EAP-NOOB : Nimble Out-of-Band Authentication for EAP

EMU WG, 31 May 2020
Tuomas Aura, Aalto University
Mohit Sethi, Ericsson
various other contributors
EAP-NOOB architecture

Remote AAA

Local AAA

AP

New device

UI or API

EAP in-band

User-assisted OOB channel

OOB output (or input)
e.g. dynamic QR code
EAP-NOOB timeline

draft-ietf-emu-eap-noob

draft-aura-eap-noob

draft-ietf-emu-eap-noob
Changes in since last IETF

• WG Version 01:
  • Add NIST P-256 as Cryptosuite 2
    → Successfully tested ciphersuite update
  • Renumber message types

• WG Version 02:
  • Updated message examples (cross-checked between updated implementations)
  • Many editorial fixes and other updates based on the IoT directorate review by Dave Thaler
  • Text on cloning attacks based on review by Hannes Tschofenig
Many good observations that led to clarifications and improvement of interoperability in the details:

- Explained the benefits of dynamic OOB vs static registration code
- Replaced printer with LED and light bulb as the example of output-only peer device
- Changed MAY to MUST where it makes sense for interoperability
- More precise about character sets, string length, and upper vs lower case hex
- Specifying ServerInfo and PeerInfo? Not before we gain experience of where the protocol is actually used
- To be added: discussion of server UI clogging attacks
Review by Hannes Tschofenig

Challenged us in a friendly way about the goals and assumptions.

• Need to consolidate remarks about not repeating the OOB step and user reset, which are currently scattered around the document

• Added discussion of cloning to security considerations
Early IANA review

• Amanda Baber: “we don't have any issues with the document.”

TODO at the right time:

• Request **EAP method number** from IANA

• Reserve domain name **eap-oob.arpa** for the NAI
JSON vs. CBOR

- CBOR given serious thought but rejected in 2016. However, there has been progress since.
  - Implementations [https://cbor.io/impls.html](https://cbor.io/impls.html)
  - CBOR signatures [RFC 8152](https://tools.ietf.org/html/rfc8152) vs JWK

- *wpa_supplicant* has a built-in JSON encoder and parser.

- Factors to consider:
  - Completeness and stability of the specifications and implementations
  - Major changes like new message encoding cause substantial delay: need to update spec and implementations
  - (Lack of) canonical form that enables extraction of message fields and composing an unambiguous HMAC input

- We need WG advice on this.
EAP-NOOB implementation status

• `wpa_supplicant` and `hostapd` by Aalto University and others:
  https://github.com/tuomaura/eap-noob

• `wpa_supplicant` and `hostapd` by Ericsson:
  https://github.com/Vogeltak
  • Based on the above, refactored code, updated to latest draft

• Contiki:
  https://github.com/eduingles/coap-eap-noob

• Formal models in mCRL2 (protocol and DoS-resistance) and ProVerif (authentication)
Next steps

Only one major open issue:

• Decision on staying with JSON vs changing to CBOR

Editorial TODO:

• Update of security considerations and other explanations based on the recent reviews and other discussions