DoH and DoT Server Discovery
& Deployment Considerations for Home and Mobile Networks

draft-btw-add-home

IETF 107 -- March 2020

M. Boucadair (Orange)
T. Reddy (McAfee)
D. Wing (Citrix)
N. Cook (Open-Xchange)
Agenda

• Scope & Objectives
• Target DoT/DoH deployments
• Which discovery information?
• The discovery procedure
• Rogue servers
• DoH-specific: one pending issue
• Next steps
Scope

Excerpt from the ADD WG Charter:

“Define a mechanism that allows clients to discover DNS resolvers that support encryption and that are available to the client either on the public Internet or on private or local networks.”
Objectives

• Discuss DoT/DoH deployment considerations for home networks
  – Both Home and Mobile networks
  – ISP, public, and private resolvers
  – Enterprise networks are out of scope

• Specify the required server discovery mechanism(s)

• Sketch the required steps to use DoT/DoH capabilities provided by local networks
Sample Encrypted DNS Deployments: Managed CPEs

(1) Receives the DNS configuration

DoT/DoH Server

DoT/DoH: Means DoT and/or DoH

(2) Relays the DNS information

DoT/DoH Server

Configures a 3rd Party DNS Server. The one received from the ISP will be ignored

Communicates the 3rd Party DNS information
Sample Encrypted DNS Deployments: Unmanaged CPEs

1. Receives the DNS configuration
2. Announces the DNS information
3. Relays the DNS information

DoT/DoH Server

ISP

Internal CPE

CPE

Internet
To avoid relying upon Do53 or opportunistic profile to resolve the resolver’s name

For PKIX authentication

1. How to construct the URL to use for resolution
2. Other URI variables may be supported in the future
3. DoH resolvers may expose customized services: no-filtering, filtering+malware detect, filtering+adult block, ...
Discovery Channel

Do53

DoT

DoH

List of IP addresses

Authentication Domain

Name

URI Templates

Existing DHCP/RA options

Define a new DHCP/RA option: Reference Identifier

Retrieved directly from the DoH server or using a dedicated RA/DHCP option
Verified Resolver: Detecting Rogue Server (1/2)

Attacker:
(1) Gets a valid name and a valid certificate
(2) Announces rogue server name and address via DHCP/RA RI
Verified Resolver: Detecting Rogue Server (2/2)

Host notices rogue server address and ADN are not pre-configured as **verified resolver**. Rogue server will not be used.
Verified Resolvers

• Auto-upgrade
  – If the **DNS server's IP address** discovered using DHCP/RA is pre-configured in the OS or Browser as a verified resolver, the DNS client auto-upgrades to use the pre-configured DoH/DoT server tied to the discovered DNS server IP address

  – If the **ADN (RFC8310)** conveyed in DHCP/RA is pre-configured in the OS or browser as a verified resolver, the DNS client auto-upgrades to establish a DoH/DoT session with the ADN

• Other approaches are discussed in the draft, e.g.,
  – If the discovered DoH/DoT server is not pre-configured in the OS or browser, the client may validate the signatory (e.g., cryptographically attested by the ISP)
ISP DoH Redirect to CPE DoH

• Offload DoH traffic from ISP DoH
• Local DoH = better round-trip time

• HTTP redirect to send host to ISP-managed CPE
ISP DNS Redirect to CPE DNS

1. ISP assigns a name and public certificate to the CPE.
2. Receives the DNS configuration in RI options.
3. Relays the DNS information in RI options.

LAN

ISP#1

Internet

DHCP (isp1.com, @)

DoH Server

HTTP 303 (See Other)

DoH session

Do53(cpe1.isp1.com) ➔ internal@

DHCP (isp1.com, @)

DoH Server

CPE

ISP DNS Redirect to CPE DNS
DoH Services & URI Templates

• Why?
  – RFC8484 supports URI templates with “dns” as the only variable, but future extensions may allow for queries with other variables
  – DoH resolvers may host many services; each identified by a URI scheme
  – DoH clients have to be instructed about valid URI templates to use

• How?
  – retrieved by querying a discovered DoH resolver
  – enclosed in a dedicated RA/DHCP option

• How the client uses these services is out of scope
URI Templates in RA/DHCP

• Trade-offs detailed in document

**Issues**
- Risk of stale information
- Dependency between DHCP servers (access routers) and DoH resolvers
- Fails if DoH resolver is not managed by the ISP
- Larger RA/DHCP messages

**Advantages**
- Clients can immediately use the service(s)
- Convenient if very few (stable) URIs are in use
- Per-host policy (See next slide)

• Need discussion to choose approach
Customized DHCP Configuration: Example filtering child’s device

(1) An administrator configures the following DNS policies:
- If C ➞ parental filtering
- Else ➞ no-filtering

(2) Receives a list of supported DoH services (e.g., parental, no-filtering)

(3) Communicates the “no-filtering” DoH server using DHCP URI option

(3’) Communicates the “parental filtering” DoH server using DHCP URI option
Implementation

• Ported DNSDist v1.4.0 with DoT/DoH support to OpenWRT-19.07

• Extended DNSDist to do DoT/DoH in the upstream (CPE to resolver)
Next Steps
draft-btw-add-home

• More feedback URI Templates discovery

• Consider adopting this document as a WG item

• Questions?
Appendix
Host a Forwarder in a Managed CPE

1. ISP assigns a name and public certificate to the CPE
2. Receives the DNS configuration in RI options
3. Relays the DNS information in RI options

- Certificates are managed by the ISP
- ACME fully automates certificate management (e.g., certificate issuance, expiry etc.) and no human intervention is required
- ACME and https://letsencrypt.org/ (to generate certificates for millions of home routers) are already in place by some security vendors. No roadblocks is reported so far
- Certificates are pushed by ISPs to the CPEs
Multi-Interface Devices: Out of Scope

Which one to use?
Do53 for Redirect: **Not a Threat**

The host won’t authenticate the server that spoofs the CPE@: PKIX authentication will fail.