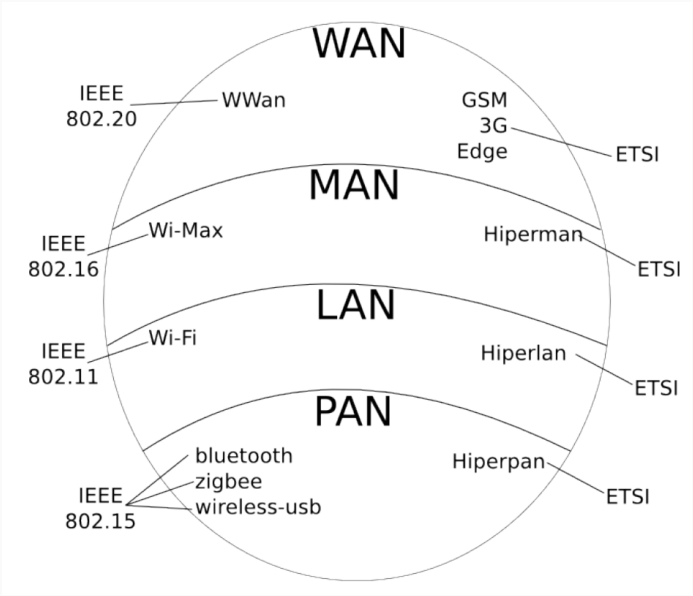
Sécurité des réseaux non-filaires

Sécurité des réseaux Wifi

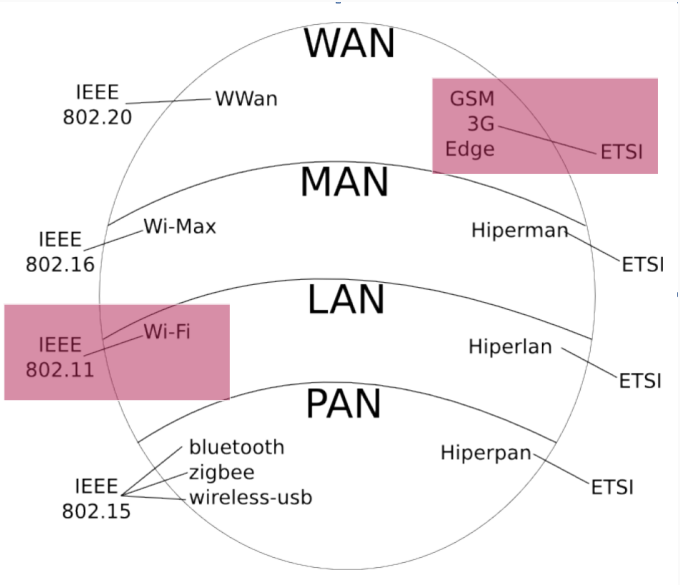
Anaïs Gantet, Benoît Camredon

TLS-SEC 2019/2020

Le monde du sans fil



Le monde du sans fil



Dans ce cours

Le réseau Wifi, 802.11

- Rappels de terminologie du Wifi
- Evolution des sécurisations existantes
  - WEP
  - WPA
  - WPA2
- Attaques sur le 802.11

Dans ce cours

Le réseau Wifi, 802.11

- Rappels de terminologie du Wifi
- Evolution des sécurisations existantes
  - WEP
  - WPA
  - WPA2
- Attaques sur le 802.11

Eléments de réponses à :

- @Architecte : quelle solution préconiser ?
- @Red Team : points faibles à auditer ?
- @Blue Team : quoi surveiller ?

Rappels des bases du 802.11

Les normes 802.11

802.11 : norme IEEE publiée en 1999 et amendée au fil du temps

Les normes 802.11

802.11 : norme IEEE publiée en 1999 et amendée au fil du temps

- Exemples d'amendements précédents
  - 11a/11b/11g/11n/11ac(/11ax) : description de la couche physique
  - 11d/f : sur les domaines réglementaires
  - 11e : sur de la QoS additionnelle
  - 11i : sur la sécurité

Topologies réseau dans chaque cellule

Vocabulaire 802.11

- AP : access point
- STA : stations
- BSS : Basic Service Set

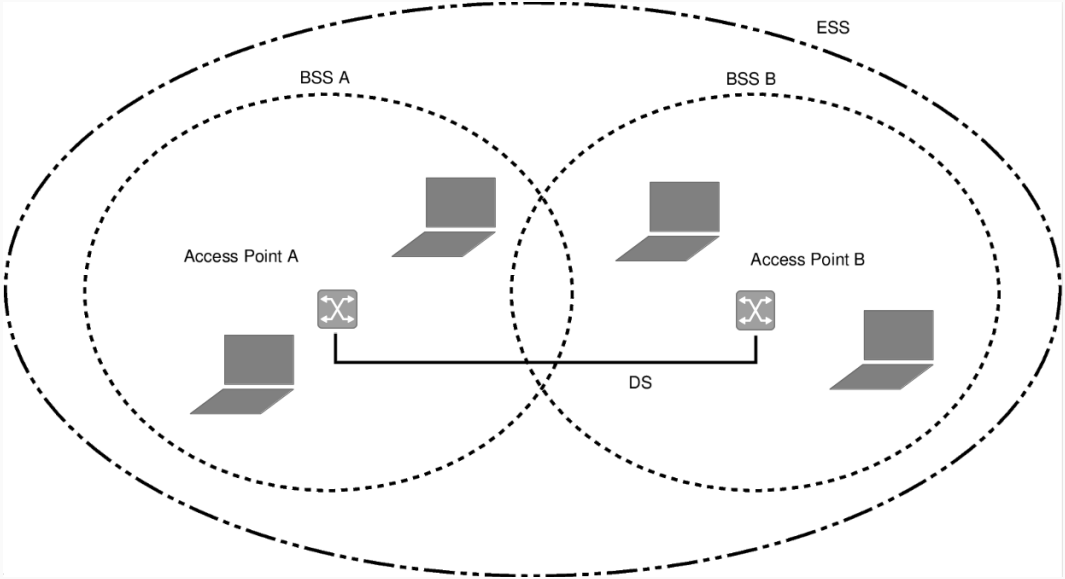
802.11 offre 2 modes d'opération

- Le mode Infrastructure : Le réseau est traité par une entité centrale, appelée point d'accès (AP)
- Le mode Adhoc : chaque participant peut créer et maîtriser un réseau

Les deux modes peuvent étendre des réseaux

- Avec le mode WDS (Wireless Distribution System) pour le mode infrastructure
- Avec des structures maillées pour le mode adhoc

BSS, DS, ESS, etc.



Informations et configuration de l'interface réseau sur le client (Linux)

- `iwconfig`
- `iwlist`

```
$ iwlist [interface] frequency
         [interface] channel
         [interface] bitrate
         [interface] rate
         [interface] power
         [interface] txpower
         [interface] ap
         [interface] accesspoints
         [interface] peers
         [interface] event
         [interface] modulation
```

Informations sur les AP environnants

- `iwlist scanning`

Scan et informations des AP environnants

```
$ iwlist wlan0 scanning
wlan0     Scan completed :
Cell 01 - Address: 11:11:11:11:11:11
          Channel:11
          Frequency:2.462 GHz (Channel 11)
          Quality=27/70  Signal level=-83 dBm
          Encryption key:off
          ESSID:"TLS-SECbox-open"
          Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 22 Mb/s
                    6 Mb/s; 9 Mb/s; 12 Mb/s
          Bit Rates:18 Mb/s; 24 Mb/s; 36 Mb/s; 48 Mb/s; 54 Mb/s
          Mode:Master
          ...
```

```
Cell 02 - Address: 11:22:33:44:55:66
          Channel:6
          Frequency:2.437 GHz (Channel 6)
          Quality=51/70  Signal level=-59 dBm
          Encryption key:on
          ESSID:"TLS-SEC-box-000"
          Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 6 Mb/s
                    9 Mb/s; 12 Mb/s; 18 Mb/s
          Bit Rates:24 Mb/s; 36 Mb/s; 48 Mb/s; 54 Mb/s
          Mode:Master
          ...
          IE: IEEE 802.11i/WPA2 Version 1
              Group Cipher : TKIP
              Pairwise Ciphers (2) : CCMP TKIP
              Authentication Suites (1) : PSK
          IE: WPA Version 1
              Group Cipher : TKIP
              Pairwise Ciphers (2) : CCMP TKIP
              Authentication Suites (1) : PSK
```

Informations sur l'interface client

```
$ iwconfig wlan0
wlan0     IEEE 802.11  ESSID:"TLS-SEC-box-000"
          Mode:Managed  Frequency:2.437 GHz  Access Point: 11:22:33:44:55:66
          Bit Rate=144.4 Mb/s   Tx-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=48/70  Signal level=-62 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:398   Missed beacon:0
```

Différents types de trafic

802.11 repose sur 3 types de trafic :

Différents types de trafic

802.11 repose sur 3 types de trafic :

- Le trafic de contrôle (pour la bonne arrivée des trames entre les pairs)

Différents types de trafic

802.11 repose sur 3 types de trafic :

- Le trafic de contrôle (pour la bonne arrivée des trames entre les pairs)
- Le trafic de gestion (pour l'établissement et le maintien de la communication)

Différents types de trafic

802.11 repose sur 3 types de trafic :

- Le trafic de contrôle (pour la bonne arrivée des trames entre les pairs)
- Le trafic de gestion (pour l'établissement et le maintien de la communication)
- Le trafic de données (pour la transmission des données utilisateur)

La procédure d'association

L'*Association* est un concept clé des réseaux sans fil

- Choisir l'ESS via l'ESSID
- Choisir le BSS à l'intérieur de l'ESS
- Demander à s'authentifier (open vs. shared)
- Demander à s'associer
- Une fois associé, la communication peut s'effectuer à travers l'AP

À peu près équivalent à avoir son câble Ethernet pluggé

Protocoles de sécurisation du Wifi

Les schémas de sécurité du 802.11

Il existe 3 schémas de sécurité pour le 802.11, en plus de la version sans sécurité (réseau ouvert)

- WEP (Wired Equivalent Privacy)
- WPA (Wireless Protected Access)
- 802.11i/WPA2

Les schémas de sécurité du 802.11

Il existe 3 schémas de sécurité pour le 802.11, en plus de la version sans sécurité (réseau ouvert)

- WEP (Wired Equivalent Privacy)
- WPA (Wireless Protected Access)
- 802.11i/WPA2

Concerne essentiellement le trafic de données

Les schémas de sécurité du 802.11

Il existe 3 schémas de sécurité pour le 802.11, en plus de la version sans sécurité (réseau ouvert)

- WEP (Wired Equivalent Privacy)
- WPA (Wireless Protected Access)
- 802.11i/WPA2

Concerne essentiellement le trafic de données

Quelques outils

- `iwlist wlan0 keys/enc/auth/wpa`
- `hostapd - IEEE 802.11 AP, IEEE 802.1X/WPA/WPA2/EAP/RADIUS authenticator`
- `wpasupplicant`

Examples : information sur les protocoles supportés

- Côté AP :

```
$ iwlist wlan0 scanning
    Encryption key:on
    ...
    IE: IEEE 802.11i/WPA2 Version 1
        Group Cipher : TKIP
        Pairwise Ciphers (2) : CCMP TKIP
        Authentication Suites (1) : PSK
    IE: WPA Version 1
        Group Cipher : TKIP
        Pairwise Ciphers (2) : CCMP TKIP
        Authentication Suites (1) : PSK
```

- Côté interface client :

```
$ iwlist wlan0 auth
wlan0     Authentication capabilities :
    WPA
    WPA2
    CIPHER-TKIP
    CIPHER-CCMP
```

Exemples : connexion à des réseaux divers

Connexion à un réseau ouvert

```
# iwconfig wlan0 essid "TLS-SEC-open" channel 3 key off
# dhclient wlan0
```

Connexion à un réseau WEP

```
# iwconfig wlan0 essid "TLS-SEC-WEP" channel 4 key 1234ABCD
# dhclient wlan0
```

Connexion à un réseau WPA PSK avec wpasupplicant

```
network={
   ssid="TLS-SEC-WPA"
   scan_ssid=1
   proto=WPA
   key_mgmt=WPA-PSK
   psk="monmotdepassetressecurise"
}
```

```
# wpa_supplicant -D wext -i wlan0 -c
/etc/wpa_supplicant.conf &
# dhclient wlan0

Ou bien :

# wpa_supplicant -i "$IFACE" -c
<(wpa_passphrase "$SSID" "$PASSPHRASE")
```

WEP : Wired Equivalent Privacy

Un premier effort de sécurisation du lien de communication...

Chiffrement

- Basé sur RC4 (symétrique)
- Clé partagée entre AP/clients
- taille de clé : 40 bits

"Intégrité"

- CRC32

WEP : Wired Equivalent Privacy

Un premier effort de sécurisation du lien de communication...

Chiffrement

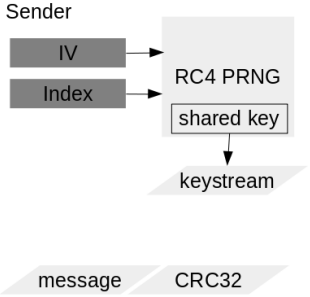
- Basé sur RC4 (symétrique)
- Clé partagée entre AP/clients
- taille de clé : 40 bits

"Intégrité"

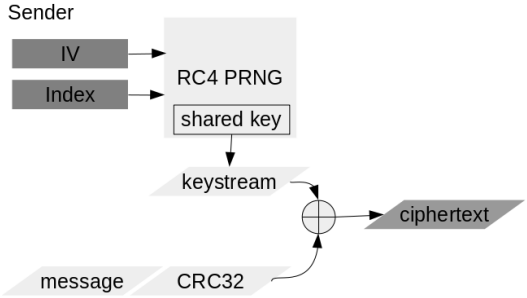
- CRC32

WEP aurait pu vouloir dire Weak Encryption Protocol...

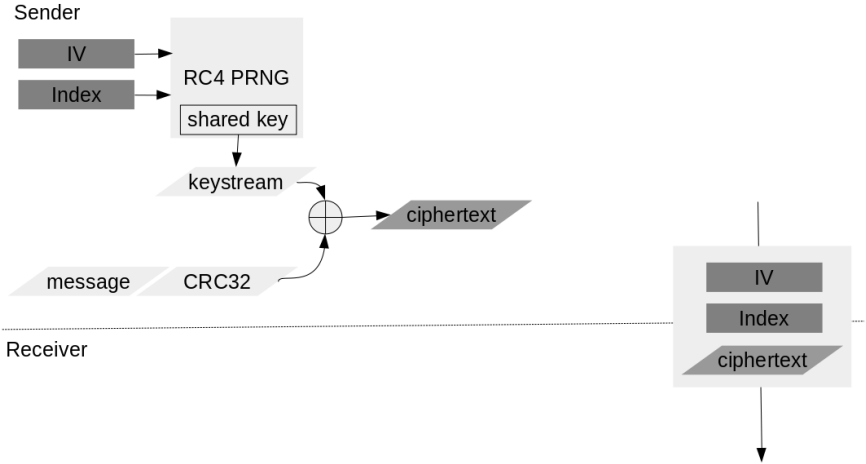
Chiffrement et intégrité WEP



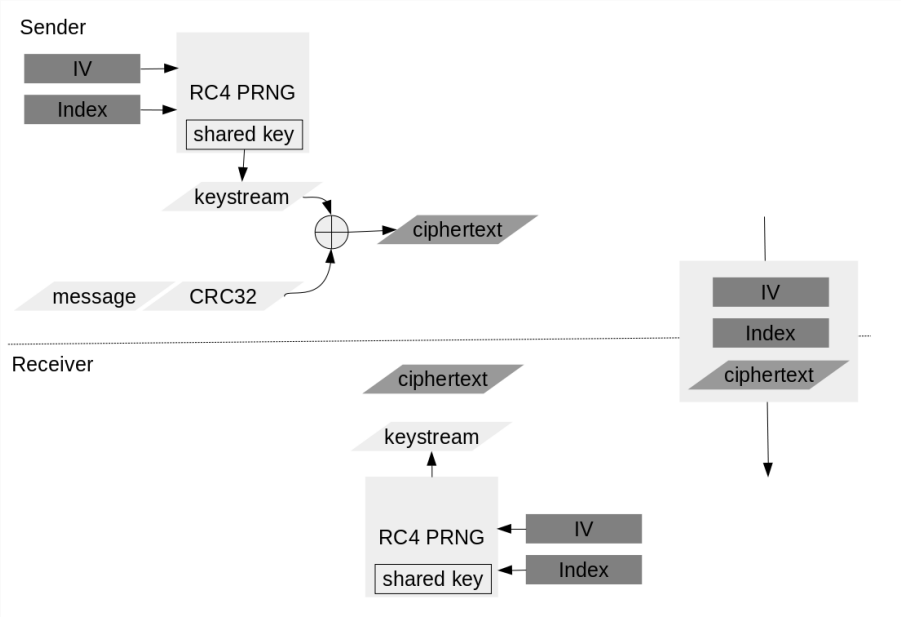
Chiffrement et intégrité WEP



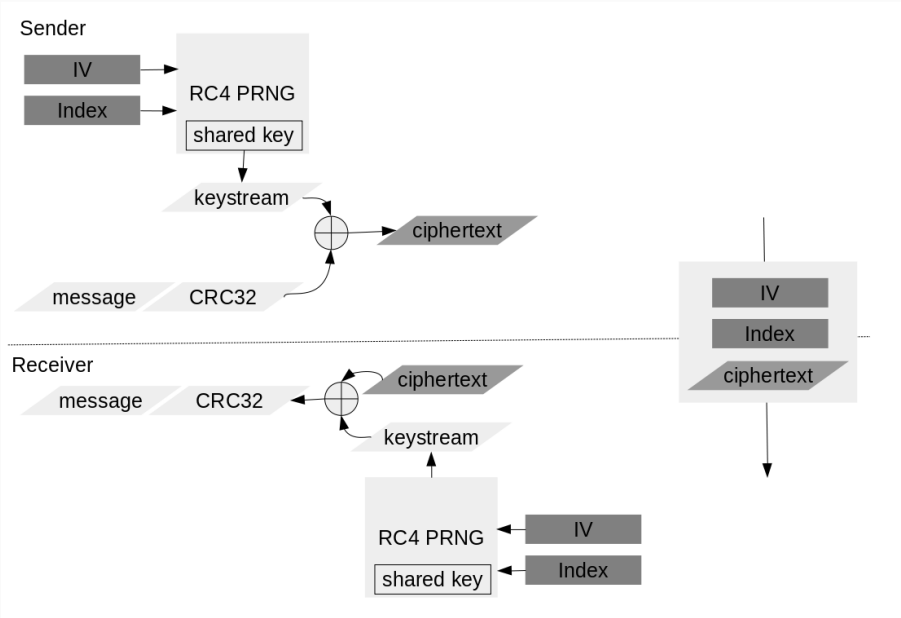
Chiffrement et intégrité WEP



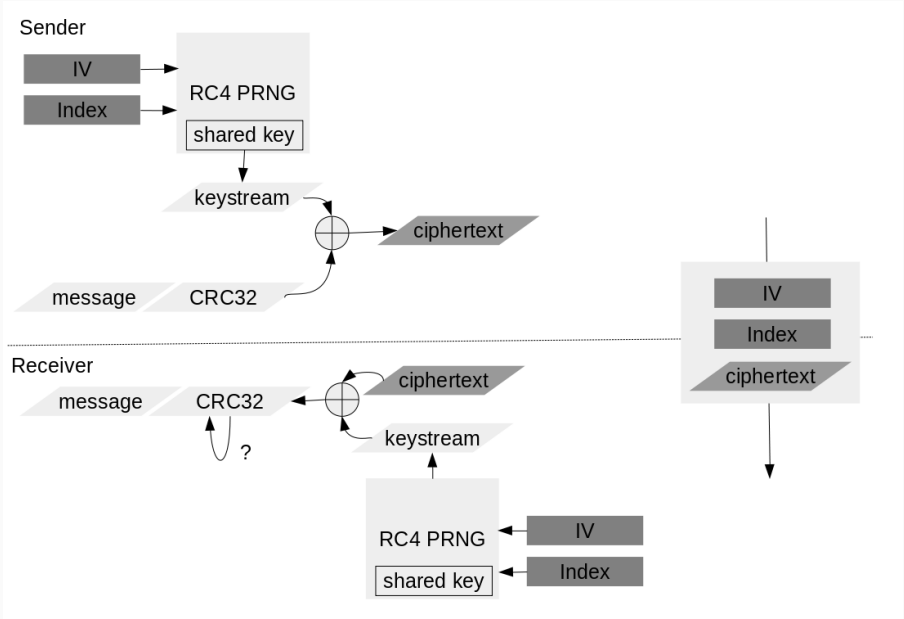
Chiffrement et intégrité WEP



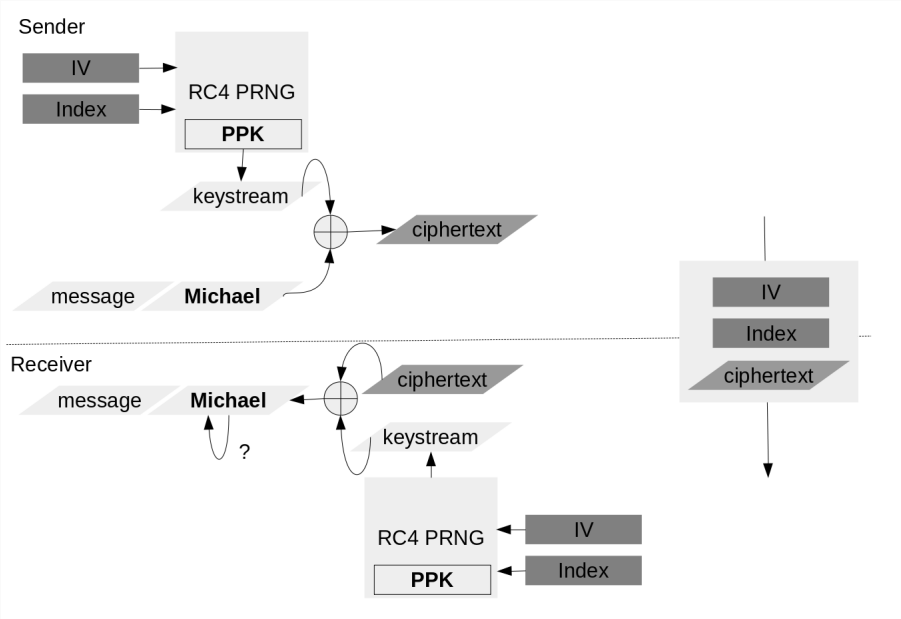
Chiffrement et intégrité WEP



Chiffrement et intégrité WEP



Chiffrement et intégrité WPA[1]



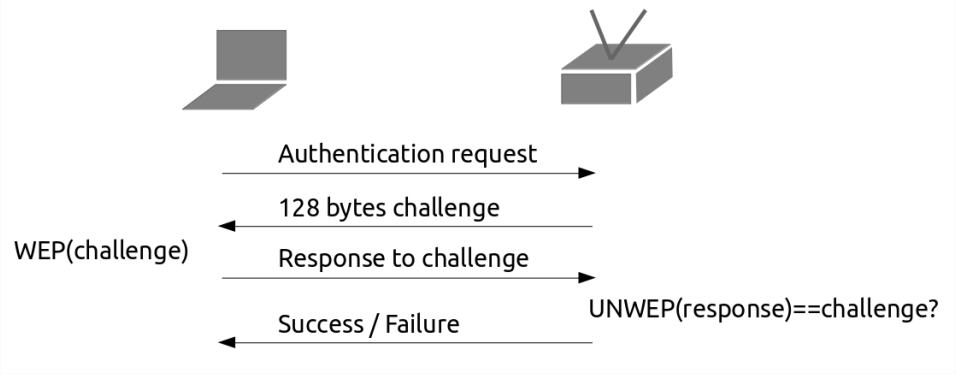
WPA2 et le mode CCM

CCMP est un protocole basé sur AES CCM

- N'a pas besoin de gérer la préparation de clés
- Offre du chiffrement AES-128
- Contient son propre MIC
- Authentifie la totalité des MPDU

Énorme progrès par rapport à TKIP...

4 messages handshake avec challenge et réponse



But : vérification de la connaissance de la clé K pré-partagée

Authentification WPA

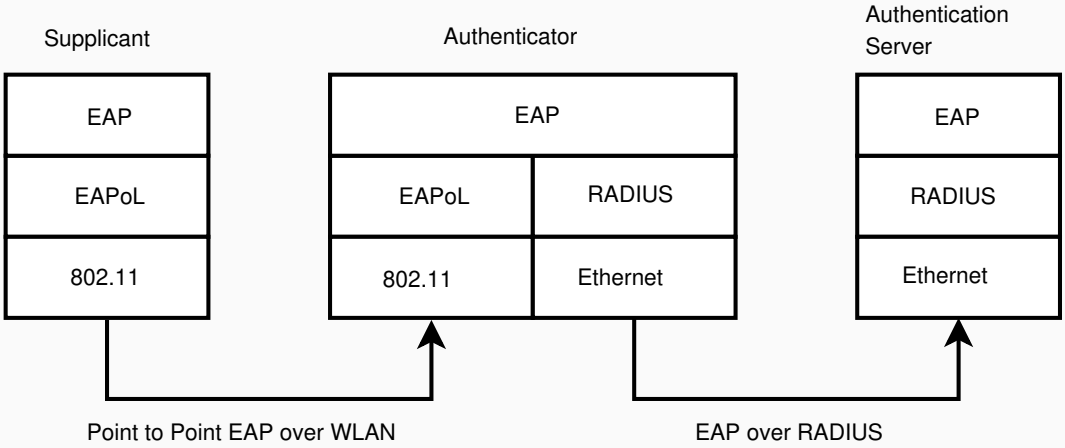
2 méthodes d'authentification possibles :

- WPA-personnel, ou WPA par secret pré-partagé (WPA-PSK)
- WPA-enterprise, ou WPA-802.1x ou WPA-EAP

802.1x définit le protocole d'authentification de la couche 2 pour l'ensemble des protocoles 802 (y compris filaires)

- Utilise un serveur RADIUS
- Se base sur le protocole EAP
- Un équipement de couche 2 pour relais EAP
- De nombreuses variantes de méthodes d'authentification (PEAP, EAP-TLS, etc.)

Chaine d'authentification du IEEE 802.1x



Le 802.1x supporte la distinction de *ports logiques*

- L'étape de handshake dans l'authentification gère la génération de clés
- Chaque association possède son propre ensemble de clés
- La durée de chaque association peut être limitée par un timeout

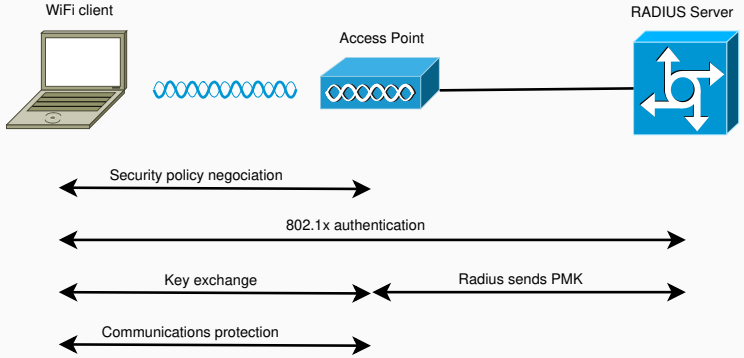
Avantages du 802.1x

- Le client ne peut pas accéder au réseau sans s'être authentifié
- Le 802.1x gère la distribution et la préparation de clés
- Il offre des mécanismes d'authentification forte

Robust Security Network (RSN)

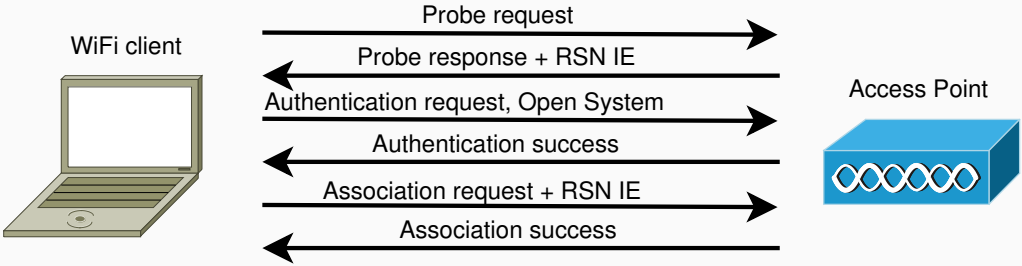
La norme 802.11i RSN décrit l'établissement d'une session 802.11i

- Négociation de la politique de sécurité
- Authentification 802.1x
- Distribution des clés
- Protection des communications réseaux

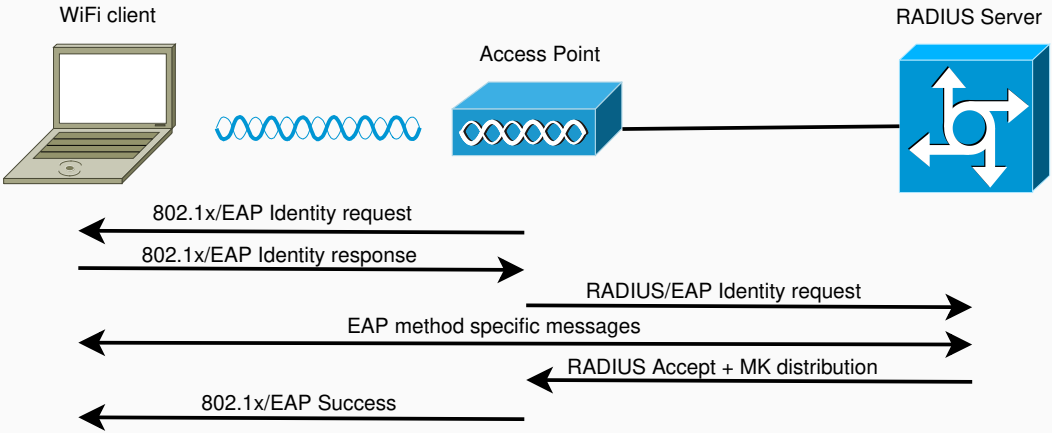


Négociation de la politique de sécurité

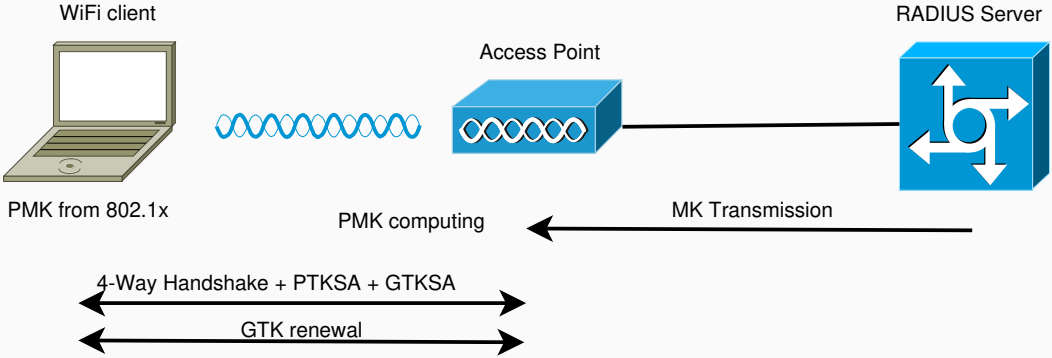
- Probe request
- Probe response dont le RSN IE
- Open authentication
- Association request avec le RSN IE du client
- Association success



Authentification 802.1x
Elle permet d'authentifier le client et d'effectuer un échange de Master Key

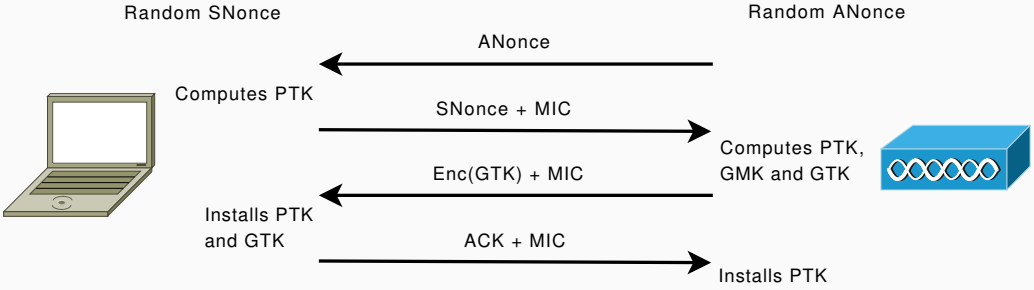


Echange de clé
La 3ème étape est la distribution de clés avec le 4-Way Handshake



4-Way Handshake

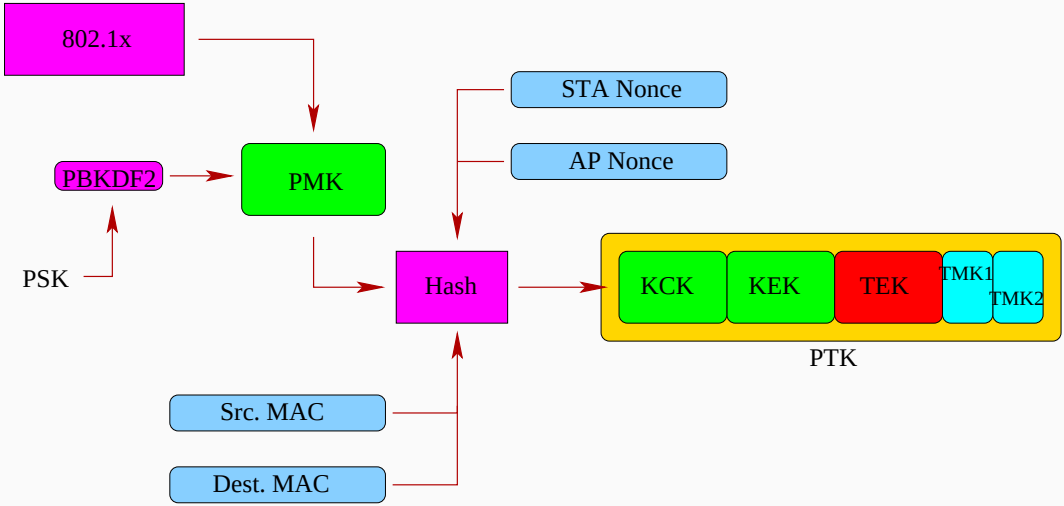
- Vérification de la connaissance de la PMK
- Installation de l'ensemble de clés



Calcul du PTK

La PMK du 802.1x (256 bits)

Si authentification par PSK, la PMK est le hash de la PSK



Dissociation de PTK
PTK est un ensemble de sous-clés

PTK est de 384 bits pour AES ou de 512 bits pour TKIP

Dissociation de PTK
PTK est un ensemble de sous-clés

- Key Confirmation Key (128 bits)

PTK est de 384 bits pour AES ou de 512 bits pour TKIP

Dissociation de PTK
PTK est un ensemble de sous-clés

- Key Confirmation Key (128 bits)
- Key Encryption Key (128 bits)

PTK est de 384 bits pour AES ou de 512 bits pour TKIP

Dissociation de PTK
PTK est un ensemble de sous-clés

- Key Confirmation Key (128 bits)
- Key Encryption Key (128 bits)
- Transcient Encryption Key (128 bits)

PTK est de 384 bits pour AES ou de 512 bits pour TKIP

Dissociation de PTK
PTK est un ensemble de sous-clés

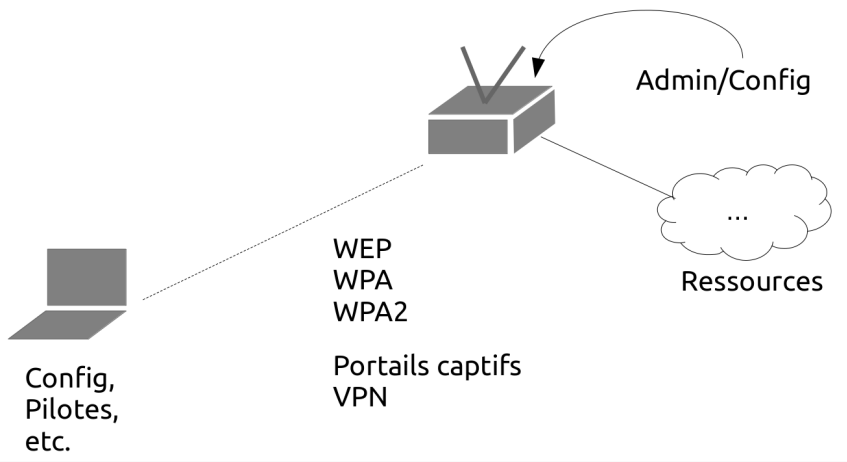
- Key Confirmation Key (128 bits)
- Key Encryption Key (128 bits)
- Transcient Encryption Key (128 bits)
- Transcient MIC Keys for TKIP (2x 64 bits)

PTK est de 384 bits pour AES ou de 512 bits pour TKIP

WPA3 ?

- Nouvelle génération de sécurisation du wifi (2018)
- WPA3-personnel avec *Simultaneous Authentication of Equals (SAE)*
  - Protocole d'échange de clés empêchant les attaques offline
  - Confidentialité persistante
- WPA3-enterprise avec suite cryptographique de 192 bits

Que reste-t-il à protéger ?



Protection des AP

- Configurer l'AP en WPA AES CCMP
- Renouveler les mots de passe en WPA-PSK
- Désactiver le WPS
- Installation de mécanisme de supervision
- Mettre à jour OS / firmwares
- etc.

Protection des stations

- Désactiver la carte wifi si non utilisée
- Désactiver l'association automatique
- Mettre à jour OS / pilotes wifi
- etc.

Autres mesures de sécurité

Ne font pas partie du 802.11 mais souvent disponibles :

Autres mesures de sécurité

Ne font pas partie du 802.11 mais souvent disponibles :

- SSID cloaking

Autres mesures de sécurité

Ne font pas partie du 802.11 mais souvent disponibles :

- SSID cloaking
- Filtrage d'adresse MAC source

Autres mesures de sécurité

Ne font pas partie du 802.11 mais souvent disponibles :

- SSID cloaking
- Filtrage d'adresse MAC source
- Isolation des stations

Protection du trafic de gestion

802.11w : protection des trames de gestion

- Authentification des trames de gestion unicast avec PTK
- Authentification des trames de gestion multicast avec BIP and IGTK

Implementations rares (Cisco MFP et wpa_supplicant/hostapd)

Attaques sur les réseaux 802.11

Outils

Outils d'attaques

- aircrack-ng
- BoopSuite
- bully
- coWPAtty
- eaphammer
- mana
- mdk3
- mitmap
- reaver
- wifiphisher
- wifi-pumpkin
- wifite
- wpa-bruteforcer
- etc.

Outils de défense

- kismet
- pidense
- waidps
- wireless-ids
- etc.

Attaques possibles

- Couche physique : Perturbations electromagnétiques (four à micro-ondes, etc.)
- Couche MAC, en se faisant passer pour l'AP (avec spoofing de l'adresse MAC, par exemple) :
  - Envoi de trames de désassociation aux stations
  - Envoi continu de trames CTS aux stations voisines (stations mises en attente d'envoi)
- etc.

Contre-mesures

- 802.11w sur la sécurisation des trafics de contrôle/gestion

Moyens de détection ?

- Alertes Kismet (DEAUTHFLOOD, BCASTDISCON, DISASSOCTRAFFIC)

Attaques possibles

- Sniffing de l'ensemble des communications en mode *monitor* !
- Découverte passive des AP environnants (grâce aux *beacons* envoyés régulièrement par les AP)
  - airodump-ng
  - Kismet
- Découverte active (par envoi de *probe requests*)
  - iw dev $iface scan
  - Netstumbler
- Wardriving
- etc.

Contre-mesures

- Masquage du SSID ?
  - Les beacons ne contiennent plus le ESSID
  - Les probe requests ne recoivent de réponse que si elles contiennent un ESSID

Attaques possibles

- Rejeu en réseau ouvert ou réseau WEP
- Injection de trafic arbitraire
  - Car faiblesse des vérifications d'intégrité (absence, CRC32 ou Michael)

Contre-mesures

- Portails captifs insuffisants en réseaux ouverts (protection couche supérieure...)
- Arrêter d'utiliser WEP !

Problèmes spécifiques au WEP

Attaques possibles

- Retrouver la clé WEP
  - Collisions des IV qui réduisent l'effort de BF
  - Attaque implémentée dans `aircrack-ng`
- Attaque chopchop
  - Décrypter les données (sans connaissance de la clé)
  - Implémentée dans `aireplay-ng`
- Authentication unilatérale, donc rogue AP et MitM possibles

Contre-mesures

- Arrêter d'utiliser WEP !
- Vérifier que vos AP ne peuvent pas être downgradés

Moyens de détection ?

- Alertes Kismet (CRYPTODROP)

Problèmes spécifiques au WPA

Attaques possibles

- Attaque par dictionnaire contre la PSK
  - Implémentée dans aircrack-ng
- KRACK (Key Reinstallation Attacks)
- Attaques connues sur EAP
  - Attaques par dictionnaire sur EAP-MD5

Contre-mesures

- Définir une PSK longue et complexe et la changer régulièrement
- Utiliser des méthodes d'authentification autres que EAP-MD5

Moyens de détection ?

- Alertes Kismet (NONCEDEGRADE) contre KRACK

Attaque par dictionnaire de la PSK : méthodologie

Nécessite de capturer au moins 1 MIC valide

- Identifier une station légitimement associée
- Desauthentifier la station
- Capturer le 4 way handshake
- Comparer le MIC au résultat calculé pour la PSK candidate

Un exemple récent[1] :

- Découverte d'une commande cachée (RE) disponible sur l'AP
- Prérequis : connaître le numéro de série du point d'accès
- Condition d'arrêt de bruteforce du mot de passe à passer à cette commande
- Résultat : shell root sur tous les AP de ce fabricant

[1] https://www.sstic.org/2019/presentation/analyse_de_firmwares_de_points_dacces_retro_ingenierie_et_elevation_de_privileges

Bonus

Crédits...

...à Cédric Blancher pour ses supports de cours dont ceux-ci sont fortement inspirés

Vos commentaires

Votre avis compte

- remarques ?
- améliorations ?
- suggestions ?
- questions ?

anais.gantet.pro@gmail.com
benoit.camredon@gmail.com