RPKI Deep Dive – SAFNOG 6

Job Snijders
Fastly
job@fastly.com

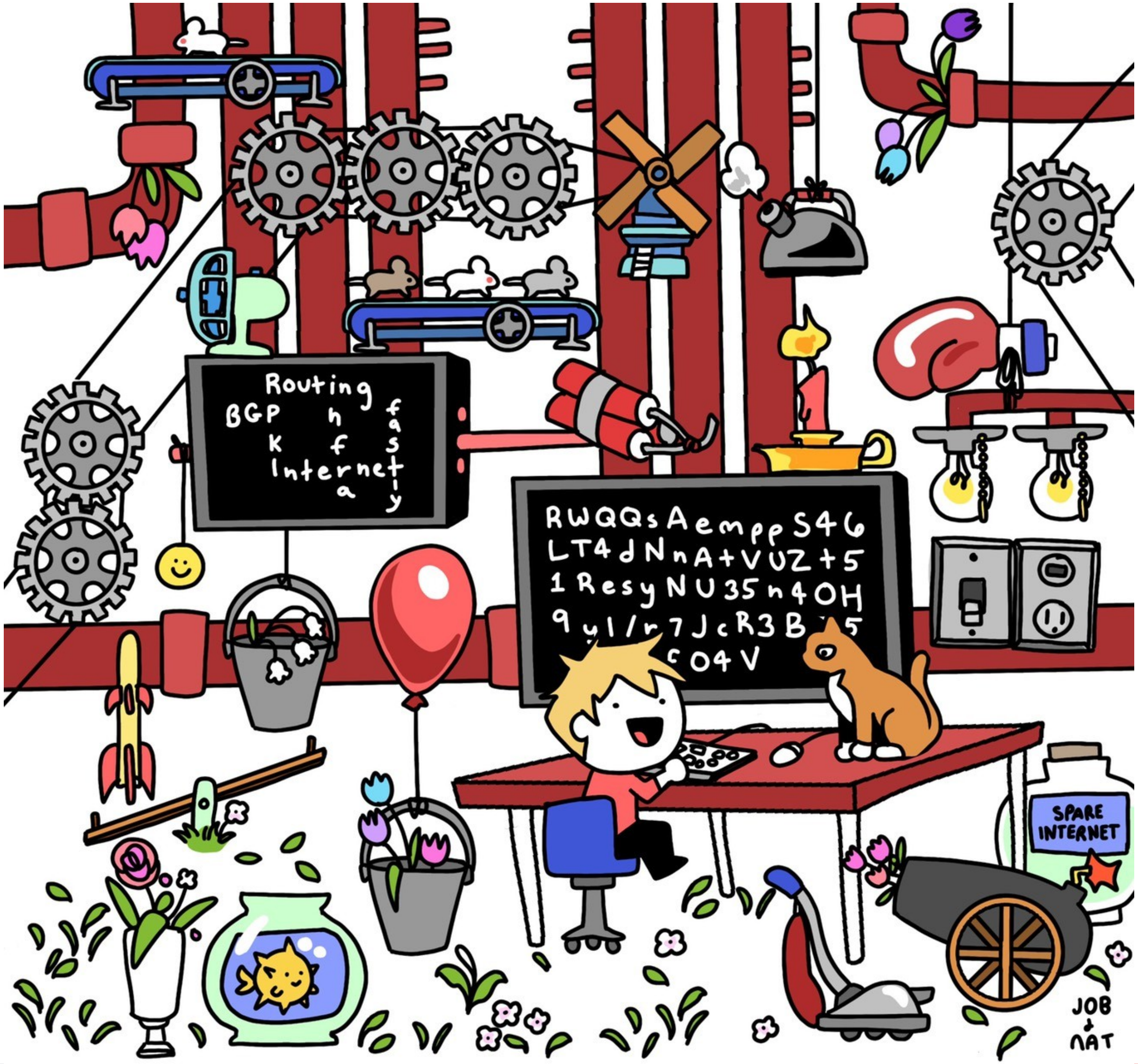
Who am I?

Job Snijders
job@fastly.com
Principal Software Engineer
Fastly

Web: https://sobornost.net/~job
Github: https://github.com/job

Volunteer at

- OpenBSD
- IETF
- RIPE NCC
- PeeringDB
- Route Server Support Foundation



Today's agenda for the RPKI deep dive

- How popular is RPKI?
- Analogies between BGP and RPKI
- RPKI: an *offline* protocol
- *New way of thinking:* Transitive Expiration Timers
- Building a future on top of the RPKI: *BGPsec, RSC, ASPA, and Certificate Transparency*
- Questions, Comments, Contact

How popular is RPKI?

Very popular!

- 31% of IP space covered by RPKI ROAS
- 38% of ASNs (seen in the DFZ), have ROAs pointed at them
- 27,000+ companies participating in the global RPKI *(estimate)*
- All major carriers & IXPs nowadays filter BGP routes with RPKI

(sources: https://rpki-monitor.antd.nist.gov, AS 15562 routers, and https://rpki.exposed)

What is *the* RPKI?

	BGP	RPKI
Nodes in the graph	Autonomous Systems	Certificate Authorities
What truths and lies you can tell to neighbors	No technical limitation	Constrained by entitlements received from parent
Direction of flow of information	Bi-directional peer-to-peer protocol	One way protocol: CA to RP (*kinda like Multicast)*
Plane of existence	**Online** BGP session down == routes withdrawn	**Offline** Information "*liveliness*" is time-based

An *offline* protocol – what does that mean?

Figure of speech: let's call the Default-Free Zone (BGP) *Online*, and the global RPKI system *Offline*. BGP and RPKI exist in different realms!

BGP: In the global Internet Routing system, stateful TCP sessions (BGP sessions with bi-directional KEEPALIVE messages) are used as a proxy variable for potential IP forwarding path.
Rip out all fibers, and within seconds your BGP router's routing table is empty.

RPKI: The Certificate Issuer (CA) tells everyone (inside each message) until when the message will be valid. BGP messages expire when the session goes down; contrast to RPKI messages: those expire at predefined moments in the future.
Force your computer's clock forward 2 days, and see all RPKI data disappear.

New way of thinking: Transitive Expiration Timers

There are LOTS of timers in a given RPKI validation chain:

This ROA:

rpki.afrinic.net/repository/member_repository/F36D8DFA/0E9B19BA140A11E5A7F5FC4CF8AEA228/8A1CC04C140B11E58809AA4DF8AEA228.roa

Authorizes AS 37271 to originate IP Prefix 2c0f:fa90:f00::/40

Timeline:

The ROA's EE certificate expires on June 16th, 09:39:04 2025 GMT
The EE cert's parent expires on March 31st, 00:00:00 2022 GMT
The Parent's CRL is valid until September 28th, 00:30:59 2021 GMT
The parent's parent is valid until March 30th, 00:00:00 2025 GMT
The parent's parent's CRL is valid until October 20th, 06:40:20 2021 GMT
The parent's parent's parent is valid until March 28th, 09:58:36 2030 GMT

New way of thinking: Transitive Expiration Timers

There are LOTS of timers in a given RPKI validation chain:

This ROA:

rpki.afrinic.net/repository/member_repository/F36D8DFA/0E9B19BA140A11E5A7F5FC4CF8AEA228/8A1CC04C140B11E58809AA4DF8AEA228.roa

Authorizes AS 37271 to originate IP Prefix 2c0f:fa90:f00::/40

Timeline:

Transitive expiry time

The ROA's EE certificate expires on June 16th, 09:39:04 2025 G
The EE cert's parent expires on March 31st, 00:00:00 2022 GMT
The Parent's CRL is valid until September 28th, 00:30:59 2021 GMT
The parent's parent is valid until March 30th, 00:00:00 2025 GMT
The parent's parent's CRL is valid until October 20th, 06:40:20 2021 GMT
The parent's parent's parent is valid until March 28th, 09:58:36 2030 GMT

Building our business futures on top of RPKI

The global RPKI system gives the operator community the tools to grow the global Internet routing system. To expand the network and expand business.

In the next few years, keep an eye out for these technologies:

- *Resource Signed Checklists* (RSC, spec)
  → Use RPKI as a building block for automating BYOIP or XC provisioning
- *ASPA* (Autonomous System Provider Authorization, spec)
  → Ability to sign & distribute desired EBGP routing policy to the world
- *Certificate Transparency* (CT, very early stages, discussion here)
  → CT enables automated and complete auditing, increasing trust in the RPKI
- *BGPsec* (cloud operators are preparing for lab-testing, spec)
  → Peer with even more confidence with Route Servers and Public IX peers.
  Protect your high value private peerings.

Questions, comments, follow-up?

Reach out to me!

Email: job@fastly.com

Twitter: https://twitter.com/JobSnijders

Photo credit slide #5 - Marco Verch - https://www.flickr.com/photos/30478819@N08/47459566892