Lightweight Authorization using EDHOC

https://datatracker.ietf.org/doc/draft-ietf-lake-authz (diff)

Geovane Fedrecheski, Inria
Contents

● Recap
● Merged PRs
● Proposal: *advertisement* of lake-authz capability
● Input from WG?
Recap: **Lightweight Authorization using EDHOC**

Also referred to as:
- **authz**
- **zero-touch network join**
Merged PRs for -01

- #28 Explain error handling in the VREQ/VRES protocol leg
- #30 Update references now that EDHOC is an RFC
- Marco's review
  - #31 Editorial updates
  - #32 Specify missing CoAP status codes and Content-Format
  - #33 Rename section Problem Description to Outline
  - #38 Credentials and clarifications
- #34 CDDL nits
- #37 Read-through updates
- #39 Fix contact for media type registration
Proposal: Advertising lake-authz support
Context

Problem at -00 version:
● blind attempts may lead to several retries

Proposal at -01:
● have U and W share hints to minimize retries

Issues discussed in the working group:
● privacy of sending network identifiers around
● increased message footprint
Advertise: have V tell U about lake-authz support (send V_INFO)

\[ V_INFO = \]
\[ ("I support lake-authz", "I am part of acme.com") \]

Impact: enrollment attempt sent directly to supported gateway

But how exactly? (next slide)
Two approaches

A1  **Layer two** beacons and EDHOC *forward* flow

A2  **CoAP** anycast/response and EDHOC *reverse* flow
Layer two beacons and EDHOC forward flow

use of L2 beacons to carry V_INFO
- assumes extensible L2 at the beacon level
  - includes: IEEE 802.15.4, raw BLE
- optional trigger packet
  - needed by some L2, including non-beaconed IEEE 802.15.4 and BLE with GATT

EDHOC forward message flow
- no change to current state, except that a previous discovery phase is added
- CoJP appendix already considers discovery; the difference here is the addition of V_INFO
**CoAP anycast/response and EDHOC reverse flow**

**Use of CoAP to carry V_INFO**
- assumption: L2 allows transporting packets before enrollment takes place
  - works with: raw BLE, BLE with GATT
- automatic filter: V’s that do not support lake-authz will simply not respond

**EDHOC reverse message flow**
- U = Responder, and V = Initiator
- msg_1 carried in the CoAP response
- V_INFO sent in EAD1
- Voucher_Info carried in EAD2 and Voucher in EAD3
Discussion and impacts

1. Layer two profiling
   a. **A1**: requires updates in beacons to carry V_INFO, one profile per L2 technology
   b. **A2**: may or may not require L2 profiling, as CoAP messages can be just sent as payloads

2. **A1** is a smaller change

3. **A2** allows for EDHOC msg_1 and V_INFO in same packet

4. **A2** requires CoAP communication **before enrollment**

5. **A2** uses the EDHOC reverse flow
   a. is it **commonly deployed**? any impact on **implementations**?
   b. stronger identity protection for V than for U

6. **A2** offers better protection for some fields
   a. Voucher_Info: sent in the clear in A1, but confidentiality-protected in A2
   b. Voucher: confidentiality-protected in A1, but confidentiality and integrity -protected in A2

7. looking forward to WG input
Thank you!

https://datatracker.ietf.org/doc/draft-ietf-lake-authz

geovane.fedrecheski@inria.fr