Secure Name Resolution in the IoT

Martine S. Lenders
TU Dresden
Dresden, Germany
martine.lenders@tu-dresden.de

Thomas C. Schmidt
HAW Hamburg
Hamburg, Germany
t.schmidt@haw-hamburg.de

Matthias Wählisch
TU Dresden
Dresden, Germany
Barkhausen Institut
Dresden, Germany
m.waehlisch@tu-dresden.de

EXTENDED ABSTRACT

Motivation and Background The constrained Internet of Things (IoT) is characterized by only a few hundreds of kilobytes of available persistent and non-persistent memory and by networking technologies that have low throughput, high packet loss, and asymmetric link characteristics [1]. Current approaches to enable secure and privacy-friendly name resolution, such as DNS over HTTPS, DNS over QUIC, and even DNS over DTLS, conflict with these constraints [2]. Consequently, these approaches are not suitable.

We propose DNS over CoAP (DoC) to allow for *encrypted* DNS in constrained environments. DoC is adopted by the IETF [3] and has been extensively evaluated [2]. Our proposal features RESTful communication by using the Constrained Application Protocol (CoAP) [5], which provides communication principles similar to HTTP (see Figure 1).

Objective The aim of this presentation is twofold. First, we want to raise further awareness of DoC to identify new questions of interest to researchers and operations in the context of constrained but secure name resolution. Second, we want to discuss gaps in datasets we identified while trying to better understand the potentials of constrained name resolution for the broader Internet.

Outline In detail, we present our evaluation of different design choices of DoC. Our findings indicate that plain DoC is on par with common DNS solutions for the constrained IoT but significantly outperforms other encrypted solutions (*e.g.,* DTLS) when combining DoC with object security using OSCORE. With OSCORE, we can save more than 10 kBytes of code memory compared to DTLS when a CoAP application is already present (see Figure 2), and retain the end-to-end trust chain with intermediate CoAP proxies, while leveraging features such as group communication or encrypted en-route caching.

We also discuss a more concise DNS message format based on CBOR [4] that utilizes the features of RESTful DNS, allowing a resolver to change the exchanged content type. This new concise message format reduces DNS responses by 50% for the vast majority of requests visible in our DNS data set, compared to common DNS message format.

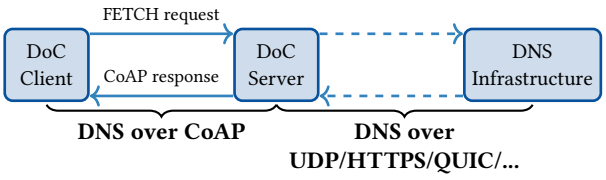
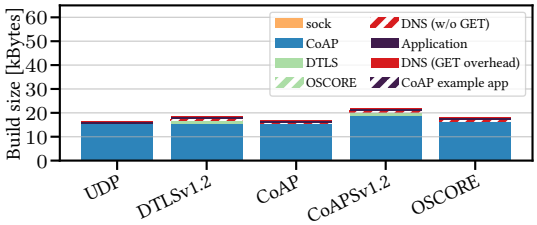
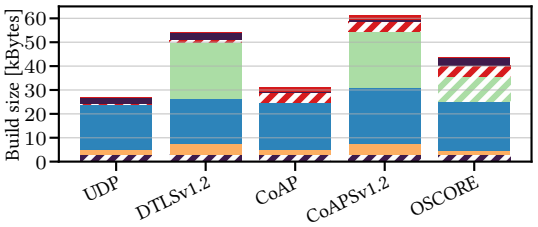


Figure 1: Basic DNS over CoAP (DoC) architecture



(a) RAM



(b) ROM

Figure 2: Memory consumption of each DNS transport with existing CoAP example application.

REFERENCES

[1] C. Bormann, M. Ersue, and A. Keranen. 2014. *Terminology for Constrained-Node Networks.* RFC 7228. IETF. https://doi.org/10.17487/RFC7228

[2] Martine S. Lenders, Christian Amsüss, Cenk Gündogan, Marcin Nawrocki, Thomas C. Schmidt, and Matthias Wählisch. 2023. Securing Name Resolution in the IoT: DNS over CoAP. *Proceedings of the ACM on Networking (PACMNET)* 1, CoNEXT2 (September 2023), 6:1–6:25. https://doi.org/10.1145/3609423

[3] Martine Sophie Lenders, Christian Amsüss, Cenk Gündoğan, Thomas C. Schmidt, and Matthias Wählisch. 2023. *DNS over CoAP (DoC).* Internet-Draft – work in progress 05. IETF. https://datatracker.ietf.org/doc/html/draft-ietf-core-dns-over-coap-05

[4] Martine Sophie Lenders, Carsten Bormann, Thomas C. Schmidt, and Matthias Wählisch. 2023. *A Concise Binary Object Representation (CBOR) of DNS Messages.* Internet-Draft – work in progress 06. IETF. https://datatracker.ietf.org/doc/html/draft-lenders-dns-cbor-06

[5] Z. Shelby, K. Hartke, and C. Bormann. 2014. *The Constrained Application Protocol (CoAP).* RFC 7252. IETF. https://doi.org/10.17487/RFC7252