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

EMU @ IETF 109
20 November 2020

Tuomas Aura, Aalto University
Mohit Sethi, Ericsson
various other contributors
EAP-NOOB overview

• EAP is a generic authentication framework with many methods, **but currently no OOB authentication method**

• EAP-NOOB is a solution for this
EAP-NOOB overview

EAP method for bootstrapping smart devices out-of-the-box without professional administration

• **User-assisted out-of-band (OOB) authentication**
  • E.g. scanning a dynamic QR code, dynamic NDEF tag

• **Registration of authenticated devices to AAA**
  • Create persistent association between AAA and device and authorize network connectivity at the same time

• **Fast reauthentication** of previously registered devices without further user interaction
EAP-NOOB timeline

draft-ietf-emu-eap-noob

Base specification and PoC prototype

Implementation for Linux hostapd and wpa_supplicant

Modeling and verification

Peer implementation in Contiki
EAP-NOOB status summary

• draft-ietf-emu-eap-noob-02 is ready

• Implementations:
  • wpa_supplicant and hostapd
    https://github.com/tuomaura/eap-noob
  • Contiki
    https://github.com/eduingles/coap-eap-noob
  • wpa_supplicant and hostapd
    https://github.com/Vogeltak/hostap

• Formal models in mCRL2 (protocol and DoS-resistance) and ProVerif (authentication)
Updates since IETF 108

• New Deployments –
  • Analog devices worked on an internal PoC and opened two issues on github implementation: https://github.com/Vogeltak/hostap/issues
  • Pull requests fixing minor implementation issues with reconnect exchange: https://github.com/Vogeltak/hostap/pulls

• Several other private email conversations about deployments
CBOR vs JSON

• CBOR is a major change at this late stage given deployments starting to creep up
• While direct JSON-to-CBOR mapping is possible, for real gains a complete re-specification is needed
• EAP-EDHOC (https://tools.ietf.org/html/draft-ingles-eap-edhoc-01) perhaps more suitable for extremely constrained devices and EDHOC is already built with CBOR
• CBOR can be defined in future versions of EAP-NOOB
Next steps

• Early reviews from IoT and Security directorate completed
• IANA is okay with the current requests
• Ready for WG last call?