Recommendations for DNS Privacy Service Operators

draft-dickinson-dprise-bcp-op-00

Sara Dickinson
Roland van Rijswijk-Deij
Allison Mankin
Benno Overeinder

sara@sinodun.com
roland.vanrijswijk@surfnet.nl
allison.mankin@gmail.com
benno@nlnetLabs.nl
Overview

• Document is a work in progress - currently an IETF Internet Draft

• Document Goals:

1. **Operational, policy and security** considerations for DNS operators who offer DNS Privacy services
   • DoT, but need to consider DoH in more detail

2. **DNS Privacy Policy and Practices Statements** framework
## Current Deployed DNS Privacy Services

<table>
<thead>
<tr>
<th></th>
<th>Standalone</th>
<th>Large Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DoT</strong></td>
<td>• 20 test servers</td>
<td>• <strong>Quad9</strong> (9.9.9.9)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Cloudflare</strong> (1.1.1.1)</td>
</tr>
<tr>
<td><strong>DoH</strong></td>
<td>• Google</td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="https://dns.google.com/experimental">https://dns.google.com/experimental</a></td>
<td>• <strong>Cloudflare</strong></td>
</tr>
<tr>
<td></td>
<td>• Few other test servers</td>
<td><a href="https://cloudflare-dns.com/dns-query">https://cloudflare-dns.com/dns-query</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="https://mozilla.cloudflare-dns.com/dns-query">https://mozilla.cloudflare-dns.com/dns-query</a></td>
</tr>
</tbody>
</table>
This presentation

- Latest revision of document based on feedback from this WG and RIPE BCOP (fairly big changes)

- Open discussion - where do we go from here?
  - Continue working on this in DPRIVE?
Document Updates

• Added Document section for reference (Appendix)

• Significantly re-framed Recommendations section:
  • Threats (RFC7626/RFC6973) vs mitigations
    • On the wire
    • In the server
    • Upstream

• Expanded section on Pseudo/Anonymisation

• DPPPS framework - added comparison of policies
Document Updates

- Mitigations actions separated into 3 categories
- ‘SHOULD do (if applicable)’
  - Mitigations (minimal compliance)
  - Optimisations (moderate compliance)
  - Additional options (maximal compliance)
Definitions

- Privacy-enabling DNS server (from RFC8310):
  - A DNS server that implements DOT
  - DoT server that can be authenticated (Cert or SPKI)

- DNS privacy service:
  - Privacy-enabling server +
  - Documentation: informal statement of policy and practice OR formal DPPPS

Need to add DoH…
On the wire

CONSIDER: Protocol and service

- Transport (DoT and/or DoH)
- Authentication
- Certificate management
- Protocol (Padding, SR, Cookies, performance)
- Availability & service options
At rest on the server

CONSIDER: Data Handling and Minimisation

- Transient data (real-time monitoring)
- Logging
- Tracking
- Data access
- Cache snooping
At rest on the server

CONSIDER: Data Handling and Minimisation

- Review current techniques for data minimisation
  - Focus on IP address
  - Talk about pseudonymization vs anonymization
  - Survey of current options (Appendix) - no clear choice
Data sent upstream

CONSIDER: Queries and shared data

- Protocol (QNAME min, ECS, local root)
- Traffic obfuscation
- Data sharing (some overlap with ‘Data at rest’)
Policy comparisons

- Try to analyse Google/Cloudflare/Quad9/OpenDNS using the framework of the suggested DPPPS
- Try to reduce lots of text to easier to inspect tables (needs work)
- GOAL: Consider how useful this comparison is for users and operators
Feedback & Open Questions

- Recommendations: Does the new structure address previous comments?
- Feedback on new content
- Continue working on it here?