Measuring RPKI deployment in the DNS

A Deployment Study Focusing on a Specific Use

Edward Lewis

NANOG 89
17 October 2023

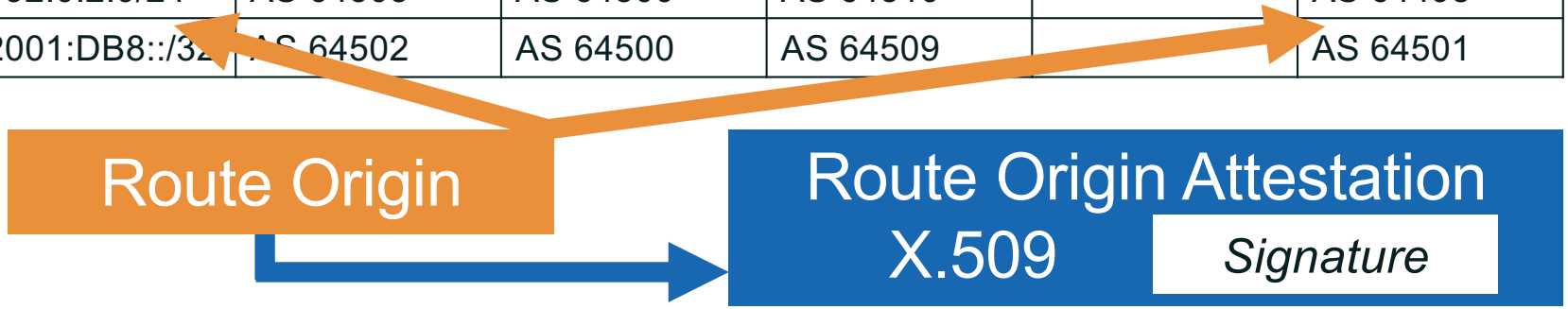
Layout of the talk

- Why would DNS operators think about routing security?
  - Why expect to see RPKI adoption?
- Are DNS operators deploying RPKI?
  - In the DNS core (root, TLDs, reverse map)
  - Below the commercial registration boundary
- What can we take away from the measurements?

ROAs = Route Origination Authorization

- RPKI is a Public Key Infrastructure framework deployed to secure BGP against invalid or unauthorized route announcements
  - ROA stands for Route Origination Authorization is a cryptographic attestation that the ASN is authorized to originate a network prefix

IP Prefix	Next ASN	Another ASN	Another ASN	...	Last Hop ASN
192.0.2.0/24	AS 64502	AS 64500	AS 64510		AS 64501
192.0.2.0/24	AS 64505	AS 64500	AS 64510		AS 64498
2001:DB8::/32	AS 64502	AS 64500	AS 64509		AS 64501



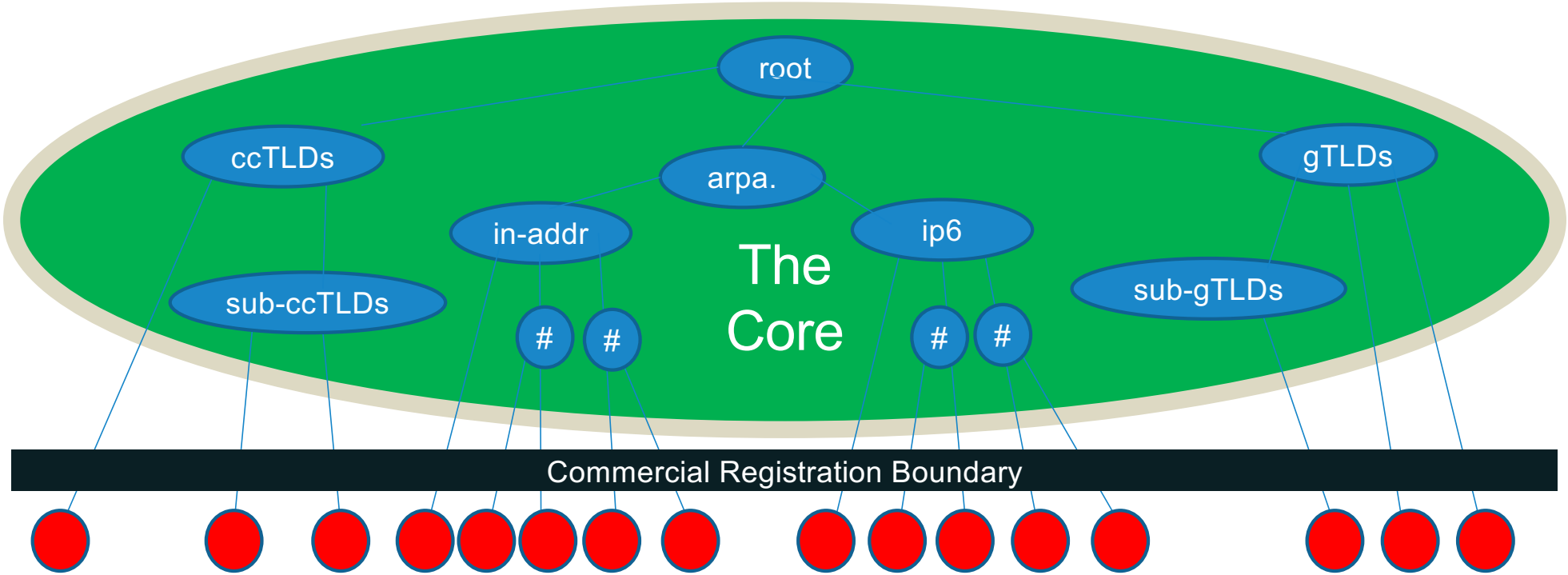
The Role Routing Security Plays in DNS Operations

- DNS publishes information on servers, routes lead to them
  - Securing the routing system improves the reliability and availability of servers
  - Providing route origin attestations (ROA) as part of RPKI is one way to provide security meta-data
- Validating route advertisements is not as critical to name server service
  - Basic enterprise security is the goal

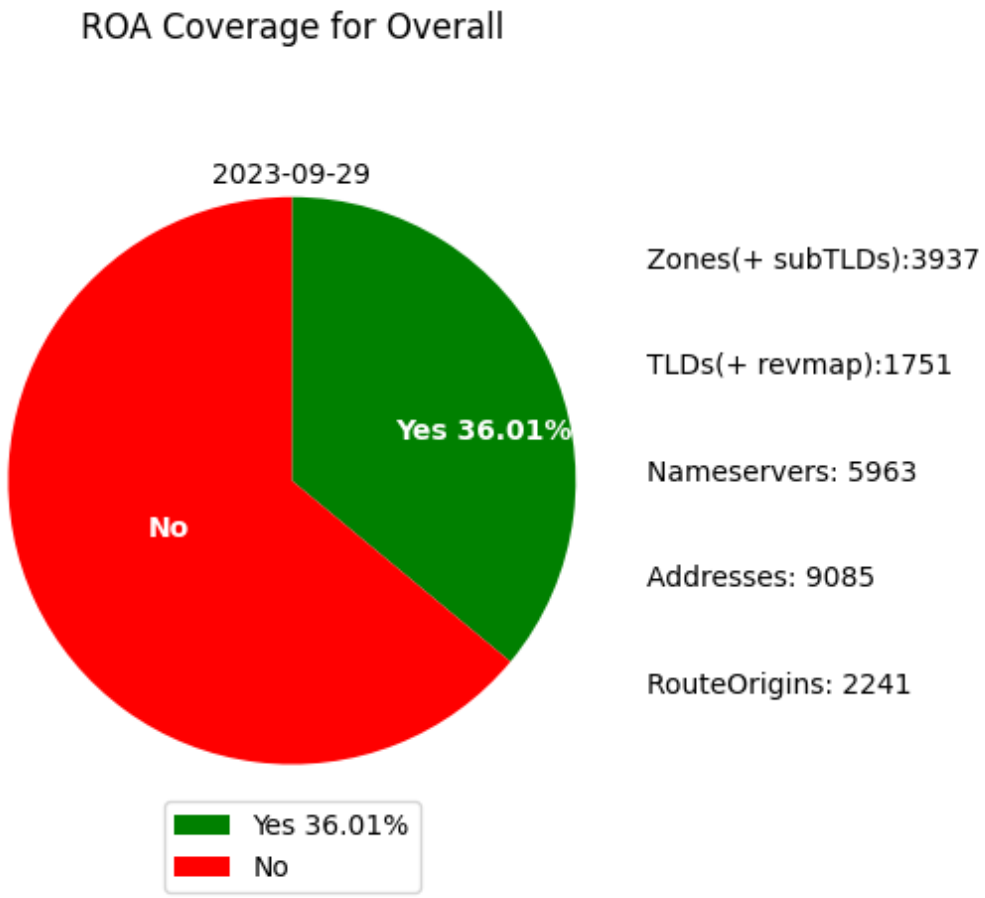
Measurement Method

- For a collection of zones
  - For each zone, find…
    - For each nameserver, find…
      - For each address, find…
        - For each route origination look for a ROA
  - Relying on Team Cymru's *IP to ASN mapping service*
- Does the route origination have a validated ROA?
  - Yes/No, percentages are `"Yes"/("Yes"+"No")`
  - Being careful to avoid double counting, i.e., routes shared by zones
  - Tossing error cases out

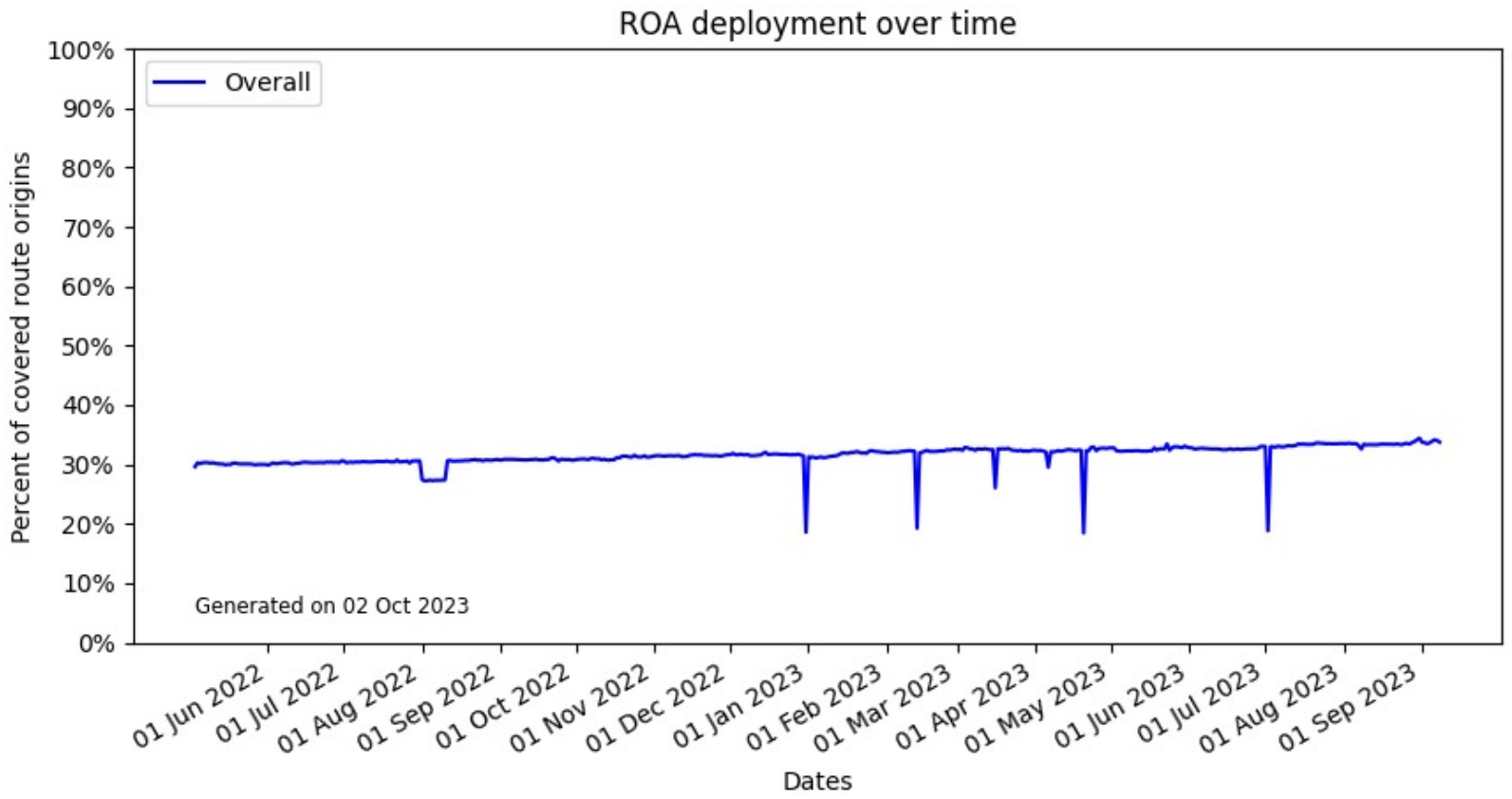
The DNS Core and Commercial Registration Boundary



Overall ROA Coverage for DNS Core



Overall ROA Coverage (DNS Core) Trend

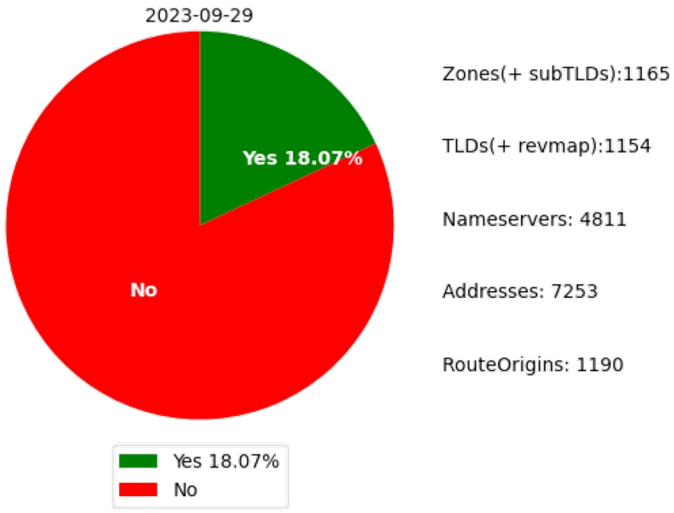


Looking Deeper into the DNS Core

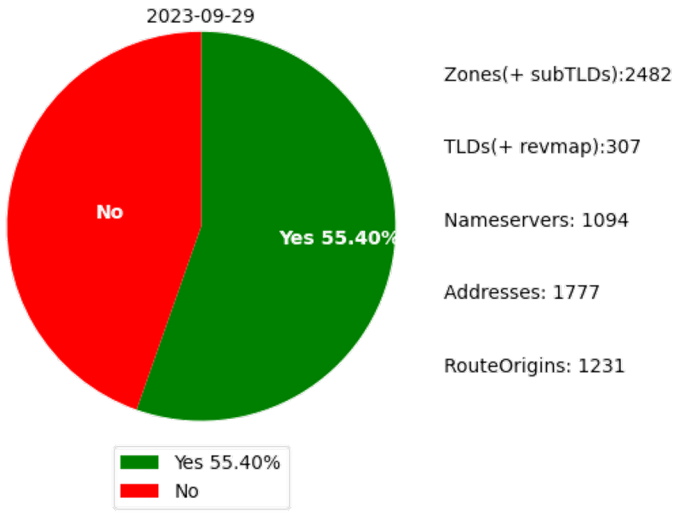
- For this to be helpful
  - Would be good to identify patterns
  - Does deployment follow any structure of the DNS?
- gTLDs, ccTLDs, and the reverse map zones
  - Each category is structured different
  - Other measurements show differences in operations
- And then look below that level

ccTLD / gTLD / Reverse Map

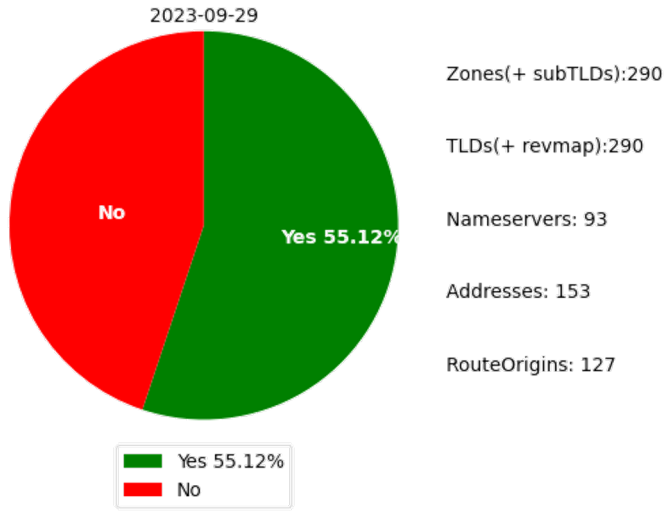
ROA Coverage for gTLD



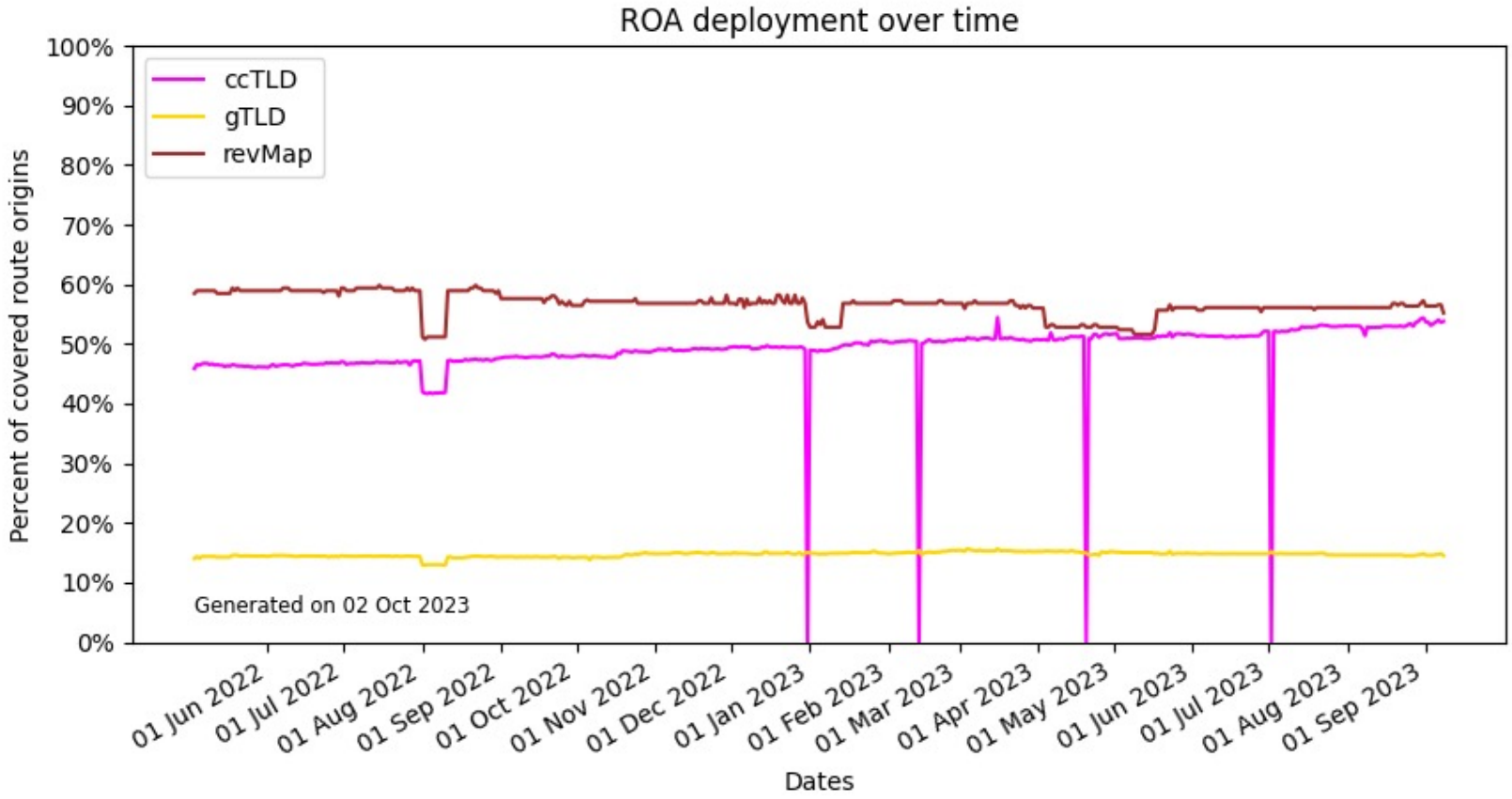
ROA Coverage for ccTLD



ROA Coverage for revMap



ccTLD / gTLD / Reverse Map (trends)



That revMap adoption seems lower than expected

- It’s good to question data that does not match expectations
- revMap includes more zones than those operated by the RIRs
  - 8 legacy “class A’s” and historical exceptions in the “B and C ranges”
  - Some IPv6 delegations were made straight to LIRs
- Within the RIR’s, all but one NS resource record’s pair of IPv4/IPv6 addresses are covered, with that pair accounting for 8 route origins.

Adoption within gTLDs

- This began with an invited measurement of a ccTLD
  - It's ROA coverage was around 4%
- Ran the same measurement for 14 selected gTLDs
  - Different sizes, from 1.7 million delegations to 2,400 delegations
  - Compared Traditional to IDN
- Results…

RPKI coverage metrics

- Withholding the gTLD names
  - The 1.2 M zone is a class-of-2000 gTLD
  - The 109 K zone is a class-of-2004 regional gTLD
  - Rest are class-of-2012 gTLD

Delegations	Route Origins	Valid ROAs	RPKI Rate
1,691,583	5,094	228	4.48%
1,294,099	20,044	917	4.57%
731,274	4,659	169	3.63%
426,400	2,189	94	4.29%
292,068	1,797	44	2.45%
109,887	2,979	128	4.30%
94,715	5,614	247	4.40%
2,733	700	13	1.86%
2,347	3,451	127	3.68%

Traditional gTLDs vs. IDN-gTLDs

- Withholding the gTLD name
  - Comparing the largest IDN gTLDs with comparable sized non-IDN gTLDs

Type	Delegations	Route Origins	Valid ROAs	RPKI Rate
ASCII	94,715	5,614	247	4.40%
IDN	91,736	555	9	1.62%
ASCII	28,671	2,967	140	4.72%
IDN	28,826	559	16	2.86%
ASCII	27,821	3,451	127	3.68%
IDN	28,297	700	13	1.86%

Who makes deployment decisions?

Category	Full Adoption (=100%)	Mixed (>0%, <100%)	No Adoption (=0%)
Zone Operators	98	145	27
Aut-Num Holders	253	38	195
IP Holders	296	17	183

- Percent is number of ROA'd route origins/all route origins
- Began the study as a measure of DNS adoption of RPKI
- RPKI isn't a DNS decision, looks like it's a routing decision
  - This should not have been a surprise!

Is there Meaning to This?

- The DNS Core ~36%
  - gTLDs ~18%, revMap ~55% steady, ccTLDs ~55% with a slight climb
- Commercial Registration Boundary
  - gTLDs ~4%, IDN-gTLDs ~2%, no data on ccTLDs
  - With commercial DNS hosting being independent of TLD, consistency in the deployment numbers isn't too surprising

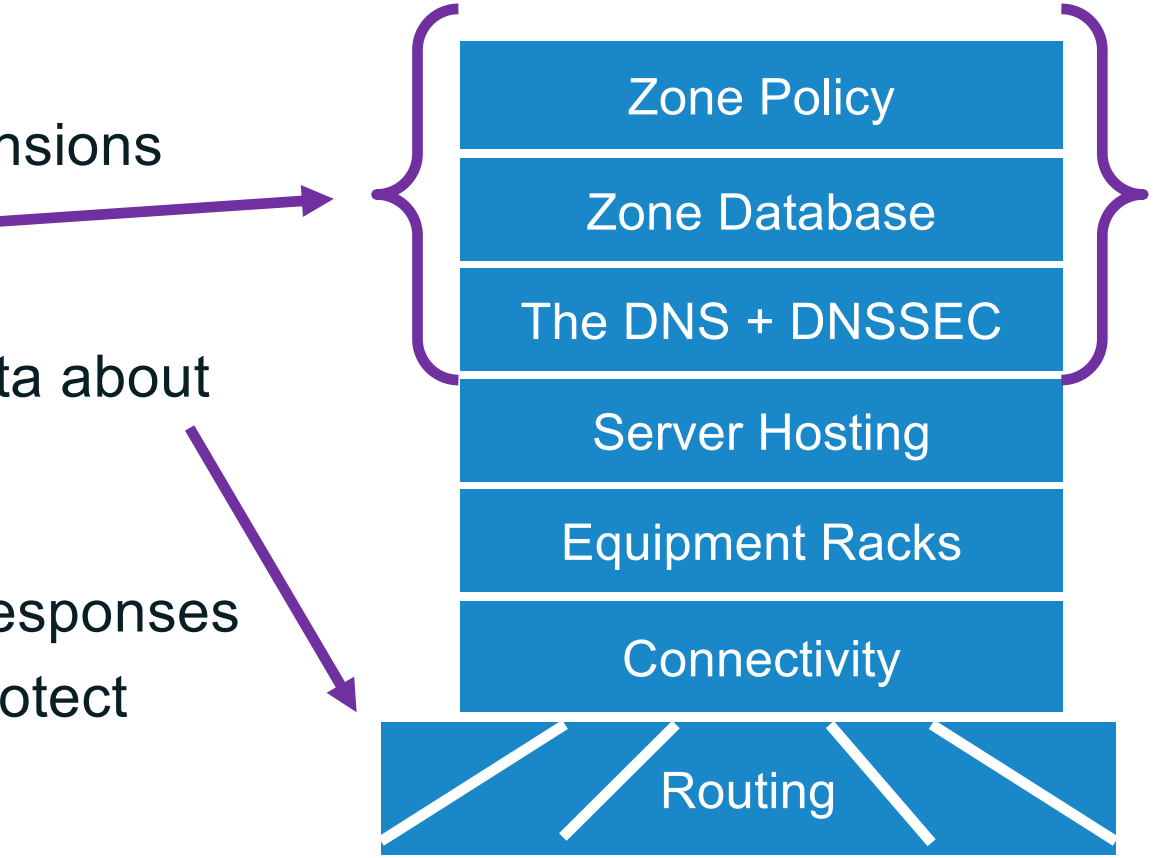
- The adoption rates seem a bit low
  - Seem as in, the numbers are small, but are they meaningful?

Searching for Significance

- This isn’t much data, maybe compare to DNSSEC for context
  - I have more familiarity with DNSSEC’s history
  - Adoption of DNSSEC has gone on for 25 years

Relationship of RPKI, ROAs and DNSSEC

- DNSSEC is a set of extensions helping secure DNS
- RPKI / ROA are meta-data about routes
- DNSSEC helps protect responses
- Routing security helps protect queries+responses

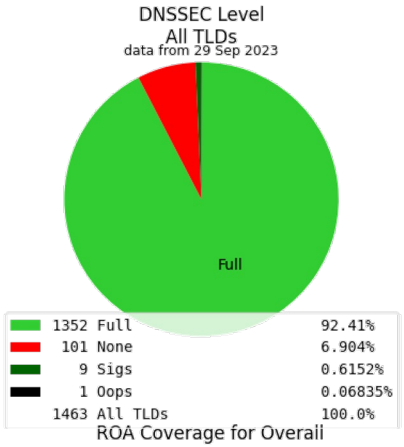


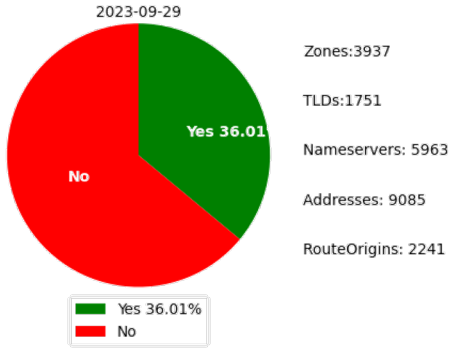
DNSSEC and RPKI

- They are similar:
  - Based on digital signatures
  - Use a hierarchy for scale
  - Administrator of the data signs – makes the signature
  - User/receiver verifies the signature
- They are different:
  - DNSSEC deployment 25 years+, my data on RPKI ~4 years
  - What they cover (DNS data vs. routing announcements)
  - Data structures (DNS protocol vs. X.509 certificates)
  - Key management operations

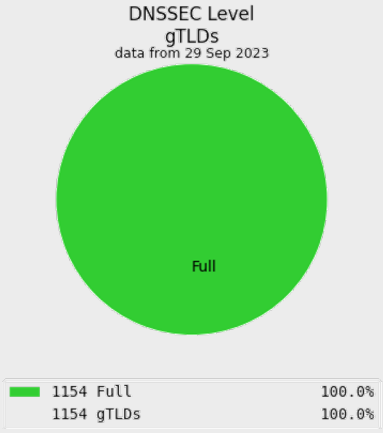
DNSSEC & RPKI coverage metrics (Core)

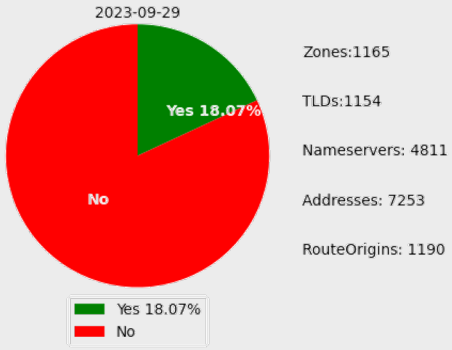
All TLDs



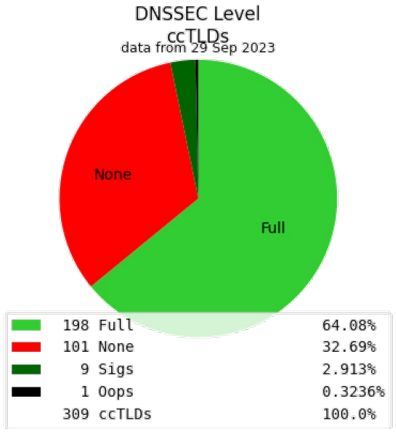


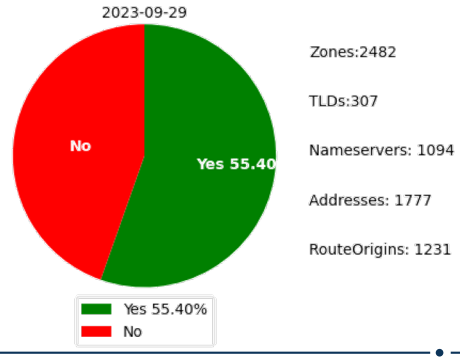
gTLDs





ccTLDs





Note: DNSSEC, all TLDs=gTLDs+ccTLDs; RPKI all TLDs=gTLDs+ccTLDs+revMap

DNSSEC & RPKI coverage metrics (Commercial Registration)

- Withholding the gTLD names
  - The 1.2 M zone is a class-of-2000 gTLD
  - The 109 K zone is a class-of-2004 regional gTLD
  - Rest are class-of-2012 gTLD

Delegations	With DS	DNSSEC Rate	Route Origins	Valid ROAs	RPKI Rate
1,691,583	22,472	1.33%	5,094	228	4.48%
1,294,099	42,049	3.25%	20,044	917	4.57%
731,274	2,188	0.30%	4,659	169	3.63%
426,400	1,050	0.25%	2,189	94	4.29%
292,068	581	0.20%	1,797	44	2.45%
109,887	8,751	7.96%	2,979	128	4.30%
94,715	6,085	6.42%	5,614	247	4.40%
2,733	152	5.56%	700	13	1.86%
2,347	2,346	99.96%	3,451	127	3.68%

DNSSEC & RPKI coverage metrics (CommReg IDN comps)

- Withholding the gTLD name
  - Comparing the largest IDN gTLDs with comparable sized non-IDN gTLDs

Type	Delegations	Names with DS	DNSSEC Rate	Route Origins	Valid ROAs	RPKI Rate
ASCII	94,715	6,085	6.42%	5,614	247	4.40%
IDN	91,736	8	0.01%	555	9	1.62%
ASCII	28,671	1,503	5.24%	2,967	140	4.72%
IDN	28,826	6	0.02%	559	16	2.86%
ASCII	27,821	678	2.44%	3,451	127	3.68%
IDN	28,297	1	0.00%	700	13	1.86%

Commentary

- Using any adjectives is risky with a small sample set, but
  - DNSSEC coverage is much more variable, TLD to TLD than RPKI
    - Seems zone admins, on average, are more aware of DNSSEC than RPKI
  - IDN gTLDs are substantially different in coverage from ASCII gTLDs
    - DNSSEC is scant, RPKI is half (2%)
    - Law of small numbers? Maybe, but these are the largest IDN gTLDs
- Nonetheless – these deployment numbers are low!

My Reaction

- Operators have spoken:
  - These technologies are just not being deployed
- What prevents an operator from deploying?
  - It can’t simply be “more training” or “more promotion” is needed
- What would make security enhancements operations-friendly?
  - I’d like to learn from operators what they feel is needed

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: edward.lewis@icann.org

@icann

linkedin/company/icann

facebook.com/icannorg

slideshare/icannpresentations

youtube.com/icannnews

soundcloud/icann

flickr.com/icann

instagram.com/icannorg