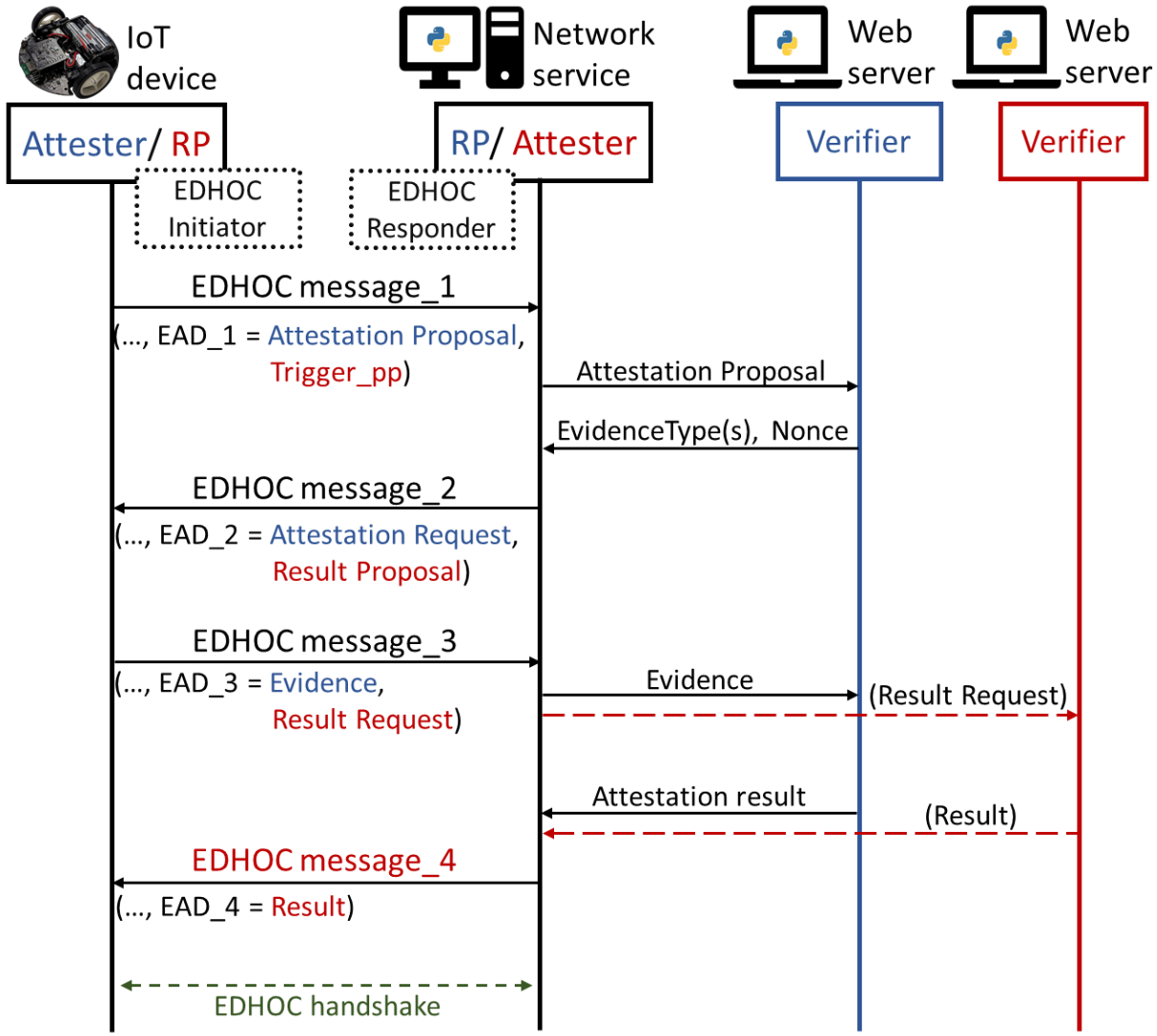
Remote attestation over EDHOC draft-ietf-lake-ra-04

Yuxuan Song, Inria

Göran Selander, Ericsson

Recap

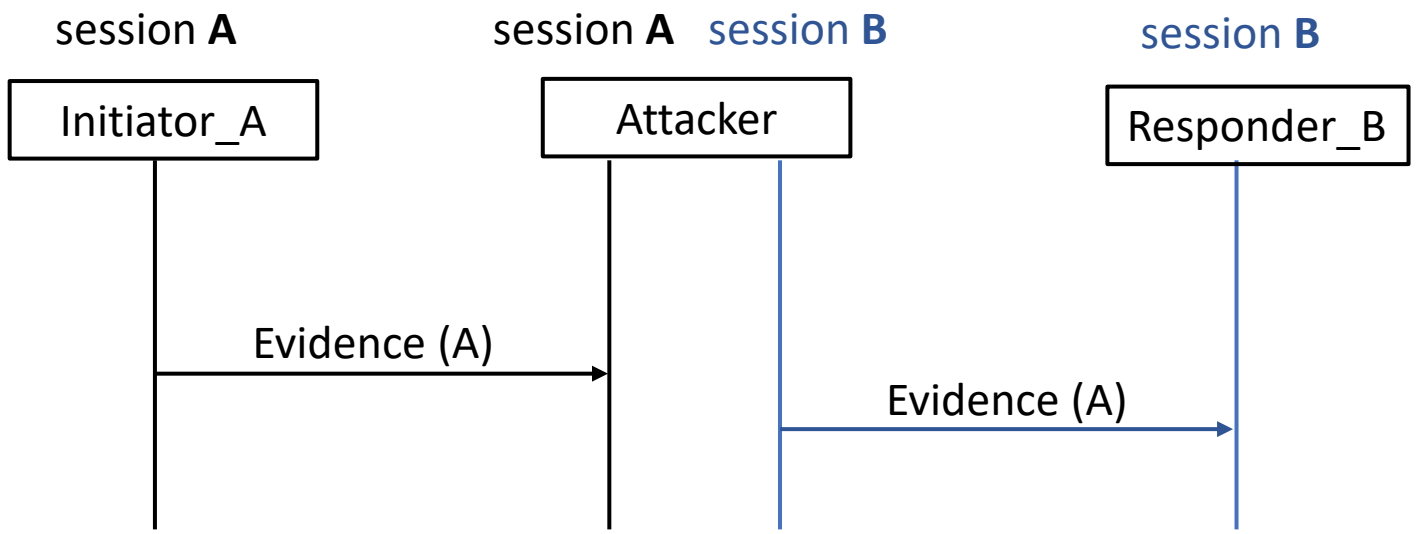
The draft specifies how to perform remote attestation by using EDHOC EAD fields to carry attestation elements.



#36 Channel binding does not hold in lake-ra-03

- Based on the formal verification results:
  - The attestation evidence is not bound to the authentication session

Attack when authentication key leaks: the Attester who generates the evidence is not guaranteed to be the Initiator who authenticates.



Mitigation: attestation binder

Case Attester as Initiator:

- when evidence is sent in EAD_3 (EDHOC message_3):

```
attestation_binder = H(message_1, message_2)
```

  where H() is the EDHOC hash algorithm of the selected cipher suite.

- because of implementation considerations and alignment with lake-authz, we will change to:

```
attestation_binder = H(H(message_1), message_2)
```

The attestation_binder is included in the evidence, signed by the attestation key

Mitigation: attestation binder

Case Attester as Responder:

- when evidence is sent in EAD_4 (EDHOC message_4):

```
attestation_binder = EDHOC_Exporter (exporter_label, context, length)
```

where

- exporter_label = 2
- context = "attestation_binder"
- length = 32

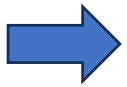
The attestation_binder is included in the evidence, signed by the attestation key

#21 Validate snippets

- fixed the CDDL errors throughout the draft

```
Attestation_request = bstr .cbor Selected_EvidenceType

Selected_EvidenceType = (
  content-format: uint,
  nonce: bstr .size 8..64
)
```



```
Attestation_request = bstr .cbor Selected_EvidenceType

Selected_EvidenceType = (
  content-format: uint,
  nonce: bstr .size (8..64)
)
```

- validate CDDL as part of CI?

#23, 29, 34 Clarifications and editorials

- Explain the difference between the background-check model and the passport model
- Add RATS part in privacy consideration
- Add the requirement of the ability to generate random nonce

Thank you!

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

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

Welcome any comments and advice ☺