EAP-NOOB Observations and EAP-UTE

draft-rieckers-emu-eap-noob-observations[1]

draft-rieckers-emu-eap-ute

Jan-Frederik Rieckers

German National Research and Education Network

IETF 115 – emu WG

[1] Expired draft (only -00 published), with no intention to be an RFC some day

DFN DEUTSCHES FORSCHUNGSNETZ

Universität Bremen

EAP-NOOB Observations

- JSON as payload encoding
  - Strings as map keys → long messages
  - Some form of 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

- High 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 sequence/map as payload encoding
  - Integer as map keys $\rightarrow$ 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

- -01 published
- more or less complete specification of the base protocol
- Still a lot of TODOs in the draft
  - Definition of extensions
  - Security Considerations
  - ...
- Initial/Completion Exchange implemented in ESP-IDF with own EAP-UTE server

Questions/Discussion

- Is this a possible/useful work item for emu?
- If so: Should this be a separate protocol or aim for EAP-NOOB v2?
- Other feedback?

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