It’s DNS Jim, but not as we know it!

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

Stub to recursive

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

RIPE 77

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

DNS-over-TLS (DoT) Status

Date	Event
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

Date	Event
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

Date	Event
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)
  - 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**

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

- 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

Encrypted DNS: the good… ✔

- Defeats **passive surveillance**

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

- 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…)

Strict DoT: need a name too

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

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
imgflip.com

…..to their own chosen cloud resolver service!

DNS-over-HTTPS (DoH)

1987

RIPE 77

March 2017

IETF 98

First DoH draft published (query init)

May 2017

DoH WG formed

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

Sep 2017

Oct 2017

DoH draft adopted

Jul 2017

Aug 2018

It’s DNS Jim, but not as we know it!

DNS-over-HTTPS (DoH)

1987

RIPE 77

March 2017

IETF 98

May 2017

First DoH draft published (query init)

Sep 2017

DoH WG formed

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

Oct 2017

DoH draft adopted

Jul 2017

Submitted to IESG

Aug 2018

Approved

It’s DNS Jim, but not as we know it!

DNS-over-HTTPS (DoH)

1987

RIPE 77

March 2017

IETF 98

May 2017

First DoH draft published (query init)

Sep 2017

DoH WG formed

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

Oct 2017

DoH draft adopted

FAST!

Jul 2017

Submitted to IESG

Aug 2018

Approved

It’s DNS Jim, but not as we know it!

Specification differences

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.

Specification differences

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)**

No ‘Opportunistic’

- **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.

Specification differences

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)**

No ‘Opportunistic’

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

Specification differences

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)**

No ‘Opportunistic’

- **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.

New privacy concerns

DoH Status

	Standalone	Large Scale
Servers	• ~10 other test servers	• Cloudflare (https://cloudflare-dns.com/dns-query) • Google (https://dns.google.com/experimental) • Quad9 (https://dns*.quad9.net/dns-query) • 3 flavours of service

DoH Status

	Standalone	Large Scale
Servers	• ~10 other test servers	• Cloudflare (https://cloudflare-dns.com/dns-query) • Google (https://dns.google.com/experimental) • Quad9 (https://dns*.quad9.net/dns-query) • 3 flavours of service

	Client	Servers
Implementations	• **Firefox** config option • Chrome/Bromite • Android 'Intra' App • Cloudflared • Stubby (next release) • Various experimental	• **dnsdist (WIP)** • **Knot resolver (patches)** • Various experimental

DoH Status

	Standalone	Large Scale
Servers	• ~10 other test servers	• Cloudflare (https://cloudflare-dns.com/dns-query) • Google (https://dns.google.com/experimental) • Quad9 (https://dns*.quad9.net/dns-query) 3 flavours of service

"**Moziflare**"

	Client	Servers
Implementations	• **Firefox** config option • Chrome/Bromite • Android 'Intra' App • Cloudflared • Stubby (next release) • Various experimental	• **dnsdist (WIP)** • **Knot resolver (patches)** • Various experimental

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….**

Dedicated DoH connections

- 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…

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….**

Dedicated DoH connections

- 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?

Dedicated DoH connections

DoH in Firefox

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

Dedicated DoH connections

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)”**

Dedicated DoH connections

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

Dedicated DoH connections

- 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

Dedicated DoH connections

- 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

Dedicated DoH connections

- 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 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 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 on it :)).”
- DNS community is in limbo waiting for this decision!

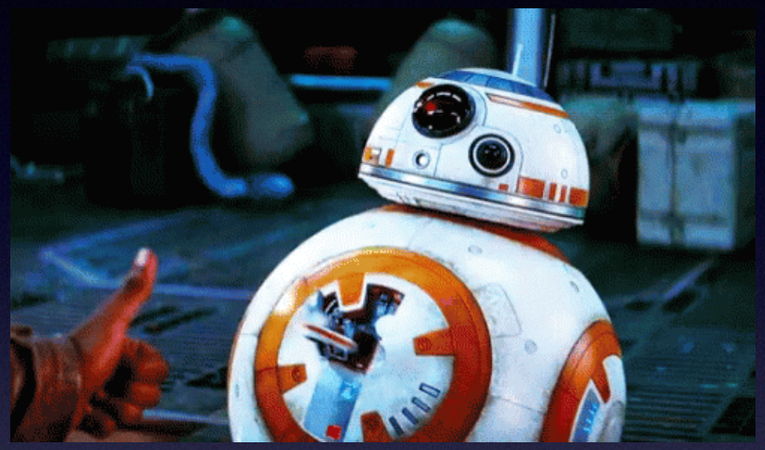
Impact of TRRs? Applications using default TRRs fundamentally change the existing **implicit** consent model for DNS:

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

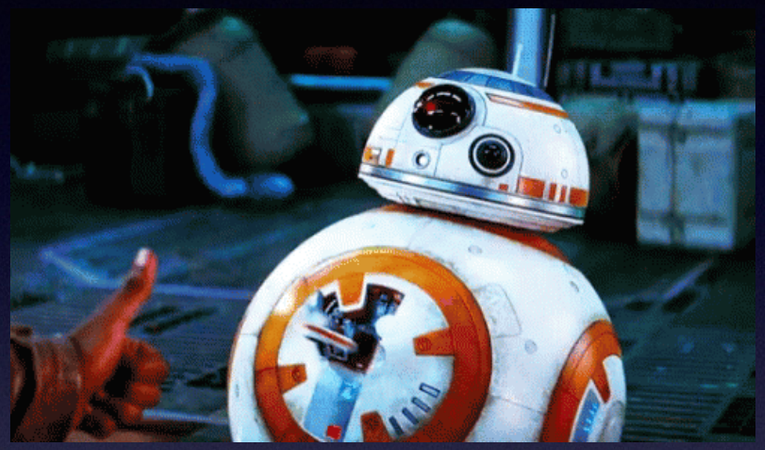
Potential **centralisation** of DNS resolution to a few providers?

Reactions are mixed…

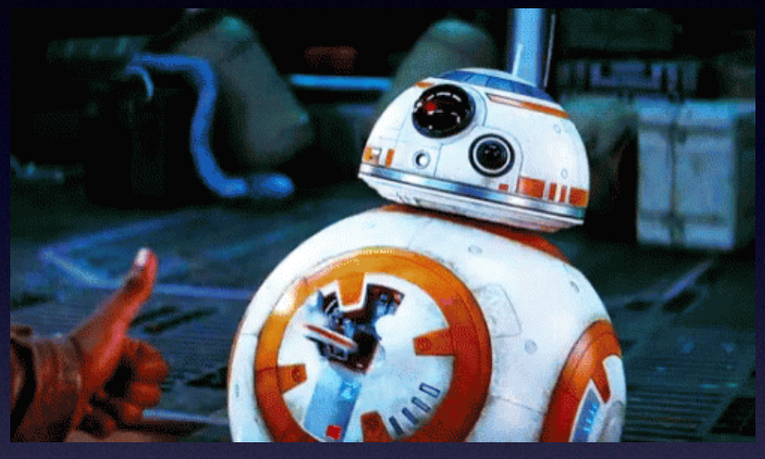
Reactions are mixed…



Reactions are mixed…



Reactions are mixed…



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

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….

Thank you!