Adaptive DNS Privacy

draft-pauly-dprive-adaptive-dns-privacy-01

Tommy Pauly, Chris Wood,
Eric Kinnear, Patrick McManus

ABCD
IETF 106, November 2019, Singapore
Status Quo DNS
Public Recursive

Local Recursive DNS53

Public Recursive DoH

domain.example.com
How can clients discover encrypted DNS resolvers?

How can networks advertise local policy?

How can clients choose the right resolvers to use?
How can clients discover encrypted DNS resolvers?

How can networks advertise local policy?

How can clients choose the right resolvers to use?
How can clients discover encrypted DNS resolvers?

- Hard-coded or configured policy
- Bootstrapping off of HTTP connections
- Using records in the DNS

Proposal uses Service Binding (SVCB/HTTPSSVC) records to indicate DoH URIs

DNSSEC signing can prove that the owner of a name designated a specific DoH service
Choice of Protocol

Encrypting DNS traffic is clearly beneficial for privacy and security

**DoT** and **DoH** both provide encryption

**DoH** provides additionally:

- Ability to multiplex DNS with other traffic
- More direct transition to QUIC
- Ability to proxy requests
Designated DNS Server
How can clients discover encrypted DNS resolvers?

How can networks advertise local policy?

How can clients choose the right resolvers to use?
How can networks advertise local policy?

- Canary DNS domains
- DHCP/RA options
- **Provisioning Domain Options**
  - Indicate filtering rules
  - Indicate walled garden/captive
  - Define domains that designate the local resolver to optimize results
Local Designated DNS Server

- Local Designated DoH (isp.com)
- Locally Optimized Content
- Designated DoH (example.com)
- example.com
Network-Based Filtering

PvD configuration can specify filtering policy

Partial/optional filtering:

```json
{
    "identifier": "myhome.net",
    "dnsZones": [ "myisp.com", "myhome.net" ],
    "requireDNSFiltering": false,
    "dnsFilteredZones": [ "sensitivedomain.net" ]
}
```

Complete filtering:

```json
{
    "identifier": "myschool.net",
    "dnsZones": [ "myschool.net" ],
    "requireDNSFiltering": true,
    "dnsFilteredZones": [ "." ]
}
```
How can clients discover encrypted DNS resolvers?

How can networks advertise local policy?

How can clients choose the right resolvers to use?
Client Resolution Algorithm

Names belonging to a VPN or enterprise
Resolve “internal.example.net” with internal VPN server

Names with a local DoH designation
Resolve “wifi-router.home” with local server

Names with an known designated DoH server
Resolve “google.com” with Google server

Other privacy-sensitive user traffic names
Resolve “example.com” with proxying between multiple servers

Default & bootstrapping system traffic
Lookup initial setup names and captive portals locally
Many Designated DNS Servers
Bootstrapping

If the local network is trusted, Designated DoH servers are discovered using local queries.

Otherwise, the resolver can use Oblivious DoH to proxy queries between different public resolvers without revealing client data to public resolvers.

Come to DPRIVE for more details!
Get involved!

Draft Issues and PRs

https://github.com/tfpauly/draft-pauly-adaptive-dns-privacy

Oblivious DoH Library

https://github.com/chris-wood/odoh

Sample Proxy/Target

https://github.com/chris-wood/odoh-server