

DoT or DoH: Intro to DNS Privacy

Sheryl (Shane) Hermoso
Network Operations Engineer, APNIC

DNS Privacy Risks

- “DNS is public data”
- **DNS requests** contain fields that are considered private
 - Source IP address
 - QNAME
 - (any personally identifiable information or PII)
- **DNS caches** in the servers
 - Query logs
 - “your recursive server knows a lot about you”
- The lack of privacy protection in DNS is actively exploited

Privacy is an issue

“Pervasive Monitoring is an attack.”
(RFC7258)

- widespread (and often covert) surveillance through intrusive gathering of protocol artefacts, including application content, or protocol metadata such as headers.

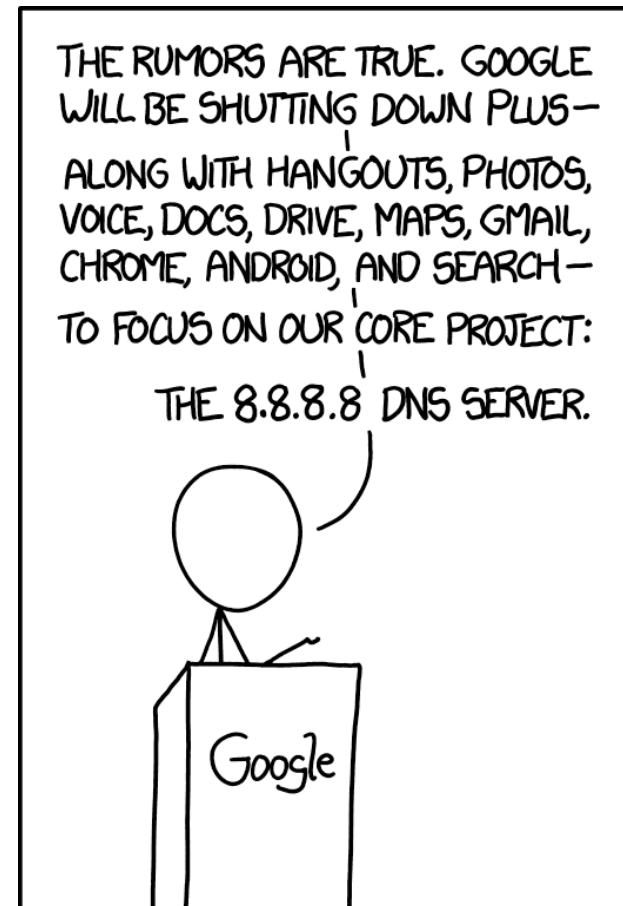


DNS cloud providers

There has been a rise in DNS cloud providers

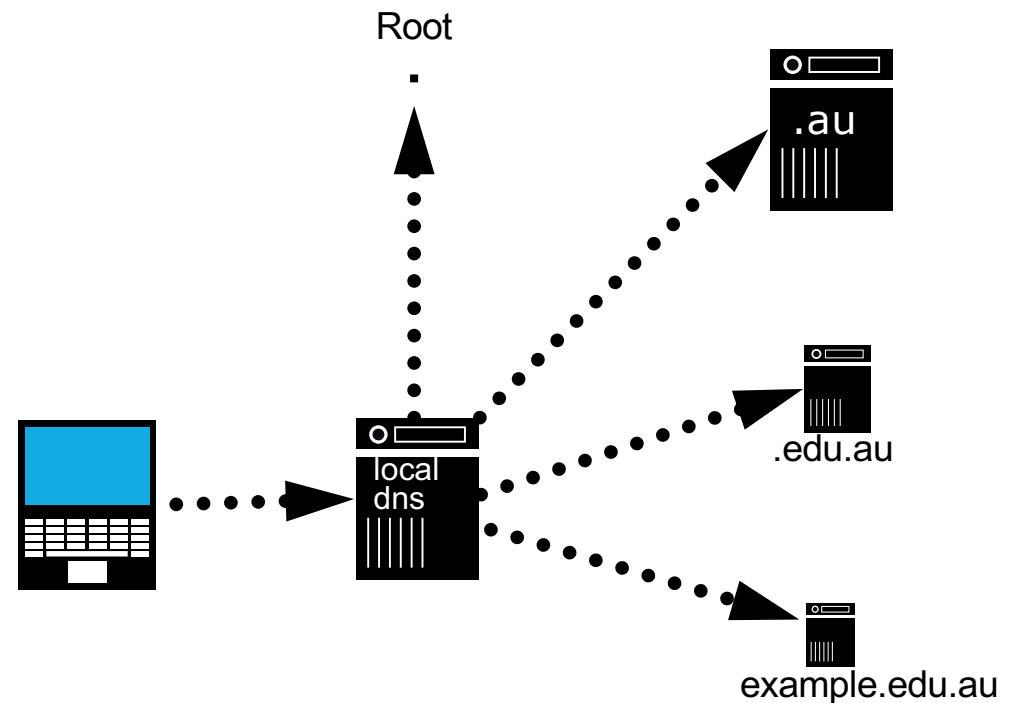
Why do we use them?

- Free and generally fast
- Avoid surveillance and blocking
- Don't trust your ISP
- Focus on privacy



Improving DNS Privacy

- DNS Privacy Considerations (RFC7626)
- Secure DNS transactions
 - Between stub resolver to recursive DNS server
 - Between recursive server to authoritative server
- Query Name Minimisation
- Encryption
 - DNS over TLS
 - DNS over DTLS
 - DNS over HTTPS



DNS over TLS (DoT)

- RFC 7858
- Uses port 853
- DNS queries are sent over TLS-encrypted TCP connections
- Avoids spoofing, eavesdropping and DNS-based filters
- Two profiles (RFC8310)
 - Strict
 - Requires an encrypted and authenticated to a privacy-enabling DNS server and creates TLS connections
 - Failure to establish connection results to no service
 - Opportunistic
 - Desires privacy when possible
 - DNS server may be obtained by DHCP or an untrusted source

Using Stubby DNS with DoT

- Stubby is a local DNS privacy stub resolver that
 - Runs as a daemon
 - Listens on loopback and sends out queries via TLS
 - Uses *Strict* privacy profile
- Simple setup

```
brew install stubby
vi /usr/local/etc/stubby/stubby.yml
/usr/local/sbin/stubby
```

```
# stubby.yml
# The getdnsapi.net server
- address_data: 185.49.141.37
  tls_auth_name: "getdnsapi.net"
  tls_pubkey_pinset:
    - digest: "sha256"
      value:
foxZRnIh9gZpWnl+zEiKa0EJ2rdCGroMWm02
gaxSc9Q=
```

<https://github.com/getdnsapi/stubby>

DoT Support - Servers

Servers

Mode		Load Balancer	Recursive					Auth		
Software		dnscdist	Unbound	BIND	Knot Res	CoreDNS ^(e)	Tenta ^(e)	NSD	BIND	Knot Auth
General	QNAME minimisation	n/a	✓	✓	✓					
TCP/TLS Features	TCP fast open ^(b)	✓	✓	✓	✓				✓	✓
	Process Pipelined queries	✓	✓	✓	✓			✓	✓	✓
	Provide OOR	(g)	✓	✓	✓			n/a	n/a	n/a
	EDNS0 Keepalive ^(c)		✓	✓	✓				✓	
TLS Features	TLS encryption (Port 853)	✓	✓	(d)	✓	✓	✓			
	Provide TLS auth credentials	✓	✓	(d)	✓	✓	✓			
	EDNS0 Padding (basic)			✓	✓				✓	
	TLS DNSSEC Chain Extension ^(h)									

<https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Implementation+Status>

DNS over HTTPS (DoH)

- RFC 8484
- DNS queries done securely over HTTPS
 - prevents on-path devices from interfering with DNS operations
 - allows web applications to access DNS information via existing browser APIs
- Client follows a URI template to construct the URL to use for resolution
 - Uses the "application/dns-message" type



<https://tools.ietf.org/html/rfc8484>

DNS Query using JSON

```
curl -s -H 'accept: application/dns+json' \  
      'https://dns.google.com/resolve?name=www.apnic.net&type=A' | jq  
{  
  "Status": 0,  
  "TC": false,  
  "RD": true,  
  "RA": true,  
  "AD": true,  
  "CD": false,  
  "Question": [  
    {  
      "name": "www.apnic.net.",  
      "type": 1  
    }  
  ],  
  .....  
}
```

DNS Response using JSON

```
"Answer": [  
  {  
    "name": "www.apnic.net.",  
    "type": 1,  
    "TTL": 299,  
    "data": "203.119.101.73"  
  }  
],  
"Comment": "Response from 202.12.31.53."  
}
```

DoH - Firefox (1/2)

- Preferences > Network Settings

Connection Settings

Configure Proxy Access to the Internet

No proxy

Auto-detect proxy settings for this network

Use system proxy settings

Manual proxy configuration

HTTP Proxy Port

Use this proxy server for all protocols

SSL Proxy Port

FTP Proxy Port

SOCKS Host Port

SOCKS v4 SOCKS v5

No Proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24

Automatic proxy configuration URL

Do not prompt for authentication if password is saved

Proxy DNS when using SOCKS v5

Enable DNS over HTTPS

Use default (https://mozilla.cloudflare-dns.com/dns-query)

Custom

about:config

Preference Name	Status	Type	Value
network.trr.allow-rtc1918	default	boolean	false
network.trr.blacklist-duration	default	integer	60
network.trr.bootstrapAddress	default	string	
network.trr.confirmationNS	default	string	example.com
network.trr.credentials	default	string	
network.trr.custom_uri	default	string	
network.trr.disable-ECS	default	boolean	true
network.trr.early-AAAA	default	boolean	false
network.trr.max-fails	default	integer	5
network.trr.mode	default	integer	0
network.trr.request-timeout	default	integer	1500
network.trr.uri	default	string	https://mozilla.cloudflare-dns.com/dns-query
network.trr.useGET	default	boolean	false
network.trr.wait-for-portal	default	boolean	true

DoH - Firefox (2/2)

about:networking#dns

DNS

Refresh Autorefresh every 3 seconds

HTTP

Sockets

DNS

WebSockets

DNS Lookup

Logging

RCWN Stats

Trusted Recursive Resolver

Hostname	Family	TRR	Addresses	Expires (Seconds)
adservice.google.com	ipv4	true	2404:6800:4006:80a::2002 172.217.25.130	55
sec-tws-prod-vip.webex.com	ipv4	false	66.163.35.36	41
twitter.com	ipv4	false	104.244.42.129 104.244.42.193	35
w.usabilla.com	ipv4	true	13.236.227.253 54.66.140.226	58
www.google.com.au	ipv4	true	216.58.199.67 2404:6800:4006:808::2003	55
beta-login.apnic.net	ipv4	true	2001:dd8:9:2::101:66 203.119.101.66	7198
www.apnic.net	ipv4	true	104.20.36.173 104.20.22.173 2606:4700:10::6814:24ad 2606:4700:10::6814:16ad	295
twitter.com	ipv4	false	104.244.42.129 104.244.42.193	99
ssl.gstatic.com	ipv4	true	2404:6800:4006:80a::2003 216.58.199.67	54
www.facebook.com	ipv4	false	2a03:2880:f119:8083:face:b00c::25de 157.240.8.35	35
ocsp.digicert.com	ipv4	false	117.18.237.29	41
mozilla.cloudflare-dns.com	ipv4	false	2606:4700::6810:f8f9 2606:4700::6810:f9f9 104.16.248.249 104.16.249.249	99
www.reddit.com	ipv4	false	151.101.97.140	35
www.amazon.com	ipv4	false	104.120.224.132	99
cgi1.apnic.net	ipv4	true	2001:dc0:2001:11::250 202.12.29.250	297
www.youtube.com	ipv4	false	2404:6800:4006:806::200e 172.217.25.174 172.217.167.78 216.58.199.78 172.217.25.142 216.58.200.110 216.58.203.110 216.58.199.46	99
www.wikipedia.org	ipv4	false	2001:df2:e500:ed1a::1 103.102.166.224	35
mozilla.cloudflare-dns.com	ipv4	false	2606:4700::6810:f9f9 2606:4700::6810:f8f9 104.16.248.249 104.16.249.249	99

TRR Values
0 – off
1 – FF pick
3 – TRR only
5 – explicit off

DoH – Cloudflared

- simple setup

```
# Install on MAC
brew install cloudflare/cloudflare/cloudflared
cloudflared - version

# Run
sudo cloudflared proxy-dns
INFO[0000] Adding DNS upstream          url="https://1.1.1.1/dns-query"
INFO[0000] Starting metrics server     addr="127.0.0.1:51291"
INFO[0000] Adding DNS upstream          url="https://1.0.0.1/dns-query"
INFO[0000] Starting DNS over HTTPS proxy server addr="dns://localhost:53"
```

dnscrypt-proxy

- Simple setup

```
cp example-dnscrypt-proxy.toml
dnscrypt-proxy.toml
./dnscrypt-proxy
```



dnscrypt-proxy

Ref: <https://github.com/jedisct1/dnscrypt-proxy>

```
[2019-06-24 06:01:47] [NOTICE] Source [public-resolvers.md] loaded
[2019-06-24 06:01:47] [NOTICE] dnscrypt-proxy 2.0.19
[2019-06-24 06:01:47] [NOTICE] Now listening to 127.0.0.1:53 [UDP]
[2019-06-24 06:01:47] [NOTICE] Now listening to 127.0.0.1:53 [TCP]
[2019-06-24 06:01:47] [NOTICE] Now listening to [::]:53 [UDP]
[2019-06-24 06:01:47] [NOTICE] Now listening to [::]:53 [TCP]
[2019-06-24 06:01:49] [NOTICE] [doh.appliedprivacy.net] OK (DoH) - rtt:
397ms
[2019-06-24 06:01:50] [NOTICE] [arvind-io] OK (crypto v2) - rtt: 407ms
[2019-06-24 06:01:50] [NOTICE] [bottlepost-dns-nl] OK (crypto v2) - rtt:
352ms
[2019-06-24 06:01:50] [NOTICE] [charis] OK (crypto v2) - rtt: 358ms
[2019-06-24 06:01:51] [NOTICE] [cloudflare] OK (DoH) - rtt: 59ms
[2019-06-24 06:01:51] [NOTICE] [cpunks-ru] OK (crypto v1) - rtt: 387ms
[2019-06-24 06:01:51] [NOTICE] [cs-ch] OK (crypto v2) - rtt: 408ms
[2019-06-24 06:01:52] [NOTICE] [cs-swe] OK (crypto v2) - rtt: 408ms
[2019-06-24 06:01:52] [NOTICE] [cs-nl] OK (crypto v2) - rtt: 408ms
[2019-06-24 06:01:53] [NOTICE] [cs-nl2] OK (crypto v2) - rtt: 408ms
[2019-06-24 06:01:53] [NOTICE] [cs-fi] OK (crypto v2) - rtt: 408ms
[2019-06-24 06:01:53] [NOTICE] [cs-pl] OK (crypto v2) - rtt: 408ms
[2019-06-24 06:01:54] [NOTICE] [cs-dk] OK (crypto v2) - rtt: 415ms
...
[2019-06-24 06:02:38] [NOTICE] [ventricle.us] OK (crypto v2) - rtt: 288ms
[2019-06-24 06:02:38] [NOTICE] [opennic-R4SAS] OK (crypto v2) - rtt: 385ms
[2019-06-24 06:02:38] [NOTICE] Server with the lowest initial latency:
quad9-dnscrypt-ip4-nofilter-alt (rtt: 53ms)
[2019-06-24 06:02:38] [NOTICE] dnscrypt-proxy is ready - live servers: 75
```

DoH Public Available Servers

<https://github.com/curl/curl/wiki/DNS-over-HTTPS>

Google	https://dns.google.com/experimental	
Cloudflare	https://cloudflare-dns.com/dns-query	Supports both -04 and -13 content-types
Quad9	Recommended: https://dns.quad9.net/dns-query Secured: https://dns9.quad9.net/dns-query Unsecured: https://dns10.quad9.net/dns-query	Secured provides: Security blacklist, DNSSEC, no EDNS Client-Subnet Unsecured provides: No security blacklist, no DNSSEC, no EDNS Client-Subnet Recommend is currently identical to secure.
CleanBrowsing	https://doh.cleanbrowsing.org/doh/family-filter/	anycast DoH server with parental control (restricts access to adult content + enforces safe search)
@chantra	https://dns.dnsverhttps.net/dns-query	"toy server" which runs doh-proxy
@jedist1	https://doh.crypto.sx/dns-query	a server which runs another project called doh-proxy , written in Rust.
PowerDNS	https://doh.powerdns.org	Based on dnsdist-doh branch

Some issues

- DNS centralisation
 - cloud DNS providers have majority of the market share
- Privacy issues
 - Your DNS data will not be be subject to local privacy laws
- Debugging and protection
 - DoH can be used for data exfiltration
 - ISPs can't localise DNS filters
 - Who handles troubleshooting?



Questions

