Discovery of Equivalent Encrypted Resolvers

draft-pauly-add-deer

Tommy Pauly, Tommy Jensen, Eric Kinnear, Patrick McManus, Chris Wood
ADD
IETF 109, November 2020, Virtual
Equivalent Resolvers :=

Accessible on the same IP address

OR

Certificate claims ownership over both resolvers
Use Cases

1. Given an IP address of a Do53 server, discover equivalent encrypted resolvers

2. Given the name of an encrypted resolver, discover resolver properties and other equivalent encrypted resolvers

*Does not include non-equivalent encrypted resolvers, such as resolvers upstream from forwarders without a common certificate*
DNS Service Binding Record
draft-schwartz-svcb-dns

DNS SVCB records can list available resolvers for DoT, DoH, DoQ, etc.

_dns.example.net  7200  IN  SVCB  1  .  (  
alpn=h2 dohpath=/dns-query{?dns} ipv4hint=x.y.z.w )

_dns.example.net  7200  IN  SVCB  1  dot.example.net  (  
alpn=dot port=8530 ipv4hint=x.y.z.w )
Do53 upgrade using IP address

IP address can be provisioned by network (DHCP/RA), VPN, manually, etc.

Client sends a query for `_dns.resolver.arpa`

Response can list one or multiple equivalent resolvers
Do53 upgrade using IP address

Authenticated mode

Certificate of the encrypted resolver MUST include the original IP address in the SAN

Required if the IP address is different

Opportunistic mode

Certificate name implicitly trusted

Only allowed if on the same IP address
Discovery using known names

A resolver name may already be known

- Provisioned by new network mechanisms (DHCP/RA/PvD)
- Entered manually
- Configured for an encrypted protocol that isn’t accessible (DoT is blocked, but DoH might work, etc)
Discovery using known names

Query for the known resolver name, such as _dns.resolver.example.com

Certificate must cover the originally known name

Name will generally match, but an alternate protocol may have a different hostname
Questions?