Recommendations for DNS Privacy Service Operators

draft-dickinson-bcp-op-00

Sara Dickinson  sara@sinodun.com

Roland van Rijswijk-Deij, Allison Mankin, Benno Overeinder
Overview

- Operational, policy and security considerations for DNS operators who offer DNS Privacy services
  - Include, but are not limited to, DNS-over-TLS.

- Framework to assist writers of *DNS Privacy Policy and Practices Statements*
  - Analogous *DNSSEC Policies and DNSSEC Practice Statements* described in RFC6841.
Status

• First cut, lots of TODOs

• Submitted here for initial review and for feedback on the best forum for future versions of this document.
  • RIPE BCP WG?

• Feedback from Stéphane (thanks!)
Existing Implementation Guidance

• Note that draft-ietf-dprive-dtls-and-tls-profiles (RFC8310) already specifies a bunch of things

  • **MUST**: RFC7525 (TLS BCP), TLS session resumption, Raw public keys, etc.

  • **SHOULD**: EDNS(0) Padding, EDNS(0) Client Subnet

  • Bits and pieces in RFC7858 (SPKI)
Definitions

- **Privacy-enabling DNS server:**
  - From RFC8310
  - A DNS server that implements DNS-over-TLS and may optionally implement DNS-over-DTLS.
  - The server should also offer at least one of the credentials described in Section 8 of RFC8310 (Cert, SPKI)
  - Implement the (D)TLS profile described in Section 9 of RFC8310.

- **DNS privacy service:**
  The service that is offered via a privacy-enabling DNS server and is documented either in an informal statement of policy and practice with regard to users privacy or a formal DPPPS.
Operational Guidance

- Server capabilities to maximise DNS privacy:
  - **SHOULD**: QNAME min, Connection management (Keepalive/DSO), not require TLS SR, etc.
  - **MAY**: Port 443, Root zone on loopback, Aggressive Use of DNSSEC-Validated Cache, etc.
- Client query obfuscation - mix with generated traffic
Certificate management

• RECOMMEND:
  • Choose a short, memorable authentication name
  • Automate the generation and publication of certificates
  • Monitor certificates to prevent accidental expiration of certificates

Might seem obvious but….
Operational management

- Limitations of using a pure TLS proxy
- Anycast
- ...

...
Data Handling

- Logging and Monitoring (minimise and/or anonymise)
- Data retention (minimise and/or anonymise)
- Access to stored data (minimise)
- User tracking (don’t)
- Share data with third parties (don’t)

Might seem obvious but....
Psuedo-anonymisation and de-identification methods

- IPCCipher for pseudo-anonymisation
- Bloom filters for monitoring
- Identify so-called Indicators of Compromise (IOCs) originating from specific subnets without storing information about queries of an individual user.
- Expect more here....
DNS Privacy Policy + Practice Statement DP-PPS

• Policy:
  • Specify data collection + retention, shared, exceptions, third-party affiliations, data correlation

• Practice:
  • Temp or perm deviations
  • 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

- TODO:
  - Compare Google, Quad9, OpenDNS
  - Trusted vs Trustworthy
Major questions

- **Scope**: Authoritative section, Research Data

- **Generality**:
  - Are data handling practices issues generic (not limited to DNS Privacy… GDPR)?
  - Filtering (‘Normal’ DNS vs ‘Private’ DNS)

- **Approach**: Currently very prescriptive, could be more contextual/discursive (threat analysis, options, mitigations)

- **Does the WG want to work on this?**