Experimental Results on DNSSEC Record Delivery

Austin Hounsel ¹  Eric Rescorla ²
Chris Wood ³  Nick Feamster ³

¹Princeton University
²Mozilla
³Cloudflare

2022-07-28
Lots of DNSSEC Validation
Nearly all of this is by recursive resolvers

- No major operating system does endpoint DNSSEC validation by default
- Browsers don’t do it either
- This is limiting
  - A number of DNSSEC-based mechanisms need endpoint validation (e.g., DANE)
Why don’t endpoints validate?

- Concerns about performance
  - More requests may be slower

- **Concerns about breakage**
  - If DNSSEC records aren’t delivered this is indistinguishable from an attack
  - Resolvers are supposed to hard-fail
  - Any significant rate of non-delivery will create unacceptable failure rates
  - Little actual data
Experimental Setup

- Set up some domains with known contents
  - Correct DNSSEC records
  - Some other less-common records
- Use Firefox as a measurement platform
  - Randomly select a sample of clients
  - Each client directly resolves the relevant records via UDP and TCP
    - Bypassing the system resolver
  - Measure the success rate
Queries

- A record via the Firefox `dns.resolve()` API
- A records with all values of DO and CD
- DNSKEY
- HTTPS SVCB record.
- SMIMEA record.
- Small (8 bytes) and large (1023 bytes) records with code points in “Expert Review” and “Private Use” ranges
## Results

<table>
<thead>
<tr>
<th>Query</th>
<th>Failure Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0.022 (0.021–0.023)</td>
</tr>
<tr>
<td>A (CD=1)</td>
<td>0.024 (0.023–0.024)</td>
</tr>
<tr>
<td>A (DO=1)</td>
<td>0.387 (0.385–0.389)</td>
</tr>
<tr>
<td>A (DO=1, CD=1)</td>
<td>0.388 (0.386–0.390)</td>
</tr>
<tr>
<td>DNSKEY</td>
<td>0.023 (0.022–0.023)</td>
</tr>
<tr>
<td>SMIMEA</td>
<td>0.140 (0.138–0.141)</td>
</tr>
<tr>
<td>HTTPS</td>
<td>0.065 (0.064–0.066)</td>
</tr>
<tr>
<td>NEWONE</td>
<td>0.203 (0.201–0.204)</td>
</tr>
<tr>
<td>NEWTWO</td>
<td>0.214 (0.212–0.216)</td>
</tr>
<tr>
<td>NEWTHREE</td>
<td>0.281 (0.279–0.283)</td>
</tr>
<tr>
<td>NEWFOUR</td>
<td>0.289 (0.287–0.291)</td>
</tr>
<tr>
<td>A (WebExt API)</td>
<td>0.004 (0.004–0.005)</td>
</tr>
</tbody>
</table>
Impact

- It’s not safe to enable endpoint DNSSEC validation over Do53
  - At least not for end-user clients
  - The situation is different for servers
- Might be safe to enable over DoH/DoT
  - Public resolvers do a lot better
  - Might be the case that ADD-advertising resolvers do better
- Somewhat practical to deploy other record types
  - As long as it fails safe if they are not found
  - HTTPS looks especially good
Questions?