DNS over CoAP (DoC)

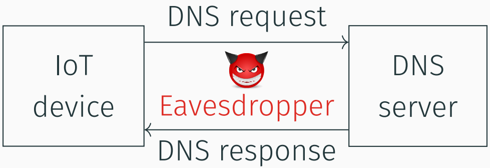
draft-ietf-core-dns-over-coap

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



DNS request

IoT device

Eavesdropper

DNS server

DNS response

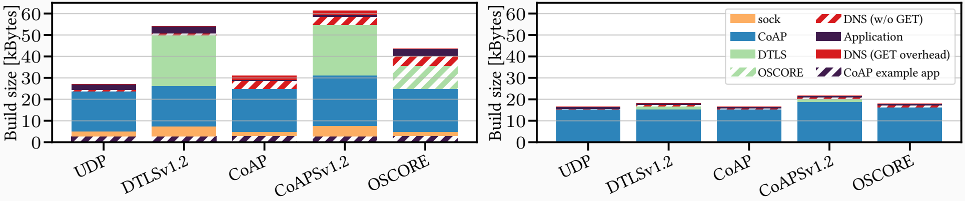
Countermeasure: Encrypt name resolution triggered by IoT devices against eavesdropping

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

Evaluation?

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)

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)

`draft-lenders-dns-cbor`

CBOR-based `application/dns+cbor` format to reduce message size

- More concise: Omit (redundant) DNS fields
- More compressed: Optional support for packed CBOR (`draft-ietf-cbor-packed`)
- `application/dns-message` serves as fallback

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

Open Discussions on DoC

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?