IMC 2019: AN END-TO-END, LARGE-SCALE MEASUREMENT OF DNS-OVER-ENCRYPTION: HOW FAR HAVE WE COME?

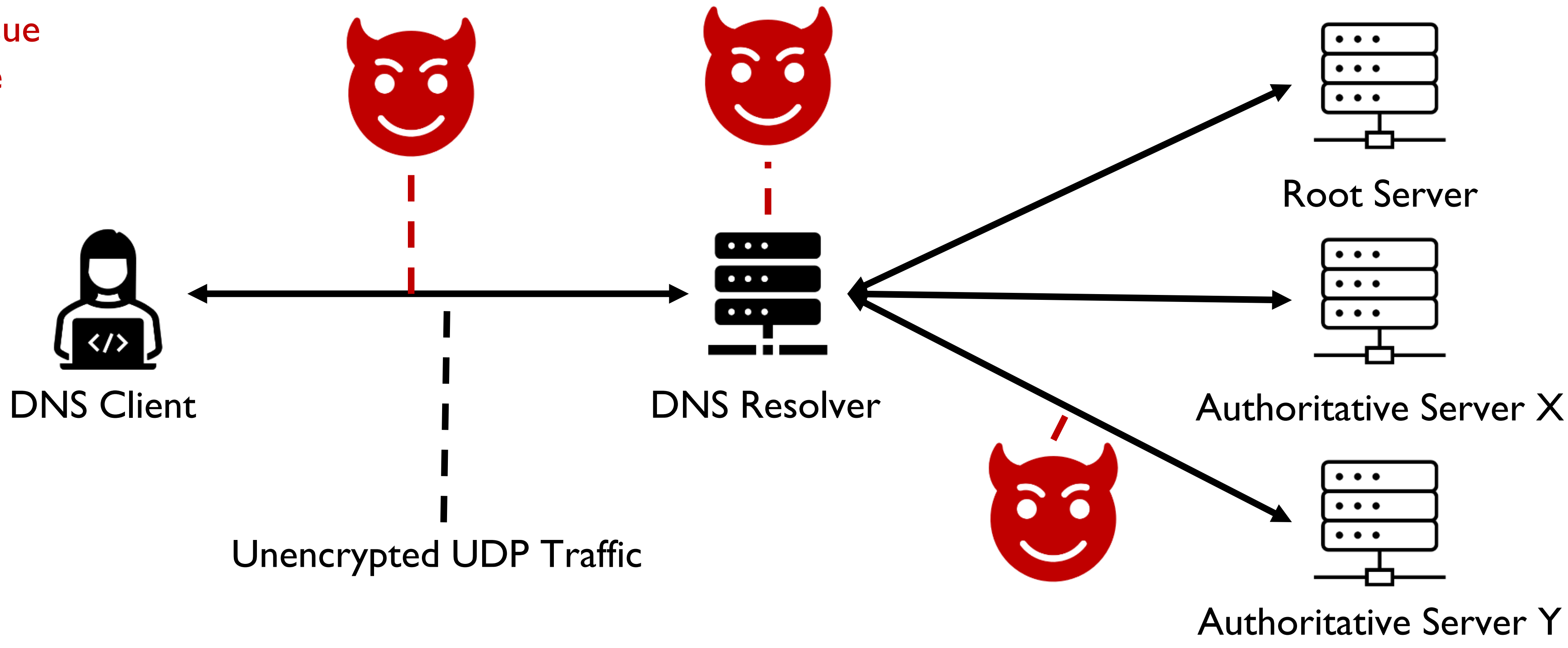
ORIGINAL AUTHORS: CHAOYI LU + 9

PAPER SUMMARY PRESENTATION BY LAM YONGXIAN

BACKGROUND

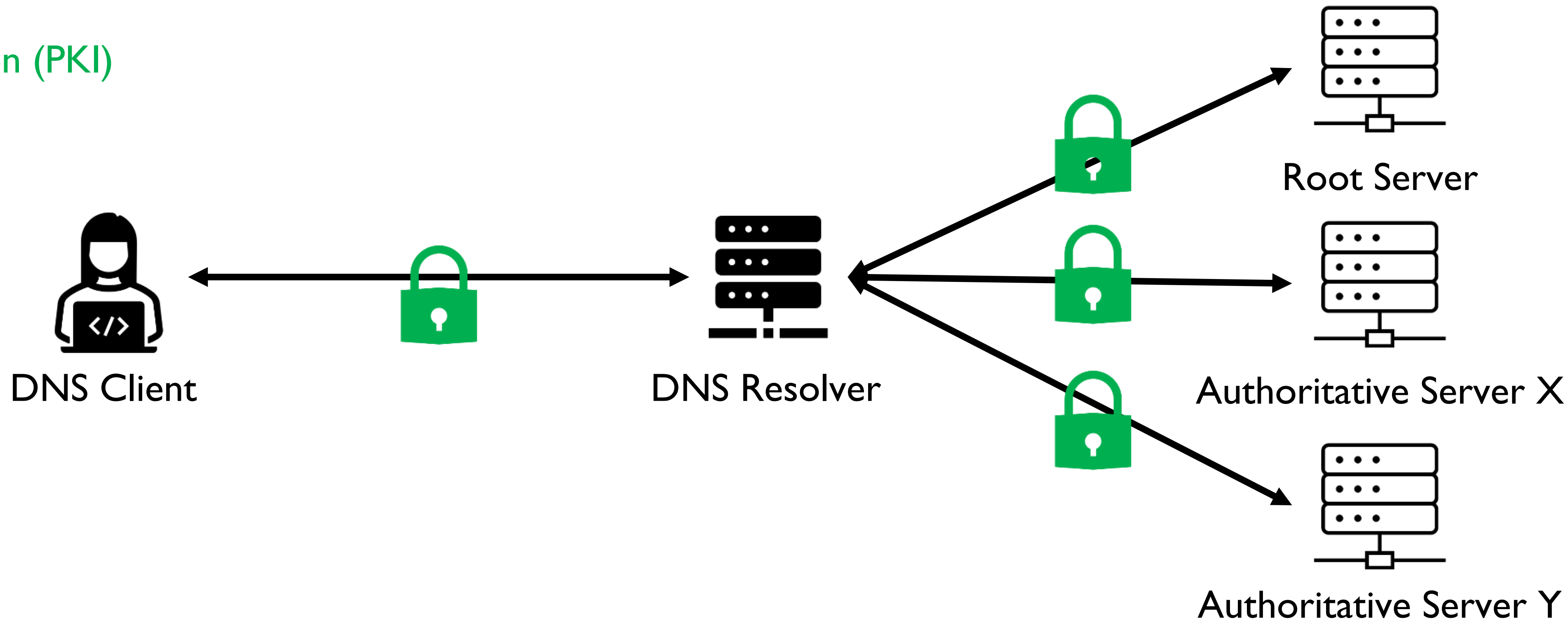
BACKGROUND: DNS ARCHITECTURE

- Confidentiality Issue
- Authenticity Issue



BACKGROUND: DNS OVER ENCRYPTION

- DNS Encryption
- SSL Authentication (PKI)



BACKGROUND: DNS OVER ENCRYPTION PROTOCOLS

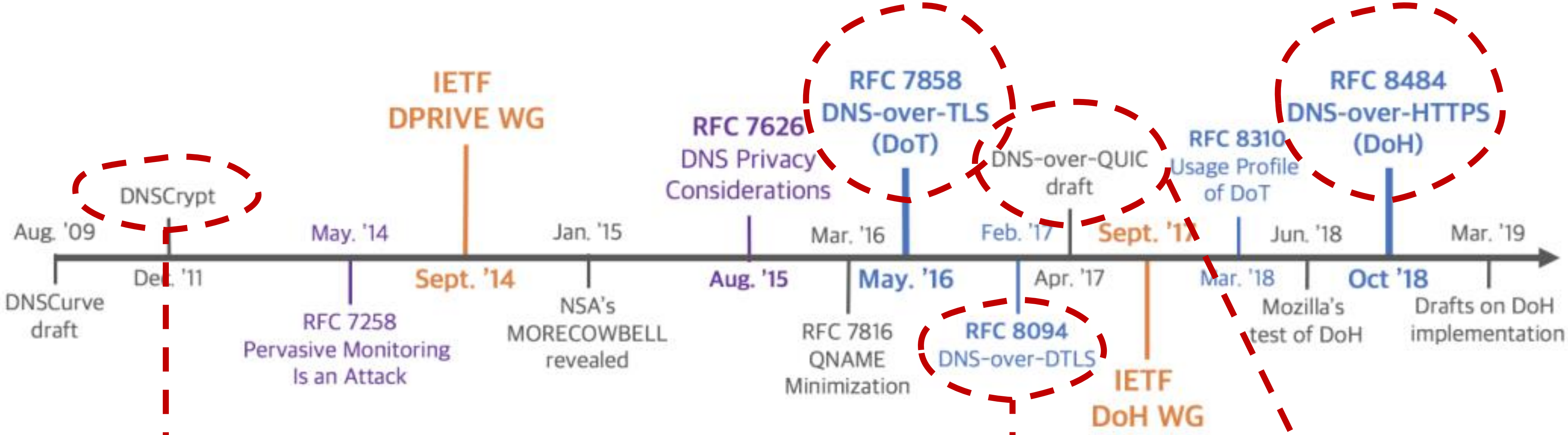


Figure 1: Timeline of important DNS privacy events, including DNS-over-Encryption standards (blue), IETF WGs (orange), Informational RFC and Best Common Practice (purple).

- Installed on client
- Route DNS traffic over proxy

- Over UDP version of TLS
- Fallback for DoT

- Replacing TCP/UDP
  Built-in encryption

BACKGROUND: DOE STANDARDIZED PROTOCOLS

- Runs on Port 853
- Require update to resolvers
- Strict Privacy or Opportunistic (Non-auth/encrypted fallback)

- Runs on Port 443 (HTTPS)
- Embed DNS queries into HTTPS messages
- Requires both encryption and authentication

BACKGROUND: DOE STANDARDIZED PROTOCOLS

- **DNS-over-TLS**
  using kdig shell command

```
$ 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
```

- **DNS-over-HTTPS**
  via browser http request

```
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"}]}
```

BACKGROUND: EVALUATION CRITERIA

Table 1: Comparison of different DNS-over-Encryption protocols

Category	Criterion	DNS-over-TLS	DNS-over-HTTPS	DNS-over-DTLS	DNS-over-QUIC	DNSCrypt
Protocol Design	Uses other application-layer protocols	○	●	○	○	●
	Provides fallback mechanism	●	○	●	●	○
Security	Uses standard TLS	●	●	●	●	○
	Resists DNS traffic analysis	◐	●	◐	◐	●
Usability	Minor changes for client users	◐	●	○	○	◐
	Minor latency above DNS-over-UDP	◐	◐	●	●	◐
Deployability	Runs over standard protocols	●	●	●	○	○
	Supported by mainstream DNS software	●	◐	○	○	◐
Maturity	Standardized by IETF	●	●	●	○	○
	Extensively supported by resolvers	●	●	○	○	◐

- Scope of study focuses on **DNS-over-TLS** and **DNS-over-HTTPS**

BACKGROUND: DOE CLIENT-SIDE (MAY 2019)

Table 8: Current implementations of DNS-over-Encryption (last updated on May 1, 2019).

		DoT	DoH	DC	Since Ver.
Browser	Firefox		✓		Firefox 62.0
	Chrome		✓		Chromium 66
	IE				
	Safari				
	Opera				
	Yandex			✓	
	Tenta	✓	✓		Tenta v2
OS	Android	✓			Android 9
	Linux (systemd)	✓			systemd 239
	Windows				
	macOS				

[1] DoE is short for DNS-over-Encryption. DC is short for DNSCrypt. QM is short for QNAME minimization.
[2] DNS-over-DTLS and DNS-over-QUIC do not have implementations yet.
[3] All surveyed software is the latest version at the last update (May 1, 2019).
[4] For OS, we only consider built-in support.

BACKGROUND: DOE RESOLVER SOFTWARES (MAY 2019)

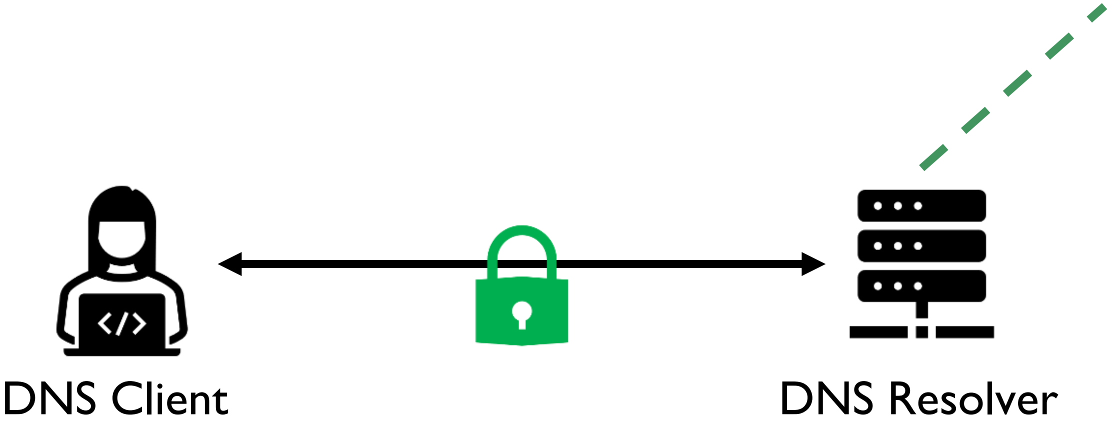


Table 8: Current implementations of DNS-over-Encryption (last updated on May 1, 2019).

Category	Name	DoE			Others	
		DoT	DoH	DC	DNSSEC	QM
DNS Software (Server)	Unbound	✓		✓	✓	✓
	BIND				✓	✓
	Knot Res	✓	✓		✓	✓
	dnsdist	✓	✓	✓	✓	
	CoreDNS	✓			✓	
	AnswerX				✓	
	Cisco Registrar					
	MS DNS				✓	
DNS Software (Stub)	Ldns (drill)				✓	–
	Stubby	✓			✓	–
	BIND (dig)				✓	–
	Go DNS			✓		–
	Knot (kdig)	✓			✓	–

BACKGROUND: DOE ON PUBLIC DNS (MAY 2019)

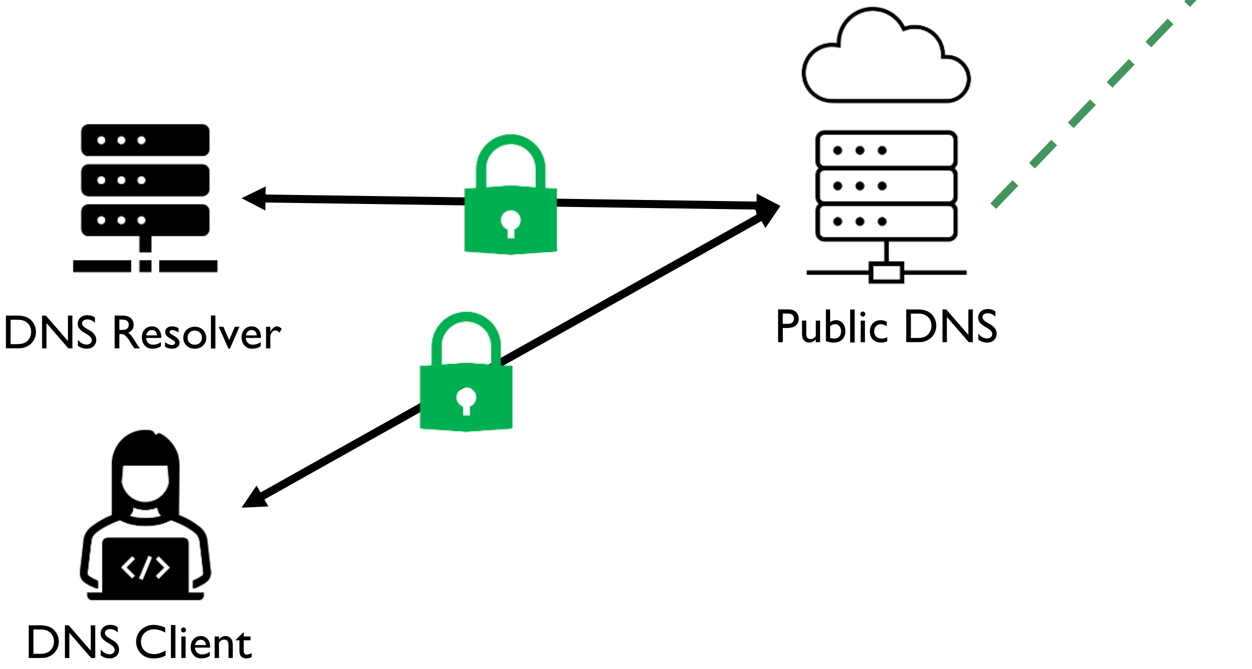


Table 8: Current implementations of DNS-over-Encryption (last updated on May 1, 2019).

Category	Name	DoE			Others	
		DoT	DoH	DC	DNSSEC	QM
Public DNS	Google	✓	✓		✓	
	Cloudflare	✓	✓		✓	✓
	Quad9	✓	✓	✓	✓	
	OpenDNS			✓		
	CleanBrowsing	✓	✓	✓		
	Tenta	✓	✓		✓	
	Verisign				✓	
	SecureDNS	✓	✓	✓	✓	
	DNS.WATCH				✓	
	PowerDNS		✓		✓	
	Level3				✓	
	SafeDNS				✓	
	Dyn				✓	
	BlahDNS	✓	✓	✓	✓	
	OpenNIC			✓	✓	
	Alternate DNS				✓	
	Yandex.DNS			✓	✓	

SERVERS

TO *OFFER* DNS-OVER-ENCRYPTION

Discovering open DNS-over-TLS resolvers

- Scan over Port 853 using **ZMap**
- Internet wide scan
- Query over **getdns**
- Verify SSL certificate chain using **OpenSSL**

Limitations

- Only open resolvers, not local ones deployed by ISPs
- Local deployment scarce among ISPs (~0.3% for researcher's own domain)

SERVERS: METHODOLOGY

Discovering open DNS-over-HTTPS resolvers

- URI templates on large datasets
- Common path templates (e.g., /dns-query and /resolve)

Limitations

- Unknown URL patterns will be overlooked

SERVERS: METHODOLOGY

SERVERS: KEY OBSERVATION 1

"Except for large providers, there are many small providers which are less-known and missed by the public resolver lists. However, a quarter of DoT providers use invalid SSL certificates on their resolvers, which exposes their users to security risks."

Finding 1.1: 1.5K open **DoT resolvers** are mostly owned by large providers, but there are also ones run by small providers which are absent from public resolver lists. By contrast, the number of open **DoH resolvers is small**.

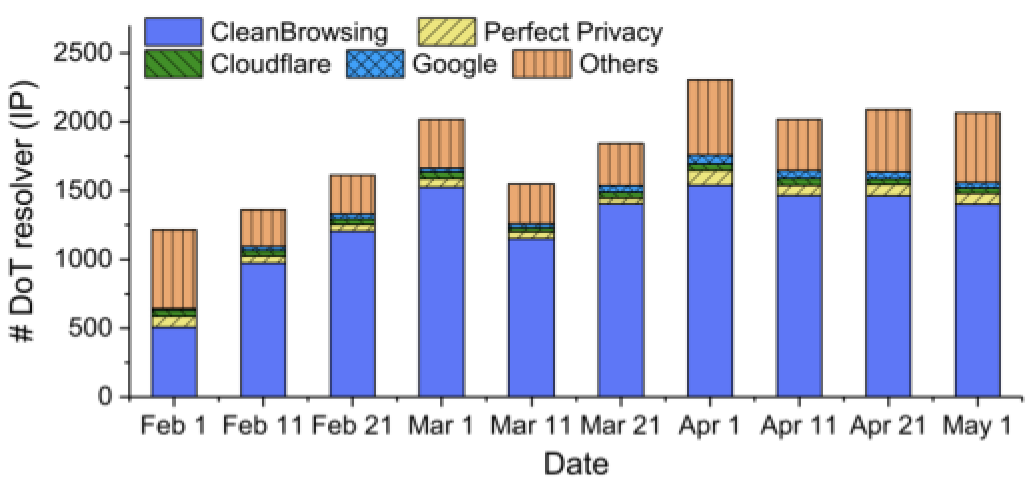
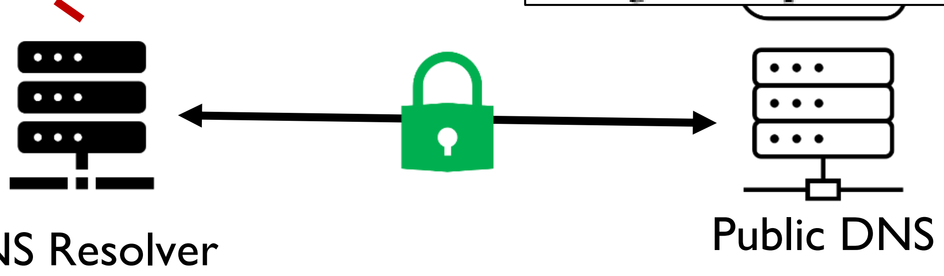


Figure 3: Open DoT resolvers identified by each scan

~17 public DoH resolvers



SERVERS: KEY OBSERVATION 1

"Except for large providers, there are many small providers which are less-known and missed by the public resolver lists. However, a quarter of DoT providers use invalid SSL certificates on their resolvers, which exposes their users to security risks."

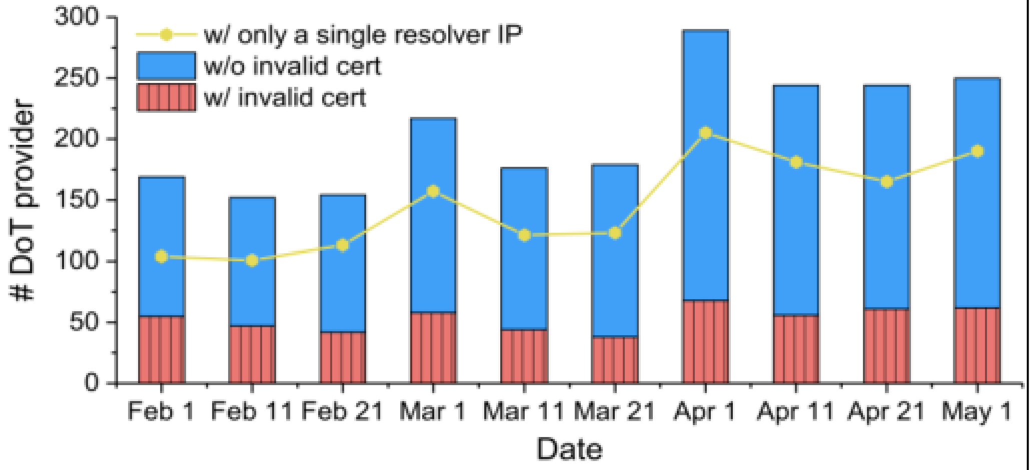
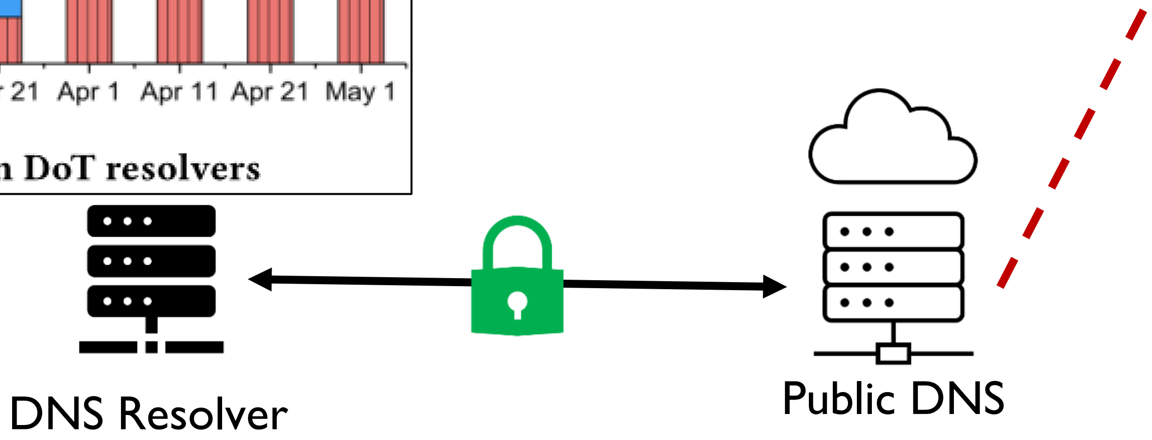


Figure 4: Providers of open DoT resolvers

Finding 1.2: 25% providers own **DoT resolvers** equipped with **invalid SSL certificates**, including a large provider and TLS inspection devices. By contrast, **public DoH servers** have **good maintenance of certificates**.



CLIENTS

TO *USE* DNS-OVER-ENCRYPTION

Measurement of Reachability

- SOCK5 Measurement Platform
- ~114000 vantage points globally
- DoT, DoH, and DNS-over-TCP query on 3 public resolvers

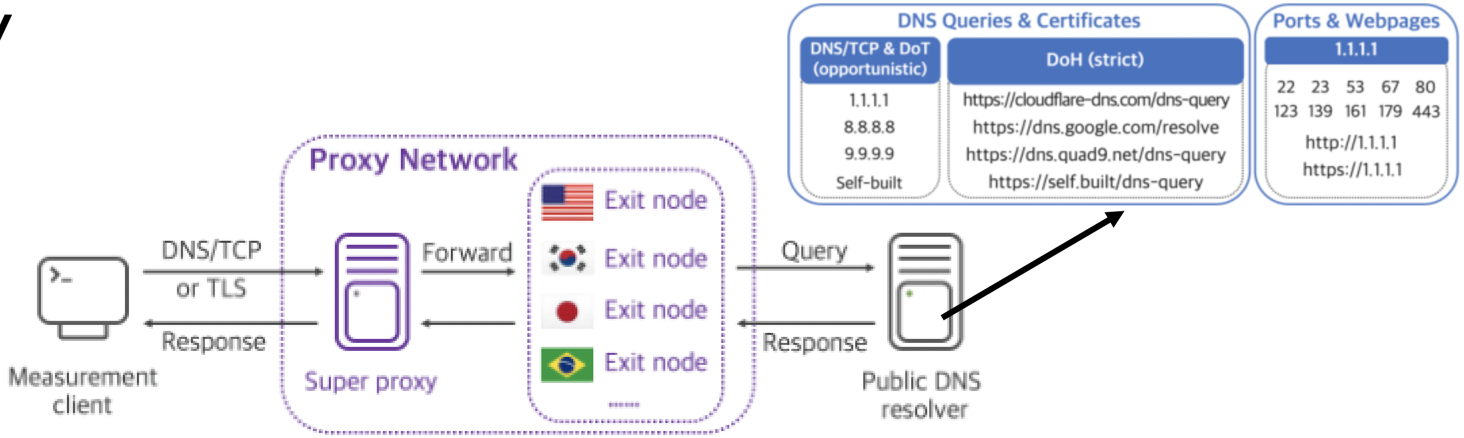


Figure 5: Proxy network architecture

Limitations

Table 3: Evaluation of client-side dataset

Test	Platform	# Distinct IP	# Country	# AS
Reachability	ProxyRack (Global)	29,622	166	2,597
	Zhima (Censored)	85,112	1 (CN)	5

- Researcher's Proxy Network only allows TCP Traffic

CLIENTS: METHODOLOGY

CLIENTS: KEY OBSERVATION 2

"Over 99% global users can normally access large DNS-over-Encryption servers, whilst less than 1% clients are experiencing problems caused by IP conflict, censorship and TLS interception."

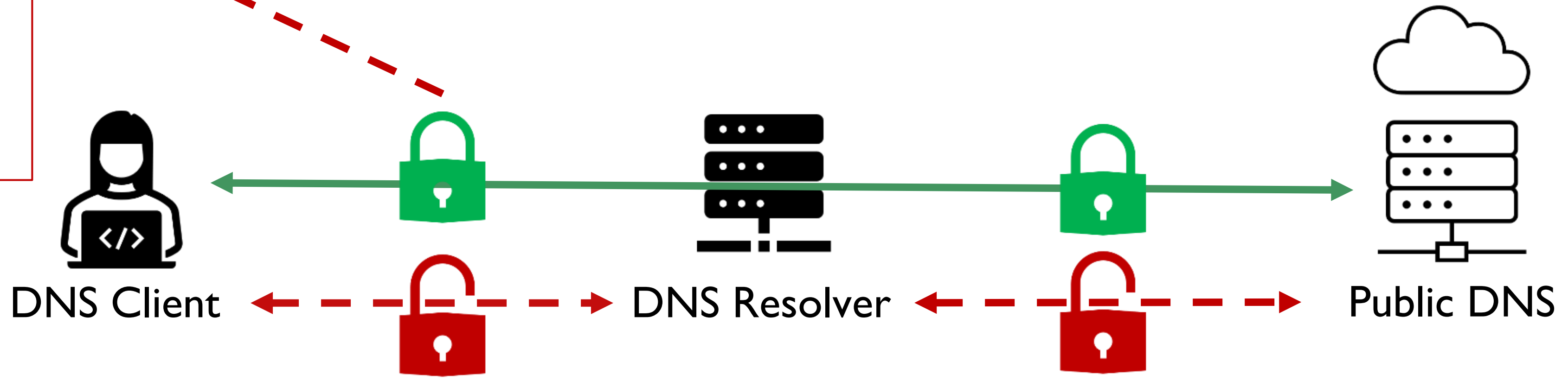
Finding 2.1: Compared to traditional DNS, large DNS-over-Encryption services are **less affected by in-path devices**, with 99% global reachability.

Finding 2.4: A configuration issue of **Quad9 DoH** potentially causes unnecessary query failures for their clients.

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.

Finding 2.2: Censorship blocks users in China from Google DoH.



CLIENTS: KEY OBSERVATION 2

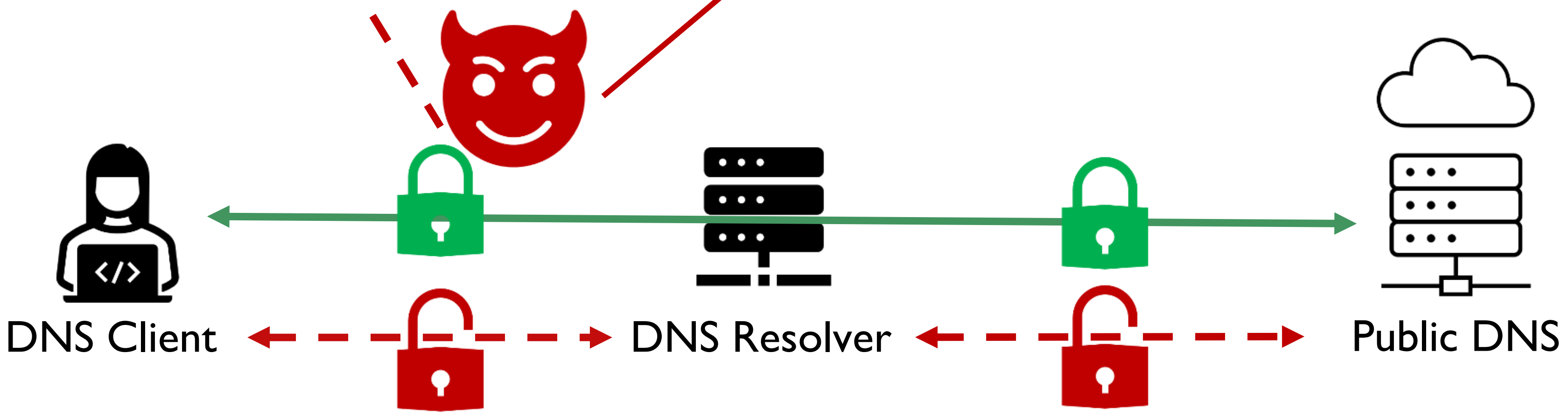
"Over 99% global users can normally access large DNS-over-Encryption servers, whilst less than 1% clients are experiencing problems caused by IP conflict, censorship and TLS interception."

Finding 2.3: While not pervasive yet, TLS interception breaks opportunistic DoT.

MITM: Resolver cert re-signed by untrusted CA

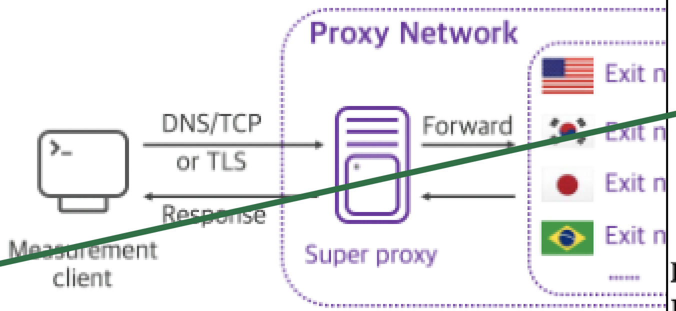
Table 6: Example clients affected by TLS interception

Client IP	Country	Common Name of untrusted CA	Port 443	Port 853
202.123.177.*	LA	SonicWall Firewall DPI-SSL	✓	✓
98.186.202.*	US	"None"	✓	
177.133.9.*	BR	Sample CA 2	✓	✓
5.18.250.*	RU	NThmYzgyYT 2	✓	✓
60.48.98.*	MY	c41618c762bf890f 2	✓	✓



Measurement of Performance

- 8257 proxy nodes
- Relative performance overhead between DNS-over-Encryption and DNS
- Assumption: Connection reuse, only measure DNS transaction time



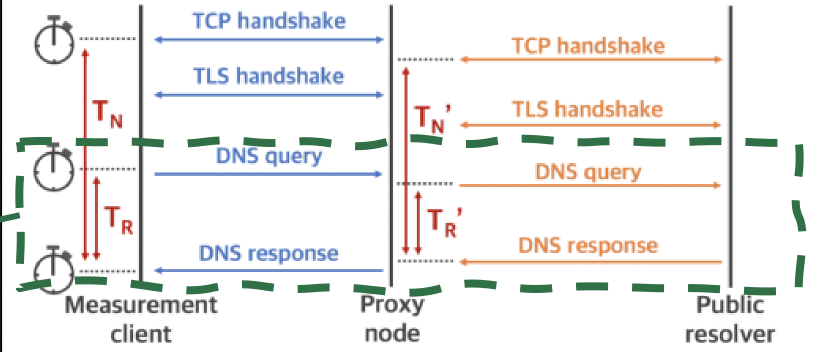


Figure 8: DNS queries via proxy networks for DoT and DoH. DNS/TCP includes all but the TLS handshake.

Figure 5: Proxy network architecture

Limitations

- TCP only. Does not measure DNS-over-UDP and reusing connection is not possible under UDP.

Table 3: Evaluation of client-side dataset

Test	Platform	# Distinct IP	# Country	# AS
Performance	ProxyRack (Global)	8,257	132	1,098

"DNS/TCP has equivalent performance to DNS/UDP with reused connections…"

CLIENTS: METHODOLOGY

CLIENTS: KEY OBSERVATION 3

"When connection is reused, encrypting DNS transactions introduces a **tolerable overhead** on query latency for global clients, and can perform well as clear-text DNS."

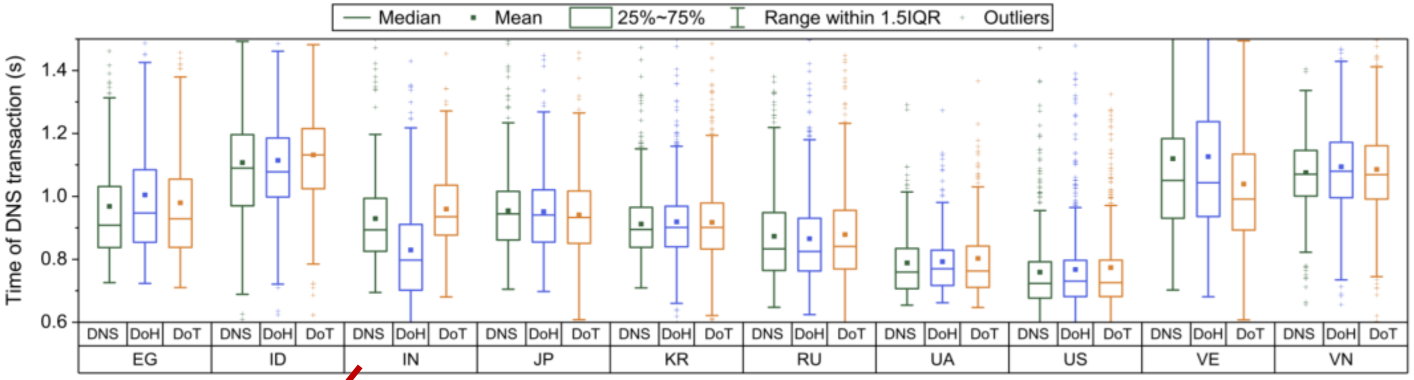
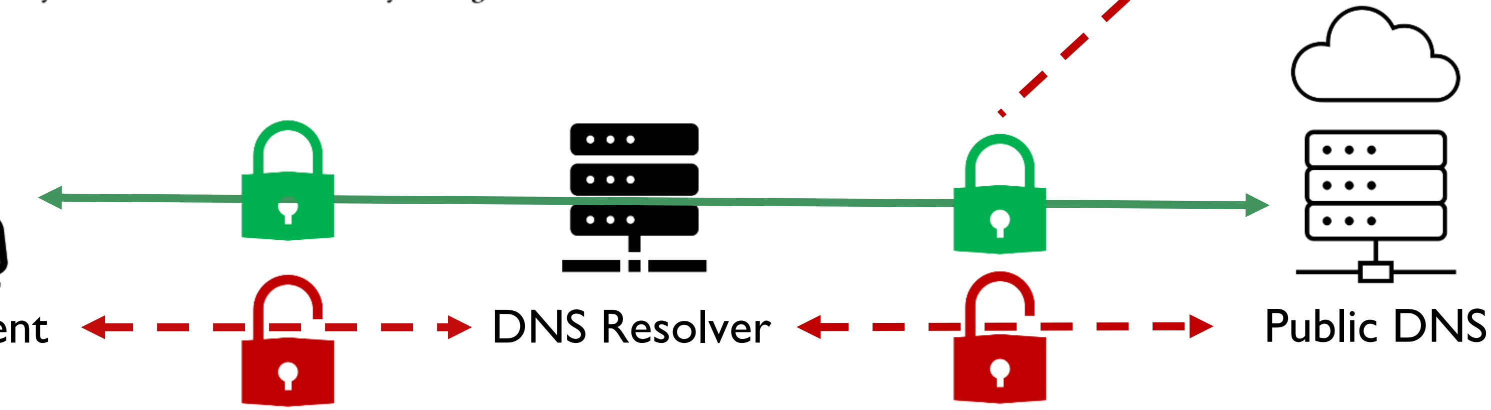


Figure 9: Query performance per country. The countries are selected by having most of our clients.

Finding 3.1: On average, query latency of encrypted DNS with reused connection is **several milliseconds longer** than traditional lookups.

Finding 3.2: Performance of DNS-over-Encryption services fluctuates in different countries.



USAGE

DNS-OVER-ENCRYPTION TRAFFIC

Observing DNS-over-TLS traffic

- Uses Port 853
- 18-month NetFlow dataset between Jul 2017 to Jan 2019
- Collected by the backbone routers of a large Chinese ISP
- Dataset scanned by **NetworkScan Mon** and not generated by automated scanners

Limitations

- Passive datasets contain geographical bias

USAGE: METHODOLOGY

USAGE: KEY OBSERVATION 4 (DOT)

"Although still at a small scale compared to traditional DNS, real-world traffic to DNS-over-Encryption services is observed, and reflects a **growing usage** in recent months."

"the top five netblocks account for 44% of all DoT traffic, and the **top 20 account for 60%**"

"(96%) netblocks are only active **for less than one week**"

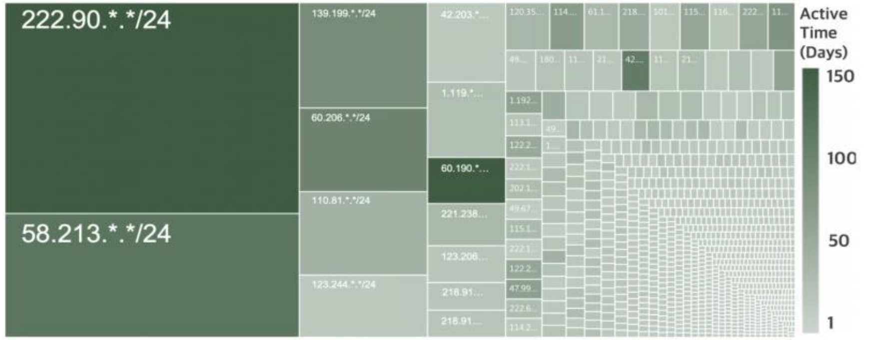


Figure 12: DoT traffic to Cloudflare DNS per /24 network. The size indicates the proportion of DoT traffic, and the color shows the active time of each network.

Finding 4.1: DoT traffic to large public resolvers is still at a small scale, mostly coming from both **centralized clients** and **temporary users**.

DNS Client

USAGE: KEY OBSERVATION 4 (DOT)

"Although still at a small scale compared to traditional DNS, real-world traffic to DNS-over-Encryption services is observed, and reflects a **growing usage** in recent months."

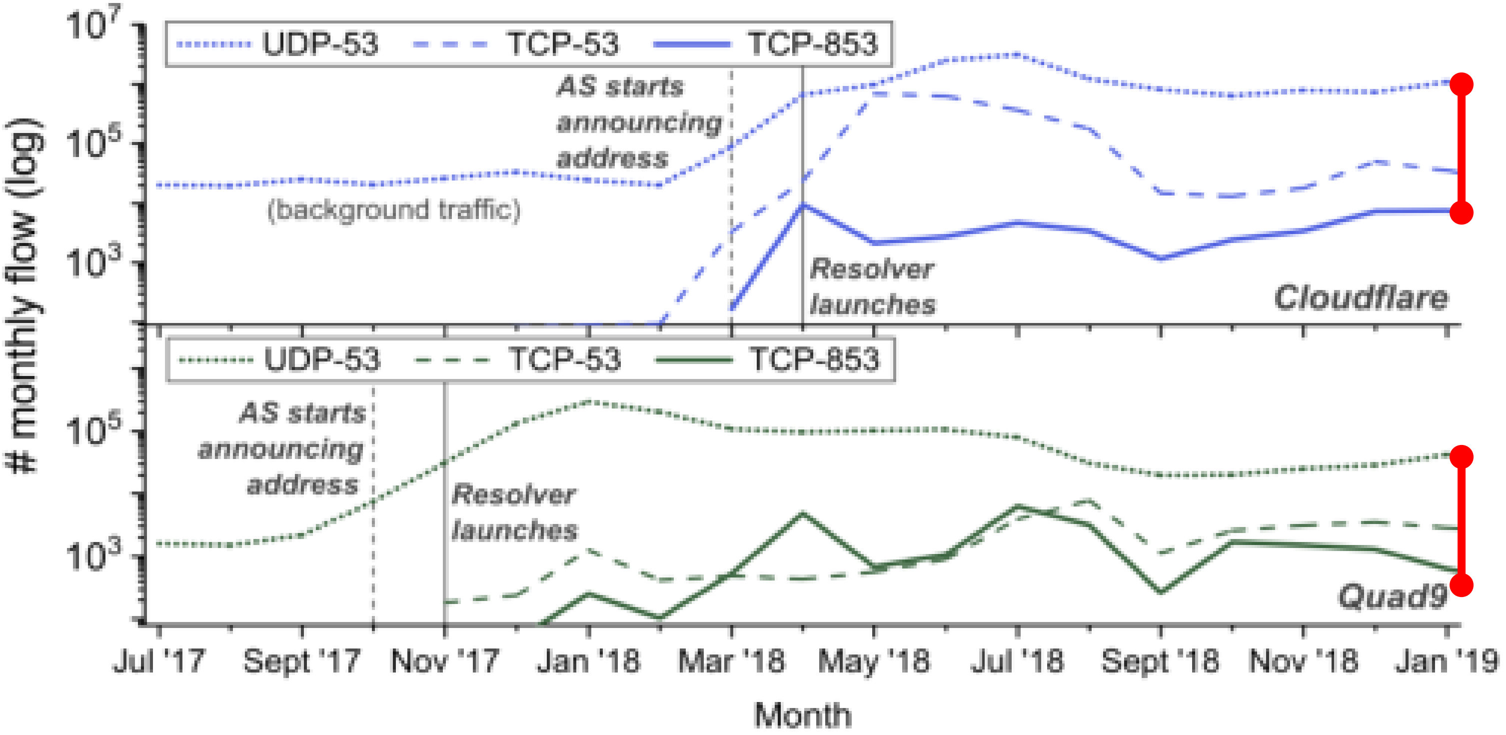


Figure 11: Traffic to Cloudflare and Quad9 DNS

"about 2-3 orders of magnitude less than traditional DNS…"

Observing DNS-over-HTTPS traffic

- DNSDB and 360 PassiveDNS are two large passive DNS
- Datasets maintained by Farsight Security and Qihoo 360 respectively

Limitations

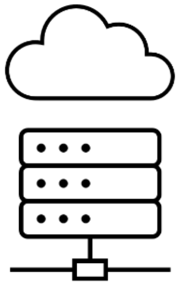
- Passive datasets contain geographical bias
- Underestimating the query volume due to DNS Caching

USAGE: METHODOLOGY

USAGE: KEY OBSERVATION 4 (DOH)

"Although still at a small scale compared to traditional DNS, real-world traffic to DNS-over-Encryption services is observed, and reflects a **growing usage** in recent months."

Finding 4.2: **Large providers** dominate in all DoH services, and their **usage is growing**.



Public DNS

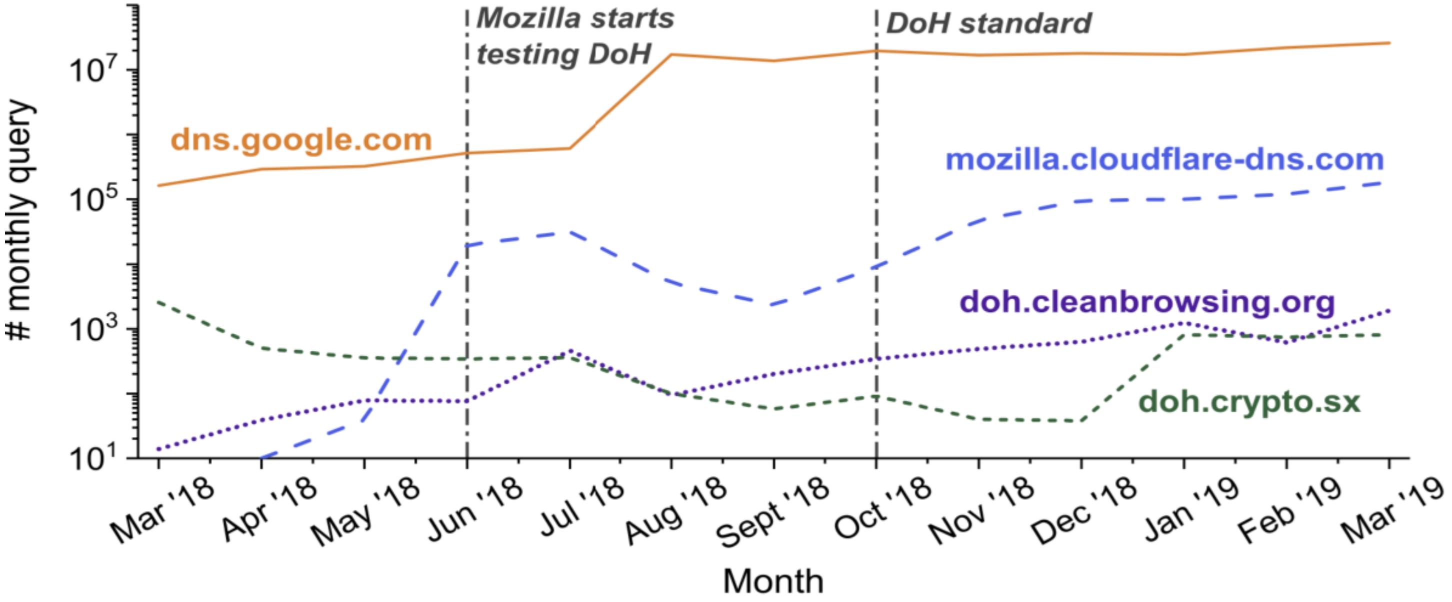
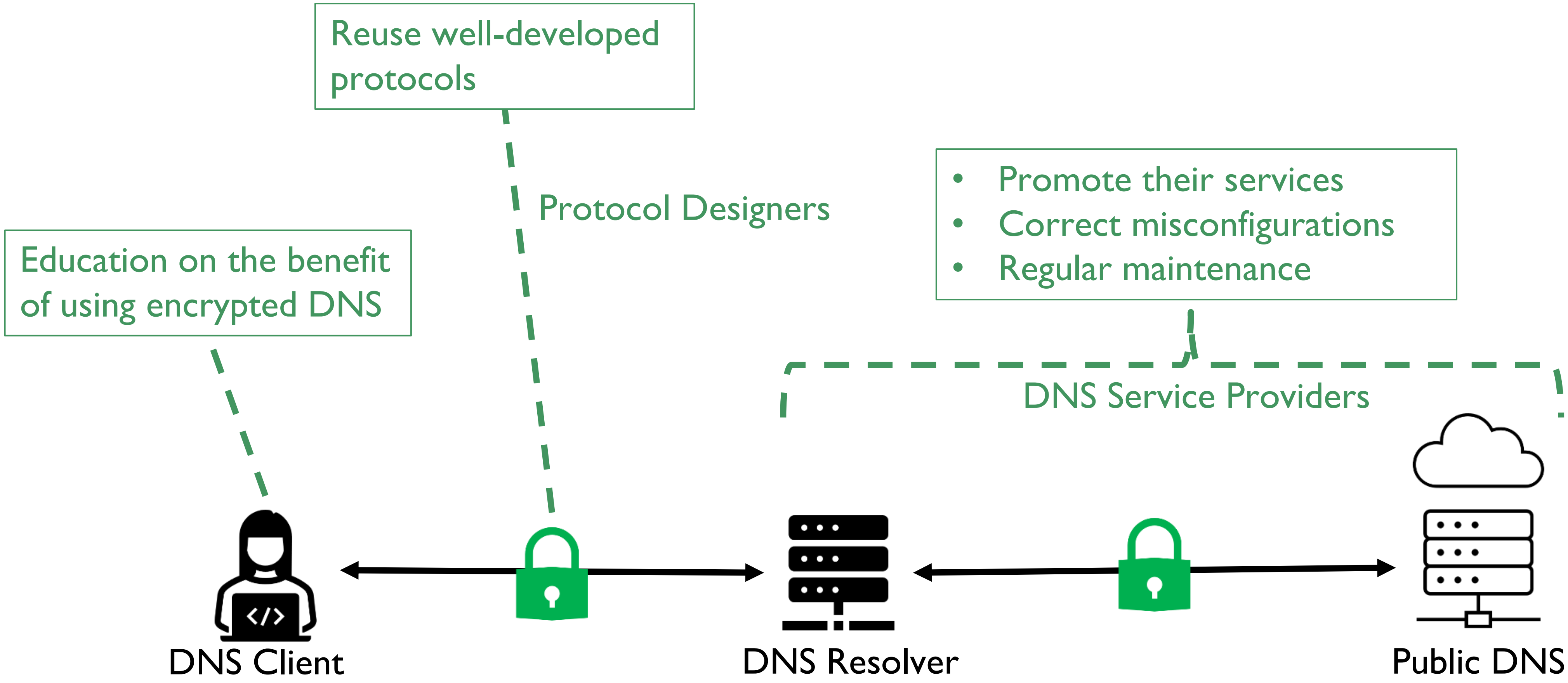


Figure 13: Query volume of popular DoH domains

DISCUSSION

ALMOST…

DISCUSSION: RECOMMENDATIONS



Dataset & code release

https://dnsencryption.info/imc19-doe.html

DNS Research @ Tsinghua

IMC2019 Video & Slides

https://chaoyi.lu/publications.html

RESOURCES

THANK YOU

LAMYONGXIAN@U.NUS.EDU