Recommendations for DNS Privacy Service Operators

draft-ietf-dprive-bcp-op-00

Sara Dickinson
Roland van Rijswijk-Deij
Allison Mankin
Benno Overeinder

Overview of BCP

- Document Goals:

1. **Operational, policy and security** considerations for DNS operators who offer DNS Privacy services
   - DoT and/or DoH

2. **DNS Privacy Policy and Practices Statements** framework (akin to the DNSSEC PPS)

Where are we with the draft?

- Jul 2018: Presented in DPRIVE (Montreal)
- Aug 2018: Adopted by WG
- Mar 2019: Latest rev -02
  - No major changes since adoption

Document Structure

1. Operational, policy and security considerations

- Consider 3 contexts
  - On the wire (stub to resolver)
  - In the server (at rest)
  - Upstream (including data sharing)

- For each, enumerate the threats & recommend mitigations

- Mitigations - 3 categories
  - Mitigations (minimal compliance)
  - Optimisations (moderate compliance)
  - Additional options (maximal compliance)

Document Structure

1. Operational, policy and security considerations

- Consider 3 contexts
  - On the wire (stub to resolver)
  - In the server (at rest)
  - Upstream (including data sharing)

RFC7626-bis

RFC6973

- For each, enumerate the threats & recommend mitigations

- Mitigations - 3 categories
  - Mitigations (minimal compliance)
  - Optimisations (moderate compliance)
  - Additional options (maximal compliance)

Document Structure

1. Operational, policy and security considerations

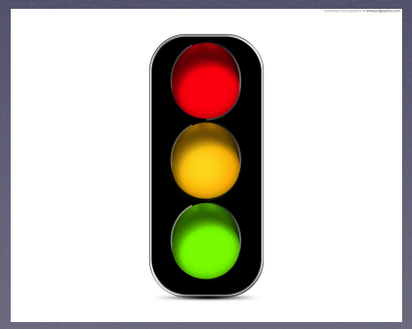
- Consider 3 contexts
  - On the wire (stub to resolver)
  - In the server (at rest)
  - Upstream (including data sharing)

RFC7626-bis

RFC6973

- For each, enumerate the threats & recommend mitigations

- Mitigations - 3 categories
  - Mitigations (minimal compliance)
  - Optimisations (moderate compliance)
  - Additional options (maximal compliance)



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 Minimisation and Handling

- Transient data (real-time monitoring)
- Logging - including (psuedo-)anonymisation
- Tracking/correlation
- Data access
- Cache snooping

Data sent upstream

CONSIDER: Queries and share data

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

Document Structure
2. Practice & Policy Statement

- **Framework** which outlines what **categories of details** operators should provide about their service (~2.5 pages)
- Usefulness?
  - Consistency in representation for user consumption/analysis
    - 3 QUAD services: 1000's of lines of text, written in different styles in multiple locations
  - Informed user choice of provider
  - Basis for external audit or monitoring

Document Structure

2. Practice & Policy Statement

- **AS AN EXERCISE:** Use DPPPS framework to analyse

Google/Cloudflare/Quad9/OpenDNS

- Results on https://dnsprivacy.org/wiki/display/DP/Comparison+of+policy+and+privacy+statements (reference to this in the draft)

Policy comparison

Policy

List Item	1	2	3				4	5		6	7	
Redirect NXDOMAIN	**IP address are PII**	**IP address logging**	**Clear list of what data stored and for how long**	**Share anonymized data with partners**	**Share identifiable data with partners**	**Share or sell data to third parties**	**Exceptions to collection for attack analysis**	**non-profit**	**Partners**	**Combine DNS data with other data sources**	**Redirect NXDOMAIN**	**Block domains**
Quad9 Secure	Y	N	Y	Y	N	N	Y	Y	IBM PCH GCA	N	N	Y
Quad9 Unsecured	Y	N	Y	Y	N	N	Y	Y		N	N	N
Cloudflare	Y	N	Y	Y	N	N	N	N	APNIC	N	N	?
Cloudflare DoH	Y	N	Y	Y	N	N	N	N	Mozilla/ Firefox	N	N	?
Google	N	Y(1)	Y	?	?	?	N	N	?	N	N	N(1)
OpenDNS	Y	Y	N	?	Y	Y	?	N	?	Y	N	?

(1) Only in temporary logs

Policy comparison

Policy

List Item	1	2	3				4		5	6	7	
Redirect NXDOMAIN	**IP address are PII**	**IP address logging**	**Clear list of what data stored and for how long**	**Share anonymized data with partners**	**Share identifiable data with partners**	**Share or sell data to third parties**	**Exceptions to collection for attack analysis**	**non-profit**	**Partners**	**Combine DNS data with other data sources**	**Redirect NXDOMAIN**	**Block domains**
Quad9 Secure	Y	N	Y	Y	N	N	Y	Y	IBM PCH GCA	N	N	Y
Quad9 Unsecured	Y	N	Y	Y	N	N	Y	Y		N	N	N
Cloudflare	Y	N	Y	Y	N	N	N	N	APNIC	N	N	?
Cloudflare DoH	Y	N	Y	Y	N	N	N	N	Mozilla/ Firefox	N	N	?
Google	N	Y(1)	Y	?	?	?	N	N	?	N	N	N(1)
OpenDNS	Y	Y	N	?	Y	Y	?	N	?	Y	N	?

(1) Only in temporary logs

Policy comparison

Policy

List Item	1	2	3				4	5		6	7	
Redirect NXDOMAIN	**IP address are PII**	**IP address logging**	**Clear list of what data stored and for how long**	**Share anonymized data with partners**	**Share identifiable data with partners**	**Share or sell data to third parties**	**Exceptions to collection for attack analysis**	**non-profit**	**Partners**	**Combine DNS data with other data sources**	**Redirect NXDOMAIN**	**Block domains**
Quad9 Secure	Y	N	Y	Y	N	N	Y	Y	IBM PCH GCA	N	N	Y
Quad9 Unsecured	Y	N	Y	Y	N	N	Y	Y		N	N	N
Cloudflare	Y	N	Y	Y	N	N	N	N	APNIC	N	N	?
Cloudflare DoH	Y	N	Y	Y	N	N	N	N	Mozilla/ Firefox	N	N	?
Google	N	Y(1)	Y	?	?	?	N	N	?	N	N	N(1)
OpenDNS	Y	Y	N	?	Y	Y	?	N	?	Y	N	?

(1) Only in temporary logs

Practice comparison

Practice

List Item	2								3	4	5	6
	DNSSEC	EDNS(0) Padding	OOOR	EDNS(0) Keepalive	Query Name Minimization	Send ECS	Respect client ECS	Local root zone	Auth Domain Name	SPKI pinset	Juristdiction (TBD)	Obtaining consent (TBD)
Quad9 Secure	Y	N	N	N	N	N	?	N	Y	N		
Quad9 Unsecured	N	N	N	N	N	N	?	N	Y	N		
Cloudflare	Y	Y	Y	N	Y	N	-	Y	Y	N		
Cloudflare DoH	Y	Y	Y	N	Y	N	-	Y	-	-		
Google	Y	N	Y	N	N	Y	Y	N	Y	N		
OpenDNS	N	-	-	-	?	?	?	?	-	-		

(1) Only in exceptional circumstances

Practice comparison

Practice

List Item	2								3	4	5	6
	DNSSEC	EDNS(0) Padding	OOOR	EDNS(0) Keepalive	Query Name Minimization	Send ECS	Respect client ECS	Local root zone	Auth Domain Name	SPKI pinset	Juristdiction (TBD)	Obtaining consent (TBD)
Quad9 Secure	Y	N	N	N	N	N	?	N	Y	N		
Quad9 Unsecured	N	N	N	N	N	N	?	N	Y	N		
Cloudflare	Y	Y	Y	N	Y	N	-	Y	Y	N		
Cloudflare DoH	Y	Y	Y	N	Y	N	-	Y	-	-		
Google	Y	N	Y	N	N	Y	Y	N	Y	N		
OpenDNS	N	-	-	-	?	?	?	?	-	-		

(1) Only in exc[illegible]umstances

Practice comparison

Practice

List Item	2								3	4	5	6
	DNSSEC	EDNS(0) Padding	OOOR	EDNS(0) Keepalive	Query Name Minimization	Send ECS	Respect client ECS	Local root zone	Auth Domain Name	SPKI pinset	Juristdiction (TBD)	Obtaining consent (TBD)
Quad9 Secure	Y	N	N	N	N	N	?	N	Y	N		
Quad9 Unsecured	N	N	N	N	N	N	?	N	Y	N		
Cloudflare	Y	Y	Y	N	Y	N	-	Y	Y	N		
Cloudflare DoH	Y	Y	Y	N	Y	N	-	Y	-	-		
Google	Y	N	Y	N	N	Y	Y	N	Y	N		
OpenDNS	N	-	-	-	?	?	?	?	-	-		

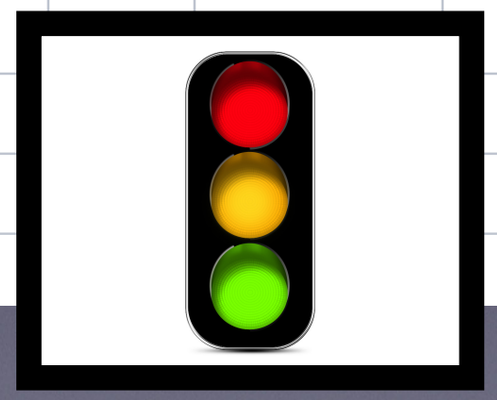
(1) Only in exceptional circumstances

Practice comparison

Practice

List Item	2								3	4	5	6
	DNSSEC	EDNS(0) Padding	OOOR	EDNS(0) Keepalive	Query Name Minimization	Send ECS	Respect client ECS	Local root zone	Auth Domain Name	SPKI pinset	Juristdiction (TBD)	Obtaining consent (TBD)
Quad9 Secure	Y	N	N	N	N	N	?	N	Y	N		
Quad9 Unsecured	N	N	N	N	N	N	?	N	Y	N		
Cloudflare	Y	Y	Y	N	Y	N	-	Y	Y	N		
Cloudflare DoH	Y	Y	Y	N	Y	N	-	Y	-	-		
Google	Y	N	Y	N	N	Y	Y	N	Y			
OpenDNS	N	-	-	-	?	?	?	?	-			

(1) Only in exceptional circumstances



Monitoring of DoT servers (dnsprivacy.org)

Configuration Matrix		TLS	TLS 443	Strict Name	Strict SPKI	Cert 0	Cert 14	QNAME min	RTT 250	DNSSEC	Keepalive	Padding	TLS 1.3	OOOR
dnsovertls.sinodun.com	v4	✓	✓	✓	✓	✓	✓	!	✓	✓	✓	✓	!	✓
	v6	✓	✓	✓	✓	✓	✓	!	✓	✓	✓	✓	!	✓
dnsovertls1.sinodun.com	v4	✓	✓	✓	✓	✓	✓	!	✓	✓	✓	✓	!	✓
	v6	✓	✓	✓	✓	✓	✓	!	✓	✓	✓	✓	!	✓
getdnsapi.net	v4	✓	!	✓	✓	✓	✓	✓	✓	✓	!	!	!	!
	v6	✓	!	✓	✓	✓	✓	✓	✓	✓	!	!	!	!
dns.quad9.net	v4	✓	!	✓	●	✓	✓	!	✓	✓	!	!	✓	!
	v6	✓	!	✓	●	✓	✓	!	✓	✓	!	!	✓	!
dns.google	v4	✓	!	✓	●	✓	✓	!	✓	✓	!	!	✓	✓
	v6	✓	!	✓	●	✓	✓	!	✓	✓	!	!	✓	✓
1dot1dot1dot1.cloudflare-dns.com	v4	✓	!	✓	●	✓	✓	✓	✓	✓	!	✓	✓	✓
	v6	✓	!	✓	●	✓	✓	✓	✓	✓	!	✓	✓	✓
security-filter-dns.cleanbrowsing.org	v4	✓	!	✓	●	✓	✓	!	!	✓	!	!	!	!
	v6	●	●	●	●	●	●	●	●	●	●	●	●	●
unicast.censurfridns.dk	v4	✓	!	✓	✓	✓	✓	!	✓	✓	!	!	!	✓
	v6	✓	!	✓	✓	✓	✓	!	✓	✓	!	!	!	✓
kaitain.restena.lu	v4	✓	!	✓	✓	✓	✓	✓	✓	✓	!	!	!	!
	v6	✓	!	✓	✓	✓	✓	✓	✓	✓	!	!	!	!
dnsovertls3.sinodun.com	v4	✓	!	!	✓	!	!	!	✓	✓	✓	✓	✓	✓
	v6	!	!	!	!	!	!	!	!	!	!	!	!	!
dnsovertls2.sinodun.com	v4	✓	!	✓	✓	✓	✓	✓	✓	✓	✓	✓	!	!

Monitoring of DoT servers (dnsprivacy.org)

Configuration Matrix		TLS	TLS 443	Strict Name	Strict SPKI	Cert 0	Cert 14	QNAME min	RTT 250	DNSSEC	Keepalive	Padding	TLS 1.3	OOOR
dnsovertls.sinodun.com	v4	✓	✓	✓	✓	✓	✓	!	✓	✓	✓	✓	!	✓
	v6	✓	✓	✓	✓	✓	✓	!	✓	✓	✓	✓	!	✓
dnsovertls1.sinodun.com	v4	✓	✓	✓	✓	✓	✓	!	✓	✓	✓	✓	!	✓
	v6	✓	✓	✓	✓	✓	✓	!	✓	✓	✓	✓	!	✓
getdnsapi.net	v4	✓	!	✓	✓	✓	✓	✓	✓	✓	!	!	!	!
	v6	✓	!	✓	✓	✓	✓	✓	✓	✓	!	!	!	!
dns.quad9.net	v4	✓	!	✓	●	✓	✓	!	✓	✓	!	!	✓	!
	v6	✓	!	✓	●	✓	✓	!	✓	✓	!	!	✓	!
dns.google	v4	✓	!	✓	●	✓	✓	!	✓	✓	!	!	✓	✓
	v6	✓	!	✓	●	✓	✓	!	✓	✓	!	!	✓	✓
1dot1dot1dot1.cloudflare-dns.com	v4	✓	!	✓	●	✓	✓	✓	✓	✓	!	✓	✓	✓
	v6	✓	!	✓	●	✓	✓	✓	✓	✓	!	✓	✓	✓
	v6	●	●	●	●	●	●	●	●	●	●	●	●	●
unicast.censurfridns.dk	v4	✓	!	✓	✓	✓	✓	!	✓	✓	!	!	!	✓
	v6	✓	!	✓	✓	✓	✓	!	✓	✓	!	!	!	✓
kaitain.restena.lu	v4	✓	!	✓	✓	✓	✓	✓	✓	✓	!	!	!	!
	v6	✓	!	✓	✓	✓	✓	✓	✓	✓	!	!	!	!
dnsovertls3.sinodun.com	v4	✓	!	!	✓	!	!	!	✓	✓	✓	✓	✓	✓
	v6	!	!	!	!	!	!	!	!	!	!	!	!	!
dnsovertls2.sinodun.com	v4	✓	!	✓	✓	✓	✓	✓	✓	✓	✓	✓	!	!

Open Questions

- Splitting the document?
  - Split out data handling
  - Split out DPPPS

- Include more detailed recommendations for
  - DNS resolver + CDN or
  - Handling DoH + other traffic at the same endpoint ?

- Not much discussion on the list - are we done?
  (Currently a BCP)

Open Questions

- Splitting the document?
  - Split out data handling
  - Split out DPPPS

Varying support for both

- Include more detailed recommendations for
  - DNS resolver + CDN or
  - Handling DoH + other traffic at the same endpoint ?

- Not much discussion on the list - are we done?
  (Currently a BCP)

Questions?