The DNS Over HTTPS – What It Is All About

Introduction

Whenever we open launch a Web browser (whether it is Firefox, Opera, Safari, Chrome, Edge, etc.) and enter in a URL, which is essentially the domain name, the entire process takes just a matter of seconds to accomplish.

There could be other factors that impede this load times, such as the speed of your Internet connectivity, and also, just how graphics intense the website you are trying to access is. For example, if there is a lot of dynamic content, such as videos, the website could take longer to load up versus a website with just static content.

But within these seconds, a lot transpires. For example, the domain name that you entered gets transmitted to what is known as the DNS, which stands for the Domain Name System. From here, the domain name of the website that you are trying to access then gets broken down into what is known as an IP Address. In other words, the domain of www.name.com could have an IP Address of 192.168.1.1.

The conversion process is technically known as the DNS Resolution. From here, the DNS then locates the specific Web server upon which this IP Address is hosted at, and then transmits your request to it, so that you can access that particular website. But this process has its own set of security issues, and attempts have been to overcome these obstacles, which is the focal point of this article.

The Shortcomings Of The DNS

There are a number of key security issues with the DNS, which are as follows:

- Any requests that are transmitted to the DNS is sent over in a plaintext format and remains unencrypted. Meaning, the information/data that is transmitted cane seen literally by anybody, especially the Cyberattacker. The bottom line here is that if this intercepted, this could be a huge backdoor in which to leverage and deploy malicious payloads, such as that of Ransomware, Trojan Horses, and other forms of Malware. But it is not just the DNS Servers and the device of the end user that are grave risk. Every other network node that is involved with transmitting the domain name are exposed as well, which can have a cascading effect.
- Because the DNS translation is done in an unencrypted fashion, all of the other intermediaries that are involved, such as other Internet Service Providers, governments of nation state threat actors, etc. can use this information/data for covert surveillance, censorship, and even the hijacking of Personal Identifiable Information (PII) of the end user.
- The DNS is also very much prone to Spoofing. For example, a firewall or router that has been misconfigured or that has been tampered with intentionally, can quite easily modify or replicate the request sent over by the end user. Thus, the DNS may not even receive this at all, and instead, the end user will be directed to a spoofed website that looks almost like the real website that he or she was trying to access in the first place.

So, what can be done to resolve these security issues? This is where the DNS over HTTPS comes into play.

The DNS Over HTTPS

This standard, also known as the "DoH", was introduced just three years ago, in 2018. This aims to protect the privacy of the DNS protocol by adding an extra layer of encryption, which is the HTTPS (this is an acronym for Hyper Text Transport Protocol – Secure). But, in order for the DoH to work, there are two components that are needed in order to make it work, which are as follows:

- An application that is DoH enabled, which in this case is the Web browser;
- A server which can support this extra layer of encryption.

So, when the end user submits their request to the DNS to access a particular website, the data packets that are involved are actually encased, or further encapsulated in the data packets that are also being transmitted by the HTTPS. This is then sent over to the server (also known as the DoH Resolver) which supports the DoH standard and sends the request back to the end user in through an encrypted line of network communications.

This actually provides a double layer of protection, so that if any of these data packets were be to be actually intercepted by a malicious third party, they would be rendered into a garbled and useless state. Also, if these communications are actually being monitored by a Cyberattacker, they would not be able to easily discern what is DNS traffic versus the HTTPS traffic.

Also, since many of the network topologies make use of the Public Key Infrastructure (also known as the PKI, or Asymmetric Cryptography), the only way that that data packets can be translated back into a decipherable format are with the Private Key. Thus, in these situations, the chances of this happening are statistically greatly diminished.

As an added benefit the data packets that are transmitted back and forth between the device of the end user and the DoH resolver actually contain a minimal amount of information/data within them, in a further effort to protect the identity of the end user. Also, only partial domain names and IP Addresses are transmitted back and forth in an effort to mask the entire request made by the end user.

Which Web Browsers Support the DoH?

At the present time, the two Web browsers that have implemented the DoH or are still in the testing phases include the following:

1) Mozilla Firefox:

   Mozilla was the first entity to actually adopt the DoH standard, and this was done in a full partnership with Cloudfare. So, when an end user transmits a request over the Firefox browser, they are then transmitted over DoH Resolvers that are hosted by Cloudflare, rather than sending them to the traditional DNS servers that also support DoH functionality. This is technically done by overriding the default network settings of the device of the end user. But, because Cloudflare is actually deemed to be a third party, there have been some privacy issues with regards to the actual storage of the PII of the end user. In response to this, Cloudflare that it will delete this within a 24-hour time span after the particular request has been made. Further, they have also announced that they will not share the PII with any other entity, unless specifically authorized to do so.

2) Google Chrome:

Google actually started testing the DoH standard with 1% of the Chrome end users late last year, and introduced this functionality in Chrome version 79, which came out on December 11th, 2019. But the approach that Google is taking in this instance, is that it will not override the network settings of the device of the end user and send the requests to a third party for further processing. Rather, the DNS servers that support DoH will be made use of instead.

Conclusions

Overall, this article has examined as to what the DoH is all about, and how it can be used to address the shortcomings of the DNS. But because other third parties may be involved with the processing of requests that are transmitted; the question now becomes of one of privacy (as illustrated by the Mozilla/Cloudflare partnership) versus security.

Also, businesses in Corporate America have always used the DNS in order to blacklist forbidden domain names, as well as to use DNS based firewalls in order to block those domains that have been known to transmit Phishing attacks, as well as malware. By using the DoH, the business it becomes much more difficult to enforce these processes.

Remember, using the old means of DNS processing offers literally no security whatsoever, because all of the requests are transmitted in a plaintext fashion. But, DoH offers this extra layer of protection, by further encrypting these requests.

At Zvelo, we recognize that privacy is important, but in the end, we err more towards the security side of the equation, and the needs for a multi-tiered approach, as exemplified by the Circles of Trust.

Sources

1) https://www.cloudflare.com/learning/dns/what-is-dns/
2) https://portswigger.net/daily-swig/a-guide-to-dns-over-https-how-a-new-web-protocol-aims-to-protect-your-privacy-online