Workgroup: ADD
Internet-Draft: draft-ietf-add-requirements-00
Published: 7 March 2021
Intended Status: Informational
Expires: 8 September 2021
Authors: C. Box (BT), T. Pauly (Apple), C.A. Wood (Cloudflare), T. Reddy (McAfee), D. Migault (Ericsson)

Requirements for Discovering Designated Resolvers

Abstract

Adaptive DNS Discovery is chartered to define mechanisms that allow clients to discover and select encrypted DNS resolvers. This document describes one common use case, namely that of clients that connect to a network but where they cannot securely authenticate the identity of that network. In such cases the client would like to learn which encrypted DNS resolvers are designated by that network or by the Do53 resolver offered by that network. It lists requirements that any proposed discovery mechanisms should seek to address.

Discussion Venues

Source for this draft can be found at https://github.com/ietf-wg-add/draft-ietf-add-requirements/.

Discussion of this document and associated solutions takes place in the ADD Working Group mailing list (add@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/add/.

Status of This Memo

Table of Contents

1. Introduction

Several protocols for protecting DNS traffic with encrypted transports have been defined, such as DNS-over-TLS (DoT) [RFC7858] and DNS-over-HTTPS (DoH) [RFC8484]. Encrypted DNS can provide many security and privacy benefits for network clients.

While it is possible for clients to statically configure encrypted DNS resolvers to use, dynamic discovery and provisioning of

encrypted resolvers can expand the usefulness and applicability of encrypted DNS to many more use cases.

The Adaptive DNS Discovery (ADD) Working Group is chartered to define mechanisms that allow clients to automatically discover and select encrypted DNS resolvers in a wide variety of network environments. This document describes one common use case, namely that of clients that connect to a network but where they cannot securely authenticate that network. Whether the network required credentials before the client was permitted to join is irrelevant; the client still cannot be sure that it has connected to the network it was expecting.

In such cases the client would like to learn which encrypted DNS resolvers are designated by that network, or by the Do53 resolver offered by that network. It lists requirements that any proposed discovery mechanisms should seek to address. They can do this either by providing a solution, or by explicitly stating why it is not in scope.

1.1. Requirements language

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 makes use of the following terms.

Encrypted DNS: DNS-over-HTTPS [RFC8484], DNS-over-TLS [RFC7858], or any other encrypted DNS technology that the IETF may publish, such as DNS-over-QUIC [I-D.ietf-dprive-dnsoquic].

Do53: Unencrypted DNS over UDP port 53, or TCP port 53 [RFC1035].

Designated: See Section 3.1.

Designator: The network or resolver that issued the designation.

3. Use case description

It is often the case that a client possesses no specific configuration for how to operate DNS, and at some point joins a network that it cannot authenticate. It may have no prior knowledge of the network, or it may have connected previously to a network that looked the same. In either case the usual behaviour, because of lack of specific configuration, is to dynamically discover the

network's designated Do53 resolver and use it. This long-standing practice works in nearly all networks, but presents a number of privacy and security risks that were the motivation for the development of encrypted DNS.

The network's designated Do53 resolver may have a number of properties that differ from a generic resolver. It may be able to answer names that are not known globally, it may exclude some names (for positive or negative reasons), and it may provide address answers that have improved proximity. In this use case it is assumed that the user who chose to join this network would also like to make use of these properties of the network's unencrypted resolver, at least some of the time. However they would like to use an encrypted DNS protocol rather than Do53.

Using an encrypted and authenticated resolver can provide several benefits that are not possible if only unencrypted DNS is used:

*Prevent other devices on the network from observing client DNS messages

*Authenticate that the DNS resolver is the correct one

*Verify that answers come from the selected DNS resolver

To meet this case there should be a means by which the client can learn how to contact a set of encrypted DNS resolvers that are designated by the network it has joined.

3.1. Designation

Designation is the process by which a local network or a resolver can point clients towards a particular set of resolvers. This is not a new concept, as networks have been able to dynamically designate Do53 resolvers for decades (see Section 3.4). However here we extend the concept in two ways:

*To allow resolvers to designate other resolvers

*The inclusion of support for encrypted DNS

The designated set could be empty, or it could list the contact details (such as DoH URI Template) of DNS resolvers that it recommends. It is not required that there be any relationship between the resolvers in the set, simply that all of them are options that the designator asserts are safe and appropriate for the client to use without user intervention.

There are two possible sources of designation.

- The local network can designate one or more encrypted DNS resolvers (B, C, etc) in addition to any Do53 resolver (A) it may offer. This is known as network-identified.

- During communication with the (often unencrypted) resolver (A), this resolver can designate one or more encrypted DNS resolvers (B, C, etc). This is known as resolver-identified.

Network-identified has the advantages that it derives from the same source of information as the network's Do53 announcement, and removes the need to talk to the Do53 resolver at all. However it cannot be the sole mechanism, at least for several years, since there is a large installed base of local network equipment that is difficult to upgrade with new features. Hence the second mechanism should support being able to designate resolvers using only existing widely-deployed DNS features.

3.2. Local addressing

Many networks offer a Do53 resolver on an address that is not globally meaningful, e.g. [RFC1918], link-local or unique local addresses. To support the discovery of encrypted DNS in these environments, a means is needed for the discovery process to work from a locally-addressed Do53 resolver to an encrypted DNS resolver that is accessible either at the same (local) address, or at a different global address. Both options need to be supported.

3.3. Use of designation information

After the client receives designation information, it must come to a decision on whether and when to use any of the designated resolvers.

In the case of resolver-identified designation, it would be advantageous for a solution to enable the client to validate the source of the assertion in some way. For example it may be possible to verify that the designation comes from an entity who already has full control of the client's Do53 queries. Network-identified designation should not require this, unless the network-identified resolver in turn initiated a new resolver-identified designation. It would be beneficial to extend such a verification process to defend against attackers that have only transient control of such queries.

Clients may also seek to validate the identity of the designated resolver, beyond what is required by the relevant protocol. Authors of solution specifications should be aware that clients may impose arbitrary additional requirements and heuristics as they see fit.

3.4. Network-identified designated resolvers

DNS servers are often provisioned by a network as part of DHCP options [RFC2132], IPv6 Router Advertisement (RA) options [RFC8106], Point-to-Point Protocol (PPP) [RFC1877], or 3GPP Protocol Configuration Options (TS24.008). Historically this is usually one or more Do53 resolver IP addresses, to be used for traditional unencrypted DNS.

A solution is required that enhances the set of information delivered to include details of one or more designated encrypted DNS resolvers, or states that there are none. Such resolvers could be on the local network, somewhere upstream, or on the public Internet.

3.5. Resolver-identified designated resolvers

To support cases where the network is unable to identify an encrypted resolver, it should be possible to learn the details of one or more designated encrypted DNS resolvers by communicating with the network's designated Do53 resolver. This should involve an exchange that uses standard DNS messages that can be handled, or forwarded, by existing deployed software.

Each resolver in the set may be at a different network location, which leads to several subcases for the mapping from Do53 to a particular designated resolver.

3.5.1. Local to local

If the local resolver has been upgraded to support encrypted DNS, the client may not initially be aware that its local resolver supports it. Discovering this may require communication with the local resolver, or an upstream resolver, over Do53. Clients that choose to use this local encrypted DNS gain the benefits of encryption while retaining the benefits of a local caching resolver with knowledge of the local topology.

Clients will be aware when the designated resolver has the same IP address as the Do53 (after looking up its name if required). They can use this information in their decision-making as to the level of trust to place in the designated resolver. In some networks it will not be possible to deploy encrypted DNS on the same IP address, e.g. because of the increased resource requirements of encrypted DNS. Discovery solutions should work in the presence of a change to a different local IP address.

An additional benefit of using a local resolver occurs with IoT devices. A common usage pattern for such devices is for it to "call home" to a service that resides on the public Internet, where that service is referenced through a domain name. As discussed in

Manufacturer Usage Description Specification [RFC8520], because these devices tend to require access to very few sites, all other access should be considered suspect. However, if the query is not accessible for inspection, it becomes quite difficult for the infrastructure to suspect anything.

3.5.2. Local to upstream

It is frequently the case that Do53 resolvers announced by home networks are difficult to upgrade to support encrypted operation. In such cases it is possible that the only option for encrypted operation is to refer to a separate globally-addressed encrypted DNS resolver, somewhere upstream. Other networks may choose deploy their encrypted DNS resolver away from the local network, for other reasons.

The use of an upstream resolver can mean the loss of local knowledge, such as the ability to respond to queries for locally-relevant names. Solutions should consider how to guide clients when to direct their queries to the local Do53. For example this could be through pre-emptive communication ("if you ever need to query *.example.com, use your local Do53"), or reactively ("I don't know the answer to that, but your local Do53 should know").

3.5.3. Public to public

In cases where the local network has designated a Do53 resolver on the public Internet, this resolver may designate its own or another public encrypted DNS service. Since public IP addresses may appear in TLS certificates, solutions may use this as one way to validate that the designated encrypted resolver is legitimately associated with the original Do53.

3.6. Identification over an encrypted channel

In cases where the designation is delivered over an authenticated and encrypted channel, such as when one encrypted DNS resolver designates another, one form of attack is removed. Specifically, clients may be more confident that the received designation was actually sent by the designator. Clients may take this into account when deciding whether to follow the designation.

4. Privacy and security requirements

Encrypted (and authenticated) DNS improves the privacy and security of DNS queries and answers in the presence of malicious attackers. Such attackers are assumed to interfere with or otherwise impede DNS traffic and corresponding discovery mechanisms. They may be on-path or off-path between the client and entities with which the client communicates [RFC3552]. These attackers can inject, tamper, or

otherwise interfere with traffic as needed. Given these capabilities, an attacker may have a variety of goals, including, though not limited to:

- Monitor and profile clients by observing unencrypted DNS traffic
- Modify unencrypted DNS traffic to filter or augment the user experience
- Block encrypted DNS

Given this type of attacker, resolver discovery mechanisms must be designed carefully to not worsen a client's security or privacy posture. In particular, attackers under consideration must not be able to:

- Redirect secure DNS traffic to themselves when they would not otherwise handle DNS traffic.
- Override or interfere with the resolver preferences of a user or administrator.
- Cause clients to use a discovered resolver which has no designation from a client-known entity.

When discovering DNS resolvers on a local network, clients have no mechanism to distinguish between cases where an active attacker with the above capabilities is interfering with discovery, and situations wherein the network has no encrypted resolver. Absent such a mechanism, an attacker can always succeed in these goals. Therefore, in such circumstances, viable solutions for local DNS resolver discovery should consider weaker attackers, such as those with only passive eavesdropping capabilities. It is unknown whether such relaxations represent a realistic attacker in practice. Thus, local discovery solutions designed around this threat model may have limited value.

5. Statement of Requirements

This section lists requirements that flow from the above sections.

Requirement	Description
R1.1	Discovery SHOULD provide a local network the ability to announce to clients a set of, or absence of, designated resolvers.
R1.2	Discovery SHOULD provide a resolver the ability to announce to clients a set of, or absence of, designated resolvers.
R1.3	Discovery SHOULD support all encrypted DNS protocols standardised by the IETF.

Requirement	Description
R2.1	Networks SHOULD be able to announce one or more designated encrypted DNS resolvers using existing mechanisms such as DHCPv4, DHCPv6, IPv6 Router Advertisement, and the Point-to-Point Protocol.
R2.2	The format for resolver designation SHOULD be specified such that provisioning mechanisms defined outside of the IETF can advertise encrypted DNS resolvers.
R2.3	This format SHOULD convey, at minimum, the information the client needs to make contact with each designated resolver.
R2.4	This format MAY convey additional resolver information.
R3.1	In resolver-identified designation (R1.2), the communication with the designator MAY be encrypted or not, depending on the capability of the resolver.
R3.2	In resolver-identified designation (R1.2), that resolver MAY be locally or globally reachable. Both options SHOULD be supported.
R4.1	If the local network resolver is a forwarder that does not offer encrypted DNS service, an upstream encrypted resolver SHOULD be retrievable via queries sent to that forwarder.
R4.2	Achieving requirement 4.1 SHOULD NOT require any changes to DNS forwarders hosted on non-upgradable legacy network devices.
R5.1	Discovery MUST NOT worsen a client's security or privacy posture.
R5.2	Threat modelling MUST assume that there is a passive eavesdropping attacker on the local network.
R5.3	Threat modelling MUST assume that an attacker can actively attack from outside the local network.
R5.4	Attackers MUST NOT be able to redirect encrypted DNS traffic to themselves when they would not otherwise handle DNS traffic.

Table 1

6. Security Considerations

See Section 4.

7. IANA Considerations

This document has no IANA actions.

8. References

8.1. Normative References

[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>.

8.2. Informative References

[I-D.ietf-dprive-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>.

[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>.

[RFC1877] Cobb, S., "PPP Internet Protocol Control Protocol Extensions for Name Server Addresses", RFC 1877, DOI 10.17487/RFC1877, December 1995, <https://www.rfc-editor.org/info/rfc1877>.

[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>.

[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>.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <https://www.rfc-editor.org/info/rfc3552>.

[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>.

[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>.

[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>.

[RFC8520] Lear, E., Droms, R., and D. Romascanu, "Manufacturer Usage Description Specification", RFC 8520, DOI 10.17487/RFC8520, March 2019, <https://www.rfc-editor.org/info/rfc8520>.

Acknowledgments

This document was started based on discussion during the ADD meeting of IETF108, subsequent meetings, on the list, and with text from draft-pauly-add-requirements. In particular this document was informed by contributions from Martin Thomson, Eric Rescorla, Tommy Jensen, Ben Schwartz, Paul Hoffman, Ralf Weber, Michael Richardson, Mohamed Boucadair, Sanjay Mishra, Jim Reid, Neil Cook, Nic Leymann, Andrew Campling, Eric Orth, Ted Hardie, Paul Vixie, Vittorio Bertola, and Vinny Parla.

Authors' Addresses

Chris Box
BT
2000 Park Avenue
Bristol
United Kingdom

Email: chris.box@bt.com

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

Email: tpauly@apple.com

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

Email: caw@heapingbits.net

Tirumaleswar Reddy
McAfee
Embassy Golf Link Business Park

Bangalore
India

Email: TirumaleswarReddy_Konda@McAfee.com

Daniel Migault
Ericsson
8275 Trans Canada Route
Saint Laurent, QC
Canada

Email: daniel.migault@ericsson.com