Quantifying DNSSEC Validators

Yingi Yu & Duane Wessels
October, 2012
Motivation

• How is client-side DNSSEC deployment progressing?
• Informs discussions about issues such as rolling root zone keys.
• Do validators have fingerprints?
• What percent of com/net responses are validated?
Related Work

• “Observing DNSSEC Validation in the Wild”
  • Guðmundsson and Crocker, SATIN 2011
  • Analyzed queries to .ORG name servers.

• “Measuring Occurrence of DNSSEC Validation”
  • Wander and Weis
  • browser-based (1x1 images and javascript)

• “Counting DNSSEC”
  • Geoff Huston/RIPE
  • browser-based (advertisement images)
Our Approach

• DNS-based
  • some help from browser DNS prefetching

• Relies on validators to retry if given a mal-signed response.

• An RRSIG-remover sits in front of signed zones.
  • First response, RRSIG is removed (A query only)
  • Subsequent responses have all signatures

• Initial queries are redirected to unique query names with CNAME response.
How to find a validator?

Evidence of DNSSEC Validators

End users

Validator

Non-validator

RRSIG Remover

Authoritative Name server

foo.bar.com A ?

foo.bar.com A 127.0.0.1

foo.bar.com A 127.0.0.1

foor.bar.com RRSIG

foo.bar.com A 127.0.0.1

foor.bar.com RRSIG
How to find a validator?

Evidence of Non-Validators

- End users
- Validator
- Non-validator
- RRSIG Remover
- Authoritative Name server

foo.bar.com A ?
foo.bar.com A 127.0.0.1

foo.bar.com A 127.0.0.1
foo.bar.com RRSIG
Complications with Our Method

• Needs retry behavior, which is inconsistent and not required by RFCs.
  • But seems to work reasonably well for this experiment.
• Packet loss could be interpreted as validation.
  • Reduced by examining multiple lookups over course of a day.
  • Other causes of repeated queries?
• Fails to find a validator behind a forwarder.
  • Retries don’t make it past the forwarder.
WPAD

• The Web Proxy Auto Discovery protocol says that HTTP agents should query for wpad.$domainname in order to locate a proxy autoconfiguration file.
• Naturally, some implementations will query for wpad.$tld, or even “wpad.”
• Duane registered wpad.{com,net,org,biz,us} shortly after reading the internet-draft. Hooray!
• These domains receive ~2,000,000 queries per day.
Prefetching

• We asked people to add the following line to web pages in order to drive DNS queries to us:
  \(<a href="http://prefetch.validatorsearch.verisignlabs.com">\</a>\)

• Most browsers will automatically pre-fetch the DNS name.
Results
Number of Resolvers Observed

<table>
<thead>
<tr>
<th>Date</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Sep12</td>
<td>0</td>
</tr>
<tr>
<td>17 Sep12</td>
<td>5000</td>
</tr>
<tr>
<td>24 Sep12</td>
<td>10000</td>
</tr>
<tr>
<td>1 Oct12</td>
<td>15000</td>
</tr>
<tr>
<td>8 Oct12</td>
<td>20000</td>
</tr>
<tr>
<td>15 Oct12</td>
<td>25000</td>
</tr>
</tbody>
</table>
Percent of Resolvers Doing Validation

Date

Percent

Sep12 10 17 24 Oct12 8 15

Oct12

9 17 24 1 8 15

Percent of Resolvers Doing Validation

0 1 2 3 4 5

Sep12 10 17 24 Oct12 8 15
Comparison with All Resolvers Seen at COM/NET sites

- October 11, 2012
- 4 Verisign sites: AMS, IAD, NYC, SFO

- 4,801,160 unique IPs seen at sites
- 26,379 (5.5%) unique resolver IPs observed by test
- 1,087 (0.023%) unique validator IPs found by test

- 19,197,063,214 total queries received at sites
- 9,296,623,161 (48.4%) queries from observed resolvers
- 1,449,625,183 (7.6%) queries from observed validators
### Geographic Distribution

<table>
<thead>
<tr>
<th>CC</th>
<th>#Resolvers</th>
<th>%Validators</th>
</tr>
</thead>
<tbody>
<tr>
<td>SE</td>
<td>145</td>
<td>46.2%</td>
</tr>
<tr>
<td>CZ</td>
<td>197</td>
<td>33.5%</td>
</tr>
<tr>
<td>BR</td>
<td>1098</td>
<td>13.6%</td>
</tr>
<tr>
<td>NL</td>
<td>267</td>
<td>10.1%</td>
</tr>
<tr>
<td>DE</td>
<td>577</td>
<td>8.8%</td>
</tr>
<tr>
<td>CH</td>
<td>182</td>
<td>7.7%</td>
</tr>
<tr>
<td>ID</td>
<td>173</td>
<td>7.5%</td>
</tr>
<tr>
<td>TR</td>
<td>110</td>
<td>5.5%</td>
</tr>
<tr>
<td>CL</td>
<td>315</td>
<td>5.1%</td>
</tr>
<tr>
<td>AT</td>
<td>121</td>
<td>5.0%</td>
</tr>
<tr>
<td>FR</td>
<td>1093</td>
<td>4.7%</td>
</tr>
<tr>
<td>CO</td>
<td>113</td>
<td>4.4%</td>
</tr>
<tr>
<td>UA</td>
<td>161</td>
<td>4.3%</td>
</tr>
<tr>
<td>PL</td>
<td>474</td>
<td>4.0%</td>
</tr>
<tr>
<td>GB</td>
<td>569</td>
<td>3.7%</td>
</tr>
<tr>
<td>JP</td>
<td>519</td>
<td>3.3%</td>
</tr>
<tr>
<td>TH</td>
<td>124</td>
<td>3.2%</td>
</tr>
<tr>
<td>AU</td>
<td>224</td>
<td>3.1%</td>
</tr>
<tr>
<td>BE</td>
<td>133</td>
<td>3.0%</td>
</tr>
<tr>
<td>US</td>
<td>10306</td>
<td>2.8%</td>
</tr>
<tr>
<td>CA</td>
<td>654</td>
<td>2.6%</td>
</tr>
<tr>
<td>CN</td>
<td>1302</td>
<td>2.5%</td>
</tr>
<tr>
<td>BG</td>
<td>109</td>
<td>1.8%</td>
</tr>
<tr>
<td>HU</td>
<td>110</td>
<td>1.8%</td>
</tr>
<tr>
<td>AR</td>
<td>446</td>
<td>1.8%</td>
</tr>
<tr>
<td>RU</td>
<td>701</td>
<td>1.6%</td>
</tr>
<tr>
<td>HK</td>
<td>130</td>
<td>1.5%</td>
</tr>
<tr>
<td>PH</td>
<td>205</td>
<td>1.5%</td>
</tr>
<tr>
<td>TW</td>
<td>950</td>
<td>1.3%</td>
</tr>
<tr>
<td>IT</td>
<td>278</td>
<td>1.1%</td>
</tr>
<tr>
<td>RO</td>
<td>214</td>
<td>0.9%</td>
</tr>
<tr>
<td>IN</td>
<td>468</td>
<td>0.9%</td>
</tr>
<tr>
<td>ES</td>
<td>249</td>
<td>0.8%</td>
</tr>
<tr>
<td>MX</td>
<td>250</td>
<td>0.8%</td>
</tr>
<tr>
<td>KR</td>
<td>545</td>
<td>0.0%</td>
</tr>
<tr>
<td>??</td>
<td>109</td>
<td>0.0%</td>
</tr>
</tbody>
</table>

For Countries with 100 or more resolvers observed
Fingerprints

- The order of queries allows us to identify the name server software.

- Nominum DNS does not requery for other types of RRs if signature is missing.
Fingerprints

- **Unbound**: 24%
- **Mixed**: 2%
- **Nominum**: 11%
- **Unknown**: 1%
- **BIND**: 62%
Comparison With Related Work
Comparison

• Guðmundsson and Crocker
  • “In both periods the percentage of confirmed validators is about 1.2 percent of the total number of resolvers…”
  • November 2010, January 2011

• Wander and Weis
  • “Overall 3,443 trials were positive (4.5%) …”
  • Note, these are “trials,” not resolvers

• Huston
  • “2,316 out of 57,267, or 4.0% of the DNS resolvers were observed to perform DNSSEC validation”
Project Website

http://validator-search.verisignlabs.com/
Thank You