EAP-NOOB Observations and EAP-UTE

`draft-rieckers-emu-eap-noob-observations`

`draft-rieckers-emu-eap-ute`

Jan-Frederik Rieckers

German National Research and Education Network

IETF 113 – emu WG

EAP-NOOB Observations

- JSON as payload encoding
  - Strings as map keys → long messages
  - Canonicalization necessary for deterministic MAC/Hoob calculation
  - Possible deep structure in ServerInfo/PeerInfo, needs to be replicated exactly for MAC/Hoob
- Unclear/Ambiguous Status of ServerInfo/PeerInfo
  - Sec. 3.3.2: „The format and semantics of these objects MUST be defined by the application that uses the EAP-NOOB method.“
  - Sec. 5.4/5.5: IANA Registry definitions for Data Fields with „Specification Required“
  - Sec. 6.7: „The peer MAY include in PeerInfo any data items that it wants to bind to the EAP-NOOB association and to the exported keys.“

EAP-NOOB Observations

- Number of messages
  - First message from server to peer has no information, first message from peer to server transmits only PeerId and PeerState
  - Possibility to reduce by at least one roundtrip
- Editorial nit: Version is never explicitly defined as 1

EAP-UTE (User-assisted Trust Establishment)

- Same design principle as EAP-NOOB
- CBOR as payload encoding
  - Integer as map keys → shorter messages
  - No need for Base64-encoding of byte strings
- MAC-Calculation over whole messages, communication partners do not need to understand all protocol fields

Current state of EAP-UTE

- -00 version is a very early draft version
    - Part of a Masters project at the University of Bremen, will be developed further in the next months
    - still a lot of questions
- Some modifications done already
    - Removed MAC from the Initial Exchange (no need for it there)
    - Finalized first specification of MAC calculation and KDF for the Completion Exchange
- Completely open questions:
    - Specification of Cipher Suites
        - Piggyback on existing registries (e.g. COSE Elliptic Curves)
        - Separate EC and Hash or maybe even define one fixed Hash function?

Questions/Discussion

Contact:
rieckers@(dfn|uni-bremen).de