A Bootstrapping Procedure to Discover and Authenticate DNS-over-(D)TLS and DNS-over-HTTPS Servers
draft-reddy-dprive-bootstrap-dns-server-00

Abstract

This document specifies mechanisms to automatically bootstrap endpoints (e.g., hosts, Customer Equipment) to discover and authenticate DNS-over-(D)TLS and DNS-over-HTTPS servers provided by a local network.

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 September 6, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents
carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction ................................................. 2
2. Requirements Language ....................................... 4
3. Bootstrapping IoT Devices and CPE .......................... 4
4. Bootstrapping Endpoint Devices .............................. 5
5. Discovery Procedure ......................................... 6
  5.1. DNS Reference Identifier DHCP Options .................. 6
    5.1.1. DHCPv6 DNS Reference Identifier Option ............. 7
    5.1.2. DHCPv4 DNS Reference Identifier Option ............. 8
  5.2. Resolution ................................................ 8
6. Security Considerations ...................................... 9
7. IANA Considerations ......................................... 9
  7.1. DHCPv6 Option ............................................ 9
  7.2. DHCPv4 Option ............................................ 10
  7.3. Application Service & Application Protocol Tags ....... 10
    7.3.1. DNS Application Service Tag Registration .......... 10
    7.3.2. dns.tls Application Protocol Tag Registration .... 10
    7.3.3. dns.dtls Application Protocol Tag Registration ... 10
    7.3.4. dns.https Application Protocol Tag Registration ... 10
8. Acknowledgments .............................................. 11
9. References ................................................... 11
  9.1. Normative References .................................... 11
  9.2. Informative References .................................. 13
Authors’ Addresses ............................................. 13

1. Introduction

Various network security services are provided by Enterprise, secure home and wall-gardened networks to protect endpoints (e.g., hosts, IoT devices). Some of these security services act on DNS requests from endpoints. However, if an endpoint is configured to use public DNS-over-(D)TLS [RFC7858] [RFC8094] or DNS-over-HTTPS [RFC8484] servers, network security services in the local network cannot act efficiently on DNS requests from the endpoints. In order to act on DNS requests from endpoints, network security services can block DNS-over-(D)TLS traffic by dropping outgoing packets to destination port 853, and by identifying the domains offering DNS-over-HTTPS servers, DNS-over-HTTPS traffic can be blocked by dropping outgoing packets to these domains. If the endpoint has enabled strict privacy profile (Section 5 of [RFC8310]), and the network security service blocks the traffic to the public DNS server, DNS service is not available to the
endpoint and ultimately the endpoint cannot access Internet. If the endpoint has enabled opportunistic privacy profile (Section 5 of [RFC8310]), and the network security service blocks traffic to the public DNS server, the endpoint will either fallback to an encrypted connection without authenticating the DNS-over-(D)TLS and DNS-over-HTTPS servers provided by the local network or fallback to clear text DNS, and cannot exchange encrypted DNS messages. This can compromise the endpoint security and privacy; some of the potential security threats are listed below:

- Pervasive monitoring of DNS traffic.
- If the endpoint is an IoT device which is configured to use public DNS-over-(D)TLS or DNS-over-HTTPS servers, and if a policy enforcement point in the local network is programmed using a Manufacturer Usage Description (MUD) file [I-D.ietf-opsawg-mud] by a MUD manager to only allow intended communications to and from the IoT device, the policy enforcement point cannot enforce the Network Access Control List rules based on domain names (Section 8 of [I-D.ietf-opsawg-mud]).
- The network security service cannot prevent an endpoint from accessing malicious domains. Attacks like DNS cache poisoning can lead the user to visit malicious websites to inject malware on the endpoint. For instance, malwares like DNSChanger can modify the endpoint’s DNS entries to point toward its own rogue name servers which then injected its own advertising into Web pages.

The DPRIVE and DoH working groups have not defined an automated mechanism to securely bootstrap the endpoints to discover and authenticate DNS-over-(D)TLS and DNS-over-HTTPS servers in the local network. Some clients have pre-configured specific public DNS servers (such as Mozilla using Cloudflare’s DNS-over-HTTPS server). If endpoints continue to use hard-coded public DNS servers, this has a risk of relying on few centralized DNS services. Further, Content Delivery Networks (CDNs) that map traffic based on DNS may lose the ability to direct end-user traffic to a nearby cluster in cases where a DNS service is being used that is not affiliated with the local network and which does not send "EDNS Client Subnet" (ECS) information to the CDN’s DNS authorities [CDN].

The document proposes a mechanism to automatically bootstrap the endpoints to discover and authenticate the DNS-over-(D)TLS and DNS-over-HTTPS servers provided by the local network. The overall procedure can be structured into the following steps:
2. 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.

3. Bootstrapping IoT Devices and CPE

The following steps discuss the mechanism to automatically bootstrapping IoT devices with local network’s CA certificates and DNS server certificate. The below steps can also be used by CPE acting as DNS forwarders to discover and authenticate DNS-over-(D)TLS and DNS-over-HTTPS servers provided by the access networks.

- The IoT device can use Bootstrapping Remote Secure Key Infrastructures (BRSKI) discussed in [I-D.ietf-anima-bootstrapping-keyinfra] to automatically bootstrap the IoT device using the IoT manufacturer provisioned X.509 certificate, in combination with a registrar provided by the local network and IoT device manufacturer’s authorizing service (MASA).

1. The IoT device authenticates to the local network using the IoT manufacturer provisioned X.509 certificate. The IoT device can request and get a voucher from the MASA service via the registrar. The voucher is signed by the MASA service and includes the local network’s CA public key.

2. The IoT device validates the signed voucher using the manufacturer installed trust anchor associated with the MASA,
stores the CA’s public key and validates the provisional TLS connection to the registrar.

3. The IoT device requests the full Enrollment over Secure Transport (EST) [RFC7030] distribution of current CA certificates (Section 5.9.1 in [I-D.ietf-anima-bootstrapping-keyinfra]) from the registrar operating as a BRSKI-EST server. The IoT device uses the Explicit Trust Anchor database to validate the DNS server certificate.

4. TBD: The IoT device learns the End-Entity certificates [RFC8295] from the BRSKI-EST server. The certificate provisioned to the DNS server in the local network will be treated as an End-Entity certificate. The IoT device needs to identify the End-Entity certificate is provisioned to the DNS server, the key usage extension [RFC5280] can be used to restrict the use of the End-Entity certificate to authenticate the DNS server, a new bit will be added to the KeyUsage type to identify the DNS server certificate.

4. Bootstrapping Endpoint Devices

The following steps explain the mechanism to automatically bootstrap an endpoint with the local network’s CA certificates and DNS server certificate:

1. The endpoint authenticates to the local network and establishes provisional TLS connection with the registrar operating as the BRSKI-EST server. The endpoint discovers registrar using DNS-based Service Discovery [RFC6763].

2. The endpoint uses Salted Challenge Response Authentication Mechanism (SCRAM) [RFC7804] to perform mutual authentication with the discovered BRSKI-EST server.

3. If the BRSKI-EST server authentication is successful, the endpoint requests the full EST distribution of current CA certificates and validates the provisional TLS connection to the BRSKI-EST server. If the BRSKI-EST server certificate cannot be verified using the CA certificates downloaded, the TLS connection is immediately discarded and the endpoint abandons the attempt to bootstrap from the BRSKI-EST server and discards the CA certificates conveyed by the BRSKI-EST server. The endpoint uses the Explicit Trust Anchor database to validate the DNS server certificate.
4. TBD: The endpoint learns the End-Entity certificates [RFC8295] from the BRSKI-EST server. The certificate provisioned to the DNS server in the local network will be treated as a End-Entity certificate. The endpoint needs to identify the End-Entity certificate is provisioned to the DNS server, the key usage extension [RFC5280] can be used to restrict the use of the End-Entity certificate to authenticate the DNS server, a new bit will be added to the KeyUsage type to identify the DNS server certificate.

5. Discovery Procedure

A DNS client discovers the DNS server in the local network supporting DNS-over-TLS, DNS-over-DTLS and DNS-over-HTTPS protocols by using the following discovery mechanism:

- The DNS client uses DHCP to discover the authentication domain name for the DNS server, as specified in Section 5.1.

- The DNS client then uses S-NAPTR [RFC3958] lookup to learn the protocols DNS-over-TLS, DNS-over-DTLS, and DNS-over-HTTPS supported by the DNS server and the DNS privacy protocol preferred by the DNS server administrators, as specified in Section 5.2 and Section 7.3.1. If DNS-over-HTTPS protocol is supported by the DNS server, the DNS client queries for the URI resource record type [RFC7553] to use the https URI scheme (Section 3 of [RFC8484]).

- The DNS client initiates (D)TLS handshake with the DNS server, the server presents its certificate and the client validates the server certificate using the End-Entity certificate and Explicit Trust Anchor database downloaded in steps 3 and 4 in Section 3 and Section 4. The DNS client uses validation techniques as described in [RFC6125] to compare the authentication domain name to the certificate provided by the DNS server.

- If the DNS client cannot reach or establish an authenticated and encrypted connection with the privacy-enabling DNS server provided by the local network, the DNS client can fallback to the privacy-enabling public DNS server.

5.1. DNS Reference Identifier DHCP Options

As reported in Section 1.7.2 of [RFC6125]:

"few certification authorities issue server certificates based on IP addresses, but preliminary evidence indicates that such certificates are a very small percentage (less than 1%) of issued certificates."
In order to allow for certificate authentication between a DNS client and server while accommodating for the current best practices for issuing certificates, this document allows for configuring authentication domain name to clients. This name can be used as a reference identifier for authentication purposes.

5.1.1. DHCPv6 DNS Reference Identifier Option

5.1.1.1. Option Format

The DHCPv6 DNS Reference Identifier option is used to configure an authentication domain name. The format of this option is shown in Figure 1.

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     OPTION_V6_AUTH_DOMAIN     |         Option-length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|            authentication-domain-name (FQDN)                  |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: DHCPv6 DNS Reference Identifier option

The fields of the option shown in Figure 1 are as follows:

- Option-code: OPTION_V6_AUTH_DOMAIN (TBA1, see Section 7.1)
- Option-length: Length of the authentication-domain-name field in octets.
- authentication-domain-name: A fully qualified domain name of the DNS server. This field is formatted as specified in Section 10 of [RFC8415].

5.1.1.2. DHCPv6 Client Behavior

DHCP clients MAY request options OPTION_V6_AUTH_DOMAIN as defined in [RFC8415], Sections 18.2.1, 18.2.2, 18.2.4, 18.2.5, 18.2.6, and 21.7. As a convenience to the reader, it is mentioned here that the DHCP client includes the requested option code in the Option Request Option.

If the DHCP client receives more than one instance of OPTION_V6_AUTH_DOMAIN option, it MUST use only the first instance of that option.
5.1.2. DHCPv4 DNS Reference Identifier Option

5.1.2.1. Option Format

The DHCPv4 DNS Reference Identifier option is used to configure an authentication domain name. The format of this option is illustrated in Figure 2.

```
<table>
<thead>
<tr>
<th>Code</th>
<th>Length</th>
<th>authentication domain name</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBA2</td>
<td>n</td>
<td>s1 s2 s3 s4 s5 ...</td>
</tr>
</tbody>
</table>
```

The values s1, s2, s3, etc. represent the domain name labels in the domain name encoding.

Figure 2: DHCPv4 DNS Reference Identifier option

The fields of the option shown in Figure 2 are as follows:

- **Code**: OPTION_V4_AUTH_DOMAIN (TBA2, see Section 7.2);
- **Length**: Includes the length of the authentication domain name field in octets; the maximum length is 255 octets.
- **Authentication domain name**: The domain name of the DNS server.
  This field is formatted as specified in Section 10 of [RFC8415].

5.1.2.2. DHCPv4 Client Behavior

To discover an authentication domain name, the DHCPv4 client MUST include OPTION_V4_AUTH_DOMAIN in a Parameter Request List Option [RFC2132].

If the DHCP client receives more than one instance of OPTION_V4_AUTH_DOMAIN option, it MUST use only the first instance of that option. The content of OPTION_V4_AUTH_DOMAIN is used as reference identifier for authentication purposes.

5.2. Resolution

Once the DNS client has retrieved the authentication domain name for the DNS server, an S-NAPTR lookup with ‘DPRIVE’ application service and the desired protocol tag is made to obtain information necessary to securely connect to the DNS server. The S-NAPTR lookup is performed using an untrusted recursive DNS resolver from an untrusted source (such as DHCP).
This specification defines "DPRIVE" as an application service tag (Section 7.3.1) and "dns.tls" (Section 7.3.2), "dns.dtls" (Section 7.3.3), and "dns.https" (Section 7.3.4) as application protocol tags.

If no DNS-specific S-NAPTR records can be retrieved, the discovery procedure fails for this authentication domain name. However, before retrying a lookup that has failed, a DNS client MUST wait a time period that is appropriate for the encountered error (e.g., NXDOMAIN, timeout, etc.).

6. Security Considerations

The bootstrapping procedure to discover and authenticate DNS-over-(D)TLS and DNS-over-HTTPS Servers MUST be enabled by the endpoint in a trusted network (e.g., Enterprise, Secure home networks) and disabled in an untrusted network (e.g., public WiFi network), similar to the way VPN connection from the endpoint to a VPN gateway is disconnected in a trusted network and VPN connection is established in an untrusted network.

If the endpoint has enabled strict privacy profile, and the network security service blocks the traffic to the privacy-enabling public DNS server, a hard failure occurs and the user is notified. The user has a choice to switch to another network or if the user trusts the network, the user can enable strict privacy profile with the DNS-over-(D)TLS or DNS-over-HTTPS server discovered in the network instead of downgrading to opportunistic privacy profile.

The primary attack against the methods described in Section 5 is one that would lead to impersonation of a DNS server. An attacker could attempt to compromise the DHCP discovery and S-NAPTR resolution. The attack is prevented by validating the certificate presented by the DNS server. DHCP-related security considerations are discussed in [RFC2131] and [RFC8415].

Security considerations in [I-D.ietf-anima-bootstrapping-keyinfra] and [RFC7804] need to be taken into consideration.

7. IANA Considerations

7.1. DHCPv6 Option

IANA is requested to assign the following new DHCPv6 Option Code in the registry maintained in http://www.iana.org/assignments/dhcpv6-parameters:
7.2. DHCPv4 Option

IANA is requested to assign the following new DHCPv4 Option Code in the registry maintained in http://www.iana.org/assignments/dhcpv4-parameters/:

<table>
<thead>
<tr>
<th>Option Name</th>
<th>Value</th>
<th>Data length</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPTION_V4_AUTH_DOMAIN</td>
<td>TBA2</td>
<td>Variable; the maximum length is 255 octets.</td>
<td>Includes the authentication domain name.</td>
</tr>
</tbody>
</table>

7.3. Application Service & Application Protocol Tags

This document requests IANA to make the following allocations from the registry available at: https://www.iana.org/assignments/s-naptr-parameters/s-naptr-parameters.xhtml.

7.3.1. DNS Application Service Tag Registration

- Application Protocol Tag: DPRIVE
- Intended Usage: See Section 5.2
- Security Considerations: See Section 6
- Contact Information: <one of the authors>

7.3.2. dns.tls Application Protocol Tag Registration

- Application Protocol Tag: dns.tls
- Intended Usage: See Section 5.2
- Security Considerations: See Section 6
- Contact Information: <one of the authors>

7.3.3. dns.dtls Application Protocol Tag Registration

- Application Protocol Tag: dns.dtls
- Intended Usage: See Section 5.2
- Security Considerations: See Section 6
- Contact Information: <one of the authors>

7.3.4. dns.https Application Protocol Tag Registration

- Application Protocol Tag: dns.https
- Intended Usage: See Section 5.2
- Security Considerations: See Section 6
8. Acknowledgments

Thanks to Joe Hildebrand for his comments and suggestions.

9. References

9.1. Normative References

[I-D.ietf-anima-bootstrapping-keyinfra]


9.2. Informative References


Authors’ Addresses

Tirumaleswar Reddy
McAfee, Inc.
Embassy Golf Link Business Park
Bangalore, Karnataka  560071
India
Email: kondtir@gmail.com

Dan Wing
USA
Email: dan@danwing.org

Michael C. Richardson
Sandelman Software Works
USA
Email: mcr+ietf@sandelman.ca