The background to DNS encryption

Date
23 November 2018 (version 1.0)

Author
Marco Davids

Page
1/3

Classification
Public

Contact
sidnlabs@sidn.nl

Contact
T +31 26 352 5500
support@sidn.nl
www.sidn.nl

Office
Meander 501
6825 MD Arnhem The Netherlands

Postal address
Postbus 5022
6802 EA Arnhem The Netherlands

DNS privacy is a hot topic in the internet community. Various DNS privacy-enhancing innovations have emerged in recent years. In this article, we compare the various technologies concerned. There's also an accompanying blog examining the controversy that surrounds one of the technologies: DNS over HTTPS (DoH).

1 Introduction

In recent years, the IETF community has been working to increase the security of the DNS protocol, as illustrated by the growth of DNSSEC. The focus on DNS security may be traced back to the following two key events.

1.1 The Kaminsky attack

Adoption of DNSSEC was given a major boost in 2008 by the so-called 'Kaminsky attack'. The incident showed how easy it was to falsify DNS responses ('DNS spoofing'). What had previously been regarded as a largely theoretical risk suddenly became a real threat. People therefore turned to DNSSEC, which assures the integrity of DNS responses, thus largely eliminating the risk of spoofing. More than half of the 5.8 million-plus .nl domain names now have DNSSEC protection.

1.2 Snowden disclosures

Edward Snowden's disclosures in 2013 focused further attention on privacy and the interception of internet traffic by state agencies and others. Snowden leaked classified information about the alleged surveillance activities of his then employer, America's National Security Agency (NSA).

The IETF, the body that develops internet standards, accordingly decided that standards should in future pay more attention to 'interceptability' and privacy.

That resulted in renewed attention for the DNS protocol. The reason being that, although DNSSEC had been introduced to protect against DNS spoofing, DNS was one of the few remaining protocols that had no encrypted variant. In other words, anyone that intercepts DNS traffic can read the queries and responses without a problem. And, by doing so, learn a great deal about the user's internet behaviour.

The renewed focus on privacy has led to a series of new developments in the field of DNS privacy. One way of enhancing privacy is to encrypt DNS traffic.

2 Benefits of DNS encryption

If DNS messages are encrypted, they can't be read by anyone except the intended recipient. That increases the user's privacy, because almost everything you do on the internet is preceded by a DNS lookup, so anyone that can read your DNS traffic has a good idea what you've been doing on the net. In the interests of complete clarity, it is worth pointing out that, if traffic is encrypted, the party at the other end of the secure connection (the resolver

operator, for example) still has that oversight of your activities. That, incidentally, is the issue that Oblivious DNS (ODNS; see above) is intended to address.

DNS encryption has two further implicit benefits:

First, encrypted traffic can't easily be tampered with. Like DNSSEC, therefore, encryption can help to prevent the falsification ('spoofing') of DNS responses. However, that is the case only if the encryption is end-to-end, which isn't going to be the case any time soon. Without end-to-end coverage, encryption is not a proper substitute for DNSSEC. Rather, the two technologies are mutually complementary. Some experts see the rise of DNS encryption as a potential driver for the further adoption of DNSSEC and standards based upon it, such as DANE.

Second, DNS encryption helps to protect against source address spoofing: a form of IP spoofing (not to be confused with DNS spoofing) often used in DDoS attacks. From time to time, the internet suffers 'plagues' of DNS amplification attacks with source address spoofing, which cause considerable problems.

Finally, TCP-based DNS encryption eliminates the problem of truncated DNS responses, albeit at the cost of a substantial IP overhead.

3 Various forms of DNS encryption

Various routes have been explored, leading to various types of solution. The main DNS encryption technologies are briefly outlined below. The technologies generally protect the 'last mile', i.e. the pathway between the client (stub) and the resolver (see Figure 1). In the descriptions below, any exceptions to that rule are highlighted.

In theory, the technologies could also be used to secure the pathway between the resolver and the authoritative server. However, that remains some way off in terms of standardisation and scalability and therefore not currently relevant.

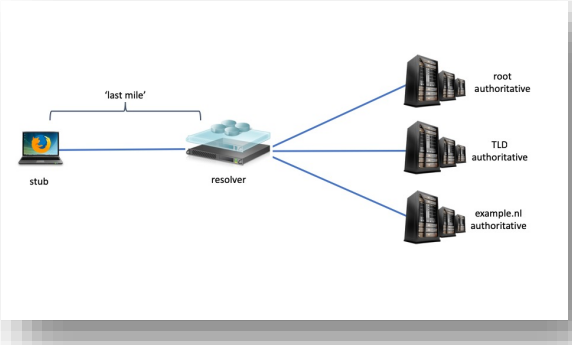

Figure 1

The list of technologies below is not exhaustive. For example, we have not included QNAME minimisation, because it isn't strictly an encryption technology. With QNAME minimisation, DNS privacy is achieved by using an alternative DNS query form, where no more information is included than strictly necessary. Oblivious DNS (ODNS) isn't included in the list, ether. Not only is there no encryption involved in ODNS, but the technology has yet to progress beyond the conceptual experimental stage.

3.1 DNSCrypt and DNSCurve

The encryption of DNS traffic to prevent third-party monitoring is not new: people were experimenting with it before the Snowden revelations. One of the oldest ideas is DNSCrypt, which is supported by several big players, including OpenDNS, Quad9 and the Yandex web browser. However, the protocol has never been brought to the IETF for standardisation, despite development being completed in 2013.

DNSCrypt works over both TCP and UDP. Its default port is 443, but no HTTPS traffic is sent via that port. Consequently, no TLS (stack) or X.509 certificates are required. DNSCrypt secures the pathway between the client (stub) and the resolver.

Another technology that uses UDP and TCP is DNSCurve. Again, the protocol hasn't been standardised by the IETF, although a draft was produced. It has relatively few applications in the wild. DNSCurve works on a 'hop-by-hop' basis between resolvers and authoritative name servers. It doesn't therefore protect

the 'last mile' between the client (stub) and the resolver. The technology may be regarded as a rival to DNSSEC, although DNSSEC is end-to-end and doesn't involve DNS encryption (implying that traffic *can* be intercepted, but can't be manipulated).

3.2 DNS over TLS (RFC7858, 2016) and DNS over DTLS (RFC8094, 2017)

By default, DNS over TLS works on TCP port 853. As its name suggests, the DNS traffic is packaged over an encrypted TLS connection. A few big public DNS providers already support it, including Quad9 and Cloudflare 1.1.1.1. Client software is also available, such as Stubby. Unfortunately, using TCP for DNS traffic has challenging overhead implications. Consideration has therefore been given to standardising DNS over DTLS, i.e. UDP-based DTLS. To the best of our knowledge, however, there are no working implementations.

3.3 DNS over HTTPS (RFC8484, 2018)

DNS over HTTPS (DoH) is a technology that involves the encryption of DNS traffic as 'ordinary' HTTPS or HTTP/2 traffic, of the kind that goes to and from websites (with the familiar green lock). TCP, in other words. The standard was developed with remarkable speed and has made significant waves. Various major players, including Google Public DNS and Cloudflare, as well as Quad9 and others, have been strikingly quick to support it. Google has incorporated the technology into the latest version of Android 9 "Pie" and is preparing its Chrome browser to support it. Meanwhile, Cloudflare has brought out an app enabling access to its service for Android and iOS users. Software developer Mozilla has already built DoH into its Firefox browser, dubbing the feature the 'Trusted Recursive Resolver' (TRR). Mozilla's support for DoH is enabled by a partnership with Cloudflare.

3.4 DNS over QUIC (draft)

QUIC (or, as it may be called in the future, HTTP/3) is a new transmission protocol with built-in encryption. A draft defining DNS over QUIC is under development. QUIC works over UDP. As a result, it's efficient and has a low overhead. It offers the best of two worlds, with the advantages of both traditional DNS over UDP and the newer DNS over TLS. It's therefore a very promising solution. The protocol specifically addresses traffic between the client (stub) and the recursive resolver, but that may change in due course.

4 Summary

It will be apparent that there are good reasons for increasing the privacy of the DNS protocol. The internet community has been looking for ways of achieving that for some time. However, Snowden's revelations served to raise the issue's profile and trigger further IETF standardisation work. Most proposed methods involve routing DNS traffic over an encrypted pathway. The landscape remains highly dynamic, but we have so far seen limited adoption of DNSCrypt, a little more adoption of DNS over TLS and strikingly rapid adoption of DNS over HTTPS (DoH).

The remarkable development of DoH and the associated controversies are considered in more detail in a separate blog. This article serves to describe the technical background to that blog.