Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 23, 2019

P. Sood
Google
R. Arends
P. Hoffman
ICANN

May 22, 2019

DNS Resolver Information: "doh"
draft-sah-resinfo-doh-00

Abstract

This document defines a name-value pair, "doh", for the "DNS Resolver Information Self-publication" protocol described in draft-sah-resolver-information. This name-value pair describes whether the resolver acts as a DoH server and, if so, the URI template for it.

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 November 23, 2019.

Copyright Notice

Table of Contents

1. Introduction

[I-D.sah-resolver-information] defines a format for information about a DNS resolver and protocols to get that information. Stub resolvers and applications that can act as DoH clients [RFC8484] may want to know the URI templates used by a resolver that is acting as a DoH server.

1.1. Definitions

In this document, the term "resolver" without qualification means "recursive resolver" as defined in [RFC8499]. Also, the term "stub" is used to mean "stub resolver".

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.

2. Definition of the "doh" Name-value Pair

The "doh" name has a value of a JSON object. That object has the following name-value pairs. The "templates" name MUST be present; the "domain-to-match" name is OPTIONAL.

templates: array of strings. Each string is a URI template for the DoH server. The array MAY have zero values; if so, this indicates that the resolver does not support DoH. The values MUST NOT be empty.

domain-to-match: array of strings. Each string is a fully-qualified domain name that is expected to appear in the certificate used for TLS. These names can be used for matching in the TLS handshake if the DoH client accesses the DoH server with a template that has an IP address. The array MAY have zero values; if so, this indicates that the certificate should only be matched using IP addresses as subject names. The values MUST NOT be empty.

For example, a pair might look like:

```
{ "doh":
  { "domain-to-match": [ "resolver.example.net" ],
    "templates: [ "https://resolver.example.net/dns-query{?dns}",
    "https://192.0.1.2/dns-query{?dns}" ]
  }
}
```

As another example, where the TLS certificate is expected to have identifiers of IP addresses, not domain names:

```
{ "doh":
  { "templates: [ "https://192.0.1.2/dns-query{?dns}" ],
    "domain-to-match": [ ]
  }
}
```

3. Use of Data from the "doh" Name-value Pair

If the "template" array has more than one string, a client can consider them all to be of equal value when finding a DoH server associated with the resolver.

4. IANA Considerations

4.1. Entry for the "Registry for DNS Resolver Information"

This document adds one new entry to the "Registry for DNS Resolver Information".

Name: doh

Value type: object

Specification: This document

5. Security Considerations

The data in the "doh" object MUST be received from an authoritative source, and MUST be authenticated. Currently, that means either using DNSSEC validation if using DNS to get the data, or TLS certificate validation if using DNS-over-TLS [RFC7858] or DNS-over-HTTPS from the resolver itself.

6. References

6.1. Normative References

[I-D.sah-resolver-information]
Sood, P., Arends, R., and P. Hoffman, "DNS Resolver Information Self-publication", draft-sah-resolver-information-00 (work in progress), April 2019.

[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>.

[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>.

[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>.

6.2. Informative References

[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>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

Authors' Addresses

Puneet Sood
Google

Email: puneets@google.com

Roy Arends
ICANN

Email: roy.arends@icann.org

Paul Hoffman
ICANN

Email: paul.hoffman@icann.org