Comments on DNS Robustness

Mark Allman
Reformed IETF Native

Applied Networking Research Workshop
July 2018

"Been away so long I hardly knew the place,
Gee, it's good to be back home"
Observation #1

Dyn Analysis Summary Of Friday October 21 Attack

Company News // Oct 26, 2016 // Scott Hilton
Observation #2

Growth Rate

SLDs
How Robust Is DNS?

• “Good Enough”

• But, … um … ahem …
How Robust Is DNS?

• What do we mean by “robust”?
  • many dimensions
  • our focus:
    • *always* able to communicate with an auth server holding the DNS record we seek
DNS Robustness

- root
  - .org
    - .icir.org
      - git.icir.org
    - .eff.org
  - .com
    - .cnn.com
    - .ebay.com
  - .edu
    - .berkeley.edu
      - .icsi.berkeley.edu
      - imaphost.icsi.berkeley.edu
    - .case.edu
DNS Robustness

- Community infrastructure
- Many named replicas e.g., a-root, b-root, etc.
- Many unnamed replicas i.e., via anycast routing
DNS Robustness

- Few named replicas
  ~80% of SLDs have <= 2 named auth servers
- Unknown / variable use of anycast replicas
- Myriad operators / policies
How Robust Is DNS?

• Let’s measure some facets of the system at the SLD level that bear on robustness
Datasets

- .com zone file
- .net zone file
- .org zone file

Alexa Top 1M

Winnowed Zone File

Once / Month
Apr 09 - Apr 18

Data courtesy of Verisign, Alexa, Emile Aben (RIPE) and Quirin Scheitle (TUM)
Robustness Specifications

- RFC 1034: must have multiple authoritative nameservers for robustness
- RFC 2182: authoritative nameservers must be geographically and topologically diverse
What Is Network Diversity?

- We start cheap & conservative:
  - use /24 address blocks to define diversity
  - two addresses in one /24: no diversity
  - two addresses in two /24s: diversity
    (but, really, who knows?!)  

- Future work includes using historical routing data
Spec. vs. Reality

Percentage of SLDs

= Min
Spec. vs. Reality

Percentage of SLDs

= Min  < Min  > Min  

Upper Bound

Lower Bound

Shared Infrastructure

- root
  - .org
    - .icir.org
    - .eff.org
      - git.icir.org
  - .com
    - .cnn.com
    - .ebay.com
  - .edu
    - .berkeley.edu
      - .icsi.berkeley.edu
        - imaphost.icsi.berkeley.edu
    - .case.edu
Shared Infrastructure

- Different parts of the tree, but rely on same auth servers

- .org
  - .icir.org
  - git.icir.org
- .com
  - .eff.org
  - .cnn.com
  - .ebay.com
- .edu
  - .berkeley.edu
  - .icsi.berkeley.edu
  - imaphost.icsi.berkeley.edu
- .org
  - .com
  - .edu
Shared Infrastructure

- Hierarchy belies much concentration
- Concentration compounds issues
- Perhaps concentration invites trouble
Nameserver-Level Analysis

• For each SLD, determine the number of other SLDs that use the same set of nameservers (by IP address)

• Repeat for each month in dataset
Nameserver-Level Analysis

Distributions are fairly stable across time.

Half the SLDs share the same nameservers as > 100 other SLDs.

9-10K SLDs share the same set of nameservers.
Network-Level Analysis

• For each SLD determine the number of other SLDs whose nameservers fall within the same /24 address blocks

• Repeat for each month in dataset
Network-Level Analysis

Half the SLDs are in groups with > 3K other SLDs

Nameserver concentration is increasing over time.
## Top 10 SLD Groups

<table>
<thead>
<tr>
<th>Rank</th>
<th>Num. SLDs</th>
<th>Num. /24s</th>
<th>Same Last Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>71,472</td>
<td>2</td>
<td>✓</td>
</tr>
<tr>
<td>2</td>
<td>69,637</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>15,421</td>
<td>2</td>
<td>✓</td>
</tr>
<tr>
<td>4</td>
<td>13,044</td>
<td>2</td>
<td>✓</td>
</tr>
<tr>
<td>5</td>
<td>8,347</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>6,111</td>
<td>2</td>
<td>✓</td>
</tr>
<tr>
<td>7</td>
<td>5,568</td>
<td>3</td>
<td>✗</td>
</tr>
<tr>
<td>8</td>
<td>5,076</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>4,788</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>4,611</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>204,075</td>
<td>23</td>
<td></td>
</tr>
</tbody>
</table>

> 20% of the popular SLDs fall within 23 /24 blocks!> 20% of the popular SLDs rely on 19 edge networks!
Conclusions

- DNS sky is not falling
- But, we have some unhealthy habits ...
  - too little auth server replication
  - too much auth server concentration
- Note: concentration is not wholly bad
Questions? Comments?

Draft paper:
https://www.icir.org/mallman/pubs/All18

Mark Allman, mallman@icir.org
https://www.icir.org/mallman/
@mallman_icsi