature complete (but getting close)
- - Awkward deployment model - no binaries
- - Bundled ARIN TAL - **caution**

RP Software - cont.

Others:

- OctoRPKI / goRTR (Cloudflare)
- rpki-client(8) (OpenBSD)

Not enough experience to comment.... Come to the mic please.

Local Policy

How to handle validation of routes for customer assignments?

E.g.

2001:db8::/32 origin: **AS65000** (Aggr. announcement)

2001:db8:f00::/48 origin: **AS65001** (Non-exported customer more-specific)

Local Policy - options

A. Local ROAs per-assignment

   Lots of work, fragile

B. Locally ignore ROAs for own address space

   Easier than A but still fragile

C. Exempt local prefixes from “Invalid => reject” policy

benm@workonline.co.za

workonline communications

OV on Cisco IOS-XE

Ben Maddison - SAFNOG-5 - 28 Aug 2019 - Johannesburg ZA
benm@workonline.co.za

workonline communications

OV on Cisco IOS-XE - Intentional Behaviour

- Only eBGP-In validated - not iBGP or locally originated (not configurable)
- iBGP-In validation state signalled via ext. communities (disabled by default)
- Invalid == reject by default (configurable, but buggy)
- No RFC8097 ext. community => state=Valid (not configurable)
- Bestpatch selection **prefers Valid to Not Found** (not configurable!!!)

... and just add Add-Paths for awesome routing loops

OV on Cisco IOS-XE - Bugs

- Route-map based Invalid matching flakey
  - Cisco are attempting to reproduce
  - No meaningful feedback
  - Workaround: `bgp bestpath prefix-validate allow-invalid` – but see option C on slide 18 :-(
- Routes with no covering ROA *magically* become Valid for no reason!
  - Bug IDs CSCvp99869 / CSCvp99881
  - Fixed release pending...

Ask Your Vendor for RFC8481

What’s next?

Prefix-filter integration

- Workonline filters based on data in the IRR. **This has not changed**
- *Only* having a ROA is not currently enough to get into the filters
- We are planning:

1. Treat VRPs as equivalent to route(6) objects for the purpose of filter generation
2. Ignore route(6) objects in the IRR that conflict with a VRP (i.e. would be Invalid if announced)

Solution to Path Validation

Go read!:

- draft-azimov-sidrops-aspa-profile-01
- draft-ietf-grow-rpki-as-cones-01

Fin

Ben Maddison - SAFNOG-5 - 28 Aug 2019 - Johannesburg ZA
benm@workonline.co.za

workonline communications