HURRICANE ELECTRIC
INTERNET SERVICES

RPKI at Hurricane Electric

Susan Forney

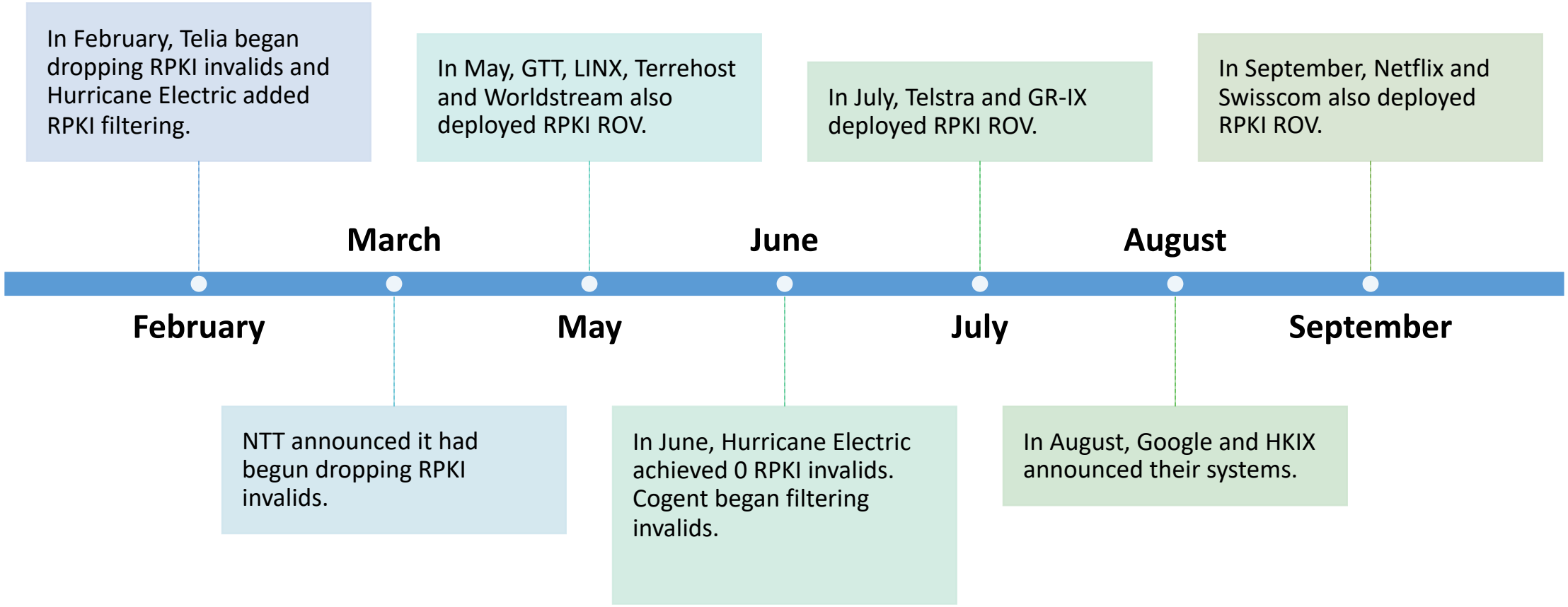
Hurricane Electric AS6939

RPKI at Hurricane Electric

2020 has not lacked for significant developments, but one of the positives was the progress made globally in the adoption of RPKI route origin validation (ROV).

- Hurricane Electric's deployment and what is going on globally.
- Hurricane Electric's supporting tools that help you in the event of a problem.
- A look at RPKI in general and how it is faring.

ISP RPKI ROV Adoption



RPKI at Hurricane Electric

Our system does not rely on routers with a full set of validated ROA payloads (VRPs) from a RPKI-to-Router (RTR) protocol.

- We generate filters for our peers daily that validate RPKI and IRR records.
- Like many ISPs, we have devices deployed at our edge that do not support the RTR protocol.
- Our system will identify an invalid announcement and remove it from our table in less than a minute.

Submit

ROUTE FILTERING HOME ALGORITHM

28603 sessions
21090 filters

RPKI at Hurricane Electric

This is the route filtering algorithm that we document on routing.he.net:

1. Attempt to find an as-set to use for this network.

    1.1 Inspect the aut-num for this ASN to see if we can extract from their IRR policy for what they would announce to Hurricane by finding export or mp-export to AS6939, ANY, or AS-ANY.

    1.2 Also see if they set what looks like a valid IRR as-set name in peeringdb.com.

2. Collect the received routes for all BGP sessions with this ASN. This details both accepted and filtered routes.

RPKI Implementation at Hurricane Electric

3. For each route, perform the following rejection tests:

- 3.1 Reject default routes 0.0.0.0/0 and ::/0.
- 3.2 Reject paths using BGP AS_SET notation (i.e. {1} or {1 2}, etc). See draft-ietf-idr-deprecate-as-set-confed-set.
- 3.3 Reject prefix lengths less than minimum and greater than maximum. For IPv4 this is 8 and 24. For IPv6 this is 16 and 48.
- 3.4 Reject bogons (RFC1918, documentation prefix, etc).
- 3.5 Reject exchange prefixes for all exchanges Hurricane Electric is connected to.
- 3.6 Reject routes that have RPKI status INVALID_ASN or INVALID_LENGTH based on the origin AS and prefix.

RPKI Implementation at Hurricane Electric

4. For each route, perform the following acceptance tests:
   - 4.1 If the origin is the neighbor AS, accept routes that have RPKI status VALID based on the origin AS and prefix.
   - 4.2 If the prefix is an announced downstream route that is a subnet of an accepted originated prefix that was accepted due to either RPKI or an RIR handle match, accept the prefix.
   - 4.3 If RIR handles match for the prefix and the peer AS, accept the prefix.
   - 4.4 If this prefix exactly matches a prefix allowed by the IRR policy of this peer, accept the prefix.
   - 4.5 If the first AS in the path matches the peer and path is two hops long and the origin AS is in the expanded as-set for the peer AS and either the RPKI status is VALID or there is an RIR handle match for the origin AS and the prefix, accept the prefix.
5. Reject all prefixes not explicitly accepted.

RPKI Implementation at Hurricane Electric

If you want to know at a glance how your network measures up, we have the following tools to help:

- Bgp.he.net—Our classic site featuring information from public sources about BGP and the Internet
- Routing.he.net—Our site that lets you look at any network advertises prefixes to Hurricane Electric and see how we filtered the routes.

HURRICANE ELECTRIC
INTERNET SERVICES

Search

AS44684 Mythic Beasts Ltd

Quick Links

- BGP Toolkit Home
- BGP Prefix Report
- BGP Peer Report
- Exchange Report
- Bogon Routes
- World Report
- Multi Origin Routes
- DNS Report
- Top Host Report
- Internet Statistics
- Looking Glass
- Network Tools App
- Free IPv6 Tunnel
- IPv6 Certification
- IPv6 Progress
- Going Native
- Contact Us

AS Info | Graph v4 | Graph v6 | Prefixes v4 | Prefixes v6 | Peers v4 | Peers v6 | Whois | IRR | IX

Prefix	Description
45.13.66.0/24	Operation Enterprise LLC
46.235.224.0/21	Mythic Beasts Ltd
93.93.128.0/21	Mythic Beasts Ltd
176.126.240.0/21	Mythic Beasts Ltd
185.47.60.0/22	Mythic Beasts Ltd
185.101.96.0/24	
185.159.24.0/24	Calaberis-Pi
195.10.223.0/24	Mythic Beasts Ltd

Updated 04 Mar 2020 22:56 PST © 2020 Hurricane Electric

HURRICANE ELECTRIC INTERNET SERVICES

Search

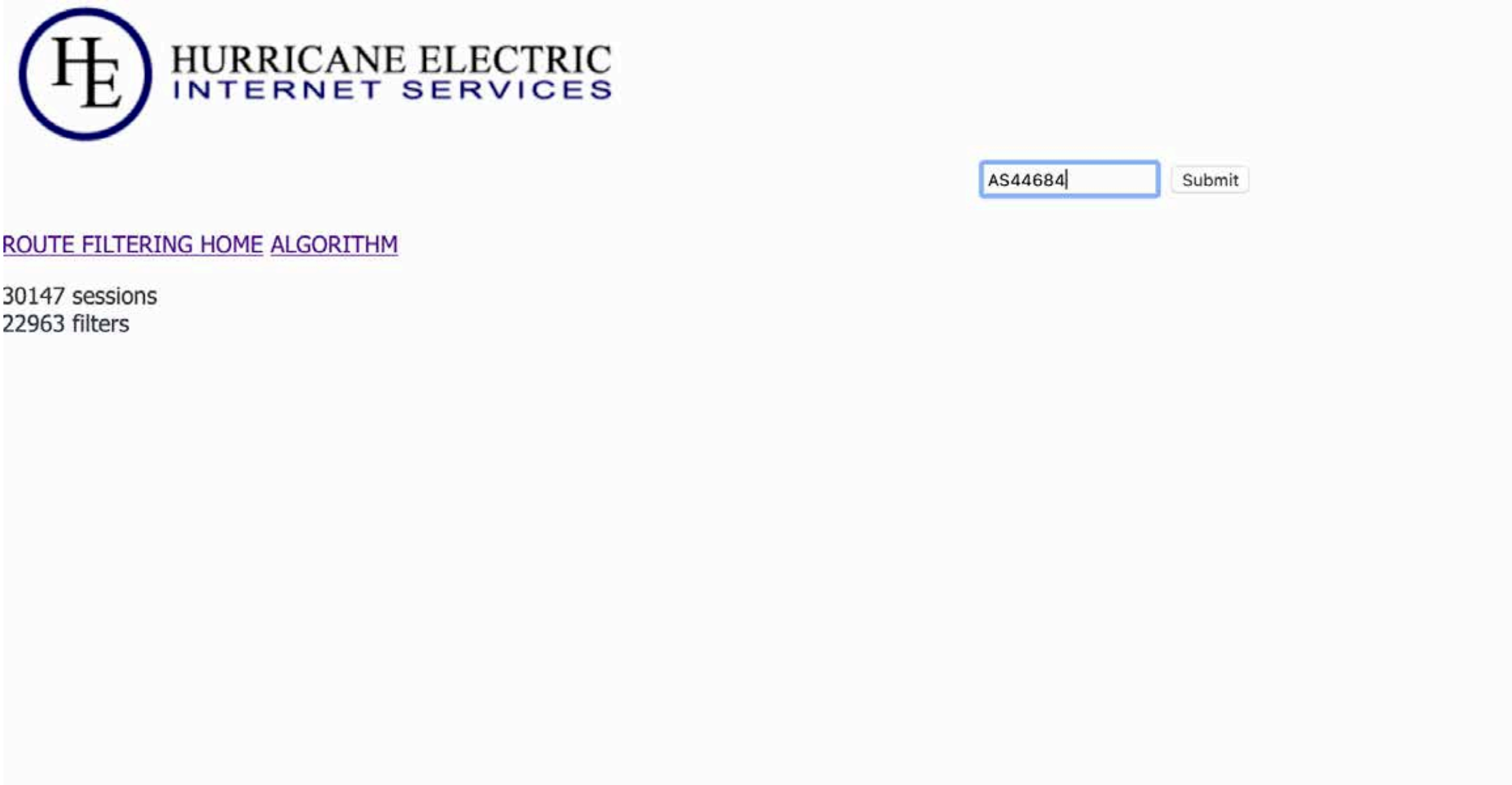
AS9873 Lao Telecom Communication, LTC

Quick Links

- BGP Toolkit Home
- BGP Prefix Report
- BGP Peer Report
- Exchange Report
- Bogon Routes
- World Report
- Multi Origin Routes
- DNS Report
- Top Host Report
- Internet Statistics
- Looking Glass
- Network Tools App
- Free IPv6 Tunnel
- IPv6 Certification
- IPv6 Progress
- Going Native
- Contact Us

AS Info | Graph v4 | Graph v6 | Prefixes v4 | Prefixes v6 | Peers v4 | Peers v6 | Whois | IRR | IX

Prefix	Description
43.224.36.0/22	Lao Telecommunication Co Ltd
43.224.36.0/24	Lao Telecommunication Co Ltd
43.224.37.0/24	Lao Telecommunication Co Ltd
43.224.38.0/24	Lao Telecommunication Co Ltd
43.224.39.0/24	Lao Telecommunication Co Ltd
103.43.76.0/22	Lao Telecommunication Co Ltd
103.43.76.0/24	Lao Telecommunication Co Ltd
103.43.77.0/24	Lao Telecommunication Co Ltd
103.43.78.0/24	Lao Telecommunication Co Ltd
103.43.79.0/24	Lao Telecommunication Co Ltd
115.84.64.0/18	Telecommunication Service
115.84.64.0/24	Telecommunication Service
115.84.65.0/24	Telecommunication Service
115.84.66.0/24	Telecommunication Service
115.84.67.0/24	Telecommunication Service
115.84.68.0/24	Telecommunication Service


HURRICANE ELECTRIC
INTERNET SERVICES
AS44684
Submit
ROUTE FILTERING HOME ALGORITHM
30147 sessions
22963 filters

HURRICANE ELECTRIC
INTERNET SERVICES

Submit

ROUTE FILTERING HOME ALGORITHM REPORTS

AS44684

ASN	STATUS	PEERINGDB_IRR	EXTRACTED_V4	EXTRACTED_V6	OK_V4	OK_V6	SOURCE
44684	explicit	AS-MYTHIC	AS-MYTHIC	AS-MYTHIC	AS-MYTHIC	AS-MYTHIC	peeringdb

FILTERS

AF	AS-SET NAME	IRR STATUS	IRR BUILT	IRR LINES	PREFIXES RECEIVED	FILTER BUILT	FILTER LINES	POLICY	REASONS	FILTER
4	AS-MYTHIC	good	March 05 2020 01:49:06	170	21	March 05 2020 01:49:07	21	DISPLAY	DISPLAY	DISPLAY
6	AS-MYTHIC	good	March 05 2020 01:49:09	16	57	March 05 2020 01:49:09	29	DISPLAY	DISPLAY	DISPLAY

PREFIX LISTS

AF	ROUTER	NAME	STATUS	CHECKED	EXISTING_LINES	VERIFIED	EXISTING	DELTA	LOG
4	core1.ams1.he.net	prefix-filter-as44684	verified	November 11 2019 19:02:01	20	November 11 2019 19:02:01	DISPLAY	DISPLAY	DISPLAY
4	core1.lon2.he.net	prefix-filter-as44684	updated	March 05 2020 04:06:10	20	March 05 2020 04:06:27	DISPLAY	DISPLAY	DISPLAY
4	core3.lon1.he.net	prefix-filter-as44684	updated	March 05 2020 03:15:35	84	March 05 2020 03:15:43	DISPLAY	DISPLAY	DISPLAY
6	core1.ams1.he.net	ipv6-prefix-filter-as44684	verified	November 12 2019 02:55:42	9	November 12 2019 02:55:43	DISPLAY	DISPLAY	DISPLAY
6	core1.lon2.he.net	ipv6-prefix-filter-as44684	verified	March 05 2020 08:33:22	29	March 05 2020 08:33:23	DISPLAY	DISPLAY	DISPLAY
6	core3.lon1.he.net	ipv6-prefix-filter-as44684	updated	March 05 2020 03:53:41	41	March 05 2020 03:53:50	DISPLAY	DISPLAY	DISPLAY

SESSIONS

8 sessions.

SESSION STATUS IS NON REALTIME, DATA IN TABLE IS DELAYED APPROXIMATELY 24 HOURS

IP	ROUTER	STATUS	ACCEPTED	FILTERED	RECEIVED	RCVD STATUS	RCVD UPDATED	RCVD ACCEPTED	RCVD FILTERED
195.66.224.72	core1.lon2.he.net	ESTAB	20	1	DISPLAY	good	March 02 2020 12:56:00	20	1
2001:7f8:17::ae8c:1	core3.lon1.he.net	ESTAB	7	3	DISPLAY	good	January 14 2020 00:07:35	7	3
2001:7f8:17::ae8c:2	core3.lon1.he.net	ESTAB	7	3	DISPLAY	good	January 14 2020 00:07:38	7	3
2001:7f8:1::a504:4684:1	core1.ams1.he.net	ESTAB	8	17	DISPLAY	good	November 12 2019 02:22:24	8	48

HURRICANE ELECTRIC
INTERNET SERVICES

Submit

ROUTE FILTERING HOME ALGORITHM REPORTS

AS44684

ASN	STATUS	PEERINGDB_IRR	EXTRACTED_V4	EXTRACTED_V6	OK_V4	OK_V6	SOURCE
44684	explicit	AS-MYTHIC	AS-MYTHIC	AS-MYTHIC	AS-MYTHIC	AS-MYTHIC	peeringdb

FILTERS

AF	AS-SET NAME	IRR STATUS	IRR BUILT	IRR LINES	PREFIXES RECEIVED	FILTER BUILT	FILTER LINES	POLICY	REASONS	FILTER
4	AS-MYTHIC	good	March 05 2020 01:49:06	170	21	March 05 2020 01:49:07	21	DISPLAY	DISPLAY	DISPLAY
6	AS-MYTHIC	good	March 05 2020 01:49:09	16	57	March 05 2020 01:49:09	29	DISPLAY	DISPLAY	DISPLAY

PREFIX LISTS

AF	ROUTER	NAME	STATUS	CHECKED	EXISTING_LINES	VERIFIED	EXISTING	DELTA	LOG
4	core1.ams1.he.net	prefix-filter-as44684	verified	November 11 2019 19:02:01	20	November 11 2019 19:02:01	DISPLAY	DISPLAY	DISPLAY
4	core1.lon2.he.net	prefix-filter-as44684	updated	March 05 2020 04:06:10	20	March 05 2020 04:06:27	DISPLAY	DISPLAY	DISPLAY
4	core3.lon1.he.net	prefix-filter-as44684	updated	March 05 2020 03:15:35	84	March 05 2020 03:15:43	DISPLAY	DISPLAY	DISPLAY
6	core1.ams1.he.net	ipv6-prefix-filter-as44684	verified	November 12 2019 02:55:42	9	November 12 2019 02:55:43	DISPLAY	DISPLAY	DISPLAY
6	core1.lon2.he.net	ipv6-prefix-filter-as44684	verified	March 05 2020 08:33:22	29	March 05 2020 08:33:23	DISPLAY	DISPLAY	DISPLAY
6	core3.lon1.he.net	ipv6-prefix-filter-as44684	updated	March 05 2020 03:53:41	41	March 05 2020 03:53:50	DISPLAY	DISPLAY	DISPLAY

SESSIONS

8 sessions.

SESSION STATUS IS NON REALTIME, DATA IN TABLE IS DELAYED APPROXIMATELY 24 HOURS

IP	ROUTER	STATUS	ACCEPTED	FILTERED	RECEIVED	RCVD STATUS	RCVD UPDATED	RCVD ACCEPTED	RCVD FILTERED
195.66.224.72	core1.lon2.he.net	ESTAB	20	1	DISPLAY	good	March 02 2020 12:56:00	20	1
2001:7f8:17::ae8c:1	core3.lon1.he.net	ESTAB	7	3	DISPLAY	good	January 14 2020 00:07:35	7	3
2001:7f8:17::ae8c:2	core3.lon1.he.net	ESTAB	7	3	DISPLAY	good	January 14 2020 00:07:38	7	3
2001:7f8:1::a504:4684:1	core1.ams1.he.net	ESTAB	8	17	DISPLAY	good	November 12 2019 02:22:24	8	48

Submit

ROUTE FILTERING HOME ALGORITHM

AS44684 AF v4 irr

Last Modified March 10 2020 01:46:57

```
no ip prefix-list NN
ip prefix-list NN permit 45.13.66.0/24
ip prefix-list NN permit 45.142.136.0/24
ip prefix-list NN permit 45.154.32.0/23
ip prefix-list NN permit 46.235.224.0/21
ip prefix-list NN permit 62.50.96.0/19
ip prefix-list NN permit 62.50.96.0/24
ip prefix-list NN permit 62.50.97.0/24
ip prefix-list NN permit 62.50.98.0/24
ip prefix-list NN permit 62.50.99.0/24
ip prefix-list NN permit 62.50.100.0/24
ip prefix-list NN permit 62.50.101.0/24
ip prefix-list NN permit 62.50.102.0/24
ip prefix-list NN permit 62.50.103.0/24
ip prefix-list NN permit 62.50.104.0/24
ip prefix-list NN permit 62.50.105.0/24
ip prefix-list NN permit 62.50.106.0/24
ip prefix-list NN permit 62.50.107.0/24
ip prefix-list NN permit 62.50.108.0/24
ip prefix-list NN permit 62.50.109.0/24
```

HURRICANE ELECTRIC
INTERNET SERVICES

Submit

ROUTE FILTERING HOME ALGORITHM REPORTS

AS44684

ASN	STATUS	PEERINGDB_IRR	EXTRACTED_V4	EXTRACTED_V6	OK_V4	OK_V6	SOURCE
44684	explicit	AS-MYTHIC	AS-MYTHIC	AS-MYTHIC	AS-MYTHIC	AS-MYTHIC	peeringdb

FILTERS

AF	AS-SET NAME	IRR STATUS	IRR BUILT	IRR LINES	PREFIXES RECEIVED	FILTER BUILT	FILTER LINES	POLICY	REASONS	FILTER
4	AS-MYTHIC	good	March 05 2020 01:49:06	170	21	March 05 2020 01:49:07	21	DISPLAY	DISPLAY	DISPLAY
6	AS-MYTHIC	good	March 05 2020 01:49:09	16	57	March 05 2020 01:49:09	29	DISPLAY	DISPLAY	DISPLAY

PREFIX LISTS

AF	ROUTER	NAME	STATUS	CHECKED	EXISTING_LINES	VERIFIED	EXISTING	DELTA	LOG
4	core1.ams1.he.net	prefix-filter-as44684	verified	November 11 2019 19:02:01	20	November 11 2019 19:02:01	DISPLAY	DISPLAY	DISPLAY
4	core1.lon2.he.net	prefix-filter-as44684	updated	March 05 2020 04:06:10	20	March 05 2020 04:06:27	DISPLAY	DISPLAY	DISPLAY
4	core3.lon1.he.net	prefix-filter-as44684	updated	March 05 2020 03:15:35	84	March 05 2020 03:15:43	DISPLAY	DISPLAY	DISPLAY
6	core1.ams1.he.net	ipv6-prefix-filter-as44684	verified	November 12 2019 02:55:42	9	November 12 2019 02:55:43	DISPLAY	DISPLAY	DISPLAY
6	core1.lon2.he.net	ipv6-prefix-filter-as44684	verified	March 05 2020 08:33:22	29	March 05 2020 08:33:23	DISPLAY	DISPLAY	DISPLAY
6	core3.lon1.he.net	ipv6-prefix-filter-as44684	updated	March 05 2020 03:53:41	41	March 05 2020 03:53:50	DISPLAY	DISPLAY	DISPLAY

SESSIONS

8 sessions.

SESSION STATUS IS NON REALTIME, DATA IN TABLE IS DELAYED APPROXIMATELY 24 HOURS

IP	ROUTER	STATUS	ACCEPTED	FILTERED	RECEIVED	RCVD STATUS	RCVD UPDATED	RCVD ACCEPTED	RCVD FILTERED
195.66.224.72	core1.lon2.he.net	ESTAB	20	1	DISPLAY	good	March 02 2020 12:56:00	20	1
2001:7f8:17::ae8c:1	core3.lon1.he.net	ESTAB	7	3	DISPLAY	good	January 14 2020 00:07:35	7	3
2001:7f8:17::ae8c:2	core3.lon1.he.net	ESTAB	7	3	DISPLAY	good	January 14 2020 00:07:38	7	3
2001:7f8:1::a504:4684:1	core1.ams1.he.net	ESTAB	8	17	DISPLAY	good	November 12 2019 02:22:24	8	48

HURRICANE ELECTRIC
INTERNET SERVICES

Submit

ROUTE FILTERING HOME ALGORITHM REPORTS

AS44684 AF v4 reasons

Last Modified March 05 2020 01:49:07

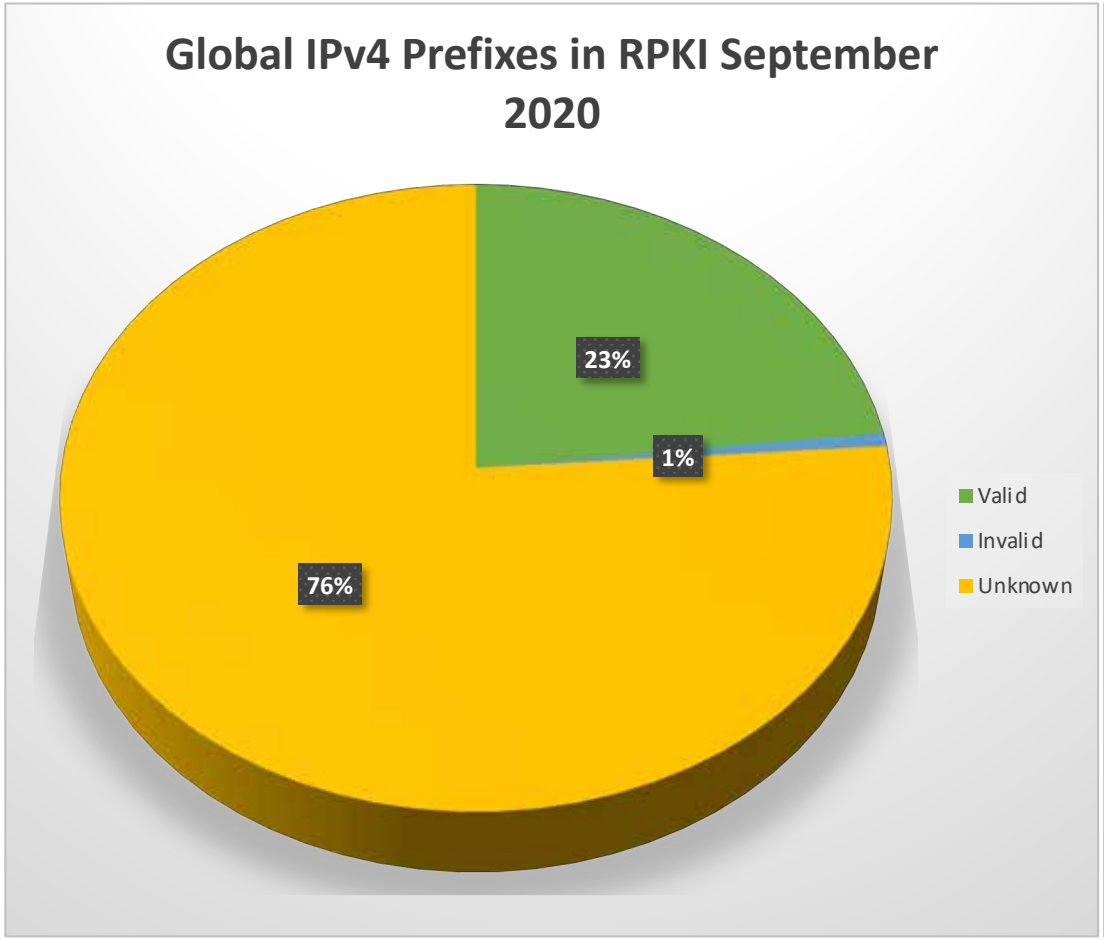
```
45.13.66.0/24,accepted,origin 44684 RPKI status VALID
46.235.224.0/21,accepted,origin 44684 RPKI status VALID
86.63.0.0/18,accepted,origin 60426 RPKI status UNKNOWN. Prefix matched IRR policy.
91.135.0.0/20,accepted,origin 12496 RPKI status UNKNOWN. Prefix matched IRR policy.
91.199.183.0/24,accepted,origin 44697 RPKI status UNKNOWN. Prefix matched IRR policy.
91.244.180.0/24,accepted,origin 199121 RPKI status VALID
93.89.128.0/20,accepted,origin 12496 RPKI status UNKNOWN. Prefix matched IRR policy.
93.93.128.0/21,accepted,origin 44684 RPKI status VALID
109.234.176.0/21,accepted,origin 60426 RPKI status UNKNOWN. Prefix matched IRR policy.
176.126.240.0/21,accepted,origin 44684 RPKI status VALID
185.17.164.0/22,accepted,origin 60426 RPKI status UNKNOWN. Prefix matched IRR policy.
185.47.60.0/22,accepted,origin 44684 RPKI status VALID
185.101.96.0/24,accepted,origin 44684 RPKI status UNKNOWN. matched handles MNT-PETE MA15007-RIPE for 185.101.96.0/24 and 44684
185.106.232.0/24,accepted,origin 45034 RPKI status VALID
185.106.234.0/24,accepted,origin 45034 RPKI status VALID
185.159.24.0/24,accepted,origin 44684 RPKI status VALID
185.203.224.0/24,accepted,origin 208036 RPKI status VALID
193.187.71.0/24,accepted,origin 60217 RPKI status UNKNOWN. Prefix matched IRR policy.
195.10.223.0/24,accepted,origin 44684 RPKI status VALID
212.69.32.0/19,accepted,origin 12496 RPKI status UNKNOWN. Prefix matched IRR policy.
217.144.80.0/20,accepted,origin 12496 RPKI status UNKNOWN. Prefix matched IRR policy.
```

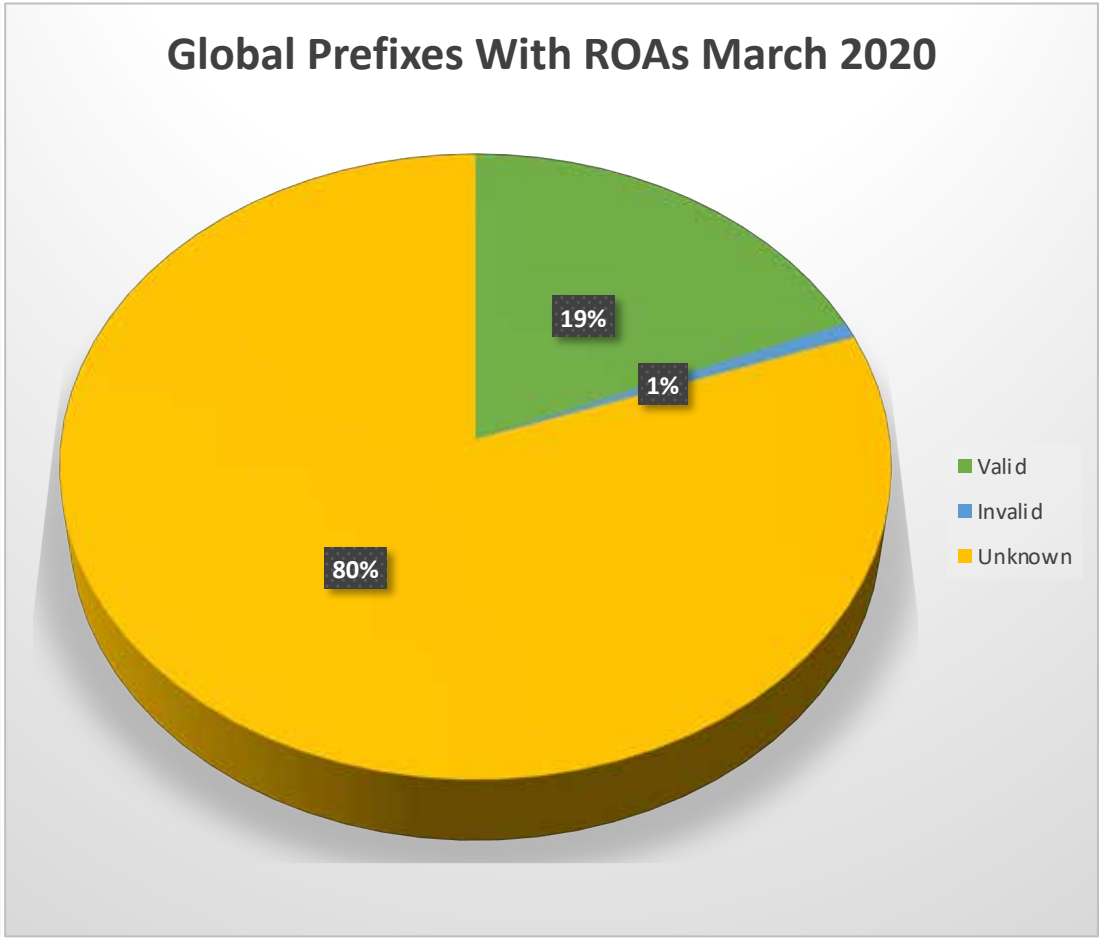
RPKI Lessons Learned

What we learned from our deployment:

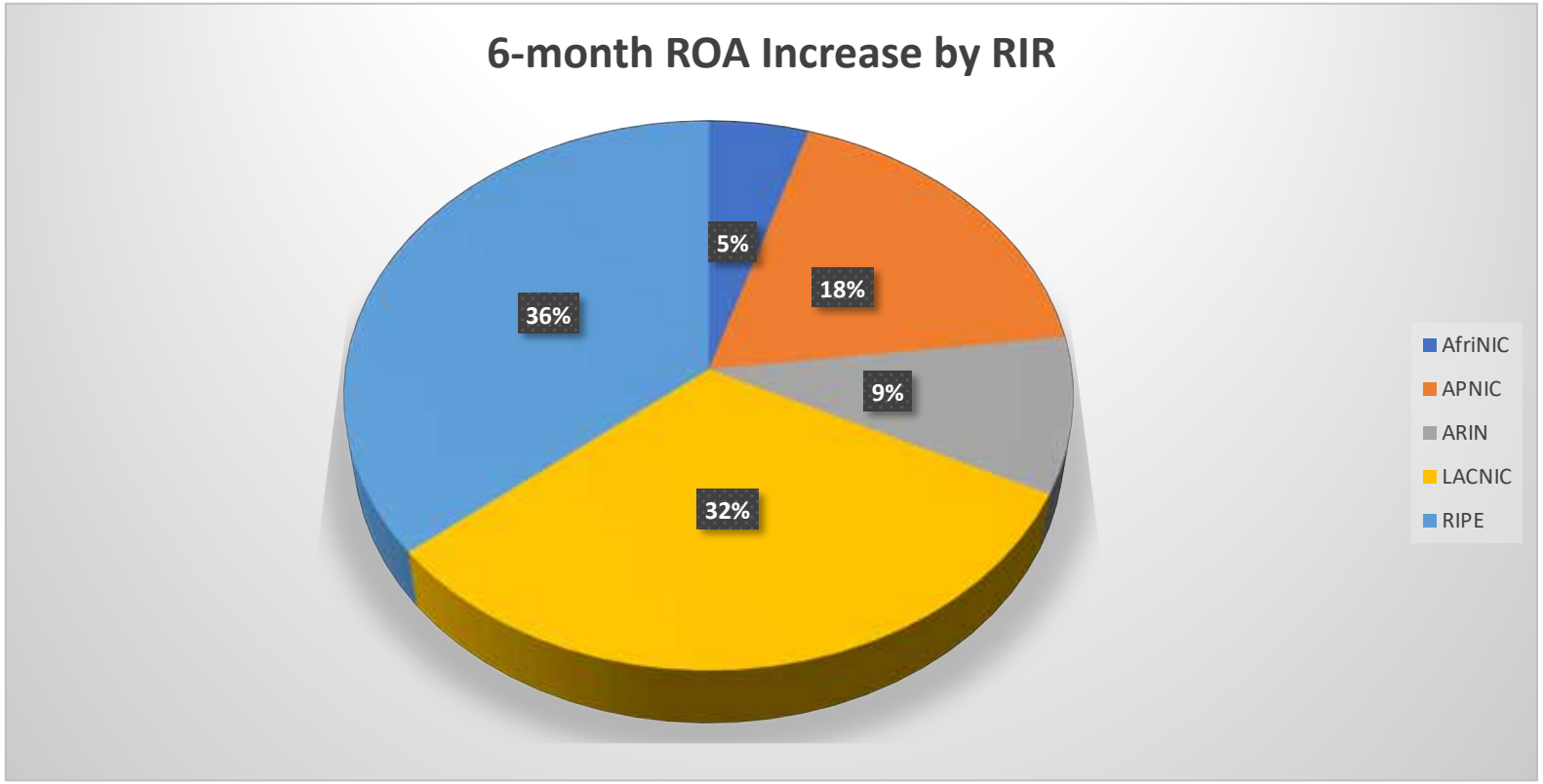
- Frank Sinatra was right: you need to do it your way.
- Getting RPKI right doesn’t help if you don’t have IRR filters right.
- Tools give you an advantage.

The Current State of RPKI

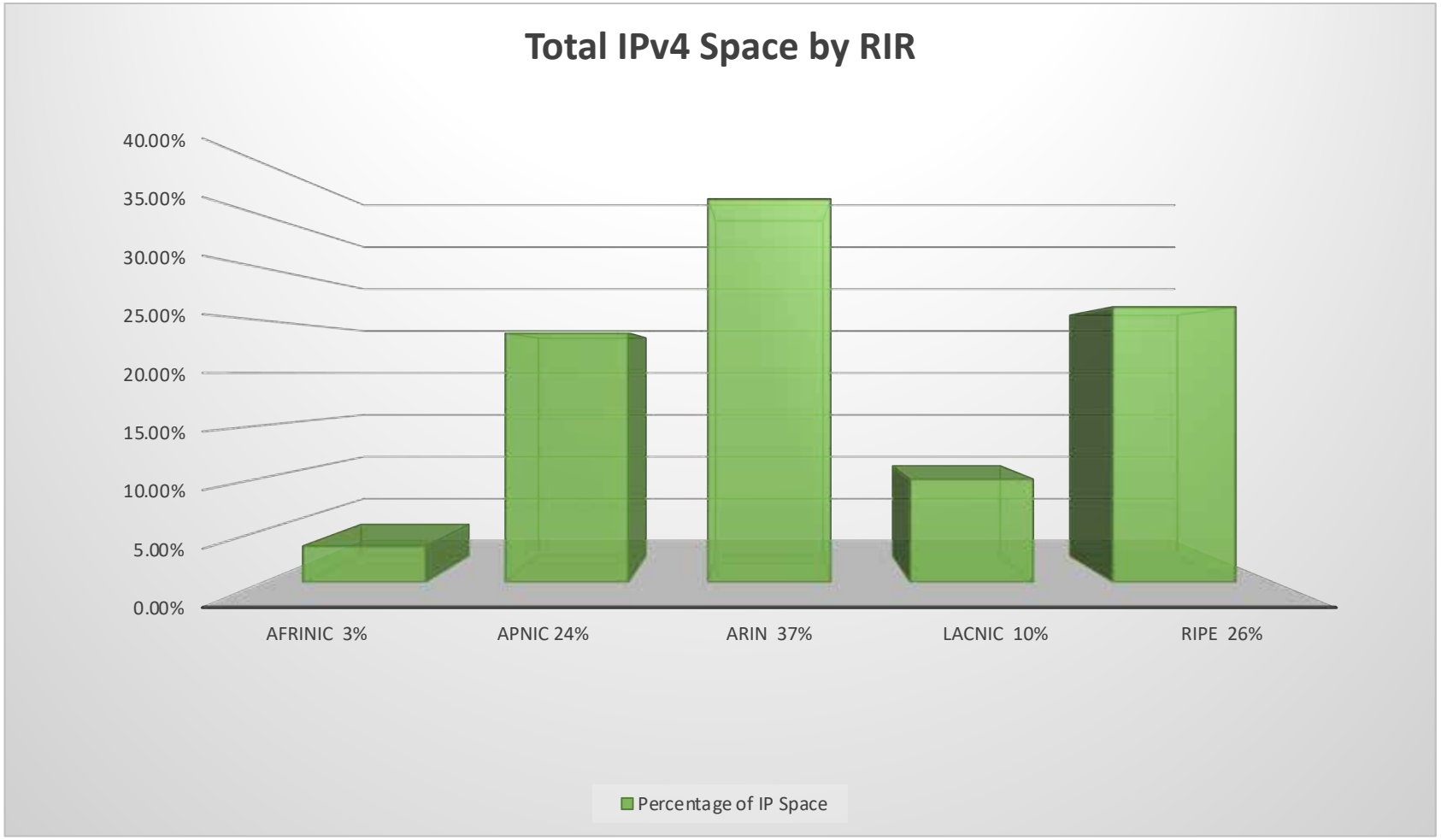




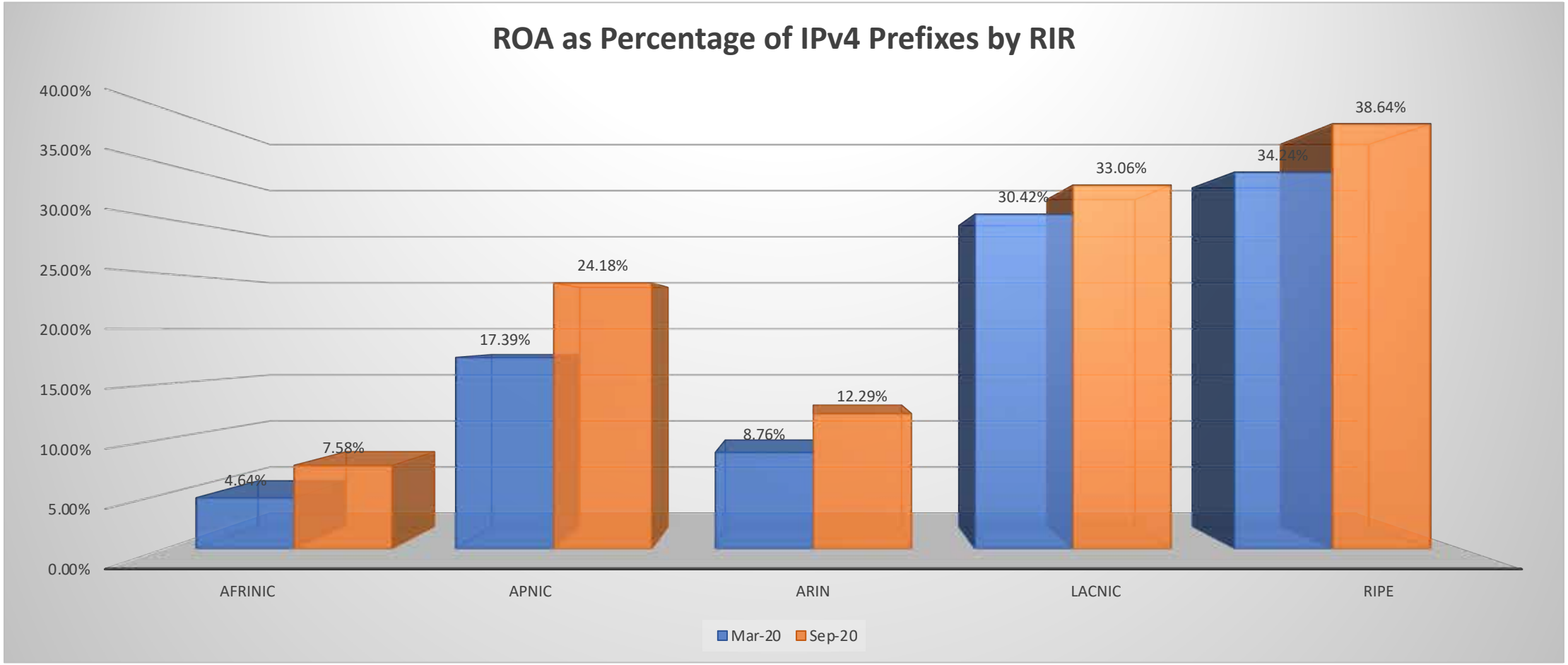
The Current State of RPKI



The Current State of RPKI



The Current State of RPKI



IRR Records: Still the last defense

IRR records are still the only way to validate AS paths.

If you are not already doing this, you should:

- Maintain your IRR records as accurately as you possibly can.
- Filter for bogons.
- Use AS Path filters or Peer Lock.
- Announce all your IP space.
- Set prefix limits.

IRR Records: Still the last defense

Here's what happens when you don't do that:

12 November 2018 Google Route Leak

- Affected Google and a number of other services for 74 minutes.
- The sources was a small, unfiltered ISP that re-advertised about 500 Google prefixes learned from an IX route server.

What could have prevented this?

- RPKI ROAs?
- AS Path filters (peer lock)?
- IRR Path filters?
- Maximum prefix limits?

IRR Records: Still the last defense

Verizon's June 24, 2019 outage.

This was a route leak from a small company with a route optimizer, making this downstream the preferred path of a large quantity of Internet routes transiting Verizon (AS701).

- RPKI ROAs?
- AS Path filters (peer lock)?
- IRR Path filters?
- Maximum prefix limits?

What Could Make Routing More Secure

Today, networks document the ASNs they are authorized to to advertise to other networks, and you have to trust them. A more secure system would have clients identify their providers.

Thank you for your kind attention.

Questions?

Resources

- RPKI Status Data
  https://bgp.he.net

- Routing Filter information
  http://routing.he.net

- Global Prefix/Origin Validation using RPKI
  https://rpki-monitor.antd.nist.gov