A Longitudinal and Comprehensive Measurement of DNS Strict Privacy

Ruixuan Li, Xiaofeng Jia, Zhenyong Zhang, Jun Shao, *Senior Member, IEEE*, Rongxing Lu, *Fellow, IEEE*, Jingqiang Lin, Xiaoqi Jia, and Guiyi Wei, *Member, IEEE*

***Abstract*— The DNS privacy protection mechanisms, DNS over TLS (DoT) and DNS over HTTPS (DoH), only work correctly if both the server and client support the Strict Privacy profile and no vulnerability exists in the implemented TLS/HTTPS. A natural question then arises: what is the landscape of DNS Strict Privacy? To this end, we provide the first longitudinal and comprehensive measurement of DoT/DoH deployments in recursive resolvers, authoritative servers, and browsers. With the collected data, we find the number of DoT/DoH servers increased substantially during our ten-month-long scan. However, around 60% of DoT and 44% of DoH recursive resolver certificates are invalid. Worryingly, our measurements confirm the centralization problem of DoT/DoH. Furthermore, we classify DNS Strict Privacy servers into four levels according to daily scanning results on TLS/HTTPS-related security features. Unfortunately, around 25% of DoH Strict Privacy recursive resolvers fail to meet the minimum level requirements. To help the Internet community better perceive the landscape of DNS Strict Privacy, we implement a DoT/DoH server search engine and recommender system. Additionally, we investigate five popular browsers across four operating systems and find some inconsistent behavior with their DNS privacy implementations. For example, Firefox in Windows, Linux, and Android allows DoH communication with the server without the SAN certificate. At last, we advocate that all participants head together for a bright DNS Strict Privacy landscape by discussing current hindrances and controversies in DNS privacy.**

***Index Terms*— DoT, DoH, strict privacy, centralization, HTTPS, TLS.**

Manuscript received 24 April 2022; revised 4 October 2022 and 4 December 2022; accepted 26 March 2023; approved by IEEE/ACM TRANSACTIONS ON NETWORKING Editor K. Ren. This work was supported in part by the National Natural Science Foundation of China under Grant 62272413; in part by the National Key Research and Development Program of China under Grant 2019YFB1005201; and in part by the Digital+ Foundation of Zhejiang Gongshang University under Grant SZJ2022C001, Grant SZJ2022A002, and Grant SZJ2022A010. *(Corresponding author: Jun Shao.)*

Ruixuan Li, Xiaofeng Jia, Zhenyong Zhang, and Jun Shao are with the School of Computer Science and Technology, Zhejiang Gongshang University, Hangzhou 310018, China, also with the Zhejiang E-Commerce Key Laboratory, Hangzhou 310018, China, and also with the Key Laboratory of Network Assessment Technology, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China (e-mail: chn.junshao@gmail.com).

Rongxing Lu is with the Faculty of Computer Science, University of New Brunswick, Fredericton, NB E3B5A3, Canada (e-mail: rlu1@unb.ca).

Jingqiang Lin is with the School of Cyber Security, University of Science and Technology of China, Hefei 230026, China (e-mail: linjq@ustc.edu.cn).

Xiaoqi Jia is with the Key Laboratory of Network Assessment Technology, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China.

Guiyi Wei is with the School of Information and Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, China (e-mail: weigy@mail.zjgsu.edu.cn).

Digital Object Identifier 10.1109/TNET.2023.3262651

I. INTRODUCTION

AS AN essential cornerstone of the Internet, the Domain Name System (DNS) inevitably contains a large amount of private information. However, the original DNS design [1] is vulnerable to many active and passive attacks due to the clear-text transmission approach, which seriously affects users' privacy. Numerous studies and reports have fueled the desire to encrypt the DNS traffic [2], [3], but changing an already widely deployed mechanism is not an easy job. Among encrypted DNS mechanisms, only DNS over TLS (DoT) [4] and DNS over HTTPS (DoH) [5] have been standardized and widely adopted by large DNS providers [6], [7], browsers [8], [9], and operating systems [10], [11], as TLS/HTTPS has gained rapid development during the past years.

DoT and DoH are quite related in terms of supported profiles. In particular, DoT supports the Opportunistic Privacy profile and the Strict Privacy profile [12], while DoH only has the latter [13]. The encrypted and authoritative connection is mandatory in the Strict Privacy profile, while the clear-text connection is still allowed in the Opportunistic Privacy profile. From a security standpoint, the Strict Privacy profile is more advantageous. Hence, the main subjects in this paper are DNS Strict Privacy (DNS/SP), which contains DoT-SP and DoH-SP. The DNS/SP server not only supports DNS encryption but is also equipped with a pair of available (IP address, domain name).

Although DNS/SP enjoys secure transmission from TLS/HTTPS, it is also subject to corresponding threats, such as CA compromise [14] and private key leakage [15]. Therefore, DNS/SP needs the supplementary mechanisms, such as DANE-TLSA [16], CT [17], Expect-CT [18], CAA [19], certificate revocation [20], [21], [22], [23], TLS downgrade protection [24], [25], and HSTS [26]. However, as an online survey [27] by a research group from the University of Chicago indicates, Internet users currently don't know how many players can provide reliable DNS/SP. A natural question then arises: *what is the landscape of DNS Strict Privacy?*

To this end, we in this paper systematically evaluate the extent to which all players involved in DoT/DoH, including recursive resolvers, authoritative servers (authoritative name servers and TLD name servers), and browsers, in terms of Strict Privacy responsibilities. Our research expands previous measurements of the DNS privacy ecosystem, which usually focus on the impact of encryption on DNS performance [28], [29], [30] and the analysis of encrypted DNS traffic [31],

[32], [33]. In contrast, we provide the first longitudinal and comprehensive evaluation of the entire DNS/SP ecosystem with the following contributions.

- We conduct monthly scans of the DoT/DoH adoption in recursive resolvers. In particular, we design a new search approach with 24 test suites that find nearly 28 times more open DoH servers than the recent result in 2021 [33].[1] And to comprehensively study the server-side adoption of DoT/DoH, we also perform daily measurements of DoT/DoH deployments in authoritative servers. Furthermore, we collect a dataset of DNS/SP servers by using Subject Alternative Name (SAN), PTR record, and some public lists.
- For the first time, we perform daily scans of the deployment of TLS/HTTPS-related security features in DNS/SP servers and rate them on four levels based on the benefits and complexity of security features. Particularly, we implement a DoT/DoH server search engine and recommender system[2] that visually displays all measurements on the world map to help Internet users choose close and reliable DNS/SP servers.
- Furthermore, we perform in detail the first inspection of Chrome, Firefox, Edge, Brave, and Opera for the DoT/DoH implementation in Windows, Linux, macOS, and Android.
- At last, we discuss the current hindrances and controversies to the development of DNS privacy and propose initiatives to the Internet community.

Note 1: In this paper, if we do not clarify it explicitly, the data we use was collected on September 11th, 2022.

Taken together, our results suggest that DNS Strict Privacy has a long way to go. The actual configuration has not kept pace with the rapid adoption, and our main findings are as follows.

- During our scan, the numbers of DoT and DoH servers in recursive resolvers increased by 15.89% and 11.98%, respectively. Unfortunately, 60.78% of DoT and 44.05% of DoH recursive resolvers are configured with invalid certificates in the worst case.
- Among recursive resolvers, we observe that the top five DoH organizations operate 57.05% of DoH servers. In addition, 71.74% of DoH servers are clustered in five countries, and the USA accounts for 34.43%. The above data confirm the centralization problem in public DoT/DoH, i.e., public DoT/DoH servers are operated mainly by a small set of service providers and are concentrated in a few countries.
- We find that only 0.45% of DoH-SP servers in recursive resolvers deploy DANE correctly, 1.73% advocate OCSP Must-Staple, and 9.37% support HSTS. Furthermore, according to our rating criterion, 25.84% of DoH-SP servers in recursive resolvers fail to meet the minimum requirements.
- All five browsers only support DoH and generally enforce the Strict Privacy profile well. However, only Firefox in Windows and Linux supports CRL/OCSP to detect the revocation status of the DoH server certificate, but it accepts responses from the DoH server that does not provide the SAN certificate.

Note 2: Due to the rules we used for assembling the DNS/SP list, the real configuration of DoT/DoH servers would be **far worse** than our analysis result on DNS/SP servers. The details of the applied rules can find in Section IV-A.

To help other scholars and Internet players reprise and expand our research, we publish our code and data at

https://lrxgoat.github.io

II. Background

In this section, we first outline the background of DoT and DoH, as well as the factors hindering their development. Then, we briefly describe the security mechanisms of the TLS and HTTPS ecosystem that we investigate in this paper.

A. DNS Privacy Ecosystem

DNS acts like a phonebook containing mappings between domain names and IP addresses that help users access Internet resources. Almost all activities on the Internet start with a DNS query; however, the DNS traffic is very vulnerable to malicious monitoring and tampering due to its clear-text transmission over UDP on port 53 [2].

1) DoT & DoH: To protect user privacy, DNS over TLS (DoT), standardized in 2016 [4], utilizes TLS to encrypt and wrap DNS packets. By default, the DoT client first negotiates a TLS connection with the DoT server on port 853, and then all DNS requests and responses are encrypted and transported through TCP. However, since DoT uses a dedicated port, it is easy for attackers to identify and block the DoT traffic.

DNS over HTTPS (DoH), standardized in 2018 [5], can solve the above problem of DoT. In particular, the DoH server and the DoH client communicate with each other through the HTTP method (GET, POST, and JSON) after completing the TLS handshake on port 443, making it difficult for attackers to distinguish the DoH traffic from the regular HTTPS traffic. Furthermore, DoH is easily adopted by browsers that support HTTPS well.

2) Privacy Profiles: There exist two privacy profiles for DoT, namely Opportunistic Privacy profile and Strict Privacy profile [12]. The former requests the DoT server and client to establish an encrypted and authoritative connection. If any of the corresponding requirements fails, the communication would fall back to the non-authoritative one or, even worse, to the clear-text one. In contrast, the fallback action is forbidden in the latter privacy profiles, and the communication would be terminated instead. Unlike DoT, DoH only supports the Strict Privacy profile with the help of HTTPS. According to the requirements of TLS and HTTPS, the Strict Privacy profile has the following two premises [12]: 1) The server should provide *a PKIX certificate* or *a DNSSEC-validated chain to a TLSA record*. 2) The client should obtain the IP address and corresponding domain name of the connecting server.

[1]Another possible reason is that the number of DoH servers grow a lot during this period.

[2]https://dns-sp.info

3) Stumbling Block: The unreliable servers and the centralization problem are the main obstacles to the development of DoT/DoH [34]. However, choosing a reliable DNS privacy server is difficult if the client does not have the corresponding list. Currently, Internet users generally select the DNS privacy server in the default configuration or publicized by some large organizations. While this can prevent some ISPs from selling user DNS data, it undoubtedly exacerbates the already criticized centralization problem [35]. Furthermore, the resulting geographic centralization of DNS resolution increases the delay caused by DNS encryption to a certain extent [29]. This paper provides a DNS/SP server list and the corresponding map with ranking, which would be a meaningful attempt to alleviate the above problems.

B. TLS and HTTPS Related Mechanisms

Many works [36], [37], [38], [39], [40], [41] show that TLS and HTTPS are insufficient to provide a secure and encrypted channel between client and server. Hence, this paper investigates the corresponding supplementary mechanisms for DoT/DoH.

1) Authentication Credential: The server is under threat from an unreliable Certificate Authority (CA) when using the certificate as an authentication credential, such as `DigiNotar` compromise [14]. DNS-based Authentication of Named Entities (DANE) [16] is one of the mechanisms to solve this problem. It works as follows. The server first publishes a DNS record called TLS Authentication (TLSA) to instruct the client on how to verify the certificate. After that, the client verifies the integrity of the server's TLSA record using Domain Name System Security Extensions (DNSSEC) [41]. Finally, the client checks whether the certificate delivered by the server is consistent with its TLSA record.

2) Mis-Issuance Protection: The primary framework for monitoring and auditing certificates is Certificate Transparency (CT) [17], which contains the following three steps. A CA or server should first obtain a Signed Certificate Timestamp (SCT) from CT logs after submitting a valid certificate chain to them. After that, the server can deliver the SCT to the client via certificates extension, TLS extension, or Online Certificate Status Protocol (OCSP) stapling during the TLS handshake. At last, the client gets the promise that the CT log contains the server's certificate through verifying SCT. Moreover, the `Expect-CT` field is added to the HTTP header [18] to ensure the execution of CT. It is worth mentioning that some browsers like Chrome [42] and Safari [43] already enforce the CT policy independently of Expect-CT. Furthermore, there is another mis-issuance protection mechanism named Certification Authority Authorization (CAA) [19]. It indicates which CA can issue a certificate for a domain but does not mandate DNSSEC.

3) Certificate Revocation: Certificate revocation serves as a remedy in the event of a leaked private key or mis-issued certificate [44], rendering the certificate invalid before it expires. Certificate Revocation List (CRL) [20] is the earliest revocation mechanism; however, it requires the client to download the CRL file, which brings considerable delay and burden to the client.

To alleviate the delay and burden, OCSP [21] enables the client to obtain only the revocation status of a single certificate. However, OCSP still requires the client to perform additional queries and exposes the user's browsing behavior to the CA.

To further relieve the client's pressure from the Certificate revocation and user privacy concerns, OCSP Stapling [22] stipulates that the server obtains the certificate's revocation status from the CA in advance and then sends it to the client during the TLS handshake. However, some clients still accept certificates when they cannot obtain the revocation information. In contrast, an X.509 certificate extension called OCSP Must-Staple [23] instructs the client to block the connection if a stapled OCSP response is not received during the TLS handshake.

4) Downgrade Protection: To prevent the client from vulnerabilities in low TLS versions, Signaling Cipher Suite Value (SCSV) [24] is designed to avoid downgrade from TLS 1.2 and below. During the TLS handshake, if the server supports a higher TLS version than the client does, and `TLS_FALLBACK_SCSV` is included in the ClientHello packet, then the server must return an alert and terminate the corresponding connection.

TLS 1.3 has its own downgrade protection [25]. Suppose a TLS 1.3 server finds that it can only negotiate TLS 1.2 or below with the client. In that case, the server labels the downgrade with a particular value set in ServerHello.random. And then, the client would abort the connection according to the particular value.

Furthermore, the HTTP Strict Transport Security (HSTS) [26] can prevent TLS stripping attacks by instructing the client only to access the domain via HTTPS.

III. DoT and DoH Server

This section introduces our approach to obtaining public DoT/DoH server datasets covering both recursive resolvers and authoritative servers. After that, we analyze their evolution and centralization problem.

A. Datasets

Without considering the cache case, a complete DNS query process is initiated from the client to the recursive resolver. And then, the recursive resolver lookups the root name server, TLD name server, and authoritative name server successively. Finally, the recursive resolver returns the query result to the client [1]. Therefore, we need to obtain comprehensive DoT/DoH server datasets covering both recursive resolvers and authoritative servers to describe the landscape of DNS/SP services.

1) Recursive Resolver: We have two main steps for discovering DoT/DoH recursive resolvers. We first find all DoT/DoH servers that open their service to the public, and then we verify whether each of them is still a recursive resolver. Regarding the first main step. We begin with using Zmap [45] to discover IP addresses opening port 853 or 443, which correspond to

DoT and DoH, respectively. After that, we need to confirm which IP address indeed provides the DoT/DoH service. For the DoT service, we first establish a TLS connection with the IP address that opens port 853 and then initiate an A record request for a domain through TCP. If we get a correct DNS response, it has the DoT service in this IP address. It is more complex for the DoH case. Based on previous research [13], [33], [46], we combine 24 test suites to send DNS requests over HTTPS for each IP address with open port 443. Firstly, we have four common path templates, including `/dns-query`, `/query`, `/resolve`, and `/`, for constructing URI templates (e.g., https://8.8.8.8/dns-query). Secondly, we use three request methods, including GET, POST, and JSON. Thirdly, DoH servers accept requests via HTTP/1 or HTTP/2. If the HTTP response status code is 200, and the `Content-Type` field of the HTTP response header is "application/dns-message" for GET/POST or "application/dns-json" for JSON, then we confirm that the IP address provides a DoH service.

Regarding the second main step. We use the kdig 3.1.4 [47] to set the Recursion Desired (RD) flag in the DNS request header and initiate encrypted A record queries to DoT/DoH servers. If the server returns with the Recursion Available (RA) flag set in their DNS responses, we consider the server as a recursive resolver.

At last, by adding some public DoT/DoH server lists,[3] we can obtain the comprehensive DoT/DoH server dataset covering recursive resolvers. From November 2021 to September 2022, we repeated the above scanning process every month.

2) Authoritative Server: Regarding root name servers, operators are reluctant to implement authoritative DNS encryption due to concerns about DDoS attacks and performance [48]. Hence, we only focus on TLD and authoritative name servers here.

Considering the following reasons, we cannot use the method of identifying recursive resolvers to construct our authoritative server dataset. First, distinguishing authoritative name servers from TLD name servers is difficult. Second, determining which domain an authoritative server is authoritative for is difficult. Therefore, we first obtain the list corresponding to TLD and authoritative name servers and then verify whether servers provide DoT/DoH services.

We get possible servers by scanning the NS records of the TOP domain list and TLD list [49]. The TOP domain list includes 3M unique domains after merging Alexa TOP-1M [50], Majestic TOP-1M [51], Umbrella TOP-1M [52], and Tranco TOP-1M [53]. After that, we use the same method as in the recursive resolver case to identify DoT/DoH servers. From January 2022 to September 2022, we repeated the above scanning process every day (TOP domain list and TLD list are updated monthly).

In addition, we use ip-api [54] to obtain the organization, geographic location, country, and autonomous system (AS) information of all DoT/DoH servers for further analysis.

[3]Lists and sources of public DoT/DoH servers are available at https://lrxgoat.github.io

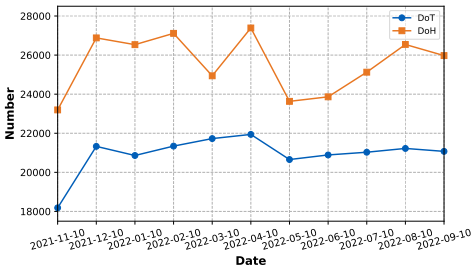


Fig. 1. Number of DoT/DoH recursive resolvers over time.

Particularly, to investigate the impact of vantage points on our measurements, we measure the number and configuration of the global DoT/DoH server from Hong Kong (AS45102), Virginia (AS45102), and Frankfurt (AS45102), respectively. The results show little difference in the measurements of the three vantage points. Therefore, this paper uses data measured from Hong Kong.

3) Ethical Considerations: One of our ethical considerations is the burden that active scanning places on servers, which we mitigated by limiting the rate of requests and not making malicious requests. Another ethical consideration is to respect the willingness of the server to refuse scanning. For example, we found that 512 DoH servers belonging to `Control D` [55] were unavailable for a period of time during the scan. We emailed the company to report the situation and got a reply saying that all these DoH servers are private resolvers and we are not authorized to use them. Therefore, we excluded these IP addresses from the measurement.

B. DoT and DoH Adoption

We first investigate the popularity of DoT/DoH among recursive resolvers and authoritative servers by the number of servers and focus on analyzing the configuration of DoT/DoH servers.

1) Open Server: According to our scan results, the numbers of IP addresses opening port 853 and port 443 are stable at around 3M and 53M, respectively. This statistical data is not much different from the previous measurement results [13], [33]. However, open DoT and DoH servers have increased significantly. Specifically, we found 22K open DoT servers in September 2022, while Doan et al. [56] found only 2.1K in January 2020. Furthermore, our DoH server list contains nearly 28 times more servers than the recent result in [33]. In addition, nearly 99.3% of open DoT/DoH servers can provide recursive query capabilities.

2) Recursive Resolver: As shown in Figure 1, the number of DoT/DoH servers is on the rise overall, and DoH has gained greater favor among recursive resolvers. In the following, we analyze TLS versions and certificates of DoT/DoH servers.

As shown in Table I, the ratio of TLS 1.3 in DoT servers significantly increased compared to the previous result in 2020 [56] (only 20% of open DoT servers). However, the support of TLS 1.3 in DoH servers is still insufficient. In particular, 1421 DoH servers operated by `Scape Reach` [57] only support TLS 1.2. Unfortunately, 3812 (18.09%) DoT and

TABLE I
STATISTICS OF TLS VERSIONS SUPPORTED BY DOT/DOH SERVERS

	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
Recursive				
DoT	3269 (15.51%)	3812 (18.09%)	17986 (85.35%)	14855 (70.49%)
DoH	9801 (37.73%)	10037 (38.64%)	23713 (91.30%)	14315 (55.11%)
Authoritative				
DoT	110 (37.29%)	115 (38.98%)	261 (88.47%)	229 (77.63%)
DoH	14 (22.95%)	15 (24.59%)	59 (96.72%)	47 (77.05%)

TABLE II
STATISTICS OF BASIC CONFIGURATION OF DOH SERVERS

	Recursive	Authoritative
Path Template		
/dns-query	9501 (36.58%)	51 (83.61%)
/query	5855 (22.54%)	2 (3.28%)
/resolve	5529 (21.29%)	3 (4.92%)
/	5089 (19.59%)	5 (8.20%)
HTTP Method		
GET	18130 (69.80%)	58 (95.08%)
POST	24968 (96.13%)	58 (95.08%)
JSON	8919 (34.34%)	4 (6.56%)
GET & POST	17128 (65.94%)	55 (90.16%)
HTTP Version		
HTTP/1	23307 (89.73%)	61 (100%)
HTTP/2	23049 (88.74%)	61 (100%)
HTTP/1 & 2	20382 (78.47%)	61 (100%)
GETH2 & POSTH2	16526 (63.63%)	53 (86.89%)

10051 (38.70%) DoH servers still support deprecated TLS versions.[4]

Regarding server certificates,[5] we find that 12633 (59.95%) DoT server certificates are invalid, which is worse than the measurement in 2019 [13] (8% of open DoT servers). Surprisingly, self-signed certificates account for 34.58% of invalid certificates, and the CA field in them is mostly "Fortinet" (72.12%). The situation is slightly better for the DoH server. Specifically, 11226 (43.22%) certificates are invalid, and 8464 invalid certificates are self-signed.

Overall, the above results show that the secure communication assurance of DoT and DoH has not kept pace with their rapid adoption. We focus on analyzing the basic configuration of DoH servers in the following.

First, we observe that 4679 (41.83%) DoH IP addresses support only one path template, while 3095 (27.67%) support all four path templates. As shown in Table II, we cannot find all DoH IP addresses by only using the `/dns-query` path template, which only results in 84.94%. This situation is due to the absence of a standardized DoH path template. Fortunately, if we further use path templates `/query` and `/`, we can obtain 99.21% of DoH IP addresses. Therefore, we recommend that future active scans of DoH servers adopt this new advantage.

Second, as shown in Table II, only 17128 (65.94%) DoH servers support both GET and POST, which MUST be satisfied by DoH servers as specified in RFC 8484 [5]. Furthermore, 8919 DoH servers support JSON, and most of them (78.92%) belong to `NextDNS` [59]. Surprisingly, six of these DoH servers only support the JSON method, while all the corresponding IP addresses support GET or POST on other path templates.

[4]For TLS versions less than 1.2, we call them deprecated TLS versions [58].

[5]Since the DoT/DoH recursive resolver list only contains IP addresses, we do not compare domains when validating certificates for DoT/DoH recursive resolvers.

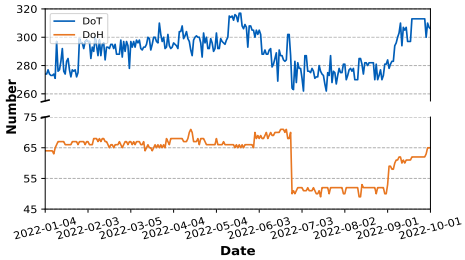


Fig. 2. Number of DoT/DoH authoritative name servers over time.

We guess these six DoH servers may be implemented for specific needs or experimental purposes.

Third, there exist 2925 (11.26%) DoH servers only supporting HTTP/1, while RFC 8484 [5] stipulates that HTTP/2 is the minimum RECOMMENDED version of HTTP for DoH use. Furthermore, as we can see from Table II, 20382 (78.47%) DoH servers support both HTTP/1 and HTTP/2 for compatibility with older client software.

Overall, only 16526 (63.63%) DoH recursive resolvers follow the RFC well (simultaneously supporting GET, POST, and HTTP/2). Hopefully, our measurements could drive the norm for DoH implementations.

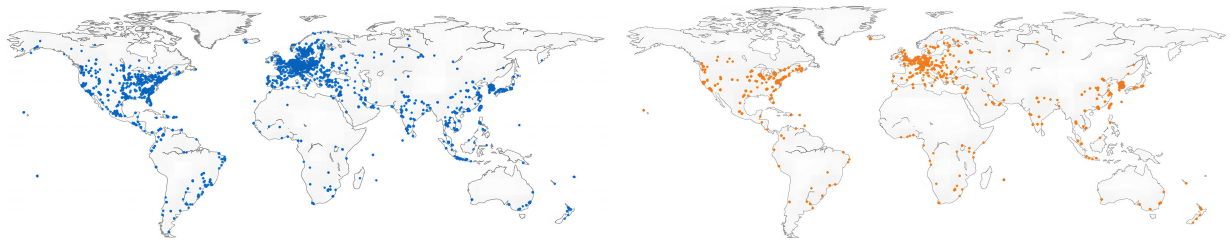
3) Authoritative Server: Although DoT and DoH between recursive-to-authoritative are not standardized, their privacy issues between them have also attracted widespread attention [48], [60]. However, to the best of our knowledge, no existing work measures the deployment of DoH in authoritative servers. Furthermore, only Deccio et al. [61] measured DoT support in authoritative servers in 2019. They only found 12 DoT authoritative name servers and no DoT TLD name server.

During our entire scan, we could not find any TLD name server supporting DoT or DoH. For authoritative name servers, we found 295 DoT and 61 DoH servers on September 11th, 2022. As shown in Figure 2, the number of DoH authoritative name servers declined on June 26th, 2022. The reason is that the 20 servers authoritative for ndnslab.com no longer provide DoH services. We also note that DoT and DoH authoritative name servers are authoritative for 3843 and 226 domains in the TOP domain list, respectively. Considering organizations, we observe that 116 different organizations provide DoT services, with `Onavo Mobile` (9.76%) and `Facebook` (9.41%) relatively large. DoH is more concentrated, with only 29 different organizations operating DoH servers, and `Google` (20.75%) accounts for about a quarter. Therefore, it is fair to say that DoT is more popular than DoH in authoritative servers.

However, the configuration of the DoT server is not satisfactory. From Table I, we can see that more than half of DoT servers support deprecated TLS versions. Furthermore, 166 (56.27%) DoT server certificates can not be verified, of which 27.10% are expired and 66.27% are self-signed. Fortunately, 46 (75.41%) DoH server certificates are valid, and 53 (86.89%) DoH servers follow the RFC well.

C. DoT and DoH Centralization

Centralization has heightened concerns among Internet users about the single point of failure and their browsing



(a) DoT (b) DoH

Fig. 3. Global distribution map of DoT/DoH recursive resolvers.

TABLE III
STATISTICS OF ORGANIZATION, COUNTRY, AND AS FOR DOT/DOH RECURSIVE RESOLVERS

DoT		DoH	
Organization		**Organization**	
NextDNS	2268 (10.76%)	NextDNS	7911 (30.46%)
Hot-Net Internet	1869 (8.87%)	CONY BRAKE	3142 (12.10%)
BroadNet	1163 (5.52%)	Scape Reach	2199 (8.47%)
Cloudflare	1025 (4.86%)	Controld	862 (3.32%)
CleanBrowsing	1020 (4.84%)	Win Soon Lee	700 (2.70%)
Country		**Country**	
United States	4290 (20.36%)	United States	8943 (34.43%)
South Korea	2494 (11.84%)	South Korea	3180 (12.24%)
Israel	1720 (8.16%)	India	2967 (11.42%)
Canada	1383 (6.56%)	France	1853 (7.13%)
Germany	1254 (5.95%)	Canada	1693 (6.52%)
AS		**AS**	
AS34939	2479 (11.76%)	AS34939	8125 (31.28%)
AS12849	1843 (8.75%)	AS55303	5628 (21.67%)
AS9318	1186 (5.63%)	AS398962	862 (3.32%)
AS13335	1031 (4.89%)	AS15557	713 (2.75%)
AS205157	1018 (4.83%)	AS797	711 (2.74%)

patterns being tracked. We evaluate the current situation of centralization in public DoT/DoH recursive resolvers in terms of organization, geographic location, country and AS. As shown in Table III, we observe that the top five DoT and DoH organizations operate 7345 (34.85%) and 14814 (57.05%) servers, respectively. In addition, we find that 7051 (33.46%) DoT and 17234 (66.35%) DoH IP addresses are operated by organizations that have at least 100 IP addresses.

In Figure 3, we can see that the physical location of DoH servers is more concentrated than that of DoT servers, even though there are more DoH servers. One possible reason for this centralization is that large DNS providers deploy the DNS privacy services on the CDN servers that are mostly co-located. As shown in Table III, 11141 (52.87%) DoT and 18636 (71.74%) DoH servers are clustered in the top five countries. Furthermore, DoT and DoH servers are distributed over 1570 and 661 ASes, respectively. In particular, AS34939 is hosting 8125 (31.28%) DoH servers. According to the above data, we can conclude that the centralization problem of public DoH is more severe than that of public DoT.[6] One promising solution under the current situation is to provide an exhaustive well-configurated DNS/SP servers list for Internet users, which we give in the next section.

IV. DOT-SP AND DOH-SP SERVER

In this section, we first introduce the construction of our DNS/SP recursive resolver list (Section IV-A). After that, we analyze DNS/SP recursive resolvers (sections IV-C.1-IV-C.5) and authoritative name servers (Section IV-C.6). Finally, we evaluate the security level of DNS/SP recursive resolvers (Section IV-D) and compare them with HTTPS servers (Section IV-E).

A. Datasets

It is impossible to measure the deployment of TLS/HTTPS-related security features of servers without the corresponding domains. Hence, the first task is to complement the IP addresses of DoT/DoH recursive resolvers we obtained in Section III-A. Since there is no standard method to get the correct corresponding domain based on IP addresses dynamically, we ask for help from SAN extensions and PTR records containing domain information we could use.

We first obtain the certificate to fetch the DNS names in the SAN extension that lists all domains associated with the certificate [63]. Particularly, we perform a TLS handshake with each DoT and DoH IP address on ports 853 and 443, respectively. However, we still need to filter out the collected domains from SAN extensions for the following reasons. Specifically, one IP address may serve different domains on the same port, and one certificate could be associated with other domains that do not provide the DoT/DoH service. Combining previous reports [33], [64], we apply the following filtering rules on the domains without any wildcard. 1) It contains "dns" or "dot" on port 853. 2) It contains "dns" or "dot" on port 443. If none of the domains without any wildcard satisfies the above rules, we get the domain from the domains allowing a wildcard by retaining the right part of the wildcard.[7] For instance, we get "dns.com" for "*.dns.com".

Compared to the SAN extension, the PTR record directly shows the relationships between IP addresses and domains. However, we still need to filter the collected domains by applying the same rules used in the case of SAN extensions, as one IP address may serve different domains.

After the above two methods, we obtain a candidate list of DoT/DoH servers with corresponding (IP address, domain name) pair, i.e., a candidate list of DNS/SP servers. Note that the candidate list contains public DoT/DoH server lists we mentioned in Section III-A.1.

To ensure that all the (IP address, domain name) pairs in the candidate list are the correct ones for DoT/DoH servers, we re-check them by using the method applied in Section III-A for finding DoT/DoH servers and specifying the domain as the

[6]Since few players deploy encrypted DNS compared to traditional DNS [62], the centralization of DoT/DoH services would not significantly affect the DNS ecosystem.

[7]According to [65], more than one wildcard in a domain is not allowed, which is also reflected by our collected domains.

value of the SNI field. We use the result as our list of DNS/SP recursive resolvers, which we update monthly.

Specifically, 46.53% of DoT and 47.29% of DoH recursive resolvers obtain the corresponding domains. However, when looking for domains using SAN extensions, we observe that many of the filtered DNS names in the DoT and DoH recursive resolver certificates are in the form "FG*" (43.26%) and "bb-in" (45.35%), respectively. Digging deeper, we find that most of these DoT server certificates are issued by "Fortinet" (87.32%), and most of them belong to SFR (34.38%). This is probably because SFR delegates its security management to FortiGuard Labs [66]. Considering DoH, the CA filed in most of these certificates is "bb-in" (99.27%), and most of these certificates belong to Scape Reach [57] (43.87%). This may be due to the partnership between Scape Reach and the Hong Kong Broadband Network[8] [67]. Note that these certificates are all invalid and account for 25.37% of DoT and 24.95% of DoH server datasets. According to our rules, the list of DNS/SP recursive resolvers won't contain the DoT/DoH servers corresponding to "FG*" and "bb-in", which clearly cannot satisfy the security requirement. Therefore, the configuration of the DoT and DoH recursive resolvers is **far worse** than our subsequent analysis of DoT-SP and DoH-SP recursive resolvers.

Limitation. We are aware of some limitations of our data collection methods, including the lack of local private servers and IPv6 addresses, the rules we use to filter the domains collected from SAN extensions and PTR records, and how we deal with the domains with a wildcard. However, we believe that our method is still a meaningful attempt to find DNS/SP servers.

B. Measurement Process

To show the landscape of DNS Strict Privacy, we measure various security features of TLS and HTTPS for DNS/SP servers. Specifically, TLSA records and CAA records of the DNS/SP server are collected from DNS, and other data are obtained via performing TLS negotiation with DoT-SP and DoH-SP servers on ports 853 and 443, respectively.

1) Authentication Credential: We use Mozilla Root CA certificates [68] to verify the certificate chain of the DNS/SP server. For DANE-TLSA, we use UNBOUND [69] to get the TLSA records of the DNS/SP servers and perform DNSSEC verification. Then we complete the verification of DANE according to the Certificate Usage, Selector, Matching Type, and Certificate Association Data fields in the TLSA record and the certificate chain of the DNS/SP server.

2) Mis-Issuance Protection: Recall the mis-issuance protection. It contains CT, Expect-CT, and CAA. The measurement of CT is related to the existence and verification of SCTs, which can be found in the certificate extension, TLS extension, and OCSP Stapling. To measure Expect-CT, we need to send an HTTP HEAD request to the DNS/SP server that successfully establishes a TLS connection and check whether the HTTP response header contains the Expect-CT field. At last, CAA records can be obtained via UNBOUND.

3) Certificate Revocation: As we mentioned before, certificate revocation mechanisms contain CRL, OCSP, OCSP Stapling, and OCSP Must-Staple. Hence, we need to determine which mechanism the server uses. The first, second, and last ones can be respectively decided by using the CRL server URL, OCSP server URL, and extension OID in the certificate extension. The third one can be nailed down by the OCSP response in the TLS extension.

After that, we can check the revocation status of the certificate accordingly. We need to request the CRL server and OCSP server for the first two mechanisms, respectively. However, no additional request is needed for OCSP Stapling. Note that besides the revocation status, we also need to verify the signature of the CRL and OCSP responses. At last, we check the supporting status of OCSP Stapling for the OCSP Must-Staple case.

4) Downgrade Protection: If the DNS/SP server can support TLS 1.3, we then negotiate with the server using TLS 1.2, TLS 1.1, and TLS 1.0 in order. After that, we check whether the last 8 bytes of the ServerHello.random match the particular value that identifies the downgrade. If the DNS/SP server only supports TLS 1.2, we use TLS 1.1 to handshake with the DNS/SP server and include TLS_FALLBACK_SCSV in the Clienthello cipher suite. Then we observe whether the DNS/SP server returns an alert and terminates the connection.

Detection of HSTS is similar to Expect-CT. In particular, we check whether the Strict-Transport-Security field exists in the HTTP response header.

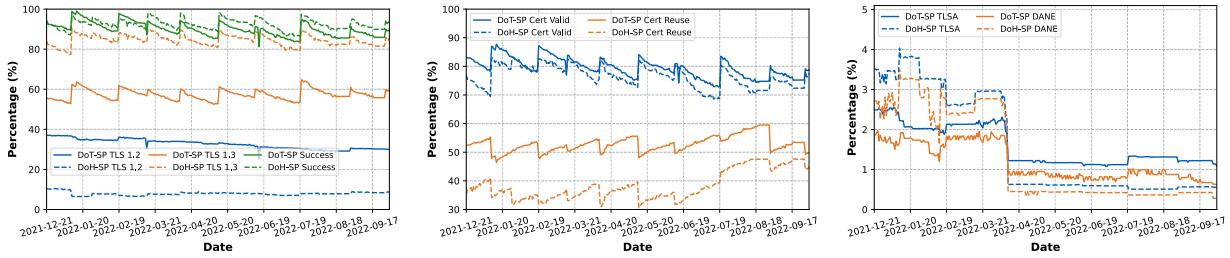
C. DoT-SP and DoH-SP Management

For a more persuasive and accurate evaluation of the data we collect as above, we only keep one piece of data for one domain if different (IP address, domain name) pairs have the same domain. The main reason for the filtering is that one domain usually corresponds to one configuration, even if the domain is associated with many IP addresses [36], [70].

1) Availability: The availability of TLS service is the paramount premise for using the Strict Privacy profile on the client-side. Figure 4(a) plots the availability and version of TLS connections in DNS/SP servers over time. It is easy to see that DNS/SP servers show a slight downward trend after each update of the dataset, leading to a similar trend in the deployment of valid certificates (Figure 4(b)), CT (Figure 6(a)), and OCSP (Figure 6(b)). This situation may be due to domain change or service unavailable of the DNS/SP server. Compared to the data in Table I, the ratio for supporting TLS 1.3 in DoH servers increases, while that in DoT servers decreases. This change is mainly due to the data filtering rule for (IP address, domain name) pairs. For example, 3051 domain names in the DoT-SP dataset before deduplication are "dns.nextdns.io", and all of these servers support TLS 1.3.

2) Authentication Credential: **Certificate.** As shown in Figure 4(b), we find that the proportion of DoH-SP servers with valid certificates is lower than that of DoT-SP, which is

[8]bb-in may be short for Broadband internet.



(a) Availability (b) Certificate (c) DANE-TLSA

Fig. 4. Proportions of availability and authentication credential mechanisms deployed in DNS/SP recursive resolvers over time.

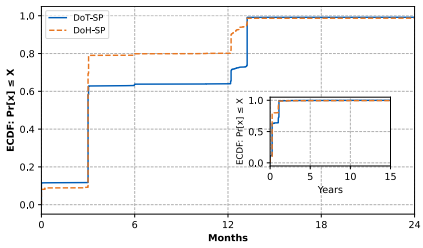


Fig. 5. Distribution of certificate lifetime for DNS/SP recursive resolvers.

different from the expected case since DoH-SP is compatible with HTTPS well.

After counting the number of valid certificates, we further analyze the invalid certificates, certificate lifetime, and certificate reuse.

The most common error for certificate verification failures is the certificate expiration according to the collected data. Specifically, 212 (41.81%) and 137 (48.24%) invalid certificates in DoT-SP and DoH-SP servers are expired, respectively. Furthermore, 23 (4.54%) and 54 (19.01%) invalid certificates in DoT-SP and DoH-SP servers are self-signed, respectively. Hopefully, the server administrator could update the certificate from a reliable CA in time.

From the security viewpoint, the shorter the lifetime of a certificate, the better, which can effectively reduce the harm caused by CA compromise, private key leakage, and website impersonation [71]. Figure 5 plots the cumulative distribution of certificate lifetimes for DNS/SP servers. We find that 284 (12.62%) DoT-SP and 105 (9.55%) DoH-SP servers' certificates have a certificate lifetime of greater than 398 days. It violates the rules of `Apple` [72], `Mozilla` [71], and `Google` [73]. Furthermore, we find the certificate lifetime of 14 DoT-SP and 13 DoH-SP servers is over 825 days, which would be potentially risky, as shown in [74].

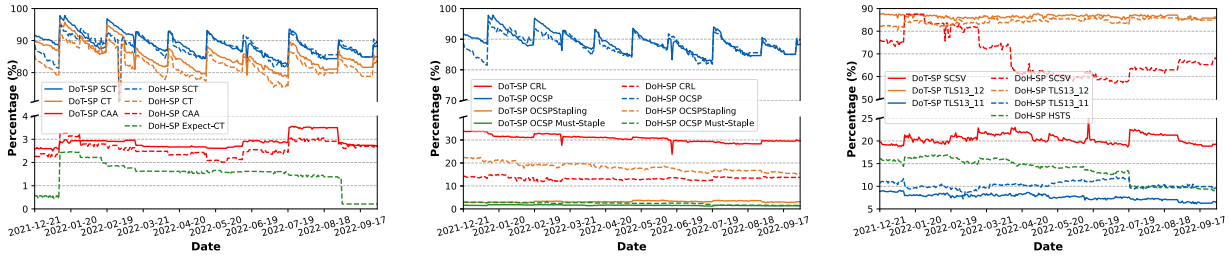
The popularity of CDN services and multi-domain certificates dramatically facilitates the realization of certificate sharing among multiple servers [63], but also aggravates the security risks caused by private key leakage and certificate misuse. We show the upward trend of certificate reuse in DNS/SP servers in Figure 4(b), especially DoH-SP servers. Furthermore, we notice that the certificate reuse ratio of DNS/SP servers goes up sharply right after each dataset update. It is mainly due to the criteria of certificate reuse. In particular, we only consider available servers that allow certificate reuse. As shown in Figure 4(a), the number of available servers goes down after each dataset update, and the servers becoming unavailable usually do not share certificates with others. However, certificate reuse is still a non-negligible problem. Specifically, 1103 DoT-SP and 479 DoH-SP servers reuse the certificate. Unfortunately, we found 11 DoH-SP servers using the same expired certificate on April 11th, 2022. Furthermore, 41.34% of the certificates for DoT-SP servers are find in DoH-SP servers, and conversely, 38.56% for DoH-SP servers. However, this certificate reuse may cause DoT and DoH services to fail simultaneously, and we find 29 such DNS/SP servers.

Additionally, the centralization problem exacerbates certificate reuse as server operators usually share certificates for convenience. For example, there exist 524 DoT-SP servers sharing the certificates, and all of them belong to `CleanBrowsing` [75]. These certificates should be maintained carefully; otherwise, all 526 servers would be out of service simultaneously.

DANE-TLSA. DANE-TLSA is another way to ensure the authoritativeness of DNS/SP servers, which is protected by DNSSEC. We find that 1180 (52.45%) DoT-SP and 532 (48.41%) DoH-SP servers correctly support DNSSEC, indicating that DNSSEC is not the primary factor hindering support for DANE-TLSA. As shown in Figure 4, we observe that DNS/SP servers' support for DANE-TLSA dropped by about 2% after April 11th, 2022, and DoH-SP servers were more severe. This is mainly because the servers belonging to `Danmarks Tekniske Universitet` and `Kracon ApS` no longer provide DNS encryption services. Additionally, 84.12% of DoT-SP and 85.71% of DoH-SP servers with TLSA records deploy DANE correctly. Two main reasons for the DANE verification failure are 1) mismatch between the certificate and the TLSA record and 2) invalid DNSSEC.

3) Mis-Issuance Protection: **CT.** Only if a DNS/SP server can provide a valid SCT, we consider it as the one supporting CT. As shown in Figure 6(a), most DNS/SP servers are under the protection of CT. Specifically, 1889 (83.96%) DoT-SP and 902 (82.07%) DoH-SP servers can provide valid SCTs. All valid SCTs can be found in the certificate, and some of them also are delivered via OCSP Stapling. However, none of the valid SCT is transmitted by TLS extension. The main reason for this delivery situation is that the SCT delivered via a certificate only requires effort from the CA, while the other two ways need to burden the server operator.

`Google` released its new CT policy [76] in March 2022. It states that certificates issued before April 15th, 2022, should still follow the old CT policy, i.e., they are logged



(a) Mis-Issuance Protection (b) Certificate Revocation (c) Downgrade Protection

Fig. 6. Proportions of mis-issuance protection, certificate revocation, and downgrade protection mechanisms deployed in DNS/SP recursive resolvers over time.

by at least one Google CT log and one non-Google CT log. Unfortunately, we find that 549 (24.40%) DoT-SP and 161 (14.65%) DoH-SP server certificates violate this requirement. Moreover, as stated in [76], for certificates issued on-or-after April 15th, 2022, `Google` delegates the power of logging certificates to other CT logs. Specifically, certificates with a lifetime of 180 days or less are required to be logged by two different CT logs, and other certificates are logged by three different CT logs. All of these distinct CT logs could be non-Google. If all DNS/SP servers still keep their current certificate management after April 14th, 2022, we find that there would be more 1.04% of DoT-SP and 2.28% of DoH-SP server certificates violating the CT policy. These data indicate that the updated CT policy does not impact the current operation of the CT framework in DNS/SP servers.

Expect-CT. In Figure 6(a), it can be seen that DoH-SP servers have a drop in support for Expect-CT. This phenomenon is inseparable from the possible obsolete of Expect-CT [77] due to some browsers enforcing CT [42], [43]. Among the DoH-SP servers that support Expect-CT, only two servers set the `enforce` directive to instruct the client to terminate the connection when the server violates the CT requirements. Furthermore, eight servers use the value of URI in the `report-uri` directive to indicate the address clients should report Expect-CT failures to, and six addresses are Cloudflare.

CAA. As shown in Figure 6(a), we find that only around 3% of DNS/SP servers support CAA. What's worse, not all CAA records are followed by CAs. In particular, 70.18% of DoT-SP and 55.56% of DoH-SP servers' CAA records are followed by CAs. Almost all CAs following the CAA records are `Let's Encrypt`. This poor situation of CAA may give another reason that clients typically do not consider CAA check errors as a criterion for server violations [78].

4) Certificate Revocation: Figure 6(b) shows the trend of the support of certificate revocation mechanisms in DNS/SP servers. It is easy to see that OCSP is greatly supported in DNS/SP servers, but OCSP Stapling and OCSP Must-Staple are rarely deployed. Specifically, 149 (13.56%) and 19 (1.73%) DoH-SP servers support OCSP Stapling and OCSP Must-Staple, respectively. However, the corresponding ratios of DoT-SP servers are only 68 (3.02%) and 31 (1.38%), respectively. In particular, `NextDNS` plays a crucial role in the deployment of OCSP Must-Staple. For example, `NextDNS` supports 11 DoH-SP servers to implement OCSP Must-Staple. Unfortunately, a relatively large number of servers (83.82% of DoT-SP servers and 74.98% of DoH-SP servers) only support CRL or OCSP, which undoubtedly burdens clients.

We also find that most DoH-SP servers supporting certificate revocation can work as expected,[9] while it is not the same situation in DoT-SP servers. In particular, only 1128 (57.38%) signatures in the OCSP responses in DoT-SP servers supporting OCSP can pass the verification, compared to 802 (82.77%) in DoH-SP servers. These errors would prevent clients from using OCSP to block revoked certificates. Additionally, only 58.06% of DoT-SP servers supporting OCSP Must-Staple send OCSP responses during the TLS handshake, compared to 94.74% in DoH-SP servers. Once clients respecting OCSP Must-Staple cannot receive the OCSP response, they may terminate the connection.

5) Downgrade Protection: **TLS downgrade protection.** In Figure 6(c), we give the trend for the ratios of DNS/SP servers that are equipped with the downgrade protection features. To give a clearer illustration, the ratios related to the different TLS versions in Figure 6(c) are computed according to the number of TLS connection versions.

We intuitively find that the SCSV supporting ratio in TLS 1.2 DoH-SP servers is significantly higher than that of TLS 1.2 DoT-SP servers. It is mainly because none of 525 TLS 1.2 DoT-SP servers from `Cleanbrowsing` can support SCSV. We also find that most TLS 1.3 DNS/SP servers return the correct particular value when we try to establish a TLS connection with TLS 1.2. In contrast, we cannot find the correct particular value in most TLS responses when we use TLS 1.1 or TLS 1.0 to establish the connection. One possible reason for this situation is that many browsers no longer support TLS 1.1 or TLS 1.0 [79], and it does not need to set the corresponding configuration in the DoT/DoH service. Furthermore, we find that 1095 (84.95%) TLS 1.3 DoT-SP and 644 (71.08%) TLS 1.3 DoH-SP servers can also support SCSV. This is probably because the server sees `TLS_FALLBACK_SCSV` as a signal to detect the downgrade.

HSTS. Since HSTS can only be found in the HTTP response, only DoH-SP servers can support it. Figure 6(c) shows that the ratio is only around 10%. Among them, 34 (33.01%) set the `preload` directive, indicating that the server's HSTS policy has been pre-embedded in the client so that no insecure connection would occur between them.

[9] If the corresponding revocation response is available and the corresponding signature verification is successful, we say that the CRL, OCSP, or OSCP Stapling work as expected. If a server provides the stapled OCSP response, we say OCSP Must-Staple works as expected.

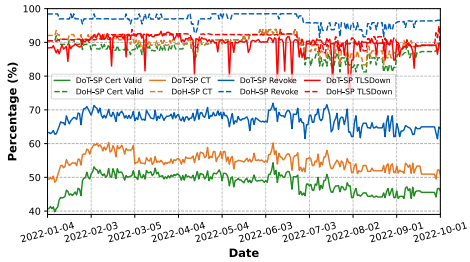


Fig. 7. Proportions of valid certificates, CT, certificate revocation, and TLS downgrade protection mechanisms deployed in DNS/SP authoritative name servers over time[10].

In addition, 58 (56.31%) set the `includeSubDomains` directive, making HSTS equally applicable to all subdomains of the site. DoH-SP servers usually set the `max-age` directive as 365 days (52.43%) or 730 days (30.10%), and four servers set it to zero. The zero value may cause the connection between the user and the server to no longer be protected by HSTS.

6) Authoritative Name Server: To more comprehensively assess the landscape for DNS/SP, we also evaluate the situation in authoritative name servers. We do not give the trend for all the security features in Figure 7, since the missing features are either unavailable or with a low supporting ratio. We can intuitively find in Figure 7 that the situation of the DoH-SP server is significantly better than that of the DoT-SP server. Specifically, the ratio of valid certificates in DoT-SP servers is about half of that in DoH-SP servers, and the reason for invalidation is mainly due to self-signed (66.27%) and expired (27.11%) certificates. Unfortunately, there are 11 DoT-SP and two DoH-SP servers with certificate lifetime zero. Furthermore, certificate reuse is widespread in authoritative name servers, reaching about 63.38% in DoT-SP and 57.69% in DoH-SP servers. Considering DANE-TLSA, although 67 (22.71%) DoT-SP servers have TLSA records (none in DoH-SP), only three can pass DANE verification, and most (59) fail due to invalid DNSSEC.

Compared to DoT-SP servers, DoH-SP servers have better support for CT. However, none of the DoH-SP servers support Expect-CT, and only two DoT-SP servers and three DoH-SP servers have CAA records. Furthermore, none of the DNS/SP servers support OCSP Must-Staple; almost all DoH-SP servers support one of CRL and OCSP at least. Remarkably, the ratio (38.32%) of DoH-SP servers supporting OCSP Stapling is much higher than that of DoT-SP authoritative name servers (5.08%) and DoH-SP recursive resolvers (20.08%). About 90% of DNS/SP servers are equipped with good protection for TLS downgrade attacks, while only two DoH-SP servers support HSTS.

D. Security Level Analysis

To describe the prospect of DNS/SP servers more intuitively, we present four rating criterions as shown in Table IV, according to the security benefit and configuration complexity of the mechanism. We do not consider HSTS, Expect-CT, or CAA in our rating standards. It is because the first two are only supported by DoH-SP servers while we aim to rank all the DNS/SP servers in a unified criterion, and the last one does not mandate DNSSEC and is usually complied by CAs.

[10]It should be noted that certificate revocation refers to supporting at least one revocation mechanism; TLS downgrade protection refers to supporting downgrade protection measures corresponding to the TLS connection version.

TABLE IV

RATING STANDARDS FOR THE SECURITY LEVELS OF DNS/SP SERVERS. EXCEPT FOR `Level-C`, THE CONDITIONS OF OTHER LEVELS MUST MEET SIMULTANEOUSLY

	TLSVer[1]	CertValid[2]	CT	CertRev[3]	TLSDownPro[4]	DANE-TLSA
`Level-S`	1.3	✔[5]	✔	✔	✔	✔
`Level-A`	1.3	✔	✔	✔	✔	○[5]
`Level-B`	1.2/1.3	✔	○	○	○	○
`Level-C`	<1.2	✘[5]	○	○	○	○

[1] TLSVer indicates the TLS version.
[2] CertValid indicates the vertificate valid.
[3] CertRev indicates any certificate revocation mechanism.
[4] TLSDownPro indicates the TLS downgrade protection.
[5] ✔ denotes deploy; ✘ denotes no deploy; ○ denotes not considering.

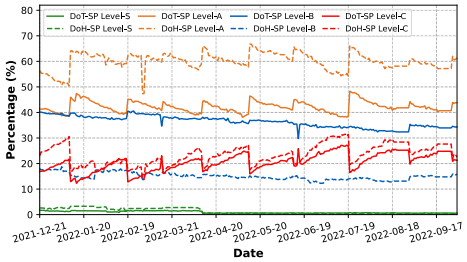


Fig. 8. Proportions of security levels for DNS/SP recursive resolvers over time.

We consider `Level-B` the minimum requirement for the DNS/SP server to satisfy the Strict Privacy profile. Specifically, the server should support the TLS version greater than 1.1 and provide a valid certificate. If the TLS version is lower than TLS 1.2 or the certificate is invalid, the server cannot guarantee a secure connection, so we rank it as `Level-C`. If the DNS/SP server deploys TLS 1.3, a valid certificate, CT, at least one certificate revocation mechanism, and TLS downgrade protection, we rank it as `Level-A`. If DNS/SP servers further support DANE-TLSA, we rank it as `Level-S`.

Figure 8 shows the evolution of the proportions of the four levels in DNS/SP recursive resolvers. We find that `Level-A` DNS/SP servers account for the highest proportion, especially DoH-SP servers. Nevertheless, the proportion of `Level-C` DoH-SP servers is higher than that of `Level-C` DoT-SP servers. According to the data on September 11th, 2022, we find that 11 (0.49%) DoT-SP and five (0.45%) DoH-SP servers are ranked as `Level-S`. However, upon further investigation, we find that only two `Level-S` DoT-SP servers and one `Level-S` DoH-SP server appear in the public lists we collected.

In conclusion, DoH-SP servers can provide better security protection, which may benefit from their better compatibility with the existing HTTPS ecosystem. The development of DNS Strict Privacy can promote the evolution of the TLS/HTTPS ecosystem, and in turn, DoT/DoH can also benefit from future TLS/HTTPS-related security features.

E. Comparison With the HTTPS Ecosystem

We can better understand the actual security state of the DNS privacy ecosystem by comparing DNS/SP services with HTTPS services. In this section, we comprehensively compare the deployment of TLS/HTTPS-related security features

TABLE V
COMPARISON OF SECURITY FEATURE DEPLOYMENTS BETWEEN DNS/SP RECURSIVE RESOLVERS AND HTTPS SERVERS

	DoT-SP	DoH-SP	HTTPS
TLS Version			
TLS 1.3	1289 (57.29%)	906 (82.44%)	327546 (32.75%)
TLS 1.2	692 (30.76%)	104 (9.46%)	546110 (54.61%)
TLS 1.1	–	–	179427 (17.94%)
TLS 1.0	–	–	162256 (16.23%)
AuthCred			
CertValid	1743 (77.47%)	815 (74.16%)	749255 (74.93%)
DANE-TLSA	15 (0.67%)	5 (0.45%)	461 (0.05%)
MisIssPro			
CT	1889 (83.96%)	902 (82.07%)	751188 (75.12%)
Expect-CT	–	2 (0.18%)	543 (0.05%)
CAA	57 (2.53%)	27 (2.46%)	35494 (3.55%)
CertRev			
CRL	694 (30.84%)	129 (11.74%)	357646 (35.76%)
OCSP	1966 (87.38%)	969 (88.17%)	775417 (77.54%)
OCSPStap	68 (3.02%)	149 (13.56%)	328639 (32.86%)
OCSPMust	31 (1.38%)	19 (1.73%)	708 (0.07%)
DownPro			
TLSDown	1217 (54.09%)	850 (77.34%)	749255 (74.93%)
HSTS	–	103 (9.37%)	25538 (2.55%)
Security Level			
Level-S	11 (0.49%)	5 (0.45%)	369 (0.04%)
Level-A	937 (41.64%)	644 (58.60%)	516046 (51.60%)
Level-B	795 (35.33%)	166 (15.10%)	232379 (23.24%)
Level-C	507 (22.53%)	284 (25.84%)	250748 (25.07%)

by Majestic TOP-1M servers [51] and DNS/SP recursive resolvers on September 11th, 2022.

As we can see from Table V, DNS/SP recursive resolvers and HTTPS servers differ in their support of some security features. We discuss highlighted data below.

First, DoH-SP servers are much better than other servers in terms of TLS 1.3 support. Furthermore, 183017 (18.30%) HTTPS servers still support deprecated TLS versions, which are not present in DNS/SP servers.

Second, DNS/SP servers deploy CT and HSTS better than HTTPS servers. This shows that DNS/SP server administrators have recognized the importance of security features. However, DNS/SP servers are still insufficiently deployed for some features, such as TLS downgrade protection in DoT-SP servers.

Third, DNS/SP servers have worse support for certificate revocation than HTTPS servers. Specifically, 44.75% of HTTPS servers only support CRL/OCSP, while the corresponding ratios in DoT-SP and DoH-SP servers are 83.82% and 74.89%, respectively. In addition, the number of DNS/SP servers supporting OCSP Stapling is much lower than HTTPS servers.

To help the Internet community better understand the deployment situation of DNS Strict Privacy, we have implemented a DoT/DoH server search engine and recommender system[11]. Specifically, the search engine displays the security configuration and historical evolution of DNS/SP servers. The recommender system recommends reliable and close DNS/SP servers based on the user's geographic location.

V. CLIENT-SIDE BEHAVIOR

As the most common application between Internet users and DNS privacy servers, browsers are responsible for verifying the identity of the server and encrypting DNS packets. Nevertheless, we do not yet know whether browsers in different operating systems (OSes) can support DNS Strict Privacy and how to react after failure. To this end, we present a detailed inspection of five popular browsers for DNS Privacy implementation in four OSes in this section.

[11]For detailed usage, please visit https://dns-sp.info

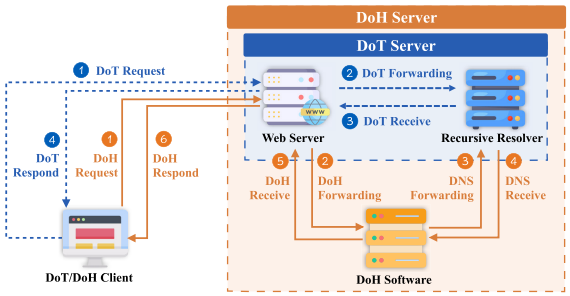


Fig. 9. DoT/DoH client experiment architecture.

A. Methodology

The crux of the measurement is to simulate DoT and DoH services. To this end, we first purchase a domain as our experimental DNS privacy server. Then we use the Nginx web server to receive DoT and DoH requests from the browsers and specify the web server IP address as the A record for the domain. Furthermore, we use UNBOUND [69] as the DNS recursive resolver for DNS lookups and to unpack (pack) DoT queries (responses) from (into) TCP packets. As a result, we can simulate the DoT service by combining Nginx and UNBOUND. On this basis, we integrate the open-source tool `dns-over-https` [80] to implement the DoH service, which is convenient for us to change the DoH server configuration. Figure 9 shows the whole process of DoT/DoH services, from initiating the query to getting the response in the experiment.

After implementing DoT/DoH services, we select five browsers providing DNS privacy settings according to previous reports and research [81], [82]. Specifically, we inspect Chrome, Firefox, Edge, Brave, and Opera for the DoT/DoH implementation in Windows 11, Ubuntu 20.04, macOS 12, and Android 11. Some of the five browsers require the underlying OS to support DNS privacy. To this end, we use mobileconfig files [83] and the ControID APP to realize the support of DoT/DoH in macOS and Android, respectively.

Particularly, we focus on the basic implementation of DNS privacy and the reactions related to the certificate. For the former one, our evaluation is made by changing the server configuration. For the latter one, we use OpenSSL to generate various test certificates, including the common errors we found in Section IV-C.2, and we also set browsers to trust our root certificate. Furthermore, we build four unique revoked certificates as CRL, OCSP, OCSP Stapling, and OCSP Must-Staple test suites. Specifically, the revoked certificates for the CRL, OCSP, and OCSP Must-Staple test suites include only the CRL server, OCSP server, and OID (1.3.6.1.5.5.7.1.24), respectively. For the OCSP Stapling test suite, we prefetch the OCSP response file for the revoked certificate and transmit it in the TLS handshake.

TABLE VI
IMPLEMENTATION OF DOH BY BROWSERS IN DIFFERENT OPERATING SYSTEMS

	Firefox				Chrome				Edge/Opera/Brave			
	Win.	Lin.	Mac.	Andr.	Win.	Lin.	Mac.	Andr.	Win.	Lin.	Mac.	Andr.
Browser Version	97	97	97	97	97	97	97	97	99/82/1.36	99/82/1.33	99/82/1.36	99/70/1.33
Content-Type	✔[1]	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
TLS Version	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
HTTP Version	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
HTTP Method	POST	POST	GET	POST	POST	POST	GET	POST	POST	POST	GET	POST
Self-signed Cert	✔[2]	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Expired Cert	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
SAN Error Cert	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
No SAN Cert	✗[2]	✗	✔	✗	✔	✔	✔	✔	✔	✔	✔	✔
Revoked Cert (CRL/OCSP)	✔	✔	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Revoked Cert (OCSPStap)	✔	✔	✔	✔	✔	✔	✔	✗	✔	✔	✔	✗
Revoked Cert (OCSPMust)	✔	✔	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Fallback	○[3]	○	○	●[3]	●	●	●	●	●	●	●	●

[1] ✔ denotes compliance with RFC requirements.
[2] ✔ denotes correct identification of certificate errors; ✗ denotes incorrect.
[3] ● denotes no fallback to clear-text; ○ denotes fallback to.

B. Results

All five browsers only support DoH in the selected four OSs, so our analysis below is for DoH only. Furthermore, it is not surprising that there is no difference in measurements for Chrome, Edge, Brave, and Opera, as all of them are original from the Chromium kernel [84].

Considering the unawareness of DNS privacy, browser users usually use the default configuration of the underlying browser. We find that Firefox and Opera use `Cloudflare` as the default DoH provider and only have another optional provider, which undoubtedly exacerbates the centralization problem. Reassuringly, other browsers do not have default DoH server settings and offer at least four options.

We give the measurement summary in Table VI, which clearly shows that the basic configuration of the browsers is generally in good condition. Specifically, when we configure the TLS version in the DoH server lower than 1.2, all the browsers terminate the DoH query. Furthermore, all the browsers can set Content-Type to `application/dns-message` correctly, and support HTTP/1.1 and HTTP/2.0 to transmit DoH packets with HTTP/2.0 first rule. As we discover in Table II, about 90% of DoH servers support HTTP/2.0. Hence, the browsers would use HTTP/2.0 to communicate with the server in most cases. The supporting HTTP method is the only defect in the basic configuration. Especially when the default HTTP method is not available, all browsers do not try other methods but directly terminate DoH queries, resulting in clients not being able to communicate with DoH servers that only support one HTTP method.

Considering certificate validation, we only get expected results when the certificate is self-signed, expired, or a mismatch between the domain and the DNS names in the SAN extension. Firefox in Windows, Linux, and Android accepts the DoH response even when the SAN extension is not included in the DoH server certificate.

Unfortunately, revoked certificate detection in the five browsers is poor. If the DoH server only supports CRL or OCSP, we find that almost all browsers except Firefox in Windows and Linux communicate with the DoH server configured with revoked certificates. In this case, the user may have a false sense of security that there is nothing wrong with the DoH server's certificate. Unfortunately, we find 10,048 such public DoH servers. Furthermore, only Firefox in Windows and Linux respects OCSP Must-Staple and stops sending DoH requests to DoH servers.

Regarding the fallback policy in the browsers, we, unfortunately, find that Firefox in Windows, Linux, and macOS would fall back to clear-text DNS for queries when DoH is unavailable, though it can force no fallback by setting `network.trr.mode` to 3 in `about:config`. Furthermore, only Firefox does not prompt the user to check secure DNS settings when DoH is unavailable.

C. Summary

DNS clients should also support DNS/SP well; otherwise, all the efforts on the server side would be in vain. Although browsers already support HTTPS well, we still find inconsistent behaviors, even the same browsers on different OSes. Some problems are only related to DoH, such as the SAN problem in Firefox, while some problems are also related to HTTPS, such as the certificate revocation problem. Therefore, proper implementation of DNS Strict Privacy on the client side could not only urge unreliable server updates but also benefit both the DNS privacy and HTTPS ecosystem.

VI. RELATED WORK

In this section, we present previous research related to our work, especially the DNS privacy ecosystem and security mechanisms related to TLS/HTTPS.

A. DNS Privacy Ecosystem

Many works have been devoted to the DNS privacy ecosystem from different perspectives, including the adoption of DoT/DoH [13], [28], [33], [61], the impact of encryption on DNS performance [28], [29], [30], [56], the analysis of encrypted DNS traffic [31], [32], [33], [85], and mitigation of centralization problems [35], [86], [87]. In the following, we briefly review the works close to this paper. The first comprehensive analysis of DNS-over-Encryption is conducted by Lu et al. [13]. They mainly focused on server-side deployment, worldwide availability and performance, and traffic analysis of DoT/DoH. However, their DoH server dataset is not comprehensive, and it is assembled using passive data. Furthermore,

they only analyzed the certificates of DoT/DoH servers but not other TLS/HTTPS-related security features. Many subsequent works complement these deficiencies [28], [33]. For example, García et al. [33] collected a more comprehensive list of open DoH servers and analyzed DoT, DoH, and DNS over QUIC traffic from the perspective of a large ISP, a large university, and a global company. Böttger et al. [28] measured the TLS version, CT, CAA, and OCSP Must-Staple support across ten public DoH servers. Nevertheless, there is no work so far that comparatively analyzes the deployment and evolution of TLS/HTTPS-related security features of DoT/DoH servers on a large scale, which is what this paper is devoted to.

There are also some papers that evaluated other players in the DNS privacy ecosystem [61], [81]. Deccio et al. [61] conducted an active scan of open DoT/DoH servers and analyzed TFO support. In particular, they also measured DoT adoption in authoritative servers. Huang et al. [81] observed the DoH communication behavior of browsers with the public DoH server when faced with four attack vectors. Compared to them, this paper extensively measures the implementation of DoT/DoH in recursive resolvers, authoritative servers, and browsers.

The centralization problem is one of the main factors hindering the development of DNS privacy, and many solutions have been proposed, such as the Oblivious DNS over HTTPS (ODoH) [86] and the de-monopoly name resolution [87]. In this paper, we quantify the centralization problem of public DoT/DoH servers and construct the most comprehensive list of DNS/SP servers, providing users with more reliable options to mitigate the centralization problem.

B. TLS and HTTPS Related Mechanisms

Many previous studies [36], [37], [38], [39], [40], [41] have conducted comprehensive evaluations of TLS/HTTPS-related security features. In 2015, Zhu et al. [38] performed the first long-term measurements of DANE-TLSA and analyzed the cause of DANE validation errors. Liu et al. [37] conducted the first end-to-end evaluation of the certificate revocation ecosystem by analyzing website administrators, CAs, and browsers. The most comprehensive assessment of the entire HTTPS ecosystem is the work of Amann et al. [36] in 2017. They analyzed the deployment and security benefits of different mechanisms by measuring CT, HSTS, HPKP, TLSA, CAA, SCSV, and the evolution of TLS versions. To the best of our knowledge, our work is the first to give a longitudinal and comprehensive measurement of TLS/HTTPS-related security features in DoT/DoH servers.

VII. Discussion

Our measurements show significant improvements in DNS privacy support both on the server-side and client-side. Nevertheless, choosing plaintext DNS or encrypted DNS, DoT or DoH, is far from being a matter of ephemeral and dictatorship, but a trade-off between user privacy and stakeholder interests. In this section, we discuss the roadblocks to the evolution of DNS privacy and propose initiatives for various plays to advance DNS privacy forward.

A. Roadblock

DNS privacy, a technique innovating the DNS mechanism that pervades the corners of the Internet, undoubtedly shakes the web's foundation and offends the interests of stakeholders.

Centralization. Our results clearly show the centralization problem in public DoT/DoH, which indicates that Internet users can only get the DoT/DoH service from a few providers. In this case, DNS messages cannot be genuinely protected. For example, unscrupulous providers can easily obtain full DNS logs of Internet users and sequentially infer users' privacy, such as hobbies, occupations, and health status. Furthermore, the single point of failure, unhealthy data competition, and increased DNS resolution distance affecting performance are also undesirable by-products of the centralization problem.

According to our analysis, the centralization problem is not due to the DoT/DoH mechanism itself but mainly to the default setting of application software. Unlike traditional DNS servers that can be auto-configured, it is hard for Internet users to discover other DNS privacy servers and configure them correctly in the application's obscure UI. For example, Firefox and Opera have `Cloudflare` as the default provider and only offer one additional option. Although the users can configure a new DNS privacy server, there is no instruction to complete the setting.

Reliability. The authority and confidentiality of DNS messages are the advertising advantages of DNS privacy. However, our measurements show that DoT/DoH servers' configuration on TLS/HTTPS-related security features is far from the expected situation. For instance, around 60% of DoT and 40% of DoH recursive resolver certificates are invalid. Furthermore, DNS manipulation may also happen in DNS privacy servers, as in regular DNS servers [88]. Given the centralization problem, it is uncomplicated to imagine what damage a compromised DNS privacy server can cause. At last, DNS privacy can only protect the client-server DNS communication, but not the integrity of DNS responses. Hence, DNSSEC is still required.

Supervision. Encrypted DNS undoubtedly increases the difficulty for network administrators to monitor the DNS traffic, especially for DoH. For example, DoT/DoH can bypass DNS-based corporate policies and parental controls, and even help malware evade DNS detection [89]. As a result, compared to DoH, some participants are more willing to support DoT to maintain the power to regulate the behavior of Internet users.

False sense of security. After DNS privacy solves the biggest remaining task in Internet encryption engineering, ignorant users may have the illusion that their privacy is guaranteed. However, due to the existence of metadata such as certificate, OCSP, HTTP connection, SNI, and IP address, DoT/DoH cannot wholly prevent ISPs and attackers from snooping on users' browsing patterns. Therefore, what DoT/DoH provides may be just illusory privacy.

B. Initiative

DNS, the cornerstone of the Internet, cannot survive the encrypted torrent of the Internet. DoT/DoH is an integral approach to solving this predicament. Like CT and TLS 1.3,

the current evolution of DNS privacy mainly benefits from Internet centralization and large organizations (such as Mozilla and Google). However, we believe that the deployment of DNS privacy is not the responsibility of the minority but requires the endeavor of all participants in DNS privacy, including large DNS providers, local DNS suppliers, clients, and Internet users.

Server. As we have witnessed, DoT/DoH is the best choice for protecting DNS privacy currently, which suggests DNS server administrators embrace rather than block DoT/DoH. We are pleased to observe that this process is being advanced. Specifically, we found 21,073 open DoT and 25,974 open DoH servers in September 2022, while there were only 6,016 and 931 in previous results [33], [88]. Nevertheless, DoT/DoH adoption is still far from our expectation, given over 3 million open DNS resolvers [62]. Furthermore, we observe that only 2854 and 1070 different organizations are involved in DoT and DoH, respectively. The actual situation for DoH may be better since the DoH template is not standardized. Hence, we advocate that the Internet community standardizes the DoH template to identify DoH servers and further facilitate user configuration and DNS censorship. Furthermore, since encrypting DNS messages can hinder Internet security supervision, we endorse that network administrators deploy DoT/DoH servers in their local network if they want to protect DNS communication without losing DNS information visibility.

As discussed in Section IV-D, `Level-B` is the baseline for any qualified DNS privacy server. Furthermore, the server should also support DNSSEC to protect DNS responses. Fortunately, these two mechanisms are compatible. In particular, DNS privacy can reduce the middlebox interference during DNSSEC validation.

Client. We expect clients to improve the shortcomings of DNS privacy implementations mentioned in Section V-B. Inconsistent behavior and vague instructions on the client-side would lead to a poor experience for Internet users. Considering the unfriendly prompts, we recommend that clients split the custom DoH server setting into domain and path and inform users why DNS encryption failed.

The default setting of the DNS privacy provider in clients would exacerbate the tension between the immaturity and enforcement of DNS privacy. Furthermore, it would impede the development of local DNS privacy servers, if the user cannot set the current service provider as the DNS privacy provider. However, Firefox and Opera are not good examples of the above two problems. Furthermore, the client must show the details and ethical guarantees of the built-in DNS privacy provider to give users safety and peace of mind. Unfortunately, almost all clients only show the provider name. As well, clients should respect OS security strategies, corporate policies, and parental controls to minimize the impact of DNS privacy on network regulation.

Internet user. Unlike other stakeholders on the Internet, Internet users have little knowledge or voice on DNS privacy. The only thing they can do is to entrust DNS information to specific third-party entities or opt-out. The more choices they can make, the more benefits they can obtain from DNS privacy. Hence, maintaining a comprehensive public and reliable DNS/SP server list, which we are trying to do in this paper, is vital.

Remnant metadata. Recall the plaintext metadata available to network snoopers. We still need to prevent privacy leaking from certificates, OCSP, HTTP connections, SNI, and IP addresses. TLS 1.3, OCSP Stapling, and HTTPS can handle well with certificates, OCSP, and HTTP connections, respectively. However, Encrypted SNI or Encrypted Client Hello [90] should work together with DoT/DoH to deal with the leak in SNI. Lastly, we recommend multiple domains associated with one server to expand the difficulty of coupling the domain name to an IP address.

VIII. Conclusion

In this paper, we have provided the first longitudinal and comprehensive evaluation of the implementation of DoT/DoH in recursive resolvers, authoritative servers, and browsers. We have found that the configuration of DNS privacy has not kept pace with its adoption. The numerous hindrances and controversies in the evolution of DNS Strict Privacy can only be overcome by all participants heading together. On the bright side, a considerable number of DNS Strict Privacy servers are properly equipped with TLS/HTTPS-related security features, and DoH performs better. Our research highlights the need for servers and clients to re-check their configurations and encourages more players to deploy DNS privacy.

References

[1] P. Mockapetris, *Domain Names—Implementation and Specification*, document RFC 1035, Nov. 1987.
[2] S. Bortzmeyer, *DNS Privacy Considerations*, document RFC 7626, Aug. 2015.
[3] P. Pearce et al., "Global measurement of DNS manipulation," in *Proc. USENIX Secur.*, 2017, pp. 1–19.
[4] Z. Hu, L. Zhu, J. Heidemann, A. Mankin, D. Wessels, and P. Hoffman, *Specification for DNS Over Transport Layer Security (TLS)*, document RFC 7858, May 2016.
[5] P. Hoffman and P. McManus, *DNS Queries over HTTPS (DoH)*, document RFC 8484, Oct. 2018.
[6] M. Vale. (Jan. 2019). *Google Public DNS Now Supports DNS-Over-TLS*. [Online]. Available: https://security.googleblog.com/2019/01/google-public-dns-now-supports-dns-over.html
[7] Cloudflare Docs. (Apr. 2022). *Encrypt DNS Traffic*. [Online]. Available: https://developers.cloudflare.com/1.1.1.1/encrypted-dns
[8] Chrome. (Dec. 2019). *Chrome DNS-Over-HTTPS*. [Online]. Available: https://groups.google.com/a/chromium.org/g/net-dev/c/lIm9esAFjQ0/m/MyfjWzwlBgAJ
[9] Mozilla. (Nov. 2019). *Firefox DNS-Over-HTTPS*. [Online]. Available: https://support.mozilla.org/en-US/kb/firefox-dns-over-https
[10] T. Jensen. (Nov. 2019). *Windows Will Improve User Privacy With DNS Over HTTPS*. [Online]. Available: https://techcommunity.microsoft.com/t5/networking-blog/windows-will-improve-user-privacy-with-dns-over-https/ba-p/1014229
[11] S. Samat. (Aug. 2018). *Android 9 Pie: Powered by AI for a Smarter, Simpler Experience That Adapts to You*. [Online]. Available: https://www.blog.google/products/android/introducing-android-9-pie/
[12] S. Dickinson, D. Gillmor, and T. Reddy, *Usage Profiles for DNS over TLS and DNS over DTLS*, document RFC 8310, Mar. 2018.
[13] C. Lu et al., "An end-to-end, large-scale measurement of DNS-over-encryption: How far have we come?" in *Proc. IMC*, Oct. 2019, pp. 22–35.
[14] ENISA. (Dec. 2011). *Operation Black Tulip: Certificate Authorities Lose Authority*. [Online]. Available: https://www.enisa.europa.eu/media/news-items/operation-black-tulip/

[15] R. Wright. (Mar. 2018). *23,000 Symantec Certificates Revoked Following Leak of Private Keys*. [Online]. Available: https://www.techtarget.com/searchsecurity/news/252436120/23000-Symantec-certificates-revoked-following-leak-of-private-keys

[16] P. Hoffman and J. Schlyter, *The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA*, document RFC 6698, Aug. 2012.

[17] B. Laurie, A. Langley, and E. Kasper, *Certificate Transparency*, document RFC 6962, Jun. 2013.

[18] E. Stark. (Dec. 2018). *Expect-CT Extension*. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-expect-ct-08

[19] P. Hallam-Baker and R. Stradling, *DNS Certification Authority Authorization (CAA) Resource Record*, document RFC 6844, Jan. 2013.

[20] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, document RFC 5280, May 2008.

[21] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol—OCSP*, document RFC 6960, Jun. 2013.

[22] Y. Pettersen, *The Transport Layer Security (TLS) Multiple Certificate Status Request Extension*, document RFC 6961, Jun. 2013.

[23] P. Hallam-Baker, *X.509v3 Transport Layer Security (TLS) Feature Extension*, document RFC 7633, Oct. 2015.

[24] B. Moeller and A. Langley, *TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks*, document RFC 7507, Apr. 2015.

[25] E. Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.3*, document RFC 8446, Aug. 2018.

[26] J. Hodges, C. Jackson, and A. Barth, *HTTP Strict Transport Security (HSTS)*, document RFC 6797, Nov. 2012.

[27] A. Nisenoff, N. Feamster, M. A. Hoofnagle, and S. Zink, "User expectations and understanding of encrypted DNS settings," in *Proc. NDSS DNS Privacy Workshop*, 2021, pp. 1–8.

[28] T. Böttger et al., "An empirical study of the cost of DNS-over-HTTPS," in *Proc. IMC*, Oct. 2019, pp. 15–21.

[29] R. Chhabra, P. Murley, D. Kumar, M. Bailey, and G. Wang, "Measuring DNS-over-HTTPS performance around the world," in *Proc. IMC*, Nov. 2021, pp. 351–365.

[30] A. Hounsel, K. Borgolte, P. Schmitt, J. Holland, and N. Feamster, "Comparing the effects of DNS, DoT, and DoH on web performance," in *Proc. WWW*, Apr. 2020, pp. 562–572.

[31] R. Houser, Z. Li, C. Cotton, and H. Wang, "An investigation on information leakage of DNS over TLS," in *Proc. CoNEXT*, Dec. 2019, pp. 123–137.

[32] S. Siby, M. Juarez, C. Diaz, N. Vallina-Rodriguez, and C. Troncoso, "Encrypted DNS –> privacy? A traffic analysis perspective," in *Proc. 27th Annu. Netw. Distrib. Syst. Secur. Symp.*, 2020.

[33] S. García, K. Hynek, D. Vekshin, T. Čejka, and A. Wasicek, "Large scale measurement on the adoption of encrypted DNS," 2021, *arXiv:2107.04436*.

[34] M. Lyu, H. H. Gharakheili, and V. Sivaraman, "A survey on DNS encryption: Current development, malware misuse, and inference techniques," *ACM Comput. Surv.*, vol. 55, no. 8, pp. 1–28, Aug. 2023.

[35] G. C. M. Moura, S. Castro, W. Hardaker, M. Wullink, and C. Hesselman, "Clouding up the internet: How centralized is DNS traffic becoming?" in *Proc. IMC*, Oct. 2020, pp. 42–49.

[36] J. Amann, O. Gasser, Q. Scheitle, L. Brent, G. Carle, and R. Holz, "Mission accomplished? HTTPS security after diginotar," in *Proc. IMC*, Nov. 2017, pp. 325–340.

[37] Y. Liu et al., "An end-to-end measurement of certificate revocation in the web's PKI," in *Proc. IMC*, Oct. 2015, pp. 183–196.

[38] L. Zhu, D. Wessels, A. Mankin, and J. S. Heidemann, "Measuring DANE TLSA deployment," in *Proc. TMA* 2015, pp. 219–232.

[39] T. Chung et al., "Is the web ready for OCSP must-staple?" in *Proc. IMC*, Oct. 2018, pp. 105–118.

[40] E. Stark et al., "Does certificate transparency break the web? Measuring adoption and error rate," in *Proc. IEEE SP*, May 2019, pp. 211–226.

[41] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, *DNS Security Introduction and Requirements*, document RFC 4033, 2005 .

[42] R. Sleevi. (Apr. 2017). *Certificate Transparency in Chrome—change to Enforcement Date*. [Online]. Available: https://groups.google.com/a/chromium.org/g/ct-policy/c/sz_3W_xKBNY/m/6jq2ghJXBAAJ

[43] Apple. (Mar. 2021). *Apple's Certificate Transparency Policy*. [Online]. Available: https://support.apple.com/en-us/HT205280

[44] C. Cimpanu. (2020, March) Let's encrypt to revoke 3 million certificates on march 4 due to software bug. https://www.zdnet.com/article/lets-encrypt-to-revoke-3-million-certificates-on-march-4-due-to-bug/

[45] Z. Durumeric, E. Wustrow, and J. A. Halderman, "ZMap: Fast internet-wide scanning and its security applications," in *Proc. USENIX Secur. Symp.*, 2013, pp. 605–620.

[46] (Apr. 2022). *Publicly Available Servers*. [Online]. Available: https://github.com/curl/curl/wiki/DNS-over-HTTPS#publicly-available-servers

[47] Knot DNS. (Apr. 2022). *kdig—Advanced DNS Lookup Utility*. [Online]. Available: https://www.knot-dns.cz/docs/3.0/html/man_kdig.html

[48] Root Servers Operators. (Mar. 2021). *Statement on DNS Encryption*. [Online]. Available: https://root-servers.org/media/news/Statement_on_DNS_Encryption.pdf

[49] CISCO. (Apr. 2022). *TLD List Download*. [Online]. Available: https://tld-list.com/free-downloads

[50] (Apr. 2022). *Alexa Top-1M*. [Online]. Available: https://www.alexa.com/topsites

[51] (Apr. 2022). *The Majestic Million*. [Online]. Available: https://majestic.com/reports/majestic-million

[52] CISCO. (Apr. 2022). *Cisco Umbrella 1 Million*. [Online]. Available: https://umbrella.cisco.com/blog/cisco-umbrella-1-million

[53] (Apr. 2022). *Tranco Top-1M*. [Online]. Available: https://tranco-list.eu/

[54] (Mar. 2022). *IP Geolocation API*. [Online]. Available: https://ip-api.com/

[55] (Jan. 2022). *Control D*. [Online]. Available: https://controld.com/

[56] T. V. Doan, I. Tsareva, and V. Bajpai, "Measuring DNS over TLS from the edge: Adoption, reliability, and response times," in *Proc. PAM*, 2021, pp. 192–209.

[57] Scape Reach Ltd. (Jan. 2022). [Online]. Available: https://www.scapetechnologies.com/

[58] K. Moriarty and S. Farrell, *Deprecating TLS 1.0 and TLS 1.1*, document RFC 8996, Mar. 2021.

[59] (Jan. 2022). *NextDNS*. [Online]. Available: https://nextdns.io/zh

[60] P. Hoffman and P. van Dijk. (Sep. 2021). *Recursive to Authoritative DNS With Unauthenticated Encryption*. [Online]. Available: https://draft-ietf-dprive-unauth-to-authoritative-04

[61] C. Deccio and J. Davis, "DNS privacy in practice and preparation," in *Proc. CoNEXT*, Dec. 2019, pp. 138–143.

[62] J. Park, R. Jang, M. Mohaisen, and D. Mohaisen, "A large-scale behavioral analysis of the open DNS resolvers on the internet," *IEEE/ACM Trans. Netw.*, vol. 30, no. 1, pp. 76–89, Feb. 2022.

[63] S. Santesson, *Internet X.509 Public Key Infrastructure Subject Alternative Name for Expression of Service Name*, document RFC 4985, Aug. 2007.

[64] DNS Privacy Project. (Jan. 2023). *Public Resolvers*. [Online]. Available: https://dnsprivacy.org/public_resolvers/

[65] Wikipedia. (Nov. 2022). *Wildcard Certificate*. [Online]. Available: https://en.wikipedia.org/wiki/Wildcard certificate

[66] Fortinet. (Feb. 2021). *Investor Relations*. [Online]. Available: https://www.fortinet.com/blog/business-and-technology/sfr-business-launches-managed-sd-wan-service-with-fortinet-secure-sd-wan

[67] (Jan. 2022). *Scape Reach Partners*. [Online]. Available: http://www.scapereach.com/about/partner.html

[68] mkcert. (Jan. 2023). *Who do you Trust?* [Online]. Available: https://mkcert.org/

[69] NLnet Labs. (Feb. 2021). *Unbound 1.13.1 DNS Resolver*. [Online]. Available: https://www.unbound.net

[70] B. VanderSloot, J. Amann, M. Bernhard, Z. Durumeric, M. Bailey, and J. A. Halderman, "Towards a complete view of the certificate ecosystem," in *Proc. IMC*, Nov. 2016, pp. 543–549.

[71] Mozilla. (Jul. 2020). *Reducing TLS Certificate Lifespans to 398 Days*. [Online]. Available: https://blog.mozilla.org/security/2020/07/09/reducing-tls-certificate-lifespans-to-398-days/

[72] Apple. (Mar. 2020). *About Upcoming Limits on Trusted Certificates*. [Online]. Available: https://support.apple.com/en-us/HT211025

[73] Chromium. (Sep. 2020). *Certificate Lifetimes*. [Online]. Available: https://chromium.googlesource.com/chromium/src/+/master/net/docs/certificate_lifetimes.md

[74] Cab Forum. (Mar. 2017). *Ballot 193—825-Day Certificate Lifetimes*. [Online]. Available: https://cabforum.org/2017/03/17/ballot-193-825-day-certificate-lifetimes/

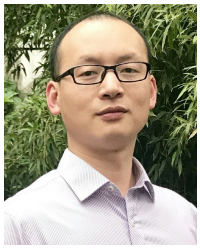
[75] (Jan. 2022). *CleanBrowsing*. [Online]. Available: https://cleanbrowsing.org/

[76] GoogleChrome. (Mar. 2022). *Chrome Certificate Transparency Policy*. [Online]. Available: https://github.com/GoogleChrome/Certificate Transparency/blob/master/ct_policy.md
[77] Mozilla. (Nov. 2022). *Expect-CT*. [Online]. Available: https://developer.mozilla.org/en_US/docs/Web/HTTP/Headers/Expect-CT
[78] DigiCert. (Mar. 2017). *New CAA Requirement: What You Should Know*. [Online]. Available: https://www.digicert.com/blog/new-caa-requirement-2
[79] J. Medley. (Feb. 2020). *Deprecations and Removals in Chrome 81*. [Online]. Available: https://developers.google.com/web/updates/2020/02/chrome-81-deps-rems
[80] m13253. (Nov. 2022). *DNS-Over-HTTPS*. [Online]. Available: https://github.com/m13253/dns-over-https
[81] Q. Huang, D. Chang, and Z. Li, "A comprehensive study of DNS-over-HTTPS downgrade attack," in *Proc. FOCI*, 2020, pp. 1–8.
[82] DNS Privacy Project. (Apr. 2022). *DNS Privacy Clients*. [Online]. Available: https://dnsprivacy.org/dns_privacy_clients/
[83] P. Miller. (Mar. 2022). *Encrypted-DNS*. [Online]. Available: https://github.com/paulmillr/encrypted-dns
[84] C. Cimpanu. (Jan. 2019). *All the Chromium-Based Browsers*. [Online]. Available: https://www.zdnet.com/pictures/all-the-chromium-based-browsers/
[85] J. Bushart and C. Rossow, "Padding ain't enough: Assessing the privacy guarantees of encrypted DNS," in *Proc. FOCI*, 2020, pp. 1–8.
[86] E. Kinnear, P. McManus, T. Pauly, T. Verma, and C. Wood. (Jan. 2022). *Oblivious DNS Over HTTPS*. [Online]. Available: https://draft-pauly-dprive-oblivious-doh-09
[87] A. Hounsel, P. Schmitt, K. Borgolte, and N. Feamster, "Encryption without centralization: Distributing DNS queries across recursive resolvers," in *Proc. ANRW*, Jul. 2021, pp. 62–68.
[88] L. Jin, S. Hao, H. Wang, and C. Cotton, "Understanding the impact of encrypted DNS on internet censorship," in *Proc. WWW*, Apr. 2021, pp. 484–495.
[89] C. Cimpanu. (Jul. 2019). *First-Ever Malware Strain Spotted Abusing New DoH (DNS Over HTTPS) Protocol*. [Online]. Available: https://www.zdnet.com/article/first-ever-malware-strain-spotted-abusing-new-doh-dns-over-https-protocol/
[90] E. Rescorla, K. Oku, N. Sullivan, and C. Wood. (Feb. 2022). *TLS Encrypted Client Hello*. [Online]. Available: https://draft-ietf-tls-esni-14

Ruixuan Li is currently pursuing the master's degree with the School of Computer Science and Technology, Zhejiang Gongshang University. His research interests include internet security and network measurement.

Xiaofeng Jia is currently pursuing the master's degree with the School of Computer Science and Technology, Zhejiang Gongshang University. His research interests include applied cryptography and blockchain.

Zhenyong Zhang is currently a Security Researcher in Dbappsecurity Co., Ltd. His research interests include internet security and network monitoring.



Jun Shao (Senior Member, IEEE) received the Ph.D. degree from the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China, in 2008. He is currently a Professor with the School of Computer Science and Technology, Zhejiang Gongshang University, Hangzhou, China. His research interests include network security and applied cryptography.

Rongxing Lu (Fellow, IEEE) is currently an Associate Professor with the Faculty of Computer Science (FCS), University of New Brunswick (UNB), Canada. His research interests include applied cryptography, privacy enhancing technologies, and the IoT-big data security and privacy. He was a recipient of nine best (student) paper awards from some reputable journals and conferences.

Jingqiang Lin received the M.S. and Ph.D. degrees from the University of Chinese Academy of Sciences in 2004 and 2009, respectively. He is currently a Full Professor with the School of Cyber Security, University of Science and Technology of China. His research interests include applied cryptography and system security.

Xiaoqi Jia received the Ph.D. degree from the Chinese Academy of Sciences, China, in 2010. He is currently a Professor with the Institute of Information Engineering, Chinese Academy of Sciences. His main research interests include operating system security, cloud security, and virtualization technologies.

Guiyi Wei (Member, IEEE) received the Ph.D. degree from Zhejiang University in December 2006, where he was advised by Cheung Kong chair professor Yao Zheng. He is currently a Professor with the School of Information and Electronic Engineering, Zhejiang Gongshang University. His research interests include wireless networks, mobile computing, cloud computing, social networks, and network security.