Recent developments in DNS and Related protocols

DDI User Group

23rd June 2022

Andrew Campling
Andrew.Campling@419.Consulting

419.Consulting

Agenda

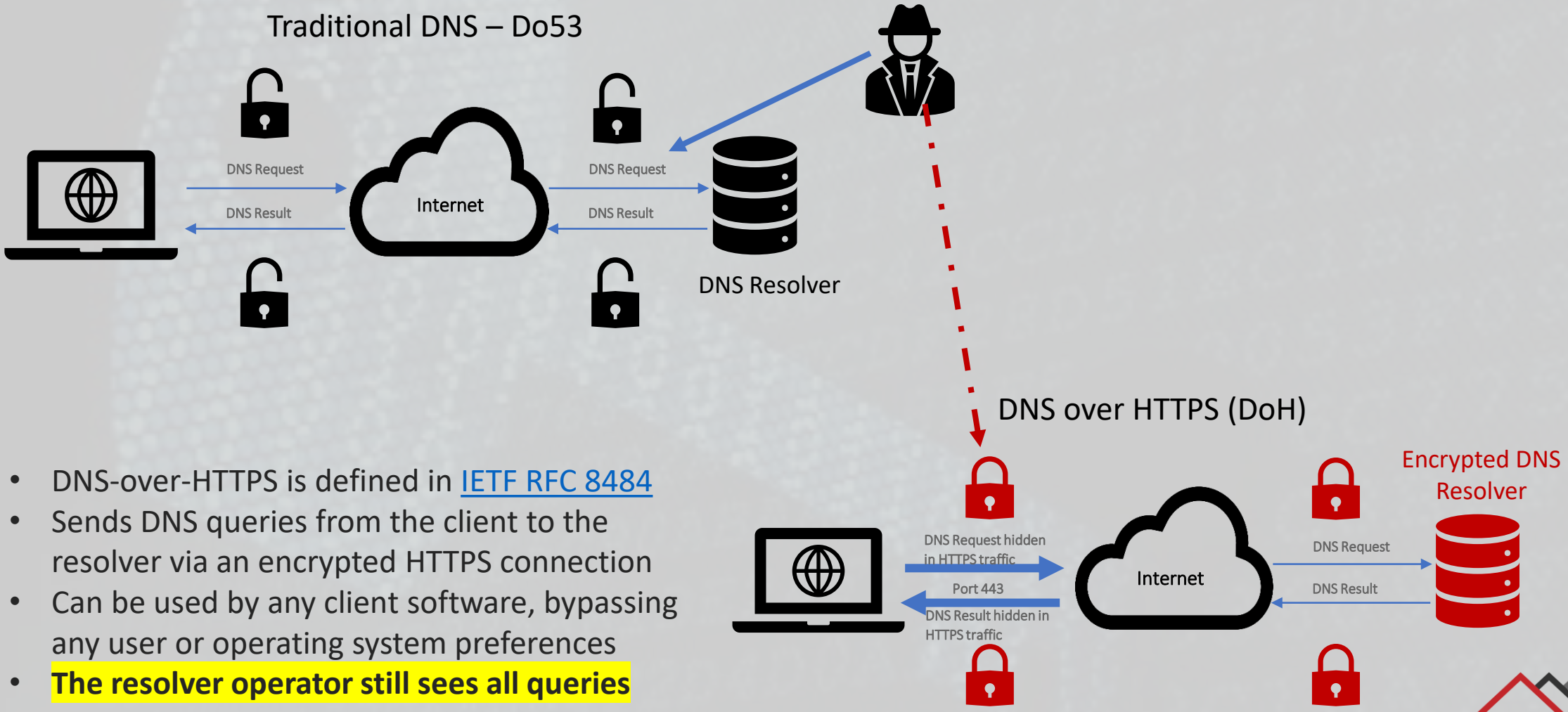
- Context – Why Network Operators, Enterprises, Civil Society Should Care
- Encrypted DNS
  - DNS-over-HTTPS
  - Approaches to Resolver Upgrades
  - Other Developments
- Apple Private Relay
- What Else is Coming?
- Can Technology Alone Solve the Problem?
- Privacy and Transparency
- Additional Information

Context – Why Network Operators, Enterprises, Civil Society Should Care

- Domain Name System – the directory of the Internet
  - A key control mechanism for some network operators*
    - Parental Controls
    - Malware Filtering
    - Cybersecurity
  - Recent changes to standards focused on user privacy or application (particularly browser) performance
- Rise of cloud-based resolvers, eg Google, Cloudflare, Quad9 etc
  - Reduced infrastructure resilience
  - Greater exposure of personal data to mainly US tech companies
  - Antitrust concerns
- Risk to network operators of loss of visibility and control of network traffic

** Both public and 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 the resolver, a problem for many ISP-operated resolvers

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, Cloudflare and Apple (iOS 16 / macOS Ventura)
- DNR suited to ISPs with DNS forwarders

Other DNS Developments

- DNS-over-QUIC
  - AdGuard claimed first deployment of DoQ clients and a resolver
  - DoQ standard just finalised at the IETF
  - **Should 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
  - Marked as an Experimental protocol within the IETF – the focus is currently on Oblivious HTTP
  - **Depending on the implementation, Oblivious may not offer real privacy improvements**

- 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

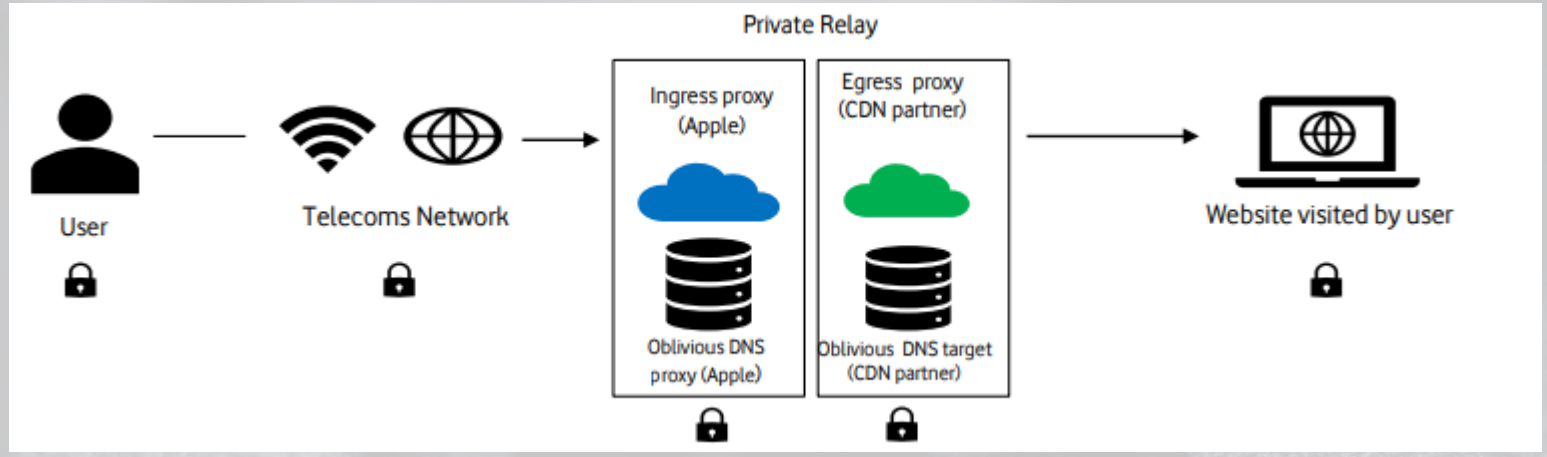
Other DNS Developments

- DNS4EU

  "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."

  - Connecting Europe Facility (CEF2) – European Cloud Federation Initiative
  - 50% of the initial infrastructure investment
  - Call for proposals issued January 2022
  - Submissions currently being evaluated
  - Target to award grant to the winning consortium towards the end of 2022

Apple Private Relay



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

- "Neither websites, nor Apple, nor its CDN partners can track users based on their IP address"
- Users, device owners and network operators can disable private relay

Issues (more details here)

- Users cannot select which proxies to use and the underlying Oblivious protocol is currently unable to detect "colluding proxies", so Private Relay requires user trust that it offers privacy
- 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)

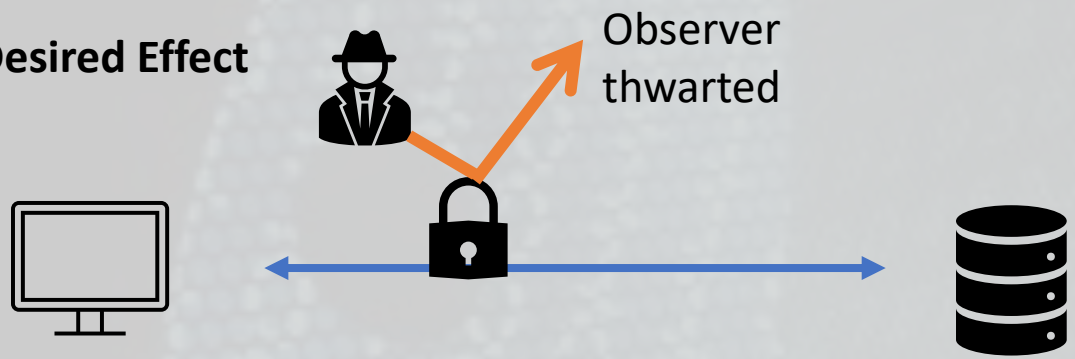
- Builds on TLS 1.3 and DoH, encrypts the Server Name Indication (SNI) data
- Early, pre-standard deployments underway - standard to be finalised in late 2022 or 2023?

- **Issues** (more details here)
  - Can bypass content filtering software (eg in schools, enterprises) - far more intrusive techniques may be needed, impacting privacy
  - Support for BYOD becomes problematic
  - Cybersecurity issues in private network environments – eg loss of another indicator of compromise
  - Zero-rated traffic will be metered – an issue for broadband / mobile users with data caps
  - Anti-trust considerations – see the report linked above for details

- User Impacts discussed at IETF 113 in Vienna in March 2022
  - 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, schools etc)

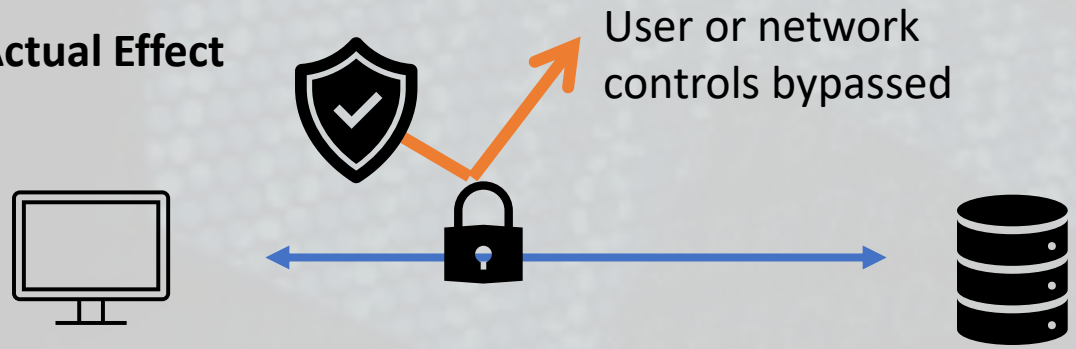
Unintended Consequences for Users, Device Owners and Network Operators

Desired Effect



Communication with target takes place without observation or interference

Actual Effect

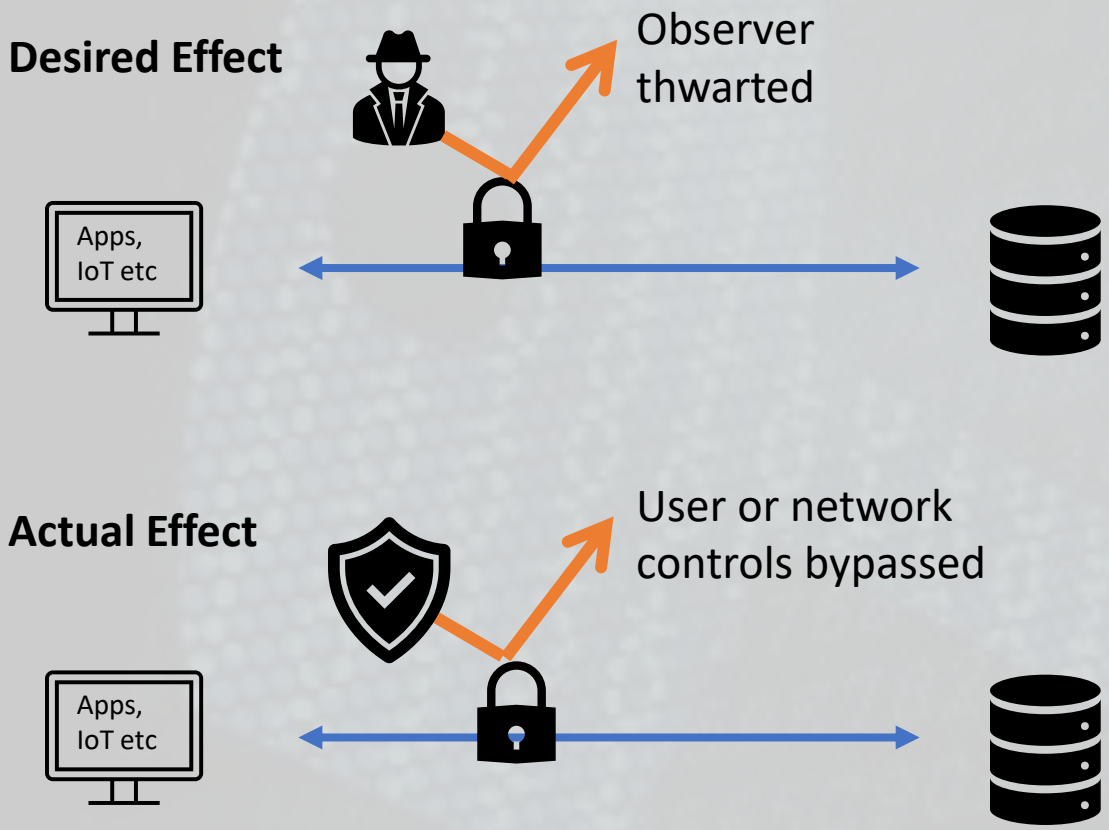


Communication with malicious content
Surveillance by client software
Access to age-inappropriate content
Access to CSAM

NB Better tools exist for dissidents, eg Tor etc

419.Consulting

Unintended Consequences for Users, Device Owners and Network Operators



Applications go dark: communications are hidden from users and networks, become hard to distinguish from malicious traffic

NB Better tools exist for dissidents, eg Tor etc

419.Consulting

Can Technology Alone Solve the Problem of Privacy?

- Technology can take us so far but
  - **The policy and societal 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

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

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 by Google for support for ECH in Chrome following the discussion at IETF 113, details here**

Thank You

Any Questions?

Andrew.Campling@419.Consulting

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