Developments in Encrypted DNS: Implications for the Internet Ecosystem

Andrew Campling, 419 Consulting

2nd July 2020

419.Consulting

Agenda

- Background
- Client Software Support for Encrypted DNS
  - Firefox (DoH)
  - Chrome (DoH)
  - Windows (DoH)
  - Apple (DoT and DoH, then DNSSEC and ECH)
- The IETF ADD Working Group
  - Options for Resolver Discovery
  - Documenting the ISP Use Case
  - What About Policy Matters?
- Other Developments
  - What About ISPs?
  - What About Resolver Policy?
  - What Else is Changing?
- Additional Information
  - The Encrypted DNS Deployment Initiative
  - Encrypted DNS Weekly Call

Background

- Pressure to encrypt DNS
  - Allegations of abuse of DNS data
- DoT adoption static
- Drive to allow applications to access the DNS directly
- DNS over HTTPS standard ratified by the IETF
  - October 2018, RFC 8484
  - Just a protocol, no specification to discover or select DoH resolvers
  - Can impact illegal content blocking, malicious content filtering, parental controls, CDNs, split-horizon DNS etc

Client Software Support for Encrypted DNS

- Firefox (DoH)
  - First major browser to support DoH
  - Implemented by default in the US (Cloudflare and NextDNS)
- Chrome (DoH)
  - Support from mid May 2020
  - Auto-upgrade facility
- Windows (DoH)
  - Support in beta (Windows Insider programme)
  - Auto-upgrade facility
- Apple (DoT and DoH, DNSSEC and ECH to follow)
  - IoS and MacOS - announced at WWDC 2020, full release later 2020?
  - Configuration options for enterprises, individuals and applications

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.”
  - Current papers focus on options for resolver discovery
  - Not all methods proposed reflect the way that the Internet ecosystem functions, especially outside the US

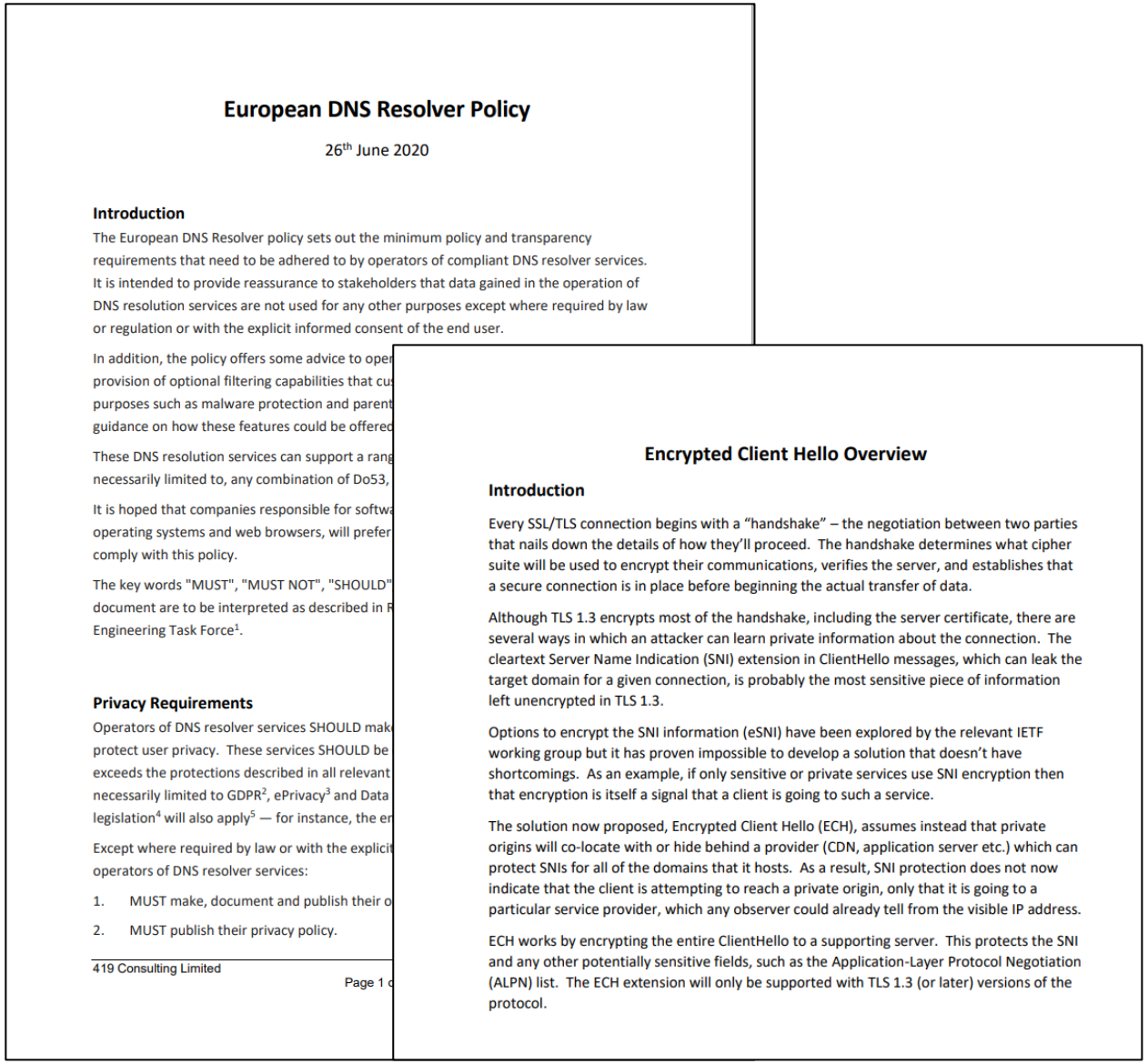
The IETF ADD Working Group

- What About Policy Matters?
  - [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**."
  - Is this important?
  - If Not The IETF Then Where?
    - The Internet Governance Forum
    - The EC's High-Level Group on Internet Governance
    - Encrypted DNS Deployment Initiative

419.Consulting

Other Developments

- What About ISPs?
  - Comcast (US) – DoH, Firefox
  - Deutsche Telekom
  - BT Group
- What About Resolver Policy?
  - Mozilla Trusted Recursive Resolver Programme
  - European Resolver Policy
- What Else is Changing?
  - Encrypted Client Hello (ECH)



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 oper
provision of optional filtering capabilities that cu
purposes such as malware protection and parent
guidance on how these features could be offered

These DNS resolution services can support a rang
necessarily limited to, any combination of Do53,

It is hoped that companies responsible for softwa
operating systems and web browsers, will prefer
comply with this policy.

The key words "MUST", "MUST NOT", "SHOULD"
document are to be interpreted as described in R
Engineering Task Force[1].

Privacy Requirements

Operators of DNS resolver services SHOULD mak
protect user privacy. These services SHOULD be
exceeds the protections described in all relevant
necessarily limited to GDPR[2], ePrivacy[3] and Data
legislation[4] will also apply[5] — for instance, the er

Except where required by law or with the explicit
operators of DNS resolver services:

1. MUST make, document and publish their o
2. MUST publish their privacy policy.

419 Consulting Limited

Page 1 o

Encrypted Client Hello Overview

Introduction

Every SSL/TLS connection begins with a "handshake" – the negotiation between two parties that nails down the details of how they'll proceed. The handshake determines what cipher suite will be used to encrypt their communications, verifies the server, and establishes that a secure connection is in place before beginning the actual transfer of data.

Although TLS 1.3 encrypts most of the handshake, including the server certificate, there are several ways in which an attacker can learn private information about the connection. The cleartext Server Name Indication (SNI) extension in ClientHello messages, which can leak the target domain for a given connection, is probably the most sensitive piece of information left unencrypted in TLS 1.3.

Options to encrypt the SNI information (eSNI) have been explored by the relevant IETF working group but it has proven impossible to develop a solution that doesn't have shortcomings. As an example, if only sensitive or private services use SNI encryption then that encryption is itself a signal that a client is going to such a service.

The solution now proposed, Encrypted Client Hello (ECH), assumes instead that private origins will co-locate with or hide behind a provider (CDN, application server etc.) which can protect SNIs for all of the domains that it hosts. As a result, SNI protection does not now indicate that the client is attempting to reach a private origin, only that it is going to a particular service provider, which any observer could already tell from the visible IP address.

ECH works by encrypting the entire ClientHello to a supporting server. This protects the SNI and any other potentially sensitive fields, such as the Application-Layer Protocol Negotiation (ALPN) list. The ECH extension will only be supported with TLS 1.3 (or later) versions of the protocol.

419.Consulting

Additional Information

- The IETF ADD Working Group
  - On the preliminary agenda for IETF 108 (27th – 31st July – ADD 14:10-15:50, 30th July)
  - 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

Any Questions?

Andrew.Campling@419.Consulting

419.Consulting