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

Sara Dickinson  sara@sinodun.com
               sinodun.com
               @SinodunCom
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)

- 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
- **RFC7766**: DNS-over-TCP
- **RFC7858**: DNS-over-TLS
- **DPRIVE WG formed**
- **Goals**:
  1. Encrypt Stub-Rec DNS
  2. Think about Rec-Auth?
- **Snowdon Revelations**
- **Port 853**

1987 → 2012 → 2013 → 2014 → 2016 → 2018

It’s DNS Jim, but not as we know it!
### 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><strong>Clients:</strong> Android Pie, systemd, Stubby</td>
</tr>
<tr>
<td></td>
<td><strong>Servers:</strong> Unbound, Knot resolver, dnsdist, (BIND)</td>
</tr>
<tr>
<td>2015 - now</td>
<td><strong>Set of 20 test DoT servers</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 launch 1.1.1.1 with DoT</td>
</tr>
</tbody>
</table>
# 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><strong>Clients</strong>: Android Pie, systemd, Stubby</td>
</tr>
<tr>
<td></td>
<td><strong>Servers</strong>: Unbound, Knot resolver, dnsdist,</td>
</tr>
<tr>
<td>2015 - now</td>
<td><strong>Set of 20 test DoT servers</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 launch 1.1.1.1 with DoT</td>
</tr>
</tbody>
</table>

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>
</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
- **Easy to run a DoT server**
Encrypted DNS: the good... 

- Defeats **passive surveillance**

- Server **authentication** if a name is **manually configured** (PKIX or DANE - [RFC8310](https://rfc-editor.org/rfc/rfc8310.html))
  - 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](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

**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](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

**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](https://www.rfc-editor.org/rfc/rfc9465))
- 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](https://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)

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

1987

RIPE 77

May 2017

Sep 2017

Oct 2017

Jul 2017

Aug 2018

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.”

First DoH draft published (query init)

DoH WG formed

DoH draft adopted

Submitted to IESG

Approved

IETF 98

May 2017

Sep 2017

Oct 2017

Jul 2017

Aug 2018

RIPE 77

1987

March 2017

May 2017

Sep 2017

Oct 2017

Jul 2017

Aug 2018

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

FAST!

IETF 98

May 2017

Sep 2017

Oct 2017

Jul 2017

Aug 2018

RIPE 77

1987

1987

May 2017

March 2017

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.
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 ‘User-agent’ (application), language, etc.

Impossible to block JUST DNS traffic

No ‘Opportunistic’

New privacy concerns
## DoH Status

<table>
<thead>
<tr>
<th>Servers</th>
<th>Standalone</th>
<th>Large Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• ~10 other test servers</td>
<td>• <a href="https://cloudflare-dns.com/dns-query">Cloudflare</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="https://dns.google.com/experimental">Google</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="https://dns*.quad9.net/dns-query">Quad9</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 3 flavours of service</td>
</tr>
</tbody>
</table>
DoH Status

<table>
<thead>
<tr>
<th>Implementations</th>
<th>Client</th>
<th>Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Servers</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>~10 other test servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Large Scale</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloudflare (<a href="https://cloudflare-dns.com/dns-query">https://cloudflare-dns.com/dns-query</a>)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google (<a href="https://dns.google.com/experimental">https://dns.google.com/experimental</a>)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quad9 (<a href="https://dns*.quad9.net/dns-query">https://dns*.quad9.net/dns-query</a>)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 flavours of service</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Standalone</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firefox config option</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chrome/Bromite</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Android ‘Intra’ App</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloudflared</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stubby (next release)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Various experimental</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## DoH Status

<table>
<thead>
<tr>
<th>Servers</th>
<th>Standalone</th>
<th>Large Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• ~10 other test servers</td>
<td>• <a href="https://cloudflare-dns.com/dns-query">Cloudflare</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="https://dns.google.com/experimental">Google</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="https://dns*.quad9.net/dns-query">Quad9</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 flavours of service</td>
</tr>
<tr>
<td>Implemenations</td>
<td>• Firefox config option</td>
<td>• dnsdist (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>• Various experimental</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>
DNS in Browsers

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

  - Firefox had DoH since 61, not enabled by default
  - Firefox experiment being performed....

- Chrome has a DoH implementation (not exposed, not advertised)
  - Recent a PR to add config option
  - And Google has a handy recursive resolver service in 8.8.8.8...
It’s DNS Jim, but not as we know it!

DNS in Browsers

- Some already have their own DNS stub (e.g. Chrome)
- Some already use encrypted DNS (Yandex, Tenta)
- Firefox had DoH since 61, not enabled by default
- Firefox experiment being performed....
- Chrome has a DoH implementation (not exposed, not advertised)
  - Recent a PR to add config option
  - 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:
      - Another experiment in Firefox Beta announced… (Sept)
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?”

- Another experiment in Firefox Beta announced…(Sept)
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.”

- Another experiment in Firefox Beta announced…(Sept)
“Trusted recursive resolver”

- Tweet from Mozilla developer: “We haven’t announced what that config will be or when it will be deployed (because we’re still working on it :)).”
- DNS community is in limbo waiting for this decision!
“Trusted recursive resolver”

- Tweet from Mozilla developer: “We haven't announced what that config will be or when it will be deployed (because we're still working on it :)).”
- DNS community is in limbo waiting for this decision!

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 Mozilla developer: “We haven't announced what that config will be or when it will be deployed (because we're still working on it :)).”
- DNS community is in limbo waiting for this decision!

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:
  - [DoH discovery mechanism & Best Current Practices](#)
  - [More detailed DNS-OARC talk](#)
  - [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:
  - [DoH discovery mechanism](#) & [Best Current Practices](#)
  - [More detailed DNS-OARC talk](#)
  - [dnsprivacy.org](#) website & [twitter](#)

Stay tuned…. 

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