Failles de WPA2

Les attaques sur les méthodes d'authentification :

- Une attaque par dictionnaire hors-ligne : contre EAP MD5
  - Grâce à une écoute de ce qui transite sur le réseau, on peut donc identifier le hash du défi et le défi qui transitent
  - Ensuite on recherche le mot de passe de manière hors ligne via une recherche par dictionnaire, une fois trouvé on soumet une requête d'authentification au serveur

https://arxiv.org/ftp/arxiv/papers/1812/1812.01533.pdf

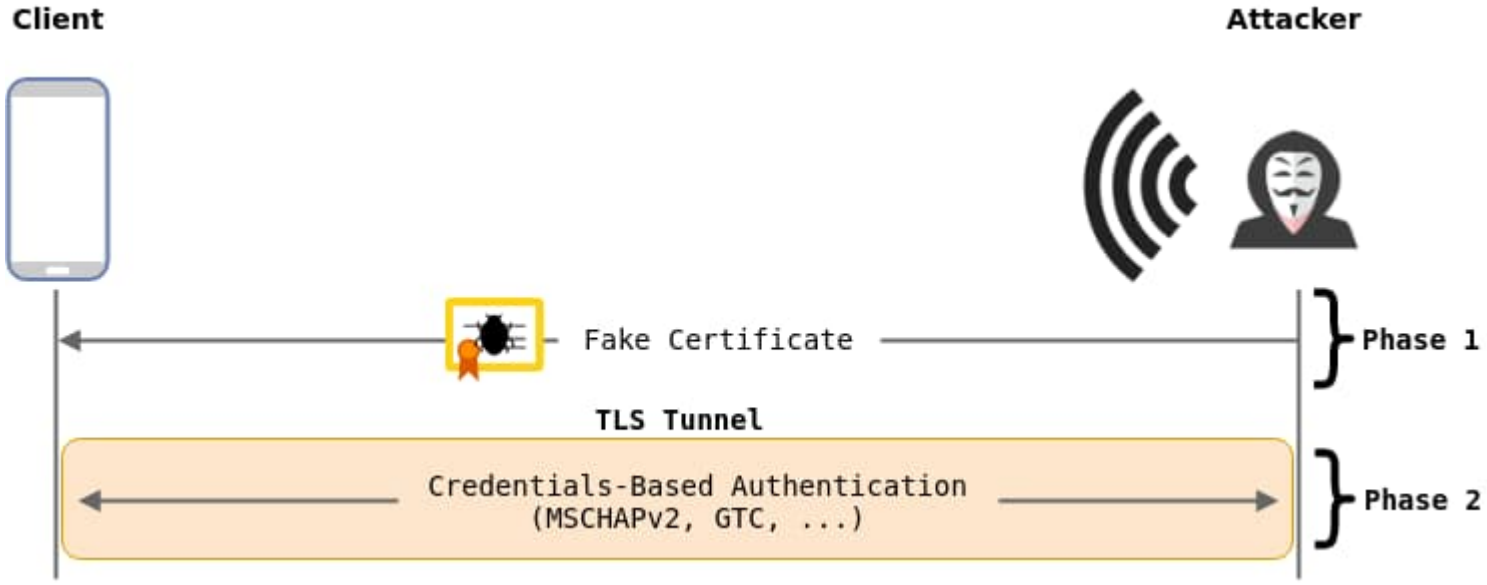
Les solutions

- Pas de MD5 dans un réseau WIFI
- Utiliser une méthode plus efficace
- Privilégier les méthodes EAP tunnelisées que celles non tunnelisées
- Le serveur refuse un nombre trop grand de tentatives pour un même utilisateur (il se bloque pendant 10 mins par exemple)

Failles de WPA2

Les attaques MITM:

- Exemple1 : Evil Twin Attack pour EAP-TLS
  - Le serveur RADIUS factice peut forger des faux certificats
  - Les clients légitimes « acceptent » les faux certificats forgés et envoient à leurs tour des « vrais » certificats
  - La connexion est alors établie entre le client et le AP factice

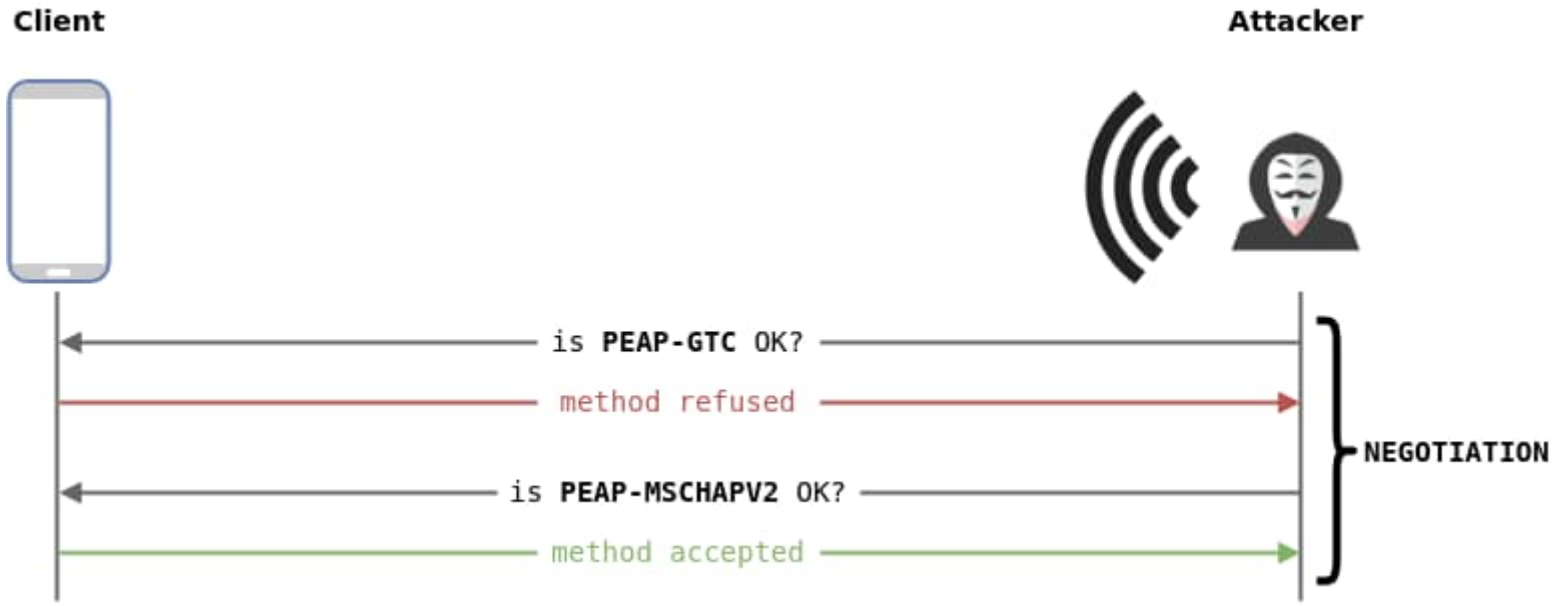


https://github.com/koutto/pi-pwnbox-rogueap/wiki/08.-Evil-Twin-Attacks

Failles de WPA2

Les attaques MITM:

- Exemple2 : Downgrade attack
  - Pour des raisons de compatibilité, les devices WiFi sont configurés à supporter diverses méthode EAP (+/- robustes)
  - Puisque la négociation de la méthode EAP est initiée par le Evil Twin AP, il est possible de tromper les clients pour qu'ils utilisent un protocole d'authentification faible

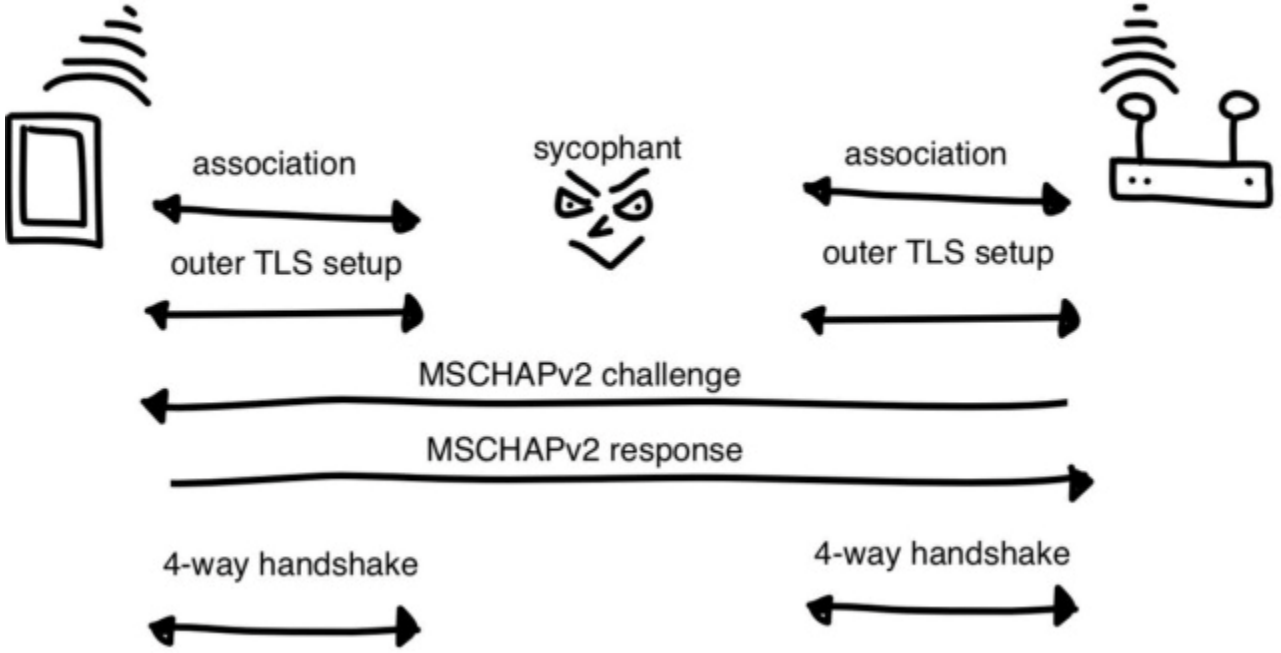


https://github.com/koutto/pi-pwnbox-rogueap/wiki/08.-Evil-Twin-Attacks

Failles de WPA2

Les attaques MITM:

- Exemple3 : PEAP Relay attack
  - Cette attaque permet à un attaquant d'obtenir une position de Man-in-the-Middle dans le réseau cible, sans connaître les informations d'identification valides (pas besoin de cracker les informations d'identification MSCHAPv2)



https://github.com/koutto/pi-pwnbox-rogueap/wiki/08.-Evil-Twin-Attacks

Failles de WPA2

Certaines vulnérabilités WPA2 ont été découvertes apparentées au TKIP 4-way handshake

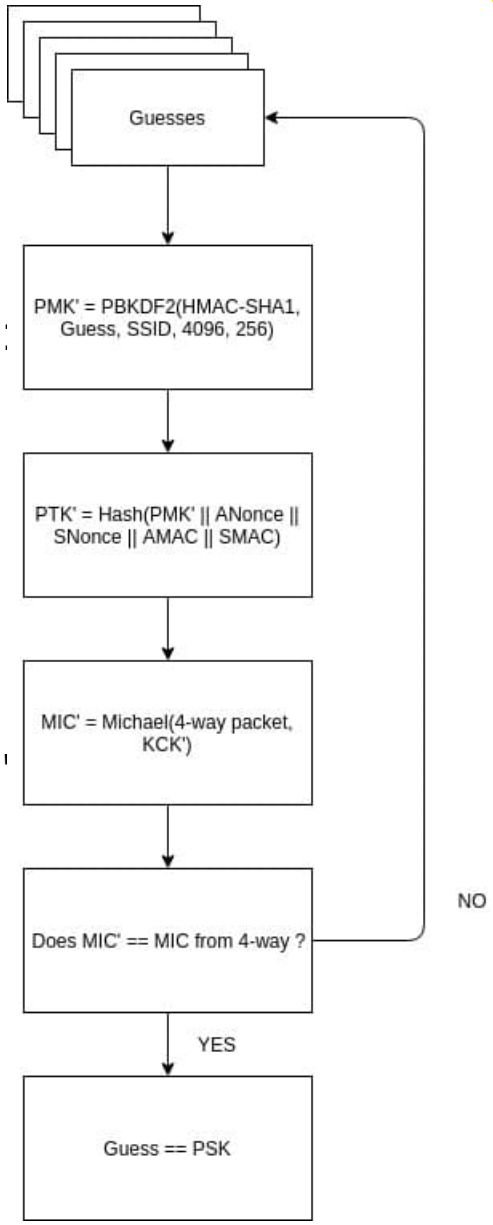
- Attaque par brute forcing sur la clé PSK
  - L'écoute du 4-way handshake suffit pour construire une attaque hors ligne et essayer de trouver la phrase secrète PSK
  - Améliorée par une attaque par dictionnaire
- Attaque KRACK (*Key Reinstallation Attack*)
  - Exploite la vulnérabilité de réinstallation de clé
  - Force la réutilisation de nonce (nonce reuse)

Failles de WPA2

PSK Brute force

- Un attaquant observe une connexion client et obtient :
  - le SSID du point d'accès
  - les Nonces Anonce , SNonce (ils sont transmis en clair)
  - les adresses MAC (Authenticator et Supplicant)
  - le MIC d'un message calculé avec un PTK valide

Pour chaque supposition PSK, l'attaquant calcule le PMK' et le PTK'. Il utilise son PTK' pour calculer un MIC' pour le paquet 2, 3 ou 4 du TKIP 4-way handshake
➔ Si le MIC' calculé est égal au MIC des paquets, l'estimation PSK est correcte.



https://cylab.be/blog/32/how-does-wpawpa2-wifi-security-work-and-how-to-crack-it

Failles de WPA2

Performances de l'attaque

- A cause du coût de calcul élevé des hachages, il n'est pas possible d'utiliser un mot de passe de plus de 12 ou 15 caractères.

	Nvidia GTX 960M	96 cores Intel Xeon	Google Cloud 4 Nvidia Tesla T4
8-digits brute-force attack	+/-30 minutes	+/- 19 minutes	+/- 80 seconds
10-digits brute-force attack	+/- 2 days	+/- 30 hours	+/- 140 minutes
8-lowercase letters brute-force attack	+/- 40 days	+/- 28 days	+/- 2 days
12-characters (digits + lowercase) brute-force attack	+/- 160 years	+/- 100 years	+/- 7 years

https://cylab.be/blog/32/how-does-wpawpa2-wifi-security-work-and-how-to-crack-it

Failles de WPA2

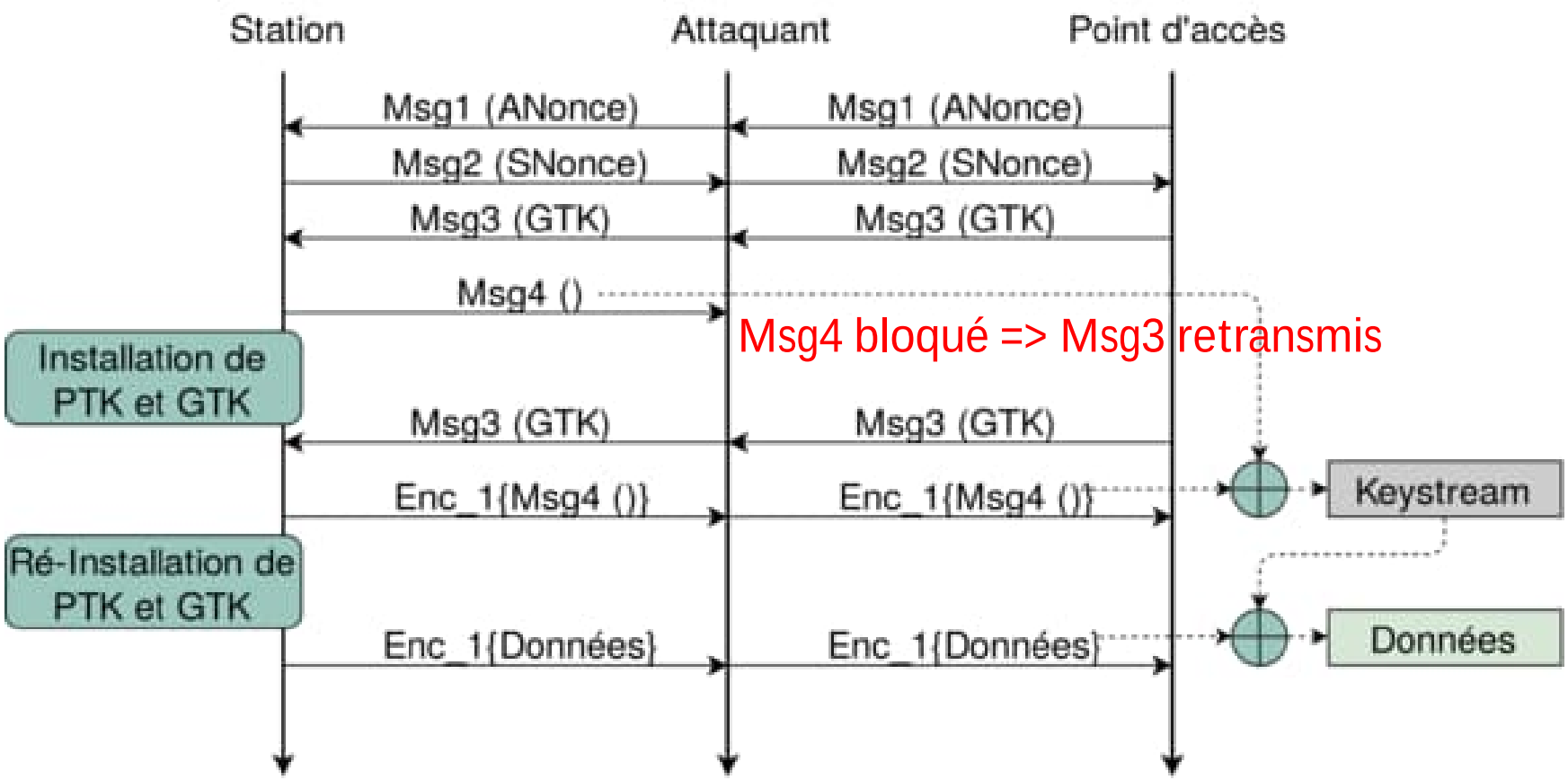
Attaque par réinstallation de clé (KRACK)

Mise en œuvre d'une attaque par réinstallation de clef:

- L'attaquant placé en interposition entre la station et le point d'accès, va bloquer la transmission du message 4.
- Ceci provoque la retransmission d'un message 3
- Ceci va déclencher la réinstallation des clefs au niveau de la station
- Le même nonce, et donc le même keystream, sera alors utilisé pour protéger le second message 4 et le premier paquet de données.
- Une combinaison linéaire (à l'aide de l'opérateur XOR) des deux messages 4 et des données chiffrées permet de récupérer les données en clair

https://connect.ed-diamond.com/GNU-Linux-Magazine/glmfhs-099/comprendre-les-attaques-krack

Failles de WPA2



https://connect.ed-diamond.com/GNU-Linux-Magazine/glmfhs-099/comprendre-les-attaques-krack

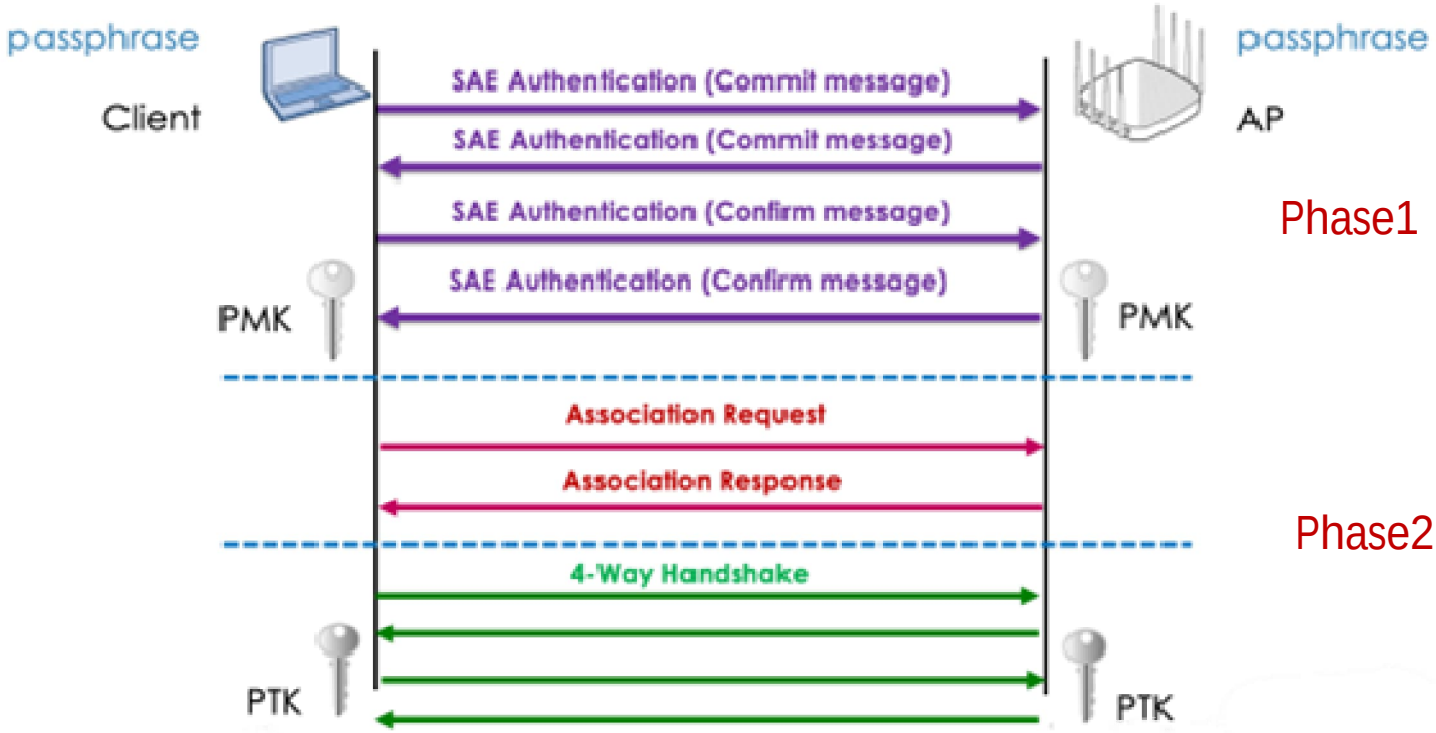
La sécurité WPA3

- Est standardisé depuis 2018
- La Wi-Fi Alliance rend obligatoire la prise en charge de la sécurité WPA3 pour la certification Wi-Fi 6

  Les entreprises continuent toujours à utiliser WPA2!
- Nouveautés de WPA3
  - MFP (*Management Frame Protection*) pour assurer la protection des trames de management unicast ou multicast contre l'écoute clandestine (*eavesdropping*) et la falsification (*forging*)
  - WPA3-Personal basé sur SAE *(Simultaneous Authentication of Equals)* pour protéger les utilisateurs contre les attaques par force brute /dictionnaire
  - Un chiffrement 256-bit GCMP/AES (Galois/Counter Mode Protocol) remplace CCMP/AES avec 128-bit.
  - Un contrôle d'intégrité basé sur GMAC: Galois Message Authentication Code
- Formes de WPA3
  - ➢ WPA3-Personal
  - ➢ WPA3-Entreprise
  - ➢ Open Enhanced

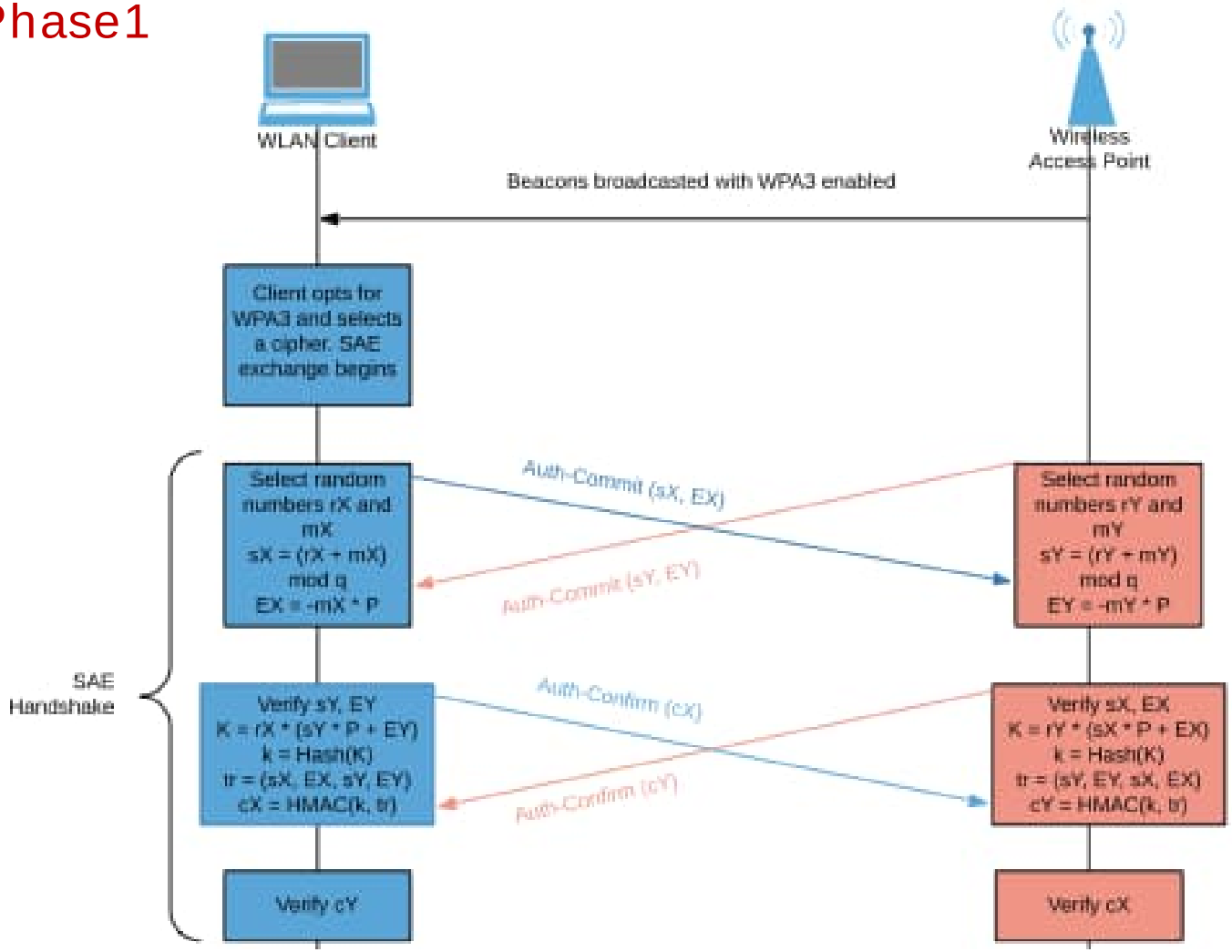
WPA3-Personal

- WPA3 SAE remplace la PSK et génère une clé (PMK) totalement unique pour chaque authentification en se basant sur ECC (*Elliptic Curve Cryptography*)
  - ✓ Protection contre Brute force
  - ✓ Le trafic ne peut pas être espionné par les autres utilisateurs



Echange WPA3-SAE (DragonFly)

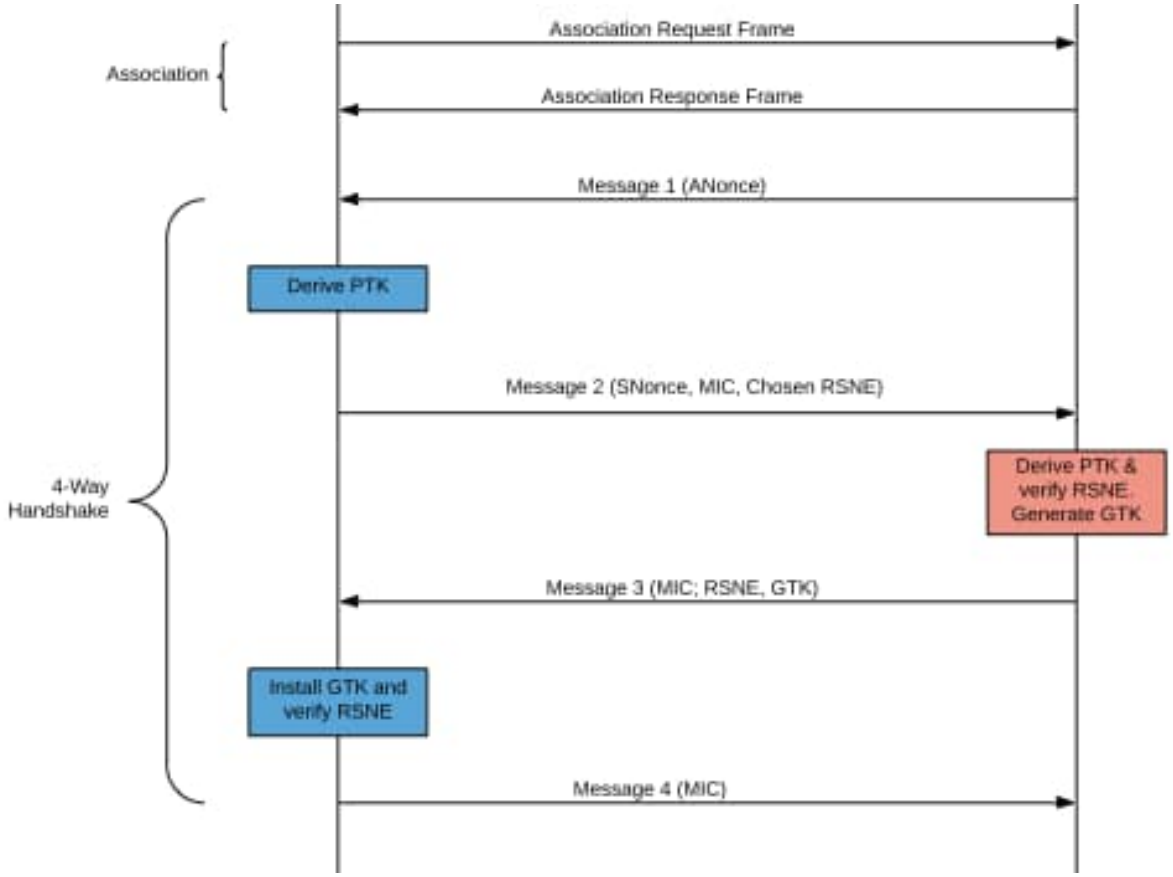
Phase1



k = PMK

Echange WPA3-SAE (DragonFly)

Phase 2



WPA3-Personal

- 2 modes de fonctionnement :
  - WPA3-Personal Only
    - Exige SAE et remplace totalement la PSK
    - Peut être activé si TOUS les équipements supportent WPA3
    - La protection MFP est alors obligatoire
  - WPA3-Personal Transition
    - Permet une rétro-compatibilité avec WPA2-Personal
    - Les clients WPA2 peuvent toujours se connecter au même BSS
    - Les clients WPA2 s'authentifient via PSK, les clients WPA3 s'authentifient via SAE
    - La protection MFP est activée uniquement pour les clients WPA3

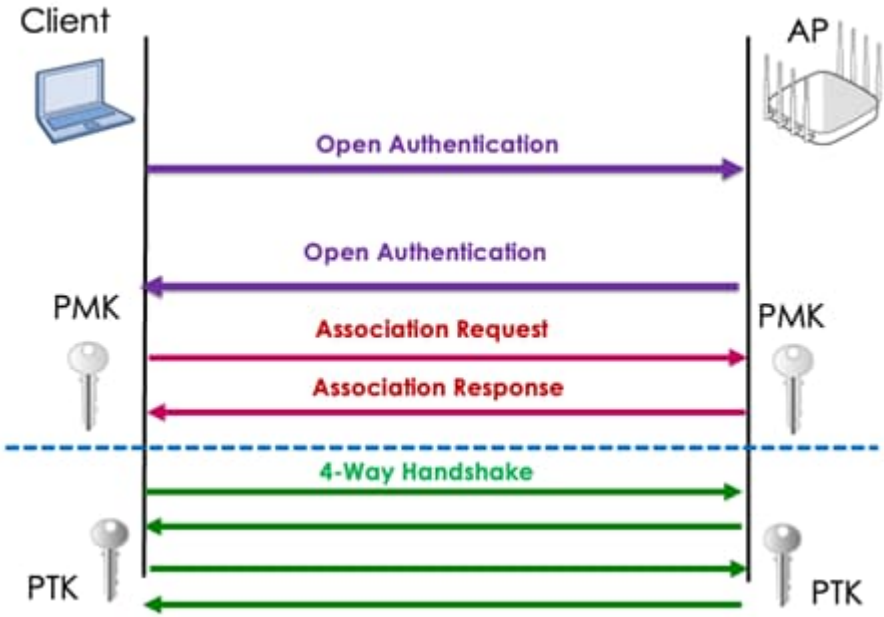
WPA3-Entreprise

- 3 modes de fonctionnement :
  - ➢ WPA3-Entreprise Only
    - Authentification 802.1x/EAP reste la même
    - Peut être activé si TOUS les équipements supportent WPA3
    - La protection MFP est alors obligatoire
  - ➢ WPA3-Entreprise Transition
    - Permet une rétro-compatibilité avec WPA2-Personal
    - Les clients WPA2 peuvent toujours se connecter au même BSS
    - La protection MFP est activée uniquement pour les clients WPA3
  - ➢WPA3-Entreprise 192 bit
    - Dédié pour les environnements critiques exigeant un haut niveau de sécurité
    - Un chiffrement 256-bit GCMP/AES
    - Une protection des trames de management basée sur 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)
    - MFP obligatoire
    - EAP-TLS est la méthode d'authentification utilisée utilisant l'échange Elliptic Curve Diffie-Hellman (ECDH) et le Elliptic Curve Digital Signature Algorithm (ECDSA) utilisant 384-bit elliptic curve

Open enhanced

- Défini par le certification Wi-Fi CERTIFIED Enhanced Open pour la protection des données dans des réseauw WiFi ouverts
- Basé sur le protocole *Opportunistic Wireless Encryption* (OWE), défini dans le RFC IETF 8110
- Intègre des mécanismes de cryptographie pour fournir à chaque utilisateur un chiffrement individuel unique via un échange de clé Diffie-Hellman

- 2 Modes de fonctionnement :
  - ➢ Enhanced Open Only
    - Chiffrement 128-bit CCMP/AES
    - Aucune authentification
  - ➢ Enhanced Open Transition
    - Un SSID caché est automatiquer créé pour desservir les clients WPA2



WPA3: les failles

- https://wpa3.mathyvanhoef.com/