Developments in Encrypted DNS

DDI User Group
3rd December 2020

Andrew Campling
Andrew.Campling@419.Consulting

419.Consulting

Agenda

- What is Encrypted DNS?
- Client Software Support for Encrypted DNS
  - Firefox (DoH)
  - Chrome (DoH)
  - Apple (DoT and DoH, then DNSSEC and ECH)
  - Windows (DoH)
- The IETF ADD Working Group
  - Options for Resolver Discovery
  - Documenting the ISP Use Case
- Policy Matters
  - Where are policy matters discussed
  - What about formal resolver policies?

Other Developments

- Encrypted Client Hello
- Tools

Additional Information

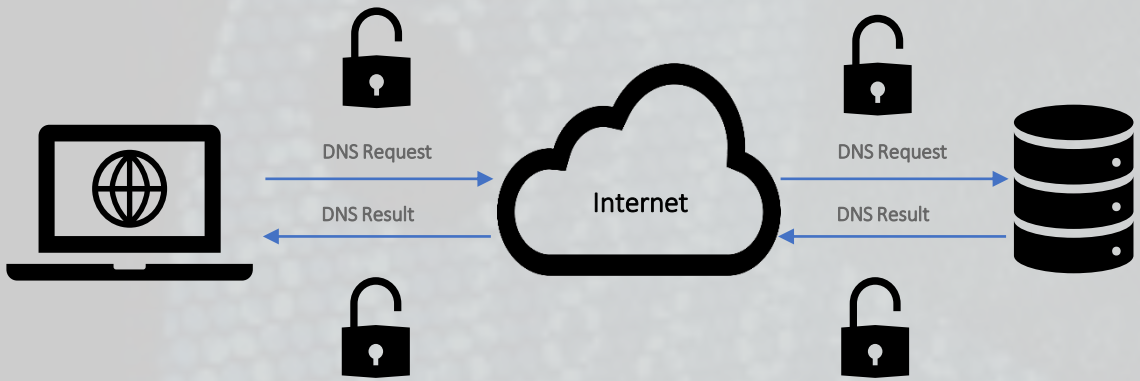
- The Encrypted DNS Deployment Initiative
- Encrypted DNS Weekly Call

Background

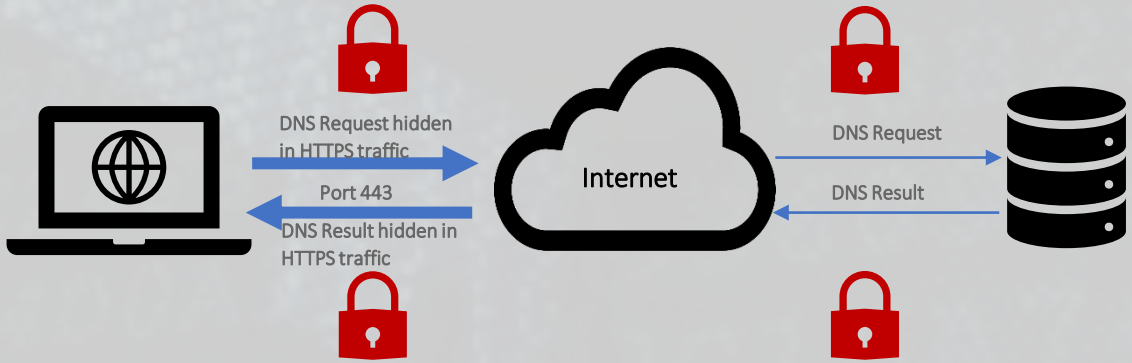
- Pressure to Encrypt DNS
  - Part of a drive to end-to-end encryption
  - Allegations of abuse of DNS data
- DoT Adoption Static
- Drive to Allow Applications to Access the DNS Directly
- DNS over HTTPS (DoH) Standard Ratified by the IETF
  - October 2018, RFC 8484
  - Just a protocol, no specification to discover or select DoH resolvers
  - Protects DNS queries from being monitored by third parties
  - But can impact blocking of illegal content, filtering of malicious content, parental controls, CDNs, split-horizon DNS etc

What is Encrypted DNS?

Traditional DNS – Do53



Encrypted DNS – DoH



Client Software Support for Encrypted DNS

- Firefox (DoH)
  - First major browser to support DoH
  - Implemented by default in the US (Cloudflare then NextDNS, now Comcast too)

- Chrome (DoH)
  - Support from mid May 2020
  - Auto-upgrade facility – doesn't currently work well with the resolvers of many European ISPs*
- Apple (DoT and DoH, DNSSEC and ECH to follow)
  - Added in IoS / iPadOS 14 and MacOS Big Sur – first announced at WWDC 2020
  - Configuration options for enterprises, individuals and applications
- Windows 10 (DoH)
  - Support in beta (Windows Insider programme)
  - Auto-upgrade facility – doesn't currently work well with the resolvers of many European ISPs*
  - Full release first half 2021?

* See https://datatracker.ietf.org/meeting/108/materials/slides-108-add-practical-observations-from-encrypted-dns-deployments-by-network-operators-00 and https://datatracker.ietf.org/doc/draft-campling-operator-observations/

419.Consulting

The IETF ADD Working Group

- Adaptive DNS Discovery Working Group
  - Formed February 2020
  - “This working group will focus on discovery and selection of DNS resolvers by DNS clients in a variety of networking environments, including public networks, private networks, and VPNs, supporting both encrypted and unencrypted resolvers.”
  - Recent discussions have been focused on agreeing use cases and associated requirements
  - Use cases are likely to be formally adopted by the working group shortly
  - Proposals expected by IETF 110 (early March 2021) covering at least two use cases

Where are Policy Matters Discussed?

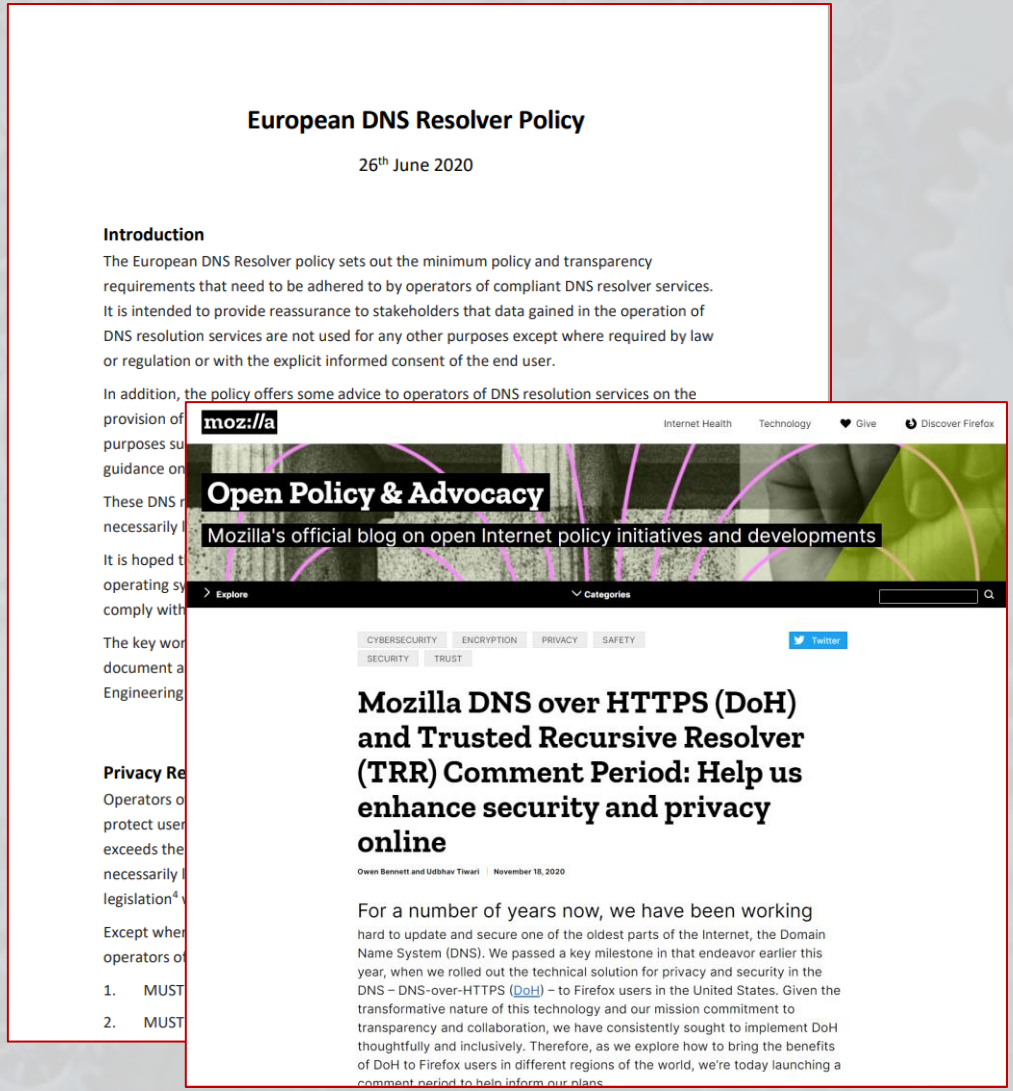
- Not in the ADD Working Group
  - [The ADD Working Group] "…is chartered solely to develop technical mechanisms. **Making any recommendations about specific policies for clients or servers is out of scope**."
- Related IETF Policy Documents
  - RFC 8932 – Recommendations for DNS Privacy Service Operators
  - RFC 8890 – The Internet is for End Users
- Outside The IETF
  - The Internet Governance Forum
  - The EC's High-Level Group on Internet Governance
  - Encrypted DNS Deployment Initiative (EDDI)

Encrypted DNS Deployment Initiative

419.Consulting

Resolver Policy

- Mozilla Trusted Recursive Resolver Programme Consultation
  - Intention to extend outside North America
  - Consultation closes 4th January 2021
- European Resolver Policy
  - Developed with the industry and key stakeholders
  - To be launched shortly



European DNS Resolver Policy

26th June 2020

Introduction

The European DNS Resolver policy sets out the minimum policy and transparency requirements that need to be adhered to by operators of compliant DNS resolver services. It is intended to provide reassurance to stakeholders that data gained in the operation of DNS resolution services are not used for any other purposes except where required by law or regulation or with the explicit informed consent of the end user.

In addition, the policy offers some advice to operators of DNS resolution services on the

moz://a

Internet Health Technology Give Discover Firefox

Open Policy & Advocacy

Mozilla's official blog on open Internet policy initiatives and developments

Explore Categories

CYBERSECURITY ENCRYPTION PRIVACY SAFETY SECURITY TRUST

Twitter

Mozilla DNS over HTTPS (DoH) and Trusted Recursive Resolver (TRR) Comment Period: Help us enhance security and privacy online

Owen Bennett and Udbhav Tiwari | November 18, 2020

For a number of years now, we have been working hard to update and secure one of the oldest parts of the Internet, the Domain Name System (DNS). We passed a key milestone in that endeavor earlier this year, when we rolled out the technical solution for privacy and security in the DNS – DNS-over-HTTPS (DoH) – to Firefox users in the United States. Given the transformative nature of this technology and our mission commitment to transparency and collaboration, we have consistently sought to implement DoH thoughtfully and inclusively. Therefore, as we explore how to bring the benefits of DoH to Firefox users in different regions of the world, we're today launching a comment period to help inform our plans

https://blog.mozilla.org/netpolicy/2020/11/18/doh-comment-period-2020/

https://blog.mozilla.org/netpolicy/files/2020/11/DoH-Public-Comment-Period-Question-for-Comment.pdf.pdf

419.Consulting

Other Developments

- Encrypted Client Hello (ECH)
  - New protocol to encrypt the Server Name Indication (SNI) data
  - Currently being developed by the IETF's TLS working group
  - Still in draft, interoperability testing likely to start in 2021
  - Google will commence prototyping ECH in Chrome next quarter

- Tools
  - Some work has been undertaken to detect DoH data streams without decryption
  - This is now achieving high success rates (< 5% false positives)

Additional Information

- The IETF ADD Working Group
  - An interim working group session is likely to be held in late January or early February 2021
  - Further working group sessions will be included in IETF 110, 6-12th March 2021
  - Associated mailing list - https://mailarchive.ietf.org/arch/browse/add/

- The Encrypted DNS Deployment Initiative
  - Free to join – see https://www.encrypted-dns.org/
  - Associated mailing list - https://www.encrypted-dns.org/mailing-list
  - Work streams documented on GitHub - https://github.com/Encrypted-DNS-Deployment-Initiative

- Encrypted DNS Weekly Call
  - Every Monday at 4:00pm UK (currently 4:00pm UTC)
  - Free to join – email Andrew.Campling@419.Consulting
  - Apple support for Encrypted DNS - https://419.consulting/encrypted-dns/f/apple-on-encrypted-dns
  - DNS, DoH and GDPR - https://419.consulting/encrypted-dns/f/gdpr-and-its-application-to-dns
  - Prototyping ECH in Chrome – https://419.consulting/encrypted-dns/f/proto-typing-encrypted-client-hello-in-the-chrome-browser
  - Detecting DoH in the Wild - https://419.consulting/encrypted-dns/f/detecting-dns-over-https-traffic

Any Questions?

Andrew.Campling@419.Consulting

419.Consulting