Finding DNSSEC Validators with Check-Repeat

Duane Wessels
April 19, 2013
Joint Work

- Yingdi Yu, UCLA
- Duane Wessels, Verisign Labs
- Matt Larson, Verisign Labs
- Lixia Zhang, UCLA
Why Count Validators

- DNSSEC suffers somewhat from the “chicken-and-egg problem.”
- The publication-side of DNSSEC is well studied. The consumer-side, not so much.
- Surveys and estimates of validator population inform the upcoming root KSK rollover (2015).
Enumerating Validating Resolvers is Hard

• Resolver chaining
• Multiple resolvers per user
• Multiple IPs per resolver
• NATs
• Dynamic addressing
• Unexpected query behavior
• Trust Anchor configuration not conveyed in queries
Simplistic Model

User -> Resolver -> Internet -> Auth
Chaining

User → Resolver → Resolver → Internet → Auth
Multiple Resolvers per User
Multiple IPs per Resolver
Public Resolvers

User

Resolver

Google

OpenDNS

Internet

Auth
NATs

User -> Resolver -> NAT -> Internet -> Auth

User -> Resolver -> NAT -> Internet -> Auth
Unexpected Query Behavior

A/AAAA queries from here

DS/DNSKEY queries from here
Previous Approaches

- Look for DNSKEY and DS queries at authoritative name servers.
  - Assumption that only validating resolvers make DNSKEY/DS queries might not be true.
- Correlate DNS/HTTP requests for pairs of DNS names. Lack of use of improperly signed name implies validation.
  - Web browser bias?
  - Good for measuring end user adoption
  - Could measure application-based validation, vs resolver-based.
Check-Repeat

• When presented with an improperly signed DNSSEC response, most validating resolver implementations will retry the query.
  • At least once.
  • To another authoritative name server.

• However…
  • Query retries look a lot like packet loss.
  • Not all implementations retry.
  • Doesn’t work for “chained” resolvers.
Signature Remover

Resolver

bar.example.com MX?

bar.example.com MX mail
bar.example.com RRSIG MX ...

abcd1234.example.com A?

abcd1234.example.com A 127.0.0.1

(abcd1234.example.com A 127.0.0.1
(no RRSIG)

abcd1234.example.com A?

abcd1234.example.com A 127.0.0.1

abcd1234.example.com A 127.0.0.1

 foo.example.com A?

foo.example.com CNAME abcd1234.example.com
foo.example.com RRSIG CNAME ...

foo.example.com A?

foo.example.com CNAME abcd1234.example.com
foo.example.com RRSIG CNAME ...

Signature Remover

target query

Authoritative
NS on 127.0.0.1

Non-Validator accepts bad reply

Validator repeats the query

bar.example.com MX?

bar.example.com MX mail
bar.example.com RRSIG MX ...

bar.example.com MX?

bar.example.com MX mail
bar.example.com RRSIG MX ...

probe query
How to attract DNS queries?

• A web bug via DNS prefetching.

  <link rel="prefetch" href="http://prefetch.validatorsearch.verisignlabs.com" />
  <a href="http://prefetch.validatorsearch.verisignlabs.com"></a>

• Take advantage of popular, yet non-critical domains.
wpad.{com,net,org,us,biz}

• “Web Proxy Auto Discovery”
• Work by Microsoft and others, documented as Internet-Draft but never RFC.
• HTTP agents (browsers) try to load URLs by prepending “wpad” to their local domain:
  http://wpad.cs.ucla.edu/wpad.dat
• On failure, try again by removing domain labels:
  http://wpad.ucla.edu/wpad.dat
  http://wpad.edu/wpad.dat
  http://wpad/wpad.dat
Results
Indicators of Validation

- DS/DNSKEY queries
- Repeats
- Consistent pattern over time
Nominum/Vantio

• Nominum’s resolver product, Vantio, does not consistently retry signature-removed queries.
• Fortunately, Vantio openly answers “version.bind” queries by default.
• Whitelisted for this study.
### Trace-I

<table>
<thead>
<tr>
<th>Totals</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Days</td>
<td>36</td>
</tr>
<tr>
<td>Queries</td>
<td>24,786,845</td>
</tr>
<tr>
<td>Trials</td>
<td>6,498,277</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Daily Averages</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IPs</td>
<td>24,143</td>
</tr>
<tr>
<td>Resolvers</td>
<td>18,224</td>
</tr>
<tr>
<td>Validators</td>
<td>836</td>
</tr>
<tr>
<td>%Validating</td>
<td>4.6%</td>
</tr>
</tbody>
</table>
Quantifying False Positives

- Queries repeated due to packet loss could be misinterpreted as validations.
- Signature remover disabled for 9 days to find false positives.

**Daily Averages**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IPs</td>
<td>24,522</td>
</tr>
<tr>
<td>Resolvers</td>
<td>18,247</td>
</tr>
<tr>
<td>Validators</td>
<td>33</td>
</tr>
<tr>
<td>False Positives</td>
<td>0.18%</td>
</tr>
</tbody>
</table>
Number of Resolvers and Validators Measured

<table>
<thead>
<tr>
<th>Day</th>
<th>Number of Resolvers</th>
<th>Detected Validators</th>
<th>Detected Resolvers</th>
<th>Possible Validators</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>10</td>
<td>False</td>
<td>10</td>
<td>False Positive</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td></td>
<td></td>
<td>False Positive</td>
</tr>
<tr>
<td>4</td>
<td>10</td>
<td></td>
<td></td>
<td>False Positive</td>
</tr>
<tr>
<td>6</td>
<td>10</td>
<td></td>
<td></td>
<td>False Positive</td>
</tr>
<tr>
<td>8</td>
<td>10</td>
<td></td>
<td></td>
<td>False Positive</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td></td>
<td></td>
<td>False Positive</td>
</tr>
<tr>
<td>12</td>
<td>10</td>
<td></td>
<td></td>
<td>False Positive</td>
</tr>
<tr>
<td>14</td>
<td>10</td>
<td></td>
<td></td>
<td>False Positive</td>
</tr>
<tr>
<td>16</td>
<td>10</td>
<td></td>
<td></td>
<td>False Positive</td>
</tr>
<tr>
<td>18</td>
<td>10</td>
<td></td>
<td></td>
<td>False Positive</td>
</tr>
<tr>
<td>20</td>
<td>10</td>
<td></td>
<td></td>
<td>False Positive</td>
</tr>
<tr>
<td>22</td>
<td>10</td>
<td></td>
<td></td>
<td>False Positive</td>
</tr>
<tr>
<td>24</td>
<td>10</td>
<td></td>
<td></td>
<td>False Positive</td>
</tr>
<tr>
<td>26</td>
<td>10</td>
<td></td>
<td></td>
<td>False Positive</td>
</tr>
<tr>
<td>28</td>
<td>10</td>
<td></td>
<td></td>
<td>False Positive</td>
</tr>
<tr>
<td>30</td>
<td>10</td>
<td></td>
<td></td>
<td>False Positive</td>
</tr>
<tr>
<td>32</td>
<td>10</td>
<td></td>
<td></td>
<td>False Positive</td>
</tr>
<tr>
<td>34</td>
<td>10</td>
<td></td>
<td></td>
<td>False Positive</td>
</tr>
<tr>
<td>36</td>
<td>10</td>
<td></td>
<td></td>
<td>False Positive</td>
</tr>
<tr>
<td>38</td>
<td>10</td>
<td></td>
<td></td>
<td>False Positive</td>
</tr>
<tr>
<td>40</td>
<td>10</td>
<td></td>
<td></td>
<td>False Positive</td>
</tr>
<tr>
<td>42</td>
<td>10</td>
<td></td>
<td></td>
<td>False Positive</td>
</tr>
<tr>
<td>44</td>
<td>10</td>
<td></td>
<td></td>
<td>False Positive</td>
</tr>
</tbody>
</table>
Quantifying False Negatives

• Cases where resolver received DNSKEYs, signatures were removed, but did not see repeated query.
• Likely caused by multi-level caching, a.k.a. DNS forwarding.
• About 30 false negatives out of 20,000 resolvers daily.
• False negative rate 0.15%.
## Geographic Distribution of Validating Resolvers

The diagram below illustrates the geographic distribution of detected validators and resolvers across various countries. The x-axis represents the countries, and the y-axis shows the detected numbers on a logarithmic scale.

### Countries
- US
- FR
- BR
- RU
- DE
- CA
- GB
- CL
- PL
- CN
- AR
- JP
- NL
- IN
- IT

### Detected Numbers

The detected numbers are shown for both validators (blue bars) and resolvers (green bars) in each country. The scales range from $10^0$ to $10^5$.

### Countries and Detected Numbers

<table>
<thead>
<tr>
<th>Country</th>
<th>Detected Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>US</td>
<td>$10^4$</td>
</tr>
<tr>
<td>FR</td>
<td>$10^3$</td>
</tr>
<tr>
<td>BR</td>
<td>$10^2$</td>
</tr>
<tr>
<td>RU</td>
<td>$10^1$</td>
</tr>
<tr>
<td>DE</td>
<td>$10^0$</td>
</tr>
<tr>
<td>CA</td>
<td>$10^2$</td>
</tr>
<tr>
<td>GB</td>
<td>$10^3$</td>
</tr>
<tr>
<td>CL</td>
<td>$10^4$</td>
</tr>
<tr>
<td>PL</td>
<td>$10^5$</td>
</tr>
<tr>
<td>CN</td>
<td>$10^1$</td>
</tr>
<tr>
<td>AR</td>
<td>$10^0$</td>
</tr>
<tr>
<td>JP</td>
<td>$10^2$</td>
</tr>
<tr>
<td>NL</td>
<td>$10^3$</td>
</tr>
<tr>
<td>IN</td>
<td>$10^4$</td>
</tr>
<tr>
<td>IT</td>
<td>$10^5$</td>
</tr>
</tbody>
</table>
Did we find all Resolvers on the Internet?

- Compared resolvers observed by Check-Repeat to those seen by G.GTLD-SERVERS.NET (one of 13 COM/NET name servers).
- Check-Repeat sees 1.6% of resolvers seen by G.GTLD.
- But 63.5% of all responses from G.GTLD go to Check-Repeat resolvers.
- At least 12.3% of all responses from G.GTLD go to DNSSEC validators.
Comparison with Previous Work

- [2010] Gudmundsson and Crocker found 10% (upper limit) of queries to ORG name servers are from resolvers that ask for DNSKEY/DS.
  - We find 12.3% for COM/NET (lower limit)
- [2012] Wander and Weis report 4.8% of trials indicate validation.
- [2012] Huston reports 9% of Internet end users have validating resolvers and 4% of resolvers validate.
  - 7 days of data
- [2012] Huston later revises and reports 1.6% of end users and 1.7% of resolvers perform validation.
  - 17 days of data
  - We find 4.6% (of resolvers)
Thank You