# RPKI drop invalids – one year later

Sebastian Wiesinger
sebastian.wiesinger@noris.net

DENOG 11

noris network

# RPKI Basics

# Outgoing RPKI

- Cryptographically signs your prefixes
- "Binds" prefix to Origin AS and maximum CIDR length

## Validated ROAs

Show 10 entries

Search: 213.95.0.0/16

| ASN | Prefix | Max Length | Trust Anchors | URI of ROA |
|---|---|---|---|---|
| 12337 | 213.95.0.0/16 | 24 | RIPE NCC RPKI Root | |

« « 1 » »

Showing 1 to 1 of 1 entries (filtered from 113594 total entries)

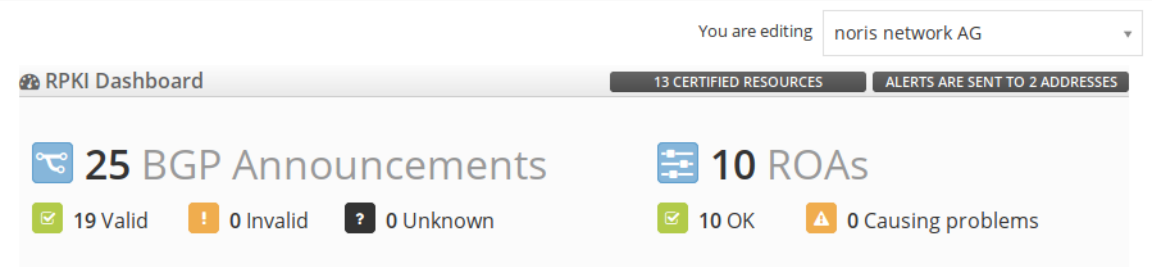
# Incoming RPKI

- RPKI Validator software – Validates cryptographic signatures
- Result of validation transferred via RTR protocol to routers
- Routers use validation results in routing policy

# What we did

# Create ROAs

- RIPE NCC makes this very easy
- Available at the LIR portal `https://lirportal.ripe.net/`
- End Users: your sponsoring LIR can do this for you!



# Install Validator Software

- Two servers with different software
- RIPE NCC RPKI Validator (v2, later v3)
  `https://github.com/RIPE-NCC/rpki-validator-3`
  Java will eat your memory :( but has a webinterface
- Routinator 3000
  `https://github.com/NLnetLabs/routinator`
  Smaller memory footprint but Rust toolchain neccessary
- ARIN TAL is special somehow and needs to be installed separately

# Configure Routers

- We use Juniper MX
- Feature “Origin validation for BGP” – Available since JunOS 12.2R1
- Peering routers need TCP session with RPKI Validator
- You need to explicitly set BGP `validation-state` in route policies
- Here you need to finally decide: Just mark invalid prefixes or drop them!

# Why do it?

# Why did we implement RPKI?

- Security is important to our customers
- It's good for the Internet
- Because we can

# D-Day

# Drop Invalids

2018-10-08 10:00 CEST

# Impact

- 5000 invalid prefixes dropped
- 2000 not covered by less-specific prefix


UNDERGROUND
THIS WAY
TO THE
AIR RAID SHELTER

# Aftermath

# First Impact

- Two days later
- /22 unreachable
- Contacted by provider
- Fixed ROA three hours later

# Difficulties with reports

- Identification of root cause difficult
- Many people not familiar with RPKI
- Customers report problems with DNS or e-Mail
- Traceroute from other provider looks like blackholing (which it kinda is)
- Own traceroutes end when reaching network core (without default route)

# Difficulties when communicating with providers and customers

- Support does not know RPKI
- Support does not know whom to contact
- Mailserver is affected by RPKI invalid
- Customer does not understand why it works “everywhere else”

# Lessions for communication

- Brief colleagues on RPKI and create SOPs
- Templates for communicating with customers and providers
  - Explanations on what RPKI is
  - How customer/provider can check RPKI status themselves
- Search for missed cases (“unreachable”, “connectivity issue”, “DNS problem”)

# Individual Cases

# Case 1 – Biggest Breakage

- Unitymedia / Vodafone
- /16, /17 and /19 invalid
- Announced with AS6830 (Liberty Global / UPC)
- ROAs had AS29562 (KabelBW / Unity Media) as origin
- Three separate customer reports in the first hour
- ROAs fixed in three hours

# Case 2 – No Exceptions! (Maybe just one)

- Customer was unable to reach API endpoint
- Detected on Thursday, provider informed
- Planned change on weekend with 20+ people
- Exception for /24 was created on Friday
- ROA was fixed 45 minutes after that

# Case 3 – Contact Lost

- All nameservers for domain in one /24
- No reaction from announcing AS or AS in ROA
- No reaction from prefix owner
- Company in prefix description does not know prefix
- Real hijack? – Turns out it wasn't.

# Conclusions

# Summary for the last year

- 13 known reports
  - 3 by affected providers
  - 10 by customers
  - Last report in April 2019

# Happy End

- All reports were resolved in one way or another
  - 12 ROAs fixed
  - 1 ROA deleted (but fixed some time later)
- Most people fix ROAs fast (maximum 10 days)
- Some people lose interest (providers and customers)
- (Our?) customers are cooperative if you explain RPKI

# Happy End – Part 2

- We're still filtering!
- You should, too!

# Questions?

Sebastian Wiesinger
sebastian.wiesinger@noris.net

noris network