The State of DNS Privacy Technologies

AusNOG 2021

7th April 2022

Andrew Campling
Andrew.Campling@419.Consulting

419.Consulting

Agenda

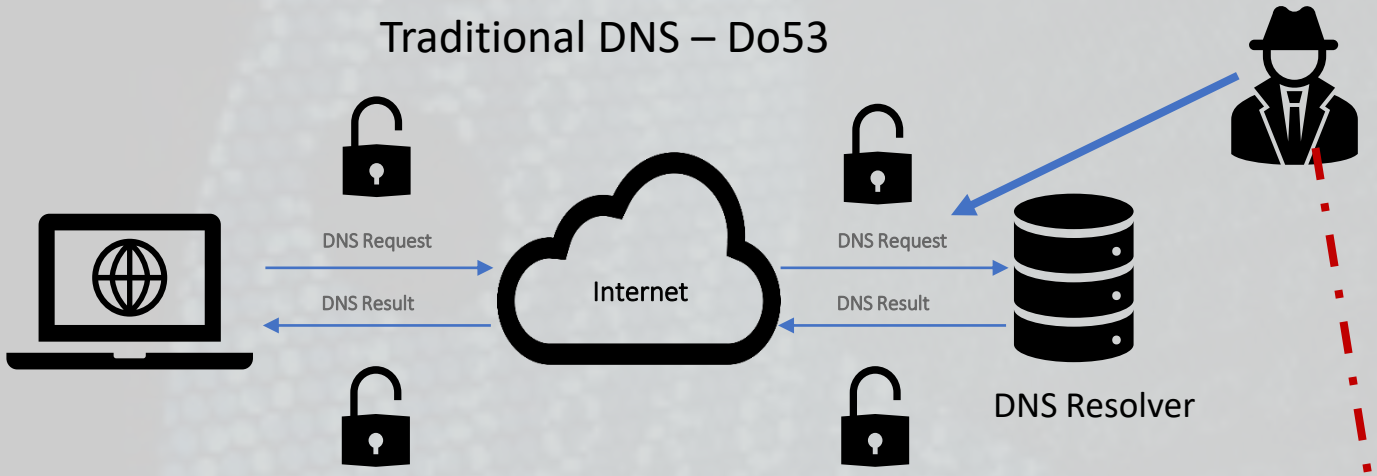
- Context – Why Operators Should Care
- Encrypted DNS
  - DNS-over-HTTPS
  - Approaches to Resolver Upgrades
  - Other Developments
  - Private Relay
- What Else is Coming?
- Can Technology Alone Solve the Problem?
- Privacy and Transparency
- Additional Information

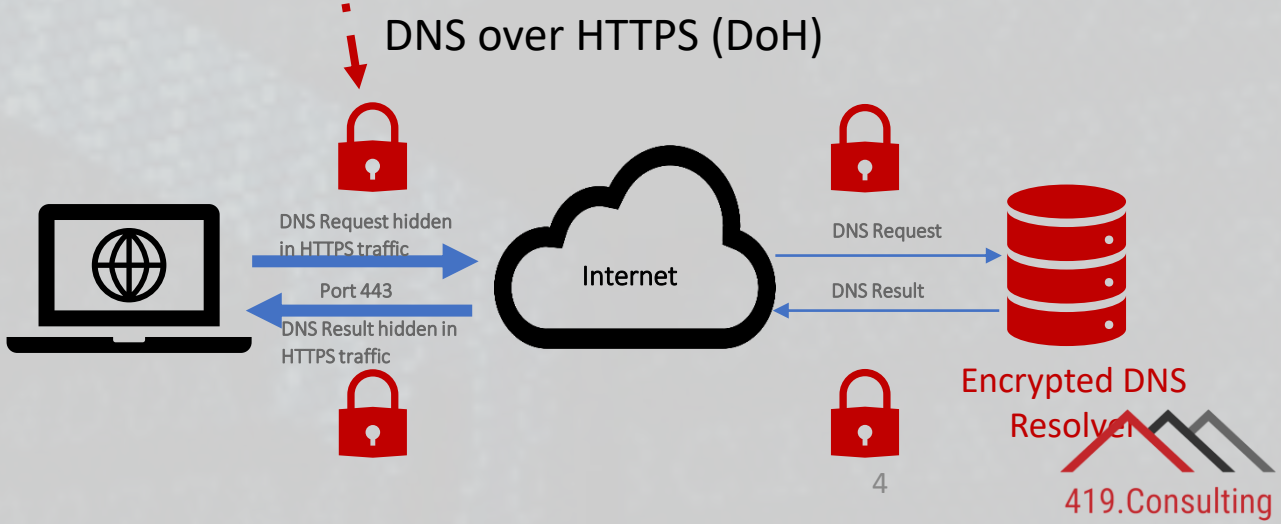
Context – Why Operators Should Care

- Domain Name System – backwater of Internet Standards
- A key control mechanism for some network operators*
  - Parental Controls
  - Malware Filtering
  - Cybersecurity
- Recent changes to standards focused on privacy or application performance
- Rise of cloud-based resolvers, eg Google, Cloudflare, Quad9 etc
- Risk to network operators of loss of visibility and control of network traffic

** Of both public <u>and</u> private networks*

What is (Encrypted) DNS?





- DNS-over-HTTPS is 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
- **The resolver operator still sees all queries**

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 improves protection vs status quo
  - The existing resolver may already be encrypted
  - The "upgrade" option may not provide malware filtering etc
- **Creates policy challenges, for example by over-riding local choices**

Google Chome and Windows 10+

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

Resolver Discovery Standards

- 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, Quad9 and Cloudflare
- DNR suited to ISPs with DNS forwarders – requires upgraded CPE

419.Consulting

Other Developments

- DNS-over-QUIC
  - AdGuard claimed first deployment of DoQ client and resolver
  - DoQ standard is close to being finalised at the IETF
  - **Believed to offer performance benefits over DoH but the resolver operator still has visibility of queries**

- Oblivious DoH
  - Requires two proxies - hides DNS query from first proxy, source IP address of query from the second
  - Experimental, not being progressed as a standard within the IETF – the focus is on Oblivious HTTP instead
  - **Oblivious currently unable to detect colluding proxies so may not offer real privacy**

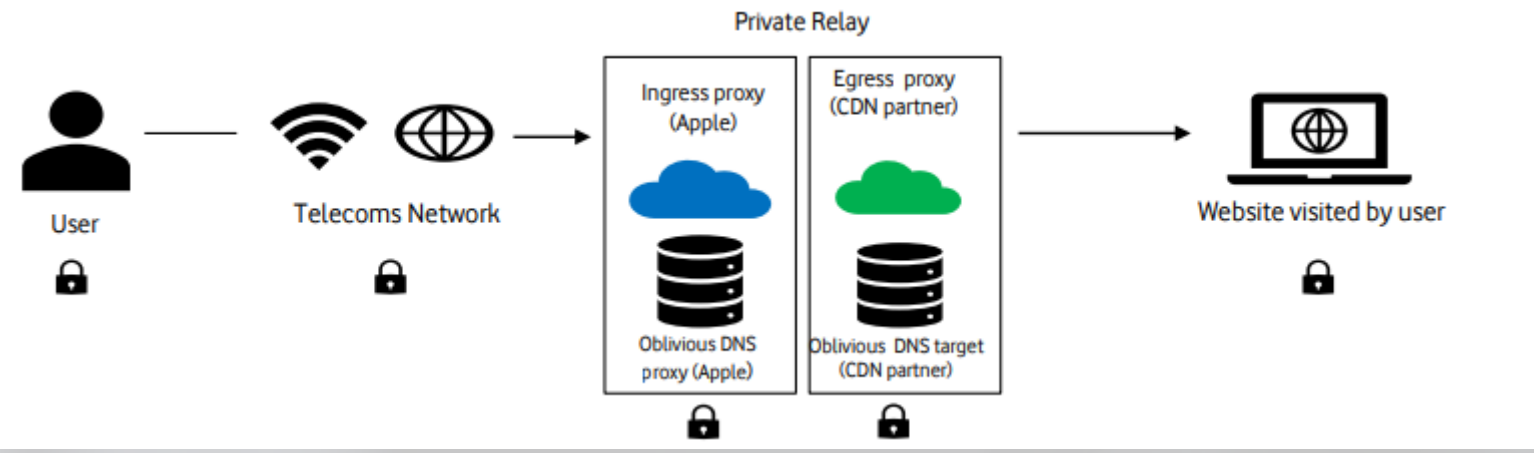
- DoH-over-Tor
  - Slower than other options but with additional privacy benefits
  - Not for the mass market!
  - Presentation outlining the key concept here
  - **Without care, digital fingerprinting may still be possible**

419.Consulting

Private Relay

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

- Traffic is encrypted and sent to an 'ingress' proxy managed by Apple then forwarded to an 'egress' proxy managed by Apple's 3rd party partner.
- The proxy allocates a random IP address to each user so websites cannot track them based on their IP address. The ingress proxy can't see the query, the egress proxy can't see the user's address so neither can see the full details of the request.
- Neither websites, nor Apple, nor the CDN partner can track users based on their IP address



Issues (more details here)

- Operational impacts – QoS, network resilience, network costs, content filtering, zero rating
- Compliance impacts in some markets
- Antitrust considerations – competitive advantage by CDN/proxy partners, centralisation and control, market power

419.Consulting

What Else is Coming?

Encrypted Client Hello (ECH)

- Builds on TLS 1.3 and DoH, encrypts the Server Name Indication (SNI) data
- Early, pre-standard deployments beginning - standard to be finalised in 2022?
- **Issues** (more details here)
  - Can bypass content filtering software
  - Zero-rated traffic will be metered
  - May require use of far more intrusive techniques in environments where SNI could cause problems – eg enterprises, schools etc
  - Cybersecurity issues in private network environments
  - Anti-trust considerations – see the report linked above for details

- User Impacts discussed at IETF 113 in Vienna last month
  - IETF community not interested in the issues raised
  - Since IETF, Google has changed its approach to ECH in Chrome, at least for now (seeking feedback from the community about the impact of ECH, eg on enterprises, home users etc)

Can Technology Alone Solve the Problem of Privacy?

- Technology can go so far but
  - The policy implications of new standards are often ignored
  - Often written with a US market perspective, not all markets are the same
  - The voice of the end-user is often very quiet
  - Network management and cybersecurity may be disrupted
  - New developments may raise centralisation and anti-trust concerns
  - New techniques are often helpful to malware developers too

- Policy Solutions Matter
  - Regulation and legislation needs to keep pace
  - Should also consider the privacy and transparency policies of suppliers

Privacy and Transparency

- What are the issues with current resolver policies?
  - Often written with a US market perspective, lacks a US-wide GDPR equivalent
  - May not make explicit references to applicable legislation and regulations
  - US CLOUD Act, FISA 702
  - Fragmented, often complex and difficult to understand

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 the service operates under

419.Consulting

Additional Information

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

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

- Private Relay
  - 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

- Encrypted Client Hello
  - Paper prepared for IETF 113, details here
  - Presentation material used at IETF 113, details here
  - Q&A about ECH implementation in Chrome, details here
  - Amended approach to EC|H in Chrome following the discussion at IETF 113, details here

419.Consulting

Thank You

Any Questions?

Andrew.Campling@419.Consulting

419.Consulting