Privacy in the Domain Name System (DNS):

Tutorial

Sara Dickinson  sara@sinodun.com
https://sinodun.com
@SinodunCom
Tutorial Overview

• **The problem**: Why Internet privacy and DNS Privacy are important (DNS leakage)

• **Recent Progress**: Chart progress during last 6 years (DNS-over-TLS, DNS-over-HTTPS)

• Where are we now, what is next and who decides?

Specification vs Implementation vs Deployment

https://github.com/Sinodun/tma_phd_school
Hands on Overview

- Do some DNS traffic inspection
  - Look at queries and responses
  - See what your machine sends over time
- Set up encrypted DNS on your desktop, mobile, browser…
- (Set up a DNS server that does encrypted DNS)
My Background

• Co-founder of Sinodun IT - small UK based consultancy
• Focussed on DNS, DNSSEC and DNS Privacy
• R&D, Open source dev, Standards dev (IETF)
• DNS-over-TLS (DoT): Directly involved (dnsprivacy.org)
• DNS-over-HTTPS (DoH): Not directly involved
My Background

• Co-founder of Sinodun IT - small UK based consultancy
• Focussed on DNS, DNSSEC and DNS Privacy
• R&D, Open source dev, Standards dev (IETF)

• DNS-over-TLS (DoT): Directly involved (dnsprivacy.org)
• DNS-over-HTTPS (DoH): Not directly involved

Goal today is provide context for DNS Privacy, technical background on solutions and arm you with choices!
dnsprivacy.org

- DNS Privacy Project homepage

- **Who?** Sinodun, NLnet Labs, Salesforce,… (plus various grants and individual contributions)

- **What?** Point of reference for DNS Privacy services
  - Quick start guides for operators & end users
  - Ongoing work - presentations, IETF, Hackathons
  - Tracking of DNS-over-TLS experimental servers
What is the IETF?
What is the IETF?

- Internet Engineering Task Force
- Develop *Internet Standards* (RFCs) that mostly define *Internet Protocols* (e.g. TCP/IP, HTTP, DNS…)
- Formed in 1986, meets 3 times a year (+1200)
- Divided into Working Groups, *consensus* reached via open mailing, review by Steering Group (IESG)

- *Anyone* can participate, *open* process
What is the IETF?

• Internet Engineering Task Force
• Develop *Internet Standards* (RFCs) that mostly define *Internet Protocols* (e.g. TCP/IP, HTTP, DNS…)

• Formed in 1986, meets 3 times a year (+1200)

• Divided into Working Groups, *consensus* reached via open mailing, review by Steering Group (IESG)

• *Anyone* can participate, open process
Why does Internet privacy matter?

• We hear about data breaches/abuses all the time but....

• Machine learning at scale today means **small number of people controlling network** can perform mass surveillance

• Surveillance can be used as social control
Behaviour changes
(even when no-one is watching, you just think they are)

Under Surveillance: Examining Facebook’s Spiral of Silence Effects in the Wake of NSA Internet Monitoring

Elizabeth Stoycheff, Journalism & Mass Communication Quarterly 1-16
DNS is part of the leaky boat problem

DNS

Traffic size

TLS SNI

Timing patterns

...?
DNS Basics

• One of the core Internet infrastructure components

• Consistent **namespace** used for referring to resources

  • **DNS Data** is globally maintained in a distributed manner

  • **DNS Protocol**: ‘simple’ Query/Response model (port 53)
    • IP address resource lookup is most frequent
    • A record (IPv4) and AAAA record (IPv6)
    • Others exist (MX, SRV, PTR, TXT)
DNS Basics

• DNS is an ‘enabler’ service, initial lookup typically followed by a connection attempt (HTTPS, TLS, SMTP/IMAP, XMPP,…)

• Uses **caching** servers for scalability and performance

• DNS outages/attacks impact virtually every other Internet service
DNS Basics

It's not DNS

There's no way it's DNS

It was DNS
DNS Basics - resolution
DNS Basics - resolution

- s/w is in OS
- IP from DHCP
DNS Basics - resolution

Stub

- s/w is in OS
- IP from DHCP

Recursive
DNS Basics - resolution

Stub
- s/w is in OS
- IP from DHCP

Recursive
- ISP, Google, etc.
- Caches answers
DNS Basics - resolution

Stub

Recursive

www.example.com

- s/w is in OS
- IP from DHCP

- ISP, Google, etc.
- Caches answers

TMA, Jun 2019
DNS Basics - resolution

- **Stub**
  - s/w is in OS
  - IP from DHCP

- **Recursive**
  - ISP, Google, etc.
  - Caches answers

- **Authoritative**
  - ‘Root’
  - Auth for .com
  - Auth for example.com

www.example.com

TMA, Jun 2019
DNS Basics - resolution

Stub

Recursive

Authoritative

www.example.com

- s/w is in OS
- IP from DHCP

- ISP, Google, etc.
- Caches answers

Root

Auth for .com

Auth for example.com

DNS Privacy
DNS Basics - resolution

- **Stub**
  - s/w is in OS
  - IP from DHCP

- **Recursive**
  - ISP, Google, etc.
  - Caches answers

- **Authoritative**
  - Auth for www.example.com
  - NS .com

- ‘Root’
  - Auth for .com

- DNS Privacy

TMA, Jun 2019
DNS Basics - resolution

- **Stub**
  - s/w is in OS
  - IP from DHCP

- **Recursive**
  - ISP, Google, etc.
  - Caches answers

- **Authoritative**
  - Auth for example.com
  - Auth for .com

- **‘Root’**

TMA, Jun 2019
DNS Basics - resolution

### Stub
- s/w is in OS
- IP from DHCP

### Recursive
- ISP, Google, etc.
- Caches answers

### Authoritative
- Auth for example.com
- Auth for .com
- ‘Root’

www.example.com

NS .com

NS .example.com

DNS Privacy

TMA, Jun 2019
DNS Basics - resolution

- **Stub**
  - s/w is in OS
  - IP from DHCP

- **Recursive**
  - ISP, Google, etc.
  - Caches answers

- **Authoritative**
  - Auth for .example.com
  - Auth for .com
  - ‘Root’

- **DNS Privacy**
DNS Basics - resolution

Stub
- s/w is in OS
- IP from DHCP

Recursive
- ISP, Google, etc.
- Caches answers

Authoritative
- ‘Root’
- Auth for .com
- Auth for example.com
- 93.184.216.34

www.example.com
- NS .com
- NS .example.com
- www.example.com
- www.example.com
- www.example.com

DNS Privacy
DNS Basics - resolution

Stub
- s/w is in OS
- IP from DHCP

Recursive
- ISP, Google, etc.
- Caches answers

Authoritative
- ‘Root’
- Auth for .com
- Auth for example .com

DNS Privacy

www.example.com
93.184.216.34

www.example.com
NS .com
www.example.com
NS .example.com
www.example.com
93.184.216.34
DNS Basics - network view

Recursive resolver (from DHCP) → DNS servers on Internet

Desktop → DNS → system stub resolver

App: DNS system library call `getaddrinfo()`

Local Network
DNS Basics - network view

Desktop

App

DNS system library call
getaddrinfo()

system stub resolver

Local Network

Auth servers on Internet

TMA, Jun 2019

DNS Privacy
DNS Basics - network view

Desktop

App

DNS system library call
getaddrinfo()

Local Network

system stub resolver

DNS

Google 8.8.8.8

Auth servers on Internet
The DNS is showing its age


- Original design availability, redundancy and speed!

- Wire traffic is (cleartext):
  - UDP (~99%)
  - TCP only used for ‘fallback’
The DNS is showing its age


- No Security or Privacy in the original design (or versioning)!
  - Security == Authentication
    - DNSSEC: DNS Security Extensions (1990-97, 2005, ....)
  - Privacy == Confidentiality
    - Even recently: The DNS is public, right? Why encrypt?
DNSCrypt

- **DNSCrypt**
  - Encrypts contents on DNS UDP message (port 443)
  - Never proposed as an IETF standard but was developed as an independent specification
  - Several clients and many DNSCrypt Resolvers
    - Yandex browser
    - OpenDNS, Quad9, DNSCrypt browser list
  - Requires manual config, not a RFC, limited adoption
DNSCrypt

- **DNSCrypt**
  - Encrypts contents on DNS UDP message (port 443)
  - Never proposed as an IETF standard but was developed as an independent specification
  - Several clients and many DNSCrypt Resolvers
    - Yandex browser
    - OpenDNS, Quad9, DNSCrypt browser list
  - Requires manual config, not a RFC, limited adoption

Original Goals were:
- Anti-spoofing
- Anti DoS
- Access control
  **NOT PRIVACY**
Everything changed in 2013....
Snowdon

- June 2013: Snowdon reveals of mass surveillance by NSA, including DNS
Snowdon

• June 2013: Snowdon reveals of mass surveillance by NSA, including DNS

• May 2014: IETF Response (RFC7258):

  “Pervasive Monitoring is an attack on the privacy of Internet users and organisations.”

  “…that needs to be mitigated where possible, via the design of protocols that make PM significantly more expensive or infeasible.”
DNS Disclosure Example 1

www.example.com

Rec

www.example.com

www.example.com

www.example.com

www.example.com

www.example.com

www.example.com

Root

Auth for .com

Auth for example.com

DNS Privacy
DNS Disclosure Example 1
DNS Disclosure Example 2
DNS Disclosure Example 2

ISP Parental Filtering

Stub

CPE

Rec

Auth
DNS Disclosure Example 2

ISP Parental Filtering

Stub

CPE

Rec

ISP Parental Filtering

Auth

[User src address] MAC address or id in DNS query
DNS Disclosure Example 2

ISP Parental Filtering

www.example.com
[00:00:53:00:53:00]

Stub

CPE

Rec

Auth

[User src address]
MAC address or id
in DNS query

TMA, June 2019
DNS Disclosure Example 2

ISP Parental Filtering

CDN Geo-location

www.example.com
[00:00:53:00:53:00]

Stub

[User src address]
MAC address or id
in DNS query

Rec

ISP Parental Filtering

CPE

Auth

DNS Privacy
DNS Disclosure Example 2

ISP Parental Filtering

www.example.com [00:00:53:00:53:00]

Stub

CPE

Rec

Auth

[User src address]  
MAC address or id in DNS query

Client Subnet (RFC7871) contains source subnet in DNS query

ISP Parental Filtering

CDN Geo-location
DNS Disclosure Example 2

ISP Parental Filtering

www.example.com [00:00:53:00:53:00]

CDN Geo-location

www.example.com [192.168.1]

Stub

CPE

Rec

[User src address] MAC address or id in DNS query

Auth

Client Subnet (RFC7871) contains source subnet in DNS query

TMA, June 2019

DNS Privacy
DNS: It’s not just for names

Almost every activity starts with a DNS query (try it)!

- SRV records (services e.g chat)
- OPENPGPKEY (email addresses)
- MX records (email domain)
- …this is only going to increase….
DNS: It’s not just for names

Almost every activity starts with a DNS query (try it)!

- SRV records (services e.g. chat)
- OPENPGPKEY (email addresses)
- MX records (email domain)
- …this is only going to increase….
DNS: It’s not just for names

Almost every activity starts with a DNS query (try it)!

- SRV records (services e.g. chat)
- OPENPGPKEY (email addresses)
- MX records (email domain)
- …this is only going to increase…..

Leakage of meta data: Reveals behaviour and allows fingerprinting of individuals
DNS Disclosure Example 3

- (AUTH) Who monitors here ISP/law enforcement/NSA?
- (AUTH) Does my ISP (or Google....) sell my data?
- (UNAUTH) How safe is this data?
DNS Disclosure Example 3

- (AUTH) Who monitors here ISP/law enforcement/NSA?
- (AUTH) Does my ISP (or Google…) sell my data?
- (UNAUTH) How safe is this data?

- When at work…
- When in a coffee shop…
DNS Disclosure Example 3

- (AUTH) Who monitors here ISP/law enforcement/NSA?
- (AUTH) Does my ISP (or Google…) sell my data?
- (UNAUTH) How safe is this data?

When at work…
When in a coffee shop…

Who monitors or has access here?
Who monitors or has access here?
## DNS Risk Matrix

<table>
<thead>
<tr>
<th>Risk</th>
<th>In-Flight</th>
<th>At Rest</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Stub =&gt; Rec</td>
<td>Rec =&gt; Auth</td>
</tr>
<tr>
<td>Passive Monitoring (network sniffing)</td>
<td><img src="https://via.placeholder.com/150" alt="Diagram" /> <img src="https://via.placeholder.com/150" alt="Diagram" /></td>
<td><img src="https://via.placeholder.com/150" alt="Diagram" /> <img src="https://via.placeholder.com/150" alt="Diagram" /></td>
</tr>
<tr>
<td>Active Monitoring (divert traffic)</td>
<td><img src="https://via.placeholder.com/150" alt="Diagram" /> <img src="https://via.placeholder.com/150" alt="Diagram" /></td>
<td><img src="https://via.placeholder.com/150" alt="Diagram" /> <img src="https://via.placeholder.com/150" alt="Diagram" /></td>
</tr>
<tr>
<td>Other Disclosure Risks (e.g. Misuses of Data, Data breaches)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Passive Monitoring (network sniffing)**
- **Active Monitoring (divert traffic)**
- **Other Disclosure Risks (e.g. Misuses of Data, Data breaches)**
IETF DPRIVE WG

WHO'S LOOKING INTO THE ISSUE?

TOP ... MEN

meme-generator.net
Problem statement

- Rebuts “alleged public nature of DNS data”
  - The *data* may be public, but a DNS ‘transaction’ is not/should not be.

**RFC 7626**: "DNS Privacy Considerations": Expert coverage of risks throughout DNS ecosystem
Problem statement

RFC 7626: "DNS Privacy Considerations":
Expert coverage of risks throughout DNS ecosystem

- Rebuts “alleged public nature of DNS data”
  - The data may be public, but a DNS 'transaction' is not/should not be.

“A typical example from outside the DNS world is: the web site of Alcoholics Anonymous is public; the fact that you visit it should not be.”
DNS-over-TLS (DoT)

RFC7258: Pervasive Monitoring is an attack

DPRIVE WG formed

Goals:
1) Encrypt Stub-Rec DNS
2) Think about Rec-Auth?

Snowden Revelations

1987 2012 2013 2014 2016 2018

TMA, Jun 2019

DNS Privacy
DNS-over-TLS (DoT)

- RFC 7258: Pervasive Monitoring is an attack
- DPRIVE WG formed
- Goals:
  1) Encrypt Stub-Rec DNS
  2) Think about Rec-Auth?
- RFC 7766: DNS-over-TCP
- RFC 7858: DNS-over-TLS
- Snowden Revelations
- Port 853
UDP vs TLS?

• Unreliable vs reliable transport

• TLS is session based and has a handshake - this is an overhead

• Session re-use is important for performance (100 msg on a session gives this)

• DoT Keepalive - leave sessions open when idle

• Server management is important to avoid overload
UDP vs TLS?

Query
Response
Query
Response
Query
Response
UDP vs TLS?

Query
Response
Query
Response
Query
Response

No source address verification => DDoS

TMA, Jun 2019
UDP vs TLS?
UDP vs TLS?

TCP HANDSHAKE

TLS HANDSHAKE

Query

Response

Query

Response

TLS Session

DNS Privacy
Authentication in DoT?

- TLS: Transport Layer Security
  - Encrypts data on the wire (defeat passive mon)
  - Authentication of server based on PKIX (defeat active mon)

- DoT: DNS-over-TLS ([RFC8310](https://tools.ietf.org/html/rfc8310))
Authentication in DoT?

- **TLS**: Transport Layer Security
  - Encrypts data on the wire (defeat passive mon)
  - Authentication of server based on PKIX (defeat active mon)

- **DoT**: DNS-over-TLS ([RFC8310](https://tools.ietf.org/html/rfc8310))

<table>
<thead>
<tr>
<th>Mode</th>
<th>Requires</th>
<th>Logic</th>
<th>Similar too…</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strict</strong></td>
<td>IP address and name*</td>
<td>Authenticate &amp; Encrypt OR Fail</td>
<td>Bailing if HTTPS website cert is bad</td>
</tr>
<tr>
<td><strong>Opportunistic</strong></td>
<td>Just IP address (probe port 853)</td>
<td>Try in order: 1. Encrypt &amp; Authenticate 2. Encrypt only 3. Clear text</td>
<td>2. Clicking through a bad cert 3. Downgrading to HTTP</td>
</tr>
</tbody>
</table>

DPRIVE WG
Authentication in DoT?

- TLS: Transport Layer Security
  - Encrypts data on the wire (defeat passive mon)
  - Authentication of server based on PKIX (defeat active mon)

- DoT: DNS-over-TLS (RFC8310)

<table>
<thead>
<tr>
<th>Mode</th>
<th>Requires</th>
<th>Logic</th>
<th>Similar too…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strict</td>
<td>IP address and name*</td>
<td>Authenticate &amp; Encrypt OR Fail</td>
<td>No DNS, no Internet</td>
</tr>
<tr>
<td>Opportunistic</td>
<td>Just IP address (probe port 853)</td>
<td>Try in order:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Encrypt &amp; Authenticate</td>
<td>2. Clicking through a bad cert</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Encrypt only</td>
<td>3. Downgrading to HTTP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Clear text</td>
<td></td>
</tr>
</tbody>
</table>
Authentication in DoT?

- **TLS**: Transport Layer Security
  - Encrypts data on the wire (defeat passive mon)
  - Authentication of server based on PKIX (defeat active mon)

- **DoT**: DNS-over-TLS ([RFC8310](https://tools.ietf.org/html/rfc8310))

<table>
<thead>
<tr>
<th>Mode</th>
<th>Requires</th>
<th>Logic</th>
<th>Similar too…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strict</td>
<td>IP address and name*</td>
<td>Authenticate &amp; Encrypt OR Fail</td>
<td>No DNS, no Internet</td>
</tr>
<tr>
<td>Opportunistic</td>
<td>Just IP address (probe port 853)</td>
<td>Try in order: 1. Encrypt &amp; Authenticate 2. Encrypt only 3. Clear text</td>
<td>Opportunistic has no guarantees, but always get DNS service</td>
</tr>
</tbody>
</table>

2. Clicking through a bad cert
3. Downgrading to HTTP

Opportunistic has no guarantees, but always get DNS service.
# DoT Implementation & Deployment

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015 - now</td>
<td><strong>Implementations:</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Stubs:</strong> Mobile: Android Pie*, 14 app, Quad9 app</td>
</tr>
<tr>
<td></td>
<td>Desktop: Stubby, (systemd, FreeBSD)</td>
</tr>
<tr>
<td></td>
<td><strong>Recursives:</strong> Unbound, Knot resolver, dnsdist, (BIND)</td>
</tr>
<tr>
<td>2015 - now</td>
<td><strong>Set of ~30 test DoT recursive resolvers</strong></td>
</tr>
<tr>
<td>Nov 2017</td>
<td>Quad9 (9.9.9.9) offer DoT</td>
</tr>
<tr>
<td>Mar 2018</td>
<td>Cloudflare (1.1.1.1) offer DoT</td>
</tr>
<tr>
<td>Jan 2019</td>
<td>Google (8.8.8.8) offer DoT</td>
</tr>
</tbody>
</table>

* Does Opportunistic DoT to system recursive by default
# DoT Implementation & Deployment

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015 - now</td>
<td><strong>Implementations:</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Stubs:</strong> Mobile: Android Pie*, 14 app, Quad9 app</td>
</tr>
<tr>
<td></td>
<td>Desktop: Stubby, (systemd, FreeBSD)</td>
</tr>
<tr>
<td></td>
<td><strong>Recursives:</strong> Unbound, Knot resolver, dnsdist, (BIND)</td>
</tr>
<tr>
<td></td>
<td><strong>Set of ~30 test DoT recursive resolvers</strong></td>
</tr>
<tr>
<td>Nov 2017</td>
<td>Quad9 (9.9.9.9) offer DoT</td>
</tr>
<tr>
<td>Mar 2018</td>
<td>Cloudflare (1.1.1.1) offer DoT</td>
</tr>
<tr>
<td>Jan 2019</td>
<td>Google (8.8.8.8) offer DoT</td>
</tr>
</tbody>
</table>

* Does Opportunistic DoT to system recursive by default

**MISSING PIECE:**
- Stub resolver support in:
  - Windows
  - macOS/iOS
  - Linux

---

TMA, Jun 2019
## DoT Implementation & Deployment

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015 - now</td>
<td><strong>Implementations:</strong>&lt;br&gt;<strong>Stubs:</strong> Mobile: Android Pie*, 14 app, Quad9 app&lt;br&gt;Desktop: Stubby, (systemd, FreeBSD)&lt;br&gt;<strong>Recursives:</strong> Unbound, Knot resolver, dnsdist, (BIND)</td>
</tr>
<tr>
<td>2015 - now</td>
<td><strong>Set of ~30 test DoT recursive resolvers</strong></td>
</tr>
<tr>
<td>Nov 2017</td>
<td>Quad9 (9.9.9.9) offer DoT</td>
</tr>
<tr>
<td>Mar 2018</td>
<td>Cloudflare (1.1.1.1) offer DoT</td>
</tr>
<tr>
<td>Jan 2019</td>
<td>Google (8.8.8.8) offer DoT</td>
</tr>
</tbody>
</table>

* Does Opportunistic DoT to system recursive by default

**MISSING PIECE:**

Stub resolver support in:<br>• Windows<br>• macOS/iOS<br>• Linux

‘Cloud’ DNS providers (or ‘Quads’)
Recursive Resolver policies

- Do you read the small print of your ISPs contract?

- ‘Best Current Practices’ Guidelines draft in progress
  - Minimum requirements to be a ‘DNS Privacy Service’
  - Clearly publish exactly what you do
  - Reduce tracking/leakage even when encrypted
  - Anonymise logs, don’t share/sell data
  - Get audited for transparency

- Filtering/Blocking/Censorship
RFC7816: QNAME Minimisation

www.example.com

DNS Privacy
# Risk Mitigation Matrix

<table>
<thead>
<tr>
<th>Risk</th>
<th>In-Flight</th>
<th>At Rest</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Stub =&gt; Rec</strong></td>
<td><strong>Rec =&gt; Auth</strong></td>
</tr>
<tr>
<td><strong>Passive monitoring</strong></td>
<td>Encryption (e.g. TLS)</td>
<td>QNAME Minimization</td>
</tr>
<tr>
<td><strong>Active monitoring</strong></td>
<td>Authentication &amp; Encryption</td>
<td></td>
</tr>
<tr>
<td><strong>Other Disclosure Risks e.g. Data breaches</strong></td>
<td></td>
<td>Best Practices (Policies) e.g. De-identification</td>
</tr>
</tbody>
</table>
2017 - Job done?

- Still some **technical** issues
  - DoT: A dedicated port (853) can be **blocked** (443 fallback)
  - Strict needs manual configuration (no discovery)
  - Crucial that operators have good privacy practices - they are the weakest link once the transport is encrypted...

- **Deployment** will take time
  - Need OS’s to implement
  - Not deployed by many (any?) ISPs_ENTERPRISES… so early adopters using test servers or Quad providers….
2017 - Job done?

- Still some **technical** issues
  - DoT: A dedicated port (853) can be **blocked** (443 fallback)
  - Strict needs manual configuration (no discovery)
  - Crucial that operators have good privacy practices - they are the weakest link once the transport is encrypted…

- **Deployment** will take time
  - Need OS’s to implement
  - Not deployed by many (any?) ISPs/enterprises… so early adopters using test servers or Quad providers…

For DoT, seen as short term or rare…BUT Opportunistic DoT by default seems feasible.
WHAT IF I TOLD YOU BROWERS ARE GOING TO DO THEIR OWN DNS OVER HTTPS
WHAT IF I TOLD YOU BROWSERS ARE GOING TO DO THEIR OWN DNS OVER HTTPS

......to their own chosen cloud resolver service!
DNS-over-HTTPS (DoH)

Goals: “This working group will standardize encodings for DNS queries and responses that are suitable for use in HTTPS.”

First DoH draft published (query init)

IETF 98

1987

TMA, Jun 2019
DNS-over-HTTPS (DoH)

Goals: “This working group will standardize encodings for DNS queries and responses that are suitable for use in HTTPS.”

First DoH draft published (query init)

DoH WG formed

DoH draft adopted

Approved

RFC8484

IETF 98

May 2017

Sep 2017

Oct 2017

Aug 2018

Oct 2018

1987

March 2017

May 2017

Sep 2017

Oct 2017

Aug 2018

Oct 2018

TMA, Jun 2019

DNS Privacy
DNS-over-HTTPS (DoH)

Goals: “This working group will standardize encodings for DNS queries and responses that are suitable for use in HTTPS.”

- First DoH draft published (query init) - May 2017
- DoH WG formed - Sep 2017
- DoH draft adopted - Oct 2017
- Approved - Aug 2018
- RFC 8484 - Oct 2018

IETF 98 - March 2017

1987 - TMA, Jun 2019

DNS Privacy
# How is DoH different to DoT?

<table>
<thead>
<tr>
<th></th>
<th>What is different?</th>
<th>What is impact?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use cases</strong></td>
<td>1. Use directly from application via existing API</td>
<td>1. Bypass system resolver</td>
</tr>
<tr>
<td></td>
<td>2. Avoid accidental and deliberate blocking (853)</td>
<td>2. Runs on port 443</td>
</tr>
<tr>
<td><strong>Discovery</strong></td>
<td>Must use URI template, not an IP address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No ‘Opportunistic’ mode possible, must configure</td>
<td></td>
</tr>
<tr>
<td><strong>Tracking</strong></td>
<td>HTTP headers allow tracking of query via e.g. ‘User-agent’ (application), language,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>etc.</td>
<td>New Privacy concerns</td>
</tr>
<tr>
<td><strong>Connections</strong></td>
<td>1. <strong>Dedicated</strong> connections (only DoH traffic)</td>
<td>1. Very hard to block</td>
</tr>
<tr>
<td></td>
<td>2. <strong>Mixed</strong> connections (send DoH on existing HTTPS connections)</td>
<td>2. <strong>Impossible to block</strong> just DNS traffic</td>
</tr>
</tbody>
</table>

TMA, Jun 2019
## How is DoH different to DoT?

<table>
<thead>
<tr>
<th><strong>Use cases</strong></th>
<th><strong>What is different?</strong></th>
<th><strong>What is impact?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Use directly from application via existing API</td>
<td>1. Bypass system resolver</td>
</tr>
<tr>
<td></td>
<td>2. Avoid accidental and deliberate blocking (853)</td>
<td>2. Runs on port 443</td>
</tr>
</tbody>
</table>

| **Discovery** | **Must use URI template, not an IP address** | **No ‘Opportunistic’ mode possible, must configure** |

| **Tracking** | **HTTP headers allow tracking of query via e.g. ‘User-agent’ (application), language, etc.** | **New Privacy concerns** |

<table>
<thead>
<tr>
<th><strong>Connections</strong></th>
<th><strong>What is different?</strong></th>
<th><strong>What is impact?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. <strong>Dedicated</strong> connections (only DoH traffic)</td>
<td>1. Very hard to block</td>
</tr>
<tr>
<td></td>
<td>2. <strong>Mixed</strong> connections (send DoH on existing HTTPS connections)</td>
<td>2. <em><strong>Impossible to block just DNS traffic</strong></em></td>
</tr>
</tbody>
</table>
DoH in Browsers

• Why encrypt directly from the browser? Browser folks say:

• Why DoH, not DoT? Mozilla’s answer:
DoH in Browsers

• Why encrypt directly from the browser? Browser folks say:

  - OS’s are slow to offer new DNS features (DoT/DoH)
  - Selling point: “we care about the privacy of our users”
  - Performance: “reduce latency within browser by doing DNS there”

• Why DoH, not DoT? Mozilla’s answer:
DoH in Browsers

- Why encrypt directly from the browser? Browser folks say:
  - OS’s are slow to offer new DNS features (DoT/DoH)
  - Selling point: “we care about the privacy of our users”
  - Performance: “reduce latency within browser by doing DNS there”

- Why DoH, not DoT? Mozilla’s answer:
  - Integration: “leverage the HTTPS ecosystem”
  - HTTPS everywhere: “it works… just use port 443, mix traffic”
  - Cool stuff: “JSON, Server Push, ‘Resolverless DNS’….!”
DoH in Browsers

• Why encrypt directly from the browser? Browser folks say:

  OS’s are slow to offer new DNS features (DoT/DoH)
  Selling point: “we care about the privacy of our users”
  Performance: “reduce latency within browser by doing DNS there”

• Why DoH, not DoT? Mozilla’s answer:

  Integration: “leverage the HTTPS ecosystem”
  HTTPS everywhere: “it works… just use port 443, mix traffic”
  Cool stuff: “JSON, Server Push, ‘Resolverless DNS’ ….”

DNS 2.0?
DoH in Firefox

- Mozilla blogs:
  - Experiment & Future plans (May 2018):
DoH in Firefox

- Mozilla blogs:
  - Experiment & Future plans (May 2018):
    - “We’d like to turn this [DoH] on as the default for all of our users”
    - “Cloudflare is our ‘Trusted Recursive Resolver’ (TRR)”
DoH in Firefox

- Mozilla blogs:
  - Experiment & Future plans (May 2018):
    - “We’d like to turn this [DoH] on as the default for all of our users”
    - “Cloudflare is our ‘Trusted Recursive Resolver’ (TRR)”

“With this [agreement], we have a resolver that we can trust to protect users’ privacy. This means Firefox can ignore the resolver that the network provides and just go straight to Cloudflare.”
TRR by default?

Impact of TRRs? Applications using default TRRs fundamentally change the existing **implicit** consent model for DNS:

- (Current) Log onto a network and use the DHCP provided resolver
- (New?) Use an app and agree to app T&C’s (including DNS?)
TRR by default?

Impact of TRRs? Applications using default TRRs fundamentally change the existing *implicit* consent model for DNS:

- (Current) Log onto a network and use the DHCP provided resolver
- (New?) Use an app and agree to app T&C’s (including DNS?)
TRR by default?

Impact of TRRs? Applications using default TRRs fundamentally change the existing **implicit** consent model for DNS:

- (Current) Log onto a network and use the DHCP provided resolver
- (New?) Use an app and agree to app T&C’s (including DNS?)

**Major deployment model shift**

- Mozilla perceived benefits (aligned with their Core Principles)?
  - Cloudflare do not filter at all - Censorship avoidance
    “If you control the network but not the device, you are an attacker”
  - Network provided resolvers vary hugely….Cloudflare have publicly published an (audited) privacy policy
TRR by default...but?

Major deployment model shift - with implications
TRR by default...but?

Major deployment model shift - with implications

- Centralisation: Using purely ‘Cloud’ based resolvers risks centralisation of DNS
  - Few people override the default
  - Legislation for blocking/filtering/interception (US based)?
  - Neutrality of DNS operators (CDN’s?)

- ‘One size fits all’: does not work for all networks or regions
  - ISP vs enterprise (company) vs coffee shop
  - US centric view of ISPs? (No Net neutrality, no GDPR)

- Browsers and Apps become gatekeepers for blessed list of TRRs (like CAs)
  - What if Government mandate certain TRRs or TRR operators offer money?
TRR by default…but?

- Centralisation: Using purely ‘Cloud’ based resolvers risks centralisation of DNS
  - Few people override the default
  - Legislation for blocking/filtering/interception (US based)?
  - Neutrality of DNS operators (CDN’s?)

- ‘One size fits all’: does not work for all networks or regions
  - ISP vs enterprise (company) vs coffee shop
  - US centric view of ISPs? (No Net neutrality, no GDPR)

- Browsers and Apps become gatekeepers for blessed list of TRRs (like CAs)
  - What if Government mandate certain TRRs or TRR operators offer money?
TRR by default...but?

Local Operator loses ability to monitor/control traffic
TRR by default…but?

Local Operator loses ability to monitor/control traffic

- Security risks: Using a resolver NOT on the local network breaks many things!
  - Local monitoring and security policies
    - Malware filtering
    - Malicious website filtering
    - Parental controls
    - Government mandated filtering
  - Split horizon DNS (fallback possible)

- Informed consent issues - for the DNS - really?
- Technical issues: Doesn’t play well with VPN & Captive Portals
TRR by default…but?

- Security risks: Using a resolver NOT on the local network breaks many things!
  - Local monitoring and security policies
    - Malware filtering
    - Malicious website filtering
    - Parental controls
    - Government mandated filtering
  - Split horizon DNS (fallback possible)
- Informed consent issues - for the DNS - really?
- Technical issues: Doesn’t play well with VPN & Captive Portals

Local Operator loses ability to monitor/control traffic

Users may have actively opt-ed in!
‘In trusted networks the network is your protector, not attacker’
DoH Implementation & Deployment

<table>
<thead>
<tr>
<th>Implementations</th>
<th>Stub</th>
<th>Recursive</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Firefox</strong> config option</td>
<td><strong>dnsdist</strong> (WIP)</td>
</tr>
<tr>
<td></td>
<td>• Chrome/Bromite</td>
<td>• Knot resolver (patches)</td>
</tr>
<tr>
<td></td>
<td>• Android ‘Intra’ App</td>
<td>• <a href="#">Various experimental</a> (proxy)</td>
</tr>
<tr>
<td></td>
<td>• Cloudflared</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Stubby (next release)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <a href="#">Various experimental</a></td>
<td></td>
</tr>
</tbody>
</table>
## DoH Implementation & Deployment

<table>
<thead>
<tr>
<th>Implementations</th>
<th>Stub</th>
<th>Recursive</th>
</tr>
</thead>
</table>
| • Firefox config option  
• Chrome/Bromite | Fast? Browser vendors control the client and update frequently. | • dnsdist (WIP)  
• Knot resolver (patches)  
• Various experimental (proxy) |
# DoH Implementation & Deployment

<table>
<thead>
<tr>
<th>Implementations</th>
<th>Stub</th>
<th>Recursive</th>
</tr>
</thead>
</table>
| • Firefox config option  
• Chrome/Bromite | Fast? Browser vendors control the client and update frequently. | • dnsdist (WIP)  
• Knot resolver (patches)  
• Various experimental (proxy) |

<table>
<thead>
<tr>
<th>Servers</th>
<th>Standalone</th>
<th>Large Scale</th>
</tr>
</thead>
</table>
| • ~10 other test servers | | • [Cloudflare](https://cloudflare-dns.com/dns-query)  
• [Google](https://dns.google.com/experimental)  
• [Quad9](https://dns*.quad9.net/dns-query) |
the Quads

- Quad9
  - Not-for-profit, offers blocking purely for security
  - Partners are IBM, PCH and Global Cyber Alliance

- Cloudflare
  - Currently privately owned, IPO possible (delayed in 2019)
  - Is really a CDN - provides free DNS to reduce latency

- Google
  - Is, well Google…Business model is advertising…
  - ‘Best Internet Innovator and provider of free services’ or ‘Biggest surveillance capitalist in the world’?
the Quads

- Quad9
  - Not-for-profit, offers blocking purely for security
  - Partners are IBM, PCH and Global Cyber Alliance

- Cloudflare
  - Currently privately owned, IPO possible (delayed in 2019)
  - Is really a CDN - provides free DNS to reduce latency

- Google
  - Is, well Google…Business model is advertising…
  - ‘Best Internet Innovator and provider of free services’ or ‘Biggest surveillance capitalist in the world’?
Today

Recursive resolver (from DHCP)

DNS

Internet

Desktop

DNS

system stub resolver

Local Network

App

DNS system library call getaddrinfo()
The DoH Future?

Recursive resolver (from DHCP)

DNS

Internet

Desktop

App
App
App
App

system stub resolver

DNS

Local Network

App
App
App
App

DoH

TRR 1
TRR 2
TRR 3
TRR 4

DNS Privacy
The DoH Future++?

Recursive resolver (from DHCP)

DNS

Desktop

App

system stub resolver

App

Local Network

Mixed DoH

Internet

Webserver

DNS Privacy
Other impacts of DoH/TRR
Other impacts of DoH/TRR

Not just at network operator level
Other impacts of DoH/TRR

- What if every application does its own DoH to its own chosen TRR?
- **Loss of central point of config on an end device**
  - Loss of easy user control of DNS
  - DNS no longer part of the device infrastructure, becomes part of a service. Do we need a system DOH service?
  - Will average user notice or care?
- Fragmented DNS service - How do you debug it (Support issue)?
- Fragmentation of the namespace - where does DNSSEC fit?
Does DoH pose new problems?

• VPNs share many characteristics of DoH
• Malicious programmers can hide in HTTPS anyway…..

• Can argue current architecture is flawed (not end-to-end)
  • Control should be managed at end points: Devices (Individuals or MDM)

• But
  • The potential scale and rapidity of changes to the architecture effected by DoH/TRR are unprecedented (highly disruptive to status quo)
  • None of the other supporting technologies to move to a full end-to-end model are in place or even agreed
  • Few companies are highly influential (IETF is having to be reactive, rather than lead design changes)
Where are we now?

- Mozilla are still experimenting - future default configuration not announced (DNS community is in limbo)

- Chrome have said they won’t have a default (Microsoft haven’t said anything officially but….)

- At the IETF: Several drafts listing issues with DoH deployment.
  - Questions on IETF role here… DoH genie is out of the bottle

- In the real world: Operators threatening to Ban/Block/Intercept DoH
  - ‘My network, my rules’
  - Huge concerns from ISPs and agencies that work with them (Cyber security, Child protection agencies, etc.)
Where are we now?

- Mozilla are still experimenting - future default configuration not announced (DNS community is in limbo)

- Chrome have said they won’t have a default (Microsoft haven’t said anything officially but….)

- At the IETF: Several drafts listing issues with DoH deployment.
  - Questions on IETF role here… DoH genie is out of the bottle

- In the real world: Operators threatening to Ban/Block/Intercept DoH
  - ‘My network, my rules’
  - Huge concerns from ISPs and agencies that work with them (Cyber security, Child protection agencies, etc.)

Many enterprise customers….
What is next?

• At the IETF:
  • Another DNS WG is likely to appear (ADD - Applications Doing DNS) to tackle deployment questions
  • DNSOP is working on how to discover server properties e.g. DoT, DoH but there are security issues with the proposal (as with DHCP)
  • DPRIVE has updated it’s goals, now working on recursive to authoritative

• In the real world:
  • Questions asked in the UK parliament - Could this lead to countries considering legislation to on this topic?
  • More operators are planning to deploy DoT
  • Waiting on Mozilla’s decision....
What is next?

• At the IETF:
  • Another DNS WG is likely to appear (ADD - Applications Doing DNS) to tackle deployment questions
  • DNSOP is working on how to discover server properties e.g. DoT, DoH but there are security issues with the proposal (as with DHCP)
  • DPRIVE has updated it’s goals, now working on recursive to authoritative

• In the real world:
  • Questions asked in the UK parliament - Could this lead to countries considering legislation to on this topic?
  • More operators are planning to deploy DoT
  • Waiting on Mozilla’s decision…. 

Stay tuned....
Summary

• DNS historically is a huge source of privacy leakage and a critical control point in the Internet Architecture

• Solutions exist to solve privacy issues but
  • Deployment of DoT is slow
  • Deployment of DoH is controversial

• You can encrypt your DNS today by choice

• Future is hard to predict (DoH, Namespace Fragmentation, Blockchain….)

• Internet Privacy is technical, practical and political.
Thank you!

Questions please
DNS tools

- https://dnsleaktest.com/results.html
- internet.nl