The potential impact of Encrypted Client Hello (ECH) on public and private network operators and others

OARC 39

23rd October 2022

Andrew Campling
Andrew.Campling@419.Consulting

419.Consulting

Introduction

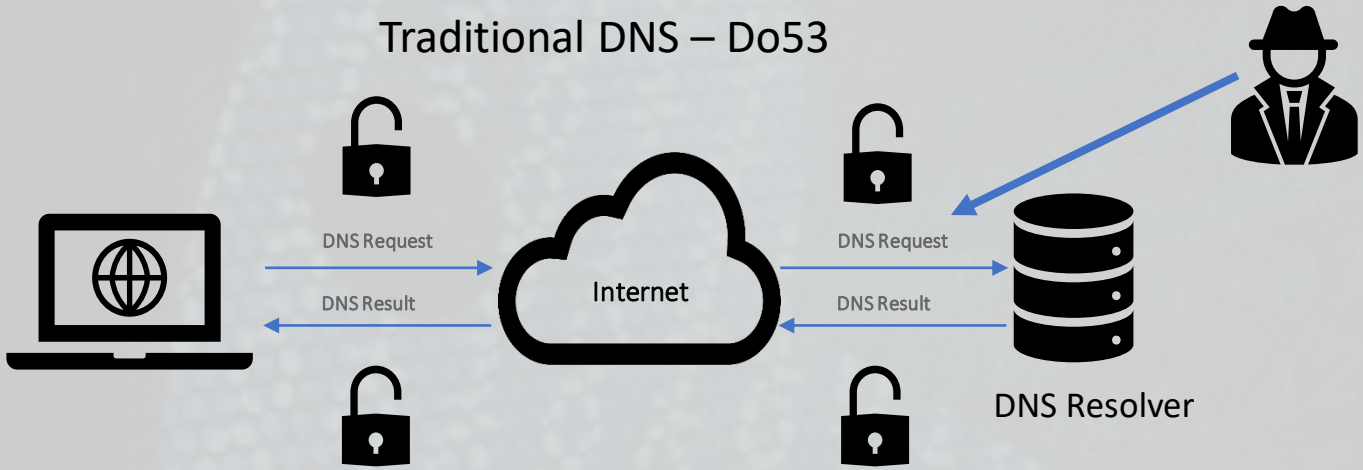
- Encryption is being used to secure all parts of the Internet ecosystem
- Recent developments have covered the Domain Name System (DNS) and related elements
- The input of end-users (and operational security people) is often missing in the development of Internet standards
- The operational impact of encrypted DNS and Encrypted SNI (Encrypted Client Hello or ECH) are often overlooked
- Changes designed to improve privacy may actually weaken both privacy and security

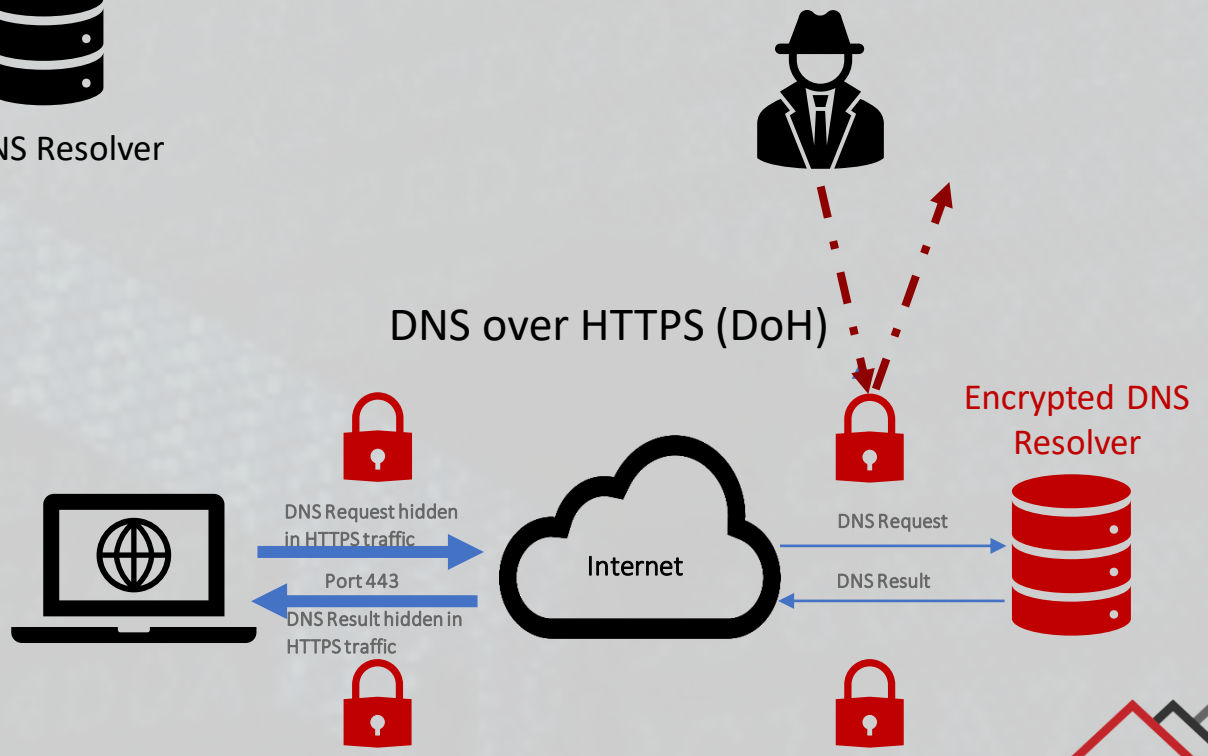
The Domain Name System and Encryption

- 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
  - More user choice, bypass restrictive filtering
  - 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

This Photo by Unknown Author is licensed under CC BY-SA-NC

Approaches to DNS 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 Chrome and Windows 10

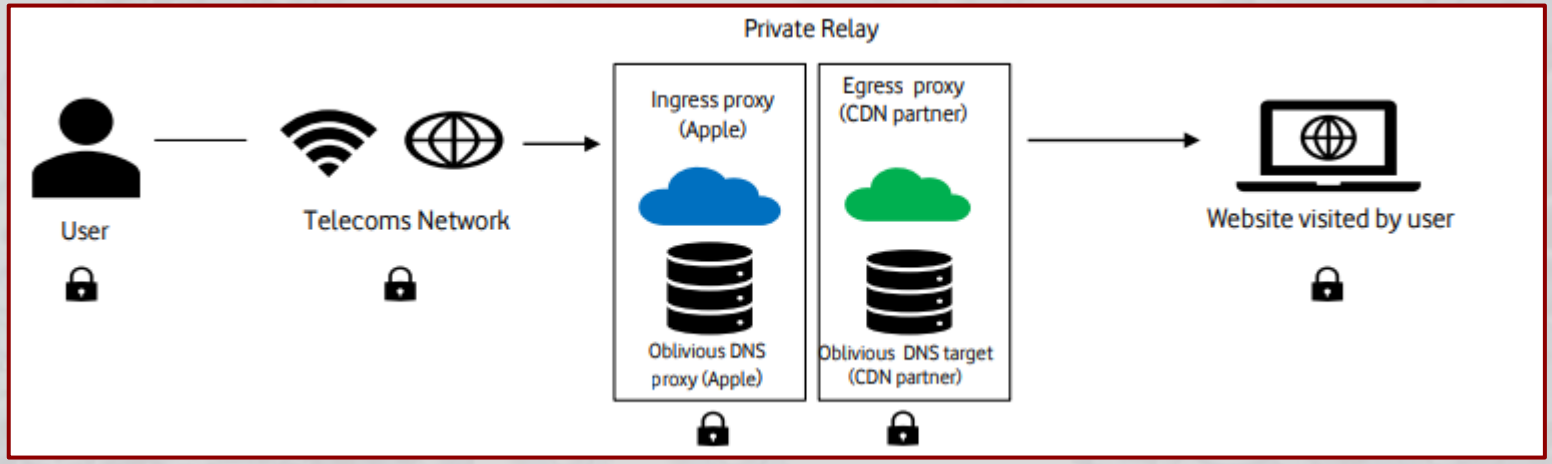
- "Same-Provider, Auto-upgrade"
- Switches to an encrypted option from the same resolver operator, so should carry forward existing policies
- Currently relies on a curated list maintained by the client software provider
- Requires a public IP address for the resolver, a problem for many ISP-operated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

Resolver Discovery Standards

- Options being developed within the IETF (the ADD working group)
  - DDR (discovery of designated resolvers)
  - DNR (discovery of network resolvers)
- Early deployment of DDR by Cisco, Microsoft, Quad9, Cloudflare and Apple (iOS 16 / macOS Ventura)
- DNR suited to ISPs with DNS forwarders (common in Europe)
- Both DDR and DNR are progressing towards ratification as standards

Other Options for Encryption?

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
- Used by Apple within Private Relay
- Depending on the implementation, Oblivious may not offer real privacy improvements

This Photo by Unknown Author is licensed under CC BY-SA

419.Consulting

Do the Encrypted DNS Protocols Ensure DNS Queries are Private?

- Both queries and results may still be visible to the resolver operator (addressed by Oblivious DoH)
- Server Name Indication (SNI) data still leaves details of the domain names that are being accessed in plaintext
- Work currently underway within the standards body to address this
  - Originally Encrypted SNI (eSNI)
  - Now Encrypted Client Hello (ECH)

This Photo by Unknown Author is licensed under CC BY-SA-NC

How is SNI Data Used?

- Schools and businesses – to aid their content filtering policies
- Enterprises – to allow bring your own device (BYOD) policies to be implemented in a relatively light-touch way
- Zero rating of specific content on broadband and mobile networks for users with data caps
- Cybersecurity in enterprises
  - The SNI data can be a very useful so-called “indicator of compromise”
  - It can help to detect unusual behavior on a network that could be caused by, for example, malware

This Photo by Unknown Author is licensed under CC BY

Unintended Consequences of the Encryption of DNS and SNI Data

Desired Effect

Communication with target takes place without observation or interference

Additional Consequences

- 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

This Photo by Unknown Author is licensed under CC BY-SA-NC

What About Zero-Trust?

- Instead of assuming everything behind the corporate firewall is safe, the Zero Trust model verifies each request as though it originates from an open network
  - Recent and current developments make the use of DNS and SNI data to monitor communications to and from applications increasingly difficult
  - Difficult to differentiate the behaviour of benign software from that of malware
- Software that doesn't provide control and visibility to enterprises is likely to be removed
- The motivation for enterprises to act is significant

  US regulators are in the process of levying fines of $200m each on a number of institutions because they were unable to track all communications by their employees because some were encrypted though the use of WhatsApp or Signal
- Consumers will face greater exposure to malware

419.Consulting

This Photo by Unknown Author is licensed under CC BY-SA

Conclusion

- The introduction of encrypted DNS and SNI protocols may benefit privacy in some cases but can also have negative operational impacts
- Insufficient consideration to these impacts is currently being given
- New approaches are being developed without significant input from the various end-user communities, information security practitioners and others that may be affected

This Photo by Unknown Author is licensed under CC BY-NC-ND

Any Questions?

Andrew.Campling@419.Consulting