SÉCURITÉ DES RÉSEAUX

SÉCURITÉ DES RÉSEAUX SANS-FIL

A. Guermouche

Plan

WEP

WPA/WPA2

WPA3

Plan

WEP

WPA/WPA2

WPA3

WEP : *Wired Equivalent Privacy*

- Mécanisme simple de chiffrement de données du standard 802.11.
- Utilisation de l'algorithme de chiffrement RC4.
- Utilisation de clés statiques de 64 ou 128 bits.

Au niveau de l'émetteur :

1. Calculer le code CRC des données et l'ajouter à la trame.
2. Calculer un nouvel IV (*Initialisation Vector*) et l'ajouter à la clé secrète pour former une clé pour ce paquet.
3. Utiliser RC4 pour générer une clé de flux dont la longueur est égale à la longueur des données à envoyer plus leur code CRC.
4. Utiliser la clé de flux pour chiffrer le contenu du message ainsi que le code CRC (en faisant un XOR).
5. Mettre l'IV dans un champs de l'en-tête de la trame.
6. Envoyer la trame.

WEP : *Wired Equivalent Privacy*

- Mécanisme simple de chiffrement de données du standard 802.11.
- Utilisation de l'algorithme de chiffrement RC4.
- Utilisation de clés statiques de 64 ou 128 bits.

Au niveau du récepteur :

1. Extraire l'IV à partir de l'en-tête de la trame.
2. Ajouter l'IV à la clé secrète pour générer la clé du paquet.
3. Utiliser RC4 et la clé de paquet pour générer une clé de flux.
4. Utiliser la clé de flux pour déchiffrer le trame.
5. Calculer un code CRC sur les données et le comparer au code CRC contenu dans la trame.
6. Si les deux codes correspondent, la trame est acceptée.

Problèmes de WEP

- L'IV a une longueur de 24 bits.
- WEP ajoute l'IV à la clé secrète pour former une famille de 2^{24} clés distinctes.

Problèmes :

- Faiblesse de certaines clés RC4.
- Le principal problème est qu'une clé de flux ne peut pas être réutilisée.
- Théoriquement, une fois que les 2^{24} clés possibles ont été utilisées, il est nécessaire de changer de clé secrète.
- La norme ne spécifie pas de méthode précise de gestion de clés.
- En pratique, les clés secrètes ne sont quasiment jamais changées.
- Pour une borne avec un client avec une connexion de 11Mb/s et ayant une activité réseau normale, il suffit d'une heure pour couvrir tout l'espace des clés.

Stratégies de choix de l'IV

Stratégie séquentielle. La probabilité de collision est de 100% si le nombre de clients est supérieur à 1.

Stratégie Random. La probabilité de collision P_n que deux paquets aient le même IV après n paquets est :

$$\begin{cases} P_2 = 1/2^{24} \\ P_n = P_{n-1} + (n-1)(1 - P_{n-1}))/2^{24} \end{cases}$$

50% de chances d'avoir une collision au bout de 4823 paquets (2^{12}).

Attaques contre WEP (1/2)

Attaque passive :

- Un attaquant écoute le trafic 802.11 et va appliquer un XOR entre des données chiffrées avec la même clé (même IV).
- Les données chiffrées correspondent à :

$$c_i = p_i \oplus k_i, \ pour\ i = 1, 2, \ldots$$

$$c_i^{'} = p_i^{'} \oplus k_i, \ pour\ i = 1, 2, \ldots$$

où les k_i correspondent aux bits de la la clé de flux.

- En faisant un XOR entre les c_i et $c_i^{'}$ on obtient :

$$p_i \oplus p_i^{'} \ pour\ i = 1, 2, \ldots$$

- L'attaquant connaît alors le XOR des données initiales p_i et $p_i^{'}$.
- L'attaquant sait alors quels bits (p_i,$p_i^{'}$) sont égaux (ou différents) dans les deux flux.
- Ainsi, pour chaque paire de bits, l'attaquant arrive à réduire la taille de son espace de recherche de 2^{16} à 2^8.
- Avoir plus de trames d'informations permet de réduire l'espace de recherche pour la détermination de la clé.

FMS

- Article de Fluhrer, Mantin, Shamir (FMS), 2001 :

  http://wiki-files.aircrack-ng.org/doc/rc4_ksaproc.pdf

- Attaque passive sur WEP capable de récupérer la totalité de la clé secrète en une durée relativement courte (4.000.000 de paquets)
- obtenir des informations sur tous les octets de la clé lorsque l'entrée PRNG est connu :
  - Capture de paquets avec un IV faible (valeurs IV spécifiques qui facilitent le calcul d'un octet de la clé lorsque les les octets précédents de la clé sont connus)
  - On connaît le premier octet du chiffré par IV : Chaque trame sans fil possède un premier octet fiable et connu
    - En-tête du protocole d'accès au sous-réseau (SNAP) utilisé dans les couche de contrôle des liaisons, sous-couche supérieure de la couche de liaison de données.
    - Le premier octet est 0xAA
- Amélioration par la suite par Korek en 2004.

Attaques contre WEP (2/2)

Attaques actives :

Forger un paquet. Vu que RC4 et CRC sont linéaires, il est possible de modifier certains bits du messages chiffrés d'une manière telle que le code CRC reste correcte et que le messages se décrypte en un autre qui peut être valide.

- Les adresses IP sont toujours au même endroit dans la trame.
- Il est possible de modifié l'adresse IP de destination d'un paquet en modifiant certains bits du message chiffré qui correspondent a l'adresse IP et au CRC.
- Il suffit de positionner l'adresse IP de destination à celle d'une machine que l'attaquant contrôle (une machine connectée à internet).
- En gardant, la version chiffrée du message, l'attaquant va recevoir la version en clair du message sur sa machine distante, il peut alors déduire la clé de flux.

Attaques contre WEP (2/2)

Attaques actives :

Rejouer un paquet. En retransmettant un paquet capturé, il est possible d'obtenir une réponse chiffré avec un autre IV. En répétant cette opération, on peut récupérer *n* fois le même paquet chiffré avec des clés de flux différentes.

- Possibilité de rejouer un message modifié :
  1. prendre un message vide,
  2. modifier certains bits,
  3. calculer le code CRC,
  4. faire un XOR entre le message obtenu et un message capturé,
  5. envoyer le message ainsi modifié.

chopchop

Permet à l'attaquant de déchiffrer interactivement les derniers m octets de d'un paquet chiffré :

- Étape 1 : sniffer un paquet chiffré
- Étape 2 : Enlever un octet de la fin (que nous voulons révéler)
- Étape 3 : Lors de la première itération, faire l'hypothèse que la valeur en clair de l'octet est 0
  - Somme de contrôle correcte (en utilisant, par exemple, le bitflipping)
- Étape 4 : envoi du paquet réparé au point d'accès
- Étape 5 : Si l'AP diffuse le paquet, alors l'hypothèse sur le dernier octet est correcte (aller à étape 7)
- Étape 6 : Si ce n'est pas le cas, essayer de réparer la somme de contrôle en utilisant les valeurs 1 puis 2, 3 ... et répéter l'étape 3 jusqu'à ce que l'AP diffuse le paquet
- Étape 7 : Passez à l'étape 2, découpez l'octet secret suivant à partir de la fin

Plan

WEP

WPA/WPA2

WPA3

WPA : *Wi-Fi Access Protocol*

- WPA a été proposé en Octobre 2002 en réponse aux failles mises à jour dans WEP.

Propriétés :

Authentification. Deux modes de fonctionnements :

- WPA est conçu pour fonctionner avec un serveur d'authentification 802.1X (un serveur *radius* en général) qui se charge de la distribution des clés à chaque utilisateur.
- WPA propose aussi un mode moins sécurisé (PSK) basé sur un secret partagé commun à tous les utilisateurs.

Gestion des clés. Utilisation d'un protocole (TKIP) pour pallier les failles de WEP (changement de clé de chiffrement de manière périodique).

Intégrité des messages. Utilisation d'un code de vérification d'intégrité (MIC) en remplacement de CRC.

802.1X

- Norme définissant des mécanismes d'authentification pour des hôtes dans un réseau local.
- L'authentification est généralement faite par un tiers (généralement un serveur *radius*).

Composants de 802.1X :

Demandeur (*supplicant*). Entité voulant accéder d'accéder aux ressources (donc ayant besoin de se faire authentifier).

Serveur d'accès (*authenticator*). switch, borne sans-fil, ...

Serveur d'authentification (*Authentication server*). Entité avec laquelle le serveur d'accès dialogue pour authentifier le demandeur.

802.1X

- Norme définissant des mécanismes d'authentification pour des hôtes dans un réseau local.
- L'authentification est généralement faite par un tiers (généralement un serveur *radius*).

Notion de ports :

en filaire commuté.

- Le port correspond au port du switch (le demandeur s'authentifie sur ce port).

en sans fil.

- Utilisation de ports logiques.
- La borne d'accès donne à chaque client qui s'est authentifié une clé de session qui lui est propre.

EAP : *Extensive Authentication Protocol*

Objectif :

- Permettre l'ajout de nouveaux protocoles d'authentification.

Propriétés :

- EAP est un protocole de transport d'authentification.
- EAP n'est pas un protocole d'authentification.
- Les bornes d'accès ne servent que de relais entre le demandeur et le serveur d'authentification.
- La borne d'accès n'a pas besoin de connaître la méthode d'authentification utilisée (pratique pour l'évolutivité).

Types et hiérarchie des clés

Clé Pré-partagées (PSK).

- Positionnées sur le client mobile ainsi que sur la borne émettrice avec un mécanisme indépendant de WPA.
- La possession de la clé est à la base de l'authentification.

Clé fournies par un serveur d'authentification.

- Les clés sont générées par un protocole d'authentification de plus haut niveau.
- Le serveur d'authentification fournit à la borne la clé nécessaire à la protection d'une session (cette clé ayant une durée de vie prédéterminée).

- La PMK (*Pairwise Master Key*) est au sommet de la hiérarchie.
- Peut être fournie par un serveur d'authentification ou peut utiliser un secret partagé.
- Il y a une seule PMK par hôte mobile.

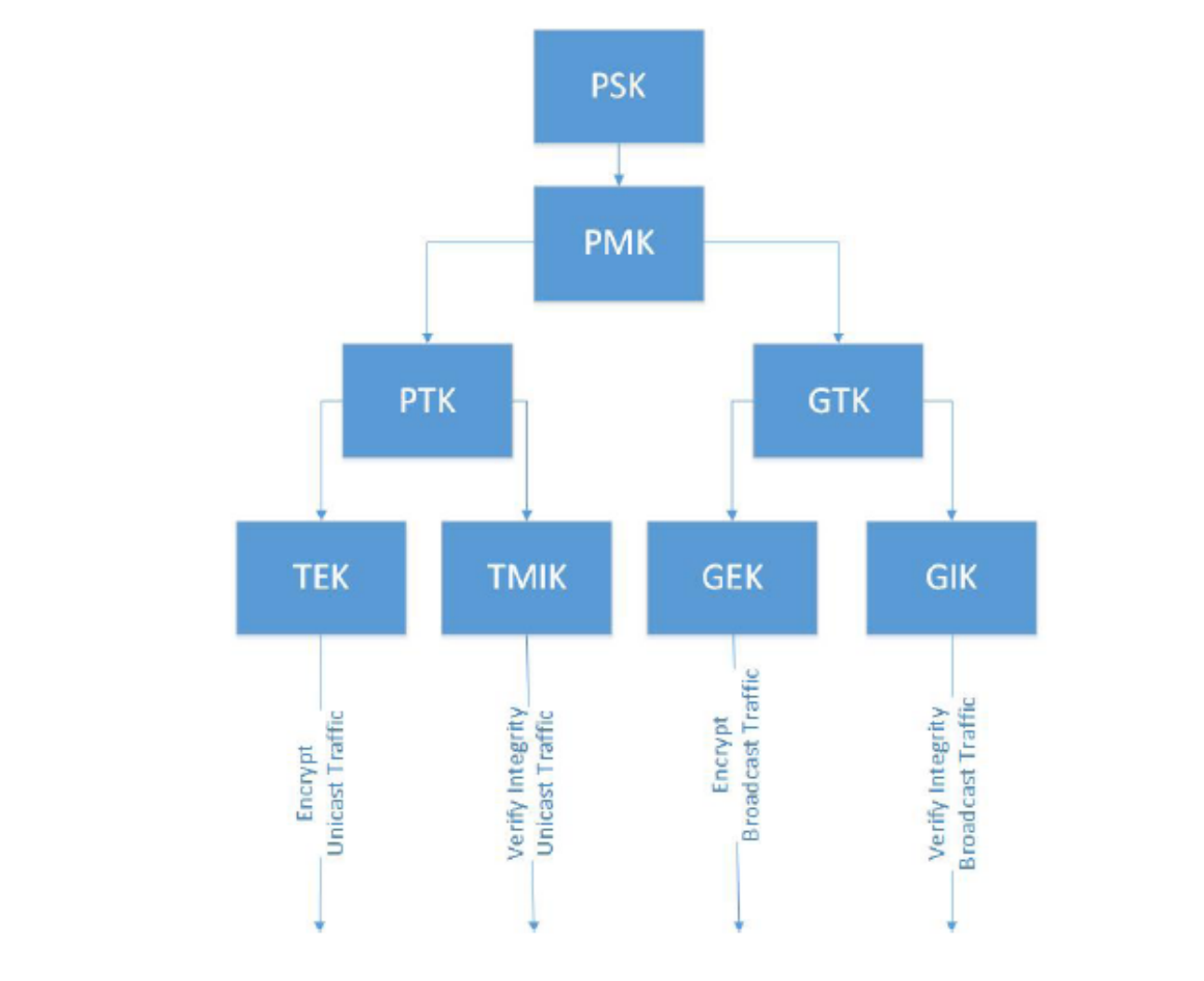
Création et acheminement de la PMK

- La génération de la PMK est basée sur une clé connue par le serveur d'authentification et le client.
- Pendant le processus d'authentification EAP, la méthode prouve que les deux parties connaissent le secret.
- Après l'authentification, une clé aléatoire est générée.
- Cette clé est utilisée pour générer la PMK.
- La PMK est ainsi connue par le serveur d'authentification et par le client.
- La PMK doit être alors transférée sur la borne (WPA recommande RADIUS pour cette opération).

Génération des clés “temporelles”

- WPA utilise des clés temporelles qui sont dérivées de la PMK.
- Les clés temporelles ne sont utilisées que pour une session.
- Les clés temporelles sont recalculées dès qu’un client mobile veut s’associer à une borne.
- Quatre clés sont créées à cet effet :
  - Clé de chiffrement des données (128 bits).
  - Clé d’intégrité (128 bits).
  - Clé de chiffrement EAPOL (128 bits).
  - Clé d’intégrité EAPOL (128 bits).
- Les deux premières sont utilisées pour protéger les données.
- Les deux dernières sont utilisées pour protéger la poignée de main initiale.
- Pour assurer qu’une clé temporelle est liée à une session, des nonces sont utilisés dans le calcul des clés.
- Chaque acteur génère un nonce et l’envoie à l’autre.
- Pour lier les clés à un périphérique, l’adresse MAC est utilisée dans le processus de génération.

Génération des clés “temporelles”



source http://webpages.eng.wayne.edu/~fy8421/16sp-csc5991/slides/lab7/wpa2-cracking-kolias.pdf

Authentification à quatre étape

Objectif : Authentifier mutuellement la borne et le client.

1. *authenticator* $\rightarrow$ *supplicant*
   - Contient le nonce de A (celui de la borne).
   - Le message est envoyé en clair.
   - À la réception de ce message, le *supplicant* calcule les clés temporelles.
2. *supplicant* $\rightarrow$ *authenticator*
   - Contient le nonce de S (celui du client mobile).
   - Contient un code MIC, généré à partir de la clé EAPOL d'intégrité, pour éviter l'altération du message.
   - L'*authenticator* calcul sa clé PTK à partir du nonce de S.
   - Il vérifie le message à l'aide du code MIC et de la clé PTK générée.
   - Ce code MIC assure que le *supplicant* a la même PMK que borne.

Les transparents suivants sont issus de http://webpages.eng.wayne.edu/ fy8421/16sp-csc5991/slides/lab7/wpa2-cracking-kolias.pdf

Authentification à quatre étape

Objectif : Authentifier mutuellement la borne et le client.

3. *authenticator* $\rightarrow$ *supplicant*
   - Le Message indique que la borne est prête à commencer à utiliser l'ensemble des clés.
   - Le message contient un MIC pour que le *supplicant* puisse vérifier que la borne a bien la bonne PMK.
   - Le message contient aussi le numéro de séquence de la première trame chiffrée
4. *supplicant* $\rightarrow$ *authenticator*
   - Le message acquitte la poignée de main.
   - Le message indique que le *supplicant* va utiliser les clés temporelles générées.

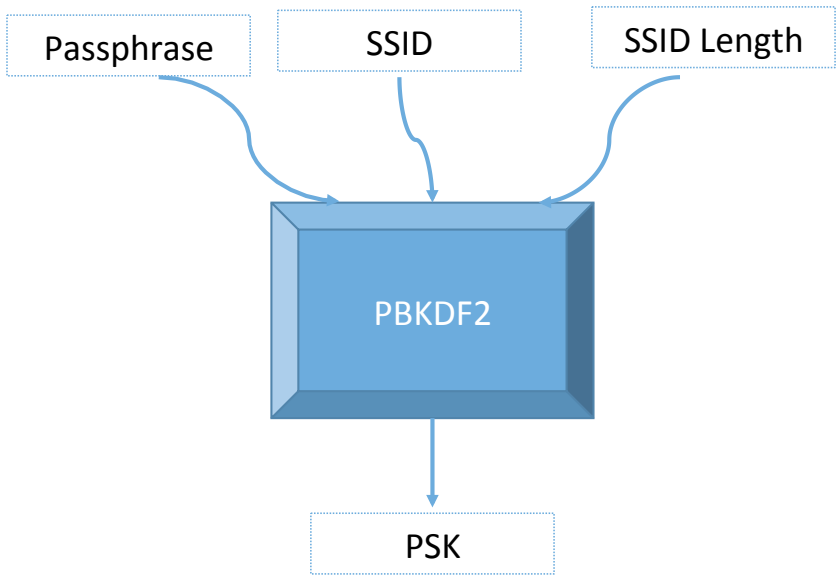
Les transparents suivants sont issus de http://webpages.eng.wayne.edu/ fy8421/16sp-csc5991/slides/lab7/wpa2-cracking-kolias.pdf

WPA/WPA2 Four Way Handshake

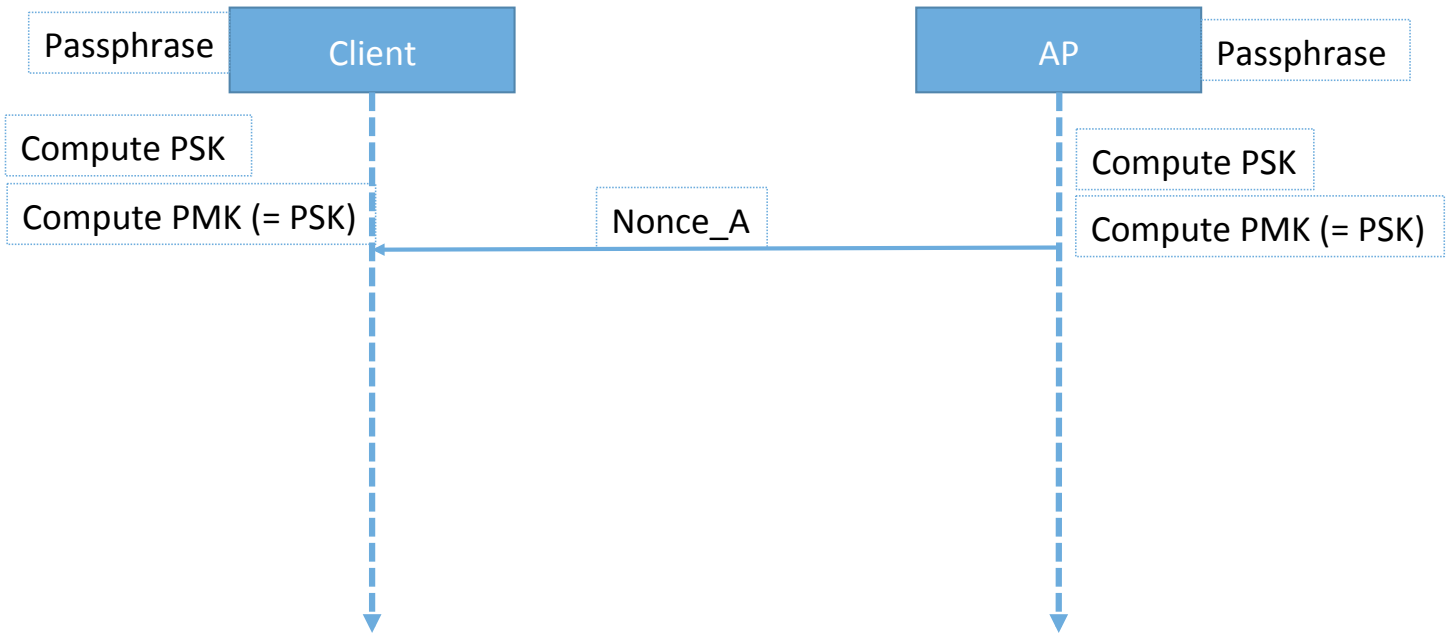
WPA/WPA2 Four Way Handshake

Computation of PSK

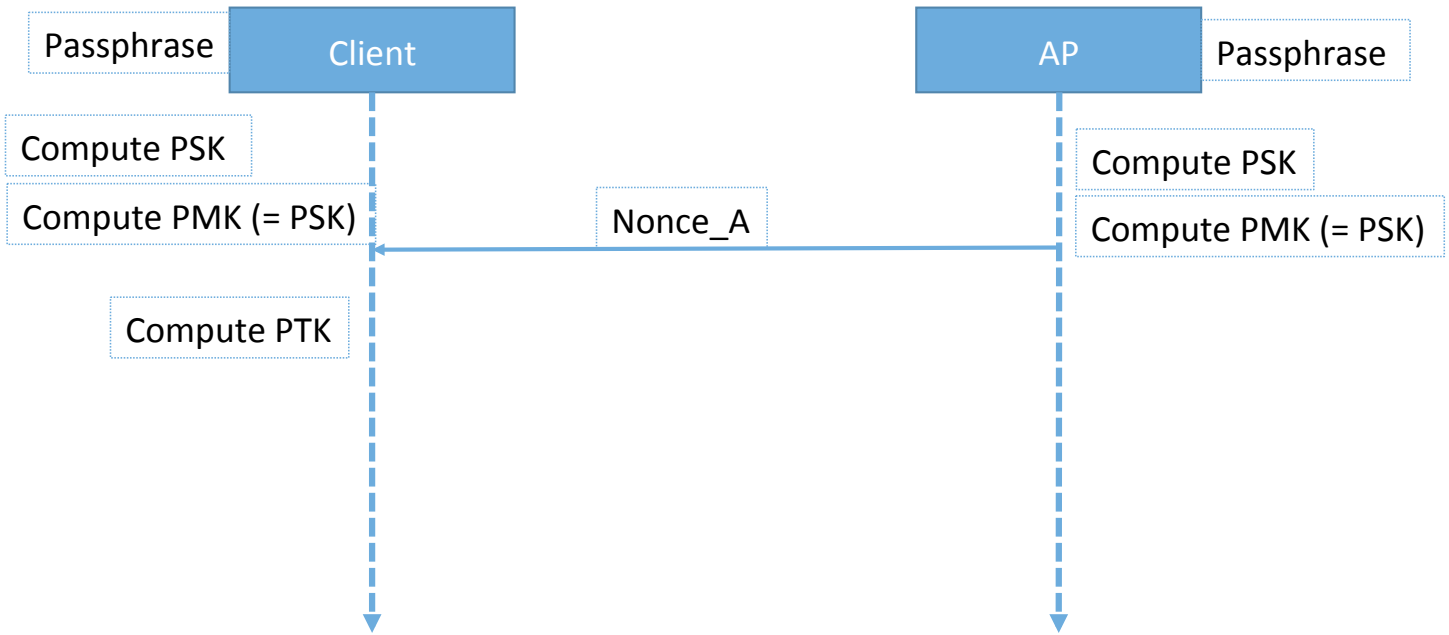
- Passphrase is a secret “phrase” you choose during the AP configuration
  - 8-63 characters long
- It is also the secret you insert in your device when you connect to a network
- SSID is the name of network
- PBKDF2 hashes 3 components 4096 times
- Heavy computation



WPA/WPA2 Four Way Handshake

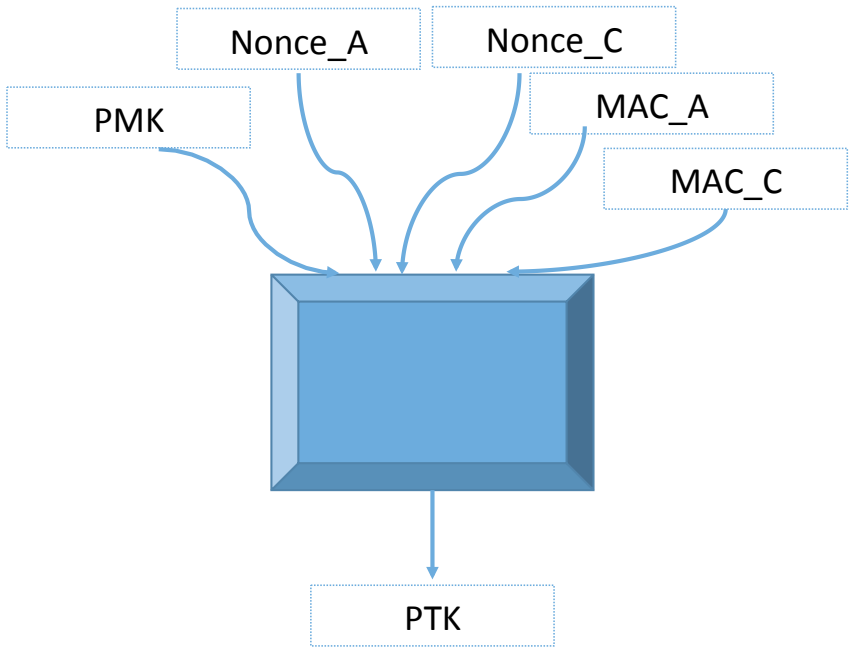


WPA/WPA2 Four Way Handshake

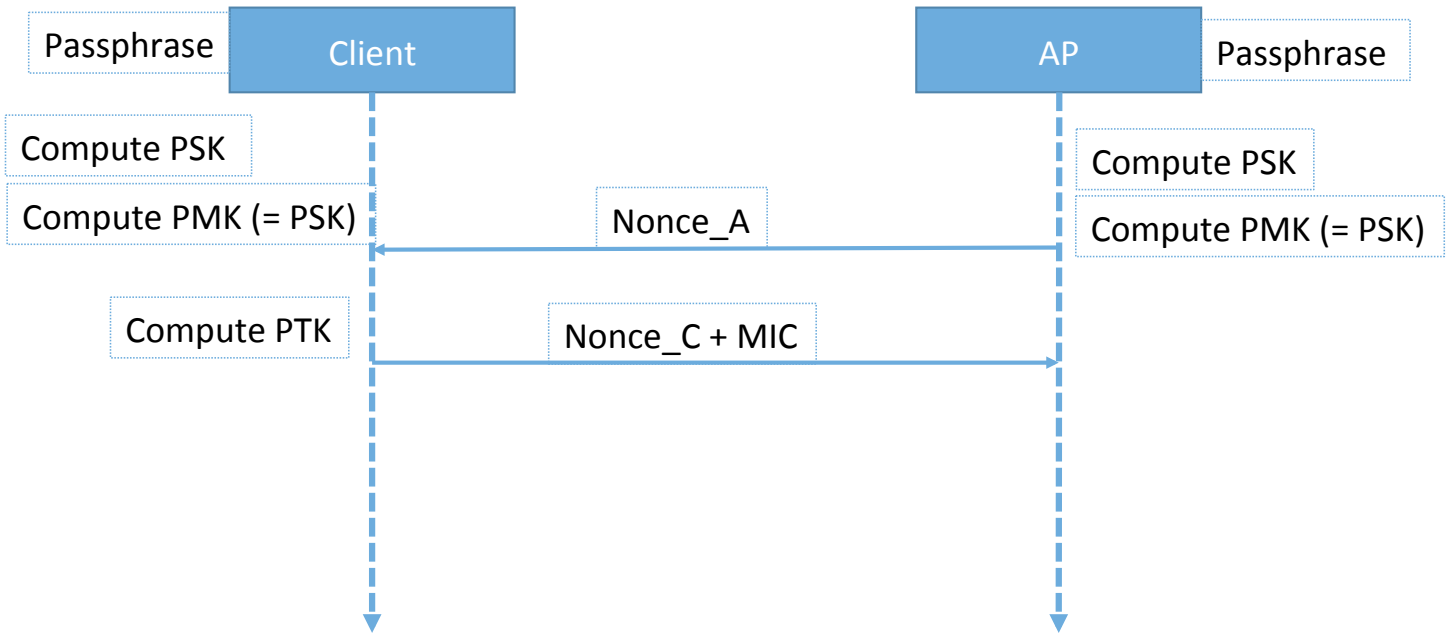


Computation of PTK

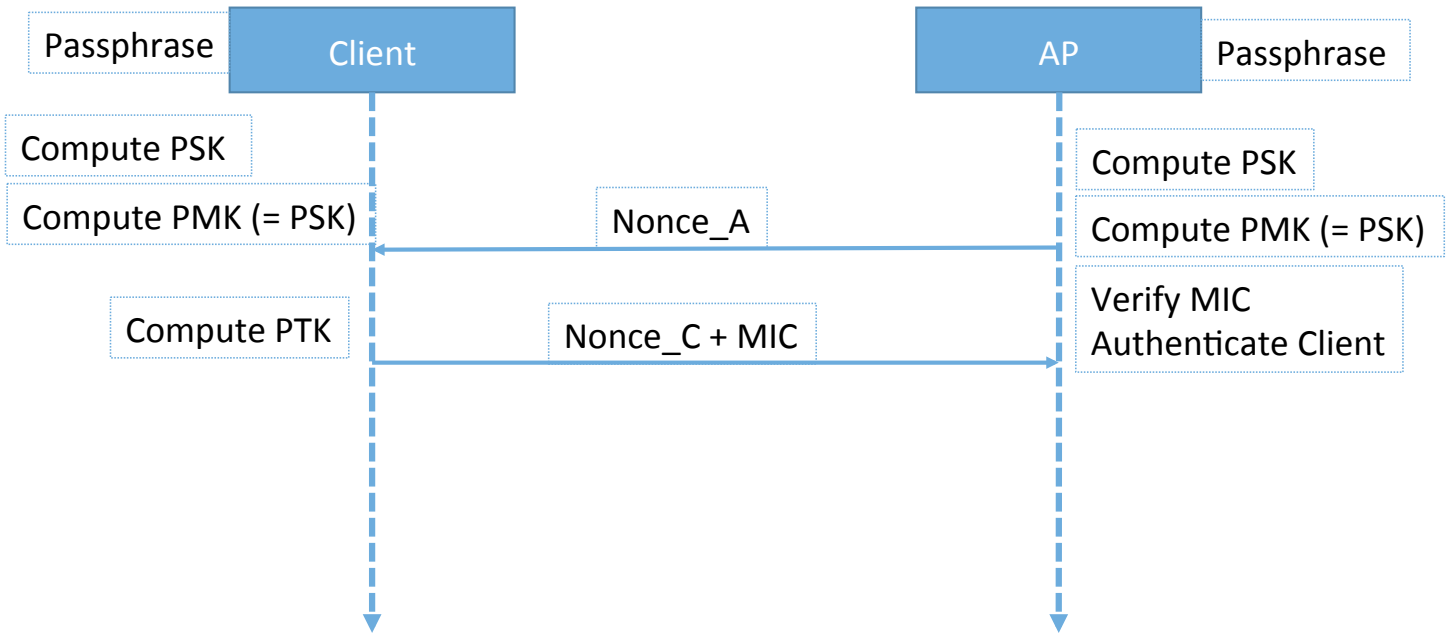
- PMK is derived from the Passphrase
- Nonce_A is a random number chosen by the AP and received through the first message
- Nonce_C is a random number chosen by the client
- MAC_A the hardware address of the AP
- MAC_C the hardware address of the client



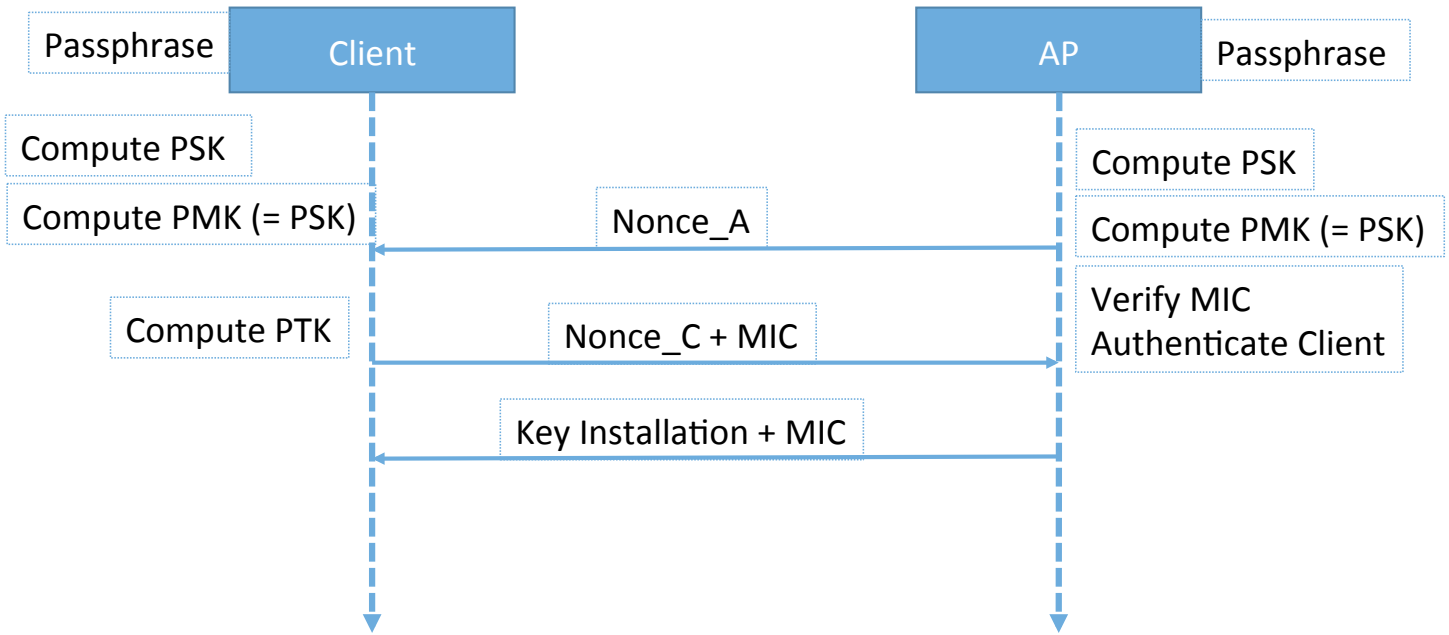
WPA/WPA2 Four Way Handshake



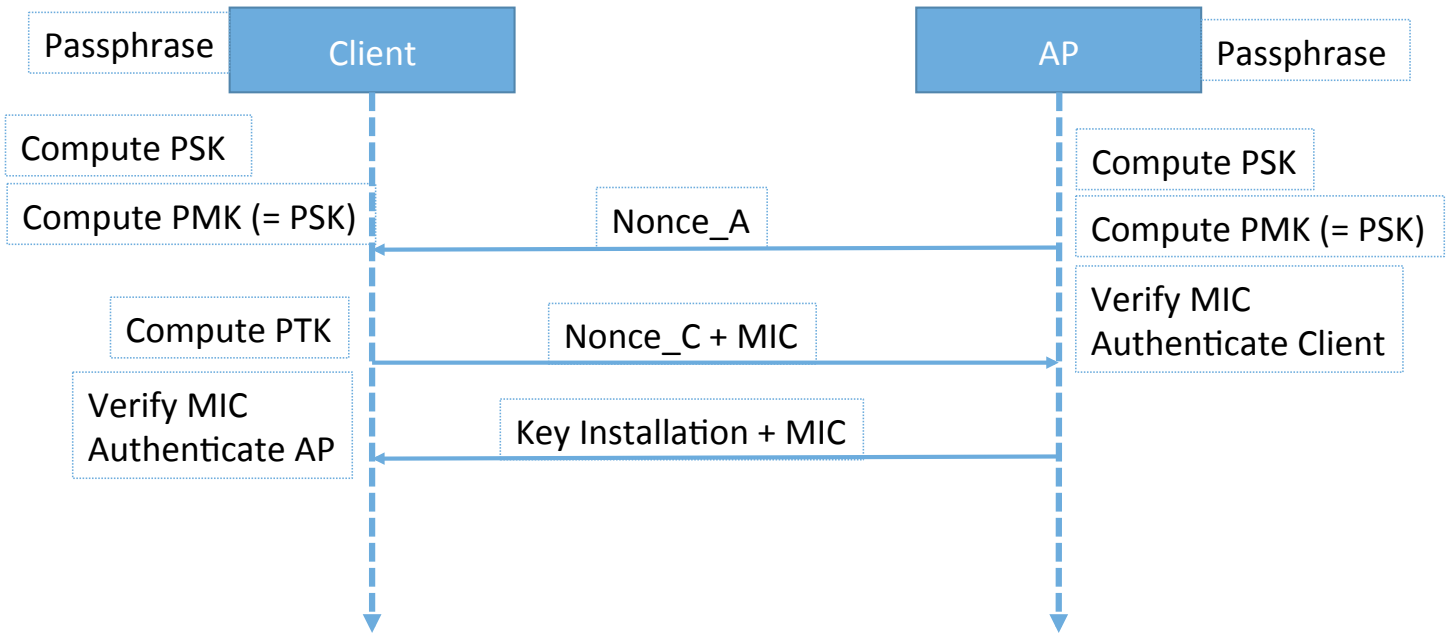
WPA/WPA2 Four Way Handshake



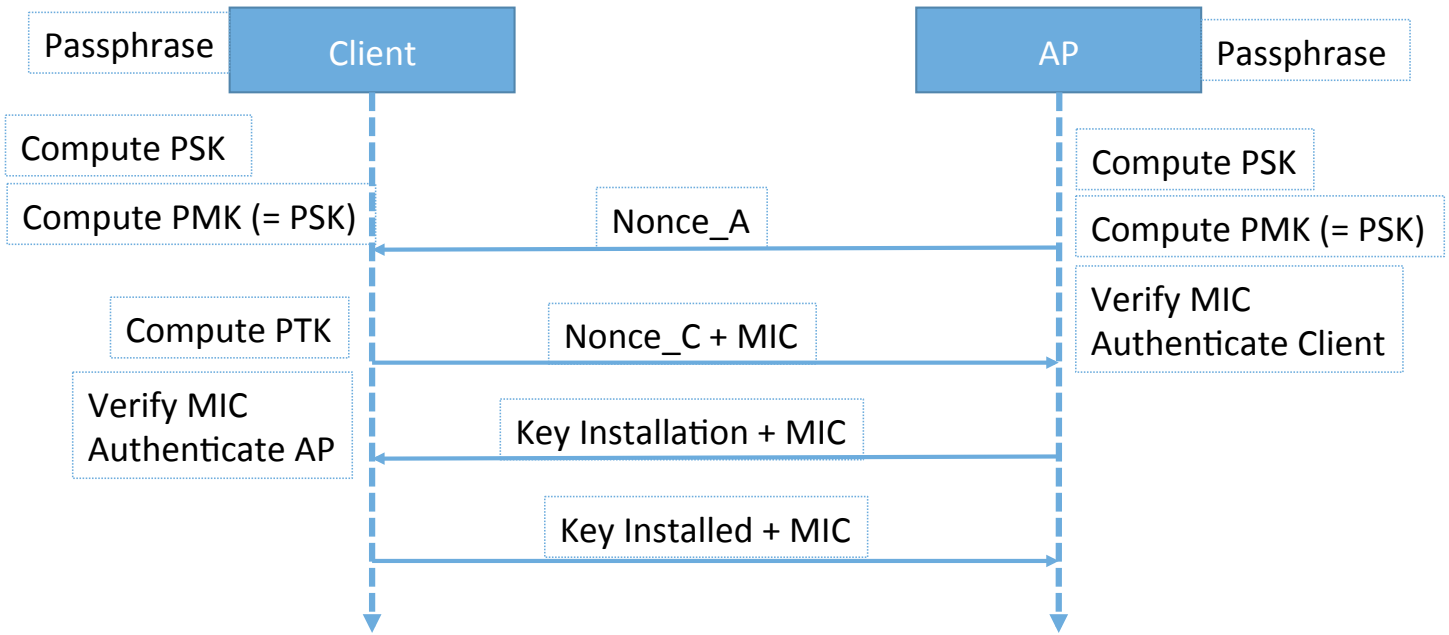
WPA/WPA2 Four Way Handshake



WPA/WPA2 Four Way Handshake



WPA/WPA2 Four Way Handshake



TKIP

- Utilisation de RC4 comme algorithme de chiffrement (pour des raisons économiques).
- Utilisation d'un algorithme de hachage cryptographique non-linéaire : MIC (*Message Integrity Code*) basé sur Michael.
- Impossibilité d'utiliser le même IV avec la même clé (l'IV joue maintenant le rôle d'un compteur appelé TSC (*TKIP Sequence Counter*)) et augmentation de la taille de l'IV à 48 bits.
- Utilisation de clé à 128 bits.
- Intégration de mécanisme de distribution et de changement des clé.
- Utilisation de clés différentes pour le chiffrement de chaque paquet.

MIC (dit *Michael*)

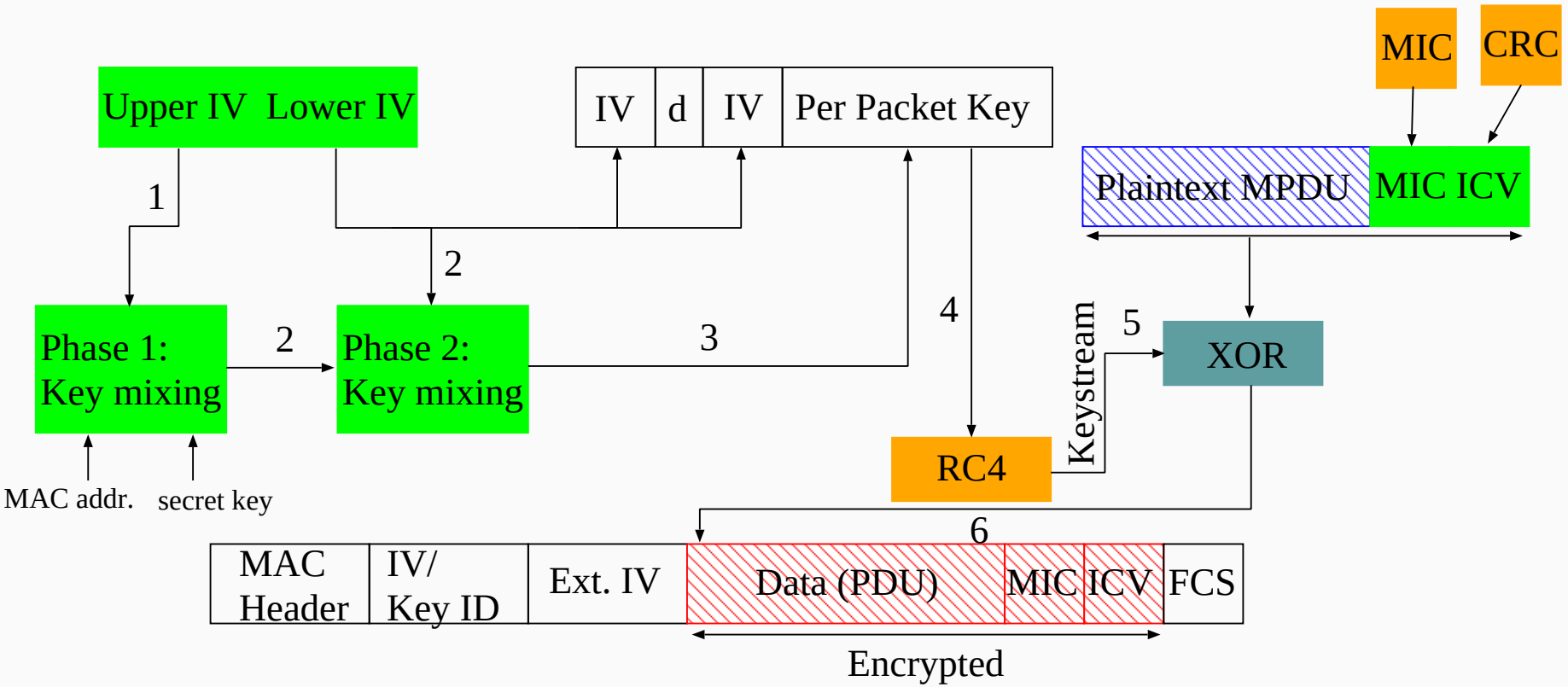
- Contrôle d'intégrité basé sur HMAC-SHA1 (clé de 64 bits) créé spécialement pour les besoins TKIP (contraintes processeur).
- Authentifie l'émetteur et le récepteur.
- Calcul d'un code de hachage, puis chiffrement de ce dernier à l'aide d'une clé secrète.
- Plusieurs algorithme de chiffrement peuvent être utilisés pour la dernière étape.

MIC (dit *Michael*)

En pratique :

- Les points d'accès ne peuvent pas faire des calculs intensifs.
- TKIP utilise une méthode de calcul appelée *Michael*.
- *Michael* utilises des opérations simples d'addition et de décalage en lieu et place des multiplications.
- *Michael* est utilisé sur les MSDU (au lieu des MPDU). (une MSDU peut correspondre à une série de MPDU).
  - Le calcul du code peut être fait au niveau du pilote au lieu d'être fait sur la carte elle même.
  - Réduction de coût vu que *Michael* n'est pas calculé pour chaque paquet de la couche physique (MPDU) envoyé.
- *Michael* étant "simple", il n'offre pas une forte sécurité.
- Pour palier les faiblesse, *Michael* offre un ensemble de contremesures :
  - Arrêt des communications (désactivation des clés) pendant une minute lors de la détection d'une attaque sur une station.

Schéma TKIP


MIC
CRC
Upper IV
Lower IV
IV
d
IV
Per Packet Key
Plaintext MPDU
MIC ICV
1
2
2
3
4
5
Phase 1:
Key mixing
Phase 2:
Key mixing
Keystream
XOR
RC4
MAC addr.
secret key
6
MAC
Header
IV/
Key ID
Ext. IV
Data (PDU)
MIC
ICV
FCS
Encrypted

TKIP et envoi de trames

Pour chaque trame de la couche MAC (MSDU) :

1. Calculer le code MIC sur la trame en utilisant une clé MIC dérivée de la clé principale.
2. Ajouter MIC à la trame.
3. Fragmenter la trame si besoin est au niveau de la couche physique (MPDU).
4. Générer un IV pour chaque MPDU.
5. Utiliser l'IV ainsi que la clé principale pour générer la clé de chiffrement de paquet.
6. Ajouter l'IV à la MPDU.
7. Chiffrer le contenu de la MPDU.
8. Envoyer la MPDU.

TKIP et réception de trames

À L'arrivée d'une MPDU :

1. Extraire l'IV.
2. Vérifier le numéro de séquence. S'il n'est pas valide, alors la trame est rejetée.
3. Générer la clé de paquet à partir l'IV et de la clé principale.
4. Déchiffrer le paquet.
5. Rassembler les MPDU correspondant à une même MSDU (si le paquet reçu est la dernière MPDU).
6. Calculer le code MIC et le comparer à celui contenu dans le message. S'il le résultat est différent, rejeter toute la MSDU.
7. Faire remonter la MSDU aux couches supérieures.

CCMP (*Counter mode-CBC MAC Protocol*)

- Protocole de sécurité basé sur le chiffrement *AES* en mode *CCM* (clé et bloc de 128 bits).
- N'est pas un compromis comme *TKIP*.
- Repose sur une refonte des mécanismes de sécurité.
- *CCM* combine *CTR* pour la confidentialité et *CBC-MAC* pour l'authenticité et l'intégrité.
- Est la base de *WPA2* qui est successeur de *WPA*.

Vulnérabilité de WPA

Attaque sur la PSK.

- Sécurité basée sur la qualité de la PSK.
- Solutions : choisir une PSK de plus de 20 caractères ou la générer directement en hexadécimal de manière aléatoire.

Attaque sur la poignée de main.

- Pas d'authentification sur le premier message.
- Le client se doit de conserver les données entre le premier et le troisième message (la signature contenue dans le troisième message lui permettant de déduire la bonne clé temporelle).
- Exploitation : inondation du client par des trames n° 1 *spoofées*.
- Conséquence : problème de mémoire sur le client.

Attaques sur WPA/WPA2 (1/2)

Attaque de Beck et Tews sur RC4 (2011)

- Adaptation de Chopchop au contexte WPA.
- Utilise les canaux de QoS de WPA.
- Améliorée plus tard par l'attaque Ohigashi-Morii en ajoutant un MiTM au processus.

Hole196 (2011)

- Attaque visant à mettre en place un MiTM sans le borne ne s'en aperçoive.
- Première attaque visant WPA2.
- Exploitation d'un problème dans la norme WPA2 concernant l'utilisation de la GTK.

Attaques sur WPA/WPA2 (2/2)

KRACKs (2017)

- Attaques visant la poignée de main WPA2.
- Permet de forcer le client et la borne à réutiliser des clés de chiffrement.

KrooK (2019)

- Attaque exploitant des failles certains types de cartes.
- Permet de forcer la carte à utiliser une clé nulle pour le chiffrement des paquets.
- N'est pas liée à KRACK mais a été mise en évidence en étudiants les différentes variantes de KRACK.

Plan

WEP

WPA/WPA2

WPA3

WPA3

- Le mode Open est remplacé par OWE - Opportunistic Wireless Encryption
  - Problème : tout le trafic sans fil est passé au clair.
  - Solution : tout le trafic sans fil est chiffré.
- Le mode PSK est remplacé par le mode SAE (Simultaneous Authentication of Equals)
  - Problème : une attaque passive entraîne une attaque de dictionnaire hors ligne pour découvrir la PSK.
  - Solution : le protocole est résistant aux attaques actives, passives et par dictionnaire.
- Le mode Entreprise fournit désormais des ciphresuites très robustes.

“Passwords are like underwear: don’t let people see ‘em, change ‘em very often, and you shouldn’t share ‘em with strangers.”

- Chris Pirillo, blogger, on-line celebrity

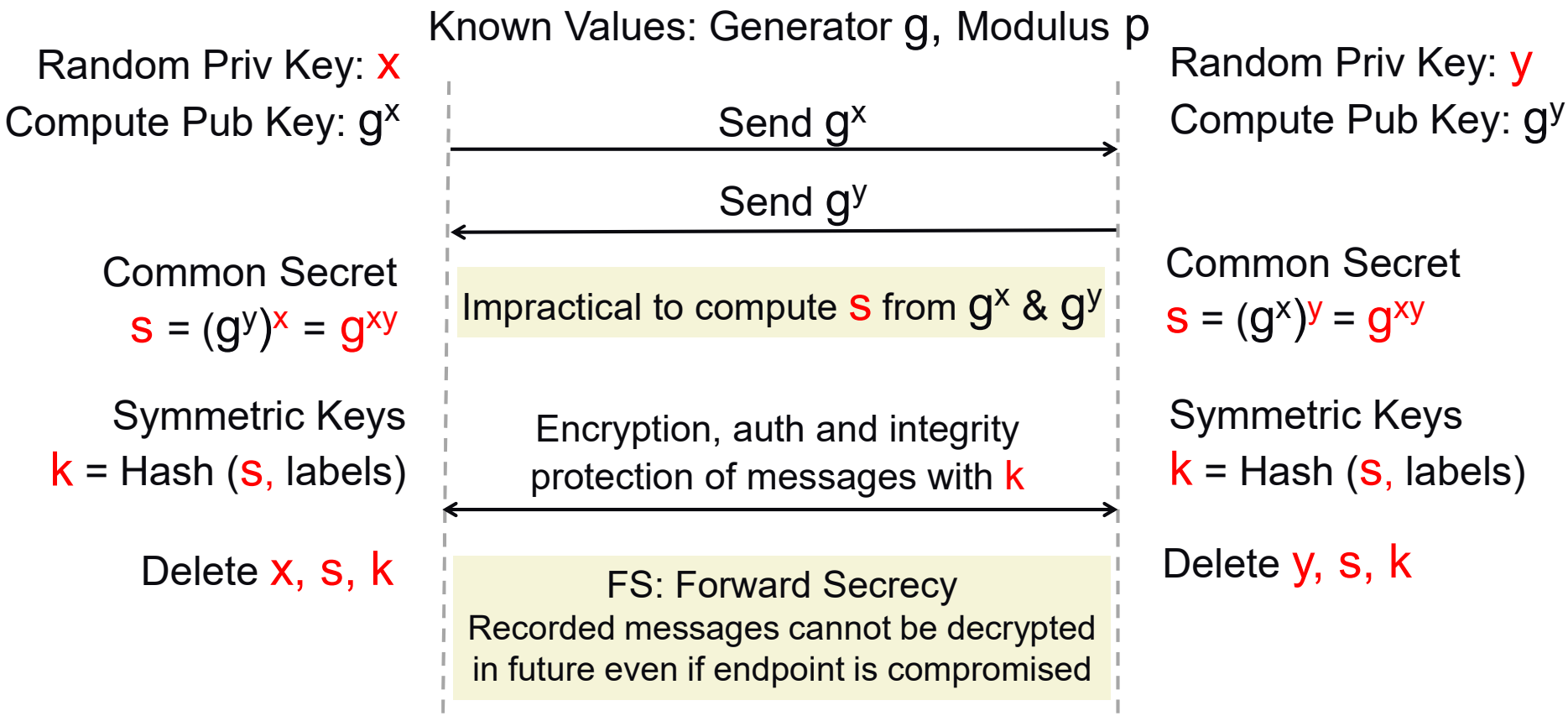
OWE (*Opportunistic Wireless Encryption*)

OWE (RFC 8110)

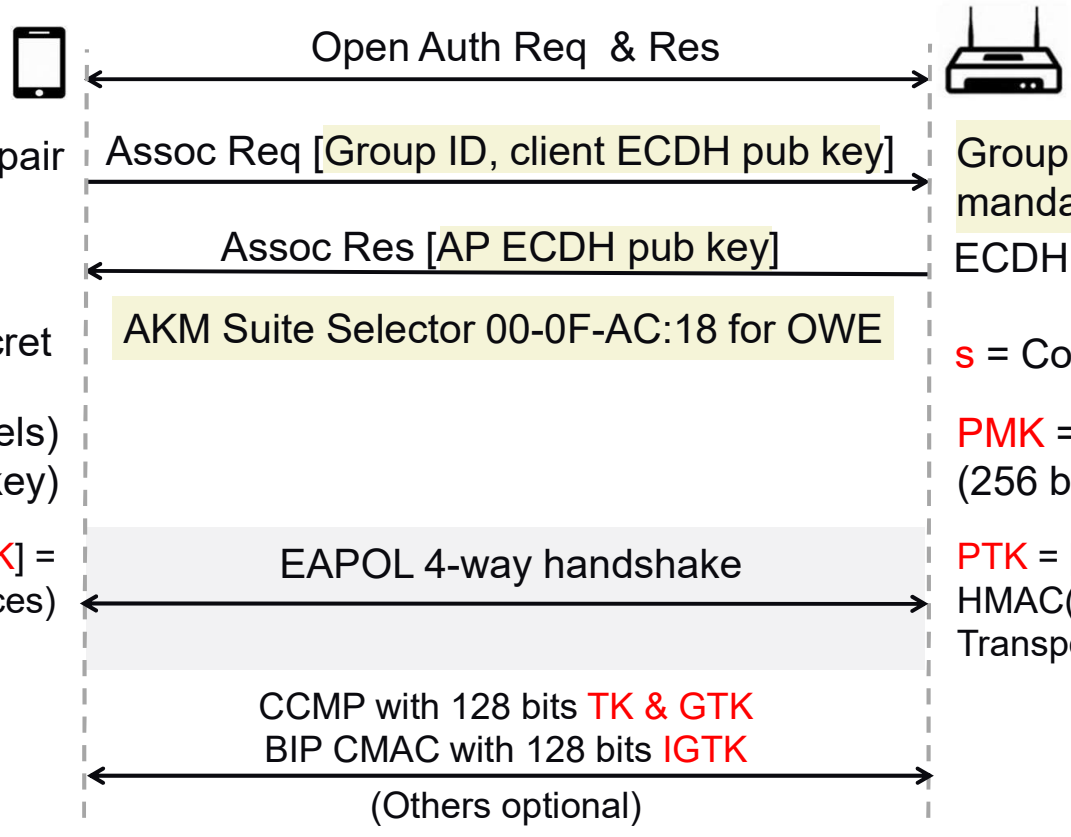
- OWE effectue un échange Diffie-Hellman non authentifié au moment de l'association
  - Requêtes d'association et réponses échanges les clés publiques de Diffie-Hellman
  - Le STA et l'AP calculent une PMK à la suite de l'association
  - La PMK est utilisée dans une poignées de main pour générer les clés de chiffrement
- L'aspect non-authentifié n'est-il pas dangereux ?
  - Oui, il n'y a aucune garantie concernant qui se connecte à quoi
  - Mais c'est plus sûr qu'une PSK partagée et publique (dans un café !)
- Totalement transparent pour les utilisateurs - ressemble à Open
  - Une sécurité accrue sans complexité supplémentaire !
- Cas d'utilisation :
  - Cafés, bars, partout où le chiffrement est nécessaire mais où l'authentification ne l'est pas

source https://d2cpnw0u24fjm4.cloudfront.net/wp-content/uploads/WLPC_2019_WPA3-OWE-and-DDP_Hemant-Chaskar.pdf

Key Generation Steps



OWE Message Flow

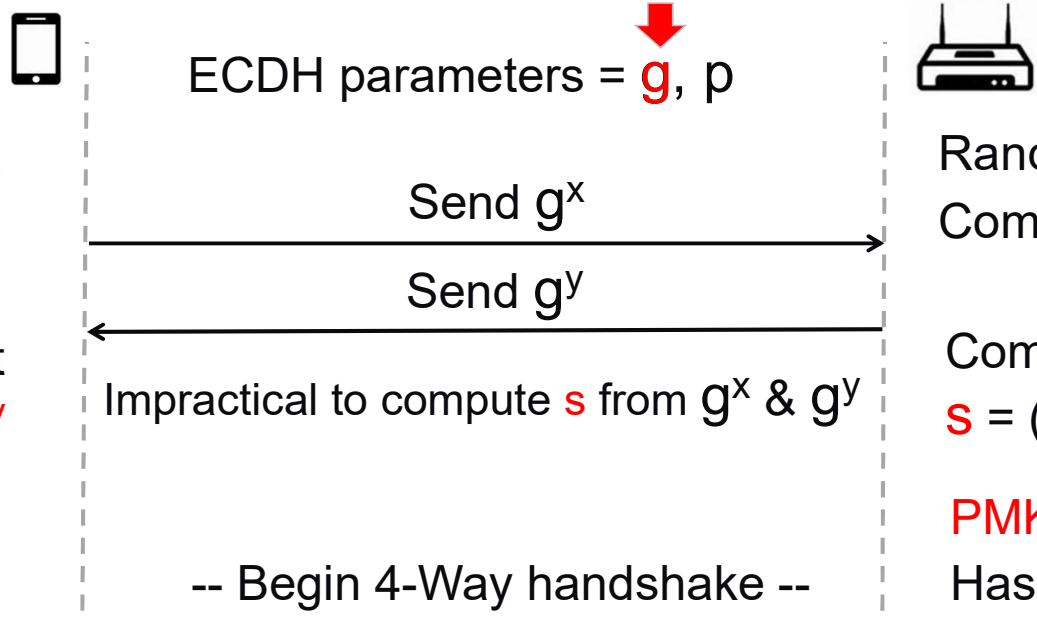


Simultaneous Authentication of Equals (*Drangonfly*)

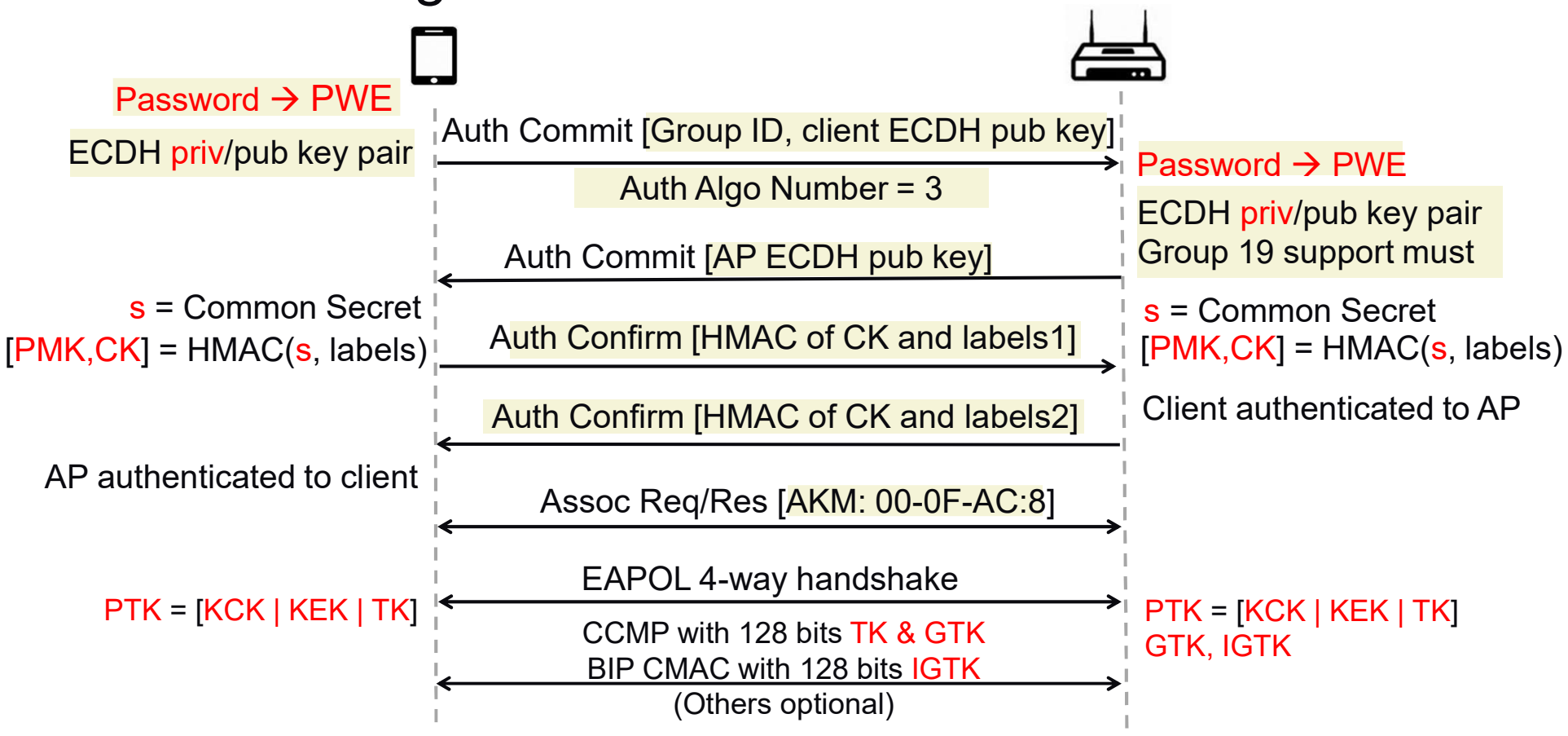
- Dragonlfy: Poignée de main basée une zero knowledge proof
  - Problème classique des protocoles de mots de passe : vous passez en premier !
  - La zero knowledge proof prouve que vous savez quelque chose mais n'expose pas ce que c'est
- Caractéristiques de sécurité de la SAE :
  - L'observation passive de l'échange ne révèle rien
  - Une attaque active révèle si une simple supposition du mot de passe était correcte ou non
  - Une attaque par dictionnaire hors ligne n'est pas possible
- Le résultat du SAE est une clé connue par seulement des 2 entités
  - Garantit la PFS même dans le cas où un agresseur connaît le mot de passe
- Résiste aux attaques par dictionnaire.
- *Protected Management Frames* (PMF) est obligatoire.

SAE = OWE + Password

- g is derived as function of password (and MAC adrs). It is called PWE (PassWord Element).
- p is still taken from standard set.



SAE Message Flow



WPA3-SAE: attaques

Dragonblood - 2019

- Les attaques contre le protocole ne sont pas pertinentes (groupes faibles) ou peuvent être traitées par d'autres moyens (attaque DoS)
- L'attaque en mode de transition n'est pas une véritable attaque
- L'attaque par side channel est très grave mais n'est pas une attaque contre la norme
- La mise en oeuvre susceptible d'être attaquée par les side channels a déjà été corrigée
- WPA3-SAE est toujours un protocole robuste

WPA3 Entreprise

- Fondamentalement la même implémentation que 802.1X/EAP basé sur l'authentification, l'autorisation et la comptabilité
- Qu'est ce qui est différent pour l'AP ?
  - *Protected Management Frames* (PMF) est obligatoire
  - Le mode de transition consiste à demander PMF : Les clients WPA3 se connecteront en utilisant PMF alors que les clients WPA2 ne supportant pas PMF se connecteront sans PMF
- Qu'est ce qui est différent pour les clients ?
  - PMF est obligatoire
  - Validation des certificats et Validation de la chaîne de certificats
- Tout ceci si vous n'utilisez pas la suite B/CNSA qui impose les ciphersuites à utiliser et est extrêmement contraignante.

802.1x EAP-TLS 192-bit Security

TLS_ECDHE_ECDSA_WITH_
AES_256_GCM_SHA384;
with P-384

[Server ECDSA static pub key]$_{\text{in x509 cert}}$

[Server ECDH pub key]$_{\text{Sig by server ECDSA static priv key}}$

ECDHE_ECDSA with both being keys from P-384 curve (Group 20)

[Client ECDSA static pub key]$_{\text{in x509 cert}}$

[Client ECDH pub key]$_{\text{Sig by client ECDSA static priv key}}$

ECDHE_ECDSA with both being keys from P-384 curve (Group 20)

Symmetric key gen with HMAC-SHA-384

TLS tunnel with encryption and integrity protection

AES-GCM with 256 bits key

PMK

PMK transport outside of WPA3 scope: Use IPSec, RadSec etc.

4-way handshake

AKM #12: KCK 192 bits, KEK 256 bits

Encrypted wireless link

Ciphers #09 & #12: GCMP and BIP GMAC with 256 bits key