Measuring Occurrence of DNSSEC Validation

Matthäus Wander
<matthaeus.wander@uni-due.de>

DNS-OARC Workshop
Toronto, October 14, 2012
Overview

• What is the ratio of validating clients in the Web?

• Validating $\Rightarrow$ rejects invalid signatures

• Outline
  ◦ Measurement methodology
  ◦ Result analysis
  ◦ What's next?
Measurement Methodology

- Signed zone *verteiltesysteme.net*
  - Domain name `sigok` with valid signature
  - Domain name `sigfail` with broken signature
- Two web-based resolver tests (interactive, hidden)
Interactive Test

⇒ http://dnssec.vs.uni-due.de

• Client-side JavaScript and images
  • Load image from sigfail× domain name
    ◦ Success: no DNSSEC validation
    ◦ Failure: go ahead
  • Load image from sigok✓ domain name
    ◦ Success: DNSSEC validation enabled
    ◦ Failure: inconclusive result
• Result is shown to the user and POSTed to our webserver
• Load transparent 1x1 pixel images from \textcolor{red}{\textbf{sigok}} and \textcolor{green}{\textbf{sigfail}}
  
  \begin{itemize}
  \item Static HTML snippet (no JavaScript)
  \end{itemize}

\begin{verbatim}
<img src="http://dnssec.vs.uni-due.de/r/a" alt="" height="1" width="1">
<img src="http://dnssec.vs.uni-due.de/r/b" alt="" height="1" width="1">
\end{verbatim}

- HTTP and DNS requests logged and evaluated offline
Client Identification

- Correlate client with resolver IP address in different server logfiles

<table>
<thead>
<tr>
<th>77.181.135.120</th>
<th>&quot;GET /ok.png?aa53 HTTP/1.1&quot; 200 413</th>
</tr>
</thead>
<tbody>
<tr>
<td>62.53.190.69#22782: query: aa53.sigok.verteiltesysteme.net IN A -ED</td>
<td></td>
</tr>
</tbody>
</table>

- HTTP redirect to [http://ID.sigok.verteiltesysteme.net/ok.png?ID](http://ID.sigok.verteiltesysteme.net/ok.png?ID)
  - Where $\text{ID} := \text{hex(SHA256(client_ip))}[0:4]$ 
  - Stateless mapping of client IP address to 16 bit ID
  - Unlikely to collide at the same time with different clients

- Pre-generated zone with $2^{19}$ resource record (88 MB)
  - Delivers broken signatures without nameserver adaptation
  - Vanilla zone layout
Accuracy

- **sigfail** might fail to load for unrelated reasons → **false positive**
- Require loading **sigok** to exclude some fault sources, e.g.:
  - failing to receive EDNS0 messages with packet size > 512 bytes
  - not loading images or not following cross-domain HTTP redirects
- Some fault sources remain, e.g.:
  - network fault
  - user closes browser tab prematurely
- Another possible fault: **sigfail** loads, **sigok** fails
  - Harmless invalid result (false negatives are not possible)
  - Same fault pattern like a false positive (occurs with non-validators only) → estimate ratio of false positives
Result Analysis

- 2.6M DNS/HTTP requests since May 2012
  - Grouped by ID into 336k Bernoulli trials
  - Δtime between requests < 30s

- 220k complete trials:
  - DNS request for sigok✓ and sigfail✗
  - Both HTTP redirects and HTTP 1x1 sigok✓ image

- Validating:
  - no sigfail✗ HTTP query OR
  - all DNS queries without DNSSEC OK flag

- 116k incomplete trials:
  - Mostly same client visiting several pages + browser caching
  - 326 trials missing sigok✓ → estimated 0.15% false positives
DNSKEY Missing

- Seemingly positive result but DNSKEY query is missing
- Indicates **false positive**
  - Occurred in 369 trials (0.17%)
  - Comparable to estimated ratio of false positive
- Limitation: we correlate DNSKEY via IP address, not ID
  - Might be a true positive in forwarding scenario
Data Cleaning

- Positive result but DNSKEY missing (0.17%)
- Duplicate results per IP address within 24h (59%)
- ID hash collision (<0.01%)
  - Different client IP addresses with same ID
- Inconsistent user agent (1.2%)
  - Mostly harmless e.g. same user accessing website with two browsers
  - But also: 2 clients behind NAT with different resolvers
⇒ one or more filter conditions applied to 130k (59%) trials

Not filtered: inconsistent IP addresses (1.5%)
  - HTTP images queried from different IP addresses than redirects
  - Occurred with enterprise and carrier-grade NAT
⇒ 89k results from 70k distinct IP addresses
DNSSEC Validation Ratio

Chart 1: Validation ratio per calendar week, overall 4.7%

Chart 2: Absolute numbers per country
DNSSEC per Country

Results from 179 countries, 31 with >500 trials

<table>
<thead>
<tr>
<th>No.</th>
<th>Country</th>
<th>Trials</th>
<th>Validation</th>
<th>σ</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Sweden</td>
<td>738</td>
<td>55.6%</td>
<td>±1.8%</td>
</tr>
<tr>
<td>2.</td>
<td>Czech Republic</td>
<td>626</td>
<td>35.8%</td>
<td>±1.9%</td>
</tr>
<tr>
<td>3.</td>
<td>United States</td>
<td>10739</td>
<td>13.7%</td>
<td>±0.3%</td>
</tr>
<tr>
<td>4.</td>
<td>Netherlands</td>
<td>1332</td>
<td>4.7%</td>
<td>±0.6%</td>
</tr>
<tr>
<td>5.</td>
<td>Brazil</td>
<td>911</td>
<td>4.3%</td>
<td>±0.7%</td>
</tr>
<tr>
<td>6.</td>
<td>France</td>
<td>2159</td>
<td>4.3%</td>
<td>±0.4%</td>
</tr>
<tr>
<td>7.</td>
<td>Switzerland</td>
<td>1894</td>
<td>4.2%</td>
<td>±0.5%</td>
</tr>
<tr>
<td>8.</td>
<td>Poland</td>
<td>1372</td>
<td>3.9%</td>
<td>±0.5%</td>
</tr>
<tr>
<td>9.</td>
<td>Germany</td>
<td>29975</td>
<td>3.7%</td>
<td>±0.1%</td>
</tr>
<tr>
<td>10.</td>
<td>Italy</td>
<td>1095</td>
<td>3.5%</td>
<td>±0.6%</td>
</tr>
<tr>
<td>11.</td>
<td>Indonesia</td>
<td>1015</td>
<td>2.4%</td>
<td>±0.5%</td>
</tr>
<tr>
<td>12.</td>
<td>Ukraine</td>
<td>1708</td>
<td>1.9%</td>
<td>±0.3%</td>
</tr>
<tr>
<td>13.</td>
<td>Greece</td>
<td>1014</td>
<td>1.7%</td>
<td>±0.4%</td>
</tr>
<tr>
<td>14.</td>
<td>United Kingdom</td>
<td>2373</td>
<td>1.6%</td>
<td>±0.3%</td>
</tr>
<tr>
<td>15.</td>
<td>Serbia</td>
<td>615</td>
<td>1.5%</td>
<td>±0.5%</td>
</tr>
<tr>
<td>16.</td>
<td>Philippines</td>
<td>752</td>
<td>1.2%</td>
<td>±0.4%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>No.</th>
<th>Country</th>
<th>Trials</th>
<th>Validation</th>
<th>σ</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.</td>
<td>Belgium</td>
<td>606</td>
<td>1.0%</td>
<td>±0.4%</td>
</tr>
<tr>
<td>18.</td>
<td>Austria</td>
<td>2100</td>
<td>0.9%</td>
<td>±0.2%</td>
</tr>
<tr>
<td>19.</td>
<td>Australia</td>
<td>711</td>
<td>0.8%</td>
<td>±0.3%</td>
</tr>
<tr>
<td>20.</td>
<td>Russia</td>
<td>2606</td>
<td>0.7%</td>
<td>±0.2%</td>
</tr>
<tr>
<td>21.</td>
<td>Mexico</td>
<td>627</td>
<td>0.5%</td>
<td>±0.3%</td>
</tr>
<tr>
<td>22.</td>
<td>China</td>
<td>627</td>
<td>0.5%</td>
<td>±0.3%</td>
</tr>
<tr>
<td>23.</td>
<td>Canada</td>
<td>1066</td>
<td>0.5%</td>
<td>±0.2%</td>
</tr>
<tr>
<td>24.</td>
<td>Spain</td>
<td>1932</td>
<td>0.5%</td>
<td>±0.2%</td>
</tr>
<tr>
<td>25.</td>
<td>Malaysia</td>
<td>529</td>
<td>0.4%</td>
<td>±0.3%</td>
</tr>
<tr>
<td>26.</td>
<td>Romania</td>
<td>1039</td>
<td>0.3%</td>
<td>±0.2%</td>
</tr>
<tr>
<td>27.</td>
<td>India</td>
<td>2325</td>
<td>0.1%</td>
<td>±0.1%</td>
</tr>
<tr>
<td>28.</td>
<td>Vietnam</td>
<td>2517</td>
<td>0%</td>
<td>±0%</td>
</tr>
<tr>
<td>29.</td>
<td>Egypt</td>
<td>727</td>
<td>0%</td>
<td>±0%</td>
</tr>
<tr>
<td>30.</td>
<td>Turkey</td>
<td>651</td>
<td>0%</td>
<td>±0%</td>
</tr>
<tr>
<td>31.</td>
<td>Israel</td>
<td>591</td>
<td>0%</td>
<td>±0%</td>
</tr>
</tbody>
</table>
Further Results

- 36k trials (40.7%) comprise $\geq 2$ resolvers
- 3k trials (3.5%) comprise $\geq 2$ resolvers from different ASes
- 1.3k (1.5%) were negative but contained DNSKEY query
  - Trials with one and with multiple resolvers
  - DNSKEY query is a weak validation indicator

- Some clients use mixed validating and non-validating resolvers
  - Get SERVFAIL from validator, fall back to non-validator
  - Our test yields negative result in case of mixed validation
  - **Except** when application aborts waiting for name resolution

⇒ Effect of mixed validation needs to be investigated further
What's next?

- Raw data (anonymized) will be available in a few days
  - http://dnssec.vs.uni-due.de
- Paper with details currently under peer-review
- Want to contribute? Add HTML snippet to your website
  - Privacy note: discloses to us client address, referer, user-agent
- Pending enhancements
  - Minimize traffic of duplicate tests
  - Generate online statistics
- Related project: VeriSign prefetch test
  - Less privacy invasive
  - http://validator-search.verisignlabs.com/