Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 6 May 2021

T. Pauly
E. Kinnear
Apple Inc.
C.A. Wood
Cloudflare
P. McManus
Fastly
T. Jensen
Microsoft

2 November 2020

Discovery of Equivalent Encrypted Resolvers
draft-pauly-add-deer-00

Abstract

This document defines Discovery of Equivalent Encrypted Resolvers (DEER), a mechanism for DNS clients to use DNS records to discover a resolver's encrypted DNS configuration. This mechanism can be used to move from unencrypted DNS to encrypted DNS when only the IP address of an encrypted resolver is known. It can also be used to discover support for encrypted DNS protocols when the name of an encrypted resolver is known. This mechanism is designed to be limited to cases where equivalent encrypted and unencrypted resolvers are operated by the same entity.

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 6 May 2021.

Copyright Notice

Table of Contents

1. Introduction

When DNS clients wish to use encrypted DNS protocols such as DNS-over-TLS (DoT) [RFC7858] or DNS-over-HTTPS (DoH) [RFC8484], they require additional information beyond the IP address of the DNS server, such as the resolver's hostname, non-standard ports, or URL paths. However, common configuration mechanisms only provide the resolver's IP address during configuration. Such mechanisms include network provisioning protocols like DHCP [RFC2132] and IPv6 Router Advertisement (RA) options [RFC8106], as well as manual configuration.

This document defines two mechanisms for clients to discover equivalent resolvers using DNS server Service Binding (SVCB, [I-D.ietf-dnsop-svcb-https]) records:

1. When only an IP address of an Unencrypted Resolver is known, the client queries a special use domain name to discover DNS SVCB records associated with the Unencrypted Resolver (Section 4).

2. When the hostname of an encrypted DNS server is known, the client requests details by sending a query for a DNS SVCB record. This can be used to discover alternate encrypted DNS protocols supported by a known server, or to provide details if a resolver name is provisioned by a network (Section 5).

Both of these approaches allow clients to confirm that a discovered Encrypted Resolver is equivalent to the originally provisioned resolver. "Equivalence" in this context means that the resolvers are operated by the same entity; for example, the resolvers are accessible on the same IP address, or there is a certificate that claims ownership over both resolvers.

1.1. Specification of Requirements

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. Terminology

This document defines the following terms:

DEER: Discovery of Equivalent Encrypted Resolvers. Refers to the mechanisms defined in this document.

Encrypted Resolver: A DNS resolver using any encrypted DNS transport. This includes current mechanisms such as DoH and DoT as well as future mechanisms.

Equivalent Encrypted Resolver: An Encrypted Resolver which is considered to provide answers equivalent to a given resolver. This equivalency can be authenticated with TLS certificates.

Unencrypted Resolver: A DNS resolver using TCP or UDP port 53.

3. DNS Service Binding Records

DNS resolvers can advertise one or more Equivalent Encrypted Resolvers that offer equivalent services over encrypted channels and are controlled by the same entity.

When a client discovers Equivalent Encrypted Resolvers, it learns information such as the supported protocols, ports, and server name to use in certificate validation. This information is provided in Service Binding (SVCB) records for DNS Servers, defined by [I-D.schwartz-svcb-dns].

The following is an example of an SVCB record describing a DoH server:

```
_dns.example.net  7200  IN SVCB 1 . (
     alpn=h2 dohpath=/dns-query{?dns} ipv4hint=x.y.z.w )
```

The following is an example of an SVCB record describing a DoT server:

```
_dns.example.net  7200  IN SVCB 1 dot.example.net (
     alpn=dot port=8530 ipv4hint=x.y.z.w )
```

If multiple Equivalent Encrypted Resolvers are available, using one or more encrypted DNS protocols, the resolver deployment can indicate a preference using the priority fields in each SVCB record [I-D.ietf-dnsop-svcb-https].

This document focuses on discovering DoH and DoT Equivalent Encrypted Resolvers. Other protocols can also use the format defined by [I-D.schwartz-svcb-dns]. However, if any protocol does not involve some form of certificate validation, new validation mechanisms will need to be defined to support validating equivalence as defined in Section 4.1.

4. Discovery Using Resolver IP Addresses

When a DNS client is configured with an Unencrypted Resolver IP address, it SHOULD query the resolver for SVCB records for "dns://resolver.arpa" before making other queries. Specifically, the client issues a query for "_dns.resolver.arpa" with the SVCB resource record type (64) [I-D.ietf-dnsop-svcb-https].

If the recursive resolver that receives this query has one or more Equivalent Encrypted Resolvers, it will return the corresponding SVCB records. When responding to these special queries for "dns://resolver.arpa", the SVCB records SHOULD contain at least one "ipv4hint" and/or "ipv6hint" keys. These address hints indicate the address on which the corresponding Encrypted Resolver can be reached and avoid additional DNS lookup for the A and AAAA records of the Encrypted Resolver name.

4.1. Authenticated Discovery

In order to be considered an authenticated Equivalent Encrypted Resolver, the TLS certificate presented by the Encrypted Resolver MUST contain both the domain name (from the SVCB answer) and the IP address of its equivalent Unencrypted Resolver within the SubjectAlternativeName certificate field. The client MUST check the SubjectAlternativeName field for both the Unencrypted Resolver's IP address and the advertised name of the Equivalent Encrypted Resolver. If the certificate can be validated, the client SHOULD use the discovered Equivalent Encrypted Resolver for any cases in which it would have otherwise used the Unencrypted Resolver. If the Equivalent Encrypted Resolver has a different IP address than the Unencrypted Resolver and the TLS certificate does not cover the Unencrypted Resolver address, the client MUST NOT use the discovered Encrypted Resolver. Additionally, the client SHOULD suppress any further queries for Equivalent Encrypted Resolvers using this Unencrypted Resolver for the length of time indicated by the SVCB record's Time to Live (TTL).

If the Equivalent Encrypted Resolver and the Unencrypted Resolver share an IP address, clients MAY choose to opportunistically use the Encrypted Resolver even without this certificate check (Section 4.2).

4.2. Opportunistic Discovery

There are situations where authenticated discovery of encrypted DNS configuration over unencrypted DNS is not possible. This includes Unencrypted Resolvers on non-public IP addresses whose identity cannot be confirmed using TLS certificates.

Opportunistic Privacy is defined for DoT in Section 4.1 of [RFC7858] as a mode in which clients do not validate the name of the resolver presented in the certificate. A client MAY use information from the SVCB record for "dns://resolver.arpa" with this "opportunistic" approach (not validating the names presented in the SubjectAlternativeName field of the certificate) as long as the IP address of the Encrypted Resolver does not differ from the IP address of the Unencrypted Resolver, and that IP address is a private address (such as those defined in [RFC1918]). This approach can be used for DoT or DoH.

If the IP addresses of the Encrypted and Unencrypted Resolvers are not the same, or the shared IP address is not a private IP address, the client MUST NOT use the Encrypted Resolver opportunistically.

5. Discovery Using Resolver Names

A DNS client that already knows the name of an Encrypted Resolver can use DEER to discover details about all supported encrypted DNS protocols. This situation can arise if a client has been configured to use a given Encrypted Resolver, or if a network provisioning protocol (such as DHCP or IPv6 Router Advertisements) provides a name for an Encrypted Resolver alongside the resolver IP address.

For these cases, the client simply sends a DNS SVCB query using the known name of the resolver. This query can be issued to the named Encrypted Resolver itself or to any other resolver. Unlike the case of bootstrapping from an Unencrypted Resolver (Section 4), these records SHOULD be available in the public DNS.

For example, if the client already knows about a DoT server "resolver.example.com", it can issue an SVCB query for "_dns.resolver.example.com" to discover if there are other encrypted DNS protocols available. In the following example, the SVCB answers indicate that "resolver.example.com" supports both DoH and DoT, and that the DoH server indicates a higher priority than the DoT server.

```
_dns.resolver.example.com  7200  IN SVCB 1 . (
     alpn=h2 dohpath=/dns-query{?dns} )
_dns.resolver.example.com  7200  IN SVCB 2 . (
     alpn=dot )
```

Often, the various supported encrypted DNS protocols will be accessible using the same hostname. In the example above, both DoH and DoT use the name "resolver.example.com" for their TLS certficates. If a deployment uses a different hostname for one protocol, but still wants clients to treat the DNS servers as equivalent, the TLS certificates MUST include both names in the SubjectAlternativeName fields. Note that this name verification is not related to the DNS resolver that provided the SVCB answer.

For example, being able to discover an Equivalent Encrypted Resolver for a known Encrypted Resolver is useful when a client has a DoT configuration for "foo.resolver.example.com" but is on a network that blocks DoT traffic. The client can still send a query to any other accessible resolver (either the local network resolver or an accessible DoH server) to discover if there is an equivalent DoH server for "foo.resolver.example.com".

6. Deployment Considerations

Resolver deployments that support DEER are advised to consider the following points.

6.1. Caching Forwarders

If a caching forwarder consults multiple resolvers, it may be possible for it to cache records for the "resolver.arpa" Special Use Domain Name (SUDN) for multiple resolvers. This may result in clients sending queries intended to discover Equivalent Encrypted Resolvers for resolver "foo" and receiving answers for resolvers "foo" and "bar".

A client will successfully reject unintended connections because the authenticated discovery will fail or the resolver addresses do not match. Clients that attempt unauthenticated connections to resolvers discovered through SVCB queries run the risk of connecting to the wrong server in this scenario.

To prevent unnecessary traffic from clients to incorrect resolvers, DNS caching resolvers SHOULD NOT cache results for the "resolver.arpa" SUDN other than for Equivalent Encrypted Resolvers under their control.

6.2. Certificate Management

Resolver owners that support authenticated discovery will need to list valid referring IP addresses in their TLS certificates. This may pose challenges for resolvers with a large number of referring IP addresses.

7. Security Considerations

Since client can receive DNS SVCB answers over unencrypted DNS, on-path attackers can prevent successful discovery by dropping SVCB packets. Clients should be aware that it might not be possible to distinguish between resolvers that do not have any Equivalent Encrypted Resolver and such an active attack.

While the IP address of the Unencrypted Resolver is often provisioned over insecure mechanisms, it can also be provisioned securely, such as via manual configuration, a VPN, or on a network with protections like RA guard [RFC6105]. An attacker might try to direct Encrypted DNS traffic to itself by causing the client to think that a discovered Equivalent Encrypted Resolver uses a different IP address from the Unencrypted Resolver. Such an Encrypted Resolver might have a valid certificate, but be operated by an attacker that is trying to observe or modify user queries without the knowledge of the client or network.

If the IP address of an Equivalent Encrypted Resolver differs from that of an Unencrypted Resolver, clients MUST validate that the IP address of the Unencrypted Resolver is covered by the SubjectAlternativeName of the Encrypted Resolver's TLS certificate (Section 4.1).

Opportunistic use of Encrypted Resolvers MUST be limited to cases where the Unencrypted Resolver and Equivalent Encrypted Resolver have the same IP address (Section 4.2).

8. IANA Considerations

8.1. Special Use Domain Name "resolver.arpa"

This document calls for the creation of the "resolver.arpa" SUDN. This will allow resolvers to respond to queries directed at themselves rather than a specific domain name. While this document uses "resolver.arpa" to return SVCB records indicating equivalent encrypted capability, the name is generic enough to allow future reuse for other purposes where the resolver wishes to provide information about itself to the client.

9. References

9.1. Normative References

[I-D.ietf-dnsop-svcb-https]
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-01, 13 July 2020, <http://www.ietf.org/internet-drafts/draft-ietf-dnsop-svcb-https-01.txt>.

[I-D.ietf-tls-esni]
Rescorla, E., Oku, K., Sullivan, N., and C. Wood, "TLS Encrypted Client Hello", Work in Progress, Internet-Draft, draft-ietf-tls-esni-08, 16 October 2020, <http://www.ietf.org/internet-drafts/draft-ietf-tls-esni-08.txt>.

[I-D.schwartz-svcb-dns]
Schwartz, B., "Service Binding Mapping for DNS Servers", Work in Progress, Internet-Draft, draft-schwartz-svcb-dns-01, 10 August 2020, <http://www.ietf.org/internet-drafts/draft-schwartz-svcb-dns-01.txt>.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, DOI 10.17487/RFC1918, February 1996, <https://www.rfc-editor.org/info/rfc1918>.

[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>.

[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>.

9.2. Informative References

[I-D.schinazi-httpbis-doh-preference-hints] Schinazi, D., Sullivan, N., and J. Kipp, "DoH Preference Hints for HTTP", Work in Progress, Internet-Draft, draft-schinazi-httpbis-doh-preference-hints-02, 13 July 2020, <http://www.ietf.org/internet-drafts/draft-schinazi-httpbis-doh-preference-hints-02.txt>.

[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>.

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, DOI 10.17487/RFC2132, March 1997, <https://www.rfc-editor.org/info/rfc2132>.

[RFC5507] IAB, Faltstrom, P., Ed., Austein, R., Ed., and P. Koch, Ed., "Design Choices When Expanding the DNS", RFC 5507, DOI 10.17487/RFC5507, April 2009, <https://www.rfc-editor.org/info/rfc5507>.

[RFC6105] Levy-Abegnoli, E., Van de Velde, G., Popoviciu, C., and J. Mohacsi, "IPv6 Router Advertisement Guard", RFC 6105, DOI 10.17487/RFC6105, February 2011, <https://www.rfc-editor.org/info/rfc6105>.

[RFC8106] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", RFC 8106, DOI 10.17487/RFC8106, March 2017, <https://www.rfc-editor.org/info/rfc8106>.

[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>.

Appendix A. Rationale for using SVCB records

This mechanism uses SVCB/HTTPS resource records [I-D.ietf-dnsop-svcb-https] to communicate that a given domain designates a particular Equivalent Encrypted Resolver for clients to use in place of an Unencrypted Resolver (using a SUDN) or another Encrypted Resolver (using its domain name).

There are various other proposals for how to provide similar functionality. There are several reasons that this mechanism has chosen SVCB records:

* Discovering encrypted resolver using DNS records keeps client logic for DNS self-contained and allows a DNS resolver operator to define which resolver names and IP addresses are related to one another.

* Using DNS records also does not rely on bootstrapping with higher-level application operations (such as [I-D.schinazi-httpbis-doh-preference-hints]).

* SVCB records are extensible and allow definition of parameter keys. This makes them a superior mechanism for extensibility as compared to approaches such as overloading TXT records. The same keys can be used for discovering Equivalent Encrypted Resolvers of different transport types as well as those advertised by Unencrypted Resolvers or another Encrypted Resolver.

* Clients and servers that are interested in privacy of names will already need to support SVCB records in order to use Encrypted TLS Client Hello [I-D.ietf-tls-esni]. Without encrypting names in TLS, the value of encrypting DNS is reduced, so pairing the solutions provides the largest benefit.

* Clients that support SVCB will generally send out three queries when accessing web content on a dual-stack network: A, AAAA, and HTTPS queries. Discovering an Equivalent Encrypted Resolver as part of one of these queries, without having to add yet another query, minimizes the total number of queries clients send. While [RFC5507] recommends adding new RRTypes for new functionality, SVCB provides an extension mechanism that simplifies client behavior.

Authors' Addresses

Tommy Pauly
Apple Inc.
One Apple Park Way
Cupertino, California 95014,
United States of America

Email: tpauly@apple.com

Eric Kinnear
Apple Inc.
One Apple Park Way
Cupertino, California 95014,
United States of America

Email: ekinnear@apple.com

Christopher A. Wood
Cloudflare
101 Townsend St
San Francisco,
United States of America

Email: caw@heapingbits.net

Patrick McManus
Fastly

Email: mcmanus@ducksong.com

Tommy Jensen
Microsoft

Email: tojens@microsoft.com