Interoperable DNS Server Cookies

Willem Toorop
Ondřej Surý
Donald E. Eastlake 3rd
Mark Andrews

draft-sury-toorop-dnsop-server-cookies-00
Why DNS Cookies

- DNS Native Protection Mechanism against Amplification Attacks
- To be helpful it needs to be enabled everywhere
- Multi-vendor cooperation desirable
DNS Cookies Operation

- Valid Server Cookie? Large answers
- Valid Server Cookie? RRL Disabled!
DNS Cookies in Anycast
Hackthon @IETF104 Results

- draft-sury-toorop-dns-cookies-algorithms-00
- Witold Krecicki, Pieter Lexis, Willem Toorop
- Interoperable Server Cookies for:
  
  ![BIND](image1)
  ![PowerDNS](image2)
  ![unbound](image3)
  ![KnotDNS](image4)
  ![NSD](image5)
Donald & Mark joined

• Merge of:
  - draft-sury-toorop-cookie-algorithms-00
  - draft-eastlake-dnsop-server-cookies-00

• Into
  - draft-sury-toorop-dnsop-server-cookies-00
Include client IP in Server Cookie hash calculation

Use only SipHash2.4 with this Version

IANA sub-registry “DNS Server Cookie versions”:

<table>
<thead>
<tr>
<th>Version</th>
<th>Algorithm</th>
<th>Server Cookie Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Reserved</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>SIPHASH24</td>
<td>16</td>
</tr>
<tr>
<td>2-240</td>
<td>Unassigned</td>
<td>-</td>
</tr>
<tr>
<td>240-254</td>
<td>Private use</td>
<td>-</td>
</tr>
<tr>
<td>255</td>
<td>Reserved</td>
<td>-</td>
</tr>
</tbody>
</table>

Operator advise on Server Secret roll-over

Implementation advise for smooth roll-over

Appendix with Test vectors
Hackthon @IETF105 Results

- Witold Krecicki, Ondřej Surý, Pieter Lexis, Willem Toorop

- Interoperable Server Cookies for:

  - BIND
  - 9
  - POWERDNS
  - NSD
  - unbound
3. Constructing a Client Cookie

The Client Cookie is a nonce and should be treated as such. It is RECOMMENDED but not required that the following pseudorandom function be used to construct the Client Cookie:

\[
\text{Client-Cookie} = \text{MAC\_Algorithm}(\text{Client IP Address} | \text{Server IP Address}, \text{Client Secret})
\]

where "|" indicates concatenation.

- Source IP for Client cookie is impractical
- Text to RECOMMEND it for Stub resolvers
Next steps

- Upload WG version with new Client Cookie generation advise
- Test interoperability on production quality implementations

https://github.com/NLnetLabs/draft-sury-toorop-dns-cookies-algorithms