Network Working Group
Internet-Draft
Intended status: Experimental
Expires: 18 December 2021

P. Hoffman
ICANN
P. van Dijk
PowerDNS

16 June 2021

Recursive to Authoritative DNS with Unauthenticated Encryption
draft-ietf-dprive-unauth-to-authoritative-02

Abstract

This document describes a use case and a method for a DNS recursive resolver to use unauthenticated encryption when communicating with authoritative servers. The motivating use case for this method is that more encryption on the Internet is better, and some resolver operators believe that unauthenticated encryption is better than no encryption at all. The method described here is optional for both the recursive resolver and the authoritative server. This method supports unauthenticated encryption using the same mechanism for discovery of encryption support for the server as [FULL-AUTH].

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 18 December 2021.

Table of Contents

1. Introduction

A recursive resolver using traditional DNS over port 53 may wish instead to use encrypted communication with authoritative servers in order to limit snooping of its DNS traffic by passive or on-path attackers. The recursive resolver can use unauthenticated encryption (defined in [OPPORTUN]) to achieve this goal.

This document describes the use case for unauthenticated encryption in recursive resolvers in Section 1.1. The encryption method with authoritative servers can be DNS-over-TLS [DNSOTLS] (DoT), DNS-over-HTTPS [DNSOHTTPS] (DoH), and/or DNS-over-QUIC [DNSOQUIC] (DoQ), as described in Section 3.

The document also describes a discovery method that shows if an authoritative server supports encryption in Section 2.

See [FULL-AUTH] for a description of the use case and a proposed mechanism for fully-authenticated encryption. See [COMMON] for a definition of the features that are in common between this document and [FULL-AUTH].

NOTE: The draft uses the SVCB record as a discovery mechanism for encryption by a particular authoritative server. Any record type that can show multiple types of encryption (currently DoT, DoH, and DoQ) can be used for discovery. Thus, this record type might change in the future, depending on the discussion in the DPRIVE WG.

1.1. Use Case for Unauthenticated Encryption

The use case in this document for unauthenticated encryption is recursive resolver operators who are happy to use encryption with authoritative servers if doing so doesn't significantly slow down getting answers, and authoritative server operators that are happy to use encryption with recursive resolvers if it doesn't cost much. In this use case, resolvers do not want to return an error for requests that were sent over an encrypted channel if they would have been able to give a correct answer using unencrypted transport.

Resolvers and authoritative servers understand that using encryption costs something, but are willing to absorb the costs for the benefit of more Internet traffic being encrypted. The extra costs (compared to using traditional DNS on port 53) include:

* Extra round trips to establish TCP for every session (but not necessarily for every query)

* Extra round trips for TLS establishment

* Greater CPU use for TLS establishment

* Greater CPU use for encryption after TLS establishment

* Greater memory use for holding TLS state

This use case is not expected to apply to all resolvers or authoritative servers. For example, according to [RSO_STATEMENT], some root server operators do not want to be the early adopters for DNS with encryption. The protocol in this document explicitly allows authoritative servers to signal when they are ready to begin offering DNS with encryption.

1.2. Summary of Protocol

This summary gives an overview of how the parts of the protocol work together.

* The resolver discovers whether any authoritative server of interest supports DNS with encryption by querying for the SVCB records [SVCB]. As described in [DNS-SVCB], SVCB records can indicate that a server supports encrypted transport of DNS queries.

  NOTE: In this document, the term "SVCB record" is used _only_ for SVCB records that indicate encryption as described in [DNS-SVCB]. SVCB records that do not have these indicators in the RDATA are not included in the term "SVCB record" in this document.

* The resolver uses any authoritative server with a SVCB record that indicates encryption to perform unauthenticated encryption.

* The resolver does not fail to set up encryption if the authentication in the TLS session fails.

1.3. Definitions

The terms "recursive resolver", "authoritative server", and "classic DNS" are defined in [DNS-TERM].

"DNS with encryption" means transport of DNS over any of DoT, DoH, or DoQ. A server that supports DNS with encryption supports transport over one or more of DoT, DoH, or DoQ.

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 [MUSTSHOULD1] [MUSTSHOULD2] when, and only when, they appear in all capitals, as shown here.

2. Discovering Whether an Authoritative Server Uses Encryption

A recursive resolver discovers whether an authoritative server supports DNS with encryption by using the discovery mechanism described in Section 2.1 of [COMMON]. A resolver MAY also use port probing, although the mechanism for that is not described here.

If the cache has no positive or negative answers for any SVCB record for any of a zone's authoritative servers, the resolver MAY send queries for the SVCB records (and for the A/AAAA records of names mentioned in those SVCB records) for some or all of the zone's authoritative servers and wait for a positive response so that the resolver can use DNS with encryption for the original query. In this situation, the resolver MAY instead just use classic DNS for the original query but simultaneously queue queries for the SVCB (and subsequent A/AAAA) records for some or all of the zone's authoritative servers so that future queries might be able to use DNS with encryption.

DNSSEC validation of SVCB RRsets used strictly for this discovery mechanism is not mandated.

3. Resolving with Encryption

A resolver following this protocol processes the discovery response using the processing mechanism described in [COMMON].

A resolver following this protocol does not need to authenticate TLS servers. Thus, when setting up a TLS connection, if the server's authentication credentials do not match those expected by the resolver, the resolver continues with the TLS connection. Privacy-oriented resolvers (defined in [PRIVACY-REC]) following this protocol MUST NOT indicate that they are using encryption because this protocol is susceptible to on-path attacks.

3.1. Resolver Session Failures

The following are some of the reasons that a DNS with encryption session might fail to be set up:

* The resolver receives a TCP RST response

* The resolver does not receive replies to TCP or TLS setup (such as getting the TCP SYN message, the first TLS message, or completing TLS handshakes)

* The TLS handshake gets a definitive failure

* The encrypted session fails for reasons other than for authentication, such as incorrect algorithm choices or TLS record failures

4. Serving with Encryption

An authoritative server following this protocol publishes the discovery records using the serving mechanism described in [COMMON].

5. IANA Considerations

Relevant IANA considerations are covered in [COMMON].

6. Security Considerations

The method described in this document explicitly allows a resolver to perform DNS communications over traditional unencrypted, unauthenticated DNS on port 53, if it cannot find an authoritative server that advertises that it supports encryption. The method described in this document explicitly allows a resolver using encryption to choose to allow unauthenticated encryption. In either of these cases, the resulting communication will be susceptible to obvious and well-understood attacks from an attacker in the path of the communications.

7. Acknowledgements

Puneet Sood contributed many ideas to early drafts of this document.

The DPRIVE Working Group has contributed many ideas that keep shifting the focus and content of this document.

8. References

8.1. Normative References

[COMMON] Dijk, P. V. and P. Hoffman, "Common Features for Encrypted Recursive to Authoritative DNS", Work in Progress, Internet-Draft, draft-pp-dprive-common-features-01, 19 May 2021, <https://www.ietf.org/archive/id/draft-pp-dprive-common-features-01.txt>.

[DNS-SVCB] Schwartz, B., "Service Binding Mapping for DNS Servers", Work in Progress, Internet-Draft, draft-schwartz-svcb-dns-03, 19 April 2021, <https://www.ietf.org/archive/id/draft-schwartz-svcb-dns-03.txt>.

[DNS-TERM] Hoffman, P. and K. Fujiwara, "DNS Terminology", Work in Progress, Internet-Draft, draft-ietf-dnsop-rfc8499bis-01, 20 November 2020, <https://www.ietf.org/archive/id/draft-ietf-dnsop-rfc8499bis-01.txt>.

[FULL-AUTH]
Pauly, T., Rescorla, E., Schinazi, D., and C. A. Wood, "Signaling Authoritative DNS Encryption", Work in Progress, Internet-Draft, draft-rescorla-dprive-adox-latest-00, 26 February 2021, <https://www.ietf.org/archive/id/draft-rescorla-dprive-adox-latest-00.txt>.

[MUSTSHOULD1]
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>.

[MUSTSHOULD2]
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>.

[OPPORTUN] Dukhovni, V., "Opportunistic Security: Some Protection Most of the Time", RFC 7435, DOI 10.17487/RFC7435, December 2014, <https://www.rfc-editor.org/info/rfc7435>.

[SVCB] Schwartz, B., Bishop, M., and E. Nygren, "Service binding and parameter specification via the DNS (DNS SVCB and HTTPS RRs)", Work in Progress, Internet-Draft, draft-ietf-dnsop-svcb-https-06, 16 June 2021, <https://www.ietf.org/archive/id/draft-ietf-dnsop-svcb-https-06.txt>.

8.2. Informative References

[DNSOHTTPS]
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>.

[DNSOQUIC] Huitema, C., Mankin, A., and S. Dickinson, "Specification of DNS over Dedicated QUIC Connections", Work in Progress, Internet-Draft, draft-ietf-dprive-dnsoquic-02, 22 February 2021, <https://www.ietf.org/archive/id/draft-ietf-dprive-dnsoquic-02.txt>.

[DNSOTLS] 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>.

[PRIVACY-REC]
Dickinson, S., Overeinder, B., van Rijswijk-Deij, R., and A. Mankin, "Recommendations for DNS Privacy Service Operators", BCP 232, RFC 8932, DOI 10.17487/RFC8932, October 2020, <https://www.rfc-editor.org/info/rfc8932>.

[RSO_STATEMENT]
"Statement on DNS Encryption", 2021, <https://root-servers.org/media/news/Statement_on_DNS_Encryption.pdf>.

Authors' Addresses

Paul Hoffman
ICANN

Email: paul.hoffman@icann.org

Peter van Dijk
PowerDNS

Email: peter.van.dijk@powerdns.com