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

EMU WG virtual interim
22 May 2020

Tuomas Aura, Aalto University
Mohit Sethi, Ericsson
various other contributors

What problems EAP-NOOB solves?

- 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

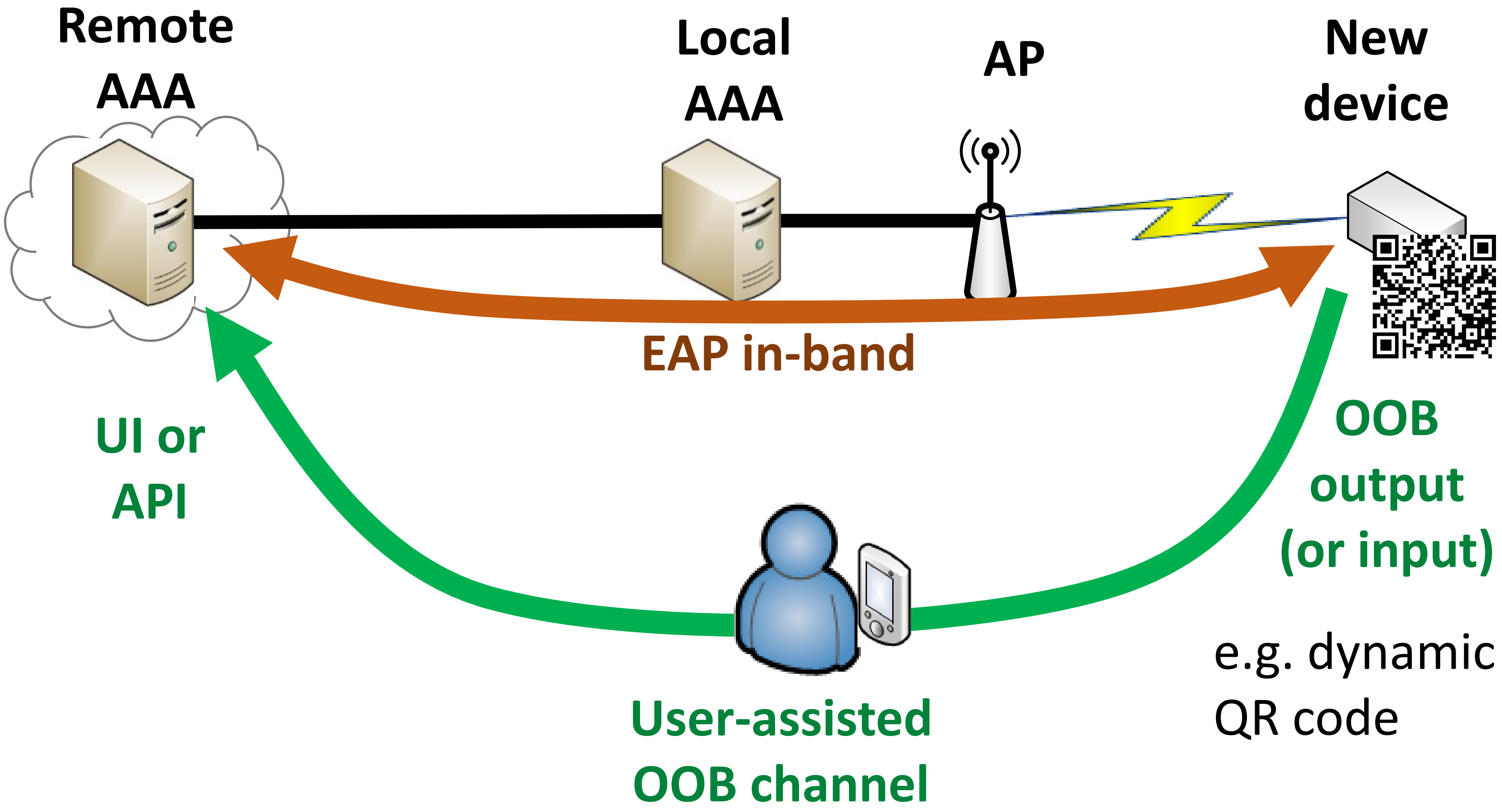
(2-slide refresher)

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

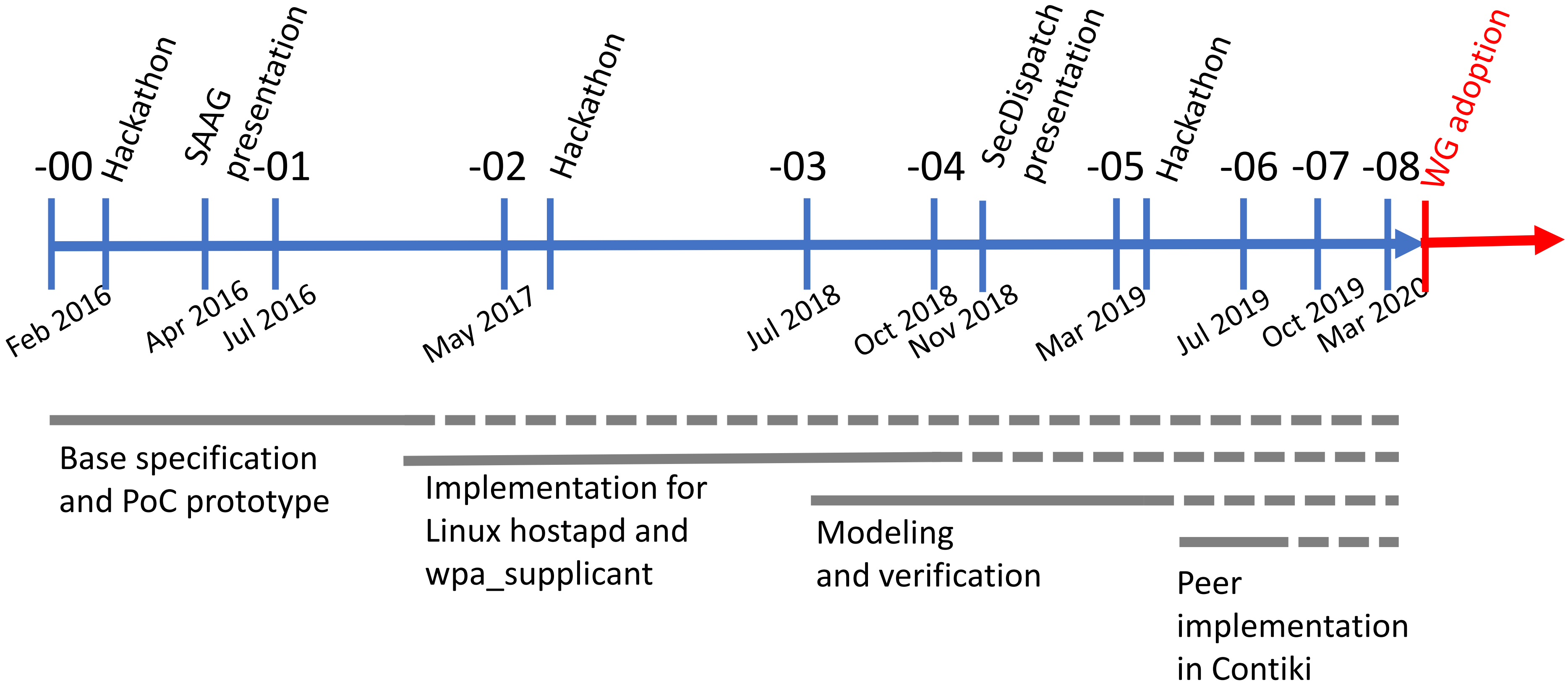
EAP-NOOB architecture

Trick: in-band communication over EAP between peer and server before device is registered



EAP-NOOB timeline

draft-ietf-emu-eap-noob



-00
Feb 2016

Hackathon

SAAG presentation
Apr 2016

-01
Jul 2016

-02
May 2017

Hackathon

-03
Jul 2018

-04
Oct 2018

SecDispatch presentation
Nov 2018

-05
Mar 2019

Hackathon

-06
Jul 2019

-07
Oct 2019

-08
Mar 2020

WG adoption

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-00 is pretty mature
- Implementations:
  - wpa_supplicant and hostapd
    https://github.com/tuomaura/eap-noob
  - Contiki
    https://github.com/eduingles/coap-eap-noob
- Formal models in mCRL2 (protocol and DoS-resistance) and ProVerif (authentication)

Next steps 1

- Defining second ciphersuite
  - Currently ECDHE with Curve25519 and SHA-256
  - Suggestions for the second curve and hash?
- Testing of ciphersuite updates
  - Formal model ok but not tested with running code yet
- Renumbering messages
- Updating implementation to current draft

Next steps 2

What else is still needed before WG last call?

- Reviews
- Request EAP method number from IANA
- IAB allocated domain name for the NAI (noob.arpa or noob.eap.arpa?)