Protecting Routing with RPKI

Mark Kosters, ARIN CTO

@TeamARIN

Agenda

- Operational routing challenges
- Do we have a solution?
- Using ARIN's RPKI components
- RPKI Statistics
- IRR Status
- Research Opportunities

Core Internet Functions: Routing & DNS

- The Internet relies on two critical resources
  - DNS: Translates domain names to IP addresses and IP addresses to domain names
  - Routing: Tells us how to get to an IP address
- These critical resources are not secure
- DNSSEC and RPKI secure these critical resources

Operational Routing Challenges

Focus on Interconnections

- Started out as informal arrangements to route address blocks
- Address reachability based on ISP to ISP “trust”
- Moved into contracts
- Moved from a small set of “trustable” ISPs into a worldwide group – some have questionable business practices

Focus on Interconnections (cont'd)

- Technology was incomplete at best to deal with automation to filter
- Misconfigurations/nefarious events on these interconnections have occurred to affect significant parts of the Internet
- IAB Statement on Routing – Routing is based on rumors

Case Study: YouTube

- Pakistan Telecom was ordered to block YouTube
  - Naturally, they originated their own route for YouTube's IP address block
- YouTube's traffic was temporarily diverted to Pakistan

- This incident could have been prevented with widespread adoption of RPKI

Case Study: Turk Telekom

- Turkish President ordered censorship of Twitter
- Turk Telekom's DNS servers were configured to return false IP addresses
  - So people started using Google's DNS (8.8.8.8)
- Turk Telekom hijacked Google's IP addresses in BGP

- Could have been prevented with RPKI

Many More Examples

- Late 2013 & early 2014, Dell Secure Works noticed /24 announcements being hijacked
  - Many networks routed to a small network in Canada
  - Intercepted communications between between Bitcoin miners and Bitcoin data pools
- In April, 2017, AS12389 (PJSC Rostelecom) announced 37 new routes
  - These 37 prefixes belonged to various financial institutions and credit card processors (Visa International, MasterCard Technologies LLC, etc.)

Many More Examples

- In April, 2018, Amazon's Route 53 DNS infrastructure service hijacked
  - Used both BGP and DNS within their attack
  - Traffic to the cryptocurrency website MyEtherWallet.com was redirected to a server hosted in Russia
  - Served up a phishing site to collect private keys to accounts
- In June, 2019, Cloudflare, Amazon, Akamai, etc. sent through AS396531 (a steel plant)
  - Route Optimizer to blame
  - Upstream (Verizon) did not filter the "optimized" routes

Do we have a solution?

Ways that are used today

- Existing Technologies dealing with Routes with the ISP of origin:
  - IRR registries
  - LOAs
  - or just “Seems legit”
- Monitoring BGP Announcements
  - BGPmon, Qrator, Thousand Eyes, etc
- Do we have an alternative?

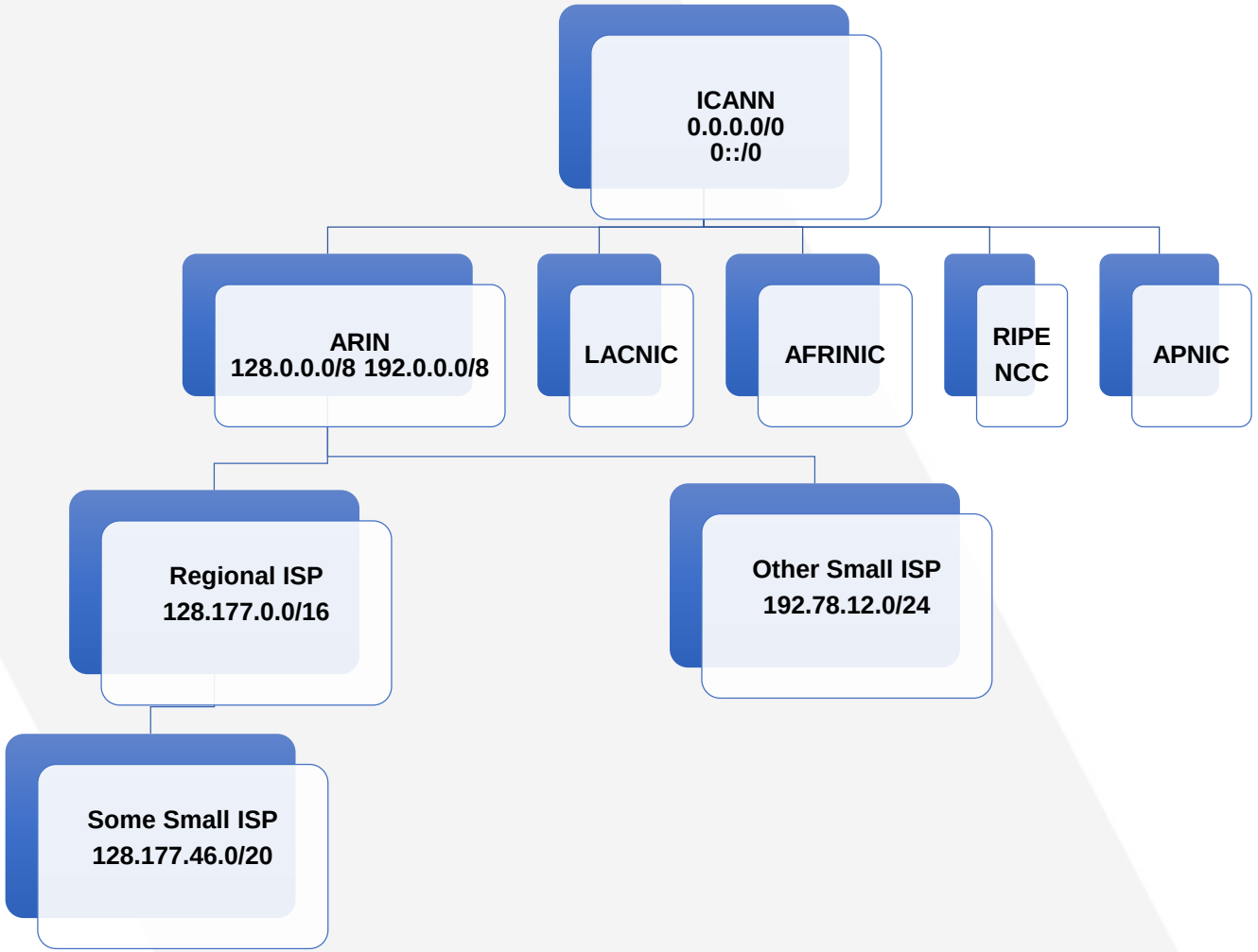
Enter RPKI

- Resource Public Key Infrastructure
- Cryptographically certifies network resources
  - AS Numbers
  - IP Addresses
- Also certifies route announcements
  - Route Origin Authorizations (ROAs) allow you to authorize your block to be routed

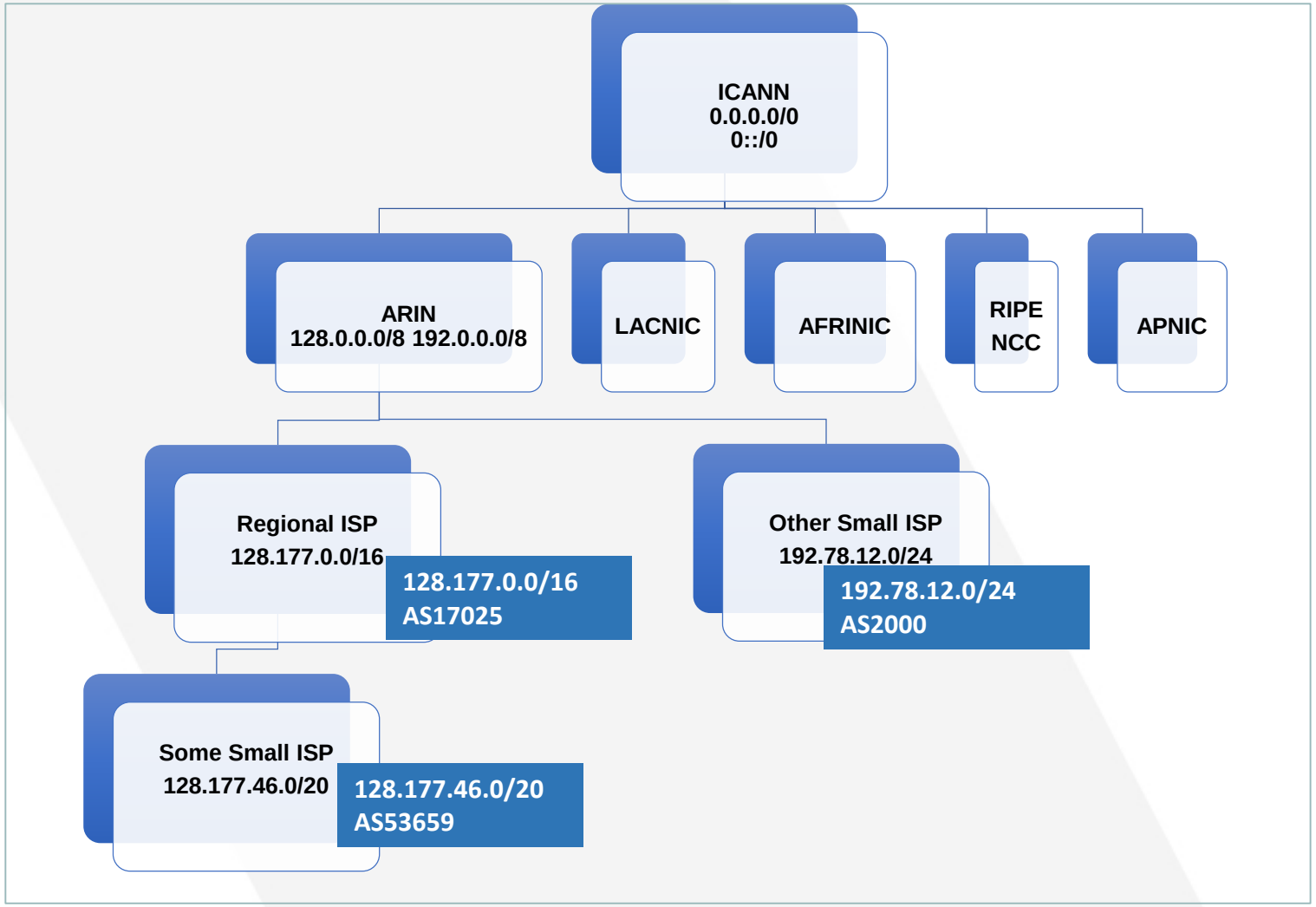
RPKI Basics

- All of ARIN's RPKI data is publicly available in a repository
- RFC 3779 certificates show who has each resource
- ROAs show which AS numbers are authorized to announce blocks
- CRLs show revoked records
- Manifests list all data from each organization

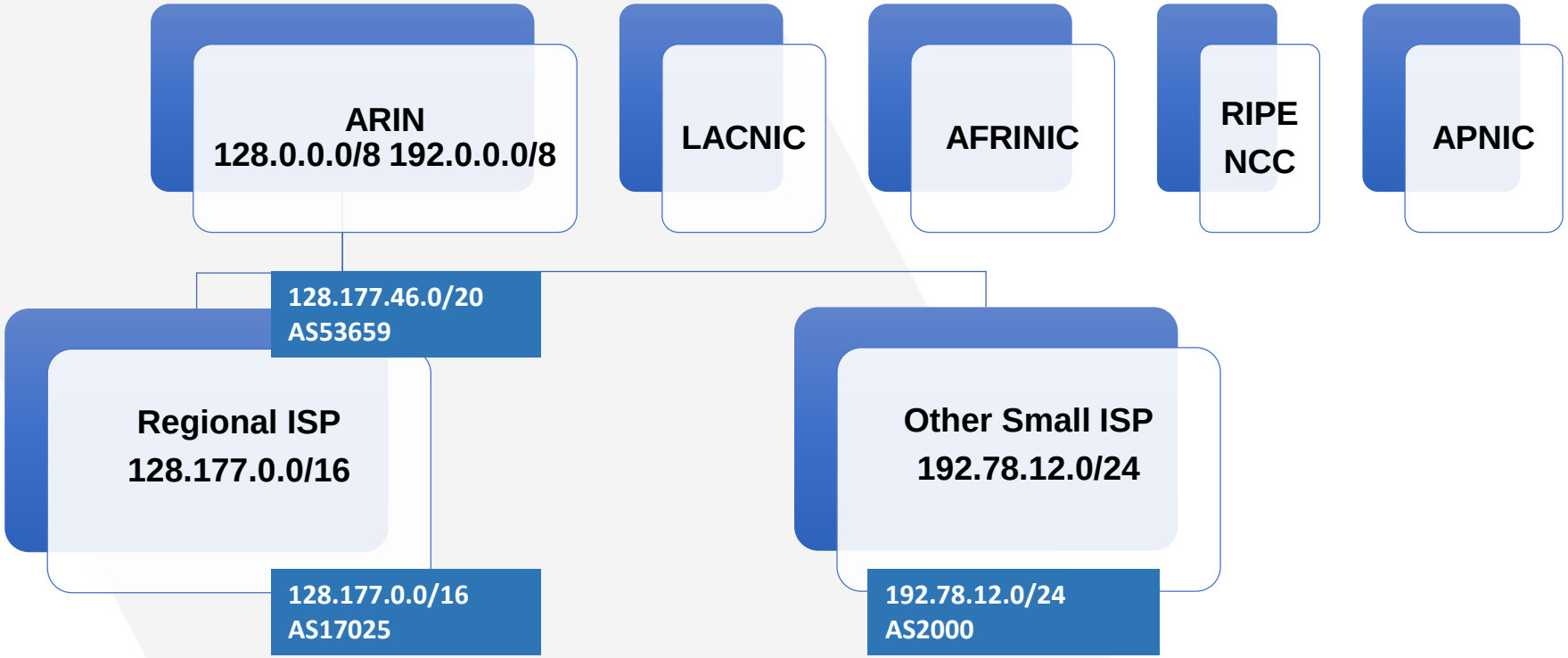
Hierarchy of Resource Certificates



Route Origin Authorizations



Current Practices



Using a RPKI Repository (Theory)

- Pull down these files using a manifest-validating mechanism
- Validate the ROAs contained in the repository
- Communicate with the router to mark routes:
  - Valid
  - Invalid
  - Unknown
- Ultimately, the ISP uses local policy on how to route to use this information.

What does RPKI Protect

- Protects unauthorized origination attacks
  - Stops ISPs to announce routes with a direct AS path to the upstream
- What it does not stop today
  - AS padding
  - Man-in-the-middle route attacks
- RPKI is envisioned to use future technologies to stop these in-path attacks
  - First attempt failed – too complex
  - Second attempt underway using a variant of Secure Origin BGP – ASPA

Steps to use RPKI

- Provision your networks tying your networks to your origin AS
- Fetch and configure a validator
- Look at the results
- Configure your validator to feed these results to your edge routers
- Filter them based on validation rules

Using ARIN's RPKI System

Using ARIN's RPKI Repository

- Provisioning RPKI
- Using RPKI

Provisioning Your Routes in RPKI

- Determine if you want to allow ARIN to host your Certificate Authority (CA), or if you want ARIN to delegate to your Certificate Authority
- Sign up with ARIN Online
- Create Resource Certificates and ROAs

Hosted vs. Delegated RPKI

- Hosted
  - ARIN has done all of the heavy lifting for you
  - Think “point click ship”
  - Available via web site or RESTful interface
- Delegated using Up/Down Protocol
  - A whole lot more work
  - Might make sense for very large networks

Hosted RPKI - ARIN Online

- Pros
  - Easy-to-use web interface
  - ARIN-managed (buying/deploying HSMs, etc. is expensive and time consuming)
- Cons
  - Downstream customers can’t use RPKI
  - Large networks would probably need to use the RESTful interface to avoid tedious management
  - We hold your private key

Delegated RPKI with Up/Down

- Pros
  - Allows you to keep your private key
  - Follows the IETF up/down protocol
  - Allows downstream customers to use RPKI
- Cons
  - Extremely hard to set up
  - Requires operating your own RPKI environment
  - High cost of time and effort

Delegated with Up/Down

- You have to do all the ROA creation
- Need to set up a Certificate Authority
- Have a highly available repository
- Create a CPS

Using ARIN's RPKI Repository

1. Get the RIPE NCC RPKI Validator

Enabled	Trust anchor	Processed Items	Expires in	Last updated	Next update in	Update all
☑	APNIC from AFRINIC RPKI Root	13 1 0	2 years and 11 months	15 minutes ago	Updating ROAs	
☑	APNIC from ARIN RPKI Root	130 1 0	4 years and 8 months	15 minutes ago	Updating ROAs	
☑	APNIC from IANA RPKI Root	2589 1 0	4 years and 8 months	14 minutes ago	Updating ROAs	
☑	APNIC from LACNIC RPKI Root	6 0 0	2 years and 11 months	4 seconds ago	10 minutes	Update
☑	APNIC from RIPE RPKI Root	28 1 0	4 years and 8 months	15 minutes ago	Updating ROAs	
☑	ARIN RPKI Root	1315 3 0	9 years and 7 months	8 minutes ago	2 minutes	Update
☑	AfriNIC RPKI Root	387 0 0	9 years and 11 months	9 minutes ago	1 minute	Update
☑	LACNIC RPKI Root	3446 0 1	5 years and 2 months	5 minutes ago	5 minutes	Update
☑	RIPE NCC RPKI Root	17192 0 0	4 years and 10 months	13 minutes ago	Updating ROAs	

Using ARIN's RPKI Repository

2. Get the ARIN TAL
   - https://www.arin.net/resources/rpki/tal.html

3. Visually validate

Using ARIN's RPKI Repository

4. Plug the validator into your routing policy engine:
   - Directly to the router via RTR protocol
     - Configuration recipes for Junos OS, Cisco IOS, Nokia SR OS at:
       - https://www.ripe.net/manage-ips-and-asns/resource-management/certification/router-configuration
     - Software Solutions
       - BIRD
       - OpenBGPD
       - FRROUTING
       - GOBGP
       - VyOS
- You're now a part of the RPKI ecosystem!

Using ARIN's RPKI Repository – Other Validators

- RIPE is not the the only validator (and this is not an exhaustive list)
  - Dragon Research
    - rpki.net
  - NLNET Routinator
    - https://github.com/NLnetLabs/routinator
  - OpenBSD rpki-client and GoRTR
    - https://github.com/openbsd/src/tree/master/usr.sbin/rpki-client
  - RIPSTR
    - https://github.com/bgpsecurity/rpstir
  - The FORT Project
    - https://fortproject.net
  - RPKI validation services
    - Cloudflare Validates and you get the results
    - https://github.com/cloudflare/gortr

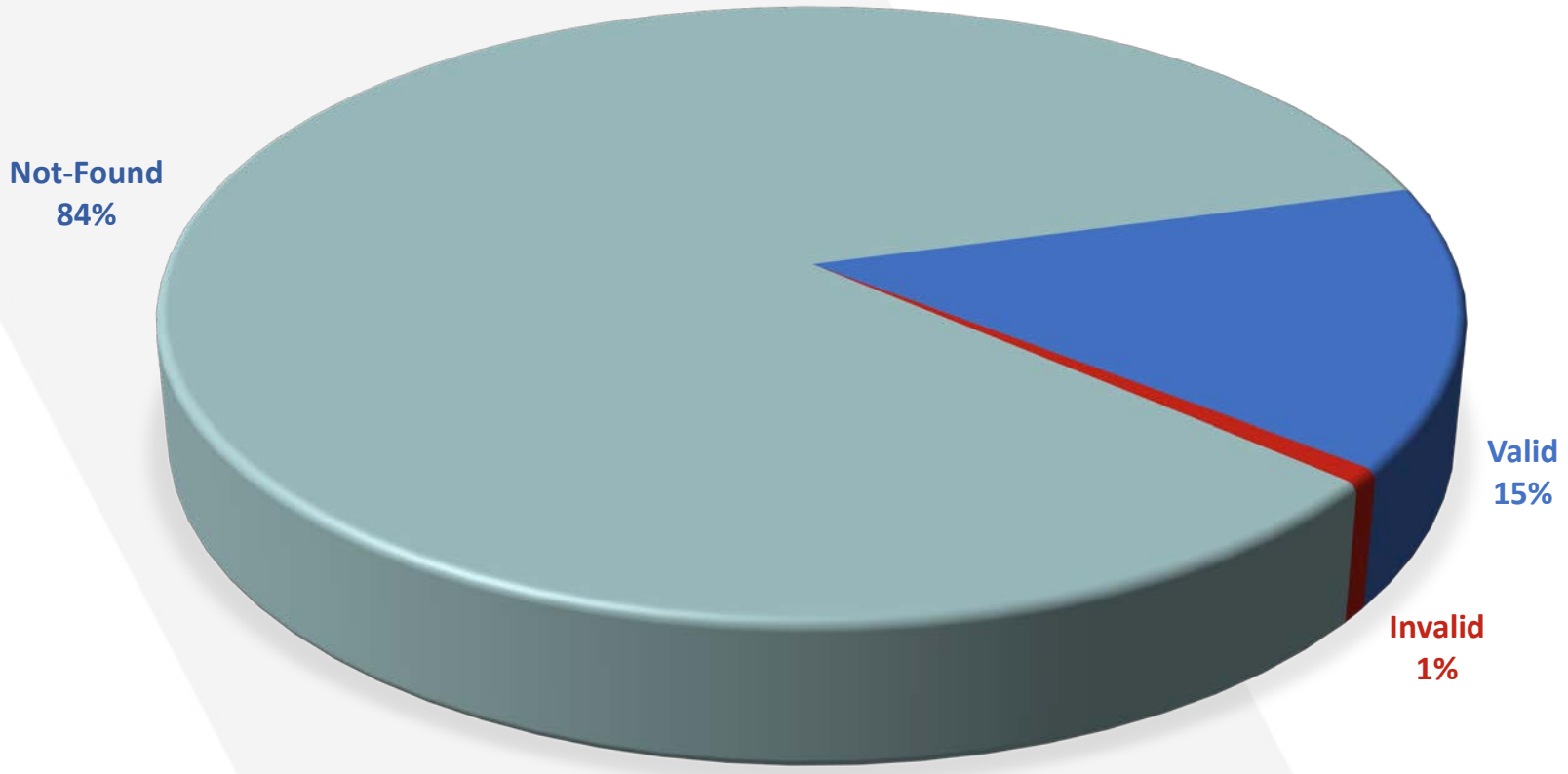
RPKI Statistics

RPKI Usage

	Oct 2012	Apr 2013	Oct 2013	Apr 2014	Oct 2014	Apr 2015	Oct 2015	Apr 2016	Oct 2016	Apr 2017	Oct 2017	Apr 2018	Sep 2018	Apr 2019	Sep 2019
Certified Orgs		47	68	108	153	187	220	250	268	292	328	361	434	591	793
ROAs	19	60	106	162	239	308	338	370	414	470	538	604	1013	4519	5454
Covered Resources	30	82	147	258	332	430	482	528	577	640	741	825	1953	5816	7514
Up/Down Delegated			0	0	0	1	2	1	2	2	2	1	1	1	1

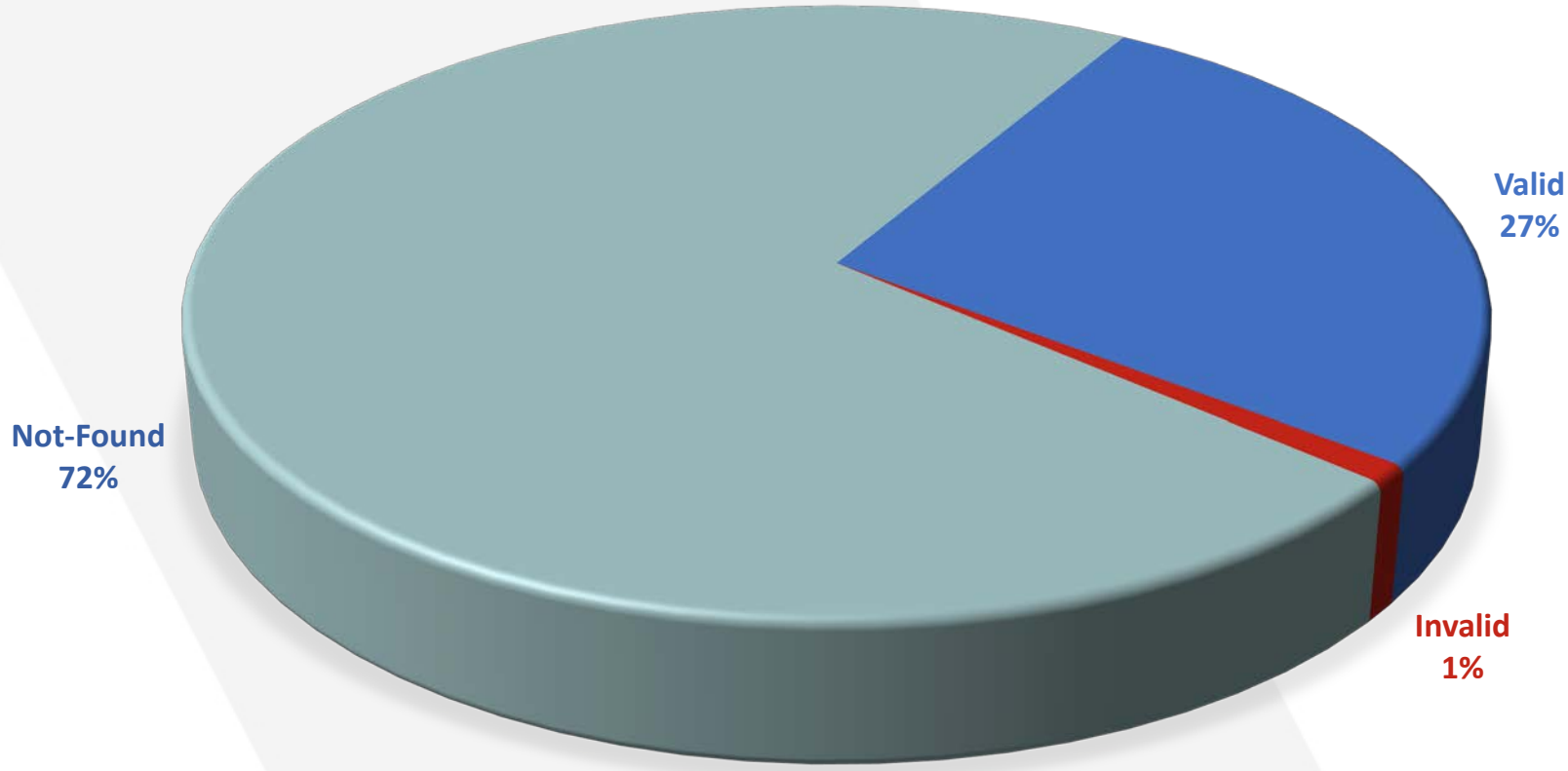
RPKI vs The Routing Table: Global

Global: Validation Snapshot of Unique P/O Pairs
831,319 Unique IPv4 Prefix/ Origin Pairs



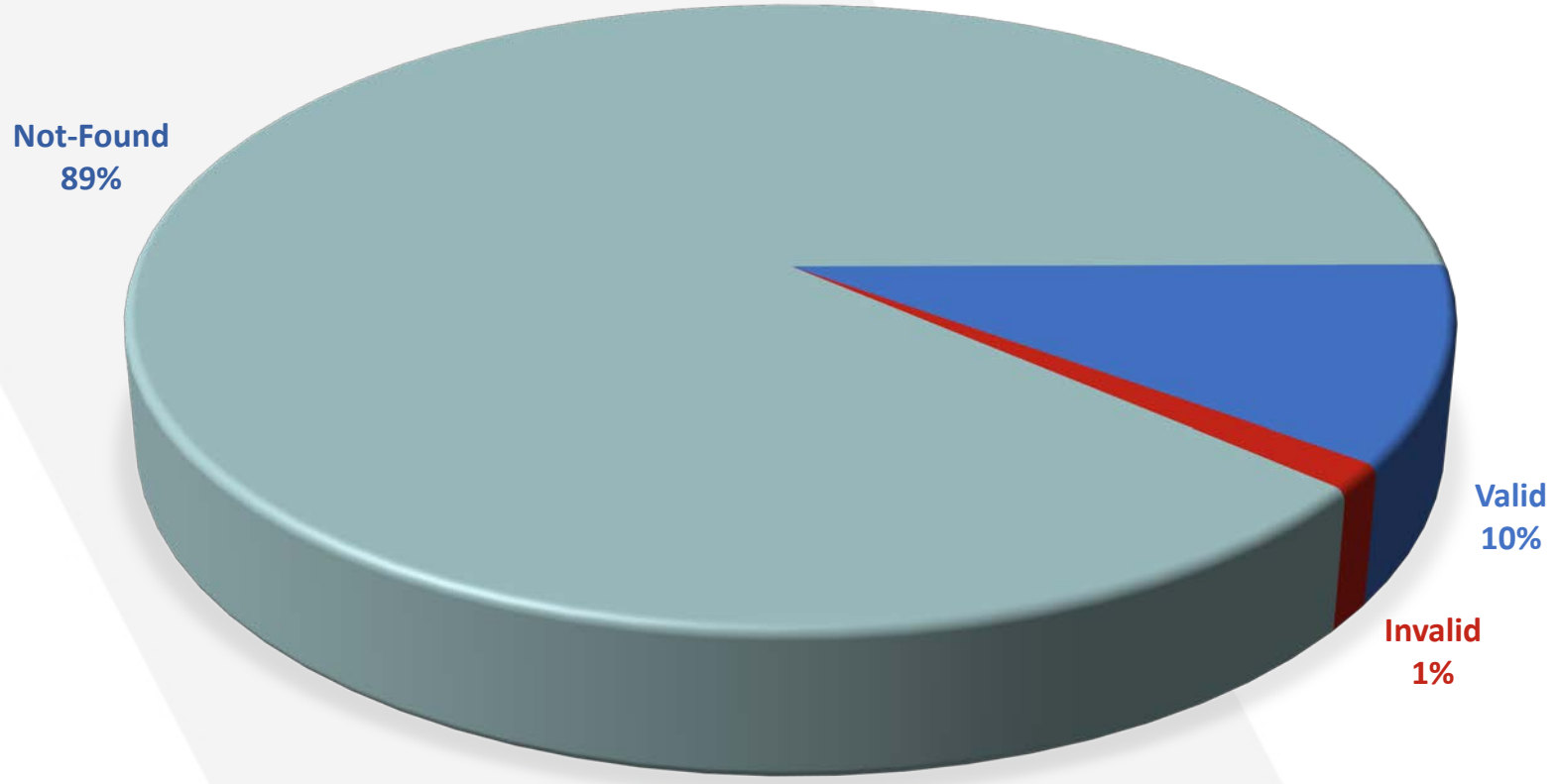
RPKI vs The Routing Table: RIPE

RIPE: Validation Snapshot of Unique P/O Pairs
217,406 Unique IPv4 Prefix/ Origin Pairs



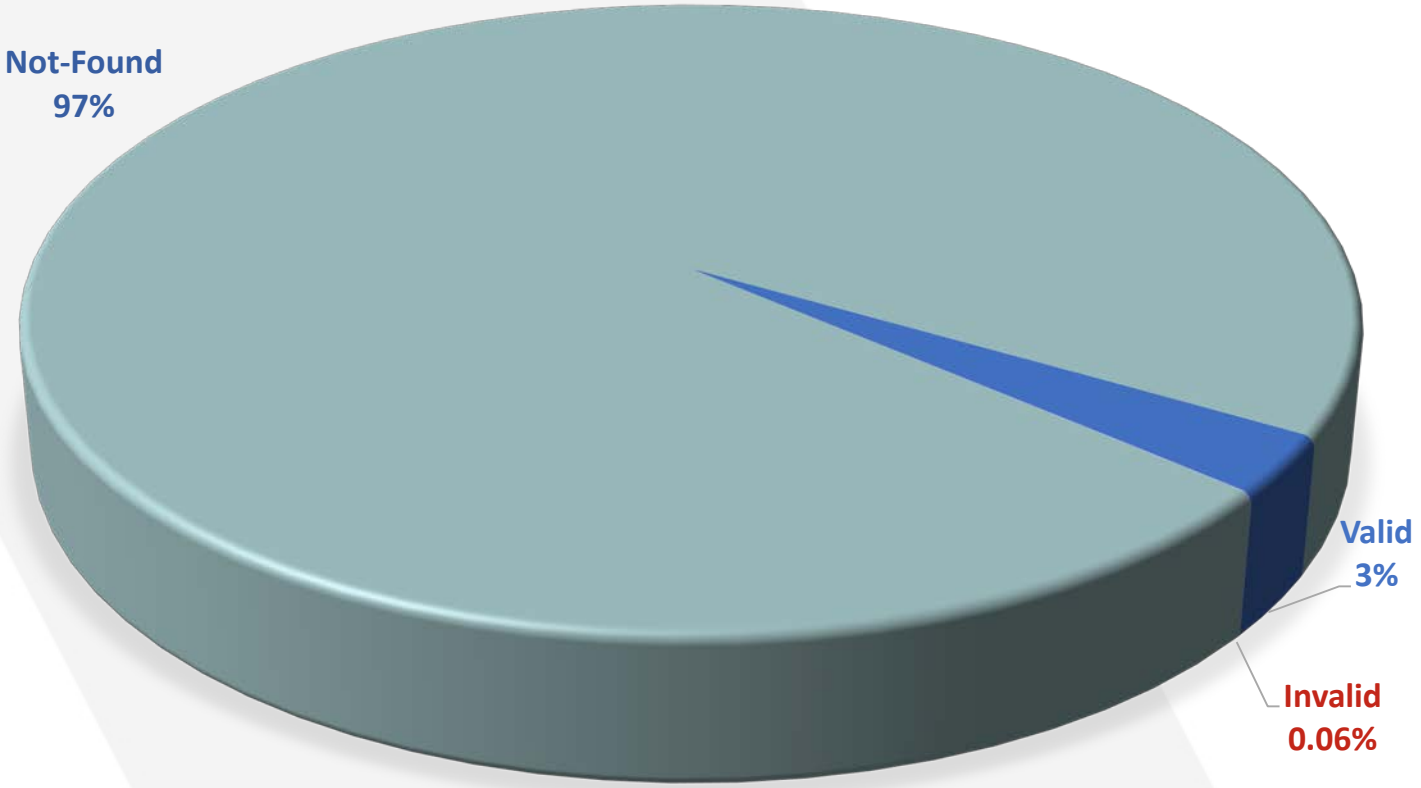
RPKI vs The Routing Table: APNIC

APNIC: Validation Snapshot of Unique P/O Pairs
204,379 Unique IPv4 Prefix/ Origin Pairs



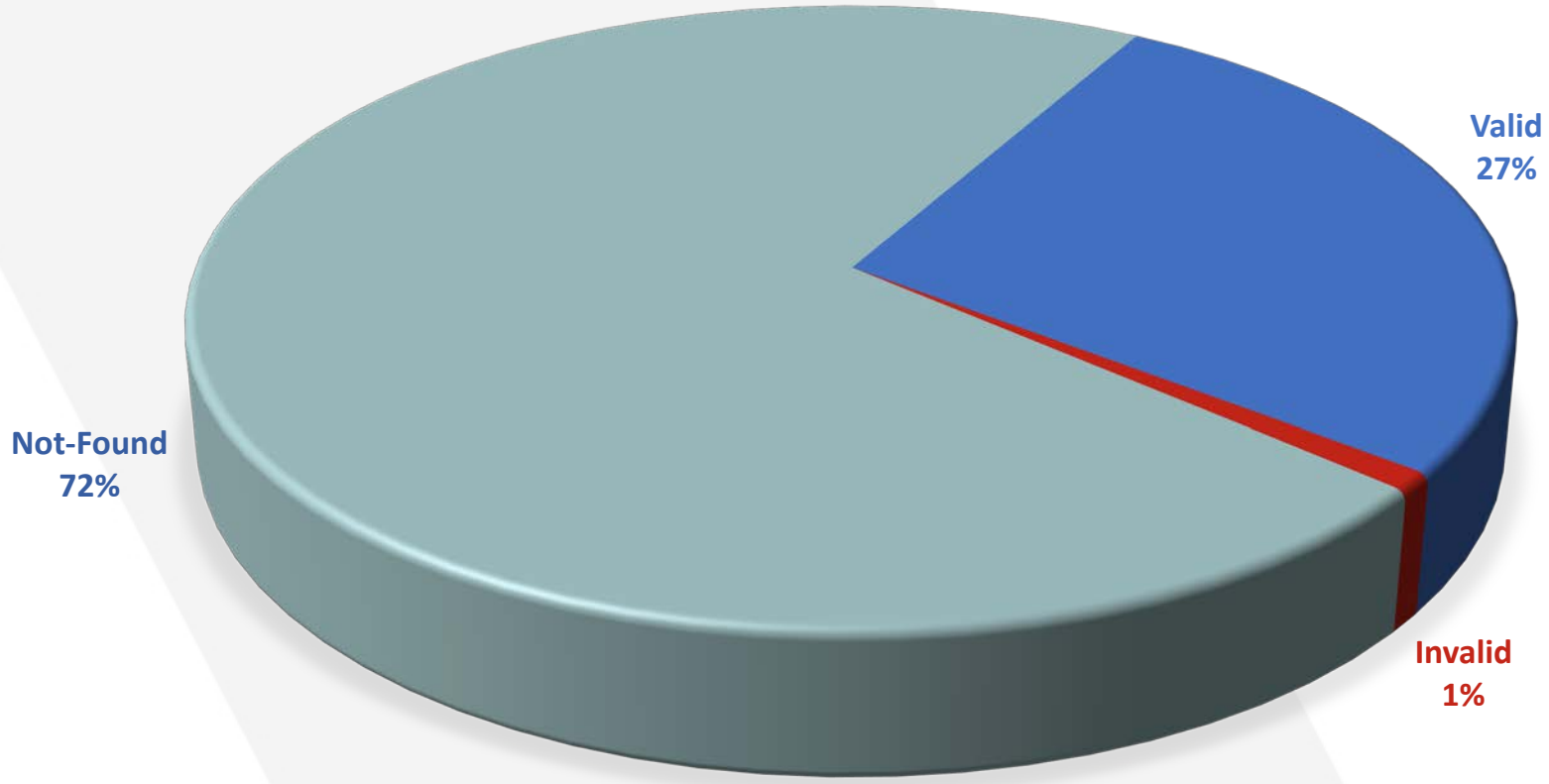
RPKI vs The Routing Table: AFRINIC

AFRINIC: Validation Snapshot of Unique P/O Pairs
27,122 Unique IPv4 Prefix/ Origin Pairs



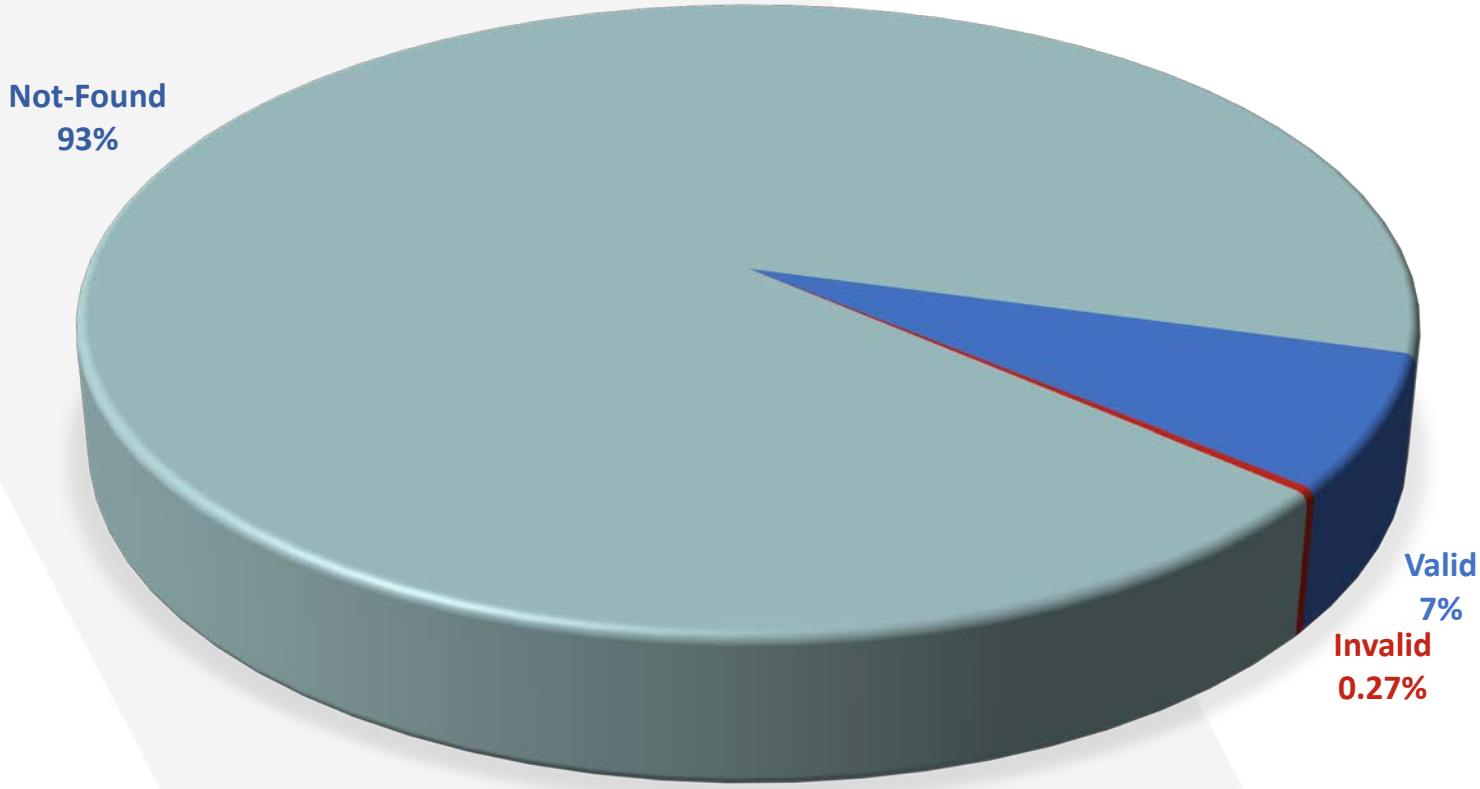
RPKI vs The Routing Table: LACNIC

LACNIC: Validation Snapshot of Unique P/O Pairs
82,587 Unique IPv4 Prefix/ Origin Pairs



RPKI vs The Routing Table: ARIN

ARIN: Validation Snapshot of Unique P/O Pairs
299,822 Unique IPv4 Prefix/ Origin Pairs



Takeaways

- If you're not using RPKI, you're vulnerable to route hijacking
- Plenty of readily available documentation regarding implementation details
- If we can help, contact us

What about the IRR?

RPKI vs IRR

- RPKI could provide closer to real-time route validation
- IRR is mostly used to generate filters
- Maybe use RPKI within IRR for better validation of data
  - https://www.nanog.org/meetings/nanog43/presentations/DanMcP_Route_Filter_Panel_N43.pdf
- Many have strong opinions for/against each approach

IRR

- Been around for decades
  - RIPE-181 published in 1994
  - Varying degree of success
- ARIN's IRR
  - Uses old IRR software from RIPE that is bolted to the side
  - Really showing its age, not customer friendly

IRR Statistics

Number of Organizations	Number of Objects
7	1001-19,574
59	100-1000
6	90-99
9	80-89
12	70-79
19	60-69
22	50-59
654	10-49
798	5-9
1,943	1-4

IRR within the ARIN Region

- There are five suggestions (ACSPs in ARIN-lingo) to improve the IRR
  - Two were completed over the years
- Community Consultation was in favor of upgrading the IRR
- ARIN is in the beginning stages of development

IRR Themes

- Improve the validity of the IRR data
- Work with the other RIR's on authorization schemes
- Provide appropriate proxy registration services
- Integrate/validate with the registration database
- Cross reference RPKI work where appropriate

How is this to be done?

- Work with the community to produce a Simplified Profile of Routing Policy Specification Language (RPSL)
  - Use RESTful services
  - Make it simple
- Collaborate with the other RIR's on cross-authentication
- Provide an easy way to integrate IRR functions within ARIN Online

Research Opportunities

RPKI and IRR Uptake

- We can easily provide provisioning numbers
  - # of ROAS
  - # of route/route6/as-sets/route-sets
- That does not show who is using the system
  - Who is using IRR to generate filters
  - Who is using RPKI to validate/filter routes
- Need to see who is pulling down the data…
  - Look who is fetching from the logs
  - IRR is complicated
    - IRR aggregators
    - Potential downstream cases
    - Multiple ways of getting data -> FTP or NRTM
  - RPKI is a bit easier
    - Look at who is fetching from the repository (validators come directly to the RIR)
    - Wildcard is 3rd party tools like Cloudflare's GoRTR that validates on your behalf

Potential Research Opportunity

- ARIN likes to use 3rd party organizations to send data
  - DNS data -> DNS OARC
- Those orgs vet the researchers – not ARIN
- Many of the privacy issues are taken care by these orgs.
- Where is a good place for this data to be housed?

ANY QUESTIONS ?