A testbed for evaluating Post-Quantum Algorithms for the DNS

Elmer Lastdrager
Research Engineer at SIDN Labs
A testbed for evaluating post-quantum algorithms for the DNS

Elmer Lastdrager | PQC Conference

8 November 2023
A testbed for evaluating post-quantum algorithms for the DNS
Where can I find www.example.nl?
Where can I find www.example.nl?
Where can I find www.example.nl?

Ask example.nl

Where can I find www.example.nl?
Where can I find www.example.nl?

The address is 2a00:d78:0:712:94:198:159:35

nl

example.nl
Where can I find www.example.nl?

The address is 2a00:d78:0:712:94:198:159:35
Why is it when something happens, it's always you three?

IT'S ALWAYS DNS

ABRAHAM LINCOLN
.nl = the Netherlands
17M inhabitants
6.3M domain names
3.8M DNSSEC-signed
4.0B DNS queries/day
8.6B NTP queries/day
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 1

Queries
  > example.nl: type AAAA, class IN

Answers
  > example.nl: type AAAA, class IN, addr 2a00:d78:0:712:94:198:159:35
    Name: example.nl
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x001)
    Time to live: 3367

Data length: 16
AAAA Address: 2a00:d78:0:712:94:198:159:35

Additional records

Response Length (dns.resp.len), 2 bytes
Packets: 44 - Displayed: 6 (13.6%) - Dropped: 0 (0.0%) - Profile: Default
DoH, DoT, DNScrypt

https://dns4all.eu/

X25519Kyber768

DNSSEC
www.example.nl

Where can I find www.example.nl?

The address is 2a00:d78:612:94:198:159:35

The address is 2a00:d78:612:94:198:159:35

example.nl

nl
Where can I find www.example.nl?
.nl DNSSEC keys

example.nl
.nl DNSSEC keys

example.nl
Root DNSSEC keys

- nl

- example.nl
A testbed for evaluating post-quantum algorithms for the DNS
Requirements
<table>
<thead>
<tr>
<th>Prio</th>
<th>Requirement</th>
<th>Good</th>
<th>Accepted Conditionally</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1</td>
<td>Signature Size</td>
<td>≤ 1,232 bytes</td>
<td>—</td>
</tr>
<tr>
<td>#2</td>
<td>Validation Speed</td>
<td>≥ 1,000 sig/s</td>
<td>—</td>
</tr>
<tr>
<td>#3</td>
<td>Key Size</td>
<td>≤ 64 kilobytes</td>
<td>&gt; 64 kilobytes</td>
</tr>
<tr>
<td>#4</td>
<td>Signing Speed</td>
<td>≥ 100 sig/s</td>
<td>—</td>
</tr>
</tbody>
</table>

Table 2: Requirements for quantum-safe algorithms.
A testbed for evaluating post-quantum algorithms for the DNS
Thank you for your attention!

Elmer Lastdrager
elmer.lastdrager@sidn.nl

@elmerlastdrager
@elmer@c.im

https://www.sidnlabs.nl/en
A testbed for evaluating Post-Quantum Algorithms for the DNS

Elmer Lastdrager
Research Engineer at SIDN Labs