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 117 CoRE Meeting, 2023-07-25
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
System Evaluation: With CoAP app present, OSCORE has least memory consumption

- 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

draft-ietf-core-dns-over-coap

Provides Content-Format for
application/dns-message media type

• Classic DNS wire format
• Easily transferable to other DNS transports
• However: Sometimes not small enough (even with classic name compression)
<table>
<thead>
<tr>
<th>draft-ietf-core-dns-over-coap</th>
<th>draft-lenders-dns-cbor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provides Content-Format for</td>
<td>CBOR-based application/dns+cbor</td>
</tr>
<tr>
<td>application/dns-message media type</td>
<td>format to reduce message size</td>
</tr>
<tr>
<td>• Classic DNS wire format</td>
<td>• More concise: Omit (redundant) DNS fields</td>
</tr>
<tr>
<td>• Easily transferable to other DNS transports</td>
<td>• More compressed: Optional support for packed CBOR (draft-ietf-cbor-packed)</td>
</tr>
<tr>
<td>• <strong>However</strong>: Sometimes not small enough (even with classic name compression)</td>
<td>• application/dns-message serves as fallback</td>
</tr>
</tbody>
</table>
Changes to DoC Draft

Since IETF 116

+ Recommend root path "/" as DNS resource path
+ Rationalize TTL rewriting
+ Added "Implementation Status" section

Since last interim

+ Clarify mapping between DoC and DoH (use DNS forwarder)
+ Set "application/dns-message" CF to 553 (53 planned for application/dns+cbor)
  - Clarify that DoC is disjunct from DoH
  - Do NOT RECOMMEND on unencrypted use, but provide security considerations for it
Address feedback from DNSOP (thanks Ben Schwartz!):

- 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
    - Interim: Keep TLS only, define new ID for DTLS (see mailing list)
- SVCB with OSCORE/EDHOC: Discussion started on mailing list, some concensus needed
- Overall: DoC draft probably not the best place for this
Next Steps

• Waiting for input from CoRE WG on draft about SVCB with OSCORE/EDHOC and CoAP-over-DTLS resources

• Any other feedback?
Next Steps

- Waiting for input from CoRE WG on draft about SVCB with OSCORE/EDHOC and CoAP-over-DTLS resources
- Any other feedback?
- What needs to be done before WGLC?