Encrypted DNS Discovery and CPEs

Recap, Status and Next Steps

Neil Cook

PowerDNS/Open-Xchange

6th December 2019

Stay Open.

DNS Discovery – Why is it needed?

Enter your subtitle here

- If you “know” in advance the IP Address & Port (DoT) or URL (DoH) of an encrypted DNS resolver, you can use it
  - No need for discovery
- However upgrading known plain-text DNS to Encrypted DNS is not straightforward
  - DoT
    - DNS53 -> DoT **seems** simplest, i.e. just use port 853 instead of 53
    - However doesn’t work for forwarders/proxies (e.g. CPEs) which haven’t been upgraded to DoT
    - Doesn’t work if DoT service is on different IP Addresses from DNS53
  - DoH
    - No way to “automatically” discover what URL a DoH service is running on

IETF Discovery Drafts

Enter your subtitle here

- DoH WG decided that discovery was out of scope
- Discovery topic moved to dnsop at some point
- Initial drafts focused on DoH Discovery only
  - https://www.ietf.org/archive/id/draft-ietf-resolver-associated-doh-03.txt
  - Lookup TXT record of SUDN or well-known URI using resolver IP address
- This morphed into drafts that focused on resolvers self-publishing information about themselves
  - https://datatracker.ietf.org/doc/draft-ietf-dnsop-resolver-information/
  - New RESINFO RRtype
  - Mechanism 1: Reverse IP lookup - <reverse-ip>.{in-addr,ip6}.arpa/IN/RESINFO
  - Mechanism 2: Well-known URI - https://IPADDRESSOFRESOLVER/.well-known/resolver-info/

Problems with Current Resolver Information Draft

- In our opinion there are some issues with the current discovery draft
  - Two mechanisms are specified to retrieve information
    - But neither is specified as mandatory
    - This leaves the option for clients to only implement one
  - The HTTPS mechanism does not work with DNS forwarders/proxies
    - i.e. A large proportion (maybe majority) of CPEs installed in the UK and Europe
  - The use of reverse IP to perform the DNS RESINFO lookup could be problematic for DNS mechanism
    - Resolvers would have to “know” all the IP addresses they could be contacted on
      - Or more likely just return RESINFO data for all looked-up IPs
    - There is a suggestion that DNSSEC could be used – but the draft is somewhat confused on this

Security Issues with Discovery

- Asking the resolver advertised by DHCP for information about itself provides no additional security on top of DHCP (which is already insecure)
- An on-path attacker could modify the RESINFO data
    - Remove advertised DoT/DoH information (downgrade attack)
    - Return information about a malicious DoT/DoH server
- DNSSEC validation (in the client) could address the above (unless access network is compromised)
- Malicious DoT/DoH servers could be avoided by checking certificate against a trusted list
    - However this doesn’t prevent an on-path attacker from returning a different (but still trusted, and presumably public) DoT/DoH server
    - Not sure what the point of such an attack would be as it removes visibility for on-path attacker

Get Involved

- PowerDNS have commented on resolver draft in dnsop WG
  - Mainly about making the DNS mechanism mandatory to implement
  - Almost nobody else has commented
- Our recommendations for EDDI participants are:
  - Think about if you are interested in DoH discovery
  - If so, participate in WG discussions. Take a position. For or against.

Open-Xchange AG

Rollnerstraße 14
D-90408 Nuernberg

Phone:	+49 2761-8385-0
Fax:	+49 2761-8385-30

info@open-xchange.com
www.open-xchange.com

Stay Open. OX