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

Chaoyi Lu[1,2], Baojun Liu[3], Zhou Li[4], Shuang Hao[5], Haixin Duan[1,2,6], Mingming Zhang[1], Chunying Leng[1], Ying Liu[1], Zaifeng Zhang[7] and Jianping Wu[1]
[1]Institute for Network Sciences and Cyberspace, Tsinghua University
[2]Beijing National Research Center for Information Science and Technology (BNRist), Tsinghua University
[3]Department of Computer Science and Technology, Tsinghua University [4]University of California, Irvine
[5]University of Texas at Dallas [6]Qi An Xin Technology Research Institute [7]360 Netlab

ABSTRACT

DNS packets are designed to travel in unencrypted form through the Internet based on its initial standard. Recent discoveries show that real-world adversaries are actively exploiting this design vulnerability to compromise Internet users' security and privacy. To mitigate such threats, several protocols have been proposed to encrypt DNS queries between DNS clients and servers, which we jointly term as DNS-over-Encryption. While some proposals have been standardized and are gaining strong support from the industry, little has been done to understand their status from the view of global users.

This paper performs by far the first end-to-end and large-scale analysis on DNS-over-Encryption. By collecting data from Internet scanning, user-end measurement and passive monitoring logs, we have gained several unique insights. In general, the service quality of DNS-over-Encryption is satisfying, in terms of accessibility and latency. For DNS clients, DNS-over-Encryption queries are less likely to be disrupted by in-path interception compared to traditional DNS, and the extra overhead is tolerable. However, we also discover several issues regarding how the services are operated. As an example, we find 25% DNS-over-TLS service providers use invalid SSL certificates. Compared to traditional DNS, DNS-over-Encryption is used by far fewer users but we have witnessed a growing trend. As such, we believe the community should push broader adoption of DNS-over-Encryption and we also suggest the service providers carefully review their implementations.

CCS CONCEPTS

• **Networks → Application layer protocols**; **Network measurement**; *Naming and addressing*.

Haixin Duan and Ying Liu are the corresponding authors.
This work is done during Chaoyi Lu's research internship at 360 Netlab.

IMC '19, October 21–23, 2019, Amsterdam, Netherlands

ACM ISBN 978-1-4503-6948-0/19/10…$15.00
https://doi.org/10.1145/3355369.3355580

KEYWORDS

Domain Name System, DNS Privacy, DNS-over-TLS, DNS-over-HTTPS, DNS Measurement

ACM Reference Format:
Chaoyi Lu[1,2], Baojun Liu[3], Zhou Li[4], Shuang Hao[5], Haixin Duan[1,2,6], Mingming Zhang[1], Chunying Leng[1], Ying Liu[1], Zaifeng Zhang[7] and Jianping Wu[1]. 2019. An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come?. In *Internet Measurement Conference (IMC '19), October 21–23, 2019, Amsterdam, Netherlands.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3355369.3355580

1 INTRODUCTION

Domain Name System (DNS) is one of the fundamental building blocks of the Internet, mapping a user-friendly domain name to numerical IP addresses. According to its initial IETF standard, DNS packets are transmitted over UDP protocol *in clear-text*. Therefore, communication integrity and confidentiality are absent. Unfortunately, this design makes DNS communications vulnerable to attacks like eavesdropping and tampering [29]. In fact, real-world adversaries have been exploiting DNS to harm Internet users. As an example, released secret documents show that NSA has been covertly monitoring and hijacking DNS traffic, under the MoreCowBell [44] and QuantumDNS [12] projects. A recent study also shows that network middleboxes are actively intercepting DNS packets and rerouting them to alternative resolvers [60].

One of the mainstream approaches to mitigating such threat is to *encrypt DNS communications*. To this end, various techniques are proposed, including DNS-over-TLS (DoT), DNS-over-HTTPS (DoH), DNS-over-QUIC and DNSCrypt. In this paper, we jointly term them as DNS-over-Encryption (DoE). Although most of the protocols have only been established for a few years, some have been gaining strong support from large DNS service providers [2, 4, 14], OS [24, 56] and software [6, 38, 63].

However, despite the "top-down" effort made by the industry, little has been done to understand the operational status of DNS-over-Encryption from the *"bottom-up" view*, or from the view of Internet users. In this paper, we aim to give a comprehensive and end-to-end review of DNS-over-Encryption, which we believe will provide good guidance in pushing the adoption and improving the ecosystem of DNS-over-Encryption in the future. The research questions we seek to answer include: 1) How many providers are offering DNS-over-Encryption services? Are their implementations secure? 2) What does their performance look like for users distributed globally? Is there any issue preventing access or causing

errors? 3) What does the real-world usage of DNS-over-Encryption look like?

Our Study. So far, DNS-over-TLS (DoT) and DNS-over-HTTPS (DoH) are two *standardized and extensively supported protocols* to secure the traditional DNS, and our study focuses on measuring the two protocols. First, we perform a comparative study on the DNS-over-Encryption protocols to outline their strengths and weaknesses (Section 2). Second, we launch Internet-wide scanning to discover DNS-over-Encryption service providers and analyze their security issues (Section 3). Third, we assess the accessibility and performance of DNS-over-Encryption services by recruiting geographically distributed vantage points (Section 4). Getting access to real-world DNS-over-Encryption traffic from massive vantage points without violating participants' privacy is challenging. We address this challenge by running controlled experiments on a carefully designed Internet measurement platform. Finally, we compare the traffic volume between traditional DNS requests and DNS-over-Encryption requests using several large-scale datasets, including passive DNS datasets and 18-month NetFlow data from a large ISP (Section 5).

Findings. So far, we have obtained some unique discoveries about the deployment of DNS-over-Encryption. On one hand, the service quality of DNS-over-Encryption providers is satisfying in general, suggesting the industry is prepared for large-scale real-world usage. On the other hand, we also spot misconfigurations on some services, and more efforts should be made to push its correct adoption. Below, we highlight the key findings.

- We discover over 150 DoT and 17 DoH providers that offer DNS-over-Encryption services to client users with over 1.5K addresses. Interestingly, a lot of them do not show up in public resolver lists. However, 25% DoT providers, including large ones (Perfect Privacy), use invalid SSL certificates which could break the server authentication process. Particularly, TLS inspection devices are found to act as DoT proxies. In addition, we find that Quad9 DoH has a misconfiguration which causes DNS lookup errors. We have reported the issue to the provider.
- Compared to traditional DNS, the reachability to DNS-over-Encryption servers turns to be better, with only less than 1% global clients experiencing service disruption. But still, there are DNS-over-Encryption services disrupted by censorship (e.g., Google DoH blocked in China) and TLS interception, which diminishes the benefits brought by encrypting DNS queries.
- The extra overhead incurred by DNS-over-Encryption is tolerable to global users. On average, compared to traditional DNS, transmitting encrypted DNS queries brings several milliseconds of extra query latency.
- The traffic volume and active users of encrypted DNS are still at a small scale compared to traditional DNS. However, the usage of DNS-over-Encryption services has been growing in recent months. For example, Cloudflare DoT witnesses a 56% traffic increase from Jul 2018 to Dec 2018.

The "Early" View of Ecosystem. This paper presents the first systematic and large-scale study on the ecosystem of DNS-over-Encryption since its proposal. One may think the ecosystem is small, because major users still choose clear-text DNS, and the measurement study is yet too early. We agree the study is an early view in terms of user base, but on the other hand, the first DNS-over-Encryption protocol has been established for around 10 years, and many resolvers including Google and Cloudflare have started to run DNS-over-Encryption services. We believe it is necessary to understand the gap between the deployment and user adoption, and identify success and pitfalls of different protocols. Such effort can help the community to adjust the roadmap for the better future of DNS-over-Encryption. To this end, we also publish our collected data and results to help further studies, and will continue to monitor the ecosystem.

Contributions. The contributions of this paper are outlined as follows.

- *Comparative study.* Using 10 criteria under 5 categories, we present the first comparative study on five DNS-over-Encryption protocols, which sheds light on the development of the ecosystem.
- *Methodology.* Combining a suite of techniques, we design and deploy a large-scale measurement platform with 122,991 vantage points in 166 countries, to understand the client-side usability of DNS-over-Encryption services. Meanwhile, we launch Internet-wide scanning to discover new service providers.
- *Observations.* Leveraging several large-scale datasets, we investigate the current deployment and usage of DNS-over-Encryption. With multi-faceted insights, we provide concrete recommendations to the DNS community.
- *Dataset release.* We are continuously collecting data and measuring the development of DNS-over-Encryption. We release our datasets for public use at `https://dnsencryption.info`.

2 BACKGROUND

In this section, we first describe the privacy considerations regarding DNS. We then elaborate and perform a comparative study on current protocols to encrypt DNS communications.

2.1 DNS Privacy Considerations

DNS precedes almost all Internet activities: email senders look up recipients' server addresses; patients query hospital domain names; devices use DNS to discover each other. By design, DNS packets are sent in clear-text, which makes it vulnerable to both passive (e.g., on-path eavesdroppers) and active attackers (e.g., rogue DNS servers).

The unencrypted design of DNS exposes Internet users to privacy threats. It has been known that DNS traffic can be used to fingerprint client machines and analyze user behavior [32, 48, 54, 55]. Previous works have also shown that client machines can be tracked across the Internet, by simply analyzing passive DNS data [52]. What's worse, documents reveal that massive DNS surveillance does exist on the Internet, such as NSA's QuantumDNS and MoreCowBell projects [12, 44]. In short, unprotected DNS traffic can introduce significant privacy risks to Internet users.

2.2 DNS-over-Encryption Protocols

Driven by the concerns, the community has been devoting significant efforts to mitigating DNS privacy issues. Shown in Figure 1, the earliest proposal to protect DNS communications dates back to 2009. Since 2014, IETF have established two Working Groups, and various protocols have been proposed to secure traditional

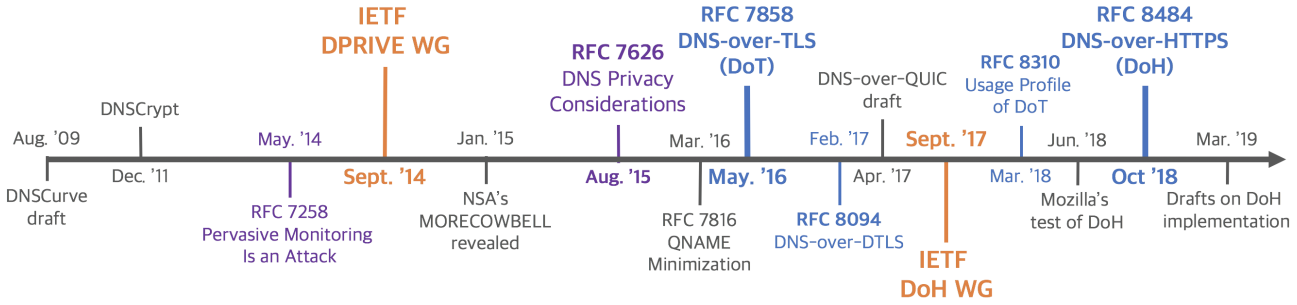

Figure 1: Timeline of important DNS privacy events, including DNS-over-Encryption standards (blue), IETF WGs (orange), Informational RFC and Best Common Practice (purple).

DNS. Meanwhile, the techniques have gained support from large industrial providers including Mozilla [62] and Google [4]. In fact, it would be unsurprising that clear-text DNS will be replaced by the secured format in the near future, similar to HTTPS being mandated when visiting high-profile websites (e.g., banking site).

Adding confidentiality and authentication properties to the DNS protocol is an effective approach to addressing DNS privacy threats. In this work, we focus on techniques that are dedicated to securing the *stub-to-recursive link* of DNS resolutions, as it's the primary focus of the community and most proposals [45, 49, 50]. Below we give an overview and perform a comparative study on different DNS-over-Encryption protocols.

Evaluation Criteria. We consider 10 criteria under 5 categories to evaluate different DNS-over-Encryption protocols.

- *Protocol Design:* 1) whether the new protocol is based on traditional DNS or switches to a different application-layer protocol; 2) whether it provides a fallback option when certain cryptographic operations cannot be applied (i.e., back to non-authenticated or clear-text connections).
- *Security:* 1) whether the protocol is based on standard cryptographic protocols (e.g., TLS); 2) whether it can defend against on-path passive DNS traffic analysis (or at least offers options against it).
- *Usability:* 1) changes that client users need to make before using the protocol: no extra software needed (low), extra software installation or configuration needed (medium), or no supporting software yet (high); 2) whether the protocol incurs query overhead over traditional DNS-over-UDP (e.g., by using TCP or requiring TLS handshake) or provides options to amortize it.
- *Deployability.* 1) whether the protocol is designed over standardized and well-supported protocols; 2) whether it is supported by mainstream DNS software (e.g., BIND [34], Knot Resolver [6] and Unbound [21], see Appendix A).
- *Maturity.* 1) whether the protocol is currently standardized by IETF; 2) whether it is extensively supported by DNS service providers (e.g., large public DNS resolvers, see Appendix A).

Currently, 5 major DNS-over-Encryption protocols are proposed to secure the stub-to-recursive link, including DNS-over-TLS (DoT), DNS-over-HTTPS (DoH), DNS-over-DTLS, DNS-over-QUIC and DNSCrypt. Using the criteria above, we present their evaluation in Table 1. Each protocol is categorized under "satisfying" (denoted as ●), "partially satisfying" (denoted as ◐), or "not satisfying" one criterion (denoted as ○). Below we elaborate each protocol in detail.

DNS-over-TLS (DoT). DoT is standardized by RFC7858 [49] in 2016, and its concept is straightforward: clients and servers negotiate a Transport Layer Security (TLS) session before DNS lookups, and use it to wrap wire-format DNS queries transported through TCP. As a result, clients and recursive resolvers can exchange encrypted DNS messages (preventing passive monitoring), and resolvers can be authenticated by verifying SSL certificates (preventing man-in-the-middle attackers). By default, DoT uses port 853 for communication. The use of a dedicated port could make DoT requests distinguishable from other traffic, but padding options (e.g., EDNS(0) padding [61]) can be leveraged to reduce adversaries' capability of traffic analysis.

To provide different levels of security and privacy protections, DoT is designed with two usage profiles (i.e., *Strict Privacy profile* and *Opportunistic Privacy profile*) for DNS clients [69], and provides fallback mechanisms. Under the Strict Privacy profile, a DNS client is required to both *authenticate* the DoT server and *encrypt* transactions. If either requirement is not available, the DoT query will fail. By contrast, clients using an Opportunistic Privacy profile only *attempt for best protection*, and may fallback to a non-authenticated connection or even clear-text connection.

Regarding implementation, as shown in Appendix A, DoT has been extensively supported by OS (e.g., Android 9 [56]), DNS software (e.g., Unbound [21] and Stubby [38]), and large public DNS resolvers (e.g., Cloudflare [2], Google [4] and Quad9 [14]). For service providers, current implementations reduce the cost to operate a DoT resolver, and SSL certificates are easy to install with automated CAs like Let's Encrypt [8]. However, before a client uses DoT, extra changes have to be made, including switching to new stub resolvers (e.g., by updating the OS or installing stub resolvers like Stubby) and manual configuration of DoT resolvers. With encryption and connection setup, DoT introduces extra query time overhead compared to DNS-over-UDP. However, it can be amortized by connection reuse [49] and we measure the overhead in Section 4.3.

DNS-over-DTLS. A variation of DoT is DNS-over-DTLS, which works over UDP for better performance. While DNS-over-DTLS and DoT share most properties, it is designed only as a *backup proposal* for DoT, and the RFC document expects DoT to be widely deployed [70]. To our best knowledge, DNS-over-DTLS has no real-world implementations yet, including stub and recursive resolvers,

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	●	●	○	○	◐

```
GET /dns-query?dns=AAABAAABAAAAAAAAB2V4YW1wbGUDY29tAAABAAE HTTP/1.1
Host: dns.example.com
Accept: application/dns-message

POST /dns-query HTTP/1.1
Host: dns.example.com
Accept: application/dns-message
Content-Type: application/dns-message
Content-Length: 29
00 00 01 00 00 01 00 00 00 00 00 00 07 65 78 61
6d 70 6c 65 03 63 6f 6d 00 00 01 00 01
```

Figure 2: Two types of DoH requests. They both contain a wire-format DNS A-type query of `example.com`.

thus its usability for clients and deployability for DNS operators are ranked as low.

DNS-over-HTTPS (DoH). Described by RFC8484 [50], the core of DoH is to embed DNS queries into HTTPS messages, which are protected by TLS. Particularly, DoH uses URI templates (e.g., `https://dns.example.com/dns-query{?dns}`) to locate a service, and the hostname in the template should be resolved to bootstrap DoH lookups (e.g., via clear-text DNS). As shown in Figure 2, wire-format DNS packets are encoded in URI parameters (using `GET`) or HTTP message body (using `POST`). As such, two application-layer protocols (HTTP and DNS) are leveraged for DoH.

DoH shares port 443 with HTTPS visits to websites, which mixes DoH queries with other HTTPS traffic, and therefore effectively resists traffic analysis that only targets DNS. By design, DoH requires *both encryption and authentication* of DNS servers (i.e., Strict-Privacy-profile-only). Without fallback options, DoH lookups will fail if either operation is not available. Similar to DoT, query time overhead can be caused by connection establishment and encryption.

DoH runs on top of HTTPS, therefore is particularly suitable for user-space applications like web browsers. Typically, the applications already contain stub resolvers, so the changes for DNS clients to use DoH are minor (compared to updating OS or installing other software). As an example, Firefox supports DoH since Version 62 [63], and offers a UI for DoH configuration. For DNS operators, however, as the combination of HTTP and DNS is less supported by mainstream DNS software (see Appendix A), they need to deploy other implementations in order to offer service. Currently, DoH is supported by large resolvers include Cloudflare [2], Google [4] and Quad9 [14].

DNS-over-QUIC. On top of QUIC, DNS-over-QUIC offers similar privacy properties as DoT, but has similar performance as DNS-over-UDP. According to its current draft, it is designed for minimum latency and solving issues like TCP's head-of-line blocking [51]. For better usability, it also provides a fallback mechanism, using DoT or plain-text DNS when the QUIC connection fails. DNS-over-QUIC is planning to use a dedicated port 784. Still, there are not yet real-world implementations for DNS clients or operators.

DNSCrypt. Proposed in 2011, DNSCrypt is not based on standard TLS, and uses the X25519-XSalsa20Poly1305 cryptographic construction [11]. DNSCrypt messages are transferred over port 443, which are also mixed with HTTPS traffic, and can be used over both UDP and TCP.

As one of the earliest protocols in the list, DNSCrypt has been supported by several large public resolvers for years, including OpenDNS (since 2011) [77], Yandex (since 2016) [25], and OpenNIC [9]. To use DNSCrypt, clients need to install extra software (e.g., DNSCrypt-proxy [3]), and servers need certificates signed on dedicated hardware [11]. Since proposal, DNSCrypt has never been standardized by the IETF.

DNS-over-Encryption and DNSSEC. DNSSEC aims to protect the integrity of DNS records by signing them, but does not protect DNS privacy. DNS-over-Encryption and DNSSEC are dedicated to solving different problems, and they can be fully compatible and used together [49].

The above survey provides the first comparative study of DNS-over-Encryption protocols as far as we know. We do acknowledge that there could be disagreement on the metrics we use and the grades we give to each protocol. However, we believe our survey shows new insights into the development of the DNS-over-Encryption ecosystem, and will enlighten the path for future development of this technology.

Scope of study. DNS-over-TLS (DoT) and DNS-over-HTTPS (DoH) are two leading and mature protocols to secure traditional DNS communications. On top of well-supported and standard protocols (i.e., TLS and HTTP), they are both *standardized* by IETF, and *extensively implemented* by various DNS software and public resolvers (see Table 8 of Appendix A). For the remaining of this paper, we focus on DoT and DoH and measure them from the view of Internet users.

3 SERVERS: TO OFFER DNS-OVER-ENCRYPTION

Servers, especially resolvers, play a vital role in the deployment of DNS-over-Encryption protocols. In this section, we describe our scanning methodology that can identify open DNS-over-Encryption resolvers operated in the wild, and their security analysis. Then, we report our findings.

3.1 Methodology

Though, public resolver lists such as [39, 73] have already complied tens of providers offering DNS-over-Encryption services, it is unclear to us whether they achieve good coverage of all such services, especially the ones less known but still in operation. As such, our first step is to identify DoT and DoH servers through systematic service discovery.

Discovering open DoT resolvers. As DoT uses a dedicated port 853 for communication, it is required that by default, DNS servers that support DoT `MUST` listen for and accept TCP connections on this port [49]. Therefore, discovering open DoT resolvers is conceptually simple through *Internet-wide scanning* using port 853 as input. While a DoT resolver could choose other ports, such setting requires extra configuration changes on DoT clients, which is cumbersome for normal users. As such, those services are not considered in this study.

In practice, we first use ZMap [42] to discover all IPv4 addresses with port 853 open (using the `zmap -p 853` command), and then probe the addresses with DoT queries of a domain registered by us, using `getdns` API [17]. In the first stage, our scan originates from 3 IP addresses in China and the US (on cloud platforms), and we configure the tool to cover the entire IPv4 address space in a random order. For addresses with port 853 open, only those *successfully responding to our DoT queries* are regarded as open DoT resolvers. We repeat our scan process every 10 days from Feb 1, 2019 to May 1, 2019, and each scan takes 24 hours to finish.

For ethical considerations, we offer an opt-out option from our scanning activities, by setting a reverse DNS record for our scanning system and building a website that tells the scanning details and collects opt-out requests. During our scan period, we did not receive any opt-out requests.

Discovering open DoH resolvers. Compared to DoT resolvers, it is much more difficult to discover DoH servers, because they share port 443 with other HTTPS visits, and use URI templates to be located. While we have tried to look for DoH resolvers in public DNS zone files, the discovery turns out to be unsatisfying, as many resolvers are hosted on the subdomains of second-level domains (SLDs) of the providers (e.g., `dns.example.com` in Figure 2), while public zone files only contain SLDs. As an alternative approach, we attempt to discover DoH resolvers by inspecting a large-scale URL dataset provided by our industrial partner. The dataset consists of URLs from their web crawlers, malware sandbox and VirusTotal data feed. Over time, the dataset has recorded billions of URLs.

To discover DoH resolvers, we need to know their URI patterns. Fortunately, the DoH RFC and large resolvers have specified several common path templates (e.g., `/dns-query` and `/resolve`, see Figure 2) that can point to DoH resolvers, and most DoH resolvers in public lists [73] adopt the templates, including Cloudflare [2] and Quad9 [14]. Therefore, we scan the whole URL dataset using the known templates. For ethics, the dataset does not contain user information or URL parameters, so the privacy risk should be minimized.

Limitations. Firstly, our Internet-wide scan only covers open resolvers, and misses those deployed by ISPs (i.e., local resolvers which are not open to public). To evaluate DoT deployment on local resolvers, we launch DoT queries of our own domain to local resolvers using RIPE Atlas [23]. In the end, only 24 of 6,655 probes (0.3%) succeed in the query, suggesting the current ISP DoT deployment is still scarce[1]. Therefore, we believe the impact of lacking local resolvers is small on the overall result. Secondly, while we do discover DoH resolvers (particularly, resolvers beyond known lists) using our methodology, resolvers with unknown URL patterns will be overlooked. Also, despite our URL dataset being large, it could be possible to find more resolvers using other data traces. We do acknowledge that our method has limitations, but given the challenges discussed above, we regard our method as a best-effort attempt.

Table 2: Top countries of open DoT resolvers

CC	# DoT Resolver		Growth	CC	# DoT Resolver		Growth
	Feb 1	May 1	%		Feb 1	May 1	%
IE	456	951	+108%	JP	34	27	-20%
CN	257	40	-84%	NL	30	36	+20%
US	100	531	+431%	GB	25	21	-16%
DE	71	86	+21%	BR	22	49	+122%
FR	59	56	-5%	RU	17	40	+135%

3.2 Open DNS-over-Encryption Resolvers

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. From each Internet-wide scan, we discover 2 to 3 million hosts with port 853 open (e.g., 356M on Feb 1 and 230M on May 1), yet a vast majority of them do not provide DoT (i.e., they cause `getdns` errors). As shown in Figure 3, over 1.5K open DoT resolvers are discovered in each scan, *significantly more* than the public resolver lists. Geographically, Table 2 shows the top 10 countries with most resolvers, and their fluctuation during our scan period. DoT resolvers in Ireland, Brazil and Russia have doubled in three months, and those in the US increased by four times. By contrast, we also find a significant drop of DoT resolvers (-84%) in China, and the shut resolvers mostly belong to a cloud hosting platform.

[1] Our ratio is lower than a previous report [47], because we exclude probes using well-known public resolvers (e.g., 8.8.8.8) as their local resolver. Example DoT-capable local resolvers we find include 194.109.6.66 (AS3265, Xs4all Internet BV), 212.242.40.51 (AS9158, Telenor A/S) and 78.158.0.2 (AS43700, UAB Consilium Optimum)

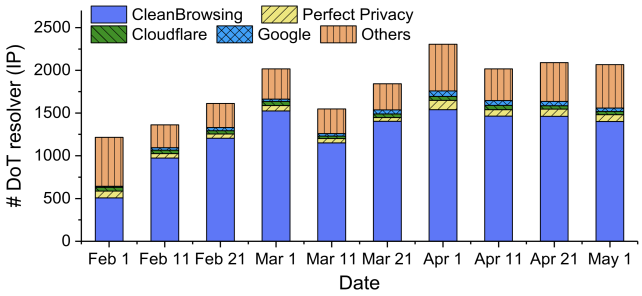

Figure 3: Open DoT resolvers identified by each scan

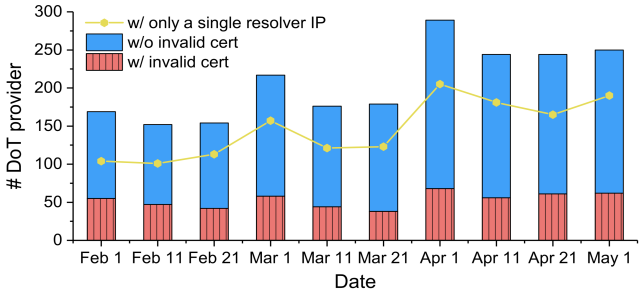

Figure 4: Providers of open DoT resolvers

To identify their providers, we group the DoT resolvers by Common Names in their SSL certificates on port 853[2]. From Figure 3 we find several large providers account for more than 75% resolver addresses, such as CleanBrowsing. Besides their well-known addresses (e.g., Cloudflare's 1.1.1.1), the big players also offer DoT on dozens of other addresses that are not advertised to public (e.g., 89.81.172.185 for Cloudflare).

Apart from large ones, we also find small DoT providers which account for the long tail. Figure 4 counts the DoT providers, and the yellow line shows that *70% providers only operate one single resolver address* (e.g., `qq.dog` and `securedns.zone`). The small resolvers are hardly included in public lists such as [39], which could be a result of lacking promotion, or misconfiguration (i.e., resolvers mistakenly open to public). In the end, our Internet-wide scan discovers more options for DNS clients, and we suggest the providers promote their services if they are intended for public use, or otherwise correct the misconfigurations.

For DoH, we find 61 valid URLs with common DoH paths (e.g., `/dns-query` and `/resolve`) in our dataset. For each URL, we manually check its availability by adding DoH query parameters (see Figure 2). Besides the known 15 providers in [73] (at the time of writing), we also find two DoH resolvers beyond the list (i.e., `dns.adguard.com` and `dns.233py.com`). As a result, we find 17 public DoH resolvers in total, which is fewer than the number of DoT resolvers we find.

In addition, we further validate the DNS answers provided by the open servers using our authoritative data. Resolvers owned by `dnsfilter.com` (e.g., 103.247.37.37) constantly resolve arbitrary domain queries to a fixed IP address, because we do not subscribe to their service (i.e., our scan hosts are not in their users list). All other resolvers respond with the correct answers.

[2]If the Common Name is a domain name, we group them by Second-Level Domains (SLD).

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. SSL certificate plays an important role for clients to authenticate their DNS servers. Using `openssl` [13], we fetch and verify the certificates of all resolvers we discover. We configure the tool to trust the system-wide trust store of CentOS 7.6 (i.e., Mozilla CA list [19]). As the names of DoT resolvers are unknown to us[3], we do not compare domain names to the certificates provided, but only verify the certificate paths.

As shown by Figure 4, around 25% DoT providers install invalid certificates on at least one of their resolvers. In our latest scan (May 1), 122 resolvers of 62 providers use invalid certificates, including 27 expired, 67 self-signed and 28 invalid certificate chains. Among the 27 expired certificates, 9 expired in 2018 (e.g., 185.56.24.52, expired Jul 2018), suggesting that they could be out of maintenance. 2 resolvers of a large provider (Perfect Privacy, see Figure 3) use self-signed certificates. We also find that 47 resolvers use self-signed default certificates of FortiGate (a firewall of Fortinet) [43], acting as DoT proxies that will inspect encrypted queries from DNS clients. By contrast, we find no invalid certificates on port 443 of all 17 DoH resolvers we discover. In fact, it is reasonable because DoH is Strict-Privacy-profile-only (see Section 2), and DoH queries will fail if resolvers cannot be authenticated.

Using invalid certificates can pose privacy threats to DNS clients, as they cannot authenticate the servers. Therefore, we suggest that providers carefully examine their resolvers regularly, and correct the misconfigurations.

4 CLIENTS: TO USE DNS-OVER-ENCRYPTION

For traditional DNS, studies have shown that public DNS services can be broken for some DNS clients, such as inability to connect [60, 74]. Meanwhile, for common users, there have been concerns on the performance overhead of encrypting DNS transactions [62, 68]. To assess the current technology readiness of DNS-over-Encryption, we perform a global large-scale measurement study on its client-side usability. In this section, we first describe our methodology which encounters two major challenges. We then focus on what's preventing global clients from using public DNS-over-Encryption resolvers, and perform a country-level analysis on the performance overhead of encrypted DNS queries.

4.1 Methodology

Experiment setup. To perform a large-scale measurement, the first challenge we encounter is to collect a large number of global vantage points. Particularly, as we study the client-side usability of public DNS-over-Encryption resolvers, the vantage points should be able to send encrypted DNS queries *directly to public server addresses*, instead of their local DNS resolvers. Using two SOCKS proxy networks, we address this challenge as described below in *Vantage points*. From the collected clients, we develop a measurement platform and perform a *Reachability test* to a set of popular public DNS-over-Encryption resolvers. The second challenge is how to perform a *Performance test* on query latency using proxy networks, without direct control over the vantage points.

[3]Currently, authentication domain names should be obtained out of band [69].

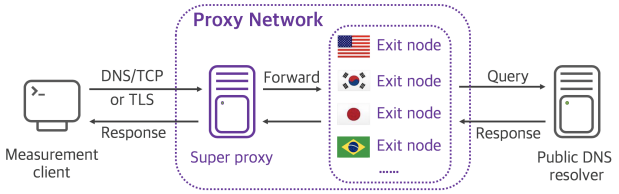

Figure 5: Proxy network architecture

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
Performance	ProxyRack (Global)	8,257	132	1,098

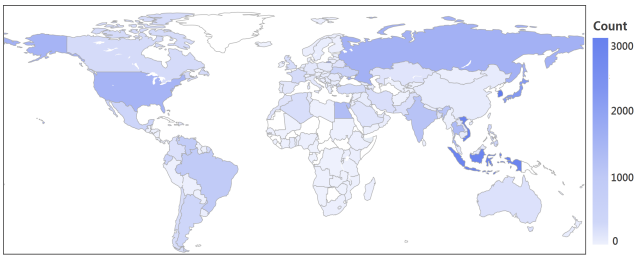

Figure 6: Geo-distribution of ProxyRack endpoints

Vantage points. One major challenge posed by our design requirements, is to obtain different vantage points globally. The clients should be able to *send DoT and DoH queries directly to any given public resolvers*, which makes common platforms including advertising networks [28, 58], HTTP proxy networks [18, 33, 76] and RIPE Atlas [23] (which has no DoH support) not suitable for this task. As such, we collect our vantage points by leveraging two residential TCP SOCKS proxy networks. As shown in Figure 5, the proxy network accepts traffic generated by our measurement client, and forwards it to various proxy nodes. It is suitable for encrypted DNS queries, as DoT and DoH are both based on TCP and TLS.

In practice, we first leverage ProxyRack [5], a residential TCP SOCKS proxy network. This network has been examined as a representative platform by previous studies [60, 64], with more than 600,000 endpoints in over 150 countries. While gaining a global view, we are also interested in DNS-over-Encryption usability in *censored networks*, where DNS traffic is oftentimes manipulated [27, 66]. As such, we complement our dataset with another TCP SOCKS proxy network called Zhima [10], whose endpoints are all located in 5 ASes of two Chinese ISPs. Particularly, the two platforms only forward our traffic to exit nodes, and do not intercept TLS sessions. All encrypted DNS queries that we generate are not visible to the proxy networks.

In the end, Table 3 summarizes our collected dataset, with 122,991 vantage points in total. Through ProxyRack, we collect over 29K clients from 166 countries globally, and Figure 6 shows their geographic distribution.

Reachability test. To test whether DNS-over-Encryption services are broken by in-path devices, we perform DNS lookups on each proxy client. As it is challenging yet inefficient to investigate a wide range of resolvers, plus the platforms set rate limits for our query, we narrow down our test scope to three large and representative public resolvers: Cloudflare [2], Google [4] and Quad9 [14]. For comparison, we also include a self-built resolver which supports clear-text DNS, DoT and DoH.

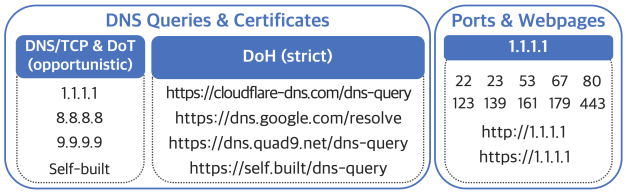

Figure 7: Reachability test items on each proxy client. Each request is repeated 5 times maximum if a failure occurs, and has a 30-second timeout.

Figure 7 presents the workflow of our reachability test. From each vantage point, we first issue clear-text DNS, DoT and DoH queries to each resolver in our list. Studies and forum posts [7, 74] have shown that compared to secondary ones, primary addresses of the resolvers are more likely to encounter reachability problems, therefore we only consider their *primary addresses* (listed in Figure 7). Each DNS query we issue contains an A-type request of our own domain name, which is uniquely prefixed in order to avoid caching.

When testing DoT and DoH, we also collect and verify their SSL certificates. In order to study the real-world risks of opportunistic requests, we use Opportunistic Privacy profile for DoT queries (i.e., authentication is not required before DNS lookup), while DoH is Strict-Privacy-profile-only (i.e., resolver is strictly authenticated).

Furthermore, to understand why DNS-over-Encryption resolvers are not accessible, from the failed clients we probe common ports and fetch the webpages of the resolvers (listed in Figure 7). This check distinguishes *whether the clients are connecting to the real resolvers*, by comparing our probing results with open ports and webpages of the genuine resolvers. However, the proxy networks set a limited lifetime for each vantage point, making it infeasible to perform many probes for all resolvers in our list. Moreover, a previous work shows that 10% DNS clients are not able to query Cloudflare's 1.1.1.1 [74], making it a representative case. Therefore, while testing the reachability of all resolvers in the list, on each endpoint we only probe the ports and fetch the webpages of the Cloudflare resolver, to understand why its DNS-over-Encryption services are not accessible (see Figure 7).

Performance test. DNS-over-Encryption can incur performance overhead for DNS clients, particularly on *query latency*. For DoT and DoH, extra delay can be introduced by TLS session setup and encryption. To measure their performance, we focus on the *relative performance overhead* between DNS-over-Encryption and clear-text DNS, instead of their absolute query latency.

The reuse of connections has a great impact on the performance of DNS-over-Encryption. To amortize query latency, it is required that clients and servers should *reuse connections when resources are sufficient* [49]. In current implementations, connection reuse is the *default setting* of popular client-side software [36, 38] and servers [46, 75], with connection lifetime of tens of seconds. Under this lifetime, a study shows from passive traffic that connection reuse can be frequent (over 90% connection hit fraction) [79].

Therefore, we consider that *connection reuse* is the major scenario of DNS-over-Encryption queries, and take it as the main focus of our performance test. Meanwhile, as our platforms only accepts TCP traffic, we can only use DNS/TCP as the baseline of clear-text DNS, to compare with DNS-over-Encryption. However, [79] also shows that TCP latency is equivalent to UDP after connection establishment (i.e., with reused connections, which is our major focus), therefore we regard DNS/TCP as a reasonable baseline for clear-text DNS.

To observe DNS query latency, we encounter another major challenge, as we do not have direct control over the vantage points. As shown in Figure 8, instead of directly on the proxy clients, we can only observe query latency on our measurement client (i.e., T_N and T_R), which is larger than the actual DNS query latency for the proxy node (i.e., T'_N and T'_R which we cannot observe).

We first consider the relative performance with reused connections (i.e., our major focus). Under this scenario, the latency of both encrypted and clear-text queries only includes DNS transactions (i.e., T'_R), and we aim to compare T'_R of DNS-over-Encryption and DNS/TCP. While we don't have T'_R, we find that it is equivalent to compare their T_R. This is because for each client, T_R only adds one RTT between our measurement client and the proxy node to *both encrypted and clear-text queries*, so their differences remain. Therefore, on each proxy client we issue 20 DNS/TCP, DoT and DoH queries respectively (the maximum number of queries we can send during the limited lifetime of our vantage points), calculate the medians of T_R for each kind of DNS request, and compare their differences as relative performance overhead.

By contrast, when connection is not reused, comparing T_N of DNS-over-Encryption and DNS/TCP is not equivalent to comparing their T'_N. In fact, the relative overhead becomes larger, as T_N incurs several RTTs between our measurement client and the proxy node to encrypted queries (via TLS handshake), but not to clear-text queries. As such, we choose to perform the test on several controlled vantages. On each machine, we issue 200 DNS/TCP, DoT and DoH queries without reusing their connections, and compare their median value of query latency. The test has a limitation on the number of vantages, but according to our above discussion, connection reuse is the more common setting. The results of this test are only used for comparison, but not our focus.

Because the ProxyRack exit nodes rotate, it's important that the repeated DNS queries be sent from one identical node. To this end, before using each proxy, we first check its remaining uptime (using ProxyRack API) and discard it if expiring soon, to make sure it can survive all our queries. Moreover, upon any service disruption of exit nodes (e.g., unexpected connection drop with the super proxy), we remove this node from our dataset.

Limitations. For security reasons, our proxy networks only allow TCP traffic. As a result, in the client-side test we use DNS/TCP for the baseline test, but DNS/UDP is a more common choice for Internet users. While platforms such as RIPE Atlas [23] support DNS/UDP, it is not suitable because: 1) it does not allow a node connecting to arbitrary destinations through DoH; 2) it cannot reuse connections for subsequent queries (i.e., performance test cannot be done). Nevertheless, our discussion earlier shows that DNS/TCP has equivalent performance to DNS/UDP with reused connections (our major focus) [79], thus using DNS/TCP does not influence our test results.

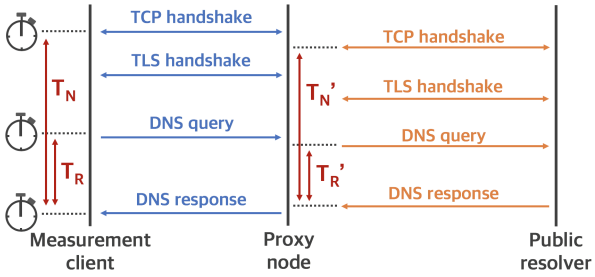

Figure 8: DNS queries via proxy networks for DoT and DoH. DNS/TCP includes all but the TLS handshake.

Ethics. The ethical consideration centers on the proxy networks. Firstly, the platforms we use are both commercial, and we abide their terms of service. The endpoints are recruited by the platforms, and have agreements to route traffic. We only generate DNS and HTTP requests of benign domains and addresses, thus no harm is incurred to the proxy clients.

4.2 Reachability to DNS-over-Encryption Servers

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.

Table 4 presents our reachability test results. From previous works on traditional DNS, we investigate if DNS-over-Encryption services are affected by the following behaviors.

- *IP conflict.* The reasons of IP conflict vary from address being taken by in-path devices, address being blackholed, or used for internal communication, to name a few. Taking Cloudflare's 1.1.1.1 as an example, it has been formerly used by devices of vendors including Cisco and AT&T [15, 31]. A study by Cloudflare shows that more than 10% global clients have reachability problems querying 1.1.1.1 [74].
- *Censorship.* In censored networks, approaches including IP blocking, domain spoofing and connection reset are used to block users from sensitive contents. DNS queries are oftentimes manipulated as a result [27, 66].
- *TLS interception.* Middleboxes and anti-virus software are increasingly intercepting TLS connections and inspecting traffic [41]. If encrypted DNS traffic is intercepted, queries are no longer protected, as they are exposed to interceptors.

Finding 2.1: Compared to traditional DNS, large DNS-over-Encryption services are less affected by in-path devices, with 99% global reachability. From our global dataset, we find that the overall reachability of DNS-over-Encryption resolvers is promising: they can be normally used by over 99% of global clients. Taking Cloudflare as an example, over 16% clients fail to use its clear-text DNS[4], which is similar to previous results [74]. By contrast, the failure rate of Cloudflare DoT drops to 1.1%, suggesting clients can

[4]Over 60% affected clients are located in Indonesia, Vietnam and India.

Table 4: Reachability test results of public resolvers

Platform	Type	Cloudflare			Google			Quad9			Self-built		
		Correct	Incorrect	Failed	Correct	Incorrect	Failed	Correct	Incorrect	Failed	Correct	Incorrect	Failed
ProxyRack (Global)	**DNS**	83.46%	0.08%	16.46%	84.12%	0.08%	15.80%	99.78%	0.11%	0.11%	99.90%	0.06%	0.04%
	DoT	98.84%	0.02%	1.14%	n/a[2]	n/a	n/a	99.78%	0.06%	0.15%	99.90%	0.05%	0.05%
	DoH	99.91%	0.04%	0.05%	99.85%	0.00%	0.15%	85.99%	13.09%	0.92%	99.93%	0.02%	0.05%
Zhima (Censored, China)	**DNS**	84.86%	0.00%	15.14%	98.91%	0.01%	1.08%	99.76%	0.01%	0.23%	99.90%	0.05%	0.05%
	DoT	84.90%	0.00%	15.10%	n/a	n/a	n/a	99.47%	0.02%	0.51%	99.81%	0.02%	0.18%
	DoH	99.74%	0.00%	0.25%	0.01%	0.00%	99.99%	99.25%	0.15%	0.60%	99.92%	0.00%	0.08%

[1] Failed: clients receive no DNS response packets. Incorrect: we only see `SERVFAIL` responses and responses with 0 answers.
[2] At the time of experiment, Google DoT was not announced.

Table 5: Ports open on the address 1.1.1.1, probed from global clients which fail to use Cloudflare DoT.

Port	# Client	Example Client AS
None	155	AS44725 Sinam LLC
22 (SSH)	28	AS17488 Hathway IP Over Cable Internet
23 (Telnet)	40	AS24835 Vodafone Data
53 (DNS)	79	AS4713 NTT Communications Corporation
67 (DHCP)	7	AS52532 Speednet Telecomunicacoes Ldta
80 (HTTP)	131	AS27699 Telefnica Brazil S.A
123 (NTP)	5	AS23693 PT Telekomunikasi Selular
139 (SMB)	3	AS23693 PT Telekomunikasi Selular
161 (SNMPv2)	10	AS9870 Dong-eui University
179 (BGP)	23	AS3269 Telecom Italia S.p.a
443 (HTTPS)	93	AS27699 Telefnica Brazil S.A

[*] Cloudflare's 1.1.1.1 opens port 53, 80 and 443. Others indicate IP conflict.

switch to DNS-over-Encryption if clear-text DNS fails. We suppose the difference is caused by filtering policies on a particular port (i.e., port 53), as supported by devices like [67]. Port 443 (DoH) and 853 (DoT) may currently be ignored by the policies, resulting in better reachability. Also when blocking, the devices appear to focus on the most prominent service addresses, as the failure rate of Cloudflare and Google DNS are higher.

However, compared to other DNS-over-Encryption servers, the failure rate of Cloudflare DoT is higher (over 1.1%). By port scan and checking webpages of 1.1.1.1, we find devices that are conflicting this address, resulting in inability to use. As shown in Table 5, most destinations do not have any of our probed port open, so we presume that they are used for internal routing or blackholing [74]. By their webpages, we find routers (e.g., MikroTik Router in AS17974), modems (e.g., Powerbox Gvt Modem in AS27699) and authentication systems which use 1.1.1.1 for other purposes.

Moreover, security issues can rise when devices conflicting the resolver addresses are compromised. Among our clients which cannot reach the Cloudflare resolver, 12 are connected to *crypto-hijacked MikroTik routers* [53]. The webpages on their 1.1.1.1 are injected with coin-mining codes to abuse computing resource.

Finding 2.2: Censorship blocks users in China from Google DoH. In our China-wide dataset, 99.99% clients fail to query Google DoH. Instead of 8.8.8.8 for its clear-text DNS, `dns.google.com` for Google DoH points to other addresses (e.g., 216.58.192.*). The addresses also carry other Google services, therefore are blocked from Chinese users.

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	✓	✓

For maximum usability, we suggest DNS-over-Encryption services be hosted on addresses with a clean history, or cloud platforms and CDNs which are less likely to have reachability problems. In fact, recently Google is already migrating its DoH to anycast addresses (e.g., 8.8.8.8) [40].

Finding 2.3: While not pervasive yet, TLS interception breaks opportunistic DoT. TLS interception exposes DNS queries to Man-in-the-Middle (MITM) attackers, and eliminates the benefits of encryption. In our global dataset, we find 17 clients (of 29,622) with intercepted queries. In these cases, all resolver certificates are re-signed by an untrusted CA, while other fields remain unchanged (examples given in Table 6), therefore cannot pass strict verification. Except for 3 cases which only listen on port 443, both DoT and DoH traffic are intercepted.

For opportunistic DoT in our test, as it does not require strict authentication, all intercepted clients *proceed with the DNS lookup and successfully get an answer*. From our authoritative server, we find that the MITM devices *proxy the TLS sessions, and forward the queries to the original resolvers*. As a result, queries from clients are visible to the interceptors (e.g., DPI devices in table 6).

On the contrary, as DoH strictly authenticate the servers, it reports a certificate error and terminates the TLS handshake. Consequently, interceptors cannot see the DoH queries, but clients experience query failures.

Finding 2.4: A configuration issue of Quad9 DoH potentially causes unnecessary query failures for their clients. We find that from Quad9 DoH, our clients are getting `SERVFAIL` at a significantly high rate (about 13%). A close inspection at the responses shows that Quad9 forwards all DoH queries to its own DNS/UDP on port 53, and *sets a 2-second timeout* waiting for responses. However, this timeout can be small due to busy networks or faraway nameservers, and therefore causes unnecessary errors for DNS clients.

After reporting the issue to the Quad9 DNS team, we quickly get their response in 24 hours, which acknowledges and confirms our

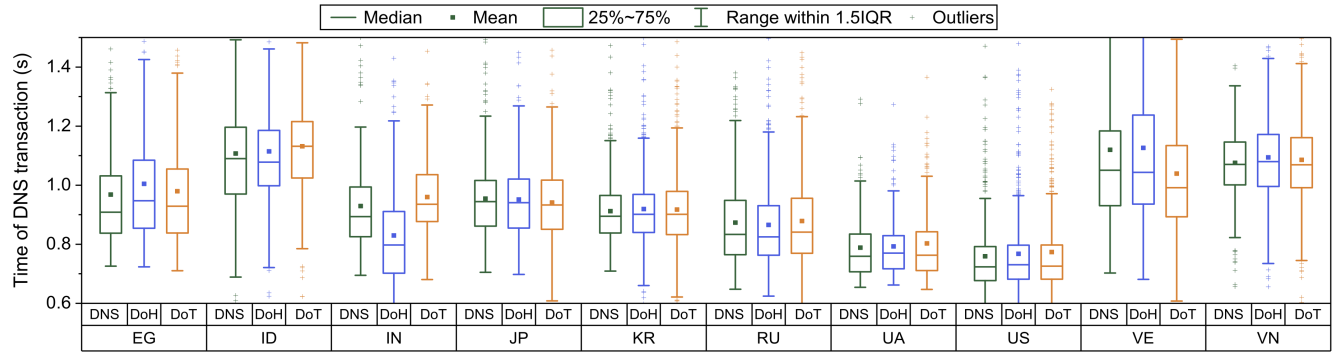

Figure 9: Query performance per country. The countries are selected by having most of our clients.

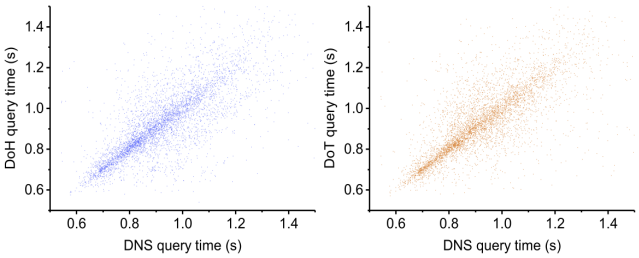

Figure 10: Query time of DNS and DoH (left), DoT (right) on individual proxy clients.

report. According to the response, they are now considering loosening the timeout. In the end, we suggest that DNS-over-Encryption servers be carefully designed and implemented, and eliminate configuration issues.

4.3 Performance of Encrypted Queries

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.

Finding 3.1: On average, query latency of encrypted DNS with reused connection is several milliseconds longer than traditional lookups. Connection reuse is required by the standard documents whenever possible. Our discussion in Section 4.1 also shows that connection reuse can be frequent for DNS-over-Encryption in practice. As shown in Figure 9, when connection is reused, encrypting DNS transactions brings a tolerable performance overhead on query time. Comparing the query latency of Cloudflare's clear-text DNS, DoT and DoH, we are getting *average/median performance overhead of 5ms/9ms (for DoT) and 8ms/6ms (for DoH)* from our global clients. If we look at individual clients, Figure 10 shows their query performance of clear-text DNS and DNS-over-Encryption. The majority of clients distribute near the y=x line, suggesting they do not suffer from significant performance downgrade.

By contrast, with each query establishing a complete new TCP and TLS session (i.e., not reusing connections), we find that the performance overhead can be large, especially when resolvers are far from the clients. Table 7 shows the test results comparing query latency of our self-built DNS resolver: the performance overhead without connection reuse can be up to hundreds of milliseconds.

Table 7: Performance test results w/o connection reuse

Vantage	DNS/TCP	DoT (overhead)	DoH (overhead)
US	0.272	0.349 (77ms)	0.361 (89ms)
NL	0.449	0.707 (258ms)	0.712 (263ms)
AU	0.569	0.955 (386ms)	0.968 (399ms)
HK	0.636	1.106 (470ms)	1.169 (533ms)

* The values are medians of 200 tests on each vantage.

Finding 3.2: Performance of DNS-over-Encryption services fluctuates in different countries. As shown in Figure 9, while the global performance overhead is minor, we find countries where the extra latency of DNS-over-Encryption is above average. Our 504 clients in Indonesia, for example, witness an average/median overhead of 25ms/42ms when using Cloudflare's DoT. By contrast, DNS-over-Encryption can be even faster than traditional DNS for some clients. For instance, our 282 clients in India, gain an average/median of 99ms/96ms performance improvement when using Cloudflare DoH, compared to its clear-text DNS. Though surprising, a possible performance improvement when using DNS-over-Encryption has also been reported by other tests, like Mozilla's test on DoH [62]. Their hypothesis include that DoH has better service consistency, and uses modern features of HTTP such as loss recovery and congestion control for better operation. We presume that it also could be caused by anycast or different routes that the queries are taking, and that resolvers in different regions have different latency to nameservers [59].

5 USAGE: DNS-OVER-ENCRYPTION TRAFFIC

For the DNS community, it's crucial to understand how DNS-over-Encryption is positioned in the contemporary DNS ecosystem, including the trend and characteristics of its real-world traffic. On this basis, the DNS community can better push forward the future deployment and usage of DNS-over-Encryption. In this section, we investigate its current usage using several large-scale passive traffic datasets.

5.1 Methodology

Observing DoT traffic. DoT by default uses port 853, therefore can be distinguished from other traffic. As such, we use a 18-month NetFlow [1] dataset (Jul 2017 to Jan 2019) collected by the backbone routers of a large Chinese ISP. NetFlow-enabled routers aggregate

sequential packets in a flow (i.e., packets with the same transfer protocol, IP addresses and ports) and create a record containing its statistics. Each NetFlow record include IP addresses, ports, total bytes of packets, and the union of TCP flags. When collecting NetFlow, our provider ISP uses a sampling rate 1/3,000, and expires a flow if idle for 15 seconds.

To begin our analysis, we first select all NetFlow records over TCP port 853, and exclude all flows which only contain a single SYN flag[5]. We then check if the traffic is DoT by matching the destination address with the DoT resolver list we create in Section 3. If a flow is sent by a client to TCP port 853 of a DoT resolver, we consider it as DoT traffic. For ethical considerations, we only keep the /24 of each client IP address before further processing and analysis.

Observing DoH traffic. DoH queries are mixed with HTTPS traffic, thus it's infeasible to observe them from traffic datasets such as NetFlow. However, the URI template of a DoH service contains a domain that should be resolved before DoH lookups (e.g., `dns.example.com`, see Section 2). This inspires us to evaluate DoH usage, by checking the query volumes of resolver domain names in passive DNS datasets.

DNSDB [22] and 360 PassiveDNS [16] are two large passive DNS datasets maintained by Farsight Security and Qihoo 360, respectively. They both contain aggregated statistics of a given domain, including timestamps of its first and last query, and number of historical lookups. While DNSDB has a wider coverage of resolvers across the globe, 360 PassiveDNS provides us with more fine-grained statistics such as daily query volume per domain. Therefore, we leverage DNSDB to study the scale of lookups for DoH domains, and use 360 PassiveDNS to investigate their query trends over time.

Limitations. While large, our passive datasets inevitably contain geographical bias. Admittedly, traffic collected directly by DNS-over-Encryption resolvers allows us to perform more fine-grained and systematic analysis, yet we currently do not have access to such dataset. Second, due to DNS cache, we may underestimate the query volume of DoH domains from passive DNS datasets. However, it still provides us with an opportunity to evaluate the current trend of DoH usage.

5.2 DoT Traffic

Key observation 4: 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 4.1: DoT traffic to large public resolvers is still at a small scale, mostly coming from both centralized clients and temporary users. From our NetFlow dataset, we only spot traffic to large public DoT resolvers (e.g., Cloudflare and Quad9), yet its amount is still small compared to traditional DNS. Particularly, the traffic does not originate from automated scanners.

Figure 11 depicts the monthly count of bidirectional flows to Cloudflare and Quad9 DNS. We find that the amount of DoT traffic is still small: about *2-3 orders of magnitude less* than traditional DNS, under the same sampling rate. We also notice an increase of traffic to Cloudflare DoT: it grows by 56% from Jul 2018 (4,674 flows recorded) to Dec 18 (7,318 flows recorded), while traffic to Quad9 DoT fluctuates.

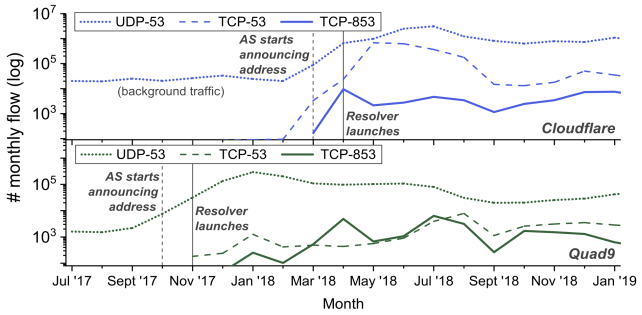

Figure 11: Traffic to Cloudflare and Quad9 DNS

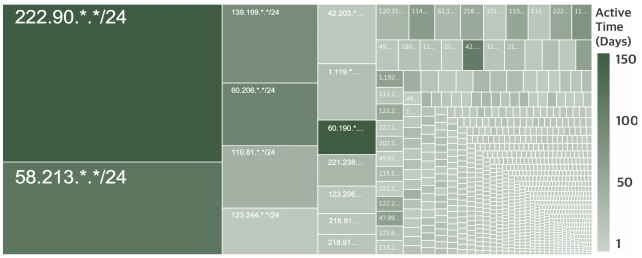

Figure 12: DoT traffic to Cloudflare DNS per /24 network. The size indicates the proportion of DoT traffic, and the color shows the active time of each network.

Zooming into client distribution, we find several networks account for a great proportion of DoT traffic. Among all 5,623 /24 netblocks which send DoT traffic to Cloudflare resolver, *the top five netblocks account for 44% of all DoT traffic, and the top 20 account for 60%* [6]. As shown in Figure 12, the active time (i.e., count of days when we observe DoT traffic from this network) of giant client networks tends to be several weeks or months long. On the other hand, we also notice a number of temporary users: *5,416 (96%) netblocks are only active for less than one week*, producing 25% of all DoT traffic we observe.

Moreover, in order to verify whether the DoT traffic we observe comes from automated scanners, we submit all client networks to NetworkScan Mon [20] and check their behaviors. Developed and maintained by 360 Netlab, it runs on various data inputs including NetFlow, darknet and honeypot, and detects scan behaviors based on real-time traffic statistics and state transition model. The system has been effective in quickly reporting attacks including Mirai, IoT Reaper and Hajime botnet [65]. In the end, we do not get any alert on port-853 scanning activities related to the client networks. As a complement, we also check the SOA and PTR records of the client addresses, and do not find them potentially related to scanning experiments. Therefore, we regard the DoT traffic we observe from our NetFlow dataset is not generated by automated scanners.

[5] The TCP flags field unions all flags observed in a NetFlow. A single SYN flag indicates an incomplete TCP handshake and cannot contain DoT queries.

[6] 9 of the 10 top networks belong to ISPs, and the remaining one is owed by a cloud platform. We speculate the reasons for their large ratio include: 1) DoT is less popular in other networks, 2) the observed addresses under the two netblocks are associated with proxy or NAT.

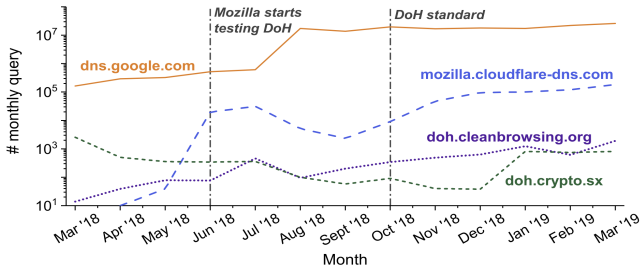

Figure 13: Query volume of popular DoH domains

5.3 DoH Traffic

Finding 4.2: Large providers dominate in all DoH services, and their usage is growing. According to DNSDB, among the 17 public DoH resolvers we discover (15 in [73] and 2 beyond, see Section 3) [7], only 4 domains have more than 10K queries. As the rest resolvers do not witness much traffic, we focus on the query trend of the 4 popular DoH resolvers (i.e., Cloudflare, Google, CleanBrowsing and `crypto.sx`).

Figure 13 shows the monthly query volume of the 4 popular DoH domains, according to 360 PassiveDNS. Google DoH, as the most popular DoH resolver with the longest history (since 2016), receives several orders of magnitude more queries than other domain names. Cloudflare's DoH also receives much traffic, owing to the support of DoH on Firefox, and the recent DoH test on Firefox Nightly [62]. The query volumes of the DoH resolvers have all witness a growth. For instance, the query volume of CleanBrowsing DoH has increased by nearly 10 times from Sept 2018 (200 queries recorded) to Mar 2019 (1,915 queries recorded).

6 DISCUSSION

Recommendations. We believe to push forward the development and deployment of DNS-over-Encryption, efforts from all parties in the Internet ecosystem are required. For protocol designers, it is important to reuse well-developed protocols to encrypt DNS messages, for new protocols to be widely supported and implemented. For DNS service providers, as we find less-known resolvers, invalid SSL certificates and configuration issues, we suggest that they promote their services, correct misconfigurations, and keep their services under careful and regular maintenance. Meanwhile, we recommend them to use resolver addresses with a clean history. For DNS clients, as we find the usability of public DNS-over-Encryption servers is promising, we believe education is necessary to let them understand the benefits of encrypting their DNS queries.

Dataset and code release. We release our source code and collected datasets at `https://dnsencryption.info`. We believe our dataset release is helpful for further studies.

7 RELATED WORK

DNS Privacy Threats. The lack of encryption and authentication in DNS is widely seen as one of the Internet's biggest unpatched bugs. Unencrypted DNS queries are vulnerable to attacks including eavesdropping and manipulation. Previous studies have shown that DNS queries and logs can be used to accurately fingerprint client machines and even identify users [32, 48, 54, 55, 72]. On-path attackers can therefore build a profile for each client and track them across the Internet from DNS queries [52].

Because DNS lacks authentication, adversaries can arbitrarily manipulate unprotected DNS traffic. Transparent proxies can spoof the IP addresses of user-specified resolvers and surreptitiously intercept DNS queries [60]. Moreover, adversaries can build rogue DNS servers and return malicious responses to launch an attack [35, 57], or redirect traffic of non-existent domains for illegal monetization [78]. Attackers can also build fake DNS root servers to hijack all DNS root traffic [26]. Their motivations include malware distribution, censorship, ad injection [57] and performance improvement [26].

Improving DNS Privacy. The DNS community have been discussing DNS privacy threats [29]. To add confidentiality to traditional DNS, DNS-over-TLS [49] and DNS-over-HTTPS [50] have been standardized, which offer both encryption and authentication. Besides adding confidentiality, there are also techniques to eliminate privacy data in DNS packets, such as QNAME minimization [30].

Currently, significant efforts have been devoted by the DNS community to pushing forward the deployment of DNS-over-Encryption. Before the standards, [79] presents a performance evaluation of encrypted DNS (T-DNS), which concludes that it only introduces a modest cost with careful implementation. To study side-channel problems of DoH, [71] performs traffic analysis to distinguish webpages from encrypted DNS traffic. Cloudflare, as a DNS service provider, measures and tries to fix the global reachability to its public resolvers [74]. Meanwhile, the DNSPrivacy Project [37] has gathered latest updates of DNS-over-Encryption, and performed studies on their implementations.

Compared to previous researches, our work presents the first systematic and large-scale research on the evolution of DNS-over-Encryption techniques, serving as a complement to understanding the DNS ecosystem.

8 CONCLUSION

To solve DNS privacy concerns, various protocols are proposed to encrypt and secure DNS transactions. In this paper, we perform the first systematic and large-scale measurement study on the ecosystem of DNS-over-Encryption. Our study shows that two recent standardized protocols, DoT and DoH, are with promising global reachability, minor performance overhead and growing usage. We also provide recommendations for the DNS community to push forward the future deployment of DNS-over-Encryption, and release our collected datasets. Our findings highlight the need for service providers to re-evaluate their implementations, and encourage more Internet users to use DNS-over-Encryption and secure their DNS queries.

ACKNOWLEDGMENTS

We sincerely thank our shepherd Prof. kc claffy, and all anonymous reviewers for their valuable reviews and comments to improve the paper. We also thank Genshen Ye, Haosheng Han, Yuanhao Chen,

[7] For Cloudflare, we use `mozilla.cloudflare-dns.com` instead of the more popular `cloudflare-dns.com`, because the second domain is *not exclusively* used for DoH service. We also exclude `dns.quad9.net`, because it's not for DoH until Oct 2018, and most of its queries are recorded before this date.

Yang Xu, Jinjin Liang, Fengpei Li, Yiming Zhang and Vern Paxson for their help on the paper.

This work is supported by National Key R&D Program of China (No. 2017YFB0803202, No. 2018YFB1800405), NSFC Program (grants U1836213, U1636204, 61772307) and BNR2019TD01004.

APPENDIX

A CURRENT IMPLEMENTATIONS OF DNS-OVER-ENCRYPTION PROTOCOLS

We provide an extensive survey on current implementations of DNS-over-Encryption protocols in Table 8. DNS-over-DTLS and DNS-over-QUIC are not included, as we do not find implementations yet.

Compared to DNSSEC (a widely-deployed security extension standardized in 2005) and QNAME Minimization (also used to improve DNS privacy, standardized in 2016), we find DoT (standardized in 2016) and DoH (standardized in 2018) is getting quickly supported by large DNS service providers and software vendors.

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			✓	✓	
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)	✓			✓	–
		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.

REFERENCES

[1] [n. d.]. Cisco IOS NetFlow. https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-netflow/index.html.
[2] [n. d.]. Cloudflare Resolver. https://cloudflare-dns.com/.
[3] [n. d.]. DNSCrypt-proxy 2. https://github.com/jedisct1/dnscrypt-proxy.
[4] [n. d.]. Google Public DNS. https://developers.google.com/speed/public-dns/.
[5] [n. d.]. HTTP and SOCKS PROXIES. https://www.proxyrack.com/.
[6] [n. d.]. Knot DNS. https://www.knot-dns.cz/.
[7] [n. d.]. Latest 1.1.1.1 Topics - Cloudflare Community. https://community.cloudflare.com/c/reliability/1111.
[8] [n. d.]. Let's Encrypt - Free SSL/TLS Certificates. https://letsencrypt.org.
[9] [n. d.]. OpenNIC Project. https://www.opennic.org/.
[10] [n. d.]. Zhima Proxy. http://h.zhimaruanjian.com/.
[11] 2013. DNSCrypt version 2 protocol specification. https://dnscrypt.info/protocol.
[12] 2014. The NSA and GCHQ's QUANTUMTHEORY Hacking Tactics. https://theintercept.com/document/2014/03/12/nsa-gchqs-quantumtheory-hacking-tactics/.
[13] 2018. OpenSSL Cryptography and SSL/TLS toolkit. https://www.openssl.org/.
[14] 2018. Quad9 DNS: Internet Security & Privacy In a Few Easy Steps. https://www.quad9.net/.
[15] 2018. WLC Virtual IP address 1.1.1.1. https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/213535-wlc-virtual-ip-address-1-1-1-1.html.
[16] 2019. 360 PassiveDNS. https://passivedns.cn/help/.
[17] 2019. Getdns API. https://github.com/getdnsapi/getdns.
[18] 2019. Luminati: Residental Proxy Service for Businesses. https://luminati.io.
[19] 2019. MOZILLA Included CA Certificate List. https://ccadb-public.secure.force.com/mozilla/IncludedCACertificateReport.
[20] 2019. NetworkScan Mon. https://scan.netlab.360.com/#/dashboard.
[21] 2019. NLnet Labs - Unbound. https://www.nlnetlabs.nl/projects/unbound/about/.
[22] 2019. Passive DNS historical internet database: Farsight DNSDB. https://www.farsightsecurity.com/solutions/dnsdb/
[23] 2019. RIPE Atlas - RIPE Network Coordination Centre. https://atlas.ripe.net/.
[24] 2019. Systemd - News. https://github.com/systemd/systemd/blob/master/NEWS.
[25] 2019. Yandex.DNS. https://dns.yandex.com/.
[26] Mark Allman. 2016. Detecting DNS Root Manipulation. In *PAM 2016, Heraklion, Greece, March 31-April 1, 2016. Proceedings*, Vol. 9631. Springer, 276.
[27] Anonymous. 2014. Towards a Comprehensive Picture of the Great Firewall's DNS Censorship. In *FOCI 14*. USENIX Association, San Diego, CA. https://www.usenix.org/conference/foci14/workshop-program/presentation/anonymous
[28] APNIC. 2019. DNSSEC Measurement Maps. https://stats.labs.apnic.net/dnssec.
[29] Stephane Bortzmeyer. 2015. *DNS privacy considerations*. Technical Report.
[30] Stephane Bortzmeyer. 2016. *DNS query name minimisation to improve privacy*. Technical Report.
[31] Jon Brodkin. 2018. AT&T explains why it blocked Cloudflare DNS: It was just an accident. https://arstechnica.com/information-technology/2018/05/att-is-blocking-cloudflares-privacy-focused-dns-calls-it-an-accident/.
[32] Deliang Chang, Qianli Zhang, and Xing Li. 2015. Study on os fingerprinting and nat/tethering based on dns log analysis. In *IRTF & ISOC Workshop on Research and Applications of Internet Measurements (RAIM)*.
[33] Taejoong Chung, Roland van Rijswijk-Deij, Balakrishnan Chandrasekaran, David Choffnes, Dave Levin, Bruce M Maggs, Alan Mislove, and Christo Wilson. 2017. A Longitudinal, End-to-End View of the {DNSSEC} Ecosystem. In *26th {USENIX} Security Symposium ({USENIX} Security 17)*. 1307–1322.
[34] Internet Systems Consortuim. 2019. BIND 9 Open Source DNS Server. https://www.isc.org/downloads/bind/.
[35] David Dagon, Niels Provos, Christopher P Lee, and Wenke Lee. 2008. Corrupted DNS Resolution Paths: The Rise of a Malicious Resolution Authority.. In *NDSS*.
[36] John Dickinson and Sara Dickinson. 2019. DNS Privacy Implementation Status. https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Implementation+Status.

[37] Sara Dickinson. 2018. DNS Privacy Project. https://dnsprivacy.org/wiki/display/DP.

[38] Sara Dickinson. 2019. DNS Privacy Daemon - Stubby. https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Daemon+-+Stubby.

[39] Sara Dickinson. 2019. DNS Privacy Test Servers. https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Test+Servers.

[40] Google Public DNS. 2019. Migration to anycast and RFC 8484 DoH. https://developers.google.com/speed/public-dns/docs/doh/migration.

[41] Zakir Durumeric, Zane Ma, Drew Springall, Richard Barnes, Nick Sullivan, Elie Bursztein, Michael Bailey, J Alex Halderman, and Vern Paxson. 2017. The security impact of HTTPS interception. In *NDSS*.

[42] Zakir Durumeric, Eric Wustrow, and J Alex Halderman. 2013. ZMap: Fast Internet-wide Scanning and Its Security Applications.. In *USENIX Security Symposium*, Vol. 8. 47–53.

[43] Fortinet. 2017. Preventing certificate warnings (default certificate). https://cookbook.fortinet.com/preventing-certificate-warnings-defaultcert-56/.

[44] Christian Grothoff, Matthias Wachs, Monika Ermert, and Jacob Appelbaum. 2015. NSA's MORECOWBELL: Knell for DNS. https://leaksource.files.wordpress.com/2015/02/nsas-morecowbell-knell-for-dns.pdf.

[45] DPRIVE Working Group. 2018. DNS PRIVate Exchange WG. https://datatracker.ietf.org/doc/charter-ietf-dprive/.

[46] Olafur Guomundsson and Marek Vavrusa. 2018. DoH and DoT experience. https://indico.dns-oarc.net/event/29/contributions/653/attachments/640/1027/DoT_and_DoH_experience.pdf.

[47] Brian Haberman and Catherine Master. 2018. DNS-over-TLS Measurements with RIPE Atlas Probes. https://datatracker.ietf.org/meeting/102/materials/slides-102-dprive-dns-over-tls-measurements-with-ripe-atlas-probes-01.

[48] Dominik Herrmann, Christian Banse, and Hannes Federrath. 2013. Behavior-based tracking: Exploiting characteristic patterns in DNS traffic. *Computers & Security* 39 (2013), 17–33.

[49] Z Hu, Liang Zhu, John Heidemann, Allison Mankin, Duane Wessels, and Paul Hoffman. 2016. *Specification for DNS over transport layer security (TLS)*. Technical Report.

[50] P Huffman and P McManus. 2018. *DNS Queries over HTTPS (DoH)*. Technical Report.

[51] Christian Huitema, Melinda Shore, Allison Mankin, Sara Dickinson, and Jana Iyengar. 2018. Specification of DNS over Dedicated QUIC Connections. https://tools.ietf.org/html/draft-huitema-quic-dnsoquic-05.

[52] Daniel Kahn Gillmor. 2018. Trust relationships between users and private DNS resolvers. https://drive.google.com/file/d/13AeDutZJ1WZ-PrNZ9ZROsAc1-jfdhHvm/view

[53] Karthikeyan C Kasiviswanathan. 2018. Postmortem of a Compromised MikroTik Router. https://www.symantec.com/blogs/threat-intelligence/hacked-mikrotik-router.

[54] Dae Wook Kim and Junjie Zhang. 2015. You are how you query: Deriving behavioral fingerprints from DNS traffic. In *International Conference on Security and Privacy in Communication Systems*. Springer, 348–366.

[55] Matthias Kirchler, Dominik Herrmann, Jens Lindemann, and Marius Kloft. 2016. Tracked without a trace: linking sessions of users by unsupervised learning of patterns in their DNS traffic. In *Proceedings of the 2016 ACM Workshop on Artificial Intelligence and Security*. ACM, 23–34.

[56] Erik Kline and Ben Schwartz. 2018. DNS over TLS support in Android P Developer Preview. https://android-developers.googleblog.com/2018/04/dns-over-tls-support-in-android-p.html

[57] Marc Kührer, Thomas Hupperich, Jonas Bushart, Christian Rossow, and Thorsten Holz. 2015. Going wild: Large-scale classification of open DNS resolvers. In *IMC*. ACM, 355–368.

[58] Wilson Lian, Eric Rescorla, Hovav Shacham, and Stefan Savage. 2013. Measuring the Practical Impact of DNSSEC Deployment.. In *USENIX*.

[59] Jinjin Liang, Jian Jiang, Haixin Duan, Kang Li, and Jianping Wu. 2013. Measuring query latency of top level DNS servers. In *PAM*. Springer, 145–154.

[60] Baojun Liu, Chaoyi Lu, Haixin Duan, Ying Liu, Zhou Li, Shuang Hao, and Min Yang. 2018. Who is answering my queries: understanding and characterizing interception of the DNS resolution path. In *USENIX Security Symposium*. 1113–1128.

[61] Alexander Mayrhofer. 2016. The edns (0) padding option. (2016).

[62] Patrick McManus. 2018. Firefox Nightly Secure DNS Experimental Results. https://blog.nightly.mozilla.org/2018/08/28/firefox-nightly-secure-dns-experimental-results/.

[63] Patrick McManus. 2018. Improving DNS Privacy in Firefox - Firefox Nightly News. https://blog.nightly.mozilla.org/2018/06/01/improving-dns-privacy-in-firefox/.

[64] Xianghang Mi, Ying Liu, Xuan Feng, Xiaojing Liao, Baojun Liu, XiaoFeng Wang, Feng Qian, Zhou Li, Sumayah Alrwais, and Limin Sun. 2019. Resident Evil: Understanding Residential IP Proxy as a Dark Service. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE.

[65] 360 Netlab. 2019. Netlab OpenData. https://data.netlab.360.com/.

[66] Paul Pearce, Ben Jones, Frank Li, Roya Ensafi, Nick Feamster, Nick Weaver, and Vern Paxson. 2017. Global measurement of dns manipulation. In *USENIX Security Symposium*. *USENIX*. 307–323.

[67] Matt Prytuluk. 2018. Preventing Circumvention of Cisco Umbrella with Firewall Rules. https://support.umbrella.com/hc/en-us/articles/230904088-Preventing-Circumvention-of-Cisco-Umbrella-with-Firewall-Rules.

[68] Rod Rasmussen. 2016. The Pros and Cons of DNS Encryption. https://www.infosecurity-magazine.com/opinions/the-pros-and-cons-of-dns-encryption/.

[69] Tirumaleswar Reddy, Daniel Gillmor, and Sara Dickinson. 2018. Usage Profiles for DNS over TLS and DNS over DTLS. (2018).

[70] Tirumaleswar Reddy, D Wing, and P Patil. 2017. *DNS over Datagram Transport Layer Security (DTLS)*. Technical Report.

[71] Sandra Siby, Marc Juarez, Narseo Vallina-Rodriguez, and Carmela Troncoso. 2018. DNS Privacy not so private: the traffic analysis perspective. (2018).

[72] Jonathan M Spring and Carly L Huth. 2012. The impact of passive dns collection on end-user privacy. *Securing and Trusting Internet Names* (2012).

[73] Daniel Stenberg. 2019. Public available servers. https://github.com/curl/curl/wiki/DNS-over-HTTPS#publicly-available-servers.

[74] Marty Strong. 2018. Fixing Reachability to 1.1.1.1, GLOBALLY! https://labs.ripe.net/Members/marty_strong/fixing-reachability-to-1-1-1-1-globally

[75] Nick Sullivan. 2017. Introducing Zero Round Trip Time Resumption (0-RTT). https://blog.cloudflare.com/introducing-0-rtt/.

[76] Gareth Tyson, Shan Huang, Felix Cuadrado, Ignacio Castro, Vasile C Perta, Arjuna Sathiaseelan, and Steve Uhlig. 2017. Exploring HTTP header manipulation in-the-wild. In *Proceedings of the 26th International Conference on World Wide Web*. International World Wide Web Conferences Steering Committee, 451–458.

[77] David Ulevitch. 2011. DNSCrypt: Critical, fundamental, and about time. https://umbrella.cisco.com/blog/2011/12/06/dnscrypt-critical-fundamental-and-about-time/.

[78] Nicholas Weaver, Christian Kreibich, and Vern Paxson. 2011. Redirecting DNS for Ads and Profit.. In *FOCI*.

[79] Liang Zhu, Zi Hu, John Heidemann, Duane Wessels, Allison Mankin, and Nikita Somaiya. 2015. Connection-oriented DNS to improve privacy and security. In *Security and Privacy (SP), 2015 IEEE Symposium on*. IEEE, 171–186.