In rDNS We Trust
Revisiting rDNS Use by Clients on the Internet

Tobias Fiebig¹,²,³, Kevin Borgolte², Shuang Hao⁴, Christopher Kruegel², Giovanni Vigna², Anja Feldmann³,⁵

¹ TU Delft
² UC Santa Barbara
³ TU Berlin
⁴ UT Dallas
⁵ Max Planck Institute for Informatics
What is reverse DNS?
Forward DNS

• Usually gives you an IPv(4|6) Address for a name (A|AAAA query):

Client ➔ ?A google.com ➔ Server

Client ➔ A google.com 8.8.8.8 ➔ Server
Reverse DNS (rDNS)

- Gives you a pointer to a name in the tree:

Client

?PTR
1.0.168.192.in-addr.arpa.

Server

Client

PTR
1.0.168.192.in-addr.arpa.

gw.privnet.local.
rDNS Zones

- **IPv4:**
  - in-addr.arpa.
  - Four octets
  - One level per octet:
    - `xxx.xxx.xxx.xxx.in-addr.arpa`.

- **IPv6:**
  - ip6.arpa.
  - 32 nibbles
  - One level per nibble:
    - `x.x.x.x.x.x.x.x.x.x.x.x.x.x.x.x.x.x.x.x.x.x.x.x.x.x.x.x.x.x.x.x.ip6.arpa`. 
WHATEVER
WHO CARES
You can use it to understand links…
...topologies...
…IPv6 deployments…
...even build IPv6 security scan seeds
How does real-world rDNS use look?

• Earlier work, e.g., Gao et al. suggests no
  – Argument: High SERVFAIL share for PTR requests indicates low maintenance state

• Still:
  – Not focusing on rDNS
  – More an afterthought of “real” DNS
Passive trace results
Data source: Farsight DNS stream

- Collected from DNS recursors around the globe
- Provided to researchers and IT security professionals
- Large 😊
Passive DNS Data Flow

(Slide referenced from: https://www.slideshare.net/apnic/2014-03-dnstap-1410824032)
Full Dataset

- Flat-line for A/Total
- Daily anti-pattern AAAA vs. PTR
- Looks funny

(a) Full Farsight dataset.
Isolated biasing operator

- Cause: Single Operator with odd lookup pattern:
  - Flatline PTR
  - ip6.int. for 70::/8
  - DNS-SD for dell.com, apple.com etcetc. (~same No. Req/name)
- Close to 50% of the Dataset

(b) Only biased operator.
Cleaned dataset

- Solution: Filtering
- Patterns start to look as expected
- Outliers in MX: Single Russian ISP running a regular “Digest Mailinglist” for users

(c) w/o biased operator.
Types of PTR: v4, v6, DNS-SD

- Not all PTR are .arpa!
  - ~99% in-addr.arpa.
  - ~0.9% ip6.arpa
  - ~0.1% DNS-SD
- Outliers starting week 14:
  - Possible deployment of new set-top-box CPE (software)
  - Queries for TV Channel Domain
rDNS Response Codes: in-addr.arpa.

- Stable SERVFAIL socket (~3%)
- Relatively few NXDOMAIN (~25%)
- ~47% NOERROR
- ~15% REFUSED

<table>
<thead>
<tr>
<th>rcode</th>
<th>in-addr.arpa</th>
<th>ip6.arpa</th>
<th>ip6.arpa w/o Resv.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOERROR</td>
<td>47.21%</td>
<td>4.00%</td>
<td>32.30%</td>
</tr>
<tr>
<td>NXDOMAIN</td>
<td>25.36%</td>
<td>94.87%</td>
<td>63.87%</td>
</tr>
<tr>
<td>REFUSED</td>
<td>15.47%</td>
<td>0.14%</td>
<td>1.11%</td>
</tr>
<tr>
<td>FAILURE</td>
<td>8.77%</td>
<td>0.81%</td>
<td>1.34%</td>
</tr>
<tr>
<td>SERVFAIL</td>
<td>3.17%</td>
<td>0.18%</td>
<td>1.38%</td>
</tr>
<tr>
<td>FORMERR</td>
<td>0.01%</td>
<td>≤0.01%</td>
<td>≤0.01%</td>
</tr>
<tr>
<td>NOTAUTH</td>
<td>≤0.01%</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>NOTIMP</td>
<td>≤0.01%</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

(a) in-addr.arpa
rDNS Response Codes: ip6.arpa.

- Hardly any SERVFAIL (>0.2%)
- Dominated by NXDOMAIN (~95%)
- Only 4% NOERROR
- Hardly any REFUSED (>0.2%)
rDNS Response Codes: ip6 w/o Resv.

- More SERVFAIL (>1.4%)
- Still strong on NXDOMAIN (~64%)
- Now ~32% NOERROR
- Still hardly any REFUSED (>1.2%)
rDNS Response Types

- CNAMEs common for in-addr.arpa delegation
- Hardly any in ip6.arpa.
- DNAMEs are a thing!
Passive Measurements Summary

• Beware of biases in data sets

• There is more v4 than v6 rDNS (100:1) and PTR ≠ rDNS

• Way more noise (priv./resv. For IPv6 rDNS)

• Less CNAMEs in v6 (as expected)

• More SERVFAIL in v4

Active measurement...
Active rDNS measurements

• Easy for in-addr.arpa (brute-force)

• Hard for ip6.arpa (too large)

• Use RF8020 compliance as suggested in RFC7707 globally

Enumerating (r)DNS trees
Collecting Data

• Used RFC8020 enumeration for v4 and v6
  – Quicker than brute-force for in-addr.arpa
    • Compared with a brute-force dataset

• Cluster of 16 machines (beware of the single IP stack)
  – Performed better than single machine for PAM2017 paper
Limitations

• We can not enumerate zone on RFC8020 violating authoritatives

• Cross-test with active trace:
  – 39.58% RFC8020 compliant
  – 46.42% always NXDOMAIN
  – 11.61% always return NOERROR

• Seeding makes things better, but we at best see only ~40%
rcodes in Active Measurements

Share of rcode/termination reason

IPv6 Prefix Size

IPv4 Pref x Size
Delegations in rDNS

![Graph showing the distribution of delegations in IPv6 and IPv4 prefix sizes with a log scale for the number of delegations. CNAMEs are highlighted in the IPv4 prefix size graph.]
CNAMEs

• IPv4:
  – Mostly delegation for </24 zones (RFC2317)

• IPv6:
  – Heavy hitter: 87.81% of CNAMEs belong to a DHCPv6 setup (Dynamic Zone?)
  – 80.77% of the rest point to in-addr.arpa names
    • IPv4 first, consistent naming for multi-homed hosts
Special Case: rDNS64?

- Found a single operator mapping in-addr.arpa. to a /96 via CNAMEs
  - NAT64 range?

- Smart idea:
  - Preserves rDNS for customers
  - Does not break DNSSEC(!)
  - Should we have an RFC for this?
A/AAAA-less PTRs

• Found large operators with only PTR records set
  – Actual forward zones not populated or delegated?
  – Forward zones in split-view?
  – Potential information leak
Active Measurements Summary

• CNAME have different usecases in IPv4 and IPv6

• SERVFAIL is more common in v4 rDNS but overall relatively low

• IPv6 rDNS is top-driven

• Dynamically generated v6 zones are mostly /48

• We found a funny case of v4 rDNS for DNS64 delegation in a Japanese ISP

• There are names without a matching forward-record in .arpa
Summary & Conclusion

- PTR is not only for .arpa
- People still use rDNS
- IPv6 rDNS is ~1% of IPv4 rDNS
- We should take a look at whether people actually maintain their rDNS
Backup Slides
## rDNS Response Codes: Table

<table>
<thead>
<tr>
<th>rcode</th>
<th>in-addr.-arpa</th>
<th>ip6.arpa</th>
<th>ip6.arpa w/o Resv.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOERROR</td>
<td>47.21%</td>
<td>4.00%</td>
<td>32.30%</td>
</tr>
<tr>
<td>NXDOMAIN</td>
<td>25.36%</td>
<td>94.87%</td>
<td>63.87%</td>
</tr>
<tr>
<td>REFUSED</td>
<td>15.47%</td>
<td>0.14%</td>
<td>1.11%</td>
</tr>
<tr>
<td>FAILURE</td>
<td>8.77%</td>
<td>0.81%</td>
<td>1.34%</td>
</tr>
<tr>
<td>SERVFAIL</td>
<td>3.17%</td>
<td>0.18%</td>
<td>1.38%</td>
</tr>
<tr>
<td>FORMERR</td>
<td>0.01%</td>
<td>≤0.01%</td>
<td>≤0.01%</td>
</tr>
<tr>
<td>NOTAUTH</td>
<td>≤0.01%</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>NOTIMP</td>
<td>≤0.01%</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Churn in Queried Names

(a) in-addr.arpa

(b) ip6.arpa (/64)

(c) ip6.arpa (/128)
Biases and Volume

(a) Full Farsight dataset.  (b) Only biased operator.  (c) w/o biased operator.