DoH - Coming soon to a browser near you!

- Browsers are starting to use DoH
- Multiple deployment proposals
Proposed Deployment Models

- Chrome: opportunistic encryption
- If the system-configured resolver is DoH, capable, use DoH
Proposed Deployment Models

- Firefox: single privacy-preserving DoH server
New model: multiple simultaneous DNS servers

- Picking a single, fixed resolver can have downsides
  - Performance
  - Privacy
  - Security
  - Commercial considerations
Performance

- A large network/CDN/Cloud provider may be able to perform fast resolution for a given website (e.g. because the authoritative servers are on its network)
Privacy

● Spreading DNS queries out across multiple resolvers conceals full browsing history from a single provider
Security

- Sites may want to specify that users should use a resolver that meets specific requirements for security or functionality.
Commercial Considerations

- There may be real or perceived pressure for resolvers operating by entities that have other commercial interests to slow resolution for sites hosted on competing platform
Proposed Deployment Models

- Firefox’s future(?): curated list of DoH servers
Proposed Deployment Models

- Future(?): Discovery of designated DoH providers
New model: multiple DoH servers

- Which set of DNS resolvers to use?
  - Pre-set list
  - Discovery

- How to choose which DNS resolver for a given query?
  - Round-robin
  - Sticky associations
Downsides of pre-set list + round-robin

- **Performance**
  - Less-than optimal selection

- **Privacy**
  - Some DoH servers are co-located with authoritative servers
Proposed solution: DoH-Preference Header

Let users and the site have a say in how future DNS resolutions are performed.

Inspired by HSTS

Completely optional, user agent is free to decide

DoH-Preference: "https://dnsserver.example.net/dns-query{?dns}";
max-age=15768000
Intended Deployment

- Browsers ship with
  - a vetted list of servers or
  - a discovery mechanism for trustworthy resolvers
- Content providers can supply a hint, if the hint is in the vetted list, the browser may use that resolver in the future
First request

Q: site.com
A: 4.3.2.1
GET https://site.com
DoH-Preference: 1.1.1.1
Second request

Q: site.com
A: 4.3.2.1
GET https://site.com
DoH-Preference: 1.1.1.1

site.com : 1.1.1.1
Solving the single resolver issues

- **Performance**
  - Origin knows fastest DoH resolver for its host

- **Privacy**
  - Origin knows best which resolvers to be trusted with queries

- **Security**
  - Origin can choose resolvers with high security (e.g. DNSSEC-validating)

- **Commercial considerations**
  - Origin can choose resolver that does not conflict commercially with HTTP service provider
Fallback

- *Unlike* HSTS, fallback is always to the default DNS resolution mechanism, any failure results in fallback
Preventing tracking

- In order to be useful, preference must survive longer than DNS cache, preferably until next time user visits the site.
- Could be a vector for tracking users.
- Hint is only accepted if it matches a vetted list of DoH templates.
- Needs to be properly double-keyed
  - Proposal avoids leaking information by keying to both first party domain and the domain sending the header.
  - Prevents tracking across site visits.