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

P. van Dijk
PowerDNS
P. Hoffman
ICANN

16 June 2021

Common Features for Encrypted Recursive to Authoritative DNS
draft-pp-dprive-common-features-02

Abstract

Encryption between recursive and authoritative DNS servers is currently being defined in two modes: unauthenticated and fully-authenticated. These two modes have some features in common, and this document defines those common features so that the documents defining the modes do not need to point to each other.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The DPRIVE Working Group in the IETF is working on standardizing methods for encrypted communication between DNS recursive resolvers and authoritative servers. At the time of this writing, [UNAUTH] is a work item in the working group, and [FULL-AUTH] has been widely discussed. The working group expressed a desire that the modes share as much design as possible to simplify the working group's process of evaluating the security and operational aspects of the methods. If the DPRIVE Working Group later adopts other modes, those modes should be considered in this document.

This document lists the major technical features that are shared by [UNAUTH] and [FULL-AUTH]. Differences from the common features in this document are listed in the respective method documents. The following are the features in common between and [UNAUTH] and [FULL-AUTH]:

- Discovery of an authoritative server's encryption support (Section 2)

- Order of processing discovered authoritative servers (Section 3)

- Serving with Encryption (Section 4)

Other topics might be added as the working group discusses [UNAUTH] and [FULL-AUTH] (and maybe other methods).

2. Discovery of Authoritative Server Encryption

This section describes methods for resolvers to discover whether an authoritative server supports encryption. At the current time, there is only one method listed.

2.1. DNS SVCB Records

An authoritative server that supports DNS with encryption makes itself discoverable by publishing one or more DNS SVCB records that contain "alpn" parameter keys. SVCB records are defined in [SVCB], and the DNS extension to those records is defined in [DNS-SVCB].

A recursive resolver discovers whether an authoritative server supports DNS with encryption by looking for cached SVCB records for the name of the authoritative server with a positive answer. A cached DNS SVCB record with a negative answer indicates that the authoritative server does not support any encrypted transport.

3. Processing Discovery Responses

After a resolver has DNS SCVB records in its cache (possibly due to having just queried for them), it needs to use those records to try to find an authoritative server that uses DNS with encryption. This section describes how the resolver can make that selection.

A resolver MUST NOT attempt encryption for a server that has a negative response in its cache for the associated DNS SVCB record.

After sending out all requests for SVCB records for the authoritative servers in the NS RRset for a name, if all of the SVCB records for those authoritative servers in the cache are negative responses, the resolver MUST use classic (unencrypted) DNS instead of encryption. Similarly, if none of the DNS SVCB records for the authoritative servers in the cache have supported "alpn" parameters, the resolver MUST use classic (unencrypted) DNS instead of encryption.

If there are any DNS SVCB records in the cache for the authoritative servers for a zone with supported "alpn" parameters, the resolver MUST try each indicated authoritative server using DNS with encryption until it successfully sets up a connection. The resolver only attempts to use the encrypted transports that are in the associated SVCB record for the authoritative server. ((Note that this completely prohibits "simple port 853 probing" even though that is what some operators are currently doing. Does the WG want to be this strict?))

A resolver SHOULD keep a DNS with encryption session to a particular server open if it expects to send additional queries to that server in a short period of time. [DNS-OVER-TCP] says "both clients and servers SHOULD support connection reuse" for TCP connections, and that advice could apply as well for DNS with encryption, especially as DNS with encryption has far greater overhead for re-establishing a connection. If the server closes the DNS with encryption session, the resolver can possibly re-establish a DNS with encryption session using encrypted session resumption.

For any DNS with encryption protocols, TLS version 1.3 [TLS-13] or later MUST be used.

3.1. Resolver Process as Pseudocode

This section is meant as an informal clarification of the protocol, and is not normative. The pseudocode here is designed to show the intent of the protocol, so it is not optimized for things like intersection of sets and other shortcuts.

In this code, "signal_rrset(this_name)" means an "SVCB" query for the "'_dns'" prefix of "this_name". The "Query over secure transport until successful" section ignores differences in name server selection and retry behaviour in different resolvers. The pseudocode was written to roughly cover the shared behaviour between [UNAUTH] and [FULL-AUTH]. Specifically, whether an implementation waits for the resolution of "queue a query" would differ between the two.

```
# Inputs
ns_names = List of NS Rdatas from the NS RRset for the queried name
can_do_secure = List of secure transports supported by resolver
secure_names_and_transports = Empty list, filled in below

# Fill secure_names_and_transports with (name, transport) tuples
for this_name in ns_names:
  if signal_rrset(this_name) is in the resolver cache:
    if signal_rrset(this_name) positively does not exist:
      continue
    for this_transport in signal_rrset(this_name):
      if this_transport in can_do_secure:
        add (this_name, this_transport) to secure_names_and_transports
  else: # signal_rrset(this_name) is not in the resolver cache
    queue a query for signal_rrset(this_name) for later caching

# Query over secure transport until successful
for (this_name, this_transport) tuple in secure_names_and_transports:
  query using this_transport on this_name
  if successful:
    finished

# Got here if no this_name/this_transport query was successful
#   or if secure_names_and_transports was empty
query using classic DNS on any/all ns_names; finished
```

4. Serving with Encryption

An operator of an authoritative server following this protocol SHOULD publish SVCB records as described in Section 2. If they cannot publish such records, the security properties of their authoritative servers will not be found. If an operator wants to test serving using encryption, they can publish SVCB records with short TTLs and then stop serving with encryption after removing the SVCB records and waiting for the TTLs to expire.

It is acceptable for an operator of authoritative servers to only offer encryption on some of the named authoritative servers, such as when the operator is determining how far to roll out encrypted service.

A server MAY close an encrypted connection at any time. For example, it can close the session if it has not received a DNS query in a defined length of time. The server MAY close an encrypted session after it sends a DNS response; however, it might also want to keep the session open waiting for another DNS query from the resolver. [DNS-OVER-TCP] says "both clients and servers SHOULD support connection reuse" for TCP connections, and that advice could apply as

well for DNS with encryption, especially as DNS with encryption has far greater overhead for re-establishing a connection. If the server closes the DNS with encryption session, the resolver can possibly re-establish a DNS with encryption session using encrypted session resumption.

For any DNS with encryption protocols, TLS version 1.3 [TLS-13] or later MUST be used.

5. Resolvers Reporting Errors to Authoritative Servers

Resolvers should have a method of telling authoritative servers that there are problems with the encrypted service they are offering. There is a proposal that the DNSOP Working Group might adopt [ERROR-REPORTING], which would enable such reporting.

((Clearly, more will need to go here.))

6. IANA Considerations

((Update registration for TCP/853 to also include ADoT))

((Maybe other updates for DoH and DoQ))

7. Security Considerations

An authoritative server that wants to only serve data to resolvers that use fully-authenticated encryption as described in [FULL-AUTH] cannot differentiate between those resolvers and resolvers using the mechanisms described in this document.

((Talk about requiring TLS 1.3))

8. Acknowledgements

The use of SVCB records for discovering whether an authoritative server supports encryption was first described by the authors of [FULL-AUTH].

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

9. References

9.1. Normative References

[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>.

[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>.

[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>.

[TLS-13] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[UNAUTH] Hoffman, P. and P. V. Dijk, "Recursive to Authoritative DNS with Unauthenticated Encryption", Work in Progress, Internet-Draft, draft-ietf-dprive-unauth-to-authoritative-01, 19 May 2021, <https://www.ietf.org/archive/id/draft-ietf-dprive-unauth-to-authoritative-01.txt>.

9.2. Informative References

[DNS-OVER-TCP] Dickinson, J., Dickinson, S., Bellis, R., Mankin, A., and D. Wessels, "DNS Transport over TCP - Implementation Requirements", RFC 7766, DOI 10.17487/RFC7766, March 2016, <https://www.rfc-editor.org/info/rfc7766>.

[ERROR-REPORTING] Arends, R. and M. Larson, "DNS Error Reporting", Work in Progress, Internet-Draft, draft-arends-dns-error-reporting-00, 30 October 2020, <https://www.ietf.org/archive/id/draft-arends-dns-error-reporting-00.txt>.

Authors' Addresses

Peter van Dijk
PowerDNS

Email: peter.van.dijk@powerdns.com

Paul Hoffman
ICANN

Email: paul.hoffman@icann.org