Briefing „Encrypted DNS“
DNS over TLS / DNS over HTTPS

2019-01-15 · Alex Mayrhofer · Head of Research & Development
About nic.at

Domain Registry for „.at“
- Since 1997, ~1.3M Domains

Registry-in-a-Box – new gTLDs
- Operation of .berlin, .hamburg, .versicherung, ...

RcodeZero DNS
- Anycast DNS for TLDs and Registrars / ISPs

Research & Community
- Technology, Organisations, Standardization, --
Background

Why DNS encryption was developed
The DNS anno circa 2012

• Sensational Success Story
  – Age 25, and practically unmodified
• Today: „Nothing goes“ without DNS
• Clear text. Everything
  – „DNS is public anyways?“
• 99% UDP, 1% TCP „fallback“
  – Worst TCP support ever!
• DNSSEC? Makes everything secure, doesn‘t it !!?!?
  – Does only „sign“, not „encrypt“
• 2013: Snowden revelations
  – NSA: „Clear text PII data ... mmmmm...“
  – IETF: „Ohh sheesh – we didn‘t expect *that* scale!“
„Pervasive Monitoring is an Attack“

• RFC 7258 – „Pervasive Monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible“

• Consequence: Review of all important protocols
• DNS – there’s not even a standardized *option* for encryption
• Worse – contains „privacy defeating“ mechanism
  – Unnecessarily transmits full QNAME in many cases
  – EDNS(0) Client Subnet
• Leak of Meta-Data & Fingerprinting
  – Re-identification of individuals across networks

Photo by Kote Puerto on Unsplash
„We need encryption“

But where to start?
The DNS Protocol arena

„Recursive DNS Server“

„Authoritative DNS Server“
IETF DPRIVE* („PRIVate Exchange“)

• 2014: „Let’s deal with the stub resolver to recursor leg“
  – Most significant information leakage
  – 1:few Relation – Authentication simple
  – „Don’t attempt to boil the ocean“

• 2018: Re-Chartering: Includes „recursive to authoritative“
  – More complex: m:n connections (Authentication!)
  – Milestone for end of 2019

*https://datatracker.ietf.org/wg/dprime/about/
DNS over (D)TLS

IETF: DPRIVE / DNSOP / (TLS)
Liste of relevant RFCs

- RFC 7626 – DNS Privacy Considerations (DPRIVE)
- RFC 7766 – TCP Transport for DNS (DNSOP)
- RFC 7816 – QNAME Minimization (DNSOP)
- RFC 7828 – EDNS keepalive (DNSOP)
- RFC 7858 – DNS over TLS (DPRIVE)
- RFC 8094 – DNS over DTLS (DPRIVE)
- RFC 7830 (+RFC 8467) – DNS Padding (DPRIVE)
- RFC 8310 – Usage Profiles
- RFC 8446 – TLS 1.3 (TLS)
RFC 7626 – DNS Privacy Considerations

• Privacy aspects / issues in areas of the DNS:
  – In the DNS message (Query Name, IP Adresse)
  – On the server
  – On the Wire
  – Re-Identification based on patterns

• Kills the „DNS is public anyways!“ argument
  – Website of „Alcoholics Anonymous“ is public
  – The fact that someone visits that website regularly is definitely privacy relevant!

• Practical example (similar..)
  – drugstoremorningafterpillvienna16.at
  – (Browser search requests leaking to the DNS?)
RFC 7766 – TCP Transport for DNS

• Goal: Establish DNS over TCP als „first class citizen“

• Features
  – Persistent connections (client soll die schliessen)
  – Connection re-use
  – Pipelining
  – Response Reordering
  – TCP Fast Open
  – Web: „Happy Eyeballs“
RFC 7816 – QNAME Minimization
RFC 7828 – EDNS keepalive

• EDNS Option for Session Management
• For TCP only!
• Clients: „Please leave connection open for X seconds“
• Server: „Ok, leave it open for X seconds“ or „Please close connection now!“
RFC 7858 – DNS over TLS (DoT)

• New Port 853 / TCP
• „On the wire“ protocol is unmodified
• Authentification: Certificates usw? -> RFC 8310
  – „Opportunistic“ vs. „Strict“
  – Chicken/Egg -> Bootstrapping des DoT Servers wie?
• Does not change the „path“ of the DNS message
  – Existing Recursive Nameserver can simply offer an additional, encrypted channel
RFC 8094 – DNS over DTLS

• Port 853 / UDP
• „Same Same but Different“
• Experimental!
  – Issues with fragmentation
  – DTLS is not widely implemented
• Performance advantage of UDP?
  – Mostly because TCP implementation used to be so „lousy“.
DNS over HTTPS

An alternative encryption scheme, driven by browser vendors
Motivation – Browser Vendors

• (a) Browsers do a lot of DNS these days
  – Websites + assets (JS, Ads, Statistics...), CDNs
  – Certificate Validation (OCSP), SafeBrowsing lists, updates, ...
  – More direct control over the DNS API desired

• (b) Timing and availability is critical
  – „Happy Eyeballs“ – Slow or lousy (local) DNS servers create bad user experience
  – „Bad Hotel WiFi“ is often „Bad Hotel DNS“...

• (c) DNS is used for censorship
  – Circumventing local (censoring) DNS servers protects Freedom of Speech
  – Eg. Google Jigsaw
IETF DoH* (DNS over HTTPs) group

• Founded 2017
• 2018: RFC 8484
  – GET or POST
  – URI Templates (https://dnsserver.example.net/dns-query{?dns})
  – Wire-Format: application/dns-message (identical zu „normal“ DNS), oder JSON
  – HTTP Response-Code always 2xx (if successful), no matter which DNS response code

*https://datatracker.ietf.org/wg/doh/about/
Effects of encrypted DNS

The implications of typical operational models
„Plain“ DNS
DNS over TLS
DNS over HTTPS (typical)
Concerns regarding DoH

- 4 Browser Vendors
- Few big public recursor vendors (1.1.1.1, 8.8.8.8, 9.9.9.9)
- Market concentration / Control?
  - Pre-configured public recursors
  - Example: Mozilla / Cloudflare discussion
- Media echo (German only, sorry!)
  - https://Heise.de/-4203225.html („Die DNS Gruft gehört ausgelüftet“)
  - https://heise.de/-4205380.html („Vom DNS, aktuellen Hypes, Überwachung und Zensur“)
Implementations

Server, Clients, Tools
# DoT Clients

<table>
<thead>
<tr>
<th>Mode</th>
<th>Software</th>
<th>idns</th>
<th>digit</th>
<th>getdns (Stubby)</th>
<th>BIND</th>
<th>Go DNS</th>
<th>Knot (kdig)</th>
<th>Unbound</th>
<th>BIND</th>
<th>Knot Res</th>
<th>dndist</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>General</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Send ECS with SOURCE PREFIX-LENGTH value of 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP/TLS Features</td>
<td>TCP fast open(b)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Connection reuse (Q/R, Q/R, Q/R)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Pipelining of queries (Q,Q,Q,R,R,R)</td>
<td>n/a</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Process OOR (Q1,Q2,R2,R1)</td>
<td>n/a</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>EDNS0 Keepalive(c)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>TLS Features</td>
<td>TLS encryption (Port 533)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TLS authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EDNS0 Padding</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TLS DNSSEC Chain Extension</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- [Link](https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Implementation+Status)
# DoT Server Software

## Servers

<table>
<thead>
<tr>
<th>Mode</th>
<th>Load Balancer</th>
<th>Recursive</th>
<th>Auth</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Software</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>General</td>
<td>QNAME minimisation</td>
<td>n/a</td>
<td>✔</td>
</tr>
<tr>
<td><strong>TCP/TLS Features</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP fast open</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Process Pipelined queries</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Provide OOR</td>
<td>(g)</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>EDNS0 Keepalive</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>TLS Features</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLS encryption (Port 853)</td>
<td>✔</td>
<td></td>
<td>(d)</td>
</tr>
<tr>
<td>Provide TLS auth credentials</td>
<td>✔</td>
<td></td>
<td>(d)</td>
</tr>
<tr>
<td>EDNS0 Padding (basic)</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLS DNSSEC Chain Extension</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
DoT (and DoH) public recursors

- Google DNS (8.8.8.8)
- Cloudflare (1.1.1.1)
- Quad9 (9.9.9.9)
- CleanBrowsing (various, with Filters)
DoH

• Clients
  – Mozilla Firefox
  – Google Chrome
  – (plus test tools)

• Server Software
  – https://github.com/facebookexperimental/doh-proxy
  – https://github.com/curl/curl/wiki/DNS-over-HTTPS#doh-tools
Android 9 – DNS over TLS by default

- Uses DNS over TLS if available on local nameserver
- Falls back to unencrypted DNS if unavailable
Exec Summary

• DNS can now be encrypted, either via TLS or HTTPS
• DNS over HTTPs is more „disruptive“ than DNS over TLS
• Public recursors have implemented either (or both)
  – But few local providers have implemented it (see below :-/)
• Browser Vendors are implementing DNS over HTTPs
  – Ongoing policy discussions around pre-configuration of recursors
• Android 9 implements DNS over TLS *by default*
  – Automatically uses it if available (see above :-/)
  – Google suggesting to configure „dns.google“ manually
• Windows / MacOS – no „out of the box“ solutions – „Stubby“