ADD
Internet-Draft
Intended status: Informational
Expires: 6 May 2021

C. Box
BT
T. Pauly
Apple
C.A. Wood
Cloudflare
T. Reddy
McAfee
D. Migault
Ericsson

2 November 2020

Requirements for Adaptive DNS Discovery
draft-box-add-requirements-01

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, that of discovering the encrypted DNS resolver that corresponds to the Do53 resolver offered by a network. It lists requirements that any proposed discovery mechanisms should address.

Discussion Venues

This note is to be removed before publishing as an RFC.

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

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 currently focusses on one common use case, that of discovering the encrypted DNS resolver that corresponds to the Do53 resolver offered by a network. Additional use cases can be added in future versions. As well as describing the use case, it lists requirements that any proposed discovery mechanisms should 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].

Equivalent: See Section 3.1.

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 has no previous knowledge about. In such a case the usual existing behaviour is to dynamically discover the network's recommended 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 recommended unencrypted 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 that is equivalent to the one provisioned by the network 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 an encrypted DNS resolver that provides equivalent responses as the ones served by the network's recommended unencrypted resolver. It is not a requirement that these two resolvers are the same physical or logical machine. Often they will be, but they could equally be separated, perhaps by hundreds of miles. However it is deployed, the key is that they are equivalent.

3.1. Equivalence

Given two resolvers A and B, equivalence is the claim that A and B can provide the same upper-layer DNS function to the client. This does not include the DNS transport protocol (e.g. Do53 or DNS-over-HTTPS) which can differ between equivalent resolvers. To provide equivalence it is frequently likely to be the case that A and B are operated by the same administrative domain, but this document does not require that.

There are two possible ways to claim equivalence.

* The local network can claim that one or more encrypted DNS resolvers (B, C, etc) are equivalent to the Do53 resolver (A) it has offered. This is known as network-identified.

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

Network-identified is preferred since it comes from the same source of information, 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 must support being able to announce an equivalent resolver 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.

4. Network-identified encrypted 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 equivalent encrypted DNS resolvers, or states that there are none.

5. Resolver-identified encrypted 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 equivalent encrypted DNS resolvers by communicating with the network-recommended unencrypted Do53 resolver. This should involve an exchange that uses standard DNS messages that can be handled, or forwarded, by existing deployed software.

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.

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.

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.

6. 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 authenticated delegation from a client-known entity.

* Influence automatic discovery mechanisms such that a client uses one or more resolvers that are not otherwise involved with providing service to the client, such as: a network provider, a VPN server, a content provider being accessed, or a server that the client has manually configured.

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.

7. Statement of Requirements

This section lists requirements that flow from the above sections.

Requirement	Description
R1.1	Discovery MUST provide a local network the ability to announce to clients a set of, or absence of, equivalent resolvers.
R1.2	Discovery MUST provide a resolver the ability to announce to clients a set of, or absence of, equivalent resolvers.
R1.3	Discovery MUST support at least one encrypted DNS protocol.
R1.4	Discovery SHOULD support all standardised encrypted DNS protocols.
R2.1	Networks MUST be able to announce one or more equivalent 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 information MUST be specified such that provisioning mechanisms defined outside of the IETF can advertise encrypted DNS resolvers.
R3.1	When discovery is instantiated from a resolver (R1.2), that resolver MAY be encrypted or not.
R3.2	When discovery is instantiated from a resolver (R1.2), that resolver MAY be locally or globally reachable. Both options MUST be supported.
R4.1	In a home network use case, if the local network forwarder does not offer encrypted DNS service, the ISP's encrypted DNS server information MUST be retrievable via a query sent to a local network forwarder.
R4.2	Encrypted DNS server discovery MUST 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.
R5.5	An attacker in the network MUST NOT be able to override or interfere with the resolver preferences of a user or administrator.
R5.6	Attackers MUST NOT be able to influence automatic discovery mechanisms such that a client uses one or more resolvers that are not otherwise involved with providing service to the client, including a network provider, a VPN server, a content provider being accessed, or a

| | server that the client has manually configured. |
+-------------+---+

Table 1

8. Security Considerations

See Section 6.

9. IANA Considerations

This document has no IANA actions.

10. References

10.1. 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>.

10.2. 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-01, 20 October 2020, <http://www.ietf.org/internet-drafts/draft-ietf-dprive-dnsoquic-01.txt>.

[RFC1035] Mockapetris, P.V., "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, the subsequent interims, 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 and Andrew Campling.

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