Recommendations for DNS Privacy Service Operators

draft-dickinson-dprive-bcp-op-00

Sara Dickinson sara@sinodun.com
Roland van Rijswijk-Deij roland.vanrijswijk@surfnet.nl
Allison Mankin allison.mankin@gmail.com
Benno Overeinder 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

	Standalone	Large Scale
DoT	• 20 test servers	• Quad9 (9.9.9.9) • Cloudflare (1.1.1.1)

DoH*	• Google
	https://dns.google.com/experimental
	• Few other test servers
		• Cloudflare
		  • https://cloudflare-dns.com/dns-query
		  • https://mozilla.cloudflare-dns.com/dns-query

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)

Need to add DoH…

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

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?