DNS over CoAP (DoC)

`draft-ietf-core-dns-over-coap`

Martine S. Lenders (m.lenders@fu-berlin.de), Christian Amsüss, Cenk Gündoğan, Thomas C. Schmidt, Matthias Wählisch

IETF 116 CoRE Meeting, 2023-03-28

Motivation for DNS over CoAP

Attack Scenario

Countermeasure: Encrypt name resolution triggered by IoT devices against eavesdropping

Our Proposal: DNS over CoAP (DoC), `draft-ietf-core-dns-over-coap`

- **Encrypted communication** based on DTLS or OSCORE
- **Block-wise message transfer** to overcome Path MTU problem (DNS over DTLS)
- **Share system resources** with CoAP applications
  - Same socket and buffers can be used
  - Re-use of the CoAP retransmission mechanism

Changes to DoC Draft Since IETF 115

Addressing DNSDIR review from Tim Wicinski (thanks!):

+ Specify DoC server role in terms of DNS terminology
+ Add subsection on how to implement DNS Push in DoC
+ Add appendix on reference implementation
  - Clarify that communication between DoC and DNS components is agnostic of the transport

Open Discussions on DoC (I)

Starting to address feedback from DNSOP (thanks Ben Schwartz!) in `-03`:

- Why isn't DoH via CoAP proxy sufficient? The draft should explain.
  - Performance advantages (caching and PDU) of FETCH
  - TTL rewriting
  - The real question: "How to translate DoC to DoH at CoAP-to-HTTP proxy?" (or generalized: "How to translate FETCH?")
- Explain why TTL rewriting proposed is notably different from DoH.
  - Evaluation with publication TBA
  - In HTTP(S) proxies do not have the same importance as in CoAP

Open Discussions on DoC (II)

Starting to address feedback from DNSOP (thanks Ben Schwartz!) in `-03`:

- Does DoC live at a URI path? If so, consider defining a default path, if this is a common practice in CoAP.
  - Default paths not a common practice in CoAP (we have CoRE-RD)
  - RECOMMENDATION for root path (since it requires no URI-Path option)
  - Maybe an inconvenience to not have default path, but so can be enforcing one
- Recommendation to add a section describing how to bootstrap DoC in a SVCB-DNS record. May require to allocate a new ALPN ID for CoAP/DTLS.
  - `coap` ID already exists in ALPN registry for TLS (RFC 8323)
  - Never mandated for DTLS: Discussion started on mailing list
  - SVCB with OSCORE/EDHOC: Discussion started on mailing list

Next Steps

- Address feedback where possible
- Pick ID for `application/dns-message` Content-Format