ADD WG
Internet-Draft
Intended status: Standards Track
Expires: January 27, 2021

T. Reddy
McAfee
D. Wing
Citrix
M. Richardson
Sandelman Software Works
M. Boucadair
Orange

July 26, 2020

A Bootstrapping Procedure to Discover and Authenticate DNS-over-TLS and DNS-over-HTTPS Servers for IoT and BYOD Devices

draft-reddy-add-iot-byod-bootstrap-01

Abstract

This document specifies mechanisms to bootstrap endpoints (e.g., hosts, IoT devices) to discover and authenticate DNS-over-TLS and DNS-over-HTTPS servers provided by a local network for IoT/BYOD devices in Enterprise networks.

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 January 27, 2021.

Copyright Notice

Copyright (c) 2020 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

Traditionally a caching DNS server has been provided by local networks. This provides benefits such as low latency to reach that DNS server (owing to its network proximity to the endpoint). However, if an endpoint is configured to use Internet-hosted or public DNS-over-TLS (DoT) [RFC7858] or DNS-over-HTTPS (DoH) [RFC8484] servers, any available local DNS server cannot serve DNS requests from local endpoints. If public DNS servers are used instead of using local DNS servers, some operational problems can occur such as those 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 service-specific 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].

If public DNS servers are used instead of local DNS servers, the following discusses the impacts on network-based security:

- Various network security services are provided by Enterprise networks to protect endpoints (e.g,. Hosts, IoT devices). Network-based security solutions such as firewalls (FW) and Intrusion Prevention Systems (IPS) rely on network traffic inspection to implement perimeter-based security policies. The network security services may for example prevent malware download, block known malicious URLs, enforce use of strong ciphers, stop data exfiltration, etc. These network security services act on DNS requests originating from endpoints. However, if an endpoint is configured to use public DoH/DoT servers, network security services cannot act on DNS requests from these endpoints.

- In order to act on DNS requests from endpoints, network security services can block DoT traffic by dropping outgoing packets to destination port 853. Identifying DoH traffic is far more challenging than DoT traffic. Network security services may try to identify the domains offering DoH servers, and DoH traffic can be blocked by dropping outgoing packets to these domains. If an endpoint has enabled strict privacy profile (Section 5 of [RFC8310]), and the network security service blocks the traffic to the public DNS server, the DNS service won't be available to the endpoint and ultimately the endpoint cannot access Internet-reachable services.

- If an 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.

If the network security service fails to block DoH/DoT traffic, this can compromise the endpoint security; some of the potential security threats are listed below:

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

- If the endpoint is an IoT device which is configured to use public DoH/DoT servers, and if a policy enforcement point in the local

network is programmed using, for example, a Manufacturer Usage Description (MUD) file [RFC8520] 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 (ACL) rules based on domain names (Section 8 of [RFC8520]).

If the network security service successfully blocks DoT and DoH traffic, this can still compromise the endpoint security and privacy; some of the potential security threats are listed below:

- Networks are susceptible to internal attacks as discussed in Section 3.2 of [I-D.arkko-farrell-arch-model-t]. An internal attacker can modify the DNS responses to re-direct the client to malicious servers.

- Pervasive monitoring of DNS traffic.

In addition, the local network's DNS server is advertised using DHCP/RA which is insecure and also provides no mechanism to securely authenticate the DNS server. To overcome the above threats, this document specifies a mechanism to bootstrap endpoints to discover and authenticate the DoT and DoH servers provided by their local network. The overall procedure can be structured into the following steps:

- Bootstrapping (Section 4) is necessary only when connecting to a new network or when the network's DNS certificate has changed. Bootstrapping procedure authenticates the Enrollment over Secure Transport (EST) [RFC7030] server to the endpoint. After authenticating the EST server, DNS server certificate used by the local network is downloaded to the endpoint. This DNS server certificate enables subsequent authenticated encrypted communication with the local DNS server (e.g., DoH) during in the connection phase.

- Connection handshake and service invocation (Section 6): The DNS client initiates a TLS handshake with the DNS server learned in the discovery phase, and validates the DNS server's identity using the credentials obtained in the bootstrapping phase.

Note: The strict and opportunistic privacy profiles as defined in [RFC8310] only applies to DoT protocol, there has been no such distinction made for DoH protocol.

2. Scope

The problems discussed in Section 1 will be encountered in Enterprise networks. Typically Enterprise networks do not assume that all devices in their network are managed by the IT team or Mobile Device

Management (MDM) devices, especially in the quite common BYOD ("Bring Your Own Device") scenario. The mechanisms specified in this document can be used by BYOD devices to discover and authenticate DoT and DoH servers provided by the Enterprise network. This mechanism can also be used by IoT devices (managed by IT team) after onboarding to discover and authenticate DoT and DoH servers provided by the Enterprise network.

Wireless LAN as frequently deployed is vulnerable to various attacks ([Evil-Twin],[Krack] and [Dragonblood]). Because of these attacks, only cryptographically authenticated communications are trusted on Wireless LAN networks. This means information provided by such networks via DHCP, DHCPv6, or RA (e.g., NTP server, DNS server, default domain) are untrusted because DHCP and RA are not authenticated. [I-D.btw-add-home] discusses DoH/DoT server discovery using DHCP/RA but requires the DoH/DoT server to be pre-configured in the endpoint (OS or Browser) or the DNS client must be able cryptographically identify it is connecting to a DoT/DoH server hosted by a specific organization (e.g., ISP or Enterprise) (see [I-D.reddy-add-server-policy-selection]) to prevent the client from connecting to a attackers server.

Users have to indicate to their system in some way that they desire bootstrapping to be performed only when connecting to a specific network (e.g., organization for which a user works or a user works temporarily within another corporation), similar to the way users disable VPN connection in specific network (e.g., Enterprise network) and enable VPN connection by default in other networks. If the discovered DNS server meets the privacy preserving data policy requirements of the user, the user can select to use the discovered DoT and DoH servers.

3. 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.

This document makes use of the terms defined in [RFC8499] and [I-D.ietf-dnsop-terminology-ter].

'DoH/DoT' refers to DNS-over-HTTPS and/or DNS-over-TLS.

4. Bootstrapping Endpoint Devices

If a device is managed by an enterprise's IT department, the device can be configured to use Enterprise-provided DoH/DoT servers. This configuration might be manual or rely upon whatever deployed device management tool in an Enterprise. For example, customizing Firefox using Group Policy to use the Enterprise DoH server is discussed in [Firefox-Policy] for Windows and MacOS, and setting Chrome policies is discussed in [Chrome-Policy] and [Chrome-DoH].

If mobile device management (MDM) (e.g, [MDM-Apple]) is used to secure endpoint, MDM can be used to configure OS/browser with the Enterprise provided DoH/DoT server. If an endpoint is on-boarded, for example, using Over-The-Air (OTA) enrollment [OTA] to provision the device with a certificate and configuration profile, the configuration profile can include the authentication domain name (ADN) of the DoH/DoT server. The OS/Browser can use the configuration profile to use the Enterprise provided DoH/DoT server. In this case, MDM is not installed on the device.

4.1. Bootstrapping BYOD

This section focuses on bootstrapping Bring your own device (BYOD) to discover and authenticate DoH/DoT server provided by the enterprise network but without MDM or configuration profile on the endpoint. If an endpoint uses the credentials (username and password) provided by the IT admin to mutually authenticate to the Enterprise WLAN Access Point (e.g., PEAP-MSCHAPv2 [PEAP], EAP-pwd [RFC8146], EAP-PSK [RFC4764]), the following steps can be used to securely bootstrap the endpoint with the authentication domain name (ADN, defined in [RFC8310]) and DNS server certificate of the local network's DoH/DoT server:

1. The endpoint authenticates to the local network and discovers the Enrollment over Secure Transport (EST) [RFC7030] server using the procedure discussed in Section 7.

2. The endpoint establishes provisional TLS connection with that EST server, i.e., the endpoint provisionally accepts the unverified TLS server certificate. However, the endpoint MUST authenticate the EST server before it accepts the DNS server certificate. The endpoint either uses password-based authenticated key exchange (PAKE) with TLS 1.3 [I-D.barnes-tls-pake] as an authentication method or uses the mutual authentication protocol for HTTP [RFC8120] to authenticate the discovered EST server.

   As a reminder, PAKE is an authentication method that allows the use of usernames and passwords over unencrypted channels without

revealing the passwords to an eavesdropper. Similarly, the mutual authentication for HTTP is based on PAKE and provides mutual authentication between an HTTP client and an HTTP server using username and password as credentials. The cryptographic algorithms to use with the mutual authentication protocol for HTTP are defined in [RFC8121].

Note that the Crypto Forum Research Group (cfrg) has selected draft-haase-cpace and draft-krawczyk-cfrg-opaque drafts to recommend for balanced and augmented password-based authenticated key establishment in IETF protocols. This step will be further updated.

3. The endpoint needs to use PAKE scheme to perform authentication the first time it connects to an EST server. If the EST server authentication is successful, the server's identity can be used to authenticate subsequent TLS connections to that EST server. The endpoint configures the reference identifier for the EST server using the DNS-ID identifier type in the EST server certificate. On subsequent connections to the EST server, the endpoint MUST validate the EST server certificate using the Implict Trust Anchor database (i.e, the EST server certificate must pass PKIX certification path validation [RFC6125]) and match the reference identifier against the EST server's identity according to the rules specified in Section 6.4 of [RFC6125].

4. The endpoint learns the End-Entity certificates [RFC8295] from the EST server. The certificate provisioned to the DNS server in the local network will be treated as a End-Entity certificate. As a reminder, the End-Entity certificates must be validated by the endpoint using an authorized trust anchor (Section 3.2 of [RFC8295]). The endpoint needs to identify the certificate provisioned to the DNS server. The SRV-ID identifier type [RFC6125] within subjectAltName entry MUST 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". The SRV service label "domain-s" is defined in Section 6 of [RFC7858] for DoT protocol. The SRV service label "doh" is defined in Section 11 for DoH protocol.

5. The endpoint configures the authentication domain name (ADN) (defined in [RFC8310]) for the DNS server from the DNS-ID identifier type within subjectAltName entry in the DNS server certificate. The DNS server certificate is associated with the ADN to be matched with the certificate given by the DNS server in

TLS. To some extent, this approach is similar to certificate usage PKIX-EE(1) defined in [RFC7671].

Figure 1 illustrates a sequence diagram for bootstrapping an endpoint with the local network's ADN and DNS server certificate.

Figure 1: Bootstrapping Endpoint Devices

5. Bootstrapping IoT Devices

The following steps explain the mechanism to bootstrap IoT devices supporting Bootstrapping Remote Secure Key Infrastructures (BRSKI) discussed in [I-D.ietf-anima-bootstrapping-keyinfra] with local network's CA certificates, ADN and DNS server certificate:

- 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. The IoT device can use BRSKI to 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 EST 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 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 certificate provisioned to the DNS server. The SRV-ID identifier type within subjectAltName entry MUST be used to identify the DNS server certificate (see Step 4 in Section 4.1).

5. The endpoint configures the ADN for the DNS server from the DNS-ID identifier type within subjectAltName entry in the DNS server certificate. The DNS server certificate is associated with the ADN to be matched with the certificate given by the DNS server in TLS.

6. Connection Handshake and Service Invocation

The DNS client resolves the ADN using the mechanism discussed in Section 7.2 of [RFC8310]. The DNS client initiates TLS handshake with the DNS server, the DNS server presents its certificate in ServerHello message, and the DNS client MUST match the DNS server

certificate downloaded in Step 4 in Section 4.1 or Section 5 with the certificate provided by the DNS server in TLS handshake. If the match is successful, the DNS client MUST validate the server certificate using an authorized trust anchor.

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 a privacy-enabling public DNS server.

The DoH client contacts the DoH resolver to retrieve the list of supported DoH services using the well-known URI defined in [I-D.btw-add-rfc8484-clarification].

7. EST Service Discovery Procedure

An EST client discovers the EST server in the local network by using DNS-based Service Discovery (DNS-SD) [RFC6763] or Multicast DNS (mDNS) [RFC6762]. The <Domain> portion specifies the DNS sub-domain where the service instance is registered. It may be "local.", indicating the mDNS local domain, or it may be a conventional domain name such as "example.com.". The <Service> portion of the EST service instance name MUST be "_est._tcp".

A EST client application can proactively discover an EST server being advertised in the site by multicasting a PTR query to the following:

"_est._tcp.local"

An EST server can send out gratuitous multicast DNS answer packets whenever it starts up, wakes from sleep, or detects a change in EST server configuration. EST client application can receive these gratuitous packets and cache information contained in them.

8. Network Reattachment

On subsequent attachments to the network, the endpoint initiates TLS handshake with the DoH/DoT server (configured in Step 5 of Section 4.1 or Section 5) and follows the mechanism discussed in Section 6 to validate the DNS server certificate.

If the DNS server certificate is invalid (e.g., revoked or expired), the endpoint discovers and initiates TLS handshake with the EST server, and uses the validation techniques described in [RFC6125] to compare the reference identifier (created in Step 2 of Section 4.1 in

this document) to the EST server certificate and verifies the entire certification path as per [RFC5280]. The endpoint then gets the DNS server certificate from the EST server. If the DNS-ID identifier type within subjectAltName entry in the DNS server certificate does not match the configured ADN, the ADN is replaced with the DNS-ID identifier type. The DNS server certificate associated with the ADN is replaced with the one provided by the EST server. The endpoint initiates TLS handshake with the newly discovered ADN and follows the mechanism discussed in Section 6 to validate the DNS server certificate.

Figure 2 illustrates a sequence diagram for re-configuring an endpoint with ADN and local network's DNS server certificate on subsequent attachments to the network.

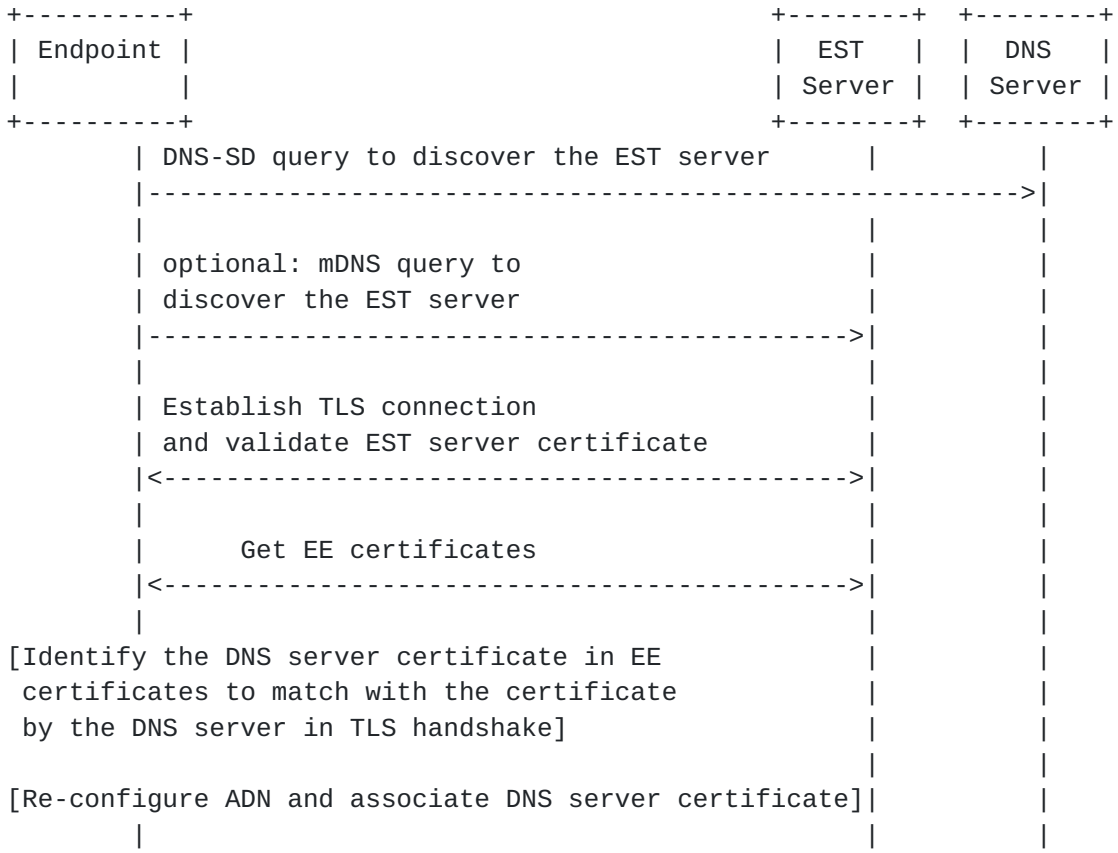

Figure 2: Bootstrapping Endpoint Devices on subsequent attachments to the network

9. 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 mechanism defined in [I-D.reddy-add-server-policy-selection] can be used by the DNS server to communicate its privacy statement URL and filtering policy to a DNS client. This communication is cryptographically signed to attest to its authenticity. By evaluating the DNS privacy statement, filtering policy and the signatory, the client can use the discovered DNS server if it meets privacy preserving data policy and filtering requirements of the user.

10. Security Considerations

The bootstrapping procedure to obtain the certificate of the local network's DNS server uses a client identity and password to authenticate the EST server using PAKE schemes. Security considerations such as those discussed in [I-D.barnes-tls-pake] or [RFC8120] and [RFC8121] need to be taken into consideration.

Users cannot be expected to enable or disable the bootstrapping or the discovery procedure as they switch networks. Thus, it is RECOMMENDED that users indicate to their system in some way that they desire bootstrapping to be performed when connecting to a specific network, similar to the way users disable VPN connection in specific network (e.g., Enterprise network) and enable VPN connection by default in other networks.

If an 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 DoH/DoT server discovered in the network instead of downgrading to opportunistic privacy profile.

The primary attacks against the methods described in Section 7 are the ones that would lead to impersonation of a EST server and spoofing the DNS response to indicate that the network does not support any EST server. To protect against DNS-vectored attacks, secured DNS (DNSSEC) can be used to ensure the validity of the DNS records received. Impersonation of the EST server is prevented by authenticating the EST server using the PAKE scheme. The PAKE scheme is only used once to configure the reference identifier of the EST server and the server certificate is validated for subsequent TLS connections to the EST server.

Security considerations in [I-D.ietf-anima-bootstrapping-keyinfra] need to be taken into consideration for IoT devices.

11. IANA Considerations

11.1. Service Name for EST

IANA is requested to allocate the following service name from the registry available at: https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml.

Service Name:	est
Port Number:	N/A
Transport Protocol(s):	TCP
Description:	Enrollment over Secure Transport (EST)
Assignee:	IESG <iesg@ietf.org>
Contact:	IETF Chair <chair@ietf.org>
Reference:	[ThisDocument]

11.2. Service Name for DoH

IANA is requested to allocate the following service name from the registry available at: https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml.

Service Name:	doh
Port Number:	N/A
Transport Protocol(s):	TCP
Description:	DNS-over-HTTPS
Assignee:	IESG <iesg@ietf.org>
Contact:	IETF Chair <chair@ietf.org>
Reference:	[ThisDocument]

12. Acknowledgments

Thanks to Joe Hildebrand, Harsha Joshi, Shashank Jain, Patrick McManus, Bob Harold, Livingood Jason, Winfield Alister, Eliot Lear, Stephane Bortzmeyer, Ted Lemon and Sara Dickinson for the discussion and comments.

13. References

13.1. Normative References

[I-D.ietf-anima-bootstrapping-keyinfra]
Pritikin, M., Richardson, M., Eckert, T., Behringer, M., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructures (BRSKI)", draft-ietf-anima-bootstrapping-keyinfra-41 (work in progress), April 2020.

[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>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[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>.

[RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762, DOI 10.17487/RFC6762, February 2013, <https://www.rfc-editor.org/info/rfc6762>.

[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>.

[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>.

[RFC8121] Oiwa, Y., Watanabe, H., Takagi, H., Maeda, K., Hayashi, T., and Y. Ioku, "Mutual Authentication Protocol for HTTP: Cryptographic Algorithms Based on the Key Agreement Mechanism 3 (KAM3)", RFC 8121, DOI 10.17487/RFC8121, April 2017, <https://www.rfc-editor.org/info/rfc8121>.

[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>.

[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>.

13.2. Informative References

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

[Chrome-DoH] The Unicode Consortium, "Chrome DNS over HTTPS (aka DoH)", <https://www.chromium.org/developers/dns-over-https>.

[Chrome-Policy] The Unicode Consortium, "Chrome policies for users or browsers", <https://support.google.com/chrome/a/answer/2657289?hl=en>.

[Dragonblood] The Unicode Consortium, "Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd", <https://papers.mathyvanhoef.com/dragonblood.pdf>.

[Evil-Twin] The Unicode Consortium, "Evil twin (wireless networks)", <https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks)>.

[Firefox-Policy] "Policy templates for Firefox", <https://github.com/mozilla/policy-templates/blob/master/README.md#dnsoverhttps>.

[I-D.arkko-farrell-arch-model-t]
Arkko, J. and S. Farrell, "Challenges and Changes in the Internet Threat Model", draft-arkko-farrell-arch-model-t-04 (work in progress), July 2020.

[I-D.barnes-tls-pake]
Barnes, R. and O. Friel, "Usage of PAKE with TLS 1.3", draft-barnes-tls-pake-04 (work in progress), July 2018.

[I-D.btw-add-home]
Boucadair, M., Reddy.K, T., Wing, D., and N. Cook, "Encrypted DNS Discovery and Deployment Considerations for Home Networks", draft-btw-add-home-07 (work in progress), July 2020.

[I-D.btw-add-rfc8484-clarification]
Boucadair, M., Cook, N., Reddy.K, T., and D. Wing, "Supporting Redirection for DNS Queries over HTTPS (DoH)", draft-btw-add-rfc8484-clarification-02 (work in progress), July 2020.

[I-D.ietf-dnsop-terminology-ter]
Hoffman, P., "Terminology for DNS Transports and Location", draft-ietf-dnsop-terminology-ter-01 (work in progress), February 2020.

[I-D.reddy-add-server-policy-selection]
Reddy.K, T., Wing, D., Richardson, M., and M. Boucadair, "DNS Server Selection: DNS Server Information with Assertion Token", draft-reddy-add-server-policy-selection-03 (work in progress), June 2020.

[Krack]
The Unicode Consortium, "Key Reinstallation Attacks", 2017, <https://www.krackattacks.com/>.

[MDM-Apple]
Apple, "Mobile Device Management", <https://developer.apple.com/documentation/devicemanagement>.

[OTA]
Apple, "Over-the-Air Profile Delivery Concepts", <https://developer.apple.com/library/archive/documentation/NetworkingInternet/Conceptual/iPhoneOTAConfiguration/OTASecurity/OTASecurity.html>.

[PEAP] Microsoft, "[MS-PEAP]: Protected Extensible Authentication Protocol (PEAP)", <https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-peap/5308642b-90c9-4cc4-beec-fb367325c0f9>.

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

[RFC4764] Bersani, F. and H. Tschofenig, "The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method", RFC 4764, DOI 10.17487/RFC4764, January 2007, <https://www.rfc-editor.org/info/rfc4764>.

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

[RFC7671] Dukhovni, V. and W. Hardaker, "The DNS-Based Authentication of Named Entities (DANE) Protocol: Updates and Operational Guidance", RFC 7671, DOI 10.17487/RFC7671, October 2015, <https://www.rfc-editor.org/info/rfc7671>.

[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>.

[RFC8120] Oiwa, Y., Watanabe, H., Takagi, H., Maeda, K., Hayashi, T., and Y. Ioku, "Mutual Authentication Protocol for HTTP", RFC 8120, DOI 10.17487/RFC8120, April 2017, <https://www.rfc-editor.org/info/rfc8120>.

[RFC8146] Harkins, D., "Adding Support for Salted Password Databases to EAP-pwd", RFC 8146, DOI 10.17487/RFC8146, April 2017, <https://www.rfc-editor.org/info/rfc8146>.

[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>.

[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>.

Authors' Addresses

Tirumaleswar Reddy
McAfee, Inc.
Embassy Golf Link Business Park
Bangalore, Karnataka 560071
India

Email: kondtir@gmail.com

Dan Wing
Citrix Systems, Inc.
USA

Email: dwing-ietf@fuggles.com

Michael C. Richardson
Sandelman Software Works
USA

Email: mcr+ietf@sandelman.ca

Mohamed Boucadair
Orange
Rennes 35000
France

Email: mohamed.boucadair@orange.com