8. Wi-Fi

M1 Outils de l'Internet
lundi 22 novembre 2010

victor.poupet@lif.univ-mrs.fr

Présentation

Où sont les fiiiiiils ?

(avec leurs gestes pleins de charme)

- Réseaux sans fil
- Plus simple
- Portable
- Encore mieux que *plug-and-play* !

Utilisation

- Un appareil capable de communiquer par Wi-Fi (ordinateur, PDA, téléphone, console, etc.)
- Un réseau connecté à Internet
- Un point d'accès (*hotspot*) Wi-Fi (sur le réseau)

Intérêt

- Pas de fils
- Facilité en extérieur
- Bâtiments où les travaux ne sont pas possibles
- Compatibilité internationale (“Wi-Fi certified”)

Côté machines

- Ajout d'une "carte WLAN" (émission/réception)
- La plupart des portables actuels sont équipés
- 1999 : les *iBook* sont les premiers ordinateurs avec Wi-Fi intégré (appelé *AirPort*)

Développement

Origine

- Le Wi-Fi repose sur les technologies Direct Sequence Spread Spectrum (DSSS) et Orthogonal Frequency Division Multiplexing (OFDM)
- Ces technologies datent d'environ 1985
- Fin 1980s : AT&T développe le WaveLAN
- Puis l'IEEE développe les normes

Direct Sequence Spread Spectrum

- Chaque bit d'information est encodé par une séquence (appelée séquence *Barker*)
- 1 = 10110111000, 0 = 01001000111
- Redondance donne de la robustesse (détection et correction d'erreurs)

Deux modes de fonctionnement

- Mode *infrastructure* : chaque station reliée à un point d'accès (lui-même sur une réseau filaire)
- Mode *ad-hoc* : stations reliées entre elles (connexions directes uniquement par défaut)

Standardisation

- Norme IEEE 802.11b
- Standard de réseau sans fil (WLAN)
- Wireless Ethernet Compatibility Alliance (WECA) fournit un label “Wi-Fi” aux appareils respectant le standard

Wi-Fi Alliance

- Consortium créé en 1999 possédant la marque Wi-Fi
- Objectif : promouvoir l'utilisation des WLAN
- Certifie la compatibilité avec la norme 802.11
- Initialement WECA
- Environ 300 membres aujourd'hui

Certification Wi-Fi

- Interopérabilité (et rétro-compatibilité)
  - Compatibilité
  - Conformité
  - Efficacité

Il existe différents niveaux de certification (avec des critères obligatoires et des critères optionnels)

Fréquences

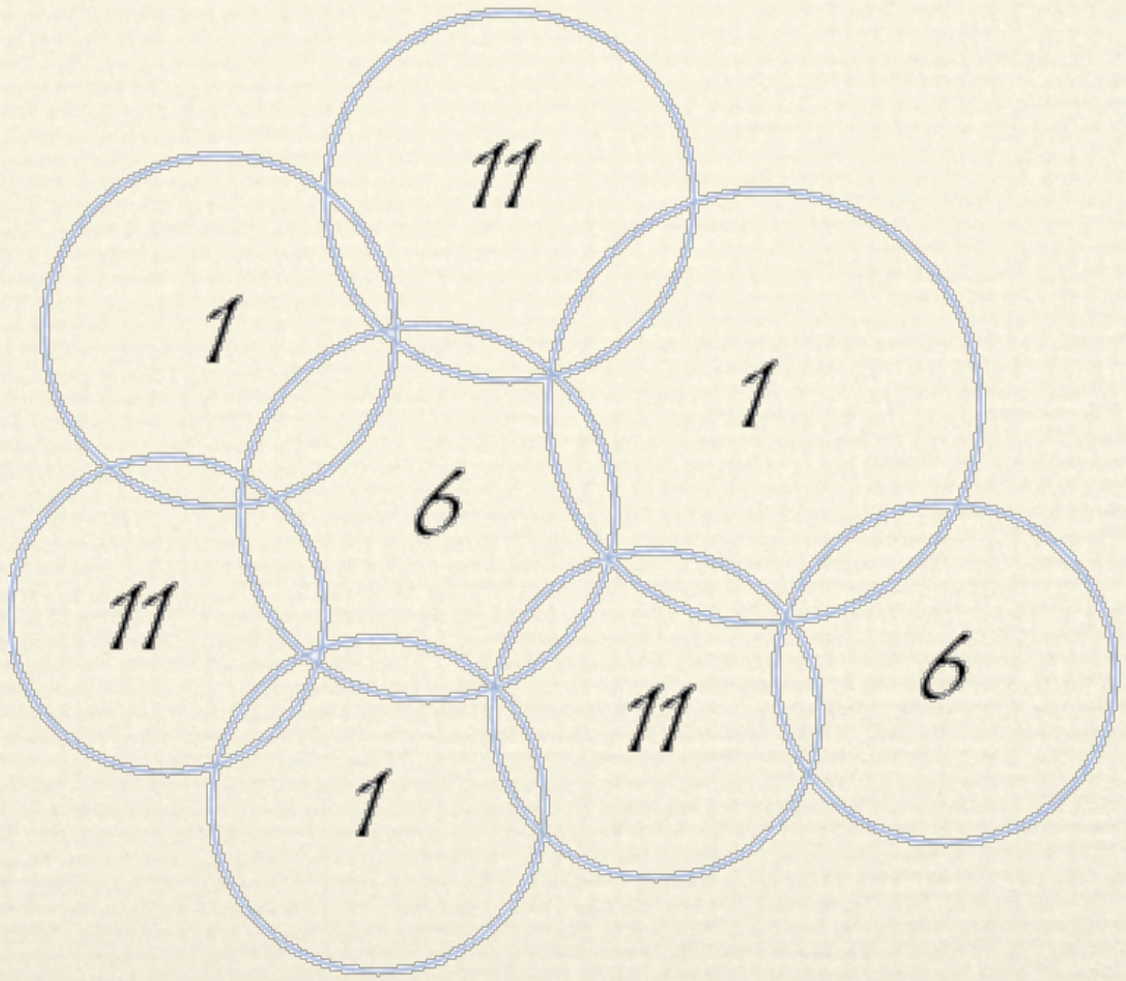
- 3 bandes de fréquence : 2,4 GHz (14 canaux) et 5,150-5,350 GHz et 5,470-5,725 GHz
- Bande ISM (2,4GHz) partagée par de nombreuses autres technologies → interférences

International

- Canaux 1 à 11 de 2,412 à 2,462 GHz : Europe, USA, Japon
- Canaux 12 et 13 à 2,467 et 2,472 GHz : Europe, Japon
- Canal 14 à 2,484 GHz : Japon
- En réalité un signal s'étend sur 5 canaux...

Interférences

- Utiliser des canaux bien distincts



Frequency Hopping Spread Spectrum

- Initialement, technique militaire pour brouiller les communications
- On change de canal à intervalles réguliers (400ms)
- Bande de 2,4kGHz permet de définir 79 canaux d'un MHz
- Évite partiellement les interférences

Méthode d'accès

- Dans un réseau classique : CSMA/CD
- Impossible dans un réseau sans fil
- On utilise la méthode *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA)

CSMA/CA

- Fonctionnement à l'aide d'accusés de réception (ACK)
- Si le réseau est libre, on émet une demande (*Ready to Send*)
- Récepteur répond si le réseau est libre
- Les données sont envoyées
- Le récepteur accuse réception

Fragmentation

- Risque d'erreur de transmission dans un réseau sans fil
- Probabilité d'erreur augmente exponentiellement avec la longeur du message
- Possibilité de fragmenter les paquets
- Checksum à la fin de chaque fragment

Portée

- La portée dépend beaucoup de l'environnement
- Routeur personnel : environ 30m en intérieur et 90m en extérieur
- Portée dépend également de la fréquence
- On peut atteindre une portée de plusieurs kilomètres en extérieur avec des antennes directionnelles

Muni-Fi

Accès municipal

- Réseau sans fil à l'échelle d'une ville
- Utilise une structure de réseau maillé
- Globalement plus rentable
- Risque de monopole

Financement

- L'installation est le principal coût (intialement payé par la municipalité ou le FAI)
- Service payant par abonnement, financé par la publicité ou gratuit
- Modèle financier difficile à mettre en place

Exemples

- Google WiFi : Mountain View, Californie (nécessite un compte google, gratuit)
- Déjà existant dans plusieurs villes à travers le monde : Auckland, Boston, Montreal, Paris, Singapour, etc.

Réseaux communautaires

Accès communautaire

- Alternative au Muni-Fi
- Ne nécessite pas de structure officielle
- Partage de connexions Wi-Fi entre utilisateurs
- Le réseau s'étend avec l'arrivée de nouveaux membres

Origine

- Très semblable au principe des radio amateurs
- Rendu possible par les appareils 802.11b et les connexions persistantes (début en 1998)
- 2005 : les réseaux deviennent suffisamment grands pour être utilisables

Structures

- Groupement libre (partage de la connexion par des utilisateurs séparés)
- Réseaux maillés purs
- WISP : réseaux maillés jusqu'à une structure centrale connectée à Internet

Réseaux maillés

- *Mesh networks*
- Chaque nœud se connecte aux machines proches de lui
- Le routage est dynamique
- Le réseau est robuste

Santé

Des ondes dans la tête

- Après les téléphones portables, le Wi-Fi pose certaines questions de santé
- Puissance 20 fois moindre que les téléphones portables
- Intensité chute rapidement avec la distance

Micro-ondes

- Les ondes Wi-Fi sont des micro-ondes
- Possibilité de faire entrer en résonnance les molécules d'eau
- Risques génotoxiques possibles...

OMS

“Compte tenu des très faibles niveaux d'exposition et des résultats des travaux de recherche obtenus à ce jour, il n'existe aucun élément scientifique probant confirmant d'éventuels effets nocifs des stations de base et des réseaux sans fil pour la santé.”

La voix des experts

La quasi-totalité des recherches scientifiques s'accordent à dire que les ondes Wi-Fi ne présentent aucun risque pour l'homme :

- Journal of Health Physics
- Fondation Santé et Radiofréquences
- L'Agence française de sécurité sanitaire de l'environnement et du travail (AFSSET)
- Health Protection Agency (HPA) (UK)

Mais quand même...

- De nombreux lieux publics évitent d'utiliser le Wi-Fi par précaution
- Interdit dans les écoles en Angleterre, Allemagne et Autriche, dans certaines universités américaines et canadiennes, etc.

Intrusion

Piggybacking

- Utilisation non autorisée d'une connexion internet par Wi-Fi
- Législation floue (et variable d'un pays à l'autre)
- Pratique courante aujourd'hui (et facile)

Motivation

- Economie du prix d'un abonnement Internet
- Utilisateur en déplacement sans Internet
- Parfois accidentellement suite à une mauvaise configuration
- Activité illégale

Pourquoi est-ce possible

- Utilisateurs partagent volontairement leur connexion
- Certains utilisateurs ne savent pas protéger leur réseau (ou n'ont pas envie de le savoir)
- Incompatibilité matérielle interdit la sécurisation
- Le possesseur de la connexion n'est en général pas considéré comme responsable

Légalité

- Les termes sont en général mal définis
- Parfois on considère que le DHCP et le protocole 802.11 agissent au nom du propriétaire et donc autorisent les utilisateurs
- Non respect des chartes des FAI (partage de la connexion)

Comparaisons favorables

- Lire par dessus l'épaule de quelqu'un
- Ecouter la musique que son voisin écoute
- S'asseoir sur une chaise dans un lieu public
- Lire en utilisant la lumière d'une fenêtre voisine

Comparaisons défavorables

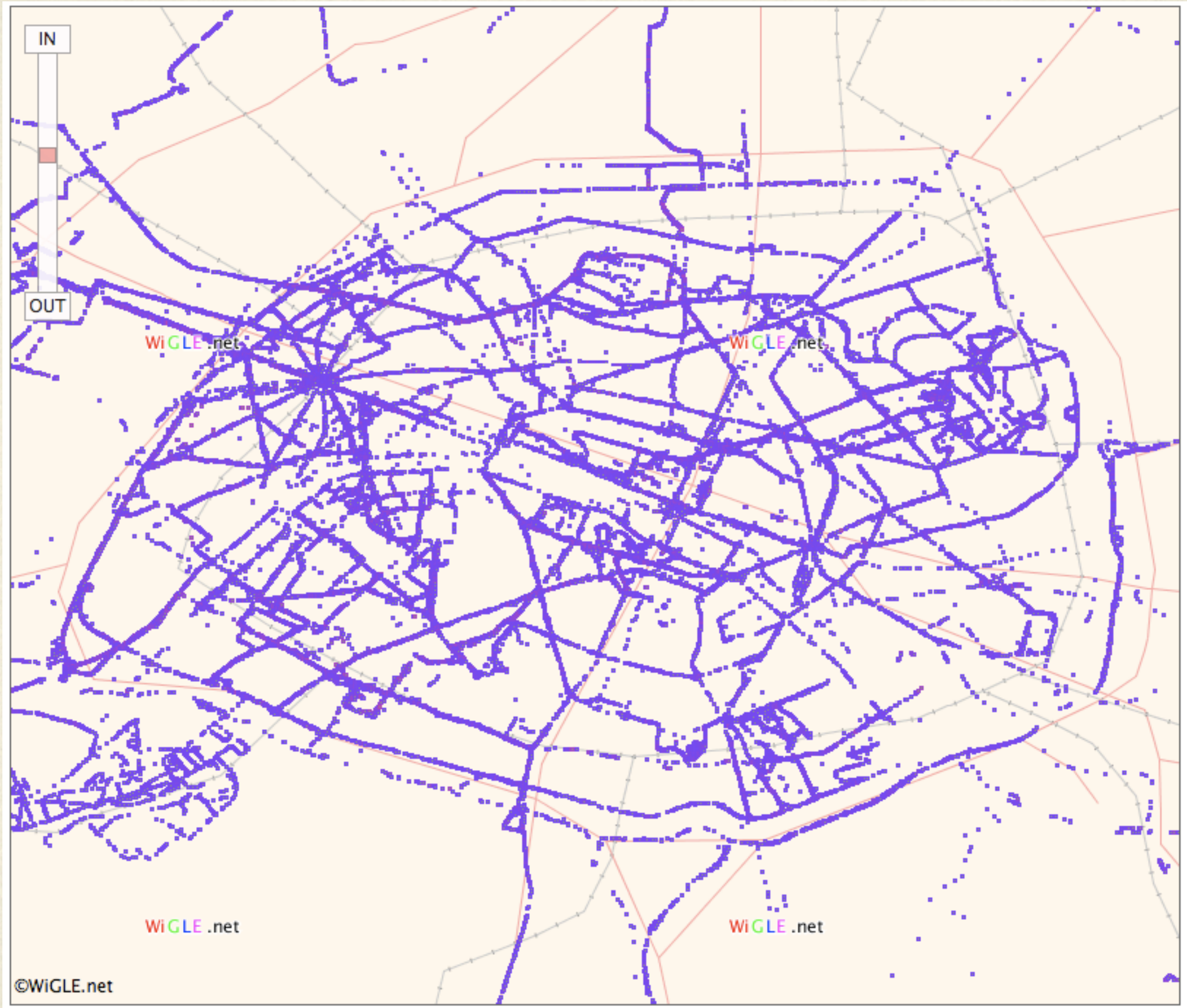
- Entrer dans une maison parce que la porte n'est pas fermée
- S'accrocher à l'arrière d'un bus
- Détourner l'installation d'un voisin pour profiter de son abonnement au câble

Wardriving

- Recherche de réseaux Wi-Fi à l'aide d'un PDA ou ordinateur portable
- De préférence dans un véhicule (sinon *warwalking* ou *warjogging*)

Cartographie

- En utilisant un GPS on peut répertorier la localisation et l'intensité du signal
- *Wireless Geographic Logging Engine* (www.wigle.net)


IN
OUT
WiGLE.net
WiGLE.net
WiGLE.net
WiGLE.net
©WiGLE.net

Source : http://wifinetnews.com/archives/vertical-markets/academia/

Salt Lake City (Utah)

Questions légales

- Différent du *piggyback*
- Le réseau n’est pas utilisé
- Version passive n’a pas de conséquence
- Version active se connecte au réseau

Protection

Le problème

- Tout le monde à portée peut lire tous les messages échangés
- Possibilité d'utiliser l'adresse IP du réseau pour des actions plus ou moins légales (spam, hack, etc.)
- Les ordinateurs autorisés peuvent étendre la portée du réseau sans le savoir

Solutions

- Limiter l'accès au réseau (crypto et vérification des adresses MAC)
- Réseau Wi-Fi isolé (il faut passer par une passerelle pour se connecter à Internet)
- Encryption de toutes les communications

WEP

- *Wired Equivalent Privacy*
- Facile à mettre en place (supporté par tous les appareils), demande peu de CPU
- Faible sécurité
- Mieux que rien
- Beaucoup de personnes ignorent qu'il existe d'autres techniques
- Encombre le réseau (plus de paquets échangés)

La courte histoire du WEP

- Protocole de sécurité inclus dans la norme 802.11 de 1999
- Plusieurs failles de sécurité sont découvertes
- Usage déconseillé en 2004

WPA

- *Wi-Fi Protected Access*
- Aujourd'hui WPA2
- Considéré sûr
- Pas toujours supporté par le vieux matériel

WPA et WPA2

- Certification de la Wi-Fi Alliance
- Norme 802.11i
- Aujourd'hui la certification WPA2 est nécessaire pour avoir le label Wi-Fi
- Fonctionne à l'aide d'une clé commune

Clés WPA

- Deux modes de fonctionnement :
  - Personel : clés échangées au préalable (manuellement)
  - Entreprise : Utilisation d'EAP pour donner une clé à chaque client authentifié

WEP vs WPA

- Le vecteur d'initialisation passe de 24 à 48 bits
- La clé passe de 40/104 à 128 bits
- *Temporal Key Integrity Protocol* (TKIP) génère une clé différente pour chaque communication et modifie la clé sur chaque paquet
- Utilisation de MIC pour vérifier l'intégrité, numérotation des paquets pour éviter les attaques par *replay*

WEP vs WPA

- La réutilisation des clés génère un risque de sécurité
- Plus d'IV → moins de réutilisation
- TKIP annule l'effet des IV faibles

DHCP et MAC

- Régler le DHCP pour n'autoriser qu'une liste d'adresses MAC
- Nécessite de modifier la liste à chaque nouvel utilisateur
- Les données ne sont pas protégées
- Possibilité de falsifier son adresse MAC

IPsec

- *Internet Protocol Security*
- Authentification et encryption de chaque paquet
- Fonctionne sur la couche Internet (donc en dessous de la couche TCP)
- Standard IETF
- Pas toujours disponible

WIPS

- *Wireless Intrusion Prevention System*
- Surveillance des émissions d'ondes dans une région
- Détection des points d'accès non-autorisés

RADIUS

- Fonctionne avec certains routeurs récents
- Effectue l'authentification de toutes les connexions
- Nécessite en général d'adapter le firmware

Pot de miel

- *Honeypot*
- On place une machine vulnérable et un point d'accès particulièrement facile
- On observe les connexions
- Permet aux administrateurs de repérer les activités non autorisées