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

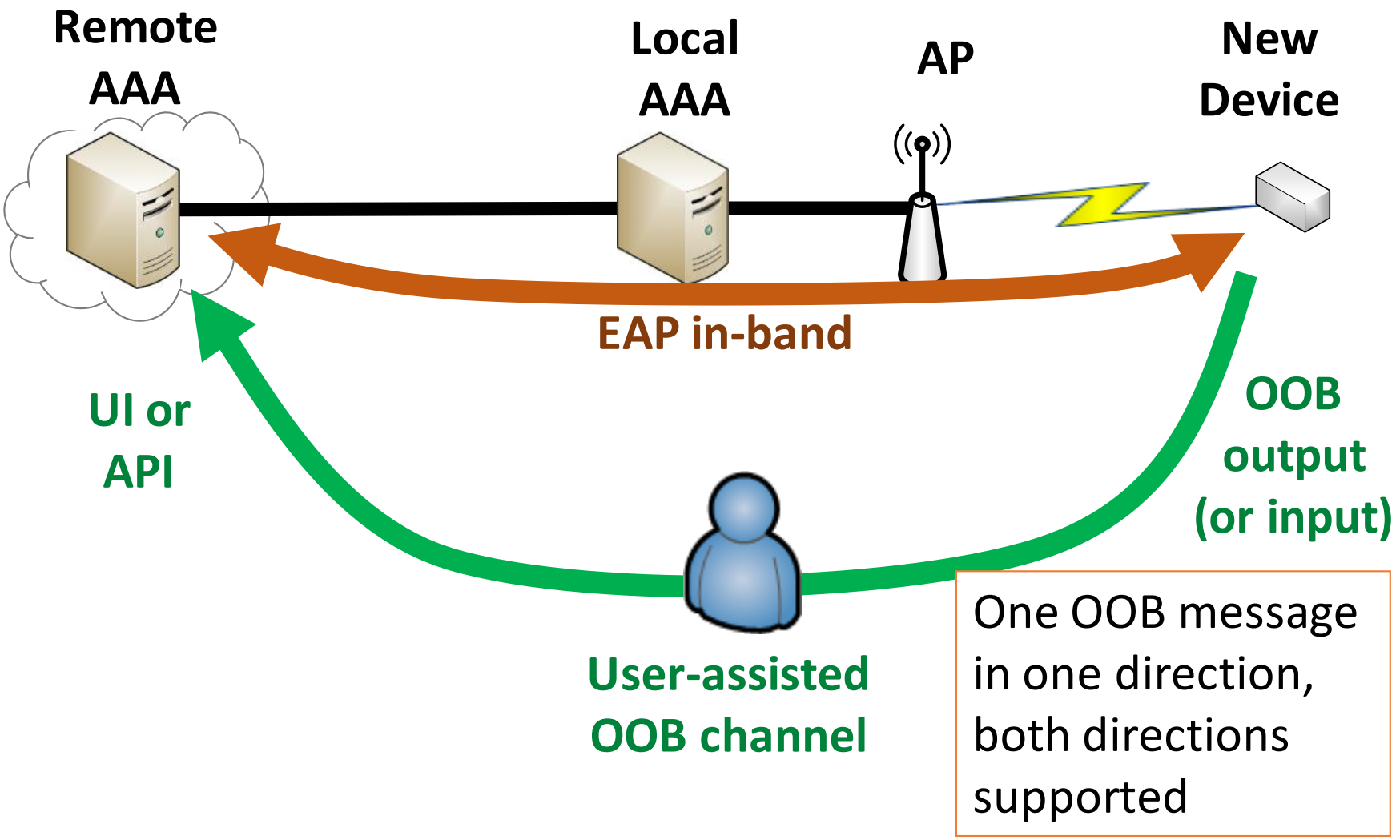
draft-aura-eap-noob

IETF 104 – Hackathon - Prague

What problems EAP-NOOB solves?

- EAP method for deploying devices out-of-the-box without professional administration
- User-assisted out-of-band (OOB) authentication method for EAP
  - E.g. scanning a dynamic QR code, dynamic NDEF tag
  - No such method currently
- Registration of new peer devices
  - Create persistent association between AAA and device
  - Authorize network connectivity
  - Assign an owner (AAA server) to the device
  - Current EAP methods require peer to be pre-registered

EAP-NOOB architecture



One OOB message in one direction, both directions supported

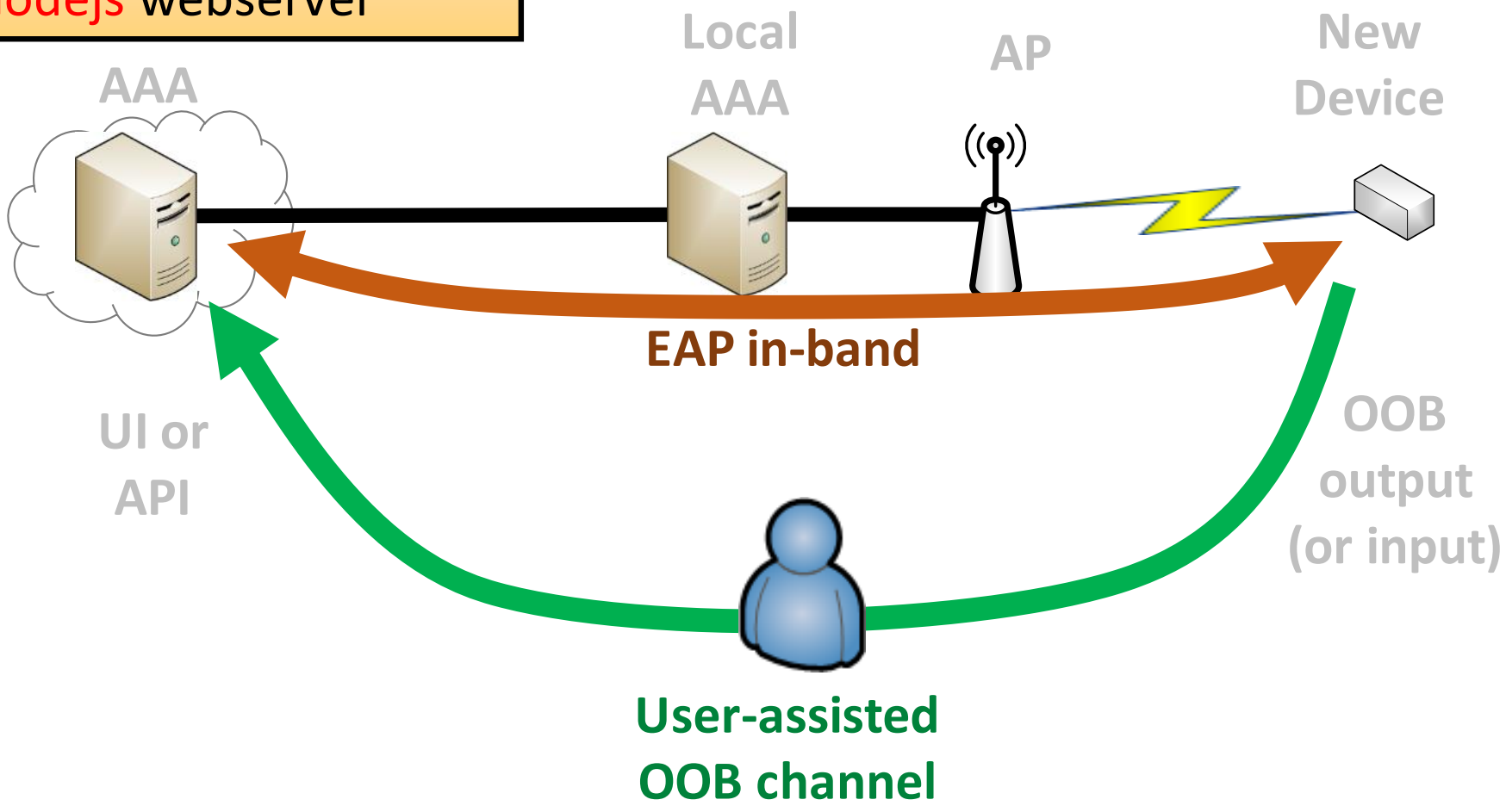
C for EAP server

Python for OOB message parsing

Nodejs webserver

C for EAP peer

Python for scanning networks



Reducing implementation dependencies

- Initial Exchange
- Waiting Exchange
- OOB Step
- Completion Exchange
- Reconnect Exchange

Reducing implementation dependencies

- Initial Exchange
- Waiting Exchange
- OOB Step
- Completion Exchange
- Reconnect Exchange

Lessons

- Discussed path to randomized temporal PeerId
  - Identifier update must be synchronized between peer and server. Must balance anonymity, reliability and server scalability
  - Decided to remove recently added key identifier, which would make future randomization of PeerId useless
- Decided to try adding one roundtrip to each exchange to deliver PeerId and peer state to server without constantly updating NAI
  - Simpler peer implementation in wpa_supplicant
  - Comply better with RFC 3748 section 5.1 guidance
  - Better support for identifier randomization

Team

- Eduardo Inglés Sánchez — First IETF and first hackathon
- Anoop Kumar Pandey — First IETF and first hackathon
- Alex Roscoe — Hackathon Only
- Aleksi Peltonen

- Tuomas Aura
- Mohit Sethi