March 2019 – Version 1.1

DNS Privacy

Frequently Asked Questions (FAQ)

Author
Fernando Gont

Internet Society

1. What are the privacy implications of the Domain Name System?

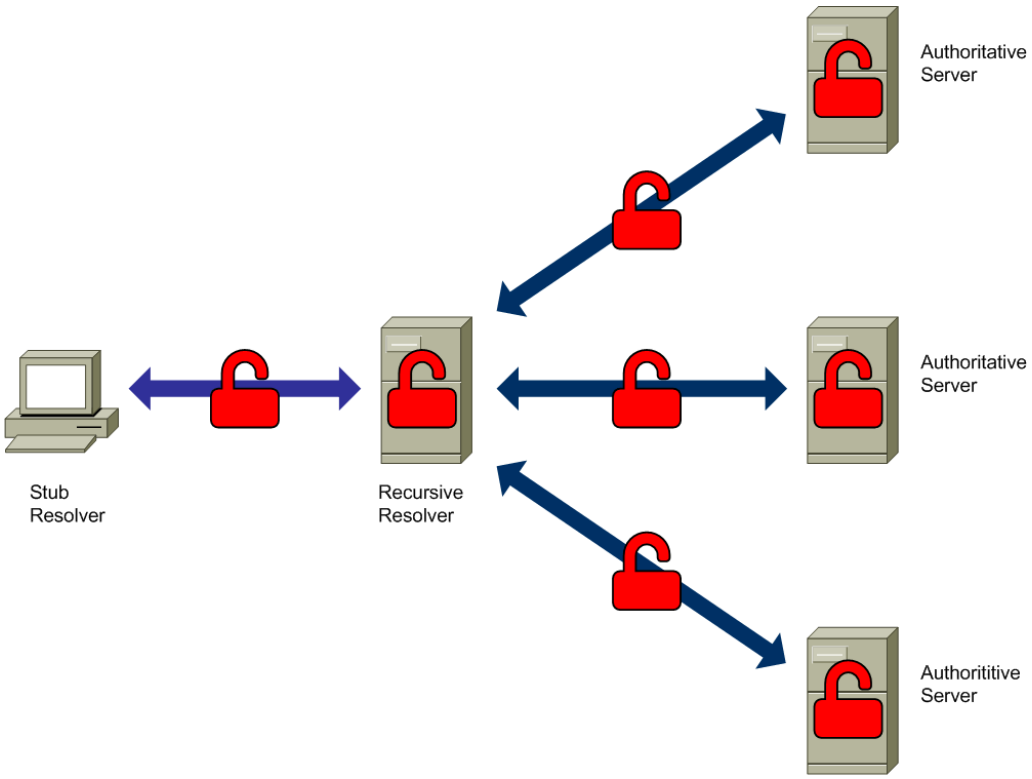
Almost every time we use an Internet application, one or more DNS transactions are performed to translate human-friendly domain names into a set of IP addresses that can be used to deliver packets over the Internet. DNS transactions can therefore be correlated with the applications we use, the websites we visit, and sometimes even the people we communicate with.

Whilst the domain name information itself is public, the transactions performed by the hosts are not. Unfortunately, the DNS does not inherently employ any mechanisms to provide confidentiality for these transactions, and the corresponding information can therefore easily be logged by the operators of DNS resolvers and name servers, as well as be eavesdropped by others.

2. Where could DNS privacy be affected?

DNS queries can be captured or logged at:

- the communications links and devices between the stub resolver and the recursive resolver;
- the recursive resolver;
- the communications links and devices between the recursive resolver and the authoritative DNS servers; and
- the authoritative nameservers.



The recursive resolver is in a privileged position to log all of the DNS queries and responses. After all, DNS queries are explicitly sent to the recursive resolver by the stub resolvers.

Any entity with access to the communications links or devices between the stub resolver and the recursive resolver, or the recursive resolver and the authoritative names servers could passively monitor the DNS transactions. Alternatively, an attacker that does not have access to such communications links or devices might still be able to eavesdrop on such DNS transactions – e.g. by attacking the routing system to divert traffic to a communications link they can eavesdrop on.

Finally, since the original query is normally re-sent to all of the authoritative nameservers involved in the recursive resolution process, authoritative nameservers might also be in a position to log information about user queries.

3. Isn't privacy for DNS transactions already provided by DNSSEC?

No. DNSSEC provides DNS data authentication, but does not provide confidentiality for DNS transactions. Confidentiality was not among the design goals of DNSSEC.

4. What kind of privacy improvements have been developed for the DNS?

There have been improvements in two areas:

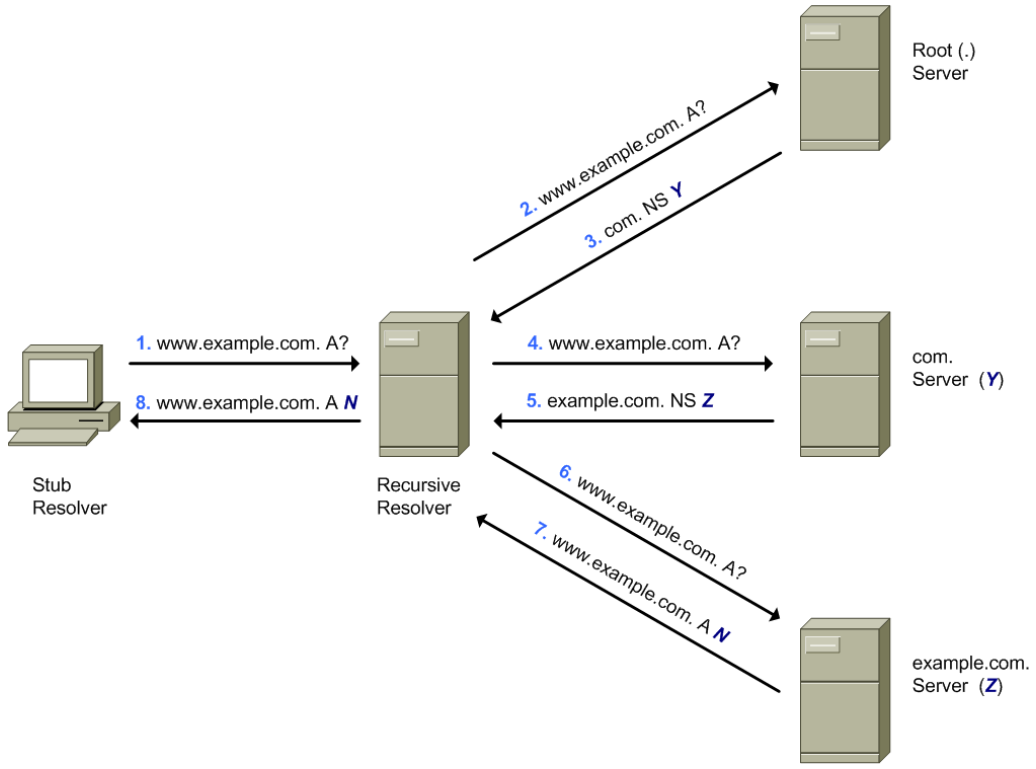
- Query name minimization (QNAME minimisation)
- Privacy improvements for transactions between stub resolvers and recursive resolvers

The improvements on these two areas are orthogonal. QNAME minimisation reduces the amount of data disclosed to authoritative nameservers. On the other hand, a number of technologies are available that provide confidentiality for DNS transactions between stub resolvers and recursive resolvers (see "6. What technologies are available for providing confidentiality to DNS transactions between stub resolvers and recursive resolvers?").

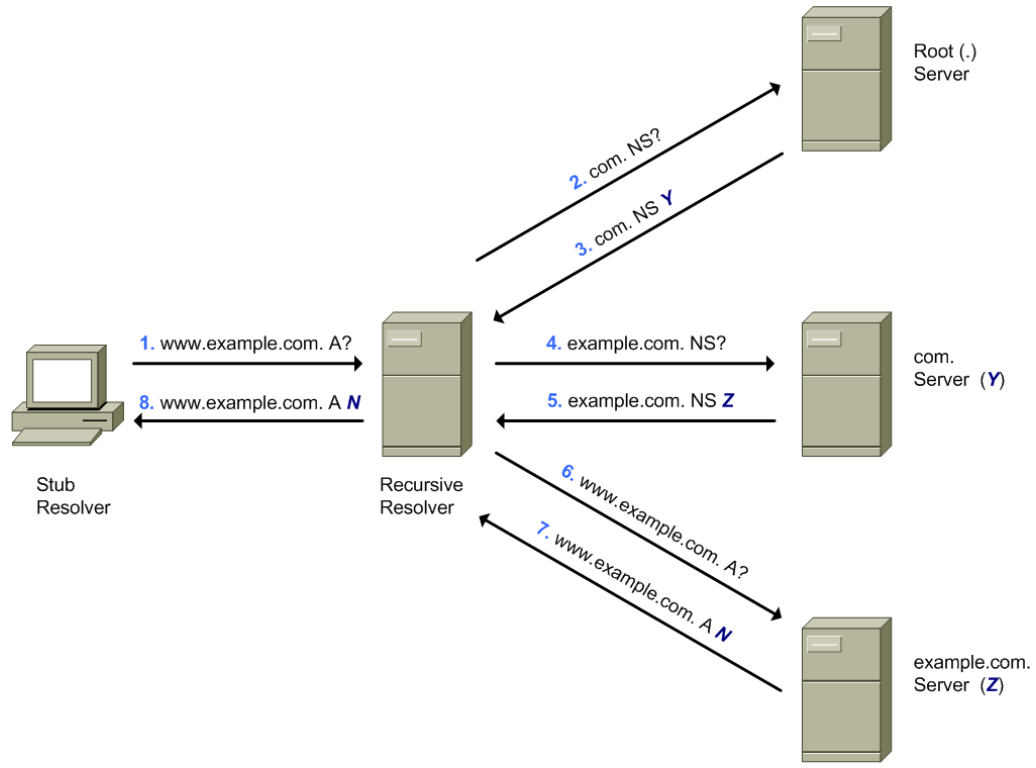
5. What is Query Name (QNAME) minimization?

QNAME minimisation is an experimental method specified in [RFC7816] to minimize the amount of data sent in DNS queries. Rather than re-sending the same DNS query to each authoritative name server that is queried during the recursive resolution process, QNAME minimisation argues that the recursive resolver should walk the authority hierarchy of a domain name by querying NS records, starting with the Top-level Domain (TLD), and increasing one level in the domain depth in each subsequent query.

For example, one possible scenario for obtaining A resource records for the domain name "www.example.com" might be:



Whereas the DNS transactions that would take place for the same scenario with QNAME minimisation would be:



QNAME minimisation is already implemented in popular recursive resolver software (see [DNS-IMPL]), and there is ongoing work at the DPRIVE working group of the IETF to publish QNAME minimisation on the Standards Track [QNAME-S].

6. What technologies are currently available for providing confidentiality to DNS transactions between stub resolvers and recursive resolvers?

At the time of this writing, the following technologies have been specified and/or implemented:

- DNSCrypt
- DNS over TLS (DoT)
- DNS over DTLS (DoD)
- DNS over HTTPS (DoH)

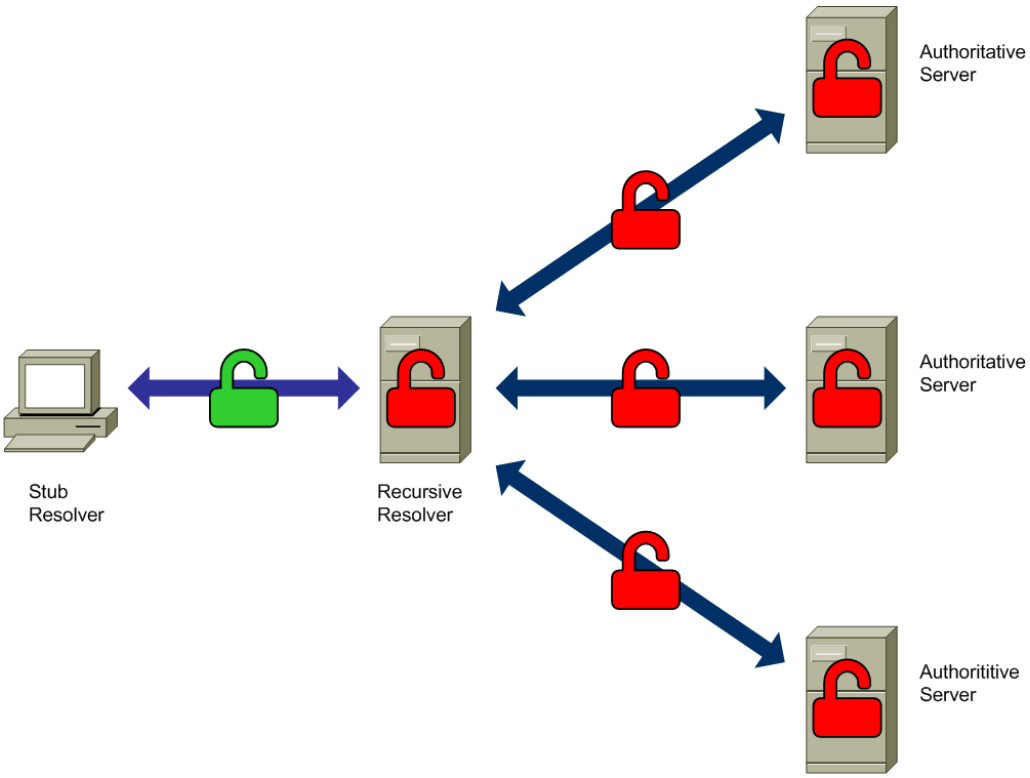
DNSCrypt has been developed outside of formal standardization bodies (such as the IETF). More information about DNSCrypt is available at [DNS-CRYPT].

DNS-over-TLS specifies how to communicate with a recursive resolver over a TLS-secured connection, and has been formally standardized in [RFC7858].

DNS-over-DTLS specifies how to communicate with a recursive resolver over DTLS-secured 'connections' and has been formally standardized in [RFC8094].

DNS-over-HTTPS specifies how to communicate with a recursive resolver over HTTPS, and has been formally standardized in [RFC8484].

The above mechanisms provide confidentiality for the communications between the stub resolver and the recursive resolver, but **not** between the recursive resolver and the authoritative name servers. Furthermore, they do not prevent possible information leakages at the recursive resolver or the authoritative name servers involved in DNS resolution:



7. What are the limitations of technologies such as DoT and DoH?

Technologies such as DoT and DoH are typically employed to provide confidentiality to DNS transactions between stub resolvers and recursive resolvers. However, they do not mitigate other vectors for vulnerating DNS privacy, such as the collection of information about DNS queries at the recursive resolver.

In some cases, using technologies such as DoT or DoH may imply using a third-party resolver (e.g. if the local resolver does not support any of these mechanisms). When a third-party resolver is employed, trust shifts from the local DNS provider to the third-party organization providing the recursive resolver, without affecting the ability of the organization operating the recursive resolver (whichever it is) to collect information about DNS queries.

There are a number of trade-offs associated with the selection and placement of a recursive resolver. Please see "9. What are the tradeoffs between running a recursive resolver on my own host vs. using my ISP's recursive resolver vs. using a third-party recursive resolver?" for further details.

8. Will information such as the names of the websites I visit be concealed from eavesdroppers and rogue actors if I employ DNS privacy technologies?

No. DNS privacy technologies only improve the privacy of DNS transactions, but do not mitigate other information leakages. Information such as the web sites you visit may leak in a number of ways, including via the Server Name Identification (SNI) TLS extension – **even if HTTPS is employed**.

Even when it comes to DNS traffic, technologies such as DoT and DoH only encrypt transactions between the stub resolver (at the local host) and the recursive resolver. DNS queries can therefore still be collected, e.g. by the recursive resolver.

9. What are the tradeoffs between using a recursive resolver on my own host, versus using my ISP's recursive resolver, versus using a third-party recursive resolver?

The following table summarizes the tradeoffs between different recursive resolvers:

Resolver	On host	On CPE	At ISP	Third Party
Logged queries	No	No	Yes	Yes
Eavesdropped	Anywhere	Anywhere	From host to ISP	No
Identity exposed to Authoritatve Servers	Host	Network	ISP	Third-Party
Legal jurisdiction	Same as host	Same as host	Same as host	Same as third-party resolver
Topologically-dependent responses	Yes	Yes	Yes	No

In the table above, the meaning of each row is as follows:

- Logged queries: whether DNS query information can be trivially logged, without even the need of eavesdropping.
- Eavesdropped: where in the network queries could be eavesdropped such that the identity of the host or host network becomes exposed.
- Identity exposed to authoritative servers: identity being exposed to authoritative nameservers via the source address of the DNS queries.
- Legal jurisdiction: relates to the legal power over the recursive nameservers.
- Topologically-dependent responses: whether DNS responses may be topologically-dependent (e.g. a CDN responding with the address of a close server)

In the table above, "CPE" assumes a user-controlled and user-configured CPE router. We note that in many deployments, the CPE may actually be controlled and operated by the ISP.

10. Should I enable mechanisms such as DoH or DoT for encrypting transactions with the recursive resolver?

It depends. Whilst there is a tendency to assume that it is preferable to employ a *privacy-enhanced* recursive resolver over the one advertised on the local network (e.g. the one provided by local ISP), the choice of the recursive resolver should be based on an actual threat model. For example, if the adversary is expected to operate closer to the local ISP (or is assumed to be the ISP itself), encrypting all queries towards a third-party recursive resolver might help improve privacy. However, if the main adversary is assumed to operate on external networks, then using a third-party recursive resolver might actually have a negative impact on privacy.

Employing a third-party recursive resolver might imply that DNS traffic is handled by an organization with a different legal jurisdiction, and may result in the use of recursive resolvers that are shared by a larger number of users. This has the effect of the concentrating trust of a large number of hosts to a small set of recursive resolvers which become more attractive to rogue actors, etc..

On the other hand, when communicating with the recursive resolver of choice, it is generally preferable to employ mechanisms that encrypt DNS transactions (such as DoT) as opposed to traditional plain text DNS transactions. For example, if an ISP-provided recursive resolver is to be employed that implements DoT, it will prevent eavesdroppers on the local network from collecting information about the DNS queries made by local users.

11. May I be (inadvertently) using a third-party recursive resolver, as opposed to the recursive resolver advertised by my local network or the recursive resolver on my local host?

Yes. There have been news from organizations developing web browsers and operating systems that they have considered enabling DNS privacy technologies that would send all DNS queries to a third-party recursive resolver, as opposed to the recursive resolver advertised by the local network. (see [ANDROID] and [FIREFX-DOH]) – albeit the controversy has been rather significant [UNGLEICH].

Please check the documentation of your operating system and your web browser for an authoritative answer on the DNS technologies they employ.

12. Should I employ QNAME minimisation?

Yes. QNAME minimization is useful to minimize the amount of data exposed to authoritative nameservers. Please check "5. What is Query Name (QNAME) minimization?" for more information.

13. Do any of the DNS privacy improvements relieve me from using privacy technologies such as VPNs or the Tor network?

Not at all. Technologies such as VPNs or the Tor network [TOR] offer other privacy services, normally concealing a lot more than the DNS queries.

14. Where can I find more detailed information about DNS privacy?

We have published a document entitled "Introduction to DNS Privacy" [DNSP-INTRO] that contains more detailed information about this topic, along with a number of references for further information.

Acknowledgements

Stéphane Bortzmeyer, Kevin Meynell, Hugo Salgado, Dan York, and Jan Žorž provided valuable comments on this document.

References

[ANDROID] "DNS over TLS support in Android P Developer Preview ". Google Security Blog. April 17, 2018. https://security.googleblog.com/2018/04/dns-over-tls-support-in-android-p.html

[DNS-CRYPT] DNSCrypt web site. https://dnscrypt.info/

[DNS-IMPL] "DNS Privacy Implementation Status", last updated September 11, 2018. https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Implementation+Status

[DNSP-INTRO] Gont, F. "Introduction to DNS Privacy". March 2019. https://www.internetsociety.org/resources/deploy360/dns-privacy/intro/

[DPRIVE-WG] DNS PRIVate Exchange (dprive) working group. https://datatracker.ietf.org/wg/dprive/about/

[FIREFX-DOH] "Improving DNS Privacy in Firefox". https://blog.nightly.mozilla.org/2018/06/01/improving-dns-privacy-in-firefox/

[QNAME-S] "DNS Query Name Minimisation to Improve Privacy", IETF Internet-Draft (work in progress), draft-ietf-dnsop-rfc7816bis-01 https://tools.ietf.org/html/draft-ietf-dnsop-rfc7816bis

[RFC7816] Bortzmeyer, S., "DNS Query Name Minimisation to Improve Privacy", RFC 7816, DOI 10.17487/RFC7816, March 2016. https://www.rfc-editor.org/info/rfc7816

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016. https://www.rfc-editor.org/info/rfc7858

[RFC8094] Reddy, T., Wing, D., and P. Patil, "DNS over Datagram Transport Layer Security (DTLS)", RFC 8094, DOI 10.17487/RFC8094, February 2017. https://www.rfc-editor.org/info/rfc8094

[RFC8484] Hoffman, P., and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018. https://www.rfc-editor.org/info/rfc8484

[TOR] Tor Project.
https://www.torproject.org/

[UNGLEICH] "Mozilla's new DNS resolution is dangerous". Ungleich blog.
https://blog.ungleich.ch/en-us/cms/blog/2018/08/04/mozillas-new-dns-resolution-is-dangerous/