Remote attestation over EDHOC
draft-song-lake-ra-01

Yuxuan SONG
Inria
Recap: version-00

- Forward attestation in Background-check model
  - Use case: An IoT device remotely attests its firmware version to a server for network access.
  - Three EAD items: Attestation_proposal, Attestation_request, Evidence

- RATS Background-check model
  RATS: Remote ATtestation procedureS [1]

- message flow

• Different message flows
  • forward attestation
  • reverse attestation (new)
  • mutual attestation (new)

• Consider two RATS architectures
  • Background-check model
  • Passport model (new)

• New EAD items for passport model

• New EDHOCS Error "Attestation failed"
Attestation in passport model

**Process over EDHOC:**
The Attester proposes Verifier identities from which it can relay the attestation result.
The Relying Party selects a trusted Verifier identity in common and gets the attestation result.

**EAD items:**
**Result_proposal**

```plaintext
Result_proposal = bstr .cbor ProposedVerifierIdentity
ProposedVerifierIdentity = [ + VerifierIdentity ]
```

VerifierIdentity = {
  label => values
}  # similar to ID_CRED, from COSE Header Param. registry

**Result_request**

```plaintext
Result_request = bstr .cbor Request_structure
Request_structure = {
  selected_verifier: VerifierIdentity
}
```

Result is a serialized EAT (Entity Attestation Token).
Reverse attestation

• Use case: A server attests remotely to gain the device's trust and retrieve its sensitive data.
• over reverse EDHOC message flow

Seeking input from the WG: the feasibility of both the background-check model and the passport model

In background-check model:
Reverse attestation

In passport model:

-seeking input from the WG:

What kind of freshness is expected for the attestation result?

1. Fresh attestation result with nonce a new remote attestation is performed after receiving Result request

2. Pre-stored attestation result with timestamp

the attestation result is stored at the Verifier with a timestamp indicating the generation time
Mutual attestation:

**Background-check — Background-check** (seeking input from the WG on feasibility)
- for devices with no connectivity constraints

![Diagram of attestation process]

- **EAD_1** = Attestation proposal
- **EAD_2** = Attestation request, Attestation proposal
- **EAD_3** = Evidence, Attestation request
- **EAD_4** = Evidence

Diagram notes:
- **A / RP** device
- **RP / A** Server
- **EDHOC session**
- **Verifier**
- **Provided EvidenceTypes**
- **Selected EvidenceType(s)**
- **Evidence**
- **Attestation result**
Mutual attestation:

Background-check — **passport** (seeking input from the WG on feasibility)

- for constrained devices with connectivity problem

A / RP  | device  | RP / A  | Server  | Verifier
---|---|---|---|---
Initiator | EDHOC session | Responder |  |  

EAD_1 = Attestation proposal

EAD_2 = Attestation request, Result proposal

EAD_3 = Evidence, Result request

EAD_4 = Result

Provided EvidenceTypes

Selected EvidenceType(s)

Evidence

Attestation result

Result
New error: Attestation failed

<table>
<thead>
<tr>
<th>ERR_CODE</th>
<th>ERR_INFO Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBD7</td>
<td>attestation</td>
<td>Attestation failed</td>
</tr>
</tbody>
</table>

To indicate to the receiver that the remote attestation failed after the evidence is sent.

The error will be sent in two cases:
1. Verifier evaluates the evidence and generates a negative attestation result
2. Relying Party cannot establish a sufficient level of trust to proceed with decision-specific actions.

Relying Party generates the error, the application layer decides how to handle the error message.
Conclusion

• Defined three attestation flows
  • forward attestation
  • reverse attestation
  • mutual attestation

• Applied on two RATS architectures
  • Background-check model
  • Passport model

• EDHOC error: Attestation failed

• Looking for inputs from the WG
  • freshness type of attestation result, reverse attestation, mutual attestation, or any other advice.
Thank you!

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

https://github.com/ysong02/draft-song-lake-ra

Welcome any comments and advice 😊