Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 29, 2019

P. Hoffman
ICANN

September 25, 2018

Associating a DoH Server with a Resolver
draft-hoffman-resolver-associated-doh-02

Abstract

Browsers and web applications may want to know if there are one or more DoH servers associated with the DNS recursive resolver that the client is already using. This would allow them to get DNS responses from a resolver that the user (or, more likely, the user's network administrator) has already chosen. This document describes a protocol for a resolver to tell a client what its associated DoH servers are.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on March 29, 2019.

Table of Contents

1. Introduction

DoH [I-D.ietf-doh-dns-over-https] requires that one or more DoH servers be configured for the DoH client. That document does not say how the DoH servers are found, nor how to select from a list of possible DoH servers, nor what the user interface (UI) for the configuration should be.

There is a use case for browsers and web applications who have one or more currently-configured DNS recursive resolvers wanting to use DoH for DNS resolution instead. For example, the recursive resolver knows how to give correct answers to DNS queries that contain names that are only resolvable in the local context. Users typically configure their DNS recursive resolvers with through manual configuration (such as manually editing a /etc/named.conf file) or through automatic configuration from a protocol such as DHCP.

The client that wants to change from its currently-configured DNS recursive resolvers might be the stub resolver in an operating system, although at this time it is rare that such stub resolvers can use DoH. A much more likely use case is a browser or web application that is getting name resolution through the stub resolver on the computer on which it is running. The user of the browser might have a preference for using a DoH server, and they might need to use a DoH server that is associated with the resolver that the computer is currently using so that its queries for non-global names are answered correctly. They may also be required to use only resolvers that are approved by their organization's network operators.

To address this use case, this document defines a new special use domain name "resolver-associated-doh.arpa." and describes how it is used. The design choices made are described in Section 4.

2. Terminology

In this document, "DoT" is used to indicate DNS over TLS as defined in [RFC7858].

In this document, "Do53" is used to indicate DNS over UDP or TCP as defined in [RFC1035].

"DoH client" and "DoH server" are defined in [I-D.ietf-doh-dns-over-https].

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Signalling the DoH Servers Associated with a Resolver

To find the DoH servers associated with a resolver, the client sends that resolver a query for resolver-associated-doh.arpa in class IN with the RRtype of TXT [RFC1035] (that is, the query is resolver-associated-doh.arpa/IN/TXT).

The resolver replies with its associated DoH servers as URI Templates [RFC6570] in the TXT RRset in the Answer section.

3.1. Signalling in the Resolver

A resolver that understands this protocol MUST send a TXT RRset in the Answer section. Each TXT record contains one URI Template.

If a resolver that understands this protocol has no associated DoH servers, the TXT RRset contains exactly one record that has an empty string as the RDATA; that is, the RDLENGTH in that record is 1, and the RDATA contains just the byte 0x00.

Note that the zone resolver-associated-doh.arpa, as it is delegated in Section 5, has no TXT records of its own. The resolver adds its own TXT records to the answer.

3.2. Client Handling of the Signals

The client uses the TXT records in the response to the resolver-associated-doh.arpa/IN/TXT query as a list of the URI Templates of the DoH servers associated with the resolver. Note that TXT records can contain multiple "character-strings" [RFC1035]; for this protocol, all characters-strings in a TXT record are concatenated to form a single URI Template.

If a client sends the resolver-associated-doh.arpa/IN/TXT query over a transport that assures data integrity (such as DoT), and it receives a response that has the RCODE set to NOERROR and no relevant answers in the Answer section (also called a "NODATA" response in [RFC2308]), the client can assume that the resolver does not know this protocol.

See Section 7 for warnings about sending the resolver-associated-doh.arpa/IN/TXT query over a transport that does not assure data integrity (such as Do53).

The client SHOULD only use a DoH server listed in the response to resolver-associated-doh.arpa/IN/TXT for the length of time listed as the TXT RRset's TTL field. Using an associated DoH server beyond the TTL can expose the client to problems such as loss of DNS service. The client SHOULD send a resolver-associated-doh.arpa/IN/TXT query before the expiration of the TTL in a previous response in order to allow the client to continue to use an associated DoH server without interruption.

A client MUST issue a new resolver-associated-doh.arpa/IN/TXT query every time the configured resolver in the operating system changes.

4. Design Choices

The primary use case for this protocol is a browser or web application that is getting name resolution through the stub resolver on the computer on which it is running wanting to switch its name resolution to DoH. A secondary use case is an OS that wants to make a similar switch.

An earlier design suggestion was to use a new RRtype with a query to ./IN/NEWRRTYPE. However, it was pointed out that this would not work going through stub resolvers that validate DNSSEC.

An earlier design suggestion was to use DHCP to tell the OS the DoH servers that the stub resolver might use. That protocol is orthogonal to the one in this document in that it addresses a different use case. If both the protocol in this document and a

DHCP-based protocol are standardized, they could co-exist. However, there is no current mechanism for a stub resolver to tell a browser, or a web application, what DoH server the stub resolver is using, so DoH configuration in the stub resolver would not prevent the browser from trying to find a DoH server on its own.

An earlier design suggestion was to use an EDNS0 [RFC6891] extension. The design chosen (the new RRtype and resolver-associated-doh.arpa/IN/TXT query) meets the use case better because if the stub resolver does not understand EDNS0, or there is a middlebox that mishandles EDNS extensions between the computer and the resolver, the information about associated DoH servers will not make it back to the browser or web application.

For this protocol to be useful in a browser, the browser needs to have an entry in its configuration interface where the allowed DoH servers are listed that indicates that a DoH server from the configured Do53 or DoT resolver is allowed. That wording might say something like "DoH server associated with my current resolver".

5. IANA Considerations

IANA will record the domain name "resolver-associated-doh.arpa." in the "Special-Use Domain Names" registry [SUDN].

IANA, with the approval of the IAB, will delegate "resolver-associated-doh.arpa." in the ".arpa." zone.

The delegation for "resolver-associated-doh.arpa." MUST NOT include a DS record.

The delegation for "resolver-associated-doh.arpa." MUST point to one or more black hole servers, for example, "blackhole-1.iana.org." and "blackhole-2.iana.org.".

The delegation for "resolver-associated-doh.arpa." MUST NOT ever have a resource record with the RRtype "TXT".

6. Privacy Considerations

Allowing a user to use DoH instead of Do53 increases communication privacy because of the TLS protection.

When a Do53 or DoT server indicates that a particular DoH server is associated with it, the client might assume that the DoH server has the same information privacy policies as the Do53 or DoT server. Therefore, a Do53 or DoT server SHOULD NOT recommend a DoH server

unless that DoH server has the same (or better) information privacy policy as the Do53 or DoT server.

7. Security Considerations

If a client sends the resolver-associated-doh.arpa/IN/TXT query over a transport that does not assure data integrity (such as Do53), an attacker between the client and the resolver can change the response.

- A client that sends a query over such a transport and begins to use a DoH server based on the response MUST NOT assign a level of trust to that DoH server greater than to the trust it gave to the resolver itself.

- A client that sends a query over such a transport and receives a response that has an NXDOMAIN response code cannot be sure that the response comes from a resolver that does not know this protocol. Instead, the client SHOULD assume that there could be an on-path attack where the attacker does not want the client to use DoH.

8. References

8.1. Normative References

[I-D.ietf-doh-dns-over-https]
Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", draft-ietf-doh-dns-over-https-14 (work in progress), August 2018.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC6570] Gregorio, J., Fielding, R., Hadley, M., Nottingham, M., and D. Orchard, "URI Template", RFC 6570, DOI 10.17487/RFC6570, March 2012, <https://www.rfc-editor.org/info/rfc6570>.

[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>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[SUDN] "Special-Use Domain Names", n.d., <https://www.iana.org/assignments/special-use-domain-names/>.

8.2. Informative References

[RFC2308] Andrews, M., "Negative Caching of DNS Queries (DNS NCACHE)", RFC 2308, DOI 10.17487/RFC2308, March 1998, <https://www.rfc-editor.org/info/rfc2308>.

[RFC6891] Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", STD 75, RFC 6891, DOI 10.17487/RFC6891, April 2013, <https://www.rfc-editor.org/info/rfc6891>.

Acknowledgments

The use case in this document was inspired by discussions and the DRIU BoF at IETF 102 and later in the DNSOP Working Group. Vladimir Cunat, Philip Homburg, and Shumon Huque offered useful advice to greatly improve the protocol.

Author's Address

Paul Hoffman
ICANN

Email: paul.hoffman@icann.org