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

Bootstrapping security for smart appliances
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 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

Remote AAA

Local AAA

AP

IoT appliance

Aura, Sethi: draft-aura-eap-noob 4
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

Remote AAA

Local AP

IoT appliance

UI or API

User-assisted OOB channel

EAP in-band

Unauthenticated ECDHE key exchange
EAP-NOOB protocol

1. Unauthenticated ECDHE key exchange

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

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

Remote AAA
UI or API
Local AAA
AP
IoT appliance
OOB output (or input)

EAP in-band

Aura, Sethi: draft-aura-eap-noob 9
EAP-NOOB protocol

1. Unauthenticated ECDHE key exchange

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

3. Key confirmation

Remote AAA

Local AAA

AP

IoT appliance

User-assisted OOB channel

UI or API

OOB output (or input)

OOB Step

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

4. Rekeying with nonces or ECDHE

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
• Tricky case: peer-to-server OOB with no secrecy
  • In this case, one-directional OOB message not enough
  • User must note failure of server to register peer and, in that case, reset the peer

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

[Diagram showing a user interface with QR codes and text related to Aalto University and account login]
Use case: bootstrapping cloud-connected display

- New display device has no owner or domain, no credentials for cloud or Wi-Fi
- One-step process to:
  - register display device to cloud + get Wi-Fi access
  - link device to a user account (ownership)
  - export URL and key for application-layer device management
- Display device can **output OOB message is URL as QR code**, but has no input, except reset button
- User has a smart phone (app optional)
- Remote AAA server integrated to display-management service in cloud
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
Resolved and open issues in EAP-NOOB design
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=ZrD7qkczoNoHGbGcN2bN0&N=rMi
  nS04F4EfCU8D91jxX_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
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
Identifier allocation

• Must not rely on unauthenticated identifiers

• Need to avoid identifier squatting

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

• Device can send app-layer identifiers and capabilities to server in PeerInfo field
  • Cryptographic assertions about the peer device could be added as protocol extension
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
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
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
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
Dropped last messages

• **If last message of the Reconnect is dropped**, peer moves to new cryptosuite while server keeps old one → Synchronization failure between peer and server
  • Man-in-the-middle attacker can cause 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 it received confirmation that server has upgraded in the next attempted rekeying
  • Server never rolls back
  • Cryptosuite upgrade completes when the packet-dropping attacker goes away
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 isolated to a VLAN and isolated from 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
Software requirements

• Peer device and AAA server need to support EAP-NOOB
  • We implemented the EAP method for Linux hostapd and wpa_supplicant
  • Integrating EAP method and user interaction for OOB delivery can be a bit tricky
• AP does not need any changes
• Local AAA at the access network typically requires only minor configuration changes
  • Forward authentication for @eap-noob.net and server-assigned Realm to remote AAA that supports EAP-NOOB
Other issues on our TODO list:

• Thorough modeling and analysis of error message handling
• Timeouts in the protocol need modeling and user testing
• Should add separate message field for application-layer bootstrapping info
• API for exporting application-layer keys and bootstrapping info
• Update the security considerations section
Summary
What is the trick?

• Tricks in EAP-NOOB
  • Thanks to inband 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 AAA, e.g. Wi-Fi with WPAX-Enterprise
  • Network admin has to choose one AAA server for device bootstrapping in that network
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
EAP-NOOB Summary

• EAP method with user-assisted OOB authentication for bootstrapping security of smart appliances

• Current version: draft-aura-eap-noob-04

Requests to the EMU WG:

• If the WG is rechartered, consider including EAP-NOOB
• Can we use the EMU git for the draft and issue tracker?