Comments on DNS Robustness

Mark Allman
International Computer Science Institute

ACM Internet Measurement Conference
November 2018
Observation #1

Dyn Analysis Summary Of Friday October 21 Attack

Company News // Oct 26, 2016 // Scott Hilton
Observation #2
How Robust Is DNS?

- What do we mean by “robust”?
  - many dimensions

- Our focus: can we *always* communicate with an auth server holding the DNS record we seek
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
Spec. vs. Reality

Percentage of SLDs

- Min
- > Min

Years
- 2009
- 2010
- 2011
- 2012
- 2013
- 2014
- 2015
- 2016
- 2017
- 2018
- 2019

Values
- 10
- 15
- 20
- 25
- 30
- 35
- 40
- 45
- 50
- 55
Shared Infrastructure

- different parts of tree rely on same auth servers
- hierarchy belies (some) concentration
Network-Level Concentration

• For each SLD $x$ determine:
  • determine $N_x$: set of /24s containing $x$’s nameservers
  • determine number of other SLDs, $M_x$, relying on same $N_x$
  • Build distribution of $M_x$ across all SLDs

• Repeat for each month in dataset
Half the SLDs are in groups with > 3K other SLDs.

Nameserver concentration is increasing over time.
## Network-Level Concentration

<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></td>
<td></td>
</tr>
</tbody>
</table>

> 20% of the popular SLDs rely on 19 edge networks!

> 20% of the popular SLDs fall within 23 /24 blocks!
Summary

• DNS sky is not falling
• But, we have some unhealthy habits …
  • too little auth server replication
  • too much auth server concentration

• More details, analysis, comments in the paper
Questions? Comments?

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