A Proposal for a
DoH Discovery Trial
draft-cook-doh-discovery-trial-00
IETF 108, Virtual

Neil Cook <neil.cook@noware.co.uk>
What is this?

- An interim discovery mechanism for quick deployment
- Developed by a group of ISPs and vendors
- Inspired by the Chrome/Windows «same provider auto upgrade» model
- Extends it to a common use case that is currently not supported: CPEs acting as DNS forwarders
  - Most common consumer architecture at major ISPs, at least in Europe
- Complementary, not overlapping
  - The current mechanism is only triggered if the resolver has a public IP
  - This mechanism is only triggered if the resolver has a private IP
How does this work?

• Similar to draft-pp-add-resinfo and draft-rescorla-doh-cdisco
• Does a Do53 query for a special name to ask the system resolver for its DoH URI
  • By using Do53, the query works with forwarders
• Uses a TXT record to convey the DoH URI
• Then (if successful) the client can establish a DoH connection to the discovered URI
  • After the initial query, the CPE is bypassed
  • The client could also ask the user or do other things – this is out of scope
How does this work?

ISP’s DNS resolver
62.6.40.178

Home router
192.168.1.1

User device

DoH connection

DNS query

DNS query

TXT record

TXT record

TXT record
Security assessment

• An attacker on the user’s home network or local loop could redirect the user to a malicious DoH server or «downgrade» to Do53
• This can be countered by maintaining a safelist of known legitimate DoH servers
  • Same approach as current Chrome/Windows mechanism
  • Not very scalable, but not less scalable than the current mechanism
• An attacker could still redirect the user to a different safe DoH server
• This can be countered by only safelisting «closed» DoH servers (i.e. accessible only from inside their ISP’s network)
Security assessment

• Opportunistic security for users of DNS-forwarding CPEs and of clients following the «same provider auto upgrade» model

• Does not create additional risks
  • An attacker on the user’s home network or local loop could already hijack DNS today

• Provides additional security
  • DNS traffic moves from cleartext to encrypted

• Does not prevent implementing better solutions once found