

# SECURITE SANS FIL

Alberto Escudero Pascual

# Contenu

- Partie I
  - Introduction à la sécurité wireless et à la sécurité des systèmes d'information
  - Rappel du model OSI et du cryptage au niveau liaison.
- Partie II
  - Cinq attributs de sécurité dans le contexte du WLAN

# Définition de la sécurité Wi-Fi

- Un concept général.
- Que touche le concept de sécurité?
- Une définition du concept dans le cadre du WLAN est nécessaire.
- Nous présenterons la sécurité dans le cadre plus large de la sécurité de l'information.

# Qu'est ce que la sécurité de l'information?

## COMSEC

- Selon COMSEC (Communication Security.)
- “Les mesures prises et les contrôles effectués pour refuser aux personnes non autorisées l'accès aux informations dérivées des télécommunications et pour assurer l'authenticité de telles télécommunications.”
- COMSEC introduit d'abord 2 concepts de sécurité:
  - Confidentialité.
  - Authentification.

# Confidentialité

**« Assurance que l'information n'est pas révélée aux personnes , aux processus, ou aux dispositifs non autorisés(protection contre la révélation non autorisée de l'information »**

# Authentication

“Une mesure de sécurité conçue pour établir la validité d'une transmission, d'un message, ou d'un expéditeur, ou un moyen de vérifier l'autorisation d'un individu de recevoir des catégories spécifiques d'information (Vérification de l'expéditeur).”

# Qu'est ce que la sécurité de l'information?

## COMPUSEC

- COMPUSEC : (80's) trois nouveaux concepts de sécurité:
  - Intégrité
  - Disponibilité
  - La non répudiation

# Intégrité

“La qualité d'un système informatique (IS), elle reflète l'exactitude et la fiabilité locales du système d'exploitation; la perfection logique du matériel et des logiciels mettant en application les mécanismes de protection; et l'uniformité des structures de données et de l'occurrence des données stockées...”

# Disponibilité

“Accès opportun et fiable aux données et services d'information pour les utilisateurs autorisés.”

# Non répudiation

« L'assurance comme quoi on fournit à l'expéditeur une preuve de la livraison des données et au destinataire une preuve de l'identité de l'expéditeur, ainsi ni l'un ni l'autre ne peuvent plus tard nier pour avoir traité les données. »

# La methodologie

**Quoi:** La sécurité sans fil du point de vue conceptuel.

**Pourquoi:** Présenter un approche méthodologique pour la conception de réseaux san fil sécurisés.

**Comment:** Les aspects conceptuels de la sécurité définis, la suite présentera comment implémenter ces concepts dans un réseau sans fil

# A revoir...

- Le model OSI et le WLAN
- Le cryptage au niveau liaison

# Le model OSI et la sécurité sans fil (rappels)

- Wlan => couches 1&2 de OSI
- Sécurité WLAN<=> cryptage sur le niveau liaison (MAC/LLC)
- La sécurité aux niveaux supérieurs n'incombe pas au 802.11 ( à la base)

# Cryptage au niveau liaison

- **Definition:** sécurisation du lien entre un ou pls communicants
- **Requis:** (clé secrete) partagée+ algorithme de cryptage

# Cryptage au niveau liaison

- Wired Equivalent Privacy (WEP) <>IEEE 802.11 (1999-2004)
- Wi-Fi Protected Access (WPA2).

# Cryptage au niveau liaison

- Pas de sécurité de bout-en-bout
- Doit être considéré uniquement comme une mesure supplémentaire de sécurité
- Demande plus de ressources à l'AP qu'un système de clé managée de façon centrale.

# Cinq attributs de sécurité dans le WLAN

- Confidentialité (WEP, WPA, WPA-PSK...)
- Authentification
- Intégrité
- Disponibilité
- Non-repudation

# Confidentialité : WEP

- WEP signifie "Wired Equivalent Privacy".
- Norme de cryptage implémentée dans la norme IEEE 802.11b/g (Wi-Fi)
- Il existe 2 puissances de chiffrement pour le cryptage WEP : 40, 64 bits (RC4).
- Le WEP fonctionne sur le principe du secret partagé, chaque éléments du réseau voulant communiquer entre eux doit connaître la clé secrète qui va servir au cryptage WEP. Une fois le WEP est mise en place, toutes les données obligatoirement cryptées

# WEP

## (faiblesses)

- L'université de Californie à Berkeley a démontré qu'il existait une faille de sécurité pouvant compromettre la confidentialité de données transmises sur le WLAN.
- Cette faille est "facilement" exploitable grâce à des logiciels tels que WEPCrack, fonctionnant sous Linux, et qui permettent de "sniffer" la clé secrète des clés WEP environ 3 heures en fonction du trafic.
- Il est préférable d'utiliser le WPA proposant une puissance de chiffrement nettement plus fiable.

# Confidentialité : WPA & WPA2

- Wi-Fi Protected Access (WPA) ratifié en 2004
- Mise à jour logicielle. Inclus l'AES en remplacement du RC4 .
- Fonctionnement avec ou sans clé managée

# Confidentialité : WPA & WPA2

- WPA sans management de clé=> (WPA-PSK)
- Avec un management de clé=> WPA2
- WPA2: Possibilité de clé dynamiques avec TKIP (Temporary Key Integrity Protocol)

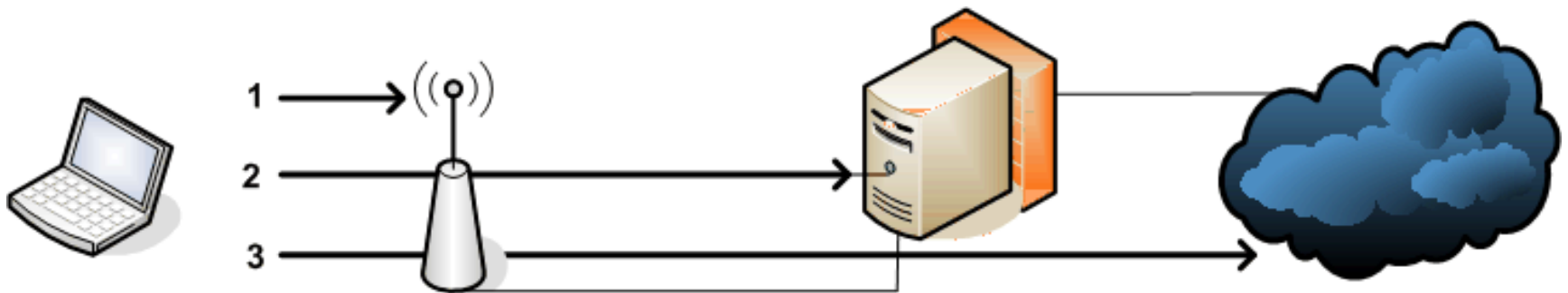
# Authentification

- Objectif: avoir le droit de transmettre des données à travers le point d'accès
- Processus:
  - Authentification ouverte sans clé
  - Authentification ouverte avec clé (clé partagée)
  - Authentification fermée (clé partagée)

# Authentification

## Recommendations:

- Système ouvert + clé.
- Décaler l'authentification au niveau des couches supérieures avec un "portail captif"



- Arrêt de diffusion du SSID
- Filtre MAC

# Intégrité

- Capacité de déterminer si les données ont été modifiées au cours de la transmission
- WEP contient le Code Redundancy Check (CRC)

**NON EFFICACE!**

# Intégrité

**Resultat** : Les données peuvent subir des modification sans aucnes notifications.

## **SOLUTION**

**WPA and WPA2** : Incluent le (MAC – cryptographic checksum) reconnu pour être réeement efficace.

# Disponibilité

- Interference radio de forte puissance => D.O.S
- Noeud cachés => Chute de la bande passante
- Virus
- Spam
- Logiciels P2P

# Conclusions

- La sécurité telle que définie par COMSEC
- Est implémentée sur les différentes couches du modèle OSI
- Si de la sécurité est nécessaire au niveau liaison: préférer WPA2. Aller vers 802.11 i dès que possible.
- Prévoir des mesures précises de contre réaction à chaque situation