EAP-NOOB : Nimble Out-of-Band Authentication for EAP
— Bootstrapping security for smart appliances

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

IETF 103 SecDispatch
EAP-NOOB: Nimble Out-of-Band Authentication for EAP

draft-aura-eap-noob

- Base specification and PoC prototype
- Implementation for Linux hostapd and wpa_supplicant
- Modeling and verification
What problems EAP-NOOB solves?

• EAP method for deploying IoT devices out-of-the-box, with no pre-configured identity or credentials and without professional administration

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

• One-step process to get Wi-Fi access + register new device
  + link device to user account (optional)
  + bootstrap application-layer security (optional)

• Current EAP methods require peer to be pre-registered
EAP-NOOB architecture

Remote AAA

Local AAA

AP

IoT appliance
EAP-NOOB architecture

EAP tunnel and AAA routing enable in-band communication with the authentication server before the device is registered.
EAP-NOOB architecture

- Remote AAA
- Local AAA
- AP
- IoT appliance

UI or API

EAP in-band

User-assisted OOB channel

One OOB message in one direction, both directions supported

Aura, Sethi: draft-aura-eap-noob
EAP-NOOB protocol

1. Unauthenticated ECDHE key exchange

EAP in-band

User-assisted OOB channel

Remote AAA

Local AP

IoT appliance

UI or API

Unauthenticated ECDHE key exchange

 Aura, Sethi: draft-aura-eap-noob
EAP-NOOB protocol

1. Unauthenticated ECDHE key exchange

2. Hash of ECHDE parameters $H_{oob}$
   Secret nonce $N_{oob}$

Remote AAA

UI or API

Local AAA

AP

IoT appliance

EAP in-band

OOB channel

Aura, Sethi: draft-aura-eap-noob
EAP-NOOB protocol

1. Unauthenticated ECDHE key exchange

2. Hash of ECHDE parameters $H_{oob}$
   Secret nonce $N_{oob}$

3. Key confirmation

EAP in-band

Remote AAA

UI or API

Local AAA

AP

IoT appliance

OOB output (or input)
Rekeying with nonces or ECDHE

EAP in-band

After successful OOB step, persistent association is created. OOB step is not repeated
EAP-NOOB security

Minimal assumptions on OOB channel:

• One OOB message in either direction

• OOB channel may provide only integrity or secrecy
  • If no secrecy, user must note failure of one endpoint to accept the OOB message and reset the other endpoint

Resist denial-of-service by man-in-the-middle:

• Avoid persistent failure caused by limited number of dropped or tampered messages
Use case: secure bootstrapping of cloud-managed displays
EAP-NOOB user experience example

1. User is presented with a login interface.
2. User scans a QR code.
3. User is directed to the Aalto University login page.
4. User logs in to the AAA/cloud account.
EAP-NOOB in the background

1. EAP-NOOB Initial Exchange: ECDHE in-band

2. OOB message: hash + secret

3. EAP-NOOB Completion: key confirmation in-band
Some security design details
OOB message details

• Short and convenient OOB message format

• OOB message contents:
  
  PeerId = server-allocated peer identifier

  Noob = secret nonce (16 bytes)

  Hoob = hash of ECDHE parameters (16 bytes)

• OOB message can be encoded as URL:

  https://example.com/Noob?P=ZrD7qkcNoHGbGcN2bN0&N=rMInS04F4EfCU8D91jxX_A&H=QvnMp4UGxuQVFaXPW_14UW

• URL output e.g. in dynamic QR code or NDEF tag

• OOB security requirements:

  • Noob confidentiality must be protected, or

  • Hoob integrity must be protected
Identifier allocation

• Must not rely on unauthenticated identifiers provided by the device

• Need to avoid identifier squatting

• EAP-NOOB solution:
  • Peer is initially anonymous: fixed NAI noob@eap-noob.net
  • Server allocates new PeerId in every Initial Exchange
  • User may name devices at server UI
Cryptosuite upgrade

• Common solution: Upgrade of long-term credentials (e.g. certificate) requires admin action

• EAP-NOOB solution:
  • Avoid user action (new OOB step) at all cost
  • Reconnect Exchange may negotiate a new cryptosuite and update the persistent association keys

but this leads to another problem...
Dropped last messages

• If last message of the Reconnect is dropped during cryptosuite upgrade, peer moves to new cryptosuite while server keeps old one

• Man-in-the-middle attacker can drop messages for DoS

• Unavoidable problem in distributed systems
  • EAP retransmission does not help
  • Adding another ack message would not help

• EAP-NOOB solution:
  • Peer willing to roll back to old cryptosuite until the next attempted rekeying when it receives confirmation that server has upgraded (or not)
  • Server never rolls back
  • Cryptosuite upgrade completes when the packet-dropping attacker goes away
  • DoS resistance verified in mCRL2 model
Multiple OOB messages

• Peer device may have multiple OOB messages in flight, by the same or different user

• Peer may support both peer-to-server and server-to-peer directions for the OOB message
  • not encouraged for usability reasons

• If peer tries to connect to multiple wireless networks in parallel, multiple users may deliver OOB messages to different servers

• EAP-NOOB solution:
  • The first delivered OOB message wins
  • If two OOB messages delivered at the same time in different directions, server-to-peer message wins
  • The first server to complete wins
  • Deadlock freedom verified in mCRL2 model
Summary
What is the trick?

• Tricks in EAP-NOOB
  • Thanks to in-band communication over EAP, we only need one short OOB message, in either peer-to-server or server-to-peer direction
  • OOB message designed so that either secrecy or integrity is sufficient for security

• Is there a catch?
  • Requires Wi-Fi with WPAx-Enterprise (better for IoT devices anyway)
  • Network admin has to choose one AAA server for device bootstrapping in that network
EAP-NOOB Summary

• EAP method with user-assisted OOB authentication for bootstrapping security of smart appliances
• Current version: draft-aura-eap-noob-04
• Your reviews and feedback are welcome!

Questions to SecDispatch:
• EAP-NOOB currently individual submission, needs a WG
• EMU WG is the closest match, but its charter currently does not cover EAP-NOOB
Backup slides
Comparison to...

• Configuring the peer offline with all it needs
  • Peer UI may have only output and no suitable input

• Simply transferring a secret key to/from the peer?
  • OOB channel may be vulnerable to spying. EAP-NOOB can work with only integrity

• Static QR code with hash of device public key
  • EAP-NOOB establishes two-way trust
  • EAP-NOOB assigns a network and owner to the device

• Reading and writing configuration data over NFC
  • EAP-NOOB only requires one OOB message in one direction
  • EAP-NOOB supports a variety of OOB channels incl. NFC

• Home networks with shared passphrase
  • Devices need to be managed and revoked individually; WPA-Enterprise is better
Bootstrapping application security

• Network connectivity and association with application server in one step

• AAA server may be integrated with application-layer device management
  • Can export keys to application layer
  • Can convey initial app-layer configuration to peer

• Compare with entering wireless credentials and then application-layer cloud credentials
Persistent association

• **Must avoid rerun of user-assisted authentication (OOB step) at all cost**

• **EAP-NOOB solution:**
  • After OOB message delivered and Completion takes place, peer and server create **persistent association**
  • Future authentication requires no user interaction
  • User reset is the only way to move back to initial state
Roaming support

• **Devices may need to roam** like personal computers, e.g. in Eduroam
  • Feature requested by Josh Howlett (Jisc.ac.uk)

• **EAP-NOOB solution:**
  • Server sends to peer a list of SSIDs where the persistent association is valid
  • Peer uses server-allocated PeerId@Realm for future authentications
Wireless network selection

• Out-of-the-box peer does not know the current wireless network or AAA server – how to discover?

• EAP-NOOB solution 1:
  • Peer device scans all wireless networks for EAP-NOOB support, performs Initial Exchange with all
  • Peer device outputs multiple OOB messages (e.g. alternative QR codes)
  • User typically only knows one AAA server and delivers the OOB message to/from it

• EAP-NOOB solution 2:
  • User selects SSID on peer device
Isolating devices on access network

• In typical use of EAP-NOOB:
  • users can register new peer devices to network
  • remote AAA trusted to register new devices for wireless access
  • corrupt IoT device could share its access credentials

• These devices probably should be put into a VLAN and isolated from other local network hosts
  • Local AAA can signal APs to do this

• Isolation of devices from each other on VLAN possible but not supported on most Wi-Fi networks

• Not for us to solve, but something to keep in mind