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 118, CoRE WG Session, 2023-11-09

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

Research Paper

Accepted at CoNEXT'23, published in PACMNET:

> Martine S. Lenders, Christian Amsüss, Cenk Gündogan, Marcin Nawrocki, Thomas C. Schmidt, Matthias Wählisch. 2023. **Securing Name Resolution in the IoT: DNS over CoAP**, *Proceedings of the ACM on Networking (PACMNET)* 1, CoNEXT2, Article 6 (September 2023), 25 pages. `https://doi.org/10.1145/3609423`
>
> ArXiv pre-print: `https://arxiv.org/abs/2207.07486`

Changes to DoC Draft

Since IETF 117

+ Amended Introduction with short contextualization of constrained environments
+ Added appendix about research paper

Open Discussions on DoC: SVCB-DNS record

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

Open Discussions on DoC: SVCB-DNS record

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

Should we start a draft on that?

Open Discussions on DoC: Cachable OSCORE

Address feedback from Marco Tiloca:

- Cachability ⇔ OSCORE: Reference draft-amsuess-core-cachable-oscore (see also PR 26)

WGLC?