DNS over DTLS (DNSoD)

draft-ietf-dprive-dnsodtls-01

July 2015

IETF 93 - Prague

Authors: Tiru Reddy, Dan Wing and Prashanth Patil

Presenter: Dan Wing

Agenda

- DNSoDTLS Advantages
- Problem unique to DNSoDTLS
  - Anycast
- Problems common with DNSoDTLS & DNSoTLS
  - Firewall interfering with UDP/53
  - Authenticating DPRIVE server
  - Polling and discovery
  - Downgrade attack

DNSoDTLS Advantages

- Avoids network head-of-line blocking
- DTLS session resumption is fast
  - DTLS session resumption w/o server-side state (RFC5077)
  - 1 RTT with DTLS 1.0-1.2
  - 0 RTT with DTLS 1.3
- Anycast
- DTLS also used for WebRTC media and data channels, COAP, TURN, VPN, and more

Anycast

Problem: server w/o cryptographic state receives DTLS packet

Possible Solution 1: DTLS Alert message in response

Possible Solution 2: Send session resumption if it's been awhile

(probably want anyway!)

Firewall interfering with UDP/53

Problem: Firewall blocks encrypted traffic on UDP port 53

Firewall interfering with UDP/53

Possible solution:

- IANA-assigned port for encrypted traffic

Authenticating the DNS privacy server

Problem: How to perform DNS server authentication ?

Authenticating the DNS privacy server

- Possible solution:
  - Configure client with server names
  - Server certificate matches SubjectAltName
  - Validate using normal CA trust model
- Example of /etc/resolv.conf file:

```
nameserver 8.8.8.8
certificate google-public-dns.google.com
nameserver 208.67.220.220
certificate resolver.opendns.com
```

Authenticating the DNS privacy server

Problem: DNS privacy server doesn't have CA-signed certificate

e.g., home network (192.168.1.1)

Authenticating the DNS privacy server

- Possible solution:
  - Subject Public Key Info (SPKI) fingerprint of the DNS privacy server.
- Example of /etc/resolv.conf file:

```
nameserver 192.168.1.1
SPKI-Fingerprint 01:56:D3:AC:CF:5B:3F:B8:8F:
0F:B4:30:88:2D:F6:72:4E:8C:F2:EE
```

Polling and Discovery

- Problem: How does a client determine if a DNS server and network supports DNSoD?
- Possible Solution: Send a DTLS ClientHello message and retry
  - OMG, downgrade attack! (see next slide)

Downgrade attacks

Problem: What if DNSoD is not supported or blocked ?

Downgrade attacks

- Possible Solution:
- Order of preference
  - **DNS servers on the local network**
  - **DNS servers on the Internet**
- Attempt connectivity in parallel to both servers
- Endpoint has three choices
  - **Refuse to send DNS queries on the network**
  - **Use DNS privacy with an un-authorized server**
  - **Fallback to plain DNS**

DNS over DTLS (DNSoD)
draft-ietf-dprive-dnsodtls