

# Sécurité des réseaux Wi-Fi

Ludovic Eschard

**Mars 2020**

(support modifié repris de Laurent Butti et Benoît Michau)

**Slides :**

**[eschard.com/wifi.pdf](http://eschard.com/wifi.pdf)**

# Plan de la formation

## Sécurité des réseaux Wi-Fi

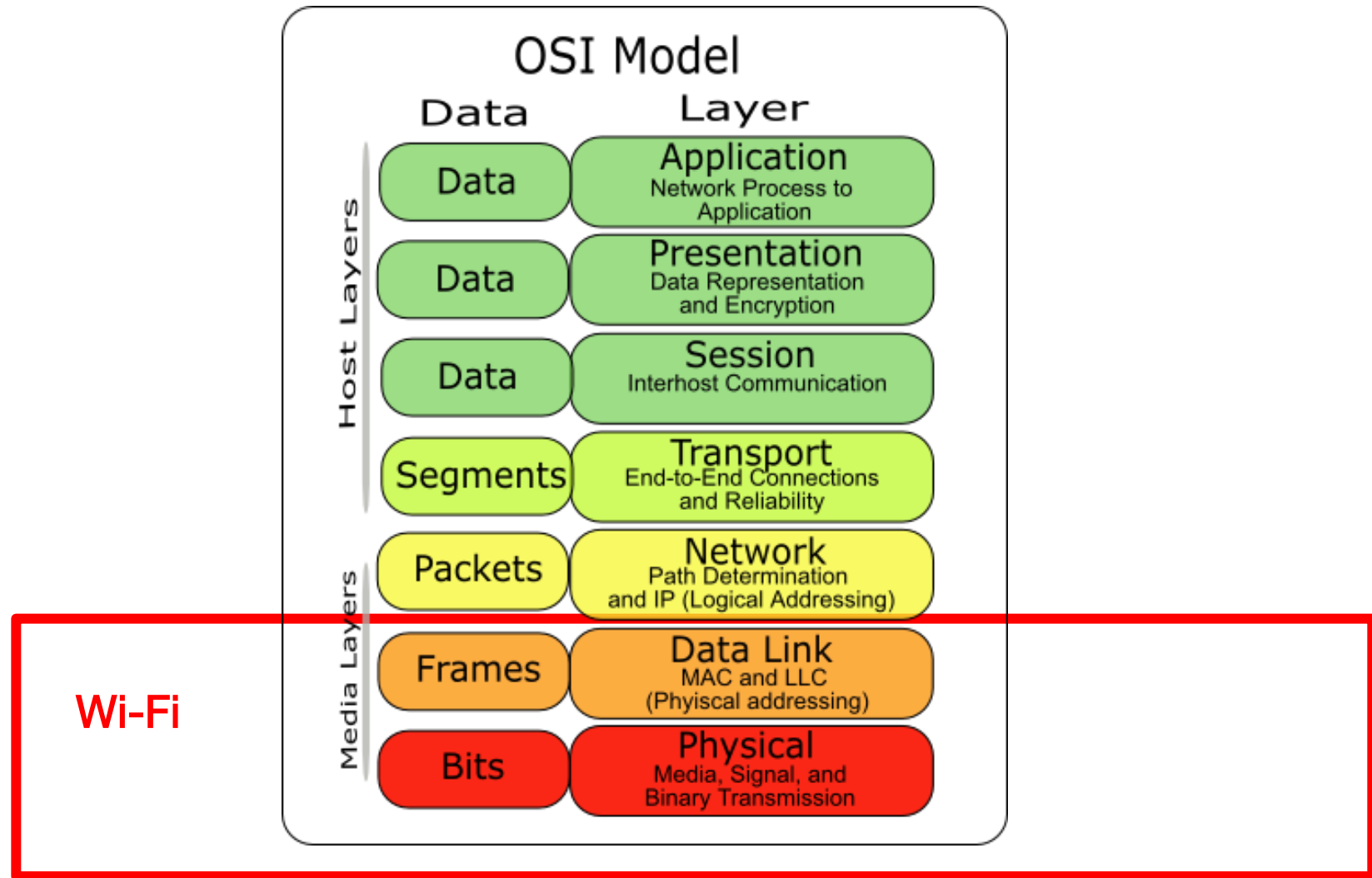
- Principes et fonctionnement
- Mise en œuvre
- Sécurité

# **Principes et fonctionnement**

# Définitions préalables

- **Station (STA)** : machine ou appareil client
- **Access Point (AP)**: élément sur lequel s'associent les stations
- **PSK** : Pre-Shared Key , clé pré-partagée

# Couches de l'OSI – IEEE 802.11



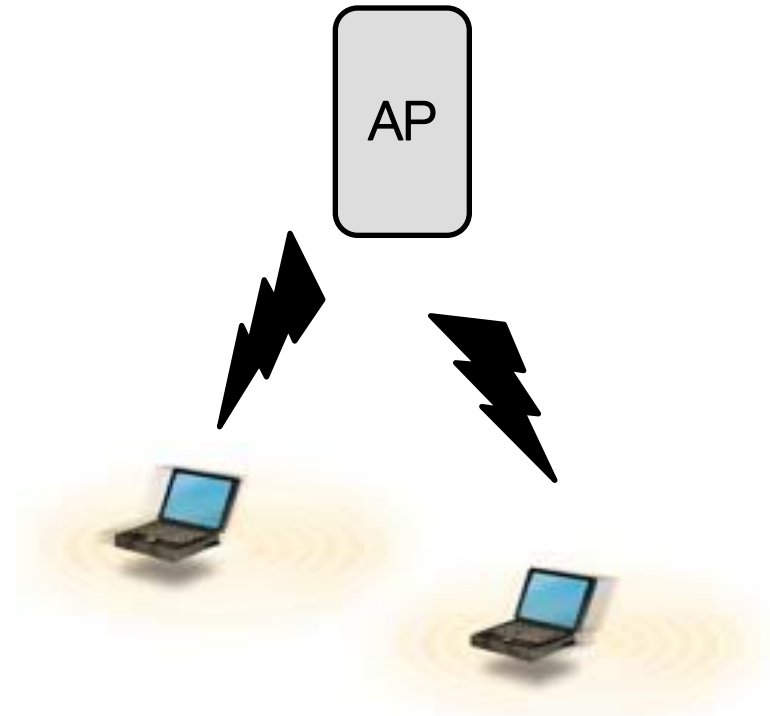
# Technologie Wi-Fi

Mode ad-hoc



Les stations se connectent de pair à pair.

Mode infrastructure



Les stations se connectent à un point d'accès (AP)

# La norme IEEE 802.11 et ses amendements

- IEEE 802.11 (1997) est la norme de réseaux radio locaux sans-fil la plus utilisée
- IEEE 802.11a (1999) – High Speed Physical Layer in the 5 GHz band (54 Mb/s)
- IEEE 802.11b (1999) – Higher Speed Physical Layer Extension in the 2.4 GHz band
  - > Bande de fréquence 2,4 GHz – 11 Mb/s
- IEEE 802.11g (2003) – Standard for Higher Rate : 2.4GHz (jusqu'à 54 Mb/s)
- IEEE 802.11i (2004) : Amendement sécurité : WPA et WPA2
- IEEE 802.11n (2009) : High Throughput (300 – 600 Mb/s) en 2,4 et 5 Ghz
- IEEE 802.11ac (2014) → Wi-Fi 5 (433 – 6900 Mb/s)
- 2018 : WPA3
- IEEE 802.11ax (2019) → Wi-Fi 6 (600 – 9608 Mb/s)



# Découverte

- En permanence (sauf si désactivé) un **AP diffuse les informations le concernant** (SSID, mode de sécurité, ...) et cela plusieurs fois par secondes grâce aux **trames « beacon »**
- La station doit découvrir les APs dans sa zone géographique avec lesquels elle peut s'associer
  - > Écoute des « beacons » et possibilité de créer une liste ordonnée d'APs en fonction de la puissance du signal reçue et paramétrage de sécurité
- Si l'AP n'émet pas de beacon, la station devra émettre une trame « Probe Request » pour que l'AP lui réponde

# Portée des signaux

# Portée d'un signal Wi-Fi

- Dépend:
  - de la couche PHY (fréquence porteuse, modulation / codage)
  - de la puissance d'émission (limitations légales)
  - du chemin de parcours des ondes (visibilité directe)
- Distance maximale de 100m généralement admise
  - Sur la bande 2.4 GHz, sans obstacle majeur
- Possibilité d'augmenter la sensibilité du récepteur
  - Antenne adaptée
  - Carte Wi-Fi avec instrumentation précise
  - Quelques kilomètres de portée
- Avec des émetteurs sur-amplifiés
  - Plusieurs dizaines de kilomètres

## Quelques antennes



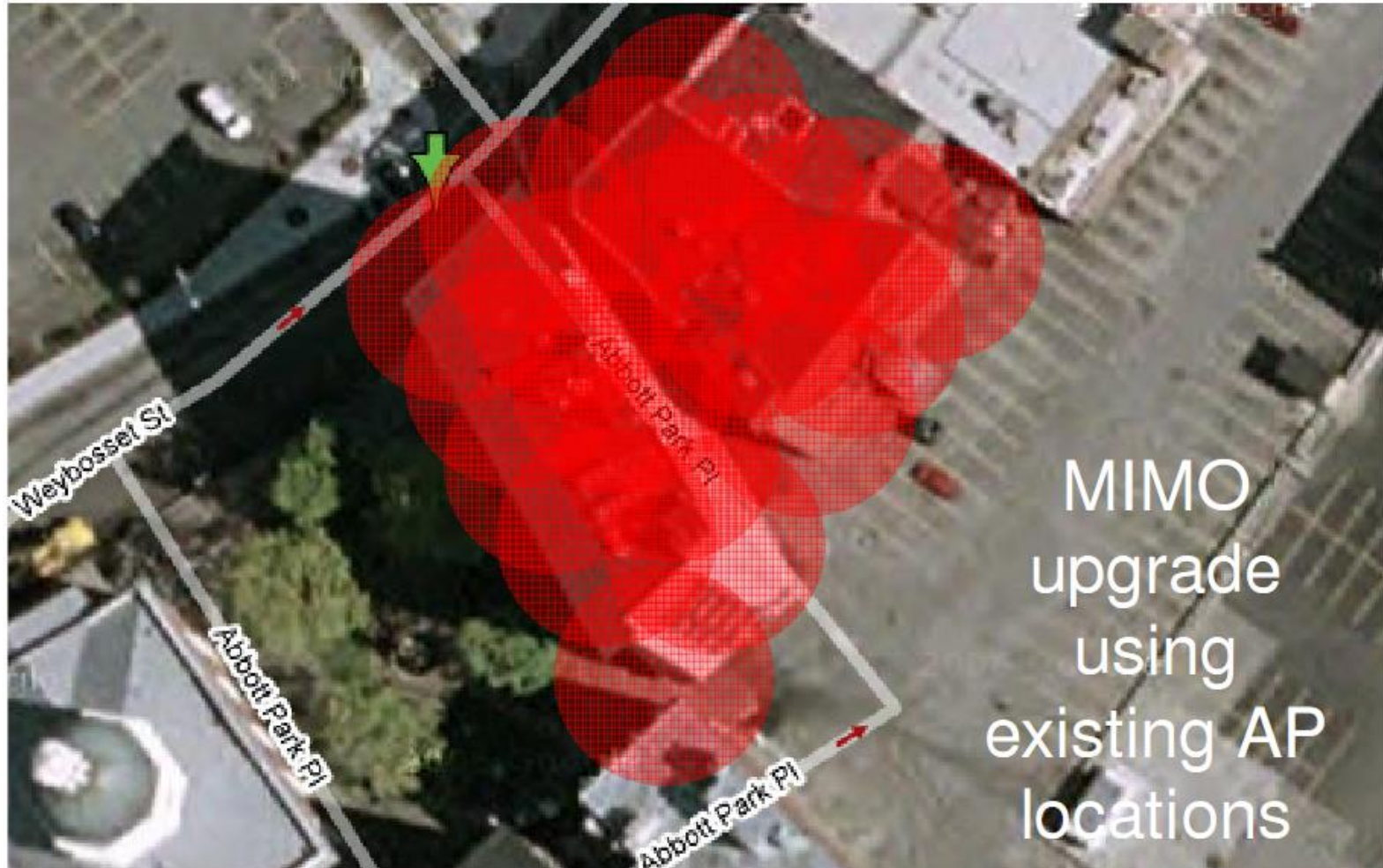
# Attention aux évolutions du standard





# Evolution du standard radio 802.11n

- Portée augmentée avec l'intégration du MIMO



# Trames Wi-Fi

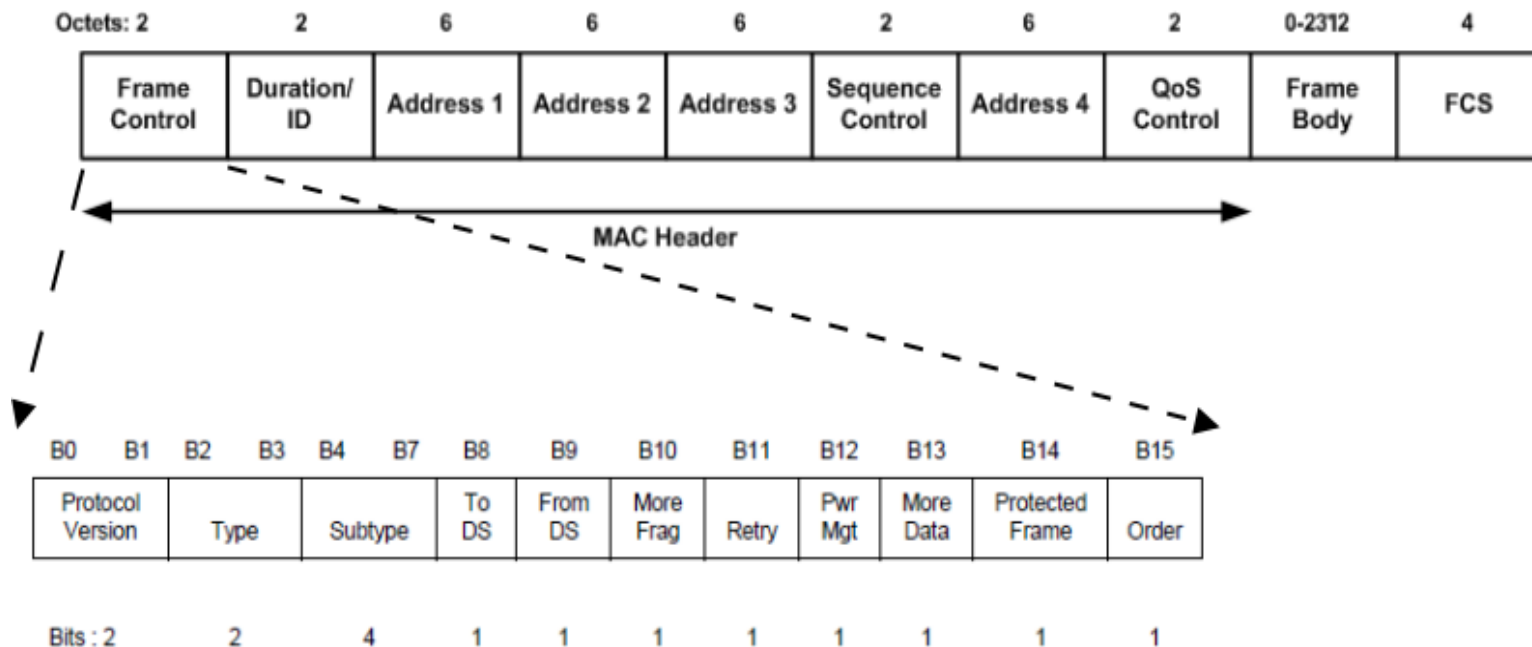
# Trames 802.11

- Couche MAC constituée de trames logiques
  - Trames de gestion (beacon, association, authentication, ...), de contrôle
  - Trames de données (MSDU: "Medium Service Data Unit")



# Format des trames MAC 802.11

- En-tête: jusqu'à 32 octets
- Données: jusqu'à 2312 octets (la seule partie chiffrée)
- Contrôle d'erreur: 4 octets (CRC 32)



# Quelques exemples de trames 802.11

# Beacon

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Z-Com_35:66:08	Broadcast	802.11	238	Beacon frame,
+ Frame 1: 238 bytes on wire (1904 bits), 238 bytes captured (1904 bits)						
- IEEE 802.11 Beacon frame, Flags: .....						
Type/Subtype: Beacon frame (0x08)						
+ Frame Control: 0x0080 (Normal)						
Duration: 0						
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)						
Source address: Z-Com_35:66:08 (00:19:70:35:66:08)						
BSS Id: Z-Com_35:66:08 (00:19:70:35:66:08)						
Fragment number: 0						
Sequence number: 1884						
- IEEE 802.11 wireless LAN management frame						
- Fixed parameters (12 bytes)						
Timestamp: 0x0000001783a291cf						
Beacon Interval: 0,102400 [Seconds]						
+ Capabilities Information: 0x0431						
- Tagged parameters (202 bytes)						
+ Tag: SSID parameter set: Wifimitch						
+ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]						
+ Tag: DS Parameter set : Current Channel: 7						
+ Tag: Traffic Indication Map (TIM): DTIM 2 of 0 bitmap						
+ Tag: ERP Information						
+ Tag: RSN Information						
+ Tag: Vendor Specific: Microsof: WPA Information Element						
+ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]						
+ Tag: Vendor Specific: Microsof: WMM/WME: Parameter Element						
+ Tag: HT Capabilities (802.11n D1.10)						
+ Tag: HT Information (802.11n D1.10)						
+ Tag: Vendor Specific: AtherosC: Advanced Capability						
+ Tag: Vendor Specific: AtherosC: Unknown						
+ Tag: Country Information: Country Code FR, Environment Any						
0000	80 00 00 00 ff ff ff ff	ff ff 00 19 70 35 66 08	.....	....p5f.		
0010	00 19 70 35 66 08 c0 75	cf 91 a2 83 17 00 00 00	..p5f..u	.....		
0020	64 00 31 04 00 09 57 69	66 69 4d 69 74 63 68 01	d.1...w	fimitch.		
0030	08 82 84 8b 96 0c 12 18	24 03 01 07 05 04 02 03	.....	\$......		
0040	00 00 2a 01 00 30 18 01	00 00 0f ac 02 02 00 00	..*..0..	.....		

# Association

No.	Time	Source	Destination	Protocol	Length	Info
178	23.110597	SonyComp_f1:f7:b4	Z-Com_35:66:08	802.11	85	Association Request,
180	23.112121	Z-Com_35:66:08	SonyComp_f1:f7:b4	802.11	121	Association Response,

+ Frame 178: 85 bytes on wire (680 bits), 85 bytes captured (680 bits)

IEEE 802.11 Association Request, Flags: .....
 

Type/Subtype: Association Request (0x00)
 

Frame Control: 0x0000 (Normal)
 

Version: 0
 Type: Management frame (0)
 Subtype: 0
 Flags: 0x0
 Duration: 314
 Destination address: Z-Com\_35:66:08 (00:19:70:35:66:08)
 Source address: SonyComp\_f1:f7:b4 (00:24:8d:f1:f7:b4)
 BSS Id: Z-Com\_35:66:08 (00:19:70:35:66:08)
 Fragment number: 0
 Sequence number: 27

IEEE 802.11 wireless LAN management frame
 

+ Fixed parameters (4 bytes)
 + Tagged parameters (57 bytes)
 

Tag: SSID parameter set: wifimitch
 Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
 Tag: Extended Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
 Tag: RSN Information
 Tag: Vendor Specific: Marvell's

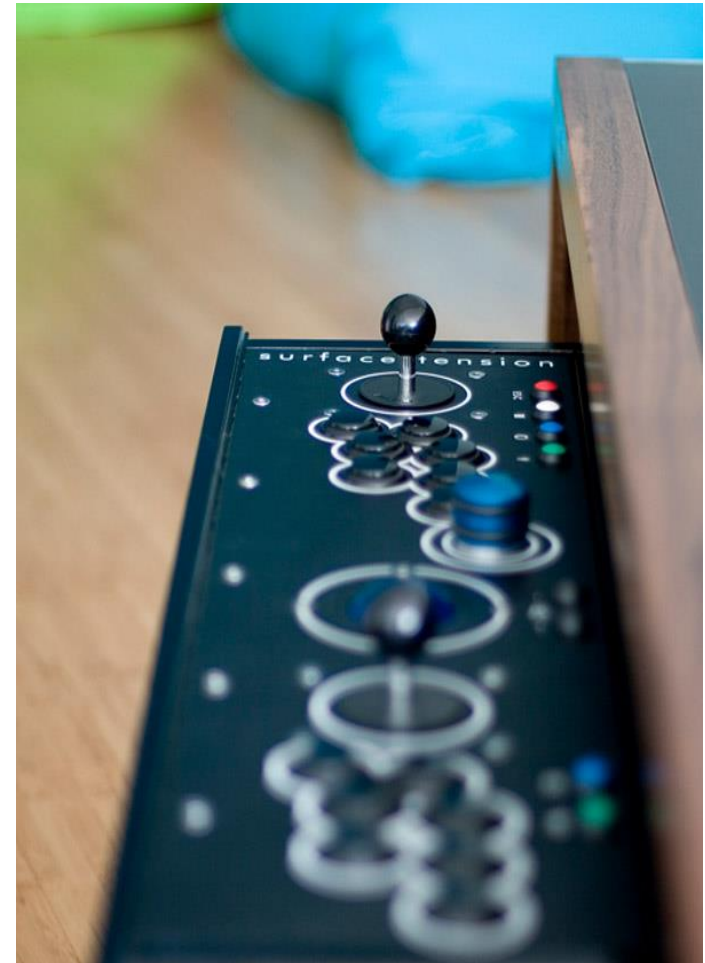
# Omni-présence

# Où se trouve le Wi-Fi ?

- En 2011, 761 million de produits vendus équipés du Wi-Fi
  - Smartphones, netbooks, TV, walkman, consoles de jeux...
  - Estimation: plus de 2 milliard en 2015
- Mais aussi
  - Voitures, systèmes d'alarme, systèmes médicaux, électroménager et domotique, systèmes de télé-conference, balances connectées...

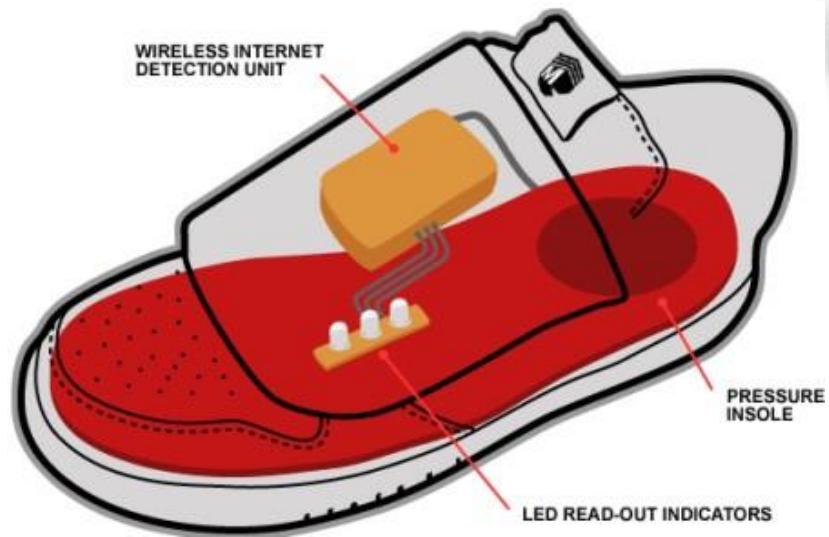


## La table basse arcade Wi-Fi...





# Les chaussures Wi-Fi...



# L'électroménager Wi-Fi



# Du Wi-Fi partout, tout le temps



Les trains Pendolino de [Virgin](#) au Royaume-Uni proposent un service Wi-Fi payant (sauf si vous voyagez en première classe) : 1 heure à £5, 1 jour à £10 ou 12 mois à £240. Les clients T-Mobile ont des réductions.



# Détection de réseaux Wi-Fi

# Détection d'équipements Wi-Fi

- Écoute passive des canaux 802.11
  - Détection des AP par leur *beacon*
  - Écoute des communications entre terminaux :
    - Nombreux logiciels open-source et commerciaux disponibles
- Détection active
  - 802.11 MAC permet l'émission de la trame PROBE\_REQUEST
  - Le modem qui la décode y répond avec un PROBE\_RESPONSE



# Exemple de "PROBE"

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	SonyComp_f1:f7:b4	Z-Com_35:66:08	802.11	51	Probe Request,
2	0.002586	Z-Com_35:66:08	SonyComp_f1:f7:b4	802.11	232	Probe Response,

+ Frame 1: 51 bytes on wire (408 bits), 51 bytes captured (408 bits)  
 - IEEE 802.11 Probe Request, Flags: .....  
   Type/Subtype: Probe Request (0x04)  
   + Frame Control: 0x0040 (Normal)  
   Duration: 314  
   Destination address: Z-Com\_35:66:08 (00:19:70:35:66:08)  
   Source address: SonyComp\_f1:f7:b4 (00:24:8d:f1:f7:b4)  
   BSS Id: Z-Com\_35:66:08 (00:19:70:35:66:08)  
   Fragment number: 0  
   Sequence number: 681  
 - IEEE 802.11 wireless LAN management frame  
   - Tagged parameters (27 bytes)  
     + Tag: SSID parameter set: wifiMitch  
     + Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]  
     + Tag: Extended Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]

```

0000  40 00 3a 01 00 19 70 35 66 08 00 24 8d f1 f7 b4  @.....p5 f..$....
0010  00 19 70 35 66 08 90 2a 00 09 57 69 66 69 4d 69  ..p5f...*..wifiMi
0020  74 63 68 01 04 82 84 8b 96 32 08 0c 12 18 24 30  tch......2....$0
0030  48 60 6c                                           H`l
  
```

# **Risques liés au Wi-Fi**

# Risques physiques

- Contrairement aux réseaux filaires, les réseaux Wi-Fi sont diffusés à tous
  - > Certes, il faut se trouver dans la couverture
  - > mais c'est plus simple que d'obtenir un accès physique à une prise Ethernet
- N'importe qui peut scanner passivement les réseaux et enregistrer le trafic
- Aucune protection contre un **déni de service "physique"**
  - > brouilleur de fréquence



# Risques logiques

- Les trames de management n'étaient pas authentifiées (dans la norme jusqu'à IEEE 802.11w-2009, mais qui n'est pas implémentée dans tous les équipements)
  - il est possible de "**forger des trames**" pour perturber le réseau (dé-association, dé-authentification)
- Les échanges ne sont pas forcément chiffrés (mode OPEN pour les hotspots)
- L'accès n'est pas forcément bien protégé
  - > WEP
  - > WPA(2) avec PSK faible

# **Sécurisation du Wi-Fi, les mécanismes originels de la norme**

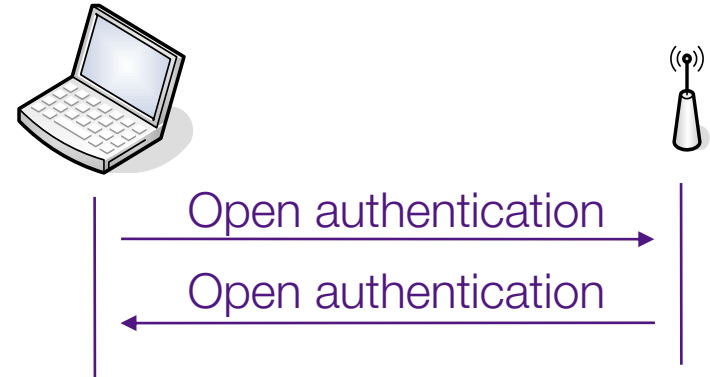
# Mécanismes originels (et faillibles)

- Autorisation
  - > Filtrage par adresse MAC
- Authentification
  - > Pre-Shared Key : Secret partagé
- Confidentialité / Intégrité
  - > Wired Equivalent Privacy (WEP)

# Authentication

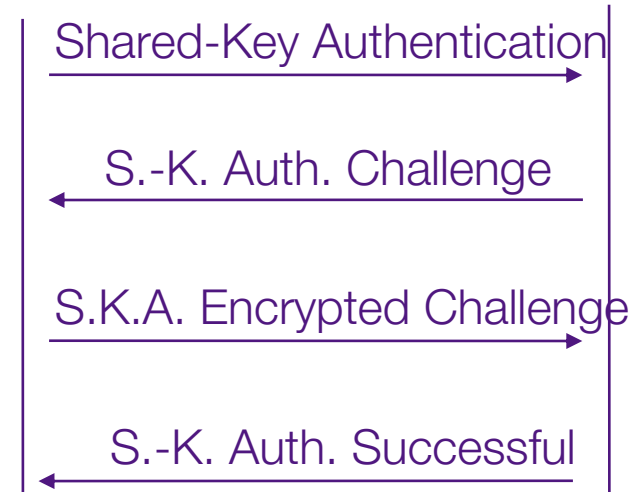
- « *Authentication* » ouverte (mode OPEN)

- > Par connaissance du SSID



- Par clé partagée (challenge-réponse) en WEP

- > Demande d'authentification sur l'AP
- > L'AP envoie un aléa (le challenge)
- > Le client retourne la réponse
- > L'AP vérifie la validité de la réponse pour accepter ou non l'association de la station



# **Sécurisation du Wi-Fi, les vulnérabilités originelles**

# MAC Access Control

- Ne peut pas être considéré comme un mécanisme de contrôle d'accès
  - > Basé sur un élément public et diffusé en clair lors d'échanges même chiffrés
  - > C'est de l'identification, pas de l'authentification
- Concrètement, il suffit :
  - > de sniffer les trames Wi-Fi pour déterminer les adresses MAC autorisées
  - > usurper une adresse MAC légitime

# Vulnérabilités du WEP

- WEP : Wired Equivalent Privacy
- Le mécanisme possède des vulnérabilités de conception cryptographique
- Les premières attaques visant le WEP sont publiées en 2004
- Plusieurs outils implémentent cette attaque (aircrack-ng) et la résistance du WEP est de l'ordre de **quelques minutes**, quelque soit la robustesse de la PSK.
  - > le WEP est à bannir quel que soit l'usage

# Faiblesse conceptuelle : le partage du secret

- Partage d'un secret entre  $n$  personnes : ce n'est plus un secret !
  - > Toutes les stations
  - > Tous les AP
- Pas de mécanisme de distribution du secret
  - > Configuration « à la main » dans les stations et AP



# Attaques & outils


- Déni de service (brouillage)
- Déni de service (dé-authentification, dé-association)
- Brute-force de la clé
- Cassage des clés WEP
  
- Outils
  - > DoS : scapy
  - > Cassage de clés : aircrack-ng
  - > Enregistrement de trafic : airodump

# **Sécurisation du Wi-Fi, les « nouveaux » mécanismes**

# IEEE 802.11i

- Objectif : sécuriser le protocole au niveau 2
- Réel contrôle d'accès est réalisé au niveau des points d'accès
  - > Volonté de réaliser un contrôle d'accès strict en fonction du résultat de l'authentification
- Faire réaliser l'authentification par une base centrale d'authentification :
  - > Volonté de flexibilité quant aux méthodes d'authentification
  - > Volonté d'avoir une authentification par utilisateur / station et non plus une authentification de groupe
- Revoir les mécanismes de confidentialité et d'intégrité
  - > Volonté d'avoir des mécanismes robustes et en fonction du matériel disponible
    - Introduction des mécanismes TKIP et CCMP

# Certification WPA

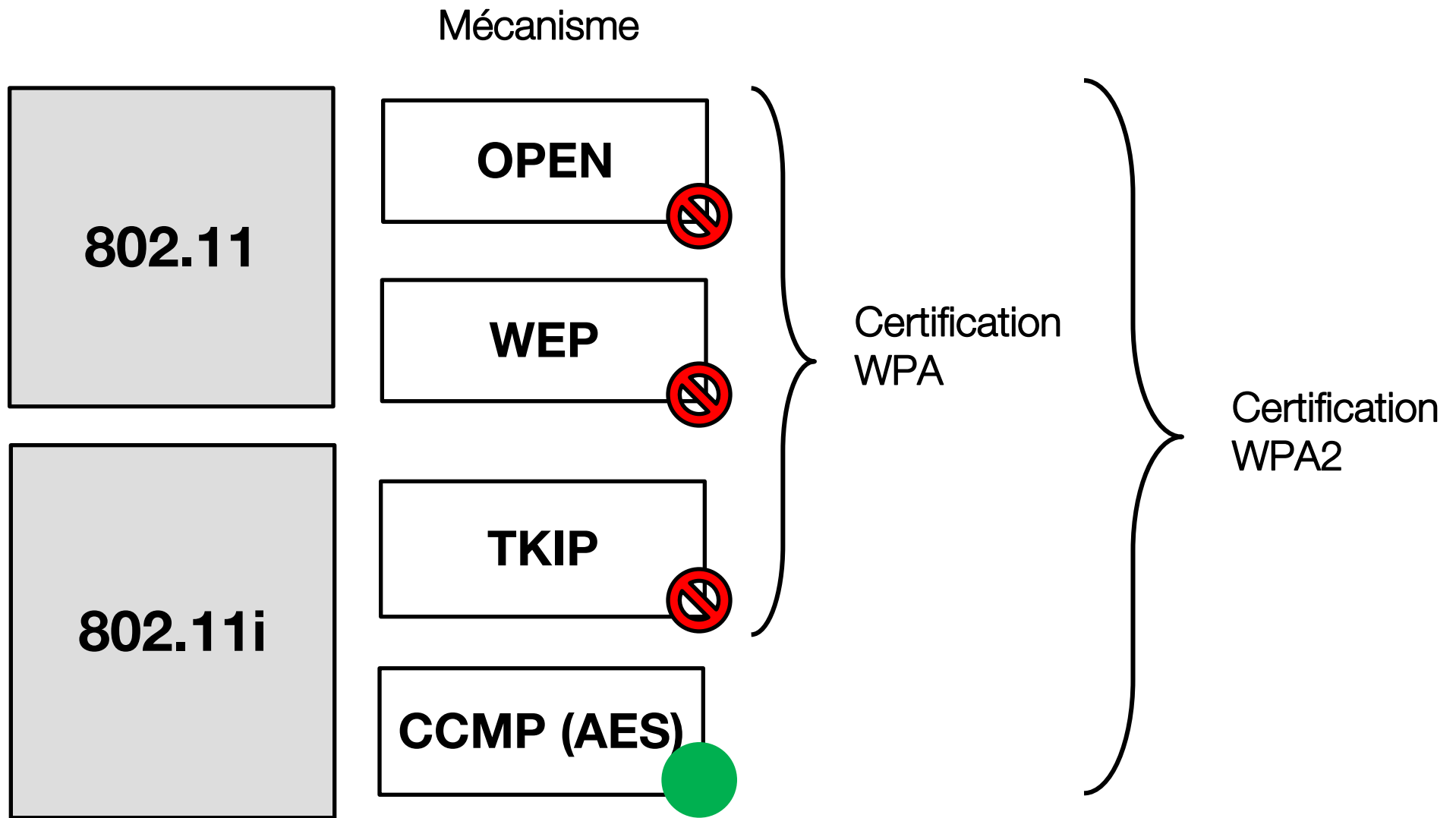
- WPA The logo for Wi-Fi Protected Access (WPA) is displayed. It features a blue circle with a white play button icon inside, followed by the text "Wi-Fi" in a light blue sans-serif font, and then "Protected Access" in a larger, bold blue sans-serif font, with a small "TM" trademark symbol at the end.
- Certification définie par la Wi-Fi Alliance en octobre 2002
- Buts :
  - > **Certifier la bonne implémentation d'une première partie du 802.11i**
  - > Volonté d'apporter ces évolutions le plus rapidement possible
  - > Doit être « rétro-compatible », et supporter un mode « mixte »
  - > **Doit implémenter TKIP en plus de WEP et mode OPEN**

# Certification WPA2



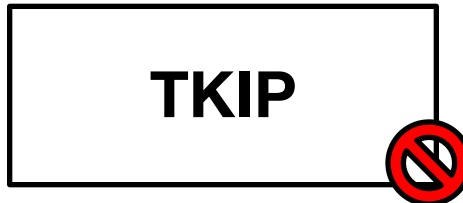
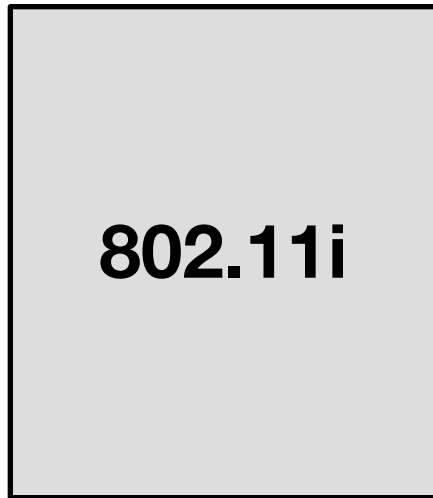
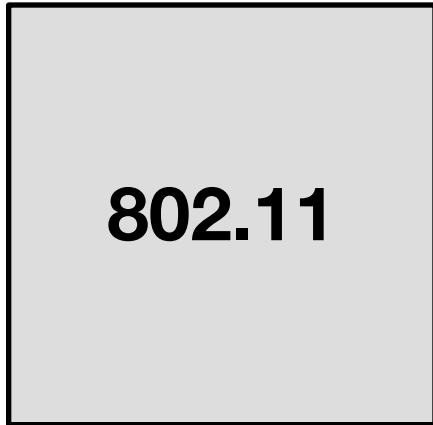
- Certification définie par la Wi-Fi Alliance à la suite de la ratification de IEEE 802.11i
  
- Buts :
  - > **Certifier les nouveaux mécanismes ratifiés dans IEEE 802.11i dans son ensemble**
  - > **L'implémentation du mécanisme CCMP est obligatoire (son utilisation optionnelle)**

# Étendue



# Étendue

## Mécanisme

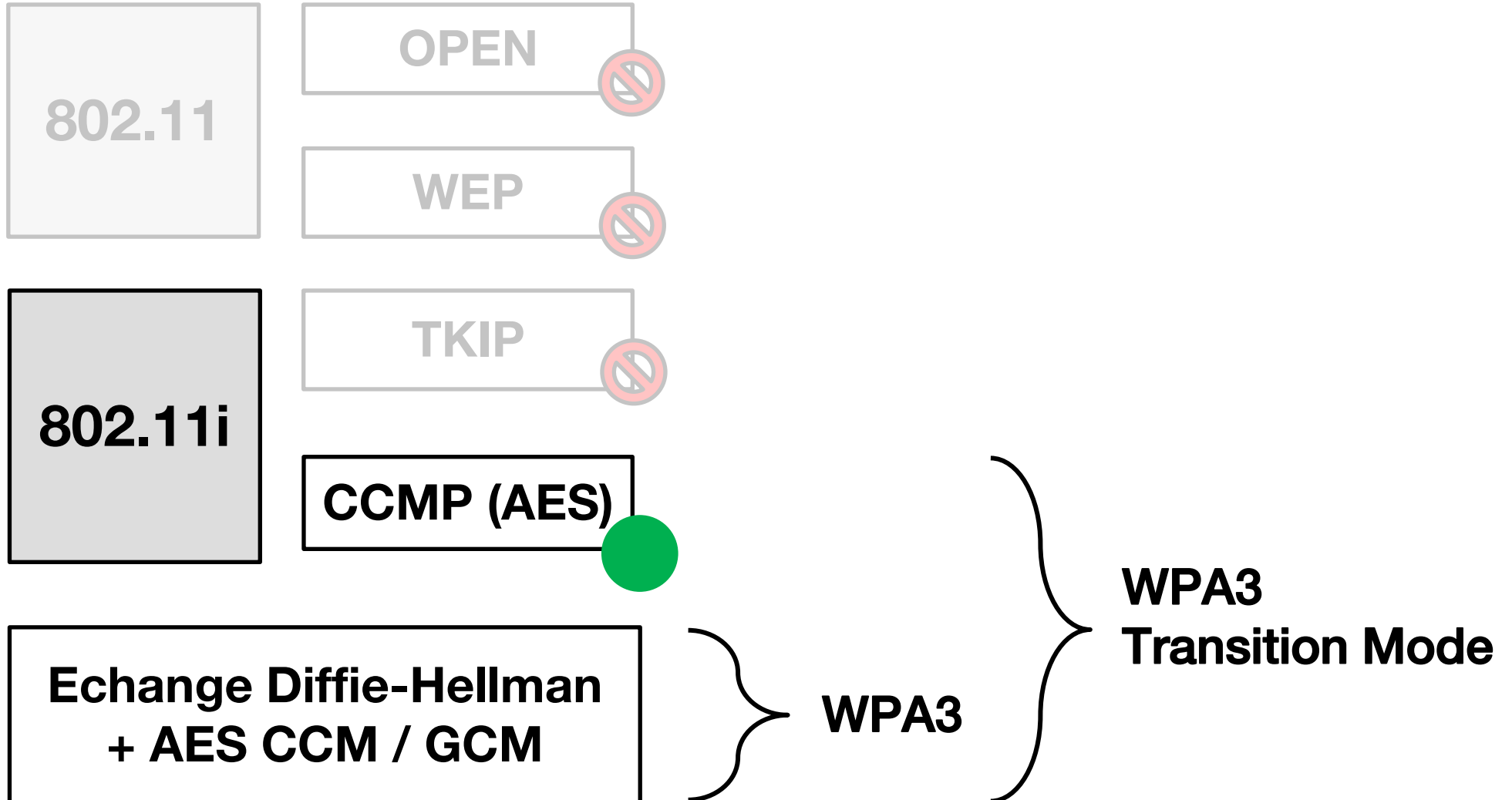


Par abus de langage : WPA

Par abus de langage : WPA2

# Étendue

## Mécanisme





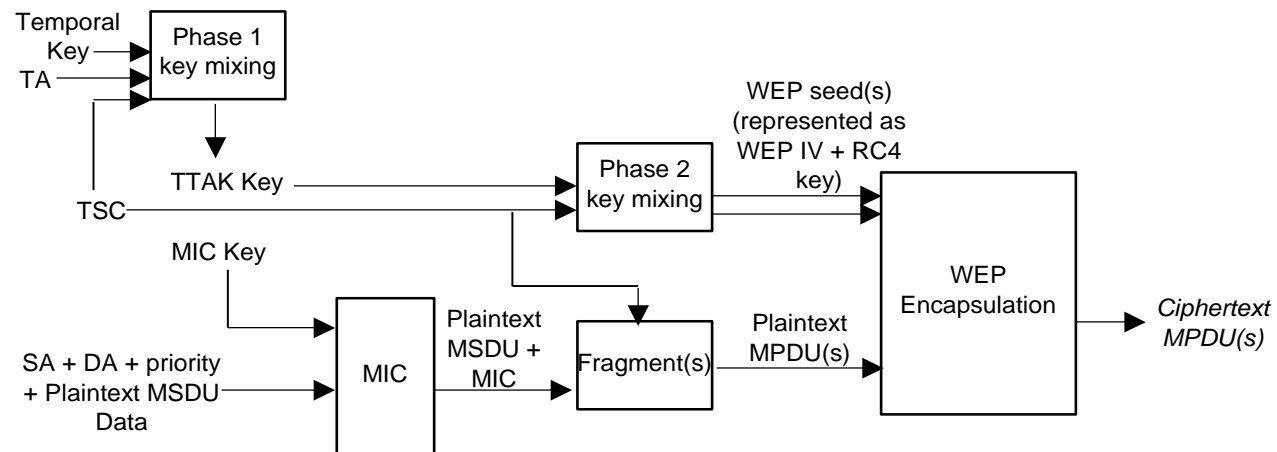
# TKIP - "WPA"



- Temporal Key Integrity Protocol

- > Amélioration du protocole WEP

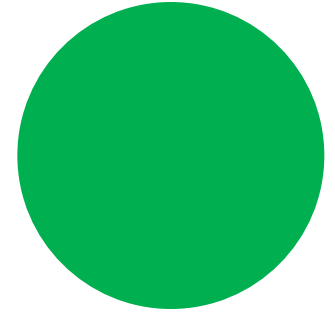
- Message Integrity Check : en plus du Integrity Check Value original de WEP
    - TKIP Sequence Counter (TSC) : numéro de séquence
    - A seulement été conçu comme **mécanisme de transition** qui continuait d'utiliser les composants matériel du WEP en intégrant quelques changements.



# TKIP – les attaques

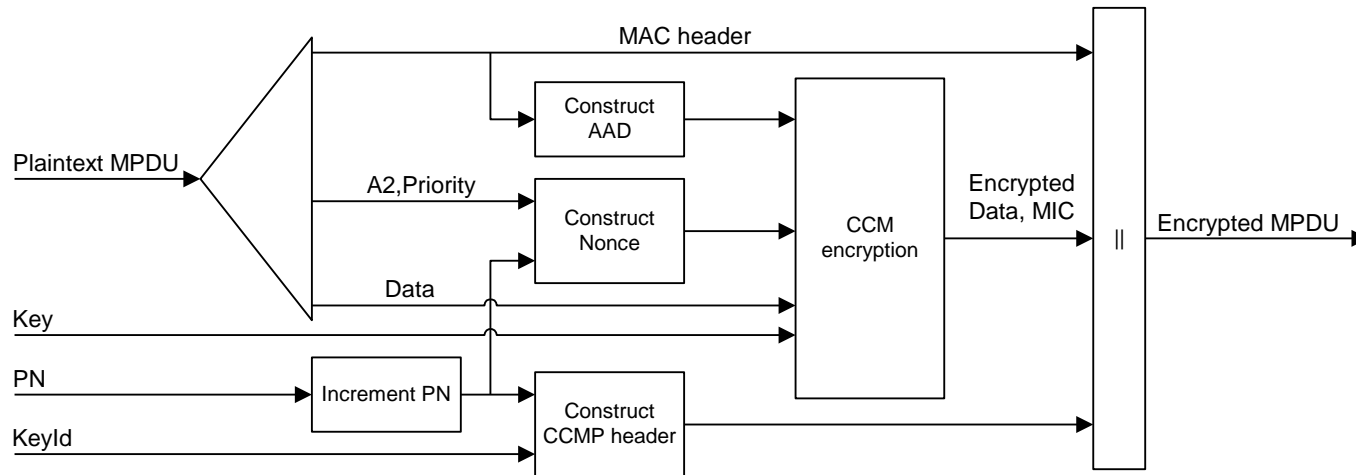
- Attaque théorique sur TKIP pour retrouver la Temporal Key (clé de chiffrement)
  - Moen, Raddum et Hole en 2004; fonction de *Key Mixing* inversible
  - A partir de quelques clés RC4 "proches" (seuls les LSB du TSC changent)
  - Réduction de la complexité du chiffrement à 105 bits (au lieu des 128 bits de clé)
- Attaques pratiques inspirées du WEP:
  - Déchiffrement d'un paquet court (requête ARP) via une attaque de type "chopchop": obtention du keystream correspondant
  - 7 à 15 réinjections de paquet possibles (grâce aux différentes valeurs de QoS disponibles), limitation dûe au compteur TSC de TKIP

# CCMP – "WPA2"



## ■ CCMP pour Counter-Mode / CBC-MAC Protocol

- > Basé sur AES (avec blocs et clé de 128 bits)
  - Counter Mode (CTR) pour le **chiffrement**
  - Cipher Block Chaining Message Authentication Code (CBC-MAC) pour l'**authentification** et l'**intégrité**
- > Packet Number (PN) : numéro de séquence pour l'anti-rejeu



# WPA3

- **Echange de clé basé sur un mécanisme Diffie-Hellman**
  - > **Obligatoire : Diffie-Hellman sur courbe elliptique module 256 bits au minimum**
  - > **Possible : Diffie-Hellman classique avec un module de 3072 bits minimum**
  
- **Chiffrement authentifié (AEAD)**
  - > **Obligatoire : AES CCM 128**
  - > **Possible : AES CCM 256, AES GCM 256**

La conception de WPA3 se rapproche des mécanismes crypto du TLS et de IPsec.

# Synthèse sur les niveaux de sécurité actuels (avant WPA3)

	Open	WEP	WPA (TKIP)	WPA2 (CCMP)
Chiffrement	Aucun	WEP	TKIP	AES (128 bits)
Echange de clé	Aucun		4 way handshake	4 way handshake
Attaques connues	Ecoute passive	Depuis 2001	Depuis 2008	
Notes	Le fameux Wi-Fi ouvert et sans sécurité.	Ne pas utiliser	Déprécié depuis janvier 2011	À utiliser avec une PSK robuste.

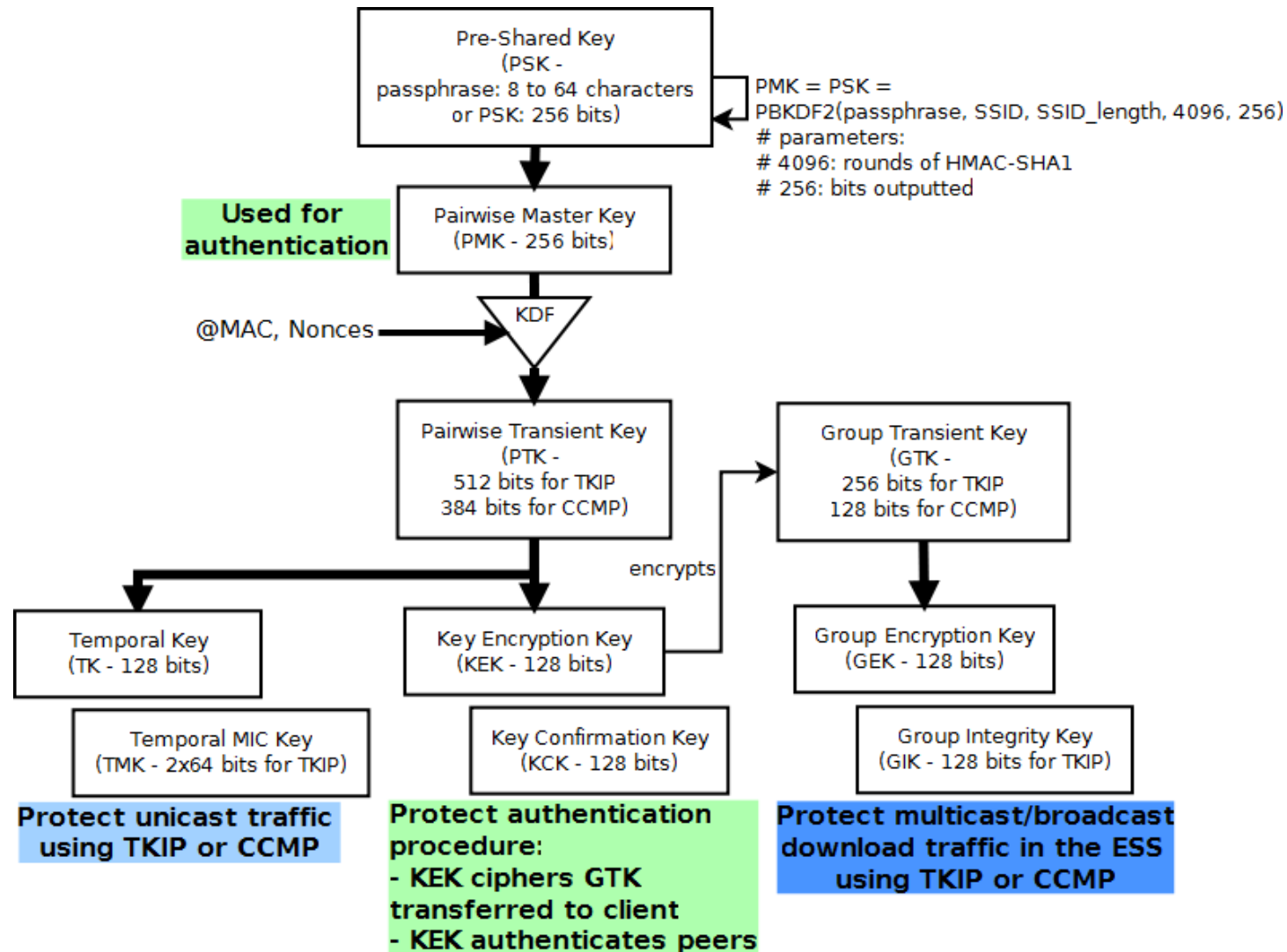
# Synthèse sur les niveaux de sécurité actuels avec WPA3

	Enhanced Open	WPA2 (CCMP) si <i>Transition Mode</i> activé	WPA3
Chiffrement	AES (128 - 256 bits)	AES (128 bits)	AES (128 - 256 bits)
Echange de clé	Diffie-Hellman Non-authentifié	4 way handshake	Diffie-Hellman
Attaques connues	Vulnérable au Man-in-the-Middle actif. Reste mieux que rien.		
Notes	L'écoute passive n'est plus possible.	À utiliser avec une PSK robuste.	

# WPA-PSK: évolution de l'authentification

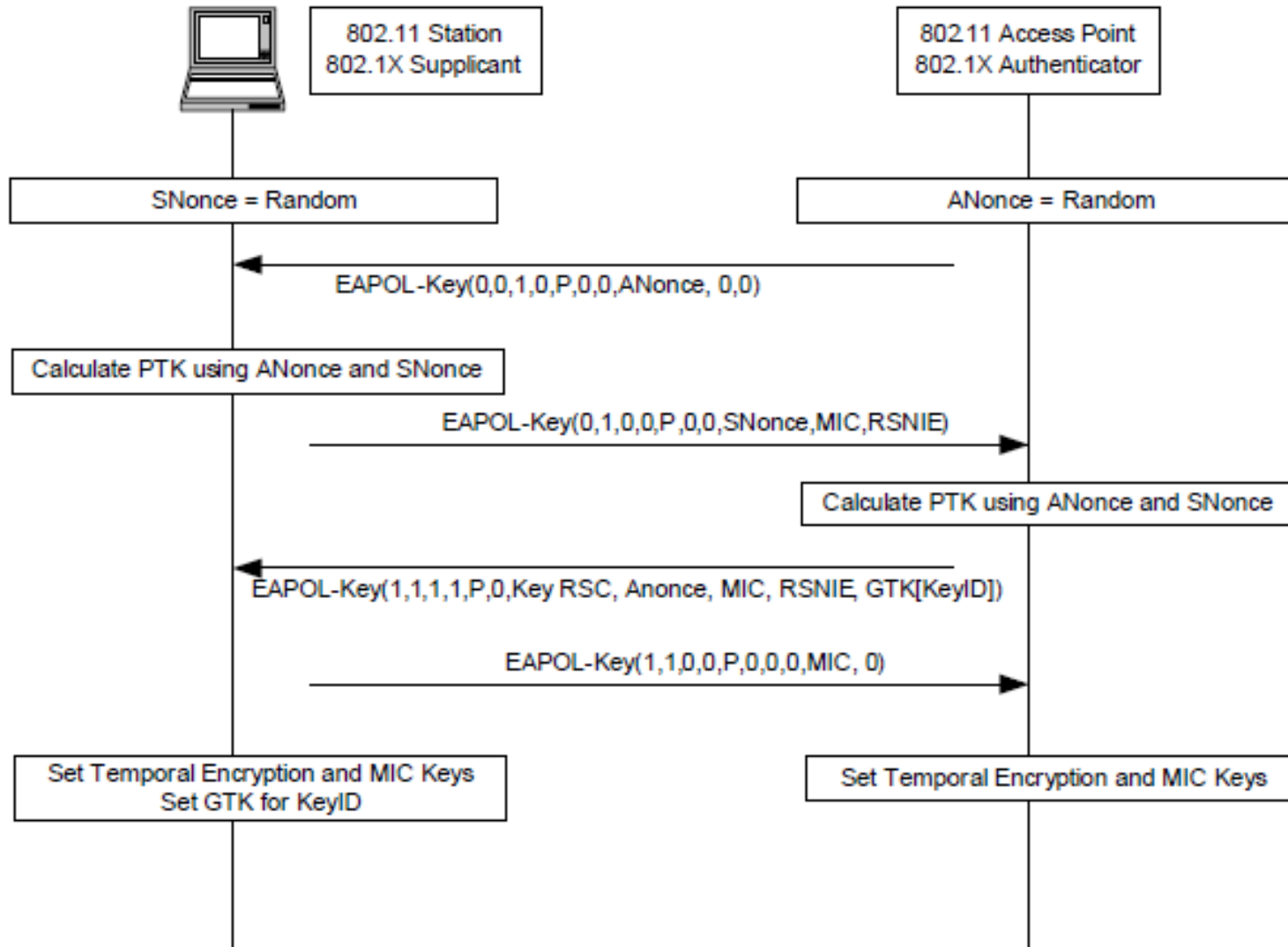
- Clé maîtresse PMK de 256 bits partagée entre STA et AP Wi-Fi
  - Souvent dérivée elle-même d'un mot de passe partagé
  - Re-dérivée à chaque session Wi-Fi en de multiples clés spécialisées
- Dissociation des clés de sessions entre utilisateurs et dans le temps
  - De la clé maîtresse PMK est dérivée une clé intermédiaire PTK (*Pairwise Transient Key*) à chaque session
  - La clé PTK est découpée en sous-clés pour la protection:
    - De certains messages dans la procédure d'authentification (KEK, KCK)
    - Des données de flux *unicast* (TK, TMK si TKIP)
    - Des données de flux *multicast* (GEK, GIK si TKIP)

# WPA-PSK : hiérarchie des clés





# Échanges d'authentification - Handshake



# Attaque du WPA-PSK

- Attaques sur la *passphrase* de WPA-PSK:
  - Écoute passive de la procédure d'authentification
    - Récupération (entre autre) des SSID, @MAC, et *nonces*
  - Tester des dictionnaires de *passphrases*
  - Pré-calculs de résultats de PBKDF2 avec dictionnaires et SSID standards
    - *Rainbow table* : accélère beaucoup la recherche de la PSK (seulement lorsque le SSID est pris en prédéfini pour la table)

**Ces attaques de brute-force, ne sont plus possibles avec WPA3, car l'échange de clé se fait par mécanisme Diffie-Hellman (sur courbe elliptique).**

# Enhanced Open

- Echange de clé : Diffie-Hellman non-authentifié
  - > Du fait qu'il est non-authentifié, cela reste possible de faire un Man-in-the-Middle actif.
  - > Cependant l'écoute passive n'est plus possible, c'est déjà mieux que le mode "Open" historique.
- Chiffrement : AES (CCM ou GCM) 128 ou 256 bits.

# WPS



- **WPS : Wi-Fi Protected Setup**

- > « Surcouche » pour la configuration sécurisée des composants de l'infrastructure Wi-Fi
- > Objectifs :
  - configurer les périphériques sans avoir à saisir manuellement la PSK

- **2 méthodes principales (au moins 4 au total)**

- > **PIN Code :**
  - saisie d'un code PIN sur chacun des équipements
- > **Push Button**
  - à utiliser si l'un des équipements ne supporte pas la méthode précédente

- **Attaque permettant le brute-force du PIN code en décembre 2011**

# WPS

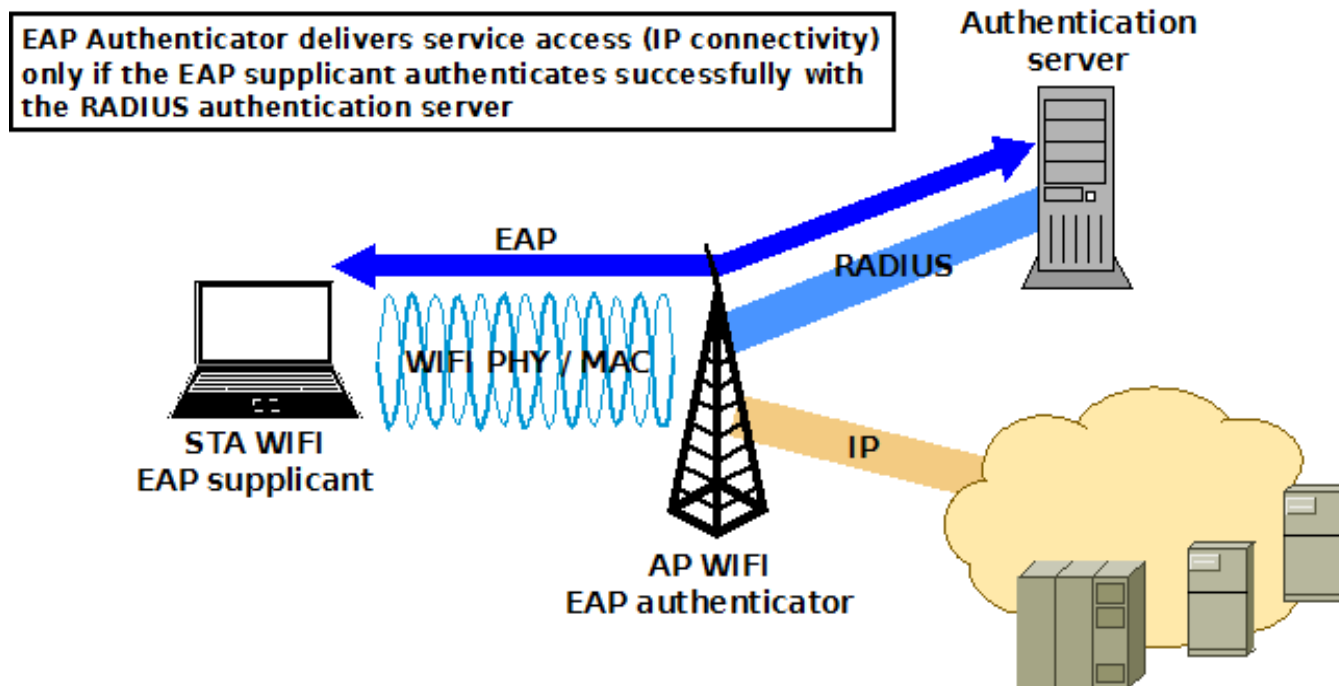
À retenir sur WPS :

**➔ Toujours désactiver WPS**

# Sécurisation par WPA2-Entreprise

# WPA2 Entreprise et 802.1X

- Authentification et contrôle d'accès centralisés
  - Utilisation de l'IEEE 802.1X entre les STA et l'AP
  - Encapsulation de trames EAP (*Extended Authentication Protocol*)
  - L'AP relaie les trames EAP vers un serveur RADIUS central



# Méthodes d'authentification EAP

- Les *supplicants* (STA Wi-Fi) et le serveur (RADIUS) EAP doivent supporter au moins une méthode d'authentification EAP commune. Les plus robustes et réputées:
  - **EAP-TLS**: authentification mutuelle entre *supplicant* et serveur par **certificats**
  - **EAP-TTLS**: authentification du serveur par certificat, et du *supplicant* par **login / password**
  - **EAP-AKA**: utilisation de la carte **USIM**, méthode privilégiée par les opérateurs mobiles
- De très nombreuses méthodes existent
  - La certification WPA Entreprise inclus 8 méthodes EAP distinctes
  - Une étude du mode de déploiement et de l'usage doit permettre de déterminer la méthode EAP la plus adaptée
  - Certaines méthodes EAP sont propriétaires (Microsoft, Cisco...)



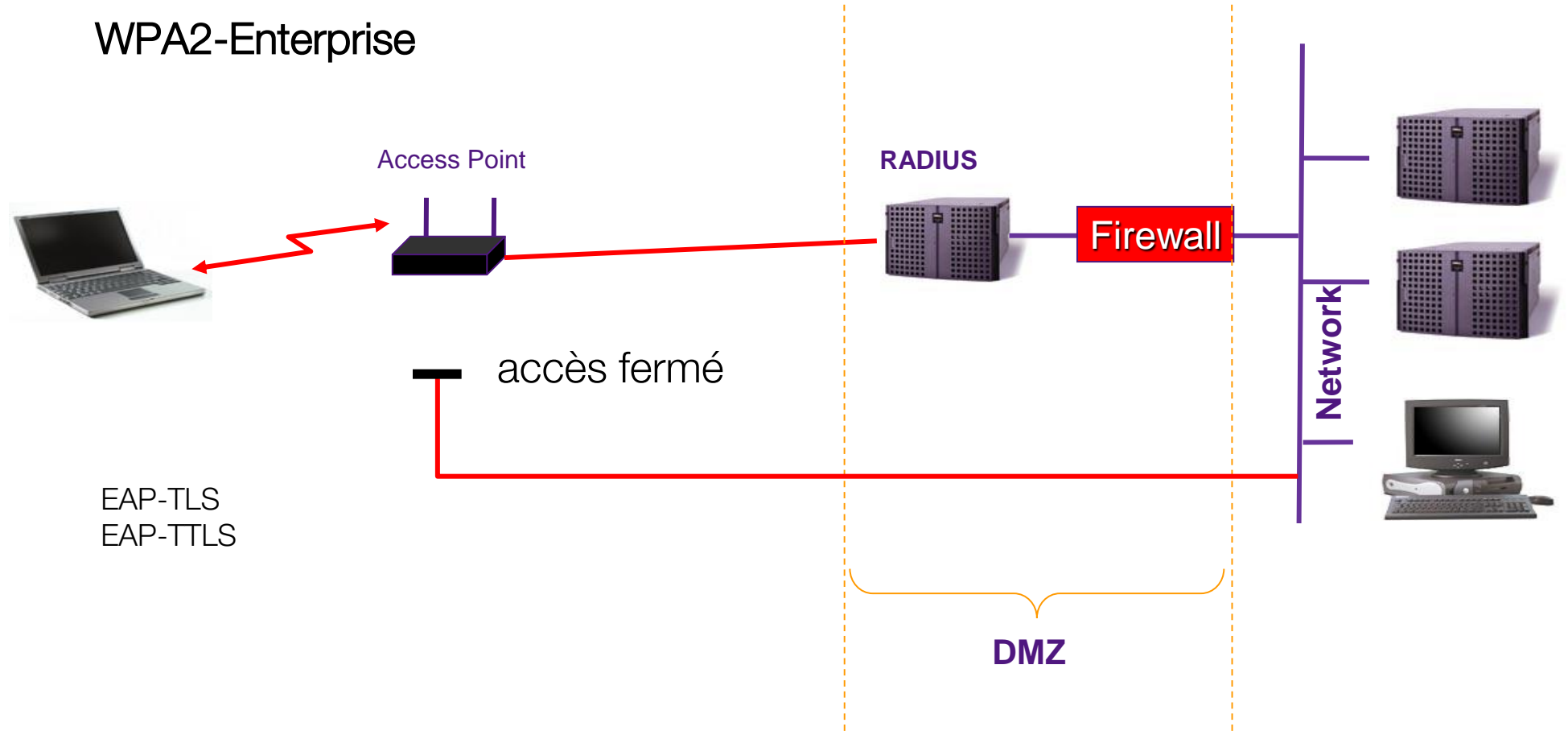
# WPA- Entreprise – les attaques

- Attaques sur des méthodes EAP peu sécurisées (exemples: EAP-MD5, LEAP)
- Attaques directes du serveur centralisé RADIUS
  - Attaques TLS (Heartbleed, ...) lorsque EAP-TLS ou EAP-TTLS est supporté

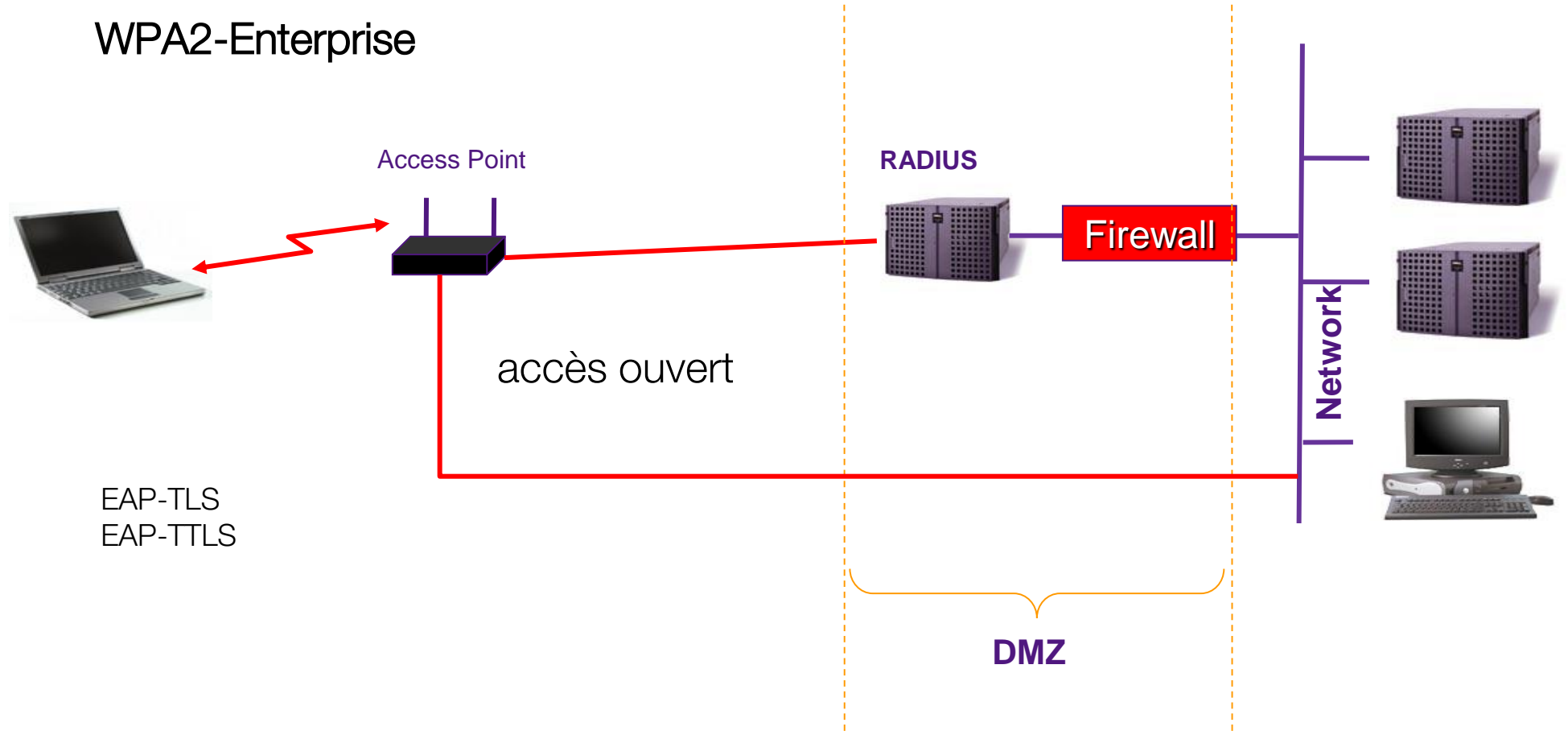
# Utilisation du Wi-Fi en contexte entreprise

- Utilisation du WPA2-Enterprise (basé sur EAP et le 802.1X)
  - > EAP-TLS
  - > EAP-TTLS
  
- Ou, en alternative : mode Wi-Fi OPEN (hotspot) avec
  - > VPN
    - VPN IPsec
    - VPN SSL

# Contexte entreprise - illustration

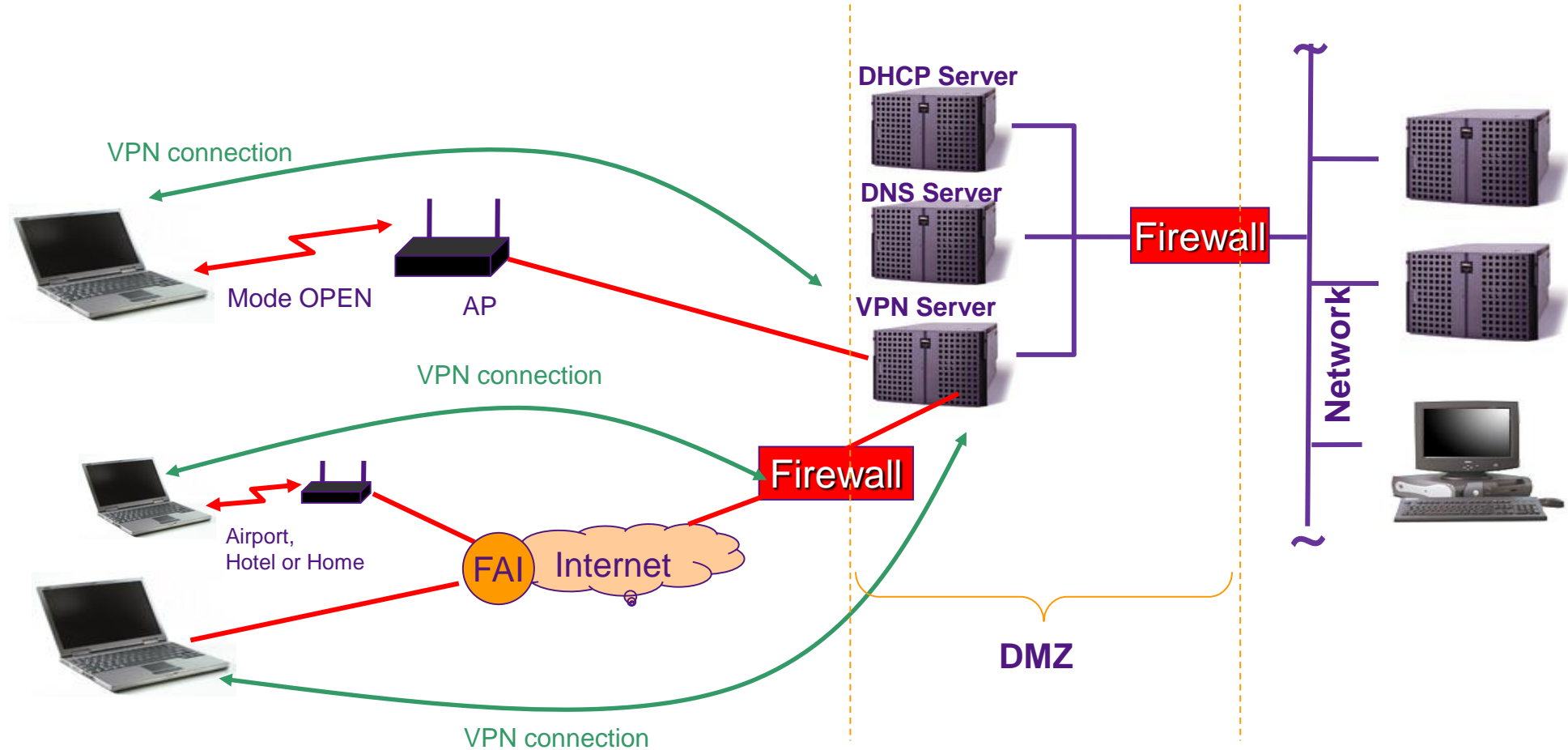


# Contexte entreprise - illustration



# Sécurisation par VPN

# Contexte entreprise - illustration



# Point d'accès illégitimes (Rogue AP)

# Interception de trafic

- **Configurer un AP ouvert**

- Mimant un AP officiel: même adresse MAC, même SSID
- Sans authentification, ni chiffrement
  - Sauf si les clés de chiffrement (WEP) ou d'authentification (WPA-PSK) peuvent être connues

- **Tout le trafic passant par l'AP illégitime est intercepté, peut-être modifié:**

- Récupération des mots de passe en clair (email, FTP, HTTP,
- injection de malwares vers les terminaux piégés



# Attachement automatique des STA

- Windows, téléphones mobiles, certains logiciels ou configurations Linux, ...
  - Paramétrés par défaut pour se connecter automatiquement aux AP connus, si disponibles
  - Y compris ceux sans sécurité ou configurés avec WEP
- Possibilité de contrefaire un AP connu "à la volée"
  - En écoutant les canaux Wi-Fi à la recherche de PROBE\_REQUEST et demandes d'association des STA
  - En cassant la clé WEP rapidement s'il le faut
- Possibilité d'attacher une STA à l'insu de l'utilisateur
- Recommandation: configurer ses connexions Wi-Fi pour ne jamais s'associer automatiquement.

## En entreprise: maîtriser ses réseaux Wi-Fi

- Nécessiter d'effectuer régulièrement des campagnes d'audits Wi-Fi sur ses sites
  - Mesurer l'exposition de son réseau
    - Et la configuration de sécurité des AP
  - Avoir conscience de l'accessibilité de son réseau hors les murs
  - Détecter des AP non officiels (voir malveillants)
    - Employé inconscient ou indélicat, facilité d'accès à l'Intranet, maintenir un accès distant illégal, ...
- Auditer même les sites ne devant pas être équipés de Wi-Fi

# Attaques sur les implémentations logicielles

# Faibles sur les modems Wi-Fi

Les chipsets Wi-Fi et leurs pilotes sont aussi sujets aux faibles logicielles

## CVE-2008-4594

**Summary:** Unspecified vulnerability in the SNMPv3 component in Linksys WAP4400N firmware 1.2.14 on the Marvell Semiconductor 88W8361P-BEM1 chipset has unknown impact and attack vectors, probably remote.

**Published:** 10/17/2008

**CVSS Severity:** 10.0 (HIGH)

## CVE-2008-4441

**Summary:** The Marvell driver for the Linksys WAP4400N Wi-Fi access point with firmware 1.2.14 on the Marvell 88W8361P-BEM1 chipset, when WEP mode is enabled, does not properly parse malformed 802.11 frames, which allows remote attackers to cause a denial of service (reboot or hang-up) via a malformed association request containing the WEP flag, as demonstrated by a request that is too short, a different vulnerability than CVE-2008-1144 and CVE-2008-1197.

**Published:** 10/14/2008

**CVSS Severity:** 7.1 (HIGH)

## CVE-2008-1144

**Summary:** The Marvell driver for the Netgear WN802T Wi-Fi access point with firmware 1.3.16 on the Marvell 88W8361P-BEM1 chipset does not properly parse EAPoL-Key packets, which allows remote authenticated users to cause a denial of service (device reboot or hang) or possibly execute arbitrary code via a malformed EAPoL-Key packet with a crafted "advertised length."

**Published:** 09/05/2008

**CVSS Severity:** 6.3 (MEDIUM)

## CVE-2008-1197

**Summary:** The Marvell driver for the Netgear WN802T Wi-Fi access point with firmware 1.3.16 on the Marvell 88W8361P-BEM1 chipset does not properly parse the SSID information element in an association request, which allows remote authenticated users to cause a denial of service (device reboot or hang) or possibly execute arbitrary code via a "Null SSID."

**Published:** 09/05/2008

**CVSS Severity:** 6.3 (MEDIUM)

# Faibles dans les pilotes Wi-Fi

Une faille dans un pilote Wi-Fi peut permettre d'exécuter du code arbitraire sur une machine distante avec les privilèges du système...

<a href="#">CVE-2008-4441</a>	May. 2008	Marvell Driver Malformed Association Request Vulnerability	Discovered by Laurent Butti and Julien Tinnes	No exploit disclosed
<a href="#">CVE-2008-1197</a>	Feb. 2008	Marvell Driver Null SSID Association Request Vulnerability (affects at least some Netgear products)	Discovered by Laurent Butti and Julien Tinnes	No exploit disclosed
<a href="#">CVE-2008-1144</a>	Nov. 2007	Marvell Driver EAPoL-Key Length Overflow (affects at least some Netgear products)	Discovered by Laurent Butti and Julien Tinnes	No exploit disclosed
<a href="#">CVE-2007-5474</a>	Oct. 2007	Atheros Vendor Specific Information Element Overflow (affects at least some Linksys products)	Discovered by Laurent Butti and Julien Tinnes	No exploit disclosed
CVE-2007-5475	Oct. 2007	To be disclosed remote vulnerability (waiting for vendor)	Discovered by Laurent Butti and Julien Tinnes	No exploit disclosed
<a href="#">CVE-2007-5651</a>	Jul. 2007	Cisco products EAP denial of service vulnerability	Discovered by Benoit Stopin, Laurent Butti, Franck Veyssset and Julien Tinnes	No exploit disclosed
<a href="#">CVE-2006-6332</a>	Nov. 2006	MadWifi buffer overflow vulnerability	Discovered by Jerome Razniewski, Laurent Butti and Julien Tinnes	Remote Linux kernel exploit published in Metasploit

## Failles dans les pilotes Wi-Fi (2)

- Plus récemment dans Android et/ou Linux:
  - CVE-2015-0973: fonctionnalité WLAN Direct
    - *Remotely exploitable memcpy() overflow in p2p\_add\_device() in wpa\_supplicant*
  - CVE-2015-1863: wpa-supPLICANT
    - *Heap-based buffer overflow in wpa\_supplicant 1.0 through 2.4 allows remote attackers to cause a denial of service (crash), read memory, or possibly execute arbitrary code via crafted SSID information in a management frame when creating or updating P2P entries.*
  - CVE-2015-5310: Android
    - An elevation of privilege vulnerability in the Wi-Fi component could enable a locally proximate attacker to gain access to Wi-Fi service related information.

## Failles dans les pilotes Wi-Fi (3)

- CVE-2016-0801, 0802: modems Broadcom
- *Multiple remote execution vulnerabilities in the Broadcom Wi-Fi driver could allow a remote attacker to use specially crafted wireless control message packets to corrupt kernel memory in a way that leads to remote code execution in the context of the kernel.*

# CVE pour "wireless"...

There are **230** matching records. Displaying matches **1** through **20**.

[1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [>](#) [>>](#)

## **CVE-2011-4507**

VU#924307

**Summary:** The D-Link DIR-685 router, when certain WPA and WPA2 configurations are used, does not maintain an encrypted wireless network during transfer of a large amount of network traffic, which allows remote attackers to obtain sensitive information or bypass authentication via a Wi-Fi device.

**Published:** 11/22/2011

**CVSS Severity:** 7.5 (HIGH)

## **CVE-2011-3386**

**Summary:** Unspecified vulnerability in Medtronic Paradigm wireless insulin pump 512, 522, 712, and 722 allows remote attackers to modify the delivery of an insulin bolus dose and cause a denial of service (adverse human health effects) via unspecified vectors involving wireless communications and knowledge of the device's serial number, as demonstrated by Jerome Radcliffe at the Black Hat USA conference in August 2011. NOTE: the vendor has disputed the severity of this issue, saying "we believe the risk of deliberate, malicious, or unauthorized manipulation of medical devices is extremely low... we strongly believe it would be extremely difficult for a third-party to wirelessly tamper with your insulin pump... you would be able to detect tones on the insulin pump that weren't intentionally programmed and could intervene accordingly."

**Published:** 09/02/2011

**CVSS Severity:** 4.0 (MEDIUM)

## **CVE-2011-2176**

**Summary:** GNOME NetworkManager before 0.8.6 does not properly enforce the auth\_admin element in PolicyKit, which allows local users to bypass intended wireless network sharing restrictions via unspecified vectors.

**Published:** 09/02/2011

**CVSS Severity:** 2.1 (LOW)

## **CVE-2011-2064**

**Summary:** Cisco IOS 12.4MDA before 12.4(24)MDA5 on the Cisco Content Services Gateway - Second Generation (CSG2) allows remote attackers to cause a denial of service (device reload) via crafted ICMP packets, aka Bug ID CSCtl79577.

**Published:** 07/11/2011



# Compromission via les interfaces radio

- La plupart des failles logicielles entraînent des dénis de service lorsqu'elles sont déclenchées
  - Arrêt / reboot d'un composant, voir de l'OS
  - Impacts sur la disponibilité de l'infrastructure Wi-Fi
- Dans certains cas, la compromission silencieuse de l'OS est possible !
- Recommandation: éteindre son interface Wi-Fi lorsque celle-ci n'est pas nécessaire
- Nécessité de maintenir à jour les firmwares et pilotes des interfaces Wi-Fi
  - Mise à jour des AP et terminaux
  - Attention: sur les terminaux, les OS ne prennent pas toujours en charge la mise à jour des périphériques Wi-Fi

# Attaques et dénis de service divers

# Transmission radio

- Transmissions radio très vulnérables au déni de service de part leur nature
  - Bande de fréquence des 2.4 Ghz très chargée: peut être simplement saturée
  - *Radio jamming*: émettre du bruit sur des bandes de fréquences spécifiques

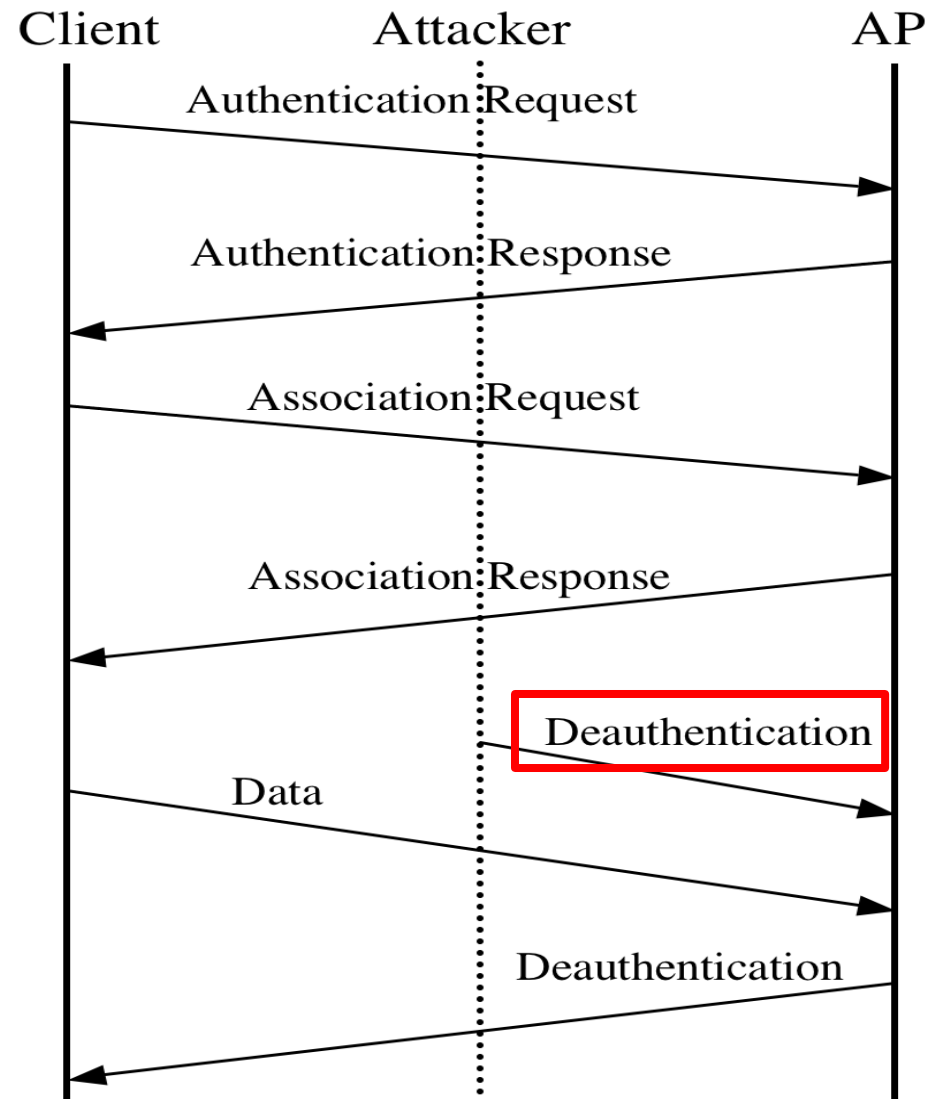
**INTERDIT !**



# Déni de service de stations Wi-Fi

- Les trames de gestion 802.11 MAC ne sont pas protégées cryptographiquement:
  - *deauthentication, disassociation*
  - Permet un déni de service ciblé, en usurpant l'adresse MAC de la victime
- En règle générale, les technologies radio acceptent systématiquement des demandes non protégées d'arrêt du lien radio
  - Permet de sauvegarder les ressources de l'infrastructure en cas de mauvais fonctionnement de terminaux

# Désauthentification Wi-Fi



# **Solutions recommandées**

La norme et les produits Wi-Fi souffrent de beaucoup d'écueils en terme de sécurité.

Il est difficile d'avoir un réseau Wi-Fi bien sécurisé.

# Recommandations ANSSI sur l'usage du Wi-Fi (résidentiel):

[http://www.ssi.gouv.fr/IMG/pdf/NP\\_WIFI\\_NoteTech.pdf](http://www.ssi.gouv.fr/IMG/pdf/NP_WIFI_NoteTech.pdf)



## En environnement professionnel

- Dans un déploiement, penser à inclure la sécurité dès le départ
- Utiliser « **WPA2** » (bientôt **WPA3**) avec un chiffrement **AES** et une authentification forte
  - Sur tous les points d'accès et les stations clientes
  - Utiliser un serveur d'authentification (de type RADIUS), mettant en oeuvre des méthodes robustes (certificats, cartes à puce)
- Maintenir les logiciels à jour
  - Firmware des points d'accès, systèmes et applicatifs des serveurs centraux (RADIUS, administration)
  - Drivers et systèmes d'exploitation des stations clientes

## Sur les points d'accès

- Configurer un SSID spécifique et non significatif
  - Ne pas utiliser de SSID par défaut
- Désactiver systématiquement le *Wi-Fi Protected Setup* (WPS)
- Sécuriser les interfaces d'administration des points d'accès
  - Ne pas rendre accessible l'interface d'admin aux stations clientes Wi-Fi
- Superviser la sécurité des points d'accès
  - Centralisation et analyse des logs

# Sur les stations de travail

- Configurer la connectivité Wi-Fi selon la politique des points d'accès de l'environnement professionnel
  - WPA2 – AES authentication 802.1X avec une méthode forte.
- En mobilité, utiliser un VPN vers le réseau professionnel
- Désactiver l'association automatique avec les points d'accès Wi-Fi connus
- Éteindre les interfaces radio lorsqu'elles ne sont pas utilisées

# **Merci**