



Collaboration CEA - Avantix

Réunion de lancement

05/09/2025

© Eviden SAS

La cible

Adapter Binsec:

- A l'analyse de firmwares
- A l'analyse de protocoles réseau

Scenario de test

Le scenario qui nous intéresse:

- Analyser un firmware qui communique par WiFi

La norme WiFi (IEEE 802.11):

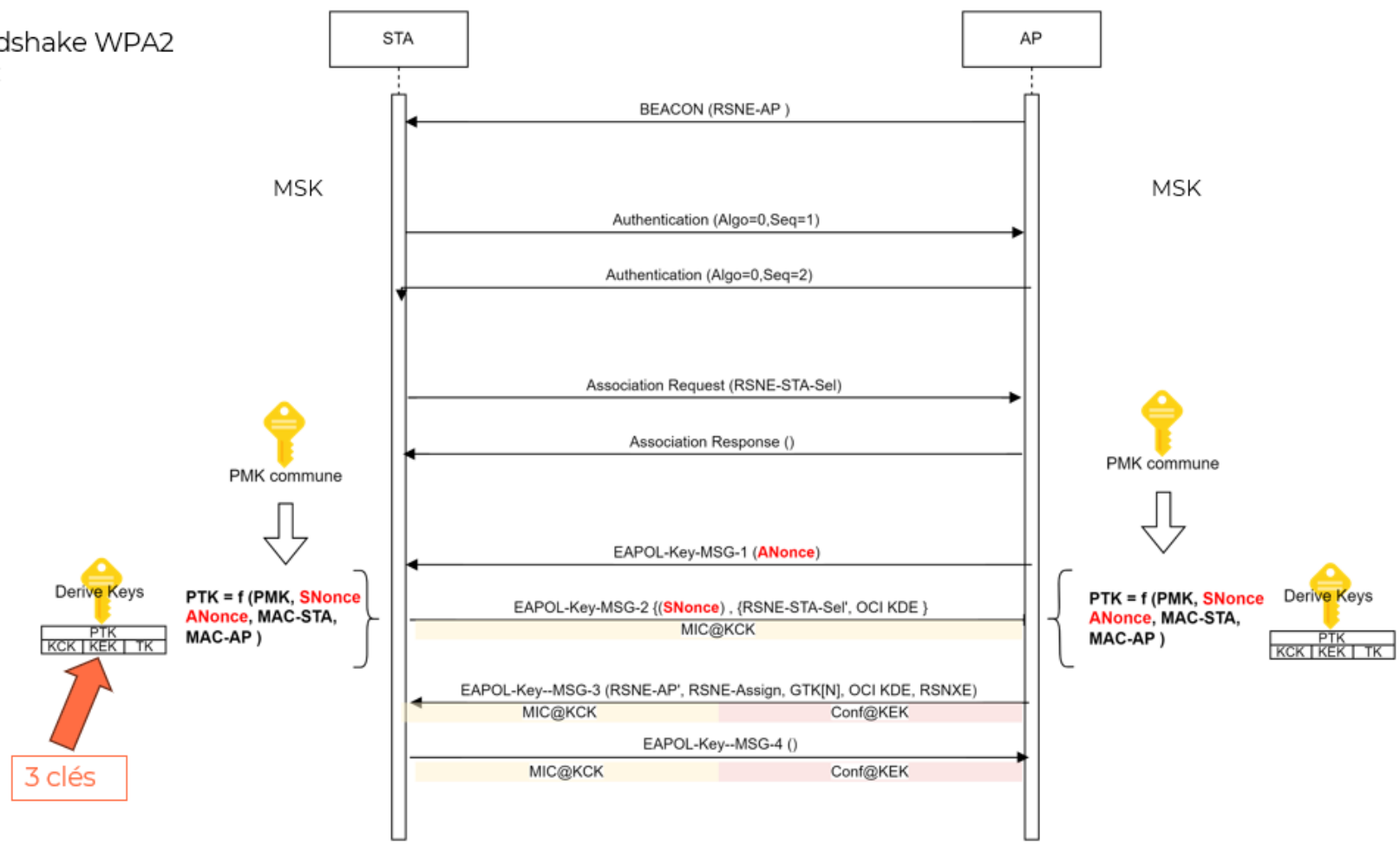
- Plusieurs protocoles: WEP, WPA2, WPA3.
- Plusieurs algorithmes de chiffrements: TKIP, CCMP
- Plusieurs méthodes d'authentification: Personal ou Entreprise (mot de passe, certificats etc.)

Les enjeux de la connexion:

- Négociation des paramètres
- Authentification des parties
- Etablissement des clés de chiffrement des données

Connexion WPA2-PSK

4Way Handshake WPA2 Personal :



AVANTIX

Wifi - Réunion d'avancement #1 - 04/03/2025
© Avantix - For internal use

EVIDEN

Les modèle de sécurité

Le modèle de l'attaquant:

- Ne connaît pas le mot de passe
- Peut écouter tous les messages
- Peut intercepter, changer l'ordre ou injecter de nouveaux messages.

Quelques propriétés:

- Protection contre les attaques de rétrogradation (downgrade attack)
- Négociation d'une clé de session fraîche et non-prévisible
- Authentification mutuelle
- Protection contre les attaques de répétition

Le firmware du ESP32

Le ESP32

- Famille de microcontrôleurs versatiles avec support WiFi et bluetooth

Le firmware:

- basé sur FreeRTOS
- Architecture Xtensa ou Risc-V

La stack WiFi:

- Stack officielle propriétaire closed source
- Stack non-officielle open-source (limité au WPA2-PSK)

Les préparatifs

Fourniture d'un firmware open source:

- Basé sur la stack open-source ESP32
- Code source Rust
- Modifié pour simuler l'interaction avec le périphérique WiFi

Les limitations:

- Compilable pour xtensa, peut-être Risc-V
- Fonctionnalités limitées de la stack open-source (e.g. pas de WPA3)

Nos interrogations

- Analyse d'un firmware complet (avec bootloader etc.)
- Support du multithreading
- Architectures supportées
- Modélisation de l'injection de messages

EVIDEN

Confidential information owned by Eviden SAS, to be used by the recipient only.
This document, or any part of it, may not be reproduced, copied, circulated
and/or distributed nor quoted without prior written approval from Eviden SAS.

© Eviden SAS