Recommendations for DNS Privacy Service Operators

Presenter: Sara Dickinson sara@sinodun.com

Co-authors: Roland van Rijswijk-Deij,
Allison Mankin,
Benno Overeinder

Brief history of DNS Privacy

Date	Event
1987	DNS is born - protocol is clear text
Sep 2014	IETF DPRIVE WG created (post Snowdon)
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-bcp-op-00

- Document Goals:

1. **Operational, policy and security** considerations for DNS operators who offer DNS Privacy services
   - Current version targets operators of resolvers offering DOT But, DOH is certainly on the way…..

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

Status

- First draft, lots of TODOs
- Submitted to IETF for initial review, presented at IETF 101 in March, lots of feedback there, support to work on it there
- Presenting here to make BCOP aware of the work and get input, think about ways forward
- Still trying to understand best forum this document
  - IETF standard vs living document?

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….
  - Server that can be authenticated using either a PKIX Cert or SPKI pinset.

- **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:
  - **SHOULD**: QNAME min, not require TLS Session Resumption, no EDNS Client subnet, 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

Operational management

- Limitations of using a pure TLS proxy
  - Hides source address of client, can limit DNS
- Anycast considerations
- …

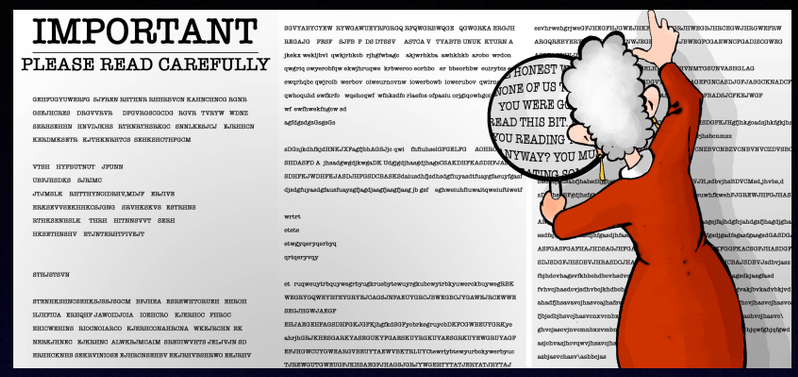
Data Handling

- 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)

Psuedo-anonymisation and de-identification methods

- **ipcipher** for psuedo-anonymisation
- **Bloom fliters** 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, 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
- **TODO**:
  - Compare Google, Quad9, OpenDNS, Cloudflare
  - Trusted vs Trustworthy

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**:
  - Currently very prescriptive, could be more contextual and discursive
    - Threat analysis, mitigations
    - Good, better, best options - ranged approach

Would BCOP be interested in adoption now or in the future?

Thank you!

More information at:
dnsprivacy.org