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

<table>
<thead>
<tr>
<th>IP Prefix</th>
<th>Next ASN</th>
<th>Another ASN</th>
<th>Another ASN</th>
<th>...</th>
<th>Last Hop ASN</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.0.2.0/24</td>
<td>AS 64502</td>
<td>AS 64500</td>
<td>AS 64510</td>
<td></td>
<td>AS 64501</td>
</tr>
<tr>
<td>192.0.2.0/24</td>
<td>AS 64505</td>
<td>AS 64500</td>
<td>AS 64510</td>
<td></td>
<td>AS 64498</td>
</tr>
<tr>
<td>2001:DB8::/32</td>
<td>AS 64502</td>
<td>AS 64500</td>
<td>AS 64509</td>
<td></td>
<td>AS 64501</td>
</tr>
</tbody>
</table>

Route Origin

Route Origin Attestation X.509 Signature
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

- ccTLDs
- sub-ccTLDs
- arpa.
- in-addr
- ip6
- sub-gTLDs
- gTLDs

The Core

Commercial Registration Boundary
Overall ROA Coverage for DNS Core

ROA Coverage for Overall

2023-09-29

Yes 36.01%

No

Zones (+ subTLDs): 3937
TLDs (+ revmap): 1751
Nameservers: 5963
Addresses: 9085
RouteOrigins: 2241
Overall ROA Coverage (DNS Core) Trend

ROA deployment over time

Generated on 02 Oct 2023
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
- 2023-09-29: Yes 18.07%
  - Zones (+ subTLDs): 1165
  - TLDs (+ revmap): 1154
  - Nameservers: 4811
  - Addresses: 7253
  - RouteOrigins: 1190

ROA Coverage for ccTLD
- 2023-09-29: Yes 55.40%
  - Zones (+ subTLDs): 2482
  - TLDs (+ revmap): 307
  - Nameservers: 1094
  - Addresses: 1777
  - RouteOrigins: 1231

ROA Coverage for revMap
- 2023-09-29: Yes 55.12%
  - Zones (+ subTLDs): 290
  - TLDs (+ revmap): 290
  - Nameservers: 93
  - Addresses: 153
  - RouteOrigins: 127
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

<table>
<thead>
<tr>
<th>Delegations</th>
<th>Route Origins</th>
<th>Valid ROAs</th>
<th>RPKI Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,691,583</td>
<td>5,094</td>
<td>228</td>
<td>4.48%</td>
</tr>
<tr>
<td>1,294,099</td>
<td>20,044</td>
<td>917</td>
<td>4.57%</td>
</tr>
<tr>
<td>731,274</td>
<td>4,659</td>
<td>169</td>
<td>3.63%</td>
</tr>
<tr>
<td>426,400</td>
<td>2,189</td>
<td>94</td>
<td>4.29%</td>
</tr>
<tr>
<td>292,068</td>
<td>1,797</td>
<td>44</td>
<td>2.45%</td>
</tr>
<tr>
<td>109,887</td>
<td>2,979</td>
<td>128</td>
<td>4.30%</td>
</tr>
<tr>
<td>94,715</td>
<td>5,614</td>
<td>247</td>
<td>4.40%</td>
</tr>
<tr>
<td>2,733</td>
<td>700</td>
<td>13</td>
<td>1.86%</td>
</tr>
<tr>
<td>2,347</td>
<td>3,451</td>
<td>127</td>
<td>3.68%</td>
</tr>
</tbody>
</table>
### Traditional gTLDs vs. IDN-gTLDs

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

<table>
<thead>
<tr>
<th>Type</th>
<th>Delegations</th>
<th>Route Origins</th>
<th>Valid ROAs</th>
<th>RPKI Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASCII</td>
<td>94,715</td>
<td>5,614</td>
<td>247</td>
<td>4.40%</td>
</tr>
<tr>
<td>IDN</td>
<td>91,736</td>
<td>555</td>
<td>9</td>
<td>1.62%</td>
</tr>
<tr>
<td>ASCII</td>
<td>28,671</td>
<td>2,967</td>
<td>140</td>
<td>4.72%</td>
</tr>
<tr>
<td>IDN</td>
<td>28,826</td>
<td>559</td>
<td>16</td>
<td>2.86%</td>
</tr>
<tr>
<td>ASCII</td>
<td>27,821</td>
<td>3,451</td>
<td>127</td>
<td>3.68%</td>
</tr>
<tr>
<td>IDN</td>
<td>28,297</td>
<td>700</td>
<td>13</td>
<td>1.86%</td>
</tr>
</tbody>
</table>
Who makes deployment decisions?

<table>
<thead>
<tr>
<th>Category</th>
<th>Full Adoption (=100%)</th>
<th>Mixed (&gt;0%, &lt;100%)</th>
<th>No Adoption (=0%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone Operators</td>
<td>98</td>
<td>145</td>
<td>27</td>
</tr>
<tr>
<td>Aut-Num Holders</td>
<td>253</td>
<td>38</td>
<td>195</td>
</tr>
<tr>
<td>IP Holders</td>
<td>296</td>
<td>17</td>
<td>183</td>
</tr>
</tbody>
</table>

- 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)

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

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

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

<table>
<thead>
<tr>
<th>Type</th>
<th>Delegations</th>
<th>Names with DS</th>
<th>DNSSEC Rate</th>
<th>Route Origins</th>
<th>Valid ROAs</th>
<th>RPKI Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASCII</td>
<td>94,715</td>
<td>6,085</td>
<td>6.42%</td>
<td>5,614</td>
<td>247</td>
<td>4.40%</td>
</tr>
<tr>
<td>IDN</td>
<td>91,736</td>
<td>8</td>
<td>0.01%</td>
<td>555</td>
<td>9</td>
<td>1.62%</td>
</tr>
<tr>
<td>ASCII</td>
<td>28,671</td>
<td>1,503</td>
<td>5.24%</td>
<td>2,967</td>
<td>140</td>
<td>4.72%</td>
</tr>
<tr>
<td>IDN</td>
<td>28,826</td>
<td>6</td>
<td>0.02%</td>
<td>559</td>
<td>16</td>
<td>2.86%</td>
</tr>
<tr>
<td>ASCII</td>
<td>27,821</td>
<td>678</td>
<td>2.44%</td>
<td>3,451</td>
<td>127</td>
<td>3.68%</td>
</tr>
<tr>
<td>IDN</td>
<td>28,297</td>
<td>1</td>
<td>0.00%</td>
<td>700</td>
<td>13</td>
<td>1.86%</td>
</tr>
</tbody>
</table>
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
facebook.com/icannorg
youtube.com/icannnews
flickr.com/icann

linkedin/company/icann
slideshare/icannpresentations
soundcloud/icann
instagram.com/icannorg