

IoT Bootstrapping for Noobs with EAP-NOOB

Raghavendra M S, Shiva Prasad T P, Mohit Sethi, Tuomas Aura

- Cloud-connected IoT appliance
- New IoT appliance has **no owner or domain, no credentials** for cloud or Wi-Fi
- Need to
 - Connect the device to access network
 - Register the device to AAA server/cloud
 - EAP-NOOB does both
- Security from a **single user-assisted out-of-band** message between peer device and AAA server



Protocol for new devices:

1. Initial exchange in-band:

ECDH over EAP

2. Out-of-band step: one user-assisted message, in either direction

3. Completion exchange in-band: authentication and key confirmation over EAP

- OOB step not repeated. **Reconnect exchange** for rekeying, algorithm upgrade
- EAP method **implemented** only in AAA/cloud server and peer devices
- **No changes to the Authenticator (AP)**
- **No new code in access-network AAA server**
- **Implemented** with Linux wpa_supplicant and hostapd (server)

