Master SDRP
Réseau Avancé
Partie 4: Sécurité Wifi

Philippe Gros ***Session 2006***

Objectif du cours

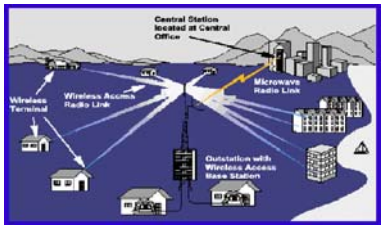
- *Connaître et savoir déployer les architectures Wifi 802.11*
- *Donner des éléments de sécurisation d'une architecture Wifi*

Sommaire

Les solutions concurrentes

- *IEEE 802.15.1 (Bluetooth), sur 2,4 Ghz*
  - *Disponible depuis début 2001 en carte PCMCIA*
  - *Intégrée en standard dans Windows XP*
  - *Ericsson 1994,*
  - *Communication orientée data flow entre PDA, Telephones, PCs, Camera*
  - *Bit rate (up to 1 Mbits/s, range 10 - 30 meters,2.4 Ghz).*
- *IEEE 802.15.3 (Bluetooth 2), sur 2,4 Ghz*
  - *Débits de 11, 22, 33, 44, & 55 Mb/s*
  - *Sécurité de groupe, authentification, gestion de clés, confidentialité...*
  - *Disponibilité prévue en 2004*
- *UWB: Ultra Wide Band ou versoin 3 de Bluetooth au sein de 802.15 groupe*
- *IEEE 1394 (FireWire ou i.Link) sur 802.11 ou Hyperlan 2*
- *Home RF:* Compaq, HP, IBM, Intel & Microsoft (11 Mbits/s).

Les solutions concurrentes: Wimax ou la boucle locale wifi



Les solutions concurrentes: Wimax ou la boucle locale wifi

- *La norme 802.16 est adoptée depuis le 29 janvier 2003:*
  - *Mono directionnel -> jusqu'à 75Mb/s*
  - *Bidirectionnel: partage de la bande passante*
  - *Possibilité d'agréger plusieurs channels pour un débit maximum de 350 Mb/s*
  - *Ligne de visée sans obstacle et utilisation d'une antenne mono directionnelle permet d'aller jusqu'à 31miles de distance.*
  - *Suivant les variantes en développement les Fréquences nécessaires vont des bandes de 2 à 66 Ghz*
- *Actuellement des bandes de fréquences sont réparties par les différentes autorités de régulations nationales*
- *Norme faisant partie de ISO/IEC 9464 series et ITU-T x.290 series of conformance testing standards.*

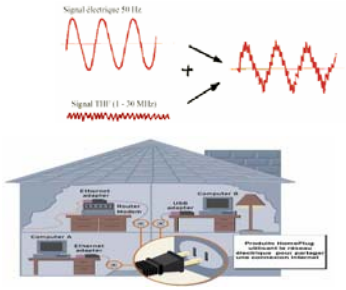
Comparaison des débits

Technology	Maximum theoretical rate	Peak rates	Measured device speed
GPRS	170 kbps	114 kbps 114/4 kbps	20-40 kbps
EDGE	470 kbps	384 kbps 384/4 kbps	100-130 kbps
1xRTT	307 kbps	153 kbps 153 kbps	40-60 kbps
EV-DO	2.4 Mbps	2.4 mbps	300-500 kbps
UMTS	2 Mbps	2 Mbps 960 kbps	220-330 kbps
UMTS/HSDPA	14 Mbps	14 Mbps	550-1100 kbps
WiMax	70 Mbps	?	few Mbps per user
WiFi	54 Mbps 100+ Mbps	30 Mbps	20-30 Mbps

Les solutions concurrentes: CPL

- *Connu sous plusieurs dénominations:*
  - ***CPL** (Courants porteurs en ligne)*
  - ***PLC** (Powerline Communications)*
  - ***PLT** (Powerline Telecommunication)*
  - ***PPC** (Power Plus Communications)*

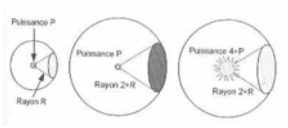
Les solutions concurrentes: CPL



Sommaire

La puissance

- La puissance de l'onde dépend de l'amplitude et de la fréquence. Elle se mesure en watts (W).
- Les émetteurs WiFi émettent en général des ondes d'une puissance de l'ordre de 100 m W.
- On parle également en décibels de milliwatts, notés dBm



$$Puissance_{dBm} = 10 \times \log(Puissance_{mW})$$

$$Puissance_{mW} = 10^{\left(\frac{Puissance_{dBm}}{10}\right)}$$

Relations puissances distances affaiblissement

- *Pour doubler la portée du signal, il faut multiplier par 4 le puissance de l'émetteur ce qui revient à une augmentation de 6 dBm*
- *Inversement un affaiblissement de 6 dbm revient à diviser le signal par 2*

Rapport Signal sur Bruit

- *Rapport Signal/bruit (RSB) = Puissance du Signal reçu(dBm)- Puissance du bruit(dBm)*
- *Le bruit naturel est de l'ordre de – 100 dBm.*
- *Auquel se rajoutent des interférences provenant de l'activité humaine (signaux industriels, électriques, radios, TV …)*

PIRE/EIRP et Gain

- *PIRE (puissance isotrope rayonnée équivalence equivalent isotropically radiated power /EIRP): Puissance du signal perçu par un observateur => souvent c'est cette mesure qui est mesurée pour rencontrer les exigences légales*
- *Gain: Le **gain d'antenne** est le pouvoir d'amplification passif d'un signal. Le gain d'une quelconque antenne dépend principalement de sa surface et de la fréquence.*
  - *Plus la fréquence est élevée, plus le gain l'est aussi à dimension identique.*

Standards du 802.11

- *802.11 est supportée par 2 couches physiques:*
  - *Infra rouge*
  - *Radios Fréquences :*
    - ➲ *FHSS: Frequency Hopping Spread Spectrum*
    - ➲ *DHSS: Direct Sequence Spread Spectrum*
- *3 sous normes:*
  - *802.11b maximum 11Mbit/s à 2.4Ghz*
  - *802.11a maximum 54Mbit/s à 5Ghz*
  - *802.11g maximum 54Mbit/s à 2.4Ghz*

Les standards 802.11

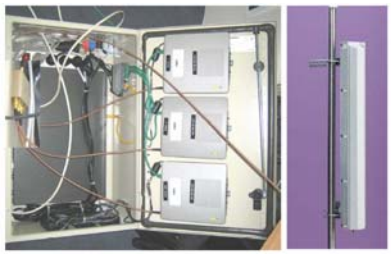
- *la couche physique:*
  - *FHSS (Frequency Hopping Spread Spectrum) (802.11 1ère génération)*
  - ***DSSS (Direct Sequence Spread Spectrum) (802.11b et g)***
  - *OFDM (Orthogonal Frequency Division Multiplexing) (802.11a et g pour atteindre 54b/s)*

DSSS

- *Normes la plus utilisée*
- *Utilisation de plusieurs bandes spectrales fixe de 22 Mhz*
- *Distance entre le début des canaux de 5 Mhz => recouvrement de canaux … on laisse 5 canaux libres entre 2 utilisés!*

Sommaire

Les antennes



Les antennes

- ***Antenne tige basique omnidirectionnelle à 2.4 GHz***
- *PIRE maximale autorisée de 100 mW, 20 dBm. (D standard indicatif = 500 m à vue)*
  - ***(Image tirée de http://fr.wikipedia.org/wiki/Wifi#Infrastructure sous GNU Free Documentation License)***

Les antennes

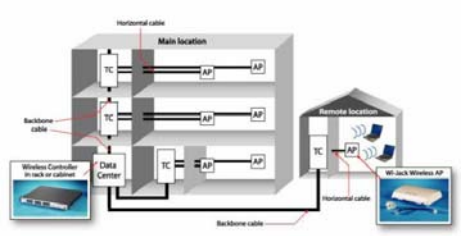
Les antennes

Type	*Forme*	*Rayonnement*	*Installation*
Verticale	*Tige*	*Omnidirectionnelle cylindrique autour de l'axe*	*Bureaux*
Dipôle	*Forme en T*	*Omnidirectionnelle double cylindrique verticale de part et d'autre de l'axe de la tige*	*Zones longues et étroites couloirs*
Sectorielle	*Panneau plat*	*Omnidirectionnelle elliptique dans le plan du panneau*	*Grande salle, hall d'entrée liaison point à multipoint*

Les antennes

Type	*Forme*	*Rayonnement*	*Installation*
Sectorielle	*Panneau plat*	*Omnidirectionnelle elliptique dans le plan du paneau*	*Grande salle, hall d'entrée liaison point à multipoint*
Yagi	*Style antenne Télé (rateau)*	*Unidirectionnelle elliptique dans l'axe des tiges*	*Liaisons inter immeubles proches*
Paraboliques	*Parabole (type antenne satellite)*	*Unidirectionnelle elliptique dans le plan perpendiculaire à la parabole*	*Liaisons inter immeubles éloignés*

Exemple de maillage Wifi sur un backbone traditionnel



Sommaire

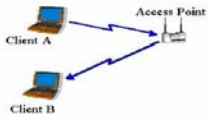
Principes du 802.11

- *Composants :*
  - *Borne ou access point (AP)= > Hub sans fil souvent un routeur*
- *Carte réseau (NIC) équivalent à un Interface Ethernet*
- *Mode 'ad-hoc' : dialogue direct entre deux interfaces (point à point)*
  - *IBSS : Independant Basic Service Set*
  - *Réseau maillé*
- *SSID (Service Set Identifier)*
- *Mode 'infrastructure' : dialogue entre une interface et une borne (multi-point)*
  - *BSS : Basic Service Set*
  - *Réseau en étoile*
  - *14 canaux*
  - *Plusieurs réseaux peuvent cohabiter au même endroit sur des canaux différents => cependant attention au recouvrement des canaux si utilisation du DSSS*

Les technologies d'interconnexion aux réseaux: 802.11 connection Had-hoc

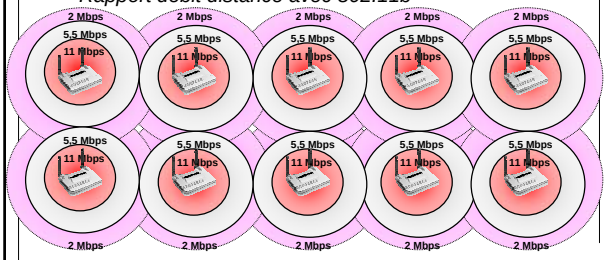
Les technologies d'interconnexion aux réseaux: 802.11 connection de type infrastructure

Dans le mode Infrastructure AP peut envoyer 10 fois par secondes une trame de contrôle contenant le SSID (Service Set Identifier). Tout interface Wlans est capable de récupérer ce SSID et se connecter sur le réseau sans autre authentification



Les technologies d'interconnexion aux réseaux: les réseaux sans fil (suite)

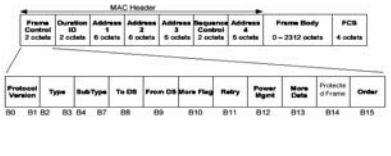
Rapport débit distance avec 802.11b



Association versus Authentification

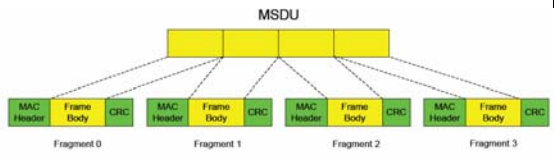
- ***Association***
  - *Enregistre la station auprès de l'AP*
  - *Obtention d'une AID (*Association Identity*) partagée entre chaque AP de l'ESS,*
  - *permettant la ré-association transparente au sein de l'ESS ou BSS*
  - *Toujours initiée par la station => Équivalent de la connexion physique pour le 10BaseT*
- ***Authentification***
  - *Action de prouver son identité afin de faire partie du BSS ou ESS*
- *Deux méthodes d'authentification :*
  - *Ouverte (*Open Authentication*) : authentification nulle*
  - *A clef partagée (*Shared Key Authentication*) : utilise la clé WEP pour chiffrer un défi en clair envoyée par la borne*
- *La dé-authentification peut être initiée par la station ou l'AP*

La trame 802.11



- ***Frame Control*** *: L'ancien champ WEP a été renommé Protected Frame pour indiquer qu'un chiffrement est utilisé*
- ***Address 1-4*** *: Adresse de la source (SA) = MAC Source, Adresse destination (DA) =MAC destination, Adresse de la station émettrice (TA), Adresse de la station réceptrice (RA)*
- ***Sequence Control*** *: comprend le numéro de séquence et le numéro de fragment*
- ***FCS*** *: CRC de 32 bits sur l'ensemble de la trame*

Principe de la fragmentation



Sommaire

Les interférences

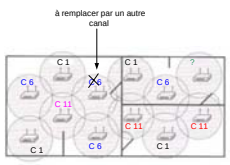
- *Interférences dites multipath (cf schéma du dessus)*
- *Les autres réseaux Wifi 802.11 partageant les mêmes canaux*
- *Les autres réseaux Wifi autres que 802.11(surtout le bluetooth)*
- *…. Et les fours à micro ondes à 2.4Ghz*

Déployer de multiples AP

- *Cela se révèle nécessaire pour avoir:*
  - *Une bonne couverture radio et éviter des zones non couvertes*
  - *Un bon débit en limitant de partager la bande passante entre plusieurs stations Wifi*

Déployer de multiples AP

- *Attention aux interférences => il faut déployer les AP avec des canaux contigus différents*
- *Bien que 802.11b et g disposent de 14 canaux mais les canaux voisins se superposent => on choisit en général les canaux 1, 6 et 11*



Sommaire

Amélioration du Wifi

- *Gestion de la Qualité de service par la mise en œuvre de 802.11e:*
  - *Plusieurs stratégies existent mais la certification WMM (Wifi Multimédia) de Wifi Alliance s'appuie sur le mode EDCF (Enhanced Distributed Coordination Function)*
- *Un mode économie d 'énergie existe qui peut être appréciable pour augmenter l'autonomie des stations, cependant elle diminue la qualité de la communication*

Sommaire

Méthodes de sécurisation

1 Masque le SSID: Comme toute requête d'authentification 802.11 nécessite de contenir le bon SSID, il suffit de ne pas le diffuser

=>Attention en sniffant le réseau un intrus découvrira le SSID.

2 Filtrer les adresses MAC autorisées à accéder au réseau => Attaque possible par MAC spoofing

La non diffusion du SSID

- **Le pour** :
  Protège contre des associations « malencontreuses »
  Ex: Windows XP, outils standards de configuration...
- Mieux que la diffusion d'un SSID par défaut
  Ex: Linksys (Linksys), Tsunami (Cisco), WLAN (SMC), 101 (3COM)...
  Arrête temporairement l'intrus « amateur » !
- **Le contre** :
  Faux sentiment de sécurité
  Problèmes de compatibilité avec certains matériels
  Ne change rien pour des pirates équipés d'un sniffer !

Méthodes de sécurisation

3 Utilisation du protocole de chiffrement WEP => actuellement facilement cassable

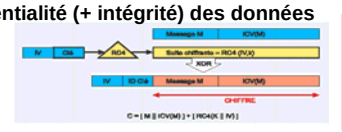
4 Authentification 802.1x et rotation de clé WEP (toutes les 10 minutes – difficile à mettre en œuvre)

5 Authentification 802.1x et WAP/TKIP => clé de chiffrement temporaire

6 Authentification 802.1x et WAP2/TKIP => clé de chiffrement temporaire ou WAP2/AES

Wep (Wired Equivalent Privacy) Algorythme RC4

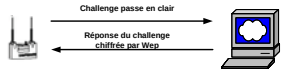
Confidentialité (+ intégrité) des données



- *Clé WEP: IV (Vecteur d'initialisation)24 bits+ clé partagée sur 40 bits = 64 bits*
- *Clé WEP 2: IV 24 bits+ clé partagée sur 104 bits = 128 bits*
- *Également utilisée pour l'authentification des stations*

Wep (Wired Equivalent Privacy) Algorithme RC4

- *Également utilisée pour l'authentification des stations*



Sommaire

Principaux types d'attaques

- *Exploitation des faiblesses du protocole 802.11*
  - *802.11 a b ou g sont des protocoles avec peu de protection.*
  - *Une majorité de réseaux accepte une interconnexion en mode broadcast*

Principaux types d'attaques: le cas du wireless: accès ouverts

Access Point

SSID: “goodguy”
Broadcast autorisé

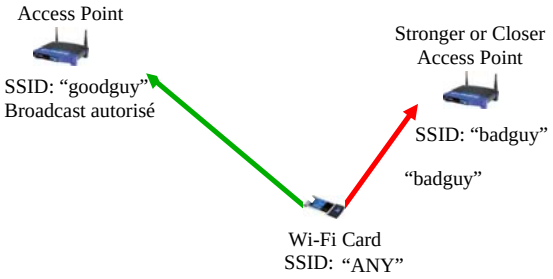
Wi-Fi Card
SSID: “any” et goodguy
après récupération
du SSID de l’AP

- *Liste des points d’accès ouverts: www.hotspotlist.com*

Principaux types d'attaques: le cas du wireless: accès ouverts

- *Rogue AP = un point d’accès non autorisé*
- *Risques Traditionnels*
  - *back-doors*
  - *espionnage*
- *Risques liés aux points d’accès ouverts ou Hotspots*
  - *DoS*
  - *Vol de droits et habilitations (credentials)*

Principaux types d'attaques: le cas du wireless: Cas du Rogue Airpoint



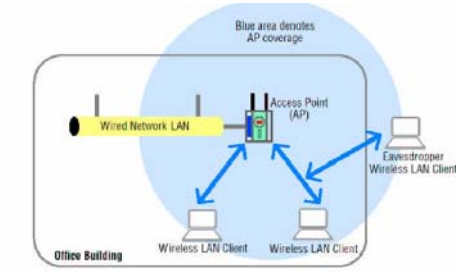
Wep: l'état des lieux en matière de sécurité

Date	Description
Septembre 1995	Vulnérabilité potentielle dans RC4 (Wagner)
Octobre 2000	Première publication sur les faiblesses du WEP : *Unsafe at any key size; An analysis of the WEP encapsulation* (Walker)
Mai 2001	*An inductive chosen plaintext attack against WEP/ WEP2* (Arbaugh)
Juillet 2001	Attaque *bit flipping* sur le CRC – *Intercepting Mobile Communications : The Insecurity of 802.11* (Borisov, Goldberg, Wagner)
Août 2001	Attaques FMS – *Weaknesses in the Key Scheduling Algorithm of RC4* (Fluhrer, Mantin, Shamir)
Août 2001	Sortie de AirSnort
Février 2002	Optimisation de l'attaque FMS par h1kari
Août 2004	Attaque de KoreK (IVs uniques) – sortie de chopchop et chopper
Juillet/Août 2004	Sortie d'Aircrack (Devine) et WepLab (Sanchez) implémentant l'attaque de KoreK.

Faiblesses du WEP

- *Wireled Equivalent Privacy (WEP) est un protocole offrant une authentification des utilisateurs et un chiffrement des données*
- *L'algorithme de chiffrement est RC4.*
- *Airsnort permet de casser la clé de chiffrement après avoir récupérer entre 500 Mo à 1 Go de données.*
- *Airsnort agit comme un sniffer: il est indétectable!*

Principaux types d'attaques: le cas du wireless: Wire Wilde Drive



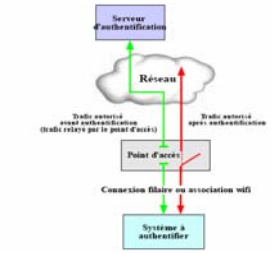
Localisation par GPS

- Possibilité de coupler les outils de détection à un GPS.
- Lors de “wardrive”, génération d'un fichier de coordonnées GPS.
- Récepteur GPS sur port Serie, USB...
- A partir de 250 dollars...
- Logiciels de cartographie populaires :
- Windows :
  - Mappoint : http://www.microsoft.com/mappoint/default.mspx
- Note : convertion netstumbler avec StumbVerter ou sur Internet
- Linux / *BSD :
  - GpsDrive : http://gpsdrive.kraftvoll.at

Détection de Wifi Netsumbler

Sommaire

802.1x



Authentification 802.1x/EAP

- *EAP:* Extensive Authentication Protocol *(RFC 2284)*
- *802.1x: normalisé par l'ISO*

Composant 802.1x: Raduis

- *Demandeur -> Supplicant*
  - *Entité Wifi voulant accéder aux ressources => doit s'authentifier*
- *Serveur d'accès; Network access server (NAS) ou Authenticator*
  - *Commutateur, Borne sans fil*
- *Serveur d'authentification: Authentication server (AS)*
  - *vérifie les accréditations présentées par le demandeur => dialogue avec le serveur d'accès.*

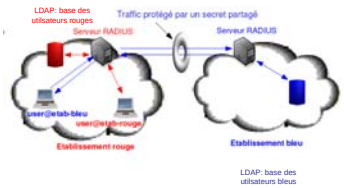
Raduis

- *Protocole d'authentification avec trois fonctions : AAA*
- *Authentification : qui demande une connexion ?*
- *Autorisation : cette personne est elle autorisée ?*
- *Accounting : temps de connexion , volume*

Raduis

- *Pour remplir ses fonctions, le protocole RADIUS dispose de 9 types de paquet :*
  - *4 pour l'authentification*
  - *2 pour l'accounting*
  - *1 code pour le status client*
  - *1 code pour le status serveur*
  - *1 code réservé*

Proxy Raduis



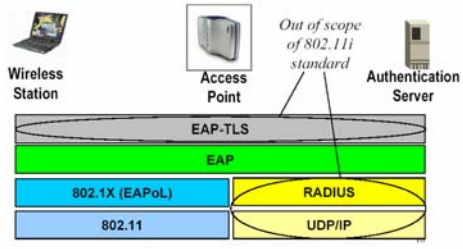
- *Délégation de l'authentification à un autre serveur*
- *RADIUS, fonction aussi appelée proxyRADIUS*
- *A qui doit on adresser la demande ?*
- *Introduction de la notion de domaine (realm) lors de la demande d'authentification*
- *Suivant la valeur du domaine le premier serveur RADIUS rencontré sait si il doit traiter l'authentification ou relayer la demande à un autre serveur*

Fillaire vs Wifi

- *Réseau filaire commuté => Chaque station est reliée à un port du commutateur et s'authentifie en 802.1x sur ce port*
- *Sur un réseau sans fil => Pas de port physiques car les accés aux AP sont partagés =>port logique*
  - *L'AP donne à chaque client qui s'est authentifié une clé de session*
  - *Toute trame n'utilisant pas de clé de session est ignorée par l'AP*

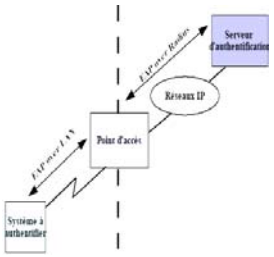
Sommaire

802.1x associé à un EAP

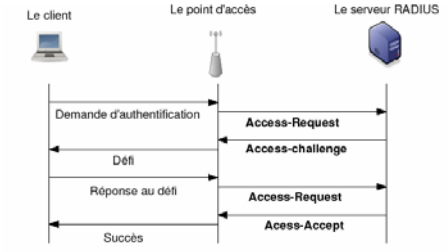


802.1x associé à un EAP

- *Le protocole 802.1X définit l'utilisation d'EAP (Extensible Authentification Protocol, RFC 2284), mécanisme décrivant la méthode utilisée pour réaliser l'authentification.*
- *On distingue deux types de trafic EAP :*
  - *entre le système à authentifier et le point d'accès (support : 802.11a, b, g ou 802.3) : EAP over LAN (EAPOL)*
  - *entre le point d'accès et le serveur d'authentification (de type RADIUS) : EAP over Radius*



Raduis et wifi



802.1x associé à un EAP

- *Le protocole 802.1X propose plusieurs méthodes d'authentification:*
  - *login / mot de passe ;*
  - *certificat électronique ;*
  - *biométrie ;*
  - *puce .*
- *Il est possible de combiner plusieurs méthodes*
- *En plus de l'authentification, EAP gère la distribution dynamique des clés de chiffrement (WEP/WAP/WAP2).*
- *Les AP ne servent qu'à relayer les messages EAP entre le client et le serveur d'authentification*
- *L'AP n'est pas obligée de connaître la méthode d'authentification utilisée entre le client et le serveur*
  => Pratique pour l'évolutivité

Sommaire

Extensible Authentication Protocol : Différents méthodes

- ***EAP-TLS (Transport Layer Security)*** *:*
  - *authentification mutuelle entre le client et le serveur Radius par le biais de certificats (côté client et côté serveur) => nécessite une PKI/ICP (infrastructure à clé publique)*
- ***EAP-TTLS (Tunneled TLS) et EAP-PEAP (Protected EAP)***
  - *authentification mutuelle du client et du serveur Radius par le biais d'un certificat côté serveur, le client peut utiliser un couple login/mot de passe ;*
- ***EAP-MD5*** *: pas d'authentification mutuelle entre client et le serveur Radius, le client s'authentifie par mot de passe (à déconseiller)*
- ***EAP-LEAP*** **(Lightweight EAP)**
  - *cas particulier, méthode propriétaire de Cisco.*
- EAP TTLS est recommandé

Comparaison des authentifications EAP

Méthodes	Authentification	Tunnel	IGC nécessaire	Client natif	Client Disponible
MD5	Non	Non	Non	Win, MacOS	Linux
LEAP	Non	Non	Non	MacOS	Win, Linux
PEAP	Serveur	Oui	Non	Win, MacOS	Linux
TTLS	Serveur	Oui	Non	MacOS	Win, Linux
TLS	Client & serveur	Oui	Oui	Win, MacOS	Linux
FAST	Serveur	Oui	Non	Non	Win, Linux

•IGC: Infrastructure de gestion de clés (PKI Public Key Infrastructure)

Sommaire

Les nouvelles formes d'authentification: historique

- *Un constat WEP : ne peut plus garantir la sécurité 802.11*
- *Janvier 2001 : Début des travaux du groupe de travail 802.11ianciennement 802.11e) au sein de l'IEEE pour développer des spécifications de sécurité pour l'authentification et le chiffrement des données.*
- *Avril 2003 : Recommandation WPA de la Wi-Fi Alliance fondée sur un sous ensemble de la norme 802.11i*
  - *depuis la mi-2003 tous les produits certifiés au label WiFi doivent supporter cette recommandation.*
- *23 Juin 2004 : Publication de la norme 802.11i => WAP 2 devient une certification*
- *Référence : http://grouper.ieee.org/groups/802/11/*

WPA

- *Permet de combler une partie des problèmes du WEP*
- *Utilisation du mécanisme TKIP (Temporal Key Integrity Protocol)*
- *Caractéristiques:*
  - *Changement des clefs de chiffrement de façon périodique*
  - *10ko de données échangées (long en cas de roaming*
  - *Clef à 128 bits*
  - *Vecteur d'initialisation de 48bits (281 474 976 710 656 possibilités)*
  - *Impossibilité de réutiliser un même IV avec la même clef*
  - *Utilisation du MIC qui est un contrôle d'intégrité de tout le message*
- *2 modes de fonctionnement*
  - *Mode PSK (PreShared Key) : secret partagé*
  - *Mode à base de 802.1X pour une authentification centralisée avec TKIP Temporal Key Integrity Protocol)*

WPA

- *Le WPA n'intègre pas les sécurisation que le 802.11i/WPA2 apporte :*
  - *La sécurisation des réseaux multi-point Ad-Hoc*
  - *N'implémente pas AES comme algorithme de chiffrement*
  - *Nécessite des équipements capables de l'implémenter*
  - *Les anciens équipements ont la plupart du temps la possibilité de mettre à jour leur software*
- *Infrastructure à base de Radius (sauf en mode PSK)*
- *C'est du 802.1X*
- *Références :*
- *Documents:*
  - *http://www.wifi.org/opensection/protected_access.asp*
  - *http://www.wifialliance.com/OpenSection/pdf/Whitepaper_Wi-Fi_Security4-29-03.pdf*

WPA 2 ou Full 802.11i

Définition d'un RSN (Robust Security Network) permettant de garantir:

- *Sécurité et mobilité*
- *Authentification du client indépendamment du lieu où il se trouve*
- *Intégrité et Confidentialité*
- *Garantie d'une confidentialité forte avec un mécanisme de distribution dynamique des clefs*
- *Passage à l'échelle et flexibilité*
- *Ré-authentification rapide et sécurisée en cas de « handover », séparation du point d'accès et du processus d'authentification pour le passage à l'échelle, architecture de sécurité*
- *Flexible*
- *Dans le cas où un réseau accepte à la fois du WAP2 et du WEP (par exemple pour une migration vers WAP2) on le nomme TSN: Transitional Security Network*

WAP2: authentification

- ***Associations construites autour d'authentifications fortes : RSNA (RobustSecurity Network Association) – dépendantes de 802.1x:***
  - *PMKSA : Pairwise Master Key Authentication Security Association (unique à la paire AP/Station)*
  - *PTKSA : Pairwise Transient Key Security Association: clé temporaire utilisée pour chiffrer les données*
  - *GTKSA : Group Transient Key Security Association => utiliser pour chiffrer les broadcasts et les mulitcasts*
  - *STAKeySA : Station Key Security Association échange de clés entre stations*
- ***Sécurité au niveau MAC :***
  - *TKIP (Temporal Key Integrity Protocol) - Optionnel*
  - *CCMP (Counter-mode/CBC-MAC-Protocol) - Obligatoire*
  - *Le TSN (Transition Security Network) permet une compatibilité avec les anciensmécanismes (Open Authentication, Shared Key Authentication, WEP)*

Sommaire

WPA Personal vs WPA Enterprise

- *WPA ou WPA2 peuvent se déployer selon 2 architectures:*
  - *Clés partagées => WPA Personal*
  - *802.1x=> WPA Enterprise*

WPA/WPA2 Personal

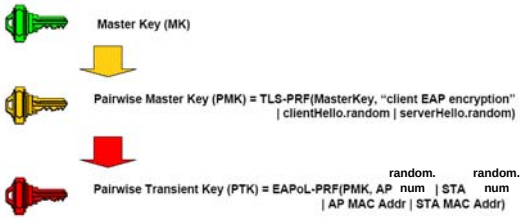
- *Solution Pre Shared Keys => facile à mettre en œuvre dans le cas d'un petit réseau…*
  - *Wep: saisir la clé elle-même en hexadécimal*
  - *WAP/WAP2 il faut rentrer une passphrase de laquelle sera dérivée la clé*
- *Défauts de cette solution:*
  - *Mot de passe faible => attaque possible de type dictionnaire ou force brute*
  - *Tous les utilisateurs partagent la même clé*

WPA/WPA2 Enterprise

- *Installer et configurer un serveur Raduis*
- *Activer la gestion 802.1x du WPA/WPA2 dans tous les AP*
  - *Si WPA2 choisir entre TKIP et AES (de préférence)*
- *Installer et configurer un client 802.1x sur les stations avec le même algorithme de gestion de chiffrement que les AP (TKIP/AES)*
- *Choisir la méthode d'authentification EAP/RADUIS et la configurer dans les clients et le serveur Raduis.*

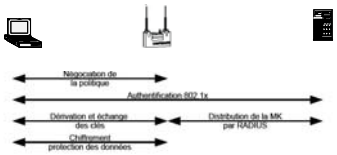
Sommaire

WAP2 Hiérarchie des clés



WPA2 : les bases

- *Phases opérationnelles*
- *Négociation de la politique de sécurité*
- *Authentification 802.1x*
- *Échange des clefs sous EAP*
- *Chiffrement des données*



TKIP

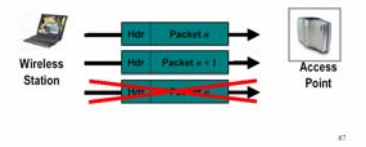
- Utilise RC 4 comme WEP
- Les apports de TKIP par rapport au WEP :
  - Utilisation d'un algorithme de hachage cryptographique non linéaire : MIC (*Message Integrity Code*) basé sur Michael (Niels Ferguson)
  - Impossibilité de réutiliser un même IV avec la même clef (l'IV joue maintenant un rôle de compteur appelé TSC (*TKIP Sequence Counter*)) et augmentation de la taille de l'IV à 48 bits
  - Utilisation de clés de 128 bits (et non 40 ou 104 bits pour le WEP)
  - Intègre des mécanismes de changement de clés
  - Utilise une clé différente pour le chiffrement de chaque paquet : PPK (*Per Packet Key*)

TKIP

- TKIP Keys
  - Temporal encryption key = PTK bits 256-383,GTK 0-127 bits
- Temporal data origin authenticity keys = PTK bits 384-511, GTK bits 128-255

TKIP

- ***Protect against replay:***
  - Séquence des paquets à 0 lors d'une nouvelle clé
  - Séquence du paquet +1 à chaque nouveau paquet
  - Supprime les paquets arrivés hors séquence

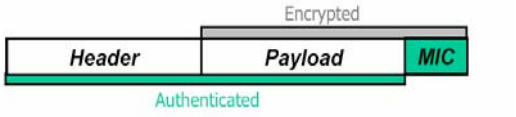


MIC AKA "*Michael*"

- ***Chiffrement de type RC4 moins dangereux car la clé change régulièrement***
- ***Contrôle d'intégrité basé sur HMAC-SHA1 (clé de 64 bits) crée spécialement pour les besoins de TKIP.***
- ***Authentifie l'émetteur et le destinataire (SA & DA)***
- ***Niveau de sécurité : 20 bits***
- ***Obligation d'implémenter des contre mesures en cas d'attaque visant à forger des MIC***
  - ***Solution choisie : invalider la clef de l'attaquant (induisant une nouvelle négociation 802.1X) + « blackout » 60s***
- ***MIC invalide => Renouvellement des clés (EAPoL message (clients) 4 way/Group Key handshake (AP)***
- ***Pour TKIP (WPA), le MIC est calculé sur le MSDU***
- ***Pour CCMP(WAP2), le MIC est calculé sur chaque MPDU***

CCMP

- *Protocole de sécurité basé sur le chiffrement AES (Advanced Encryption*
- *Standard) en mode CCM (clef et blocs de 128 bits)*
- *N'est pas un compromis de sécurité comme TKIP car c'est un nouveau protocole créé spécialement pour l'utilisation dans 802.11i RSN*
- *CCM combine CTR pour la confidentialité et CBC-MAC pour l'authenticité et l'intégrité*
- *Mode par défaut en 802.11i*
- *Ajoute 16 octets au MPDU (8 octets pour l'en-tête CCMP et 8 octets pour*
- *le MIC)*
- *Protection anti-rejeu grâce au PN (le PN est unique pour chaque PTKSA, GTKSA ou STAKeySA)*



CCMP

- AES exige beaucoup de calculs => souvent impossible de mettre à jour le firmware d'une base
- CCM est orienté octets et permet de ne chiffrer qu'une partie du payload

Comparaison des algorithmes de chiffrement

	WEP	TKIP	CCMP
Chiffrement	RC4	RC4	AES
Taille de la clé	40 ou 104 bits	64 bits authentification 128 bits chiffrements	128 bits
Taille IV	24 bits	48 bits	48 bits
changement des clés	non	oui par paquet	inutile
Intégrité des données	CRC32	MIC	CCM
Intégrité de l'en tête	Non	MIC (SA et DA)	CCM
Détection des repaly	non	oui	oui
Gestion des clés	non	802.1x	802.1x

Sommaire

Roaming

Deux mécanismes ont été introduits pour améliorer l'itinérance :

- **Pre Authentication :**
  - Permet à un client de s'identifier avec un autre AP sur lequel il risque de basculer (au sein du même BSS)
  - Comment ? : redirection des trames d'authentification générés par le client vers son futur AP par l'intermédiaire du réseau filaire
  - Avantage : Roaming plus rapide
  - Inconvénient : Accroissement significatif de la charge sur le serveur d'authentification
- **Key Caching** :
  - Permet de conserver la PMK afin de la réutiliser lors d'une future transaction avec cet AP
  - Utilisation du PMKID (*Pairwise Master Key Identifier*) pour identifier la bonne clef
  - Extension de certains constructeur « Proactive Key Caching » : partage des PMK entre AP

Sommaire

Exemple de solution de sécurisation

- Support physique : etoken

  - clé USB avec un microprocesseur
  - facile à manier
  - tous les calculs sont faits sur le etoken sans passer par l'ordinateur
  - le etoken stocke les données personnelles: clés privées, passwd, certificats etc..
  - s'actionne à partir de l'ordinateur via un mot de passe
- Architecture de l'authentification
  - système d'authentification basé sur un serveur free radius et
  - sur le protocole EAP-TLS.
  - mise en place d'une petite PKI (basée sur le serveur Free-Radius) pour gérer les clés publiques des utilisateurs.
  - permet une authentification mutuelle

Exemple de solution de sécurisation

- Le système permet une authentification mutuelle sans divulgation d'information.
- Très facile d'utilisation.
- Pour se faire authentifier il faut à la fois avoir le support physique ET le mot de passe qui permet d'activer le etoken.

=> sécurité renforcée par rapport à un simple mot de passe tout en gardant une facilité d'utilisation

Protection des échanges

- *Rajout d'un pare feu personnel pour éviter les intrusions*
- *Mise en œuvre d'un VPN pour empêcher le sniffing, par exemple IPsec*

Sommaire

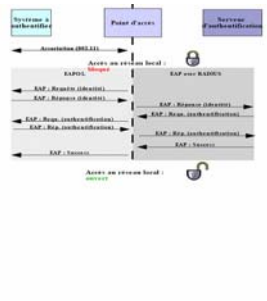
Conclusion

- *Le WEP est définitivement à éviter, la durée de vie d'une clé de 128 bits est **inférieur à 1h** avec les nouveaux outils*
- *Les bornes ne supportant pas WPA doivent implémenter une rotation des clés au maximum toutes les heures*
  - *protège de l'utilisation frauduleuse des ressources informatiques*
  - *ne protège pas de la perte de confidentialité des données*
- *WPA s'impose comme solution pour les bornes ne pouvant pas supporter le WPA2 .*
- *WPA2 est la solution la plus pérenne*
  - *Le mode PSK ne garantit pas la confidentialité entre utilisateurs d'un même BSS (Utiliser le mode Entreprise – Serveur d'authentification)*
- *Le chiffrement ne doit pas empêcher l'isolement des réseaux et la mise en place de filtrage*

Sommaire

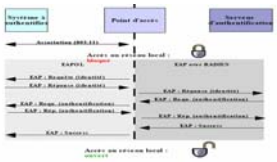
802.1x associé à un EAP

- ***Les messages EAP se décomposent en 4 classes :***
  - ***requêtes (du serveur vers le client)***
  - ***réponses (du client vers le serveur)***
  - ***succès***
  - ***échec***
- ***La première étape est l'association physique avec le point d'accès réalisé via 802.11***
- ***La deuxième étape est la phase d'authentification 802.1X:***
  - ***Le processus d'authentification est initié par l'envoi d'une requête provenant du point d'accès vers le client(EAPOL).***
  - ***Le client répond à la requête en y joignant un premier identifiant (nom de la machine, login, etc).***
  - ***Cette réponse est retransmise au serveur Radius (EAP over Radius).***



802.1x associé à un EAP suite

- ***Ensuite les échanges dépendent de la méthode d'authentification choisie (EAP-TLS, LEAP, etc.).***
- ***Au terme de ces échanges le client est:***
  - ***soit authentifié, auquel cas le point d'accès autorise le trafic du client sur le réseau,***
  - ***soit non-authentifié, et l'accès au réseau reste alors interdit.***



EAP/TLS

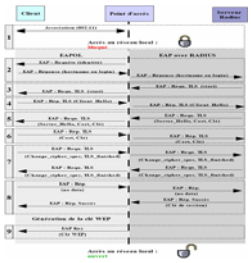
1) Le client s'associe physiquement au point d'accès.

2) Le point d'accès envoie une requête d'authentification au client. Le client répond avec son identifiant (nom de machine/ login), ce message est relayé vers le serveur Radius.

3) Le serveur Radius initie le processus d'authentification TLS par le message TLS start.

4) Le client répond avec un message client_hello, qui contient :

- ***des spécifications de chiffrement vides en attendant qu'elles soient négociées entre le client et le serveur ;***
- ***la version TLS du client ;***
- ***un nombre aléatoire (défi ou challenge) ;***
- ***un identifiant de session ;***
- ***les types d'algorithmes de chiffrement supportés par le client.***



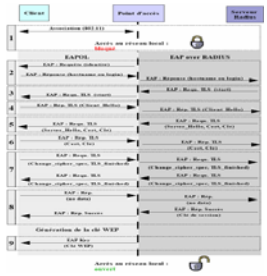
EAP/TLS suite

5) Le serveur renvoie une requête contenant un message server_hello suivi:
- *de son certificat (x509) et de sa clé publique ;*
- *de la demande du certificat du client ;*
- *d'un nombre aléatoire (défi ou challenge) ;*
- *d'un identifiant de session (en fonction de celui proposé par le client).*

Le serveur choisit un algorithme de chiffrement parmi ceux qui lui ont été proposés par le client.

6) Le client vérifie le certificat du serveur et répond avec son propre certificat et sa clé publique.

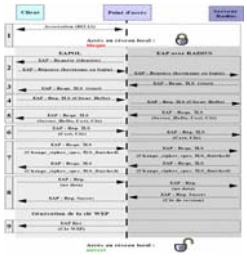
7) Le serveur et le client, définissent une clé de chiffrement principale utilisée pour la session. Cette clé est dérivée des valeurs aléatoires que se sont échangées le client et le serveur. Les messages change_cipher_spec indiquent la prise en compte du changement de clé. Le message TLS_finished termine la phase d'authentification TLS (TLShandshake), dans le cas d'EAP-TLS la clé de session ne sert pas à chiffrer les échanges suivants



EAP/TLS suite

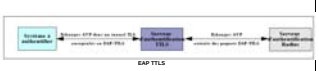
8) Si le client a pu vérifier l'identité du serveur (avec le certificat et la clé publique), il renvoie une réponse EAP sans donnée. Le serveur retourne une réponse EAP success.

9) La clé de session générée en (8) est réutilisée par le point d'accès pour créer une clé WEP/WPA/WPA2 qui est transmise au client. La clé de session est valide jusqu'à ce que le client se déconnecte ou que son authentification expire, il doit alors s'identifier à nouveau.Le tunnel TLS créé lors de la création de la clé de session n'est pas exploité. Seul le TLS Handshake est utilisé, il permet l'authentification mutuelle des deux.



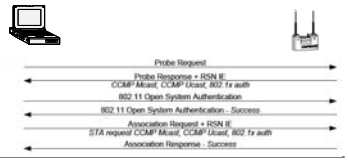
EAP TTLS ou PEAP

- *EAP TLS exige l'utilisation d'une infracstructure de gestion de clés (IGC/PKI)*
- *Dans le cas d'une utilsation de login/password ou d'une carte Token EAP-TTLS (Tunneled TLS) et EAP-PEAP (Protected EAP) peuvent être utilisés en 2 phases:*
  - *Première phase : identification du serveur par le client en utilisant un certificat (validé par une autorité de certification).*
  - *Deuxième phase : identification du client par le serveur par login/password (unique ou variant via une Token Card*
- *La méthode EAP-PEAP ne peut-être utilisée qu'avec un serveur Radius supportant EAP.*
- *EAP-TTLS est plus souple, il est toujours nécessaire de dialoguer avec un serveur Raduis via des échanges AVP (Attribut Values Pairs),cependant ce serveur peut retransmettre directement la requête auprès d'un serveur Radius ne gérant pas EAP .*



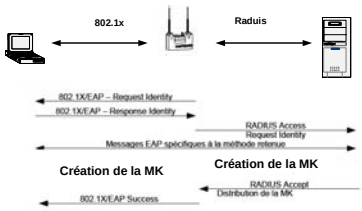
802.1i Phase1 Négociation de la politique de sécurité

- *L'AP diffuse dans les Beacons les RSN IE (Information Elements)*
- *Liste des authentification supportées (802.1x)*
- *Liste des protocoles de sécurité (CCMP, TKIP, ...)*
- *Liste des méthodes de chiffrement pour la diffusion des clefs de groupes (GTK)*
- *Le choix du client est alors précisé dans un élément d'information de sa trame Association Request*



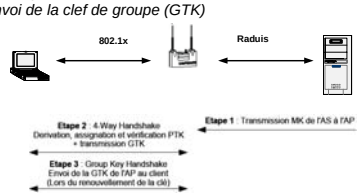
802.1i Phase2 Authentification 802.1x

- *Définition commune de la MK (Master Key) basé sur la méthode EAP choisie (EAP/TLS, EAP/TTLS, EAP/SIM, etc.)*



802.1i Phase3 Echange des clés

- *Phase 3 : Échange des clefs sous EAP en 3 étapes*
  - *Transmission de la MK du serveur d'authentification (AS) à l'AP*
  - *Message radius avec l'attribut MS-PPE-RECV-KEY*
- *Dérivation de la PMK à partir de la MK*
- *Calcul de la PTK (Pairwise Transient Key) grâce au 4-Way Handshake (cf annexe)*
- *Envoi de la clef de groupe (GTK)*



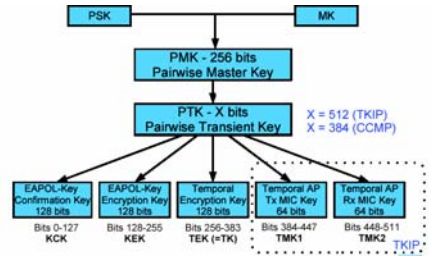
802.1i Phase4 chiffrement

- *Wep ne pouvant assurer des fonctions robustes de chiffrement, trois mécanismes ont été ajoutés à 802.11i :*
- *TKIP Temporal Key Integrity Protocol:*
  - *Basé sur un moteur WEP (RC4) et améliorant la méthode de gestion des clefs et le contrôle d'intégrité grâce à MIC (Message Integrity Control).*
- *CCMP (Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol):*
  - *Basé sur le chiffrement AES en mode CCM et signature MIC basée sur CBC-MAC*
  - *Obligatoire dans la norme 802.11i*
- *WRAP (Wireless Robust Authenticated Protocol) initialement choisi pour 802.11i*
  - *Basé sur le chiffrement AES en mode OCB (Offset Code Book)*
  - *http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/ocb/ocb-spec.pdf*
  - *Problème de licence sur cet algorithme : de nombreux groupes réclames les droits!*

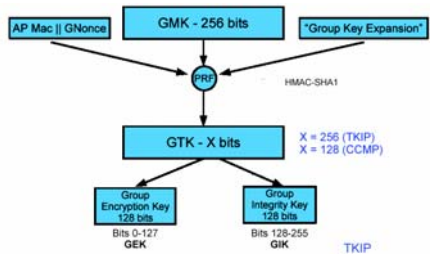
les clés

- *Master Key Clé Maître de laquelle dérivent toutes les autres*
- *Pairwise Master Key créés lors de l'accession au médium 802.11*
- *Pairwise Transient Key se dérivent en:*
  - *Key Confirmation Key (KCK) utilisées pour associer les PMK à un couple AP/station => utilisée aussi pour prouver la possession d'une PMK*
  - *Key Encryption Key (KEK) utilisée pour distribuer la Group Transient Key (GTK)*
  - *Temporal Key (TK) utilisée pour chiffrer les données du traffic*

les clés en détails



les clés en détails



les clés en détails

- *La GMK est une clef définie par l'access point*
- *La GTK est dérivée de la GMK et sert à chiffrer et authentifier les trames à destination de plusieurs stations (broadcast ou multicast), elle doit être renouvellée quand un client quitte le réseau (roaming).*
- *La fonction PRF-X est une fonction pseudo aléatoire basée sur HMAC (RFC 2104) utilisant SHA1comme méthode de hachage dont la sortie à un nombre d'octets définis :*
  - *256 bits en mode TKIP (PRF-256)*
  - *128 bits en mode CCMP (PRF-128)*
- *De la GMK on dérive :*
  - *GEK : Clef assurant le chiffrement du trafic (Group Encryption Key – 128 bits) – dans le cas de CCMP cette clef assure aussi l'intégrité*
  - *GIK : Clef assurant l'intégrité du trafic lors de l'utilisation de TKIP (Group Integrity Key –128 bits)*

EAPoL Key Message

Descriptor Type – 1 octet	
Key Information – 2 octets	Key Length – 2 octets
Replay Counter – 8 octets	
Nonce – 32 octets	
IV – 16 octets	
RSC – 8 octets	
Key ID – 8 octets	
MIC – 16 octets	
Data Length – 2 octets	Data – n octets

Champ de EAPoL Key Message

- Descriptor – value = 254 => 802.11i Key Message
- Key Information – voir plus loin
- Replay counter – utilisé pour les séquences de mise à jour GTK updates, détecte les requêtes de stations relayées (roaming)
- Nonce – détermine la fraîcheur de la clé
- IV – vecteur d'initialisation du message
- RSC – Utilisé dans le cadre des broadcast/multicast

Champ de EAPoL Key Message

- Key ID – utilisée dans le cadre d'une politique de gestion des clés (otpionnel)
- MIC – Message Integrity Code, calcul d'intégrité
- Data length – nombre d'octets des données
- Data – si utilisée
  - ➲Station RSN IE4-Way Handshake Message 2
  - ➲Access Point RSN IE 4-Way Handshake Message 3
  - ➲GTK: Group Key IE Handshake Message 1

Information Key

3 bits Version	1 bit Key Type	2 bits Key Index	1 bit Install	1 bit Ack	1 bit MIC	1 bit Secure	1 bit Error	1 bit Request	4 bits Reserved

- Version:
  - 1: HMAC-MD5 MIC, RC4 Key Wra
  - p 2: HMAC-SHA1 MIC, NIST AES Key Wrap
- Type
  - 0: Group Key
  - 1: Pairwise Key
- Index
  - 0 si Type = 1 (Pairwise)
  - 1 ou 2 si Type = 0 (Group)

Information Key

- Install: Envoyé que par AP
  - 0: Ne pas utiliser PTK pour protéger la couche supérieure
  - 1: utiliser PTK pour protéger la couche supérieure
- Ack: envoyé que par AP
  - 0: Don't reply
  - 1: Reply
- MIC:
  - 0: MIC non présent dans le message
  - 1: MIC présent dans le message

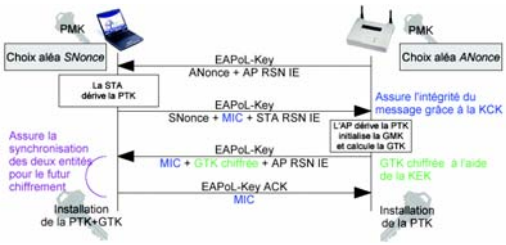
Information Key

- Secure: envoyé que par AP
  - 0: Initialization not yet complete
  - 1: Initialization complete
- Error: envoyé que par la station => indique TKIP MIC erreurs
- Request: envoyé que par la station pour demander une nouvelle clé
- Reserved: 0

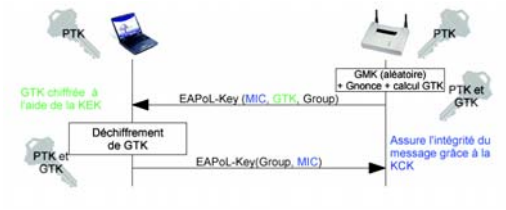
4-Way Handshake : Obtention de PTK

- Le 4-Way Handshake, initialisé par l'Access Point, permet de :
  - Confirmer de la connaissance de la PMK par le client
  - Générer une PTK à partir de la PMK
  - Installe des clés d'intégrité et de chiffrement
  - Transporter de manière sécurisée la GTK
  - Confirmer la suite de chiffrement utilisée

4-Way Handshake : Obtention de PTK

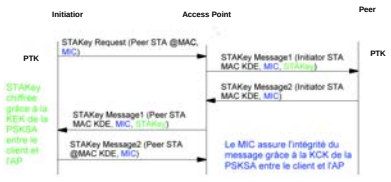


4-Way Handshake : Obtention de GTK



Handshake des clés entre stations

- *Créé une association de sécurité (STAKeySA) entre une station initiatrice (initiator) et une station distante (peer) au sein d'un même BSS*
- *LeHandshake est initié par la station*



Les antennes

- *Les antenne tige extérieure, souvent installée sur le toit:*
  - *omnidirectionnelle, son gain, 7 à 15 dBi, est lié à sa dimension verticale pouvant atteindre 2 m. Le gain (en émission) peut ne plus être compatible avec la PIRE autorisée.*
- *L'antenne panneau dite aussi plate (technologie interne antenne quad ou antenne patch, réseau de dipôles. Le gain commence vers 8 dBi (8 x 8 cm) pour atteindre 21 dBi (45 x 45 x 4.5 cm). C'est l'antenne qui présente le meilleur rapport gain/encombrement et aussi le meilleur rendement, qui tourne autour de 85 à 90 %.*
- *L'antenne type parabole pleine ou grille. Son intérêt d'emploi se situe dans la recherche du gain obtenu à partir d'un diamètre théorique d'approche suivant :*
  - *18 dBi = 46 cm, 19 dBi = 52 cm, 20 dBi = 58 cm, 21 dBi = 65 cm, 22 dBi = 73 cm, 23 dBi = 82 cm, 24 dbi = 92 cm, 25 dBi = 103 cm, 26 dBi = 115 cm, 27 dBi = 130 cm, 28 dbi = 145 cm, 29 dBi = 163 cm, 30 dbi = 183 cm.*
  - *Le rendement de la parabole est moyen, 45/55%.*
  - *Nota : n'importe quelle parabole (ex. TPS/CS sans tête 11-12 GHz) est exploitable en Wifi, à condition de prévoir une source adaptée : cornet, patch ou quad mono ou double, etc.*
- *L'antenne à fentes, sectorielle, à gain.*

- ***Les antennes à gain directionnelles ou omnidirectionnelles sont destinées à la « plus longue portée », possible, quelques kilomètres**.*
- ***Les antennes panneaux et paraboliques sont uniquement directionnelles, c'est-à-dire quelles favorisent une direction privilégiée (plus ou moins ouverte) au détriment d'autres non souhaitées**.*

