DNS over TLS or HTTPS - the rest of the story.

September 2018

DNS over TLS or HTTPS - the rest of the story

Secure DNS isn't everything it first appears… especially when you consider the impact on different roles.

Introduction

DoH (DNS over HTTPS) and/or DNS over TLS rapidly gained attention of the infosec community with CloudFlare's announcement of 1.1.1.1 offering on their worldwide anycast network. While the 35-year-old DNS protocol admittedly remains the weakest building block of the Internet in terms of security and privacy, not everything is at it seems.

Perspective

In order to objectively assess this April 1st announcement of CloudFlare's, it's important to assess the impact on audiences of all types not just what the headlines would have you believe. There are at least four identifiable audience types to whom the impact is quite significant and different from one another, and each have solid rationales for their perspectives.

1 The consumer

There's no doubt that the Internet consumer over the years has been abused in terms of tracking and targeted advertising as we need to look no further than the facebook debacle we are experiencing in Q1-Q2 of 2018. Even when someone visits https://www.example.com, the DNS or the Internet "directory" has been mostly delivered in plain-text, meaning that anyone along the way, including your Internet gateway, your ISP and anyone else in the path of the data transit had visibility into what each subscriber's habits were. So, the idea of secure DNS means that each individual DNS query, or directory lookup, is no longer visible to those parties, thereby providing additional privacy as well as security. The privacy part is more obvious since the actual question of "where is www.example.com" is completely obscured from the Internet Service Provider and everyone else from your device to the service you're asking. The security aspect happens to be a nice side benefit since the obscurity of the question and answer disallows any man-in-the-middle altering of the answer as well as profiling of your habits. All in all, secured DNS is a huge win for the consumer, most especially in a nation-state that is oppressive. That is, as long as the oppressive state isn't blocking that service of which you're

asking. This is just a small prediction: certain nation states will be blocking 1.1.1.1 if they haven't already by 2 April 2018.

2 The Systems Administrator (sysadmin)

The role of the often underappreciated sysadmin is to be the silent hero, unworthy of any outward accolades. The reward of a "job well done" is found in the lack of problems experienced by users and stakeholders alike. Sysadmins have handled the gradual, but predictable, rollout to the secured web (http to https), the "going dark" problem in stride, because it was good for the Internet community by achieving greater privacy and security. Partially this was because DNS remained a channel of control for the sysadmin. If a device tried to access a destination known to be in control of a malicious actor, it could be blocked at the DNS level because (a) it was visible and (b) it was known to be bad. When you remove the visibility to the sysadmin who is responsible to make sure nothing malicious happens over the edge of a network, this is a problem.

3 The Provider

Any organization in the position of gaining end user or sysadmin trust to have their DNS queries sent to them for answers, has a whole lot of responsibility. This kind of burden doesn't come without cost, and therefore, benefit. Any organization that offers recursive, encrypted DNS services, and fast delivery at that, needs to be analyzed in terms of motives. In the case of CloudFlare, it is obvious that their existing subscribers benefit the most, as it is even expressed in their own blog post:

> "...every new user of 1.1.1.1 makes Cloudflare's Authoritative DNS service a bit better. And, vice versa, every new user of Cloudflare's Authoritative DNS service makes 1.1.1.1 a bit better."

Of course, every company can do what they want, but an objective assessment should always consider the provider's true motive. In this case, the customers as well as the customers of Cloudflare's customers stand to win when they use 1.1.1.1.

4 The Nation State

The reality of oppressive regimes isn't lost, either. The "going dark" problem, up until now, at least still revealed clear-text DNS queries, for the most part, except for OpenDNS's DNScurve adoption, implemented as DNScrypt. Clear-text DNS allowed DNS-based filtering and analytics to play a significant role with great nation state firewalls to allow or block certain connections and services.

With secured DNS now being part of the "going dark" protocols, it simply complicates the cat-and-mouse game, in which anyone is welcome to participate. When secured DNS is standardized and can be hosted anywhere, from a directory perspective, it just made it that much more difficult for nation states to filter source/destination pairs to be blocked.

To be sure, vendors to Nation State firewalls will quickly up their game to compensate for lack of DNS visibility by offering increased threat intelligence fine-tuned to destinations including granular per-IP SANs to make up for the lack of DNS visibility.

How does DNSSEC fit into all of this?

Aside from the fact that DNSSEC is often misunderstood as private or secure, it gives no privacy advantages over non-DNSSEC DNS. This well-intentioned protocol has been a 20-year challenge and still isn't being widely adopted. When properly implemented, DNSSEC gives authenticity, making DNS man-in-the-middle attacks impossible.

Our Conclusion

Everyone agrees on the importance that the edge of a network plays in terms of network reliability and security. In the industry, we often make an analogy to physical border officials who have the unenviable job of allowing or refusing entry to visitors. In the same way that officials need to have at least a reasonable risk assessment of entering individuals, the same applies to the edge of a computer network. While detailed traffic between endpoint and secured server should remain private and encrypted, the determination of which devices are communicating where, that should remain in control of the edge.

To do so, means the edge must have DNS visibility. This is not only sensible, but it is also possible, and everybody wins. Here's how:

Endpoint ↔ [Secured DNS channel] ↔ Edge ↔ Secured DNS channel ↔ Public Resolver

To give end users the privacy while allowing sysadmins to have the tools to protect the managed network, all outgoing connections must be whitelisted with DTTS (Don't Talk To Strangers), an implementation of short-lived "allow" rules based on the TTL (Time To Live) of successful DNS answers. "Strangers" are destination IPs that were not first resolved via DNS. For example, badactor.co will not resolve to an IP address, therefore, no "allow" rule is created to its authoritative destination. On the other hand, google.com is permitted, so an "allow" rule is temporarily created for the asker, but only for the period of the TTL. Likewise, any internet traffic attempted without an allowed DNS query is simply not allowed. This approach gives the end-user the complete confidentiality of a banking transaction, while the sysadmin knows only that Internet-Exit-Point-A is conducting business with Bank-B, not aware of any further details. The Nation State is aware of the same since source-destination IP pairs always remain visible in transit. Everybody is happy.

Who doesn't like a happy ending?