Ph.D. Forum: Enhancing EDHOC Protocol with Pre-Shared Key Authentication

Elsa Lopez Perez

Ph.D. Forum: Enhancing EDHOC Protocol with Pre-Shared Key Authentication

Elsa Lopez Perez
elsa.lopez-perez@inria.fr
Inria
Paris, France

ABSTRACT

This paper explores preliminary research on improving the Ephemeral Diffie-Hellman Over COSE (EDHOC) protocol by incorporating a new pre-shared key (PSK) authentication method. The research focuses on designing this PSK-based mechanism and its potential benefits, such as enhancing session key update efficiency and reducing computational demands compared to current EDHOC authentication methods. We also outline the planned implementation and evaluation approach, which will measure key performance indicators like memory consumption, energy consumption, handshake duration, message size or number of operations. The aim is to optimize EDHOC for secure communication in resource-limited environments.

KEYWORDS

Pre-Shared Key, Security, Privacy, Wireless Communication, Lightweight

ACM Reference Format:
Elsa Lopez Perez. 2024. Ph.D. Forum: Enhancing EDHOC Protocol with Pre-Shared Key Authentication. In *Proceedings of ACM Conference (Conference'17).* ACM, New York, NY, USA, 3 pages. https://doi.org/XXXXXXX.XXXXXXX

INTRODUCTION

Motivation

The rapid expansion of the Internet of Things (IoT) has driven organizations like the Internet Engineering Task Force (IETF) to develop protocols specifically tailored to the unique needs of IoT devices and networks. Key challenges in these environments include limited bandwidth, minimal memory, sporadic communication with potential delays of several seconds, small maximum transmission units, and limited processing power.

To address these issues, the Internet community has developed and standardized protocols optimized for resource-constrained environments, such as the Object Security for Constrained RESTful Environments (OSCORE). OSCORE is a security protocol that secures CoAP (Constrained Application Protocol) communications by providing end-to-end encryption, integrity protection, replay prevention, and the ability to bind responses to requests across CoAP proxies.

While OSCORE secures communication, it lacks a key establishment mechanism. To address this limitation, the IETF's Lightweight Authenticated Key Exchange (LAKE) Working Group developed Ephemeral Diffie-Hellman Over COSE (EDHOC), a key exchange protocol designed to work within these constraints.

EDHOC: Key Concepts and Features

EDHOC is a compact handshake protocol that incorporates elements from OSCORE, including the Concise Binary Object Representation (CBOR) and CBOR Object Signing and Encryption (COSE). This design choice results in reduced message sizes. Key features of EDHOC include: handshakes with messages around 100 bytes in size, only three mandatory flights, it is transport-agnostic, and allows the code size to be low by reusing the same elements as OSCORE.

Recent research indicates that EDHOC offers significant improvements over DTLS 1.3. In particular, Fedrecheski *et al.* [1] show that EDHOC achieves a 7.75× reduction in message footprint, 1.9× reduction in energy and time, and uses up to 4× less flash and RAM than DTLS 1.3.

EDHOC's cryptographic foundation is based on the SIGMA-I protocol, specifically the MAC-then-Sign variant. SIGMA protocols are a family of key-exchange methods that use a combination of digital signatures and message authentication codes (MACs) to create authenticated Diffie-Hellman (DH) protocols.

The SIGMA-I variant provides active attacker protection for the session initiator (Initiator), and passive attacker protection for the responding peer (Responder). The MAC-then-Sign approach incorporates the MAC within the signature to minimize message size.

EDHOC supports both conventional signature keys and static Diffie-Hellman keys for authentication. The "authentication method" is specified in the initial message and determines the key types used by each peer, resulting in 4 possible methods.

The EDHOC protocol consists of three mandatory message exchanges, an optional fourth message, and an error message when needed.

Pre-shared Key Authentication in EDHOC

PSK authentication methods are gaining importance due to the widespread deployment of SIM cards and their use in modern cellular networks, such as the 5G Authentication and Key Agreement protocol.

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/XXXXXXX.XXXXXXX

EDHOC offers several advantages for next-generation network adoption. It can potentially be implemented through software updates, making it a cost-effective solution compared to replacing existing SIM cards. Furthermore, EDHOC allows for a gradual transition, as it can be implemented alongside existing PSK methods.

However, the adoption of EDHOC introduces new challenges, particularly in key management. EDHOC achieves forward secrecy through frequent rekeying, which can be resource-intensive for IoT devices. A hybrid PSK-EDHOC approach addresses this issue by maintaining the security benefits of ephemeral key exchange while reducing overhead for resource-constrained devices. In this approach, PSKs serve as a long-term root of trust, enabling lightweight key refreshes without the need for complete EDHOC exchanges.

This hybrid approach also facilitates the creation of group keys or hierarchical key structures, allowing for more efficient rekeying processes in large IoT networks.

Research Objective

Current developments in the Internet Engineering Task Force (IETF) are focused on integrating PSK authentication into EDHOC. The Lightweight Authentication and Key Exchange (LAKE) working group is developing two proposed variants, referred to as PSK1 and PSK2 and described in the Internet Draft [3]. The first part of the project was to perform a state-of-the-art to give an overview of EDHOC protocol, highlighting the improvements that have been done as a consequence of the formalization process (see Elsa *et al.* [2]). As a second step, the goal is to compare these variants based on their security properties, performance metrics, and implementation complexity in order to rule one out and proceed with the formalization and standardization in within the Working Group.

METHODOLOGY

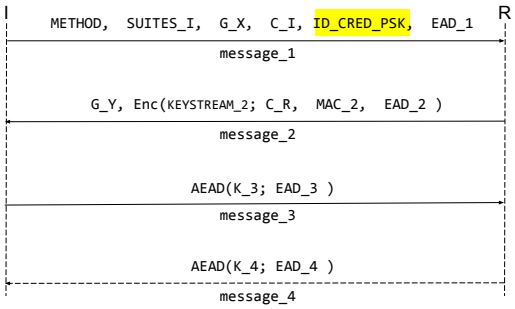
Our research aims to develop a PSK authentication method for EDHOC. We have defined two approaches, named PSK1 and PSK2, each with distinct security and privacy considerations. PSK1 follows the structure of TLS 1.3, transmitting the ID_CRED_PSK in message_1 unencrypted, with the Responder authenticating first. PSK2 deviates from TLS 1.3 by sending the ID_CRED_PSK in message_3, encrypted using a key derived from the ephemeral shared secret G_XY, with the Initiator authenticating first. Figure 1 describes the message flow of both variants.

To evaluate the performance of these approaches and compare them with existing authentication methods, we are integrating them into the current Rust implementation of EDHOC called *lakers* .[1]

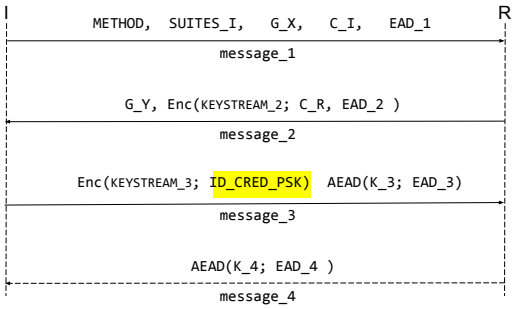
EVALUATION

Our evaluation of the PSK authentication method in EDHOC will involve measuring the mentioned metrics across different experimental setups, using both hardware and software platforms. The nRF52840-DK and nRF5340-DK development kits, featuring state-of-the-art chips, will be used to run our code.

[1] https://github.com/openwsn-berkeley/lakers



(a) Message flow of EDHOC with symmetric keys. PSK1.



(b) Message flow of EDHOC with symmetric keys. PSK2.

Figure 1: Message flow of EDHOC with PSK.

Key performance indicators include energy consumption, measured using the OTII power measurement tool; memory consumption, including both flash and RAM memory; and message size, monitored using a network analyzer tool called Wireshark.

Security evaluation will assess threats, cryptographic strength, protocol resilience, and resistance to known attacks, using formal verification and implementation testing.

Privacy assessment will review data handling, access controls, user consent, and transparency, ensuring compliance with privacy regulations. Privacy impact assessments, third-party audits, and user feedback will guide improvements.

CONCLUSION

The EDHOC protocol with PSK authentication presents a robust solution for secure key exchange in constrained environments. By leveraging pre-shared keys, it ensures strong mutual authentication and forward secrecy while remaining simple to implement and scalable. The adoption of EDHOC with PSK has the potential to enhance the security and reliability of IoT networks, promote interoperability, and drive standardization across industries, making it a valuable tool for securing communications in resource-limited settings.

REFERENCES

[1] Geovane Fedrecheski, Mališa Vučinić, and Thomas Watteyne. 2024. Performance Comparison of EDHOC and DTLS 1.3 in Internet-of-Things Environments. In *IEEE Wireless Communications and Networking Conference (WCNC)*. Dubai, United Arab Emirates.

[2] Elsa Lopez Perez, Göran Selander, John Preuß Mattsson, Thomas Watteyne, and Mališa Vučinić. 2024. EDHOC is a New Security Handshake Standard: Overview of Security Analysis. *IEEE Computer Magazine* (2024). [Manuscirpt submitted for publication].

[3] Elsa Lopez-Perez, Göran Selander Selander, John Preuß Mattsson, and Rafael Marin-Lopez. 2024. *EDHOC PSK authentication.* Internet-Draft draft-lopez-lake-edhoc-psk-01. Internet Engineering Task Force. https://datatracker.ietf.org/doc/draft-lopez-lake-edhoc-psk/01/ Work in Progress.