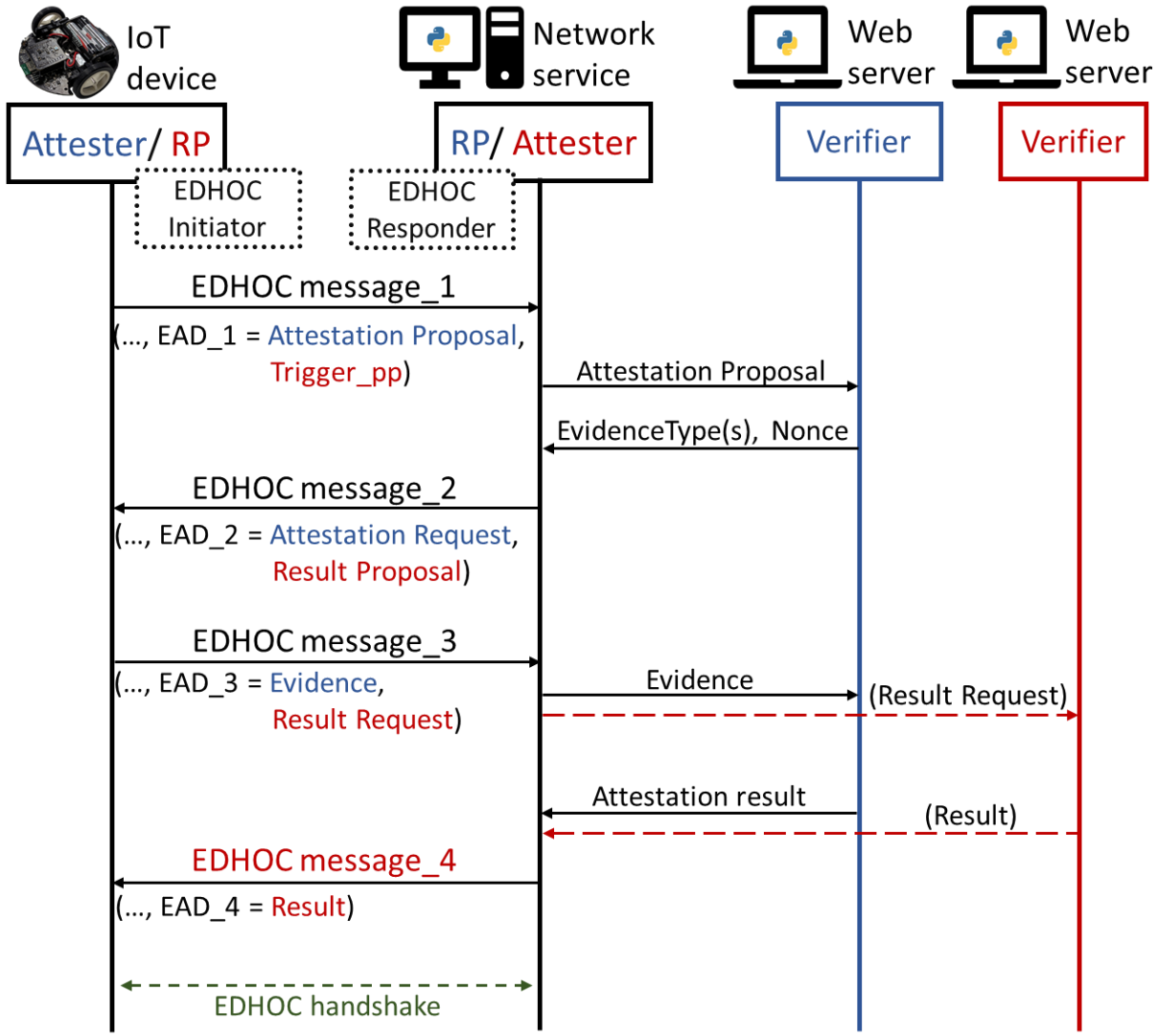
Remote attestation over EDHOC draft-ietf-lake-ra-02

Yuxuan Song, Inria

Göran Selander, Ericsson

Recap

The draft specifies how to perform remote attestation by using EDHOC EAD fields to carry attestation elements.



Since IETF122

- addressed open issues based on feedback
- 8 issues closed
- 2 issues remain open
  - continuous attestation
  - combine lake-authz and lake-ra

#11 New Section: Verifier

- Processing in the background-check model
  - Verifier generates a nonce and selects supported evidence type(s), then sends both elements back to the Relying Party for constructing the Attestation_request.
  - Verifier evaluates the Evidence (with detailed steps to follow), where the Evidence is a signed EAT within a COSE_Sign1 structure.

- Processing in the passport model
  - If the Attester sends a cached attestation result, the Verifier does not perform any real-time processing.
  - If real-time attestation is required (indicated by the inclusion of a nonce in the Result_request), then the Verifier needs to generate an attestation result formatted as an EAT.

#13 Deleted Error Handling section

- The case where attestation completes with a failed attestation result is not considered an error.

- The following EAD items are defined as critical:
  - Attestation_proposal
  - Attestation_request
  - Evidence

#14,15,16,18 Clarifications and editorials

- Explanation of all the possible instantiations
  - the focused examples in this draft are: (IoT, BG, Fwd), (Net, PP, Fwd)

- Explanation of ead_label value settings
  - ead_label TBD1 is used for EAD items: Attestation_proposal, Attestation_request, Evidence
  - ead_label TBD3 is used for EAD items: Result_proposal, Result_request, Result
  - reason: these EAD items can only appear in a fixed sequential order

#17 Reduced the section hierarchy depth

- make EAD items visible in the table of contents

#19 added support for Nonce in Result_request

OLD:

```
Result_request = bstr .cbor Request_structure

Request_structure = {
  selected_verifier: VerfierIdentity
}
```

NEW:

```
Result_request = bstr .cbor Request_structure

Request_structure = (
  selected_verifier: VerfierIdentity,
  ? nonce: bstr .size 8..64
)
```

Thank you!

Open for more discussions and collaborations: yuxuan.song@inria.fr

https://github.com/lake-wg/ra

Welcome any comments and advice ☺