DDI User Group

Encrypted DNS Update

2nd December 2021

Andrew Campling
Andrew.Campling@419.Consulting

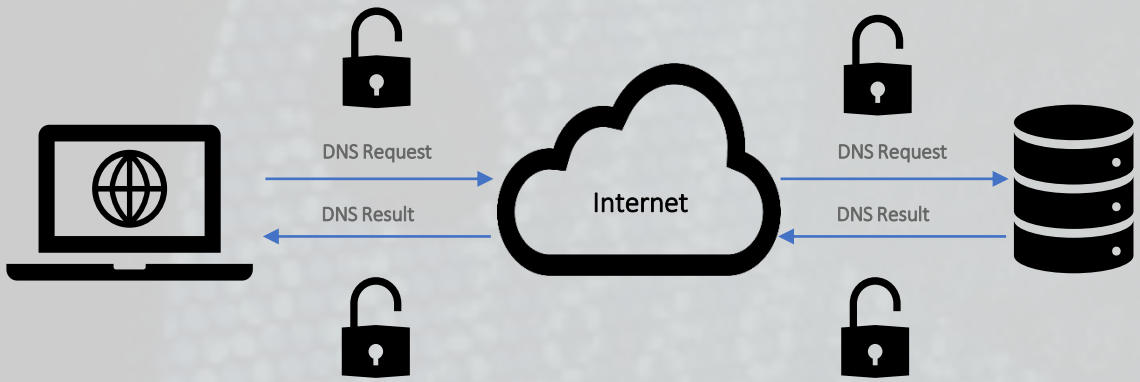
419.Consulting

Agenda

- Encrypted DNS
  - DoH
  - Approaches to Resolver Upgrades
  - Other Developments
  - Private Relay
- Privacy and Transparency
- DNS4EU
- What Else is Coming?
- Additional Information

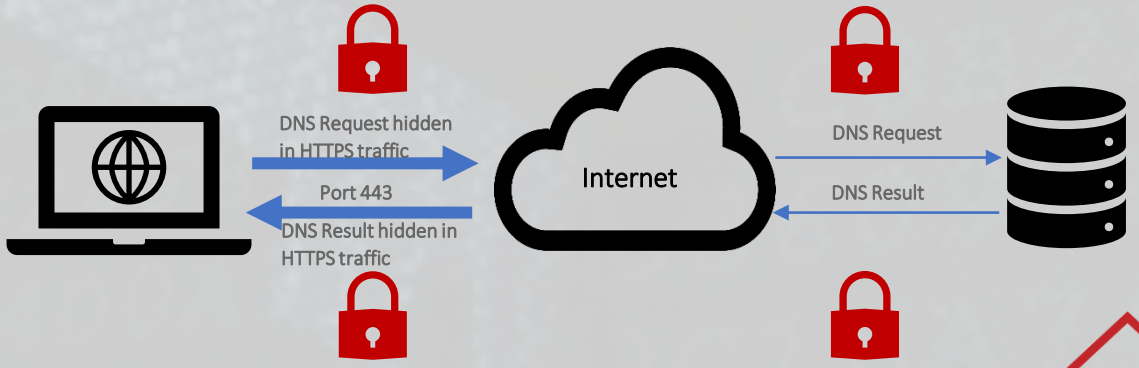
What is Encrypted DNS?

Traditional DNS – Do53



- Defined in IETF RFC 8484
- Sends DNS queries from the client to the resolver via an encrypted HTTPS connection
- Can be used by any client software, bypassing any user or operating system preferences

DNS over HTTPS (DoH)



419.Consulting

Approaches to Resolver Upgrades

Mozilla

- In the US, Firefox automatically switches from the current resolver to one trusted by Mozilla (within its TRR programme)
- It assumes that an encrypted resolver provides better protection
  - The existing resolver may be encrypted
  - The TRR option may not provide malware filtering etc
- Creates policy challenges

Google Chome and Windows 10+

- Same-Provider, Auto-upgrade
- Switches from Do53 resolver to an encrypted option from the same resolver operator
- Should carry forward existing policies
- Currently relies on a curated list maintained by the client software provider
- Requires public IP address for resolver

Resolver Discovery

- Options being developed within the IETF (the ADD working group)
  - DDR (discovery of designated resolvers)
  - DNR (discovery of network resolvers)
  - Support for "Split Horizon" DNS
- Early deployment of DDR by Cisco, Microsoft and Quad9
- DNR suited to ISPs with DNS forwarders – requires upgraded CPE

Other Developments

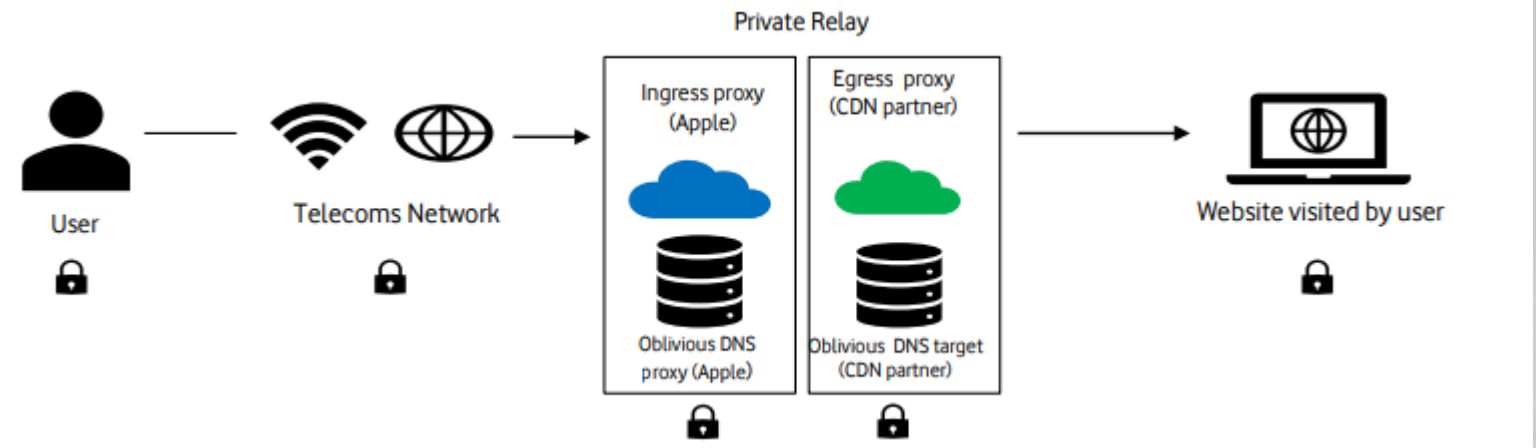
- DNS-over-QUIC
  - AdGuard claims first deployment of client and resolver
  - DoQ standard still being worked on at IETF

- Structured Data for DNS Access Denied Error Page
  - Builds on the “Extended DNS Errors” proposed standard (RFC 8914)
  - Provides option for more meaningful error message than NXDOMAIN

- Oblivious DoH
  - Requires two proxies - hides DNS query from first proxy, source IP address from the second
  - Experimental
    - Not being progressed as a standard within the IETF
    - Focus is on Oblivious HTTP instead

- DoH-over-Tor
  - Additional privacy benefits
  - Not for the mass market!
  - Presentation outlining the key concept here

Private Relay



Apple's Private Relay service encrypts traffic and masks the user's IP address via a new, dedicated system

- Traffic (specifically, browser traffic for 'tracking sites' in the basic Private Relay offering, traffic for all websites in the enhanced Private Relay offering), between the user is tunnelled and encrypted by the handset, and then sent to an 'ingress' proxy managed by Apple and then forwarded to an 'egress' proxy managed by Apple's 3rd party partner.
- The proxies allocate random IP addresses to users so that websites cannot track users based on their IP address. Neither proxy knows the user's IP address and the website they are visiting. This means neither websites, nor Apple, nor the CDN partner can track users based on their IP address
- For all iCloud+ customers, the DNS server provided by the network operator is bypassed. They are replaced by DNS nodes provided by Apple and their partner which encrypts and anonymises the domain name resolution requests. This applies to not only to browser traffic DNS requests but to all the interactions (e.g. apps) between the user and the internet.

419.Consulting

Private Relay

Summary

- A service with the iCloud+ offering for iOS / iPadOS 15+ and and macOS Monterey
- Uses ODoH for DNS traffic, also carries Safari HTTP and other data

More Information

- Announced at Apple's annual developer conference in June 2021, details here
- More technical detail made available on my weekly call shortly after WWDC, details here
- A blog post and also a report on the implications of Private Relay for network operators and ISPs are available here and here respectively

Privacy and Transparency

Mozilla / Firefox

- Trusted Recursive Resolver programme launched alongside DoH support in Firefox
- As a result of a recent public consultation, Mozilla has removed blocklist disclosure requirement

European Resolver Policy – www.EuropeanResolverPolicy.com

- Alternative to Mozilla's TRR programme
- GDPR compliant
- Clear prohibition of monetisation of personal data
- Requirement to state jurisdiction of service

419.Consulting

DNS4EU: Concept

Source – European Commission

"DNS4EU is conceived as an **alternative** to existing DNS resolution services, increasing **overall Internet resilience**, and offering European citizens and private and public organisations the capacity to access the web with a **high-quality and free service**, based in the EU, that guarantees data protection according to EU rules and increases the **protection from malware, phishing and cyber attacks**."

DNS4EU: Characteristics

Source – European Commission

- Have a large footprint within the EU, enabling paid premium services such as specific performance and security criteria for vertical sectors (health, transport, industry, finance etc) or enhanced security (filtering, 24x7 support) for companies
- Be fully transparent and compliant with GDPR
- Offer state-of-the-art, ad-hoc DNS filtering against phishing or malware based on existing global threat feeds and own feeds
- Conform to the latest security and privacy technological standards, including DoH
- Develop wholesale discovery and resolution services for other digital service providers, including ISPs and Cloud service providers

DNS4EU: Next Steps

Source – European Commission

- **Pending confirmation:** Connecting Europe Facility (CEF2) – European Cloud Federation Initiative
- 50% of the initial infrastructure investment
- Expected publication of the call: End of 2021
- Conform to the latest security and privacy technological standards, including DoH
- Federated structure: high-quality consortia, potentially including vertical industries, to best increase the footprint and customer base of DNS4EU in the EU, reduce costs through shared resources, operations and cyber security feeds and ensure the long-term sustainability of DNS4EU

Additional background information is available here

419.Consulting

What Else is Coming?

- Encrypted Client Hello (ECH)
  - Encrypt the SNI data
  - Early, pre-standard deployments beginning
  - Standard finalized in 2022?
  - More background information on ECH is available here
- Server-Side Evasion of Filtering
  - Already tested, paper presented during the IRTF Open session at IETF 112
  - A paper outlining the concepts is available here
  - Update during my weekly call next Monday (16:00 UTC)

Additional Information

- IETF Adaptive DNS Discovery (ADD) working group - https://datatracker.ietf.org/wg/add/about/

- Weekly encrypted DNS calls
  - Archive - https://419.consulting/encrypted-dns
  - Invitation and inclusion on mailing list – Andrew.Campling@419.Consulting

- Internet Governance Forum 6th – 10th December
  - See link for more details inc **IGF 2021 WS #209 The State of DNS Privacy Technologies**

- ICANN Resolver Operator Forum – 14th December, see link for more details
  - Opening talk – Paul Mockapetris, confirmed speakers include Puneet Sood, John Todd, Jason Livingood, Molay Ghosh
  - A software vendor panel, moderated by Paul Hoffman, includes Vicky Risk, Benno Overeinder, and Peter van Dijk. The panel will be discussing feature sets for resolvers: planned and wished-for.

Any Questions?

Andrew.Campling@419.Consulting