NPOC Webinar Series #6

Encrypted DNS

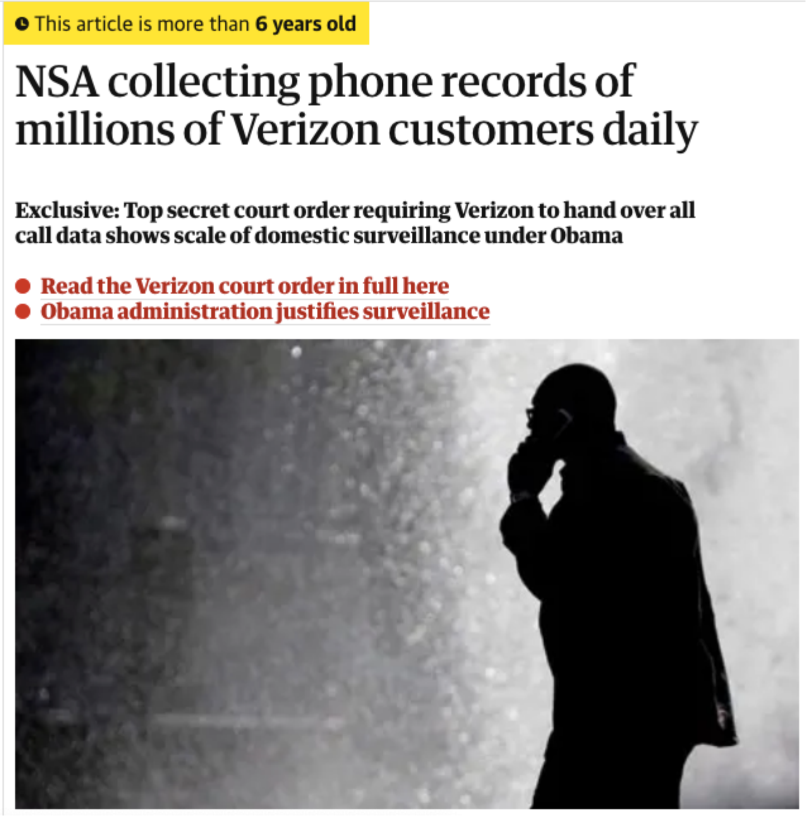
Patrick Jones, Senior Director, Global Stakeholder Engagement
David Huberman, Office of the CTO

7 April 2021

ICANN

DNS Privacy

June 2013



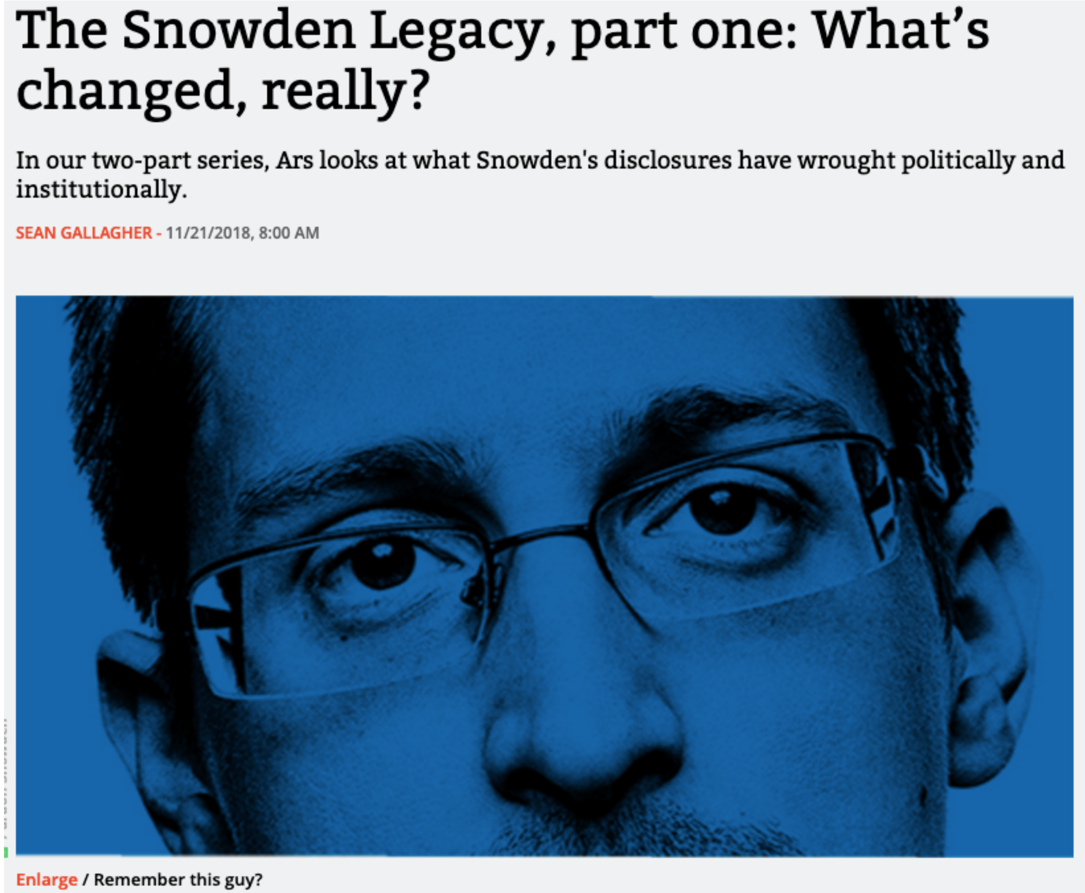
This article is more than **6 years old**

NSA collecting phone records of millions of Verizon customers daily

Exclusive: Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama

- **Read the Verizon court order in full here**
- **Obama administration justifies surveillance**

Snowden



The Snowden Legacy, part one: What’s changed, really?

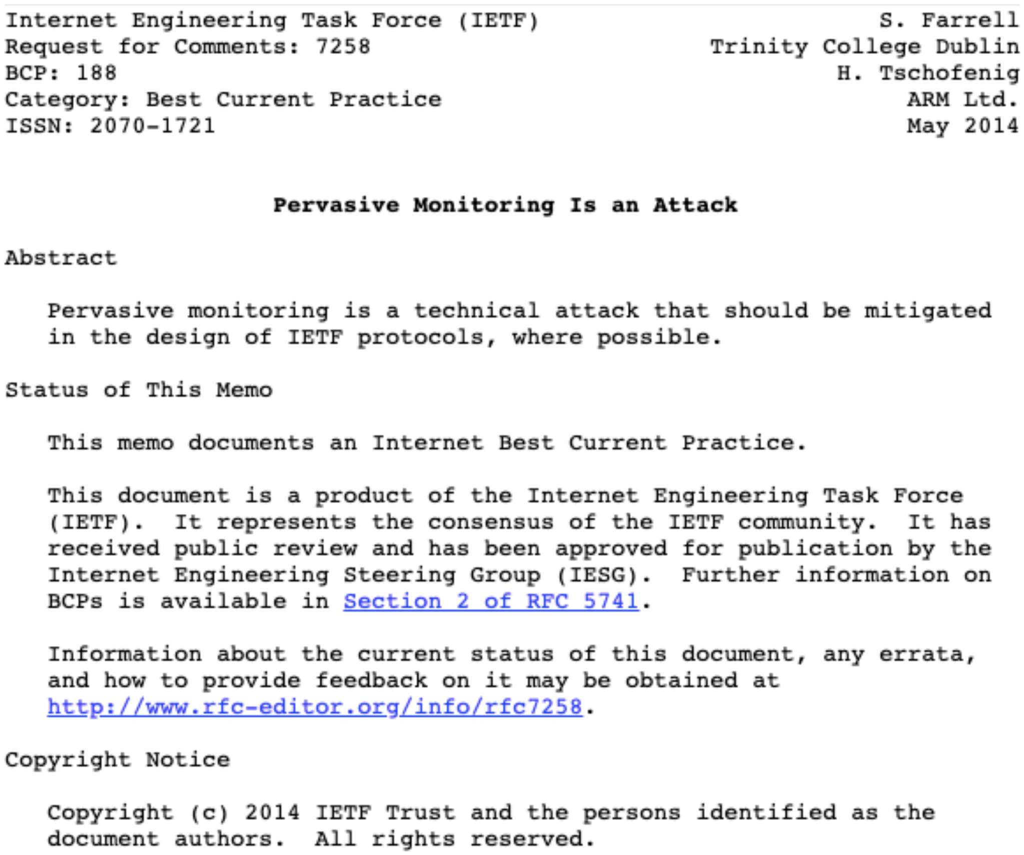
In our two-part series, Ars looks at what Snowden's disclosures have wrought politically and institutionally.

SEAN GALLAGHER - 11/21/2018, 8:00 AM

Enlarge / Remember this guy?

(ARS Technica, Nov 2018, https://arstechnica.com/tech-policy/2018/11/the-snowden-legacy-part-one-whats-changed-really/)

Technical Community Response



```
Internet Engineering Task Force (IETF)                        S. Farrell
Request for Comments: 7258                      Trinity College Dublin
BCP: 188                                                 H. Tschofenig
Category: Best Current Practice                              ARM Ltd.
ISSN: 2070-1721                                               May 2014
```

Pervasive Monitoring Is an Attack

Abstract

Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible.

Status of This Memo

This memo documents an Internet Best Current Practice.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on BCPs is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7258.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

(IETF BCP 188, https://tools.ietf.org/html/bcp188)

RFC 7258/BCP 188 – Pervasive Monitoring is an Attack

- IETF community’s technical assessment is that PM is an attack on the privacy of Internet users and organizations
  - Discussed at IETF Technical Plenary in 2013
  - Published as BCP in May 2014
  - Led to DPRIVE Working Group; development of DoT, DoH

Montevideo Statement (7 Oct 2013)

- Leaders of organizations responsible for coordination of Internet technical infrastructure met in Montevideo, Uruguay

- “expressed strong concern over the undermining of trust and confidence of Internet users globally due to recent revelations of pervasive monitoring and surveillance.”

- Called for accelerating the globalization of ICANN and the IANA functions, towards an environment in which all stakeholders, including all governments, participate on an equal footing.

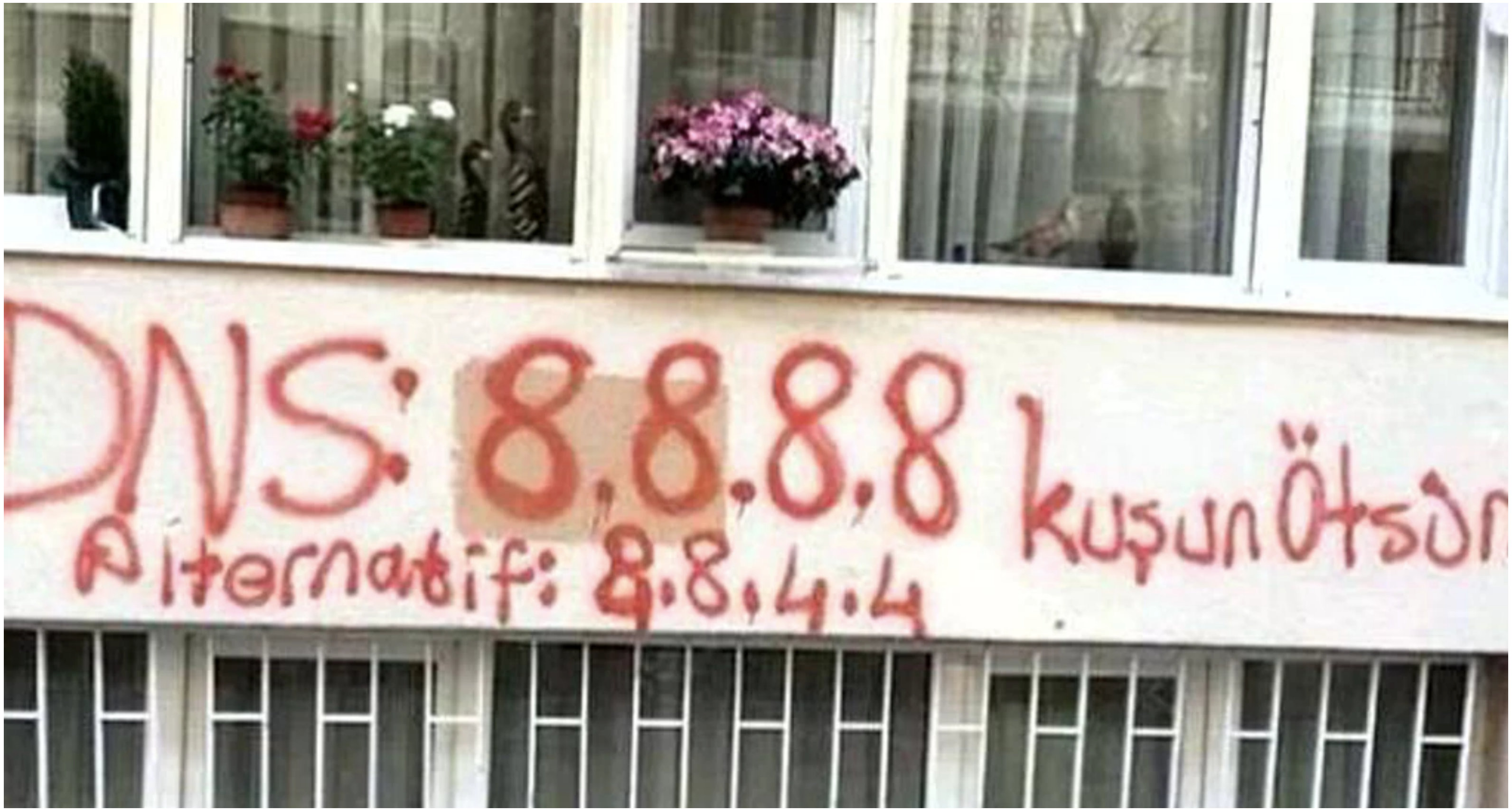
Government Responses

- **Data protection is a fundamental right in Europe**
- **European General Data Protection Regulation –** adopted in 2016, implemented in 2018.
- **Privacy legislation in Brazil, Canada, China, Japan, Singapore, among others**

Business & Consumer Responses

- Incorporation of encryption into key platforms (iOS)
- Wider use of secure messaging applications
- Increase use of Virtual Private Networks

Use of Public DNS



(https://www.mic.com/articles/85987/turkish-protesters-are-spray-painting-8-8-8-8-and-8-8-4-4-on-walls-here-s-what-it-means)

DNS Privacy Motivations

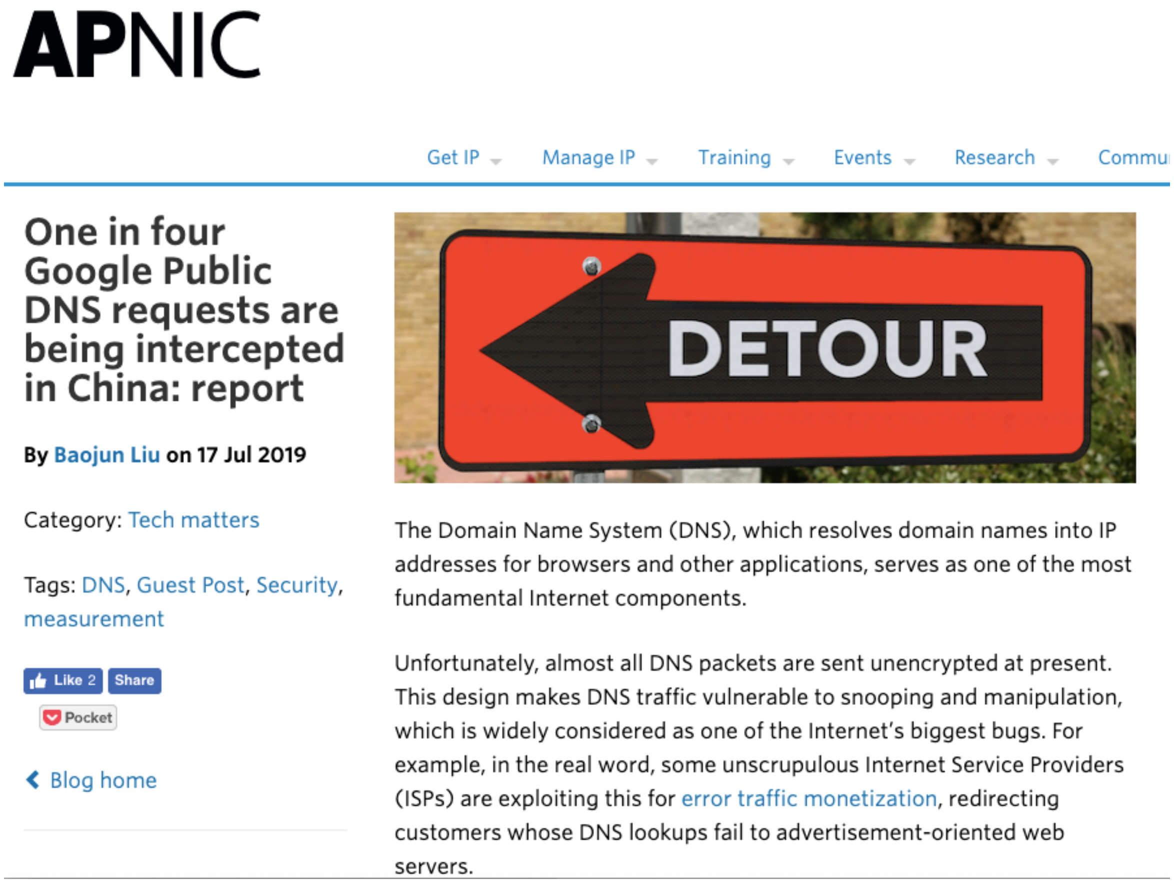
End User - Primarily HTTPS web browsing

ISP – Observing & controlling DNS resolution for customers (may be obligated by local laws to perform certain monitoring/censorship)

Enterprise – Management of corporate/university/employer network; employee risk & protections. May enforce use of VPN or control user devices. Prevention of corporate-internal networks from leaking.

Browser – Application acting on behalf of user; interface using the DNS to retrieve information for user

Use of Public DNS



One in four Google Public DNS requests are being intercepted in China: report

By Baojun Liu on 17 Jul 2019

Category: Tech matters

Tags: DNS, Guest Post, Security, measurement

Like 2 Share

Pocket

‹ Blog home

The Domain Name System (DNS), which resolves domain names into IP addresses for browsers and other applications, serves as one of the most fundamental Internet components.

Unfortunately, almost all DNS packets are sent unencrypted at present. This design makes DNS traffic vulnerable to snooping and manipulation, which is widely considered as one of the Internet's biggest bugs. For example, in the real word, some unscrupulous Internet Service Providers (ISPs) are exploiting this for error traffic monetization, redirecting customers whose DNS lookups fail to advertisement-oriented web servers.

(Source: APNIC Blog, 17 July 2019)

Use of Public DNS

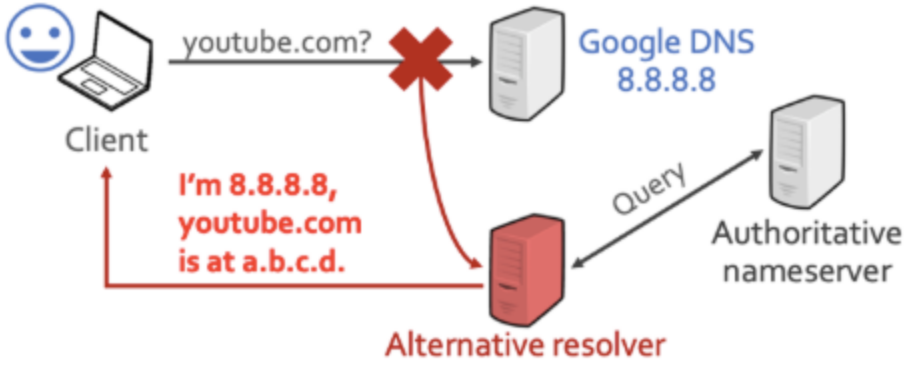


Figure 1 — Google DNS traffic can be intercepted via middleboxes.

(Source: APNIC Blog, 17 July 2019)

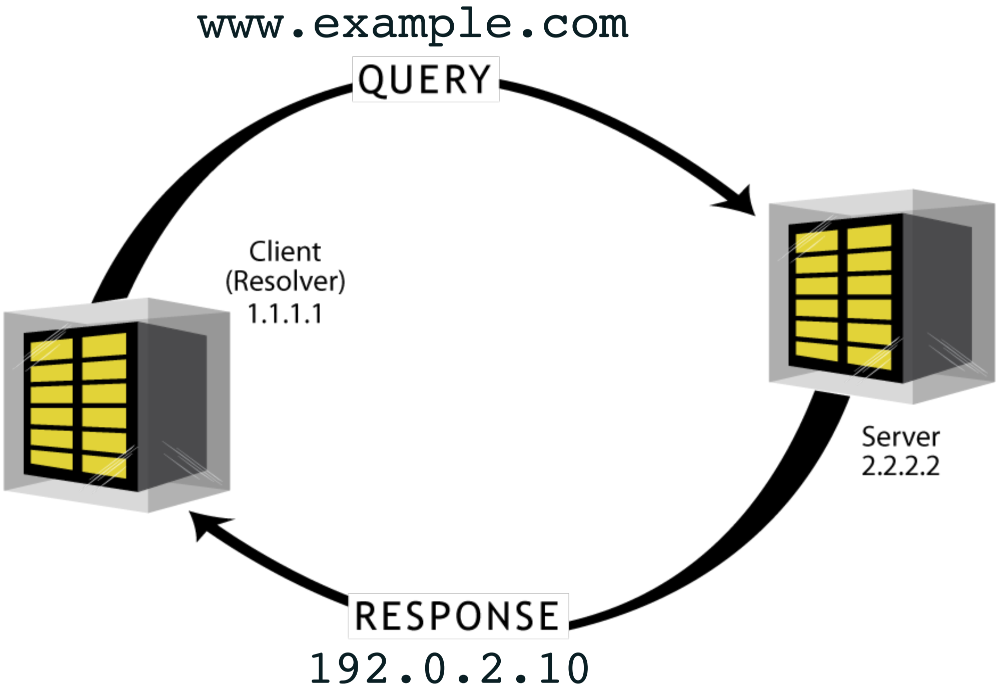
DNS Privacy: Fundamentals

Three Topics

- QNAME Minimization
- DNS-over-TLS (DoT)
- DNS-over-HTTPS (DoH)

Level Setting

- Classic DNS (by far the most used protocol today) sends messages in clear text



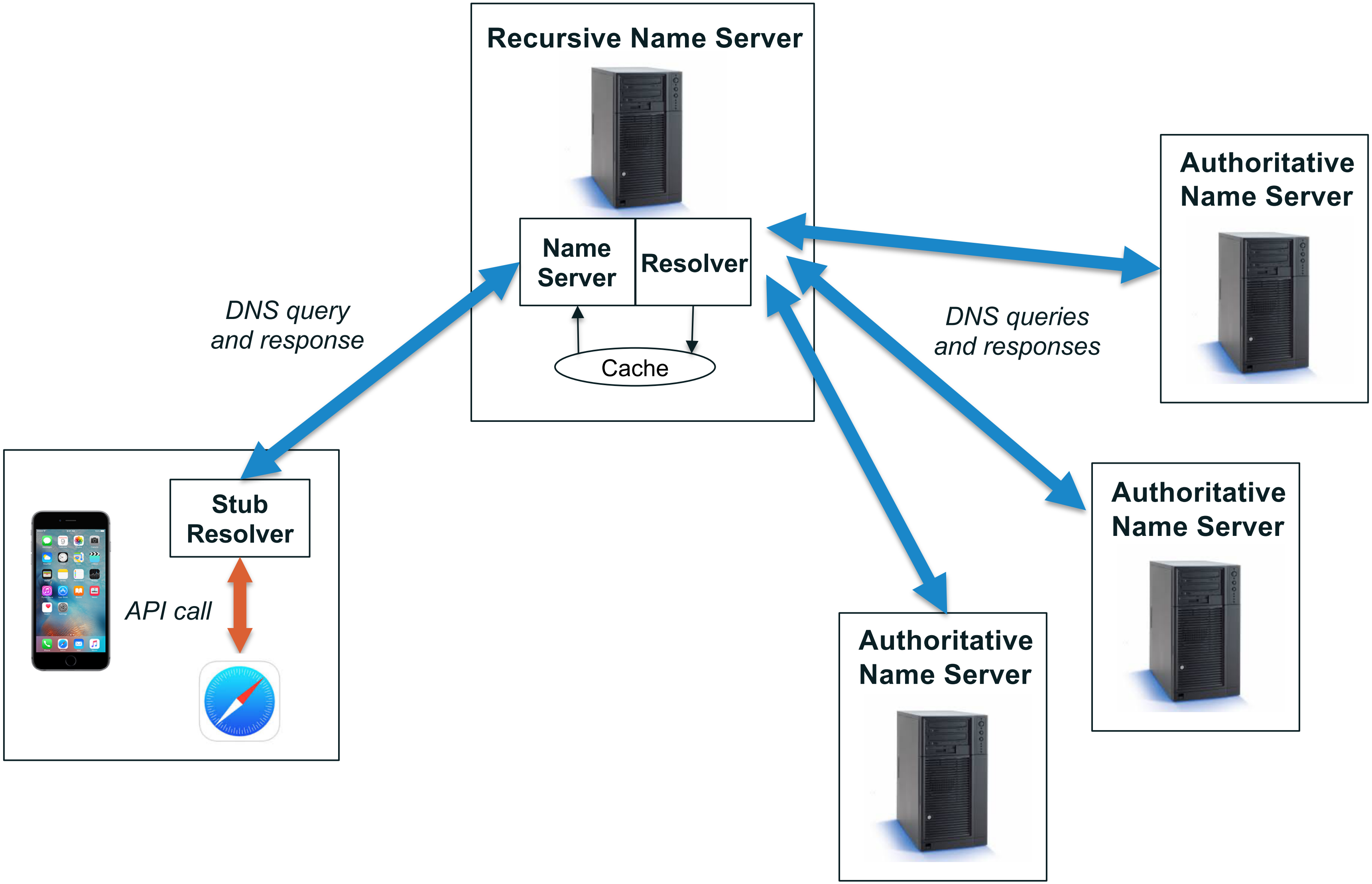
Level Setting

- Three types of resolvers:
  - Stub resolver: on the user's device
  - Recursive resolver: goes and obtains answers to questions
  - Authoritative name server: contains the answer to a specific question

- Each DNS question is broken up into constituent parts:

```
www.example.com.
```

DNS Resolution for www.example.com



QNAME Minimization

- Break up the message into constituent parts
- Only ask each authoritative name server about the specific part it knows about
  - Root only gets the query for .com
  - The .com authoritative server only gets the query for example.com
  - The example.com authoritative server gets the entire query
- The whole point is that the servers “upstream” of the destination do not get to know what you’re really querying for
  - Roots don’t get to know about example.com
  - .com doesn’t get to know about www.example.com

QNAME Minimization

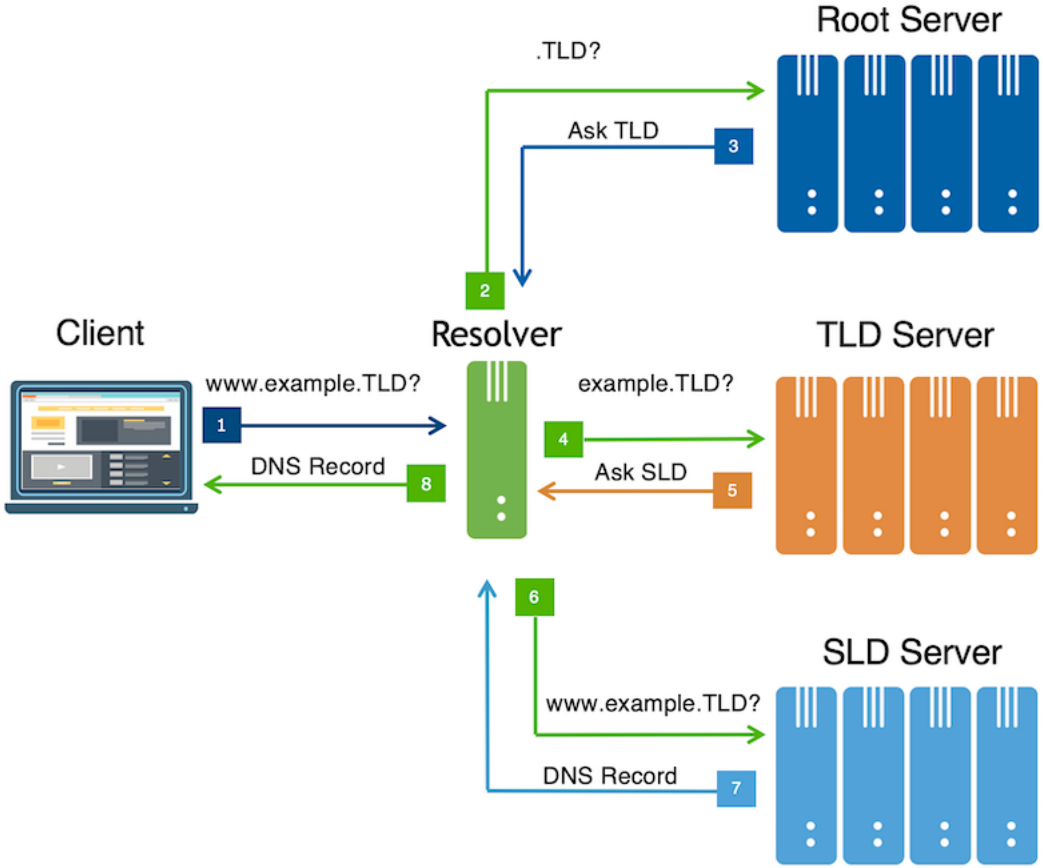


Image from a Verisign blog post on QNAME Minimization's benefits

QNAME Minimization

- QNAME Minimization is not a controversial technique:
  - Nobody has argued it is in any way “bad”
  - It does an “ok” job of increasing query privacy for end users
  - But the DNS data traffic is still sent in clear text, so anyone listening on the wire immediately upstream of the resolver can see all the DNS data

- QNAME Minimization is starting to become widely deployed:
  - Or at least, we suspect so
  - We have begun measuring this as part of ICANN’s Identifier Technology Health Indicators (ITHI) project
  - In March 2021, **34.4%** of all queries to root servers that we measured used QNAME minimization!

DNS-over-TLS (DoT)

- DoT is configured in your operating system
  - Very widely implemented in Android OS
- When an application requests a DNS lookup, the information is *encrypted* and sent to a DoT server for resolution
- Nobody listening to DNS traffic (passively or actively) can “see” the DoT traffic. User queries are assured of confidentiality by way of encrypted text.

DNS-over-HTTPS (DoH)

- DoH is for applications which transmit information via HTTPS (secure HTTP = encrypted)

- In the real world, this primarily means the web browsers (Firefox, Chrome, etc.)

- Instead of using the normal DNS resolution process described earlier, which relies on the stub resolver of a device, the application operator would rather incorporate DNS resolution into the stream of HTTPS traffic the browser is accustomed to exchanging

- Nobody listening to DNS traffic (passively or actively) can “see” the DoH traffic. User queries are assured of confidentiality by way of the queries being inside HTTPS packets intermingled with regular web traffic.

- Relies on pre-configured DoH resolvers run by third parties that users may not know about

General Concerns About Encrypted DNS

- There are no policy concerns (yet?) about QNAME minimization
- DoH and DoT and similar technologies, however, have raised eyebrows in the technical community and in governments

General Concerns About Encrypted DNS

Circumvention of DNS filtering for security purposes

- Networks put filters in place to protect users and protect the network:
  - Websites that install malware
  - Email servers that only send malware
  - Communications with malware servers after being infected
  - Exfiltration of sensitive data

- DoH and DoT circumvent these filters because the traffic is encrypted. The DNS data is not available to the filtering software. It can’t “see it”.

General Concerns About Encrypted DNS

Circumvention of DNS filtering for local policy

- Networks put filters in place to adhere to local policy:
  - Preventing users from seeing particular content (e.g., hate material or words or sites the local government has forbidden)
  - Reducing the chance of unauthorized websites tracking users
  - Enforcing limits on the use of some sites to particular hours
- DoH and DoT circumvent these filters because the traffic is encrypted. The DNS data is not available to the filtering software. It can't "see it".

Increased DNS Privacy is Good

- Technology that increases DNS privacy is good; it works towards a goal that benefits our world
- Governments that want to increase privacy for end users could do so by asking DNS operators to implement DoH, QNAME Minimization, and similar technologies
- Government that want to increase privacy for end users could do so by requiring that operating systems use DoT
- This has an interesting side benefit:
    - End users who want increased privacy for their services would not have to go outside the country anymore for that (e.g. Google’s 8.8.8.8)

Event Announcement

2021 ICANN DNS Symposium

- 25-27 May 2021, +2 UTC time zone (CEST)
- This is a virtual event
- Theme: ”DNS Ecosystem Security: We’re all in this together”
- Talks on measurements, mitigations, and progress on community work
- Registration is free and open now!

Engage with ICANN

ICANN

Thank You and Questions

Visit us at **icann.org**
Email: email

- @icann
- facebook.com/icannorg
- youtube.com/icannnews
- flickr.com/icann
- linkedin/company/icann
- soundcloud/icann
- instagram.com/icannorg