NSEC3 Hash Performance

Yuri Schaeffer
Matthijs Mekking
Research question

• What is the worst case effect of the number of NSEC3 hash iterations on the query load of a recursive name server?
  – NXDOMAIN response only
  – Unique queries, no cache responses
  – Different next closer name each time
  – Number determined by authoritative server, but affects validators too.

http://www.nlnetlabs.nl/
Test setups

Player
- tcpreplay, tcpdump

Validator
- Unbound

Authority
- NSD (root and qx)
Test setups

Player
- tcpreplay, tcpdump

Authority
- NSD (root and qx)
How many iterations?

- From RFC 5155:

<table>
<thead>
<tr>
<th>Key Size</th>
<th>Iterations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1024</td>
<td>150</td>
</tr>
<tr>
<td>2048</td>
<td>500</td>
</tr>
<tr>
<td>4096</td>
<td>2500</td>
</tr>
</tbody>
</table>
Running the tests

• For each NSD configuration, do:
  - Start NSD
  - Calculate maximum query rate
  - Start Unbound
  - Run tcpreplay
  - Stop Unbound
  - Stop NSD
Validator

Unbound

Maximum query rate [qps]

Number of hash iterations $k$

- 1024 bit key
- 2048 bit key
- 4096 bit key

http://www.nlnetlabs.nl/
Authority

NSD

Maximum query rate [qps]

Number of hash iterations k

1024 bit key
2048 bit key
4096 bit key

http://www.nlnetlabs.nl/
Observations

• Validator:
  - Key length has more impact on performance than iteration count
  - 150+ iterations halves performance

• Authority:
  - Performance independent of key length
  - 100 iterations halves performance
• http://www.nlnetlabs.nl
• dnsop mailing list