DNS Over HTTPS: What You Need To Know

By Greg Ferro

A PACKET PUSHERS - IGNITION WHITEPAPER

Takeaways

- Existing DNS protocols are clear text with a standard packet format. They were designed in an era when mass surveillance of network traffic was unimaginable and encryption was impractical.
- It is trivial to extract information from DNS on the network for passive surveillance. This can combined with other metadata to easily identify and then track users without knowledge or permission.
- An IETF standard for DNS over HTTPS (DoH) RFC 8484 is progressing on the standards track and seems likely to become a complete standard.
- Alternative improvements to DNS have failed to get support.
- Some applications are planning or have implemented DoH to bypass local DNS to prevent hijacking and improve privacy.
- DoH can avoid local DNS servers completely and use Google or Cloudflare public DNS services.
- Because DNS over HTTPS is an encrypted transport, there are ramifications for Deep Packet Inspection and flow inspection.

Introduction

DNS is the last plaintext protocol in widespread use on the Internet.

DNS over HTTPS is an enhancement to the DNS protocol to improve integrity of name resolution queries and increase security by preventing man-in-the-middle attacks.

In addition, queries are obfuscated into HTTPS traffic, requiring additional effort for an attacker to detect.

Why Should Enterprise IT Engineers Care?

DNS is a critical protocol for corporate IT infrastructure.

1. Internal DNS servers are used to manage private name spaces on internal private IP address ranges. Changes to the DNS protocol can have direct impact on operations.

2. DNS is key security tool for application inspection, content filtering, and logging. Changes to the protocol will affect security strategy.

3. Changes to DNS on public internet may create interoperability issues.

4. DNS over HTTPS (DoH) can be used within an application or inside a script to bypass internal DNS infrastructure or settings. The query would appear as typical HTTPS traffic. Troubleshooting could be difficult.

5. The current plan is to use a few centralized DoH DNS servers from Google, Cloudflare, Quad9, and others. This may leak information.

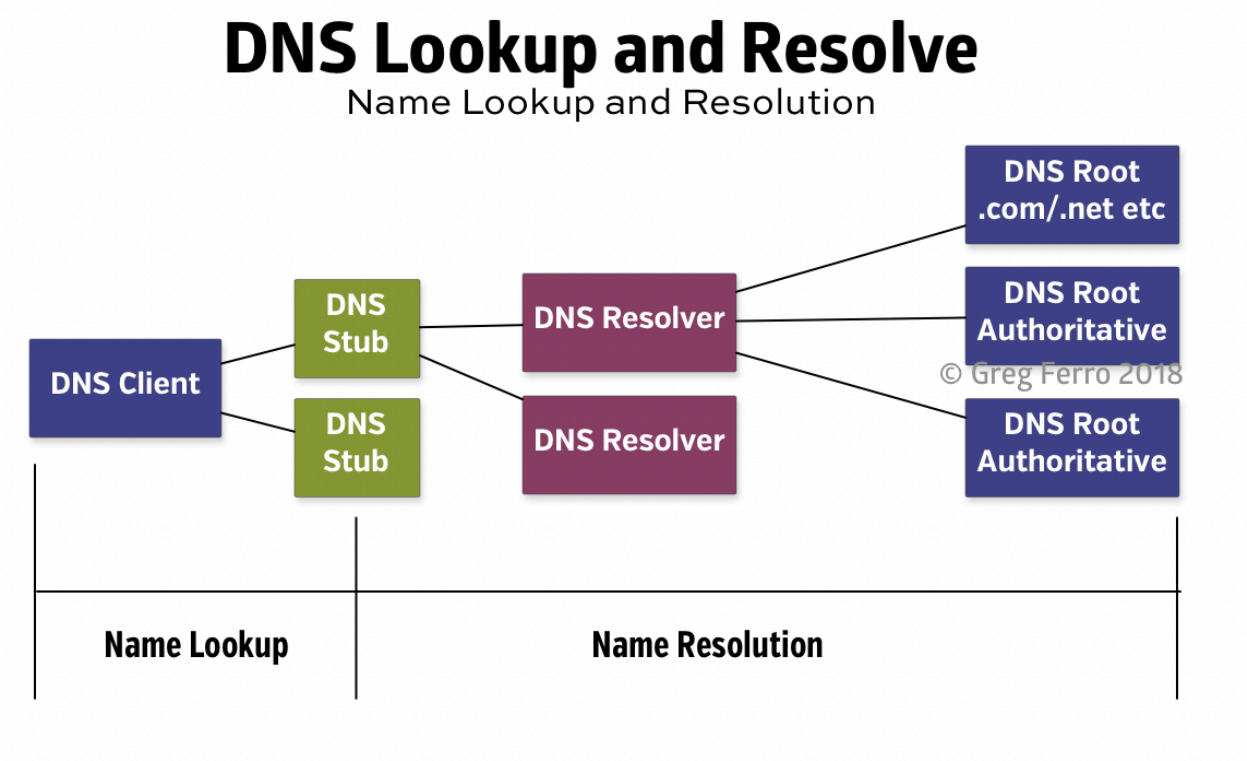
6. Consider the impact when DoH is implemented directly from the apps on smartphones. Reference

Note that DNS over HTTPS addresses the client-server interaction but doesn't solve data leakage from server-to-server DNS query.

DNS Lookups

The DNS name resolution is a distributed system. There are many layers of lookups, each with caches. Any change to the DNS systems are difficult because of these layers.

DNS over HTTPS modifies the DNS Client to DNS Stub resolver ONLY. Server-to-server queries are not modified. Changes to server-to-server communication are underway by the IETF DNS Working group.



Quick Version: What is DNS over HTTPS?

Summary: Replace the native DNS UDP protocol with HTTPS using TCP/IP with TLS encryption.

Why: To improve user privacy and safety because the DNS protocol is not encrypted and vulnerable to MITM/spoofing attacks.

Not Difficult: The general consensus is that adopting DoH is not difficult and users will not be impacted. There are known issues but not showstoppers.

Internet Ready: The use of TCP port 80 means that Internet providers are not filtering and require no change to pass DoH traffic.

Previous Attempts: Previous standards have failed to gain adoption.

Industry Momentum: DoH has support from large companies that have a motivation to see it adopted e.g. Google, Cloudflare.

Link: A cartoon intro to DNS over HTTPS - Mozilla Hacks - the Web developer blog - https://hacks.mozilla.org/2018/05/a-cartoon-intro-to-dns-over-https/

Why Everything Over HTTPS?

Why are we moving to 'everything over HTTPS'?

Prevent **Spoofing**: DNS queries from the client to the resolver, and from the resolver to recursive/authoritative/root servers, are in clear text. Therefore, it's possible to spoof/hijack DNS queries at any point in the network and redirect the user to a malicious site. For example, today some wireless portals us this redirection to force a login.

HTTPS Libraries: Access to software libraries for TLS encryption are widely available and well tested. Embedding a DoH query in a Javascript library would be reasonably secure, even with an unskilled developer. The well-known crypto software libraries are scrutinized, analyzed, and tested. They offer high confidence of integrity and safety. The availability of these libraries reduces the work needed to transition to DoH.

Browser As An App: The modern Web browser is powerful enough to act as a user interface or user application. Why develop separate apps for smartphones and desktops? The browser has security, networking, updates, etc. all packaged for you.

We Know HTTP: Many application developers have chosen to simplify development by using HTTP for all traffic. Developers learn some HTTP and DNS as part of writing Web pages as the 'hello world' of the Internet. They may not be aware that other protocols even exist.

Proxies Break Things: It was once possible to identify video, voice, and other real-time traffic as separate IP protocols and classify then by IP header information such RTP or IP Multicast streams. Many Internet providers have placed middleboxes in their networks as firewalls, TCP proxies, application proxies, and DPI engines to control traffic on public networks.

This modification of traffic flows gives unpredictable results. DiffServ QOS can fail when the TCP flow control is modified, retransmissions increase when inspection devices are overloaded (a common problem), and some applications have custom rate shaping that gets impacted.

Encryption Speed: Hardware improvements and new CPU features have increased encryption/decryption performance, which means application developers can rely on HTTPS with less worry about encryption overhead.

Software libraries have improved performance through rewrites and a new focus on speed. Newer encryption standards are selected based on speed and software performance as our understanding of computer science has improved.

HTTP Extensibility: The HTTP protocol is extensible (e.g. cookies). If DoH needs more features, HTTP can be extended to accommodate them.

DNS over HTTPS won't solve every security problem with DNS. Other protocols such as DNSSEC, DNSCurve, and DNS over TLS, have been proposed to improve DNS security. They are discussed in appendixes at the end of this document.

What Is The Value Of DNS Metadata?

Modern surveillance companies (ad-tech) collect data to track users as they move among sites. At the same time, browsers are adopting aggressive anti-tracking policies to protect user privacy, resulting in a game of one-upmanship.

DNS logs are low quality compared to other forms of data collection, but they can be useful when cross-referenced with other data.

In a subscriber operator network, DNS queries can be linked to household or user data because users pay for access. This data can be cross-linked with personal details such as credit history from accounting data.

This data may be sold to surveillance companies (Facebook, Google Ads, OpenX, etc.) to track users behavior for ad targeting and sales tracking.

DNS metadata also has value for security companies. For example, DNS logs are a primary data source for locating sites to be scanned or marked as bad. DNS

providers are often owned by security companies and for sites found in DNS lookups they can be scanned and analyzed for malware.
This data is then sold to users in the form of threat feeds, reputation scanners, and the like.

Resources

Quick Take: Anti-Tracking in Web Browsers - https://ignition.packetpushers.net/quick-take-anti-tracking-in-web-browsers/

Will Web Browsers Default to DoH?

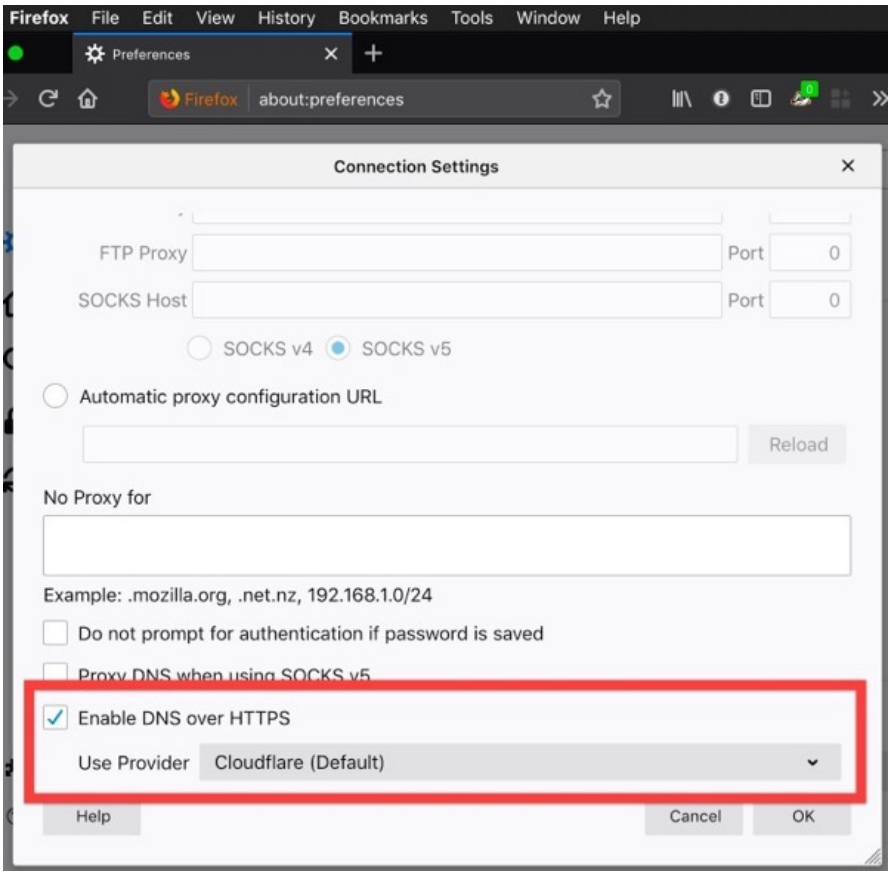
Browsers are the most significant users of DNS. There are three browser engines in the world today (Apple Webkit, Google Chromium Blink, Mozilla Gecko) behind all browser implementations.

(Note: The Microsoft Edge browser uses Blink and IE is deprecated)

It is probable that browser vendors will default to using DoH. Webkit and Firefox have a strong privacy stance that DoH addresses.

Chrome will default to Google DoH servers for additional surveillance data to improve its advertising platform. Conveniently for Google, DoH impacts competitor data gathering.

Firefox has already implemented a DoH client that can be optionally configured by users. It has announced that this will default to Cloudflare DoH for new installs.



Webkit has announced support for DoH as part of a wider anti-tracking and privacy push for browsers.

Google has shown motivation to increase Web integrity by improving Chrome safety features. Blocking known bad domains in DNS could encourage more consumer browsing and thus display more ads for revenue.

Google Chrome is not improving user privacy with browser protections, but claims that it protects users by taking their data to keep them safe.

Sources

Link: Quick Take: Anti-Tracking in Web Browsers - https://ignition.packetpushers.net/quick-take-anti-tracking-in-web-browsers/

Disabling DoH In Enterprises

Mozilla has added a feature to bypass DoH and fall back to plaintext DNS. Mozilla describes this feature as follows:

> Networks that have implemented some sort of filtering via the default DNS resolver. This can be used to implement parental controls or to block access to malicious websites.
>
> Networks that respond to names that are private, and/or that provide different responses than are provided publicly. For example, a company may only expose the address of an application used by employees on their internal network.
>
> Network administrators may configure their networks as follows to signal that their local DNS resolver implemented special features that make the network unsuitable for DoH:
>
> DNS queries for the A and AAAA records for the domain “use-application-dns.net” must respond with NXDOMAIN rather than the IP address retrieved from the authoritative nameserver.

The result here is that any network owner can perform a downgrade attack on the DoH forcing the browser to fall back to plaintext DNS by hijacking the local configuration.

Link: Configuring Networks to Disable DNS over HTTPS | Firefox Help - https://support.mozilla.org/en-US/kb/configuring-networks-disable-dns-over-https

Known Issues / Impacts

This section considers the known issues with implementing DoH.

While we would like to encourage everyone to use DoH, we also recognize that there are a few circumstances in which DoH may be undesirable, namely:
Networks that have implemented some sort of filtering via the default DNS resolver. This can be used to implement parental controls or to block access to malicious websites.

Networks that respond to names that are private, and/or that provide different responses than are provided publicly. For example, a company may only expose the address of an application used by employees on their internal network.

Firewalls And Content Filtering

DNS Firewalls: DNS firewalls lose their effectiveness with DoH and products like Cisco Umbrella are deprecated. LINK

Researchers suggest that 7 out of 10 new domains are malicious threats and DNS firewalling is a useful technique. While big DNS providers are taking steps to detect and block bad domains, they have poor granularity and quality due to scale and the intended audience.
LINK

DPI Inspection / QOS: Some DPI engines use DNS lookups as metadata for monitoring flows.

Mozilla has announced plans for a backdoor to DoH to support these requirements. This creates a downgrade attack on the DoH protocol.

Link: Configuring Networks to Disable DNS over HTTPS | Firefox Help - https://support.mozilla.org/en-US/kb/configuring-networks-disable-dns-over-https

DDOS And DOS

During a DNS amplification attack, the perpetrator sends out a DNS query with a forged IP address (i.e. the victim's) to an open DNS resolver, prompting it to reply back to that address with a DNS response.

DNS reflection/amplification attacks are managed today through patches to DNS servers and increasing adoption of MANRS to prevent IP spoofing.

Eventually DoH will remove DNS as a vector for UDP reflection attacks, but practically that is some decades away.

Regulatory Issues

Some ISP and network operators are required by their governments to block certain Web sites containing extreme content such a child abuse, or social media sites (Facebook) in crisis situations.

Currently most browsers use DNS configuration provided by their ISP. This local DNS blocking is a good effort within the control of local governments to protect (or harm) their people.

ISPs could upgrade their DNS servers to support DoH and thus meet their legal obligations, but are likely to complain that they don't want to and should not have to, and then demand government money to pay for it. Over time, DNS servers will support DoH as a standard feature; there is not extra work here.

Sources

Link: DoH! Secure DNS doesn't make us a villain, Mozilla tells UK broadband providers • The Register - https://www.theregister.co.uk/2019/07/06/mozilla_ukisp_vallain/

Link: Google, UK ISPs and Gov Battle Over Encrypted DNS and Censorship - ISPreview UK - https://www.ispreview.co.uk/index.php/2019/04/google-uk-isps-and-gov-battle-over-encrypted-dns-and-censorship.html

CDN Issues

Some CDN vendors use the ISP DNS to redirect content to a local CDN instance and reduce network costs. Using an off-network DoH server may result in name resolutions to an IP address that is not optimal.

It's reasonable to expect that CDN companies will be prepared and have a solution in place.

More Privacy Matters

DoH is a partial solution for user privacy and is part of wider movement to increase privacy.

HTTP Connection: The header in a HTTPS connection contains plain text name of the site you are connecting to.

Source IP Address: The protocol response from the Web server contains its IP address. By scanning and mapping a company's entire IP address space, the IP addresses of Web servers are generally well known.

DNS Lookups : Owners of DNS public infrastructure have access to logs that they can mine for useful data for their own ad targeting purposes or to resell.

HTTP Extensions: In the future, DoH could be extended to allow user tracking with HTTP cookies as per the HTTP protocol.

Sources

Link: draft-livingood-doh-implementation-risks-issues-03 - Centralized DNS over HTTPS (DoH) Implementation Issues and Risks - https://datatracker.ietf.org/doc/draft-livingood-doh-implementation-risks-issues/

Link: DNS over HTTPS (DoH) Considerations for Operator Networks - https://tools.ietf.org/id/draft-reid-doh-operator-00.html

Appendix: DNSSEC

DNSSEC provides a security chain of trust that provides protection from DNS vulnerabilities via private and public encryption keys. These keys validate the DNS resolution process to ensure that user name queries are protected.

- DNSSEC (Domain Name System Security Extensions) uses cryptographic keys to validate DNS queries and prevents DNS response hijacking/forging/cache poison.
- Domain owners must configure and maintain DNSSEC keys on authoritative servers for their domains.

- This requires the DNS servers, resolvers, and clients to support DNSSEC. Like any other public key infrastructure, the entire system must be supported to work as intended.
- DNSSEC requires regular operations to regenerate keys and update DNS infrastructure.
- Although cryptography is used to validate the response, it does not encrypt the query and has no privacy.

DNSSEC was supported by government security agencies and corporate surveillance companies, presumably because the DNS query was still plaintext for data gathering.

DNSSEC is not widely used. DNS providers have little incentive to upgrade their servers and encourage customers to use it.

Customers find it difficult to understand and, because it's not absolutely necessary, tend to ignore it because the penalties of misconfiguration include site outages. This research paper outlines the poor support for DNSSEC in mid-2017.

At the time of writing, DNSSEC continues to slowly gain adoption as very large companies seek to protect their domains from hijacking. If this money and effort can be sustained for a decade or so, then it's possible that the problems of DNSSEC can be overcome.

Appendix: DNSCurve

DNSCurve is a proposed new secure transport protocol for DNS designed by Daniel J. Bernstein. Bernstein is a well known cryptographer, academic, and developer (qmail) who has developed a number of crypto standards in use today.

Unfortunately, he has a poor reputation when it comes to working with the wider community and standards organizations.

DNSCurve had some early support in 2010, but it seems to have faded since then.

Opinions on DNScurve describe it as an elegant and practical solution using "the existing DNS hierarchy to propagate trust by embedding public keys into specially formatted, backward-compatible DNS records." - Wikipedia

Link: DNSCurve - Wikipedia - https://en.wikipedia.org/wiki/DNSCurve

Link: Daniel J. Bernstein - Wikipedia - https://en.wikipedia.org/wiki/Daniel_J._Bernstein

Link: draft-dempsky-dnscurve-01 - DNSCurve: Link-Level Security for the Domain Name System - https://datatracker.ietf.org/doc/draft-dempsky-dnscurve/

Appendix: DNS over TLS

DNS over TLS is a standard to encrypt DNS requests using TLS. The well-known and proven TLS software libraries would reduce implementation problems.

The standards process decided to define a new TCP protocol number 853 for this protocol. Because the Internet is substantially fire-walled, adopting this protocol number would require substantial changes across thousands of networks.

Sources

Various attempts to modify DNSoTLS to use well known ports TCP53, TCP443 did not gain acceptance.

Link: RFC 8310 - Usage Profiles for DNS over TLS and DNS over DTLS - https://tools.ietf.org/html/rfc8310

General Sources

Link: DNS Privacy Project Homepage - DNS Privacy Project - Global Site - https://dnsprivacy.org/wiki/

Link: DNS over HTTPS is coming whether ISPs and governments like it or not â€“ Naked Security - https://nakedsecurity.sophos.com/2019/04/24/dns-over-https-is-coming-whether-isps-and-governments-like-it-or-not/

Link: Newly Registered Domains: Malicious Abuse by Bad Actors - https://unit42.paloaltonetworks.com/newly-registered-domains-malicious-abuse-by-bad-actors/

Link: Firefox and DNS over HTTPS default (block DoH) â€“ Cisco Umbrella - https://support.umbrella.com/hc/en-us/articles/360001371526-Firefox-and-DNS-over-HTTPS-default

Link: Security/DOH-resolver-policy - https://wiki.mozilla.org/Security/DOH-resolver-policy

Link: What is DNS Amplification | DDoS Attack Glossary | Imperva - https://www.imperva.com/learn/application-security/dns-amplification/

Link: Can We Really Blame DNSSEC for Larger-Volume DDoS attacks? | Internet Society - https://www.internetsociety.org/blog/2016/02/can-we-really-blame-dnssec-for-larger-volume-ddos-attacks/

Link: MANRS â€“ Mutually Agreed Norms for Routing Security - https://www.manrs.org/

Link: draft-ietf-dnsop-rfc7816bis-02 - DNS Query Name Minimisation to Improve Privacy - https://datatracker.ietf.org/doc/draft-ietf-dnsop-rfc7816bis/

Link: Domain Name System Security Extensions - Wikipedia - https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions

Link: An End-to-End View of DNSSEC Ecosystem Management - https://www.usenix.org/system/files/login/articles/login_winter17_03_chung.pdf

Video: NLNOG Day 2019 - Bert Hubert - https://youtu.be/AGbFrZD_pnE?t=8950

About the Author

Greg Ferro survived 25+ years of Enterprise IT as a network engineer, architect, and designer. Involved with a wide range of companies in gaming, online, finance, carriers, energy and other, he was a team member or leader that designed, built and deployed quite a few medium & large solutions for well known large companies. He was CCIE#6920 (and a bunch of others) but that's not relevant now.

With a multi-vendor focus from the start, he has worked with a wide range of vendors, their products and technologies. Which turned out pretty well if you are going to talk about them intelligently on a podcast every week but left him with a passion for predictable, stable solutions that he never got to experience in the real world.

He is well known for his Etherealmind technology blog since 2008, and has been a regular speaker & presenter at a wide range of industry events. For a dedicated technologist, he is surprisingly passionate and committed to treating people as humans that are profit-generating productivity tools instead of 'fleshy robots as a cost centre'.