Updates to Adaptive DNS Discovery

draft-pauly-dprise-adaptive-dns-privacy

Tommy Pauly, Eric Kinnear, Patrick McManus, Chris Wood

ADD

IETF 107, March 2020, Virtually Vancouver
Goals

Resolver discovery (local or remote)

Resolver information

When should a client use this resolver?

Are there any special capabilities of this resolver?
Status Quo Model

Local DNS Server

example.com HTTPS Server

Local DNS Server

foobar.net HTTPS Server

A

B
Trusted Remote Resolver Model

A

Remote DoH Server

e.example.com HTTPS Server

B

foobar.net HTTPS Server
Multiple Trusted Remote Resolver Model

A

Remote DoH Server 1

example.com HTTPS Server

Remote DoH Server 2

B

foobar.net HTTPS Server

Adaptive DNS - ADD - T. Pauly - IETF 107
Designated Remote Resolver Model

- A: Local DNS Server
  - example.com DoH Server
  - www.example.com HTTPS Server

- B: Local DNS Server
  - a.foobar.net HTTPS Server
  - foobar.net DoH Server
Why designate resolvers for domains?

Having the same “entity” terminate TLS/HTTPS connections also terminate DoH has several benefits:

Reduction of the number of entities that see traffic from a given client IP address associated with a hostname

While the entity *can* see many clients accessing a given name, it sees those same clients in TLS connections

It becomes easier to deploy shared servers that allow DoH connections to be reused for later HTTP traffic
Discovery of Resolvers

Remote resolvers advertised in DNS Records

  Extend HTTPSSVC to include DoH URI Template

  Same mechanism as Encrypted TLS Client Hello (ECHO)

  Involves DNS bootstrapping (local resolver / TRR / oblivious)

Local resolvers advertised in PvD info from RA
Resolver Information

Access a well-known URI to fetch remote configuration as a Provisioning Domain JSON blob

For `https://example-dns.org/dns-query`, info is at `https://example-dns.org/.well-known/pvd/dns-query`

JSON information can include the DoH URI template, which is useful for finding DoH for local PvDs

Supports identifying domains used for split DNS, or other extensible behavior properties
Validating Designation

DNSSEC-signed DNS records that designate a DoH server for a given name establish a trusted relationship.

Resolver information can also identify other mechanisms for validation.

Information can hint that `example.com` designates this DoH server, which can be validated using a request such as `https://example.com/.well-known/pvd`
Scenarios
DNSSEC Signed Designation

Signed Record
example.com -> Valid DoH Server

DoH Queries

example.com Valid DoH Server

example.com HTTPS Server
Scenarios
Unsigned Designation Attack

Unsigned Record
example.com ->
Attacker DoH Server

DoH Queries

example.com
Valid DoH Server

example.com
HTTPS Server

Attacker
DoH Server
Scenarios
Unsigned Designation Mitigation

1. Information Query
   TrustedDomains = [example.com]

2. Information Query (using another DNS source for resolution)

3. DoH Queries
   example.com
   Valid DoH Server

Unsigned Record
example.com ->
Valid DoH Server

Information
Valid DoH Server

example.com
HTTPS Server

Information
Valid DoH Server
Scenarios
Unsigned Designation Attack Attempt

Unsigned Record

example.com ->
Attacker DoH Server

1. Information Query

Information

TrustedDomains
= [example.com]

Attacker
DoH Server

example.com
HTTPS Server

2. Information Query
(using another DNS source for resolution)

Information
Valid DoH Server