The Evolution of Domain Name Service (DNS) Security and Privacy

A technical paper prepared for presentation at SCTE TechExpo24

Jeff Van Dyke
Chief Product Architect
Akamai
jvandyke@akamai.com

Ralf Weber
Principal Architect
Akamai
rweber@akamai.com

Mark Dokter
Senior Product Manager
Akamai
mdokter@akamai.com

Bruce Van Nice
Senior Product Marketing Manager
Akamai
hvannice@akamai.com

Table of Contents

Title **Page Number**

List of Figures

Title **Page Number**

List of Tables

Title **Page Number**

1. Introduction

Encrypted Domain Name Service (DNS) ensures confidentiality, integrity and authentication for a critical internet protocol. There are no technical obstacles to implementation; recent standardization efforts have addressed operational gaps in connecting clients with encrypted resolvers. And there are notable success stories, yet overall usage remains low, less than 20% by our estimates. By comparison, Hypertext Transfer Protocol Secure (HTTPS) is the default protocol for 86% of web sites (W3Techs, 2024). End users have direct interaction with browsers and more familiarity with HTTP(S) than DNS which operates "under the hood". They expect encrypted protocols to be used, even if a technical comparison of both use cases is nuanced.

Growing tracking concerns have led to privacy focused approaches like oblivious DNS. It builds on encrypted DNS to prevent anyone, including network providers, from associating user identities with queries and answers. These services have been driven by device and operating system (OS) providers, such as Apple, who are using privacy to differentiate their ecosystems. Google has proposed a similar service; others may follow (Google, 2024).

These over-the-top services completely bypass the network provider's DNS. That poses challenges for operators who rely on their DNS as a control plane, for troubleshooting, compliance, and as a foundation for value-added services such as security.

Oblivious DNS services are new, and adoption is still low. Now's the time for ISPs to evaluate DNS strategies to minimize the impact and disruption these services may cause to their business and operations.

This paper will provide a technical overview of oblivious DNS and give perspective on its adoption and direction. It will explain the recent standards for connecting clients with encrypted resolvers and what they mean to network providers. Finally, it will present best practices and recommendations, based on deployment experience, for implementing DNS encryption to maximize subscribers' confidence in network-based services. Service providers have an opportunity to innovate and demonstrate their commitment to subscriber security and privacy while preserving DNS visibility to meet regulatory requirements or enable subscriber facing services.

2. DNS Privacy

2.1. Background

In 2021 Apple introduced the iCloud Private Relay service which enables all users with an iCloud+ subscription to connect to the internet and browse with Safari in a more secure and private way. The service provides enhanced privacy for DNS and HTTP/HTTPS interactions (Apple, 2021). Devices running iOS 15 or later, iPadOS 15 or later and macOS 12 or later are supported.

The DNS privacy system and protocol are called Oblivious DNS over HTTPS (ODoH) (Kinnear, E., et al., 2022).

2.2. Technical Overview

Let's first review traditional unencrypted and encrypted DNS transactions, focusing on what information is available to participants and potential attackers. We'll then introduce ODoH and compare the approaches.

2.2.1. *DNS Over Port 53 (Do53)*

Do53 relies on user datagram protocol (UDP) or transport control protocol (TCP) for transport of the DNS query and response. As a result, an attacker that was able to intercept the flow would see the DNS query and response data and associate it with the IP address of the client.

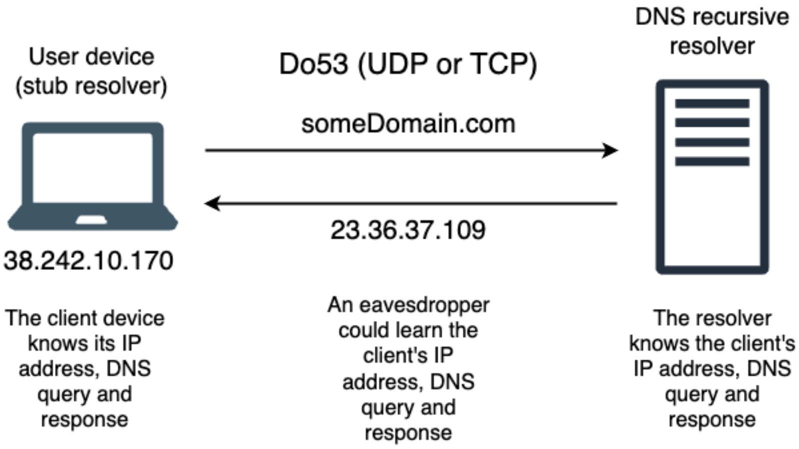

User device
(stub resolver)
Do53 (UDP or TCP)
DNS recursive
resolver
someDomain.com
23.36.37.109
38.242.10.170
The client device knows its IP address, DNS query and response
An eavesdropper could learn the client's IP address, DNS query and response
The resolver knows the client's IP address, DNS query and response

Figure 1- Do53 Message Flow

2.2.2. *Encrypted DNS Transports*

Encrypted DNS transports include DNS over HTTPS (DoH), DNS over QUIC (DoQ), and DNS over TLS (DoT). There are multiple DoH variants which we will not detail here as they provide equivalent levels of protection for DNS data.

When encrypted transports are employed, an attacker intercepting the flow cannot interpret the DNS query and response data. They can see the source IP address information and infer the type of traffic from the port number and/or the destination IP address, but that is all.

The client's IP address and the DNS query and response data are known only to the legitimate participants in the communication. However, a data breach could still make DNS transaction data available to an attacker.

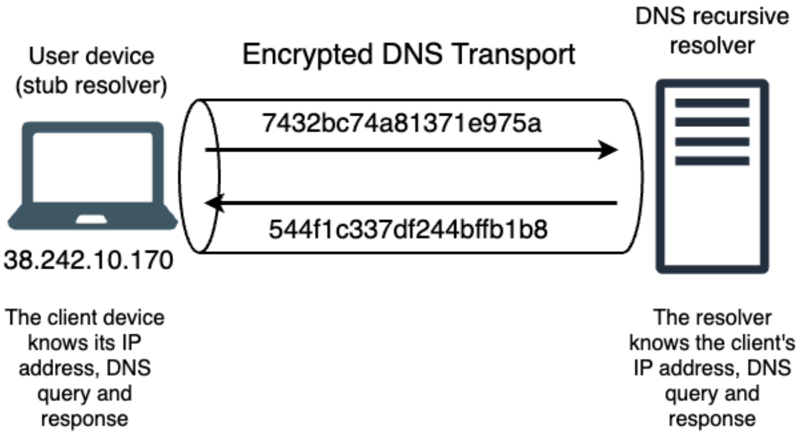

User device
(stub resolver)
Encrypted DNS Transport
DNS recursive
resolver
7432bc74a81371e975a
544f1c337df244bffb1b8
38.242.10.170
The client device knows its IP address, DNS query and response
The resolver knows the client's IP address, DNS query and response

Figure 2 - Encrypted DNS Message Flow

As shown below, many clients are now capable of supporting one or more encrypted DNS variants. There are some limitations in the Google ecosystem as noted. These and lack of automated configuration implementation on clients and in the network are holding usage back for human operated devices. Encrypted DNS support on Internet of Things (IoT) devices is also expected to be slow in developing.

Table 1 - Encrypted DNS Support

OS	Protocol			
	DoT	DoH	DoQ	ODoH
Windows 11 22H2	N	Y	N	N
macOS Ventura	Y	Y	N	Private Relay
iOS16 / iPadOS16	Y	Y	N	Private Relay
Android9+[1,2]	Y	Y	Y	N

1. Some apps for Android 9+ support DoH and DoQ.
2. Android 11+ supports Google and Cloudflare DNS only via DoH.

2.2.2.1. Extending DNS Encryption to Authoritative Queries

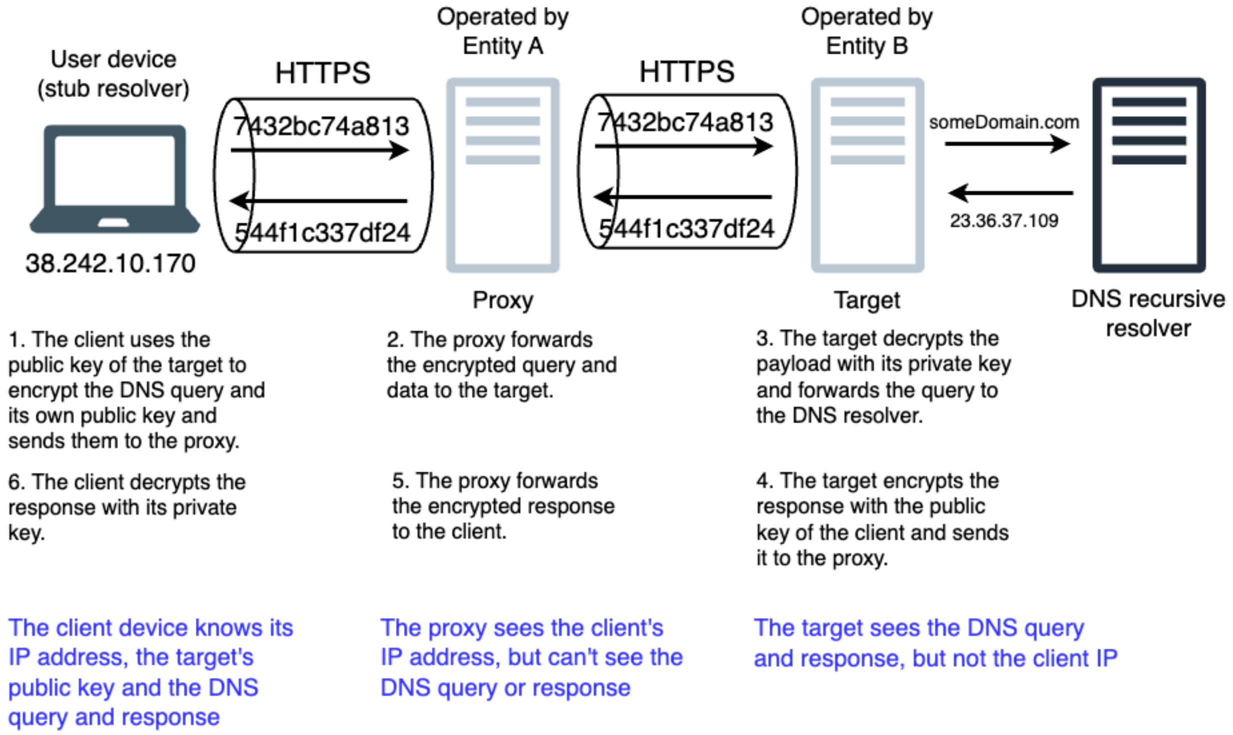
Today, encrypted transports are used solely between the client (stub) and resolver. The IETF has chartered a new working group, DNS Delegation (deleg), to enable encryption capabilities signaling for authoritative queries (IETF, n.d.). The working group’s deliverables include requirements definition and multiple specifications which define the delegation mechanism and interoperability for current and future systems (IETF, n.d.).

2.2.3. *Oblivious DNS over HTTPS (ODoH)*

ODoH addresses security and privacy through:

1. Multiple levels of encryption
   a. Public key encryption (PKE) of the DNS query and response payloads
   b. Encryption of all communications between the device, proxy and target using HTTPS
2. Processing requests through two, independently operated, relays so no single entity can generate a history of the DNS queries and responses for a specific user. The first relay is called the “proxy” and the second the “target”.

The diagram below illustrates the steps in an ODoH resolution and the roles of the proxy and target. The numbered text items detail the steps in the sequence and the blue text describes what information is available to each participant.



1. The client uses the public key of the target to encrypt the DNS query and its own public key and sends them to the proxy.

2. The proxy forwards the encrypted query and data to the target.

3. The target decrypts the payload with its private key and forwards the query to the DNS resolver.

4. The target encrypts the response with the public key of the client and sends it to the proxy.

5. The proxy forwards the encrypted response to the client.

6. The client decrypts the response with its private key.

The client device knows its IP address, the target's public key and the DNS query and response

The proxy sees the client's IP address, but can't see the DNS query or response

The target sees the DNS query and response, but not the client IP

Figure 3 - ODoH Architecture and Message Flow

The proxy and target must be operated by separate, non-colluding entities. In practice, the relays are operated by Apple and the targets and resolvers by approved third-party partners. This ensures that the data necessary for profiling simply does not exist outside of the client. An attacker could not reconstruct a user’s browsing profile even if it were able to obtain data from the proxy, target and DNS recursive resolver.

The target and DNS recursive resolver may be co-located or separate. In the case where both are co-located, which is the most common, inter-process communications are used between the target and DNS resolver. If they are separate, encrypted DNS transports may be employed.

The two-relay architecture introduces challenges to deploy and operate the service at scale.

Alternative approaches, which put full control in the hands of a single entity, have been implemented (J. Crowe, et al., 2022).

2.3. Adoption

Apple does not publicly disclose statistics on iCloud+ subscribers, so it is impossible to estimate the number of private relay and ODoH users. Apple is currently the only provider of ODoH DNS privacy services, but Google is exploring a similar service (Google, 2024).

Ongoing work in the IETF to develop a DNS privacy standard may lead to additional service offerings. This effort is described in the next section.

2.4. Future Directions

2.4.1. Integrating ODoH with Carrier Resolvers

Both Apple and Akamai want to empower subscribers with the privacy benefits that are part of iCloud Private Relay while also enabling service providers to continue to deliver DNS-based policy services.

We have developed an architecture that securely forwards all traffic from ODoH requests originating on the service provider's network to local resolvers. This solution enables the service provider to support anonymized policy enforcement for regulatory requirements (e.g., blocking prohibited content) and implement subscriber facing services for security and parental controls.

The integration, as shown below, relies on a discovery of designated resolvers (DDR) request to the local service provider's Do53 resolver to enable the client to locate a target that will forward the query to an encrypted DNS resolver operated by the service provider. In this case, the DDR response contains an ODoH configuration. Other DDR interactions, as described below, return the name of an encrypted DNS server.

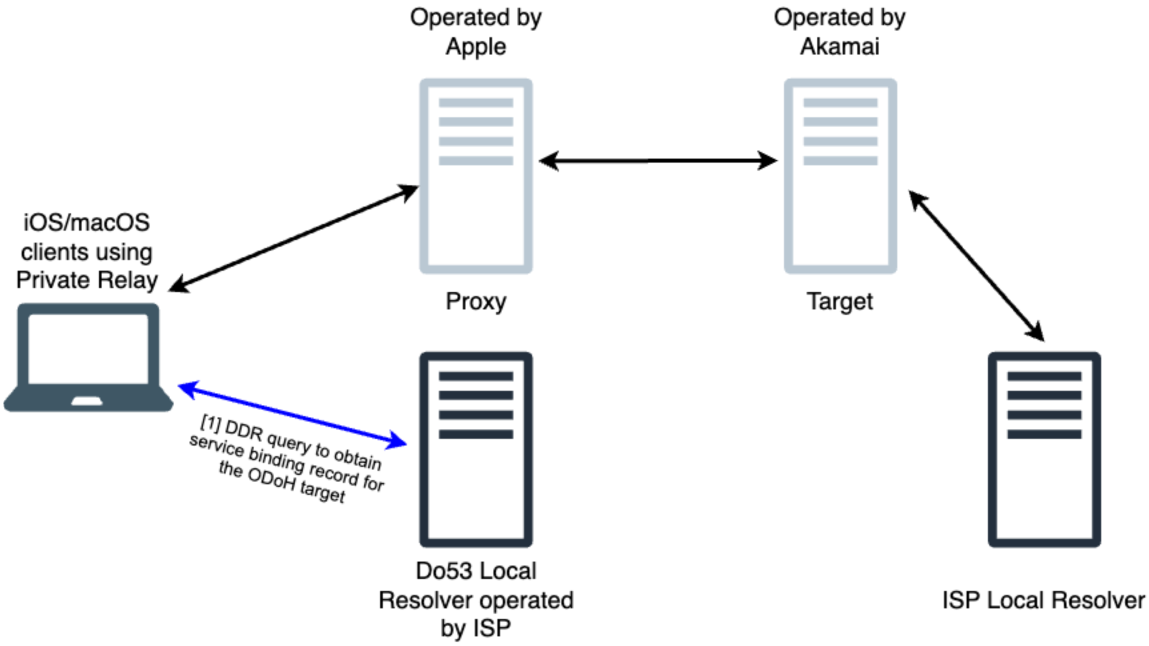

Operated by Apple
Operated by Akamai
iOS/macOS clients using Private Relay
Proxy
Target
[1] DDR query to obtain service binding record for the ODoH target
Do53 Local Resolver operated by ISP
ISP Local Resolver

Figure 4 – ODoH Carrier Integration

This approach has been successfully demonstrated in a proof of concept (PoC) with a carrier.

2.4.2. Development of DNS over Oblivious HTTP (DoOH)

Due to the intense interest in this area, the IETF is actively working to create standards for web and DNS privacy. Privacy for web interactions will be provided by Oblivious HTTP (OHTTP) (Thompson & Wood, 2024). DNS transactions will be able to use OHTTP as a transport. The combination is called DNS over Oblivious HTTP (DoOH).

Google's IP Protection service will likely be based on DoOH. Apple is also considering adopting the IETF protocols.

A broad, community-based specification would encourage implementers and help lower the barrier for others to offer privacy services.

DoOH will support integration with carrier resolvers like that described in the previous section.

2.5. Ramifications for Service Providers

The potential impacts of third-party DNS privacy offerings are the same as those posed by external DNS resolution services. However, DNS privacy services are likely to be more attractive to users because of the tracking protections they provide.

The challenges for service providers all stem from subscribers using an external, third-party service. ODoH is a completely "over the top" offering and therefore opaque to the service provider. Lack of visibility can hamper normal operations, such as troubleshooting, interfere with regulatory compliance, and limit potential value added service offerings.

Service providers have worked hard to design and deploy their DNS services to maximize responsiveness and overall performance. It may be challenging for third parties to deliver equivalent performance. When external services are used, service providers can no longer manage the subscriber experience.

Service providers should consider strategies that make their DNS services as comparable to third-party privacy enhanced services as practical.

3. Encrypted DNS Deployment

3.1. Simplifying the Connection Between Clients and Resolvers

When encrypted DNS transports were introduced some operational aspects were not fully addressed. There was no standard way for clients to discover encrypted resolvers and automatically upgrade. Manual configuration or working with the browser vendors to perform same-provider automatic-upgrade based on IP address were the only available options.

The IETF formed the Adaptive DNS Discovery (add) working group, which produced two drafts "Discovery of Designated Resolvers (DDR - RFC9642)" (T. Pauly, et al., 2023) and "Discovery of Network Resolvers (DNR - RFC9643)" (M. Boucadair, Ed., T. Reddy, Ed., D. Wing, et al., 2023) that provide the remaining piece of the puzzle. Their implementation by operating system and browser vendors is well underway.

These protocols make it simple for subscribers to take advantage of the benefits of encrypted DNS in an operationally scalable manner.

3.1.1. Discovery of Designated Resolvers (DDR)

DDR enables upgrades to encrypted transports from clients which have been configured with only the address or hostname of an unencrypted DNS resolver (Do53).

In the first case, the client queries the unencrypted DNS resolver using the special use domain name (SUDN) “dns.resolver.arpa” to obtain the service binding (SVCB) records for encrypted resolvers. The diagram below depicts the sequence of actions resulting in a successful upgrade.

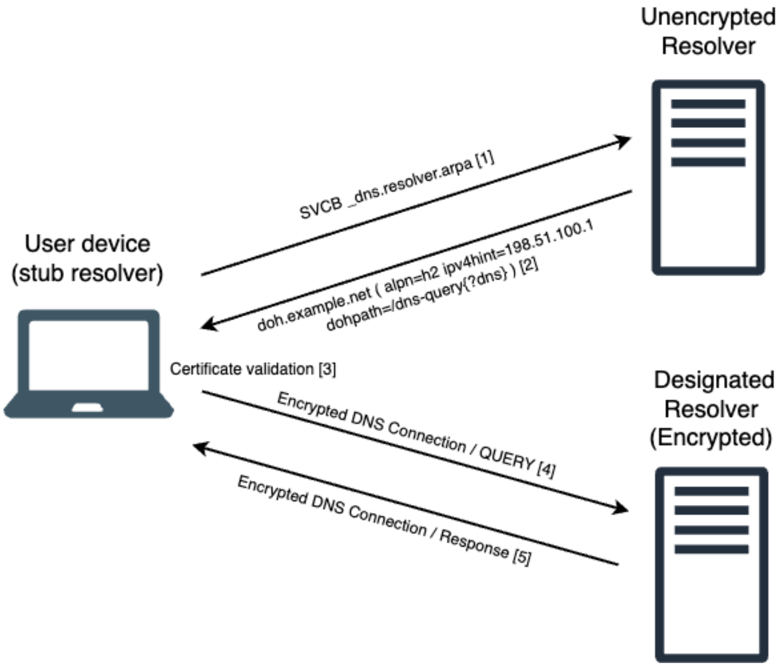

Unencrypted Resolver
User device (stub resolver)
SVCB _dns.resolver.arpa [1]
doh.example.net (alpn=h2 ipv4hint=198.51.100.1
dohpath=/dns-query{?dns}) [2]
Certificate validation [3]
Designated Resolver (Encrypted)
Encrypted DNS Connection / QUERY [4]
Encrypted DNS Connection / Response [5]

Figure 5 - Successful DDR Upgrade Message Flow

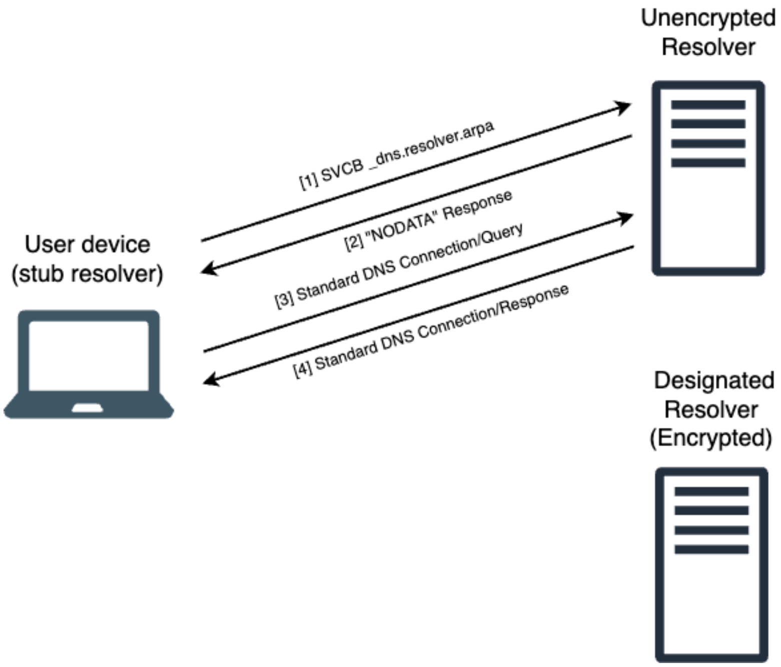

Unencrypted
Resolver
User device
(stub resolver)
[1] SVCB _dns.resolver.arpa
[2] "NODATA" Response
[3] Standard DNS Connection/Query
[4] Standard DNS Connection/Response
Designated
Resolver
(Encrypted)

Figure 6 - Unsuccessful DDR Upgrade Message Flow

The DDR interactions are a bit complex, but it has no dependencies on specific versions of DNS or DHCP software or usage of IPv6. It is applicable to client (stub) resolvers and embedded application resolvers.

Note that certificate validation only works for DNS servers with public IP addresses.

3.1.2. *Discovery of Network Resolvers (DNR)*

DNR specifies the process of discovering encrypted resolvers using DHCPv4, DHCPv6, and IPv6 Router Advertisement options. These options communicate the DNS Authentication Domain Name (ADN), a list of IP addresses and a set of associated service parameters.

DNR is most applicable to client (stub) resolvers which take configuration from the operating system.

3.1.3. *DDR and DNR Support*

The following table shows operating system and browser support for automatic upgrade mechanisms. Same-provider auto-upgrade by IP mechanisms are still working for people using Chrome today, but Google will also support DDR soon.

Table 2 - Support for Automatic Upgrades

OS	DDR			DNR	Opportunistic use of DoT
	Supported	Enabled by default	Applied to Chrome/MS Edge		
Windows 11 22H2	Y	N	N	Windows Insider builds	N
macOS Ventura	Y	Y	N	-	N
iOS16 / iPadOS16	Y	Y	Y	-	N
Android9+	N	-	-	-	Y

3.2. Best Practices and Recommendations

3.2.1. Adopt Automatic Upgrade Standards

These protocols enable operators to do network-based provisioning of DNS encryption capable resolvers and facilitate upgrades to encrypted DNS queries without any manual client configuration. In addition, DDR is an enabler for integration of local carrier resolvers with third-party privacy services. Service providers should implement DDR, DNR or both depending on their infrastructure.

3.2.2. Optimize the Performance of DNS Servers

Deployment of encrypted DNS services introduces additional capacity planning considerations. Unencrypted DNS performance is usually limited by the combination of network card and achievable kernel packets per second throughput, with CPU capacity being a secondary factor. In comparison, encrypted DNS uses more CPU time for each session resulting in more CPU cycles spent per query. This can be offset by distributing this additional workload across multiple cores or enabling TLS offload technologies. As the performance and capacity planning profiles of unencrypted and encrypted DNS are different, it is complementary to service both unencrypted and encrypted DNS on the same machine thereby allowing better overall utilization of modern server hardware. However, it remains critical to test and establish the server's performance limits while factoring in the expected mix of DNS protocols to provision enough capacity.

While many modern browsers and operating systems support encrypted DNS and automatic upgrade mechanisms, many older platforms and devices do not. We expect the transition to encrypted DNS will be gradual and have observed that today, depending on the types of devices and applications on the network, a service provider enabling encrypted DNS protocols can expect between 5% and 20% of DNS client queries to use encryption. This will grow over time to protect substantially all end user queries as client devices upgrade to versions that support DDR and DNR.

3.2.3. Consider All Elements of DNS to Maximize Security and Trust

Delivering encryption between the user and the resolver is one part of the DNS security story.

DNSSEC is an additional line of defense for query response integrity and can reliably validate the authenticity of DNS records providing optimal protection against cache poisoning. However, it only works for domains that are signed. While the number of signed zones is increasing, use of DNSSEC is not universal. Additionally, it is important to have robust defenses against cache poisoning such as a separate delegation cache, not trusting every delegation, and trusting information about a delegation only for the domain in question.

Even if you have DNSSEC verified and cached the response, it may not be safe, with attackers signing malware, DDoS, and other malicious zones to appear more legitimate. Having protective DNS mechanisms to classify and block these is of great importance when delivering a secure DNS service.

3.2.4. Keep DNS Server Software Up to Date

DNS has been evolving rapidly over the past few years. Deploying new versions of software promptly ensures the latest protocols, optimizations, and security enhancements are available.

3.2.5. Highlight Your Privacy Policy

Subscribers will not be motivated to choose alternate DNS services if they understand and are comfortable with how their data is safeguarded. Highlight limits on what data is collected and retention policies to close the perception gap.

4. Conclusion

Encrypted DNS ensures confidentiality, integrity and authentication for a critical internet protocol. There are no remaining technical obstacles to implementation. Yet overall usage remains low due to a few factors.

Growing tracking concerns have led to privacy focused approaches like oblivious DNS. These over-the-top services completely bypass the network provider's DNS. That poses challenges for operators who rely on their DNS as a control plane, for troubleshooting, compliance, and as a foundation for value-added services. The adoption of these services is currently limited, but standardization efforts will lower the barrier for new services to be offered.

Service Providers have an opportunity to demonstrate their commitment to subscriber security and privacy while maintaining DNS policies to meet regulatory requirements or enable subscriber facing services by:

a. Adopting automatic upgrade mechanisms to simplify operations, maximize encrypted DNS usage and enable carrier integration with third-party privacy services
b. Maintaining a strong focus on the performance and resiliency of their DNS service
c. Applying best security practices to all stages of DNS resolutions
d. Communicating their privacy policies

A proactive strategy will maintain the service provider's DNS as the preferred choice for subscribers.

Abbreviations

DNS	domain name system
Do53	DNS over port 53 (UDP and TCP)
DoH	DNS over HTTPS
DoOH	DNS over oblivious HTTPS
DoQ	DNS over QUIC
DoT	DNS over TLS
HTTP	hypertext transfer protocol
HTTPS	hypertext transfer protocol secure
IETF	Internet Engineering Task Force
IoT	internet of things
ODoH	oblivious DNS over HTTPS
OS	operating system
PKE	public key encryption
PoC	proof of concept
QUIC	quick UDP internet connections
RFC	request for comments
TCP	transport control protocol
TLS	transport layer security
SCTE	Society of Cable Telecommunications Engineers
SUDN	special use domain name
UDP	user datagram protocol

Bibliography

Apple. (2021, December). *iCloud Private Relay Overview.* Retrieved from www.apple.com: https://www.apple.com/icloud/docs/iCloud_Private_Relay_Overview_Dec2021.pdf

Google. (2024). *IP Protection (formerly known as Gnatcatcher).* Retrieved August 22, 2024, from https://github.com/GoogleChrome/ip-protection

IETF. (n.d.). *DNS Delegation (deleg)/about*. Retrieved August 22, 2024, from https://datatracker.ietf.org/group/deleg/about/

IETF. (n.d.). *DNS Delegation (deleg)/documents*. Retrieved August 22, 2024, from https://datatracker.ietf.org/group/deleg/documents/

J. Crowe, et al. (2022, September). *Encrypted DNS from Pilot to Production.* Retrieved August 22, 2024, from https://wagtail-prod-storage.s3.amazonaws.com/documents/FTF22_SEC02_Crowe_3833.pdf

Kinnear, E., et al. (2022, June). *RFC9230 (Experimental) Oblivious DNS over HTTPS.* Retrieved from datatracker.ietf.org: https://datatracker.ietf.org/doc/rfc9230/

M. Boucadair, Ed., T. Reddy, Ed., D. Wing, et al. (2023, November). *RFC9463 DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers (DNR)*. Retrieved August 22, 2024, from https://datatracker.ietf.org/doc/rfc9463/

T. Pauly, et al. (2023, November). *RFC9642 Discovery of Designated Resolvers.* Retrieved August 22, 2024, from https://datatracker.ietf.org/doc/rfc9458/

Thompson, M., & Wood, C. (2024, January). *RFC9458 Oblivious HTTP.* Retrieved August 22, 2024, from https://datatracker.ietf.org/doc/rfc9458/

W3Techs. (2024, August 22). *Usage statistics of Default protocol https for websites*. Retrieved from Web Technology Surveys: https://w3techs.com/technologies/details/ce-httpsdefault