DNSSEC & fragmentation
a prickly combination

Roland van Rijswijk - Deij
roland.vanrijsijk@surfnet.nl
The problem in 1 slide
Extent of the problem

• 9% of all internet hosts may have problems receiving fragmented UDP messages [1];

• 2% – 10% of all resolving name servers experience problems receiving fragmented DNS responses [2]


The problem biting us for real

• SURFnet deployed DNSSEC for surfnet.nl in 2010 (first secure delegation in .nl)

• Within a week we had problems

• Cause: largest ISP (2.5M users) in the country blocks fragments on service network edge

• Helpdesk: “SURFnet is doing something wrong” :-(
• Resolving name servers SHOULD advertise a proper max. response size to avoid fragmentation issues [RFC 2671BIS (DRAFT)];

Not explicitly stated in standards yet, nor widely implemented;

• Until then: set maximum response size at some authoritative name servers
Resolver experiments (1)
Normal operations

![Graph showing response times for different systems](image-url)
Resolver experiments (2)
Blocking fragments

Response time (ms.) [0/5 altered Authoritative Name Servers]

- Windows Server 2012
- Unbound
- BIND

- Time x10 (!)
- Time x2
- Time x100+ (!!!)

[24,195;12,167] $\bar{x}=17,787$
Resolver experiments (3) Max. resp. size on 1 authNS

Response time (ms.) [1/5 altered Authoritative Name Servers]

Max. = 16,162

Unbound: 638 ms.
BIND: 2.126 ms.
Resolver experiments (4)
Max. resp. size on 2 authNS
## Experiment on live authNS

<table>
<thead>
<tr>
<th>Traffic (IPv4 + IPv6)</th>
<th>Normal Operations</th>
<th>Max. response size 1232 bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fragmented responses</td>
<td>28.9%</td>
<td>0.0%*</td>
</tr>
<tr>
<td>Fragment receiving resolvers</td>
<td>57.3%</td>
<td>0.0%*</td>
</tr>
<tr>
<td>Truncated UDP responses</td>
<td>0.8%</td>
<td>0.9%</td>
</tr>
<tr>
<td>ICMP FRTE messages</td>
<td>5649/h</td>
<td>&lt; 1/h*</td>
</tr>
<tr>
<td>ICMP FRTE sending resolvers</td>
<td>1.3%</td>
<td>0.0%*</td>
</tr>
<tr>
<td>Total retries</td>
<td>25.8%</td>
<td>25.5%</td>
</tr>
</tbody>
</table>

*Statistically significant difference between experiments*
Rise in truncated answers

**Experiment:**
- Querying 995 zones in .com, .edu, .mil, .net and .nl
- All zones are signed and have a www-node
- Results:

<table>
<thead>
<tr>
<th>Max. response</th>
<th>A for www</th>
<th>AAAA for www</th>
<th>DNSKEY</th>
</tr>
</thead>
<tbody>
<tr>
<td>4096</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>1472</td>
<td>1.8%</td>
<td>1.8%</td>
<td>8.1%</td>
</tr>
<tr>
<td>1232</td>
<td>2.9%</td>
<td>3.5%</td>
<td><strong>40.0%</strong></td>
</tr>
</tbody>
</table>

How to move forward?


• Make sure your resolver(s) set the maximum response size to something that actually works!

Questions? Remarks?

Read our blog: https://dnssec.surfnet.nl/