It’s DNS Jim, but not as we know it!

Sara Dickinson  sara@sinodun.com
What this talk will cover

**Overview**: Summarise the most recent evolutions in how end-device DNS resolution is being done (~past 5 years)

- **New IETF standards**: Encrypted transports for DNS (TLS & HTTPS)
- **Deployment Status**: Clients and resolver services for encrypted DNS
- **DNS resolution directly from applications**: Browsers
  - **DNS resolution to third party providers**: Implications for operators
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

- **DNS-over-TLS**: involved in standards dev, implementation and deployment (we contribute to dnsprivacy.org).
- **DNS-over-HTTPS**: Not directly involved, no links to browser vendors
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

• **DNS-over-TLS:** involved in standards dev, implementation and deployment (we contribute to dnsprivacy.org).
• **DNS-over-HTTPS:** Not directly involved, no links to browser vendors

**Goal** today is to bring awareness to this audience of fast moving changes: The good, the bad and the ugly....
The DNS is showing its age

- Nov 1987 - RFC1034 and RFC1035 published!

No Security or Privacy in the original design!
DNS-over-TLS (DoT)

Snowdon Revelations

1987  2012  2013  2014  2016  2018

It’s DNS Jim, but not as we know it!
DNS-over-TLS (DoT)

RFC7258: Pervasive Monitoring is an attack

Snowdon Revelations

1987  2012  2013  2014  2016  2018

It’s DNS Jim, but not as we know it!
DNS-over-TLS (DoT)

- RFC7258: Pervasive Monitoring is an attack
- DPRIVE WG formed
- Goals: 1) Encrypt Stub-Rec DNS 2) Think about Rec-Auth?

Snowdon Revelations

1987 2012 2013 2014 2016 2018

It’s DNS Jim, but not as we know it!
DNS-over-TLS (DoT)

- RFC7258: Pervasive Monitoring is an attack
- DPRIVE WG formed
- Goals:
  1. Encrypt Stub-Rec DNS
  2. Think about Rec-Auth?
- RFC7766: DNS-over-TCP

Snowdon Revelations

It's DNS Jim, but not as we know it!

DNS-over-TLS (DoT)

RFC7258: Pervasive Monitoring is an attack

DPRIVE WG formed

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

RFC7766: DNS-over-TCP

RFC7858: DNS-over-TLS

Port 853

Snowdon Revelations

1987 2012 2013 2014 2016 2018

Goals:
1) Encrypt Stub-Rec DNS
2) Think about Rec-Auth?
# DNS-over-TLS (DoT) Status

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
</table>
| 2015 - 2018| **Implementations:**  
               Clients: Android Pie, systemd, Stubby  
               Servers: Unbound, Knot resolver, dnsdist, (BIND) |
| 2015 - now | Set of 20 test DoT servers                                           |
| Nov 2017   | Quad9 (9.9.9.9) offer DoT                                           |
| Mar 2018   | Cloudflare launch 1.1.1.1 with DoT                                   |
## DNS-over-TLS (DoT) Status

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
</table>
| 2015 - 2018 | **Implementations:**  
Clients: Android Pie, systemd, Stubby  
Servers: Unbound, Knot resolver, dnsdist, |
| 2015 - now | Set of 20 test DoT servers                                          |
| Nov 2017  | Quad9 (9.9.9.9) offer DoT                                           |
| Mar 2018  | Cloudflare launch 1.1.1.1 with DoT                                   |

**System stub resolvers:**  
Need native Windows & macOS/iOS support
# DNS-over-TLS (DoT) Status

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015 - 2018</td>
<td><strong>Implementations:</strong></td>
</tr>
<tr>
<td></td>
<td>Clients: Android Pie, systemd, Stubby</td>
</tr>
<tr>
<td></td>
<td>Servers: Unbound, Knot resolver, dnsdist,</td>
</tr>
<tr>
<td>2015 - now</td>
<td>Set of 20 test DoT servers</td>
</tr>
<tr>
<td>Nov 2017</td>
<td>Quad9 (9.9.9.9) offer DoT</td>
</tr>
<tr>
<td>Mar 2018</td>
<td>Cloudflare launch 1.1.1.1 with DoT</td>
</tr>
</tbody>
</table>

System stub resolvers: Need native Windows & macOS/iOS support

Easy to run a DoT server

It’s DNS Jim, but not as we know it!
Encrypted DNS: the good…

- Defeats **passive surveillance**

- Server **authentication** if a name is **manually configured** (PKIX or DANE - [RFC8310](https://tools.ietf.org/html/rfc8310))
  - Prevents redirects, can’t intercept DNS queries
  - Increases ‘trust’ in service (DNSSEC, filtering…)

- **Data integrity of transport** - can’t inject spoofed responses
Encrypted DNS: the good... ✓

- Defeats **passive surveillance**

- Server **authentication** if a name is **manually configured** (PKIX or DANE - RFC8310)
  - Prevents redirects, can’t intercept DNS queries
  - Increases ‘trust’ in service (DNSSEC, filtering…)

- **Data integrity of transport** - can’t inject spoofed responses

**Opportunistic DoT:**
just need IP address
(Android Pie default)
Encrypted DNS: the good…

- Defeats **passive surveillance**
- Server **authentication** if a name is **manually configured** (PKIX or DANE - RFC8310)
  - Prevents redirects, can’t intercept DNS queries
  - Increases ‘trust’ in service (DNSSEC, filtering…)
- **Data integrity of transport** - can’t inject spoofed responses

**Opportunistic DoT**: just need IP address (Android Pie default)

**Strict DoT**: need a name too
Encrypted DNS: the bad & ugly...

- **SNI still leaks** (but not for long! draft-rescorla-tls-esni)
- A dedicated port (853) can be **blocked** (443 fallback)
- **Resolver** still sees all the traffic (who do you ‘trust’?)

  - If using a resolver NOT on the local network (not available)
    - Breaks Split horizon DNS (fallback possible), leaks internal names. Similar to e.g. using 8.8.8.8 but...
Encrypted DNS: the bad & ugly...

- **SNI still leaks** (but not for long! draft-rescorla-tls-esni)
- A dedicated port (853) can be **blocked** (443 fallback)
- **Resolver** still sees all the traffic (who do you ‘trust’?)

- If using a resolver NOT on the local network (not available)
  - Breaks Split horizon DNS (fallback possible), leaks internal names. Similar to e.g. using 8.8.8.8 but....

**Encrypted traffic bypasses local monitoring & security policies**
Encrypted DNS: the bad & ugly...

- **SNI still leaks** (but not for long! draft-rescorla-tls-esni)
- A dedicated port (853) can be **blocked** (443 fallback)
- **Resolver** still sees all the traffic (who do you ‘trust’?)

- If using a resolver **NOT** on the local network (not available)
  - Breaks Split horizon DNS (fallback possible), leaks internal names. Similar to e.g. using 8.8.8.8 but….

**Encrypted traffic bypasses local monitoring & security policies**

**For DoT, seen as short term or rare…**
WHAT IF I TOLD YOU BROWSERS ARE GOING TO DO THEIR OWN DOH
It's DNS Jim, but not as we know it!

WHAT IF I TOLD YOU BROWSERS ARE GOING TO DO THEIR OWN DOH

.....to their own chosen cloud resolver service!
DNS-over-HTTPS (DoH)
It’s DNS Jim, but not as we know it!

DNS-over-HTTPS (DoH)

First DoH draft published (query init)

- IETF 98
- March 2017
- May 2017
- Sep 2017
- Oct 2017
- Jul 2017
- Aug 2018

1987

UKNOF 41
DNS-over-HTTPS (DoH)

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

IETF 98

May 2017

Sep 2017

Oct 2017

1987

March 2017

Aug 2018

It’s DNS Jim, but not as we know it!
It’s DNS Jim, but not as we know it!

DNS-over-HTTPS (DoH)

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

DoH WG formed

First DoH draft published (query init)

IETF 98

March 2017

May 2017

Sep 2017

Oct 2017

DoH draft adopted

Submitted to IESG

Jul 2017

Aug 2018

1987

10
It’s DNS Jim, but not as we know it!

DNS-over-HTTPS (DoH)

First DoH draft published (query init)

DoH WG formed

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

DoH draft adopted

Submitted to IESG

Approved

IETF 98

Mar 2017

May 2017

Sep 2017

Oct 2017

Jul 2017

Aug 2018

1987

1987

1987

1987

1987

1987

1987

1987
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

Submitted to IESG

Approved

1987

March 2017

May 2017

Sep 2017

Oct 2017

Feb 2017

Jul 2017

Aug 2018

IETF 98

FAST!

1987

It’s DNS Jim, but not as we know it!
How is DoH different to DoT?

- **A Use case (of many):** “allowing web applications to access DNS information via existing browser APIs”

- **Discovery** - MUST use a URI template (not IP address)

- **Two models:**
  - **Dedicated** connections (only DoH traffic) - hard to block
  - **Mixed** connections (send DoH on existing HTTPS connections)
    - Better privacy? Not leaking queries

- **Increased tracking:** HTTP headers allow tracking of query via e.g. ‘User-agent’ (application), language, etc.
How is DoH different to DoT?

- **A Use case (of many):** “allowing web applications to access DNS information via existing browser APIs”

- Discovery - **MUST** use a URI template (not IP address)

- **Two models:**
  - **Dedicated** connections (only DoH traffic) - hard to block
  - **Mixed** connections (send DoH on existing HTTPS connections)
    - Better privacy? Not leaking queries

- **Increased tracking:** HTTP headers allow tracking of query via e.g. ‘User-agent’ (application), language, etc.
How is DoH different to DoT?

- **A Use case (of many):** “allowing web applications to access DNS information via existing browser APIs”

- **Discovery** - MUST use a URI template (not IP address)

- **Two models:**
  - **Dedicated** connections (only DoH traffic) - hard to block
  - **Mixed** connections (send DoH on existing HTTPS connections)
    - Better privacy? Not leaking queries

- **Increased tracking:** HTTP headers allow tracking of query via e.g. ‘User-agent’ (application), language, etc.

No ‘Opportunistic’ Specification differences

Impossible to block JUST DNS traffic
How is DoH different to DoT?

- **A Use case (of many):** “allowing web applications to access DNS information via existing browser APIs”

- Discovery - MUST use a URI template (not IP address)

- **Two models:**
  - *Dedicated* connections (only DoH traffic) - hard to block
  - *Mixed* connections (send DoH on existing HTTPS connections)
    - Better privacy? Not leaking queries

  **Impossible to block JUST DNS traffic**

- **Increased tracking:** HTTP headers allow tracking of query via ‘User-agent’ (application), language, etc.
# DoH Status

<table>
<thead>
<tr>
<th>Servers</th>
<th>Standalone</th>
<th>Large Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Google</td>
<td>• Cloudflare</td>
</tr>
<tr>
<td></td>
<td>• Few other test servers</td>
<td>• <a href="https://mozilla.cloudflare-dns.com/dns-query">https://mozilla.cloudflare-dns.com/dns-query</a></td>
</tr>
</tbody>
</table>
It's DNS Jim, but not as we know it!

### DoH Status

<table>
<thead>
<tr>
<th></th>
<th>Standalone</th>
<th>Large Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Servers</strong></td>
<td>• Google</td>
<td>• Cloudflare</td>
</tr>
<tr>
<td></td>
<td>• Few other test servers</td>
<td>• <a href="https://mozilla.cloudflare-dns.com/dns-query">https://mozilla.cloudflare-dns.com/dns-query</a></td>
</tr>
<tr>
<td><strong>Implemetations</strong></td>
<td>• Firefox Nightly config option</td>
<td>• dnsdist (WIP)</td>
</tr>
<tr>
<td></td>
<td>• Chrome (Bromite)</td>
<td>• <a href="https://knot-dns.org">Knot resolver (patches)</a></td>
</tr>
<tr>
<td></td>
<td>• Android ‘Intra’ App</td>
<td>• <a href="https://github.com/mozilla/transportd">Various experimental</a></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>• Various experimental</td>
<td></td>
</tr>
</tbody>
</table>
It’s DNS Jim, but not as we know it!

### Client Implementations
- **Firefox Nightly** config option
- Chrome (Bromite)
- Android ‘Intra’ App
- Cloudflared
- Stubby (next release)
- Various experimental

### Servers
- **Cloudflare**
  - [https://cloudflare-dns.com/dns-query](https://cloudflare-dns.com/dns-query)
  - [https://mozilla.cloudflare-dns.com/dns-query](https://mozilla.cloudflare-dns.com/dns-query)

### Standalone
- Google
  - [https://dns.google.com/experimental](https://dns.google.com/experimental)
- Few others

### Large Scale
- **Cloudflare**
  - [https://cloudflare-dns.com/dns-query](https://cloudflare-dns.com/dns-query)
  - [https://mozilla.cloudflare-dns.com/dns-query](https://mozilla.cloudflare-dns.com/dns-query)

- Various experimental

"Moziflare"
DNS in Browsers

- Some already have their own DNS stub (e.g. Chrome)
- Some already use encrypted DNS (Yandex, Tenta)
- Firefox 62 already has DoH, not enabled by default
  - Firefox Nightly DoH experiment completed….
- Chrome has a DoH implementation (not exposed, not advertised)
  - Used in the Chrome fork “Bromite”
  - And Google has a handy recursive resolver service in 8.8.8.8…
DNS in Browsers

- Some already have their own DNS stub (e.g. Chrome)
- Some already use encrypted DNS (Yandex, Tenta)

Firefox 62 already has DoH, not enabled by default
Firefox Nightly DoH experiment completed....

- Chrome has a DoH implementation (not exposed, not advertised)
  - Used in the Chrome fork “Bromite”
  - And Google has a handy recursive resolver service in 8.8.8.8...

Browser vendors control the client and update frequently.
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”

• 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”

• 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”

- 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.”
DoH in Firefox

- Mozilla blogs:
  - Firefox Nightly ‘Experiment’ (June) & Experiment results (Aug)
    - Half of users opted-in: Send all DNS queries to system resolver **AND to Cloudflare**, compare the results.
    - “Initial experiment focused on validating:
DoH in Firefox

- Mozilla blogs:
  - Firefox Nightly ‘Experiment’ (June) & Experiment results (Aug)
    - Half of users opted-in: Send all DNS queries to system resolver AND to Cloudflare, compare the results.
    - “Initial experiment focused on validating:
      1. Does the use of a cloud DNS service perform well enough to replace traditional DNS?”
DoH in Firefox

- Mozilla blogs:
  - Firefox Nightly ‘Experiment’ (June) & Experiment results (Aug)
    - Half of users opted-in: Send all DNS queries to system resolver AND to Cloudflare, compare the results.
    - “Initial experiment focused on validating:
      1. Does the use of a cloud DNS service perform well enough to replace traditional DNS?”

RESULTS: 6ms performance overhead is acceptable
“We’re committed long term to building a larger ecosystem of trusted DoH providers that live up to a high standard of data handling.”
“Trusted recursive resolver”

- Tweet from Patrick McManus: “We haven’t announced what that config will be or when it will be deployed (because we’re still working on on it :))”
- New UI to make config more obvious

It’s DNS Jim, but not as we know it!
“Trusted recursive resolver”

- Tweet from Patrick McManus: “We haven’t announced what that config will be or when it will be deployed (because we’re still working on it :)).”
- New UI to make config more obvious

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?)
“Trusted recursive resolver”

- Tweet from Patrick McManus: “We haven't announced what that config will be or when it will be deployed (because we're still working on on it :)).”
- New UI to make config more obvious

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?)

Potential **centralisation** of DNS resolution to a few providers?
Reactions are mixed...
Reactions are mixed...
Reactions are mixed...
Reactions are mixed…

Soon, DoH+TRR in this browser will be fully operational!

I've got a bad feeling about this…

It’s DNS Jim, but not as we know it!
Reactions?

- Ban/Block/Intercept Moziflare - ‘My network, my rules’
  - Operators need visibility (TLS 1.3 deja vu)
  - Is it even legal?

- Threat model analysis needed:
  - TRR useful but only in untrusted networks?
  - Users need choice (US lack of net neutrality vs EU GDPR)
  - Government regulation of TRRs, monetary incentives for apps?

- Analysis of third party DNS by PowerDNS
  - Neutrality of DNS operators (CDN’s?)
  - Legislation for blocking/filtering/interception?
Reactions?

• Ban/Block/Intercept Moziflare - ‘My network, my rules’
  • Operators need visibility (TLS 1.3 deja vu)
  • Is it even legal?

• Threat model analysis needed:
  • TRR useful but only in untrusted networks?
  • Users need choice (US lack of net neutrality vs EU GDPR)
  • Government regulation of TRRs, monetary incentives for apps?

• Analysis of third party DNS by PowerDNS
  • Neutrality of DNS operators (CDN’s?)
  • Legislation for blocking/filtering/interception?

EPIC thread on DNSOP

Lots of questions…
Managing many devices in enterprises

- What are **Chrome**, Safari, IE/Edge plans?
- What if **other apps** also do their own DoH/DoT?
- **Loss of central point of config on an end device?**
  - Loss of network settings as the default
  - DNS no longer part of the device infrastructure?
What to do?

- Think about running a **DoT server** in your network: for system level resolvers e.g. *Android, Stubby, systemd* it is the right thing!
- Think about running a **DoH server** in your network: gives users the option to use that, centralisation of DNS to a few players is a bad thing!

- **Watch this space and spread the word!** Work in progress:
  - Draft on an ‘opportunistic’ DoH discovery mechanism
  - Work in progress on Best Current Practices for Operators…
  - [dnsprivacy.org](http://dnsprivacy.org) website & twitter
What to do?

- Think about running a **DoT server** in your network: for system level resolvers e.g. *Android, Stubby, systemd* it is the right thing!
- Think about running a **DoH server** in your network: gives users the option to use that, centralisation of DNS to a few players is a bad thing!

- **Watch this space and spread the word!** Work in progress:
  - Draft on an ‘opportunistic’ DoH discovery mechanism
  - Work in progress on *Best Current Practices for Operators*…
  - [dnsprivacy.org](http://dnsprivacy.org) website & twitter

Stay tuned....
And now for something completely different...!
A (EDNS) change is coming

• **When?** 1st Feb 2019
• **What?** Removal of workarounds for EDNS issues (failures, timeouts, incorrect responses due to middleboxes, firewalls, old nameserver s/w)
• **Who?** ‘Big 4’ open source DNS implementors

• **Your problem?** Only if your zone is not compliant!

• **To check:** https://dnsflagday.net/
Thank you!