



HAL
open science

Enhancing Security for Constrained IoT Devices with Lightweight Remote Attestation

Yuxuan Song, Mališa Vučinić, Thomas Watteyne

► **To cite this version:**

Yuxuan Song, Mališa Vučinić, Thomas Watteyne. Enhancing Security for Constrained IoT Devices with Lightweight Remote Attestation. Journée commune au GDR RSD, GPL (GT GLSEC) et SI (GT SSLR) sur la sécurité des piles réseau, Sep 2024, Orléans, France. hal-04716799

HAL Id: hal-04716799

<https://inria.hal.science/hal-04716799v1>

Submitted on 1 Oct 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

Enhancing Security for Constrained IoT Devices with Lightweight Remote Attestation

Yuxuan Song, Mališa Vučinić, Thomas Watteyne
Inria Paris, France
first.last@inria.fr

Abstract—We propose a lightweight remote attestation protocol designed specifically for resource-constrained IoT devices. The proposed solution enables attestation alongside mutual authentication, while reducing computational and energy costs by utilizing a newly standardized key exchange protocol called EDHOC (Ephemeral Diffie-Hellman Over COSE).

I. INTRODUCTION

As IoT devices become ubiquitous, they are increasingly targeted by cyberattacks, making it crucial to verify their software and hardware configurations before they are admitted into a network. Remote attestation provides a way to verify device integrity and trustworthiness. The remote attestation process involves three entities: the *Attester*, which generates evidence of its state; the *Verifier*, which evaluates this evidence and generates the attestation results; and the *Relying Party*, which acts based on the attestation results.

Traditional protocols are not practical for low-power IoT devices due to memory and energy constraints. This abstract proposes a lightweight remote attestation integrated into a newly standardized authenticated key exchange protocol EDHOC, designed for resource-limited environments.

II. EPHEMERAL DIFFIE-HELLMAN OVER COSE (EDHOC) PROTOCOL

EDHOC [1], standardized by the Internet Engineering Task Force (IETF), is a key exchange protocol with three mandatory messages and an optional fourth message. The execution takes place between an Initiator and a Responder. Fedrecheski *et al.* [2] demonstrated that EDHOC offers performance advantages over the DTLS 1.3 protocol in constrained environments.

EDHOC allows external security applications to be incorporated via the External Authorization Data (EAD) fields. EAD items are sent in dedicated fields of the EDHOC messages: EAD_1, EAD_2 and EAD_3.

III. REMOTE ATTESTATION OVER EDHOC

Remote attestation typically involves three entities. The *Attester* provides reliable evidence about the state of itself. The *Verifier* evaluates the evidence and produces attestation results. The *Relying Party* consumes the attestation results to execute application-specific actions.

The EDHOC session is always between the *Attester* and the *Relying Party*. We integrate remote attestation within the EDHOC handshake, with three distinct modes: forward, reverse and mutual attestation [3].

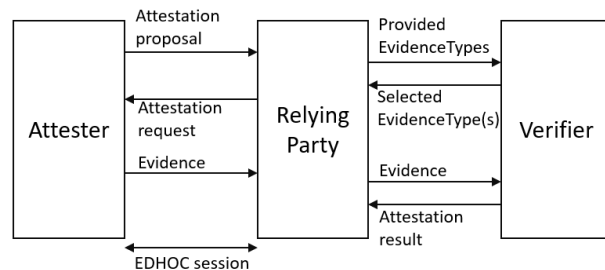


Fig. 1. Overview of message flow.

A. Forward Remote Attestation

Forward attestation occurs when the *Attester* (an IoT device) proves its integrity to a *Relying Party* (Fig. 1). The *Attester* starts the remote attestation with an attestation proposal in EDHOC’s EAD_1 field, which contains all the supported evidence types. If the *Relying Party* supports a proposed evidence type, it signals to the *Attester* an attestation request in EDHOC’s EAD_2 field. The *Attester* then provides evidence to the *Relying Party* in EDHOC’s EAD_3 field.

B. Reverse Attestation

Reverse attestation is used when the IoT device requires assurance of the server’s integrity before sharing sensitive data. The server acts as the *Attester* and starts the reverse attestation by listing *Verifier* identities in EAD_1, from which it can get the attestation result. The IoT device acting as the *Relying Party* selects a trusted *Verifier* and informs the server, which then retrieves and forwards the attestation result.

C. Mutual Attestation

Mutual attestation enables both the IoT device and server to verify each other’s integrity, combining forward and reverse attestation by using multiple EAD items within EDHOC.

IV. CONCLUSION

This abstract presents an efficient approach to integrate remote attestation with network authentication using EDHOC, making it suitable for constrained IoT networks.

REFERENCES

- [1] G. Selander, J. Preuß Mattsson, and F. Palombini, *Ephemeral Diffie-Hellman Over COSE (EDHOC)*, Internet Engineering Task Force (IETF) Std. RFC9528, 2024.
- [2] G. Fedrecheski, M. Vučinić, and T. Watteyne, “Performance Comparison of EDHOC and DTLS 1.3 in Internet-of-Things Environments,” in *IEEE Wireless Communications and Networking Conference*, 21-24 April 2024.
- [3] Y. Song, *Remote attestation over EDHOC*, Internet Engineering Task Force (IETF) Std. draft-song-lake-ra-01, 2024.