EAP-NOOB : Nimble Out-of-Band Authentication for EAP
EMU WG, IETF 105
Montreal, July 2019

Tuomas Aura, Aalto University
Mohit Sethi, Ericsson
various other contributors
What problems EAP-NOOB solves?

• **Out-of-band (OOB)** = second, independent communication channel for authenticating the primary channel
  - e.g. NFC, QR

• EAP is a generic authentication framework with many methods, but **currently has no OOB method**

• **EAP-NOOB** is one solution for this: suitable for a broad range of EAP applications, stable spec, formal models and verification, open-source implementations
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

New peer implementation in Contiki
EAP-NOOB overview

• EAP method for bootstrapping 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
  • Application-level bootstrapping: assign an owner to the device and redirect to application server

• Fast reauthentication of previously registered devices without further user interaction
EAP-NOOB architecture

Remote AAA

Local AAA

AP

New device

UI or API

EAP in-band

User-assisted OOB channel

OOB output (or input)

e.g. dynamic QR code

Trick: in-band communication over EAP between peer and server before device is registered - idea now copied by others!
New in draft version -06

Changes based on feedback from implementation and verification

• **Stop overloading NAI with peer id and state**, at the cost of an extra roundtrip to each exchange
  • Complies better with RFC 3748 section 5.1 guidance
  • Simpler peer implementation in wpa_supplicant
• **Better support for identifier randomization extensions**
  • Removed key identifier that may leak peer identity

Editorial changes:

• New subsection for the common handshake part in all exchanges
  • Text corresponds more closely to implementations
  • Avoids repetition of text
• Clarified when to peer starts using server-assigned Realm
  • Use Realm early for more seamless roaming support

“It is RECOMMENDED that the Identity Response be used primarily for routing purposes and selecting which EAP method to use.”
Analysis of misbinding and mitigation


• Generic attack against device-pairing protocols where devices have no verifiable identifiers and authentication is based on physical access,

• Device with compromised UI can trick user to pair another device instead

• Bluetooth, DPP and others are also vulnerable
TODO list

• Update message examples and implementation to draft -06
• **Timeouts** in the protocol need modeling and user testing
• Recovery from **lost last messages**: formally verified but should be written up into a report
• Possibly leave **hooks for future extensions**:
  • Device registration while roaming
  • Identifier randomization
  • Application configuration, e.g. service URL (currently only creating shared key for application layer)
  • Manufacturer certificates and other credentials
EAP-NOOB Summary

- EAP method with user-assisted OOB authentication for bootstrapping security of smart appliances
- Current version: draft-aura-eap-noob-06, no major changes expected
- Implementations:
  - wpa_supplicant and hostapd
  - https://github.com/tuomaura/eap-noob
  - New implementation on Contiki
- Formal models in mCRL2 (protocol and DoS-resistance) and ProVerif (authentication)

There seems to be interest. This could be a candidate work item when EMU WG is rechartered.
Backup slides
Roaming story

Two roaming scenarios:

1. Register device at home, then roam
   • Server assigns a Realm to the peer in Initial Exchange
   • Roaming just works
   • EAP-NOOB supports this scenario out of the box

2. Register device while roaming
   • Requires user interaction with foreign AAA to route the Initial Exchange (one EAP conversation) to home AAA
   • Server assigns a Realm to the peer in Initial Exchange
   • From then on, the roaming just works
   • EAP-NOOB is designed to not prevent this scenario

• To avoid problems, peer should start using the server-assigned Realm at the earliest possible time
Formal models and verification

• mCRL2 model
  • Modeling Protocol messages and state machines
  • Deadlock-freeness
  • DoS resistance for intentionally dropped messages

• ProVerif model
  • Cryptographic key-exchange properties
  • Authentication and confidentiality
  • Misbinding: correspondence between user intention and protocol completion