sara@sinodun.com
sinodun.com
SinodunCom

Stub to recursive

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

sinodun

Sinodun IT

dnsprivacy.org

Sinodun IT

dnsprivacy.org

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

RFC1034 RFC1035

No Security or Privacy in the original design!

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

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

2013

2014

2016

1987

2012

2018

Date	Event
2015 - 2018	Clients Servers
2015 - now	Set of 20 test DoT servers
Nov 2017	
Mar 2018	

Date	Event
2015 - 2018	Clients Servers
2015 - now	Set of 20 test DoT servers
Nov 2017	
Mar 2018	

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

Date	Event
2015 - 2018	Clients Servers
2015 - now	Set of 20 test DoT servers
Nov 2017	
Mar 2018	

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

Easy to run a DoT server

RFC8310

✓

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

RFC8310

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

[RFC8310]

Strict DoT: need
a name too

draft-rescorla-tls-esni

draft-rescorla-tls-esni

Encrypted traffic bypasses local monitoring & security policies

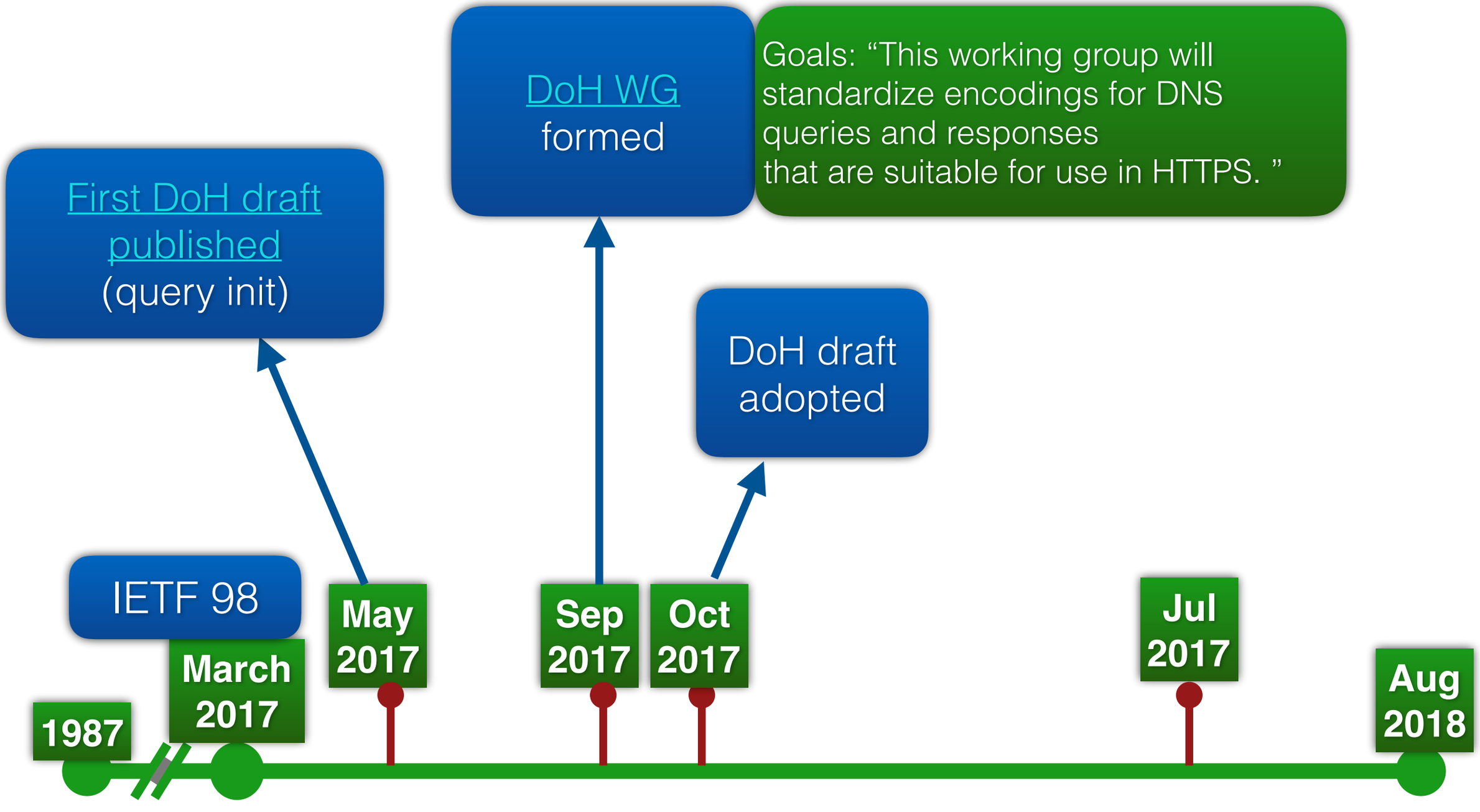
draft-rescorla-tls-esni

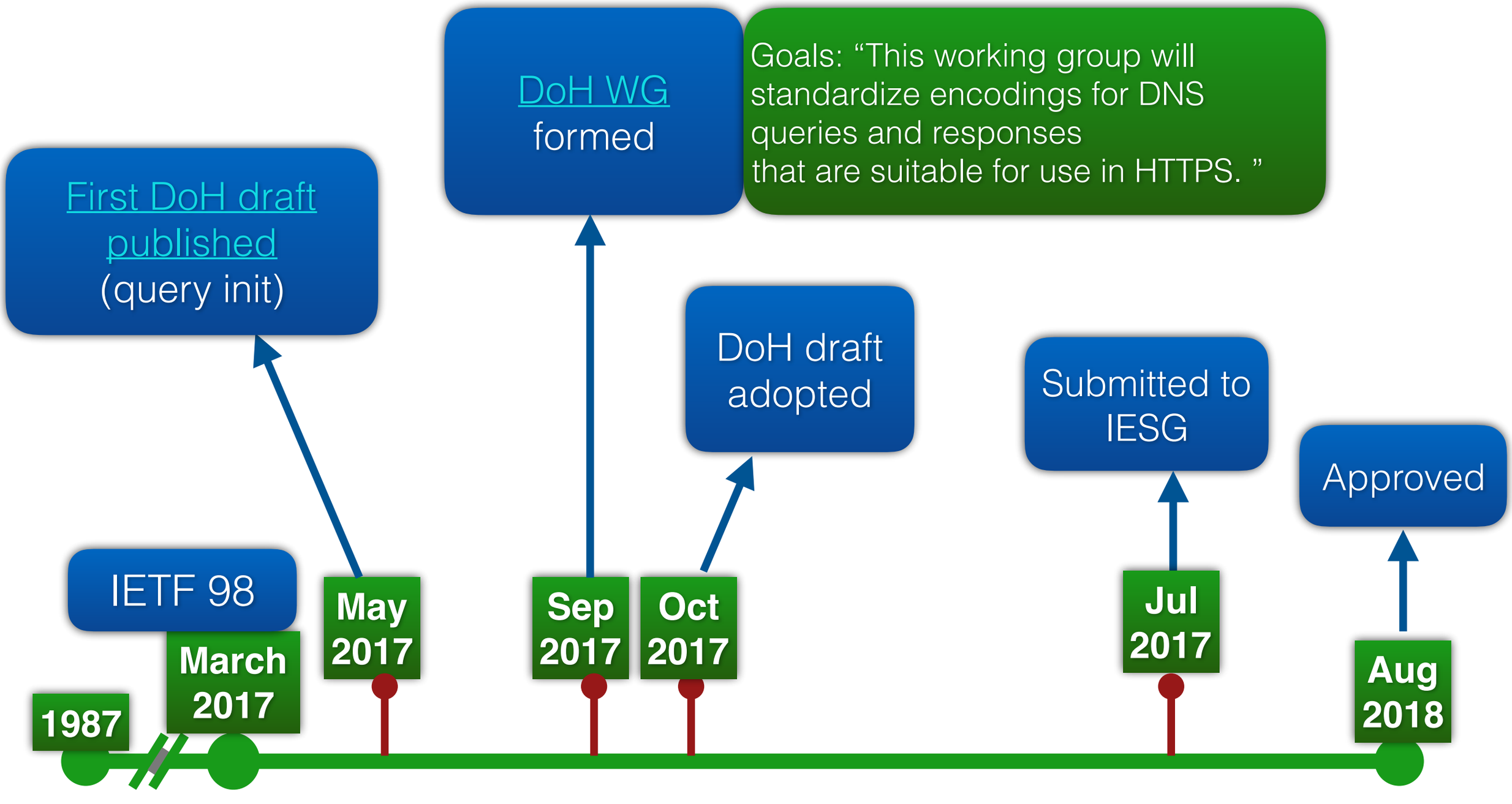
Encrypted traffic bypasses local monitoring & security policies

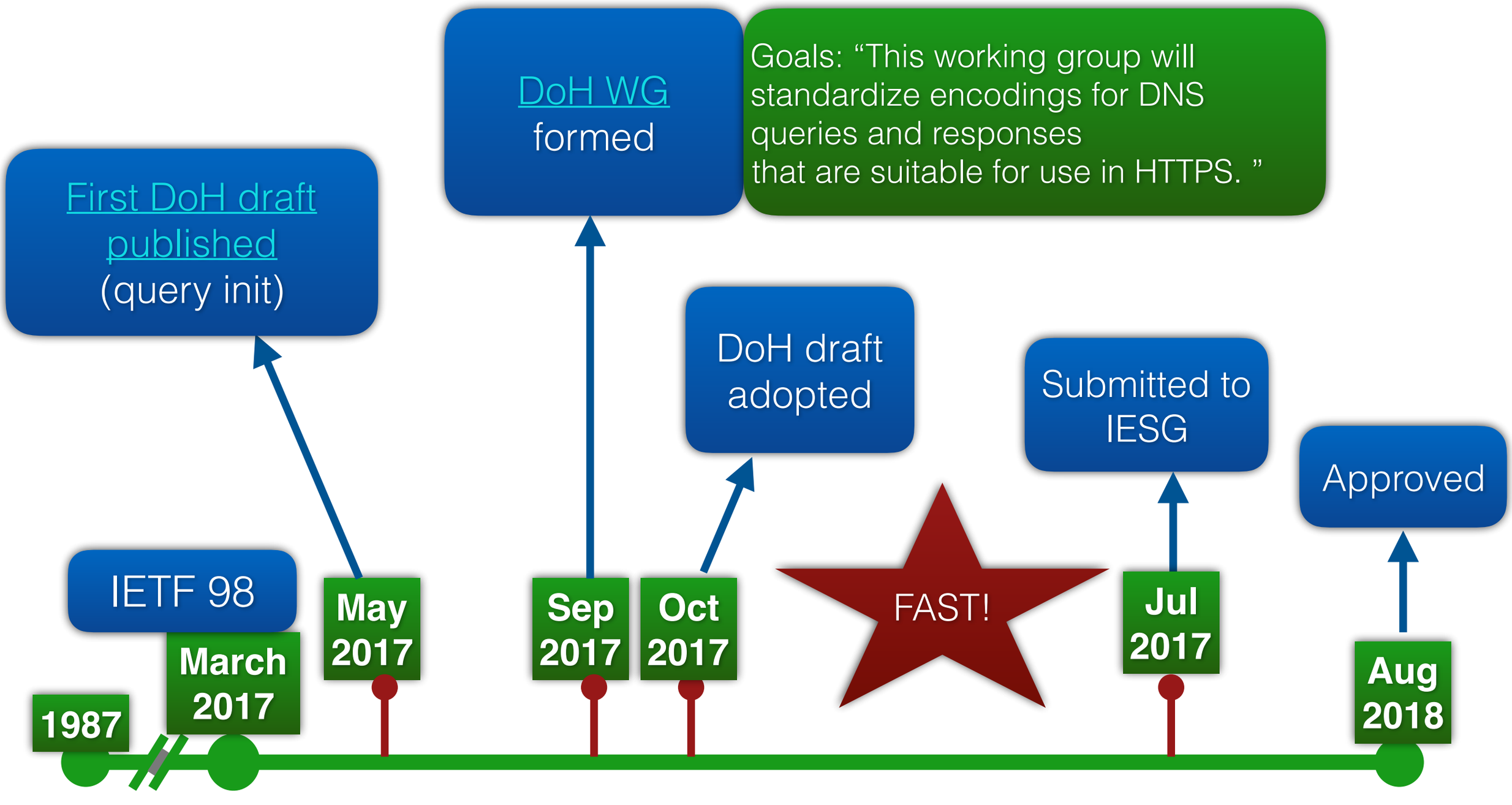
For DoT, seen as short term or rare…


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

…..to their own chosen cloud resolver service!


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
IETF 98
1987
March 2017
May 2017
Sep 2017
Oct 2017
Jul 2017
Aug 2018


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
1987
March 2017
May 2017
Sep 2017
Oct 2017
Jul 2017
Aug 2018


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
FAST!
1987
March 2017
May 2017
Sep 2017
Oct 2017
Jul 2017
Aug 2018

Specification differences

Specification differences

No ‘Opportunistic’

Specification differences

No ‘Opportunistic’

Impossible to block JUST DNS traffic

Specification differences

No ‘Opportunistic’

Impossible to block JUST DNS traffic

New privacy concerns

	Standalone	Large Scale
Servers	~10 other test servers	Cloudflare Google Quad9

	Standalone	Large Scale
Servers	~10 other test servers	Cloudflare Google Quad9

	Client	Servers
Implementations	Various experimental	Various experimental

	Standalone	Large Scale
Servers	~10 other test servers	Cloudflare Google ad9

"**Moziflare**"

	Client	Servers
Implementations	Various experimental	Various experimental

Yandex Tenta

Dedicated DoH connections

Recent a PR to add config option

Yandex Tenta

Dedicated DoH connections

Recent a PR to add config option

Browser vendors control the client and update frequently.

Mozilla’s answer:

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"

Mozilla's answer:

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"

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'…."

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"

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

Experiment & Future plans

Dedicated DoH connections

Experiment & Future plans

- **“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

Experiment & Future plans

- **“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.”

Dedicated DoH connections

[Firefox Nightly ‘Experiment’]

[Experiment results]

[Another experiment in Firefox Beta announced]

Dedicated DoH connections

[Firefox Nightly ‘Experiment’]

[Experiment results]

1. Does the use of a **cloud DNS service** perform well enough to replace traditional DNS?”

[Another experiment in Firefox Beta announced]

Dedicated DoH connections

[Firefox Nightly ‘Experiment’]

[Experiment results]

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]

Tweet from Mozilla developer

Tweet from Mozilla developer

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

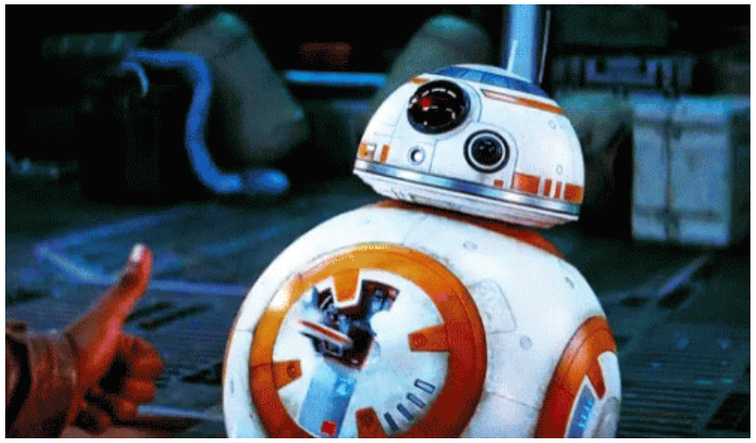
- (Current) Log onto a network and use the DHCP provided resolver
- (New?) Use an app and agree to app T&C's (including DNS?)

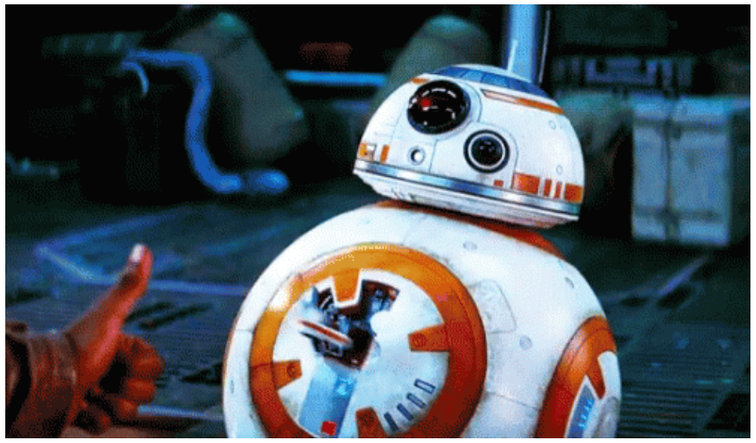
Tweet from Mozilla developer

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

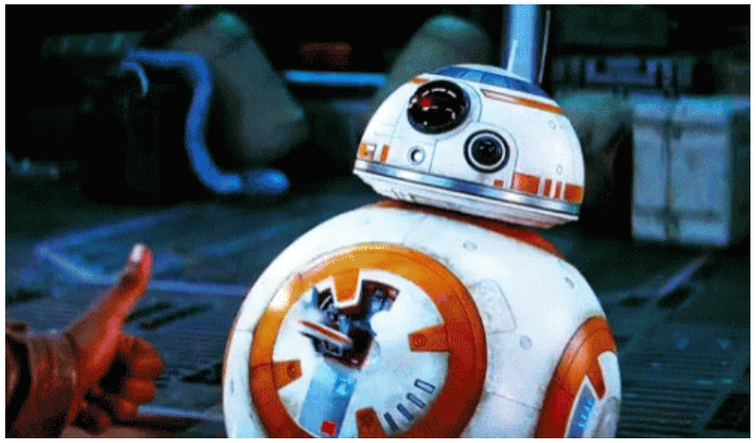
- (Current) Log onto a network and use the DHCP provided resolver
- (New?) Use an app and agree to app T&C's (including DNS?)

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






I've got a bad feeling
about this...



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

EPIC thread on DNSOP

Analysis of third party DNS by PowerDNS

EPIC thread on DNSOP

Analysis of third party DNS by PowerDNS

Lots of questions…

DoH discovery mechanism Best Current Practices

More detailed DNS-OARC talk

dnsprivacy.org twitter

DoH discovery mechanism Best Current Practices

More detailed DNS-OARC talk

dnsprivacy.org twitter

Stay tuned….