DPRIVE WG
Internet-Draft
Intended status: Standards Track
Expires: September 10, 2019

T. Reddy
McAfee
D. Wing

M. Richardson
Sandelman Software Works
M. Boucadair
Orange
March 9, 2019

A Bootstrapping Procedure to Discover and Authenticate DNS-over-(D)TLS and DNS-over-HTTPS Servers
draft-reddy-dprive-bootstrap-dns-server-01

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.

Table of Contents

1. Introduction

Traditionally a caching DNS server has been provided by the local network. This provides benefits like low latency to that DNS server (due to its network proximity to the endpoint). However, if an endpoint is configured to use Internet-hosted or public DNS-over-(D)TLS [RFC7858] [RFC8094] or DNS-over-HTTPS [RFC8484] servers, the local DNS server cannot serve the DNS requests from the endpoints. If public DNS servers are used instead of using local DNS servers, the operational problems are listed below:

- "Split DNS" [RFC2775] to use the special internal-only domain names (e.g., "internal.example.com") in enterprise networks will not work, and ".local" and "home.arpa" names cannot be locally resolved in home networks.

- 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 [RFC7871] to the CDN's DNS authorities [CDN].

- 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.

If public DNS servers are used instead of using local DNS servers, the following paragraph discusses the impact on Network-based security:

Various network security services are provided by Enterprise, secure home and wall-gardened networks to protect endpoints (e.g,. Hosts, IoT devices). [I-D.camwinget-tls-use-cases] discusses some of the Network-based security use cases. These network security services act on DNS requests from endpoints. However, if an endpoint is configured to use public DNS-over-(D)TLS or DNS-over-HTTPS servers, network security services 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. Identifying DNS-over-HTTPS traffic is far more challenging than DNS-over-(D)TLS traffic. Network security services can try to identify the domains offering DNS-over-HTTPS servers, and 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 server 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 privacy and 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 intented 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]).

- o The network security service cannot prevent an endpoint from accessing malicious domains.

The DPRIVE and DoH working groups have not yet 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. 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:

- o Bootstrapping phase (Section 3 and Section 4) is meant to automatically bootstrap endpoints with local network's CA certificates and DNS server certificate.

- o Discovery phase (Section 5) is meant to discover the privacy-enabling protocols supported by the DNS server and usable DNS server IP addresses and port numbers.

- o Connection handshake and service invocation: The DNS client initiates (D)TLS handshake with the DNS server learned in the discovery phase. Furthermore, DNS client uses the credentials discovered during the bootstrapping phase to validate the server certificate.

Note: The strict and opportunistic privacy profiles as defined in [RFC8310] only applies to DNS-over-(D)TLS protocols, there has been no such distinction made for DNS-over-HTTPS protocol.

2. Terminology

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.

(D)TLS is used for statements that apply to both Transport Layer Security [RFC8446] and Datagram Transport Layer Security [RFC6347]. Specific terms are used for any statement that applies to either protocol alone.

This document uses the terms defined in [RFC8499].

3. 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:

- o Bootstrapping Remote Secure Key Infrastructures (BRSKI) discussed in [I-D.ietf-anima-bootstrapping-keyinfra] provides a solution for secure automated bootstrap of devices. BRSKI specifies means to provision credentials on devices to be used to operationally access networks. In addition, BRSKI provides an automated mechanism for the bootstrap distribution of CA certificates from the EST server.

  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. SCRAM provides a more robust authentication mechanism than a plaintext password protected by Transport Layer Security (TLS).

  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. If the BRSKI-EST server certificate is verified using the CA certificates downloaded, the endpoint stores the CA certificates as Explicit Trust Anchor database entries. The endpoint uses the Explicit Trust Anchor database to validate the DNS server certificate. The endpoint needs to perform SCRAM authentication the first time it connects BRSKI-EST server. On subsequent connections to the BRSKI-EST server, the endpoint can validate the BRSKI-EST server certificate using the Explicit Trust Anchor database.

  4. 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 certificate provisioned to the DNS server. The SRV-ID identifier type

[RFC6125] within subjectAltName entry can be used to identify the DNS server certificate. For example, DNS server certificate will include SRV-ID "_domain-s.example.net" along with DNS-ID "example.net". This specification defines SRV service label "domain-s" in Section 9. As a reminder, the protocol component is not included in the SRV-ID [RFC4985].

4. Bootstrapping IoT Devices and CPE

The following steps explain the mechanism to automatically bootstrap 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 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 devices stores the CA certificates as Explicit Trust Anchor database entries. The IoT device uses the Explicit Trust Anchor database to validate the DNS server certificate.

    4. 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 a End-Entity certificate. The IoT device needs to identify the certificate provisioned to the DNS server. The SRV-ID identifier type [RFC6125] within subjectAltName entry can be used to identify the DNS server certificate. For example, DNS

server certificate will include SRV-ID "_domain-s.example.net" along with DNS-ID "example.net". This specification defines SRV service label "domain-s" in Section 9. As a reminder, the protocol component is not included in the SRV-ID [RFC4985].

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:

- o The DNS client retrieves the authentication domain name for the DNS server from the DNS-ID identifier type within subjectAltName entry in the DNS server certificate.

- o The DNS client then uses the authentication domain name for 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 5.1 and Section 9.1. This specification adds a SRV service label "domain-s" for privacy-enabling DNS servers. In the example below, for authentication domain name 'example.net', the resolution algorithm will result in the privacy-enabling protocols supported by the DNS server and usable DNS server IP addresses and port numbers.

```
example.net.
IN NAPTR 100 10 "" DPRIVE:dns.tls  "" dns1.example.net.
IN NAPTR 200 10 "" DPRIVE:dns.dtls "" dns2.example.net.

dns1.example.net.
IN NAPTR 100 10 S DPRIVE:dns.tls "" _domain-s._tcp.example.net.

dns2.example.net.
IN NAPTR 100 10 S DPRIVE:dns.dtls "" _domain-s._udp.example.net.

_domain-s._tcp.example.net.
IN SRV   0 0 853 a.example.net.

_domain-s._udp.example.net.
IN SRV   0 0 853 a.example.net.

a.example.net.
IN A        192.0.2.1
IN AAAA     2001:db8:8:4::2
```

Figure 1

o 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]). In the example below, for authentication domain name 'example.net' and the URL for resolution is https://example.net/dns-query. The following URI resource records could be made available:

```
$ORIGIN example.net.
_domain-s._tcp    IN URI 10 1 "https://example.net/dns-query"
```

Figure 2

5.1. 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 recursive DNS resolver discovered from an untrusted source (such as DHCP).

This specification defines "DPRIVE" as an application service tag (Section 9.1.1) and "dns.tls" (Section 9.1.2), "dns.dtls" (Section 9.1.3), and "dns.https" (Section 9.1.4) 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. Connection handshake and service invocation

The DNS client initiates (D)TLS handshake with the DNS server, the server presents its certificate in ServerHello message, and the DNS client matches the DNS server certificate downloaded in step 4 in Section 3 and Section 4 with the certificate provided by the DNS server in (D)TLS handshake. If the match is successful, the DNS client validates the server certificate using the Explicit Trust Anchor database entries downloaded in step 3 in Section 3 and Section 4.

If the match is successful and server certificate is successfully validated, the client continues with the connection as normal. Otherwise, the client MUST treat the server certificate validation failure as a non-recoverable error. 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.

7. 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 a 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 a 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 attacks against the methods described in Section 5 are the ones that would lead to impersonation of a DNS server and spoofing the DNS response to indicate that the DNS server does not support any privacy-enabling protocols. To protect against DNS-vectored attacks, secured DNS (DNSSEC) can be used to ensure the validity of the DNS records received. The explicit trust anchor database entries downloaded in step 3 in Section 3 and Section 4 can be used by the endpoint to validate the DNSSEC signature. Impersonation of the DNS server is prevented by validating the certificate presented by the DNS server. If the BRSKI-EST server conveys the DNS server certificate, but the S-NAPTR lookup indicates that the DNS server does not support any privacy-enabling protocols, the client can detect the DNS response is spoofed.

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

8. Privacy Considerations

[RFC7626] discusses DNS privacy considerations in both "on the wire" (Section 2.4 of [RFC7626]) and "in the server" (Section 2.5 of [RFC7626]) contexts. The endpoint may not know if the DNS-over-(D)TLS or DNS-over-HTTPS server in the local network has a privacy preserving data policy. A new privacy certificate extension can be defined that identifies the privacy preserving data policy of the DNS server. The extension will contain a URL that points to the privacy preserving data policy.

9. IANA Considerations

IANA is requested to allocate the SRV service name of "domain-s" for DNS-over-(D)TLS and DNS-over-HTTPS.

9.1. 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.

9.1.1. DNS Application Service Tag Registration

- Application Protocol Tag: DPRIVE
- Intended Usage: See Section 5.1
- Security Considerations: See Section 7
- Contact Information: <one of the authors>

9.1.2. dns.tls Application Protocol Tag Registration

- Application Protocol Tag: dns.tls
- Intended Usage: See Section 5.1
- Security Considerations: See Section 7
- Contact Information: <one of the authors>

9.1.3. dns.dtls Application Protocol Tag Registration

- Application Protocol Tag: dns.dtls
- Intended Usage: See Section 5.1
- Security Considerations: See Section 7
- Contact Information: <one of the authors>

9.1.4. dns.https Application Protocol Tag Registration

- Application Protocol Tag: dnshttps
- Intended Usage: See Section 5.1
- Security Considerations: See Section 7

o Contact Information: <one of the authors>

10. Acknowledgments

Thanks to Joe Hildebrand, Harsha Joshi, Shashank Jain, Patrick McManus and Sara Dickinson for the discussion and comments.

11. References

11.1. Normative References

[I-D.ietf-anima-bootstrapping-keyinfra]
Pritikin, M., Richardson, M., Behringer, M., Bjarnason, S., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructures (BRSKI)", draft-ietf-anima-bootstrapping-keyinfra-19 (work in progress), March 2019.

[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>.

[RFC3958] Daigle, L. and A. Newton, "Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS)", RFC 3958, DOI 10.17487/RFC3958, January 2005, <https://www.rfc-editor.org/info/rfc3958>.

[RFC4985] Santesson, S., "Internet X.509 Public Key Infrastructure Subject Alternative Name for Expression of Service Name", RFC 4985, DOI 10.17487/RFC4985, August 2007, <https://www.rfc-editor.org/info/rfc4985>.

[RFC6125] Saint-Andre, P. and J. Hodges, "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)", RFC 6125, DOI 10.17487/RFC6125, March 2011, <https://www.rfc-editor.org/info/rfc6125>.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012, <https://www.rfc-editor.org/info/rfc6347>.

[RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", RFC 6763, DOI 10.17487/RFC6763, February 2013, <https://www.rfc-editor.org/info/rfc6763>.

[RFC7030] Pritikin, M., Ed., Yee, P., Ed., and D. Harkins, Ed., "Enrollment over Secure Transport", RFC 7030, DOI 10.17487/RFC7030, October 2013, <https://www.rfc-editor.org/info/rfc7030>.

[RFC7553] Faltstrom, P. and O. Kolkman, "The Uniform Resource Identifier (URI) DNS Resource Record", RFC 7553, DOI 10.17487/RFC7553, June 2015, <https://www.rfc-editor.org/info/rfc7553>.

[RFC7804] Melnikov, A., "Salted Challenge Response HTTP Authentication Mechanism", RFC 7804, DOI 10.17487/RFC7804, March 2016, <https://www.rfc-editor.org/info/rfc7804>.

[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>.

[RFC8094] Reddy, T., Wing, D., and P. Patil, "DNS over Datagram Transport Layer Security (DTLS)", RFC 8094, DOI 10.17487/RFC8094, February 2017, <https://www.rfc-editor.org/info/rfc8094>.

[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>.

[RFC8295] Turner, S., "EST (Enrollment over Secure Transport) Extensions", RFC 8295, DOI 10.17487/RFC8295, January 2018, <https://www.rfc-editor.org/info/rfc8295>.

[RFC8446] 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>.

[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>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

11.2. Informative References

[CDN] "End-User Mapping: Next Generation Request Routing for Content Delivery", 2015, <https://conferences.sigcomm.org/sigcomm/2015/pdf/papers/p167.pdf>.

[I-D.camwinget-tls-use-cases] Andreasen, F., Cam-Winget, N., and E. Wang, "TLS 1.3 Impact on Network-Based Security", draft-camwinget-tls-use-cases-03 (work in progress), December 2018.

[I-D.ietf-opsawg-mud] Lear, E., Droms, R., and D. Romascanu, "Manufacturer Usage Description Specification", draft-ietf-opsawg-mud-25 (work in progress), June 2018.

[RFC2775] Carpenter, B., "Internet Transparency", RFC 2775, DOI 10.17487/RFC2775, February 2000, <https://www.rfc-editor.org/info/rfc2775>.

[RFC7626] Bortzmeyer, S., "DNS Privacy Considerations", RFC 7626, DOI 10.17487/RFC7626, August 2015, <https://www.rfc-editor.org/info/rfc7626>.

[RFC7871] Contavalli, C., van der Gaast, W., Lawrence, D., and W. Kumari, "Client Subnet in DNS Queries", RFC 7871, DOI 10.17487/RFC7871, May 2016, <https://www.rfc-editor.org/info/rfc7871>.

[RFC8310] Dickinson, S., Gillmor, D., and T. Reddy, "Usage Profiles for DNS over TLS and DNS over DTLS", RFC 8310, DOI 10.17487/RFC8310, March 2018, <https://www.rfc-editor.org/info/rfc8310>.

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

Mohamed Boucadair
Orange
Rennes 35000
France

Email: mohamed.boucadair@orange.com