Recommendations for DNS Privacy Service Operators

draft-dickinson-dprive-bcp-op-00

Presenter: Benno Overeinder

Co-authors: Sara Dickinson
Roland van Rijswijk-Deij,
Allison Mankin

Brief history of DNS Privacy

Date	Event
1987	DNS is born - protocol is clear text
Sep 2014	IETF DPRIVE WG created (post Snowden)
Aug 2015	RFC7626: DNS Privacy Considerations
May 2016	RFC7858: DNS-over-TLS (DOT*)
Feb 2017	RFC8094: DNS-over-DTLS (Exp, no imp to date)
Sep 2017	IETF DOH (DNS-over-HTTP) WG created
Nov 2017	Quad9 (9.9.9.9) offer DOT anycast
Mar 2018	RFC8310: Authentication for DNS-over-(D)TLS
Mar 2018	Cloudflare launch 1.1.1.1 with DOT and DOH
Apr 2018	Google have experimental DOH DOH draft in WGCL

*Acronym used here

Overview

- Document is a work in progress - currently an IETF Internet Draft
  - I-D: draft-dickinson-dprive-bcp-op-01

- 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. Framework for **DNS Privacy Policy and Practices Statements**
   - Analogous to *DNSSEC Policies and DNSSEC Practice Statements* described in RFC6841.

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

Status

- Submitted to IETF for initial review, presented at IETF 101 in March, lots of feedback there, support to work on it there

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

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

This presentation

- Quick overview of document content
- Discuss feedback to date
- Open discussion

Document overview

- Firstly, some definitions
- Operational guidance (features, capabilities)
- Operational management (network)
- Data handling
- Policy and Practice Statement framework

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

Operational Guidance

GOALS: Reduce user tracking and leaks in upstream queries

- Server capabilities to maximise DNS privacy:
  - On the wire
  - At rest on the server
  - Data sent upstream

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’)

DNS Privacy Policy + Practice Statement DP-PPS

- **Policy**:
  - Specify data collection & retention, sharing, exceptions, third-party affiliations, data correlation
- **Practice**:
  - Temp or perm deviations from policy
  - What capabilities are provided on address/ports
    - Filtering, EDNS(0) Client subnet usage
  - Authentication credentials
  - Contact & support

DNS Privacy Policy + Practice Statement DP-PPS

Very often no technical solutions to validate the Policy or Practice

- **Enforcement/accountability:**
  - Independent monitoring of capabilities, filtering, etc.
  - Technical vs Social vs Third-party

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

- **Generality:**
  - Many of the recommendations are applicable for any DNS service (not limited to DNS Privacy)
  - In particular, data handling in the light of GDPR
- **Approach**:
  - Feedback on organisation and content by OPSEC WG
    - Threat analysis, mitigations
    - Good, better, best options - ranged approach
  - Useful document?
    - BCP, living document, …