An End-to-End, Large-Scale Measurement of DNS-over-Encryption:

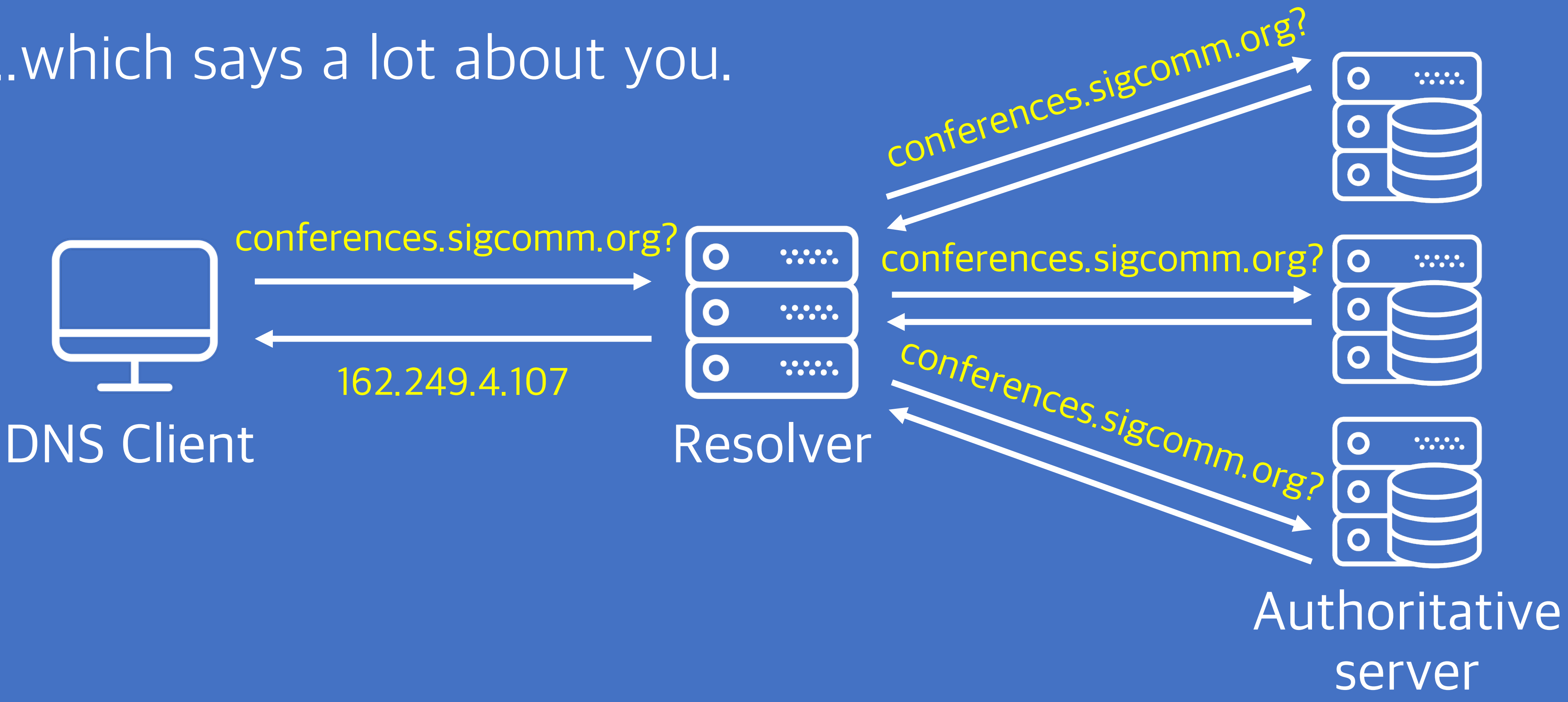
How Far Have We Come?

Chaoyi Lu, Baojun Liu, Zhou Li, Shuang Hao, Haixin Duan,
Mingming Zhang, Chunying Leng, Ying Liu, Zaifeng Zhang, Jianping Wu

Domain Name System

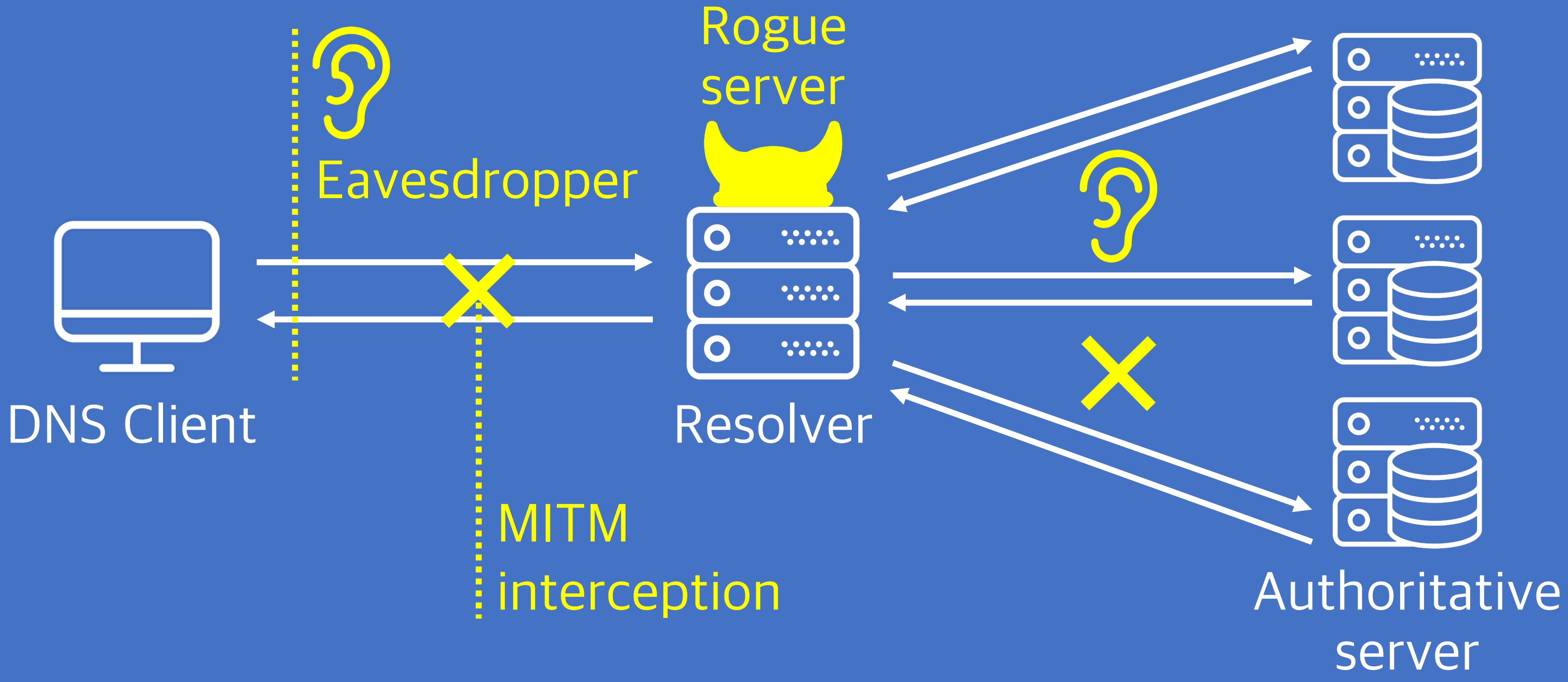
The start of Internet activities.

…which says a lot about you.



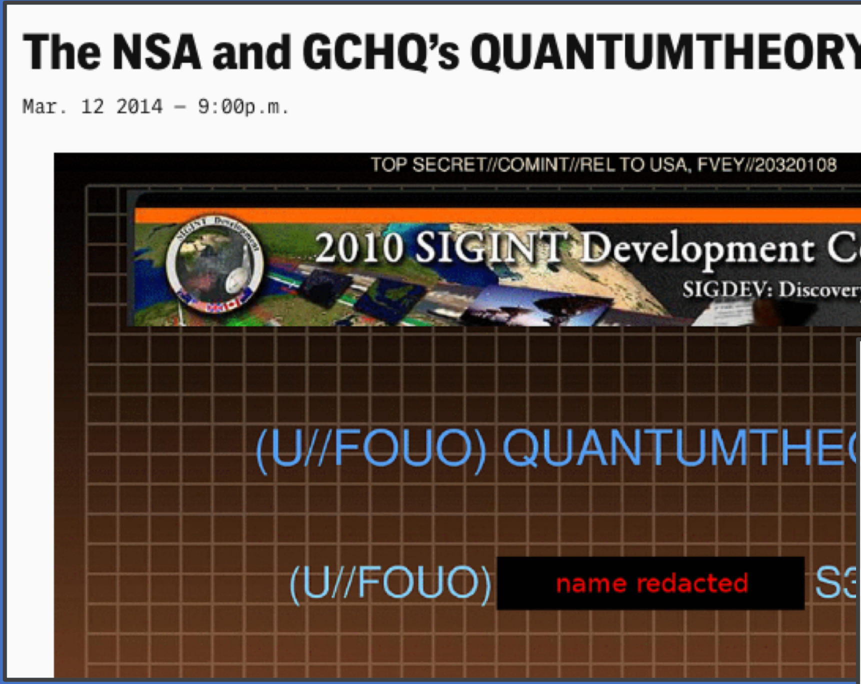
DNS Privacy

Where are the risks?



DNS Privacy

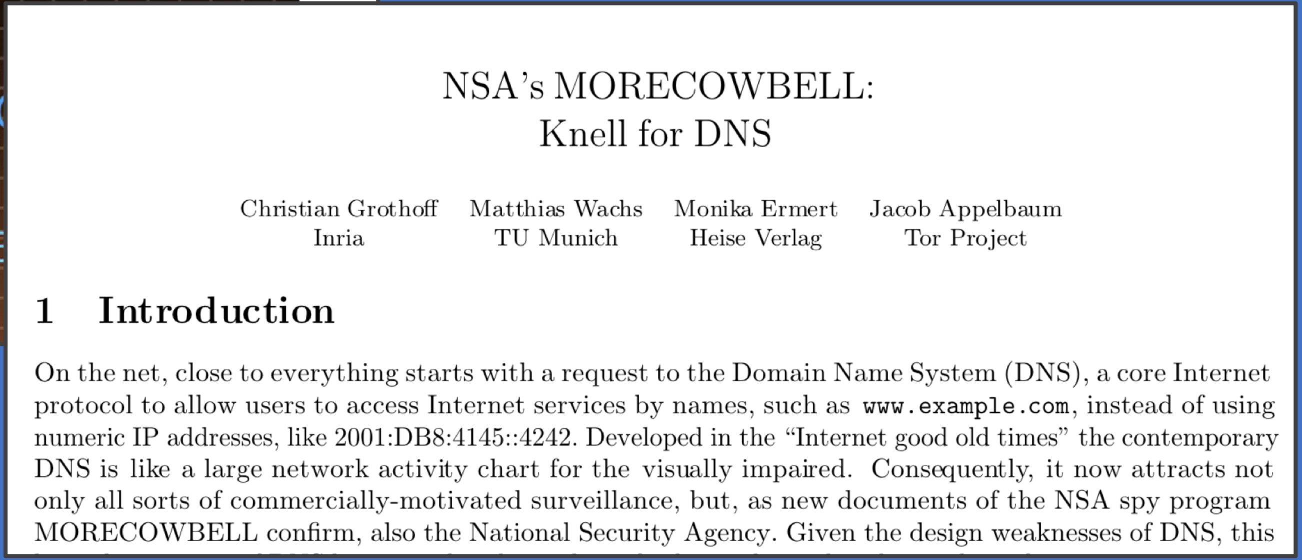
People could be watching our queries.



The NSA and GCHQ's QUANTUMTHEORY Hacking Tactics

Mar. 12 2014 – 9:00p.m.

TOP SECRET//COMINT//REL TO USA, FVEY//20320108
2010 SIGINT Development Conference
SIGDEV: Discovery in the Cyber Age
(U//FOUO) QUANTUMTHE
(U//FOUO) name redacted S3



NSA's MORECOWBELL: Knell for DNS

Christian Grothoff, Inria
Matthias Wachs, TU Munich
Monika Ermert, Heise Verlag
Jacob Appelbaum, Tor Project

1 Introduction

On the net, close to everything starts with a request to the Domain Name System (DNS), a core Internet protocol to allow users to access Internet services by names, such as `www.example.com`, instead of using numeric IP addresses, like 2001:DB8:4145::4242. Developed in the "Internet good old times" the contemporary DNS is like a large network activity chart for the visually impaired. Consequently, it now attracts not only all sorts of commercially-motivated surveillance, but, as new documents of the NSA spy program MORECOWBELL confirm, also the National Security Agency. Given the design weaknesses of DNS, this

DNS Privacy

People could be watching our queries.

And do stuff like:

Device fingerprinting

User tracking

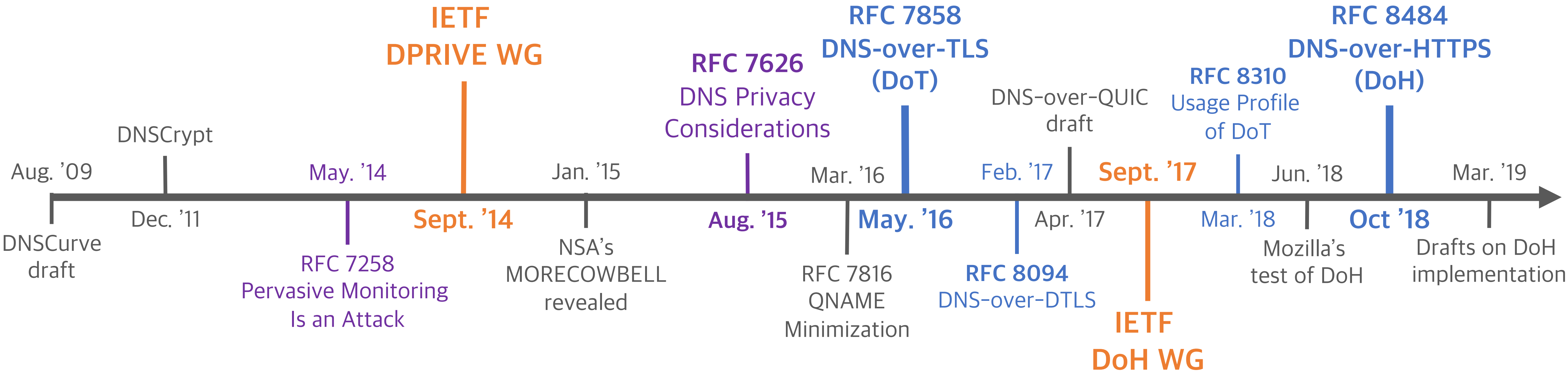
User behavior analysis

DNS Privacy: What Has Been Done?

Two IETF WGs.

Three standardized protocols.

More implementations and tests coming…



Aug. '09
DNSCurve draft

Dec. '11
DNSCrypt

May. '14
RFC 7258 Pervasive Monitoring Is an Attack

Sept. '14
IETF DPRIVE WG

Jan. '15
NSA's MORECOWBELL revealed

Aug. '15
RFC 7626 DNS Privacy Considerations

Mar. '16
RFC 7816 QNAME Minimization

May. '16
RFC 7858 DNS-over-TLS (DoT)

Feb. '17
RFC 8094 DNS-over-DTLS

Apr. '17
DNS-over-QUIC draft

Sept. '17
IETF DoH WG

Mar. '18
RFC 8310 Usage Profile of DoT

Jun. '18
Mozilla's test of DoH

Oct '18
RFC 8484 DNS-over-HTTPS (DoH)

Mar. '19
Drafts on DoH implementation

DNS-over-Encryption: Standard Protocols

DNS-over-TLS (DoT, RFC 7858, May 2016)

Uses TLS to wrap DNS messages.

Dedicated port 853.

Stub resolver update needed.

DNS-over-HTTPS (DoH, RFC 8484, Oct 2018)

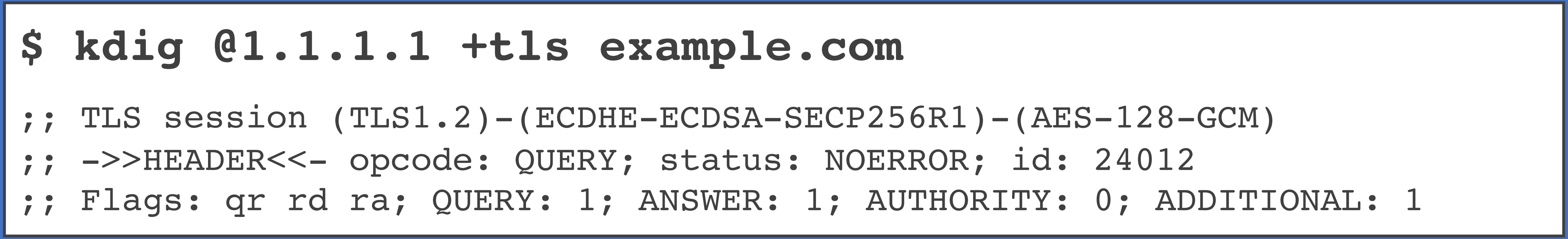
Embeds DNS packets into HTTP messages.

Shared port 443.

More user-space friendly.

DNS-over-Encryption: Standard Protocols

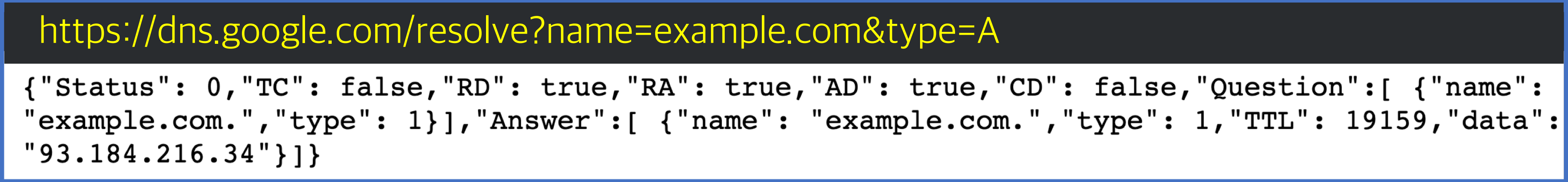
Issuing DNS-over-TLS queries with kdig.



```
$ kdig @1.1.1.1 +tls example.com

;; TLS session (TLS1.2)-(ECDHE-ECDSA-SECP256R1)-(AES-128-GCM)
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 24012
;; Flags: qr rd ra; QUERY: 1; ANSWER: 1; AUTHORITY: 0; ADDITIONAL: 1
```

Issuing DNS-over-HTTPS queries in a browser.



https://dns.google.com/resolve?name=example.com&type=A

```
{"Status": 0,"TC": false,"RD": true,"RA": true,"AD": true,"CD": false,"Question":[ {"name":
"example.com.","type": 1}],"Answer":[ {"name": "example.com.","type": 1,"TTL": 19159,"data":
"93.184.216.34"}]}
```

The Rapid Development of DoE

Widely getting support from the industry.

1.1.1.1

8.8.8.8

Public DNS resolvers

DNS server software

unbound

KNOT RESOLVER

Operating Systems

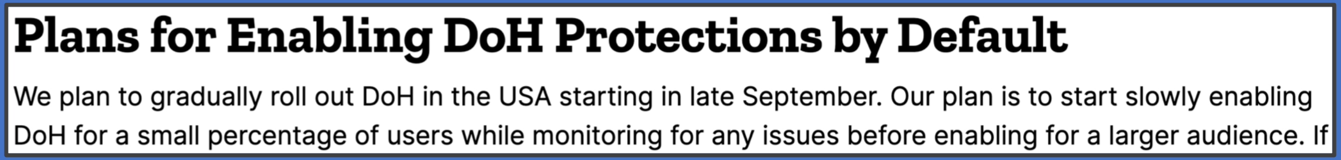
android

LINUX.ORG

Web Browsers

The Rapid Development of DoE

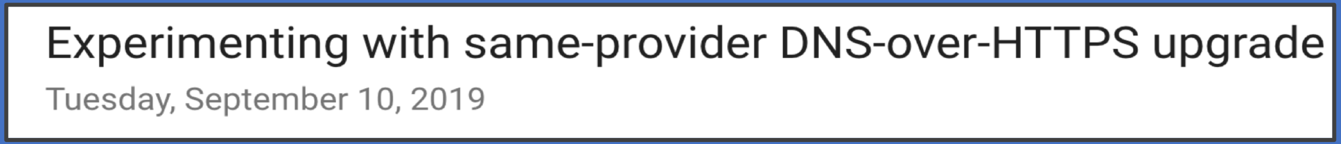
Recent updates from service providers & vendors.



Plans for Enabling DoH Protections by Default

We plan to gradually roll out DoH in the USA starting in late September. Our plan is to start slowly enabling DoH for a small percentage of users while monitoring for any issues before enabling for a larger audience. If

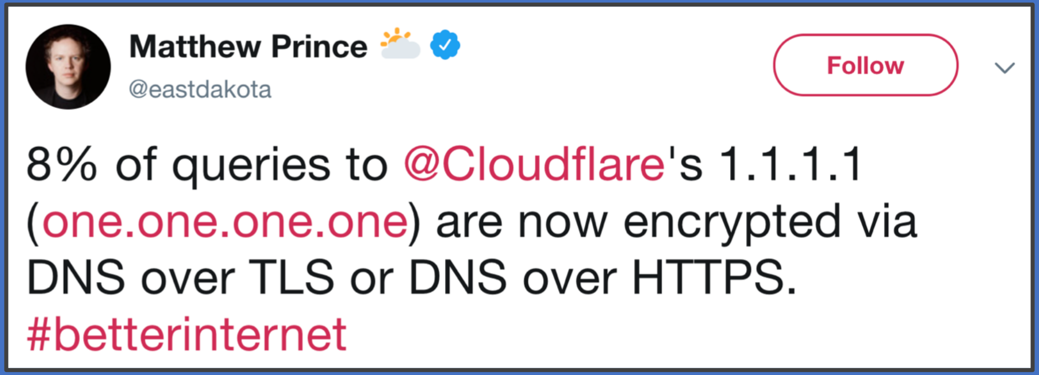
Firefox:
Plans on defaulting DoH



Experimenting with same-provider DNS-over-HTTPS upgrade

Tuesday, September 10, 2019

Google:
Chrome DoH experiment on its way



Matthew Prince ⛅

@eastdakota

8% of queries to @Cloudflare's 1.1.1.1 (one.one.one.one) are now encrypted via DNS over TLS or DNS over HTTPS. #betterinternet

Cloudflare:
8% queries are using DoT or DoH

Questions: from Users’ Perspective

How many DoE servers are there?

Methodology: Internet-wide scanning.

How are the reachability and performance of DoE servers?

Methodology: Large-scale client-side measurement.

What does the real-world usage of DoE look like?

Methodology: Analysis on passive traffic.

Q1:
How many servers are there?

DoE Server Discovery

DNS-over-TLS (DoT)

Runs over
dedicated port 853.

↓

Internet-wide Scan

DNS-over-HTTPS (DoH)

Uses common URI templates.
(/dns-query, /resolve)

↓

URL database Inspection

DNS-over-TLS Resolvers

Internet-wide probing with ZMap, getdns & OpenSSL.

zmap
getdns
Open
SSL

Zmap
Internet-wide scan
Port 853

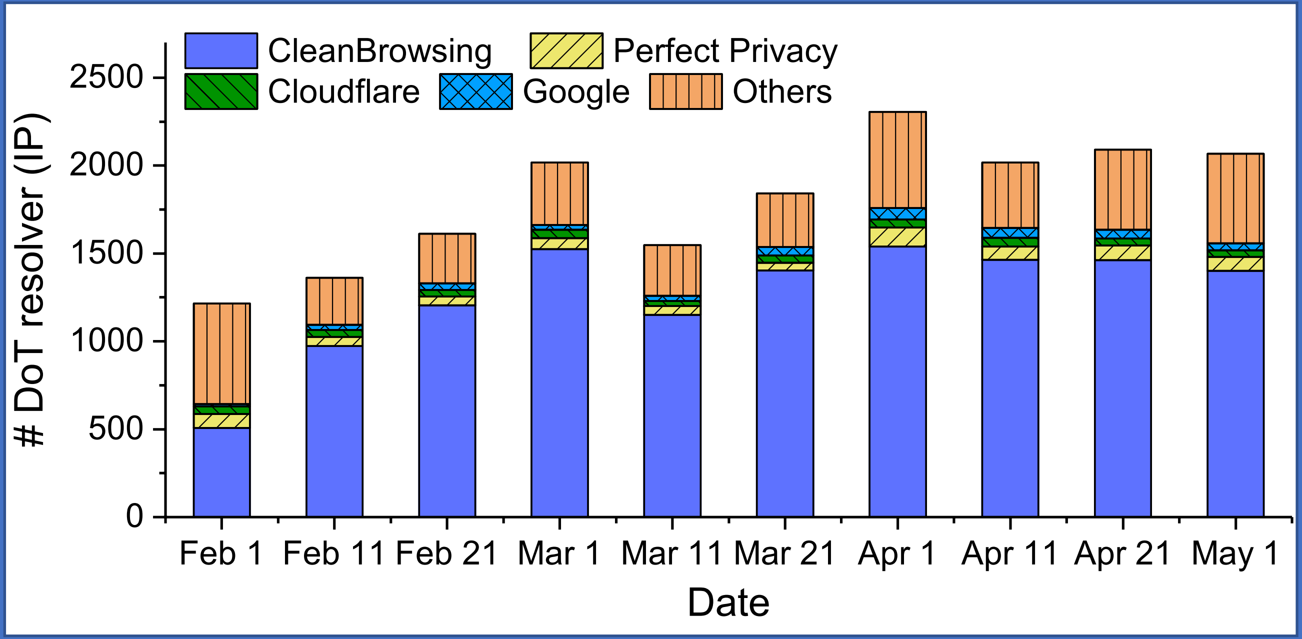
getdns
DoT query

OpenSSL
Verify SSL
certificate chain

DNS-over-TLS Resolvers

~2K open DoT resolvers in the wild.

Several big players dominate in the count of servers.



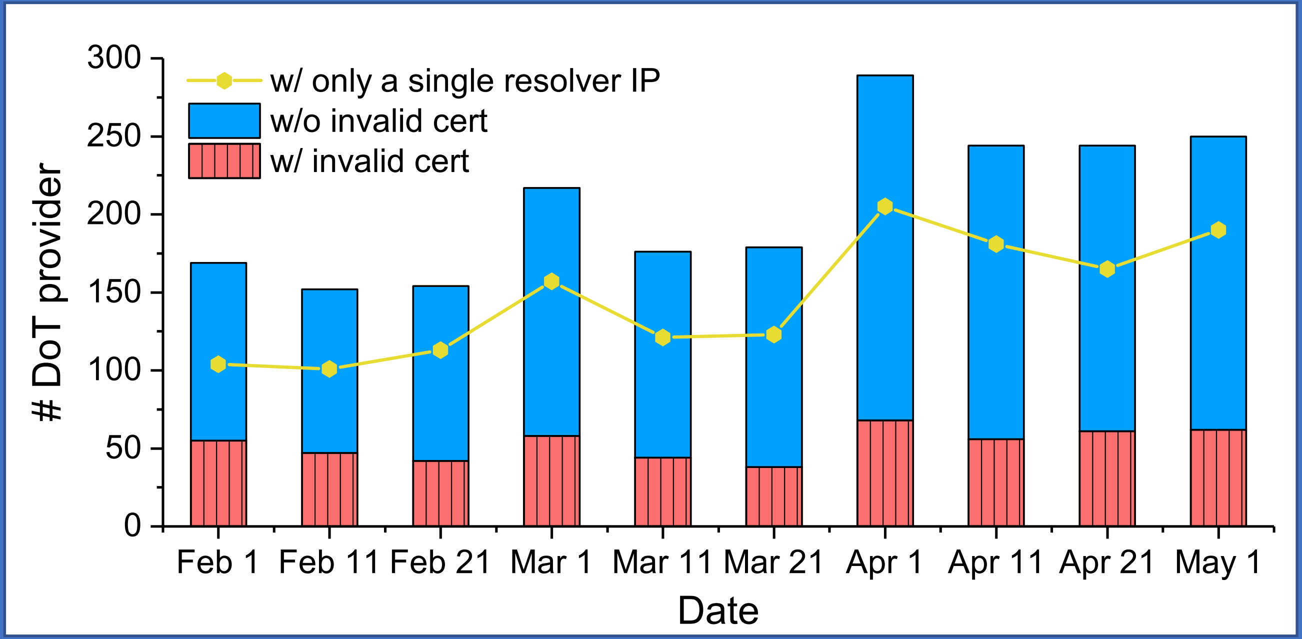
(As of May 1)

🇮🇪	IE	951	46%
🇺🇸	US	531	26%
🇩🇪	DE	86	4%
🇫🇷	FR	56	3%

DNS-over-TLS Providers

Small providers: ~70% only operate on one single address.

Security: ~25% providers use invalid TLS certificates.

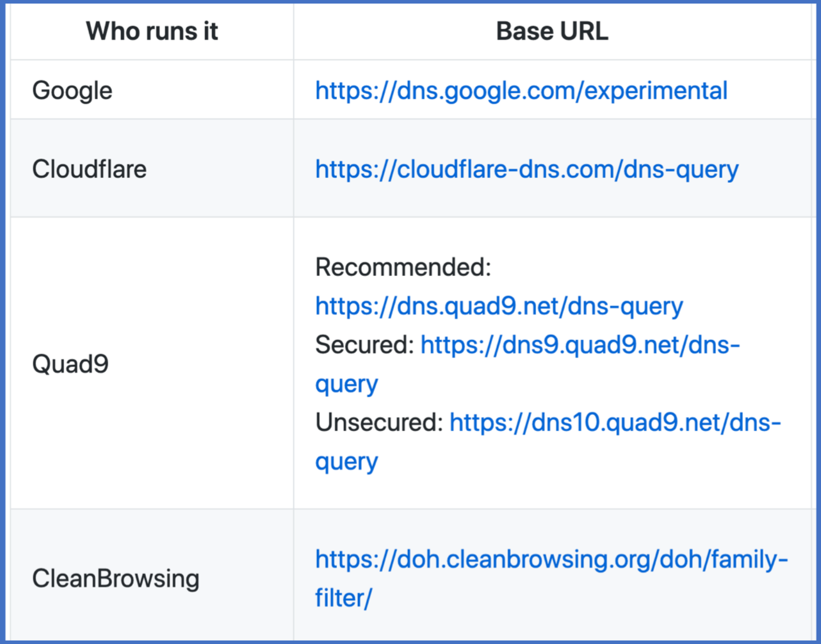


- Expired cert
- Self-signed cert
- Broken cert chain

DNS-over-HTTPS Providers

Large-scale URL dataset inspection.

Scale: only 17 providers found, mostly known in lists.



Who runs it	Base URL
Google	https://dns.google.com/experimental
Cloudflare	https://cloudflare-dns.com/dns-query
Quad9	Recommended: https://dns.quad9.net/dns-query Secured: https://dns9.quad9.net/dns-query Unsecured: https://dns10.quad9.net/dns-query
CleanBrowsing	https://doh.cleanbrowsing.org/doh/family-filter/

(DoH list maintained by the curl project)

Found 2 providers beyond the list:

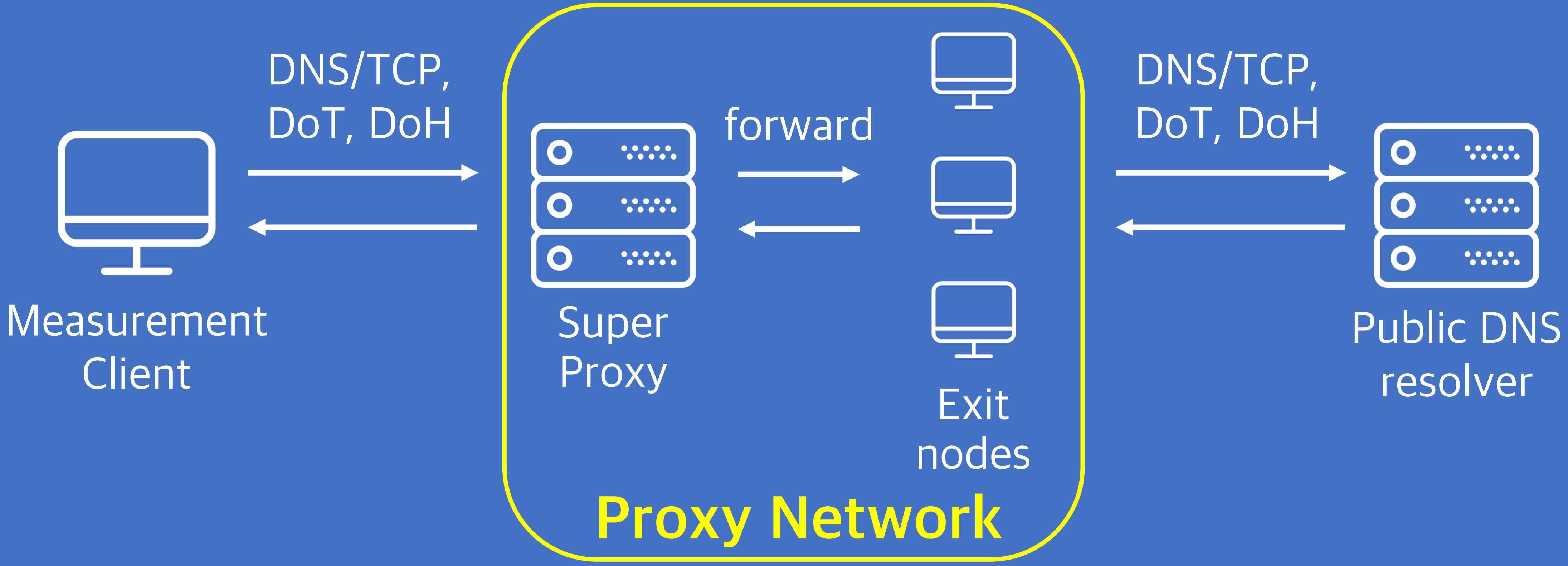
dns.adguard.com

dns.233py.com

Q2:
Are popular services reachable?

Reachability to DoE Servers

Measurement platform built on SOCKS5 proxy network.



Reachability to DoE Servers

Measurement platform built on SOCKS5 proxy network.

Vantage point: 114K vantage points from 2 proxy networks.

Vantage	Platform	Count of		
		IP	Country	AS
Global	proxyrack	29,622	166	2,597
China (Censored)	芝麻HTTP 高速HTTP代理 -h.zhimaruanjian.com-	85,122	1 (CN)	5

Reachability to DoE Servers

Measurement platform built on SOCKS5 proxy network.

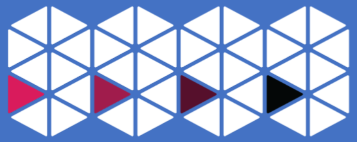
Vantage point: 114K vantage points from 2 proxy networks.

Test items on each vantage:

Are public services reachable?

1.1.1.1

8.8.8.8



Query a
controlled domain
via DNS/TCP, DoT & DoH

Why do they fail?

SSL certificate

Open ports

Webpages

Reachability Test Results

DoE is currently less interrupted by in-path devices.

~99% global reachability.

Vantage	Resolver	Query Failure Rate		
		DNS/TCP	DoT	DoH
Global	Cloudflare	16.5%	1.2%	0.1%
	Google	15.8%	-	0.2%
	Quad9	0.2%	0.2%	14.0%
China	Google	1.1%	-	99.9%

Address 1.1.1.1 conflicted, e.g., by residential network devices.

Reachability Test Results

DoE is currently less interrupted by in-path devices.

~99% global reachability.

Examples of 1.1.1.1 address conflicting:

Port open	# Client	Example client AS
22 (SSH)	28	AS17488 Hatheway IP Over Cable Internet
23 (Telnet)	40	AS24835 Vodafone Data
67 (DHCP)	7	AS52532 Speednet Telecomunicacoes Ldta
161 (SNMP)	10	AS9870 Dong-eui University
179 (BGP)	23	AS3269 Telecom Italia S.p.a

Reachability Test Results

DoE is currently less interrupted by in-path devices.

~99% global reachability.

Vantage	Resolver	Query Failure Rate		
		DNS/TCP	DoT	DoH
Global	Cloudflare	16.5%	1.2%	0.1%
	Google	15.8%	-	0.2%
	Quad9	0.2%	0.2%	14.0%
China	Google	1.1%	-	99.9%

Forward DoH queries to DNS/53, with a small timeout.

Blocked by censorship.

Q3:
Is DoE query time tolerable?

DoE lookup performance

Aim: measure the relative query time of DNS and DoE.

A major influence: connection reuse.

Specification

(RFC 7858, DNS-over-TLS)
“Clients and servers SHOULD reuse existing connections for subsequent queries as long as they have sufficient resources.”

Implementation

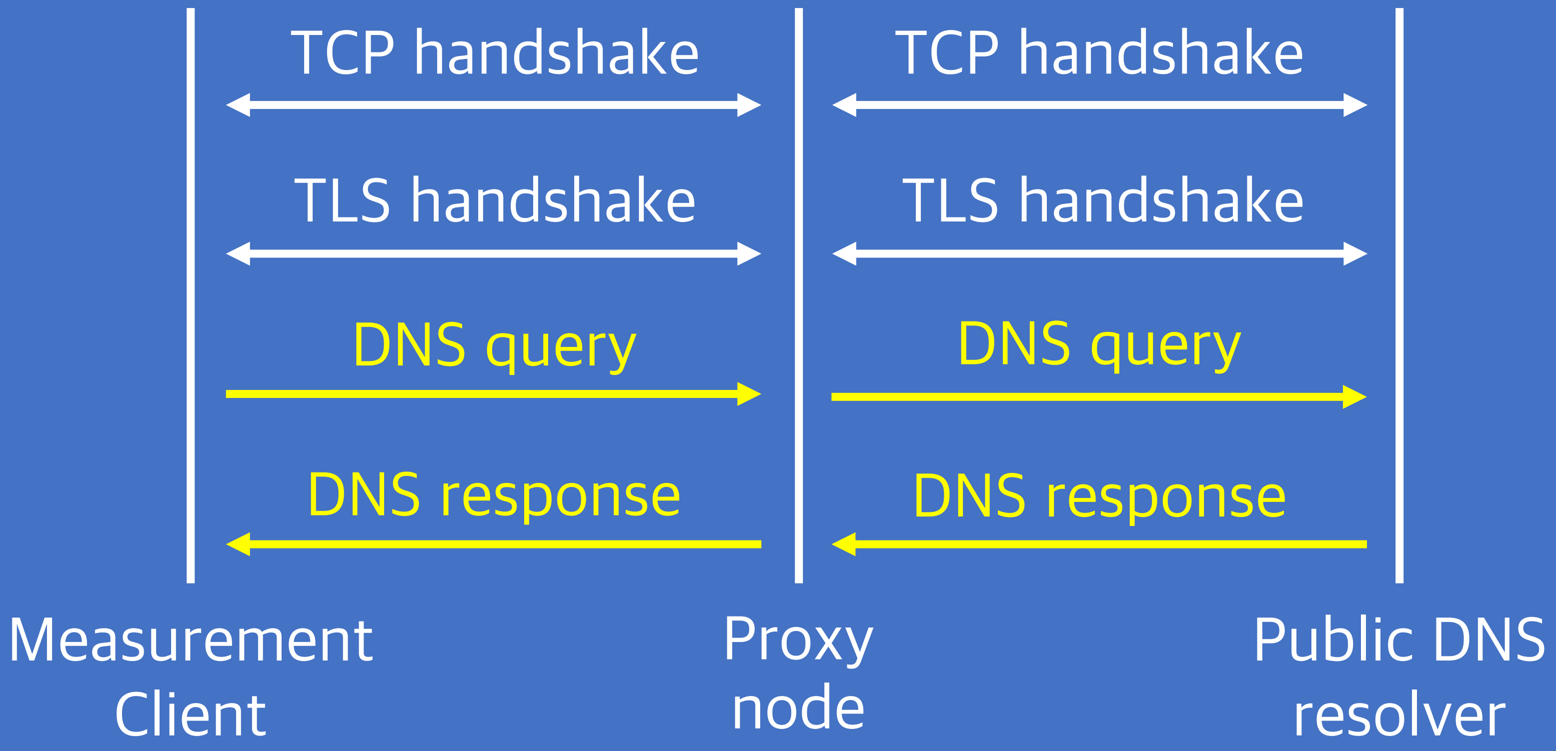
Stub: supported by dig, kdig, Stubby, etc.

Cloudflare resolver: “long-lived” connection supported (tens of seconds)

DoE lookup performance

Vantage point: 8,257 proxy nodes from ProxyRack.

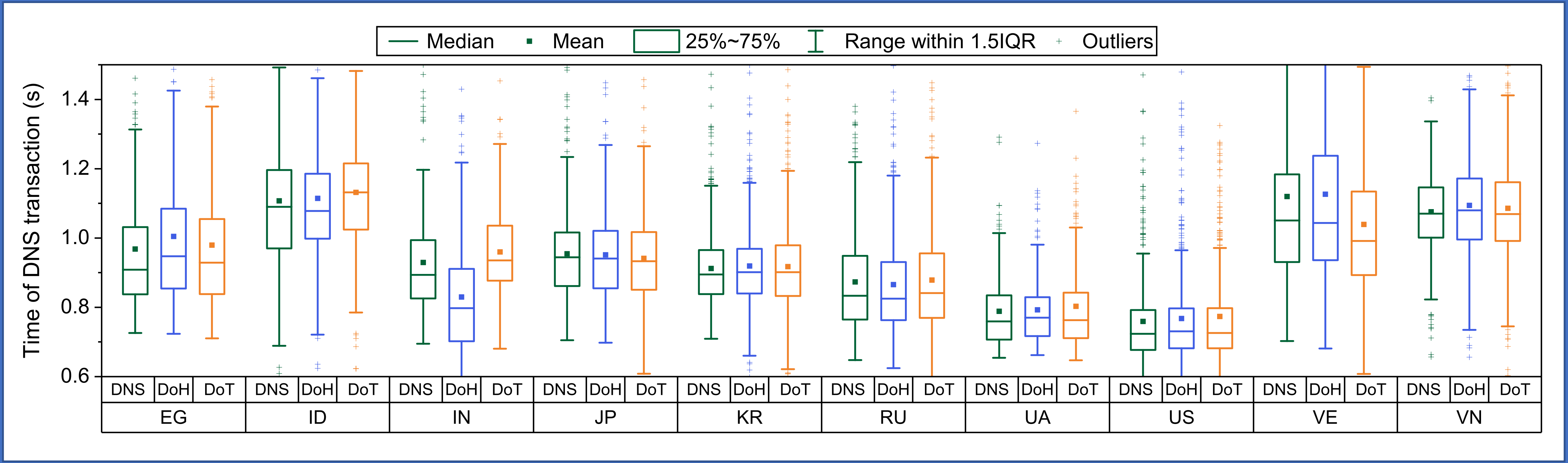
Connection reuse: only recording DNS transaction time.



Performance Test Results

Tolerable query time overhead with reused connections.

On average, extra latency on the order of milliseconds.



Q4:
What does DoE traffic scale look like?

DoE Traffic Observation

DNS-over-TLS (DoT)

Runs over
dedicated port 853.

↓

ISP NetFlow dataset

DNS-over-HTTPS (DoH)

Resolver domain name
(e.g., dns.google.com)
In URI templates.

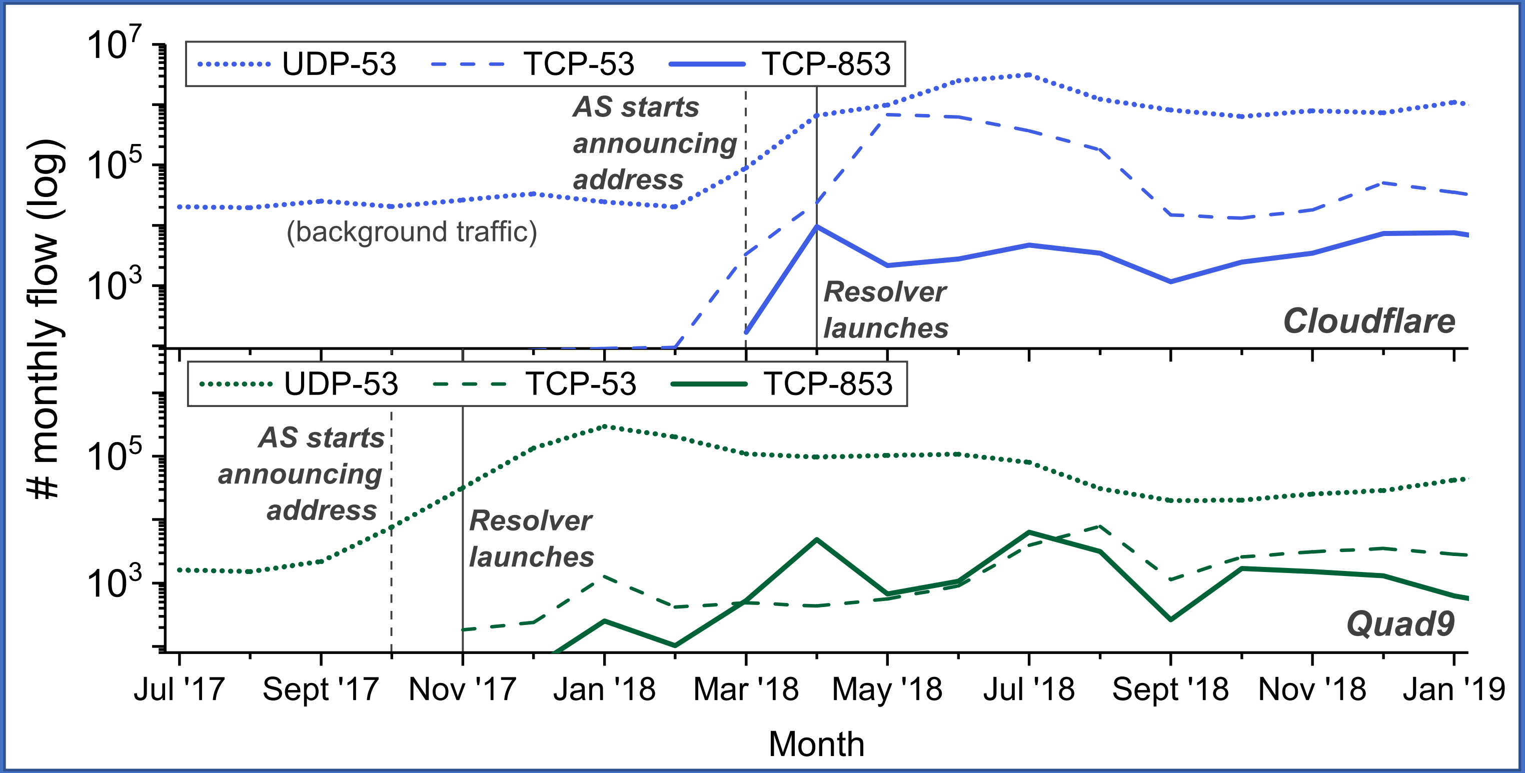
↓

Passive DNS dataset

DNS-over-TLS Traffic

Data: 18-month NetFlow dataset from a large Chinese ISP.

Scale: still much less than traditional DNS, but growing.



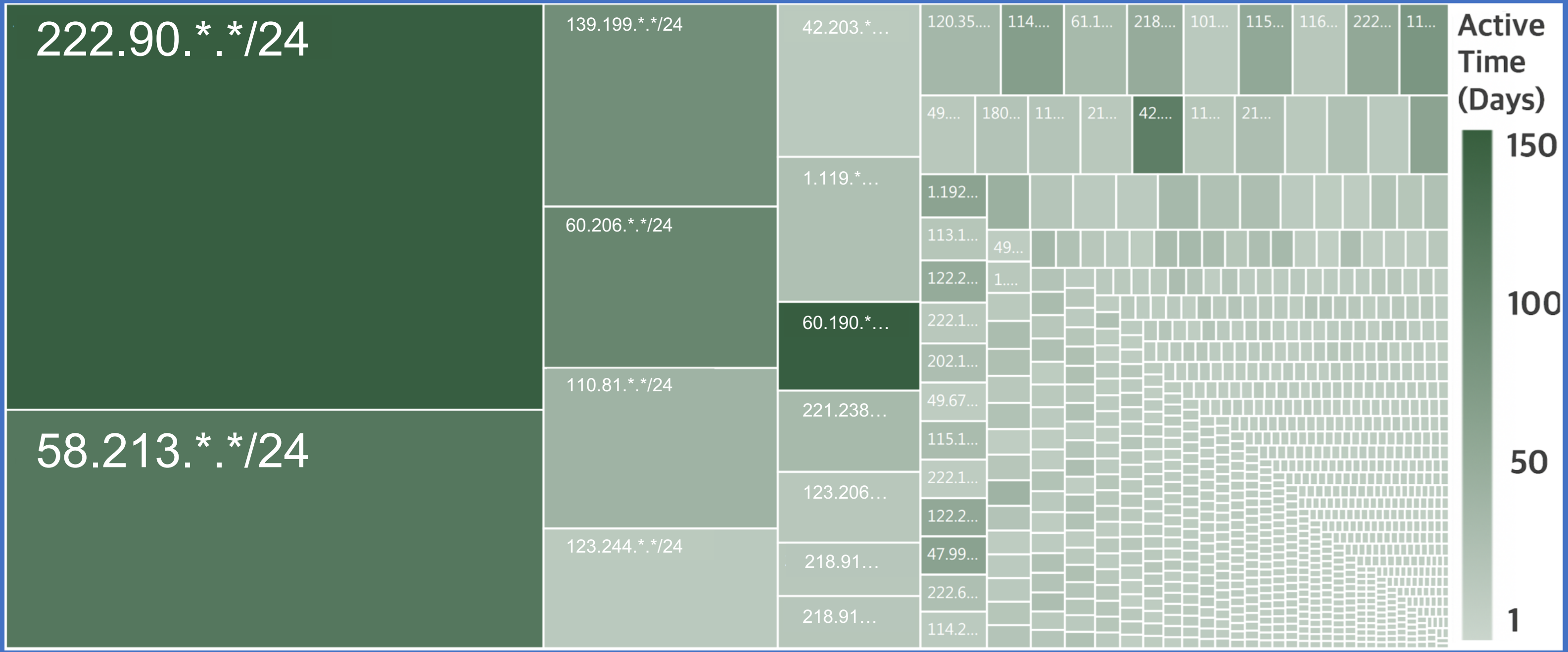
DoT:
2 to 3 orders
of magnitude
less traffic

DNS-over-TLS Traffic

Data: 18-month NetFlow dataset from a large Chinese ISP.

Scale: still much less than traditional DNS, but growing.

Clients: centralized clients + temp users.



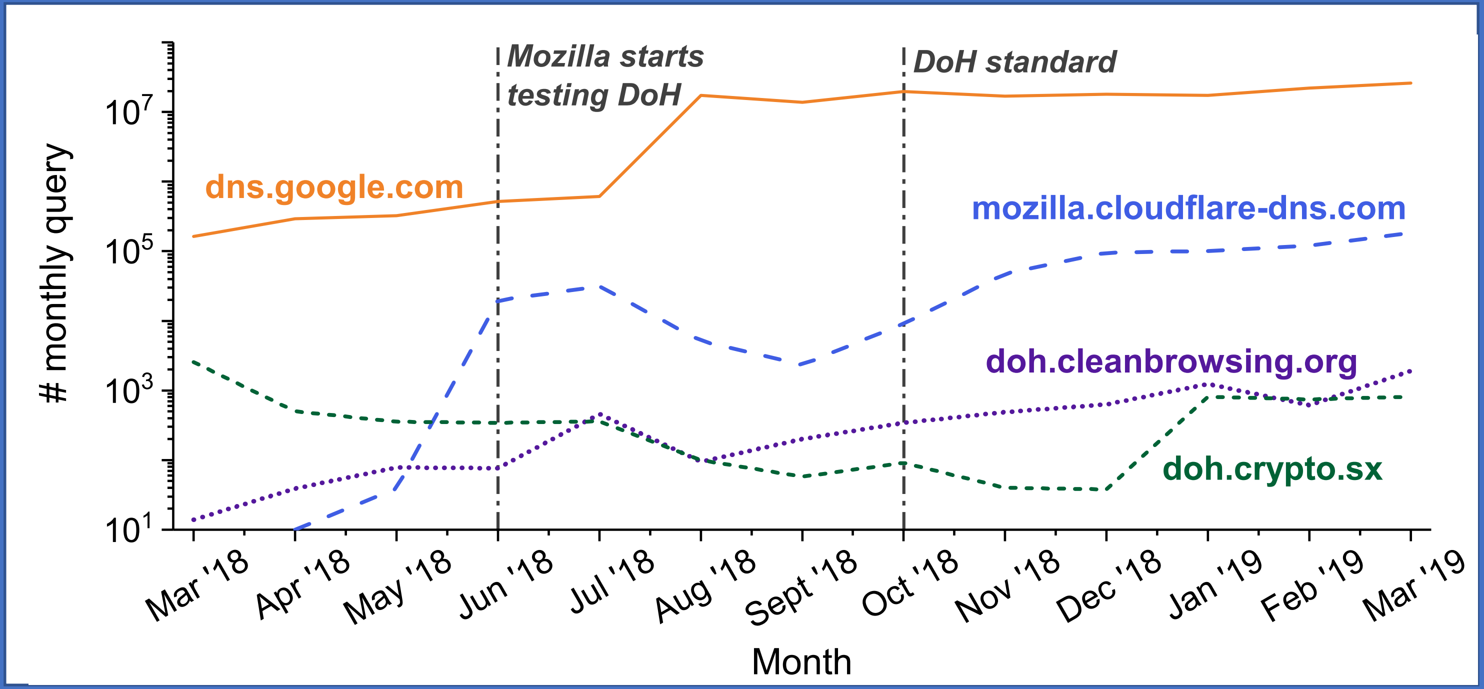
Top 20 netblocks:
> 60% DoT traffic

> 95% netblocks:
Active for < one week

DNS-over-HTTPS Traffic

Data: Passive DNS dataset, monthly query volume.

Big players dominate. Also a growing trend.



Summary: Key Observations

Open DNS-over-Encryption resolvers

A number of small providers less-known.

~25% providers use invalid TLS certificates.

Client-side usability

Currently good reachability (~99%).

Tolerable performance overhead with reused connections.

Real-world traffic

Still much less than traditional DNS, but growing.

Limitations

DoE server discovery

Internet-wide scan misses local resolvers.

DoH discovery relies on data traces.

Reachability & performance test

Proxy networks only allows TCP traffic.

DoE traffic observation

Geographic bias of dataset.

Underestimation because of DNS cache.

Discussion

Protocol designers

Reuse well-developed protocols.

Service providers

Correct misconfigurations.

Keep servers under regular maintenance.

Use addresses with a clean history.

DNS clients

Education on benefits of encryption.

Dataset & code release

Please visit https://dnsencryption.info.

An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come?

Chaoyi Lu, Baojun Liu, Zhou Li, Shuang Hao, Haixin Duan,
Mingming Zhang, Chunying Leng, Ying Liu, Zaifeng Zhang, Jianping Wu