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
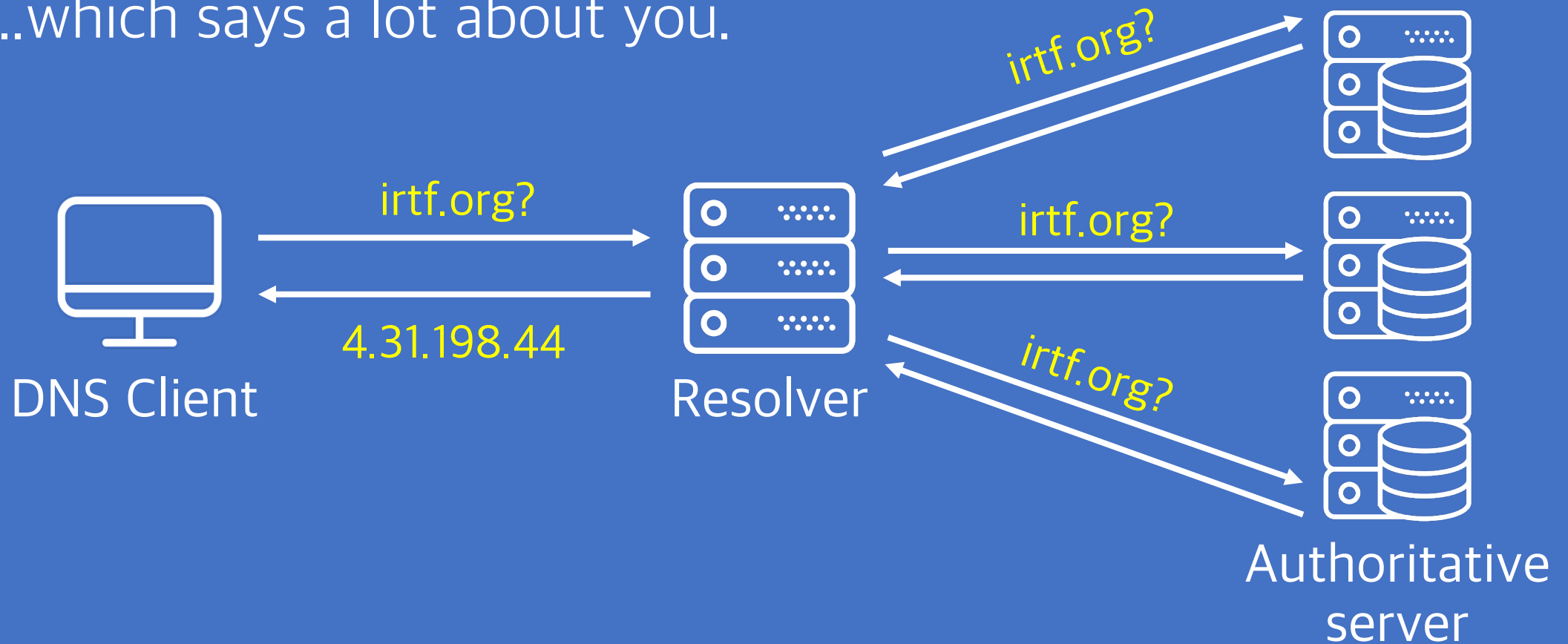
University of California, Irvine

UT DALLAS
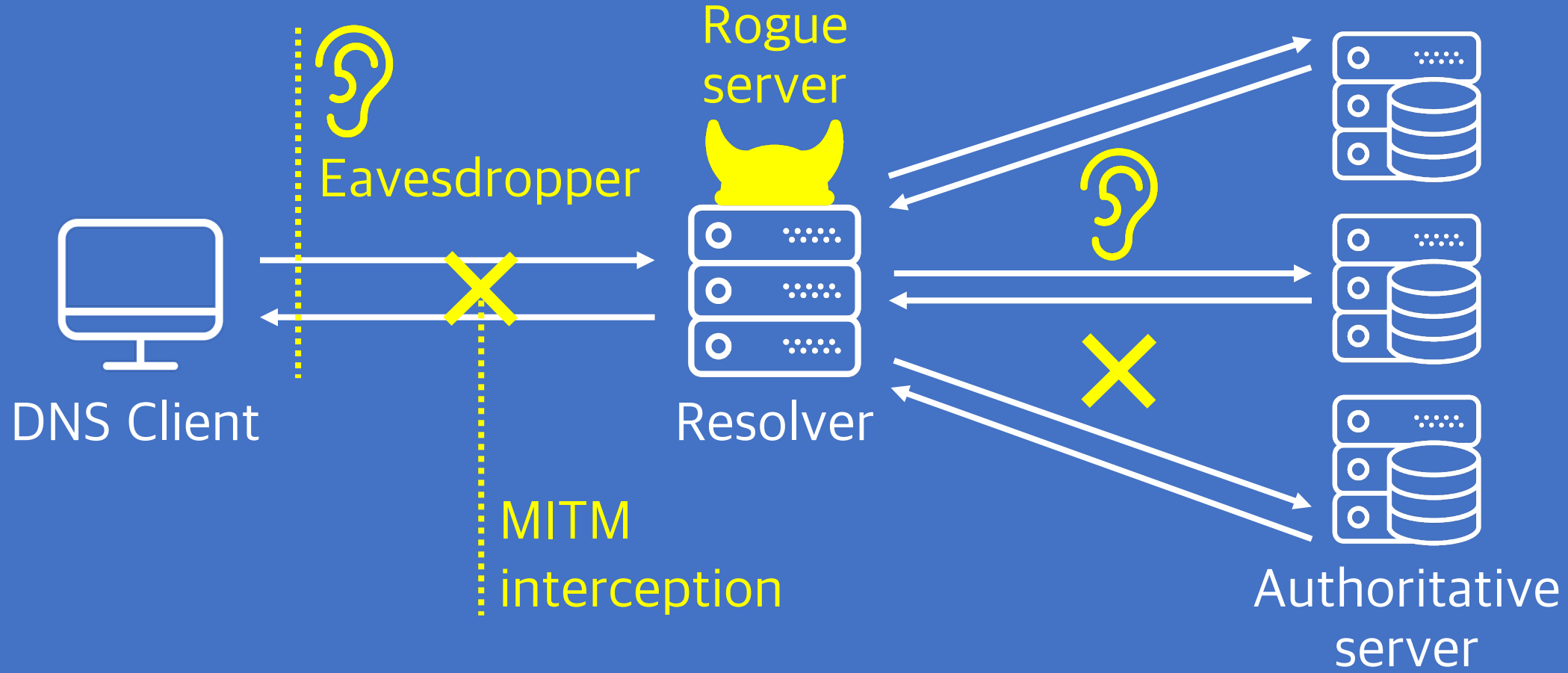The University of Texas at Dallas

Netlab 360.com

Domain Name System

The start of Internet activities.
...which says a lot about you.

DNS Client

irtf.org?

4.31.198.44

Resolver

irtf.org?

irtf.org?

irtf.org?

Authoritative server

DNS Privacy

Where are the risks?

DNS Client

Eavesdropper

Rogue server

Resolver

MITM interception

Authoritative server

DNS Privacy

People could be watching our queries.

The revelations (from the Edward Snowden documents, which were leaked from the National Security Agency (NSA)) of the MORECOWBELL surveillance program [morecowbell], which uses the DNS, both passively and actively, to surreptitiously gather information about the users, is another good example showing that the lack of privacy protections in the DNS is actively exploited.

RFC 7626 on DNS privacy

NSA's MORECOWBELL:
Knell for DNS

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

The MORECOWBELL surveillance program of NSA

4

DNS Privacy

People could be watching our queries.
And do stuff like:

**Device
Fingerprinting**
[Chang '15]
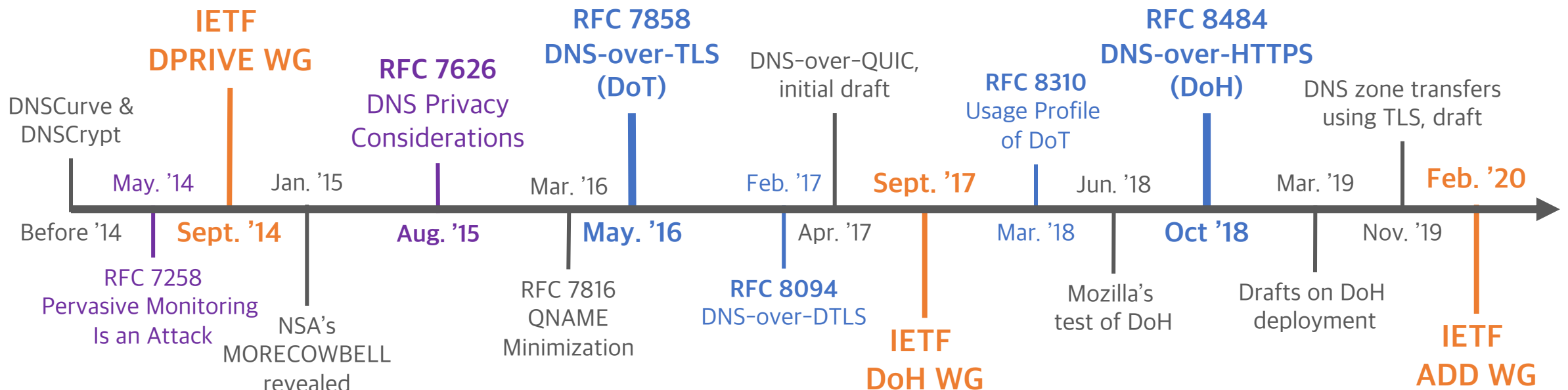
**User
Tracking**
[Kirchler '16]

**User behavior
Analysis**
[Kim '15]

DNS Privacy: What Has Been Done?

Three IETF WGs.

Three standardized protocols.

More implementations and tests coming…

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
```
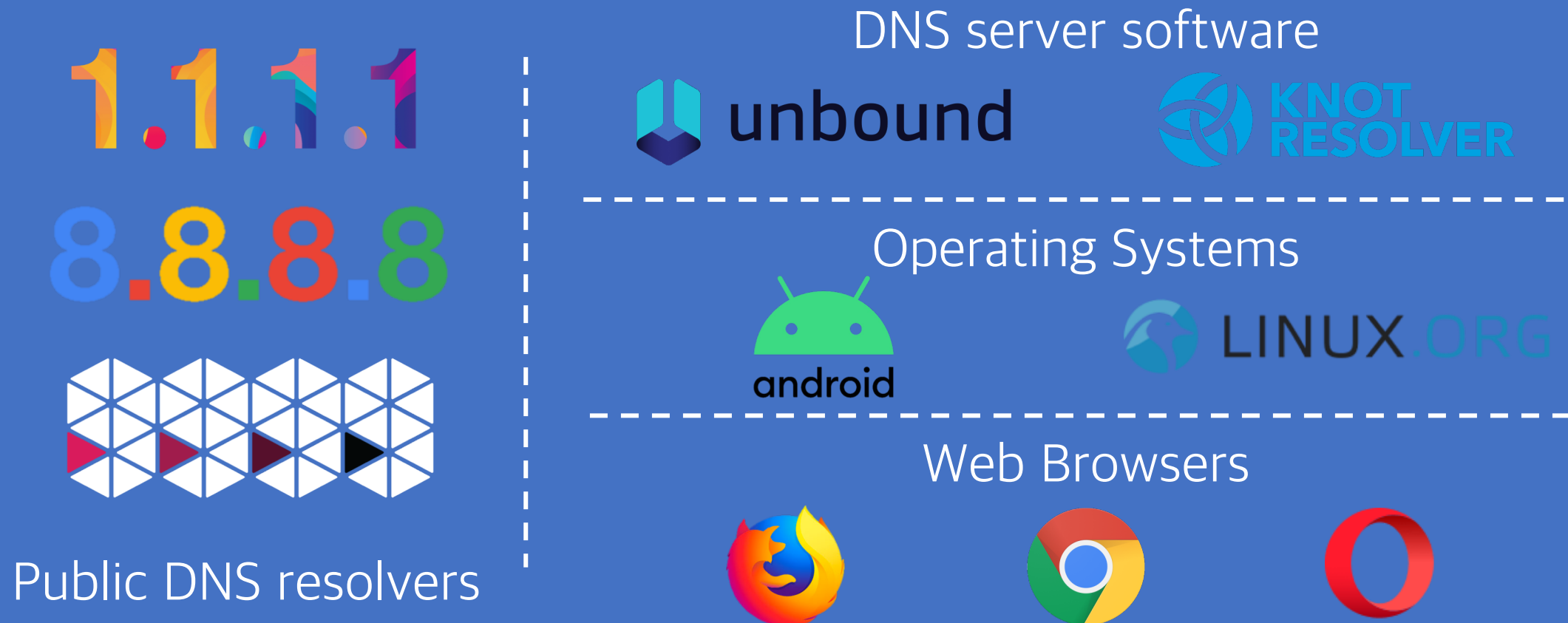
Issuing DNS-over-HTTPS queries in a browser.

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.

DNS server software

unbound

KNOT RESOLVER

Operating Systems

android

LINUX.ORG

Web Browsers

Public DNS resolvers

The Rapid Development of DoE

Recent updates from service providers & vendors.

Firefox continues push to bring DNS over HTTPS by default for US users

Selena Deckelmann | February 25, 2020

Today, Firefox began the rollout of encrypted DNS over HTTPS (DoH) by default for US-based users. The rollout will continue over the next few weeks to confirm no major issues are discovered as this new protocol is enabled for Firefox's US-based users.

Firefox: DoH by default for US users

A safer and more private browsing experience with Secure DNS

Tuesday, May 19, 2020

With Chrome 83, we've started rolling out Secure DNS, a feature built on top of a secure DNS protocol called DNS-over-HTTPS, which is designed to improve your safety and

Chrome: DoH support

Apple adds support for encrypted DNS (DoH and DoT)

Apple said this week that iOS 14 and macOS 11 will support the DNS-over-HTTPS and DNS-over-TLS protocols.

Apple:
DoT and DoH support added recently

Windows Insiders can now test DNS over HTTPS

05-13-2020 10:00 AM

If you have been waiting to try DNS over HTTPS (DoH) on Windows 10, you're in luck: the first testable version is now available to Windows Insiders! If you haven't been waiting for it, and are

Windows: DoH available for insiders

10

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. (e.g., /dns-query)

↓

URL database Inspection

DNS-over-TLS Resolvers

Internet-wide probing with ZMap, getdns & OpenSSL.

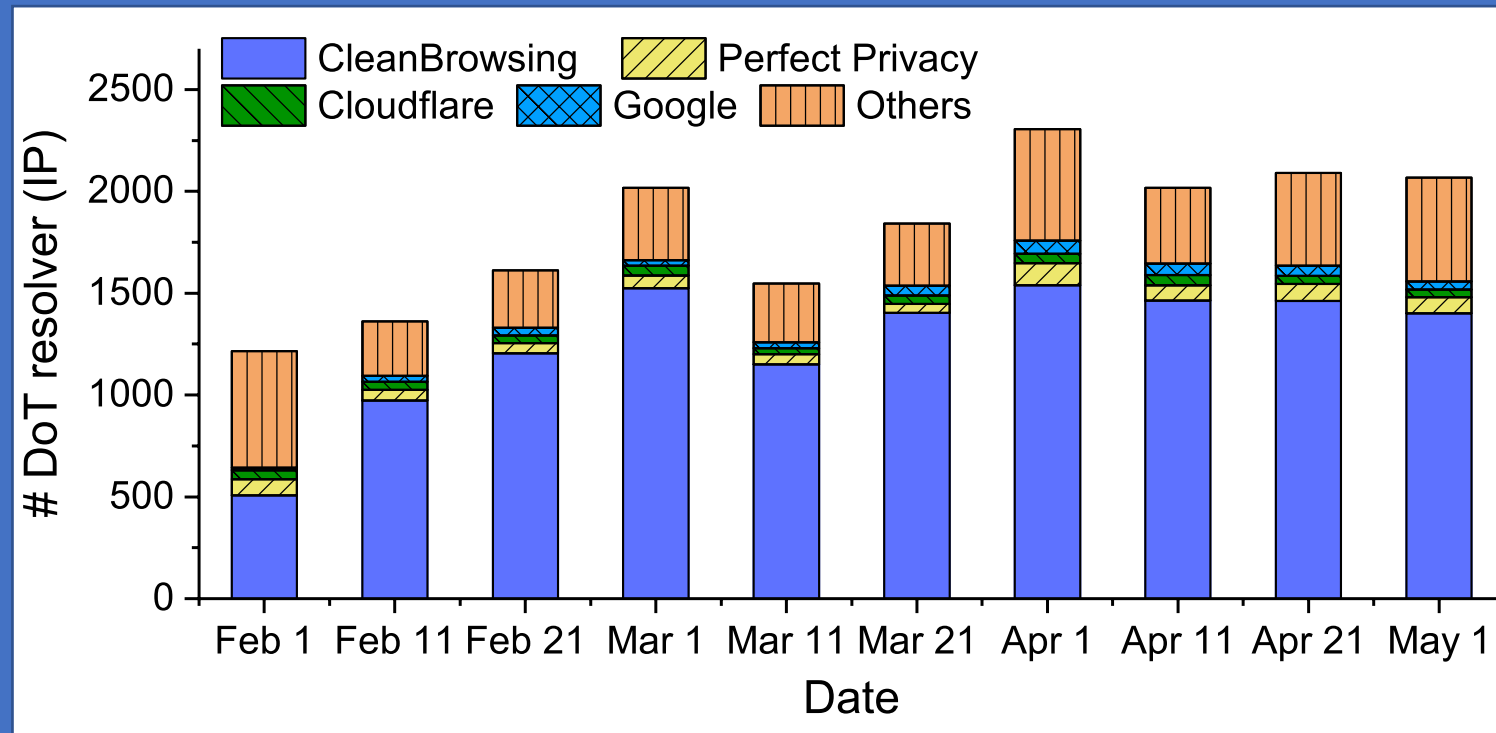**Zmap**
Internet-wide scan
Port 853

getdns
DoT query

OpenSSL
Verify
certificate chain
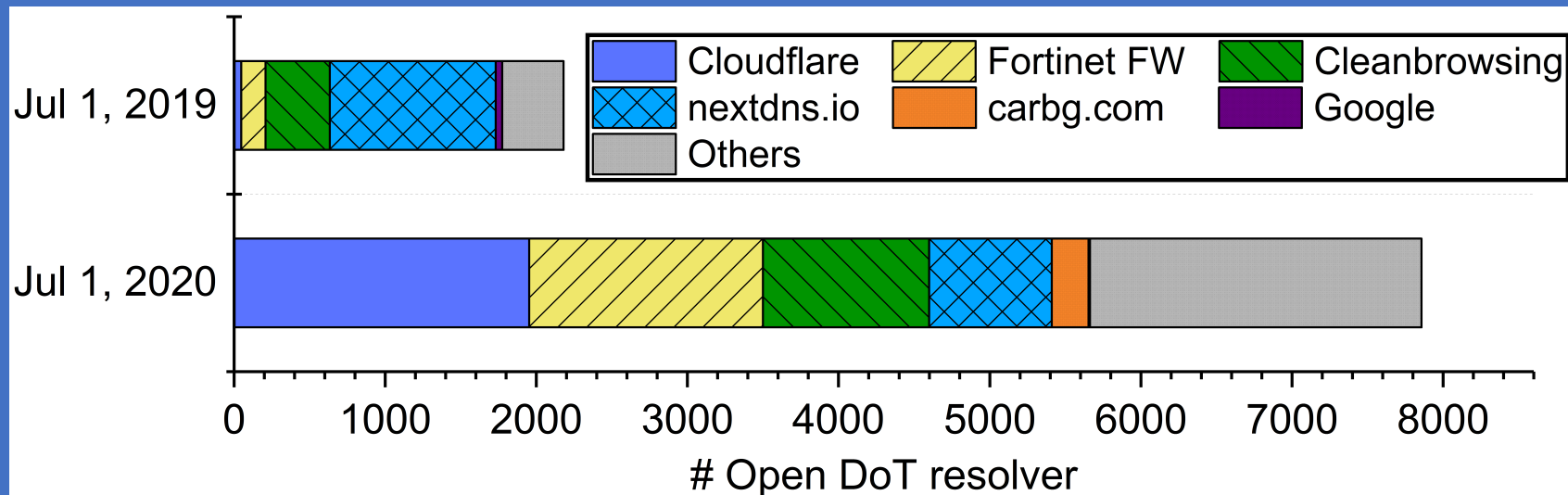
DNS-over-TLS Resolvers

Feb ~ May '19: ~2K open DoT resolvers in the wild.
Several big players dominate in the count of servers.

DNS-over-TLS Resolvers

Feb ~ May '19: **~2K open DoT resolvers** in the wild.
Several big players dominate in the count of servers.

Jul '20: rises to **7.8k resolvers** operated by **1.2K providers**

DoT Resolver Certificates
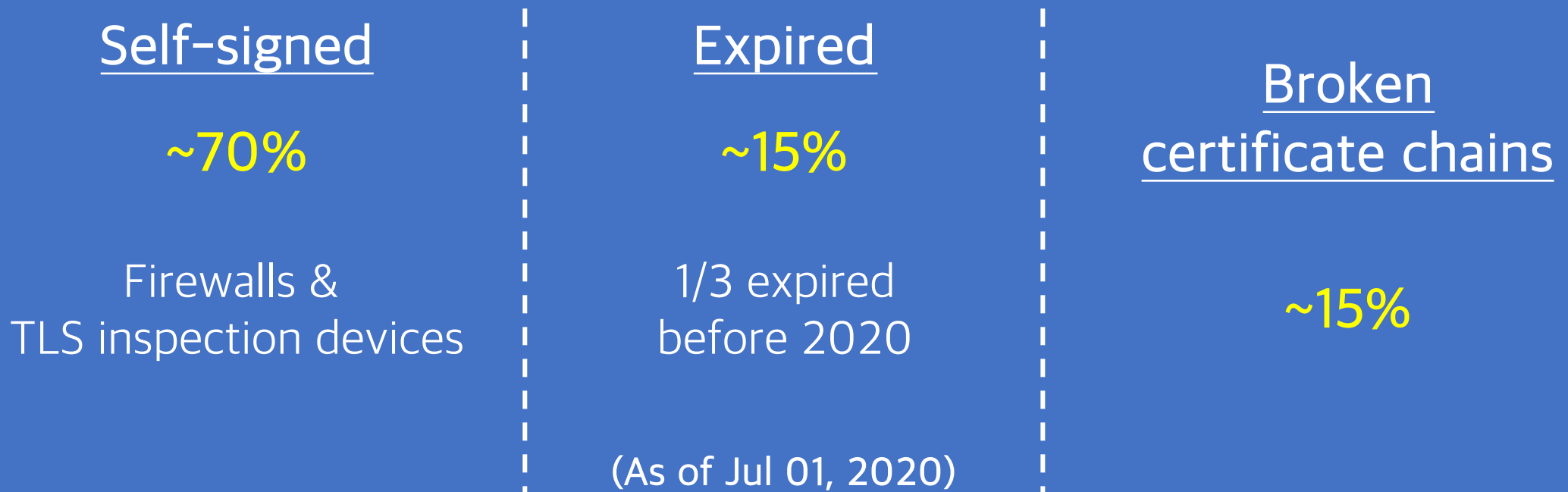
Authentication relies on PKIX certificates [RFC 8310].
Invalid certificates still poses as a problem.

Item	Jul 01, 2019	Jul 01, 2020
Resolvers that use invalid certificate	230 / 2,179 (10.6%)	**2,261 / 7,857 (28.8%)** ⬆
Providers that have invalid certificate	61 / 234 (26.0%)	**224 / 2,261 (9.9%)** ⬇

DoT Resolver Certificates

Authentication relies on PKIX certificates [RFC 8310].
Invalid certificates still poses as a problem.

Self-signed

~70%

Firewalls &
TLS inspection devices

Expired

~15%

1/3 expired
before 2020

(As of Jul 01, 2020)

Broken
certificate chains

~15%

18

DNS-over-HTTPS Providers

Large-scale URL dataset inspection.

May '19: **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

DNS-over-HTTPS Providers

Large-scale URL dataset inspection.

May '19: **17 providers found**, mostly known in lists.

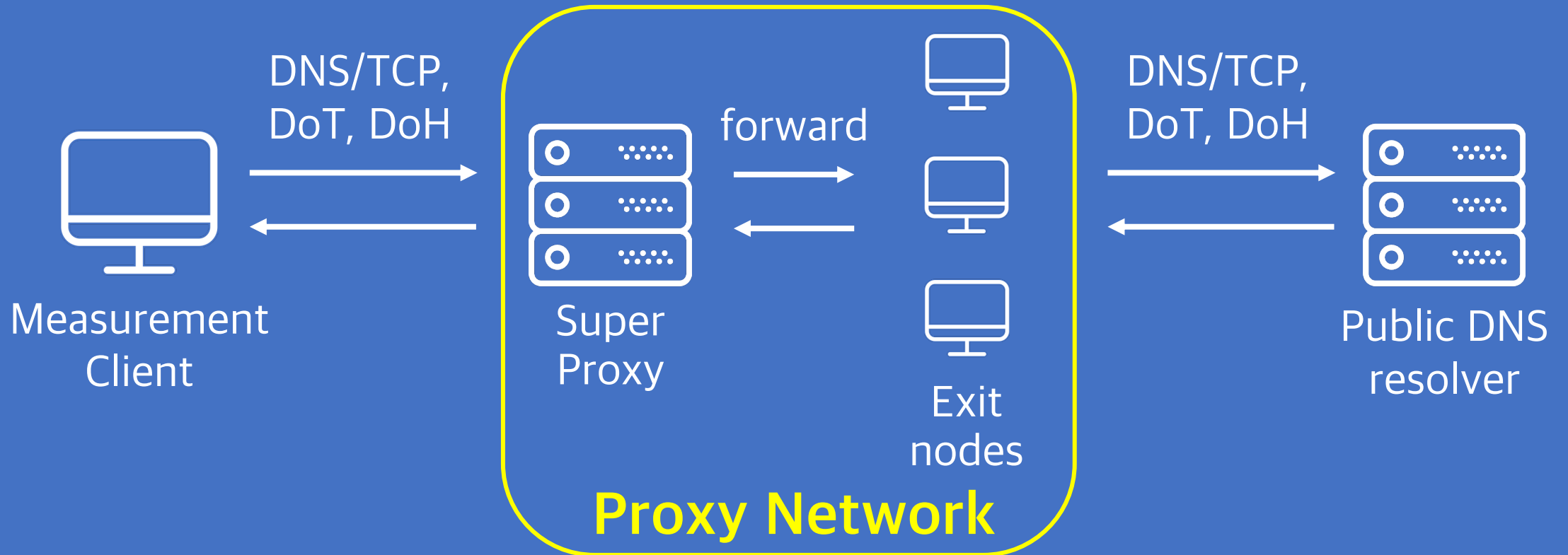Jul '20: **50+ URIs operated by 37 providers.** ⬆

Examples:

https://doh.360.cn/dns-query   https://1111.cloudflare-dns.com/dns-query

https://dohtrial.att.net/dns-query   https://8888.google/dns-query

https://public.dns.iij.jp/dns-query   https://doh.defaultroutes.de/dns-query

https://doh.xfinity.com/dns-query   https://ns-doh.licoho.de/dns-query

Q2:
Are popular services reachable?

Reachability to DoE Servers

Measurement platform built on SOCKS5 proxy network.

Measurement Client

DNS/TCP, DoT, DoH

Super Proxy

forward

Exit nodes

Proxy Network

DNS/TCP, DoT, DoH

Public DNS resolver

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?

Why do they fail?

1.1.1.1

8.8.8.8

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

TLS 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 hijacked, 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 route hijacking:

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**.
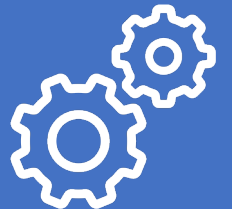
Specification

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

Implementation

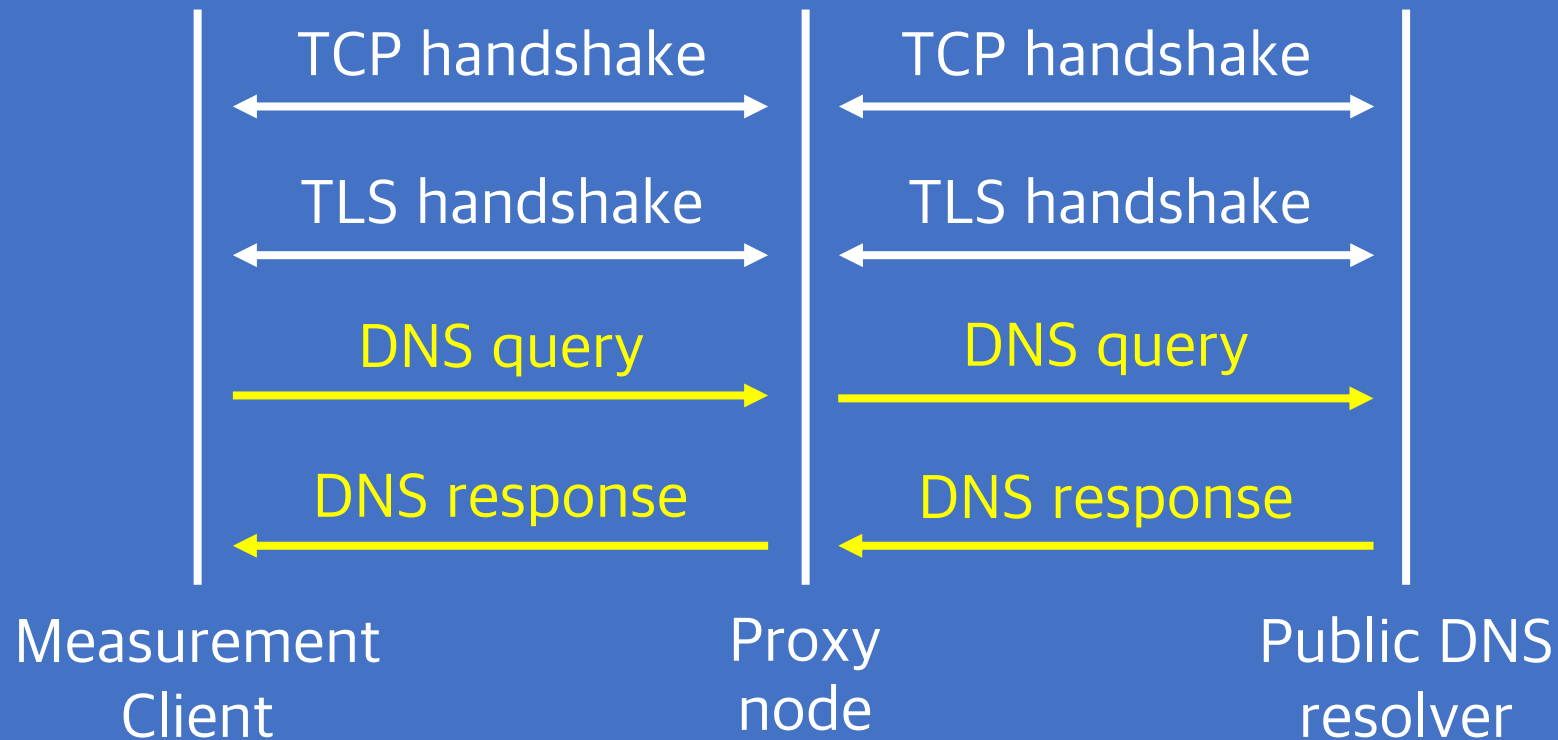Stub: supported by dig, kdig, Stubby, etc.

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

DoE lookup performance
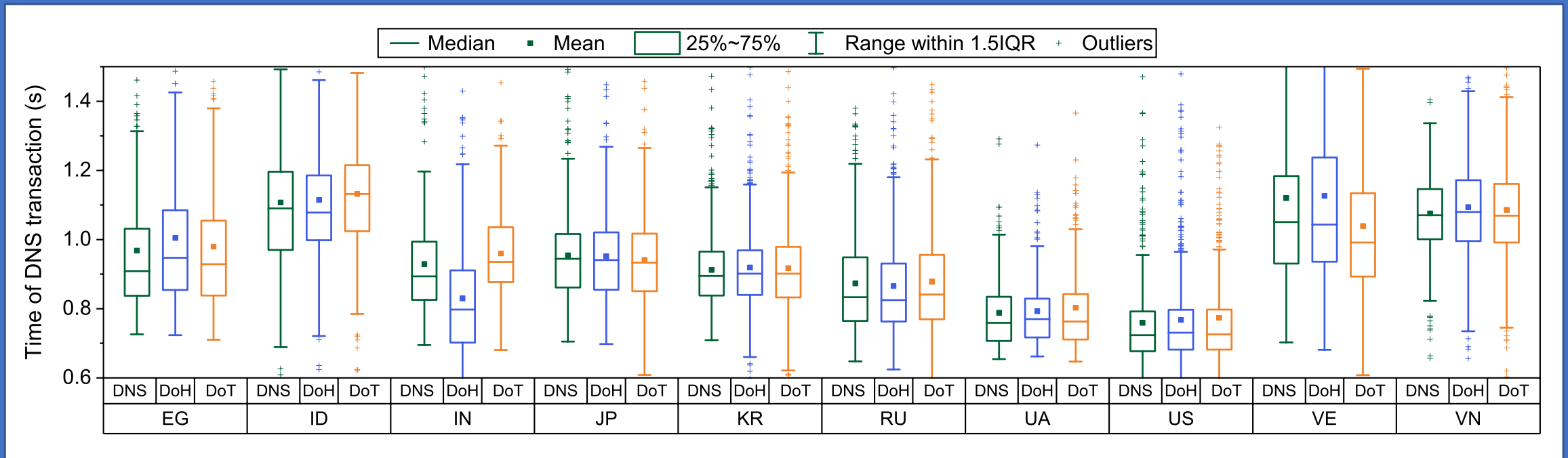
Vantage point: 8,257 proxy nodes from ProxyRack.

Connection reuse: only recording DNS transaction time.

	TCP handshake		TCP handshake	
	TLS handshake		TLS handshake	
	DNS query		DNS query	
	DNS response		DNS response	

Measurement Client

Proxy node

Public DNS resolver

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
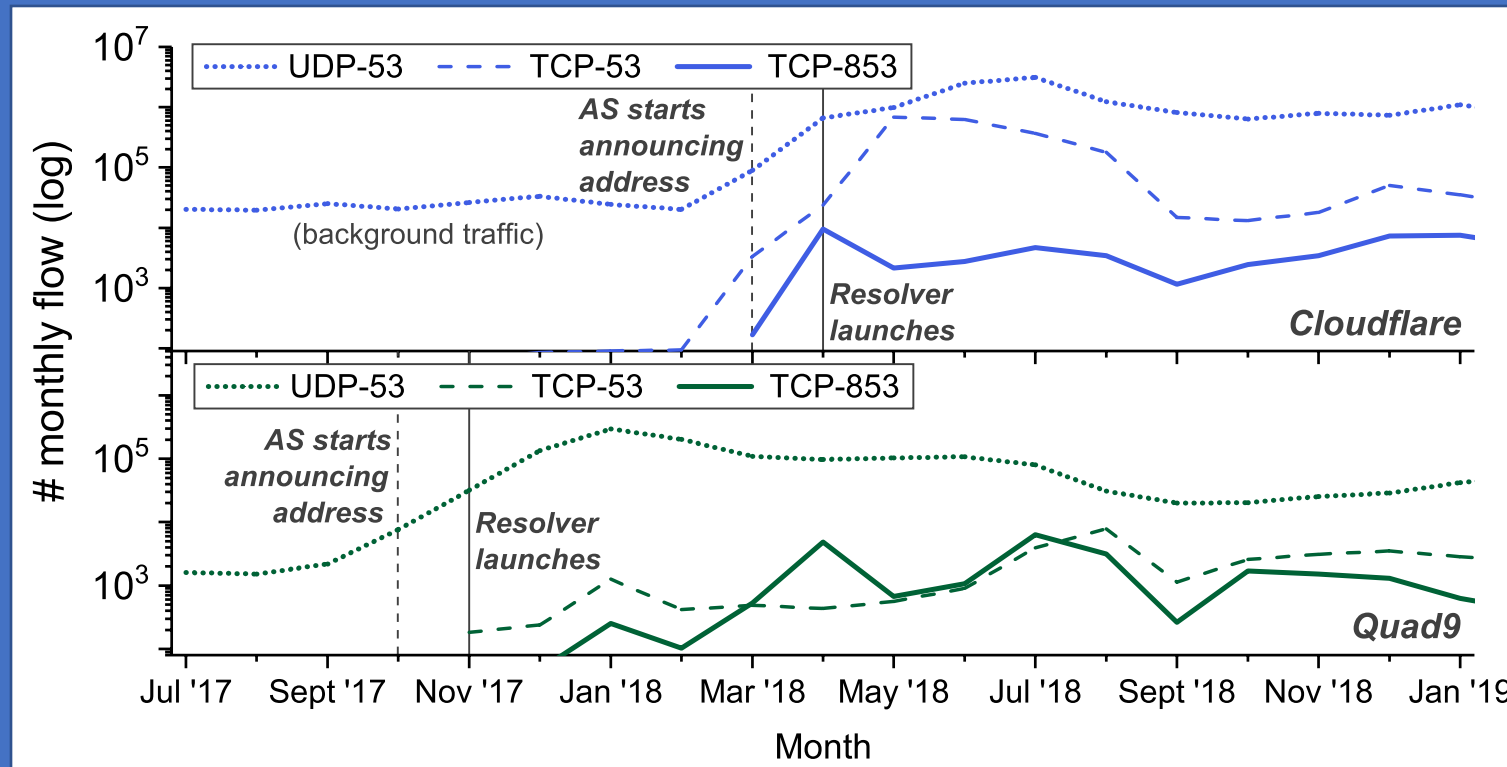dataset**

DNS-over-HTTPS (DoH)

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

↓

**Passive DNS
dataset**

DNS-over-TLS Traffic

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

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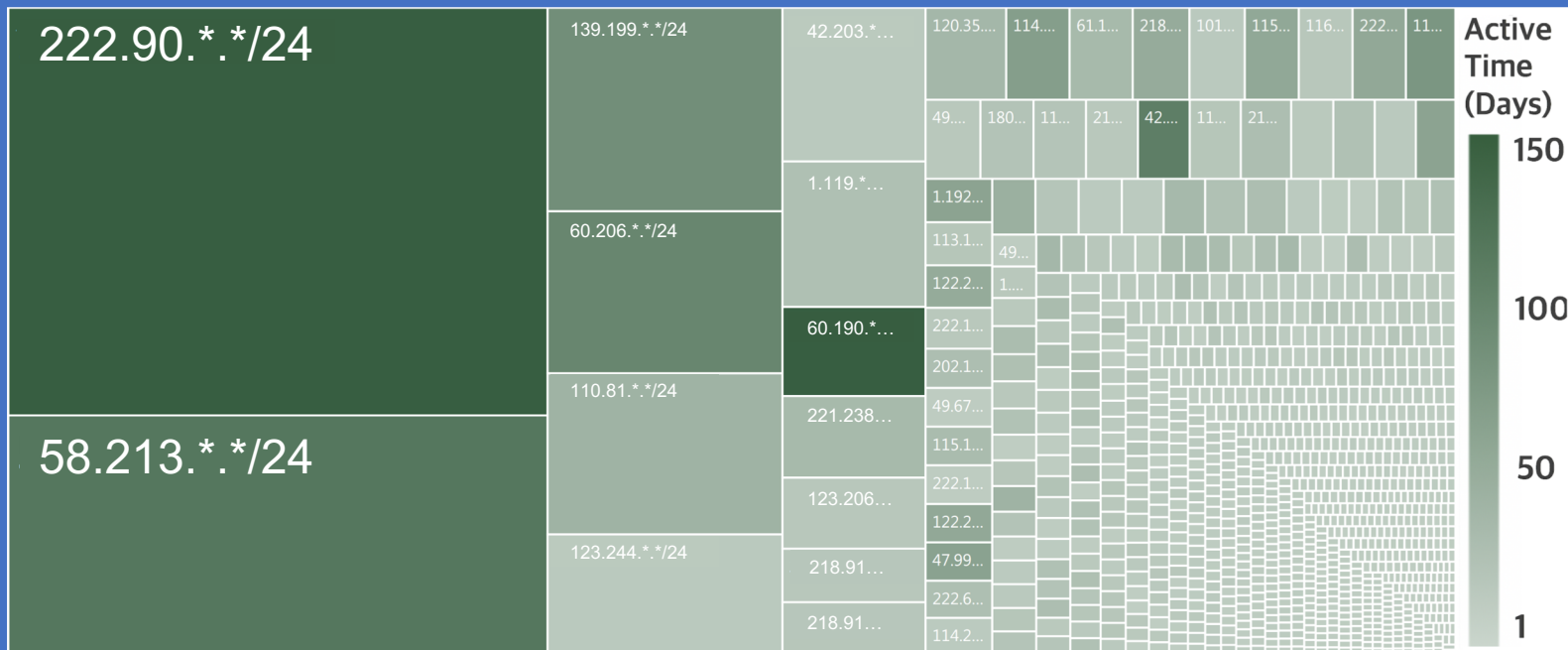

DoT:
2 to 3 orders
of magnitude
less traffic
(Early 2019)

DNS-over-TLS Traffic

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

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

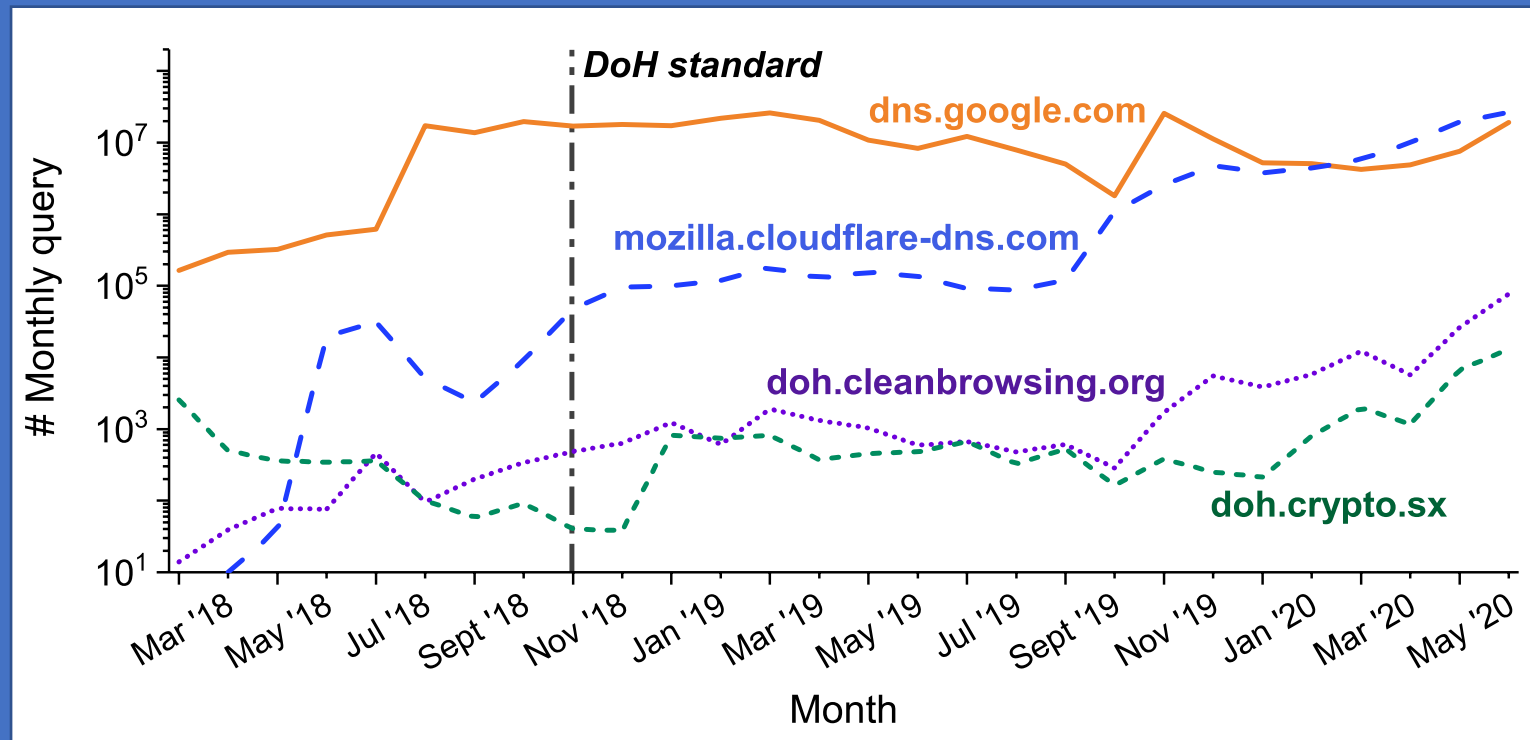Clients: centralized clients + temp users.

Top 20 netblocks:
> 60% DoT traffic

> 95% netblocks:
Active for < one week
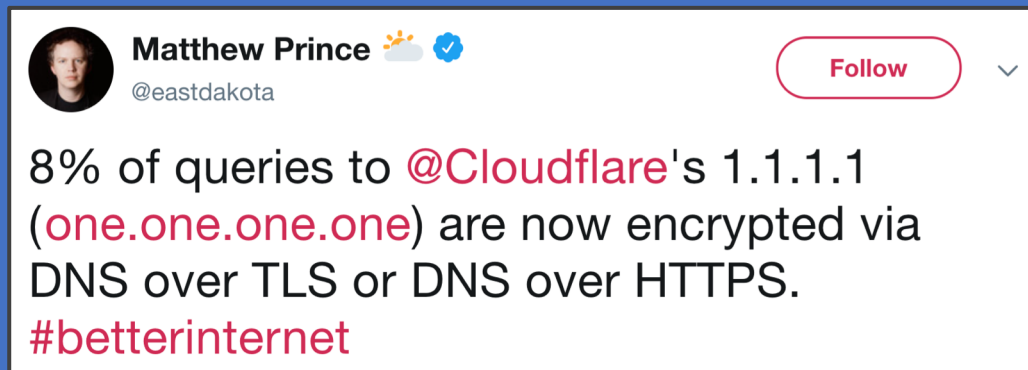
DNS-over-HTTPS Traffic

Data: Passive DNS dataset, monthly query volume.

Big players dominate. Also a growing trend.

Traffic Observed by DNS Providers

DoT and DoH usage has grown significantly.

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% of its queries are encrypted (May 2019)

360安全DNS

Qihoo 360:
360 DoH used by 1.2M clients
(July 2020)

Recommendation

Protocol designers

Reuse well-developed protocols.

Service providers

Correct misconfigurations.

Keep servers under regular maintenance.

DNS clients

Education on benefits of encryption.

Dataset & code release

Please visit https://dnsencryption.info.

Summary: Key Observations

Open DNS-over-Encryption resolvers
A number of small providers less-known.
~28% resolvers use invalid TLS certificates.

Client-side usability
Currently good reachability (~99%).
Tolerable performance overhead with reused connections.

Real-world traffic
Has been growing significantly.

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

University of California, Irvine

UT DALLAS
The University of Texas at Dallas

Netlab 360.com