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
• Full evaluation will be published at ACM CoNEXT 2023
• Pre-print available at https://arxiv.org/abs/2207.07486
How does this draft relate to draft-lenders-dns-cbor

- This draft (draft-ietf-core-dns-over-coap) introduces application/dns-message content format
  - Classic DNS wire format
  - Easily transferable to other DNS transports
- However: Sometimes not small enough (even with classic name compression)
  ⇒ CBOR-based application/dns+cbor format (draft-lenders-dns-cbor) to reduce message size
  - Optional support for packed CBOR (draft-ietf-cbor-packed) for even more compression
  - application/dns-message serves as fallback
Changes to DoC Draft Since IETF 116

(c currently only in GitHub)

+ Clarify that DoC is orthogonal to DoH
+ Recommend root path "/" as DNS resource path
+ Set "application/dns-message" CF to 35353
+ Rationalize TTL rewriting
+ Added "Implementation Status" section
Open Discussions on DoC (I)

Address feedback from DNSOP (thanks Ben Schwartz!) in -03:

- 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 (see also GH issue 22).
  - coap ID already exists in ALPN registry for TLS (RFC 8323)
  - Never mandated for DTLS; Ben recommends to keep TLS only, define new ID for DTLS (see mailing list)
  - SVCB with OSCORE/EDHOC: Discussion started on mailing list, some consensus needed
- Translate between DoC and DoH at CoAP-HTTP-Proxy or just use DNS forwarder?
  - Main question for CoRE: How to translate FETCH to HTTP?
Open Discussions on DoC (II)

Other open issues:

- **GH issue 23**: Guidance says MID≠0 for unprotected case
  - Can we keep caching advantage of MID=0 and rely on CoAP tokens to prevent response spoofing instead?
What do we need from the WG for progress?

- Guidance on how to translate FETCH to HTTP(S)
- Statement on SVCB with OSCORE/EDHOC and CoAP-over-DTLS resources
- More feedback
Next Steps

- Address feedback where possible
- Publish -03 before IETF 117 draft cut-off
- ⟨ Your thoughts.⟩