DNS Encryption: Exposure or Opportunity?

A Technical Paper prepared for SCTE•ISBE by

Mark Dokter
Senior Product Manager
Akamai
Toronto, Canada
+1 613 670 8451
mdokter@akamai.com

Bruce Van Nice
Senior Product Marketing Manager
Akamai
Santa Clara, CA
+1 650 381 6074
hvannice@akamai

Table of Contents

List of Figures

1. Introduction

Encrypting DNS traffic has been a focus of the IETF for several years, and in late 2018 two standards were formalized for use between clients (stub resolvers) and resolvers[1]: DNS over TLS and DNS over HTTPS. Numerous implementations have appeared, and DNS encryption has become a visible topic in industry media.

It's a testament to the original design that the way the DNS operates has remained largely unchanged for more than 30 years since the protocol was originally specified. Stub resolvers on clients (typically configured from a local network with a protocol like DHCP) send queries to a caching resolver which, in turn, talks to authoritative DNS servers that provide answers to queries.

DNS encryption changes the transport protocols and, due to some design choices, opens up the possibility of significant changes in the way client devices behave. This paper discusses these changes and their potential impact on service providers. It also offers guidance about how to address encrypted DNS deployments, summarized below:

- Communicate about privacy and security practices so subscribers are aware of how their service is protected and privacy is preserved
- Implement Best Practices for DNS resolution to ensure services are performant, resilient, and always available
- Understand the new DNS encryption protocols and how they can be deployed, and participate in formulation of standards to ensure they can be scaled and operationalized
- Consider additional services that protect subscribers and further enhance their privacy by preventing loss of personal data

2. DNS Encryption Protocols

The DNS over TLS protocol (DoT) is specified in IETF RFC 7858. DNS over TLS uses port 853 rather than port 53 originally specified for DNS. Currently available client implementations of DoT are summarized in a table below. It's important to point out stub resolvers on user devices can also connect to "over the top" public DNS services rather than an in-network resolver provisioned by a network operator[2]. Because it uses a dedicated port, it is easy to detect DoT in network traffic, a useful characteristic for network operators and security teams.

[1] Details of the motivations for developing these new protocols can be found on the Akamai Blog: Architectural paths for evolving the DNS

[2] Public DNS resolvers have been available for many years but the advent of DNS encryption creates the perception they are more private and secure, and integration into client software makes them more accessible.

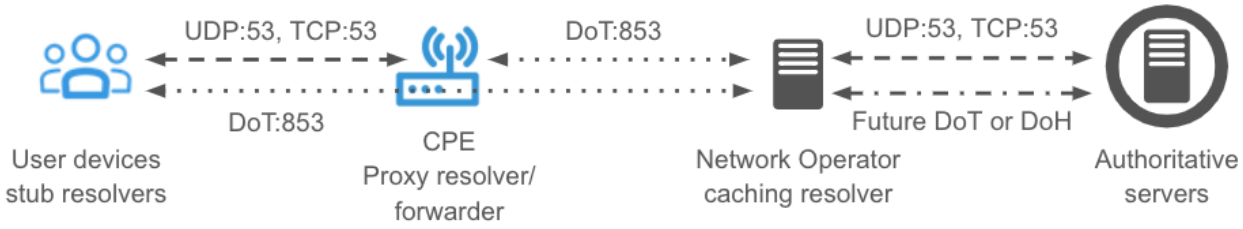

Figure 1 – DNS over TLS defines encrypted transport between stub resolvers and resolvers using TLS

The DNS over HTTPS protocol (DoH) is specified in IETF RFC 8484. DoH uses the same port, 443, as HTTPS. Currently available client implementations of DoH are summarized in a table below. As with DoT, user devices can connect to "over the top" public DNS services. Because it uses the same port as HTTPS, it's impossible to identify DoH in standard web traffic, which raises obvious security and operational concerns. Perhaps also obvious but worth stating, operators of DoH resolvers still see queries in the clear, regardless of the encrypted transport and services provided by the resolver function as they would with unencrypted transport.

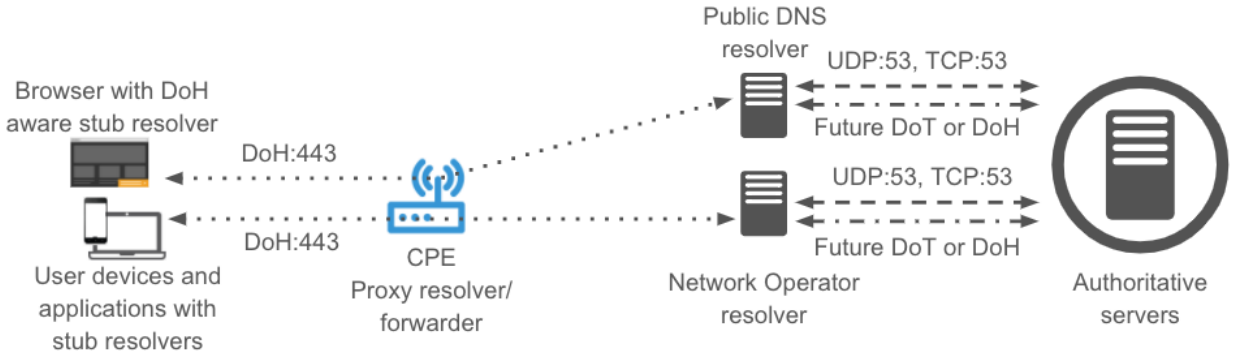

Figure 2 – DNS over HTTPS defines encrypted transport between stub resolvers and resolvers using HTTPS

3. DNS Encryption and ISPs

DNS encryption is intended to protect users from unwanted eavesdropping of DNS traffic by a third party on the path between the user and the resolver they're connected to. Most provider networks are highly secure, and it's challenging for adversaries to infiltrate them and intercept traffic. Providers in many parts of the world are also subject to data privacy regulations and/or have contractually agreed Terms of Service that spell out how they use and protect customer data.

This clouds the DNS encryption value proposition for providers. It's hard to make a business case that secure networks with defensible data protection processes and policies benefit from a layer of encryption that adds cost and complexity.

But service providers are still motivated to understand these new protocols because they may fundamentally change the way subscribers perceive DNS, and client implementations may make it easier for users to bypass provider DNS and connect to public DNS resolution services like Google and several others.

On the positive side, providers have the potential to create value added services that take advantage of DNS encryption. Technology solutions can be developed that keep business and consumer subscribers connected to encrypted DNS resolvers offered by their provider when they're off that provider's network, visiting an untrusted Wi-Fi hotspot for instance. In these cases, since their traffic is transiting untrusted networks, encryption is useful.

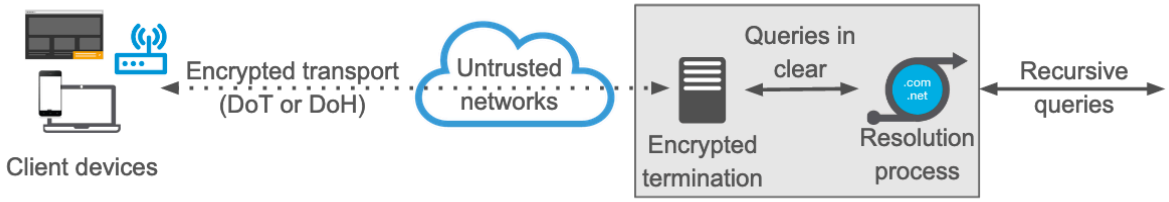

Figure 3 – Encrypted transport termination with query processing in the clear

Queries are de-encrypted at the transport layer and presented in the clear for resolution. As encryption between client and resolver is terminated at the providers DoH/DoT service, the DNS service can be equipped with threat intelligence and policies that identify malicious or unwanted domain names to enable security (blocking phishing and malware for subscribers) or content filtering (parental controls for families) to add more value. Integrated offers can also be created with a unified subscriber experience across both a providers network and other networks a subscriber traverses.

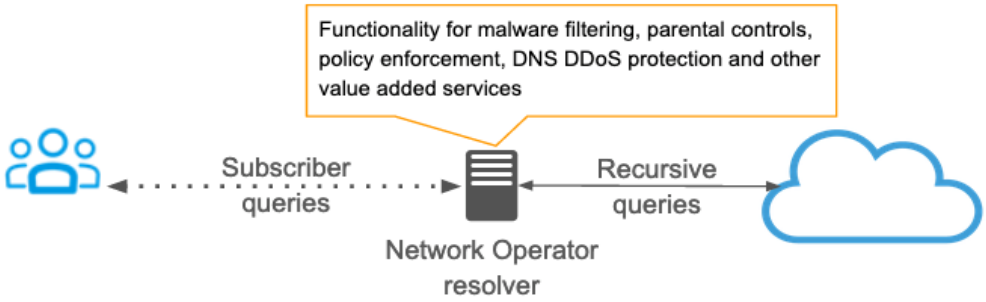

Figure 4 – Resolvers can be equipped with threat intelligence and policy to enable security and other services

4. DNS Encryption Client Implementations

Numerous client implementations of DoT and DoH are tabulated below. The client ecosystem continues to progress at rapid pace, with a broad representation of DNS Encryption capable operating systems, browsers, applications and CPEs existing today. It is expected that configuration mechanisms and awareness of local network conditions, as detailed below, will continue to evolve with ongoing standardization efforts.

Client Feature Summary as of Q3 2020

	DoT	DoH	Existing Configuration Mechanisms	Awareness of local network conditions
Operating Systems				
Android 9+			Same Provider Auto Upgrade or user specified on OS config	Auto upgrade to same DNS provider, fallback to unencrypted
Apple iOS 14			Configurable by Apps or user specified on OS/system config	Enterprise policy awareness. Fail open when auto-discovery in use. Resolver configuration specified by App is optional fallback to system specified encrypted DNS resolver
Apple MacOS 11			Configurable by Apps or user specified on OS/system config	As above
Windows 10			Limited Same Provider Auto Upgrade or user specified on OS/system config	User specified (Unencrypted only, encrypted only, encrypted preferred with unencrypted allowed)
Browsers				
Firefox			Geo Specific Opt-Out + explicitly configured	Canary domain. Fallback to system specified DNS. Enterprise policy, safe search, parental controls detection
Chrome			Limited Same Provider Auto Upgrade + explicitly configured	Auto upgrade to same DNS provider, fallback to unencrypted. Enterprise policy, parental controls detection
Chromium variants			Limited Same Provider Auto Upgrade + explicitly configured	As above
Mobile Apps				
1.1.1.1			Manually enabled, restricted to 1.1.1.1 service	User specified App exclusion
Intra			Manually enabled	User specified App exclusion

Quad9 Connect			Manually enabled, restricted to 9.9.9.9 service	User specific list of domains to send to system resolver
CPE				
FritzBox			Manually enabled	User specified (DoT servers, fallback behavior)
Turris			Manually enabled	User specified (DoT servers)
OpenWRT			Manually enabled	User specified (DoT/DoH servers)

Additional details of current client implementations can be found in the appendix at the end of this paper.

5. Provider Impact of DNS Encryption Clients

As can be seen from the descriptions above, there's currently considerable diversity in client behavior because standards only define how to use secure transport for DNS. Standards aren't yet defined for clients to discover encrypted resolvers, understand local network conditions, and establish and maintain a connection.

Today end users need to take some action in order to enable DNS encryption - navigate to a configuration interface and accept defaults and/or enter information or load an app. There are also differences in how clients fall back to DNS over port 53 if a connection to an encrypted resolver can't be established or fails. And there's no agreed upon method to acknowledge or detect local network conditions, such as the presence of a VPN, an enterprise network, or DNS filtering that might be subverted by the choice of an alternative resolver.

These are critical limitations for service providers. Manual configuration by users is completely incompatible with operation at scale. Default configurations that favor public DNS resolvers bypass provider DNS. Ignoring local network conditions can subvert security and services like parental controls.

As of July 2020, a wide range of possible solutions to these problems have been proposed in the IETF. They can be broadly categorized as: informational drafts describing the current state of the problem, proposals to use existing network technologies like DHCP or Radius to upgrade to secure transport, methods to add functions to the DNS itself, and overlay solutions.

One of the drafts is currently being tested with the Firefox browser and DoH resolvers deployed by Comcast[3]. In simplified terms, it tests for the presence of DNS policy (e.g., security, parental controls) using a "canary" domain that signals its presence and then queries for a special name to get the address of an encrypted resolver provisioned on the local network. If the query fails, then additional logic can be implemented to select an alternative DoH resolver. This mechanism is currently being tested in Firefox with DoH resolvers deployed by Comcast.

[3] https://www.ietf.org/id/draft-rescorla-doh-cdisco-00.html

To influence the way clients discover resolvers, the ISP/MNO community needs to be active in the IETF and contribute to relevant RFCs. This will ensure standards deliver the same "just works" experience users have today and are compatible with operational systems.

6. Operational Impact of DNS Encryption

Privacy is a highly visible issue almost everywhere in the world and, if subscribers perceive encrypted DNS is "better," providers may be motivated to deploy it across their resolution infrastructure, particularly if subscribers start to migrate toward public DNS services.

Providers need to consider underlying details of client implementations because they'll impact operation and scaling of DNS resolution infrastructure. The shift to TCP-based, secure, transport is a major change from almost exclusively UDP-based transport today. To maximize network efficiency, resolvers will have to support today's TCP and UDP as well as multiple transport-level authentication and encryption options going forward. Dedicated equipment for TLS termination (like load balancers) increases costs and operational burden. It also adds complexity to troubleshooting efforts with separate interfaces for transport layer problems and DNS resolution itself. Different operational teams need to be coordinated to resolve issues.

Resolver performance will be heavily driven by client side implementations, and there's little consistency at present. Connection set up overhead must be understood and resolvers need to be tuned for TCP based services in addition to UDP based services. Session reuse (reusing established sessions for multiple queries) must be evaluated as well since it can have a large impact on performance. Advancements in modern server hardware allow for comparable scaling of TLS termination negating the need for specialized appliance based solutions. Failure conditions and resultant bursts of connection setup requests also need to be factored into dimensioning decisions.

Traffic types will shift as client implementations change. Monitoring and comparing Do53, DoT and DoH workloads on an ongoing basis will allow operations teams to make educated capacity planning decisions. Insights into these factors can be found in a presentation at the DNS-OARC conference held in February 2020: DNS Encryption Operational Experience and Insights.

Because it runs over HTTPS, the advent of DoH introduced the possibility of tighter integration with applications, and DoH implementations have been released in browsers. Any app could choose to implement DoH and it is also supported in several public or "over the top" DNS resolution services. The combination of these two developments has important implications for ISPs (and other network operators) and the people who use their networks.

Migrating DNS resolution to applications is a significant change. In the past, applications running on devices relied on a stub resolver implemented as part of the devices operating system which typically query resolvers provisioned by the operator of the network a device is connected to.[4]

[4] Most operating systems also allow users to manually configure DNS settings to point to a resolver that will take precedence over a resolver configured by the local network.

Fragmentation of DNS resolution among applications raises a number of concerns. One of the most obvious is the risk of substantially complicating troubleshooting when connectivity problems arise. As can be seen from the table and appendix there is currently considerable diversity in client implementations. Individual applications could choose different resolvers and have different methods for exposing that choice to the user (or not expose it at all). They could also have different philosophies about respecting local DNS filtering policies on a network.

Additional considerations may apply when a provider offers resolution services to their enterprise customers. Businesses are potentially exposed when workers use public DNS services, knowingly or not, because sensitive internal domain names could be leaked to external sources. Internal enterprise applications also will not work properly since internal names will not resolve on public resolvers. Enterprises or provider partners may need to make provisions to block access to public DNS services to prevent these problems.

Providers may need to adjust services that use DNS filtering for parental controls or security protections to account for the presence of client implementations that may choose public DNS services. For example as discussed previously some client implementations attempt to check for the presence of DNS filtering by querying for a special canary domain name. In order to ensure their filtering services are preferred by these clients providers will need to provision canary names and respond to the queries properly. In the future there may be other methods that will have to be accommodated.

It appears as though the threat landscape will evolve as well, as attackers explore whether an encrypted DNS path offers advantages.[5] In the past it was easy to monitor DNS traffic but encrypting the transport with DoH complicates the picture since DNS queries look no different than massive volumes of HTTPS traffic traversing a network.

One possible solution is to break the bootstrapping mechanism expoits use. DoH stub resolvers have to query special hostnames to obtain the IP addresses of DNS resolution services before they can establish a connection. The stub has to use the default resolver in the operating system on the device where it resides in order to accomplish this, which is usually configured by the local network (such as a provider network). Security vendors can track host names of malicious third party DoH resolvers so access to them can be blocked.

Regardless of whether DNS encryption is deployed, the presence of public alternatives amplifies provider incentives to ensure their DNS resolution services are robust and performant. Resolvers are the glue that connects subscribers to their fixed and mobile broadband services. If operators of public DNS services succeed in persuading subscribers to use their resolvers, they will play a significant role in controlling the user experience. DNS is central to virtually every internet transaction, even simple web page loads can send tens of queries. This means performance and latency of public DNS resolvers can have a direct impact on how a user perceives their internet access. Although relatively rare, there may also be cases where a resolver is unable to resolve a name and users get an error message that a resource is unavailable.

When public DNS services operate slowly or fail, as has happened several times in the past, subscribers may associate the problem with their service provider because they may not understand the role DNS plays or may not remember they switched their DNS settings! Providers may need to bear support costs during 3rd party outages and deal with unhappy customers.

[5] https://www.sans.org/reading-room/whitepapers/dns/needle-haystack-detecting-dns-https-usage-39160

A blog post referenced in the bibliography offers design and deployment guidance to help providers establish their resolvers as the preferred choice.

7. Summary Action Plan

DNS encryption has been highly visible in industry media for more than 2 years; there are many client implementations available including those from major OS, browser, mobile app and CPE vendors and several scaled public DNS resolution services exist that support it. Whether deploying it or not, providers need to be aware of the landscape and prepared to respond by:

- Communicating about privacy and security practices including network protections that block intruders, DNS data usage and retention policies, and other privacy enhancing measures in place.
- Implementing Best Practices for DNS resolution whether or not DNS encryption is supported to ensure provider resolvers are better than OTT alternatives - more responsive, reliable, resilient, & secure.
- Considering value added services that protect subscribers by deterring phishing, bots and malware that invade privacy and steal valuable personal data. Motivate subscribers to personalize their service - so they're less likely to leave.
- Contributing to relevant standards to ensure DNS encryption implementations deliver the same "just works" experience users have today, and are compatible with operational systems.

Abbreviations

CPE	Customer Premises Equipment
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoT	DNS over TLS
DoH	DNS over HTTPS
HTTPS	Hypertext Transfer Protocol Secure
IETF	Internet Engineering Task Force
ISBE	International Society of Broadband Experts
OTT	Over The Top
OS	Operating System
RFC	Request For Comment
SCTE	Society of Cable Telecommunications Engineers
TCP	Transport Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VPN	Virtual Private Network

Appendix: DoT and DoH Client Implementations

As of August 2020, implementations will continue to expand and evolve.

DoT

Operating systems

Google Android - first with support for a DoT client in 2018. After configuration by the user (it's not a default yet) it acts as the DNS client for the device, just like the DNS over port 53 client.

Apple iOS 14 and MacOS 11 - Introduced at 2020 developer conference. There is currently no way to configure DoH/DoT from the network. Users can configure an encrypted default resolver for all apps on the system. App developers can configure an encrypted resolver independent of the system, and allow users to opt-in or configure their own encrypted resolver. DoH and DoT are context-aware, when a VPN app or corporate network is detected they will not override configured settings. Developers can also write "rules" to enable encrypted DNS in certain situations or contexts. Enterprise administrators will be able to use Mobile Device Management to configure or override encrypted DNS settings. Plans call for warning users if network providers block encrypted DNS.
https://www.zdnet.com/article/apple-adds-support-for-encrypted-dns-doh-and-dot/

Mobile Apps

1.1.1.1 - a special purpose app released by Cloudflare in 2019 acts as the default stub resolver for a device. It connects to Cloudflare's 1.1.1.1 public DNS service using DoT or DoH.

Quad 9 Connect - a special purpose app for Android and iOS released by Quad 9 in 2019 acts as the default stub resolver for a device. It connects to Quad 9s public DNS service using DoT. Quad 9 is a nonprofit founded by IBM, Packet Clearinghouse, and the Global Cyber Alliance.

CPE

FritzBox, Turris, and OpenWRT implementations proxy client requests coming in from port 53 over a secure port 853 to a resolver.

DoH

Operating Systems

Apple iOS 14 and MacOS 11 - as above for DoT

Microsoft Windows 10 - a testable version of DoH was released in May 2020 aimed at power users. Users configure Windows to use DoH and then need to separately add encrypted resolvers from Google, Cloudflare, or Quad 9 through the Control Panel or Settings.
https://techcommunity.microsoft.com/t5/networking-blog/windows-insiders-can-now-test-dns-over-https/ba-p/1381282
Microsoft plans to release additional features in their 21H1 update to include more accessible system wide configuration functionality
https://www.howtogeek.com/685996/whats-new-in-windows-10s-21h1-update-coming-spring-2021/

Browsers

Mozilla - early entrant with experimental Firefox release supporting DoH in June 2018. Currently Firefox falls back from DoH to operating system defaults for DNS when heuristics detect an enterprise DNS configuration or DNS-based parental controls. One of the heuristics is the use of a canary domain, a special domain name implemented by a network operator Firefox can query that signals the use of DNS filtering on a network.
https://support.mozilla.org/en-US/kb/firefox-dns-over-https
In 2018 they released requirements for Trusted Recursive Resolvers (TRR) organizations must meet if they want their DoH services accessible in Firefox.
https://wiki.mozilla.org/Security/DOH-resolver-policy

Chrome - early entrant with experimental Chrome release in July 2019 . Chrome preserves the user experience by doing Same Provider Auto Upgrade (auto-upgrading when the existing DNS provider supports DoH). It will also allow manual config of a 3rd party DoH resolver.
https://www.chromium.org/developers/dns-over-https
https://blog.chromium.org/2020/09/a-safer-and-more-private-browsing.html

For completeness Bromite, Brave, Edge, Opera, and Vivaldi all take advantage of DoH features built into Chromium. Their network characteristics are like Chrome.

Mobile Apps

Intra - a special purpose app released by Google's Jigsaw technology incubator in 2019 acts as the default stub resolver for a device. It connects to Google Public DNS using DoH.
https://getintra.org/#!/

1.1.1.1 - as above for DoT.

Bibliography & References

RFC 7858 Specification for DNS over Transport Layer Security (TLS)
https://tools.ietf.org/html/rfc7858

RFC 8484 DNS Queries over HTTPS (DoH)
https://tools.ietf.org/html/rfc8484

Akamai Blog - Architectural paths for evolving the DNS
https://blogs.akamai.com/2018/10/architectural-paths-for-evolving-the-dns.html

Akamai Blog - Smart DNS: Delivering the Best Subscriber Experience
Use search, link not assigned at time of publication

