一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
IA2023-11(2023-09)

DNSのプライバシー保護を強化するための権威DNSサーバ発見方式の検討

砂原　悟† 金　勇†† 飯田　勝吉†††

† 公立千歳科学技術大学　〒066–8655 北海道千歳市美々 758 番地 65
†† 東京工業大学　〒152–8550 東京都目黒区大岡山 2–12–1
††† 北海道大学　〒060–0808 北海道札幌市北区北 8 条西 5 丁目
E-mail: †s-sunaha@photon.chitose.ac.jp, ††yongj@gsic.titech.ac.jp, †††iida@iic.hokudai.ac.jp

あらまし　DNS クエリの平文通信にはプライバシーの漏洩リスクが存在する．そのため，クライアント端末からフルサービスリゾルバ間，そしてフルサービスリゾルバから権威 DNS サーバ間の DNS 通信は全て暗号化による保護が求められる．現在，IETF からフルサービスリゾルバと権威 DNS サーバ間の通信を暗号化するための仕様案が発表されているが，この方式は既存の平文通信との互換性を重視しているため，フルサービスリゾルバが暗号化通信に対応した権威 DNS サーバを発見するまでは，プライバシーの漏洩リスクが残る．本論文では，各ゾーンの親権威 DNS サーバに該当ゾーンの暗号化通信への対応状況を示すダミーの NS レコードを追加することで，互換性とプライバシー保護を両立させる方法を提案する．また，この提案方法の実装と機能確認についても述べる．
キーワード　DNS，プライバシー保護，Full-DoH，暗号通信対応権威 DNS サーバ，サーバ発見，NS レコード

A consideration about a discovering method of privacy-enhanced authoritative DNS servers

Satoru SUNAHARA†, Yong JIN††, and Katsuyoshi IIDA†††

† Chitose Institute of Science and Technology　758–65 Bibi, Chitose, Hokkaido, 066–8655 Japan
†† Tokyo Institute of Technology　2–12–1 Ookayama, Meguro-ku, Tokyo , 152–8550 Japan
††† Hokkaido University　Kita 8 ,Nishi 5,Kita–ku, Sapporo, Hokkaido 060–0811 Japan
E-mail: †s-sunaha@photon.chitose.ac.jp, ††yongj@gsic.titech.ac.jp, †††iida@iic.hokudai.ac.jp

Abstract　Plain-text communication of DNS queries poses a risk of privacy leakage. Therefore, it is imperative to achieve protection through encryption for DNS communication between end terminals and full-service resolvers, as well as between full-service resolvers and authoritative DNS servers. The IETF has published an internet-draft for encrypting communication between full-service resolvers and authoritative DNS servers. However, this approach prioritizes compatibility with existing plain-text communication, which means that the risk of privacy leakage remains until a full-service resolver discovers an authoritative DNS server compatible with encrypted communication. In this paper, we propose a method to achieve the compatibility and privacy protection by adding dummy NS records indicating the status of support for encrypted communication of respective zones to the authoritative DNS servers of each zone. Additionally, we discuss the implementation and functional verification of this proposed method.
Key words　DNS, privacy protection, Full-DoH, Encrypted DNS Authoritative Server, Servicer Discovery and NS Records.

1. はじめに

近年，インターネットアクセスの起点となる Domain Name System (DNS) 通信において，プライバシー保護の必要性が指摘され [1]，DNS over TLS（DoT）[2]，DNS Queries over HTTPS（DoH）[3]，DNS over Dedicated QUIC Connections（DoQ）[4] などの規格が IETF(Internet Engineering Task Force) によって標準化された．しかしながら，これらの規格は，主としてクライアント端末とフルサービスリゾルバ間の通信におけるプライバシー保護に焦点をあてており [5]，フルサービスリゾルバと

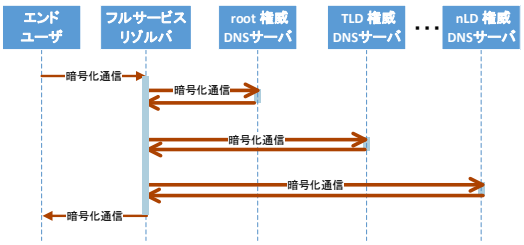

図 1　プライバシー保護を実現した DNS の通信手順

権威 DNS サーバ間の通信では依然として平文が使用されている．通常，フルサービスリゾルバと権威 DNS サーバ間の通信は，送信元がフルサービスリゾルバのアドレスであり，エンドユーザの直接的なプライバシー情報は含まれてはいない．しかしながら，実際には機関のプライバシーが含まれているため，通信経路における情報の保護は必要である [6]．フルサービスリゾルバと権威 DNS サーバ間の通信を保護する手段として，Query Name Minimization(Q-min) [7] が IETF によって標準化されている．しかしながら，Q-min は最終的に FQDN を平文で通信するため，プライバシー情報漏洩の緩和策にはなるが，完全なプライバシー保護は達成されない．通信経路上においてプライバシー情報を完全に保護するためには，DNS の全ての通信経路において暗号化が必要であると考え，我々は Full-DoH アーキテクチャの提案をしている [8].

プライバシー保護の観点においては図 1 の手順に示す通り，DNS の全ての通信において平文を一切使用せず，全ての通信を暗号化 (フル暗号化通信方式) することによって保護されることが理想である．しかし，DNS の名前解決における平文通信と暗号化通信には互換性がないため，フル暗号化通信方式を実現するためには全ての権威 DNS サーバが暗号化通信に対応していることが前提となる．フル暗号化通信方式への移行には平文通信と暗号化通信が混在する期間が存在することが予測されるため，平文通信と暗号化通信の互換性は重要である．IETF の仕様案 [9] では通信の互換性を維持しながらフルサービスリゾルバが動的に発見する方法が提案されているが，平文通信を併用するため，プライバシーの保護が完全ではない．本論文では，IETF の仕様案の通信方式におけるプライバシー保護の問題点について説明し，その後，プライバシー保護を実現可能な提案方式を紹介する．

2.　現在提案されている発見方法と問題点

現在，IETF において議論されているインターネットドラフト [9] では Probing Policy 方式「Note that a recursive resolver might initiate this query via any or all of the known transports. When multiple queries are sent, the initial packets for each connection can be sent concurrently, similar to ”Happy Eyeballs” ([RFC8305]). However, unlike Happy Eyeballs, when one transport succeeds, the other connections do not need to be terminated, but can instead be continued to establish whether the IP address X is capable of communicating on the relevant transport.」が提案されており，当該方式において

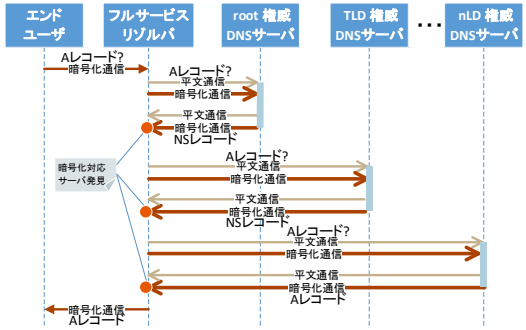

図 2　Probing Policy 方式 [9]

フルサービスリゾルバが暗号化通信をサポートする権威 DNS サーバを発見するには，実際に権威 DNS サーバへ接続を行う必要がある．この方式の通信手順を図 2 に示す．フルサービスリゾルバはクライアント端末から DNS クエリを受け取ると，各権威 DNS サーバへ平文通信と暗号化通信を同時に送信し，暗号化通信の接続に成功した場合は，それ以降の接続維持できる限りは暗号化通信の利用が可能となる．この発見方法は，従来の平文通信との互換性を維持しつつ，暗号化通信にも対応できる利点がある一方で，平文通信が発生するため，プライバシー情報の保護が完璧ではないことが問題となる．

3.　NS レコード掲載方式の提案

フルサービスリゾルバが暗号化通信に対応している権威 DNS サーバを発見する提案手法の基本的なアイデアは，権威 DNS サーバがフルサービスリゾルバに対して暗号化に対応していることを通知する仕組みを提供することである．通常，DNS クエリを受け取ったフルサービスリゾルバはキャッシュを持たない場合，root.hints ファイルの NS レコードを参照し，root, TLD, SLD...nLD の権威 DNS サーバから移譲先の権威 DNS サーバを示す NS レコードを受け取り，名前の解決を行う．

本研究では，委譲先を示す NS レコードのほかに，「暗号化通信の対応状況を示すダミーの NS レコード」を追加することでフルサービスリゾルバが暗号化通信に対応した権威 DNS サーバを発見することが可能な方式を提案する．暗号化通信の対応状況を示す NS レコードは，(1) 委譲先のサーバ名，(2) 暗号化対応状況を示す文字列，(3) 実在しないこと示すトップレベルドメイン名の 3 点を組み合わせる．例えば ns1.example.com が DoT と DoH をサポートしていることを示すには，「example.com NS ns1.example.com」が登録されている親ゾーン「com」の権威サーバにダミーの NS レコード「example.com NS ns1.example.com.TEHEQD.invalid」を登録する．このダミー NS レコードにより，ns1.example.com が TEHEQD(T は DoT, E は Enable,H は DoH,Q は DoQ,D は Disable の略) の状態であり，DoH および DoT の暗号化通信が使用可能であることを示し，さらに，存在しない invalid トップレベルドメイン [10] であることをフルサービスリゾルバに伝えることが可能となる．

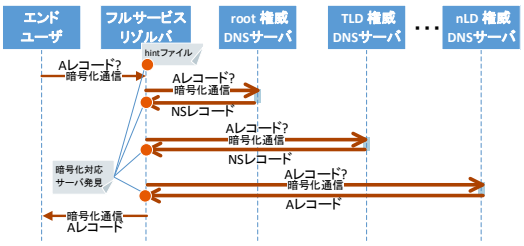

図 3　NS レコード掲載方式 (提案方式)

図 3 に提案手法の通信の手順を示す．まず最初にフルサービスリゾルバはクライアント端末から DNS クエリを受け取り，ヒントファイルファイルを参照して暗号化通信の対応した root 権威 DNS サーバを探す．そして，暗号化通信に対応している root 権威サーバを発見できた場合は暗号化通信で DNS クエリを送信する．root 権威 DNS サーバは委譲先の Top Level Domain (TLD) 権威 DNS サーバの委譲先を示す NS レコードと暗号化対応を状況を示す NS レコードをフルサービスリゾルバに送信する．フルサービスリゾルバは暗号化対応を状況を示す NS レコードから暗号化通信をサポートしている TLD 権威 DNS サーバを探し，発見した場合は暗号化通信で DNS クエリを送信する．Second Level Domain (SLD) 権威 DNS サーバ以降はこの流れを再帰的に繰り返し，最終的にフルサービスリゾルバはクライアント端末に名前解決の結果を送信する．

各方式の特徴を表 1 にまとめる．フル暗号方式は通信上のプライバシー情報を全て保護することが可能である一方で，平文通信の互換性が無いことが課題である．次に，Probing Policy 方式 [9] は権威 DNS サーバの管理者への負担が少なく，平文通信との互換性の維持が可能であるが，プライバシーの保護が完全ではない．本研究にて提案する NS レコード掲載方式では権威 DNS サーバにおいて NS レコードの追加することにより，プライバシーの情報を全て保護しつつ，平文通信の互換性を実現する．

表 1　方式と特徴の簡易表

方式名	プライバシー漏洩	管理者の負担	平文通信との互換性
フル暗号化通信方式	なし	暗号通信の有効化	なし
Probing Policy 方式 [9]	あり	暗号通信の有効化	あり
NS レコード掲載 (提案) 方式	なし	暗号通信の有効化 NS レコードの追加	あり

4.　プロトタイプの実装

本研究では，提案手法の機能評価を行うためにプロトタイプ環境を 1 台の物理サーバ内に構築した．図 4 に実装したプロトタイプ環境の概要を示す．図中にプロトタイプ環境の各

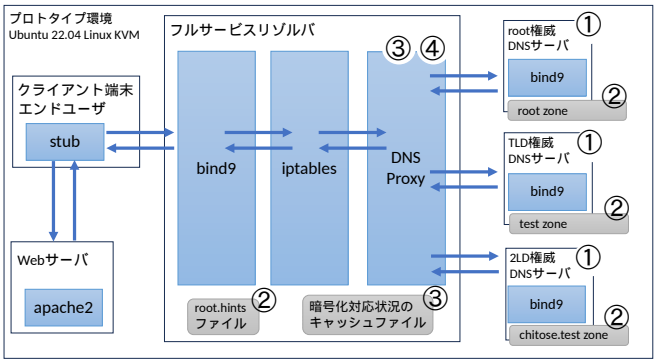

図 4　プロトタイプ環境の概要

Virtual Machine (VM) と実装上の重要なポイント①～④を示す．実装で重要なポイントは①権威 DNS サーバにおいて暗号化通信を有効化すること，②暗号化通信の対応状況を示す NS レコードの追加すること，③暗号化通信に対応している権威サーバを探す機能を実装すること，④フルサービスリゾルバが権威サーバと暗号化通信を行う機能を実装することである．それぞれのポイントについて次の節にて詳しく説明する．

4.1　①各権威 DNS サーバにおける暗号化通信の有効化

提案手法を確認するためには全ての権威 DNS サーバにおいて暗号化通信の有効化が必要となる．プロトタイプ環境ではルート認証局と自己署名証明書の root サーバ証明書を作成し，各 DNS サーバにて DoT, DoH の暗号化通信を有効化した．DoQ については現時点において bind9 [11] が未サポートであるため，今回の実装では無効としている．

4.2　②暗号化通信の対応状況を示す NS レコードの追加

全ての権威 DNS サーバとフルサービスリゾルバの root.hints ファイルに暗号化通信の対応状況を示す NS レコードを追加する必要がある．プロトタイプ環境では各暗号化プロトコルを示す文字列を表 2 の通りに定義した．

プロトタイプ実装では，複数の NS レコードを 1 つの NS レコードに集約するようにした．例えば DoT に対応している ns1.example.com と DoH に対応する ns2.example.com があった場合, ns1.example.com.TEHDQD.ns2.example.com.TDHEQD.invalid. と記述することで 2 つのネームサーバの対応状況を 1 つの NS レコードから読み取ることかできる．フルサービスリゾルバは invalid が記述されたレコードから文字列 ns1.example.com および ns2.example.com に一致する文字列を探しだし，一致した文字列を発見できた場合は，その直後に記述されているピリオドに囲まれた文字列が暗号化対応状況を示す文字列として認識できる．プロトタイプの実装ではダミーの NS レコードを複数記述することも可能であるが，1 つに集約することを基本とする．

フルサービスリゾルバの root.hints ファイルには，暗号化通信の対応状況を示す NS レコードを 13 個 (a～m.root-servers.net) 記述することを想定しているが，将来的に全ての権威 DNS サーバが暗号化に対応したときは root.hints ファイルから暗号化通信の対応状況を示す NS レコードを削除が可能である．

表 2　暗号化の対応状況示す文字列の一覧

文字列	文字列が示す意味
TE	DoT Enable
TD	DoT Disable
HE	DoH Enable
HD	DoH Disable
QE	DoQ Enable
QD	DoQ Disable
NE	Not Encrypt(ucp/tcp 53) Enable
ND	Not Encrypt(ucp/tcp 53) Disable

表 3　プロトタイプ環境の DNS レコード設定

NS レコードの登録対象	登録したレコード
フルサービス リゾルバの root.hints ファイル	. NS a.root-servers.net. . NS a.root-servers. net.HETEQD.invalid. (※) a.root-servers.net. A 192.168.53.20
root 権威 DNS サーバ	test. NS ns1.test. test. NS ns1.test.HETEQD.invalid. (※) ns1.test. A 192.168.53.30
TLS 権威 DNS サーバ	chitose NS ns1.chitose.test. chitose NS ns2.chitose.test. chitose NS ns1.chitose. test.HETEQD.ns2.chitose.test .HETEQD.invalid. (※) ns1.chitose.test. A 192.168.53.50 ns2.chitose.test. A 192.168.53.51
2LD 権威 DNS サーバ	www.chitose.test. A 192.168.53.250

プロトタイプ環境として実際に設定した NS レコードの値を表 3 に示す．表 3 に記載している※印は暗号化通信に対応した権威 DNS サーバを示すダミーの NS レコードである．

4.3　③暗号化通信に対応している権威サーバを探す機能

フルサービスリゾルバでは，root 権威 DNS サーバにおいて暗号化通信の対応状況を示す NS レコードの処理を行う機能の実装が必要となる．具体的には権威サーバから暗号化通信の対応状況を示す NS レコードを受け取った際に，構文解析を行い，暗号化通信に対応している権威サーバを探す機能である．この機能はフルサービスリゾルバの bind9 に実装することが望ましい．しかしながら bind9 への実装は複雑であるため，プロトタイプ環境ではこの機能を python3 を用いて DNS Proxy として実装した．DNS Proxy には NS レコードの構文解析の他に，DNS クエリを DoH でリクエストする機能と暗号化通信に対応している権威 DNS サーバを静的なファイルとして書き出し，キャッシュする機能も実装した．

4.4　④フルサービスリゾルバが権威サーバと暗号化通信を行う機能

フルサービスリゾルバと権威 DNS サーバが暗号化通信を行うためには，フルサービスリゾルバが暗号化通信で DNS クエリを送信する必要がある．Unbound [12], PowerDNS Recursor [13] など，一部の DNS ソフトウェアにおいて DoT 通信をリクエストする機能が実装されている．しかしながら DoT, DoH の両方をサポートするソフトウェアは今のところ見つけられていないため，本研究では DNS Proxy にその機能を実装した．DNS Proxy は暗号化通信の対応状況を示すキャッシュの情報を発見できた場合は DoT もしくは DoH にて名前解決を行う．権威 DNS サーバが複数の暗号化に対応している場合は文字列の先頭に近いプロトコルを優先的に使用する．この DNS Proxy はプライバシー保護を重視しているため，キャッシュから見つけられない場合，名前解決は行わずに RCODE:REFUSED を応答する．ただし，互換性を重視する場合には設定を変更することで，平文通信を行うことも可能である．なお，フルサービスリゾルバの bind9 と DNS Proxy の通信は iptables を用いて制御する．

5.　プロトタイプ環境における機能確認

5.1　従来の通信と DNS Proxy の暗号化通信の確認

提案手法が従来の通信を妨げていないことを確認するために，フルサービスリゾルバの root.hints ファイルと各権威 DNS サーバに暗号化通信の対応状況を示す NS レコードの追加を行った状態で，クライアント端末から web アクセス (`curl http://www.chitose.test`, `curl --doh-url https://resolv.chitose.test/dns-query http://www.chitose.test`) を実行し，従来の通信が問題なく機能し，web コンテンツが閲覧できることを確認した．さらに，DNS Proxy を有効化した場合には，全ての DNS 通信が暗号化されていることも確認した．全ての通信が暗号化されていることの確認には tcpdump コマンドを用いた．tcpdump の結果を表 4 に示す．クライアント (192.168.53.5) からフルサービスリゾルバ (192.168.53.10)，フルサービスリゾルバから root 権威 DNS サーバ (192.168.53.10)，TLD 権威 DNS サーバ (192.168.53.30),SLD 権威 DNS サーバ (192.168.53.50) 宛てにそれぞれ DoH (port 443) でアクセスを行い，クライアントが正常に Web サーバ (192.168.53.250) からコンテンツを取得している様子を確認できた．

表 4　tcpdump の結果 (抜粋)

サーバ名	tcpdump の結果 (抜粋)
クライアント 端末	192.168.53.5.47860 > 192.168.53.10.443: Flags [S] 192.168.53.10.443 > 192.168.53.5.47860: Flags [F.] 192.168.53.5.38480 > 192.168.53.250.80: Flags [S] 192.168.53.250.80 > 192.168.53.5.38480: Flags [F.]
フルサービス リゾルバ	192.168.53.5.47860 > 192.168.53.10.443: Flags [S] 192.168.53.10.60770 > 192.168.53.20.443: Flags [S] 192.168.53.20.443 > 192.168.53.10.60770: Flags [F.] 192.168.53.10.59672 > 192.168.53.30.443: Flags [S] 192.168.53.30.443 > 192.168.53.10.59672: Flags [F.] 192.168.53.10.35472 > 192.168.53.50.443: Flags [S] 192.168.53.50.443 > 192.168.53.10.35472: Flags [F.] 192.168.53.10.443 > 192.168.53.5.47860: Flags [F.]

表 5　DNS Proxy のキャッシュファイル

chitose.test. ns1.chitose.test.HETEQD.ns2.chitose.test.HETEQD.invalid.
test. ns1.test.HETEQD.invalid.
a.root-servers.net. a.root-servers.net.HETEQD.invalid.

5.2　DNS Proxy キャッシュ生成と通信機能の確認

表 5 に DNS Proxy が生成したキャッシュファイルを示す．プロトタイプ環境において DNS Proxy が暗号化の対応状況を示す NS レコードをフルサービスリゾルバの root.hints ファイルや権威 DNS サーバから受け取り，表 5 の通り最新の状態をキャッシュとして保存できること確認した．キャッシュファイルはゾーン名と暗号化を示す NS レコードの値を一覧にしたテキスト情報である．

DNS Proxy が暗号化通信に対応している権威サーバをキャッシュ情報から発見できない場合には，プライバシーの保護を優先し，フルサービスリゾルバへ RCODE:REFUSED の応答を示すことを確認した．また，キャッシュ情報から DoT 及び DoH 両方に対応する権威 DNS サーバを発見した場合には，レコード情報の先頭に近いプロトコルを優先し暗号化通信を開始することを確認した．

6. おわりに

DNS クエリの平文通信にはプライバシーの漏洩リスクが存在する．フルサービスリゾルバと権威 DNS サーバ間の暗号化する方式 (Probing Policy 方式 [9]）は平文通信との互換性が重視されており，結果としてプライバシーの漏洩リスクが残る．

本論文では権威 DNS サーバの NS レコードに暗号化通信の対応状況を示す方式を提案し，その実装および機能評価を紹介し，通信の互換性とプライバシー保護を両立が可能であることの示唆を与えた．

提案手法では，暗号化通信の対応状況を示す文字列によって文字数が増加し，ラベルが 63 文字を超えてしまう場合があり，さらに，ドメイン名には.invalid を付与するため，ドメイン名が 253 文字を超えてしまう場合があり得る．ラベルやドメイン名の文字数制限を超えた NS レコードは設定できないことについては，文字数を短縮するようなエンコード方式を使用することで解決を行う予定である．

その他にも，フルサービスリゾルバにおいて，暗号化通信から平文通信へのフォールバックを行うための判断基準について検討する必要がある．ある程度のプライバシー情報保護を考慮しつつ，互換性や応答速度を優先するエンドユーザーにとっては，フルサービスリゾルバ上で平文通信へのフォールバックを容認できる可能性がある．しかし，プライバシー情報の完全な保護を求めるエンドユーザーにとっては，平文通信へのフォールバックではなく「RCODE:REFUSED」を求める可能性がある．フルサービスリゾルバに対して，エンドユーザの意志を伝達し，フルサービスリゾルバのフォールバックをコントロールすることは，エンドユーザへカスタマイズされたプライバシー管理の提供を可能とし，エンドユーザのセキュリティと快適さのバランスを向上させる効果を期待できる．本研究では，今後の課題としてエンドユーザの意志をフルサービスリゾルバに伝達する手段についても検討を行う予定である．

文　献

[1] S. Farrell and H. Tschofenig, “Pervasive monitoring is an attack.” IETF RFC7258, May 2014.

[2] Z. Hu, L. Zhu, J. Heidemann, A. Mankin, D. Wessels, and P.E. Hoffman, “Specification for DNS over Transport Layer Security (TLS).” IETF RFC 7858, May 2016.

[3] P.E. Hoffman and P. McManus, “DNS queries over HTTPS (DoH).” IETF RFC8484, Oct. 2018.

[4] C. Huitema, S. Dickinson, and A. Mankin, “DNS over dedicated QUIC connections.” IETF RFC9250, May 2022.

[5] S. Dickinson, B. Overeinder, R. van Rijswijk-Deij, and A. Mankin, “Recommendations for DNS Privacy Service Operators.” IETF RFC 8932, Oct. 2020.

[6] B. Imana, A. Korolova, and J. Heidemann, “Institutional privacy risks in sharing dns data,” Proc. ACM/IRTF Applied Networking Research Workshop, Virtual event, pp. 69–75, Jul. 2021. DOI: 10.1145/3472305.3472324.

[7] S. Bortzmeyer, R. Dolmans, and P.E. Hoffman, “DNS Query Name Minimisation to improve privacy.” IETF RFC9156, Nov. 2021.

[8] S. Sunahara, Y. Jin, and K. Iida, “A proposal of DoH-based domain name resolution architecture including authoritative DNS servers,” Proc. 32nd IEEE Int’l Telecommun. Networks and Applications Conf. (ITNAC2022), Wellington, New Zealand, pp. 1–3, Nov. 2022. DOI: 10.1109/ITNAC55475.2022.9998349.

[9] D.K. Gillmor, J. Salazar, and P.E. Hoffman, “Unilateral Opportunistic Deployment of Encrypted Recursive-to-Authoritative DNS,” Aug, 2023. https://datatracker.ietf.org/doc/draft-ietf-dprive-unilateral-probing/, (Accessed on 30 Aug. 2023).

[10] D.E.E. 3rd and A.R. Panitz, “Reserved Top Level DNS Names.” IETF RFC 2606, Jun. 1999.

[11] Internet Systems Consortium, Inc, “BIND 9.” , available from https://www.isc.org/bind/, (Accessed on 30 Aug. 2023).

[12] NLnet Labs, “Unbound.” , available from https://nlnetlabs.nl/, (Accessed on 30 Aug. 2023).

[13] PowerDNS.com, BV, “PowerDNS.” , available from https://www.powerdns.com/, (Accessed on 30 Aug. 2023).