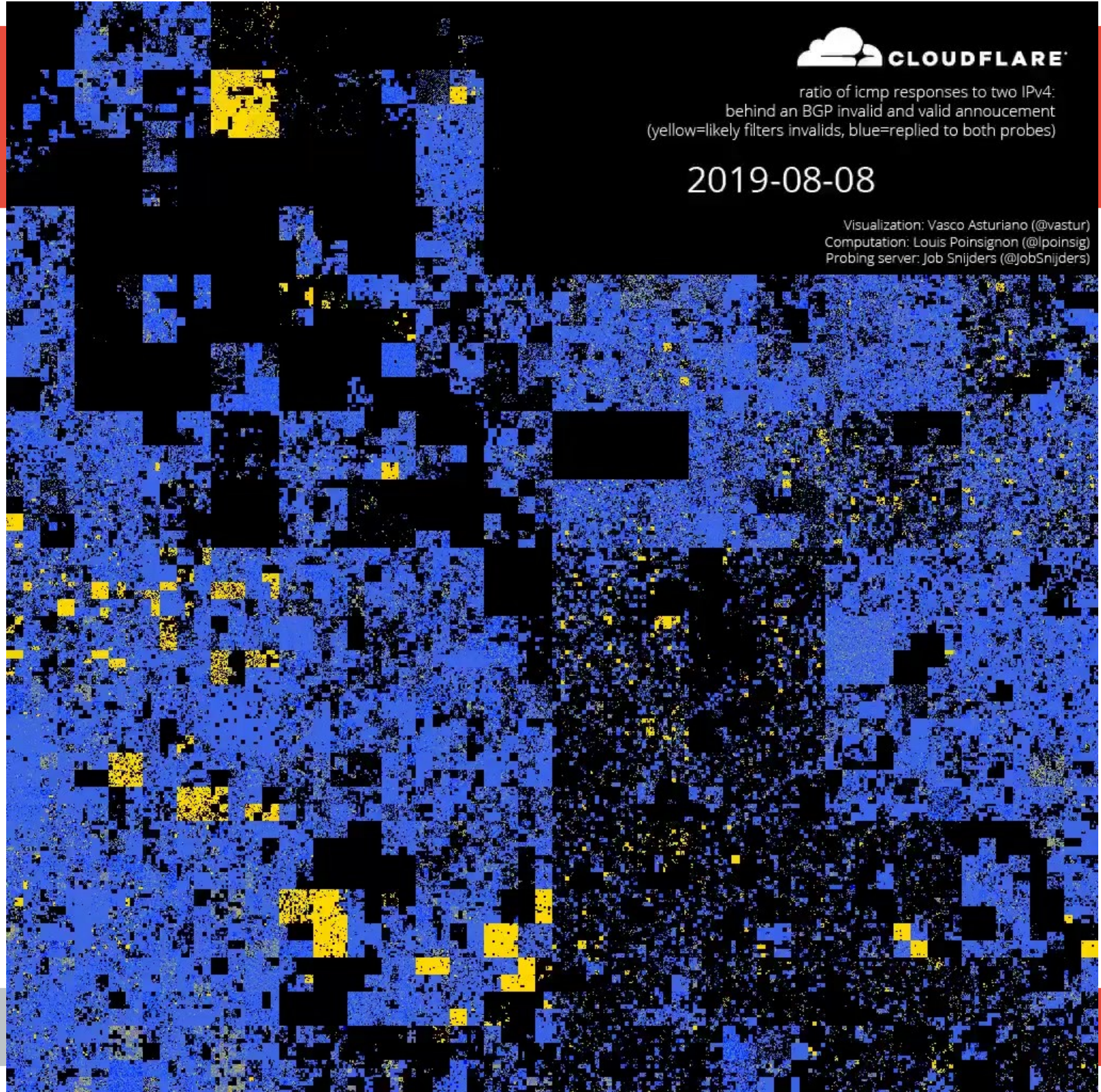
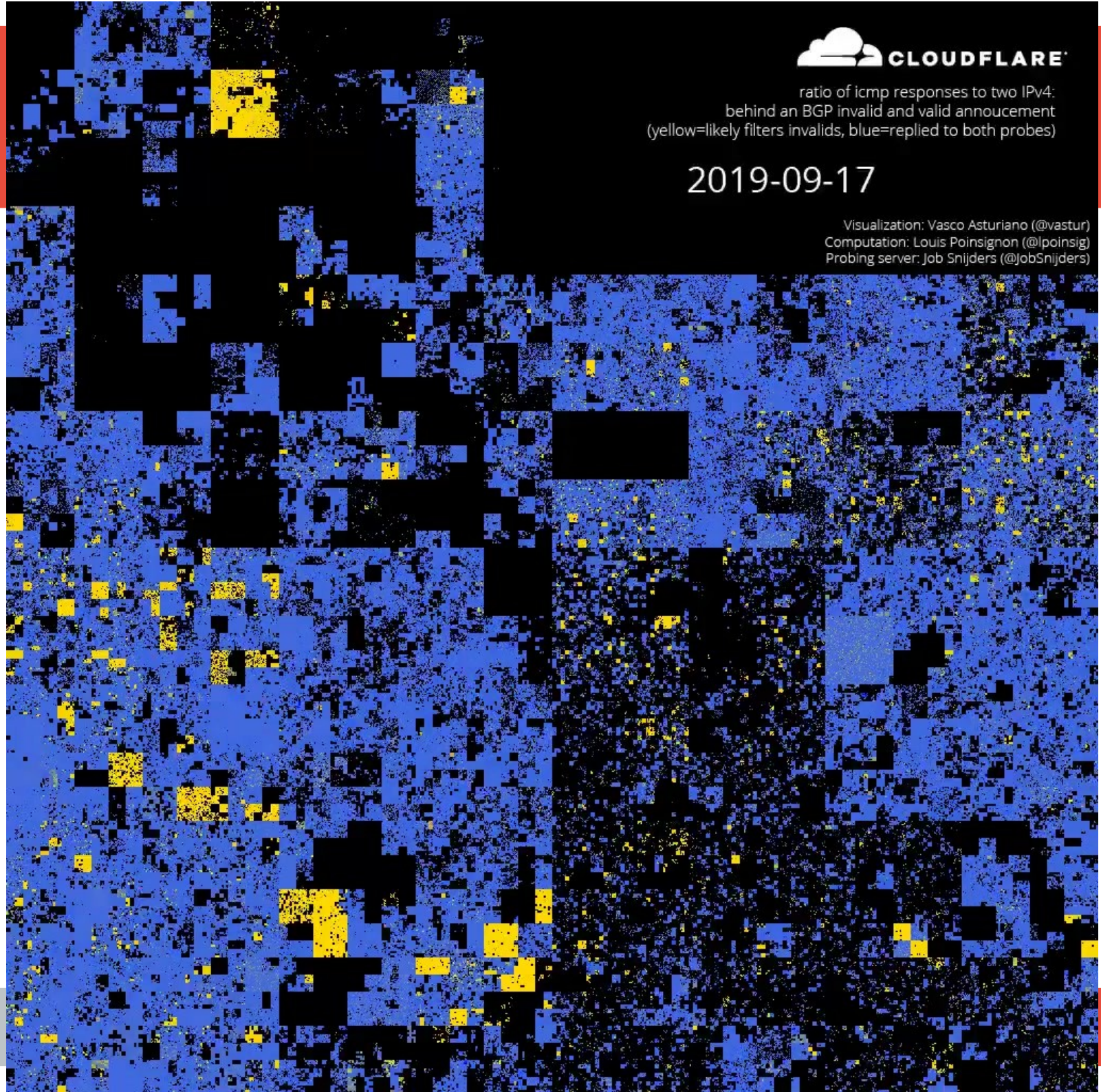
Routing security update IEPG @ IETF 106

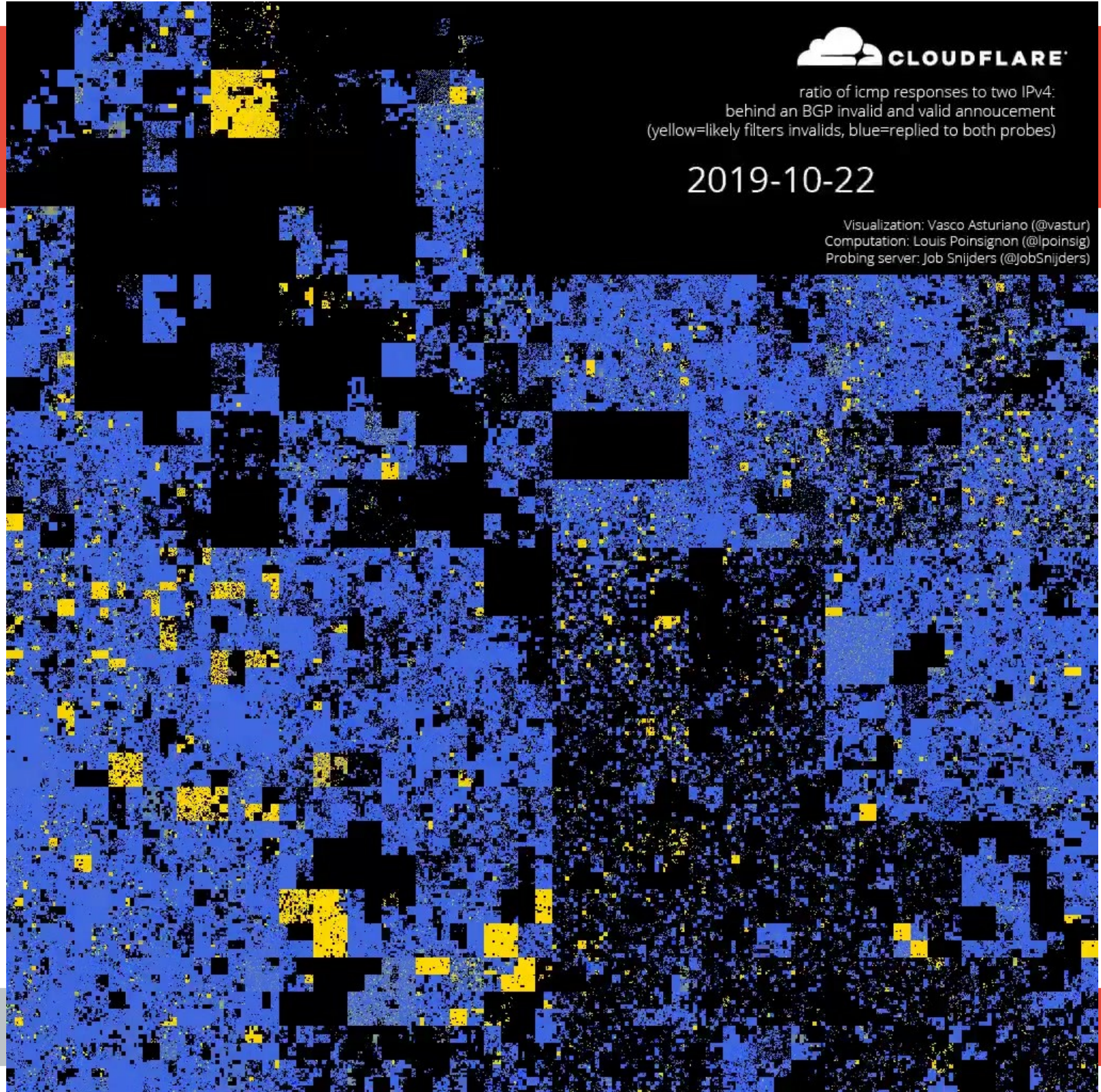
Job Snijders
NTT / AS 2914
job@ntt.net

Where we at?

- Deployment update
- RIR policy update
- IRRd 4 update
- OpenBSD update


CLOUDFLARE
ratio of icmp responses to two IPv4:
behind an BGP invalid and valid annoucement
(yellow=likely filters invalids, blue=replied to both probes)
2019-08-08
Visualization: Vasco Asturiano (@vastur)
Computation: Louis Poinsignon (@lpoinsig)
Probing server: Job Snijders (@JobSnijders)


CLOUDFLARE
ratio of icmp responses to two IPv4:
behind an BGP invalid and valid annoucement
(yellow=likely filters invalids, blue=replied to both probes)
2019-09-17
Visualization: Vasco Asturiano (@vastur)
Computation: Louis Poinsignon (@lpoinsig)
Probing server: Job Snijders (@JobSnijders)


CLOUDFLARE
ratio of icmp responses to two IPv4:
behind an BGP invalid and valid annoucement
(yellow=likely filters invalids, blue=replied to both probes)
2019-10-22
Visualization: Vasco Asturiano (@vastur)
Computation: Louis Poinsignon (@lpoinsig)
Probing server: Job Snijders (@JobSnijders)

RIPE-731 Non-Authoritative Route Object Clean-up

- Context: in fall 2018 - “RIPE” split into “RIPE” and “RIPE-NONAUTH”
- “RIPE-NONAUTH” contains 65,500 objects - a mix of useful and not useful data, deleting it wholesale wasn’t deemed good.
- Community consensus to use RPKI to delete “RPKI invalid” IRR route objects from the “RIPE-NONAUTH” IRR source.
- Currently there are ~ 900 objects that are “RIPE invalid”
- https://github.com/job/ripe-proposal-2018-06

```
$ pip3 install ripe-proposal-2018-06
```

Example of RIPE-731 cleanup

```
INVALID! The 207.32.102.0/24AS3549 RIPE-NONAUTH route object has
conflicts:

    route:          207.32.102.0/24
    descr:          GBLX-US-STATIC
    origin:         AS3549
    mnt-by:         GBLX-RIPE-MNT
    created:        1970-01-01T00:00:00Z
    last-modified:  2018-09-04T15:35:00Z
    source:         RIPE-NONAUTH

    Above non-authoritative IRR object is in conflict with this ROA:
        ROA: 207.32.64.0/18, MaxLength: 18, Origin AS2914 (arin)
```

IRRd version 4 is here!

https://github.com/irrdnet/irrd4

Funded by NTT / AS 2914, developed by Dashcare

IRRd version 4

- Reliability issues with Legacy IRRd, no room for innovation
- Critical to NTT's daily operations, all NTT's prefix-filters are generated with this software
- IRRd 4.0 Runs in production at rr.ntt.net since July 2019
- Next version - IRRd 4.1 - will support "RIPE-731"-style RPKI cleanup
  - Reject updates to, and delete conflicting objects from "Authoritative" database
  - Ignore conflicting objects when using NRTM to feed routing database cache

Using the RPKI to clean up conflicting IRR

- Industry-wide common method to get rid of stale proxy route objects – by creating a ROA you hide old garbage in IRRs

- By creating a ROA – you will significantly decrease the chances of people being able to use IRR to hijack your resource

Timeline:

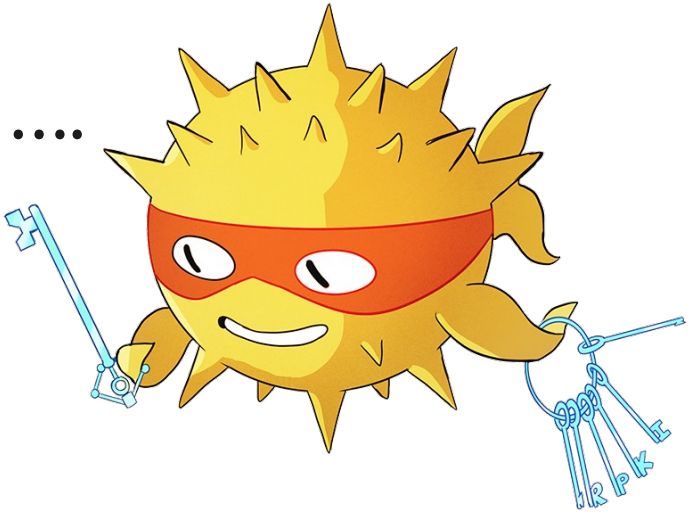
Spring 2020 – RIPE NCC to implement RIPE-731?

Spring 2020 – IRRd 4.1 release & deployment?

OpenBSD – free, functional & secure

Out-of-the-box you get BGP, OSPF & MPL and now ….

… A RPKI validator implementation “rpki-client”



The road wasn’t easy:

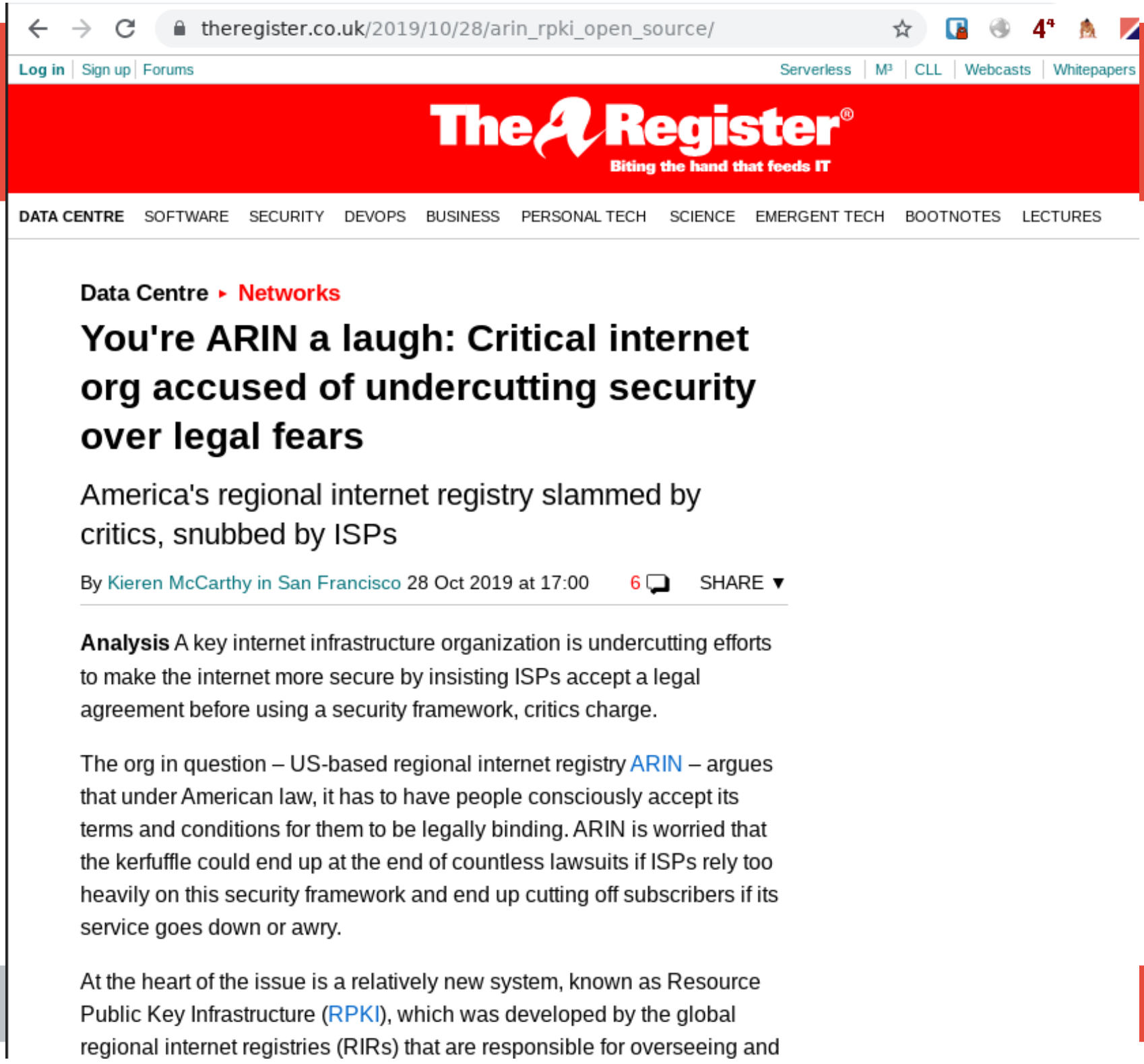
- LibreSSL had to be extended to support CMS
- BSD licensed rsync client “*openrsync*” had to be created

From the developers: “*CMS code in OpenSSL is over 6,000+ lines and crosses about 25 files, with tendrils in ASN.1, DH, DSA, EC, PEM and RSA.*”

What an open & secure Internet looks like

```
1 2 3 4 5 6 7 8   W:  91% @ ietf-hotel 31.133.154.71|T: down ||vol: 49% ||LOAD: 0.48 ||CHR 96% %00:00 min.|| 01:26:10 17-11-2019 UTC
xterm
kiera ~$ sysctl kern.version
kern.version=OpenBSD 6.6 (GENERIC.MP) #0: Sat Oct 26 08:08:07 MDT 2019
    root@syspatch-66-amd64.openbsd.org:/usr/src/sys/arch/amd64/compile/GENERIC.MP

kiera ~$ doas rcctl check bgpd
bgpd(ok)
kiera ~$ crontab -l | grep rpki
05 */13 * * * chronic /home/job/bin/fetch_rpki_irr
00 * * * * -n sleep $((RANDOM \% 2048)) && rpki-client -v /etc/bgpd/rpki.conf && bgpctl reload
kiera ~$ bgpctl show rib ovs invalid | wc -l
    5673
kiera ~$ bgpctl show rib ovs valid | wc -l
  130835
kiera ~$
```



theregister.co.uk/2019/10/28/arin_rpki_open_source/

Log in | Sign up | Forums

Serverless | M³ | CLL | Webcasts | Whitepapers

The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE SECURITY DEVOPS BUSINESS PERSONAL TECH SCIENCE EMERGENT TECH BOOTNOTES LECTURES

Data Centre ▸ Networks

You're ARIN a laugh: Critical internet org accused of undercutting security over legal fears

America's regional internet registry slammed by critics, snubbed by ISPs

By Kieren McCarthy in San Francisco 28 Oct 2019 at 17:00 6 SHARE ▼

Analysis A key internet infrastructure organization is undercutting efforts to make the internet more secure by insisting ISPs accept a legal agreement before using a security framework, critics charge.

The org in question – US-based regional internet registry ARIN – argues that under American law, it has to have people consciously accept its terms and conditions for them to be legally binding. ARIN is worried that the kerfuffle could end up at the end of countless lawsuits if ISPs rely too heavily on this security framework and end up cutting off subscribers if its service goes down or awry.

At the heart of the issue is a relatively new system, known as Resource Public Key Infrastructure (RPKI), which was developed by the global regional internet registries (RIRs) that are responsible for overseeing and

Message to IETF / IEPG

RPKI is here, it is real, it's deployed, folks are using it (Yay!)

We need to keep listening to both the implementers and the operators about what's good & bad.