Sécurité des réseaux non-filaires

Sécurité des réseaux Wifi

Anaïs Gantet, Benoît Camredon
TLS-SEC 2020/2021

Modalités 2020

- En visio
- TP effectué par le prof...
- Nouveau support de cours
- Mini-projet

Dans ce cours

Le réseau Wifi, 802.11

- Rappels de terminologie du Wifi
- Sécurisations existantes
  - WEP
  - WPA
  - WPA2
- Attaques sur le 802.11

Dans ce cours

Le réseau Wifi, 802.11

- Rappels de terminologie du Wifi
- 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 ?

Mise en contexte

Problèmatiques de déploiement du WiFi

Quels AP choisir et quelle infrastructure déployer ?

- Réponse à un besoin particulier
- Caractéristiques physiques
- Facilité de maintenance
- Contrainte de budget

Vecteurs d'attaques sur un réseau déjà en place ?

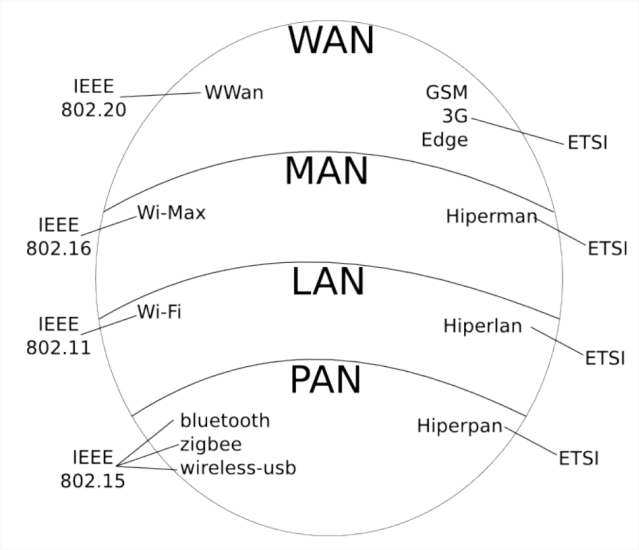
- Configuration du réseau local Wifi (configuration de l'AP, des stations)
- Nature des machines hébergeant l'infrastructure
- Gestion de l'authentification, du stockage des secrets partagés, etc.

Quoi et comment surveiller ?

- Journalisation
- Analyse des logs, sonde de détection d'attaques connues

Equipements

Le Wifi : un type de réseaux non-filaires parmi d'autres



Normes

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

Exemples d'amendements

- 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

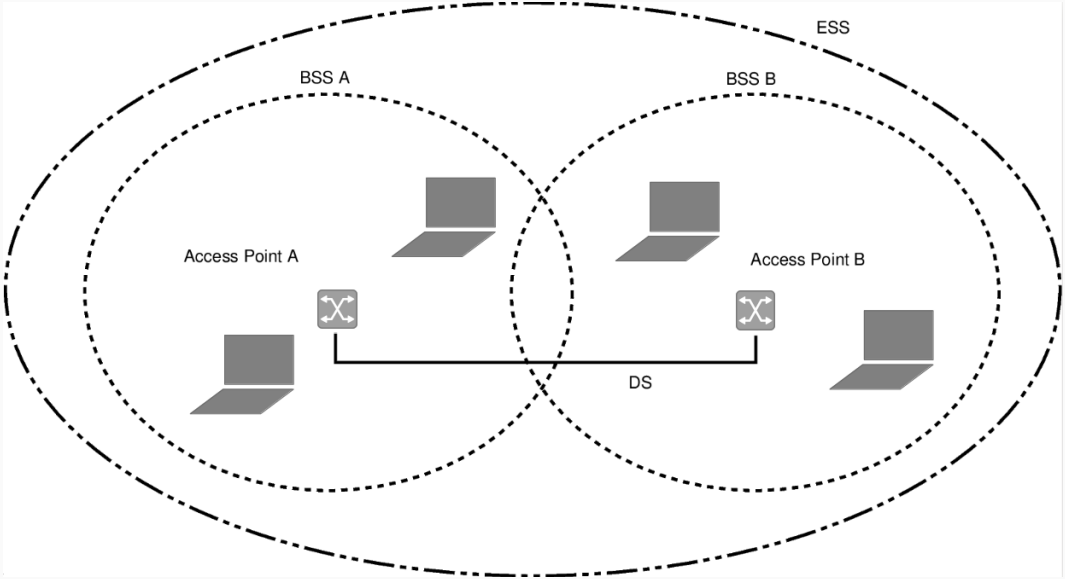
802.11 offre 2 modes d'opération

- 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

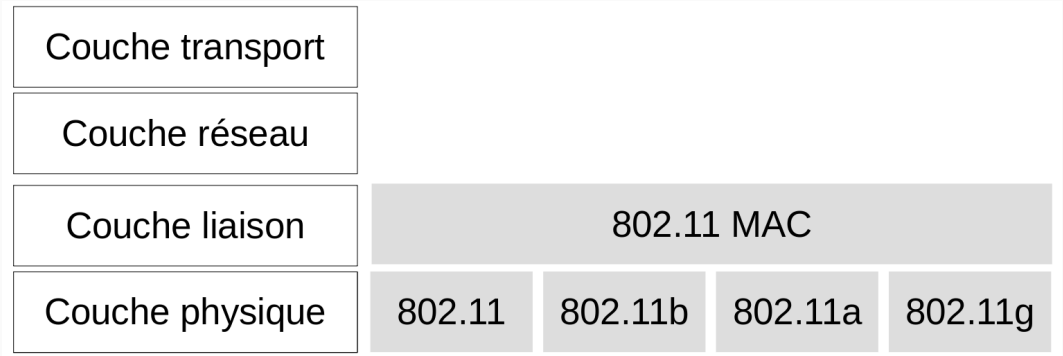
Les deux modes peuvent étendre des réseaux

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

BSS, DS, ESS, etc.



Pile OSI du WiFi



Pause TP - mode supportés

Bonjour ! Un "câble WiFi" svp...

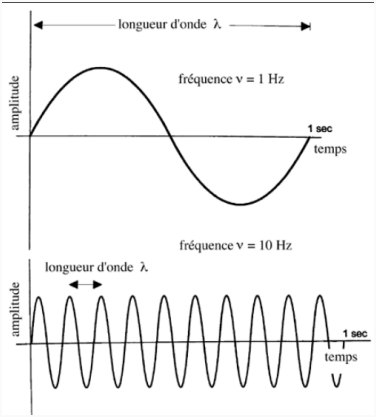
Les ondes radio, support du signal WiFi

Grandeurs physiques d'une onde électro-magnétique

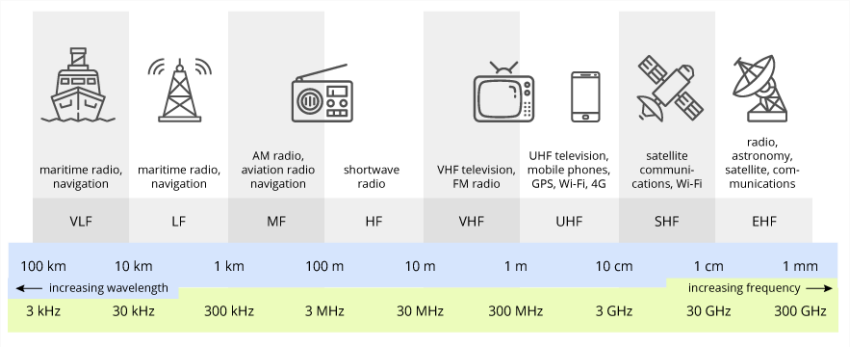
- Fréquence (inverse de la période)
- Longueur d'onde
- Amplitude
- Puissance

Caractéristiques de transmission radio

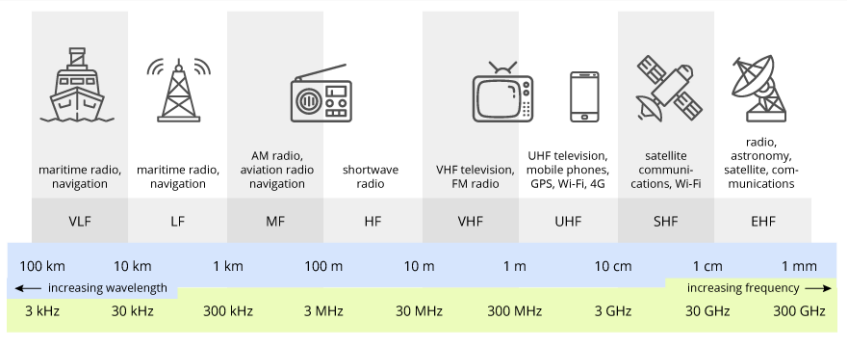
- Portée du signal
- Débit du signal
- Modulation du signal (DSSS et OFDM)

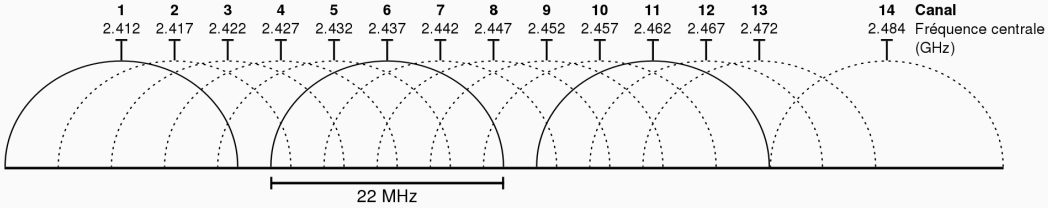


Fréquences et canaux WiFi: 2,4 GHZ, 5 GHz



Fréquences et canaux WiFi: 2,4 GHZ, 5 GHz





Pause TP - Caractéristiques physiques d'une carte Wifi et des AP environnants

Un peu de pratique... (Linux)

Affichage des débits et fréquences supportés par une carte WiFi

```
$ iw phy
[...]
  Band 1:
   [...]
    Bitrates (non-HT):
      * 1.0 Mbps
      * 2.0 Mbps (short preamble supported)
      * 5.5 Mbps (short preamble supported)
      * 11.0 Mbps (short preamble supported)
      * 6.0 Mbps
      * 9.0 Mbps
      * 12.0 Mbps
      * 18.0 Mbps
      * 24.0 Mbps
      * 36.0 Mbps
      * 48.0 Mbps
      * 54.0 Mbps
    Frequencies:
      * 2412 MHz [1] (22.0 dBm)
      * 2417 MHz [2] (22.0 dBm)
      * 2422 MHz [3] (22.0 dBm)
      * 2427 MHz [4] (22.0 dBm)
      * 2432 MHz [5] (22.0 dBm)
      * 2437 MHz [6] (22.0 dBm)
      * 2442 MHz [7] (22.0 dBm)
      * 2447 MHz [8] (22.0 dBm)
      * 2452 MHz [9] (22.0 dBm)
      * 2457 MHz [10] (22.0 dBm)
      * 2462 MHz [11] (22.0 dBm)
      * 2467 MHz [12] (22.0 dBm)
      * 2472 MHz [13] (22.0 dBm)
      * 2484 MHz [14] (disabled)
    [...]
```

Un peu de pratique... (Linux)

```
Band 2:
[...]
  Bitrates (non-HT):
     * 6.0 Mbps
     * 9.0 Mbps
     * 12.0 Mbps
     * 18.0 Mbps
     * 24.0 Mbps
     * 36.0 Mbps
     * 48.0 Mbps
     * 54.0 Mbps
```

```
 Frequencies:
      * 5180 MHz [36] (22.0 dBm) (no IR)
      * 5200 MHz [40] (22.0 dBm) (no IR)
      * 5220 MHz [44] (22.0 dBm) (no IR)
      * 5240 MHz [48] (22.0 dBm) (no IR)
      * 5260 MHz [52] (22.0 dBm) (no IR, radar detection)
      * 5280 MHz [56] (22.0 dBm) (no IR, radar detection)
      * 5300 MHz [60] (22.0 dBm) (no IR, radar detection)
      * 5320 MHz [64] (22.0 dBm) (no IR, radar detection)
[...]
      * 5905 MHz [181] (disabled)
```

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
          ...
```

Un peu de pratique... (Linux)

```
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
```

Idées d'attaques sur la couche 1 ?

A quoi ressemblent les trames WiFi ?

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)

Pause TP - Observation du trafic Wifi

Trafic de données

- les différentes adresses MAC
- le payload, qui contient les paquets issus des couches supérieures (IP, TCP, HTTP, etc.)

Trafic de contrôle

Paquets simples et courts, pour le bon partage du médium de communication

- PS-Poll
- RTS
- CTS
- ACK
- CF-End
- CF-End et CF-ACK

Trafic de contrôle

Paquets simples et courts, pour le bon partage du médium de communication

- PS-Poll
- RTS
- CTS
- ACK
- CF-End
- CF-End et CF-ACK

Une idée d'attaque de déni de service ?

Trafic de gestion

Paquets uniquement utilisés pour les fonctions de la couche MAC du Wifi

- Requête/ Réponse d'association
- Requête/Réponse de ré-association
- Requête/Réponse de sondage
- Balises (beacon)
- ATIM
- Déassociation
- Authentication
- Désauthentication

Trafic de gestion

Paquets uniquement utilisés pour les fonctions de la couche MAC du Wifi

- Requête/ Réponse d'association
- Requête/Réponse de ré-association
- Requête/Réponse de sondage
- Balises (beacon)
- ATIM
- Déassociation
- Authentication
- Désauthentication

Une idée d'attaque de déni de service ?

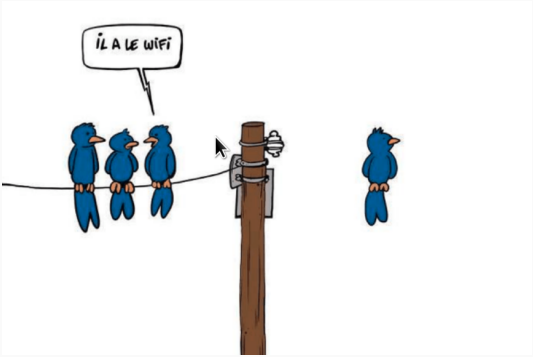
La procédure d'association (en mode infrastructure)

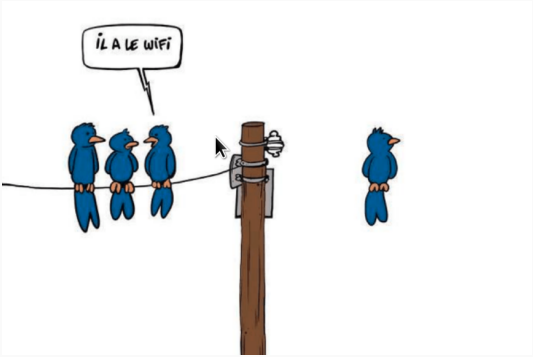
L'*Association* est un concept clé des réseaux sans fil

- 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

Station et AP associés : Couche niveau 2 opérationnelle





Risques en termes de sécurité ?

Protocoles de sécurisation (niveau 2)

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 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`

Pause TP - Protocoles de sécurité supportés

Exemples : 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"
}
```

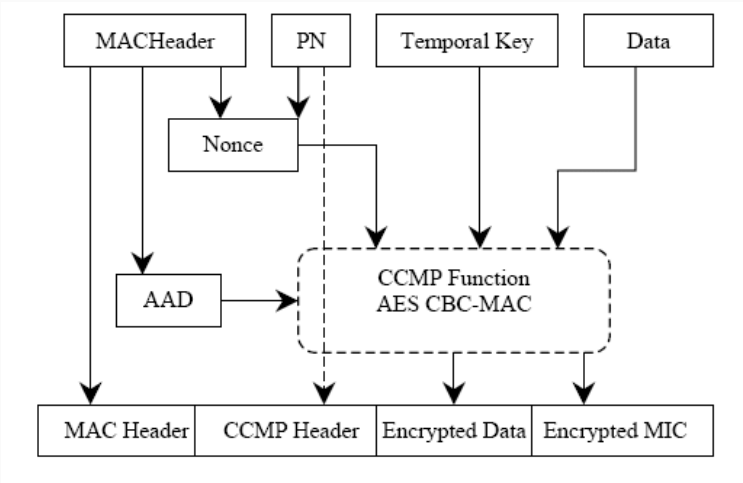
```
# wpa_supplicant -D wext -i wlan0 -c
/etc/wpa_supplicant.conf &
# dhclient wlan0

Ou bien :

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

WPA2, solution à l'état de l'art aujourd'hui

Dernier standard amendé dans la norme 802.11i

- Confidentialité : Chiffrement en AES
- Intégrité : basé sur le mode de chiffrement CCM pour AES
- Authentification : 2 modes possibles
  - WPA-PSK (pre shared key)
  - WPA-EAP
- Autres : mécanismes d'anti-rejeu, de distribution de clés

WPA2 : Protocole AES-CCMP



Authentification WPA

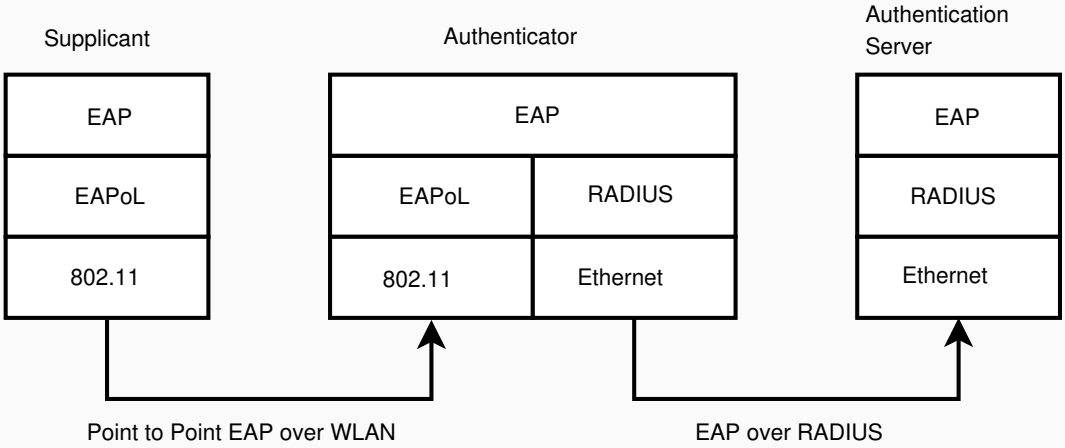
2 méthodes d'authentification possibles :

- 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

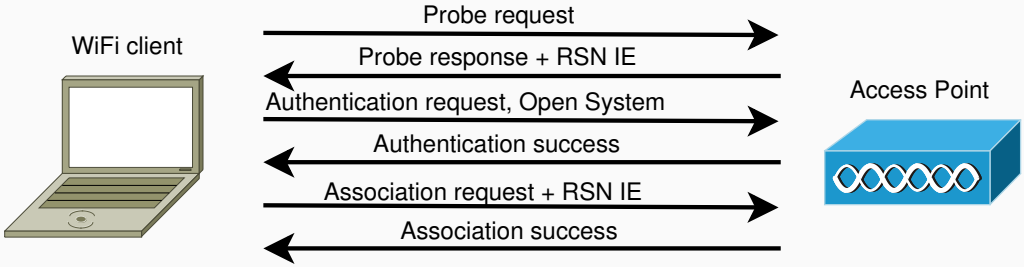
Robust Security Network (RSN)

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

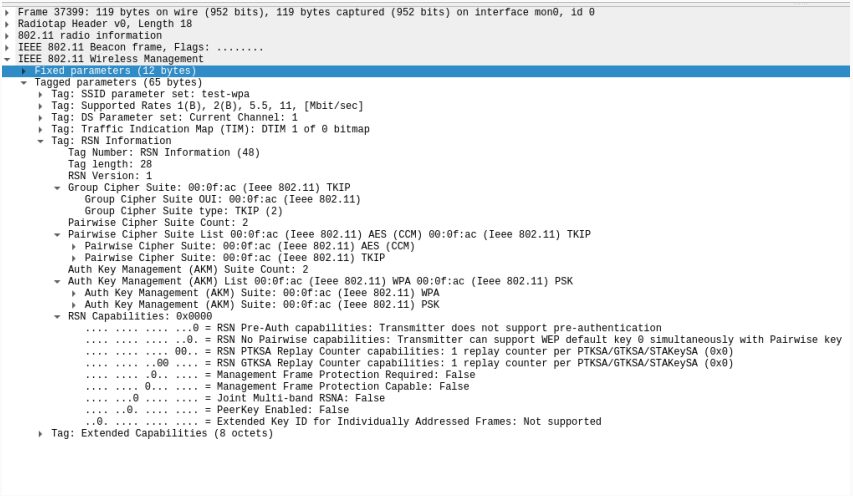
- Négociation de la politique de sécurité
- Authentification 802.1x
- Distribution des clés
- Protection des communications réseaux

Négociation de la politique de sécurité

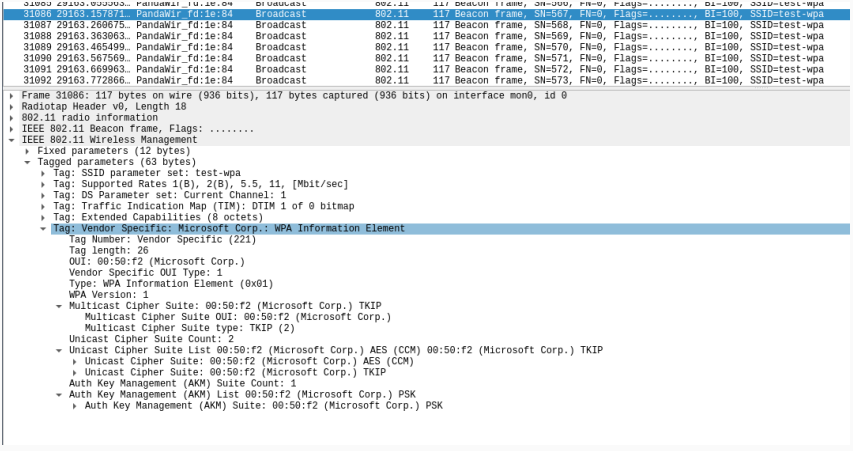
- Probe request
- Probe response dont le RSN IE
- Open authentication
- Association request avec le RSN IE du client
- Association success



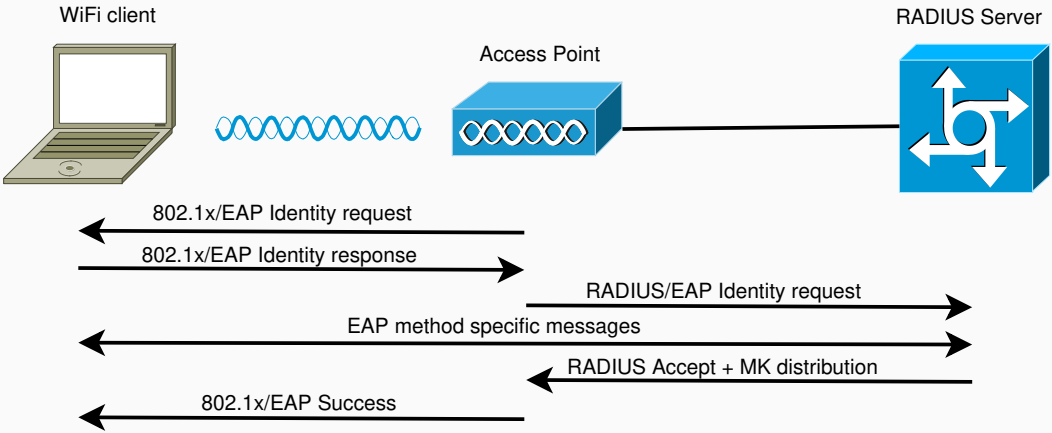
Exemples de RSN IE (dans un beacon)



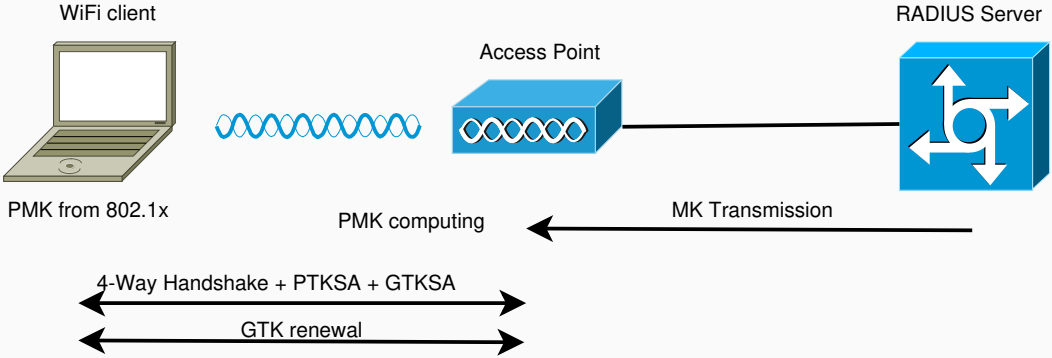
Exemples de RSN IE (dans un beacon)



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

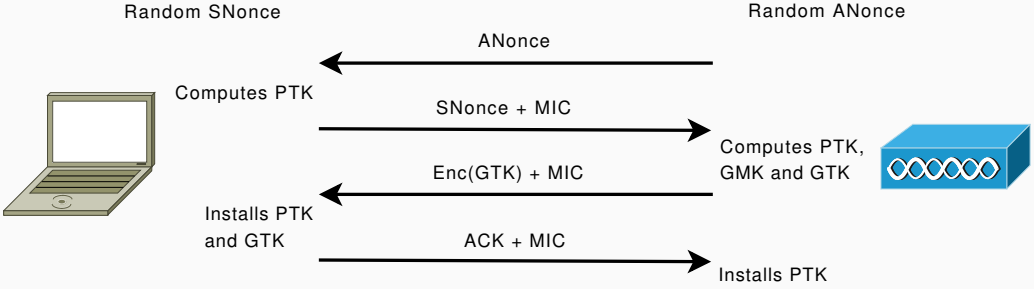


Echange de clé
La 3ème étape est la distribution de clés avec le 4-Way Handshake



4-Way Handshake

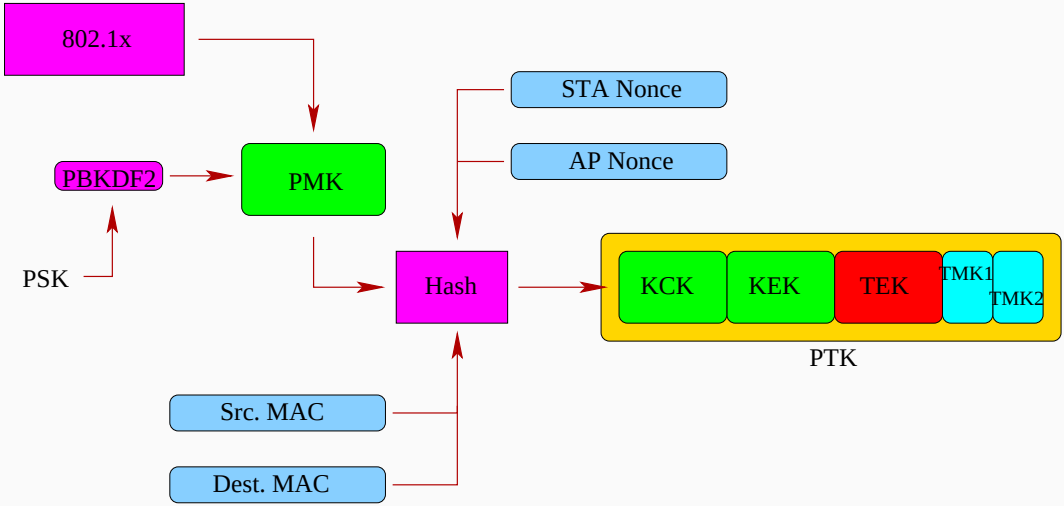
- Vérification de la connaissance de la PMK
- Installation de l'ensemble de clés



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

WEP : Wired Equivalent Privacy

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

Chiffrement

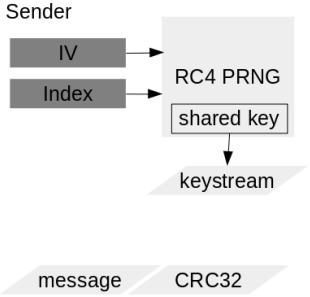
- Basé sur RC4 (symétrique)
- Clé partagée entre AP/clients
- taille de clé : 40 bits

"Intégrité"

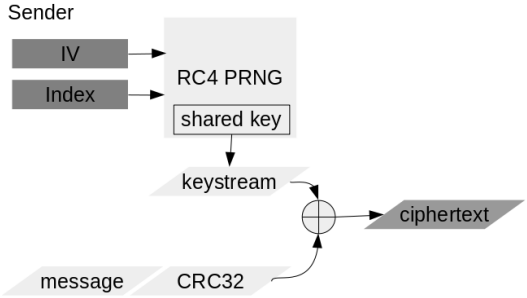
- CRC32

WEP aurait pu vouloir dire Weak Encryption Protocol...

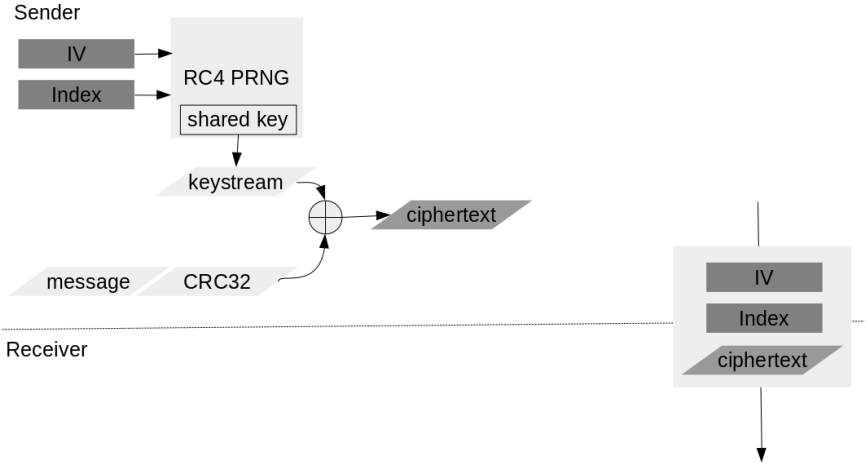
Chiffrement et intégrité WEP



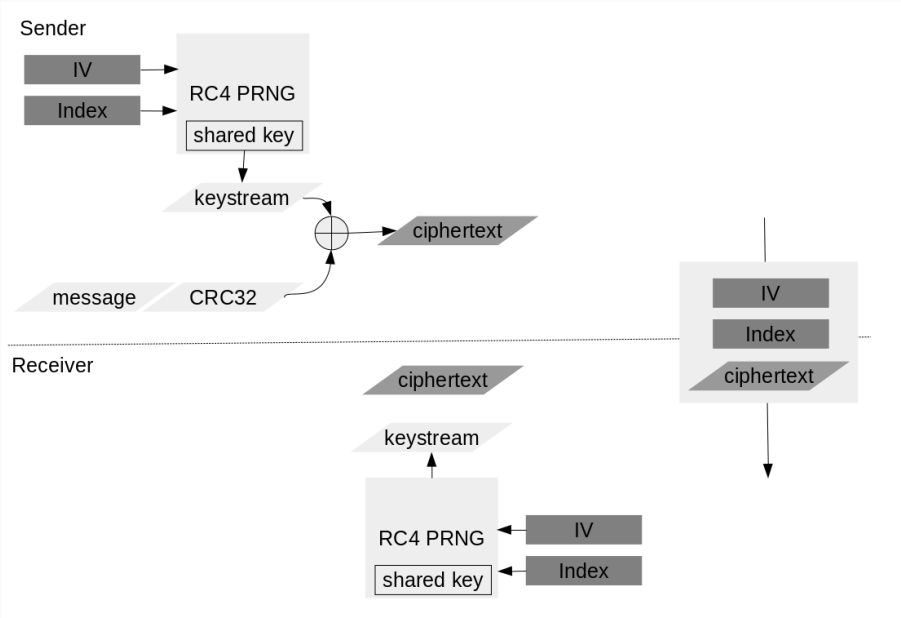
Chiffrement et intégrité WEP



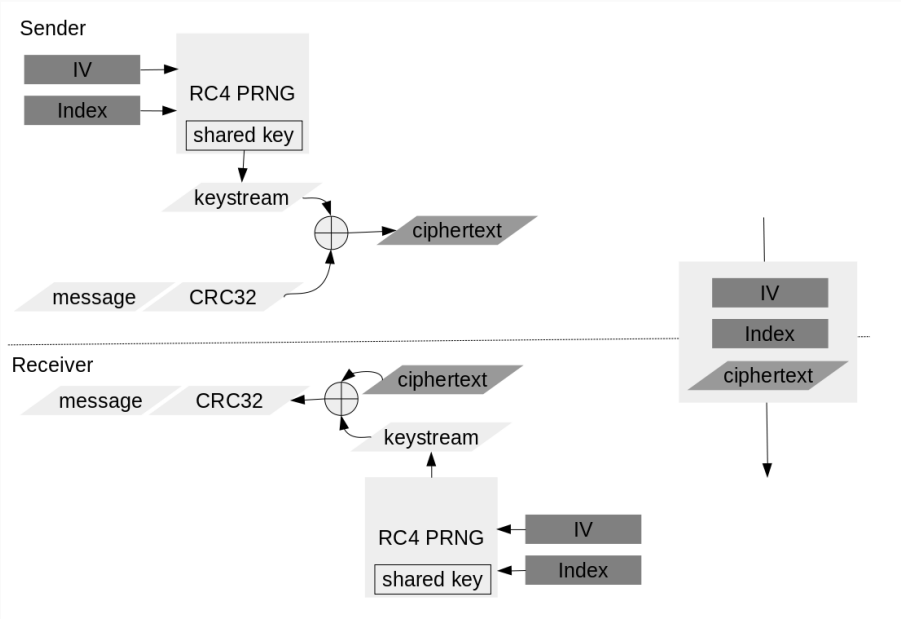
Chiffrement et intégrité WEP



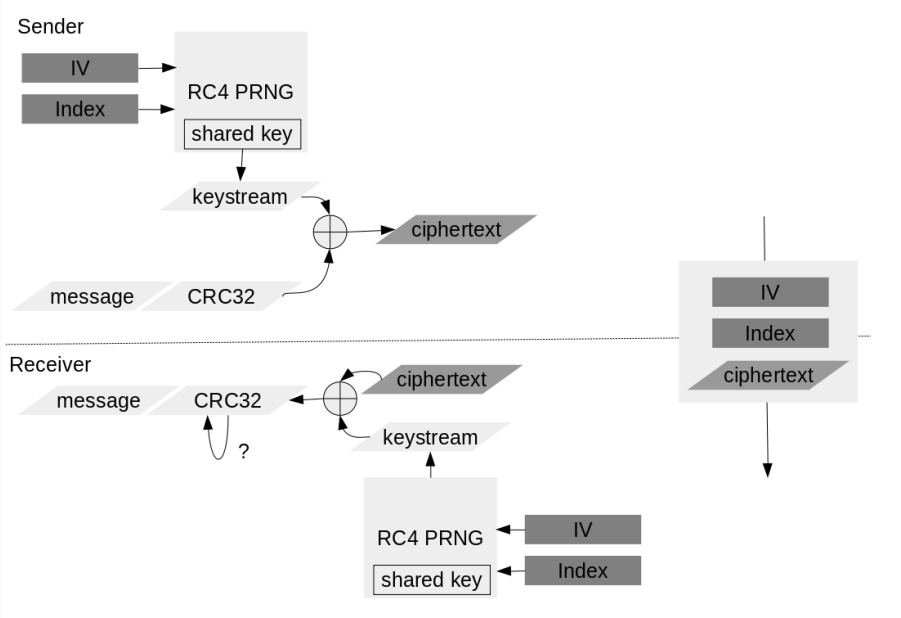
Chiffrement et intégrité WEP



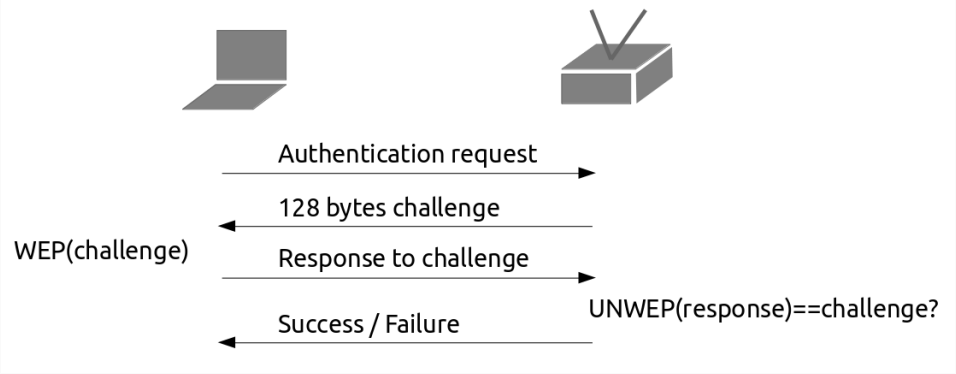
Chiffrement et intégrité WEP



Chiffrement et intégrité WEP

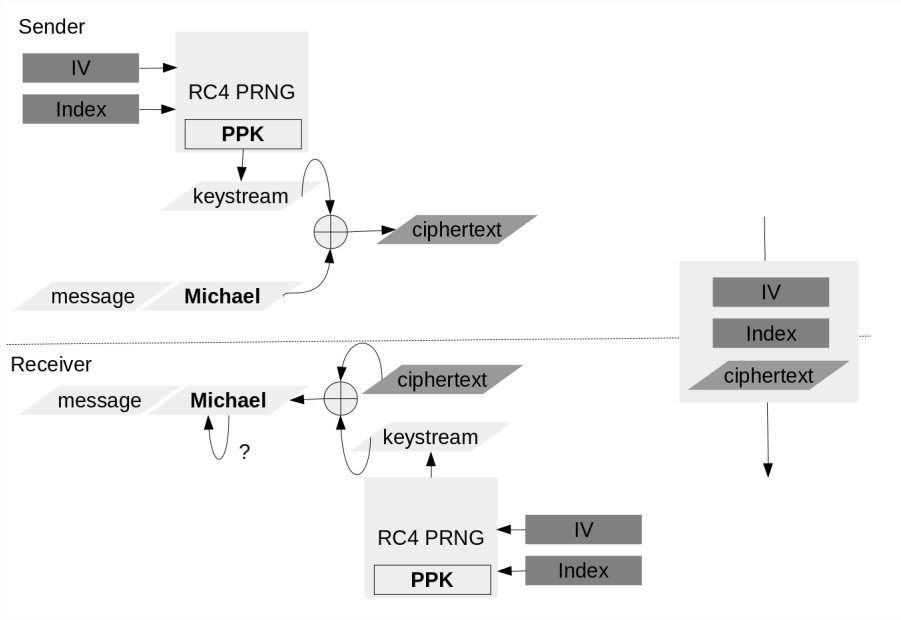


4 messages handshake avec challenge et réponse



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

Chiffrement et intégrité WPA[1]

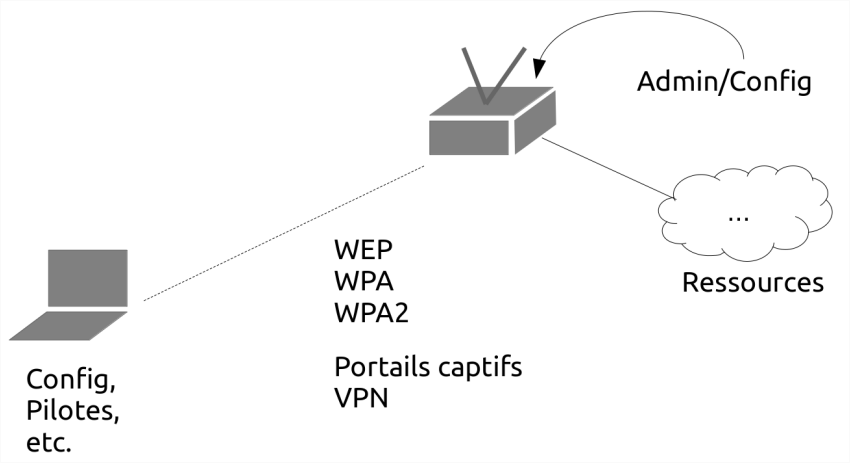


Pause TP - Configuration d'AP en WEP, WPA, WPA2

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.

Mini-projet : Enoncé

Par groupe de 3 ou 4 :

- Choisir une attaque Wifi connue
  - Dans le domaine de votre choix (cryptographique, protocolaire, ondes radio, programmation, etc.)
  - Exemples : Wardriving, chopchop, rogue AP, cassage de clé WEP ou WPA-PSK, KRACK, etc.
- Faire valider le sujet aux intervenants
- Produire une présentation orale de 3min (format libre)
  - Expliquer la ou les vulnérabilités utilisées
  - Expliquer le principe de l'attaque
  - Trouver des contre-mesures associées
- Bonus (si matériel Wifi à disposition)
  - Démo de l'attaque
  - Démo de détection de l'attaque

Sources d'inspiration : `https://www.sstic.org/2021/news/`,
`https://www.youtube.com/channel/UCuoCDm4vGr7t7MdD3zt3P3g/videos`,
`https://www.kismetwireless.net/docs/readme/alerts_and_wids/`,
`https://www.aircrack-ng.org/doku.php#documentation`, etc.

Soyez créatifs :)

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)

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

Faille d'implémentation puces Broadcom et Cypress (Kr00k - CVE-2019-15126)

Vulnérabilité

- Chiffrement WPA2 AES CCMP avec Tx-FIFO
- Si disassociation, révocation des clés
- Clé de chiffrement réinitialisée (zéros) **avant** que le buffer Tx soit vidé
- Derniers fragments de paquets **chiffrés et envoyés avec une clé nulle** !...

Exploitation

- Passive : déchiffrement par interception de trafic de disassociation naturelle
- Active : déchiffrement après envoi de trames de désassociation aux clients (ou aux AP)

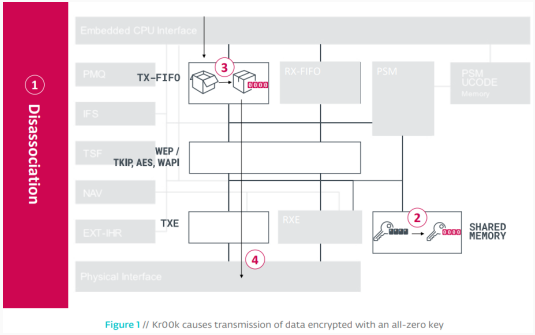


Figure 1 // Kr00k causes transmission of data encrypted with an all-zero key

https://www.welivesecurity.com/wp-content/uploads/2020/02/ESET_Kr00k.pdf

Bonus

Pour aller plus loin

- https://www.rsaconference.com/usa/agenda/kr00k-how-kracking-amazon-echo-exposed-a-billion-vulnerable-wifi-devices

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